Elementary Number Theory

Peter Hackman
HHH Productions

November 1, 2009

Contents

Preface

My last new assignment at Linköping University was to a course in Elementary Number Theory. While somewhat removed from my algebraic interests and competence, that course (which I conducted for five years) turned out to be an extremely rewarding and challenging experience, largely due to the enthusiasm of the students.

Never content to just copy text books, I put a lot of energy into finding new proofs, new ways of organizing the material, and some at least unusual topics. This quest for inspiration produced a lot of notes that I decided to compile into a short text on retiring from the University. As you might have guessed, the project grew into a full-size book.

What I hoped to contribute to the existing literature is a perhaps slimmer and more affordable volume. At the same time I wished to include some exciting and challenging, yet completely elementary, material not found in current texts.

"Elementary" means that almost no Analysis is used, and almost no "Abstract" Algebra. Algebra really becomes abstract only with the introduction of techniques like homomorphisms, direct sums and quotient constructions. We do, however, speak of (number) rings, fields, and residue classes of integers, and their arithemetic.

Among the more unusual material is a reasonably complete account of Cornacchia's algorithm for solving $x^2 + Dy^2 = p$, using Euclid's Algorithm, and that of Lagrange (revived by Matthews and Mollin) for $x^2 - Dy^2 = N$, using infinite continued fractions. There are strong analogies between the two theories, which I emphasize by using exactly the same wording in several parallel passages. Modular square roots is another of my favorite topics, and I present two algorithms for them, that of Berlekamp and the one using Lucas sequences (or, equivalently, Cipolla's algorithm) each exploiting some interesting theoretical item.

To keep the material within bounds I had to make some clear decisions what *not* to include. One main decision was to not give proofs of the statistics and complexity of algorithms. There are comprehensive accounts in the books by Riesel, Bach-Shallit, and Crandall-Pomerance cited in the Bibliography.

Another decision was to give fewer applications. The motivational value of applications does not depend on their quantity; besides, who wants to compete with such excellent texts (in Cryptography) as Trappe-Washington, or Buchmann? To be sure, almost all of the math relevant to these accounts, is included here. Whenever I found an application worthy of inclusion it was usually because it strengthened some of the main theoretical ideas of the text.

A few words about style. For the most part I stick to the strict Definition-Example-Theorem-Proof-Example format simply because I want to make it clear where things begin and end. Also, many readers (like me) will want to skip longer proofs on a first reading.

Having dabbled in journalism I try to paragraph and display often. I have also tried to minimize the number of cross-references. Further , by numbering everything in one sequence, and boxing theorems and definitions I hope to make it easier on the reader. As I never refer back to a subsection, these are un-numbered.

Finally, there is no numbering of equations, as reference to them is strictly local. They are labeled by one to three stars. I simply *hate* references like "we now return to the study of the differential operator (17) in Section XVII of Chapter Q" (that operator of course being the Laplacian).

Books are referred to by author name. Very few articles are cited; in these cases I give full reference in the text, but I have also collected them at the end of the text.

I strongly advocate the use of computers as a means of generating and investigating examples. To really understand an algorithm, or a result, it helps to program it. There are suggestions for computer projects, ranging in complexity from a few lines to maybe one or two pages.

Hopefully the suggested projects still allow the math to dominate over more delicate programming issues. Ideally much more work should be spent on checking and tracing, and varying the input and the parameters, than on devising the program. This text is *not* conceived as a book on "computational" number theory.

There are “suggestions for computing” sprinkled throughout the exercises, and the reader will often have the option to use programs of his own design or rely on existing packages, such as Maple, Mathematica, and PARI. To ascertain the feasibility of the algorithms to anyone with moderate programming experience I have written and run simple programs on just about any algorithm persented here,

In my courses students could choose their programming language freely (but multi-precision arithmetic is imperative). A very popular language is Python, which is the language I used in constructing and checking all my examples, and the tables at the end of the book.

You are never alone. Students, friends, and former colleagues helped and inspired me in several ways. Mikael Langer and Jan-Åke Larsson graciously aided the traumatic transition from Plain TeX to LaTeX. Hans Lundmark and Niels Möller read large chunks of the text and offered suggestions and corrections, immensely enhancing the readability of the text. Hans also helped me with a number of programming issues.

Pär Kurlberg (Erdös number two) read an early version of Chapter L, and offered valuable insights and comments. I am also grateful to him for introducing me to the Python programming language several years ago. I have also received valuable input and support from an email correspondence with Keith Matthews of Brisbane, Australia.

Finally, I wish to acknowledge the generous help from Thomas Bellman in explaining some of the mysteries of Python.

It is my hope that this text will give something back to the subject that brightened the last five years of my career.

Linköping, Sweden, October 2007,

Peter Hackman

Chapter A

Divisibility, Unique Factorization

A.I The gcd and Bézout

We assume you are familiar with the integers, their addition, subtraction, and multiplication. We will later introduce algebraic integers, especially complex integers. When we want to distinguish ordinary integers from more general ones we use the expression "rational integer".

We will make repeated use of division with remainder: Given integers $n > 0$, and m, there are (unique) integers q and r, $0 \leq r < n$, such that $m = qn + r$.

The existence of q, r is easily proved. The set of numbers $m - qn, q \in \mathbf{Z}$ contains non-negative numbers. If $m \geq 0$, m itself is one such number. If $m < 0$, pick $m - mn$. r is then chosen as the smallest non-negative number of the form $m - qn$. If $r \geq n$, then $m - (q+1)n$ is smaller and still non-negative, contradiction.

We have invoked the **Well-ordering Principle**:

"Every non-empty set of non-negative integers contains a smallest element."

On a few occasions we use the absolutely least remainder, satisfying $|r| \leq n/2$, or more precisely, $-n/2 < r \leq n/2$. If $m = qn + r$, $n/2 < r < n$, then also $m = (q + 1)n + (r - n)$, with $-n/2 < r - n < 0$.

We start with a very simple definition:

A.I.1 Definition. The integer m is a **factor of** the integer n, or m **divides** n, or n is **divisible by** m, if there is an integer q, satisfying $n = mq$.

Notation: $m|n$. The notation for "m does **not** divide n" is $m \nmid n$.

The number 0 is obviously divisible by any integer. If a divides m and n, then a also divides all rm, sn, $rm + sn$, for integers r, s.

A.I.2 Definition. The greatest common divisor of the two integers m, n (not both $=0$) is the greatest integer d which divides both. Notation: $d = (m, n)$ or $d = \gcd(m, n)$.

A.I.3 Example. $(8, -4) = 4$, $(7, 11) = (4, 9) = 1$. □

By convention $(0, 0) = 0$. In all other cases (m, n) is positive ("positive" in this text means "> 0").

For $m \neq 0$ obviously $(m, 0) = |m|$, the absolute value of m.

We have defined the greatest common divisor with reference to the usual *total* ordering of the integers.

More significantly, it is also the greatest common divisor according to the *partial* ordering of divisibility. That is, every other common divisor of m and n is not only smaller than $d = (m, n)$, but also divides it.

That is part c) of the following Theorem:

A.I.4 Theorem.

a) Let $d = (m, n)$. There are integers r, s such that $d = rm + sn$.

b) The linear Diophantine equation *$e = xm + yn$ is solvable in integers x, y if and only if $(m, n)|e$.*

c) Every common divisor of m, n divides their greatest common divisor.

Proof. We first show how b) follows from a). If $d = (m, n), d = rm + sn$, and $e = qd$, then $e = qrm + qsn$, proving one direction of the equivalence.

Conversely, assume $e = xm + yn$. Since $d = (m, n)$ divides $xm, yn, xm + yn$ it follows immediately that $d|e$. This was the easier direction, as we never used a).

For the proof of a) we can assume that $m, n \neq 0$. Let $d = rm + sn$ be the *least positive* number of that form. Such integers do indeed exist, e.g., $|m|, |n|$, and every non-empty set of positive integers has a smallest element.

We first show that d divides both m and n. Perform the division:

$$m = qd + t = q(rm + sn) + t; \quad 0 \leq t < d.$$

The remainder $t = (1 - qr)m - qsn$ is of the same form as d but smaller, and $t \geq 0$. The minimality of d thus forces $t = 0$, i.e., $d|m$.

In the same manner we show $d|n$. But *every* common factor of m, n obviously divides $d = rm + sn$. Therefore, d must be divisible by all common factors in m, n, hence d is the greatest among them. This finishes the proof of both parts a) and c) of the Theorem. □

Remark: The word *Diophantine* always refers to solvability in integers.

A.I.5 Definition. The integers $m, n \neq 0$ are **relatively prime** if $(m, n) = 1$, i.e., if their only common factors are ±1.

For relatively prime m, n, by the Theorem above, the equation $xm + yn = 1$, *Bézout's Identity*, is solvable in integers. Trivially, $xm + ny = 1$, for integers x, y, implies $(m, n) = 1$.

The *Euclidean Algorithm* is a very old and fast method for determining (m, n). If $m \geq n$, the number of bit operations required is quadratic in the number of bits in the binary representation of m. For detailed discussions of complexity questions of this kind I refer to more comprehensive texts in Number Theory.

We explain by example why Euclid gives the greatest common divisor. Then we redo our solution in a way that simultaneously, in the case $(m, n) = 1$, solves Bézout's identity.

A closer analysis of our Examples could be formalized into a computational proof of our previous Theorem.

A.I.6 Example (Euclidean Algorithm). Let us compute $(37, 11) = 1$. We start by dividing one number by the other:

$$37 = 3 \cdot 11 + 4.$$

By the principles we have used repeatedly above, each common factor of 37 and 11 is also one of 11 and $4 = 1 \cdot 37 - 3 \cdot 11$.

On the other hand, each common factor of 11 and 4 is one of $37 = 3 \cdot 11 + 1 \cdot 4$ and 4 as well. Hence, the two pairs $37, 11$, and $11, 4$, have the same common factors. In particular their greatest common divisors are the same.

The pattern continues:

$$\begin{aligned} 37 &= 3 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

whence

$$(37, 11) = (11, 4) = (4, 3) = (3, 1) = 1.$$

The following is a simple example with $(m, n) > 1$:

$$\begin{aligned} 77 &= 3 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

whence

$$(77, 21) = (21, 14) = (14, 7) = (7, 0) = 7.$$

□

Clearly, the gcd is the last non-zero remainder in this division scheme.

A.I.7 Example (Extended Euclid). We now show how to modify the algorithm so as to simultaneously solve Bézout ("Extended Euclidean Algorithm"). We start with two relations no one could possibly challenge:

$$\begin{aligned} 1\cdot 37 + 0\cdot 11 &= 37\\ 0\cdot 37 + 1\cdot 11 &= 11. \end{aligned}$$

We then divide the first right member by the second: $37 - 3\cdot 11 = 4$ and perform the corresponding row operation: "equation 1 minus 3 times equation 2".

We arrive at $1\cdot 37 - 3\cdot 11 = 4$.

We now drop the first equation above and add the one just derived:

$$\begin{aligned} 0\cdot 37 + 1\cdot 11 &= 11\\ 1\cdot 37 - 3\cdot 11 &= 4 \end{aligned}$$

These we combine in the same way as above. Divide: $11 - 2\cdot 4 = 3$. Form "(new) equation 1 minus 2 times (new) equation 2", yielding $-2\cdot 37 + 7\cdot 11 = 3$. After one more step we arrive at:

$$\begin{aligned} 1\cdot 37 + 0\cdot 11 &= 37 & &\\ 0\cdot 37 + 1\cdot 11 &= 11 & 37 - 3\cdot 11 &= 4\\ 1\cdot 37 - 3\cdot 11 &= 4 & 11 - 2\cdot 4 &= 3\\ -2\cdot 37 + 7\cdot 11 &= 3 & 4 - 3 &= 1\\ 3\cdot 37 - 10\cdot 11 &= 1 & & \end{aligned}$$

and we have solved Bézout! □

Note that each step only requires that the coefficients of two equations be stored. After division, the first equation is dropped, the second equation moves to the top, and a new equation takes its place. The algorithm is eminently programmable.

A.I: Exercises

1. Solve Bézout for each of the following pairs: (17,29), (33,81), (48,81).

2. Using the identity $X^{nd}-1=(X^d-1)(X^{(n-1)d}+X^{(n-2)d}+\cdots+1)$, determine the gcd's $(2^{15}-1,2^3-1)$, $(2^{10}-1,2^{15}-1)$, $(2^{15}-1,2^9-1)$, or, quite generally, $(2^m-1,2^n-1)$. If you represent these numbers in binary, what will Euclid look like?

3. Let m,n be integers. Show that

$$(m,n)=\left(\frac{m-n}{2},n\right) \text{ if both are odd.}$$

What can be said about $(2m,2n)$, and $(2m,n)$, assuming n odd in the second case?

From these observations, devise an alternative Euclidean algorithm using no divisions (division by 2 is a right shift in binary representation, checking parity is a bitwise "and" with 1).

A.II Two Divisibility Theorems

We will make repeated use of the following two Divisibility Theorems. Note the decisive role played by Bézout.

A.II.1 Theorem (First Divisibility Theorem). *If* $m|ab$, *and* $(m,a)=1$, *then* $m|b$.

Proof. Bézout gives us x,y with $xm+ya=1$. Multiplication by b yields $b=bxm+yab$. The terms of the right member are divisible by m, the first one trivially, the second one by asssumption. Hence m divides their sum, i.e., $m|b$. □

A.II.2 Theorem (Second Divisibility Theorem). *If both* m,n *divide* a, *and* $(m,n)=1$, *then their product* mn *divides* a.

Proof. The divisibility assumptions may be written $n|a=qm$. We are also assuming $(m,n)=1$. The previous Theorem immediately gives $n|q$, hence $mn|mq=a$. □

A.II: Exercises

1. If x divides my, ny, and $(m,n)=1$, then x divides y.

2. Let a,b be relatively prime integers. Suppose $x_0a+y_0b=1$. Find the general solution to the linear Diophantine equation $xa+yb=1$. Then generalize to the situation $(a,b)=d>1$.

3. Suppose the positive integers m,n satisfy $n^3+n=m^4$. Show that m,n are even; hence or otherwise, $16|n$.

4. The polynomial $f(X)=a_0X^d+a_1X^{d-1}+\cdots+a_d$ has integer coefficients. Let $X=p/q$, $(p,q)=1$, be a rational root. Show that $p|a_d$, and $q|a_0$. Hint: rewrite the relation $f(p/q)=0$ as a relation between integers.

5. A common way of factoring a number is to write it as a difference of two squares: $a^2 - b^2 = (a+b)(a-b)$.

(a) Let h be an odd positive integer. Show that

$$\frac{2^{4k+2}+1}{5}, \quad k > 1, \text{ and } 3^{2h+2} + 3^{h+1} + 1$$

are composite. Hint: $a^2 + b^2 = (a+b)^2 - 2ab$.

(b) In the case of the first number of the previous item, you will be able to decompose $2^{4k+2}+1$ into two factors one of which is divisible by 5. Which of them? The answer will depend on the remainder of k on division by some small positive integer. Determine the cases.

(c) Show that $a^2 + 4^a$ is composite, if a is an odd positive integer > 1 (trivial for even a).

A.III Unique Factorization

We recall a familiar concept.

A.III.1 Definition. A **prime number** is an integer $p > 1$ divisible only by the trivial factors ± 1 and $\pm p$.

The set of prime numbers is infinite. If $p_1 < p_2 < \cdots < p_d$ are prime numbers, then the smallest divisor $p > 1$ of $1 + p_1 p_2 \cdots p_d$ is a prime number different from all of these.

Lest you jump to conclusions, note that $1+2\cdot3\cdot5\cdot7\cdot11\cdot13 = 30031 = 59\cdot509$ is composite.

You will be familiar with the following results, but maybe not with their proofs.

A.III.2 Theorem (Prime Factorization, Existence). *Every integer $n > 1$ is a product of prime numbers.*

Proof. Induction on n. Let p be the smallest divisor > 1 of n. It is a prime number. If $p = n$ we are through. Otherwise we apply induction to the quotient $1 < n/p < n$. □

The uniqueness part is preceded by a little Lemma, a special case of our First Divisibility Theorem (A.II.1).

A.III.3 Lemma. *Let q be a prime number, a, b integers. Assume that q divides their product ab. Then q divides either a or b.*

Proof. If q does not divide a, then $(q, a) = 1$ is the only possibility. The First Divisibility Theorem then immediately gives $q|b$. □

A.III.4 Corollary. *If $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ is a prime factorization of n, and the prime number q divides n, then q equals one of the p_j's.*

Proof. If $k = 1$, then obviously $q = p_1$. If $k > 1$, and $q \neq p_1$, then q divides $p_2 \cdots p_k$ and we can proceed by induction on k. □

A.III.5 Theorem (Unique Factorization). *The prime factorization of $n > 1$ is unique, up to the order of the factors.*

Proof. Suppose $n = p_1 \cdots p_k = q_1 \cdots q_l$, $k \leq l$, are two prime factorizations of n. If $k = 1$, then n is a prime number, and obviously $l = 1, q_1 = p_1$.

If $k > 1$, then q_1 equals one of the p_j's, say $q_1 = p_j$, by the Corollary. Dividing both members by this common factor we are reduced to studying the shorter factorizations of n/p_j, and the result now follows by induction on k. □

A.III: Exercises

1. If $u, v, x > 0$ are integers, $(u, v) = 1$, and $uv = x^2$, then u, v, too, are perfect squares. Can you prove this without using unique factorization in prime factors? Generalize to arbitrary powers.

2. Let a, b be positive integers satisfying $a^j = b^k$ for positive and relatively prime integers j, k. Show that $a = r^k$, $b = r^j$ for some positive integer r.

3. Let p be a prime number, n a positive integer. Let $v_p(n)$ denote the largest integer $k \geq 0$ such that $p^k | n$. Further, let the *floor* $\lfloor a \rfloor$ denote the largest integer $m \leq a$.

(a) Express the number of integers m, $1 \leq m \leq n$, divisible by p, as a floor.

(b) Express $v_p(n!)$ as a sum of floors.

(c) Find the number of final zeros, $v_5(n!)$, for $n = 2006$.

4. Pythagorean triples. Suppose x, y, z are positive integers satisfying $x^2+y^2 = z^2$. Suppose also that they are without common factors > 1, forcing them to be pairwise relatively prime. We say that x, y, z is a *proper*, or *primitive*, Pythagorean triple.

Suppose further, as we may, that x is odd, and y is even. From the relation $(z-x)(z+x) = y^2$ deduce a parametric representation of all proper Pythagorean triples x, y, z. Start by determining $(x+z, z-x)$.

(You may wish to connect this with the rational representation of the points on the circle $x^2 + y^2 = R^2$ obtained by intersecting the circle with a line through the point $(-R, 0)$ of given rational slope – your parameters will have a familiar trigonometric interpretation.)

5. Let $a_0, a_1, \ldots, a_{n-1}$ be given (positive) distinct integers. Show that there are (positive) integers D, E such that the numbers $Da_j + E$ are pairwise relatively prime.

Hint: If p is a prime dividing two of the numbers Da_j+E, then it also divides their difference. Construct D as the product of certain prime numbers, and let E be some other prime.

A.IV Residue Classes, Congruences

A.IV.1 Definition. We fix an integer $n > 0$. **The (residue) class of** m, **modulo** n, denoted $[m]$, or $m + (n)$, is the set of all numbers of the form $m + rn, r \in \mathbf{Z}$.

Note that the class symbol $[m]$ contains no reference to the given integer, the *modulus* n. Some writers affix a subscript n to the class symbol in case of ambiguity. In that case I prefer the notation $m + (n)$. For one thing, it is easier to type.

The class of zero, modulo 3, is $[0] = \{\dots, -12, -9, -6, -3, 0, 3, 6, \dots\}$ consisting of all multiples of 3. You can think of them as equidistant points on the line, 3 units apart. Each of the numbers is said to *represent* the class.

The class of 1,

$$[1] = \{\dots, -11, -8, -5, -2, 1, 4, 7, \dots\},$$

is obtained by shifting the zero class one step to the right along the line. It consists of the numbers that yield the remainder 1, on division by 3.

Another shift to the right gives us the class

$$[2] = \{\dots, -10, -7, -4, -1, 2, 5, \dots\}.$$

These are the numbers yielding the remainder 2 on division by 3.

A third shift gives us back the class $[3] = [0]$.

For general $n > 0$ we obtain n different, and pairwise disjoint, classes

$$[0], [1], [2], \dots, [n-1].$$

Shifting one class n unit steps in either direction gives us back the same class.

Each integer belongs to exactly one class modulo n. We say that the n classes constitute a *partition* of the set $\mathbf{Z}$.

Those who have taken a course in Discrete Math will ask, what is the *equivalence relation* belonging to this partition. More concretely, the question is: when (for given $n > 0$) is $a + (n) = b + (n)$?

Equality clearly holds if and only if either of a and b belongs to the class of the other, i.e., if a and b differ by a multiple of n.

Another way of expressing this condition is that n divide the difference: $n|(a-b)$.

A third way of phrasing the condition is that a and b leave the same remainder on division by n.

We introduce a name and notation for this condition.

A.IV.2 Definition. The integers a and b are **congruent modulo** n if $n|(a-b)$. Notation: $a \equiv b \pmod{n}$.

Anyone familiar with the concept (from Discrete Math) verifies easily that this is indeed an *equivalence relation* (symmetric, transitive, reflexive). Others can safely ignore the issue.

More important is the fact that we can do arithmetic on classes.

A.IV.3 Lemma. *Fix* $n > 0$. *Assume* $a_1 \equiv b_1 \pmod{n}$, $a_2 \equiv b_2 \pmod{n}$. *Then* $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n}$ *and* $a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{n}$.

Proof. We content ourselves with proving the second property – the first one is even easier.

We are assuming that $n|(a_1 - b_1)$ and $n|(a_2 - b_2)$. Then n also divides $a_1a_2 - b_1b_2 = a_2(a_1 - b_1) + b_1(a_2 - b_2)$. □

In words, the Lemma just proved states that the class of a sum, difference, or product of two numbers depends only on the class of the terms or factors.

Therefore the following definition is meaningful:

A.IV.4 Definition.

$$[a] \pm [b] = [a \pm b]; \qquad [a] \cdot [b] = [a \cdot b].$$

As the arithmetic operations are derived from operations on integers one easily proves that the usual laws hold. Addition and multiplication are *commutative* (independent of the order of the terms or factors). They are *associative* (no need for parentheses). And we have a *distributive law*:

$$[a]([b]+[c]) = [a][b]+[a][c].$$

A.IV.5 Example. Most of the time we want to represent our classes by the numbers $0, 1, \dots n-1$. Adding, subtracting or multiplying two representatives usually leads outside this set; we remedy this by dividing by n and keeping the remainder.

For our first set of examples we fix $n = 8$. Then

$$[4]+[6] = [10] = [2]; \quad [4]\cdot[6] = [24] = [0]; \quad [5]\cdot[9] = [45] = [5],$$

as $45 = 5 \cdot 8 + 5$. Finally, $[5]\cdot[5] = [25] = [1]$.

In the second example the multiplication of two non-zero classes yields the zero class. We say that the non-zero classes [4] and [6] are *zero-divisors.* If the product of two classes equals [1] they are said to be *inverses* of one another; the two classes are then *invertible.* For $n = 8$ the classes of 1,3,5,7 are their own inverses.

For $n = 7$ all non-zero classes are invertible:

$$[1]\cdot[1] = [1]; \quad [2]\cdot[4] = [1]; \quad [3]\cdot[5] = [1]; \quad [6]\cdot[6] = [1].$$

Notation ($n = 7$): $[3]^{-1} = [5]$; $[5]^{-1} = [3]$. We sometimes use the notation a^{-1} for a representative of the class $[a]^{-1}$.

□

Let us record the formal definitions:

A.IV.6 Definition.

a) The class $[a]$ modulo $n > 0$ is **invertible** if there exists a class $[b]$ satisfying $[a][b] = [1]$.

b) The class $[a] \neq [0]$ is a **zero-divisor** if there exists a class $[b] \neq [0]$ satisfying $[a][b] = [0]$.

How do we recognize invertible classes and zero-divisors?

A.IV.7 Theorem. *Fix $n > 0$. The class $[m] = m + (n)$ is invertible if and only if $(m, n) = 1$.*

Proof. The relation $[r][m] = [1]$ is equivalent to $n|(rm - 1)$, i.e., to the existence of an integer s with $sn = rm - 1, \quad rm - sn = 1$. Therefore the inverse $[r]$ exists if and only if there are integers r, s such that $rm - sn = 1$, i.e., if and only if $(m, n) = 1$. □

A.IV.8 Corollary. *For a prime number n* all *non-zero classes modulo n are invertible.*

□

We have already seen the example $n = 7$.

The proof is constructive. Inverse classes may be computed by solving Bézout, (A.I.7), i.e., by performing the Extended Euclidean Algorithm.

A.IV.9 Example. Fix $n = 37$. Let us determine the inverse class to [11] (modulo 37).

In an earlier example we solved Bézout:

$$3 \cdot 37 - 10 \cdot 11 = 1, \quad -10 \cdot 11 \equiv 1 \pmod{37}.$$

At the class level this translates to $[11][-10] = [1]$. This gives us our inverse class $[11]^{-1} = [-10] = [27]$. □

An invertible class cannot be a zero-divisor. For if $[r][m] = [1]; [q][m] = [0], [q] \neq [0]$, then $[0] \neq [q] = [q][1] = [q][r][m] = [r][0] = [0]$, contradiction.

Our next result therefore shows that each non-zero class is *either* invertible *or* a zero-divisor.

A.IV.10 Theorem. *n as before. The class $[m] \neq [0]$ is a zero-divisor if and only if $(m, n) > 1$.*

Proof. We already know "only if": a zero-divisor $[m]$ is non-invertible, i.e., $(m, n) > 1$.

For the "if" part, suppose $(m, n) = d > 1$. We then have

$$m \cdot \frac{n}{d} = n \cdot \frac{m}{d}$$

so the product in the left member is divisible by n.

At the class level we therefore get:

$$[m] \cdot [\frac{n}{d}] = [0].$$

The second factor is clearly not the zero class; since $d > 1$, $n/d < n$ is not divisible by n. □

A.IV.11 Example. This time we let $n = 15 = 3 \cdot 5$. The invertible classes are those $[m]$, $0 < m < n$, for which $(m, n) = 1$, i.e., for which m is divisible by neither 3 nor 5, i.e., the classes of 1, 2, 4, 7, 8, 11, 13, 14;. In fact:

$$[1] \cdot [1] = [2] \cdot [8] = [4] \cdot [4] = [7] \cdot [13] = [11] \cdot [11] = [14] \cdot [14] = [1].$$

(note, e.g., that

$$[14][14] = [-1][-1] = [1]; \quad [11][11] = [-4][-4] = [16] = [1].)$$

The remaining classes are zero-divisors. If m is divisible by 3, multiplication by $[5]$ yields the zero class. If m is divisible by 5, we multiply by $[3]$ to get the zero class. For instance, $[10][3] = [0]$. □

We will move back and forth between class notation and congruences, choosing whatever seems more convenient at the moment. Congruence notation is often preferable when several different moduli are involved.

We will use the following simple idea repeatedly:

A.IV.12 Lemma (Cancellation). *If* $ac \equiv bc \pmod{n}$, *and* $(c, n) = 1$, *then* $a \equiv b \pmod{n}$

Proof. At the class level we are assuming $[a][c] = [b][c]$, and $[c]$ invertible. Multiplying the equation by $[c]^{-1}$ gives $[a] = [b]$. □

A.IV.13 Example (Tournaments). We want to schedule a tournament involving 10 teams, numbered $0, 1, \ldots, 9 = N$. The tournament is to be in 9 rounds, each team playing in each round and meeting every other team exactly once.

A classical scheme is the following. Order the 10 teams in circular fashion like this:

$$\begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ 9 & 8 & 7 & 6 & 5 \end{array}$$

This setup represents round number 0. The team in the top row plays the team below it, e.g., teams 3 and 6 meet in the zeroth round.

We now fix the zero in its place and shift the other numbers cyclically counterclockwise:

$$\begin{array}{ccccc} 0 & 2 & 3 & 4 & 5 \\ 1 & 9 & 8 & 7 & 6 \end{array}$$

This will be round number 1. Another cyclic shift, still fixing the zero, gives us round number 2:

$$\begin{array}{ccccc} 0 & 3 & 4 & 5 & 6 \\ 2 & 1 & 9 & 8 & 7 \end{array}$$

The process is repeated. After eight shifts we get:

$$\begin{array}{ccccc} 0 & 9 & 1 & 2 & 3 \\ 8 & 7 & 6 & 5 & 4 \end{array}$$

and this is to be our round number 8, the final round. The next cyclic shift will bring back the original arangement.

The reader is invited to devise his or her graphical explanation why this scheme works, that is, why no team plays any other team more than once.

Here we offer our explanation in terms of the modulo-calculus. The crucial fact is that 9 is odd, so that $(2,9)=1$, i.e., the class $2+(9)$ is invertible. (Explicitly, the inverse class of $2+(N)$, N odd, is $(N+1)/2+(N)$.)

Obviously team 0 meets every other team exactly once; it meets team r, $r<9$, in round r, and team 9 in round 0.

Now look at a number in some other fixed position in the upper row. Call it m. After a cyclic shift it is replaced either by $m'=m+1$ or (if $m=9$) by $m'=1=m-8$, that is, $m'\equiv m+1 \pmod 9$. The same goes for the number n just below it, it is replaced by n', where $n'\equiv n+1 \pmod 9$. The sum, $s=m+n$, thereby changes into $s'\equiv s+2 \pmod 9$.

As the sum in round 0 is $\equiv 0 \pmod 9$, the sum in round r, $0\le r\le 8$, is $\equiv 2r \pmod 9$.

So here is how we devise our tournament. In round m, team m opposes team 0 (except team 9 opposes team 0 in round 0, note that $9\equiv 0 \pmod 9$.)

In round r, $r\neq m$, team m opposes the unique team n satisfying

$$m+n\equiv 2r \pmod 9. \tag{$*$}$$

In order to justify this, we first note the symmetry of the condition. If team m plays team n, then certainly team n plays team m by (*).

Also, each team $m\neq 0$ meets team 0 exactly once.

Team $m\neq 0$ is never scheduled to meet itself. For if $n=m$, then $2m\equiv 2r \pmod 9$. As 2 is invertible modulo 9, this means $m\equiv r \pmod 9$, $m=r$. But in (*) we are assuming $r\neq m$.

Team $m, 0<m<9$, gets to play every other team n, $0<n<9$, exactly once. We prove this by determining which round: simply solve $2r\equiv m+n \pmod 9$, multiplying again by the inverse of 2 modulo 9. The solution (in this case $r\equiv 5(m+n) \pmod 9$) is unique modulo 9, hence r, $0\le r\le 8$, is uniquely determined.

The reader will note that we never used $N=9$ except in the explicit Example above. It could be any odd positive number. □

A.IV: Exercises

1. Determine, whenever possible, the inverses of 11, 25, 26, modulo 1729. (Short hand calculation.)

2. Verify that the classes of 11, 20 modulo 73 are inverses of one another. Run Extended Euclid for the two pairs (73,20), (73,11). Do you see a pattern? Can you explain it?

3. Let a, b be relatively prime integers.

(a) Show that $(a + 2b, 2a + 3b) = 1$.

(b) Show that $(a + 2b, 2a + b) = 1$ or 3. Exemplify the two cases!

(c) Can you generalize to $(pa + qb, ra + sb)$, $ps - qr \neq 0$?

4. Verify that $10^k \equiv 1 \pmod 9$ for all positive integers k. Use this fact to explain the divisibility test known as "casting out nines", using the sum of the digits to check divisibility by 3 or 9.

Then, by computing the residues of 10^k modulo 11, devise a similar test for divisibility by 11.

Then suggest a simple test for detecting errors in multiplying two integers.

5. Can you find a test for divisibility by 13 and 7? Hint: Look at 10^3.

6. (a) Find those n that can be expressed as $n \equiv x^2 \pmod 7$, and $\pmod 8$, respectively.

(b) Find those n that can be expressed as $n = x^2 + y^2 \pmod 8$, x, y integers.

(c) Let $f(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d$ be a polynomial with integer coefficients. Show that f has no integer roots if the constant a_d and the sum of the coefficients are both odd.

(d) Show that $x_1^3 + x_2^3 + x_3^3 \equiv 0 \pmod 9$ implies that at least one $x_i \equiv 0 \pmod 3$.

(e) Show that numbers $n \equiv 7 \pmod 8$ cannot be expressed as a sum of three squares.

(f) More generally, show the same for all numbers of the form $4^k(8n + 7)$. (A difficult theorem by Gauß states that all other positive integers are sums of three squares).

7. (a) Assume that the prime number $p \neq 2, 7$ can be be expressed as $p = a^2 + ab + 2b^2$, a, b integers. Show that $p \equiv 1, 2$, or $4 \pmod 7$. **Very useful trick:** multiply by 4 and complete the squares.

(b) Assuming $p = a^2 + ab + 2b^2$, show that $p = u^2 + 7v^2$, u, v integers. Hint: Use previous exercises to show that b is even.

8. (a) Find all integer solutions to $a^2 - ab + b^2 = 1$. Hint: Multiply by 4, and complete the squares.

(b) Assume that the prime number $p > 3$ can be expressed as $p = a^2 - ab + b^2$. Show that $p \equiv 1 \pmod 3$.

(c) Assume that the integer m can be expressed as $m = a^2 - ab + b^2$, a, b integers. Show that it can also be expressed as $m = x^2 + 3y^2$, x, y integers. Distinguish the cases a or b even, and a, b both odd.

(d) Assume that the integer m can be expressed as $m = a^2 + ab - b^2$, a, b integers. Show that it can also be expressed as $m = x^2 - 5y^2$, x, y integers. Distinguish the cases a or b even, and a, b both odd.

9. Let $a > 1$ be an integer. Prove that

$$\left(a - 1, \frac{a^d - 1}{a - 1}\right) = (a - 1, d)$$

by noting, for instance, that $a^k \equiv 1 \pmod{a - 1}$.

Then state and prove a similar statement about

$$\left(a - b, \frac{a^d - b^d}{a - b}\right).$$

10. There are infinitely many prime numbers $\equiv 3 \pmod 4$. Assume the contrary. Let P be the product of all prime numbers $\equiv 3 \pmod 4$ and derive a contradiction by studying the prime factors of $4P + 3$.

Similarly, prove that there are infinitely many primes $\equiv 5 \pmod 6$, and $\equiv 2 \pmod 3$.

11. N is an odd number. Can $1 + N^2$ be a perfect square? Or a cube? Or an arbitrary perfect (positive) power? Hint: look at a suitable congruence.

12. Let m, n be positive integers.

(a) Show that the congruence $x^2 - y^2 = (x + y)(x - y) \equiv m \pmod n$ is unsolvable in integers if $4|n$ and $m \equiv 2 \pmod 4$.

(b) Show that it is solvable if m or n is odd (in the first case the *equation* $x^2 - y^2 = m$ is solvable!)

(c) After these warm-ups, prove that $x^2 - y^2 = (x+y)(x-y) \equiv m \pmod n$ is solvable *if and only if* $4 \nmid n$ *or* $m \not\equiv 2 \pmod 4$.

13. **Suggestions for computing:** Extended Euclid, solving Bézout, finding modular inverses. You may also want a very simple routine computing only the gcd of two integers.

A.V Order, Little Fermat, Euler

The concept of order is basic to several primality tests. We often relate the order of a class to the *Euler Function* so we give its definition right away.

A.V.1 Definition. The **Euler Function**, denoted ϕ, is defined by the following, for positive integers n:

For $n = 1$, $\phi(1) = 1$.

For $n > 1$, $\phi(n)$ is the number of invertible classes modulo n; in other words, the number of integers m, $0 \leq m \leq n-1$, satisfying $(m, n) = 1$.

A.V.2 Example. By one of the last results of the previous Section (Corollary A.IV), $\phi(p) = p - 1$ for all prime numbers p, as all non-zero classes are invertible.

For a prime power $n = p^k$ start by noting that $(m, n) > 1$ if and only $p|m$. So we start with the p^k classes and delete those corresponding to multiples of p. There are $p^k/p = p^{k-1}$ of these, so $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

We have studied $n = 15$ in an earlier example. The non-invertible classes correspond to multiples of 3 and 5. There are 5 multiples of 3 between 0 and 14, and 3 multiples of 5. So we delete these, and put back the zero class which we deleted twice: $\phi(15) = 15 - 5 - 3 + 1 = 8$.

The invertible classes are, once again, $[1], [2], [4], [7], [8], [11], [13], [14]$. □

In the context of the Chinese Remainder Theorem (B.I.4) we will prove a result enabling us to compute $\phi(n)$ once we know the prime factorization of n.

A.V.3 Definition. Fix the positive integer n. The **order of m modulo n**, denoted

$$\mathrm{ord}_n(m),$$

is defined as the least positive exponent d for which

$$[m]^d = [1].$$

If clear from the context, the subscript n may be omitted.

The *existence* of such an exponent will be proved presently. Before we give the proof, let us give the orders of the invertible classes modulo 15:

A.V.4 Example.

a	1	2	4	7	8	11	13	14
$\operatorname{ord}_{15}(a)$	1	4	2	4	4	2	4	2

Note, for instance, that

$$7^2 \equiv 49 \equiv 4 \pmod{15}; \qquad 7^3 \equiv 13 \pmod{15}; \qquad 7^4 \equiv 1 \pmod{15}.$$

□

The following Theorem gives the basic facts about the order concept. It will be convenient to define negative powers of an invertible class. For positive k, set $[a]^{-k} = ([a]^{-1})^k$, a positive power of the inverse class.

A.V.5 Theorem (Main Theorem on Order). *Fix $n > 0$, let $[a]$ be an invertible class modulo n, i.e., $(a, n) = 1$. Then:*

a) There is at least one exponent $d > 0$ for which $[a]^d = [1]$.

b) Let d denote the least positive exponent with that property. Then:

$$[a]^e = [1] \Longleftrightarrow d|e.$$

c) For integers j, k,

$$[a]^j = [a]^k \Longleftrightarrow j \equiv k \pmod{d}.$$

Proof. a) As there are a finite number of classes, there are exponents $0 \leq j < k$ for which $[a]^j = [a]^k = [a]^j \cdot [a]^{k-j}$. Multiplying by (the negative power) $[a]^{-j}$ yields $[1] = [a]^{k-j}$, $k - j > 0$

b) Divide: $e = qd + r, 0 \leq r < d$. We then have $[1] = [a]^e = ([a]^d)^q \cdot [a]^r = [1]^q \cdot [a]^r$, i.e., $[a]^r = [1]$. The minimality of d forces $r = 0$, whence $d|e$.

c) By the same argument as in part a), the assumption implies $[a]^{k-j} = [1]$. Part b) then gives $d|(k-j)$ as desired. □

If we know that some power of a class equals [1] we need not compute every positive power below it in order to determine the true order:

A.V.6 Theorem. *Fix the modulus $n > 0$. Suppose $[a]^d = [1]$ for some positive exponent d. Then $d = ord_n(a)$ if and only if*

$$[a]^{d/q} \neq [1]$$

for all prime factors q in d.

Proof. Denote the true order by k. We know by the previous Theorem that $k|d$. If $k < d$, then by unique factorization some prime factor q in d is missing in k (or appears with lower multiplicity), i.e., k divides d/q for that factor.

Then, contrary to our assumption, $[a]^k = [1]$ yields $[a]^{d/q} = [1]$. This contradiction proves the Theorem. □

A.V.7 Example. One simple example is offered by the prime number $n = 13$. We will presently see ("Little Fermat") that all invertible classes modulo 13 have orders dividing $13 - 1 = 12 = 2 \cdot 2 \cdot 3$.

To check whether a class $[a]$ has order 12, we need therefore only compute $[a]^{12/2}$ and $[a]^{12/3}$. For instance, $[2]^6 = [12] = [-1]$; $[2]^4 = [3]$, so $\mathrm{ord}_{13}(2) = 12$.

As we have not proved Little Fermat yet we had better check $[2]^{12} = [1]$ as well: $[2]^{12} = ([2]^6)^2 = [-1]^2 = [1]$. □

Fermat's Little Theorem is a special case of Euler's Theorem, to be proved below. As it allows an independent proof we give that first. (Those familiar with elementary Group Theory from a course in Abstract Algebra will recognize Fermat and Euler as special cases of Lagrange's Theorem on orders of subgroups.)

A.V.8 Lemma ("Freshman's Dream"). *Let p be a prime number, a, b integers. Then*

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

Proof. We refer to the Binomial Theorem. The expansion of $(a+b)^p$ consists of terms of the form

$$\binom{p}{k} a^k \cdot b^{p-k}; \quad \binom{p}{k} = \frac{p!}{k!(p-k)!}; \qquad 0 \leq k \leq p.$$

If $0 < k < p$ the numerator contains the prime factor p which does not cancel, as it does not appear in either factor of the denominator. So all binomial coefficients except the first and the last are divisible by p. This proves that the two members of the stated congruence differ by a multiple of p. □

A.V.9 Theorem (Fermat's Little Theorem). *Let p be a prime number*

a) For any integer a,

$$a^p \equiv a \pmod{p}.$$

b) If $p \nmid a$, i.e., if $[a]$ is invertible, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

c) For invertible $[a]$, $\mathrm{ord}_p(a) | p-1$.

Proof.

a) It is enough to prove this for $0 \leq a \leq p-1$. Writing $a = 1 + 1 + \cdots + 1$, and using the Lemma repeatedly, we get

$$a^p \equiv (1+1+\cdots+1)^p \equiv 1^p + 1^p + \cdots + 1^p \equiv a \pmod{p}.$$

b) At the class level we can write part a) as $[a]^p = [a]$. Multiplying both members by $[a]^{-1}$ gives $[a]^{p-1} = [1]$ which is the class formulation of b).

c) This follows immediately from part b) and the Main Theorem. □

We now turn to the general theorem. First a useful little Lemma:

A.V.10 Lemma. *Fix the integer $n > 0$. Let $f = \phi(n)$ and let $a_1, a_2, \ldots, a_f$ represent all the f invertible classes modulo n. Suppose $(a, n) = 1$. Then the products $aa_1, aa_2, \ldots, aa_f$ also represent all the invertible classes modulo n.*

Proof. There are two things to prove. The first is that the classes $[aa_j]$ are indeed invertible. The second is that they are all different.

If the classes $[x], [y]$ are invertible, $[x][r] = [1]$, $[y][s] = [1]$ then so is their product: $[x][y][r]|s] = [1]$. That takes care of the first part.

For the second part, assume that $[a][a_j] = [a][a_k]$. Multiplying both members by $[a]^{-1}$ immediately gives $[a_j] = [a_k]$. So different $[a_j]$ produce different $[aa_j]$. □

A.V.11 Example. Let $n = 15$, $a = 7$. Then:

$[a_j]$	1	2	4	7	8	11	13	14
$[aa_j]$	7	14	13	4	11	2	1	8

The second row is a re-ordering of the first. □

A.V.12 Theorem (Euler's Theorem). *Let $n > 0$ as before. The order of each invertible class modulo n is a factor in $\phi(n)$, in other words:*

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \textit{for } (a, n) = 1.$$

Proof. Let f, $a_1, a_2, \ldots, a_f$ be as in the Lemma. The Lemma gives:

$$[a_1][a_2]\cdots[a_f] = [aa_1][aa_2]\cdots[aa_f],$$
$$[a_1][a_2]\cdots[a_f] = [a^f][a_1][a_2]\cdots[a_f].$$

Multiplying both members by the inverse classes of all the $[a_j]$, we are left with $[a]^f = [1]$, as claimed. □

A.V.13 Example. We have seen that $\phi(15) = 8$. Therefore each invertible class modulo 15 has an order dividing 8. We tabulated the orders at the beginning of this Section; they were 1, 2, or 4.

For the prime number 7 the theoretical maximum, $\phi(7) = 7 - 1 = 6$, is indeed achieved, by $a = 3, 5$ (their classes are inverses of one another). For instance, $3^2 \equiv 2 \not\equiv 1 \pmod 7$; $3^3 \equiv 6 \not\equiv 1 \pmod 7$. The order 1 (as always) is achieved by [1] only, and only the class of $6 \equiv -1 \pmod 7$ has order $2|6$. Only the classes of $2, 4$ (again inverses of one another) remain; their order is $3|6$. Check! □

A.V.14 Example (Decimal Fractions, Prime Denominator). Let p be prime number $\neq 2, 5$. As $(10, p) = 1$ the class $10 + (p)$ is invertible, and has an order d, satisfying $10^d \equiv 1 \pmod p$, i.e.,

$$10^d = 1 + ap,\ a < 10^d. \tag{$*$}$$

According to Little Fermat, $d|(p-1)$. We rewrite (*) as follows:

$$\frac{1}{ap} = \frac{1}{10^d - 1}; \quad \frac{1}{p} = \frac{a \cdot 10^{-d}}{1 - 10^{-d}}.$$

If $a = a_0 \cdot 10^{d-1} + a_1 \cdot 10^{d-2} + \cdots + a_{d-1}$ the numerator is $\alpha = a_0 \cdot 10^{-1} + a_1 \cdot 10^{-2} + \cdots + a_{d-1} \cdot 10^{d-1}$; in decimal notation: $\alpha = 0.a_0 a_1 \ldots a_{d-1}$.

Recalling the geometric series:

$$\frac{a}{1-k} = a(1 + k + k^2 + \cdots + k^n + \cdots); \quad |k| < 1$$

we expand:

$$\frac{1}{p} = \alpha + \alpha \cdot 10^{-d} + \alpha \cdot 10^{-2d} + \cdots + \alpha^{\cdot} 10^{-nd} + \cdots$$

resulting in the periodic decimal expansion:

$$\frac{1}{p} = 0.a_0 a_1 \ldots a_{d-1} a_0 a_1 \ldots a_{d-1} a_0 a_1 a_2 a_3 \ldots \tag{$*$}$$

Conversely, suppose (*) holds for some period d. Then

$$\begin{aligned} 10^d \cdot \frac{1}{p} &= a_0 a_1 a_2 \ldots a_{d-1}.a_0 a_1 \ldots a_{d-1} a_0 a_1 \ldots \\ &= a.a_0 a_1 \ldots a_{d-1} a_0 a_1 \ldots \end{aligned}$$

and

$$\frac{10^d - 1}{p} = a = a_0 \cdot 10^{d-1} + a_1 \cdot 10^{d-2} + \cdots + a_{d-1}$$

so that $10^d \equiv 1 \pmod{p}$. From this emerges that the shortest period must equal the exact order of 10 modulo p.

E.g., for $p = 13$ it is $6 = (p-1)/2$, as $10^2 \equiv 9$, $10^3 \equiv -1$, $10^6 \equiv 1 \pmod{13}$, and $1/13 = 0.0769230769\ldots$. And for $p = 7$ it is $p - 1 = 6$, as $10^2 \equiv 3^2 \equiv 2 \pmod{7}$, $10^3 \equiv 6 \pmod{7}$, $1/7 = 0.1428571428\ldots$ □

A.V.15 Example (Decimal Fractions, Composite Denominator). For composite N a similar result holds. The decimal expansion of $1/N$ is purely periodic if $(10, N) = 1$, i.e., if neither 2 nor 5 divides N. The period d equals the order of 10 modulo N and is a factor in $\phi(N)$.

If $(10, N) > 1$ the decimal expansion cannot be purely periodic. By the reasoning above, the period d would entail $10^d \equiv 1 \pmod{N}$. But if $a^d \equiv 1 \pmod{N}$, then clearly a and a^{d-1} are inverse to one another modulo N. And invertibility means $(a, N) = 1$.

Let us look at an example, $N = 840 = 2^3 \cdot 3 \cdot 5 \cdot 7$. The expansion is $1/N = 0.001190476190476109\ldots$. It has a *preperiod* of three places, 001, followed by a periodic part, of period 6. How do we explain this?

Multiplying by 10^3 gives: $10^3/N = 1.190476190467\ldots$,

$$\frac{10^3}{N} - 1 = \frac{10^3 - 1 \cdot N}{N} = \frac{1000 - 840}{840} = \frac{4}{21} = 0.190476190476\ldots$$

and $(10, 21) = 1$. The evil factors of N, the three 2's and the single 5, cancel, because 10^3 is divisible by all of them.

The order of 10 modulo 21 is 6, $(10^{20} - 1)/21 = 47619$, and $1/21 = 0.0476190476190\ldots$.

And, finally, $4 \cdot 47619 = 190476$.

We have already explained the period 6. The new modulus, 21, is the result of dividing out all factors 2 and 5 from N, and 6 is the order of 10 modulo 21.

10^3 is the smallest power of 10 divisible by all the 2- and 5-factors of $840 = 2^3 \cdot 5 \cdot 21$. It is therefore also the smallest power 10^e for which $840 | 10^e(10^6 - 1)$ (as $10^6 - 1$ is not divisible by 2 or 5).

So, from that power on, but not earlier, the powers of 10 modulo 840 repeat periodically, with period 6. □

What is the order of a power? The following Theorem answers that question. It is again preceded by a very useful Lemma.

A.V.16 Lemma. *Let m, n be integers, not both = 0. Let further $d = (m, n)$. Then*

$$\left(\frac{m}{d}, \frac{n}{d}\right) = 1.$$

Proof. By Bézout, there are integers r, s with $rm + sn = d$. Dividing both members by d gives

$$r\frac{m}{d} + s\frac{n}{d} = 1,$$

and the result is immediate. □

A.V.17 Theorem (Order of a Power). *Still considering classes modulo $n > 0$. Suppose $ord_n(a) = d$. Then*

$$ord_n(a^k) = \frac{d}{(d, k)}.$$

Proof. By our Main Theorem

$$(a^k)^e \equiv 1 \pmod{n} \Longleftrightarrow d|ke \Longleftrightarrow \frac{d}{(d,k)}|e \cdot \frac{k}{(d,k)}.$$

As $d/(d,k)$ and $k/(d,k)$ are relatively prime by the Lemma, our First Divisibility Theorem then shows that

$$(a^k)^e \equiv 1 \pmod{n} \Longleftrightarrow \frac{d}{(d,k)}|e.$$

So the least positive e with the property stated in the left member is $e = d/(d,k)$. Hence, $\mathrm{ord}_n(a^k) = d/(d,k)$. □

A.V.18 Example. There are two extreme cases, $(d, k) = 1$ and $k|d$.

For instance, modulo 13 we have verified that $\text{ord}_n(2) = 12$. The Theorem then shows that the classes $[2]^5 = [6], [2]^7 = [11], [2]^{11} = [7]$ have that same order, as the exponents are relatively prime to 12.

The class of $[2]^6 = [64] = [-1]$ has order $2 = 12/6$ as predicted by the Theorem. □

We have exemplified the fact that mutually inverse classes have the same order – we leave the simple general proof as an exercise.

A natural question regards the order of a product. The answer is simple if the orders of the two factors are relatively prime.

A.V.19 Theorem (Order of a Product). *Still working modulo $n > 0$. Suppose the orders of a, b modulo n are r, s respectively, with $(r, s) = 1$. Then $\text{ord}_n(ab) = rs$.*

Proof. Often a natural way of proving equality between two numbers is to prove mutual divisibility.

$\text{ord}_n(ab)$ divides rs:

$([a][b])^{rs} = ([a]^r)^s \cdot ([b]^s)^r = [1][1] = [1]$.

rs divides $\text{ord}_n(ab)$:

Let the order of the product be e. We then have $([a][b])^e = [1]$, $[a]^e[b]^e = [1]$. Raising both members to the power r (remembering that $[a]^r = [1]$) gives $[b]^{re} = [1]$. So the order of $[b]$ divides re: $s|re$.

As $(s, r) = 1$, our First Divisibility Theorem (A.II.1) gives $s|e$. Similarly, raising the first equation to the power s, we get $r|e$. As $(r, s) = 1$, the two divisibility relations, $r|e$, $s|e$, give $rs|e$, by the Second Divisibility Theorem (A.II.2). □

A.V.20 Example. $n = 7$. $\text{ord}_7(2) = 3, \text{ord}_7(6) = 2$, so $\text{ord}_7(2 \cdot 6) = \text{ord}_7(5) = 6$.

When $(r, s) > 1$ little can be said. Take $n = 17$. It is easy to check that the classes of 3, 5, 6, 11, 12 all have order 16 – one need only check that their 8th powers equal $[-1] \neq [1]$, as 2 is the only prime factor in 16, and 8=16/2.

You are invited to check that the classes of $[3][6] = [1], [3][11] = [-1], [6][12] = [4]$, and $[3][5] = [-2]$ have orders 1,2,4, and 8, respectively.

The reader is invited to explain these orders by writing 3, 5, 6,11,12, and their products, as powers of 3, modulo 17.

□

A.V: Exercises

1. (a) Compute $5^{15} \pmod 7$ and $7^{13} \pmod{11}$. Short hand calculation.

(b) Compute $(5^{97} + 11^{33})^8 \pmod{24}$.

(c) Show that $5, 7, 35|n^{13} - n$ and $170|(n^{17} - n)$ for all integers n.

(d) Show that the classes $[m], [m]^{-1}$ modulo $n > 0$ have the same order.

(e) The prime factors of $n > 0$ are all greater than 61. Show that $n^{60} - 1$ is divisible by $16 \cdot 9 \cdot 25 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$.

(f) Let p be a prime ≥ 7. Show that $p^4 \equiv 1 \pmod{240}$

2. Determine $\phi(70)$, and enumerate the invertible classes modulo 70.

3. Let a be a positive integer. Show that the last digits of a and a^{10} are the same.

Show that there is no corresponding result for the last k digits, $k = 2, 3$, unless $(a, 10) = 1$. Under the latter condition, what is the least exponent $d > 1$ such that a^d and a have the same k last digits?

4. (a) Let p, q be two different prime numbers. Show that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

(b) Let m be a positive integer. Show that $m^{143} - m^{13} - m^{11} + m$ is divisible by 143.

(c) Let p, q be two different primes such that $2^p \equiv 2 \pmod q$ and $2^q \equiv 2 \pmod p$. Show that $2^{pq} \equiv 2 \pmod{pq}$.

5. (a) Determine, by hand calculation, the order of 2 modulo 7, 9, 11, 13.

(b) Using the previous item, determine the order of 2 modulo 77, 91, 99 and 143.

6. (a) p is a prime, $\operatorname{ord}_p(a) = 3$. Show that $\operatorname{ord}_p(1 + a) = 6$. Hint: Compute $a^2 + a + 1$ modulo p.

(b) Suppose the prime number p divides $n^4 - n^2 + 1$. Show that $\operatorname{ord}_p(n) = 12$. Hence, or otherwise, prove that $p = 12k + 1$ for some integer k.

7. Let p be an odd prime. Show that $p | (b^n - 1)$ implies $p | (b^d - 1)$ where d is a proper divisor of n, *or* that $p \equiv 1 \pmod{n}$. Use this to factor $3^{12} - 1$ completely.

8. Show by hand calculation that $x^{81} \equiv x \pmod{935}$ for all integers x (using the factorization of 935, of course). Generalize!

9. Let p be a prime > 2. Show that the relation $2^p \equiv 1 \pmod{2p + 1}$ implies that $2p + 1$ is a prime number.

Example: $p = 1103$.

10. Suppose p is a prime factor of $b^n + 1$. Show that p is a factor of $b^d + 1$ where $d | n$ and the quotient n/d is odd, or that $p \equiv 1 \pmod{2n}$. You might start by considering the least k for which $p | (b^k + 1)$.

11. Let $n > 1$ be a composite number, and let p be a simple prime factor of n (meaning that p, but not p^2, divides n). Then

$$p \nmid \binom{n}{p}.$$

Hint: Write the binomial coefficient as a quotient of two products of exactly p factors each.

How would you modify the statement and the solution in the case $p^k | n$, $p^{k+1} \nmid n$?

12. Let $n > 1$ be an integer. Show that $n \nmid 2^n - 1$. Hint: Look at the smallest prime factor of n.

13. Let a be an integer, $1 \le a \le 34 = 5 \cdot 7 - 1$. Let $m = 12 = 5 + 7$. Find the least positive integer d such that $m^d a \equiv a \pmod{35}$. The answer depends on $(a, 35)$.

14. The composite number N is a **pseudoprime to the base** $a, (a, N) = 1$, if $a^{N-1} \equiv 1 \pmod{N}$. Determine whether the number 45 is a pseudoprime to the bases 17 or 19 respectively. Hand calculation, use the prime factorization of 45.

15. Determine the number of incongruent bases for which 91 is a pseudoprime.

16. Let $n = pq$ be the product of two different odd primes. Show that n is a pseudoprime to the base b if and only if $b^d \equiv 1 \pmod{n}$ where $d = (p - 1, q - 1)$.

17. Show that p^2, where p is an odd prime, is a pseudoprime to the base n if and only if

$$n^{p-1} \equiv 1 \pmod{p^2}.$$

18. (a) Let $a > 1$ be an integer, and $p \nmid a(a^2-1)$ a prime. Put

$$n = \frac{a^{2p}-1}{a^2-1}.$$

Show (geometric sums!) that n is a composite integer (two assertions!)

(b) Show that $a^{n-1} \equiv 1 \pmod{n}$.

(c) Conclude that infinitely many integers n are pseudoprimes to the base a.

Why did we not use $n = (a^p-1)/(a-1)$?

19. **Suggestions for computing:** At this point you could read up on fast exponentiation, Section L.V, and the probabilistic Miller-Rabin primality test in the last Chapter, and write a simple program. The problems in Section L.VI. require very little in the way of programming.

A.VI A Brief Account of RSA

In this Section we briefly describe the RSA public key cryptographic scheme. As there are many excellent comprehensive accounts in the literature (Buchmann, Trappe-Washington) we dwell on the number theory involved, leaving most of the practical issues aside.

The mathematics behind RSA is summed up in the following two Lemmas. The first is a special case of a general Theorem to be proved in the next Chapter.

A.VI.1 Lemma. *Let $n = pq$ be the product of two different prime numbers. Then $\phi(n) = (p-1)(q-1)$.*

Proof. We can prove this the same way we did in the special case $n = 15 = 3 \cdot 5$. There are $n = pq$ classes modulo pq, represented by the numbers m with $0 \leq m \leq n-1$. The non-invertible classes are represented by those m with $(m, pq) > 1$, i.e., those divisible by p or q. There are q and p of these, respectively. Only $m = 0$ is divisible by both p and q: by our Second Divisibility Theorem (A.II.2) a number divisible by both must be divisible by their product, as $(p, q) = 1$.

So we subtract q and p classes and put back the zero class, which we subtracted twice. Therefore:

$$\phi(pq) = pq - q - p + 1 = (p-1)(q-1).$$

□

The second Lemma is sometimes overlooked in the literature, probably because the probability of randomly choosing an a with $(a, pq) > 1$ is very small when p, q are large.

A.VI.2 Lemma. *Still assuming $n = pq$. For all integers a, and positive integers k, we have*

$$a^{k\phi(n)+1} \equiv a \pmod{n},$$

whether $(a, n) = 1$ or not.

Proof. If $(a, n) = 1$, Euler's Theorem (A.V.12) states that $a^{\phi(n)} \equiv 1 \pmod{n}$, so the result follows on raising both members to the power k, and multiplying them by a.

Next consider the case where $(a, n) > 1$. This means that a is divisible by p or q. If a is divisible by both, it is divisible by their product n, and the result is trivial in this case. So we can assume that $p|a$ and $q \nmid a$.

Consider the difference

$$b = a^{k\phi(n)+1} - a.$$

Under our assumption it is trivially divisible by p. The exponent is $f = k\phi(n) + 1 = k(p-1)(q-1) + 1$. So by Fermat's Little Theorem

$$a^f - a = (a^{q-1})^{k(p-1)} \cdot a - a \equiv 1^{k(p-1)} \cdot a - a \equiv 0 \pmod{q}.$$

So b is divisible by both p and q, hence by their product, by our Second Divisibility Theorem (A.II.2). □

We now briefly describe the RSA scheme. Bob expects a message from Alice. She codes the message into a number a according to some simple scheme known to both. Bob chooses two big prime numbers p, q (big = at least 100 decimal digits), and publishes their product n. He chooses an encryption exponent e, $(e, \phi(n)) = 1$, which is also made public.

Alice sends a^e (reduced modulo n). Bob, knowing p, q, hence also $\phi(n) = (p-1)(q-1)$, easily determines the inverse class $[d]$, of $[e]$, modulo $\phi(n)$. We then have the relation $de \equiv 1 \pmod{\phi(n)}$; $de = k\phi(n) + 1$. By the second Lemma he can recover a as $a^{de} \equiv a \pmod{n}$.

It is assumed to be difficult to recover a from a knowledge of $a^e \pmod{n}$ without factoring n, but no one has proved it. It is almost impossible to determine d from e without factoring n. In fact, there is a probabilistic algorithm (see exercise in Section L.VI) that cracks n with great probability once an inverse pair modulo $\phi(n)$ is known.

Many larger books include comprehensive discussions on the practical problem of generating large prime numbers, on their choice, on the choice of exponents, etc. Many texts also discuss various attacks on RSA.

The letters R, S, A are the initials of Rivest, Shamir, and Adleman.

A critical point is how to perform modular exponentiations economically. This is discussed in our last Chapter, on Factorization and Primality Tests, where further applications of Little Fermat and the order concept are given. See, e.g., Section L.V.

A.VI: Exercises

1. (a) Let $n > 0$ be a square-free integer, i.e., not divisible by a square > 1. Show that $a^{\phi(n)+1} \equiv a \pmod{n}$, even if $(a, n) > 1$. Start by looking at the prime factors of n.

(b) Suppose, conversely, that

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

for all a. Show that n is square-free. Hint: If $p^2 | n$, p prime, look at the congruence taken modulo p^2.

2. Let $n = pq$, where $p \neq q$ are two (large) prime numbers. Show that p, q may be determined if n and $\phi(n)$ are known. Hint: Knowing their sum and product you can derive a quadratic equation for them.

3. Let a be a non-zero integer, $n > m$ positive integers. Show that the greatest common divisor of $a^{2^n} + 1$ and $a^{2^m} + 1$ is 1 or 2. Describe the cases. Hint: If p is an odd prime, and $p | (a^{2^m} + 1)$, then $p | (a^{2^n} - 1)$.

4. Let $N > 1$ be an odd integer. Show that the congruence $a^{N-1} \equiv -1 \pmod{N}$ is impossible. Hint: Let $v_q(n)$ denote the multiplicity k of q in the factorization of n, i.e., $q^k | n$, $q^{k+1} \nmid n$. Consider the order of a modulo each prime factor p in N, and modulo N. Show that $a^{N-1} \equiv -1 \pmod{N}$ implies that $v_2(p-1) > v_2(N-1)$ and derive a contradiction.

Chapter B

Congruences. The CRT.

B.I The Chinese Remainder Theorem

This is as good a place as any to introduce the *least common multiple* of two integers.

B.I.1 Definition. Let m, n be non-zero integers. The **least common multiple** of m and n, denoted $[m, n]$, or $\operatorname{lcm}(m, n)$, is the smallest (positive) integer divisible by both m and n.

B.I.2 Example. $[3, 4] = [3, -4] = [4, 6] = 12$. □

The example shows that the lcm of two positive numbers may be their product or not. The following Theorem gives the full story.

B.I.3 Theorem. *The lcm of two positive integers is given by*

$$[m, n] = \frac{m \cdot n}{(m, n)}.$$

It therefore equals their product if and only if m and n are relatively prime, $(m, n) = 1$. *Furthermore, any common multiple of m and n is divisible by their least common multiple.*

Proof. Let e be any common multiple, $m|e$, $n|e$. This is clearly equivalent to

$$\frac{m}{(m,n)}\Big|\frac{e}{(m,n)}, \quad \frac{n}{(m,n)}\Big|\frac{e}{(m,n)}.$$

As $m/(m,n)$ and $n/(m,n)$ are relatively prime (Lemma A.V.16), the two conditions are equivalent to $e/(m,n)$ being divisible by their product, according to the Second Divisibility Theorem, (A.II.2). That is, to:

$$\frac{m}{(m,n)} \cdot \frac{n}{(m,n)}\Big|\frac{e}{(m,n)}.$$

Multiplying by (m,n) we therefore see that e is a common multiple of m, n if and only if

$$\frac{m \cdot n}{(m,n)}\Big|e$$

which proves both parts of the Theorem. □

We now turn to the simplest case of the Chinese Remainder Theorem, that involving two simultaneous congruences.

B.I.4 Theorem (CRT, Two Congruences). *Let n_1, n_2 be two positive integers. The pair of simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

is solvable if and only if $(n_1, n_2)|(a_1 - a_2)$. The solution is unique modulo $m = [n_1, n_2]$, i.e., the solution set is a single residue class modulo m.

In particular, the pair of congruences is solvable if $(n_1, n_2) = 1$. The solution is then unique modulo the product $n_1 \cdot n_2$.

Proof. The solution set to the first congruence is $\{x = a_1 + r \cdot n_1, r \in \mathbf{Z}\}$, that of the second congruence is $\{x = a_2 + s \cdot n_2, s \in \mathbf{Z}\}$.

The two sets have at least one element x in common if and only if there are integers r, s with $a_1 + r \cdot n_1 = a_2 + s \cdot n_2$, i.e., if and only there are r, s satisfying $a_1 - a_2 = s \cdot n_2 - r \cdot n_1$. By our early results on linear Diophantine equations (A.I.4), this is equivalent to $(n_1, n_2)|a_1 - a_2$. This settles the existence part.

As for uniqueness, fix one solution x. Then y is another solution if and only if $x - y \equiv 0 \pmod{n_1}$ and $x - y \equiv 0 \pmod{n_2}$, i.e., if and only if $x - y$ is a common multiple of n_1, n_2, i.e., if and only if $x - y$ is divisible by their lcm, i.e., if and only if $x \equiv y \pmod{[n_1, n_2]}$. □

The case of two congruences will suffice for our purposes in several theoretical instances. However, it is only fair to answer the obvious question about the solvability of $l > 2$ simultaneous congruences. A necessary condition is that each subsystem of two congruences be solvable. We prove the most important case now, and save the general case for later.

B.I.5 Theorem (CRT, $l > 2$ Congruences). *The system of simultaneous congruences*

$$\begin{array}{rcll} x & \equiv & a_1 & \pmod{n_1} \\ x & \equiv & a_2 & \pmod{n_2} \\ & \vdots & & \\ x & \equiv & a_l & \pmod{n_l} \end{array}$$

is solvable if the n_j are pairwise relatively prime, *i.e., if $(n_j, n_k) = 1$ whenever $j \neq k$.*

The solution is unique modulo $n_1 n_2 \cdots n_l$.

Proof. We have already settled the case $l = 2$. Now let $l > 2$. Suppose, by way of induction, that the Theorem has been proved for $l - 1$. Let $x \equiv b_2 \pmod{n_2 \cdots n_l}$ be the general solution of the last $l - 1$ congruences. We combine this with the first congruence into

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2 \cdots n_l}. \end{aligned}$$

The induction step will follow at once if we can prove that $(n_1, n_2 \cdots n_l) = 1$. We have assumed $(n_2, n_1) = \cdots = (n_l, n_1) = 1$, i.e., that the classes of $n_2, \ldots, n_l$ are invertible modulo n_1. Then, by the same argument as in the proof of Lemma (A.V.10) just before Euler's Theorem so is their product, which is the same as saying that $(n_1, n_2 \cdots n_l) = 1$.

That last part could also be proved using the prime factorizations of the various n_j. □

The running time of the CRT, as given, is quadratic in the bitlength of the product modulus.

B.I.6 Example. At least for hand calculations there are two ways to solve a Chinese Congruence System.

Suppose we are to solve the system

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

with $3, 5, 7$ obviously relatively prime in pairs. We start by solving Bézout for the first two moduli:

$$r_1 \cdot 3 + r_2 \cdot 5 = 1, \qquad 2 \cdot 3 - 1 \cdot 5 = 6 - 5 = 1,$$

with

$$\begin{aligned} -5 &\equiv 1 \pmod{3} \\ -5 &\equiv 0 \pmod{5} \end{aligned}$$

and

$$\begin{aligned} 6 &\equiv 0 \pmod{3} \\ 6 &\equiv 1 \pmod{5}. \end{aligned}$$

We then get the solution to the first two congruences by multiplying the first pair by 1, the second by 2, and adding:

$$x \equiv 1 \cdot (-5) + 2 \cdot 6 \equiv 7 \pmod{3 \cdot 5}.$$

This is then combined with the third congruence, and the two together are treated exactly the same way as the first two:

$$\begin{aligned} x &\equiv 7 \pmod{15} \\ x &\equiv 3 \pmod{7}. \end{aligned}$$

Solve Bézout again:

$$1 \cdot 15 - 2 \cdot 7 = 1, \qquad 15 - 14 = 1$$

and another superposition gives us:

$$x \equiv 7 \cdot (-14) + 3 \cdot 15 \equiv -53 \equiv 52 \pmod{15 \cdot 7},$$

i.e.,

$$x \equiv 52 \pmod{105}$$

We could also solve three Bézout identities. Let $n_1 = 3$, $n_2 = 5$, $n_3 = 7$ Putting $M = n_1 n_2 n_3, M_i = M/n_i$, we determine $r_i, s_i \quad i = 1, 2, 3$ such that

$$r_i M_i + s_i n_i = 1, \quad i = \quad 1, 2, 3$$

Putting $x_i = r_i M_i$ we see that $x_i \equiv 1 \pmod{n_i}$ and $x_i \equiv 0 \pmod{M_i}$, i.e., $x_i \equiv 0 \pmod{n_j}$, $j \neq i$.

The solution is then

$$x \equiv a_1 x_1 + a_2 x_2 + a_3 x_3 \pmod{n_1 n_2 n_3}.$$

In our numerical example, with $a_1 = 1, a_2 = 2, a_3 = 3$, we get:

$$-1 \cdot (5 \cdot 7) + 12 \cdot 3 = -35 + 36 = 1$$

$$1 \cdot (3 \cdot 7) - 4 \cdot 5 = 21 - 20 = 1$$
$$1 \cdot (3 \cdot 5) - 2 \cdot 7 = 15 - 14 = 1$$

and

$$x \equiv 1 \cdot (-35) + 2 \cdot 21 + 3 \cdot 15 \equiv 52 \pmod{105}$$

□

Remark: The quantities $x_i = r_i M_i$ are called the *idempotents* ("like-potent elements") of the Chinese congruence system, as $x_i^2 \equiv x_i$ modulo the product modulus. They are *orthogonal* meaning that the product of any two different x_i is congruent to zero modulo the product modulus.

B.I.7 Example. It is instructive to tabulate the solutions of a pair of congruences for any combination of right members a_1, a_2. In the case $n_1 = 3, n_2 = 5$, the special pairs

$$10 \equiv -5 \equiv 1 \pmod{3}$$
$$10 \equiv -5 \equiv 0 \pmod{5}$$

and

$$6 \equiv 0 \pmod{3}$$
$$6 \equiv 1 \pmod{5}$$

combine to give the solution $x \equiv a_1 \cdot 10 + a_2 \cdot 6 \pmod{15}$ to the general pair

$$\begin{aligned} x &\equiv a_1 \pmod{3} \\ x &\equiv a_2 \pmod{5}. \end{aligned}$$

We tabulate the result for all possible pairs a_1, a_2:

$a_1 \backslash a_2$	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

The first row (below the horizontal line) gives the multiples of 6 modulo 15. The first column (to the right of the vertical line) gives the multiples of 10 modulo 15. The remaining elements are the sum modulo 15 of the leftmost element in the same row and the uppermost element in the same column.

Here is the corresponding table for $n_1 = 4$, $n_2 = 5$:

$a_1 \backslash a_2$	0	1	2	3	4
0	0	16	12	8	4
1	5	1	17	13	9
2	10	6	2	18	14
3	15	11	7	3	19

We leave it to the reader to contemplate the result of reading off the results diagonally. Do you see a pattern? Can you explain it? □

B.I: Exercises

1. Determine all solutions of the congruence system $x \equiv 1 \pmod{7}$; $x \equiv 4 \pmod{9}$; $x \equiv 3 \pmod{5}$.

2. Find all integers x such that $5x + 8$ is divisible by 11 and 13.

3. Find all solutions to

$$\begin{aligned} x &\equiv 2 \pmod{7} \\ 4x &\equiv 5 \pmod{11} \\ 3x &\equiv 2 \pmod{13}. \end{aligned}$$

4. Determine the least positive remainder of

$$2^{13^{79}}$$

modulo $77 = 7 \cdot 11$.

Hand calculation!

B.II Euler's Phi Function Revisited

In this Section we prove a property that allows us to compute $\phi(n)$ (A.V.1) whenever a full prime factorization of n is known. The CRT plays a decisive role in the proof. The following Lemma reformulates an earlier observation:

B.II.1 Lemma. *Suppose the integers $n_1, n_2 > 0$ are relatively prime. Let $0 \leq a_1 < n_1$, $0 \leq a_2 < n_2$ and let $0 \leq x < n_1 \cdot n_2$ be the unique solution to the congruence pair*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \end{aligned}$$

Then the class $x + (n_1 n_2)$ is invertible if and only if the classes $a_1 + (n_1)$ and $a_2 + (n_2)$ are.

Proof. As $a_1 + (n_1) = x + (n_1)$, and $a_2 + (n_2) = x + (n_2)$ we are stating that the class $x + (n_1 n_2)$ is invertible if and only if $x + (n_1)$ and $x + (n_2)$ are, or equivalently:

$$(x, n_1 n_2) = 1 \Longleftrightarrow (x, n_1) = (x, n_2) = 1.$$

We proved the left arrow in the course of proving the CRT, B.I.5.

The right arrow is trivial. □

An immediate consequence of the Lemma is that we have a bijection between invertible classes $x+(n_1 n_2)$ and pairs of invertible classes $(a_1 + (n_1),\ a_2 + (n_2))$, whenever $(n_1, n_2) = 1$. As there are $\phi(n_1 n_2)$ of the former, and $\phi(n_1)\phi(n_2)$ of the latter, we have proved the following Theorem:

B.II.2 Theorem (Multiplicativity of ϕ). *Let n_1, n_2 be positive integers satisfying $(n_1, n_2) = 1$. Then:*

$$\phi(n_1 n_2) = \phi(n_1)\phi(n_2).$$

□

B.II.3 Example. Let us return to the example $n_1 = 4$, $n_2 = 5$, where we arrived at the following table:

$a_1 \backslash a_2$	0	1	2	3	4
0	0	16	12	8	4
1	5	1	17	13	9
2	10	6	2	18	14
3	15	11	7	3	19

By the proof of the Theorem, we get the invertible classes modulo 20 by selecting only those a_1 that are invertible modulo 4, i.e., $a_1 = 1, 3$, and those a_2 that are invertible modulo 5, i.e., $a_2 = 1, 2, 3, 4$.

We are left with:

$a_1 \backslash a_2$	1	2	3	4
1	1	17	13	9
3	11	7	3	19

clearly illustrating not only $\phi(4 \cdot 5) = \phi(4) \cdot \phi(5) = 2 \cdot 4 = 8$, but also why.□

B.II.4 Example. It is now clear how to compute $\phi(n)$ whenever a prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

is known. Here the p_j are k different prime numbers, and the exponents e_j are positive. In an earlier example (A.V.2) we have computed $\phi(p^k) = p^k - p^{k-1}$.

Repeated application of the Theorem yields

$$\begin{aligned}\phi(n) &= \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k}) \\ &= p_1^{e_1}(1 - \frac{1}{p_1})p_2^{e_2}(1 - \frac{1}{p_2}) \cdots p_k^{e_k}(1 - \frac{1}{p_k}) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})\end{aligned}$$

Let, more concretely, $n = 105 = 3 \cdot 5 \cdot 7$. The Theorem gives $\phi(n) = \phi(3)\phi(5)\phi(7) = 2 \cdot 4 \cdot 6 = 48$.

The form we arrived at last has a nice combinatorial interpretation:

$$\phi(3 \cdot 5 \cdot 7) = 3 \cdot 5 \cdot 7(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7})$$

Multiplying the parentheses, and expanding, we get the alternating sum

$$\phi(3 \cdot 5 \cdot 7) = 3 \cdot 5 \cdot 7 - 5 \cdot 7 - 3 \cdot 7 - 3 \cdot 5 + 3 + 5 + 7 - 1.$$

The interpretation is the following:

We start with all of the 105 classes. We then delete all classes corresponding to multiples of 3, 5, and 7, respectively. Their numbers are $5 \cdot 7, 3 \cdot 7, 3 \cdot 5$ respectively.

This however results in deleting the 3 classes corresponding to multiples of $5 \cdot 7$ twice; those corresponding to multiples of $3 \cdot 7$ (5 in number) also twice, and the same for the 7 classes corresponding to multiples of $3 \cdot 5$. So we put them back again.

But then we have deleted the zero class three times, and put it back three times, so we have to delete that one class again.

Those who have taken a course in Discrete Math may recognize this as a special application of the Principle of Inclusion-Exclusion. Of course, the alternating sum is not suitable for computation. □

B.II: Exercises

1. m, p are positive integers, $(m, p) = 1$. Show that m divides $\phi(p^m - 1)$. Hint: It is a one-line proof.

2. Show that there are no numbers n with $\phi(n) = 14$ and ten satisfying $\phi(n) = 24$. Determine these, and be careful to prove you found them all.

3. r, d, k are positive numbers, $(r, d) = 1$, and $d|k$. Consider the arithmetic sequence $r + td$, $t = 0, 1, 2, \ldots, k/d - 1$. Show that the number of elements that are relatively prime to k is $\phi(k)/\phi(d)$. Note the special case $(d, k/d) = 1$ allowing a simple proof.

Hint: Let $p_1, p_2, \ldots, p_s$ be those primes that divide k but not d. Look for those t that satisfy a certain set of congruence systems $r + td \equiv y_i \mod p_i$, $i = 1, 2, \ldots, s$.

4. Show that there are arbitrarily long sequences of integers, $x, x + 1, x + 2, \ldots x + n$, that are divisible each by a square > 1.

5. **Suggestions for computing**: A routine solving a Chinese congruence system, issuing a warning when the data are incompatible.

A sequential program for solving systems of more than two congruences, checking compatibility at each step.

Or a program computing the idempotents (in the case of pairwise relatively prime moduli). You may prefer a recursive program.

* B.III General CRT

We now proceed to proving the CRT in its full generality. We prepare the proof by generalizing the lcm and gcd to include the case of more than two numbers, and by formally introducing multiplicities of prime factors. For non-zero numbers $m_1, m_2, \ldots, m_n$ we naturally let $(m_1, m_2, \ldots, m_n)$ denote the greatest (positive) number dividing all the m_j. Obviously,

$$(m_1, m_2, \ldots, m_n) = (m_1, (m_2, \ldots, m_n)).$$

And for non-zero numbers $m_1, m_2, \ldots, m_n$ we let $[m_1, m_2, \ldots, m_n]$ denote the least number divisible by all the m_j. Obviously,

$$[m_1, m_2, \ldots, m_n] = [m_1, [m_2, \ldots, m_n]].$$

We now turn our attention to multiplicities.

B.III.1 Definition. For any non-zero integer n, and any prime number p, we denote by $v_p(n)$ the largest exponent $e \geq 0$ such that p^e divides n. It is called the **multiplicity** of p in (the factorization of) n.

We record a few elementary observations:

B.III.2 Lemma.

a) The positive integers m, n are equal if and only if $v_p(m) = v_p(n)$ for all prime numbers p.

b) m divides n if and only if $v_p(m) \leq v_p(n)$ for all prime numbers p.

c) For non-zero integers m, n, all primes p, $v_p(mn) = v_p(m) + v_p(n)$.

d) For all but finitely many prime numbers p, we have $v_p(n) = 0$.

□

We will be concerned with the multiplicities of primes entering the gcd and lcm of two numbers.

B.III.3 Lemma. *Let m, n be non-zero integers. Then, for all prime numbers p:*

a) $v_p((m,n)) = \min(v_p(m), v_p(n))$,

b) $v_p([m,n]) = \max(v_p(m), v_p(n))$.

Proof. For the first part, note that p^e divides (m,n) if and only if p^e divides both m and n, i.e., if and only if $e \leq$ both $v_p(m)$ and $v_p(n)$. This proves that $v_p((m,n))$ must equal the smaller of these two numbers.

For the second part, note that p^e is divisible by the p-power entering $[m,n]$ if and only if p^e is divisible by the corresponding factors of both m and n, i.e., if and only if $e \geq$ both $v_p(m)$ and $v_p(n)$. This proves that $v_p([m,n])$ must equal the greater of these two numbers. □

Before going on with the CRT we pause to reprove an earlier result.

B.III.4 Theorem. *For positive integers m, n,*

$$[m,n] = \frac{mn}{(m,n)}.$$

Proof. It is enough to compare the multiplicities of any prime p. By the result above, the multiplicity for the left member is:

$$v_p([m,n]) = \max(v_p(m), v_p(n)).$$

And the multiplicity for the right member is

$$v_p(mn) - v_p((m,n)) = v_p(m) + v_p(n) - \min(v_p(m), v_p(n)) = \max(v_p(m), v_p(n)).$$

□

The next, very special, Lemma unlocks the induction step in the proof of the general CRT.

B.III.5 Lemma. *Let $m_1, m_2, \ldots, m_n$, $n \geq 3$, be positive integers. Then:*

$$\big[(m_1, m_2), (m_1, m_3), \ldots, (m_1, m_n)\big] = \big(m_1, [m_2, m_3, \ldots, m_n]\big).$$

Proof. Let p be an arbitrary prime. It suffices to prove that p enters both members with the same multiplicity in their respective factorizations. We may arrange that $v_p(m_n)$ is the greatest among $v_p(m_2), v_p(m_3), \ldots, v_p(m_n)$.

Consider the left member first. A moment's reflection makes it clear that the multiplicity of p in that lcm equals the multiplicity of p in the last term, i.e., it equals $v_p((m_1, m_n))$, as p can enter the preceding terms with at most that multiplicity.

As for the right member, by our arrangement, and the previous Lemma, $v_p([m_2, m_3, \ldots, m_n]) = v_p(m_n)$. Then

$$\begin{aligned} v_p\big((m_1, [m_2, m_3, \ldots, m_n])\big) &= \min\big(v_p(m_1), v_p([m_2, m_3, \ldots, m_n]\big) \\ &= \min\big(v_p(m_1), v_p(m_n)\big) \\ &= v_p\big((m_1, m_n)\big). \end{aligned}$$

□

We can now prove the CRT in the desired full generality:

B.III.6 Theorem (General CRT, $l > 2$ Congruences). *The system of simultaneous congruences*

$$\begin{array}{rcll} x & \equiv & a_1 & \pmod{n_1} \\ x & \equiv & a_2 & \pmod{n_2} \\ & \vdots & & \\ x & \equiv & a_l & \pmod{n_l} \end{array}$$

is solvable if and only if the congruences are solvable in pairs, i.e., if and only if $(n_j, n_k)|(a_j - a_k)$ whenever $j \neq k$. The solution is unique modulo $[n_1, n_2, \ldots, n_l]$.

Proof. The proof proceeds by induction on l. The conditions are clearly necessary.

We have already proved the case $l = 2$. For the induction step, assume $l \geq 3$. Assume we have established the solution $x = a_0 + ([n_2, \ldots, n_l])$ for the last $l - 1$ congruences.

It remains to prove the solvability of the pair

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_0 \pmod{[n_2, \ldots, n_l]}. \end{aligned}$$

By the case $l = 2$ we must prove that $(n_1, [n_2, \ldots, n_l])$ divides $a_1 - a_0$.

By the preceding Lemma, $(n_1, [n_2, \ldots, n_l])$ is the lcm of all the (n_1, n_k), $k > 1$. Therefore it suffices to prove that each (n_1, n_k), $k > 1$, divides $a_1 - a_0$. However, $a_1 - a_0 \equiv a_1 - a_k \equiv 0 \pmod{n_k}$, $k > 1$, by the induction assumption.

So, a fortiori, $a_1 - a_0 \equiv 0 \pmod{(n_1, n_k)}$, by the assumption of the Theorem, and we have proved the solvability part.

By the case $l = 2$, the solution is unique modulo

$$[n_1, [n_2, \ldots, n_l]] = [n_1, n_2, \ldots, n_l],$$

which settles the uniqueness part. □

B.III.7 Example. Let us look at a simple example:

$$\begin{aligned} x &\equiv 3 \pmod{6} \\ x &\equiv 12 \pmod{15} \\ x &\equiv 6 \pmod{21}. \end{aligned}$$

The compatibility conditions are easily verified. For instance, $(6, 15) = 3$ divides $9 = 12 - 3$. The first pair requires the determination of r, s such that $x = 6r + 3 = 15s + 12$, $6r - 15s = 9$. Extended Euclid gives $-2 \cdot 6 + 1 \cdot 15 = (6, 15) = 3$. Multiplication by 3 gives the solution $r = -6, s = -3$, $x = -33 \equiv 27 \pmod{30}$, where $30 = [6, 15]$. This is then combined in the same manner with the last congruence, yielding $x \equiv 27 \pmod{210}$. □

B.III: Exercises

1. Determine the least positive integer n such that $n \equiv k - 1 \pmod{k}$ for $k = 1, 2, \dots, 10$.

2. Consider a quadratic form $Q(x, y) = ax^2 + bxy + cy^2$ with integer coefficients. x, y are integers.

Suppose the coefficients are relatively prime (not necessarily in pairs), i.e., $(a, b, c) = 1$. Let p be a prime number. Show that Q assumes at least one value not divisible by p.

Now let M be an arbitrary integer. Show that there are x, y such that $Q(x, y)$ and M are relatively prime.

3. y, M are positive integers, $(y, M) = 1$. m is another positive integer. Show that there is an integer x such that $(y + Mx, m) = 1$. Start with $m =$ prime power.

4. (a) Let $m, p_1, p_2, \dots, p_r$ be positive integers, relatively prime, but not necessarily in pairs. Example: $2 \cdot 3$, $3 \cdot 5$, 25.

$q_1, q_2, \dots, q_r$ are given integers. Show that the congruence system

$$p_j x \equiv q_j \pmod{m}, \quad j = 1, 2, \dots r,$$

is solvable if and only if

$$p_i q_j \equiv p_j q_i \pmod{m} \quad i, j = 1, 2, \dots, r.$$

Hint: Start by deriving a Bézoutian identity for $q_1, q_2, \dots, q_r, m$

(b) Show that the solution (when it exists) is unique modulo m.

B.IV Application to Algebraic Congruences

The CRT is a convenient tool for reducing algebraic congruences, $f(x) \equiv 0 \pmod{n}$, modulo composite n, to the case of, e.g., prime powers. We will deal with that special case later.

The following result will be used in the Chapter on Primitive Roots.

B.IV.1 Lemma. *Let $n = n_1 n_2$ where the factors are relatively prime, and ≥ 3. The congruence $x^2 \equiv 1 \pmod{n}$ then has at least four solutions modulo n, i.e., the solution set consists of at least four different residue classes modulo n.*

Proof. Consider the four different congruence pairs

$$\begin{aligned} x &\equiv \pm 1 \pmod{n_1} \\ x &\equiv \pm 1 \pmod{n_2}. \end{aligned}$$

Each of the pairs is uniquely solvable modulo n, by the CRT, producing four different residue classes modulo n. In each case the solutions x satisfy

$$\begin{aligned} x^2 &\equiv 1 \pmod{n_1} \\ x^2 &\equiv 1 \pmod{n_2}, \end{aligned}$$

i.e., $x^2 - 1$ is divisible by both n_1 and n_2. By the Second Divisibility Theorem, this implies that $x^2 - 1$ is divisible by their product, i.e. $x^2 \equiv 1 \pmod{n}$. □

Where did the assumption $n_i \geq 3$ enter the proof? It is needed to ensure that 1 and -1 are incongruent modulo n_i.

B.IV.2 Example. Let us return to the example $n = 4 \cdot 5 = 20$, and the table we derived:

$a_1 \backslash a_2$	0	1	2	3	4
0	0	16	12	8	4
1	5	1	17	13	9
2	10	6	2	18	14
3	15	11	7	3	19

We display the four cases by keeping $a_1 = 1$, $a_1 = 3 \equiv -1 \pmod 4$ and $a_2 = 1, a_2 = 4 \equiv -1 \pmod 5$:

$a_1 \backslash a_2$	1	4
1	1	9
3	11	19

□

B.V Linear Congruences

The number n, as usual, is a positive integer.

In this short section we study linear congruences , $ax \equiv b \pmod n$. No really new theory is required.

B.V.1 Theorem. *The congruence $ax \equiv b \pmod n$, $a \nmid n$, is solvable if and only if $(a, n)|b$.*

The solution, in this case, is unique modulo $n/(a, n)$. In other words, the solution set is a residue class modulo $n/(a, n)$, or, equivalently, is made up of (a, n) different residue classes modulo n.

As usual, we express this by saying that the congruence has (a, n) solutions modulo n.

Proof. The congruence $ax \equiv b \pmod n$ is equivalent to the existence of an integer y with $ax - b = ny$; $b = ax - ny$. Thus the congruence is solvable if and only if there are x, y satisfying $b = ax - ny$. This, as we have noted many times before, is equivalent to $(a, n)|b$. That takes care of the existence part.

For the uniqueness part, assuming the condition of the Theorem, we get an equivalent congruence by dividing everything by (a, n). Letting $a' = a/(a, n)$, $b' = b/(b, n)$, $n' = n/(a, n)$, our congruence is equivalent to

$$a'x \equiv b' \pmod{n'}.$$

Now note that $(a', n') = 1$ (Lemma A.V.16), i.e., a' is invertible modulo n'. Letting r' represent the inverse class of $a' + (n')$, $r'a' \equiv 1 \pmod{n'}$, this last congruence is equivalent to

$$x \equiv r'a'x \equiv r'b' \pmod{n'},$$

so the solution set is indeed the residue class $r'b' + (n') = r'b' + (n/(a,n))$.□

The modulus $n' = n/(a,n)$ is sometimes called the *period* of the solution.

B.V.2 Example. A very simple example is given by $27x \equiv 18 \pmod{36}$ with $(27, 36) = 9 \,|\, 18$. Dividing by 9 we get the equivalent congruence $3x \equiv 2 \pmod{4}$. The class of 3 modulo 4 is its own inverse, $3 \cdot 3 \equiv 1 \pmod{4}$. Multiplying by 3 gives us the equivalent congruence $x \equiv 3 \cdot 2 \equiv 2 \pmod{4}$.

So the solution set is the residue class $2 + (4)$. Modulo 36 we get the 9 residue classes $2 + (36)$, $6 + (36)$, $10 + (36)$, ..., $34 + (36)$. □

B.V: Exercises

1. Which of the following linear congruences are solvable? Solve those that are. Be careful to give the right period.

(a) $21x \equiv 12 \pmod{35}$

(b) $21x \equiv 14 \pmod{35}$

(c) $15x \equiv 21 \pmod{36}$

B.VI Congruences Modulo a Prime

We now turn to algebraic congruences of higher degree. It is convenient to start with the simplest modulus possible, a prime number p. The main result is known as *Lagrange's Theorem*

(Luigi Lagrange, 1776-1813, Piemontese mathematician. Lagrange was christened Giuseppe Lodovico, but wrote in French and published under the name Joseph-Louis. The inscription on his statue at Piazza Lagrange in Turin reads: “A Luigi Lagrange - La Patria”).

Most proofs given in the literature are somewhat specialized – here we try to connect with some more general principles.

We fix a prime number p and a polynomial $f(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d$, of degree d, with integer coefficients, and a_0 not divisible by p. We first state a Lemma on polynomial division:

B.VI.1 Lemma. *Let a be an integer. Then there are an integer r and a polynomial $q(X)$, with integer coefficients, such that*

$$f(X) = q(X)(X - a) + r.$$

□

In place of formal proof we remind the reader that division of one polynomial by another, in this case $X - a$, leaves a remainder of lower degree, a rational constant r. As $X - a$ has leading coefficient 1, we never divide coefficients, so all numbers appearing in the process are integers.

We now state and prove Lagrange's Theorem:

B.VI.2 Theorem (Lagrange on Congruences mod p). *The algebraic congruence $f(x) \equiv 0 \pmod{p}$ has at most d solutions modulo p.*

Proof. The case $d = 1$, i.e., a linear congruence, is covered by the result of the previous Section. The solution set to $ax + b \equiv 0 \pmod{p}$, $p \nmid a$, is a single residue class modulo $p/(p, a) = p$.

We now turn to the case $d > 1$. Let $a + (p)$ be one solution class (if there are no solutions there is nothing to prove!). Perform the division $f(X) = q(X)(X - a) + r$, according to the Lemma, with q of degree $d - 1$. Modulo p we get $0 \equiv f(a) \equiv q(a)(a - a) + r \pmod{p}$, so $r \equiv 0 \pmod{p}$.

Therefore $f(X) \equiv q(X)(X - a) \pmod{p}$ in the sense of coefficientwise congruence. If $b+(p)$ is a solution class of the congruence, then $f(b) \equiv q(b)(b-a) \pmod{p}$.

If a prime number divides a product, it divides one of the factors, $b \equiv a \pmod{p}$ or $q(b) \equiv 0 \pmod{p}$. By induction we may assume that the congruence $q(x) \equiv 0 \pmod{p}$ has at most $d - 1$ solutions modulo p. Hence the congruence $f(x) \equiv 0 \pmod{p}$ has at most $d - 1 + 1$ solutions modulo p. □

B.VI.3 Example. Let us solve the congruence $f(x) = x^2+x+5 \pmod{11}$.

We start by completing the square:

$$0 \equiv x^2 + x + 5 \equiv x^2 - 10x + 5 \equiv (x - 5)^2 + 5 - 25 \equiv (x - 5)^2 - 9 \pmod{11}.$$

So we are reduced to

$$y^2 \equiv (x - 5)^2 \equiv 9 \pmod{11}.$$

The congruence $y^2 \equiv 9 \pmod{11}$ has the two obvious solutions $y \equiv \pm 3 \pmod{11}$. By Lagrange there can be no more solutions. So our original problem reduces to $x-5 \equiv \pm 3 \pmod{11}$, giving us the solutions $x = 8+(11)$ and $x = 2 + (11)$. □

Note that we *do not* introduce "classroom formulas" involving "square roots". First, such "modular square roots" may not exist: e.g., the congruence $x^2 \equiv 2 \pmod{11}$ has no solutions at all. Second, if they do exist they come in pairs, and there is no canonical way to choose one of the two roots, in such a way that, e.g., the product rule for square roots holds. In the real case, by contrast, the (positive) square root of a non-negative number is *unique*, with a nice multiplicativity property, $\sqrt{ab} = \sqrt{a} \cdot \sqrt{b}$.

It should perhaps be noted that solving the quadratic congruence $x^2 \equiv m \pmod{p}$ is far from trivial, for large p, except for those p belonging to certain congruence classes. We will return to that question later on.

The following Theorem shows the power of polynomial congruences in proving numerical ones.

B.VI.4 Theorem (Wilson's Theorem). *Let p be a prime number. Then* $(p-1)! \equiv -1 \pmod{p}$.

Proof. The case $p = 2$ is trivial, so let us assume p odd.

Consider the polynomial $f(X) = X^{p-1} - 1$. By Little Fermat we have $f(k) \equiv 0 \pmod{p}$ for $k = 1, 2, \ldots, p-1$, giving $p-1$ incongruent solutions modulo p. By Lagrange there can be no further solutions.

By the proof of Lagrange each root produces a factor, e.g.,

$$f(X) \equiv (X-1)q(X) \pmod{p}$$

(coefficientwise congruence), with q of degree $p-2$. As there are no zero-divisors modulo p we must have $q(k) \equiv 0 \pmod{p}$ for $k = 2, 3, \ldots, p-1$. Repeating the argument several times we arrive at the factorization

$$f(X) \equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod{p},$$

again in the sense of coefficientwise congruence.

Putting $X = 0$ we get $-1 \equiv (-1)(-2)\cdots(-(p-1)) \pmod{p}$. As $p-1$ is even we get our result. □

An alternative proof is given in the exercises. The converse is also true. If $-(n-1)! \equiv 1 \pmod{n}$, then every non-zero class modulo n is invertible. Namely, the inverse is minus the product of the other non-zero classes. And this can only happen if n is prime, by Corollary A.IV.

B.VI: Exercises

1. Show that $(n-1)! \equiv 0 \pmod{n}$ if n is composite and not equal to 4.

2. Prove Wilson's Theorem (B.VI.4) by pairing factors and noting that only the classes of ± 1 are their own inverses modulo p (why?).

3. p is an odd prime. Show that $(p-3)! \equiv (p-1)/2 \pmod{p}$.

4. Let $p > 5$ be a prime. Show that $(p-1)! + 1$ has at least two different prime factors (one of them is given by Wilson's Theorem). One possible route would be to show that $(p-1)!$ is divisible by $(p-1)^2$. Assume that $(p-1)! + 1$ is a power of p and derive a contradiction.

5. (a) $f(X)$ is a polynomial with integer coefficients, of degree d. Show that $g(X) = X^d f(1/X)$ also is a polynomial with integer coefficients. Describe them in terms of f.

(b) Consider $f(X)$ modulo $n > 0$. Let a, $(a, n) = 1$ be an invertible root modulo n. Show that its inverse modulo n is a root of g

(c) Let p be a prime number. Suppose the constant term of f is 1, and that f has d roots modulo p. Show that its first-degree coefficient equals minus the sum of the inverses $\pmod p$ of the roots of f.

(d) Consider the integer

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k}$$

Show that it is divisible by p^2. Consider the polynomial $f(X) = X^{p-1} - 1$, use the previous item, and the value of $f(p)$ modulo p.

B.VII Modulo a Prime Power

The main obstacle to solving a polynomial congruence modulo the prime power p^k is finding the solutions modulo p. Once they are found, the problem reduces to the linear case.

The general theory is preceded by an Example (continuing B.VI.3.)

B.VII.1 Example. We want to solve the algebraic congruence $f(x) = x^2 + x + 5 \equiv 0 \pmod{11^2}$.

Any x satisfying the congruence also satisfies the same congruence taken modulo 11. So it is quite natural to start with the solution classes to the latter congruence and then seek to "refine" or "modify" them, so that they work modulo 11^2 as well.

So we plug $x = x_0 + r \cdot 11$, with $x_0 = 2$ or 8, into the congruence:

$$(x_0 + r \cdot 11)^2 + (x_0 + r \cdot 11) + 5 \equiv 0 \pmod{11^2}.$$

Expanding, and sorting terms, we get:

$$(x_0^2 + x_0 + 5) + r \cdot (2x_0 + 1) \cdot 11 \equiv 0 \pmod{11^2}.$$

The sum in the first pair of parentheses is $f(x_0) \equiv 0 \pmod{11}$ by the choice of x_0. The second one contains the derivative $f'(x_0) = 2x_0 + 1$.

Writing $f(x_0) = s \cdot 11$ we see, dividing by 11, that our congruence is equivalent to:

$$s + r \cdot f'(x_0) \equiv 0 \pmod{11},$$

which is a linear congruence (in r), modulo 11. We now separate the two cases.

$\underline{x_0 = 2}$: In this case $f(2) = 1 \cdot 11$, $s = 1$, and $f'(2) = 2 \cdot 2 + 1 = 5$ so we get the following:

$$1 + 5r \equiv 0 \pmod{11}.$$

The inverse class of $5 + (11)$ is $9 + (11)$. Multiplying the congruence by 9 therefore gives:

$$r + 9 \equiv 0 \pmod{11}, \quad r \equiv 2 \pmod{11}, \quad x \equiv 2 + 2 \cdot 11 \equiv 24 \pmod{11^2}.$$

$\underline{x_0 = 8}$: This time $f(x_0) = f(8) = 77 = 7 \cdot 11$, $s = 7$, and $f'(x_0) = 2 \cdot 8 + 1$, so we are led to the following linear congruence:

$$7 + 17r \equiv 7 + 6r \equiv 0 \pmod{11}.$$

The inverse class of $6 + (11)$ is $2 + (11)$ yielding

$$14 + r \equiv 3 + r \equiv 0 \pmod{11}, \quad r \equiv 8 \pmod{11},$$

and the solution is

$$x \equiv 8 + r \cdot 11 = 96 \pmod{11^2}.$$

□

In both cases each solution class $x_0 + (11)$ refined to a unique solution class modulo 11^2. Essential to both cases was the fact that $f'(x_0) \not\equiv 0 \pmod{11}$.

We now turn to the general theory. We start with a very basic case of *Taylor's Theorem.*

B.VII.2 Theorem (Short Taylor). *Let $f(x)$ be polynomial with integer coefficients, x_0 and h integers. Then*

$$f(x_0 + h) \equiv f(x_0) + f'(x_0)h \pmod{h^2}.$$

Proof. By linearity (e.g., of differentiation), it is enough to deal with monomials $f(x) = x^k, f'(x) = kx^{k-1}$. By the Binomial Theorem,

$$f(x_0 + h) = (x_0 + h)^k = x_0^k + khx_0^{k-1} + \text{terms containing higher powers of } h$$
$$\equiv f(x_0) + f'(x_0)h \pmod{h^2}.$$

□

The main result of this Section is known as *Hensel's Lemma* (Kurt Hensel, Prussian mathematician, 1861-1941). We have already exemplified the Theorem in the case $p = 11$, $k = 1$.

B.VII.3 Theorem (Hensel's Lemma). *Let $f(x)$ be polynomial with integer coefficients, Suppose the integer a, hence the whole class $a + (p^k)$, satisfies the congruence*

$$f(a) \equiv 0 \pmod{p^k},\ k \geq 1.$$

We seek to modify a to a solution $x = a + r \cdot p^k$ of the congruence

$$f(x) \equiv 0 \pmod{p^{k+1}}.$$

Such a modification is uniquely determined modulo p^{k+1} if and only if $f'(a) \not\equiv 0 \pmod{p}$.

Proof. We rewrite the assumption $f(a) \equiv 0 \pmod{p^k}$ as $f(a) = s \cdot p^k$. We seek to determine r (uniquely, modulo p) so that

$$f(a + r \cdot p^k) \equiv 0 \pmod{p^{k+1}}.$$

By Taylor's Theorem,

$$f(a + r \cdot p^k) \equiv f(a) + r \cdot f'(a)p^k \pmod{r^2p^{2k}}$$

with $2k \geq k + 1$, so the condition can be re-written as

$$f(a) + r \cdot f'(a)p^k \equiv 0 \pmod{p^{k+1}},$$

i.e.,

$$s \cdot p^k + f'(a) \cdot rp^k \equiv 0 \pmod{p^{k+1}}.$$

Dividing everything by p^k we see that this is equivalent to the following linear congruence in r:

$$s + f'(a) \cdot r \equiv 0 \pmod{p}.$$

If $f'(a) \not\equiv 0 \pmod{p}$ this congruence is uniquely solvable modulo p, hence the refinement $a' = a + rp^k$ exists, and is uniquely determined modulo p^{k+1}.

If $f'(a) \equiv 0 \pmod{p}$, and $s \not\equiv 0 \pmod{p}$, the congruence is obviously not solvable.

And if $s \equiv f'(a) \equiv 0 \pmod{p}$, any r will do, i.e., the whole class $a + (p^k)$ satisfies the congruence $f(x) \equiv 0 \pmod{p^{k+1}}$. The congruence is solvable, but we do not get a unique solution modulo p^{k+1}. □

B.VII.4 Example. We illustrate the pathological last two cases of the proof.

a) We start with the congruence $f(x) = x^3 + x^2 + 3 \equiv 0 \pmod{5}$. The solutions are easily found by trial and error: they are $x = 1 + (5)$ and $2 + (5)$.

We now try to modify the first class to a solution for the same congruence taken modulo $5^2 = 25$.

In this case we have $f(1) = 5 = s \cdot 5$, where $s = 1$, and $f'(1) = 5$. Trying $x = 1 + r \cdot 5$ the procedure of the proof leads to the linear congruence $s + 5 \cdot r = 1 + 5 \cdot r \equiv 1 + 0 \cdot r \equiv 5$, which is clearly impossible.

b) Now we study instead $f(x) = x^3 + x^2 + 23 \equiv 0 \pmod{25}$. Modulo 5 it is the same congruence as above, so again one solution class is $1 + (5)$.

This time $f(1) = 5 \cdot 5$, $f'(1) = 5$.

Trying $x = 1 + r \cdot 5$ leads to the linear congruence $5 + 5 \cdot r \equiv 0 \pmod 5$, which is visibly true for all r. So we obtain the solution class $1 + (5)$ for this congruence as well.

Modulo 25 we get five solution classes, of course: $1 + (25)$, $6 + (25)$, $11 + (25)$, $16 + (25)$, $21 + (25)$.

The solution class $2 + (5)$ does not give rise to these pathologies. In the first example it refines to $12 + (25)$, in the second to $17 + (25)$. □

B.VII.5 Example. This example shows how the pathology noted above can be used to advantage, sometimes.

We study the congruence $f(x) = x^2 - b \equiv 0 \pmod{2^e}$ where b is an odd integer, and $e \geq 3$. Suppose we have found a solution a, obviously odd. Does it refine to a solution for the congruence $f(x) = x^2 - b \equiv 0 \pmod{2^{e+1}}$?

As $f'(x) = 2x \equiv 0 \pmod 2$, for *all* x, no solution can have a unique refinement modulo 2^{e+1}. Therefore it is somewhat pointless (and messy) to try $x = a + r \cdot 2^e$– much better to try $x = a + r \cdot 2^{e-1}$ instead!

As always, we rewrite the assumption on a as $a^2 - b = s \cdot 2^e$. With the x we are trying we get

$$\begin{aligned} f(x) &= (a + r \cdot 2^{e-1})^2 - b \\ &= a^2 - b + 2ar \cdot 2^{e-1} + r^2 \cdot 2^{2e-2} \\ &= s \cdot 2^e + 2ar \cdot 2^{e-1} + r^2 \cdot 2^{2e-2}. \end{aligned}$$

By assumption, $e \geq 3$, so $2e - 2 = e + (e - 2) \geq 3 + (e - 2) = e + 1$. Hence the congruence $f(x) = x^2 - b \equiv 0 \pmod{2^{e+1}}$ translates into

$$s \cdot 2^e + 2ar \cdot 2^{e-1} \equiv 0 \pmod{2^{e+1}}.$$

Dividing everything by 2^e we get the equivalent linear congruence $s + ar \equiv 0 \pmod{2}$. Recall that $a \equiv 1 \pmod{2}$. So our solution indeed refines – simply take $r \equiv s \pmod{2}$!

Now it is easy to determine those odd b for which the congruence $x^2 \equiv b \pmod{2^3}$ is solvable. As $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ it is solvable iff $b \equiv 1 \pmod{8}$.

The above argument then shows how any of these solutions can be refined inductively modulo higher and higher powers.

So, for odd b, and $e \geq 3$, the congruence $x^2 \equiv b \pmod{2^e}$ is solvable if and only if $b \equiv 1 \pmod{8}$. □

Remark: We note that the solution set modulo 8, in the case of solvability, is given by two classes modulo 4: 1 + (4), and 3 + (4). Following the procedure of the Example, we see inductively that the solution set of $x^2 \equiv b \pmod{2}^e$, $e \geq 3$, is given by two classes modulo 2^{e-1}, or, equivalently, 4 classes modulo 2^e.

The case of an odd prime presents no pathologies, as $f'(x) = 2x \equiv 0 \pmod{p}$ if and only if $x \equiv 0 \pmod{p}$. The case of $p = 2$ is in many contexts the source of some very stimulating confusion.

Once we have dealt with prime powers, the case of an arbitrary modulus presents no problems. By the Chinese Remainder Theorem (B.I.4, B.I.5), it can be reduced to congruences modulo the prime powers entering the factorization of n. This is clear from our last Theorem of this Chapter:

B.VII.6 Theorem. *Suppose $n = n_1 n_2$, where $n_1, n_2 > 0$; $(n_1, n_2) = 1$. The algebraic congruence $f(x) \equiv 0 \pmod{n}$ is solvable if and only the two congruences $f(x) \equiv 0 \pmod{n_1}$, and $f(x) \equiv 0 \pmod{n_2}$, are.*

If the first of these has e_1 solutions modulo n_1, and the second has e_2 solutions modulo n_2, the original congruence has $e_1 e_2$ solutions modulo $n_1 n_2$.

Proof. Any x satisfying the original congruence must satisfy the two auxiliary ones, so the "only if" part is trivial.

Now suppose $x_i + (n_i)$, $i = 1, 2$ satisfy the two auxiliary congruences. Then the Chinese congruence pair

$$\begin{aligned} x &\equiv x_1 \pmod{n_1} \\ x &\equiv x_2 \pmod{n_2} \end{aligned}$$

produces a unique class $x + (n_1 n_2)$ satisfying $f(x) \equiv f(x_i) \equiv 0 \pmod{n_i}$, for $i = 1, 2$. The Second Divisibility Theorem (A.II.2) then shows that this is equivalent to $f(x) \equiv 0 \pmod{n_1 n_2}$.

The "if" part, and the quantitative statement, both follow from this observation. □

B.VII.7 Example. A simple example is afforded by the congruence $x^2 \equiv 25 \pmod{72 = 2^3 \cdot 3^2}$.

The congruence $x^2 \equiv 25 \equiv 1 \pmod 3$ has the solution classes $\pm 1 + (3)$. Using Hensel's Lemma (B.VII.3), these refine uniquely to the two solution classes $\mp 5 + (9)$ for $x^2 \equiv 25 \equiv 7 \pmod 9$.

The congruence $x^2 \equiv 25 \equiv 1 \pmod 8$ has the four solution classes $1 + (8)$, $3 + (8)$, $5 + (8)$, $7 + (8)$, as noted above. So the original congruence has $2 \cdot 4 = 8$ solution classes modulo 72. The reader might like to determine them, or at least check them. Their least positive representatives modulo 72 are $5, 13, 23, 31, 41, 49, 59, 67$. □

B.VII: Exercises

1. Suppose that x is inverse to a modulo p^k, where p is a prime. Show how to refine x into an inverse to a modulo p^{k+1}.

2. The conclusion of Hensel's Lemma may be strengthened, so as to speed up the refining process for large powers of p. Show this.

   If you are familiar with Newton's Method from (numerical) Analysis you will perhaps see a close analogy (quadratic convergence).

3. We wish to solve the congruence $2x \equiv 3 \pmod{5^e}$, $e \geq 1$. Hensel's Lemma leads us to putting $x = k_0 + k_1 5 + k_2 5^2 + \cdots + k_{e-1} 5^{e-1}$, where the k_i are to be determined.

4. Find all solutions to $x^3 \equiv 8 \pmod{31}$ and $x^3 \equiv 8 \pmod{31^2}$. Hand calculation: the first part can be reduced to a quadratic congruence, completion of squares, and a (short) simple linear search.

5. (a) Solve the congruence $x^2 + x + 34 \equiv 0 \pmod{3, 9, 27, 81}$ (short hand calculation).

(b) Solve the same congruence modulo 51, 25, 153.

(c) Solve $x^2 + x + 5 \equiv 0 \pmod{17}$ and $\pmod{17^2}$.

6. (a) The congruence $x^2 \equiv 1 \pmod{91}$ has exactly four solution classes; determine these.

(b) How many solution classes does the congruence

$$x^2 \equiv 1 \pmod{1729}$$

possess? Determine at least one $\not\equiv \pm 1 \pmod{1729}$.

7. Consider the congruence $X^4 - 15X^2 + 1 \equiv 0 \pmod{16}$. Show that the left member can be factored into to quadratic factors. Explain how this factorization proves the non-solvability of the congruence. Also show that the left member does not factor into a linear and a cubic factor (note that 16 is not a prime number!)

Finally show that the left member does not factor modulo 32.

8. p is an odd prime not dividing D or k. Suppose the congruence

$$x^2 - Dy^2 \equiv k \pmod{p^n}$$

has m solution pairs (x, y) modulo p^n. Show that

$$x^2 - Dy^2 \equiv k \pmod{p^{n+1}}$$

has mp solutions modulo p^{n+1}.

Try to generalize to arbitrary quadratic forms $ax^2 + bxy + cy^2$ – can you find the proper condition on the coefficents or some quantity derived from them?

9. (a) Derive the full Taylor expansion (cf. B.VII.2) $f(X + h) = f(X) + hf'(X) + \cdots$, by using the Binomial Theorem on each monomial.

(b) Let f be an integer polynomial, and m an integer. Show, using the Taylor expansion of $f(m + h)$ that there is some n such that $f(n)$ is properly divisible by $f(m)$. Hence conclude that f cannot assume only prime values.

10. Let p be an odd prime. Consider the product $p(X) = \prod(X - t)$ where t runs over a full system of representatives of the invertible classes modulo $n = p^k$, $k \geq 1$. The degree of that polynomial is $\phi(p^k)$. It is *not* congruent to $X^{\phi(n)} - 1$ for $k \geq 2$, in the sense of coefficientwise congruence – note that Lagrange does not apply as there are zero-divisors modulo p^k.

Instead it holds that

$$p(X) \equiv (X^{p-1} - 1)^{p^{k-1}} \pmod{p^k}$$

One possible route may be the following:

(a) Prove that

$$Y(Y - 1 \cdot p^k)(Y - 2 \cdot p^k) \cdots (Y - (p-1) \cdot p^k) \equiv Y^p \pmod{p^{k+1}},$$

in the sense of coefficientwise congruence.

(b) Using the last congruence, for $Y = X - a$, $0 < a < p^k$, $p \nmid a$, and induction on k, prove the congruence stated above. For instance, in the case $k = 2$, combine (a) with the identity

$$(X-1)(X-2) \cdots (X - (p-1)) = X^{p-1} - 1 + pg(X).$$

Chapter C

Primitive Roots

C.I False Cases Excluded

Primitive roots are an important theoretical tool, e.g., in our discussion of power residues later on. Their existence, or non-existence, explains some of the phenomena we have already encountered. In the case of existence they lead to the concept of discrete logarithms, and some cryptographic schemes connected with them.

First we give their definition.

C.I.1 Definition. Let n be a positive integer, and put $f = \phi(n)$. A **primitive root modulo** n (or "for n") is an integer g such that $\mathrm{ord}_n(g) = f$, in other words, such that the powers $1, g, g^2, \ldots, g^{f-2}, g^{f-1}$ are pairwise incongruent modulo n.

Clearly, the property of being a primitive root only depends on the class $g + (n)$ of g modulo n. Yet another way of phrasing the definition is to demand that the powers $[1], [g], [g^2], \ldots, [g^{f-2}], [g^{f-1}]$ exhaust the invertible classes modulo n. Or, equivalently: that for each m, with $(m, n) = 1$, there exist an exponent k such that

$$m \equiv g^k \pmod{n}.$$

That exponent k, the *index* (or *discrete logarithm*) of m modulo n, w.r.t. g, is then uniquely determined modulo f:

$$g^l \equiv g^k \pmod{n} \Longleftrightarrow l \equiv k \pmod{f}.$$

Before discussing the question of existence, let us give a simple example.

C.I.2 Example. Let $n = 7$. In an earlier Example (A.V.13) we noted that the orders of 3 and 5 modulo 7 are 6, so these two are primitive roots modulo 7. The following table lists the indices of $1, 2, \ldots, 6$ with respect to these primitive roots.

$g\backslash m$	1	2	3	4	5	6
3	0	2	1	4	5	3
5	0	4	5	2	1	3

Note that the classes $3 + (7), 5 + (7)$ are inverses of one another, and that the indices w.r.t to these two bases add up to 6. □

We now prove a Lemma on binomial congruences that will help us exclude all those n for which there are no primitive roots. The letter f still denotes $\phi(n)$.

C.I.3 Lemma. *Suppose g is a primitive root modulo n. Then the congruence*

$$x^k \equiv 1 \pmod{n}$$

has $(k, f) \leq k$ solutions modulo n.

Proof. Put $x \equiv g^y \pmod{n}$, with y yet to be determined. Our binomial congruence is then equivalent to a linear congruence modulo f:

$$x^k \equiv 1 \pmod{n} \Longleftrightarrow g^{ky} \equiv 1 \pmod{n} \Longleftrightarrow ky \equiv 0 \pmod{f}.$$

In the Section on linear congruences, B.V, we noted that this is equivalent to

$$\frac{k}{(k,f)}y \equiv 0 \pmod{\frac{f}{(k,f)}},$$

with (k, f) solution classes modulo f. □

C.I.4 Lemma. *In the following cases there are no primitive roots modulo n:*

a) $n = n_1 n_2$, *with* $n_1, n_2 \geq 3$ *and* $(n_1, n_2) = 1$.

b) $n = 2^e$, $e \geq 3$.

Proof. In case a), we proved in Lemma B.IV.1 that the congruence $x^2 \equiv 1 \pmod{n}$ possesses at least $4 > 2$ solutions modulo n. So that case is excluded by the Lemma above.

In case b) we easily exhibit the following four incongruent solutions to the congruence $x^2 \equiv 1 \pmod{n}$:

$$x \equiv \pm 1 \pmod{2^e}; \qquad x \equiv \pm 1 + 2^{e-1} \pmod{2^e}.$$

We check the last two:

$$(1 \pm 2^{e-1})^2 = 1 \pm 2 \cdot 2^{e-1} + 2^{2e-2} \equiv 1 \pmod{2^e}$$

as $2e - 2 > e$ for $e \geq 3$.

So that case, too, is excluded by the previous Lemma. □

The first case implies that n cannot have two different odd prime factors. If n has one odd prime factor, the factor 2 can enter its factorization only with multiplicity one, as $2^2 > 3$. So we have proved the following:

C.I.5 Theorem (Provisional). *A primitive root modulo n can exist at most in the following cases:*

$$n = 2, \qquad n = 4, \qquad n = p^k, \text{ and } n = 2 \cdot p^k,$$

where p is an odd prime.

□

For $n = 2$ obviously $g = 1$ is a primitive root. For $n = 4$, take $g = 3$.

In the remaining cases the existence of primitive roots is far from obvious. We will devote one Section to proving the case $n = p$, and then return to odd prime powers later on. The extra factor 2 will then present no problem, according to the following Theorem.

C.I.6 Theorem. *Suppose g is an odd primitive root modulo the odd positive integer n. Then g is also a primitive root modulo $2n$.*

Remark: If g is an even primitive root, then $g + n$ is an odd one.

Proof. We first note that, for odd g, $(g, n) = 1 \Longrightarrow (g, 2n) = 1$.

Next we note that $\phi(2n) = \phi(2)\phi(n) = \phi(n) = f$. So, by Euler's Theorem, $g^f \equiv 1 \pmod{2n}$.

And $g^k \not\equiv 1 \pmod{n}$ for $0 < k < f$ trivially implies $g^k \not\equiv 1 \pmod{2n}$. So the exact order of g modulo $2n$ must equal f. □

C.II Primitive Roots Modulo a Prime

Let p be a prime number. This section is devoted to a proof of the existence of a primitive root modulo p. As in all known proofs a main ingredient is Lagrange's Theorem (B.VI.2) on algebraic congruences modulo p. You may want to review that Theorem. Other important ingredients are the Theorems on the order of a power and a product.

C.II.1 Theorem (Primitive Roots mod p). *Let p be a prime number. Then there is a primitive root modulo p, i.e., an element g satisfying $\mathrm{ord}_n(g) = \phi(p) = p - 1$.*

Proof. Choose an element a such that $\mathrm{ord}_n(a) = d$ is maximal. We wish to prove that $d = f = p - 1$. We assume that $d < f$ and derive a contradiction.

According to Lagrange, the congruence $x^d \equiv 1 \pmod{p}$ has at most $d < p - 1$ solutions modulo p. So we let b be a non-solution. This is the same as saying that $e := \mathrm{ord}_p(b)$ does not divide d.

Consider the prime factorizations of d, e. The fact that $e \nmid d$ translates to the existence of a prime factor q dividing e to higher multiplicity than d. In other words, there exist a prime number q and exponents $k > j \geq 0$, such that

$$\begin{aligned} d &= q^j \cdot r, \quad (q, r) = 1 \\ e &= q^k \cdot s, \quad (q, s) = 1. \end{aligned}$$

By the Theorem on the order of powers (A.V.17), we then have

$$\begin{aligned} \operatorname{ord}_p(a^{q^j}) &= r, \\ \operatorname{ord}_p(b^s) &= q^k. \end{aligned}$$

As $(q^k, r) = 1$, by the Theorem on the order of a product (A.V.19), we then get

$$\operatorname{ord}_p(a^{q^j} \cdot b^s) = q^k \cdot r > q^j \cdot r = d,$$

contradicting the maximality of d. This contradiction proves the Theorem. □

By exactly the same reasoning one can prove the following

C.II.2 Corollary (of Proof). *Let n be a positive integer, and let $a + (n)$ be an invertible class modulo n, of maximal order e. Then the order of any other class $b + (n)$ divides e.*

□

The proof given above is obviously non-constructive. Can primitive roots be computed?

Indeed they can, if we know how to decompose $p - 1$ into prime factors. One naive method is then to select $r = 2, 3, \ldots$, and compute their various powers

$$r^{(p-1)/q} \pmod{p}$$

for all prime factors $q | (p - 1)$.

As soon as all these powers, for a given a, are incongruent to 1 (mod p), we have found a primitive root, in fact the least positive one (we are using Theorem A.V.6.) The chances of a small primitive root are fairly good.

One will then need an algorithm for fast exponentiation, e.g., the one given in Section L.V. It is a built-in feature in Python and Maple, by the way.

C.II.3 Example. Let $p = 40487$, a prime. We have the factorization $p-1 = 2 \cdot 31 \cdot 653$. Using fast exponentiation one verifies that $r = 2, 3$ satisfy

$$r^{(p-1)/2} \equiv 1 \pmod{40487}$$

so neither 2 nor 3 is a primitive root. The above congruence reflects the fact that both 2 and 3 are squares modulo p:

$$34105^2 \equiv 2 \pmod{p}, \quad 21395^2 \equiv 3 \pmod{p}$$

so that

$$2^{(p-1)/2} \equiv 340105^{p-1} \equiv 1 \pmod{p},$$

by Little Fermat, and similarly for 3.

No use testing $r = 4 = 2^2$!

$r = 5$ is more successful:

$$\begin{aligned} 5^{(p-1)/2} &\equiv -1 \pmod{p} \\ 5^{(p-1)/31} &\equiv 32940 \pmod{p} \\ 5^{(p-1)/653} &\equiv 4413 \pmod{p} \end{aligned}$$

so 5 is the least positive primitive root modulo 40487. □

C.II.4 Example (Decimal Fractions, Continued). In one of Robert Ripley's (1890-1949) "Believe It Or Not" books the number $N = 142857$ is cited as having a remarkable property. When multiplied by 2, 3 ,4, 5, 6, its digits are simply shifted cyclically, e.g., $5 \cdot 142857 = 714258$. How remarkable is that, and what is the explanation?

Well, $7 \cdot 142857 = 999999$, i.e., $(10^6 - 1)/7 = 142857$, so 142857 is the period in the decimal expansion of 1/7.

For instance, the relation $5 \cdot 142857 = 714258$ can be rewritten as $5/7 = 5 \cdot 0.1428571428 \cdots = 0.7142587142 \cdots = 10^5 \cdot (1/7) - 14285$, $10^5 = 5 + 7 \cdot 14285$, so that:

$$10^5 \equiv 5 \pmod{7}.$$

The fact that *all* the multiples $N, 2N, 3N, \ldots, 6N$ are cyclical shifts of N similarly reflects the fact that 1, 2, 3, 4, 5, 6 are powers of 10 modulo 7, i.e., $10 \equiv 3 \pmod{7}$ is a *primitive root* modulo 7.

Modulo 13, by contrast, the order of 10 is 6, and the powers of 10 are 1, 3, 4, 9, 10, 12. The expansion of 1/13 is $0.076923076\ldots$, and the expansion of 9/13 is $0.692307692\ldots$ a shift by two places, corresponding to $10^2 \equiv 9 \pmod{13}$.

On the other hand $5/13 = 0.38461538\ldots$, $7/13 = 0.538461538\ldots$ are not cyclic shifts of 1/13, but they are cyclic shifts of one another, reflecting the fact that $7 \cdot 10 \equiv 5 \pmod{13}$.

A moment's reflection makes it clear that the invertible classes modulo 13 are partitioned into two sets, the powers of 10 modulo 13, and the classes of $7 \cdot 10^k$, $k = 0, 1, 2, 3, 4, 5, 6$, modulo 13, with each of the two sets having the cyclic shift property. Here the factor 7 can be replaced by any non-power of 10 modulo 13.

Those who have taken a course in Abstract Algebra will recognize the two sets as the cosets of the subgroup generated by 10, in the group of invertible classes modulo 13.

Now, it is easy to write a program finding small primes for which 10 is a primitive root. The first few examples are 7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193.

For instance,

$$N = \frac{10^{16} - 1}{17} = 588235294117647$$

and

$$2 \cdot N = 1176470588235294,$$

not quite a cyclic shift! The explanation is simple: as $1/17 < 1/10$ the decimal expansion begins with a zero:

$$\frac{1}{17} = 0.0588235294117647 05\ldots$$

so we would have to put that zero in front of N. That, I suppose, is the reason $N = 588235294117647$ did not make it into Ripley's book.

Mathematically, the significance of 10 being a primitive root modulo the prime p is that the expansion of $1/p$ has the maximum possible period, $p - 1$.
□

C.III Binomial Congruences

In this Section we study *binomial congruences*, i.e., congruences of the form $bx^n \equiv a \pmod{n}$. Most of the time $b = 1$, and we can reduce to that case if $(b, n) = 1$, of course.

We assume that n possesses a primitive root. We already know this is the case when $n = 2$, 4, p, $2p$, for an odd prime p. In the next Section we will prove the remaining cases $n = p^k$, $2 \cdot p^k$.

Now assume $(a, n) = 1$, and let $f = \phi(n)$. By far the most important case is that of $n = p$, an odd prime, $p \nmid a$, and $f = p - 1$. The reason is that the case of a prime power may, often more conveniently, be reduced to that of a prime, using Hensel's Lemma (B.VII.3).

We now give a general condition for the solvability of the congruence $x^m \equiv a \pmod{n}$. An important special case, $m = 2$, will be used repeatedly in later Chapters.

C.III.1 Theorem (Euler's Criterion). *Assumptions as above. The congruence*

$$x^m \equiv a \pmod{n}$$

is solvable if and only if

$$a^{f/(f,m)} \equiv 1 \pmod{n}.$$

Proof. Let g be a primitive root. We can write $a \equiv g^k \pmod{n}$. We put $x \equiv g^y \pmod{n}$, and turn the given congruence into a linear one:

$$x^m \equiv a \pmod{n} \iff g^{my} \equiv g^k \pmod{n} \iff my \equiv k \pmod{f}.$$

By our Theorem on linear congruences this linear congruence is solvable in y if and only if $(m, f)|k$. As also $(m, f)|f$, this is equivalent to

$$(m, f)|(k, f).$$

The latter divisibility relation is equivalent to

$$\frac{f}{(k, f)}|\frac{f}{(m, f)},$$

i.e., to

$$\operatorname{ord}_n(a) = \operatorname{ord}_n(g^k) | \frac{f}{(m,f)}.$$

According to the basic theory of "order" (A.V.5), this is equivalent to

$$a^{f/(m,f)} \equiv 1 \pmod{n}.$$

□

C.III.2 Example.

a) We first study the congruence $x^5 \equiv 2 \pmod{13}$. Here $f = 13 - 1 = 12$, and $f/(f,5) = 12/1 = 12$. The congruence is solvable, as

$$a^{12} \equiv 1 \pmod{13},$$

by Little Fermat. Clearly, the congruence $x^5 \equiv a \pmod{13}$ is solvable for *all* $a, 13 \nmid a$ (and trivially for $13|a$).

b) What about $x^4 \equiv 10 \pmod{13}$? Here $f/(f,m) = 12/4 = 3$. Trying Euler we get

$$10^3 \equiv (-3)^3 \equiv -1 \not\equiv 1 \pmod{13}.$$

So this congruence is *not* solvable.

c) Our next example is $x^2 \equiv 10 \pmod{13}$. Here $f/(m,f) = 12/(12,2) = 6$ and

$$10^6 \equiv (-3)^6 \equiv (-27)^2 \equiv (-1)^2 \equiv 1 \pmod{13}$$

so the congruence is solvable. It is easy to find the solution classes $6 + (13)$ and $-6 + (13) = 7 + (13)$

The Legendre/Jacobi symbol (D.I.2, D.II.1), and Quadratic Reciprocity (D.I.12) will supply us with a faster method for deciding whether a given quadratic congruence is solvable or not.

d) In contrast with the case $p = 13$, let us show that the congruence $x^2 \equiv a \pmod{19}$, $19 \nmid a$, is solvable *if and only if* $x^4 \equiv a \pmod{19}$ is.

This is immediate from Euler's Criterion, as $(18,2) = (18,4) = 2$ whence $18/(18,2) = 18/(18,4) = 9$. □

C.III: Exercises

1. Verify that 2 is a primitive root modulo 29. Determine all solutions to the congruences $x^m \equiv 1 \pmod{29}$, where $m = 7, 14, 21, 4, 12$.

2. Let $p \equiv 1 \pmod 8$ be a prime number. Show that the polynomial $X^4 + 1$ divides $X^{p-1} - 1$, hence (Fermat, Lagrange!) that it has exactly four roots modulo p – do this without using primitive roots.

Then express the roots in a primitive root. Give at least two examples.

3. 5 is a primitive root modulo $p = 23$, 3 ditto modulo $p = 17$, and 2 is one modulo $p = 13$. Use these primitive roots to determine in each case those numbers m, $(m, p) = 1$, for which there exists some d such that $m^d \equiv -1 \pmod p$.

Compare the results and explain the difference between 23 on the one hand, and 13,17 on the other. And what is the crucial difference between 13 and 17?

4. Careless reasoning – and carelessly chosen examples! – may mislead one into believing that the smallest positive root modulo p is itself a prime. The smallest counterexample is $p = 41$; you can find other examples in the table at the end of the book.

Verify that the orders of 2,3,5 modulo p are 20, 8, and 10, respectively. Hand calculation possible. Note, for instance, that $2^{10} = 2^8 \cdot 2^2$ where the residue of 2^8 is obtained by repeated squaring modulo p. How do the above computations show that the order of 6 is 40? Can you state a general result? (We will prove it later.)

5. p is an odd prime, d is a positive integer. Describe, using primitive roots, the solutions to the congruence $x^d \equiv 1 \pmod p$ (be careful to give the correct period) and show that they are powers of one single solution.

6. For which invertible right members (i.e., $(y, 91)$= 1, etc.) are the following congruences solvable?

(a) $x^6 \equiv y \pmod{91}$.

(b) $x^7 \equiv y \pmod{77}$.

(c) $x^5 \equiv y \pmod{55}$.

Hand calculation. Be careful to give the correct periods, and proper theoretical explanation.

7. Let p be an odd prime number, and k a positive integer, not divisible by $p-1$. Show that

$$1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}.$$

Hint: Turn the sum into a geometric one.

8. Let g be a primitive root modulo p, and $u \not\equiv 0 \pmod{p}$. Compute the expression

$$\sum_{j=1}^{p-2} u^j \cdot (1-g^j)^{-1} \pmod{p}.$$

One way to do this is to convert the expression into one of the form

$$-\sum_{m=1}^{p-1} (m+1)^k \cdot m^{-1} \pmod{p}$$

and use the previous exercise. The answer may be given in terms of the *discrete logarithm* k of u modulo p, given by the condition

$$g^k \equiv u \pmod{p}.$$

The expression is useless for computing k. In later Sections we will discuss some algorithms.

9. What can be said about the product of all primitive roots modulo p?

10. Prove Wilson's Theorem (B.VI.4) by expressing everything in primitive roots.

11. (a) n is a positive integer, $(y,n) = 1$. Show that the congruence $x^k \equiv y \pmod{n}$ has a solution of the form $x \equiv y^u \pmod{n}$ if and only if $\operatorname{ord}_n(y)$ is relatively prime to k.

(b) Let $n = 29$ and consider the congruence $x^4 \equiv 16 \pmod{n}$. Verify that the solutions can be written $x = x_0 z^k, k \in \mathbf{Z}$ (what is their number?) and that exactly one of them is of the form y^u, $y = 16$.

12. Let p, q be different odd primes.

(a) Show that there is some r that is a primitive root for both p and q.

(b) Determine the number of incongruent powers of r modulo $m = pq$. What is the condition that this number is the maximal possible portion of $\phi(pq)$?

(c) Give the condition for the existence of an r such that every x, $(x,m) = 1$ is congruent to plus or minus a power of r modulo pq.

13. Let $p \neq q$ be two (large) odd primes, and e an odd number. Show that the number of solutions $\pmod{pq}$ to the congruence

$$t^{e^n} \equiv t \pmod{pq}$$

equals

$$g(n) = \bigl(1 + (e^n - 1, p - 1)\bigr)\bigl(1 + (e^n - 1, q - 1)\bigr)$$

and is at least 9. Can you give a lower estimate of $g(n)$ in terms of the prime factorizations of $p - 1$, $q - 1$?

Do you see the cryptological significance of this result in connection with RSA (Section A.VI,) for $e =$ the encryption key? You might like to check up on "fixed points" in Riesel's book.

C.IV Prime Powers

It is convenient to prepare the general case by studying the case p^2, p odd, first.

C.IV.1 Theorem. *Let p be an odd prime. Let g be a primitive root modulo p. Then either g or $g+p$ is a primitive root modulo p^2.*

Proof. Let r denote g or $g+p$. By assumption, the order of r modulo p is $p-1$. If $r^e \equiv 1 \pmod{p^2}$, then, a fortiori, $r^e \equiv 1 \pmod{p}$, so $\mathrm{ord}_p(r)$ divides e: $p-1|e$.

By Euler's Theorem (A.V.12), we also have $e|\phi(p^2) = p(p-1)$, which means that e equals $p-1$ or $p(p-1)$. We will show that $g^{p-1} \equiv 1 \pmod{p^2}$ implies $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$.

That is, if the order of g is less than $p(p-1)$, then the order of $g+p$ equals that number. That will complete the proof of the Theorem.

Now, by the Binomial Theorem,

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1) \cdot g^{p-2}p \pmod{p^2},$$

as the omitted terms contain higher powers of p. By assumption, $g^{p-1} \equiv 1 \pmod{p^2}$, yielding

$$(g+p)^{p-1} \equiv 1 + (p^2-p) \cdot g^{p-2} \pmod{p^2},$$

$$(g+p)^{p-1} \equiv 1 - p \cdot g^{p-2} \pmod{p^2}.$$

If the two members were congruent to 1 modulo p^2, we would get:

$$p^2|p \cdot g^{p-2},$$

which is impossible, as the prime number p does not divide g. □

C.IV.2 Example. Let us return to the example $p = 40487$. In an earlier example (Ex. C.II.3) we determined its least positive primitive root, $g = 5$. Using fast exponentiation (Section L.V) we get

$$5^{p-1} \equiv 1 \pmod{40487^2}$$

so 5 is *not* a primitive root modulo p^2.

The Theorem instead supplies us with the primitive root $g + p = 40492$.

The smallest positive primitive root is 10. For $r = 6, 7, 8$, $r^{(p-1)/2} \equiv 1 \pmod{p}$, so these are not even primitive roots modulo p. But $10^{(p-1)/k} \equiv -1, 36722, 11601 \pmod{p}$ for $k = 2, 31, 653$ (the prime factors of $p-1$) shows that 10 is a primitive root modulo p, and $10^{p-1} \equiv 580947964 \not\equiv 1 \pmod{p^2}$ then shows that 10 is a primitive root modulo p^2 (no need to test 9, as 9 is a square).

This is the smallest odd prime having the property that its smallest primitive root modulo p is not a primitive root modulo p^2.

The next larger example, $p = 6692367337$ was found by Andrzej Paszkiewicz several years ago and was communicated to me by Juliusz Brzezinski. The smallest positive primitive root modulo p is 5, the smallest modulo p^2 is 7.

□

Before proving the general case, we recall a convenient piece of notation. Let p be a prime number. If p^k, but not p^{k+1}, divides n, we put

$$v_p(n) = k$$

(the *multiplicity* of p in n, B.III.1). An important observation is the following:

C.IV.3 Lemma. *If $v_p(m) = k$, and $v_p(n) > k$, then $v_p(m + n) = k$.*

Proof. Writing $m = p^k q$, $p \nmid q$, and $n = p^{k+1} r$, we get $m + n = p^k(q + p \cdot r)$, and obviously p does not divide the second factor. □

The result we want to prove is:

C.IV.4 Theorem (Primitive Roots mod p^k). *If g is a primitive root modulo p^2, where p is an odd prime, then it is also one modulo every power p^k, $k \geq 2$.*

The Theorem will follow from the following Lemma and its Corollary.

C.IV.5 Lemma. *Let p be an odd prime. Suppose $a = 1 + t$ where $v_p(t) = j \geq 1$. Then $a^p = 1 + u$ where $v_p(u) = j + 1$.*

Proof.

$$(1+t)^p = 1 + p \cdot t + \binom{p}{2} \cdot t^2 + \binom{p}{3} \cdot t^3 + \cdots = 1 + u$$

Obviously $v_p(pt) = j+1$. The last displayed term, and the omitted terms, are divisible by $p^{3j} > p^{j+1}$ at least, and the third term is divisible by $p^{2j+1} > p^{j+1}$ (we are using $p \neq 2$) so their sum s satisfies $v_p(s) > j + 1$. By our Lemma above,

$$v_p(u) = 1 + v_p(pt) = j + 1.$$

□

C.IV.6 Corollary. *If g is a primitive root modulo p^2, then, for $j \geq 1$, we have*

$$g^{p^{j-1}(p-1)} = 1 + t \text{ where } v_p(t) = j,$$

hence

$$g^{p^{j-1}(p-1)} \not\equiv 1 \pmod{p^{j+1}}.$$

We first prove the Corollary:

Proof. The proof is by induction, starting with $j = 1$. By Little Fermat, $g^{p-1} \equiv 1 \pmod{p}$, and by assumption, $g^{p-1} \not\equiv 1 \pmod{p^2}$. This means that $g^{p-1} = 1 + t$ where p, but not p^2, divides t, i.e., $v_p(t) = 1$. That is the base step. The induction step follows by repeated application the Lemma. □

And now we prove the Theorem.

Proof. Observe that the order of g modulo p^k must divide $\phi(p^k) = p^{k-1}(p-1)$, and be divisible by $\text{ord}_{p^2}(g) = p(p-1)$. It is therefore of the form $p^{j-1}(p-1)$, $j \geq 2$. The Corollary makes it clear that $j = k$. □

We now deal with the case $n = 2^e$, $e \geq 3$. In the first Section we proved that there is no primitive root in this case, i.e., there is no class of the order $\phi(n) = 2^e/2 = 2^{(e-1)}$. There is however one of the next best possible order. That is the content of the following Theorem. Like the odd case, it is preceded by a divisibility Lemma.

C.IV.7 Lemma. *If $a = 1 + t$, $v_2(t) = k \geq 2$, then $a^2 = 1 + u$, $v_2(u) = k + 1$.*

Proof.

$$(1+t)^2 = 1 + 2t + t^2; \quad v_2(2t) = k+1; \quad v_2(t^2) = 2k > k+1.$$

□

C.IV.8 Theorem. *Let $n = 2^e$, $e \geq 3$. Then $ord_n(5) = 2^{e-2} = n/4$.*

The classes of $\pm 5^j$, $0 \leq j < 2^{e-2}$, exhaust the invertible classes modulo n (i.e., the odd ones).

Proof. Repeated application of the Lemma and its proof with $k = 2, 3, \ldots, j$ yields

$$(1+2^2)^{2^j} \equiv 1 + 2^{j+2} \pmod{2^{j+3}}, \quad j \geq 0,$$

proving the first statement.

As for the second statement, we note that the number of the classes indicated is 2^{e-1}. Having determined the order of 5 modulo n, all that remains is to prove

$$5^j \not\equiv -5^k \pmod{2^e},$$

for integers j, k.

That, however, is true already modulo 4. □

C.IV.9 Example. Let $n = 2^e$, $e \geq 3$, and a an odd integer. We return to the congruence

$$x^2 \equiv a \pmod{n},$$

which we studied in the context of Hensel's Lemma, B.VII.3. Setting

$$x \equiv \pm 5^y \pmod{n}; \quad 0 \leq y < n/4,$$

and

$$a \equiv \pm 5^k \pmod{n}; \quad 0 \leq k < n/4,$$

we are led to the following

$$5^{2y} \equiv \pm 5^k \pmod{n}.$$

By the proof of the last Theorem, only the plus sign can hold. So, remembering that $\mathrm{ord}_n(5) = n/4$, we obtain the following linear congruence:

$$2y \equiv k \pmod{\frac{n}{4}}.$$

As $n/4$ is even, this congruence is solvable if and only if k is even, $k = 2m$. It is then equivalent to

$$y \equiv m \pmod{\frac{n}{8}}$$

So the given congruence is solvable if and only if a is of the form

$$a \equiv 5^{2m} \equiv 25^m \pmod{2^e}$$

Clearly, all the admissible a are congruent to 1 modulo 8, so the condition

$$a \equiv 1 \pmod{8}$$

is necessary for solvability.

Is it sufficient? The condition just given is satisfied by exactly 1/8 of the classes modulo n, or, equivalently, by 1/4 of the invertible (odd) ones.

However, selecting the plus sign in the beginning of the solution, and then selecting the even powers, also means selecting 1/4 of the invertible classes. So the number of classes $a+(n)$ satisfying the last two conditions is the same, and the two conditions are indeed equivalent. □

As the main result of this Chapter is scattered all over the place we repeat it here for ease of reference:

C.IV.10 Theorem (Existence of Primitive Roots). *A primitive root modulo n exists in the following cases, and only these:*

$$n = 2; \quad n = 4; \quad n = p^k, \text{ and } n = 2p^k; \text{ where } p \text{ is an odd prime.}$$

The maximal order modulo $n = 2^e$, $e \geq 3$, is $\phi(n)/2 = 2^{e-2}$, and is achieved by the class of 5.

C.IV: Exercises

1. Find a primitive root for each of $p = 11$, 13, 17, 22, 121, 35, then in each case describe all primitive roots in a suitable manner – in particular give their number.

2. If g is a primitive root modulo n, $\phi(n) = f$, which powers of g are also primitive roots? Deduce that the number of primitive roots equals $\phi(f)$.

3. Considering $\phi(f)$ for $f = \phi(p)$, $\phi(p^2)$ ... explain why we should expect the step from p to p^2 to be special when proving the existence of primitive roots.

4. p is a prime number, with primitive root g. Describe those powers of g the orders of which equal a given $q|(p-1)$, hence determine their number.

5. p is a prime number, q divides $p-1$. Determine the number of classes modulo p of order divisible by q, as a sum. Then give a simple upper estimate and a simple condition for equality.

6. Review the proof for p^2. Let g be a primitive root modulo p. Consider the elements $r = g + kp$, $0 \leq k \leq p-1$, congruent modulo p, but not modulo p^2. Show that if one of them is not a primitive root modulo p^2, then the remaining ones are. Hence show that exactly one element in each such class is not a primitive root modulo p^2. Hint: Look at the expression for $\phi(p^2)$.

7. Let g be a primitive root modulo the odd prime power p^k, $k \geq 3$. Show that $g + p^2$ is a primitive root, too. What is the corresponding result for 2^k, $k \geq 4$?

8. Let p be an odd prime. Prove, without using primitive roots (e.g., by induction), that the congruence $x^d \equiv 1 \pmod{p^m}$ has at most d roots modulo p^m.

Then copy the proof for p to prove that there are primitive roots modulo p^m. It is probably convenient to write $d = q \cdot p^k$, $p \nmid q$ and reduce the exponent k using Euler's Theorem, A.V.12.

9. p is an odd prime. Suppose that

$$x^p \equiv 1 \pmod{p^b}.$$

Show that

$$x \equiv 1 \pmod{p^a}$$

for $1 \leq a \leq b-1$.

10. (a) p is an odd prime, $p \nmid y$. Show that the congruence $x^{p^2} \equiv y \pmod{p^2}$ is solvable if and only if $x^p \equiv y \pmod{p^2}$ is.

(b) Show that $x^p \equiv y \pmod{p^3}$ is solvable if and only if $x^p \equiv y \pmod{p^2}$ is.

(c) Does the previous part hold if x^p is replaced by x^{p^2} in the two congruences?

(d) n is an odd integer, $q = p^e$ is a prime power, with p odd, or $e \geq 2$. Show that the number of solutions to $x^n \equiv -1 \pmod{q}$ equals the number of solutions to $x^n \equiv 1 \pmod{q}$.

C.V The Carmichael Exponent

Let n be an integer > 1. Euler's Theorem (A.V.12) states that the order of any invertible class divides $\phi(n)$. In many cases that is a very crude estimate.

C.V.1 Example. $n = 1729 = 7 \cdot 13 \cdot 19$. Here $\phi(n) = 6 \cdot 12 \cdot 18 = 1296$. But according to Little Fermat, for $(a, 1729) = 1$ it holds that

$$a^6 \equiv 1 \pmod{7}; \quad a^{12} \equiv 1 \pmod{13}; \; a^{18} \equiv 1 \pmod{19}.$$

As $[6, 12, 18] = 36$ we get $a^{36} \equiv 1 \pmod{7, 13, 19}$; $a^{36} \equiv 1 \pmod{7 \cdot 13 \cdot 19}$, a much smaller exponent. □

In the course of proving the existence of primitive roots modulo a prime we established the following (cf. C.II.2):

C.V.2 Lemma. *Let a, with $(a, n) = 1$, have maximal order r modulo n. Then the order of any other b, $(b, n) = 1$, divides r.*

□

This leads us to the following Definition:

C.V.3 Definition. The **exponent**, or **Carmichael function**, of n, denoted $\lambda(n)$, is the maximal order of an invertible class modulo n. (By convention, $\lambda(1) = 1$.)

(R. D. Carmichael, American mathematician, 1879-1967.)

We have established the following basic cases:

$$\begin{aligned} \lambda(2) &= 1 \\ \lambda(4) &= 2 \\ \lambda(2^e) &= 2^{e-2} = \frac{\phi(2^e)}{2}, \quad e \geq 3 \\ \lambda(p^e) &= p^{e-1}(p-1) = \phi(p^e), \; p \text{ odd prime.} \end{aligned}$$

Our reduction to these basic cases is based on the following two Lemmas:

C.V.4 Lemma. *Let* $n = n_1 n_2, n_1, n_2 > 1, (n_1, n_2) = 1$. *Assume* $\mathrm{ord}_{n_i}(a) = r_i$, $i = 1, 2$. *Then* $\mathrm{ord}_n(a) = [r_1, r_2]$. *(Recall the notation* $[r, s]$ *for the least common multiple.)*

Proof. Assume $a^e \equiv 1 \pmod{n}$, then the same congruence must hold modulo n_1, n_2; therefore e must be divisible by both r_1 and r_2, hence by their least common multiple $r = [r_1, r_2]$.

Conversely, from $a^{r_i} \equiv 1 \pmod{n_i}$, $i = 1, 2$, follows immediately that $a^r \equiv 1 \pmod{n_i}$, $i = 1, 2$, hence $a^r \equiv 1 \pmod{n_1 n_2}$.

Therefore $e = r$ is the smallest positive exponent satisfying $a^e \equiv 1 \pmod{n_1 n_2}$. □

C.V.5 Lemma. $n = n_1 n_2$ *as in the previous Lemma. If* $\mathrm{ord}_{n_1}(a_i) = r_i$, $i = 1, 2$, *then there is an* $a \equiv a_i \pmod{n_i}$ *satisfying* $\mathrm{ord}_n(a) = [r_1, r_2]$.

Proof. The existence of an $a \equiv a_i \pmod{n_i}$ follows from the Chinese Remainder Theorem, B.I.5. As the order of a modulo n_i is the order of a_i modulo n_i the result now follows from the previous Lemma. □

Using the Lemmas repeatedly we arrive at the following result:

C.V.6 Theorem. *Let* $n = 2^{e_0} p_1^{e_1} p_2^{e_2} \cdots p_d^{e_d}$ *be the prime factorization of* n. *Here* $e_0 \geq 0$; *the* p_i *are distinct odd primes, and the exponents* $e_i \geq 1; i \geq 1$. *Then*

$$\lambda(n) = [\lambda(2^{e_0}), p_1^{e_1-1}(p_1 - 1), p_2^{e_2-1}(p_2 - 1), \ldots, p_d^{e_d-1}(p_d - 1)].$$

□

If there is at least one odd prime factor, and $e_0 \leq 2$, the factor 2^{e_0} contributes nothing, as $p_1 - 1$ is even.

C.V.7 Example. $n = 1729 = 7 \cdot 13 \cdot 19$. We saw above that $\lambda(1729) = [6, 12, 18] = 36$. How many classes have this maximal order? A sufficient condition for $\mathrm{ord}_n(a)$ to be maximal is that a be a primitive root modulo $7, 13, 19$. If g is a primitive root modulo the prime p, then g^k is of the same order if and only if $(k, p-1) = 1$. The number of primitive roots modulo p is therefore $\phi(p-1)$.

So the number of classes of maximal order is at least $\phi(6)\phi(12)\phi(18) = 48$. The smallest primitive roots mod 7, 13, 19 are $3, 2, 2$. Solving a Chinese congruence system we find $a = 990$ to be of maximal order.

But the condition is not necessary! As already $[12, 18] = 36$ the order of 2 modulo 1729 is $[3, 12, 18] = 36$. □

The reader is invited to find the correct number of elements of maximal order.

C.V: Exercises

1. See the last Example, last sentence.

2. Determine the maximal order of an invertible class modulo 1001, and exhibit at least one class of that order.

3. Determine $\lambda(55)$ and the number of classes modulo 55, of maximal order.

4. Show that $\lambda(N)|N$ for $N = 12 \cdot 13$ and $N = 16 \cdot 17$. Can you construct an example divisible by 29?

5. The composite integer $N > 1$ is a *Carmichael number* if $\lambda(N)|N-1$, i.e., if $a^{N-1} \equiv 1 \pmod{N}$ for $(a, N) = 1$.

(a) Verify that 561, 1005, 1729 are Carmichael numbers.

(b) Let p, q be different primes. Show that $N = pq$ is not a Carmichael number. Hint: Can we have $p-1, q-1|(N-1)$?

(c) Show that Carmichael numbers are square-free, i.e., not divisible by the square of a prime.

(d) Show that N is Carmichael if and only if N is square-free, and $p-1|(N-1)$ for all its prime factors p.

6. Let N be an odd positive integer. The number of solutions to the congruence $x^{N-1} \equiv 1 \pmod{N}$ is $\prod_{p|N}(N-1, p-1)$.

7. Determine the Carmichael exponent of 10^e, $e \geq 5$. Show that the elements of maximal order modulo 10^e fall into 32 classes modulo $8 \cdot 25 = 200$. Can you find them, or at least their number? Find at least one that is not a primitive element modulo 5^e.

8. Determine those N (finite in number) for which $a^{N+1} \equiv a \pmod{N}$. Hint: First show that N must be squarefree, then determine the prime factors of N starting from the bottom.

* C.VI Pseudorandom Sequences

This Section is a bit off-topic, but its methods are closely related to the rest of the Chapter. It could be skipped on a first reading.

We wish to generate sequences modulo a big number $m > 0$, exhibiting an irregular random-like behavior. They should be easy and fast to construct. For cryptographic purposes their behavior should be hard to predict, so their construction should be hard to detect. That is a much more stringent requirement and we will ignore it here.

A popular construction is *affine iteration*, or the *linear congruential generator* letting an affine function $f(X) = Y = aX + b \pmod{m}$ act repeatedly on an initial value x_0. We denote the iterates by $x_n = f^n(x_0)$.

If we assume that the function is invertible, the iteration will have a least period $d > 0$, $x_d \equiv x_0 \pmod{m}$, $x_k \not\equiv x_0 \pmod{m}$ for $0 < k < d$.

By the same argument as for invertible residue classes, every exponent $e > 0$ with $x_e \equiv f^e(x_0) \equiv x_0 \pmod{p}$ is a multiple of d. We hope to arrange that this period is exactly m; our sequence of iterates will then assume every value (mod m) exactly once in every period.

The function f is invertible if $(a, m) = 1$. Suppose $ar \equiv 1 \pmod{m}$. Then $Y = aX + b$ if and only if $X = r(Y - b)$, proving invertibility. We will assume $(a, m) = 1$.

We will also assume that $(b, m) = 1$ and that every prime divisor of m also divides $a - 1$. (If 4 divides m we assume that 4 divides $a - 1$.)

Then $((a - 1)x + b, m) = 1$ for *all* x, as no prime factor $p|m$ can divide $(a - 1)x + b \equiv b \pmod{p}$.

We now proceed to prove that the sequence $s_k = f^k(x_0)$ has least period m regardless of x_0. We will deal with m = prime power first, then reduce the general case to that special case.

C.VI.1 Lemma. *The least period of the sequence x_k is the least n for which*

$$\frac{a^n - 1}{a - 1} \equiv 0 \pmod{m}.$$

(for $a = 1$ the left member is interpreted as $n + 1$.)

Proof. By an easy induction

$$f^k(x) = a^k x + b(1 + a + a^2 + \cdots + a^{k-1}) = a^k x + b\frac{a^k - 1}{a - 1}.$$

We will have $f^k(x_0) \equiv x_0 \pmod{m}$ if and only if

$$0 \equiv (a^k - 1)x_0 + b\frac{a^k - 1}{a - 1} \equiv \frac{a^k - 1}{a - 1}[(a - 1)x_0 + b] \pmod{m}.$$

We have shown that the factor in brackets is invertible modulo m, hence the condition is equivalent to

$$\frac{a^k - 1}{a - 1} \equiv 0 \pmod{m}.$$

□

C.VI.2 Lemma. *Assumptions and notation as above. Let $m = p^e$ be an odd prime power.Then the least period of the sequence $f^k(x_0)$ is m.*

Proof. Let $m = p^e$. We are assuming $a - 1 = t$, $v_p(t) = d \geq 1$. We prove first that $v_p((a^{p^n} - 1)/(a - 1)) = n$.

Recall (C.IV.5) that $b = 1+u$, $v_p(u) = j \geq 1$ implies $b^p = 1+v$, $v_p(v) = j+1$. Using this repeatedly, we get $v_p(a^{p^n} - 1) = n+d$, hence $v_p((a^{p^n} - 1)/(a-1) = n + d - d = n$.

Setting $n = e$ this relation shows that $(a^{p^e} - 1)/(a - 1) \equiv 0 \pmod{p^e}$, hence the period divides p^e. Choosing $n < e$, it shows that $(a^{p^n} - 1)/(a - 1) \not\equiv 0 \pmod{p^e}$, hence the period cannot be a smaller power of p. □

C.VI.3 Lemma. *Assumptions and notation as above. Let $m = 2^e$. Then the least period of the sequence $f^k(x_0)$ is m.*

Proof. The case $e = 1$ is trivial. Now assume $e \geq 2$. This time the assumption is $a = 1+t$, $v_p(t) \geq 2$. Recalling (C.IV.7) that $b = 1+u$, $v_2(u) =$

$j \geq 2$ implies $b^2 = 1 + v$, $v_2(v) = j + 1$, the proof proceeds exactly as in the odd case. □

We now prove the general result.

C.VI.4 Theorem. *Notation and assumptions as before. The least period of the sequence $x_k = f^k(x_0)$ equals m.*

Proof. Let the minimal period modulo m be N.

Let p be a prime factor of m, $v_p(m) = e$. Taken modulo p^e the minimal period of the sequence is p^e; it also repeats with period N. Hence $p^e|N$. As this holds for all of the prime powers dividing m we must have $m|N$.

However, as $x_m \equiv x_0$ modulo each p^e, by the Second Divisibility Theorem (A.II.2), $x_m \equiv x_0$ modulo their product m, so m is indeed a period, hence also the least period. □

This kind of sequence is cryptologically insecure. Setting $y_k \equiv x_k - x_{k-1} \pmod{m}$, $k > 0$, we have $y_{k+1} \equiv ay_k \pmod{m}$, $k > 0$, hence $ay_{k+1}^2 \equiv ay_{k+2}y_k \pmod{m}$. Assuming $(a, m) = 1$ we see that $d_{k+1} = y_{k+1}^2 - y_{k+2}y_k$ is a multiple $\hat{m}$ of m. In fact, the gcd of several successive d_k is often a very small multiple of m.

Solving $y_1 \equiv ay_0 \pmod{\hat{m}}$ for a we have a guess to test. As soon as $y_{k+1} \not\equiv ay_k \pmod{\hat{m}}$ we find that $\hat{m}$ is too big, and we remove the offending factor, so as to get the largest multiple that divides $y_{k+1} - ay_k$. We may have had to make that kind of reduction already when determining a.

It can be proved that the number of y_k that determine the whole sequence is bounded by $2\log_a m$. So we will discover an error pretty quick. Details would take us too far afield.

C.VII Discrete Logarithms

Let g be a primitive root modulo n. For any b, $(b, n) = 1$, the least non-negative number m satisfying

$$g^m \equiv b \pmod{n}$$

is called the *index of b, modulo n, with respect to the base g* (or *discrete logarithm*) and denoted $\log_g(b)$. (Sometimes an extra subscript n is added).

It has the following properties:

$$\begin{aligned}\log_g(ab) &\equiv \log_g(a)\cdot\log_g(b) \pmod{\phi(n)}\\ \log_g(a^k) &\equiv k\cdot\log_g(a) \pmod{\phi(n)}.\end{aligned}$$

The proofs are easy, and left to the reader.

The problem of determining the discrete logarithm $\log_g(a)$ from the knowledge of g, n, a is considered to be very difficult. The *ElGamal cryptographic scheme* profits from this difficulty (as long as it persists). We sketch it briefly.

A large prime number q, and a primitive root g for it, are made public. Alice chooses a secret exponent d, and publishes g^d (reduced modulo q). Bob wants to send the message M (encoded as a number $< q$). He picks an exponent e at random, computes $g^{de} \equiv (g^d)^e$ (again, reduced modulo q), and sends the pair

$$(g^e, s) = (g^e, Mg^{de}).$$

Alice, knowing d, computes $r \equiv g^{de} \equiv (g^e)^d \pmod q$ and solves the congruence $rM \equiv s \pmod q$ for M.

It is assumed that there is no way of computing g^{de} from g^d and g^e, without determining either d or e.

* C.VIII Computing Discrete Logarithms

Let g be a primitive root modulo the prime number P. Let $N = \phi(P) = P-1$, and let a, $0 < a < P$ be given. Solving the congruence

$$g^x \equiv a \pmod P$$

is the Discrete Logarithm Problem, and it is notoriously difficult. The algorithms given below (except Index Calculus) have a running time that is exponential in the bitlength of P – around the square root of P, or of the largest prime factor of $P-1$.

Of the more elementary ones, the Pohlig-Hellman algorithm is probably the easiest to understand, as it rests on two of the main ideas of this text. One is reduction to prime powers and Chinese Remaindering. The other is successive refinement of a solution modulo increasing prime powers. Let us deal with the Chinese Remaindering part first.

Pohlig-Hellman, Reduction to Prime Powers

Let $N = n_1 n_2 \cdots n_d$, $n_i = p_i^{e_i}$, be the prime factorization of N. The p_i are distinct prime numbers, and all the e_i are positive. Put $N_i = N/n_i$, and $a_i = a^{N_i}$ so that the order of a_i modulo P divides n_i. Also put $g_i = g^{N_i}$ so that g_i is of exact order n_i.

Assume that we have managed to solve the congruences

$$g_i^{x_i} \equiv a_i = a^{N_i} \pmod{P}.$$

Assume further that

$$\sum_{i=1}^{d} y_i N_i = 1$$

and set

$$x = \sum_i x_i y_i N_i.$$

Then

$$g^{x_i N_i} = g_i^{x_i} \equiv a_i = a^{N_i} \pmod{P}$$

and

$$g^{\sum_i x_i y_i N_i} \equiv a^{\sum_i y_i N_i} \equiv a \pmod{P}.$$

So $x = \sum_i x_i y_i N_i$ solves the problem. As $y_i N_i \equiv 1 \pmod{n_i}$ and $y_i N_i \equiv 0 \pmod{n_j}$, $j \neq i$, x satisfies the Chinese congruence system (B.I.5):

$$\boxed{x \equiv x_i \pmod{n_i}.}$$

If we are to solve several Discrete Log problems it might be best to precompute the idempotents $z_i = y_i N_i \equiv 1 \pmod{n_i}, \equiv 0 \pmod{n_j}, j \neq i$.

Continuation, Refinement modulo p^e

Let p be one of the prime factors of N, and $e > 0$ its multiplicity. Put $M = N/p^e$, and $b = a^M$, $r = g^M$, so that the order of b divides p^e and the order of r is exactly p^e. We have reduced the problem to solving

$$r^x \equiv b; \quad \mathrm{ord}_P(b) \,|\, \mathrm{ord}_P(r) = p^e.$$

Set

$$x = x_0 + x_1 p + x_2 p^2 + \cdots + x_{e-1} p^{e-1}; \quad 0 \le x_0,\, x_1, \ldots, x_{e-1} < p.$$

We first find x_0. Putting

$$r_0 = r^{p^{e-1}}, \quad b_0 = b^{p^{e-1}}$$

we see that r_0 has order p, b_0 has order 1 or p, and x_0 satisfies

$$r_0^{x_0} \equiv b_0 \pmod{P}.$$

By some search procedure (more about that later) we find x_0. Clearly $x \equiv x_0 \pmod{p}$. We now show how to refine this modulo p^2. The rest will be a simple iteration.

Put

$$c_1 = b \cdot r^{-x_0} = r^{x_1 p + x_2 p^2 + \cdots + x_{e-1} p^{e-1}}.$$

Raise this equation to the power p^{e-2}:

$$b_1 = c_1^{p^{e-2}} \equiv (r^{p^{e-1}})^{x_1} \equiv r_0^{x_1} \pmod{P}$$

where the same search procedure produces x_1.

Then form $c_2 = c_1 \cdot r^{-x_1 p}$, so that

$$c_2 = r^{x_2 p^2 + \cdots + x_{e-1} p^{e-1}},$$

raise this to the power p^{e-3}, and so on, to determine x_2.

Note that in the right member the base will always be $r_0 = r^{p^{e-1}}$.

C.VIII.1 Example. Let $P = 199$, $N = 198 = 2 \cdot 3^2 \cdot 11$. A primitive root is 3. We want to solve $g^x \equiv 2 \pmod{P}$.

First we determine x modulo 2. By the discussion above we are to raise $2, 3$ to the power $198/2 = 99$, and solve $2^{99} \equiv (3^{99})^x \pmod{199}$. Now $2^{99} \equiv 1 \pmod{199}$ so we get $x \equiv 0 \pmod{2}$ without even computing $3^{99} \pmod{199}$ (it must be $\equiv -1$, anyway).

Next we want the residue of x modulo 11 so we take the exponent $198/11 = 18$. Here $2^{18} \equiv 61$; $3^{18} \equiv 125 \pmod{199}$. Simply raising 125 to the power $1, 2, \ldots$ finds the solution $125^7 \equiv 61 \pmod{199}$, so $x \equiv 7 \pmod{11}$.

Finally, to get x modulo 9, we take $198/(3^2) = 22$, $b \equiv 2^{22} \equiv 180 \pmod{199}$, $r \equiv 3^{22} \equiv 175 \pmod{199}$. We have to solve

$$b \equiv 180 \equiv r^{x_0+3x_1} \equiv 175^{x_0+3x_1} \pmod{199},\ 0 \leq x_0, x_1 < 3.$$

Now, $b^3 \equiv 106 \equiv r^3 \pmod{199}$ so $x \equiv 1 \pmod{3}$, hence $x_0 = 1$. The inverse of 175 modulo 199 is 58, and $180 \cdot 58 \equiv 92 \pmod{199}$. We have to solve:

$$\begin{aligned} 180 &\equiv 175^{1+3x_1} \pmod{199} \\ 92 &\equiv 175^{3x_1} \equiv 106^{x_1} \pmod{199}, \end{aligned}$$

whence $x_1 = 2$ (as it cannot be 0 or 1). So $x \equiv 1 + 2 \cdot 3 = 7 \pmod{9}$.

So we have found $x \equiv 0 \pmod{2}$, $x \equiv 7 \pmod{11, 9}$. The last two congruences state that $x \equiv 7 \pmod{99}$, and the first states that x is even, yielding the discrete logarithm $x = 7 + 99 = 106$. □

Baby Steps, Giant Steps

If $P - 1$ has a large prime factor p, a linear search through the classes to solve $g^x \equiv a$ may not be feasible. In that case the Baby Steps, Giant Steps algorithm of D. Shanks (1917-1996) may be helpful. Its main drawback is its storage requirements.

We assume given an element g of known order d, modulo P. We assume known that $g^x \equiv a \pmod{P}$. We let $m \in \mathbf{Z}$ denote the *ceiling* of $\sqrt{d}$, so that $m - 1 < \sqrt{d} \leq m$.

Then each number x, $0 \leq x \leq d - 1$, may be written $x = x_0 + mx_1$, where $0 \leq x_i \leq m - 1$, $i = 1, 2$. The congruence $g^x \equiv a \pmod{P}$ may then be rewritten thus:

$$g^{x_0+mx_1} \equiv a; \quad (g^m)^{x_1} \equiv (g^{-1})^{x_0} \cdot a \pmod{P}.$$

We make a list of the pairs $[(g^m)^i, i]$, $i = 0, 1, 2, \ldots, m - 1$ (those are the giant steps), and another list of the products $a \cdot (g^{-1})^j, j = 0, 1, 2, \ldots, m - 1$ (the baby steps). We look for a match, $(g^m)^{x_1} \equiv (g^{-1})^{x_0} \cdot a \pmod{P}$, and then $x = x_0 + mx_1$ solves the problem.

One could sort one of the lists, and run through the other, searching for a match in the first list.

It is easy to search a sorted list. Just look at the middle of list, then you will know in which half to search next. The search moves through the list, which is unchanged in the process.

Sorting could be done with an "in-place Quicksort". Python has a built-in method. Wikipedia is a surprisingly good first source of information (to be complemented with other documents, of course).

Sorting algorithms typically require $\mathcal{O}(n \log n)$ operations, so we should expect something on the order of $\sqrt{d}$. Buchmann's book on Cryptography has a fuller discussion of these complexity issues. An alternative to sorting is hashing, described in Crandall-Pomerance. It is faster. Python users will check up on "dictionaries".

(The idea behind hashing is simple. Instead of throwing things in a heap and start looking for them afterwards, we keep a record of where we put them, i.e., we label them suitably. A simple example of such a labeling, a *hash function*, is to extract the last 32 bits. Of course, it may happen that several numbers are labeled the same, and there are various strategies for handling this.

In our applications, such collisions are often short, and can be handled with a simple linear search.)

It is reasonable to sort the list of giant steps, as these are independent of a. If only one a is investigated, it is more economical to create the $a \cdot (g^{-1})^j$ sequentially. If one of them does not match, it is discarded, and the next one is investigated. This saves both time and storage. The value of j is stored and updated at each step.

If P has all its prime factors below a moderate multiple of the square root, Pohlig-Hellman, even with linear search, is faster than Shanks. So one really should use Shanks only in conjunction with Pohlig-Hellman, at the level of prime factors of $P - 1$. As generally only the smallest prime factors appear with multiplicity > 1, it is often enough to use Shanks at the prime power level.

C.VIII.2 Example. Let $P = 71$, a prime number. The smallest positive primitive root is $g = 7$, of order 70. We show how Shanks' algorithm applies to the congruence $7^x \equiv 3 \pmod{71}$. The inverse of 7 modulo 71 is $61 \equiv -10 \pmod{71}$. The ceiling of $\sqrt{70}$ is $m = 9$.

The following is the list of baby steps (I have included the exponents for the reader's convenience):

$$[[3,0],[41,1],[16,2],[53,3],[38,4],[46,5],[37,6],[56,7],[8,8]]$$

For instance, $3 \cdot (61)^7 \equiv 56 \pmod{71}$, explaining the next to last element.

Here are the giant steps:

$$[[1,0],[47,1],[8,2],[21,3],[64,4],[26,5],[15,6],[66,7],[49,8]]$$

where, for instance, $21 \equiv (7^9)^3 \pmod{71}$.

We find a matching 8: $8 \equiv 3 \cdot (61)^8 \equiv (7^9)^2 \pmod{71}$, $3 \equiv 7^8 \cdot 7^{18} \pmod{71}$, i.e., $x = 26$. □

Index Calculus

This method is quite old. It was invented for the purpose of creating tables of discrete logarithms. We introduce it directly by an example.

Take $p = 2017$. One primitive root is $g = 5$. We want to solve $g^x \equiv 23 \pmod{p}$.

We form a *factor base*, consisting of all prime numbers below a certain bound. In this case we choose the bound 7: $2, 3, 5, 7$. By some random trial-and-error procedure we find a power g^y such that the least positive residue of $a \cdot g^y$ has all its factors in ("factors over") the factor base. I found:

$$23 \cdot g^{794} \equiv 3 \pmod{p}.$$

Then we find a number of powers of g that also factor over the base, e.g.,

$$\begin{array}{lllllr}
g^{859} & \equiv & 315 & \equiv & 3^2 \cdot 5 \cdot 7 & \pmod{p} \\
g^{1150} & \equiv & 48 & \equiv & 2^4 \cdot 3 & \pmod{p} \\
g^{1060} & \equiv & 6 & \equiv & 2 \cdot 3 \cdot 5 \cdot 7 & \pmod{p} \\
g^{1875} & \equiv & 210 & \equiv & 2^4 \cdot 3^2 & \pmod{p} \\
g^{75} & \equiv & 90 & \equiv & 2 \cdot 3^2 \cdot 5 & \pmod{p} \\
g^{32} & \equiv & 50 & \equiv & 2 \cdot 5^2 & \pmod{p}
\end{array}$$

The reason for overdetermination will presently be revealed.

Taking discrete logarithms of each congruence gives a system of congruences modulo $p-1=2016$. We denote the discrete logs by "log":

$$\begin{array}{lllll}
 & 2\log 3 & +\log 5 & +\log 7 & \equiv 859 \pmod{p-1} \\
4\log 2 & +\log 3 & & & \equiv 1150 \pmod{p-1} \\
\log 2 & +\log 3 & & & \equiv 1060 \pmod{p-1} \\
\log 2 & +\log 3 & +\log 5 & +\log 7 & \equiv 1875 \pmod{p-1} \\
\log 2 & +2\log 3 & +\log 5 & & \equiv 75 \pmod{p-1} \\
\log 2 & & +2\log 5 & & \equiv 32 \pmod{p-1}
\end{array}$$

We will presently discuss the systematics in solving the system. Here we find the solution by inspection.

As $g=5$, $\log 5=1$. The last equation gives us $\log 2=32-2=30$. Substituting this into the third equation gives $\log 3=1060-30=1030$.

Finally, the relation $23\cdot g^{794}\equiv 3 \pmod{p}$ gives $\log 23=\log 3-794=1030-794=236$.

There are quite a few practical issues connected with this algorithm. How best to solve the very sparse systems that arise is far from trivial. Even the factoring part has to be managed with some cunning. An important question is also the optimal size of the factor base. For these questions I must refer to Crandall-Pomerance, who also discuss time and storage complexity.

With these difficulties suitable managed, The Index Calculus algorithm wins over the previous algorithms, but costs a lot more programming effort.

How do we solve the linear system $AX\equiv Y \pmod{N}$, where Y is a given column matrix, and the column X is sought ?

By the Chinese Remainder Theorem (B.I.5) we easily reduce to the prime powers $p_i^{e_i}$ entering the factorization of N. We will definitely need to precompute the solutions to $z_i\equiv 1 \pmod{p_i^{e_i}}$; $z_i\equiv 0 \pmod{p_j^{e_j}}$, $j\neq i$.

Gaussian elimination modulo a prime p is just like the real case; the important thing is that we need to, and can, invert non-zero pivot elements, hence create zeros in the rows below them.

As for prime powers, we need to know how to pass from p^e to p^{e+1}. We do so by a kind of Henselian refinement (cf. B.VII.3), as follows.

Suppose we know

$$AX\equiv Y \pmod{p^e}; \quad AX=Y+p^eV$$

We modify X to $X + p^e U$. U is then found from the condition

$$A(X + p^e U) \equiv Y + p^e AU + p^e V \equiv Y \pmod{p^{e+1}},$$

i.e.,

$$AU + V \equiv 0 \pmod{p}.$$

If A is a square matrix, the determinant of which is not divisible by p we get unique solvability modulo p^e. If this holds for every prime power dividing N, then, by the CRT, the system is uniquely solvable modulo N.

We can now explain why we want an overdetermined system. The determinant of a square system is far from unlikely to be zero modulo a small prime factor in $p - 1$. In that case we will get a parametrical solution. Working with these is a bit messy.

For instance, if the solution modulo 2 is $\mathbf{v_0} + t\mathbf{v_1}$, it may very well happen that $\mathbf{v_0} + \mathbf{v_1}$, but not $\mathbf{v_0}$, refines to a solution modulo 4 (assuming $p \equiv 1 \pmod{4}$). Here, e.g., the first four equations form a subsystem the determinant of which is zero. The last four have determinant$= 3$, a factor in 2016, etc. By overdetermination we hope to force unique solvability modulo all prime factors.

One may not need a complete factorization of N. Should we work modulo a composite integer M and encounter a non-invertible, non-zero, pivot element a, $(a, M) > 1$, we can factorize further!

Pollard Rho

The Pollard rho method creates collisions $a^m \cdot g^n \equiv a^q \cdot g^r \pmod{P}$ through a pseudo-random iterative process. Then $a^{m-q} \equiv g^{r-n} \pmod{P}$. At the same time we want $g^x \equiv a \pmod{P}$, so that $g^{r-n} \equiv g^{x(m-q)} \pmod{P}$, i.e., $r - n \equiv x(m - q) \pmod{d}$, where d is the order of g modulo P. The solution of this congruence is of the form $x \equiv x_0 \pmod{d/k}$ where $k = (m - q, d)$, and $0 \le x_0 < d/k$.

If k is not too large, one may then find the required $x \pmod{d}$ by testing $x = x_0 + s \cdot (d/k)$, $s = 0, 1, 2, \ldots k - 1$.

Unlike Baby Steps, Giant Steps, the storage requirements are minimal. Pollard is very easy to program, and there are no sorts or searches. Like the Steps method, Pollard's algorithm does not rely on a factorization – on the other hand, it does not benefit from a factorization with all prime factors small.

Therefore it seems reasonable to use it only on the level of congruences modulo q where q is a prime factor of $P-1$. And so I state it in terms of an element g of known order d, and an element a known to be a power of g modulo P.

We start with $x_0 = y_0 = 1 = a^0 g^0$. By the iteration to be described presently, we create a sequence $x_i \equiv a^{m_i} g^{n_i} \pmod{P}$ and, simultaneously, $y_i = x_{2i}$, until $x_i - y_i \equiv 0 \pmod{P}$.

We will then have created our collision.

At each turn of the loop we update x_i to x_{i+1}, and $y_i = x_{2i}$ to x_{2i+1}, and then to $x_{2i+2} = y_{i+1}$. At the same time the exponents are updated. That means three evaluations at every turn, and many values are computed twice. Here is the update:

$$x_{i+1} \equiv \begin{cases} a \cdot x_i \equiv a^{m_i+1} g^{n_i} \pmod{p} & \text{if } 0 < x_i \leq P/3 \\ x_i \cdot x_i \equiv a^{2m_i} g^{2n_i} \pmod{p} & \text{if } P/3 < x_i < 2P/3 \\ x_i \cdot g \equiv a^{m_i} g^{n_i+1} \pmod{p} & \text{if } 2P/3 < x_i < P \end{cases}$$

The exponents are of course reduced modulo d each time. (The displayed formulas show how they are updated, e.g., in the first case $m_{i+1} = m_i + 1$, $n_{i+1} = n_i$.)

The expected number of iterations before achieving a collision is somewhere around $\sqrt{d}$. As soon as $x_i \equiv x_{2i} \pmod{P}$ the iterates will occur with period i – the loop of the letter ρ (before that, the algorithm passes through a pre-period, the stem of the ρ.)

C.VIII.3 Example. $P = 2017$, again. The primitive root is again $g = 5$. We want to solve $g^x \equiv 23 \pmod{P}$. After 37 turns of the loop (slightly less than the square root) we get (omitting indices)

$$x \equiv a^m g^n \equiv y \equiv a^q g^r \equiv 497 \pmod{P}$$

with

$$m \equiv 1408; \quad n \equiv 1162 \pmod{P-1},$$
$$q \equiv 0; \quad r \equiv 810 \pmod{P-1}.$$

Solving the linear congruence

$$x(m-q) \equiv r - n \pmod{P-1}$$

we get

$$x \equiv 47 \pmod{63}$$

with period $63 = (P-1)/32$.

We first try $x = x_0 = 47$, giving

$$k \equiv g^{x_0} \equiv 1125 \pmod{P}.$$

We then multiply repeatedly by the factor

$$h \equiv g^{63} \equiv 500 \pmod{P}$$

until we get the right result. It turns out that

$$k \cdot h^3 \equiv 23 \pmod{P}$$

so the solution is

$$x \equiv 47 + 3 \cdot 63 \equiv 236 \pmod{P-1}.$$

□

Remark: We will almost certainly get a period (less than or) equal to $(P-1)/2^e$ where 2^e is the full power of 2 dividing $P-1$. The reason is that the middle case involves a doubling of the exponents as long as their 2-power factor is $< 2^e$. Normally that factor is very small compared to $P-1$.

If the method is used in conjunction with Pohlig-Hellman, the current order is a prime number q, and the case $q = 2$ should perhaps be treated separately. If g is of order 2 modulo P, then the solution of $g^x \equiv t \pmod{P}$ is easy to find as we will then have $g \equiv -1 \pmod{P}$ and $t \equiv \pm 1 \pmod{P}$.

C.VIII.4 Example. With the worst of luck we could get a period =1 when working at the prime factor level. While preparing this text I ran Pohlig-Hellman + rho on $g^x \equiv y = 29 \pmod{P}$, for the prime modulus $P = 2^{127}-1$, with primitive root 43.

The prime factorization of $P-1$ is of the form

$$P - 1 = Q \cdot 77158673929 = Q \cdot R$$

where R is the largest prime factor, and Q is the product of 14 smaller prime factors. Raising g, y to the power Q, and working with period R, after

418761 turns of the loop I arrived at a collision $a^m \cdot g^n \equiv a^q \cdot g^r \pmod{P}$ with $m = q, n = r$, not just congruent modulo R!

No use continuing then, as we have entered the period of the iteration.

In such a case one could start over with a modified update function or a low power of a, correcting afterwards.

I tried the inverse of 29 modulo P:

$$58669373607058355769547346108925553699,$$

which worked fine, giving the discrete logarithm

$$76746560798291881874195484158040759963,$$

then negated the answer modulo $P - 1$, giving the result

$$16246652738064004354426775530008002976 3.$$

Computer resources allowing one could run several processes in parallel until one of them results. □

Chapter D

Quadratic Reciprocity

D.I The Legendre Symbol

We start with a definition right away:

D.I.1 Definition. Let n be a positive integer, and $(a, n) = 1$. The number a is said to be a **quadratic residue modulo** n if the congruence

$$x^2 \equiv a \pmod{m}$$

is solvable. If $(a, n) = 1$ and the congruence is unsolvable, a is said to be a **quadratic non-residue** modulo n.

The property of being a residue or non-residue clearly only depends on the class of a modulo n.

We will mainly deal with the case when $n =$ a prime number p. In that case it is convenient to have the *Legendre symbol*:

D.I.2 Definition. Let p be an odd prime. The **Legendre symbol** is defined by the following requirements:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \text{ is a quadratic residue modulo } p \\ 0 & \text{if } p \text{ divides } a \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

The case $p|a$ is often left undefined.

In inline formulas the symbol is usually written (a/n).

D.I.3 Example. $p = 13$. Squaring all the invertible classes we get

$$\left(\frac{a}{13}\right) = 1 \Longleftrightarrow a \equiv 1,\ 4,\ 9,\ 3,\ 12, \text{ or } 10 \pmod{13}.$$

□

Let us see how Euler's Criterion (C.III.1) from the previous Chapter translates to this special case. As p is an odd prime, $\phi(p) = f = p - 1$ is even, so $f/(f, 2) = f/2 = (p - 1)/2$. The general Euler Criterion then immediately gives

$$\left(\frac{a}{p}\right) = 1 \Longleftrightarrow a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Setting $a^{(p-1)/2} = x$, we see, by Little Fermat (A.V.9) that $x^2 \equiv n^{p-1} \equiv 1 \pmod{p}$. That congruence has the two solution classes $x \equiv \pm 1 \pmod{p}$. By Lagrange (B.VI.2) it can have no other solutions.

So, in case $(a/p) = -1$, x must be congruent to -1 modulo p. We arrive at the following very neat formulation:

D.I.4 Theorem (Euler's Criterion). *Let p be an odd prime, and suppose p does not divide a. Then:*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

□

The Legendre symbol has a nice *multiplicativity property*:

D.I.5 Theorem. *Let g be a primitive root modulo the odd prime p. Then*

$$\left(\frac{g^k}{p}\right) = (-1)^k.$$

Proof. The Theorem states simply that the quadratic residues modulo p are exactly the even powers of g. So, let us study the congruence

$$x^2 \equiv g^k \pmod{p}.$$

Putting $x \equiv g^y \pmod{p}$ we arrive, as usual, at a linear congruence in the exponents:

$$2y \equiv k \pmod{p-1}.$$

As $(p-1, 2) = 2$, this is solvable if and only if $2|k$, and the result follows. □

From this we immediately get

D.I.6 Corollary.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. If $a \equiv g^k \pmod{p}$, and $b \equiv g^l \pmod{p}$, both members equal $(-1)^{k+l} = (-1)^k(-1)^l$.

We have assumed that $(a,p) = (b,p) = 1$. If a or b is divisible by p, both members equal 0. □

The Corollary could also have been inferred from the Euler Criterion.

D.I.7 Example. The Corollary states among other things that the product of two quadratic residues or two non-residues modulo an odd prime is a quadratic residue. The first statement is trivially true, the second is not. And it is *not* generally true for a composite modulus. For instance, it is easy to check (by squaring all invertible classes) that 2,7, *and* $2 \cdot 7 = 14$ are quadratic non-residues modulo 15. □

D.I.8 Example. $p = 13$. It is easy to check that $g = 2$ is a primitive root for p (check $g^6, g^4 \not\equiv 1 \pmod{13}$). The even powers, hence the quadratic residues, are:

$$1 \equiv g^0; \quad 4 \equiv g^2; \quad 3 \equiv g^4; \quad 12 \equiv g^6; \quad 9 \equiv g^8; \quad 10 \equiv g^{10} \pmod{13}.$$

□

The Theorem of Quadratic Reciprocity will allow us to compute the Legendre symbol by reducing the size of the numbers involved. However, two cases must be dealt with separately. They are covered by the First and Second Supplementary Theorems, often known by their German name Ergänzungssätze ("erster und zweiter Ergänzungssatz").

The first of them is an immediate consequence of the Euler Criterion:

D.I.9 Theorem (First Supplementary Theorem). *For an odd prime p,*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

□

As $(p-1)/2 \equiv 0 \pmod 2$ if and only if $p \equiv 1 \pmod 4$, the latter congruence is the condition for -1 to be a quadratic residue modulo the odd prime p.

The second Ergänzungssatz is preceded by a complex version of "Freshman's Dream" (A.V.8) from the first Chapter. It deals with complex integers $m + ni, m, n \in \mathbf{Z}$. Two such numbers are said to be congruent modulo p if their respective real and imaginary parts are.

D.I.10 Lemma (Freshman's Dream). *For ordinary, or complex, integers, and for any prime number p,*

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

The proof in the complex case is the same as in the real case. □

D.I.11 Theorem (Second Supplementary Theorem). *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \textit{ if } p \equiv 1, 7 \pmod 8, \\ -1 \textit{ if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Proof. We start with the undisputable identity $(1+i)^2 = 2i$, which we combine with an application of Freshman's Dream, $(1+i)^p \equiv 1 + i^p \pmod p$. Using

$$(1+i)^p = (1+i) \cdot (1+i)^{2 \cdot (p-1)/2} = (1+i)(2i)^{(p-1)/2}$$

we arrive at

$$1 + i^p \equiv (1+i) \cdot 2^{(p-1)/2} \cdot i^{(p-1)/2} \pmod p. \qquad (*)$$

We continue with the case $p \equiv 1 \pmod 4$, $p = 4k+1$, and leave the details of the other case as an exercise.

In this case, $i^p = i^{4k} i = i$, so we have the factor $1+i$ in both members. We first multiply the two members by $1-i$, giving the common factor 2, then by $(p+1)/2$, which is the inverse of 2 modulo p. By these operations the common factor $1+i$ cancels.

The second factor in the right member of (*) is congruent to $(2/p)$, by Euler's Criterion (D.I.4). The third equals 1 if $p \equiv 1 \pmod 8$, and -1 if $p \equiv 5 \pmod 8$ (check!). Putting everything together we arrive at

$$\left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 8, \\ -1 \text{ if } p \equiv 5 \pmod 8. \end{cases}$$

If $p \equiv 3 \pmod 4$, the left member of (*) equals $1 + i^p = 1 - i = -i(1+i)$, so again the factor $1+i$ cancels, and the rest is as above. □

This Theorem is often stated in the form

$$\boxed{\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}}$$

Of, course, this power is never computed. The smallest positive remainder of $N > 0$ modulo 8 is most conveniently found using the "bitwise and" operator on N and 7.

The following is the main result of this Chapter, and the deepest Theorem in this text. Over the years some 200 proofs have been produced, none of them very direct or intuitive, except maybe in some other, more advanced, context. We will prove it in later Sections.

The first to prove it was C.F. Gauß (1777-1855) who produced at least six different proofs. We will prove it several times in later Sections.

D.I.12 Theorem (Quadratic Reciprocity). *Let p, q be two different odd primes. Then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{(p-1)(q-1)/4}.$$

Equivalently, the two symbols are equal, except if $p \equiv q \equiv 3 \pmod 4$ (check the cases!).

□

D.I.13 Example.

a) 107 is a prime number, $\equiv 3 \pmod 4$. We compute the symbol (91/107):

$$\left(\frac{91}{107}\right) = \left(\frac{7 \cdot 13}{107}\right) = \left(\frac{7}{107}\right)\left(\frac{13}{107}\right) = -\left(\frac{107}{7}\right)\left(\frac{107}{13}\right) = -\left(\frac{2}{7}\right)\left(\frac{3}{13}\right).$$

The minus sign comes from $7 \equiv 107 \equiv 3 \pmod 4$ and the Reciprocity Theorem. Note that $13 \equiv 1 \pmod 4$, so that factor contributes no change of sign.

The last equality comes from the fact that the symbol only depends on the class of the numerator modulo the denominator, i.e., we have replaced 107 with its remainders on division by 7, and 13.

By the Second Supplementary Theorem, $(2/7) = 1$. (D.I.11).

And, finally, $(3/13) = (13/3) = (1/3) = 1$, as $13 \equiv 1 \pmod 4$, so the result is -1; 91 is a *non-residue* modulo 107.

The Jacobi symbol (D.II.1), to be introduced in the next Section, will obviate the need for factorization.

b) In this example we study the symbol $(-3/p)$ for any odd prime $p \neq 3$. The First Supplementary Theorem (D.I.9), and Reciprocity, give

$$\Big(\frac{-3}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{3}{p}\Big) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)(3-1)/4}\Big(\frac{p}{3}\Big).$$

The two signs in the last member are equal, so we are left with

$$\Big(\frac{-3}{p}\Big) = \Big(\frac{p}{3}\Big) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

□

We next deal with prime powers and composite moduli.

D.I.14 Theorem.

a) Let p be an odd prime, k a positive integer, and a an integer not divisible by p. Then a is a quadratic residue modulo p^k if and only if $(a/p) = 1$.

b) The odd integer a is a quadratic residue modulo 2^e, $e \geq 3$, if and only if $a \equiv 1 \pmod 8$.

Proof. Part b) has been proved twice before (B.VII.5, C.IV.9) so let us turn to part a).

"Only if" is easy: if $x^2 \equiv a \pmod{p^k}$, then, a fortiori, $x^2 \equiv a \pmod p$.

The "if" part is an easy induction, using Hensel's Lemma (B.VII.3). Suppose we have found an x satisfying $x^2 \equiv a \pmod{p^j}$. With $f(x) = x^2 - a$, we have $f'(x) = 2x$. As $p \nmid x$, hence $p \nmid 2x$, Hensel's Lemma shows that x refines to $y \equiv x \pmod{p^j}$ with $f(y) = y^2 - a \equiv 0 \pmod{p^{j+1}}$. □

D.I.15 Example. Is 57 a quadratic residue modulo $784 = 2^4 \cdot 7^2$?

In the Section on algebraic congruences (see B.VII) we proved that a congruence is solvable, modulo a product of relatively prime moduli, iff it is solvable modulo both factors.

So the question is reduced to the solvability of $x^2 - 57 \equiv 0$ modulo 2^4, and 7^2. We easily compute $(57/7) = (1/7) = 1$, proving solvability modulo 7^2.

Also, $57 \equiv 1 \pmod 8$, so the congruence is solvable modulo 2^4 as well. The answer is yes, 57 is a quadratic residue modulo 784.

(The number of solution classes is 8 – why? – and the smallest positive solution is 29.) □

D.I: Exercises

1. Complete the proof of the Second Supplementary Theorem for the cases $p \equiv 3, 7 \pmod 8$.

2. Find a primitive root modulo 11 and one modulo 13. Use them to describe and compute all quadratic residues and non-residues in both cases.

Then do the same for cubic residues and explain the difference. (A cubic residue is an x representable as $x \equiv y^3 \pmod p$, $(y, p) = 1$.)

3. Let p be an odd prime. What is the number of squares (not just invertible ones) modulo p? Modulo p^k (do odd and even k separately)? Modulo 2^k? Modulo an arbitrary integer?

4. Solve the congruence $x^3 \equiv 8 \pmod{41}$, with a minimum of computation or searching (reduce to a quadratic congruence). Then solve $x^3 \equiv 8 \pmod{41^2}$.

5. The integer $a \nmid p$ is a *biquadratic residue* if the congruence $x^4 \equiv a \pmod p$ is solvable.

(a) Show that -1 is a biquadratic residue modulo the odd prime p if and only if $p \equiv 1 \pmod 8$.

(b) $p = 4k + 3$, k a positive integer, is a prime number. Show for every integer a, $p \nmid a$, that exactly one of a or $-a$ is a quadratic residue modulo p. Then show that a is a biquadratic residue modulo p if and only if a is a quadratic residue.

6. Assume that -1 is a quadratic residue modulo the odd prime p, i.e., that $p \equiv 1 \pmod 4$. Show that -4 is a biquadratic residue modulo p. For instance, use the solutions to $X^2 \equiv -1 \pmod p$ to express the solutions to $X^4 \equiv -4 \pmod p$.

7. There are infinitely many prime numbers $\equiv 1 \pmod 4$. Assume the contrary, and let P be the product of all prime numbers $\equiv 1 \pmod 4$. Derive a contradiction by considering the prime factors of $4P^2 + 1$.

Similarly, prove that there are infinitely many primes $\equiv 1 \pmod 6$.

8. (a) The symbol $(-5/p)$, where p is an odd prime, depends only on the class of p modulo 20. Show this, and determine the symbol in all cases. Exemplify each case.

(b) Replace -5 by $\pm q$, q prime $\neq p$. Describe (motivate!) in which cases the quadratic character $(\pm q/p)$ depends only on the class of p modulo q, and in which cases it depends on a larger modulus.

9. The prime p is given by $p = 8n + 1$, where n is a positive integer. Let g be a primitive root modulo p. Show that the solutions to the congruence $x^2 = \pm 2$ are given by

$$x \equiv \pm(g^{7n} \pm g^n) \pmod p.$$

10. Let p be an odd prime. Show that $(a/p) = -1$ if and only if $\mathrm{ord}_p(a)$ and $p - 1$ are divisible by exactly the same power of 2.

11. (a) p, q are two different odd primes, $p \equiv \pm q \pmod{4a}$. Show that $(a/p) = (a/q)$. Hint: It is enough to prove this for $a=$ odd prime (why?).

(b) Determine $(3/p)$ for $p = 5, 7, 11, 13$.

(c) Conclude that 3 is a quadratic residue modulo the odd prime p if and only if $p \equiv \pm 1 \pmod{12}$.

12. Let p be a prime number. Find a criterion for the solvability of $x^2 \equiv a \pmod{p^e}$ if $a = p^k q$, $(p, q) = 1$, $k < e$.

13. p, q, are odd primes, $q \equiv 1 \pmod p$. Show that plus or minus p is a quadratic residue modulo q. Exemplify.

14. (a) p is an odd prime. Show that the polynomial congruence $f(X) = X^{p-1} - 1 \equiv 0 \pmod p$ has the roots $1, 2, \ldots, p-1$ modulo p.

(b) Use this fact to determine

$$\prod_{1 \le j \le (p-1)/2} (X^2 - j^2)$$

and

$$\prod_{1 \le j \le (p-1)/2} (X - j^2)$$

modulo p.

(c) Finally determine the two polynomials whose roots modulo p are all quadratic residues, and all quadratic non-residues. Connect with Euler's Criterion (C.III.1), and note that you never used the existence of primitive roots.

(d) Determine the product modulo p of all the quadratic residues, using the previous item and/or primitive roots.

15. p is an odd prime number. Compute or describe (modulo p) the products

(a) $1 \cdot 2 \cdots (p-1)/2$

(b) $2 \cdot 4 \cdots (p-1)$

(c) $1 \cdot 3 \cdot 5 \cdots (p-2)$

The answer depends on the class of p modulo 4 or 8.

16. We want a direct proof that $(\frac{-3}{p})$ equals 1 if $p \equiv 1 \pmod 3$. Let r be an element of order 3 modulo p (prove its existence!). Show that $r^2 + r + 1 \equiv 0 \pmod p$, and complete the squares.

(a) Now assume that $p \equiv 2 \pmod 3$. Show that the congruences $x^3 \equiv a \pmod p$ are *uniquely* solvable p, for all a. Choosing $a = 8$ (for example!), prove that the congruence $x^2 + 2x + 4 \equiv 0 \pmod p$ is unsolvable, hence $(\frac{-3}{p}) = -1$.

(b) Now let us prove that $p \equiv 1 \pmod 5$ yields $(\frac{5}{p}) = 1$. Let r be of order 5 (prove existence!), show that $1 + r + r^2 + r^3 + r^4 \equiv 0 \pmod 5$, then set $x = r + r^4$ and show that $x^2 + x \equiv 1 \pmod 5$. Complete the squares.

17. (a) We are looking for solutions to $x^2 \equiv -1 \pmod p$ where $p \equiv 1 \pmod 4$ is a prime number. Show, using Euler's Criterion, how a solution may be determined once we know a quadratic non-residue $a \pmod p$.

(b) In the two cases $p \equiv 5 \pmod 8$ and $p \equiv 17 \pmod{24}$ one special (small) value can be used for a. Exemplify the cases $p = 29, 41$ (and thereby solve the congruence in (a)). The remaining case, therefore, is $p \equiv 1 \pmod{24}$.

18. Let p be an odd prime number. Show that the least positive quadratic non-residue modulo p is a prime.

19. Let p be a prime of the form

$$p = 2^q - 1$$

where q is a prime $\equiv 1 \pmod 4$. Show that 10 is a quadratic residue modulo p. Exemplify.

20. Assume that both p and $q = 2p-1$ are primes, e.g., $p = 7$ and $q = 13$. Show that $n = p(2p-1)$ is a pseudoprime to the base b (p. 31) if and only if b is a quadratic residue modulo n.

21. Let p be an odd prime. x is an integer satisfying $x \not\equiv \pm 1 \pmod{p}$.

(a) Which $u \pmod{p}$ satisfy the congruence

$$x - 1 \equiv u(x+1) \pmod{p}$$

for some x?

(b) Using a), determine the number of classes $x^2 - 1 \pmod{p}$ that are quadratic residues or non-residues. Their number depends on the class of p modulo 4.

(c) Suppose $p \equiv 3 \pmod{4}$. Exhibit a bijective correspondence between those classes $x^2-1 \pmod{p}$, $x \not\equiv 0 \pmod{p}$ that are quadratic residues modulo p and those that are not. Hint: look at inverse pairs.

(d) What can be said about the classes $x^2 - a^2 \pmod{p}$ for a fixed and $x \not\equiv \pm a \pmod{p}$?

22. Let p be a prime number $\equiv 3 \pmod{4}$, $a \nmid p$. Show that a is a primitive root modulo p if and only if the order of $-a$ modulo p is $(p-1)/2$.

23. Consider the polynomial

$$f(X) = (X^2 - p)(X^2 - q)(X^2 - pq),$$

where p, q are distinct odd primes. Obviously there are no rational integer roots. Can you find p, q (or even some simple sufficient condition) such that the equation is solvable modulo every integer $n > 0$? Start with primes and prime powers.

24. The polynomial $X^4 + 1$ has non-trivial factorizations modulo every prime p. Prove the following cases.

(a) Modulo 2, or $p \equiv 1 \pmod{8}$: four linear factors.

(b) Modulo $p \equiv 5 \pmod{8}$: two quadratic factors, without linear term.

(c) Modulo $p \equiv 3, 7 \pmod{8}$: two quadratic factors with linear terms. Note that the numbers ± 2 have opposite quadratic characters modulo p.

D.II The Jacobi Symbol

The *Jacobi symbol* extends the Legendre symbol, and the notation is the same (C G Jacobi, Prussian mathematician, 1804-1851).

D.II.1 Definition. Let n be an odd positive integer,

$$n = \prod_{i=1}^{k} p_i^{e_i}, \quad e_i > 0 \quad \forall i,$$

its prime factorization. The **Jacobi symbol** is then defined, for arbitrary integers $m, (m,n) = 1$, by

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{k} \left(\frac{m}{p_i}\right)^{e_i}.$$

(The factors entering the right member are Legendre symbols.)

It would not be unnatural to define $(m/n) = 0$ if $(m,n) > 1$, but it is rarely done.

D.II.2 Example. If m is a quadratic residue modulo n, then all the Legendre symbols in the right member above equal $+1$. So $(m/n) = 1$ is a *necessary* condition for m to be quadratic residue. It is *not* sufficient. For instance,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$$

but 2 is *not* a quadratic residue modulo 15. □

This “defect” of the Jacobi symbol has proved useful in Cryptography.

The Jacobi symbol has nice *multiplicativity properties*:

D.II.3 Theorem.

a)

$$\left(\frac{m}{n_1 n_2}\right) = \left(\frac{m}{n_1}\right)\left(\frac{m}{n_2}\right).$$

b)

$$\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right).$$

Proof. Part a) follows readily from the definition. Part b) is an easy consequence of the corresponding property of the Legendre symbol. □

The two Supplementary Theorems, and the Quadratic Reciprocity Theorem, have their counterparts for the Jacobi symbol:

D.II.4 Theorem. *For odd positive integers m, n:*

a)

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$

b)

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

c)

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}.$$

Proof. The proof of each statement is a fairly easy induction on the number of prime factors involved. The base step in each of parts a)-c) is the corresponding result for prime numbers.

What is needed, then, is the identity $ab-1 = a(b-1)+(a-1)$ so that, e.g.,

$$(-1)^{(ab-1)/2} = (-1)^{a(b-1)/2}(-1)^{(a-1)/2} = (-1)^{(b-1)/2}(-1)^{(a-1)/2}$$

for odd integers a, b. Letting $n = ab$, b prime, this gives the induction step for part a).

For b), replacing a by a^2, and b by b^2, we get, similarly,

$$(-1)^{(a^2b^2-1)/8} = (-1)^{a^2(b^2-1)/8}(-1)^{(a^2-1)/8} = (-1)^{(b^2-1)/8}(-1)^{(a^2-1)/8}.$$

c) is dealt with similarly, exercise. □

D.II.5 Example. The following computation determines the Legendre symbol (91/103), without factoring.

$$\left(\frac{91}{103}\right) = -\left(\frac{103}{91}\right) = -\left(\frac{12}{91}\right) = -\left(\frac{2^2}{91}\right)\left(\frac{3}{91}\right) = \left(\frac{91}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

In fact, $20^2 \equiv 91 \pmod{103}$.

The first step comes from $91 \equiv 103 \equiv 3 \pmod 4$, and Reciprocity. The second is division. The third extracts two factors 2 from the numerator of the symbol. Then comes another Reciprocity step, and finally one more division. The process continues until we get a one in the numerator.

If we try, somewhat improperly, to compute a Jacobi symbol (m/n), $(m, n) > 1$, following the formal rules, we will arrive at a 0, not a 1, in the numerator. Accepting the definition $(m/n) = 0$ in this case, we need not really check relative primality before computing!

One example of this:

$$\left(\frac{21}{33}\right) = \left(\frac{33}{21}\right) = \left(\frac{12}{21}\right) = \left(\frac{2}{21}\right)^2 \cdot \left(\frac{3}{21}\right) = \left(\frac{21}{3}\right) = \left(\frac{0}{3}\right).$$

The reason for the zero is that (apart from extraction of 2-factors) we are mainly doing Euclid on the odd numbers $21, 33$. – inverting and dividing. The gcd of the numerator and denominator remains unchanged, =3, through the process. □

D.II.6 Example. Another example, with fewer explanations.

$$\left(\frac{93}{107}\right) = \left(\frac{107}{93}\right) = \left(\frac{14}{93}\right) = \left(\frac{2}{93}\right)\left(\frac{7}{93}\right) = -\left(\frac{7}{93}\right) = -\left(\frac{93}{7}\right) = -\left(\frac{2}{7}\right) = -1.$$

We used the Second Supplementary Theorem twice, noting, e.g., that $93 \equiv 5 \pmod 8$. In the Reciprocity Steps we used $93 \equiv 1 \pmod 4$. □

D.II.7 Example. This time the denominator, 1729, is not a prime number. We compute the symbol (17/1729) (check the steps!):

$$\left(\frac{17}{1729}\right)=\left(\frac{1729}{17}\right)=\left(\frac{12}{17}\right)=\left(\frac{2^2}{17}\right)\left(\frac{3}{17}\right)=\left(\frac{3}{17}\right)=\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

However, for $(a, 1729) = 1$, the factorization $1729 = 7 \cdot 13 \cdot 19$, along with Little Fermat, implies

$$a^{36} = \begin{cases} (a^6)^6 \equiv 1 \pmod{7} \\ (a^{12})^3 \equiv 1 \pmod{13} \\ (a^{18})^2 \equiv 1 \pmod{19} \end{cases}$$

whence $a^{36} \equiv 1 \pmod{7 \cdot 13 \cdot 19}$. As $1728/2 = 864 = 36 \cdot 24$ we get (with $a = 17$)

$$17^{(1729-1)/2} \equiv 1 \not\equiv -1 \pmod{1729},$$

i.e., the Euler Criterion (D.I.4) does *not* hold for the Jacobi symbol in general. As the simple example $2^7 \equiv 8 \pmod{15}$ shows, we need not even get a $+$ or -1 in trying to apply the Euler Criterion. So normally we would not fall into the trap here. □

This "defect" used to be exploited in a probablistic primality test, that of Solovay-Strassen. The test detects a composite number with probability at least 50%. It has however been superseded by the Miller-Rabin test (Section L.VI), which has a greater chance of detecting compositeness, and, in fact, detects all the composites that Solovay-Strassen does. They are equivalent if $n \equiv 3 \pmod{4}$.

D.II: Exercises

1. Compute the Legendre symbol (7411/9283)

2. Determine the number of solutions to the quadratic congruences $x^2+x+1 \equiv 0 \pmod{p}$ and $x^2 + x + 21 \equiv 0 \pmod{p}$ where $p = 83$ and 97.

3. (a) Let p be an odd prime, representable as $p = a^2 + b^2$ where a is odd (later we will show that every prime $p \equiv 1 \pmod{4}$ has such a representation.) Show that a is a quadratic residue modulo p.

(b) If $p \equiv 5 \pmod{8}$, also determine (b/p).

4. Show that no integers can be represented in any of the forms

$$\frac{4x^2+1}{y^2+2}, \quad \frac{4x^2-1}{y^2-2}, \quad \frac{x^2-2}{2y^2+3}, \quad \frac{x^2+2}{3y^2+4}$$

where $x, y,\ y^2 > 1$ are integers.

Also find examples, with $y = 2\cdot$prime, of integers of the form $(x^2+1)/(y^2+2)$ and $(x^2+1)/(y^2-2)$.

5. a, b are integers, $b > 0$ is odd, and $2a + b > 0$. Compare the two symbols $(a/(2a+b))$ and (a/b).

The answer depends on the class of a modulo 4.

6. **Suggestions for computing:** A Jacobi routine, returning (m/n) if $(m, n) = 1$, and 0 otherwise. The program should warn against illegitimate input.

D.III A Cryptographic Application

The “defect” of the Jacobi symbol, not to fully distinguish between quadratic residues and non-residues, is at the heart of several cryptographic schemes. Here we present one due to Goldwasser and Micali.

Bob wants to send a message to Alice. For the sake of simplicity, let us assume it consists of one bit $m = 0$ or 1.

Alice chooses two large prime numbers p, q of approximately the same size. The product $n = pq$ is made public (it is assumed that n is so large that it cannot be factored in a reasonable amount of time). Also, a number y, a non-residue modulo p and q, is chosen at random and published. y satisfies the following:

$$\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = -1; \quad \left(\frac{y}{n}\right) = 1.$$

Now Bob chooses a number x at random (the probability that $(x, n) > 1$ is very small) and computes

$$c \equiv \begin{cases} x^2 \pmod{n} \text{ if } m = 0, \\ yx^2 \pmod{n} \text{ if } m = 1. \end{cases}$$

He then sends c.

Alice, knowing p and q, evaluates (c/p) and (c/q). She concludes

$$m = \begin{cases} 0 \text{ if both symbols} = 1 \\ 1 \text{ if the symbols} = -1 \end{cases}$$

Eve, the eavesdropper, knowing only n, can only compute $(y/n) = 1$ in either case.

D.IV Gauß’ Lemma

Gauß’ Lemma is used in many proofs of Quadratic Reciprocity. It also produces very quick proofs of the Supplementary Theorems. Therefore it is worthy of its own Section. However, even stating it takes some preparation. Basic to the Lemma (and to other discussions of Quadratic Residues) is the notion of a *half-system* of residues. Let p be an odd prime. One example of such a half-system is

$$P = \{1, 2, 3, \ldots, \frac{p-1}{2}\}$$

It obviously represents half of the $p-1$ invertible classes modulo p. The decisive property, earning the name, is the following:

D.IV.1 Lemma. *For each x, $p \nmid x$ there is exactly one $r \in P$, and one sign, + or -, such that*

$$x \equiv \pm r \pmod{p}.$$

Proof. This is almost obvious, as the numbers m, $0 < m < p$, not in P,

$$m = \frac{p+1}{2}, \frac{p+3}{2}, \ldots, p-2, p-1,$$

are congruent to

$$-\frac{p-1}{2}, \ldots, -2, -1$$

modulo p. □

Now take an arbitrary a, $p \nmid a$, and consider the products ar, $r \in P$. As we have seen, for each $r \in P$ there exists an $s \in P$, such that $ar \equiv \pm s \pmod{p}$.

No s can appear twice. For if there were $r, r', s \in P$ satisfying

$$\begin{aligned} ar &\equiv s \pmod{p} \\ ar' &\equiv -s \pmod{p} \end{aligned}$$

then, adding the two congruences, we would get $p|a(r+r')$. This is impossible, as p is prime, $p \nmid a$, and $2 \leq r + r' \leq p - 1$.

And if there were $r, r', s \in P$ satisfying

$$\begin{aligned} ar &\equiv s \pmod{p} \\ ar' &\equiv s \pmod{p} \end{aligned}$$

we would have $p|a(r-r')$, hence $r \equiv r' \pmod{p}$.

So we arrive at a new Lemma:

D.IV.2 Lemma. *Suppose $p \nmid a$. Letting r run through the half-system P, and setting $ar \equiv \pm s$, $s \in P$, the s obtained run through all of P, each $s \in P$ appearing exactly once.*

□

D.IV.3 Example. We exemplify the last Lemma. Letting $p = 11$ the half-system P consists of $1, 2, 3, 4, 5$. Let $a = 3$. We then get

$$\begin{aligned} 3 \cdot 1 &\equiv 3 \pmod{11} \\ 3 \cdot 2 &\equiv -5 \pmod{11} \\ 3 \cdot 3 &\equiv -2 \pmod{11} \\ 3 \cdot 4 &\equiv 1 \pmod{11} \\ 3 \cdot 5 &\equiv 4 \pmod{11} \end{aligned}$$

and the numbers 1, 2, 3, 4, 5 appear exactly once in the right members. □

We can now finally *state* and prove Gauß' Lemma.

D.IV.4 Theorem (Gauß' Lemma). *Let the r, s be as in the previous Lemma. Let N be the number of minus signs appearing in the congruences $ar \equiv \pm s \pmod{p}$. Then*

$$\left(\frac{a}{p}\right) = (-1)^N.$$

Proof. Let R denote the product of all the $r \in P$, i.e., $((p-1)/2)!$, reduced modulo p. Multiplying all the congruences $ar \equiv \pm s \pmod{p}$, and using the previous Lemma, we get the congruence $a^{(p-1)/2}R = (-1)^N R \pmod{p}$.

As $p \nmid R$, the factor R cancels. By the Euler Criterion we are left with

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv (-1)^N \pmod{p}.$$

□

D.IV.5 Example. In the Example just before the Theorem, the number of minus signs is even, $N = 2$. Therefore $(3/11) = 1$. Indeed, $5^2 \equiv 3 \pmod{11}$. □

D.IV.6 Example (Second Supplementary Theorem, again.). The case $a = 2$ is particularly attractive, as $0 \leq 2r \leq p-1$ for all $r \in P$. Therefore, the r giving rise to minus signs, are simply those for which $(p-1)/2 < 2r \leq p-1$.

Let us study the case $p \equiv 3 \pmod 4$ in more detail. We can group the elements in P in the following manner:

$$\left\{1, 2, \ldots, \frac{p-3}{4}\right\} \qquad \left\{\frac{p+1}{4}, \ldots, \frac{p-3}{2}, \frac{p-1}{2}\right\}$$

For r from the first group, $0 \leq 2r \leq (p-3)/2 < (p-1)/2$. For r from the second group, $(p-1)/2 < (p+1)/2 \leq 2r \leq p-1$, so it is the second group that produces the minus signs. The number of elements in that group is $(p-1)/2 - (p-3)/4 = (p+1)/4$, so

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = \begin{cases} 1 \text{ if } p \equiv 7 \pmod 8 \\ -1 \text{ if } p \equiv 3 \pmod 8 \end{cases}$$

The case $p \equiv 1 \pmod 4$ is easier, and left to the reader. □

D.IV: Exercises

1. Complete the last Example just above.

D.V The “Rectangle Proof”

We will give several proofs of Quadratic Reciprocity. The first, by Gauß, is the one usually given in the literature. It leans heavily on the Gauß Lemma (D.IV.4). We start with a variant of that Lemma.

D.V.1 Lemma. *In Gauß' Lemma in the previous Section, let $a = q$, an odd prime $\neq p$, and let P denote the* halfsystem $j = 1, 2, \ldots, (p-1)/2$ *(cf. p. 123). Further let N denote the number of $j \in P$, for which $qj \equiv -k \pmod{p}$ for some $k \in P$.*

Then

$$\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor \equiv N \pmod{2},$$

so that, S denoting the sum in the left member,

$$(-1)^S = (-1)^N = \left(\frac{q}{p}\right).$$

Proof. Let $j \in P$, i.e., $1 \leq j \leq (p-1)/2$. Divide by p:

$$jq = \left\lfloor \frac{jq}{p} \right\rfloor \cdot p + r_j, \quad 0 \leq r_j < p. \tag{$*$}$$

The remainder r_j is either of the form $k \in P$ or $p - k =\equiv k + 1 \pmod{2}$, $k \in P$. By the previous Section, each $k \in P$ appears exactly once.

The number of remainders $\equiv k + 1 \pmod{2}$, $k \in P$, is N. So the sum of the remainders is the sum of all the k's plus N ones:

$$\sum_{j=1}^{(p-1)/2} r_j \equiv \sum_{k=1}^{(p-1)/2} k + N \pmod{2}.$$

Summing the equations (*) for $j = 1, 2, \ldots, (p-1)/2$ therefore gives

$$q \sum_{j=1}^{(p-1)/2} j \equiv S \cdot p + \sum_{k=1}^{(p-1)/2} k + N \pmod{2}.$$

As p, q are odd, the two sums cancel modulo 2, and the equation reduces to

$$0 \equiv S + N \pmod 2; \quad S \equiv N \pmod 2.$$

$\square$

We now turn to the proof of the Theorem. Form the rectangle having vertices $(0,0), (p/2,0), (0,q/2), (p/2,q/2)$ in an orthonormal system. We count the number of lattice points (x,y), $x,y \in \mathbf{Z}$, in the interior of that rectangle, i.e., those having $0 < x < p/2$; $0 < y < q/2$; their number is obviously

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

We can also count these points by drawing the diagonal from $(0,0)$ to $(p/2,q/2)$ and counting the number of points above and below it.

The equation of the diagonal is $y = qx/p$; $py - qx = 0$. As (p,q) are relatively prime there are no lattice points on the diagonal.

We now count the number of points (x,y) below the diagonal. For given $x = j, 0 < j \leq (p-1)/2$, we must have $0 < y < qj/p$; $1 \leq y \leq \lfloor qj/p \rfloor$, so the number of admissible y is

$$\left\lfloor \frac{jq}{p} \right\rfloor.$$

Summing over j, the number of lattice points below the diagonal is then

$$S = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor$$

satisfying

$$(-1)^S = (-1)^N = \left(\frac{q}{p}\right),$$

by the Lemma.

In the same manner, interchanging the roles of p and q, the number of lattice points above the diagonal equals

$$T = \sum_{j=1}^{(q-1)/2} \left\lfloor \frac{jp}{q} \right\rfloor$$

satisfying

$$(-1)^T = \left(\frac{p}{q}\right).$$

As

$$S+T=\frac{p-1}{2}\cdot\frac{q-1}{2}$$

we arrive at

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{S+T}=(-1)^{(p-1)(q-1)/4}$$

thereby finishing the proof. □

D.VI Gerstenhaber's Proof

Many proofs of Quadratic Reciprocity calculate with complex *roots of unity.* The most accessible among these seems to be the proof by Murray Gerstenhaber in the American Mathematical Monthly, in 1963. The idea goes back to F.G.M. Eisenstein (1823-1852).

Let p and q denote two different odd primes. We introduce the following notation.

$$\omega:=\exp(\frac{2\pi i}{p}),\qquad \epsilon:=\exp(\frac{2\pi i}{q}).$$

These complex numbers satisfy $\omega^p=\epsilon^q=1$. From some elementary course you know that the roots of the equations $X^p=1$ and $X^q=1$ are given by the powers $\omega^j, j=0,1,\ldots p-1$ and $\epsilon^k, k=0,1,\ldots,q-1$. The exponents are full sets of representatives modulo p and q, respectively.

We further have

$$\epsilon^j=\epsilon^k \iff j\equiv k \pmod q.$$

As q is odd, $(q,-2)=1$, so the set $0,-2,-4,\ldots,-2(q-1)$ is also a full set of representatives modulo q (we proved this in the context of Euler's Theorem, Lemma A.V.10.)

So the roots to the equation $X^q-1=0$ may also be written $\epsilon^k, k=0,-2,-4,\cdots-2(q-1)$. This yields the factorization

$$X^q-1=(X-1)(X-\epsilon^{-2})(X-\epsilon^{-4})\cdots(X-\epsilon^{-2(q-1)}).$$

Substituting $X\rightarrow X/Y$, and multiplying both members by Y^q then yields

$$X^q-Y^q=(X-Y)(X-\epsilon^{-2}Y)(X-\epsilon^{-4}Y)\cdots(X-\epsilon^{-2(q-1)}Y).$$

From this we get the following Lemma:

D.VI.1 Lemma.

$$X^q - Y^q = (X - Y)(\epsilon X - \epsilon^{-1}Y)(\epsilon^2 X - \epsilon^{-2}Y)\cdots(\epsilon^{q-1}X - \epsilon^{1-q}Y).$$

Proof. We start with the factorization just derived:

$$(X^q - Y^q) = (X - Y)(X - \epsilon^{-2}Y)(X - \epsilon^{-4}Y)\cdots(X - \epsilon^{-2(q-1)}Y).$$

Each factor in $(X - \epsilon^{-2m}Y)$ can be re-written as $\epsilon^{-m}(\epsilon^m X - \epsilon^{-m}Y)$. The exponents of the extracted factors form an arithmetic sum. Their product is therefore

$$(\epsilon)^{-1-2-\cdots-(q-1)} = (\epsilon)^{-(q-1+1)(q-1)/2} = 1,$$

as the exponent is divisible by q (note that $(q-1)/2$ is an integer). □

One final Lemma precedes the proof of the Quadratic Reciprocity Theorem.

D.VI.2 Lemma. *Suppose* $(a, p) = 1$. *Let* P *again denote the half-system* $1, 2, \ldots, (p-1)/2$.

$$\prod_{k \in P} \frac{\omega^{ak} - \omega^{-ak}}{\omega^k - \omega^{-k}} = \left(\frac{a}{p}\right).$$

Proof. By the arguments in the previous Section, it is clear that each factor in the denominator appears exactly once in the numerator, with the same sign if $ak \equiv s \pmod{p}, s \in P$, and the opposite sign if $ak \equiv -s \pmod{p}, s \in P$. The Lemma thus follows immediately from Gauß' Lemma. □

We are now ready to prove the Quadratic Reciprocity Theorem:

Proof. We put $a = q$ in the results above and further refine the product in the last Lemma. We look more closely at a typical factor.

Dividing the identity of the first Lemma by $X - Y$, and substituting $X = \omega^k, Y = \omega^{-k}$, we may write

$$\frac{\omega^{qk} - \omega^{-qk}}{\omega^k - \omega^{-k}} = \prod_{1 \le j \le q-1} (\epsilon^j \omega^k - \epsilon^{-j}\omega^{-k}).$$

Note that k runs over the half-system P of representatives modulo p, and that j runs over a full system modulo q. This injustice is remedied by pairing the factors corresponding to j , $1 \leq j \leq (q-1)/2$, and $q-j$.

Remembering that $\epsilon^q = 1$, we can replace $q-j$ by $-j$, obtaining

$$(\epsilon^j \omega^k - \epsilon^{-j}\omega^{-k})(\epsilon^{-j}\omega^k - \epsilon^j \omega^{-k}) = \omega^{2k} + \omega^{-2k} - \epsilon^{2j} - \epsilon^{-2j}.$$

With $1 \leq k \leq (p-1)/2$ and j now running over the half-system $Q:\ 1 \leq j \leq (q-1)/2$, we have $(p-1)(q-1)/4$ such factors. Their product is (q/p):

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{k\in P} \frac{\omega^{ak} - \omega^{-ak}}{\omega^k - \omega^{-k}} \\ &= \prod_{k\in P}\prod_{j\in Q}(\omega^{2k} + \omega^{-2k} - \epsilon^{2j} - \epsilon^{-2j})\end{aligned}$$

We now interchange the roles of p and q. In exactly the same manner we arrive at the representation of (p/q) as a product:

$$\left(\frac{p}{q}\right) = \prod_{k\in P}\prod_{j\in Q}(\epsilon^{2j} + \epsilon^{-2j} - \omega^{2k} - \omega^{-2k}).$$

This product is made up of the same $(p-1)(q-1)/4$ factors as before, but with opposite signs. This immediately gives the desired result

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right).$$

□

* D.VII Zolotareff's Proof

This proof requires a fair amount of preparation on permutations and their signs. Most of the material will be familiar to those who have taken a course in Abstract Algebra. However, for the convenience of the reader I include a full discussion of the algebraic prerequisites.

A *permutation* of a finite set is the same as a bijective function from the set to itself. The elements of the set will be often be denoted $1, 2, 3, \ldots n$ or $0, 1, 2, \ldots n-1$. The latter notation will be the most natural in dealing with residue classes mod n, for instance.

Permutations are often notated like this:

$$s : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Each element in the second row is the image of the one above it, that is, $s(1) = 2, s(2) = 1, s(3) = 4, s(4) = 5, s(5) = 3$.

The product of two permutations is defined as their composition: $st(m) = s(t(m))$. The product of s taken d times is of course denoted s^d. The inverse permutation is denoted s^{-1}. It can be visualized by swapping the two rows in the representation above, and permuting the columns so as to get the first row in straight order:

$$s^{-1} : \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

As there are finitely many permutations on a finite set, for a given s two powers must be equal: $s^d = s^e$, $d < e$. Multiplying by $s^{-d} = (s^{-1})^d$ gives $s^{e-d} = \text{id}$, the identical permutation, $\text{id}(m) = m$.

The least positive k with $s^k = \text{id}$ is called the *order* of s. The reader is invited to check that the order of the s given above is 6.

We have already encountered the inverse of s If the order of s is d, so that $s^d\!=$ id, then $s^{-1} = s^{d-1}$.

A permutation on a set partitions the set into disjoint *orbits*.

The elements m, n are said to belong to the same orbit if $n = s^k(m)$ for some non-negative k. The reader familiar with the concept will easily check that this is an equivalence relation. For instance, symmetry follows as $n = s^k(m) \iff m = s^{d-k}(n)$, where d is the order of s.

The elements of one orbit are permuted *cyclically*. Imagine them arranged in a circular fashion with the permutation acting counter-clock-wise, mapping one element to the next along the circle.

In our example, one orbit is 1, 2: $s(1) = 2$, $s(2) = 1$. We use the notation $s = (1\,2)$ to describe this permutation. It could also be written $(2\,1)$.

There is one other orbit, 3, 4, 5: $s(3) = 4$, $s(4) = 5, s(5) = 3$, denoted by $s = (3\,4\,5) = (4\,5\,3) = (5\,3\,4)$. Then s is the product of these two in arbitrary order: $s = (1\,2)(3\,4\,5) = (3\,4\,5)(1\,2)$ (the right factor acts first). The two cycles commute, because they are disjoint.

We now define the *sign* of a permutation. It is commonly defined as $(-1)^N$ where N is the number of *inversions*, the number of times a larger number precedes a smaller number in the second row of the matrix described above.

In our example the inversions are $2 = s(1) > s(2) = 1$, $4 = s(3) > s(4) = 3$, and $5 = s(4) > s(5) = 3$. Their number is odd, hence the sign is -1. The cyclic permutation $(3\,4\,5)$ has two inversions: $4 = s(3) > s(5) = 3$, $5 = s(4) > s(5) = 3$. Their number is even, hence the sign $+1$.

We use the terms *odd* and *even* for permutations having sign -1 or $+1$, respectively.

We now determine the sign of a product.

Let us introduce the expression

$$\Delta = \prod_{n \geq k > j \geq 1} (X_k - X_j)$$

where the X_j are indeterminates, and the elements of the set are notated $1, 2, \ldots, n$.

For any polynomial $p(X_1, X_2), \ldots, X_n)$ we set

$$p^s(X_1, X_2), \ldots, X_n) = p(X_{s(1)}, X_{s(2)}, \ldots, X_{s(n)})$$

so that, in particular,

$$\Delta^s = \prod (X_{s(k)} - X_{s(j)}).$$

Each factor of the product Δ enters Δ^s exactly once, possibly with the opposite sign. The number of factors in either case is $n(n-1)/2$.

Therefore

$$\Delta^s = \pm\Delta.$$

Each factor $(X_{s(k)} - X_{s(j)})$ having $s(k) < s(j)$ contributes a minus sign to the product, the remaining factors a plus sign. The number of minus signs therefore equals the number of inversions, that is:

$$\Delta^s = \operatorname{sign}(s)\Delta$$

where $\operatorname{sign}(s)$ denotes the sign of s.

For instance, for $s = (1\,2\,3)$ $(n = 3)$ we have

$$\Delta = (X_3 - X_1)(X_3 - X_2)(X_2 - X_1)$$

and

$$\Delta^s = (X_1 - X_2)(X_1 - X_3)(X_3 - X_2) = (-1)^2\Delta = \Delta.$$

For $s = (1\,2)$ the reader easily checks that $\Delta^s = -\Delta$.

D.VII.1 Lemma. *sign*(st) = *sign*(s)*sign*(t).

Proof. By definition, $\Delta^t = \mathrm{sign}(t)\Delta$. Then also

$$\Delta^{st} = \prod(X_{st(k)} - X_{st(j)}) = \left(\prod(X_{t(k)} - X_{t(j)})\right)^s = (\Delta^t)^s$$

(note that t acts first) so that

$$\begin{aligned}\mathrm{sign}(st) &= \frac{\Delta^{st}}{\Delta} = \frac{\Delta^{st}}{\Delta^t}\cdot\frac{\Delta^t}{\Delta} = \frac{(\Delta^t)^s}{\Delta^t}\cdot\frac{\Delta^t}{\Delta} = \frac{(\pm\Delta)^s}{\pm\Delta}\cdot\frac{\Delta^t}{\Delta}\\ &= \frac{\Delta^s}{\Delta}\cdot\frac{\Delta^t}{\Delta} = \mathrm{sign}(s)\cdot\mathrm{sign}(t).\end{aligned}$$

□

D.VII.2 Corollary. *A permutation and its inverse have the same sign.*

Proof. Apply the product rule just derived to

$$s^{-1}s = \mathrm{id}$$

and use the fact that id is even as it has no inversions at all. □

We now determine the signs of cyclic permutations. Once they are known, we can determine the sign of *any* permutation by decomposing it into disjoint cycles.

D.VII.3 Lemma. *The sign of a simple transposition (2-cycle)* $(i \quad i+1)$ *is* -1.

Proof. There is exactly one inversion. □

D.VII.4 Lemma. *The sign of an arbitrary transposition* $(i \quad i+m)$ *is also* -1.

Proof. We need to prove that the given transposition is the product of an odd number of simple ones.

This follows easily by induction once we prove:

$$(i \quad i+k+1) = (i+k \quad i+k+1)(i \quad i+k)(i+k \quad i+k+1)$$

We only have to check the product action, in three steps, on the three elements entering the parentheses.

$$\begin{array}{ccccccc} i+k+1 & \to & i+k & \to & i & \to & i \\ i+k & \to & i+k+1 & \to & i+k+1 & \to & i+k \\ i & \to & i & \to & i+k & \to & i+k+1 \end{array}$$

□

We finally deal with cycles of arbitrary length:

D.VII.5 Lemma. *The sign of a k-cycle* $(p_1\, p_2\, \ldots\, p_k)$ *is* $(-1)^{k+1}$. *That is, a cycle of even length is an odd permutation, a cycle of odd length is even.*

Proof. This follows easily by induction from the case $k = 2$ just proved, and the following relation:

$$(p_1\, p_2\, \ldots\, p_{k+1}) = (p_1\, p_2\, \ldots\, p_k)(p_k\, p_{k+1}).$$

The reader is invited to check the action of either member on the elements in parentheses. □

The Multiplication Permutation

We now begin the proof of Quadratic Reciprocity. p, q are two different odd prime numbers. Let g denote a primitive root modulo p. It acts on the classes of $1, 2, \ldots, p-1$ by multiplication. By invertibility the elements $g \cdot 1, g \cdot 2, \ldots, g \cdot (p-1)$ are pairwise incongruent modulo p, that is, multiplication by g permutes the invertible classes modulo p.

D.VII.6 Lemma. *The permutation s just described is* odd.

Proof. It is cyclic: $(1\, g\, g^2\, \ldots\, g^{p-2})$, of even length, as

$$s(1) \equiv g,\ s(g) \equiv g^2, \ldots, s(g^{p-3}) \equiv g^{p-2},\ s(g^{p-2}) \equiv q^{p-1} \equiv 1 \pmod{p}.$$

□

Now consider the permutation performed by *any* invertible class, on multiplication.

D.VII.7 Lemma. *Let $1 \leq r \leq p-1$. The permutation $s(m) \equiv rm$ $\pmod{p}$, $m = 1, 2, \ldots, p-1$, has the sign (r/p), i.e., it is even if and only if r is a quadratic residue modulo p.*

Proof. Writing $r \equiv g^k \pmod{p}$ we know that $(r/p) = (-1)^k$. As g performs a permutation of sign -1, g^k performs a permutation of sign $(-1)^k$. □

D.VII.8 Example. We exemplify this for $p = 7$. Multiplying 1, 2, 3, 4, 5, 6 by 2 yields, on reduction modulo p, 2, 4, 6, 1, 3, 5, i.e., the permutation is $(1\,2\,4)(3\,6\,5)$ which is even. This is due to 2 being a quadratic residue, $2 \equiv 3^2$ (mod 7).

3 is a quadratic non-residue, in fact a primitive root modulo 7. It affords the cyclic permutation $(1\,3\,2\,6\,4\,5)$, which is of even length, hence odd. □

The Matrix Transpose Permutation

We now consider an $m \times n$–matrix , the elements of which we denote by

$$X(i, j),\ 1 \leq i \leq m,\ 1 \leq j \leq n.$$

We assume that the elements represent a permutation of the numbers $1, 2, \ldots, mn$ or $0, 1, 2, \ldots mn-1$, after "straightening out" the matrix. We do this by reading the elements row-wise.

That amounts to ordering the indices as follows: We have $(i, j) < (k, l)$ if $k > i$ (second element lower), or if $i = k, l > j$ (elements in the same row, second element further to the right). Equivalently, the element $X(i, j)$ has the number $(i-1)n + j$ in that enumeration.

In the matrix

$$\begin{pmatrix} X(1,1) & X(1,2) & X(1,3) \\ X(2,1) & X(2,2) & X(2,3) \end{pmatrix}$$

the element $X(1, 3)$ succeeds $X(1, 1)$ and precedes $X(2, 1)$.

We will need to know the sign of the permutation effected by transposing the matrix. In our example we want to compare the straightening of the above matrix with that of

$$\begin{pmatrix} X(1,1) & X(2,1) \\ X(1,2) & X(2,2) \\ X(1,3) & X(2,3). \end{pmatrix}$$

D.VII.9 Lemma. *Assume that the elements of the matrix are in ascending order, when enumerated as above (i.e.,* 1 *to* mn *or* 0 *to* $mn-1$*) The sign of the matrix transpose permutation then is*

$$(-1)^{mn(m-1)(n-1)/4}.$$

Proof. We count the number of inversions.

Consider an arbitrary pair of positions $(k, l), (i, j)$, where $k > i$ or $k = i$, $l > j$. Transposing the matrix amounts to interchanging the column and row indices, yielding the pair (l, k), (j, i). In the second case, $k = i$, no inversion results.

In the first case there are $m(m-1)/2$ possible pairs k, i. One such pair results in an inversion if and only $l < j$, which means $n(n-1)/2$ possible cases. The total number of inversions is therefore $mn(m-1)(n-1)/4$. So the permutation afforded by transposing the matrix is of sign

$$(-1)^{(m-1)(n-1)mn/4}.$$

□

D.VII.10 Lemma. *Suppose the elements of the matrix are not in ascending order. The sign of the matrix transpose permutation will then still be*

$$(-1)^{mn(m-1)(n-1)/4}.$$

Proof. Suppose the given ordering arises from the standard arrangement by the permutation s. Denote the permutation discussed above by u. Then our permutation can be described as first performing s^{-1} to get everything back in straight order, followed by the matrix transposition t, and then by s. The resulting permutation, $u = sts^{-1}$, has the same sign as t by the product rule, as s and s^{-1} have the same sign. □

Remark: An alternative proof is to note that exactly those moves that would produce an inversion from the standard order will, from the given order, either create an inversion or destroy the one we already had. So the numbers of inversions in the two situations are congruent modulo 2.

D.VII.11 Example. The matrix

$$\begin{pmatrix} 2 & 3 & 4 \\ 5 & 6 & 1 \end{pmatrix}$$

arises from the standard order by the cyclic permutation

$$s = (1\,2\,3\,4\,5\,6), \quad s^{-1} = (6\,5\,4\,3\,2\,1).$$

The composition sts^{-1} then reads:

$$\begin{pmatrix} 2 & 3 & 4 \\ 5 & 6 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \to \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & 5 \\ 3 & 6 \\ 4 & 1 \end{pmatrix}.$$

Straightening out the matrices it reads

$$sts^{-1} = (1\,2\,3\,4\,5\,6)(2\,4\,5\,3)(6\,5\,4\,3\,2\,1) = (3\,5\,6\,4).$$

□

We will apply this to the case $m = p$ and $n = q$, both odd. The factors m, n in the exponent do not affect the sign. So in this case the sign is simply

$$(-1)^{(p-1)(q-1)/4} \qquad (*)$$

The proof of Quadratic Reciprocity

Write down the numbers $0, 1, 2, \ldots pq - 1$,corresponding to all the classes modulo pq, in straight order in a $p \times q$–matrix :

$$\begin{pmatrix} 0 & 1 & 2 & \ldots & q-1 \\ q & q+1 & q+2 & \ldots & 2q-1 \\ \ldots & & & & \ldots \\ (p-1)q & (p-1)q+1 & (p-1)q+2 & \ldots & pq-1 \end{pmatrix}$$

The elements of each row are mutually incongruent modulo q.

The elements of a column are mutually congruent modulo q, but incongruent modulo p. This because we move down the columns by repeated addition of q, and different multiples of q are incongruent modulo p

From the bottom of the column we reach the top by adding yet another q and reducing moduloo pq, i.e., dividing by pq and keeping the least positive remainder.

We now permute the elements within each row by replacing the j term in $(m-1)q + j$ with the least positive remainder of pj modulo q. We thus perform the same permutation within each row so that the whole columns are permuted.

We have proved that each such permutation is of sign (p/q). As the number of rows is odd, the resulting product too is of sign (p/q).

The first column is not affected by this operation. In the second column the first element is now p', the least positive remainder of p modulo q. The following elements are $p' + q$, $p' + 2q$, etc.

One of these, say the j :th one is p. Several cyclic permutations within the column will bring p to the top.

As the length of each column is odd, all these permutations are even. On performing further cyclic permutations within the second column we can bring $2p$ to the top. In the same manner we bring $3p$ to the top of the third column, etc. All these permutations are even.

We finally arrive at the following matrix:

$$\begin{pmatrix} 0 & p & 2p & \dots & (q-1)p \\ q & q+p & q+2p & \dots & q+(q-1)p \\ \dots & & & & \dots \\ (p-1)q & (p-1)q+p & (p-1)q+2p & \dots & (p-1)q+(q-1)p \end{pmatrix} \qquad (**)$$

everything taken modulo pq. The total sign of this permutation is still (p/q).

But we could have achieved the same result by a different route. Start by writing down the same elements in the same order, but in a q/p–matrix:

$$\begin{pmatrix} 0 & 1 & 2 & \dots & p-1 \\ p & p+1 & p+2 & \dots & 2p-1 \\ \dots & & & & \dots \\ (q-1)p & (q-1)p+1 & (q-1)p+2 & \dots & pq-1 \end{pmatrix}$$

We then permute the rows in the same way as before, but with p and q interchanged. A permutation of sign (q/p) will result in the transpose of (**).

We retrieve (**) by transposing the last matrix, a permutation whose sign we determined above, (*).

We finally arrive at Quadratic Reciprocity:

$$\boxed{(\frac{p}{q}) = (-1)^{(p-1)(q-1)/4}(\frac{q}{p})}.$$

D.VII.12 Example. The following Example illustrates all the steps in the case $p = 5, q = 7$. We started from

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 \\ 28 & 29 & 30 & 31 & 32 & 33 & 34 \end{pmatrix}$$

We then multiplied the first row by 5, and reduced it modulo 7: $\begin{pmatrix} 0 & 5 & 3 & 1 & 6 & 4 & 2 \end{pmatrix}$, and permuted the remaining rows in the same manner. As a result the whole columns were permuted:

$$\begin{pmatrix} 0 & 5 & 3 & 1 & 6 & 4 & 2 \\ 7 & 12 & 10 & 8 & 13 & 11 & 9 \\ 14 & 19 & 17 & 15 & 20 & 18 & 16 \\ 21 & 26 & 24 & 22 & 27 & 25 & 23 \\ 28 & 33 & 31 & 29 & 34 & 32 & 30 \end{pmatrix}$$

We then permuted the columns cyclically several times so as to bring the elements $0, p, 2p, \dots (q-1)p$ to the top:

$$\begin{pmatrix} 0 & 5 & 10 & 15 & 20 & 25 & 30 \\ 7 & 12 & 17 & 22 & 27 & 32 & 2 \\ 14 & 19 & 24 & 29 & 34 & 4 & 9 \\ 21 & 26 & 31 & 1 & 6 & 11 & 16 \\ 28 & 33 & 3 & 8 & 13 & 18 & 23 \end{pmatrix} \qquad (***)$$

The sign of the resulting permutation is $(5/7) = -1$.

We then started afresh from

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ 10 & 11 & 12 & 13 & 14 \\ 15 & 16 & 17 & 18 & 19 \\ 20 & 21 & 22 & 23 & 24 \\ 25 & 26 & 27 & 28 & 29 \\ 30 & 31 & 32 & 33 & 34 \end{pmatrix}$$

This time we multiplied by the remainder of 7 modulo 5, that is, by 2:

$$\begin{pmatrix} 0 & 2 & 4 & 1 & 3 \\ 5 & 7 & 9 & 6 & 8 \\ 10 & 12 & 14 & 11 & 13 \\ 15 & 17 & 19 & 16 & 18 \\ 20 & 22 & 24 & 21 & 23 \\ 25 & 27 & 29 & 26 & 28 \\ 30 & 32 & 34 & 31 & 33 \end{pmatrix}$$

We then permuted each column cyclically several times so as to get the row $\begin{pmatrix} 0 & 7 & 14 & 21 & 28 \end{pmatrix}$ on top:

$$\begin{pmatrix} 0 & 7 & 14 & 21 & 28 \\ 5 & 12 & 19 & 26 & 33 \\ 10 & 17 & 24 & 31 & 3 \\ 15 & 22 & 29 & 1 & 8 \\ 20 & 27 & 34 & 6 & 13 \\ 25 & 32 & 4 & 11 & 18 \\ 30 & 2 & 9 & 16 & 23 \end{pmatrix}$$

The resulting permutation is of sign $(7/5) = (2/5) = -1$ Transposing finally led to

$$\begin{pmatrix} 0 & 5 & 10 & 15 & 20 & 25 & 30 \\ 7 & 12 & 17 & 22 & 27 & 32 & 2 \\ 14 & 19 & 24 & 29 & 34 & 4 & 9 \\ 21 & 26 & 31 & 1 & 6 & 11 & 16 \\ 28 & 33 & 3 & 8 & 13 & 18 & 23 \end{pmatrix} \qquad (**)$$

The sign of the matrix transposition is

$$(-1)^{(7-1)(5-1)/4}$$

$= 1.$ □

Chapter E

Some Diophantine Problems

E.I Primes as Sums of Squares

Let p be a prime number. We want to give conditions for it to be representable as a sum of squares, $p = a^2 + b^2$, $a, b \in \mathbf{Z}$. The techniques introduced will allow as to deal with other similar *Diophantine* problems, such as $p = a^2 + m \cdot b^2$, $m = \pm 2, \pm 3$.

The case $p = 2$ is immediate: $2 = 1^2 + 1^2$. We also easily exclude the case $p \equiv 3 \pmod 4$. As $m^2, n^2 \equiv 0 \text{ or } 1 \pmod 4$, we must have $m^2 + n^2 \equiv 0, 1, \text{ or } 2 \pmod 4$.

In order to handle the case $p \equiv 1 \pmod 4$ we prove the following Lemma, due to Norwegian mathematician Axel Thue (1863-1922).

E.I.1 Lemma (Thue's Lemma). *Let $p \geq 2$ be an integer, and x an integer with $(x, p) = 1$. Then there exist integers m, n, $0 < |m|, |n| < \sqrt{p}$ satisfying*

$$mx \equiv n \pmod p.$$

One might say that the idea of Thue's Lemma is to represent an invertible class as a "quotient" of relatively small numbers. This trick often turns a congruence into an equality. The proof is based on the surprisingly productive Dirichlet Principle: if n objects are distributed over $m < n$ boxes, two of them must belong to the same box.

Proof. We recall the notation $\lfloor a \rfloor$ for the "floor" or "integral part" of a, the greatest integer n satisfying $n \leq a$.

We now form all possible numbers of the form $mx - n,\ 0 \leq m, n \leq \lfloor \sqrt{p} \rfloor$. Their number is $(\lfloor \sqrt{p} \rfloor + 1)^2 > p$. As their number is greater than the number of classes modulo p, two of them must be congruent modulo p:

$$m_1 x - n_1 \equiv m_2 x - n_2 \pmod{p}; \qquad (m_1 - m_2)x \equiv (n_1 - n_2) \pmod{p}.$$

Here $m_1 \not\equiv m_2 \pmod{p}$, or $n_1 \not\equiv n_2 \pmod{p}$.

In fact, *both* conditions must hold. Obviously $m_1 \equiv m_2 \pmod{p}$ would give $n_1 \equiv n_2 \pmod{p}$. Conversely, assume $p | (n_1 - n_2) = x(m_1 - m_2)$. As $(p, x) = 1$, the First Divisibility Theorem (A.II.1) would imply $p | (m_1 - m_2)$.

Put $m = m_1 - m_2$, $n = n_1 - n_2$. By the restriction on the sizes of m_1, m_2, n_1, n_2 we easily see that $0 < |m|, |n| < \sqrt{p}$, and we are done. □

E.I.2 Theorem. *The prime number p is representable as a sum of squares, $p = a^2 + b^2$, if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.*

Proof. It remains to settle the case $p \equiv 1 \pmod{4}$.

We first note that

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = 1 \pmod{p},$$

as $(p-1)/2$ is even by assumption. So we find an x satisfying

$$x^2 \equiv -1 \pmod{p}. \tag{$*$}$$

Next Thue's Lemma supplies us with $m, n,\ 0 < |m|, |n| < \sqrt{p}$, satisfying

$$mx \equiv n \pmod{p}.$$

Multiplying (*) by m^2 gives $m^2 x^2 \equiv -m^2 \pmod{p}$, whence

$$m^2 + n^2 \equiv m^2 + m^2 x^2 \equiv 0 \pmod{p}.$$

The sizes of m, n immediately imply $0 < m^2 + n^2 < 2p$. Therefore, the congruence implies $m^2 + n^2 = p$, and we are done. □

The representation $p = x^2 + y^2$ is essentially unique, i.e., unique up to order of terms and signs of the x, y:

E.I.3 Theorem. *Let N be an odd number, representable in two different ways as $N = x^2 + y^2 = u^2 + v^2$ (assuming x, u of equal parity, we are assuming that $x^2 \neq u^2$ and $y^2 \neq v^2$). Then there is a factorization $N = PQ$ where both factors are > 1.*

Hence, if p is a prime number, its representation as $p = x^2 + y^2$, $x > 0$ odd, $y > 0$ even, is unique.

Proof. Factoring the two members of $u^2 - x^2 = y^2 - v^2$ we get $(u - x)(u + x) = (y - v)(y + v)$. All numbers involved are even, so we may write

$$\frac{u-x}{2} \cdot \frac{u+x}{2} = \frac{y-v}{2} \cdot \frac{y+v}{2}.$$

Let e denote the gcd of $(u + x)/2$ and $(y - v)/2$;

$$\frac{u+x}{2} = eg, \quad \frac{y-v}{2} = eh, \quad (g, h) = 1,$$

where all e, g, h are $\neq 0$. Using the First Divisibility Theorem we see that $g|(y + v)/2$, and $h|(u - x)/2$, whence, for some f, the factorizations

$$\frac{u-x}{2} = fh, \quad \frac{y+v}{2} = fg.$$

Combining these relations we easily obtain

$$\begin{aligned} x &= eg - fh, \\ y &= eh + fg, \end{aligned}$$

i.e., in complex form,

$$x + iy = (eg - fh) + i(eh + fg) = (e + if)(g + ih),$$

and, in like manner,

$$u + iv = (e + if)(g - ih),$$

whence

$$N = x^2 + y^2 = u^2 + v^2 = (e^2 + f^2)(g^2 + h^2)$$

with both factors ≥ 2.

Note that, e.g., $x^2+y^2 = (x+iy)(x-iy) = (e+if)(e-if)(g+ih)(g-ih)$.□

Our technique of proof (using Thue's Lemma) is eminently programmable. The formal proof that our algorithm below really works is best presented within the framework of continued fractions, and will be given (and generalized) later on.

However, in the remark following the Example, we indicate a more direct proof. We then describe another algorithm, which is perhaps easier to understand, but which does not generalize too well.

E.I.4 Example. Let $p = 73$, a prime number $\equiv 1 \pmod 4$.

First we need to solve the congruence $x^2 \equiv -1 \pmod p$. This is easy once we have found a quadratic non-residue a. Setting $x \equiv a^{(p-1)/4} \pmod{73}$, the Euler Criterion (D.I.4) gives

$$x^2 \equiv a^{(p-1)/2} \equiv -1 \pmod p.$$

Trying $a = 2, 3, \ldots$, the first non-residue is $a = 5$, giving $x = 27$. Next we perform Extended Euclid (A.I.7) on the pair $73, 27$. Although we will need only half of the steps, we give them all below.

$$\begin{array}{rr}
1 \cdot 73 + 0 \cdot 27 = 73 & \\
0 \cdot 73 + 1 \cdot 27 = 27 & 73 - 2 \cdot 27 = 19 \\
1 \cdot 73 - 2 \cdot 27 = 19 & 27 - 1 \cdot 19 = 8 \\
-1 \cdot 73 + 3 \cdot 27 = 8 & 19 - 2 \cdot 8 = 3 \\
3 \cdot 73 - 8 \cdot 27 = 3 & 8 - 2 \cdot 3 = 2 \\
-7 \cdot 73 + 19 \cdot 27 = 2 & 3 - 2 = 1 \\
10 \cdot 73 - 27 \cdot 27 = 1 & \\
(-27 \cdot 73 + 73 \cdot 27 = 0) &
\end{array}$$

Among the right members, the first one $< \sqrt{73}$ is $n = 8$. The coefficient 3 in the corresponding left member is less than $8 < \sqrt{73}$ – it is the same as the 3 occuring in the next right member. That is the general theoretical fact that we will not prove formally here. So $m = -3$, and $n = 8$, satisfy $m \cdot 27 + n \equiv 0 \pmod{73}$. By the proof of the Theorem they are the solution to our problem: $m^2 + n^2 = 3^2 + 8^2 = 73$. □

Remark: The reason I did all of Euclid was to exhibit a beautiful symmetry. Read the right members from the top down, and the coefficients for 27 from the bottom up, and you will see the pattern. Start from the last equation, Bézout, which expresses the fact that $27^2 \equiv -1 \pmod{73}$ – and thus is known before we even start Euclid. Add the obvious identity $-27 \cdot 73 + 73 \cdot 27 = 0$ below it.

The crucial observations are the following. The right members decrease, by the very construction of Euclid. The coefficients for 27 in the left members have alternating signs, and their absolute values decrease when read from the bottom up. That is because (working downwards) at each step we subtract numbers of opposite signs.

Also every equation can be reconstructed by a row operation on the two equations just *below* it. Namely, by construction: $\text{row}(k+2) = \text{row}(k) - m \cdot \text{row}(k+1)$, for some m, hence $\text{row}(k) = \text{row}(k+2) + m \cdot \text{row}(k+1)$, for the same m.

From this it may be seen that the coefficients for 27 (apart from their signs), read from the bottom up, also arise from Euclid applied to 73 and 27.

Omitting the first equation, the number of equations given above must be even, as the sign for $27 \cdot 27$ in the last equation must equal -1. So by the symmetry stated above, in the middle of the Extended Euclidean Algorithm we must have something like this:

$$\begin{aligned} ap \pm bx &= c, \\ dp \mp cx &= b. \end{aligned}$$

Here x is the solution to $x^2 \equiv -1 \pmod{p}$ (p need not be a prime number; we are only assuming the solvability of the congruence). Multiplying the first equation by c, and the second by b, and adding, gives $p(ac + bd) = b^2 + c^2$.

All that remains, then, is to prove $ac + bd = 1$. Think of this expression as plus or minus the determinant formed from the left members of the two equations. Each step in Extended Euclid may be conceived of as a row operation, followed by swapping the two rows. So the determinants belonging to successive pairs of equations must be the same, except for alternating signs.

As the determinant formed from the first pair of equations equals 1, we get $ac + bd = \pm 1$, and only the plus sign is possible, as p, $b^2 + c^2 > 0$.

Even if p is not a prime number, we still have $(b, c) = (p, x) = 1$, so the representation $p = b^2 + c^2$ is *proper*, in the sense introduced later.

A slightly different take on Thue's Lemma, with applications, can be found in Keith Matthews, "Thue's theorem and the diophantine equation $x^2 - Dy^2 = \pm N$", *Mathematics of Computation*, **71** (239):1281-1286, 2001.

E.I.5 Example. Here we describe another algorithm for solving $a^2+b^2 = p$. It goes back to Fermat's proof by "infinite descent". It is slightly slower than the Extended Euclid method.

Again we start with $x^2 + 1 \equiv 0 \pmod p$ and set $a_0 = x$, $b_0 = 1$. We also introduce $r_0 > 0$ by $x^2 + 1 = r_0 \cdot p$.

Suppose after a number of steps we have achieved

$$a_k^2 + b_k^2 = r_k p, \quad r_k \geq 1.$$

If $r_k > 1$ we look for a step leading to a smaller multiple of p. Divide a_k, b_k by r_k (note that we are using the remainder, positive or negative, closest to zero):

$$\begin{aligned} a_k &= m_k r_k + A_k; \quad |A_k| \leq r_k/2, \\ b_k &= n_k r_k + B_k; \quad |B_k| \leq r_k/2. \end{aligned}$$

As $r_k|(a_k^2 + b_k^2)$ it then holds that $r_k|(A_k^2 + B_k^2) \leq r_k^2/2$, that is,

$$A_k^2 + B_k^2 = r_{k+1} r_k, \quad r_{k+1} \leq \frac{1}{2} r_k.$$

Now set

$$a_{k+1} + ib_{k+1} = (a_k + ib_k)(A_k - iB_k)/r_k.$$

It is clear from the expressions that the right member is a complex *integer*, as both

$$a_k A_k + b_k B_k = (a_k^2 + b_k^2) - a_k m_k r_k - b_k n_k r_k$$

and

$$b_k A_k - a_k B_k = (n_k A_k - m_k B_k) r_k$$

are divisible by r_k.

We then get

$$a_{k+1}^2 + b_{k+1}^2 = \frac{(a_k^2 + b_k^2)(A_k^2 + B_k^2)}{r_k^2} = \frac{(r_k p)(r_k r_{k+1})}{r_k^2} = r_{k+1} \cdot p$$

with $r_{k+1} \leq r_k/2$, and clearly the the algorithm will terminate within a number of steps bounded by $\log_2 p$.

In our previous example we get: $a_0 = 27, b_0 = 1, a_0^2 + b_0^2 = 10 \cdot 73$, $r_0 = 10$.

The division step is $A_0 = 27 - 3 \cdot 10 = -3, B_0 = 1$, yielding $a_1 + ib_1 = (27 + i)(-3 - i)/10 = -8 - 3i$, whence $8^2 + 3^2 = 1 \cdot 73$, and we are finished.

□

E.I: Exercises

1. Following the procedure for $p = x^2 + y^2$, show that every prime $p \equiv 1$ or 3 (mod 8) can be represented in the form $p = x^2 + 2y^2$, where x, y are integers.

2. Let p be a prime number $\equiv 1$ or 7 (mod 8). Following the proof for $p = x^2 + y^2$, and using Thue's Lemma, show that p can be represented as $p = x^2 - 2y^2$, where x, y are integers.

Probably you will manage to solve $x^2 - 2y^2 = -p$. Using $x^2 - 2y^2 = (x - y\sqrt{2})(x + y\sqrt{2})$ and multiplying by a suitable quantity, you will get the right sign.

3. Prove that the prime number p is representable as $p = 2x^2 + 3y^2$ if and only if $p \equiv 5, 11 \pmod{24}$. The condition $(-6/p)$ supplies you with four possible classes, reduction modulo 3 and 8 excludes two of them, Thue does the rest.

What are the relevant congruence conditions for $p = x^2 + 6y^2$?

4. Let p, x be integers, $p > x > 0$, $(p, x) = 1$. Show that Extended Euclid (as in Example E.I.4) produces equations of the form $s_k p + t_k x = r_k > 0$ with

$$\begin{vmatrix} t_k & r_k \\ t_{k+1} & r_{k+1} \end{vmatrix} = \pm p$$

Use this to give a constructive proof of Thue's Lemma.

5. **Suggestions for computing:** Combining a Jacobi routine (for finding a quadratic non-residue) and Extended Euclid, write the following prime numbers as a sum of two squares:

(a) 2 70688 88573

(b) 15 25852 86200 53909

(c) 2 78584 90014 12425 44371 60997

E.II Composite Numbers

We now turn to the question of representing a composite number as a sum of squares. First a little Lemma:

E.II.1 Lemma. *If the positive integers a, b are representable as a sum of squares, then so is their product.*

Proof. Assuming $a = m^2 + n^2 = (m + ni)(m - ni)$, $b = r^2 + s^2 = (r + si)(r - si)$, the proof is almost immediate:

$$\begin{aligned} ab &= (m+ni)(r+si)(m-ni)(r-si) \\ &= \big((mr-ns)+i(ms+nr)\big)\big((mr-ns)-i(ms+nr)\big) \\ &= (mr-ns)^2+(ms+nr)^2. \end{aligned}$$

□

We now have the following Theorem:

E.II.2 Theorem. *The positive integer N is representable as a sum of squares if and only if primes $p \equiv 3 \pmod 4$ enter its factorization with even multiplicity.*

Proof. Given the trivial representation $p^2 = p^2 + 0^2$, the "if" part is an immediate consequence of the Lemma above.

For the "only if" part, assume $N = m^2 + n^2$, and that $p \equiv 3 \pmod 4$ is a prime factor of N.

We take a closer look at the congruence $m^2 + n^2 \equiv 0 \pmod p$. We claim that both m and n are divisible by p, hence that N is divisible by p^2.

By way of contradiction, assume $p \nmid m$. Then also $p \nmid n$. We now achieve our contradiction by comparing Legendre symbols:

$$1 = \left(\frac{m^2}{p}\right) = \left(\frac{-n^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{n^2}{p}\right) = -1 \cdot 1 = -1.$$

We used the First Supplementary Theorem (D.I.9): As $(p-1)/2$ is odd, $(-1)^{(p-1)/2} = -1$.

So $p|m$, $p|n$, $p^2|N$. By an easy induction on the multiplicity $v_p(N)$ (or on N), using the representation

$$\frac{N}{p^2} = \left(\frac{m}{p}\right)^2 + \left(\frac{n}{p}\right)^2,$$

we may assume that N/p^2 is exactly divisible by an even power of p (e.g., $p^0 \dots$), so that N is, too. □

E.II.3 Example.

a)

$221 = 17 \cdot 13 = (4+i)(3+2i)(4-i)(3-2i) = (10+11i)(10-11i) = 10^2 + 11^2$

but also

$$221 = (4+i)(3-2i)(4-i)(3+2i) = (14-5i)(14+5i) = 14^2 + 5^2.$$

b) $539 = 7^2 \cdot 11$ is not a sum of squares, as $11 \equiv 3 \pmod 4$, of odd multiplicity.

c) $833 = 7^2 \cdot 17 = 7^2(4^2 + 1^2) = 28^2 + 7^2$. □

Perhaps a more interesting result regards what is usually known as *"proper (or primitive) representation"* in the literature. The proof is usually done in the context of complex integers. An independent proof is given here.

In the exercises you are invited to prove that the conditions in the Theorem are equivalent to the solvability of $x^2 \equiv -1 \pmod a$.

E.II.4 Theorem (Proper Representation). *The positive integer a is* properly representable *as a sum of squares,*

$$a = m^2 + n^2 = (m+in)(m-in), \quad (m,n) = 1,$$

if and only if the prime factor 2 enters its factorization at most once, and prime factors $p \equiv 3 \pmod 4$ not at all.

Proof. *(Necessity)* In the course of the last proof we showed that $m^2 + n^2 \equiv 0 \pmod{p}$, where the prime number $p \equiv 3 \pmod{4}$, implies that both m and n are divisible by p, hence $(m, n) > 1$.

And if $m^2 + n^2 \equiv 0 \pmod{4}$, m and n must be both even or both odd. In the latter case $m^2 \equiv n^2 \equiv 1$, $m^2 + n^2 \equiv 2 \pmod{4}$, contradicting the assumption. Hence $(m, n) \geq 2 > 1$. □

The *sufficiency* part of the Theorem will follow from the following two Lemmas. The first of them reduces the question, inductively, to that of (odd) prime powers.

E.II.5 Lemma. *Assume a, b, c, d rational integers, satisfying $(a, b) = (c, d) = (a^2 + b^2, c^2 + d^2) = 1$. Put $u + iv = (a + ib)(c + id)$. Then also $(u, v) = 1$.*

Proof. Any prime number dividing $u + iv$ (i.e., one dividing both u and v) will divide (the real and imaginary parts of) $(ua+vb)+i(va-ub) = (u+iv)(a-ib) = (a^2+b^2)(c+id)$ and, in the same manner, it will divide $(u+iv)(c-id) = (c^2 + d^2)(a + ib)$. As it cannot divide both $a^2 + b^2$ and $c^2 + d^2$, it must divide either $c + id$ or $a + ib$, which is impossible, as $(a, b) = (c, d) = 1$. □

The second Lemma takes care of odd prime powers.

E.II.6 Lemma. *Assume $a^2 + b^2 = p$, where p is a prime number $\equiv 1 \pmod{4}$. Obviously, then, $a \not\equiv b \pmod{2}$, and $(a, b) = 1$. Let*

$$u_n + iv_n = (a + ib)^n, \text{ so that } u_n^2 + v_n^2 = p^n.$$

Then u_n, v_n too are of opposite parity (obviously), and $(u_n, v_n) = 1$.

Proof. Any integer dividing $u_n + iv_n$ will divide all $u_m + iv_m$, $m \geq n$. Therefore it suffices to prove the Lemma for $n = 2^k$; $k = 0, 1, 2, 3, \ldots$.

By induction all we need to prove is the following: If u, v are of opposite parity, and $(u, v) = 1$, then the same holds for the real and imaginary parts of $(u + iv)^2 = u^2 - v^2 + 2iuv$.

Under the stated assumption $u^2 - v^2$ is obviously odd and $2uv$ even. Any odd prime q dividing uv divides u or v but not both. So q divides u^2 or v^2, but not both, hence cannot divide their difference. □

Here is how the Theorem follows. Clearly, the second Lemma proves it for prime powers. The proof now uses induction on the number of prime powers entering the representation $N = 2^e \cdot p_1^{e_1} \cdots p_k^{e_k}$, $e = 0$ or 1.

The inductive step is provided by the first Lemma, where we take $a^2 + b^2$ to be one of the prime powers, assuming already proved that the product of the remaining prime powers is representable as $c^2 + d^2$, $(c, d) = 1$. □

E.II.7 Example.

a) $17^2 = (4+i)^2(4-i)^2 = (15+8i)(15-8i) = 15^2+8^2$ is a proper representation of 289.

b) $34 = 2 \cdot 17 = (1 + i)(4 + i)(1 - i)(4 - i) = (3 + 5i)(3 - 5i) = 3^2 + 5^2$ is a proper representation of 34.

c) The representation $833 = 28^2 + 7^2$ is not proper, as $(28, 7) = 7$. Assuming $833 = m^2 + n^2$ leads to the congruence $m^2 + n^2 \equiv 0 \pmod 7$. As we have seen in the proof above, that would imply that both m and n are divisible by 7. Hence there is no proper representation of the number 833.

d) The representation $68 = 4 \cdot 17 = 8^2 + 2^2$ is not proper. Assuming $68 = m^2 + n^2$ leads to $m^2 + n^2 \equiv 0 \pmod 4$ which is possible only if m and n are both even. Hence the number 68 cannot be properly represented as a sum of squares. □

We record a nice Corollary to the Theorem just proved.

E.II.8 Corollary.

a) If P, Q, not both even, are properly representable in the form $x^2 + y^2$, then so is their product.

b) If N is properly representable in the form $N = x^2 + y^2$, then the same is true of every integer $P > 1$ dividing N.

□

E.II: Exercises

1. Which of the numbers 112, 851, 829, 629, 605 can be represented (resp. properly represented) as the sum of two squares? Hand calculation, with theoretical explanations.

2. Let m be an odd positive integer. Give an explicit bijection between the solution sets to the Diophantine equations $x^2 + y^2 = m$ and $x^2 + y^2 = 2m$.

Do the same for the sets of proper solutions.

By "explicit" is meant an expression for both the mapping and its inverse, with proper verifications.

3. Represent 9061 as the sum sum $x^2 + y^2, x \geq y \geq 0$, of two integer squares, in four different manners.

The divisibility theory in $\mathbf{Z}[i]$ (Chapter K) will show that the exact number is four.

Assuming that, how many lattice (integer) points are there on the circle $x^2 + y^2 = 9061$?

4. Assume a not divisible by p. Show that the congruence $x^2 + y^2 \equiv a \pmod{p}$ is solvable. Hint: How many incongruent elements are there of the form $x^2 - a$ or y^2, respectively?

5. We wish to show that the Diophantine equation $y^2 = x^3 + 7$ is unsolvable. Hint: Add a one to both members, and show that not every prime factor of the right member is $\equiv 1 \pmod{4}$.

6. Show that -1 is a quadratic residue modulo n if and only if $n = 2^e \cdot p_1 \cdot p_2 \cdots p_k$ where $e = 0$ or 1 and the odd prime factors $p_j \equiv 1 \pmod{4}$.

7. The following is a classical and useful observation:

If

$$x^2 \equiv a^2 \pmod{N},$$

but

$$x \not\equiv \pm a \pmod{N},$$

then N is composite (why?)

Suppose $D \geq 2$ (the case $D = 1$ is dealt with above, E.I.3).

(a) Show that $(a^2 + Db^2)(c^2 + Dd^2)$ can be expressed as $m^2 + Dn^2$ in two different ways.

(b) Now assume that $s^2 + Dt^2 = u^2 + Dv^2 = N$ are two different representations of the number N in this special form. Show that $(sv)^2 \equiv (tu)^2 \pmod{N}$, but $sv \not\equiv \pm tu \pmod{N}$. For the latter inequality, use (a).

Under the given assumptions, therefore, N is composite.

E.III Another Diophantine Problem

We now let p be prime $\neq 2, 3$ and ask for conditions for it to be representable as $p = 3m^2 + n^2$. A necessary condition is easy to derive. If $3m^2 + n^2 \equiv 0 \pmod{p}$, then

$$\left(\frac{n^2}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{m^2}{p}\right).$$

As neither m nor n can be divisible by p, the two symbols involving their squares equal one. So a necessary condition is

$$\left(\frac{-3}{p}\right) = 1.$$

In the Example following the statement of Quadratic Reciprocity (D.I.13) we proved that this condition is equivalent to $p \equiv 1 \pmod{3}$.

We now prove the sufficiency of that condition. We follow the pattern of the first Section as closely as possible, until it breaks down.

Again, we solve the congruence $x^2 \equiv -3 \pmod{p}$ for x. Again, Thue's Lemma supplies us with m, n, $0 < |m|, |n| < \sqrt{p}$, such that $mx \equiv n \pmod{p}$. Multiplying the congruence $x^2 \equiv -3 \pmod{p}$ by m^2 we arrive at the congruence $3m^2 + n^2 \equiv 0 \pmod{p}$. This is where the pattern breaks down. Owing to the inequalities for m, n, we can only conclude that $3m^2 + n^2 < 4p$, hence that $3m^2 + n^2 = p, 2p$ or $3p$.

The case $3m^2 + n^2 = 2p$ is easily excluded. We would get $\equiv 2 \pmod{3}$, but $3m^2 + n^2 \equiv 0$ or $1 \pmod{3}$ for all m, n.

If $n^2 + 3m^2 = 3p$, n must be divisible by 3: $n = 3k$. So in this case we get $3k^2 + m^2 = p$ as desired. In the first case there is nothing to prove. So we have indeeed proved the following:

E.III.1 Theorem. *Let p be a prime $\neq 2, 3$. The equation $3m^2 + n^2 = p$ is solvable in integers if and only if $p \equiv 1 \pmod{3}$.*

□

A problem closely related to the one just studied is $p = x^2 \pm xy + y^2$ for $p \neq 2, 3$. It is easy to prove that the same condition, $p \equiv 1 \pmod{3}$, is necessary for solvability. Just let x, y run through all possible pairs of classes modulo 3.

If $p \equiv 1 \pmod 3$ we first solve $p = 3m^2 + n^2$. Then put $\pm q = -m + n$, $n = m \pm q$, yielding $p = 4m^2 \pm 2mq + q^2 = (2m)^2 \pm (2m)q + q^2$ which is of the desired form.

We have proved:

E.III.2 Theorem. *Let p be a prime $\not\equiv 2, 3$. The equation $p = x^2 \pm xy + y^2$ is solvable in integers if and only if $p \equiv 1 \pmod 3$.*

□

Of course, both equations are solvable for $p = 3$ and unsolvable for $p = 2$.

E.III.3 Example.

a) $7 = 3 \cdot 1^2 + 2^2 = 2^2 + 2 \cdot 1 + 1^2$

b) $13 = 3 \cdot 2^2 + 1^2 = 3^2 + 3 \cdot 1 + 1^2$

c) $19 = 3 \cdot 1^2 + 4^2 = 3^2 + 3 \cdot 2 + 2^2$

d) $997 = 3 \cdot 18^2 + 5^2 = 36^2 - 36 \cdot 13 + 13^2$ □

A practical method for solving the Diophantine equation $3m^2 + n^2 = p$, Cornacchia's algorithm, will be given in the Chapter on Continued Fractions (G.VII).

E.III: Exercises

1. (a) Let p be a prime number $\neq 2, 5$. Show that

$$\left(\frac{5}{p}\right) = 1 \quad \Longleftrightarrow \quad p \equiv 1, 4 \pmod 5$$

(b) Suppose p satisfies one of these congruence conditions. Show that there are integers x, y, k, $1 \leq k \leq 4$ such that

$$x^2 - 5y^2 = -k \cdot p$$

Show that the only possibilities are $k = 1, 4$.

(c) Assume $x^2 - 5y^2 = -p$ solvable in integers. Find one solution to $x^2 - 5y^2 = -1$ and use it to show that

$$x^2 - 5y^2 = p$$

is solvable.

(d) Assume $x^2 - 5y^2 = -4p$ solvable in integers. From one solution construct one for $x^2 - 5y^2 = p$ (you may have to distinguish two cases).

2. Suppose $p = 2a^2 + 2ab + 3b^2$. Show that $p \equiv 2, 3 \pmod 5$, that we can solve $2p = u^2 + 5v^2$, and $3p = u^2 + 5v^2$, but that the equation $p = u^2 + 5v^2$ is unsolvable.

3. Let p be a prime, such that $(-5/p)$=1.

(a) Show, using Thue's Lemma (E.I.1), that we can find integers x, y, k such that $x^2 + 5y^2 = k \cdot p$, where $1 \leq k \leq 5$.

(b) If $k = 4, 5$ we can reduce to the cases $k = 1, 2$ on dividing out common factors (calculate modulo suitable integers).

(c) Suppose $x^2 + 5y^2 = 2p$ or $3p$. Show that we may assume x and y congruent modulo 2 (both odd!), or modulo 3, respectively. Use this to show that the equation $2u^2 + 2uv + 3v^2 = p$ is solvable in these two cases.

The previous exercise then shows that the two cases are equivalent, i.e., $x^2 + 5y^2 = 2p$ is solvable if and only if $x^2 + 5y^2 = 3p$ is.

Examples: $p = 47, 43$ (or, more generally: $p \equiv 3,\ 7 \pmod{20}$).

4. If x, y, z are integers satisfying $x^3 + y^3 \equiv z^3 \pmod 9$, then at least one of them is divisible by 3.

5. Suppose x, y can both be written in the form $m^2 + 3n^2$, $m, n \in \mathbf{Z}$. Show that the same holds for their product.

6. Suppose $x = m^2 + 3n^2$, $(m, n) = 1$. Show that x is the product of prime numbers $p \equiv 1 \pmod 3$, and possibly a factor 4. Is the converse true?

7. Suppose $x^3 = m^2 + 3n^2$, where x, m, n are integers, $(m, n) = 1$. Show that $x = a^2 + 3b^2$ where a, b are integers, and $(a, b) = 1$. By looking at the complex factors, deduce factorizations of m, n in terms of a, b.

8. A special case of Fermat's Last Theorem. Consider a solution in integers to the equation $x^3 + y^3 = z^3$, where $(x, y, z) = 1$ (so that the numbers are pairwise relatively prime). We wish to find a solution involving smaller numbers.

First show that we can assume x, y of equal parity. From the factorization $(x+y)(x^2-xy+y^2)=z^3$ deduce a relation of the form $2p(p^2+3q^2)=z^3$ where $(p,q)=(2p,p^2+3q^2)=1$ (be careful to check each step here!). Conclude that p^2+3q^2 and $2p$ are cubes.

Using the previous Exercise, deduce a factorization of $2p$ in smaller cubes and deduce from them a smaller (in some suitable sense) solution to $x^3+y^3=z^3$. You will have to deal the case $3|p$ separately, and be very, very careful.

How does that prove the non-solvability of that equation?

If you are stumped, you may wish to consult the text by H. M. Edwards.

E.IV Modular Square Roots

The last Section indicates the usefulness of algorithms for solving the quadratic congruence $x^2 \equiv n \pmod{p}$, where p is a prime, and n is a quadratic residue modulo p. You may want to read through the Section on fast exponentiation (Section L.V) first.

Easy Cases

We deal with the simplest cases first.

E.IV.1 Example. In the following cases there are explicit expresssions for the solution to the congruence $x^2 \equiv n \pmod{p}$.

a) $p = 4k + 3$.

b) $p = 8k + 5$, $n^{2k+1} \equiv 1 \pmod{p}$.

c) $p = 8k + 5$, $n^{2k+1} \equiv -1 \pmod{p}$.

We now outline the three cases:

a) As $n^{(p-1)/2} = n^{2k+1} \equiv 1 \pmod{p}$, by Euler's Criterion, we have $n^{2k+2} \equiv n \pmod{p}$. So the solution is $x \equiv \pm n^{k+1} \equiv n^{(p+1)/4} \pmod{p}$.

Before turning to cases b), c), note that $n^{(8k+5-1)/2} = n^{4k+2} \equiv 1 \pmod{p}$, by Euler' Criterion, hence $n^{2k+1} \equiv \pm 1 \pmod{p}$, in this case.

b) Take $x \equiv \pm n^{k+1} \equiv \pm n^{(p+3)/4} \pmod{p}$.

c) This time $n^{2k+1} \equiv -1 \pmod{p}$, so the choice $y \equiv \pm n^{k+1} = n^{(p+3)/4} \pmod{p}$ gives a solution to $y^2 \equiv -n \pmod{p}$, wrong sign!

So we need to solve $r^2 \equiv -1 \pmod{p}$.

By the second Ergänzungssatz,

$$\left(\frac{2}{p}\right) = -1, \quad 2^{(p-1)/2} = 2^{4k+2} \equiv -1 \pmod{p}$$

So $r = 2^{2k+1} = 2^{(p-1)/4}$ satisfies $r^2 \equiv -1 \pmod{p}$, and $x = \pm ry$ satisfies $x^2 \equiv n \pmod{p}$. □

E.IV.2 Example. We give numerical examples for all three cases.

a) $43 = 4 \cdot 10 + 3$, so $k = 10$. Let us look at $x^2 \equiv 11 \pmod{43}$.

Here $(11/43) = -(43/11) = -(-1/11) = 1$ and the solution to is $x \equiv \pm 11^{10+1} \equiv \pm 21 \pmod{43}$.

b) $101 = 8 \cdot 12 + 5$, so $k = 12$.

$(5/101) = (101/5) = (1/5) = 1$, and $5^{2k+1} = 5^{25} \equiv 1 \pmod{101}$.

So the solution to $x^2 \equiv 5 \pmod{101}$ is $x \equiv \pm 5^{12+1} \equiv \pm 56 \pmod{101}$.

c) Here we solve $x^2 \equiv 13 \pmod{101}$, where $(13/101) = (101/13) = (10/13) = 1$, and $13^{2k+1} \equiv -1 \pmod{101}$.

Now $13^{13} \equiv 47 \pmod{101}$, and $2^{25} \equiv 10 \pmod{101}$ so the solution is $x \equiv \pm 470 \equiv \pm 66 \pmod{101}$. □

Berlekamp's Method

E.IV.3 Example. One approach to the square root problem is to turn the quadratic congruence into a linear one. Let us start with the easy case, $p \equiv 3 \pmod{4}$. To be explicit, we want to solve $x^2 \equiv n \equiv 6 \pmod{19}$, knowing that $(6/19) = 1$. The trick is to determine $x^{(p-1)/2} \equiv x^9 \pmod{19}$, and use Euler's Criterion (D.I.4).

Squaring the given congruence twice leads to $x^4 \equiv 17$; $x^8 \equiv 4 \pmod{19}$, hence $(x/19) \equiv \pm 1 \equiv x^9 \equiv 4x \pmod{19}$. Multiplying by 5 gives $x \equiv \pm 5 \pmod{19}$.

The reason that both signs produce solutions is that $(-1/19) = -1$, so one solution will be a quadratic residue, the other not.

However, in this case it is better to go one step further: $\pm x \equiv x^{10} \equiv 4x^2 \equiv 4 \cdot 6 \equiv 5 \pmod{19}$. That amounts to computing $n^{(p+1)/4}$, so we are really repeating the old method. □

E.IV.4 Example. Trying the same for $p \equiv 1 \pmod{4}$ will not work. Clearly odd powers produce one single linear term $kx \pmod{p}$, and even powers produce a constant. Since $d = (p-1)/2$ is even we will arrive at $x^d \equiv$ the only possible constant, 1 (by Euler's Criterion).

The trick now is to replace the given quadratic congruence by a different one, by substitution. To be explicit, let us try $x^2 \equiv 3 \pmod{13}$. Putting $x = y-1$ we replace the old congruence by $(y-1)^2 \equiv 3 \pmod{13}$, $y^2 \equiv 2y+2 \pmod{13}$. We then get

$$\begin{aligned} &y^3 \equiv 2y^2 + 2y \equiv 6y + 4 \pmod{13} \\ &y^6 \equiv (6y+4)^2 \equiv 10y^2 + 9y + 16 \equiv 29y + 36 \equiv 3y + 10 \pmod{13} \end{aligned}$$

By Euler's Criterion we arrive at

$$3y + 10 \equiv y^6 = y^{(13-1)/2} \equiv \left(\frac{y}{13}\right) \equiv \pm 1 \pmod{13}.$$

Multiplying by 9, the inverse to 3 modulo 13, we get: $y+12 \equiv \pm 9 \pmod{13}$; $y \equiv 5,\ 10 \pmod{13}$, whence $x \equiv y - 1 \equiv \pm 9 \pmod{13}$. □

E.IV.5 Example (The Algorithm, $\boldsymbol{P \equiv 1 \pmod 4}$). The substitution worked because there was a linear term in the left member. Why did we not get a constant?

Suppose the powering of y had produced a constant term only. As we only used the equation for the roots, not the roots themselves, that constant would be independent of the root.

I.e., we would have either $y^{(p-1)/2} \equiv 1$ or $y^{(p-1)/2} \equiv -1 \pmod{p}$, for both, i.e., both would be quadratic residues, or both would be non-residues. However, the constant term of the congruence $y^2 - 2y - 2 \equiv 0 \pmod{13}$, is their product, and as $(-2/13) = (2/13) = -1$, the two roots must be of opposite quadratic character!

These observations readily generalize. So now we can outline an algorithm, to solve $x^2 \equiv b \pmod{p}$, $(b/p) = 1$.

1) Find, by some random procedure, an m, such that $((m^2 - b)/p) = -1$. Introduce the new unknown $y = x + m$; $x = y - m$, turning the congruence into $y^2 \equiv 2my + (-m^2 + b) \equiv Ay + B \pmod{p}$.

2) Establish the doubling rule:

$$(Cy + D)^2 \equiv 2(C^2A + CD)y + (D^2 + C^2B) \pmod{p},$$

and the one-step rule,

$$(Cy + D)y \equiv Cy^2 + Dy \equiv (2AC + D)y + BC \pmod{p}.$$

Then, by the fast exponentiation scheme (see section L.V) derive the congruences

$$\pm 1 \equiv y^{(p-1)/2} \equiv Py + Q \pmod{p},$$

where $P \not\equiv 0 \pmod{p}$.

3) Solve the two linear congruences $Py + Q \equiv \pm 1 \pmod{p}$, and return $x = y - m$. Or solve one of them, and return $x = \pm(y - m)$. □

The fast exponentiation scheme is essential here; a naive linear search, by trial squaring all classes modulo p is far too slow.

Elwyn Berlekamp (1940-) is an American mathematician and information theorist. The above method was adapted from a general method of his for splitting polynomials mod p into factors of lower degree.

Another approach to modular square roots utilizes so-called Lucas sequences, and will be outlined in the last Chapter.

E.IV: Exercises

1. Suggestions for computing: Find square roots (or disprove their existence) of

(a) 17, 19, 31, 41 modulo the prime number

$$2\,78584\,90014\,12425\,44371\,60997$$

(b) 17,19,31,41 modulo the prime number

$$72\,07242\,88365\,15754\,88249\,70521$$

.

2. A more ambitious project would be to compute square roots modulo a composite number, using one of the algorithms of this section, along with Hensel refinement (B.VII.3) and the CRT. At least, then, solve $x^2 \equiv y \pmod{n}$ for $(y, n) = 1$. You might be content to do prime powers, e.g., solve $x^2 \equiv 17 \pmod{2^e}$ or $\pmod{43^e}$.

3. (a) Suppose we know square roots r_1, $r_2 \ldots, r_k$ of n modulo the (different) odd prime numbers p_1, $p_2 \ldots, p_k$. Denote their product by M and assume $(n, M) = 1$. Suppose further that we have determined the idempotents (see p. 41) for the set of moduli $p_1, p_2 \ldots, p_k$. Give expressions for the full set of solution classes of the congruence $x^2 \equiv n \pmod{M}$.

(b) A *Gray code* is an enumeration of all bitlists of length k where each possible list of 0's and 1's appears exactly once and each list differs in exactly one position from the previous one. E.g., $k = 2$: $[0, 0]$, $[1, 0]$, $[1, 1]$ $[0, 1]$.

One such Gray code can conveniently be described by indicating which position to change (from 0 to 1 or vice versa) in each step. Number the positions 0, 1, $\ldots, k-1$. Start with an all-zero list. In step n, $n = 1, 2, \ldots, 2^k - 1$, change the list in position $v_2(n)$, e.g., change the list in position 0 if n is odd. The example above was produced in that manner.

Show that this produces a Gray code. Hint: Look at the results for $k = 2, 3$, deduce a pattern, generalize and prove.

(c) Show how this Gray code (or rather the $v_2(n)$'s) can be used to organize the computation of modular square roots in the first part of this Exercise.

E.V Applications

E.V.1 Example (Electronic Coin Flipping). Here is a spectacular application of modular square roots, and the Chinese Remainder Theorem. It is due to Venezuelan computer scientist Manuel Blum (1938-).

Alice picks two large prime numbers, $p, q \equiv 3 \pmod 4$, and sends their product $n = pq$ to Bob. Bob chooses an integer x, $(x, n) = 1$, at random and sends its square s (reduced modulo n). So $s \equiv x^2 \pmod{pq}$.

Alice can rapidly determine the square roots $\pm z_1$, $\pm z_2$ of s modulo p and q, respectively, as suitable modular powers of s. Solving the Chinese congruence system

$$z \equiv \begin{cases} z_1 \pmod p \\ z_2 \pmod q \end{cases}$$

she finds the two pairs of roots $z \equiv x, n - x \pmod{pq}$ and $z = y, n - y \pmod{pq}$ satisfying $x \equiv y$ modulo one of the primes and $x \equiv -y$ modulo the other. She is asked to choose one root – that is the flip – and communicates her choice to Bob.

If she chooses x or $n-x$ Bob declares her the winner. Otherwise he proclaims himself to be the winner.

He can justify this claim, as $x \pm y \equiv 0$ modulo p or q, and $x \pm y \equiv 2x \neq 0$ modulo the other prime. This means that $(x \pm y, pq)$ equals one of the two primes, i.e., knowing both x and one of y and $n - y$, he can factor n.

The book by Trappe-Washington has a hilarious discussion on electronic poker. □

We turn to yet another application of modular square roots, due to M.Blum, L. Blum, and M.Shub. It is a cryptologic scheme, secure, but not very fast. It is suited for sending short messages, e.g., for key exchange.

We precede the discussion with a little Lemma.

E.V.2 Lemma. *Let $N = pq$, where p, q are prime numbers, both congruent to 3 modulo 4. Let x be a quadratic residue modulo N. Then, out of the four solution classes to $y^2 \equiv x \pmod N$, exactly one is a quadratic residue modulo N.*

Proof. Modulo p, q we have the solutions $y \equiv \pm a \pmod{p}$, and $y \equiv \pm b \pmod{q}$. Now $(-1/p) = (-1/q) = -1$ so in both cases exactly one of the two signs gives a quadratic residue. Choosing the right sign in both cases, and using the Chinese Remainder Theorem to find $y \pmod{N}$, proves the result. □

E.V.3 Example. Now to the application. Bob wants to send a message of k bits $m_1, m_2, \ldots, m_k$ to Alice. Alice chooses two large prime numbers $p, q \equiv 3 \pmod{4}$, and publishes their product N. Bob chooses a *seed* x_0, a quadratic residue modulo N, at random, then computes

$$x_1 \equiv x_0^2 \pmod{N},\ x_2 \equiv x_1^2 \pmod{N},\ \ldots,\ x_{k+1} \equiv x_k^2 \pmod{N}$$

(all reduced to least positive residues modulo N). He encrypts each m_j by adding x_j modulo 2, $n_j \equiv x_j + m_j \pmod{2}$. The operation involves only the lowest bit b_j of x_j.

(In practice, the bit strings may be represented as binary words; the modular addition is then a bit-wise exclusive-or.)

Bob sends the string of n_j, along with x_{k+1}, to Alice.

Alice, knowing the factorization $N = pq$, easily finds the square roots of x_{k+1} modulo p, q. We have seen that this is particularly easy for prime moduli $\equiv 3 \pmod{4}$. And in fact a power of a quadratic residue is automatically also a quadratic residue.

She then chooses in either case the one that is a quadratic residue modulo p or q. She combines the two to find $x_k \pmod{N}$ by the Chinese Remainder Theorem.

The process is repeated until she has found all the $x_j, j = 1, 2, \ldots, k$. Exclusive-oring recovers the plaintext bits, as $m_j \equiv n_j + b_j \pmod{2}$. □

E.V: Exercises

1. Refer to the last Example above. Let $\pi(x_0)$ denote the period of the sequence $x_0, x_1, \ldots$. Show that
$$\pi(x_0) | \lambda(\lambda(N)),$$
or better even $\pi(x_0) | \lambda(\mathrm{ord}_N(x_0))$, where λ is the Carmichael function (C.V.3). An essential observation is that the order of all quadratic residues modulo N must be odd. Hint: If $v_2(\mathrm{ord}_N(x)) = k > 0$, then $v_2(\mathrm{ord}_N(x^2)) = k - 1$ (prove).

Chapter F

Multiplicative Functions

F.I Definitions and Examples

This Chapter does not belong to the main thread of this text and can be skipped. Our main motive for including it is that it gives a different perspective on the Phi function, (A.V.1), and a new proof of the existence of primitive roots modulo a prime number (C.II.1).

F.I.1 Definition. An **arithmetic function** is a function from the positive integers to $\mathbf{R}$ or $\mathbf{C}$.

The most important examples are the multiplicative ones:

F.I.2 Definition. The arithmetic function is **multiplicative** if

$$(m,n) = 1 \Longrightarrow f(mn) = f(m)f(n)$$

(forcing $f(1) = 1$ if $f \not\equiv 0$).

Clearly a multiplicative function is fully determined by its values for prime powers p^k, $k > 0$.

Here are a few examples. The first three are used in constructing further examples.

F.I.3 Example.

a) ι given by $\iota(1) = 1;\ ,\iota(n) = 0$ for $n > 1$.

b) The *identity function* I, $I(n) = n, n \geq 1$.

c) The *constant function* $[1] : [1](n) = 1, n \geq 1$.

d) The *maximal square-free factor* of n, i.e., the product of all distinct prime factors of n. E.g., for $n = 180 = 2^2 \cdot 3^2 \cdot 5$ it is $2 \cdot 3 \cdot 5 = 30$.

e) $f(n) = 2^N$ where N is the number of prime divisors of N. □

We did not include the already familiar Phi function in this list – we will later prove its multiplicativity, using some of the general principles to be developed in this Chapter.

F.I: Exercises

1. n is a positive integer. $s(n) = t_1(n) - t_3(n)$ where $t_1(n), t_3(n)$ denote the number of divisors of n congruent to 1, or 3, respectively, modulo 4. Show that $s(n)$ is a multiplicative function. Using this, express $s(n)$ in the multiplicities of those prime factors in n that are congruent to 1 or 3 modulo 4.

F.II The Dirichlet Product

F.II.1 Definition. Let f, g be arithmetic functions. Their **Dirichlet product** (or, **multiplicative convolution**) is defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}) = \sum_{d|n} g(d)f(\frac{n}{d}) = \sum_{de=n} f(d)g(e).$$

The sums extend over all positive divisors of n.

The middle members illustrate that the Dirichlet product is *commutative*, $f * g = g * f$.

It is also *associative*, in fact:

$$\big(f * (g * h)\big)(n) = \big((f * g) * h\big)(n) = \sum_{ijk=n} f(i)g(j)h(k),$$

a triple sum.

There is an identity for this product, namely $\iota, \iota(1) = 1, \iota(n) = 0, n > 1$. "Identity" means that $\iota * g = g$, check this. If $f * g = \iota$, then we say, of course, that f and g are (Dirichlet) *inverses* of one another.

An important special case of a Dirichlet product is the *summatory function* of an arithmetic function:

F.II.2 Definition. The **summatory** function F of the arithmetic function f is defined as the Dirichlet product of f and the constant function $[1]$, that is, $F = f * [1]$. Concretely,

$$F(n) = \sum_{d|n} f(d) \cdot 1 = \sum_{d|n} f(d).$$

If f is multiplicative, then so is F. This will follow presently from a more general result. We first give an important example.

F.II.3 Theorem. *The summatory function of the Euler Phi function is the identity function I, i.e.,*

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(n/d) = n.$$

Proof. The first equality comes from the fact that an arbitrary divisor of n may also be written in the form n/d.

For the second, let $1 \leq m \leq n$, $(m,n) = d$. Then $(m/d, n/d) = 1$ and $1 \leq m/d \leq n/d$.

This sets up a bijection between those m, $1 \leq m \leq n-1$, for which $(m,n) = d$, and the invertible classes modulo n/d. i.e., their number is $\phi(n/d)$.

Further, the only m, $1 \leq m \leq n$, with $(m,n) = n$, is $m = n$, and $\phi(n/n) = \phi(1)$ by definition.

Summing over all possible d we get the result. □

F.II.4 Example. Let us exemplify the proof for $n = 15$, where $d = 1, 3, 5, 15$.

The numbers $m, 1 \leq m \leq 15$, with $(m,n) = 1$ are those divisible by neither 3 nor 5: $m = 1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14$. Their number is $\phi(15) = 8$.

The numbers $m, 1 \leq m \leq 15$, with $(m,n) = 5$ are $m = 1 \cdot 5,\ 2 \cdot 5$ with $m/5 = 1, 2$, corresponding to the $2 = \phi(3)$ invertible classes modulo 3.

The numbers $m, 1 \leq m \leq 15$, with $(m,n) = 3$, are $m = 1{\cdot}3,\ 2{\cdot}3,\ 3{\cdot}3,\ 4{\cdot}3$ with $m/3 = 1,\ 2,\ 3,\ 4$, corresponding to the $4 = \phi(5)$ invertible classes modulo 5.

Finally, the only m with $(m,n) = 15$ is $m = 15$, $m/15 = 1$, and by definition $\phi(1) = 1$. □

The main result of this Section is that the Dirichlet product of two multiplicative functions is itself multiplicative. We precede the result with a divisibility Lemma:

F.II.5 Lemma. *Let $n = n_1 n_2$ where $n_1, n_2 > 1$ and $(n_1, n_2) = 1$. Any divisor $d|n, d > 0$ can be written in unique fashion as a product $d_1 \cdot d_2$, where $d_1, d_2 > 0$, $d_i|n_i$, $i = 1, 2$.*

Proof. It is easy to give a proof using unique prime factorization. However, in order not to forget the foundations of our divisibility theory we give a more fundamental proof.

We first deal with uniqueness. Suppose $d_1 d_2 = e_1 e_2$, with $e_1, e_2 > 0, e_i|n_i$. Then $d_1|e_1 e_2$, $(d_1, e_2)|(n_1, n_2) = 1$, hence $d_1|e_1$ by the First Divisibility Theorem. In like manner $d_2|e_2$. As $d_1 d_2 = e_1 e_2$, the two divisibility relations must be equalities.

Next we deal with existence. Let $d_1 = (d, n_1)|n_1$. As $(d/d_1, n/d_1) = 1$, the relation

$$\frac{d}{d_1}|\frac{n_1}{d_1} \cdot n_2$$

yields that $d_2 = d/d_1$ divides n_2, whence the result. □

F.II.6 Theorem. *The Dirichlet product $f * g$ of two multiplicative functions f, g is itself multiplicative. In particular, the summatory function F of f is multiplicative.*

Proof. Given $n = n_1 n_2, n_1, n_2 > 0, (n_1, n_2) = 1$, we want to prove that $(f * g)(n) = (f * g)(n_1)(f * g)(n_2)$ so we have a closer look at the sum

$$\sum_{d|n} f(\frac{n}{d})g(d).$$

Writing $d = d_1 d_2$ as in the Lemma above, we get a double sum:

$$\sum_{d_1|f_1} \sum_{d_2|n_2} f(\frac{n_1}{d_1} \cdot \frac{n_2}{d_2})g(d_1 d_2).$$

We are assuming that f, g are multiplicative, so that

$$f(\frac{n_1}{d_1} \cdot \frac{n_2}{d_2}) = f(\frac{n_1}{d_1})f(\frac{n_2}{d_2}),$$

and

$$g(d_1d_2) = g(d_1)g(d_2).$$

By this token the double sum reduces to the product of the two simple sums:

$$\sum_{d_1|n_1} f(\frac{n_1}{d_1})g(d_1) = (f * g)(n_1),$$

and

$$\sum_{d_2|n_2} f(\frac{n_2}{d_2})g(d_2) = (f * g)(n_2),$$

proving that

$$(f * g)(n) = \sum_{d|n} f(\frac{n}{d})g(d) = (f * g)(n_1)(f * g)(n_2).$$

F.III Möbius Inversion

We now wish to find the inverse of the constant function [1], if it exists. It will be denoted by μ.

Let us try low prime powers:

$$([1] * \mu)(1) = 1 \cdot \mu(1) = 1,$$

whence $\mu(1) = 1$; then

$$([1] * \mu)(p) = 1 \cdot \mu(p) + 1 \cdot \mu(1) = 0,$$

whence $\mu(p) = -1$; and then

$$([1] * \mu)(p^2) = 1 \cdot \mu(1) + 1 \cdot \mu(p) + 1 \cdot \mu(p^2) = 0,$$

so that $\mu(p^2) = 0$.

From this a pattern emerges. We must have, for any prime p: $\mu(p) = -1$, $\mu(p^k) = 0, k > 1$.

If μ is to be multiplicative (as we hope) we are led to the following definition:

F.III.1 Definition. The **Möbius Mu Function** $\mu : \mathbf{Z}_+ \to \mathbf{Z}$ is defined by $\mu(1) = 1$,

$$\mu(n) = \mu(p_1 p_2 \cdots p_k) = (-1)^k,$$

if n is the product of distinct (simple) prime factors p_i, and

$$\mu(n) = 0$$

otherwise.

It is obvious that μ is multiplicative. We can now state and prove the desired result:

F.III.2 Theorem. *The functions μ and $[1]$ are Dirichlet inverses of one another.*

Proof. Obviously $([1] * \mu)(1) = 1$. Also, it is easy to see that

$$([1] * \mu)(p^k) = 1 \cdot \mu(p) + 1 \cdot \mu(1) = -1 + 1 = 0$$

all other terms of the sum defining the Dirichlet product being zero.

The identity

$$([1] * \mu)(n) = \iota(n), \quad \forall n \in \mathbf{Z}_+$$

now follows because both members are multiplicative and agree on prime powers. □

We now arrive at the fundamental Möbius Inversion Formula.

F.III.3 Theorem (Möbius Inversion). *If f is an arithmetic function, and*

$$F(n) = ([1] * f)(n) = \sum_{d|n} f(d),$$

then

$$f(n) = (\mu * F)(n) = \sum_{d|n} \mu(\frac{n}{d}) F(d).$$

Proof.

$$f = \iota * f = (\mu * [1]) * f = \mu * ([1] * f) = \mu * F.$$

□

We note the following Corollary

F.III.4 Corollary.

$$\phi(n) = \sum_{d|n} \mu(\frac{n}{d}) d = (\mu * I)(n).$$

Proof. This is an immediate consequence of the above Theorem and the identity (F.II.3)

$$\sum_{d|n} \phi(d) = n.$$

□

F.III.5 Corollary. *The Euler Phi function is multiplicative.*

Proof. It is the Dirichlet product of two multiplicative functions. □

F.III.6 Example.

$$\begin{aligned} \phi(6) &= \mu(1) \cdot 6 + \mu(2) \cdot 3 + \mu(3) \cdot 2 + \mu(6) \cdot 1 \\ &= 6 - 3 - 2 + 1 = 2. \end{aligned}$$

□

The reader should compare the following Example with the same Example in the CRT Section, B.II.3.

F.III.7 Example.

$$\begin{aligned} \phi(105) =& \mu(1) \cdot 105 + \mu(3) \cdot 5 \cdot 7 + \mu(5) \cdot 3 \cdot 7 + \mu(7) \cdot 3 \cdot 5 \\ & + \mu(5 \cdot 7) \cdot 3 + \mu(3 \cdot 7) \cdot 3 + \mu(3 \cdot 5) \cdot 7 + \mu(3 \cdot 5 \cdot 7) \cdot 1 \\ =& 105 - 35 - 21 - 15 + 3 + 5 + 7 - 1 = 48. \end{aligned}$$

□

* F.IV Two More Results

For the sake of completeness we prove a few additional results on Dirichlet inverses.

F.IV.1 Theorem. *Let f be an arithmetic function. A Dirichlet inverse g exists if and only if $f(1) \neq 0$. It is then unique, and given by the following recurrence:*

$$g(n)f(1) = -\sum_{d|n, d<n} g(d)f(\frac{n}{d}). \tag{$*$}$$

Proof. The condition $f(1) \neq 0$ is necessary as we must have $g(1)f(1) = \iota(1) = 1$.

We set $g(1) = 1/f(1)$ and assume, by way of induction, that $g(k)$ has been defined for all proper divisors k, $k|n$, $1 \leq k < n$. Equation (*) then shows how to define $g(n)$. As equation (*) expresses the condition $\iota(n) = 0$, $n > 1$, g is uniquely determined by that condition, and $g(1)f(1) = 1$, and is the Dirichlet inverse of f. □

F.IV.2 Theorem. *The Dirichlet inverse of a multiplicative function is itself multiplicative.*

Proof. Suppose $g*f = \iota$, where f is multiplicative. Let $n = n_1n_2$, $(n_1, n_2) = 1$, $n_1, n_2 > 1$. By induction on n (the case where at least one $n_i = 1$ is obvious) we may assume that $g(d_1d_2) = g(d_1)g(d_2)$ for $d_i|n_i$, $d_i < n_i$, $i = 1, 2$.

Then

$$\sum_{d|n} g(d)f(\frac{n}{d}) = 0,$$

as $n > 1$, so that

$$\begin{aligned} g(n) = g(n)f(1) &= -\sum_{d|n, d<n} g(d)f(\frac{n}{d}) = \\ &= -\sum_{d_1|n_1, d_2|n_2,} \sum_{d_1 d_2 < n} g(d_1)g(d_2)f(\frac{n_1}{d_1})f(\frac{n_2}{d_2}) \\ &= -(\sum_{d_1|n_1} g(d_1)f(\frac{n_1}{d_1}))(\sum_{d_2|n_2} g(d_2)f(\frac{n_2}{d_2})) + g(n_1)g(n_2)f(1)f(1) \\ &= g(n_1)g(n_2). \end{aligned}$$

□

F.IV: Exercises

1. n is a positive integer. Let $\sum'_{1\le k<n}$ denote summation over those k for which $(k,n)=1$. Show that

$$\sum_{1\le k<n}{}' k = \frac{1}{2} n \cdot \phi(n).$$

2. ϕ is the Euler phi-function, m, n are positive integers, and $d = (m,n)$ their greatest common divisor.

Prove:

$$\frac{\phi(mn)}{\phi(m)\phi(n)} = \frac{d}{\phi(d)}.$$

In particular, show that $\phi(mn) = \phi(m)\phi(n)$ if and *only if* $(m,n) = 1$.

3. Determine the sums

(a)

$$\sum_{d|n} \mu(d)d,$$

(b)

$$\sum_{d|n} \mu(d)\phi(d).$$

The answers may be expressed in the Euler function and the prime factors of the given integer. Start with prime powers.

(c) Show that sum $s(n)$ in a) is the Dirichlet inverse of the Euler function $\phi(n)$. First prove that it is multiplicative, which means that the Dirichlet product need be computed only for prime powers.

4. The sum
$$\sum_{d|n} |\mu(d)|$$
is a power of two. Describe the exponent.

5. n is a positive integer. Let $B(x)$ be the number of m, $1 \leq m \leq x$ for which $(m, n) = 1$. $B(n)$ is of course $\phi(n)$ for which you know an expression, as a sum. How should that expression be modified in order to hold for arbitrary x? Hint: study a few simple examples, then reflect on the true meaning of the expression for $\phi(n)$.

6. Suppose the function f is defined for all positive real (or at least rational) numbers, and let
$$g(x) = \sum_{1 \leq k \leq x} f(\frac{x}{k}).$$
Prove that
$$f(x) = \sum_{1 \leq k \leq x} g(\frac{x}{k})\mu(k).$$
Also prove the converse. Hint: Arrange a certain double sum in a way that exploits the basic properties of the μ function.

7. An arithmetic function f is called *completely multiplicative* if $f(mn) = f(m)f(n)$ for all pairs of positive integers m, n.

(a) Give examples.

(b) Can you give an example of two completely multiplicative functions the Dirichlet product of which is not completely multiplicative?

(c) Show that a multiplicative function f is completely multiplicative if and only if $f(p^k) = f(p)^k$ for all prime numbers p.

(d) Show that a multiplicative function $f, \neq 0$, is completely multiplicative if and only if its Dirichlet inverse is give by $f^{-1}(n) = \mu(n)f(n)$ for all positive integers n.

8. Let f be an arithmetic function. Prove the relation
$$\sum_1^{n} {}' f(k) = \sum_{d|n} \big(\mu(d) \sum_{1 \leq k \leq n/d} f(kd)\big),$$
where the prime indicates summation over those k for which $(k, d) = 1$. For instance, start by collecting all terms, of the right member, belonging to one single value of the product kd.

9. (a) Suppose, for a fixed positive integer k, that the relation

$$T(n) = \sum_{d|n} d^k S(\frac{n}{d}))$$

holds for the two arithmetic functions S, T. Express $S(n)$ in $T(d)$, $d|n$. In particular, find the Dirichlet inverses of the functions $f(n) = n^k$.

(b) n is an odd integer ≥ 3. We wish to determine the sum

$$S(n) = \sum_{1 \leq k \leq \frac{1}{2}(n-1)}{}' k,$$

(summing over k, $(k,n) = 1$). Show first that

$$\sum_{d|n} d \cdot S(\frac{n}{d}) = \sum_{1 \leq k \leq \frac{1}{2}(n-1)} k,$$

an arithmetic sum. Solve this relation for $S(n)$, using a).

10. Using the ideas of the previous problem, find the sum

$$S(n) = \sum_{1 \leq k \leq n-1}{}' k^2,$$

(summing over k, $(k,n) = 1$), using

$$\sum_{k=1}^{n-1} k^2 = \frac{1}{6} n(n-1)(2n-1).$$

F.V Primitive Roots, Again

F.V.1 Example. As an application of the Euler function we prove again the existence of a primitive root modulo p, Theorem C.II.1, where p is a prime number. That is, we prove again the existence of an element g of order $\phi(p) = p - 1$ modulo p. We assume $p > 2$.

The invertible classes modulo p are the non-zero ones. By Little Fermat they are the roots of the polynomial $X^{p-1} - 1$. The possible orders d of any invertible class are divisors of $p - 1$, $p - 1 = de$. For such d the polynomial $X^d - 1$ divides $X^{p-1} - 1$, by the familiar identity:

$$X^{de} - 1 = (X^d - 1)(X^{(e-1)d} + X^{(e-2)d} + \cdots + 1) = (X^d - 1)q(X).$$

We claim that for each d, $d|(p - 1)$, the polynomial $X^d - 1$ has exactly d roots modulo p.

The reason is that there are no zero-divisors modulo p; if $(a^d - 1)q(a) \equiv 0 \pmod{p}$ one of the factors must be congruent to zero modulo p. As the number of solutions modulo p is de and the two factors have at most d and $(d - 1)e$ solution classes they must have exactly d and $d(e - 1)$ respectively.

We now let $\psi(c)$ denote the number of elements of (exact) multiplicative order c modulo p. (If c does not divide $p - 1$, then $\psi(c) = 0$). If c divides d, and d divides $p - 1$, then any element of order c is a root of $X^d - 1$, whence

$$\sum_{c|d} \psi(c) = d = \sum_{c|d} \phi(c).$$

The Möbius Inversion Formula (F.III.3) then yields, for $d|(p - 1)$,

$$\psi(d) = \sum_{c|d} \mu(c)(\frac{d}{c}) = \phi(d).$$

In particular,

$$\psi(p - 1) = \phi(p - 1) > 0,$$

which establishes the existence of elements of order $p - 1$. In fact, we even established, without extra effort, their exact number. □

F.V: Exercises

1. If you try to transfer the argument above to the question of primitive roots modulo p^2 – where there are zero-divisors – you cannot reason exactly as above. Can you resolve the difficulty?

F.VI A Combinatorial Application

We now give a combinatorial application of the Phi and Möbius functions.

Suppose we want to make a necklace with n beads, in a colors. They are flat on the side to be worn against the body.

The number of colorings is obviously a^n. However, arranging the beads symmetrically at the vertices of a regular polyhedron it is natural to regard two colorings as equivalent if one can be brought into the other by rotating the polyhedron.

Lumping equivalent colorings together into classes results in a partition of the a^n colorings. We wish to determine the number of equivalence classes.

For instance, if the colors are R, G, and the number of beads is six we identify the two colorings

$$\begin{array}{cccc} & \mathrm{R} & \mathrm{G} & \\ \mathrm{G} & & & \mathrm{R} \\ & \mathrm{R} & \mathrm{G} & \end{array} \qquad \begin{array}{cccc} & \mathrm{G} & \mathrm{R} & \\ \mathrm{R} & & & \mathrm{G} \\ & \mathrm{G} & \mathrm{R} & \end{array}$$

by a $\pi/6$ rotation and the colorings

$$\begin{array}{cccc} & \mathrm{R} & \mathrm{R} & \\ \mathrm{G} & & & \mathrm{R} \\ & \mathrm{G} & \mathrm{G} & \end{array} \qquad \begin{array}{cccc} & \mathrm{G} & \mathrm{G} & \\ \mathrm{R} & & & \mathrm{G} \\ & \mathrm{R} & \mathrm{R} & \end{array}$$

by a half-turn.

There are n rotations of the polyhedron. They can be written

$$\text{id}\ , r, r^2, \ldots, r^{n-1}, (r^n = \text{ id }),$$

where r is the counterclockwise rotation $2\pi/n$. Each coloring is brought into itself by applying the rotation r n times. There is a least positive number $0 < d \leq n$ having the property that r^d rotates a coloring into itself. In the examples above, $d = 2$ and 6. For

$$\begin{array}{cccc} & \mathrm{R} & \mathrm{R} & \\ \mathrm{G} & & & \mathrm{G} \\ & \mathrm{R} & \mathrm{R} & \end{array}$$

it is 3.

The number d divides n. For if $n = qd + t$, $0 \leq t < d$, $r^t = r^n \cdot r^{d-q}$ has the same property as r^d, hence, by minimality, $t = 0$.

We call the number d thus defined the *order* of the coloring. We now determine the number $f(d)$ of colorings having order d. $f(m) = 0$ if $m \nmid n$, of course.

As each of the a^n colorings is of *some* order we have

$$\sum_{d|n} f(d) = a^n.$$

The Möbius Inversion Formula then immediately gives

$$f(d) = \sum_{k|d} \mu(\frac{d}{k}) a^k.$$

Now let $F(n)$ denote the number of classes of equivalent colorings. Take one coloring from each class. Performing the n rotations on each of them gives us $nF(n)$ colorings.

Here each of the $f(d)$ colorings of order d, $d|n$ will appear n/d times, rotated by id, r^d, r^{2d}, $\ldots r^{n-d}$. So:

$$\begin{aligned} nF(n) &= \sum_{d|n} f(d) \cdot \frac{n}{d} = \\ &= \sum_{k|d} \sum_{d|n} a^k \mu(\frac{d}{k}) \frac{n/k}{d/k}. \end{aligned}$$

The double summation extends over all pairs k, d satisfying $k \mid d \mid n$.

We fix k, and sum the factor after a^k over d. Setting $d' = d/k$, $n' = n/k$, we obtain

$$\sum_{d:k|d|n} \mu(\frac{d}{k}) \frac{n/k}{d/k} = \sum_{d'|n'} \mu(d') \frac{n'}{d'} = \phi(n') = \phi(\frac{n}{k}),$$

that is,

$$nF(n) = \sum_{k|n} a^k \phi(\frac{n}{k}) = \sum_{k|n} a^{n/k} \phi(k).$$

The reader is invited to exemplify this formula.

The reader who has taken a course in Abstract Algebra may recognize this as an instance of Burnside's Counting Theorem. $\phi(k)$ is the number of rotations of order k, and $a^{n/k}$ is the number of colorings fixed by each of these.

For $n = p$, a prime number, we arrive at a new proof of Little Fermat (A.V.9), as the sum in the right member (two terms!) must be divisible by p. This same formula can then be used recursively to prove Euler's Theorem (A.V.12) for prime powers. And using the multiplicativity of the Phi function one can prove it for any modulus. See the exercises.

F.VI: Exercises

1. Use the necklace Example to prove Little Fermat and Euler's Theorem, as indicated above.

F.VII The Sum of Divisors

We give one final example of a multiplicative function, and show the classical result characterizing *even perfect numbers*.

F.VII.1 Definition. For positive integers n, the **sum of divisors function**, $\sigma(n)$, is defined as the sum

$$\sigma(n) = \sum_{d|n} d$$

of all positive divisors of n.

The following result is almost trivial:

F.VII.2 Lemma. *For $n > 1$,*

$$\sigma(n) \geq n + 1,$$

equality holding if and only if n is a prime number.

□

F.VII.3 Theorem. *σ is a multiplicative function.*

Proof. It is the summatory function of the identity function, $I(n) = n$. □

As with most multiplicative functions one wants to know its value for prime powers.

F.VII.4 Lemma. *Let p be a prime number, e a positive exponent. Then*

$$\sigma(p^e) = \frac{p^{e+1}-1}{p-1}.$$

Proof. It is a geometric sum:

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1}-1}{p-1}.$$

□

The expression for $p = 2$ is particularly simple: $\sigma(2^e) = 2^{e+1} - 1$.

Now for the main result of this Section:

F.VII.5 Definition. The positive integer n is **perfect** if $\sigma(n) = 2n$, i.e., if n equals the sum of its divisors $< n$.

No odd perfect numbers are known, but it is known that they must have many prime factors and be very large.

Here is the result characterizing the even ones. Prime numbers of the form $2^s - 1$ (forcing s to be prime, as shown in the last Chapter) are called *Mersenne primes.*

F.VII.6 Theorem. *The even number n is perfect if and only if it is of the form*

$$n = 2^{s-1}(2^s - 1), \quad s \geq 2,$$

where the second factor is a Mersenne prime.

Proof. If n is of the given form, then, by multiplicativity, and the Lemmas above, $\sigma(n) = \sigma(2^{s-1})\sigma(2^s - 1) = (2^s - 1)2^s = 2n$.

For the converse assume n even, and $\sigma(n) = 2n$. Writing $n = 2^{s-1}t$, $s \geq 2, t$ odd, the assumption is:

$$2^s t = 2n = \sigma(n) = \sigma(2^{s-1})\sigma(t) = (2^s - 1)\sigma(t).$$

As $(2^s, 2^s - 1) = 1$ it follows that $2^s | \sigma(t)$, hence (reading from the opposite direction), $(2^s - 1)|t$. We spell this out:

$$\begin{aligned} t &= (2^s - 1)u, \\ \sigma(t) &= 2^s \cdot u. \end{aligned}$$

We now see that $\sigma(t) = t + u$, which means that t has only these two divisors. Hence $u = 1$, and $t = 2^s - 1$ is a prime, and n has the form asserted. □

In December 2008, 46 Mersenne primes had been discovered, so 46 perfect numbers are known. Among the smallest ones is $2^4 \cdot (2^5 - 1) = 16 \cdot 31 = 496$. The sum of divisors < 496 is $(1 + 2 + 4 + 8 + 16) + (1 + 2 + 4 + 8) \cdot 31 = 31 + 15 \cdot 31 = 16 \cdot 31$.

F.VII: Exercises

1. Show that $2^s - 1$ prime forces s prime. Or, more generally, for integers $a > 1$, that $(a^s - 1)/(a - 1)$ prime forces s prime.

F.VIII Cyclotomic Polynomials

As another application of the Möbius function we determine the so-called *cyclotomic* polynomials $\Phi_n(X)$.

Recall (F.III.1) that μ is the Dirichlet inverse of the constant function [1]: $(\mu * [1])(n) = 1$ for $n = 1$, 0 otherwise. In plaintext:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1, \\ 0 \text{ if } n > 1. \end{cases}$$

Now consider the polynomial $F_n(X) = X^n - 1$. Its complex roots are the powers ϵ^k, $k = 0, 1, 2, \ldots n-1$, where $\epsilon = \exp(2\pi i/n)$. Each root α has a true order d, the least positive exponent for which $\alpha^d = 1$, i.e., for which α is a root of $F_d(X) = X^d - 1$.

F.VIII.1 Definition. The root α is **primitive for** $F_n(X) = X^n - 1$, or a **primitive** n**-th root (of unity)**, if its order equals n.

The following result is proved exactly as for orders of invertible residue classes modulo n (A.V.5).

F.VIII.2 Lemma.

a) $\epsilon = \exp(2\pi i/n)$ *is primitive for* F_n.

b) The order of any root of $F_n(X)$ *divides* n.

c) The order of ϵ^k *equals* $n/(k, n)$.

d) ϵ^k *is a primitive* n*-th root if and only if* $(k, n) = 1$.

□

We can now define our object of study:

F.VIII.3 Definition. The n-th **cyclotomic** polynomial $\Phi_n(X)$ is the product $\prod(X-\alpha)$ extended over all the primitive n-th roots α.

The word "cyclotomic" comes from the Greek, meaning "circle-dividing". Clearly, the degree of $\Phi_n(X)$ is $\phi(n)$. Furthermore:

F.VIII.4 Lemma.

$$F_n(X) = \prod_{d|n} \Phi_d(X).$$

Proof. The roots of $F_n(X)$ are by construction the complex numbers of order dividing n. □

F.VIII.5 Example.

a) For a prime number p, all k, $1 \leq k \leq p-1$, are relatively prime to p. Hence all roots to $F_p(X)$, except $X = 1$, are primitive, i.e.,

$$\Phi_n(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1.$$

b)

$$\Phi_8(X) = \frac{F_8(X)}{F_4(X)} = \frac{X^8 - 1}{X^4 - 1} = X^4 + 1.$$

If the order of an 8-th root is not 8, it divides 4, hence belongs to $X^4 - 1$.

c)

$$\Phi_6(X) = \frac{(X^6-1)(X-1)}{(X^3-1)(X^2-1)} = \frac{X^3+1}{X+1} = X^2 - X + 1.$$

We start with all 6 roots of $X^6 - 1$. We then exclude the roots of order 2, and 3. But then we exclude the root 1 twice, so we put it back again. □

Now we can prove our main Theorem:

F.VIII.6 Theorem.

$$\Phi_n(X) = \prod_{k|n} F_k(X)^{\mu(n/k)}.$$

Proof. Induction over the number of prime factors. The case $n = 1$ (zero prime factors) is obvious. We have already seen that

$$\Phi_p(X) = F_p(X)^{+1} \cdot F_1(X)^{-1} = F_p(X)^{\mu(p/p)} \cdot F_1(X)^{\mu(p/1)}$$

for a prime number p. That takes care of the case of one prime factor.

Now assume the Theorem proven for d with fewer than k prime factors, and let n have $k + 1$ prime factors. Consider the identity

$$F_n(X) = \Phi_n(X) \cdot {\prod_{d|n}}' \Phi_d(X),$$

where the prime denotes the omission of the index n. We may assume, by induction, that the Theorem holds for the factors after the product sign:

$$\Phi_d(X) = \prod_{k|d} F_k(X)^{\mu(d/k)}, \quad d|n, d < n.$$

Collect the contributions to one single factor F_k, $k|n$, $k < n$ (so that the induction hypothesis applies). The resulting exponent is:

$$-\mu(\frac{n}{k}) + \sum_{d:k|d|n} \mu(\frac{d}{k}).$$

Note that k, n are fixed; the sum extends over those $d|n$ that are divisible by k.

Writing $d' = d/k, n' = n/k$ this can be rewritten as

$$\sum_{d'|n'} \mu(d') - \mu(\frac{n}{k}).$$

As $n > k$, $n' > 1$, the first sum is 0, and we are left with the single term $-\mu(n/k)$. Therefore

$$F_n(X) = \Phi_n(X) \cdot {\prod_{k|n}}' F_k(X)^{-\mu(n/k)}.$$

As $\mu(n/n) = 1$ the result follows on multiplication of both members by

$$\prod_{k|n}{}' F_k(X)^{\mu(n/k)}.$$

□

We finally note:

F.VIII.7 Theorem. $\Phi_n(X)$ *is a polynomial with rational integer coefficients and leading coefficient 1.*

Proof. In the last Theorem some F_k enter with exponent 1, others with exponent -1. The Theorem therefore represents $\Phi_n(X)$ as the quotient of two integer polynomials. As the denominator has leading coefficient one, the quotient has integer coefficients. Already the defintion of $\Phi_n(X)$ shows that its leading coefficient equals one. □

F.VIII.8 Example. Two further examples:

a) $n = 12$, $\mu(12/2) = \mu(2 \cdot 3) = 1; \mu(12/6) = \mu(12/4) = -1$.

$$\begin{aligned}\Phi_{12}(X) &= \frac{(X^{12}-1)(X^2-1)}{(X^6-1)(X^4-1)} \\ &= \frac{X^6+1}{X^2+1} = X^4 - X^2 + 1.\end{aligned}$$

b) $n = 30 = 2 \cdot 3 \cdot 5$. Here $\mu(30/2) = \mu(30/3) = \mu(30/5) = 1$, $\mu(30/6) = \mu(30/10) = \mu(30/15) = -1$.

Using the rule $a^2 - b^2 = (a-b)(a+b)$ and $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$ we get:

$$\begin{aligned}\Phi_{30}(X) &= \frac{(X^{30}-1)(X^2-1)(X^3-1)(X^5-1)}{(X^{15}-1)(X-1)(X^6-1)(X^{10}-1)} \\ &= \frac{(X^{15}+1)(X+1)}{(X^3+1)(X^5+1)} = \frac{X^{10}-X^5+1}{X^2-X+1} \\ &= X^8 + X^7 - X^5 - X^4 - X^3 + X + 1.\end{aligned}$$

□

Remark 1: $\Phi_2(X) = X + 1$. For $n \geq 3$, $f = \phi(n)$ is even. For these n, -1 is not a root of $\Phi_n(X)$. The roots come in inverse pairs: ϵ^k, ϵ^{p-k}, so their product equals 1. As the degree of $\Phi_n(X)$ is even, its constant term equals one.

The *reciprocal* polynomial, $X^f \Phi_n(1/X)$, has the same roots as $\Phi_n(X)$. Its coefficients are the same as those of $\Phi_n(X)$, in reverse order, so its leading coefficient equals 1. As the two polynomials have the same roots and the same leading coefficients, they must be equal. $\Phi_n(X)$ is *self-reciprocal*, or *palindromic.*

Remark 2: The perceptive reader will no doubt have noticed that we more or less derived a general multiplicative Möbius inversion formula, replacing sums by products, and factors by exponents.

An Application Of Cyclotomic Polynomials

Cyclotomic polynomials arise in many ways in the context of factoring. One instance is numbers of the special form $a^n - b^n$. Those factors that do not divide factors of the form $a^d - b^d$, $d|n$, will divide a homogenized expression related to $\Phi_n(x)$, $b^f \Phi_n(a/b)$. Riesel's book has a wealth of remarkable formulas related to this issue.

Looking closer at the case $b = 1$ we will derive a special case of a marvelous theorem in Number Theory.

Let $n \geq 3$ and let $d|n$ be a factor $< n$. Clearly the polynomial $\Phi_n(X)$, by its construction, must divide the polynomial $(X^n - 1)/(X^d - 1)$. The same then holds for the numbers produced by substituting a value a for X.

Therefore $(a^d - 1, \Phi_n(a))$ divides $(a^d - 1, (a^n - 1)/(a^d - 1))$. Setting $n = qd$ the second number in parentheses may be written as a geometric sum, $a^{(q-1)d} + a^{(q-2)d} + \cdots + 1$. As all the terms in that sum are congruent to 1 modulo $a^d - 1$, and there are q of them, we conclude that

$$(a^d - 1, \Phi_n(a)) \quad | \quad (a^d - 1, q) \quad | \quad q,$$

which is of some significance in itself (the common factors are small).

Now let $a = n$. Obviously $\Phi_n(n) \equiv 1 \pmod{n}$, so that $(\Phi_n(n), q) = 1$. As $\big(n^d - 1, \Phi_n(n)\big)|q$, the only possibility is $(n^d - 1, \Phi_n(n)) = 1$.

Let p be a prime factor of $\Phi_n(n)$. As the relative primality holds for any proper factor $d|n$, it holds that

$$n^d \not\equiv 1 \pmod{p}$$

for these, hence

$$\mathrm{ord}_p(n) = n.$$

By Little Fermat, therefore, $n|(p-1)$, $p = 1 + kn$, i.e., the class of 1 modulo n contains a prime number. We have almost proved the following:

F.VIII.9 Theorem. *Let $n \geq 3$ ($n = 2$ is a trivial case). Then the class of 1 modulo n contains infinitely many prime numbers.*

Proof. We have shown that the class in question contains a prime $p = 1 + kn$. Now repeat the discussion above with $r \cdot n$, $r \nmid k$, in place of n, thus producing a prime $p = 1 + lrn$. Obviously, this process can be repeated indefinitely so as to produce an infinite sequence of primes $\equiv 1 \pmod{n}$. □

A beautiful theorem by Dirichlet states that *every* invertible class modulo n contains infinitely many primes. You can find it in Apostol's book.

Peter Gustav Lejeune Dirichlet (1805-1859) pioneered the use of analytic tools in Algebraic Number Theory.

F.VIII: Exercises

1. A recursive procedure for computing $\Phi_n(X)$. If q is a prime dividing n, then $\Phi_{qn}(X) = \Phi_n(X^q)$, prove this.

If q is a prime not dividing n, then $\Phi_{qn}(X) = \Phi_n(X^q)/\Phi_n(X)$, prove this.

For odd n, also note, and prove, $\Phi_{2n}(X) = \Phi_n(-X)$.

2. (a) Compute $\Phi_n(1)$. Treat $n =$ prime power first.

(b) Compute $\Phi_n(-1)$. It is convenient to start with odd n, and powers of 2.

3. Using relations like

$$1 - \epsilon^k = \epsilon^{k/2}(\epsilon^{-k/2} - \epsilon^{k/2}),$$

Euler's formula for the sine function, the previous exercise, and Gauß' Lemma (D.IV.4), derive an expression for the product of all $\sin(am\pi/n)$ where a runs over a whole or a half system of invertible classes modulo n, and $(m,n)=1$.

The case where n is neither an odd prime power nor twice an odd prime power is the easiest (as $4|\phi(n)$). The cases where n is a prime power (odd, or power of 2) are the most striking. Start with $m=1$. The answer will involve Legendre symbols.

4. Let $f=\phi(n)$. Form the polynomial

$$\Psi(X)=(X-i)^f\Phi\Big(\frac{X+i}{X-i}\Big).$$

Show that its leading coefficient is real, and that all its roots are real (find them!). Conclude that its coefficients are rational integers. Determine $\Psi(0)$ (in various cases). What trigonometric identities can you deduce?

5. Consider the algebraic congruence

$$\Phi_n(X)\equiv 0 \pmod q$$

where q is a prime not dividing n.

(a) Show (e.g., using ideas from the last subsection) that if a is a root, then $\mathrm{ord}_q(a)=n$, so that $q\equiv 1 \pmod n$.

(b) Assume, conversely, that $q\equiv 1 \pmod n$. Show that the congruence $\Phi_n(X)\equiv 0 \pmod q$ is solvable, and has $\phi(n)$ solutions modulo q.

(c) Also show that $v_q(\Phi_n(a))=v_q(a^n-1)$ for each solution.

6. (continued) Now consider the case $n=n_1\cdot q^\alpha$ where $q\nmid n_1$. Let a be a solution to the congruence above. Show that $\mathrm{ord}_n(a)$ divides n_1 (easy); then show, using the trick of the last subsection in two different ways, that $\mathrm{ord}_n(a)=n_1$ and that $v_q(\Phi_n(a))$=1.

Finally note that q can only be the largest prime factor of n.

Exemplify the two exercises by studying $\Phi_{20}(X)$ modulo 5, 41, 15.

7. Let s_d be the sum of roots of unity of exact order d. Determine the sum $\sum_{d|g}s_d$ (for instance, use the relation between roots and coefficients of a polynomial). An expression for s_d follows immediately.

Now do the same for primitive roots modulo p.

8. Let $p_1=2,3,5,\dots,p_N$ be the N first primes. Use the special case of Dirichlet's Theorem proved here, to show that there exists a prime number P such that $(p_k/P)=1$ for all $1\le k\le N$.

The trick is to find the right modulus on which to apply Dirichlet.

Conclude, for this P, that all positive numbers up to a certain limit are quadratic residues modulo P, hence not primitive roots. That is, for any given integer $M > 0$ there exists a prime P such that the least positive primitive root for P is $> M$.

Chapter G

Continued Fractions

G.I Motive, Definitions

Our presentation of this topic owes a lot to that of Harold Stark (1939 -). It has a strong geometric slant.

Most texts give the theory as an infinite analog of Extended Euclid, (A.I.7) and derive theorems about rational approximations as an afterthought. Here we start with the approximations right away. You will not see very much of the continued fractions themselves, until the end of the Chapter (they are horrible to type).

Consider the straight line given by the equation $y = \alpha x$, in a an orthonormal coordinate system. We assume $\alpha > 0$, and (for the time being) irrational. We are looking for a sequence of rational approximations

$$C_k = \frac{p_q}{q_k}, \quad p_q, q_k \in \mathbf{Z}, \quad k \geq -1,$$

converging to the slope α. It has proved fruitful to introduce the *vectors*

$$\mathbf{v}_k = \begin{pmatrix} q_k \\ p_k \end{pmatrix}$$

of slope C_k.

One obvious requirement is

$$|\alpha - \frac{p_k}{q_k}| \to 0.$$

A stronger requirement is given by the vertical distance from the head of the vector $\mathbf{v}_k$ to the line $y = \alpha x$, i.e., the distance between the points (q_k, p_k) and $(q_k, \alpha q_k)$,

$$d = |\alpha q_k - p_k|.$$

We require $d \to 0$. That is a stronger requirement as it will turn out that $q_k \to +\infty$.

We allow ourselves to start with

$$\mathbf{v}_{-1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

of infinite slope. Sometimes it is convenient start with $\mathbf{v}_{-2} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, of zero slope.

Next we set

$$\begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = \begin{pmatrix} 1 \\ a_0 \end{pmatrix},$$

where $a_0 = \lfloor \alpha_0 \rfloor$, the *floor* of $\alpha_0 = \alpha$ (the largest integer $\leq \alpha$).

Of all vectors, with integer coordinates, and first coordinate =1, it is the one coming closest to

$$\begin{pmatrix} 1 \\ \alpha_0 \end{pmatrix}$$

from below.

We now determine that integral linear combination

$$\begin{pmatrix} q_1 \\ p_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + a_1 \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + a_1 \begin{pmatrix} 1 \\ a_0 \end{pmatrix}$$

whose slope lies *just above* α_0

We first choose that irrational number α_1 (instead of the integer a_1) giving equality, so that

$$\begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} + \alpha_1 \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \alpha_1 \begin{pmatrix} 1 \\ a_0 \end{pmatrix}$$

is of slope α_0:

$$\alpha_0 = \frac{\alpha_1 a_0 + 1}{\alpha_1},$$

whence

$$\alpha_1 = \frac{1}{\alpha_0 - a_0}.$$

Then the head of our linear combination will land *on* the line $y = \alpha x$. We want to stop just before that; therefore we replace α_1 by its floor: $a_1 = \lfloor \alpha_1 \rfloor$. Our next step will be to determine the integral linear combination

$$\mathbf{v}_2 = \begin{pmatrix} q_2 \\ p_2 \end{pmatrix} = a_2 \begin{pmatrix} q_1 \\ p_1 \end{pmatrix} + \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = a_2 \mathbf{v}_1 + \mathbf{v}_0$$

giving a slope *just below* α. Again we first determine the irrational number α_2 so that the linear combination

$$\mathbf{v}_2' = \alpha_2 \mathbf{v}_1 + \mathbf{v}_0$$

is of slope exactly $= \alpha$.

We have already defined α_1 so that

$$\mathbf{v}_1' = \alpha_1 \mathbf{v}_0 + \mathbf{v}_{-1}$$

is of slope α, and

$$\mathbf{v}_1 = a_1 \mathbf{v}_0 + \mathbf{v}_{-1},$$

where $a_1 = \lfloor \alpha_1 \rfloor$.

Subtracting the two equations gives

$$\mathbf{v}_1 = \mathbf{v}_1' - (\alpha_1 - a_1)\mathbf{v}_0.$$

We are requiring that

$$\mathbf{v}_2' = \alpha_2 \mathbf{v}_1 + \mathbf{v}_0 = \alpha_2[\mathbf{v}_1' - (\alpha_1 - a_1)\mathbf{v}_0] + \mathbf{v}_0$$

have the same slope, α, as $\mathbf{v}_1'$. That will happen if and only if the coefficient for $\mathbf{v}_0$ equals zero, i.e., if and only if:

$$\alpha_2 = \frac{1}{\alpha_1 - a_1}.$$

Again, the head of our vector lands on the line. We moved forward, below the line, until reaching it. Again we stop just before it, i.e., again we take the floor of α_2:

$$a_2 = \lfloor \alpha_2 \rfloor.$$

We are led to the following *recursive definitions*:

G.I.1 Definition. Define the irrational numbers α_k, and the integers a_k, the **partial quotients**, by:

$$\alpha_0 = \alpha, \quad a_0 = \lfloor \alpha_0 \rfloor; \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \quad a_{k+1} = \lfloor \alpha_{k+1} \rfloor, \quad k \geq 0.$$

Further define the vectors

$$\mathbf{v}_k = \begin{pmatrix} q_k \\ p_k \end{pmatrix} \in \mathbf{Z}^2, \quad k \geq -1,$$

recursively by

$$\begin{aligned} \begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \\ \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} &= \begin{pmatrix} 1 \\ a_0 \end{pmatrix}, \\ \begin{pmatrix} q_{k+1} \\ p_{k+1} \end{pmatrix} &= a_{k+1} \begin{pmatrix} q_k \\ p_k \end{pmatrix} + \begin{pmatrix} q_{k-1} \\ p_{k-1} \end{pmatrix}, \quad k \geq 0, \end{aligned} \tag{R_k}$$

having slopes (the **convergents** of α):

$$C_{k+1} = \frac{p_{k+1}}{q_{k+1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}}; \quad (C_{-1} = \infty, C_0 = a_0).$$

G.I.2 Example (A computation). We choose $\alpha = \sqrt{14}$ and obtain the following:

$$\begin{aligned} \alpha_0 &= \sqrt{14} = 3 + (\sqrt{14} - 3);\ a_0 = 3 \\ \alpha_1 &= \frac{1}{\sqrt{14} - 3} = \frac{\sqrt{14} + 3}{5} = 1 + \frac{\sqrt{14} - 2}{5};\ a_1 = 2 \\ \alpha_2 &= \frac{5}{\sqrt{14} - 2} = \frac{\sqrt{14} + 2}{2} = 2 + \frac{\sqrt{14} - 2}{2};\ a_2 = 2 \\ \alpha_3 &= \frac{2}{\sqrt{14} - 2} = \frac{\sqrt{14} + 2}{5} = 1 + \frac{\sqrt{14} - 3}{5};\ a_3 = 1 \\ \alpha_4 &= \frac{5}{\sqrt{14} - 3} = \sqrt{14} + 3 = 6 + (\sqrt{14} - 3);\ a_4 = 6 \end{aligned}$$

so that $a_0 = 3, a_1 = 1, a_2 = 2, a_3 = 1, a_4 = 6$. From that point on, the a_k

repeat periodically: $a_5 = a_1 = 1$; $a_6 = a_2 = 2\ldots$ This happens because in the next step we once again invert $\sqrt{14} - 3$.

From our recurrence

$$p_{k+1} = a_{k+1}p_k + p_{k-1}, \quad q_{k+1} = a_{k+1}q_k + q_{k-1}, \quad k \geq 0,$$

we now obtain the following table:

k	-1	0	1	2	3
p_k	1	3	4	11	15
q_k	0	1	1	3	4
a_{k+1}	3	1	2	1	6
C_k	∞	3	4	$11/3$	$15/4$

with the odd C_k lying above, the even ones below, $\sqrt{14}$.

For instance,

$$C_2 = \frac{p_2}{q_2} = \frac{a_2p_1 + p_0}{a_2q_1 + q_0} = \frac{2 \cdot 4 + 3}{2 \cdot 1 + 1} = \frac{11}{3} < \sqrt{14}.$$

□

G.II Basic Theorems

We are now ready to prove a couple of Theorems.

G.II.1 Theorem. *The determinant*

$$p_kq_{k-1} - q_kp_{k-1} = \begin{vmatrix} q_{k-1} & q_k \\ p_{k-1} & p_k \end{vmatrix} = (-1)^{k-1}, \quad k \geq 0.$$

Proof. Induction on k, by column operations. $k = 0$:

$$\begin{vmatrix} q_{-1} & q_0 \\ p_{-1} & p_0 \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & a_0 \end{vmatrix} = -1.$$

$k \to k + 1$:

$$\begin{vmatrix} q_k & q_{k+1} \\ p_k & p_{k+1} \end{vmatrix} = \begin{vmatrix} q_k & a_{k+1}q_k + q_{k-1} \\ p_k & a_{k+1}p_k + p_{k-1} \end{vmatrix} = \begin{vmatrix} q_k & q_{k-1} \\ p_k & p_{k-1} \end{vmatrix} = - \begin{vmatrix} q_{k-1} & q_k \\ p_{k-1} & p_k \end{vmatrix} .$$

□

Here we never used the exact meaning of the integers a_k.

An important consequence is:

G.II.2 Theorem. *Every vector with integral components:*

$$\begin{pmatrix} s \\ r \end{pmatrix}, \quad r, s \in \mathbf{Z},$$

can be written as an integral *linear combination*

$$\begin{pmatrix} s \\ r \end{pmatrix} = l \begin{pmatrix} p_k \\ q_k \end{pmatrix} + m \begin{pmatrix} p_{k-1} \\ q_{k-1} \end{pmatrix} = l\mathbf{v}_k + m\mathbf{v}_{k-1}; \quad l, m \in \mathbf{Z}.$$

Proof. This follows simply by viewing this vector equation as a linear system of equations, of determinant $\pm 1 \neq 0$:

$$\begin{aligned} s &= lp_k + mp_{k-1} \\ r &= lq_n + mq_{k-1} \end{aligned}$$

and solving for l, m. Multiplying the first equation by q_{k-1}, the second by p_{k-1}, and subtracting, gives $sq_{k-1} - rp_{k-1} = (p_k q_{k-1} - q_k p_{k-1})l = \pm 1 \cdot l$, and similarly for m. □

Those who remember their Linear Algebra will recall the interpretation of a 2 × 2-determinant as a signed, or oriented, area.

For odd k this area equals $+1$, i.e., the two column vectors span a parallellogram of area 1, with the second vector lying “to the left” of the first. In fact, the two vectors will lie on opposite sides of the line $y = \alpha x$. We will prove this later.

For even k, the area also equals 1, but the orientation is the opposite to the odd case. The geometric significance of a column operation is that two vertices of the parallellogram are translated along the line connecting them, changing neither the base nor the altitude, hence not the area.

Another consequence is the following:

G.II.3 Theorem. $p_k, q_k,\ k \geq 0$, *are relatively prime.*

□

G.II.4 Theorem. *If, in the recurrence* (R_k) *above, the integer* a_{k+1} *is replaced by* α_{k+1} *we obtain a vector of slope equal to* α*:*

$$\alpha = \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}.$$

Proof. Induction on k.

The case $k = 0$ follows directly from our previous definition:

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} \Longrightarrow \alpha_0 = \frac{\alpha_1 a_0 + 1}{\alpha_1} = \frac{\alpha_1 p_0 + p_{-1}}{\alpha_1 q_0 + q_{-1}}.$$

We now turn to the induction step.

Suppose α_{k+1} has been defined so that the vector

$$\mathbf{v}'_{k+1} = \alpha_{k+1}\mathbf{v}_k + \mathbf{v}_{k-1} \tag{$*$}$$

is of slope $= \alpha$. Suppose we then define

$$\mathbf{v}_{k+1} = a_{k+1}\mathbf{v}_k + \mathbf{v}_{k-1}, \tag{$**$}$$

where a_{k+1} is the floor of α_{k+1}.

We must show that the recurrence for the α produces that α_{k+2} for which the vector

$$\mathbf{v}'_{k+2} = \alpha_{k+2}\mathbf{v}_{k+1} + \mathbf{v}_k \tag{$***$}$$

has slope α.

Combining (*) and (**) we get:

$$\begin{aligned} \mathbf{v}'_{k+1} - \mathbf{v}_{k+1} &= (\alpha_{k+1} - a_{k+1})\mathbf{v}_k, \\ \mathbf{v}_{k+1} &= \mathbf{v}'_{k+1} - (\alpha_{k+1} - a_{k+1})\mathbf{v}_k. \end{aligned}$$

Plugging this into (***) then gives

$$\mathbf{v}'_{k+2} = \alpha_{k+2}\mathbf{v}'_{k+1} + [1 - \alpha_{k+2}(\alpha_{k+1} - a_{k+1})]\mathbf{v}_k.$$

By the recurrence for the α the expression in brackets equals zero, so the vector $\mathbf{v}'_{k+2}$ has the same slope as $\mathbf{v}'_{k+1}$, i.e., its slope equals α. □

Remark: The critical reader will wonder where we used the fact that the integer a_k is the floor of α_k. It is the choice giving the inequalities $\alpha_{k+1} > 1$ and $a_{k+1} \geq 1$ needed to set things in motion.

G.II.5 Example. In our introductory example we found the convergent

$$C_2 = \frac{p_2}{q_2} = \frac{a_2p_1 + p_0}{a_2q_1 + q_0} = \frac{2 \cdot 4 + 3}{2 \cdot 1 + 1} = \frac{11}{3}.$$

Replacing $a_2 = 2$ by $\alpha_2 = (\sqrt{14} + 2)/2$ we get

$$\frac{(\sqrt{14} + 2) \cdot 4 + 2 \cdot 3}{(\sqrt{14} + 2) \cdot 1 + 2 \cdot 1} = \frac{4\sqrt{14} + 14}{\sqrt{14} + 4} = \sqrt{14},$$

as promised by the Theorem. □

G.II.6 Theorem. $|C_k - \alpha| < \dfrac{1}{q_kq_{k+1}} \leq 1/k^2$.

Proof. Using our earlier observations we get:

$$\begin{aligned} |C_k - \alpha| &= |\frac{p_k}{q_k} - \alpha| \\ &= |\frac{p_k}{q_k} - \frac{\alpha_{k+1}p_k + p_{k-1}}{\alpha_{k+1}q_k + q_{k-1}}| = \frac{|p_kq_{k-1} - p_{k-1}q_k|}{(\alpha_{k+1}q_k + q_{k-1})q_k} \\ &= \frac{1}{q_k(\alpha_{k+1}q_k + q_{k-1})} < \frac{1}{q_k(a_{k+1}q_k + q_{k-1})} \\ &= \frac{1}{q_kq_{k+1}}. \end{aligned}$$

This proves the first inequality. The second equality follows becuse the q_k are a strictly increasing sequence of positive integers, for $k \geq 1$.

This in turn follows from the recurrence (R_k) and the fact that $\alpha_{k+1} > 1$, $k \geq 0$, so that $a_{k+1} \geq 1$. And this finally comes from

$$1 > \alpha_k - a_k > 0, \quad k \geq 0,$$

yielding $\alpha_{k+1} = 1/(\alpha_k - a_k) > 1$. □

We note an immediate Corollary.

G.II.7 Corollary.

$$C_k \to \alpha$$

as $k \to +\infty$.

And, better still:

$$|p_k - q_k\alpha| = q_k|C_k - \alpha| < \frac{1}{q_{k+1}} \to 0.$$

□

As we have noted before, the expression $|p_k - q_k\alpha|$ signifies the vertical distance from the head of $\mathbf{v}_k$ to the line $y = \alpha x$.

In the discussion on "best approximation" below (Section G.IV) it is essential to realize that the vectors $\mathbf{v}_k$ with odd k lie above the line $y = \alpha x$, those with even k below.

By our motivating discussion at the beginning of this Chapter, we expect the following to hold:

G.II.8 Theorem. *For odd* k, $C_k > \alpha$, *for even* k, $C_k < \alpha$.

Proof. Remove the absolute value signs in the proof of the last Theorem. The denominator being positive, we see that $C_k - \alpha$ has the same sign as $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$. □

Most books show by calculation that the sequence of even convergents is increasing: $C_0 < C_2 < C_4 < \ldots$, and that of odd convergents decreasing: $C_1 > C_3 > C_5 > \ldots$, e.g., $C_{k-1} < C_{k+1} < C_k$ for even $k + 1$.

A more geometric proof comes from noting that each $C_k, k \geq 1$, must lie between the two preceding ones.

This is because the vector $\mathbf{v}_{k+1}$ is a positive linear combination of $\mathbf{v}_k$ and $\mathbf{v}_{k-1}$, hence lies strictly between them. The corresponding relation then must hold for their slopes.

G.II: Exercises

1. Compute the first five a_k, α_k, C_k for $\alpha = \sqrt{2}$. Compare to the irrationality $1 - \sqrt{2}$, and its powers. Do you see a pattern? Can you prove it?

If you know about musical intervals, you may enjoy comparing the tempered, and some Pythagorean, variants of the tritone interval.

2. Compute the first five a_k, α_k, C_k for $\alpha = \sqrt{6}$. Look more closely at the irrationalities $p_k + q_k\sqrt{6}$, and a few products among these, and guess a pattern. The correct pattern will be stated and proved later in the text.

3. We want to compute $\log_{10} a$, where a is a rational number > 1, using continued fractions. (In order to avoid finite continued fractions, you may wish to avoid an integer power of 10.)

You will probably be led to introducing $b_0 = 10$, $b_{-1} = a$, and a recurrence expressing the rational number b_{k+1} in the b_k, b_{k-1}, determining the partial quotient a_k as the largest integer satisfying $b_k^{a_k} \leq b_{k-1}$. Plus, of course, the recurrence for the convergents.

In this manner, a short hand calculation will give you, for instance, $\log_{10} 2$ and $\log_{10} 3$, with four correct decimal places.

Again, if you know about musical intervals, knowing rational approximations to the logarithms of 2, 3, etc. you may enjoy comparing the Pythogarean and tempered fifth, among others.

If you turn this into a computer algorithm what problems do you encounter (or foresee) in treating the b_k as exact rationals, or as floats?

Remark: This algorithm was presented by my grandfather, Professor Severin Johansson (1879-1929), in a book on mathematical eduction in primary and secondary schools in Finland (Swedish title: "Matematiken i Finlands skola"). It was his idea that short hand calculations of this kind would help demystify logarithms.

* G.III Negative Irrationalities

For the application to Pell's Equation $x^2 - Dy^2 = \pm 1$ it will suffice to understand the case just treated, that of positive α. We made that assumption as signs tend to confuse. For the discussion on the general equation $x^2 - Dy^2 = N$, however, it will be convenient to be able to deal with negative numbers, as well.

The following discussion may be skipped on first reading; the reader may wish to return to it in connection with the last Sections of this Chapter.

Thus, let $\beta_0 = \beta < 0$ be negative. If $\lfloor\beta\rfloor = -m$, set $\alpha_0 = \alpha = \beta + m$, $0 < \alpha < 1$. Defining

$$b_k = \lfloor\beta_k\rfloor, \quad \beta_{k+1} = \frac{1}{\beta_k - b_k}, \quad k \geq 0$$

we will have $b_0 = -m, a_0 = 0$. But then $\beta_1 = 1/(\beta_0 - b_0) = 1/(\alpha_0 - a_0) = \alpha_1$, hence $b_k = a_k$ for all $k \geq 1$. Most importantly, all b_k, $k \geq 1$, are positive.

Now look at the recurrence for the convergents:

$$\begin{pmatrix} s_{-1} \\ r_{-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} s_0 \\ r_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad \begin{pmatrix} s_{k+1} \\ r_{k+1} \end{pmatrix} = b_{k+1} \begin{pmatrix} s_k \\ r_k \end{pmatrix} + \begin{pmatrix} s_{k-1} \\ r_{k-1} \end{pmatrix}, k \geq 0.$$

Clearly the s_k form an increasing sequence of positive integers, and the r_k a decreasing sequence of negative integers, from $k = 0$ on. We also see that the vector in the left member is a positive linear combination of the two preceding ones, hence lies between them.

Then look at the corresponding recurrence for the convergents to α:

$$\begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = \begin{pmatrix} 1 \\ -m \end{pmatrix}; \quad \begin{pmatrix} q_{k+1} \\ p_{k+1} \end{pmatrix} = b_{k+1} \begin{pmatrix} q_k \\ p_k \end{pmatrix} + \begin{pmatrix} q_{k-1} \\ p_{k-1} \end{pmatrix}, k \geq 0.$$

Comparing the two we easily see that

$$\begin{pmatrix} q_k \\ p_k \end{pmatrix} = \begin{pmatrix} s_k \\ r_k + ms_k \end{pmatrix}, \quad k \geq 0,$$

so that, quite reasonably,

$$\frac{p_k}{q_k} = \frac{r_k}{s_k} + m.$$

From this we see, e.g., that $r_k s_{k-1} - s_k r_{k-1} = p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}$ and that in this case too the odd convergents lie above β, and the even ones below it.

G.IV Best Rational Approximation

The letter α still denotes an irrational number. We do not suppose $\alpha > 0$.

G.IV.1 Lemma. *Suppose $s > 0, r$ are integers with*

$$|s\alpha - r| < |q_k\alpha - p_k|$$

Then $s \geq q_{k+1}$.

Proof.

We have already pointed out that $|s\alpha - r|$ is the vertical distance from the point (s, r) to the line $y = \alpha x$.

We also noted in G.II.2 that

$$\begin{pmatrix} s \\ r \end{pmatrix} = l \begin{pmatrix} q_k \\ p_k \end{pmatrix} + m \begin{pmatrix} q_{k+1} \\ p_{k+1} \end{pmatrix} = l\mathbf{v}_k + m\mathbf{v}_{k+1},$$

with *integer* coefficients l, m. Recall that the heads of $\mathbf{v}_k$ and $\mathbf{v}_{k+1}$ lie on opposite sides of the line.

If $l \geq 0, m > 0$, then obviously $s \geq q_{k+1}$. We will prove that this is the only possible case.

If $l > 0, m = 0$, the the assumption $|s\alpha - r| < |q_k\alpha - p_k|$ is not satisfied.

So let us assume one of l, m is < 0. The other must then be > 0, else s would be negative. We proceed to derive a contradiction.

Let us assume $l = -n < 0$, $m > 0$ (the opposite case is similar, and left to the reader). We then have

$$\begin{pmatrix} s \\ r \end{pmatrix} = -n \begin{pmatrix} q_k \\ p_k \end{pmatrix} + m \begin{pmatrix} q_{k+1} \\ p_{k+1} \end{pmatrix} = -n\mathbf{v}_k + m\mathbf{v}_{k+1}.$$

With tails at the origin, the heads of the two terms now lie on the *same* side of the line $y = \alpha x$. Summing the two vectors entails *summing* their vertical distances from the line (draw a diagram!):

$$|s\alpha - r| = n|q_k\alpha - p_k| + m|q_{k+1}\alpha - p_{k+1}| \geq |q_k\alpha - p_k|$$

contrary to the assumption of the Theorem. □

G.IV.2 Corollary. *If*

$$|\alpha - \frac{r}{s}| < |\alpha - \frac{p_k}{q_k}|, \quad k \geq 0,$$

then $s > q_k$.

Proof. Suppose, by way of contradiction, that

$$|\alpha - \frac{r}{s}| < |\alpha - \frac{p_k}{q_k}|$$

and, at the same time, $s \leq q_k$. Multiplying these two inequalities gives:

$$s|\alpha - \frac{r}{s}| < q_k|\alpha - \frac{p_k}{q_k}|,$$

$$|s\alpha - r| < |q_k\alpha - p_k|.$$

By the preceding Theorem that would imply $s \geq q_{k+1} > q_k$.

This contradiction completes the proof. □

Remark: Another consequence of the Theorem is that

$$|q_k\alpha - p_k| < |q_{k-1}\alpha - p_{k-1}|, \quad k \geq 0.$$

We cannot have equality, as that would imply α rational. The opposite inequality would result in $q_{k-1} \geq q_{k+1}$, by the Theorem.

So the vertical distances $|q_k\alpha - p_k|$ decrease as k increases.

G.IV.3 Theorem. *If* $r, s > 0$ *are integers such that*

$$|\alpha - \frac{r}{s}| < \frac{1}{2s^2},$$

then r/s *is* a convergent *for* α.

Proof. For the case $r > 0$, choose k such that $q_k \leq s < q_{k+1}$. We prove the Theorem by showing $rq_k - sp_k = 0$.

By the last Theorem

$$|\alpha q_k - p_k| \leq |\alpha s - r| < \frac{1}{2s}.$$

Therefore;

$$\begin{aligned}|rq_k - sp_k| &= |s(\alpha q_k - p_k) - q_k(\alpha s - r)| < \\ &< s\frac{1}{2s} + q_k\frac{1}{2s} \leq \\ &\leq \frac{1}{2} + \frac{1}{2} = 1,\end{aligned}$$

i.e., $|rq_k - sp_k| < 1$. As the expression in the absolute value sign is an integer, it must equal $= 0$, as we hoped. □

We now apply all of this to *Pell's equation.*

G.IV.4 Theorem. *Let D be a positive integer, not a square. Suppose*

$$x^2 - Dy^2 = n, \quad |n| < \sqrt{D},$$

where x, y are positive integers.

Then x/y is a convergent (G.I.1) for α.

Proof. The case $n > 0$ is the easiest. One proves that

$$0 < \frac{x}{y} - \sqrt{D} < \frac{1}{2y^2},$$

and the result is then immediate from the preceding Theorem.

We now prove the inequality. Dividing the given equation by y^2, and factoring, we get

$$(\frac{x}{y} - \sqrt{D})(\frac{x}{y} + \sqrt{D}) = \frac{n}{y^2}. \qquad (*)$$

The second factor, and the right member, are positive, hence the same holds for the first factor:

$$\frac{x}{y} > \sqrt{D} > n, \quad \frac{x}{y} + \sqrt{D} > 2n.$$

Dividing $(*)$ by $x/y + \sqrt{D}$ gives the result.

In the case $n = -m$, $m > 0$, the factorization

$$(\frac{y}{x} - \frac{1}{\sqrt{D}})(\frac{y}{x} + \frac{1}{\sqrt{D}}) = \frac{m}{D} \cdot \frac{1}{x^2}, \quad 0 < \frac{m}{D} < \frac{\sqrt{D}}{D} = \frac{1}{\sqrt{D}}$$

shows, in the same manner, that y/x is a convergent for $1/\sqrt{D}$.

But if $\beta = 1/\alpha, \quad \alpha = \sqrt{D} > 1$, then $b_0 = 0$ and $\beta_1 = 1/(\beta - 0) = \alpha = \alpha_0$.

Inductively we then see that $\beta_k = \alpha_{k-1}$, $k \geq 1$. This shift is seen to result in inverting all the convergents, and we are reduced to the previous case. □

G.IV.5 Example. The last paragraph of the proof is best understood by an example.

Take $\alpha_0 = \sqrt{6}$, $\beta_0 = 1/\alpha$. An easy computation gives $\alpha_0 = 2, \alpha_1 = 2, \alpha_2 = 4, \alpha_3 = 2$, after which the α_k repeat with period 2.

As the floor of β_0 equals $b_0 = 0$ we see that $\beta_1 = \alpha_0 = \sqrt{6}$ so that $\beta_2 = \alpha_1 = 2$, etc.

Now let us have a closer look at the approximating vectors. For α we obtain

$$\mathbf{v}_{-1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \mathbf{v}_0 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \mathbf{v}_1 = 2\begin{pmatrix} 1 \\ 2 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \ldots$$

For β we get:

$$\mathbf{w}_{-1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \mathbf{w}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ (NB!)},$$

$$\mathbf{w}_1 = 2\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \mathbf{w}_2 = 2\begin{pmatrix} 2 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \end{pmatrix}, \ldots$$

Here we clearly see how the two coordinates are interchanged. This phenomenon will then continue, as the $\mathbf{w}$ satisfy the same recurrence as the $\mathbf{v}$, with a unit shift in the indices. Thus the convergents are inverted, and the pattern generalizes to the case of arbitrary $\sqrt{D}$, $D > 1$. □

G.IV.6 Example. Let $d = 6$. The first few convergents are easily computed (exercise!)

$$C_0 = 2, \quad C_1 = \frac{5}{2}, \quad C_2 = \frac{22}{9}, \quad C_3 = \frac{49}{20}, \quad C_4 = \frac{218}{89}.$$

The cases covered by the Theorem are $x^2 - 6y^2 = \pm 1$ and $x^2 - 6y^2 \pm 2$. Reducing modulo 6, we exclude the minus sign in the first case, and the plus sign in the second (as we can only have $x^2 \equiv 0, 1, 3, 4 \pmod{6}$).

The remaining cases are solvable:

$$5^2 - 6 \cdot 2^2 = 1$$
$$22^2 - 6 \cdot 9^2 = -2$$

and $5/2, 22/9$, are indeed convergents for $\sqrt{6}$.

The succeeding convergents produce further solutions in a periodic fashion:

$$49^2 - 6 \cdot 20^2 = 1$$
$$218^2 - 6 \cdot 89^2 = -2$$
$$\cdots$$

The reason for this periodicity will be explained in the next Chapter. □

Remark: x/y being a convergent does *not* mean that the pair x, y equals some pair p_k, q_k. It could happen that $(x, y) > 1$. This possibility is ruled out if the right member is *squarefree*, i.e., not divisible by a perfect square $a^2 > 1$.

On the other hand, it can very well happen that $x^2 - Dy^2 = a^2$, and yet $(x, y) = 1$. This often leads to a factorization of D. We will explain this in the last Chapter (Sections L.X, L.XI).

The equation $x^2 - Dy^2 = 1$ always possesses solutions $x, y > 0$, if $D > 0$ is not a perfect square. We will prove this in the next Chapter.

G.V Where Are the "Continued Fractions"?

We answer the question by unwinding our recurrence for the α_k, a_k. From

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \quad \alpha_k = a_1 + \frac{1}{\alpha_{k+1}},$$

we get

$$\alpha = \alpha_0 = a_0 + \frac{1}{\alpha_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}} =$$

$$= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\alpha_3}}} = \dots$$

By induction one may prove that the convergents C_k are obtained in each step by replacing the last α_k with a_k:

$$C_1 = a_0 + \frac{1}{a_1}; \qquad C_2 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}, \quad \dots$$

The fact that $C_k \to \alpha$ as $k \to +\infty$ justifies writing α as an *infinite continued fraction*:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\dots}}}}$$

From this one may see that an (ultimately) *periodic continued fraction* corresponds to a *quadratic* irrationality, i.e., a root of a quadratic equation $aX^2 + bX + c$ with integer coefficients. Suppose, for instance, that $a_0 = 2; a_2 = a_4 = 4 = \dots, a_1 = a_3 = 2 = \dots.$ with periodicity from a_1 on (the reader is invited to study examples of longer period, or even supply a genreal argument).

Then

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \dots}}}} = 2 + \beta$$

where, evidently,

$$\beta = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \beta}} = \cfrac{1}{2 + \cfrac{1}{4 + \beta}}$$

so that

$$\beta = \frac{4 + \beta}{9 + 2\beta}$$

leading to the quadratic equation

$$\beta^2 + 4\beta - 2 = 0; \quad \beta = -2 \pm \sqrt{6}.$$

We keep the positive root:

$$\beta = \sqrt{6} - 2,$$

hence

$$\alpha = 2 + \beta = \sqrt{6}.$$

The following notation is often used: $\alpha = [1; \overline{2, 3}]$ where the bar indicates the *period* $2, 3$ and the 1 is the *preperiod.*

The converse is also true: quadratic irrationalities give rise to (ultimately) periodic continued fractions. We will prove this later.

G.V: Exercises

1. Determine the irrational number having the periodic expansion $[9, \overline{9, 18}]$.

G.VI Finite Continued Fractions

Up to now we have assumed α irrational. If $\alpha = m/n$, $m, n > 0$, $(m, n) = 1$, we expect a steadily improving sequence of rational approximations p_k/q_k to terminate with $p_k/q_k = m/n$.

In fact, if we were to have $q_{k+1} > n$, the general inequality

$$|\frac{m}{n} - \frac{p_k}{q_k}| < \frac{1}{q_k q_{k+1}}$$

would give $|mq_k - np_k| < n/q_{k+1} < 1$, hence $mq_k - nq_k = 0$, $m/n = p_k/q_k$, and we can do no better than that!

However, more can be said. The (finite) continued fractions expansion of m/n turns out to be the same thing as Extended Euclid (A.I.7)! This is most easily explained by example. Recall the following example from that Section, with $m = 37, n = 11$:

$$\begin{array}{rr}
1 \cdot 37 + 0 \cdot 11 = 37 = r_{-2} & \\
0 \cdot 37 + 1 \cdot 11 = 11 = r_{-1} & 37 - 3 \cdot 11 = 4 \\
1 \cdot 37 - 3 \cdot 11 = 4 = r_0 & 11 - 2 \cdot 4 = 3 \\
-2 \cdot 37 + 7 \cdot 11 = 3 = r_1 & 4 - 1 \cdot 3 = 1 \\
3 \cdot 37 - 10 \cdot 11 = 1 = r_2 & 3 - 3 \cdot 1 = 0 \\
11 \cdot 37 - 37 \cdot 11 = 0 = r_3 &
\end{array}$$

We now compare this to the determination of the α_k and a_k:

$$\begin{aligned}
\alpha_0 &= \frac{37}{11}; \quad a_0 = 3 \\
\alpha_1 &= \frac{1}{\frac{37}{11} - 3} = \frac{11}{37 - 3 \cdot 11} = \frac{11}{4}; \quad a_1 = 2 \\
\alpha_2 &= \frac{1}{\frac{11}{4} - 2} = \frac{4}{11 - 2 \cdot 4} = \frac{4}{3}; \quad a_2 = 1 \\
\alpha_3 &= \frac{1}{\frac{4}{3} - 1} = \frac{3}{1} = 3; \quad a_3 = 3 \\
(\alpha_4 &= \frac{1}{\alpha_3 - a_3}; \text{ no!! })
\end{aligned}$$

Clearly, taking the floor of a rational number amounts to performing a division with remainder, and the a_k are therefore the successive quotients in

Euclid. The numerators of the α_k are the remainders, and the recurrence producing one α from the previous one amounts to using that remainder as the new divisor in the next step of Euclid.

Next look at the convergents p_k/q_k. The basic recurrence is

$$\begin{aligned}
\begin{pmatrix} q_{-2} \\ p_{-2} \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \\
\begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \\
\begin{pmatrix} q_{k+1} \\ p_{k+1} \end{pmatrix} &= a_{k+1} \begin{pmatrix} q_k \\ p_k \end{pmatrix} + \begin{pmatrix} q_{k-1} \\ p_{k-1} \end{pmatrix}, \quad k \geq -1.
\end{aligned}$$

But the right members r_k satisfy almost the same recurrence:

$$r_{k+1} = -a_{k+1} r_k + r_{k-1}; \quad k \geq -1,$$

as the a_k are the successive quotients in Euclid. Hence the coefficients of the left members in Extended Euclid:

$$(1, 0),\ (0, 1),\ (1, -3),\ (-2, 7),\ (3, -10),\ (11, -37)$$

satisfy that same recurrence, so, except for an alternating sign, they must equal the (p_k, q_k):

$$\begin{pmatrix} q_{-2} \\ p_{-2} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = a_0 \begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} + \begin{pmatrix} q_{-2} \\ p_{-2} \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix},$$

$$\begin{pmatrix} q_1 \\ p_1 \end{pmatrix} = a_1 \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} + \begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} = \begin{pmatrix} 2 \\ 7 \end{pmatrix}, \quad \begin{pmatrix} q_2 \\ p_2 \end{pmatrix} = a_2 \begin{pmatrix} q_1 \\ p_1 \end{pmatrix} + \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = \begin{pmatrix} 3 \\ 10 \end{pmatrix},$$

$$\begin{pmatrix} q_3 \\ p_3 \end{pmatrix} = a_3 \begin{pmatrix} q_2 \\ p_2 \end{pmatrix} + \begin{pmatrix} q_1 \\ p_1 \end{pmatrix} = \begin{pmatrix} 11 \\ 37 \end{pmatrix}.$$

Having seen the pattern in one example the reader should have no difficulty in supplying a formal proof for (or at least accept) the following Theorem:

G.VI.1 Theorem. *Given $m, n > 0, (m, n) = 1$. The (finite) continued fractions expansion of m/n relates to Extended Euclid as follows.*

Suppose

$$\begin{aligned}
1\cdot m + 0\cdot n &= r_{-2}\\
0\cdot m + 1\cdot n &= r_{-1}\\
q_0\cdot m - p_0\cdot n &= r_0\\
q_1\cdot m - p_1\cdot n &= -r_1\\
&\dots\\
q_{d-1}\cdot m - p_{d-1}\cdot n &= (-1)^{d-1} r_{d-1} = (-1)^{d-1}\\
q_d\cdot m - p_d\cdot n &= (-1)^d r_d = 0
\end{aligned}$$

with $q_d = n, p_d = m$,

then (with α_k, a_k *as defined by the continued fractions expansion):*

$$\alpha_k = \frac{r_{k-2}}{r_{k-1}}, \quad a_k = \lfloor \alpha_k \rfloor, \quad 0 \le k \le d,$$

$$r_{k+1} = -a_{k+1} r_k + r_{k-1}, \quad -1 \le k \le d-1.$$

G.VI.2 Example (Decimal Fractions, again). Let p be a prime number $\neq 2, 5$, A simple pseudo-random generator of decimal digits is the decimal expansion of r/p, $0 < r < p$. It is periodic, and if 10 is a primitive root, it has maximal period $p-1$. One could of course use a primitive root b as base, in order to achieve maximal period. If b is large we can generate pseudo-random sequences of large integers. If $b = 2$, as is often the case, we have a bit generator of maximal period.

One can prove that the generator has fairly good statistical properties, e.g., strings of length just around the number of digits in p appear with approximately the same frequency.

However, it is useless for cryptographic purposes, as already a small portion of the sequence suffices to reconstruct r, p once we know the number of digits in p. The critical number is $2d+1$ where d is the number of digits in p.

We illustrate this by an example. The general idea will be clear from that.

Take $r/p = 13/107 = 0.121495327\dots.$ It has a period of $53 = (107-1)/2$. We assume known that p has 3 digits, $10^2 < p < 10^3$, so that $2p^2 < 2\cdot 10^6$.

From the first 7 decimals of the expansion we see that

$$|\frac{r}{p} - 0.121495| < 5 \cdot 10^{-7} = \frac{1}{2 \cdot 10^6} < \frac{1}{2p^2}$$

so r/p is a convergent in the continued fractions expansion of $121495/1\,000\,000$ (according to G.IV.3).

So we easily find r, p by doing a bit of Extended Euclid:

$$\begin{array}{rl}
1 \cdot 1\,000\,000 + 0 \cdot 121495 = 1\,000\,000 & \\
0 \cdot 1\,000\,000 + 1 \cdot 121495 = 121495 & 1\,000\,000 - 8 \cdot 121495 = 28040 \\
1 \cdot 1\,000\,000 - 8 \cdot 121495 = 28040 & 121495 - 4 \cdot 28040 = 9335 \\
-4 \cdot 1\,000\,000 + 33 \cdot 121495 = 9335 & 28040 - 3 \cdot 9335 = 35 \\
13 \cdot 1\,000\,000 - 107 \cdot 121495 = 35 &
\end{array}$$

and we can stop here, as $2 \cdot 35 \cdot 107 < 10^6$.

Actually p can be reconstructed from *any* segment of 7 decimals, as we see by multiplying r/p by a suitable power of 10. □

G.VI.3 Example. The example $10/97 = 0.10309\ldots$ shows that $2d$ decimals may not suffice. Performing Extended Euclid on the pair $10^4, 1030$ yields $-7 \cdot 10^4 + 68 \cdot 1030 = 40$, leading to the conclusion that we are looking at the decimal expansion of $7/68$. Using $10^4, 1031$ (because of the 9 in the fifth place) leads to the desirable identity $-10 \cdot 10^4 + 97 \cdot 1031 = 7$. □

G.VII Cornacchia's Algorithm

In this Section we present an algorithmic approach to finding all proper integer solutions x, y; $(x, y) = 1$, to the Diophantine equation

$$x^2 + Dy^2 = N.$$

All that is assumed is that D, N are positive integers.

The algorithm presented was published by the Italian mathematician G. Cornacchia in 1908. Our presentation is adapted (with corrections) from an exposition by A. Nitaj in *Expositiones Mathematicae*, **13** (1995), pp. 358-365, "L'algorithme de Cornacchia".

Now, if x, y is a solution satisfying $(x, y) = 1$, then also $(y, N) = 1$, so y is invertible modulo N. Hence there is some integer P, unique modulo N, such that

$$x + Py \equiv 0 \pmod{N}. \tag{$*$}$$

Plugging this into $x^2 + Dy^2 = N$ we get $y^2(P^2 + D) \equiv 0 \pmod{N}$. By invertibility, the factor y^2 cancels, and we are left with

$$P^2 + D \equiv 0 \pmod{N}.$$

Furthermore, $Px - Dy \equiv Px + P^2y \equiv P(x + Py) \equiv 0 \pmod{N}$, hence

$$Px - Dy \equiv 0 \pmod{N}. \tag{$**$}$$

The formulas (*) and (**) can be put together like this:

$$(P + i\sqrt{D})(x + iy\sqrt{D}) \equiv 0 \pmod{N} \tag{$***$}$$

(real part $\equiv 0$, imaginary part $\equiv 0$). The original $P^2 + D \equiv 0 \pmod{N}$ can be reconstructed from (*) and (**) as they combine to $y(P^2 + D) \equiv 0 \pmod{N}$ and $(y, N) = 1$.

We say that x, y is a solution *produced by*, or *belonging to, P*. Our concern is to find all solutions belonging to any P satisfying $P^2 \equiv -D \pmod{N}$. Clearly, if x, y is a solution belonging to P, then $-x, y$ is one belonging to $-P$. The roots to $P^2 \equiv -D \pmod{N}$ come in pairs, but we need only bother with those belonging to $P : 0 < P \leq N/2$ (for instance).

By our first Lemma we will never have to check whether a solution x, y produced by our algorithms is proper.

G.VII.1 Lemma. *Let P be an integer satisfying $P^2 + D \equiv 0 \pmod{N}$. Let further x, y be integers satisfying $x + Py \equiv 0 \pmod{N}$, and $x^2 + Dy^2 = N$. Then $(x, y) = 1$ (and $(y, N) = 1$).*

Proof. We know that $(x + iy\sqrt{D})(x - iy\sqrt{D}) = x^2 + Dy^2 = N$. Formula (***) above may be written $(P + i\sqrt{D})(x + iy\sqrt{D}) = (a + ib\sqrt{D})N$, $a, b, \in \mathbf{Z}$. Hence, dividing by $x + iy\sqrt{D}$, $P + i\sqrt{D} = (a + ib\sqrt{D})(x - iy\sqrt{D})$, so that $bx - ay = 1$, proving $(a, b) = 1$. □

Next, let us deal with uniqueness. We often view $x + iy\sqrt{D}$, rather than x, y, as a solution to $x^2 + Dy^2 = (x + iy\sqrt{D})(x - iy\sqrt{D}) = N$. We use a prime to denote complex conjugation: $(x + iy)' = x - iy$ for real x, y. With $\alpha = x + iy\sqrt{D}$ the equation under investigation reads $\alpha \cdot \alpha' = N$.

G.VII.2 Lemma. *Let $\alpha_i = x_i + y_i\sqrt{D}$, $i = 1, 2$, be solutions to*

$$x_i^2 + Dy_i^2 = N,$$

belonging to the same P. Then the two solutions differ at most in sign if $D > 1$. If $D = 1$ they may also differ by the factor $\pm i$, i.e., $(x_1, y_1) = (\pm x_2, \pm y_2)$, or ($D = 1$) also $(x_1, y_1) = (\mp y_2, \pm x_2)$.

Proof. Obviously $u + iv\sqrt{D} = \gamma = \alpha_1/\alpha_2$ satisfies

$$u^2 + Dv^2 = \gamma \cdot \gamma' = \frac{\alpha_1 \cdot \alpha_1'}{\alpha_2 \cdot \alpha_2'} = \frac{N}{N} = 1$$

We will prove that u and v are *integers*. From $u^2 + Dv^2 = 1$ then will follow that $u + iv\sqrt{D} = \pm 1$ or, if $D = 1$, $u + iv = \pm 1$, $\pm i$.

Let us compute the quotient:

$$\begin{aligned}\frac{x_1 + iy_1\sqrt{D}}{x_2 + iy_2\sqrt{D}} &= \frac{(x_1 + iy_1\sqrt{D})(x_2 - iy_2\sqrt{D})}{(x_2 + iy_2\sqrt{D})(x_2 - iy_2\sqrt{D})} \\ &= \frac{(x_1x_2 + Dy_1y_2) + i(x_2y_1 - x_1y_2)\sqrt{D}}{N}\end{aligned}$$

We must prove that

$$\begin{aligned} x_1x_2 + Dy_1y_2 &\equiv 0 \pmod{N} \\ x_2y_1 - x_1y_2 &\equiv 0 \pmod{N} \end{aligned}$$

This follows immediately on substituting $x_i \equiv Py_i \pmod{N}$, $i = 1, 2$, and $P^2 + D \equiv 0 \pmod{N}$, in the two left members above. □

The next Theorem is the first step towards actually finding a solution.

G.VII.3 Theorem. *Let $x \neq 0$, $y > 0$, $(x, y) = 1$, be a proper solution to $x^2 + Dy^2 = N$, satisfying $x + Py = qN$, where $0 < P < N$, and $P^2 + D \equiv 0 \pmod{N}$. Then, excluding the trivial case $x^2 + (N-1)y^2 = N, x = y = q = 1, P = N - 1$, q/y is a convergent in the finite continued fractions expansion of P/N.*

Proof. We note at first that $q \geq 0$, otherwise we would get $|x| = |qN - Py| \geq N$.

We will also need the following useful little observation. As $(x - y)^2 \geq 0$ for real x, y it holds that $2xy \leq x^2 + y^2$. Equality occurs if and only if $x = y$.

Now

$$|\frac{q}{y} - \frac{P}{N}| = |\frac{qN - Py}{yN}| = |\frac{x}{yN}|.$$

As (x, y) is proper, we cannot have $x = y$. ($x = y =$ would lead to the case we excluded) Therefore $2|xy| < x^2 + y^2 \leq x^2 + Dy^2 = N$, and $|x|/yN < 1/2y^2$. By our previous results (G.IV.3) this proves that q/y is a convergent to P/N. □

Comparing to the result of the previous Section we see that the equation $qN - yP = x$ will be produced by Extended Euclid, and that $|x|$ will be a remainder. Which of them? Obviously, it must be $< \sqrt{N}$. The next Theorem gives the simple answer.

G.VII.4 Theorem. *Performing Extended Euclid on P, N, let r_j be the* first *remainder $< \sqrt{N}$. Then the corresponding equation reads*

$$q_j \cdot P - p_j \cdot N = (-1)^j r_j.$$

The desired solution belonging to P (if it exists) is then $y = q_j, x = (-1)^{j+1} r_j$.

Proof. We know by the previous Theorem that the desired solution must be $x = \pm r_k, y = q_k$ for some $k \geq j$. The equation $x^2 + Dy^2 = N$ then forces $|x| < \sqrt{N}, y < \sqrt{N/D}$.

Assuming $j < k$ we must have $q_j < q_k < \sqrt{N/D}$, whence $0 < r_j^2 + Dq_j^2 < 2N$. As $q_j \cdot P - p_j \cdot N = (-1)^j r_j$ we easily see that the left member is divisible by N, hence equal to it:

$$(q_jP - p_jN)^2 + Dq_j^2 = (P^2 + D)q_j^2 - 2q_jp_jN + p_j^2N^2 \equiv 0 \pmod{N}.$$

This, however, violates the uniqueness Lemma proved above. So we must have $j = k$. □

G.VII.5 Example. Let $N = 97$, a prime number $\equiv 1 \pmod{3}$. By the results in the previous Chapter, the equation $x^2 + 3y^2 = 97$ is solvable in integers. The solution to $P^2 \equiv -3 \pmod{97}$ is $P \equiv \pm 26 \pmod{97}$. By our previous remarks it is enough to deal with $P = 26$ – changing the sign of P will only change the sign of x or y, i.e., it produces essentially the same solution.

We perform a little bit of Euclid:

$$\begin{aligned} 1 \cdot 97 + 0 \cdot 26 &= 97 & & \\ 0 \cdot 97 + 1 \cdot 26 &= 26 & \qquad 97 - 3 \cdot 26 &= 19 \\ 1 \cdot 97 - 3 \cdot 26 &= 19 & \qquad 26 - 1 \cdot 19 &= 7 \\ -1 \cdot 97 + 4 \cdot 26 &= 7 & & \end{aligned}$$

Here $x = 7$ is the first remainder $< \sqrt{97}$ and we immediately read off the solution $x, y = 7, 4$, $97 = 7^2 + 3 \cdot 4^2$. □

G.VII.6 Example. In this example we study the Diophantine equation

$$x^2 + Dy^2 = N,$$

with $D = 17$, $N = 2922$. The prime factorization of N is $2922 = 2 \cdot 3 \cdot 487$. The square roots of -17 modulo $2, 3, 487$ are $1, \pm 1$, ± 38, respectively. Applying the Chinese Remainder Theorem gives the solutions to $P^2 + D \equiv 0 \pmod{2922}$ as ± 449 and ± 1423.

Let us try Extended Euclid on $2922, 1423$ first. We stop as soon as the remainder in the right member is less than the square root of 2922:

$$\begin{aligned} 1 \cdot 2922 + 0 \cdot 1423 &= 2922 \\ 0 \cdot 2922 + 1 \cdot 1423 &= 1423 \\ 1 \cdot 2922 - 2 \cdot 1423 &= 76 \\ -18 \cdot 2922 + 37 \cdot 1423 &= 55 \\ 19 \cdot 2922 - 39 \cdot 1423 &= 21 \end{aligned}$$

However, $21^2+17\cdot 39^2 = 26298 = 9\cdot 2922$, so there are no solutions belonging to $P = \pm 1423$.

Now, let us try 449:

$$\begin{aligned} 1\cdot 2922 + 0\cdot 449 &= 2922 \\ 0\cdot 2922 + 1\cdot 449 &= 449 \\ 1\cdot 2922 - 6\cdot 449 &= 228 \\ -1\cdot 2922 + 7\cdot 1423 &= 221 \\ 2\cdot 2922 - 13\cdot 1423 &= 7 \end{aligned}$$

This time we are successful:

$$7^2 + 17\cdot 13^2 = 2922$$

so the four couples $(x, y) = (\pm 7, \pm 13)$, belonging to $P = \pm 449$, are the only solutions to the given Diophantine Equation. □

G.VII: Exercises

1. Warmup. Solve $x^2 + 2y^2 = 107$. Note that the modular square root of -2 is a power of -2 modulo 107 (Section E.IV).

2. **Further suggestions for computing:** If you do not have a modular square roots routine, solve $x^2+2y^2 = 4512273113 = p$ knowing that $3488559345^2 \equiv -2 \pmod{p}$.

3. $N = 72022699481$, a prime. Assuming that you already have a routine for modular square rooting, decide which of the equations $N = x^2+Dy^2$, where $D = 1$, 2, 3, 5, 7, 11, 13, 17 are solvable in integers, and find solutions.

In at least one case with $(-D/N) = 1$ you will only find integers x, y satisfying $N|(x^2 + Dy^2)$ but $N \neq x^2 + Dy^2$. Which?

Chapter H

"QCF" and Pell's Equation

H.I An Algorithm for Quadratic Irrationalities

H.I.1 Definition. A **quadratic irrationality** is a root to an equation of the form

$$Ax^2 - Bx + C = 0, \quad A \neq 0,$$

with integer coefficients.

(We assume that $D = B^2 - 4AC$ is not a perfect square; otherwise α would be rational).

A quadratic irrationality looks like this:

$$\alpha = \frac{B \pm \sqrt{D}}{2A}, \quad D = B^2 - 4AC.$$

We can write it in the form

$$\alpha = \frac{P + \sqrt{D}}{Q} \text{ where } Q|(D - P^2). \tag{$*$}$$

H.I.2 Theorem. *Let $\alpha > 0$ be as in $(*)$. Then all the irrationalities in its continued fractions expansion are of the same form.*

Proof. Let $n = \lfloor \alpha \rfloor$ and put

$$\beta = \frac{1}{\alpha - n}.$$

Plugging in the expression for α, we get

$$\beta = \frac{Q}{\sqrt{D} + P - nQ} = \frac{Q}{\sqrt{D} - (nQ - P)}$$

We then multiply by the quantity $\sqrt{D} + (nQ - P)$, obtaining

$$\beta = \frac{Q(\sqrt{D} + nQ - P)}{D - (nQ - P)^2}.$$

Since $Q | (D - P^2)$, the denominator is also divisible by Q.

We introduce the notation $P' = nQ - P$, and write $D - (P')^2 = QQ'$. This gives us

$$\beta = \frac{P' + \sqrt{D}}{Q'}$$

where indeed $Q' | \big(D - (P')^2\big)$, of the same form as in $(*)$, and the process can be continued. □

In order to avoid cumbersome multi-name labels and sticky historic issues I will simply call this algorithm QCF, Q as in “quadratic”.

Special Case $\alpha_0 = \sqrt{D}$

Let $\alpha_0 = \sqrt{D}$, D not a perfect square.

Reintroducing our old notation, we may write

$$\alpha_j = \frac{P_j + \sqrt{D}}{Q_j} \text{ where } Q_j | (D - P_j^2),$$

starting with

$$P_0 = 0, \quad Q_0 = 1.$$

Putting $n = a_j = \lfloor \alpha_j \rfloor$, the computations above yield

$$\alpha_{j+1} = \frac{P_{j+1} + \sqrt{D}}{Q_{j+1}},$$

where

$$P_{j+1} = a_j Q_j - P_j \text{ and } D - P_{j+1}^2 = Q_j Q_{j+1}.$$

.

This gives a recurrence for computing α_j, a_j and P_j, Q_j.

We recall our old recurrence for the convergents:

$$\frac{p_0}{q_0} = a_0 = \lfloor \alpha_0 \rfloor, \quad \frac{p_1}{q_1} = \frac{1 + a_0 a_1}{a_1},$$

$$\frac{p_{j+1}}{q_{j+1}} = \frac{a_{j+1} p_j + p_{j-1}}{a_{j+1} q_j + q_{j-1}}, \quad j \geq 1.$$

Remark: From

$$Q_j \cdot Q_{j+1} = D - P_{j+1}^2, \qquad Q_j \cdot Q_{j-1} = D - P_j^2$$

we immediately see

$$(Q_{j+1} - Q_{j-1}) Q_j = P_j^2 - P_{j+1}^2 = (P_{j+1} + P_j)(P_j - P_{j+1}).$$

Here $P_{j+1} = a_j Q_j - P_j$, $P_{j+1} + P_j = a_j Q_j$.

So dividing by Q_j, and transposing terms, we arrive at

$$Q_{j+1} = Q_{j-1} + a_j (P_j - P_{j+1}).$$

This means that we can avoid division at the cost of a second-order recurrence, as for the p_j, q_j. It is then natural to extend the definition of the Q one step backwards: $Q_{-1} = D$, which is consistent with the recurrence (check!). This device cuts a few percent off the running time.

A computer program will start by initializing P_0; Q_{-1}, Q_0; a_0; p_{-1}, p_0; q_{-1}, q_0. The update order is P, Q, a, p, q. Note, for instance, that the update for Q involves the updated value of P.

We will need a simple (rational) way of computing the floors of the α_j.

H.I.3 Theorem. *If $Q > 0$, setting $m = \lfloor\sqrt{D}\rfloor$, the floor of our quadratic irrationality is given by*

$$\left\lfloor\frac{P+\sqrt{D}}{Q}\right\rfloor = \left\lfloor\frac{P+m}{Q}\right\rfloor.$$

If $Q < 0$,

$$\left\lfloor\frac{P+\sqrt{D}}{Q}\right\rfloor = \left\lfloor\frac{P+m+1}{Q}\right\rfloor.$$

Proof. The integer m is given by the requirement

$$m < \sqrt{D} < m+1.$$

Assuming that $Q > 0$, we have

$$\frac{P+m}{Q} < \frac{P+\sqrt{D}}{Q}.$$

There can be no integer strictly between the two members. Indeed, assuming

$$\frac{P+m}{Q} < n < \frac{P+\sqrt{D}}{Q}$$

would lead to

$$m < Qn - P < \sqrt{D}.$$

But there is no integer strictly between the outer members, as $m = \lfloor\sqrt{D}\rfloor$.

Therefore the quadratic irrationalities

$$\frac{P+\sqrt{D}}{Q}, \quad \frac{P+m}{Q},$$

have the same floor, completing the case $Q > 0$.

If $Q < 0$, dividing the inequality $P + m + 1 > P + \sqrt{D}$ by Q reverses it:

$$\frac{P+m+1}{Q} < \frac{P+\sqrt{D}}{Q}.$$

If there were an integer n between the two members, we would get the inequality

$$m+1 > Qn - P > \sqrt{D},$$

which again is impossible. □

H.II Conjugates

We have encountered irrationalities of the form

$$\alpha = p + q\sqrt{D},$$

where p, q are rational and D is a positive integer, not a perfect square. Alongside α we will have to study its *conjugate*

$$\alpha' = p - q\sqrt{D}.$$

(earlier we used the prime for complex conjugation).

It is easy to see that

$$\alpha \cdot \alpha' = p^2 - q^2 D,$$

so that the product of α and its conjugate is *rational.*

If α is rational, i.e., $q = 0$, then $\alpha = \alpha'$, and conversely.

It is easy to prove the laws

$$(\alpha + \beta)' = \alpha' + \beta'$$

$$(\alpha \cdot \beta)' = \alpha' \cdot \beta',$$

and

$$(c\alpha)' = c \cdot \alpha' \quad \text{for rational c},$$

not to mention

$$\alpha'' = \alpha.$$

Simply expand the two members.

We also sometimes need to take the conjugate of a quotient:

$$(\frac{\alpha}{\beta})' = \frac{\alpha'}{\beta'}.$$

This relation is trivially true if the denominator is rational. The general proof runs like this:

$$(\frac{\alpha}{\beta})' = (\frac{\alpha \cdot \beta'}{\beta \cdot \beta'})' = \frac{\alpha' \cdot \beta''}{\beta \cdot \beta'} = \frac{\alpha' \cdot \beta}{\beta \cdot \beta'} = \frac{\alpha'}{\beta'}.$$

Note that multiplying the numerator and denominator by the conjugate of the latter produced a rational denominator.

One important consequence is the following: If α satisfies a quadratic equation with rational coefficients, then α' must satisfy the same equation. We see this by conjugating the equation, and using the laws above.

We will make repeated use of the following observation.

Let $\alpha = p+q\sqrt{D}$, p, q integers, and suppose $\alpha \cdot \alpha' = p^2 - Dq^2 = M$. Similarly, let $\beta = r + s\sqrt{D}$, satisfying $\beta \cdot \beta' = r^2 - Ds^2 = N$.

Then the product $\gamma = \alpha \cdot \beta = u + v\sqrt{D}$ satisfies $u^2 - Dv^2 = \gamma \cdot \gamma' = (\alpha\beta)(\alpha\beta)' = \alpha\alpha'\beta\beta' = MN$.

H.III $x^2 - Dy^2 = \pm 1$

We will show that Pell’s Equation $x^2 - Dy^2 = \pm 1$ ($D > 0$ not a perfect square) has the solution $x = p_k$, $y = q_k$ where p_k/q_k is a convergent to $\alpha = \sqrt{D}$.

Using the QCF (Section H.I) we will be able to find a convergent with that property *without* computing $p_k^2 - Dq_k^2$.

In the last two Sections, we will prove, in the case of $\alpha_0 = \sqrt{D}$, that there is an $m > 0$ such that

$$\alpha_{m+2} = \frac{1}{\alpha_{m+1} - a_{m+1}} = \frac{1}{\alpha_0 - a_0} = \alpha_1$$

(it will presently be revealed why we use $m + 1$ for the period). That is,

$$\alpha_{m+1} - a_{m+1} = \alpha_0 - a_0.$$

We then see that $\alpha_{m+1} - \alpha_0 = \alpha_{m+1} - \sqrt{D}$ is an integer, namely $a_{m+1} - a_0$. We therefore set $\alpha_{m+1} = \alpha_0 + n = \sqrt{D} + n$.

As shown in the same Section, the conjugate $\alpha'_{m+1} = n - \sqrt{D}$ will satisfy

$$-1 < \alpha'_{m+1} < 0.$$

For this value of l, it must then hold that $\alpha_{m+1} = \alpha_0 + a_0 = \sqrt{D} + \lfloor\sqrt{D}\rfloor$, i.e., $P_{m+1} = n = \lfloor\sqrt{D}\rfloor, Q_{m+1} = 1$.

By our general formulas,

$$\sqrt{D} = \frac{p_m\alpha_{m+1} + p_{m-1}}{q_k\alpha_{m+1} + q_{m-1}} = \frac{p_m\sqrt{D} + (p_{m-1} + np_m)}{q_m\sqrt{D} + (q_{m-1} + nq_m)}.$$

The equation above is of the following form

$$\sqrt{D} = \frac{p\sqrt{D} + q}{r\sqrt{D} + s},$$

where

$$ps - qr = p_m q_{m-1} - p_{m-1}q_m = (-1)^{m+1}.$$

From

$$\sqrt{D}(r\sqrt{D} + s) = p\sqrt{D} + q;$$
$$(p - s)\sqrt{D} = rD - q,$$

we identify:

$$p = s,\ q = rD,$$

otherwise $\sqrt{D}$ would be rational.

We conclude:

$$(-1)^{m+1} = p^2 - Dr^2,$$

proving:

H.III.1 Theorem. *The equation $x^2 - Dy^2 = \pm 1$ is solvable in integers $x, y > 0$, for at least one sign, and a solution is given by $x = p_m y = q_m$, where p_m/q_m is a convergent to $\sqrt{D}$. If the period $m+1$ is odd, then the equation $x^2 - Dy^2 = -1$ is solvable in positive integers x, y.*

□

Now if $x^2 - Dy^2 = (x - y\sqrt{D})(x + y\sqrt{D}) = -1$ and $u + v\sqrt{D} = (x + y\sqrt{D})^2$ we see easily that $u^2 - Dv^2 = (x + y\sqrt{D})^2(x - y\sqrt{D})^2 = (-1)^2 = 1$. We have proved:

H.III.2 Theorem. *The equation $x^2 - Dy^2 = 1$ is solvable in integers $x, y > 0$, and the solution is given by $x = p_m$, $y = q_m$, where p_m/q_m is a convergent to $\sqrt{D}$.*

□

The fact that a solution is given by a convergent was proved in the Section on "Best Approximation" (G.IV).

Remark: The use of the "QCF" in solving Pell's equation is implicit in the work of the two Englishmen John Wallis (1616-1703) and William Brouncker (1620-1684).

A method similar to theirs was known to the Indian mathematician Bhaskara in the 12th century. It produces essentially the same calculations with a few shortcuts along the way. A clear exposition of the two methods and their relationship is given on pp. 25-36, in Edwards' book, listed under "Historic" in the Bibliography. That the "English method" actually works was proved by Lagrange in 1769.

I am grateful to J White of the Australian National University for clearing up some of the history.

The equation having -1 as right member need not be solvable. It is obviously not solvable if -1 is a quadratic non-residue modulo D, e.g., if D has a prime factor $p \equiv 3 \pmod 4$. It *is* solvable if $D =$ prime $p \equiv 1 \pmod 4$ but that is far from trivial (see the exercises).

By the same method of proof we show the general identity:

H.III.3 Theorem.

$$(-1)^{k+1} Q_{k+1} = p_k^2 - D q_k^2.$$

Remark: A moment's reflection will make it clear that the period $l = m + 1$ marks the *first appearance* of the denominator $Q_l = 1$. Hence the following converse to the previous result H.III.1.

H.III.4 Corollary. *If the period of* $\sqrt{D}$ *is even, the equation* $x^2 - Dy^2 = -1$ *has no integer solutions.*

□

Let us prove the Theorem.

Proof. Once again we start from the identity

$$\sqrt{D} = \frac{p_k \alpha_{k+1} + p_{k-1}}{q_k \alpha_{k+1} + q_{k-1}},$$

where we substitute

$$\alpha_{k+1} = \frac{P_{k+1} + \sqrt{D}}{Q_{k+1}},$$

obtaining

$$\sqrt{D} = \frac{p_k(P_{k+1} + \sqrt{D}) + p_{k-1}Q_{k+1}}{q_k(P_{k+1} + \sqrt{D}) + q_{k-1}Q_{k+1}}.$$

Multiplying up the denominators gives:

$$\sqrt{D} \cdot (q_k(P_{k+1} + \sqrt{D}) + q_{k-1}Q_{k+1}) = p_k(P_{k+1} + \sqrt{D}) + p_{k-1}Q_{k+1}.$$

By a similar identification as in the previous proof,

$$\begin{aligned} p_k &= q_k P_{k+1} + q_{k-1}Q_{k+1} \\ Dq_k &= p_k P_{k+1} + p_{k-1}Q_{k+1} \end{aligned}$$

We eliminate P_{k+1} multiplying the first equation by p_k, and the second by $-q_k$, and adding:

$$p_k^2 - Dq_k^2 = (p_k q_{k-1} - q_k p_{k-1})Q_{k+1} = (-1)^{k+1}Q_{k+1}.$$

□

The condition for terminating the algorithm in solving the equation $x^2 - Dy^2 = \pm 1$, therefore, is $Q_{k+1} = 1$. For the equation $x^2 - Dy^2 = 1$ the condition is $Q_{k+1} = (-1)^{k+1}$ (or just ±1).

In the next Section we will prove that the Q_k remain of moderate size, which is an important point. That is also the idea behind the use of continued fractions in factorization.

H.III.5 Example (A Computation). Take $D = 14$, whose expansion we determined in the previous Chapter.

$$\begin{aligned}
\sqrt{14} &= 3 + (\sqrt{14} - 3)\\
\frac{1}{\sqrt{14}-3} &= \frac{\sqrt{14}+3}{5} = 1 + \frac{\sqrt{14}-2}{5}\\
\frac{5}{\sqrt{14}-2} &= \frac{\sqrt{14}+2}{2} = 2 + \frac{\sqrt{14}-2}{2}\\
\frac{2}{\sqrt{14}-2} &= \frac{\sqrt{14}+2}{5} = 1 + \frac{\sqrt{14}-3}{5}\\
\frac{5}{\sqrt{14}-3} &= \sqrt{14}+3 = 6 + (\sqrt{14}-3)
\end{aligned}$$

From the middle members we read off the P_k, Q_k; the rightmost members give the a_k.

We verify that this is in tune with the QCF.

$$\begin{aligned}
&P_0 = 0, & Q_0 &= 1; & a_0 &= \lfloor\sqrt{14}\rfloor = 3\\
&P_1 = 3\cdot 1 - 0 = 3, & Q_1 &= (14-3^2)/1 = 5; & a_1 &= \left\lfloor\frac{3+\lfloor\sqrt{14}\rfloor}{5}\right\rfloor = 1\\
&P_2 = 1\cdot 5 - 3 = 2, & Q_2 &= (14-2^2)/5 = 2; & a_2 &= \left\lfloor\frac{2+\lfloor\sqrt{14}\rfloor}{2}\right\rfloor = 2\\
&P_3 = 2\cdot 2 - 2 = 2, & Q_3 &= (14-2^2)/2 = 5; & a_3 &= \left\lfloor\frac{2+\lfloor\sqrt{14}\rfloor}{5}\right\rfloor = 1\\
&P_4 = 1\cdot 5 - 2 = 3, & Q_4 &= (14-3^2)/5 = 1; & a_4 &= \left\lfloor\frac{3+\lfloor\sqrt{14}\rfloor}{1}\right\rfloor = 6
\end{aligned}$$

From the usual recurrence

$$p_k = a_k p_{k-1} + p_{k-2}, \quad q_k = a_k q_{k-1} + q_{k-2}, \quad k \geq 1,$$

$$p_{-1} = 1, q_{-1} = 0, \quad p_0 = a_0, \quad q_0 = 1,$$

we then get the following table:

k	-1	0	1	2	3
p_k	1	3	4	11	$\underline{15}$
q_k	0	1	1	3	$\underline{4}$
P_{k+1}	0	3	2	2	3
$(-1)^{k+1}Q_{k+1}$	1	-5	2	-5	$\underline{1}$
a_{k+1}	3	1	2	1	6

□

From the last column we read off $15^2 - 14 \cdot 4^2 = 1$. This may be written

$$(15 + 4\sqrt{14})(15 - 4\sqrt{14}) = 1,$$

and $x + y\sqrt{14} = 15 + 4\sqrt{14}$ is known as the *least positive solution* to

$$(x + y\sqrt{14})(x - y\sqrt{14}) = 1.$$

That solution is defined as the least irrationality $x+y\sqrt{D}$, $x, y \in \mathbf{Z}$, for which $x^2 - Dy^2 = 1, \quad x, y > 0$. It can also be characterized as the least $x+y\sqrt{D} > 1$ for which $x^2 - Dy^2 = 1$.

All other solutions are plus or minus integral (positive or negative) powers of that solution. This will result from the following Theorem:

H.III.6 Theorem. *Let $x_0 + y_0\sqrt{D}$, $x, y \in \mathbf{Z}$, be minimal among numbers $x_0 + y_0\sqrt{D} > 1$ satisfying $x_0^2 - Dy_0^2 = 1$. Let further $x + y\sqrt{D} > 1$ be an arbitrary solution of the equation $x^2 - Dy^2 = 1$. Then there is an integer $k > 0$ such that*

$$x + y\sqrt{D} = (x_0 + y_0\sqrt{D})^k.$$

Proof. Let us deal with existence first. Any solution $z = x + y\sqrt{D} > 1$ must satisfy $y > 0$, as the inverse quantity, $1/z = x - y\sqrt{D}$ is < 1. And, as $x - y\sqrt{D} > 0$ we must also have $x > 0$.

Further, $x^2 - Dy^2 = 1$ entails x, y relatively prime. We have proved (G.IV.4) that $x/y =$ some convergent p_k/q_k. As the p_k, q_k increase with k, there must be a smallest $p_k + q_k\sqrt{D}$ satisfying $p_k^2 - Dq_k^2 = 1$.

Now assume that the statement of the Theorem is false. Then there would be a $k \geq 0$ such that:

$$(x_0 + y_0\sqrt{D})^k < x + y\sqrt{D} < (x_0 + y_0\sqrt{D})^{k+1},$$

whence

$$1 < (x + y\sqrt{D})(x_0 - y_0\sqrt{D})^k < x_0 + y_0\sqrt{D}$$

(recall that $(x_0 - y_0\sqrt{D})(x_0 + y_0\sqrt{D}) = 1$).

Setting $u + v\sqrt{D} = (x + y\sqrt{D})(x_0 - y_0\sqrt{D})^k$ we would then get

$$\begin{aligned} u^2 - Dv^2 &= (u + v\sqrt{D})(u - v\sqrt{D}) \\ &= (x + y\sqrt{D})(x_0 - y_0\sqrt{D})^k(x - y\sqrt{D})(x_0 + y_0\sqrt{D})^k \\ &= 1 \end{aligned}$$

contrary to the choice (minimality) of $x_0 + y_0\sqrt{D}$. □

A solution $0 < x + y\sqrt{D} < 1$ is the inverse to the solution $1 < x - y\sqrt{D}$, a positive power of $x_0 + y_0\sqrt{D}$. So $x + y\sqrt{D}$ is a negative power of $x_0 + y_0\sqrt{D}$.

And a negative solution is the negative of a positive solution.

H.III.7 Example. We now give a more impressive example, $D = 29$, but omit the computations.

k	-1	0	1	2	3	4
p_k	1	5	11	16	27	$\underline{70}$
q_k	0	1	2	3	5	$\underline{13}$
P_{k+1}	0	5	3	2	3	5
$(-1)^{k+1}Q_{k+1}$	1	-4	5	-5	4	$\underline{-1}$
a_{k+1}	5	2	1	1	2	10

We obtain $70^2 - 29 \cdot 13^2 = -1$ with $70 + 13\sqrt{29}$ as least positive solution. According to a general result (see below) squaring it gives the least positive solution to $x^2 - 29 \cdot y^2 = 1$. The square is:

$$(70 + 13\sqrt{29})^2 = 9801 + 1820\sqrt{29}$$

so that

$$9801^2 - 29 \cdot 1820^2 = 1$$

(corresponding to $Q_{10} = 1$).

What happens, quite generally, when we move one period (five steps) forward is that the elements $p_{j+5} + q_{j+5}\sqrt{29}$ arise by multiplying $p_j + q_j\sqrt{29}$ by $70 + 13\sqrt{29}$.

We will prove this fact in a later Section (J.VII).

For instance, $p_0^2 - 29 \cdot q_0^2 = -4$, where $p_0 + q_0\sqrt{29} = 5 + 1 \cdot \sqrt{29}$.

Hence $p_5 + q_5\sqrt{29} = (5 + 1 \cdot \sqrt{29})(70 + 13\sqrt{29}) = 727 + 135 \cdot \sqrt{29}$. with

$$727^2 - 29 \cdot 135^2 = +4 = (-1) \cdot (-4)$$

The table above verifies this claim:

$$p_5 = a_5 p_4 + p_3 = 10 \cdot 70 + 27 = 727;$$

$$q_5 = a_5 q_4 + q_3 = 10 \cdot 13 + 5 = 135.$$

□

We conclude this Section with an extension of our Theorem on solutions to $x^2 - Dy^2 = 1$

H.III.8 Theorem. *Assume that D is not a perfect square, and that the Diophantine equation $x^2 - Dy^2 = -1$ is solvable. Let $z_0 = x_0 + y_0\sqrt{D}$ be the smallest solution > 1 to that equation, and $z_1 = x_1 + y_1\sqrt{D}$ the smallest solution > 1 to $x^2 - Dy^2 = 1$. Then $z_1 = z_0^2$.*

Proof. The fact that $x_0, y_0 > 1$, and the existence of a minimal solution, are proved much in the same manner as the previous case.

Now, let us first prove that $z_0 < z_1$. Assume the contrary:

$$x_0 + y_0\sqrt{D} > x_1 + y_1\sqrt{D}.$$

Multiplying by the (positive) inverse quantity $1/z_1 = x_1 - y_1\sqrt{D} < 1$ yields

$$x_0 + y_0\sqrt{D} > u + v\sqrt{D} = (x_0 + y_0\sqrt{D})(x_1 - y_1\sqrt{D}) > x_1^2 - Dy_1^2 = 1$$

satisfying $u^2 - Dv^2 = -1$, contradicting the choice of z_0.

Next, assume

$$z_0^2 = (x_0 + y_0\sqrt{D})^2 > x_1 + y_1\sqrt{D} = z_1 > x_0 + y_0\sqrt{D}.$$

We derive a contradiction by multiplying by the inverse quantity $1 > 1/z_0 = -x_0 + y_0\sqrt{D} > 0$:

$$x_0 + y_0\sqrt{D} > (x_1 + y_1\sqrt{D})(-x_0 + y_0\sqrt{D}) = u + v\sqrt{D} > 1,$$

with $u^2 - Dv^2 = -1$, contradicting the choice of z_0. This contradiction proves that the first inequality is false.

And equality is then the only possibility; otherwise $z_0^2 = s + t\sqrt{D} < z_1$ would satisfy $s^2 - Dt^2 = 1$, contradicting the choice of z_1. □

Combining the last two Theorems we derive the following Corollary:

H.III.9 Corollary. *Suppose the equation $x^2 - Dy^2 = -1$, $D > 0$ not a square, is solvable in positive integers. Let $x_0 + y_0\sqrt{D}$ be the smallest solution > 1 to that equation. Then the solutions $x + y\sqrt{D} > 1$ are given by the odd positive powers of that quantity. And the solutions $x + y\sqrt{D} > 1$ to $x^2 - dy^2 = 1$ are given by the even powers.*

□

H.III: Exercises

1. Show that -1 is a quadratic residue modulo 34, but that the equation $x^2 - 34y^2 = -1$ is unsolvable in integers,

   (a) by determining the (short) period of the expansion of $\sqrt{34}$, and/or

   (b) by reduction modulo 8.

2. Give all integer solutions to the equation $x^2 - 10y^2 = -1$. Then use the result to describe the solutions to the equation $4x^2 + 4xy - 9y^2 = -1$. What needs to be established about the solutions to the first equation?

3. Suppose that $D = 4d + 1$, positive, not a perfect square. Consider the continued fractions expansion of $(\sqrt{D} + 1)/2$. Suppose

$$\alpha_l = \frac{\sqrt{D} + P_l}{Q_l}.$$

Show that Q_l is even, and that

$$p^2 - pr + dr^2 = \pm Q_l/2,$$

where p/r is a convergent to D.

4. D, k positive integers, D not a perfect square. Let $p + q\sqrt{n}$ be minimal among those $p + q\sqrt{n} > \sqrt{k}$, $p, q \in \mathbf{Z}$ satisfying the equation $p^2 - nq^2 = k$. Show that p, q are positive. Hint: consider $p - q\sqrt{n}$.

5. Suppose x, y, both odd , satisfy the equation $x^2 - dy^2 = \pm 4$. Define the rational numbers u, v by:

$$u + v\sqrt{d} = (\frac{x + y\sqrt{d}}{2})^3.$$

Show that u, v are *integers* satisfying the equation $u^2 - dv^2 = \pm 1$.

6. (a) Give the continued fractions expansions of $a = \sqrt{d^2 \pm 1}$, $d \in \mathbf{Z}$. Give examples of both kinds.

(b) Determine the least positive solution of Pell's equation $x^2 - ny^2 = 1$, where $n = d^2 + 2$.

7. (a) Find, by inspection, the least positive solution to $x^2 - 13y^2 = -1$. (Start by finding the class of x modulo 13.) Use it to find the least positive solution to $x^2 - 13y^2 = +1$.

(b) Find, by inspection, the least positive solution to $x^2 - 30y^2 = 1$. Use it to decide whether $x^2 - 30y^2 = -1$ is solvable.

8. (a) Show that the arithmetic sum $1 + 2 + 3 + \cdots + n$ is a perfect square for infinitely many n. Reduce the question to the solvability of a suitable Pellian equation.

(b) Show the same for the sums $1+2+3+\cdots+2n$ and $1+2+3+\cdots+2n+1$.

9. D is a positive integer, not a perfect square. Let $x_n + y_n\sqrt{d} > 1$ be the positive solutions (i.e., $x_n, y_n > 0$) to the equation $x^2 - dy^2 = 1$. Let p be an arbitrary positive integer. Show that there exists an integer n such that $p | y_n$.

Hint: imitate the theory of order for invertible classes. Or reduce to some other Pellian equation.

10. Let $p \equiv 1 \pmod 4$ be a prime number. We want to show that the equation $x^2 - py^2 = -1$ is solvable in integers. Our starting point is the least positive solution (t, u) to $t^2 - pu^2 = 1$. Show first that t is odd and u is even.

Then show that one of the following two cases holds:

$$\frac{t+1}{2} = pa^2, \qquad \frac{t-1}{2} = b^2,$$

or

$$\frac{t+1}{2} = a^2, \qquad \frac{t-1}{2} = pb^2.$$

Show that the second case leads to a solution to $x^2 - py^2 = 1$, contrary to the choice of (t, u).

Then deduce, using the first case, a solution to $x^2 - py^2 = -1$.

11. Use the techniques of the last Exercise to show that one of the equations $x^2 - py^2 = \pm 2$ is solvable if $p \equiv 3 \pmod 4$. Describe the cases corresponding to either sign.

12. D is an odd number (≥ 11, say) that we wish to factor, using its continued fractions expansion. Suppose we have found a convergent p/q, $\quad (p, q) = 1$, giving the equation $p^2 - Dq^2 = R^2$ where R is an integer:

$$Dq^2 = (p - R)(p + R), \quad D|(p - R)(p + R).$$

Suppose now that we face the failure of having $D|(p - R)$ (we can assume this, as we are not assuming that R is positive). Show that the explanation is the following:

(a) $\underline{q \text{ is odd.}}$ Show that $((p - R)/D, p + R) = 1$. Conclude that there are positive integers s, t, $(s, t) = 1$ such that

$$s^2 - Dt^2 = 2R,$$

and that s/t is an earlier convergent in the expansion of $\sqrt{D}$.

(b) $\underline{q \text{ is even.}}$ Show that $((p-R)/D, p+R) = 2$ and determine s, t as above, but with

$$s^2 - Dt^2 = R.$$

Also show that R is odd.

How do the numbers $p + q\sqrt{D}$ and $s + t\sqrt{D}$ relate to one another?

13. Suppose $|p_1 q_2 - p_2 q_1| = 1$, p_1, p_2, q_1, q_2 integers. Further assume

$$\frac{p_1}{q_1} < \alpha < \frac{p_2}{q_2},$$

where α is irrational. Show that one of the inequalities

$$\left|\alpha - \frac{p_1}{q_1}\right| < \frac{1}{2q_1^2}$$

or

$$\left|\alpha - \frac{p_2}{q_2}\right| < \frac{1}{2q_2^2}$$

must hold, so that one of the two fractions is a convergent to α.

Hint: Assume the reverse (non-strict) inequalities in both cases. Show, and use

$$\frac{p_2}{q_2} - \frac{p_1}{q_1} = \left|\alpha - \frac{p_2}{q_2}\right| + \left|\alpha - \frac{p_1}{q_1}\right|$$

and the inequality between the arithmetic and the geometric mean of two numbers.

H.IV $x^2 - Dy^2 = N$

The inquisitive reader will have asked about the relationship between two integer solutions to $x^2 - Dy^2 = N$; $Q = |N| > 1$ (still assuming that D is not a perfect square).

We restrict ourselves to *proper* solutions, satisfying $(x, y) = 1$, forcing $(y, Q) = 1$. In that case there is an integer u satisfying $yu \equiv 1 \pmod{Q}$, whence $(xu)^2 \equiv D \pmod{Q}$. Setting $P \equiv -xu \pmod{Q}$, $-Q/2 < P \leq Q/2$, we have $P^2 \equiv D \pmod{Q}$, and $x + Py \equiv 0 \pmod{Q}$.

Furthermore, $Px + Dy \equiv Px + P^2y \equiv P(x + Py) \equiv 0 \pmod{Q}$, hence

$$Px + Dy \equiv 0 \pmod{Q}.$$

Our findings can be put together like this:

$$(P + \sqrt{D})(x + y\sqrt{D}) \equiv 0 \pmod{Q}.$$

Note that the condition $P^2 \equiv D \pmod{Q}$ can be reconstructed from that relation as $y(P^2-D) \equiv P(Py+x)-(Px+Dy) \equiv 0 \pmod{Q}$, and $(y, Q) = 1$.

By our earlier terminology (p. 217), the solution (x, y) or $x + y\sqrt{D}$ *belongs to* P, satisfying $P^2 \equiv D \pmod{Q}$.

H.IV.1 Theorem. *Let* $\alpha_i = x_i + y_i\sqrt{D}$, $i = 1, 2$, *be solutions to*

$$x_i^2 - Dy_i^2 = \epsilon_i N, \quad \epsilon_i = \pm 1,$$

belonging to the same P. *Then their quotient* $u + v\sqrt{D}$ *is an integer solution to the equation* $u^2 - Dv^2 = \epsilon_1 \cdot \epsilon_2$.

Proof. Obviously $u + v\sqrt{D} = \gamma = \alpha_1/\alpha_2$ satisfies

$$\gamma \cdot \gamma' = (\alpha_1 \cdot \alpha_1')/(\alpha_2 \cdot \alpha_2') = \epsilon_1 N/\epsilon_2 N = \epsilon_1 \cdot \epsilon_2.$$

We must prove that u and v are *integers*.

Let us compute the quotient:

$$\begin{aligned}\frac{x_1 + y_1\sqrt{D}}{x_2 + y_2\sqrt{D}} &= \frac{(x_1 + y_1\sqrt{D})(x_2 - y_2\sqrt{D})}{(x_2 + y_2\sqrt{D})(x_2 - y_2\sqrt{D})} \\ &= \frac{(x_1x_2 - Dy_1y_2) + (x_2y_1 - x_1y_2)\sqrt{D}}{\epsilon_2 N}.\end{aligned}$$

Again setting $Q = |N|$ we must prove that

$$\begin{aligned}x_1x_2 - Dy_1y_2 &\equiv 0 \pmod{Q}, \\ x_2y_1 - x_1y_2 &\equiv 0 \pmod{Q}.\end{aligned}$$

This follows immediately on substituting $x_i \equiv Py_i \pmod{N}$, $i = 1, 2$, and $P^2 - D \equiv 0 \pmod{N}$, in the two left members above. □

Here is a simple converse:

H.IV.2 Theorem. *If $x_1 + y_1\sqrt{D}$ is a solution to the equation $x^2 - Dy^2 = N$, belonging to P, and $u + v\sqrt{D}$ is a solution to $u^2 - Dv^2 = \epsilon = \pm 1$, then their product $x_2 + y_2\sqrt{D}$ is a solution to $x^2 - Dy^2 = \epsilon \cdot N$,* belonging to *$P$.*

Proof. "Belonging" is the issue. However, $(P + \sqrt{D})(x_1 + y_1\sqrt{D}) \equiv 0 \pmod{Q}$ obviously implies

$$(P + \sqrt{D})(x_2 + y_2\sqrt{D}) \equiv (P + \sqrt{D})(x_1 + y_1\sqrt{D})(u + v\sqrt{D}) \equiv 0 \pmod{Q}.$$

□

H.IV.3 Example. The cleanest case is that of $N =$ a prime number p. In that case there are at most two values (modulo p) for P. To be explicit, let us study the equation

$$x^2 - 2y^2 = -17.$$

The solutions to $P^2 \equiv 2 \pmod{17}$ are $P \equiv \pm 6 \pmod{17}$. By simple trial and error we find the solution $x + y\sqrt{2} = 1 \pm 3\sqrt{2}$ belonging to $P = \mp 6$, as $1 - 3 \cdot 6 = -17$.

The general solution to $x^2 - 2y^2 = \pm 1$ is $\pm(1 + \sqrt{2})^m$, $m \in \mathbf{Z}$, so the general solution to $x^2 - 2y^2 = \pm 17$ is

$$x + y\sqrt{2} = \pm(1 \pm 3\sqrt{2}) \cdot (1 + \sqrt{2})^m, \quad m \in \mathbf{Z},$$

even powers giving the solutions to $x^2 - 2y^2 = -17$, odd powers giving those to $x^2 - 2y^2 = 17$. □

H.IV.4 Example. The two equations $x^2 - 34y^2 = \pm 33$ are both solvable in integers. $x + y\sqrt{34} = \pm(1 \pm 1 \cdot \sqrt{34})$ works for the minus sign, $x + y\sqrt{34} = \pm(13 \pm 2 \cdot \sqrt{34})$ does it for the plus sign.

Their quotient is *not* an integer solution to $x^2 - 34y^2 = -1$. In fact the latter equation is not solvable at all in integers as we have seen in an earlier exercise (p. 236). The reason is that the first set of solutions belongs to $P = \pm 1$ whereas the second set belongs to $P = \pm 10$:

$$(10 + \sqrt{34})(13 + 2\sqrt{34}) = 33(6 + 1\sqrt{34}) \equiv 0 \pmod{33}.$$

□

Obviously this case was possible because we had more than two square roots. By contrast we have the following result:

H.IV.5 Theorem. *Let p be a prime number, D a positive number, not a perfect square, not divisible by p. Suppose the two equations $x^2 - Dy^2 = \pm p$ are solvable in integers. Then so is the equation $x^2 - Dy^2 = -1$.*

Proof. Let $\pm P + (p)$ be the square roots of D modulo p – by Lagrange there are only two of them, as p is a prime number.

Let $x_1 + y_1\sqrt{D}$ satisfy $x_1^2 - Dy_1^2 = p$, and let $x_2 + y_2\sqrt{D}$ satisfy $x_2^2 - Dy_2^2 = -p$. They each belong to either P or $-P$. Possibly by changing the sign of one y_i we can arrange that both belong to the same P.

Then by the previous Theorem their quotient provides an integer solution to $x^2 - Dy^2 = -1$. □

Remark: The proof goes through also for odd prime powers p^k, as D still has only two square roots modulo p^k. If the right members are $\pm 2^k$, $k \geq 3$, the square roots of D are residue classes of the form $\pm P \pmod{2^{k-1}}$ (see p. 64). Following the proof above we will perhaps be left with a factor 2 in the denominator, producing a solution to $x^2 - Dy^2 = -2^2 = -4$ (check this).

If x, y are even, $(x/y)^2 - D(y/2)^2 = -1$. If x, y are odd, an earlier exercise (p. 237) shows that $u + v\sqrt{D} = ((x + y\sqrt{D})/2)^3$ is an integer solution to $u^2 - Dv^2 = -1$.

These results are contained in the work of Canadian mathematician Richard Mollin.

H.IV: Exercises

1. Complete the discussion (case $D = \pm 2^k$) of the last Remark.

2. Suppose $x+y\sqrt{D}$ is a solution to $x^2-Dy^2 = \pm Q$, $Q > 0$, belonging to P. Assume $Q > \sqrt{D}$ and $|P| \leq Q/2$. Using the relation $(P + \sqrt{D})(x + y\sqrt{D}) \equiv 0 \pmod{Q}$, construct a solution $u + v\sqrt{D}$ to $u^2 - Dv^2 = \pm Q'$, $Q' > 0$, also belonging to P, and with $Q' < Q$. Do you see the significance of this reduction?

3. Describe the solutions to the Diophantine equation $x^2-5y^2 = \pm 4$. Show that $y = \pm F_k$, the *Fibonacci numbers* given by the recurrence $F_{k+2} = F_{k+1} + F_k$, $k \geq 0$, $F_0 = 0, F_1 = 1$ (in many accounts they start with F_1.) Then express the corresponding x in terms of Fibonacci numbers.

H.V Inequalities

Still assuming $\alpha = \sqrt{D}$, we now fill the gap we left in Section H.III. We show some inequalities for the P, Q appearing in the QCF and conclude periodicity (from $k = 1$ on).

Alongside

$$\alpha_k = \frac{P_k + \sqrt{D}}{Q_k}$$

we will have to study its *conjugate*

$$\alpha'_k = \frac{P_k - \sqrt{D}}{Q_k}.$$

The α_k and their conjugates α'_k each satisfy a first-order recurrence (we are using our general result on conjugates of quotients):

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}; \quad \alpha'_{k+1} = \frac{1}{\alpha'_k - a_k}; \qquad \alpha_0 = \sqrt{D}, \quad \alpha'_0 = -\sqrt{D}.$$

Since $1 > \alpha_k - a_k > 0$ we immediately see $\alpha_{k+1} > 1$, i.e., $\alpha_k > 1$ for all $k \geq 1$.

As for the conjugates, an easy induction shows that all α'_k are negative. From this follows that the denominator of α'_{k+1} is < -1.

So $-1 < \alpha'_{k+1} < 0$. That is, we inductively see that $-1 < \alpha'_k < 0$ for all $k \geq 1$. Summing up:

$$\alpha_k \geq 1, \quad -1 < \alpha'_k < 0, \quad k \geq 1;$$

There is a name for these conditions. The quadratic irrationality α_k, $k \geq 1$, is *reduced* (more on that in H.VII.1).

From the inequality $0 < \alpha_k - \alpha'_k = 2\sqrt{D}/Q_k$ then emerges that all $Q_k > 0$.

Furthermore, $\alpha_k + \alpha'_k = 2P_k/Q_k > 0, k \geq 1$, yielding $P_k > 0, k \geq 1$.

From $\alpha'_k < 0$ then follows $P_k < \sqrt{D}$.

Finally, $\alpha_k = (P_k + \sqrt{D})/Q_k > 1$ gives $Q_k < 2\sqrt{D}$.

We have proved:

H.V.1 Theorem. *The P_k, Q_k appearing in the QCF for $\sqrt{D}$ satisfy the following inequalities:*

$$P_0 = 0, \quad 0 < P_k < \sqrt{D}, \quad k \geq 1,$$

and

$$0 < Q_k < 2\sqrt{D}, \quad k \geq 0.$$

□

Thus the right members of the equations $p_k^2 - Dq_k^2 = (-1)^{k+1}Q_{k+1}$ are of a smaller order of magnitude than D (not to mention p_k, q_k).

H.VI Periodicity

Since P_k, Q_k can only assume finitely many values, two of the α_j, say α_k, α_{k+l}, $l > 0$, must be the same. This immediately gives periodicity from α_k on. And that also means that their denominators, the Q_k, repeat periodically (eventually).

We now show that if periodicity occurs from $k+1 \geq 2$ on, it also occurs from k on. By backwards induction it then follows that the expansion of $\alpha_0 = \sqrt{D}$ is periodic from $k = 1$ on.

This is the idea. We know $\alpha_{k+1} = \alpha_{k+1+l}$, $l > 0$. If we can prove that α_k, $k \geq 1$, is *uniquely determined* by α_{k+1} (and the condition of being reduced), it will follow that we also must have $\alpha_k = \alpha_{k+l}$.

We conjugate and invert the recurrence for the α_k :

$$\alpha_k - a_k = \frac{1}{\alpha_{k+1}},$$

$$\alpha'_k - a_k = \frac{1}{\alpha'_{k+1}}; \quad a_k = -\frac{1}{\alpha'_{k+1}} + \alpha'_k.$$

Using $-1 < \alpha'_k < 0$, from the last displayed equation we get

$$-\frac{1}{\alpha'_{k+1}} - 1 < a_k < -\frac{1}{\alpha'_{k+1}}.$$

As a_k is an integer, it is uniquely determined by that condition.

From this then follows that

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}$$

is uniquely determined by α_{k+1}, as desired.

Rejoice!

H.VI: Exercises

1. **Suggestions for computing:** The obvious project is to write a QCF routine, solving $x^2 - Dy^2 = \pm 1$, and determining the period. It is nice to have later on for factoring, "wait-for-a square" (Section L.X).

   As a test of your program, letting $D = 1729$, decide whether $x^2 - Dy^2 = -1$ is solvable, and find the right member N of next smallest absolute value, for which $x^2 - Dy^2 = N$ is solvable. Finally, decide which of the equations $x^2 - Dy^2 = 4, 9, 16$ are solvable in relatively prime integers. You could also check the table at the end of the book.

* H.VII Periodicity, Continued

We now give the full truth on the periodicity issue for quadratic irrationalities.

We first show again that the expansion of a reduced irrationality is ultimately periodic. The proof is independent of the previous Section.

We then turn to general quadratic irrationalities. We prove that the irrationalities appearing in their expansions are ultimately reduced, hence that their expansions are ultimately periodic.

Finally we prove that the irrationality α is *reduced if and only if it its expansion is purely periodic.*

The immediate application is $\alpha = \sqrt{D}, D \geq 1$, as one easily sees that

$$\alpha_1 = \frac{1}{\sqrt{D} - \lfloor \sqrt{D} \rfloor}$$

is reduced.

First we recall the notation.

Given the positive irrationality $\alpha = \alpha_0$ the $\alpha_k, k \geq 1$, are recursively given by

$$a_k = \lfloor \alpha_k \rfloor, \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k}.$$

We now assume that α satisfies the quadratic equation

$$AX^2 - BX + C = 0,$$

with integer coefficients A, B, C, $A \cdot C \neq 0$, the *discriminant*, $d = B^2 - 4AC$, of which is positive, but not a perfect square. The roots of the equation are the conjugate irrationalities

$$\alpha, \alpha' = \frac{B \pm \sqrt{d}}{2A},$$

whose denominator $2A$ divides $d - B^2$. One can prove by induction that all the succeeding α_k are of the same form (cf. the beginning of this Chapter).

We denote the larger root by α, the smaller one by α'. Which is which depends on the sign of A.

Remark: In our old notation

$$X = \alpha_k = \frac{P_k + \sqrt{D}}{Q_k}, \qquad D - P_k^2 = Q_k Q_{k+1}.$$

The quantity α_k is seen to satisfy the equation

$$(Q_k X - P_k)^2 - D = 0, \quad Q_k^2 X^2 - 2P_k Q_k X - (D - P_k^2) = 0$$

which simplifies to $Q_k X^2 - 2P_k X - Q_{k+1} = 0$, by the identities above. Its discriminant is $d = 4P_k^2 + 4Q_k Q_{k+1} = 4D$.

We spell out the relationship between the roots and the coefficients of the equation $AX^2 - BX + C = 0$:

$$\alpha \cdot \alpha' = \frac{C}{A}, \quad \alpha + \alpha' = \frac{B}{A}.$$

Let us recall the definition of "reduced".

H.VII.1 Definition. The quadratic irrationality α is **reduced** if

$$\alpha > 1, \quad 0 > \alpha' > -1.$$

We record a few observations in the following Lemma. Most of the proofs are easy exercises.

H.VII.2 Lemma.

a) α is reduced if and only if $-1/\alpha'$ is.

b) If α is reduced, then the same holds for

$$\beta = \frac{1}{\alpha - \lfloor \alpha \rfloor}.$$

So, if α_k is reduced, the same holds for all the succeeding α_j.

c) In fact,

$$\beta = \frac{1}{\alpha - n}$$

is reduced if and only if $n = \lfloor \alpha \rfloor$.

d) Suppose α is reduced, $\lfloor \alpha \rfloor = n$. If

$$\beta = \frac{1}{\alpha - n}$$

is the first step in the expansion of α, then

$$\frac{-1}{\alpha'} = \frac{1}{(-1/\beta') - n}$$

is the first step in the expansion of $-1/\beta'$.

e) Assume α reduced. The product of the roots, $\alpha \cdot \alpha'$, being equal to C/A, and negative, implies that A, C are of opposite sign, i.e., $AC < 0$.

Proof. We prove d). The second equation is easily derived from the first, solving for α, and then conjugating:

$$\begin{aligned} \alpha &= n + \frac{1}{\beta} \\ \frac{1}{\alpha} &= \frac{1}{n + \frac{1}{\beta}} \\ \frac{-1}{\alpha'} &= \frac{1}{-n + (\frac{-1}{\beta'})}. \end{aligned}$$

The main issue is that the floor of $-1/\beta'$ also equals n. We have seen that

$$-\frac{1}{\beta'} = -\alpha' + n.$$

As $0 > \alpha' > -1$ this proves that

$$n < -\frac{1}{\beta'} < n + 1.$$

□

Our next observation requires a more detailed proof:

H.VII.3 Lemma. *Assuming α reduced, and A, B, C, d as above, it holds that*

$$|A| + |C| < \sqrt{d}.$$

Proof. The following inequality,

$$(\alpha - 1)(\alpha' + 1) > 0,$$

is immediately clear from the definition.

The expressions for α, α' yield

$$\alpha - \alpha' = \frac{\sqrt{d}}{|A|}.$$

Expanding the inequality therefore gives

$$0 < \alpha \cdot \alpha' + \alpha - \alpha' - 1 = \frac{C}{A} + \frac{\sqrt{d}}{|A|} - 1.$$

The coefficients A, C being of opposite sign, we have $-C/A = |C|/|A|$, whence

$$1 + \frac{|C|}{|A|} = 1 - \frac{C}{A} < \frac{\sqrt{d}}{|A|},$$

and the result follows. □

Remark: In our old notation, the Lemma states that $Q_k + Q_{k-1} < \sqrt{d} = 2\sqrt{D}$.

The following Lemma helps us put everything together.

H.VII.4 Lemma. *Suppose α is reduced, and satisfies the quadratic equation*

$$AX^2 - BX + C = 0$$

with discriminant $d > 0$. Then $\beta = 1/(\alpha - \lfloor \alpha \rfloor)$ satisifies a quadratic equation

$$A'X^2 - B'X + C' = 0$$

having the same discriminant.

Proof. The proof is pure computation.

Let us set $n = \lfloor \alpha \rfloor$ and invert the relation above:

$$\alpha = n + \frac{1}{\beta}.$$

We plug this into the equation:

$$A(n + \frac{1}{\beta})^2 - B(n + \frac{1}{\beta}) + C = 0.$$

Multiplying by β^2 we obtain the equation

$$(An^2 - Bn + C)\beta^2 + (2An - B)\beta + A = 0,$$

of discriminant

$$d' = (2An - B)^2 - 4(An^2 - Bn + C) \cdot A = \cdots = B^2 - 4AC = d.$$

□

We can now state and prove the weaker form of our principal result:

H.VII.5 Theorem (Provisional). *Assume the quadratic irrationality α reduced. Then its continued fractions expansion is ultimately periodic.*

Proof. By our Lemmas, each α_k is reduced, satisfying a quadratic equation

$$Ax^2 - Bx + C = 0$$

with integer coefficients, and of the same discriminant d.

The coefficients A, B, C satisy the following inequalities:

$$|A| + |C| < \sqrt{d}; \quad d = B^2 - 4AC.$$

There can be only a finite number of pairs A, C satisfying that condition. For each pair A, C there are at most two integers B satisfying $B^2 - 4AC = d$.

Hence there are only a finite number of α_k and a_k appearing in the expansion of α. For some $k \geq 0$, $l > 0$ it must then hold that $\alpha_{k+l} = \alpha_k$. But then automatically $\alpha_{n+l} = \alpha_n$ for all $n \geq k$.

This proves the Theorem in the stated weaker form. □

We now show how the general case can be reduced to the case of a reduced irrationality α.

H.VII.6 Theorem. *If α is a quadratic irrationality, its continued fractions expansion is ultimately periodic.*

Proof. We prove that one α_j is reduced; we are then back in the situation ot the preceding Theorem.

The construction makes it clear that $\alpha_k > 1$ for all $k \geq 1$. We are finished if we can prove that some α'_k is negative, because then:

$$\alpha_{k+1} = \frac{1}{\alpha_k - \lfloor \alpha_k \rfloor} > 1, \quad 0 > \alpha'_{k+1} = \frac{1}{\alpha'_k - \lfloor \alpha_k \rfloor} > -1,$$

i.e., α_{k+1} is reduced.

Now, if α_k, α'_k are both positive, they are the roots of an equation

$$AX^2 - BX + C = 0,$$

where A and C are of equal sign, $AC > 0$, as the product of the two roots, C/A, is positive.

Putting $n = \lfloor \alpha_k \rfloor$ then gives

$$\alpha_k = \frac{B + \sqrt{d}}{2A} > n.$$

We are assuming

$$\alpha'_k = \frac{B-\sqrt{d}}{2A} > 0.$$

Summing the two inequalities we then get

$$\frac{B}{A} > n; \quad \frac{AB}{A^2} > n; \quad A(An-B) < 0.$$

We saw above that

$$\alpha_{k+1} = \frac{1}{\alpha_k - \lfloor \alpha_k \rfloor}, \quad \alpha'_{k+1} = \frac{1}{\alpha'_k - \lfloor \alpha_k \rfloor}$$

satisfy the quadratic equation $A'X^2 + B'X + C' = 0$, where

$$\begin{aligned} A' &= An^2 - Bn + C \\ B' &= 2An - B \\ C' &= A \end{aligned}$$

(recall $n = \lfloor \alpha_k \rfloor \geq 1$, $k \geq 1$).

The product of the first and third coefficients of *this* equation then equals

$$A^2n^2 - ABn + AC = AC + An(An-B) < AC,$$

as $n > 0$ and $A(An-B) < 0$.

As long as this product is positive it will therefore diminish by at least one unit in each step. It can never become zero, because in this case one of the roots would equal zero. But all the α_k, α'_k are irrational.

So, after a finite number of steps we must arrive at an equation $A''X^2 - B''X + C'' = 0$ where $A''C'' < 0$, and the product of the roots, C''/A'', is negative.

But then the smaller root must be negative. By the beginning of the proof, that is exactly what we had to prove. □

We now turn to the proof of the definitive Theorem on reduced irrationalities.

H.VII.7 Theorem. *The quadratic irrationality α has a purely periodic continued fractions expansion if and only if it is reduced.*

Proof.

α reduced necessary:

In the proof of the last Theorem we showed that the α_k are reduced from some $k = k_0$ on. However, if the sequence of the α_j is periodic from $k = 0$ on it must hold that α_0 is reduced. For if the period is $l > 0$, then for some multiple $nl > k_0$ we must have $\alpha_0 = \alpha_{nl}$, so that α_0 is reduced, as α_{nl} is.

α reduced sufficient:

We assume that α is reduced. We already know that the sequence of the α_j is ultimately periodic. We also know that they are all reduced.

So we can assume that some α_{k+1} has a purely periodic expansion.

We also know that

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}$$

is reduced.

Denoting the period by l, by assumption, $\alpha_{k+1+l} = \alpha_{k+1}$. If we can prove that $\alpha_{j+1+l} = \alpha_{j+1}$ implies $\alpha_{j+l} = \alpha_j$, we can show by backwards induction that $\alpha_0 = \alpha_l$, proving the Theorem.

The proof is the same as at the end of the preceding Section: α_j is uniquely determined by α_{j+1}, and the condition that α_j, too, is reduced. □

Chapter J

Special Topics on Continued Fractions

J.I Matrix Notation

In this Section we show how to rewrite some of our previous relations in *matrix form.* First we have the recursion for the convergents p_k/q_k:

$$\begin{pmatrix} q_{k+1} & q_k \\ p_{k+1} & p_k \end{pmatrix} = \begin{pmatrix} q_k & q_{k-1} \\ p_k & p_{k-1} \end{pmatrix} \begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix}, \quad k \geq 0.$$

We have the following initial condition:

$$\begin{pmatrix} q_0 & q_{-1} \\ p_0 & p_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a_0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Repeating we thus obtain:

$$\begin{pmatrix} q_{k+1} & q_k \\ p_{k+1} & p_k \end{pmatrix} = \begin{pmatrix} q_k & q_{k-1} \\ p_k & p_{k-1} \end{pmatrix} \begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix} =$$

$$\begin{pmatrix} q_{k-1} & q_{k-2} \\ p_{k-1} & p_{k-2} \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix} = \dots$$

$$\begin{pmatrix} q_0 & q_{-1} \\ p_0 & p_{-1} \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{k+1} & 1 \\ 1 & 0 \end{pmatrix}.$$

Replace k by $k-1$ in the first and last members above:

$$\begin{pmatrix} q_k & q_{k-1} \\ p_k & p_{k-1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Premultiplying both members by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

interchanges the rows of the left member and cancels the first matrix factor of the right member.

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \qquad (*)$$

The recurrence for the α_k,

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} \qquad (**)$$

may be inverted:

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}} = \frac{a_k \alpha_{k+1} + 1}{\alpha_{k+1}}$$

and rewritten as a matrix product:

$$\begin{pmatrix} \alpha_k \\ 1 \end{pmatrix} = C \cdot \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{k+1} \\ 1 \end{pmatrix}.$$

The constant $C = 1/\alpha_{k+1}$ cancels on dividing the two components.

By successive combination we thus obtain

$$\begin{aligned} \begin{pmatrix} \alpha \\ 1 \end{pmatrix} &= \begin{pmatrix} \alpha_0 \\ 1 \end{pmatrix} \\ &= C' \cdot \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_{k+1} \\ 1 \end{pmatrix} \\ &= C' \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} \begin{pmatrix} \alpha_{k+1} \\ 1 \end{pmatrix}, \end{aligned}$$

where we used (*). C' is again a constant that cancels on division.

So we have proved again that the recurrence (**) implies

$$\alpha = \frac{p_k \alpha_{k+1} + p_{k-1}}{q_k \alpha_{k+1} + q_{k-1}}.$$

We also see again that

$$\det \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}$$

as the matrix is the product of $k+1$ matrices of determinant $= -1$.

J.II Equivalent Quadratic Irrationalities

J.II.1 Definition. Given two quadratic irrationalities α, β, β is said to be **equivalent to** α if there are integers p, q, r, s, $ps - qr = \pm 1$ satisfying

$$\beta = \frac{p\alpha + q}{r\alpha + s}.$$

In view of the previous Section it is natural to think of the equivalence as given by the matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix},$$

$ps - qr = \pm 1$ being its determinant.

It is also given by the matrix

$$-\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

of the same determinant.

We now prove that ”equivalence” is indeed an equivalence relation!

It is trivially *reflexive*,

$$\alpha = \frac{1\alpha + 0}{0\alpha + 1}.$$

The proof of *symmetry* proceeds by inverting the above relation:

$$\alpha = \frac{s\beta - q}{-r\beta + p}$$

of the same determinant.

The matrix

$$\begin{pmatrix} s & -q \\ -r & p \end{pmatrix}$$

is plus or minus the inverse of the matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix},$$

depending on the sign of the determinant.

As for *transitivity* we rewrite the relation

$$\beta = \frac{p\alpha + q}{r\alpha + s},$$

in *matrix form*:

$$c \cdot \begin{pmatrix} \beta \\ 1 \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix}, \quad c \neq 0.$$

Assuming that γ is equivalent to β,

$$d \cdot \begin{pmatrix} \gamma \\ 1 \end{pmatrix} = \begin{pmatrix} t & u \\ v & w \end{pmatrix} \begin{pmatrix} \beta \\ 1 \end{pmatrix}, \quad d \neq 0,$$

we arrive at

$$dc \cdot \begin{pmatrix} \gamma \\ 1 \end{pmatrix} = \begin{pmatrix} t & u \\ v & w \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \end{pmatrix}, \quad cd \neq 0,$$

where the product matrix is of determinant plus or minus one, proving that γ is then equivalent to α.

J.III Equivalence and Continued Fractions

We have seen in the first and second Sections that two quadratic irrationalities that appear in the same continued fractions expansion are equivalent. We have also seen (H.VII.6, proof) that every quadratic irrationality is equivalent to a reduced one.

In this section we will prove that two reduced quadratic irrationalities are equivalent *if and only if* they appear in the same expansion. What remains to prove is "only if". We will be led to a non-symmetric assumption on the signs of the p, q, r, s, so it may appear that we can expand from one quantity to the other but not conversely. But if we arrive at the reduced irrationality α from the likewise reduced quantity β, the converse will also hold, as the expansion of β is periodic, so that β appears again, after α.

We now enter a lengthy discussion on the signs of the matrix elements p, q, r, s.

Given

$$\beta = \frac{p\alpha + q}{r\alpha + s}, \quad ps - qr = \pm 1,$$

where β, α are reduced quadratic irrationalitites. Our aim is to prove that we can assume that the p, q, r, s are of equal sign, hence can all be assumed non-negative.

We may assume that all coefficients, except possibly one, are non-zero. If two coefficients are zero (remembering that $ps - qr = \pm 1$), then either $\beta = \pm\alpha$ – and only the plus sign can hold, as $\alpha, \beta > 0$. Or $\beta = \pm 1/\alpha$, which is impossible as $\alpha, \beta > 1$.

We then note that we cannot have three of them positive and the fourth negative (or the other way around). In that case $ps - qr$ would be a sum of two integers of equal sign, hence of absolute value greater than one.

Nor can it happen that p, q are of one sign and r, s of the opposite sign (one of the four possibly=0).

As α is positive, that would force β to be negative.

We can also rule out the case with p, r of equal sign and q, s of the opposite sign (one of the four possibly =0). Conjugating:

$$\beta' = \frac{p\alpha' + q}{r\alpha' + s},$$

would give β' positive, as α' is negative.

There remain the two possibilities

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm \begin{pmatrix} + & - \\ - & + \end{pmatrix} \text{ or } \pm \begin{pmatrix} + & + \\ + & + \end{pmatrix}$$

(one of the four quantities possibly zero).

In the first case we simply invert the relation

$$\alpha = \frac{s\beta - q}{-r\beta + p},$$

where all coefficients are of the same sign. Possibly after changing our notation we may therefore assume

$$\beta = \frac{p\alpha + q}{r\alpha + s},$$

with non-negative coefficients.

We are now ready to prove the following Theorem.

J.III.1 Theorem. *If α and β are equivalent reduced quadratic irrationalities, then β appears in the continued fractions expansion of α, and conversely.*

Proof. Our introductory discussion proves that we may assume

$$\beta = \frac{p\alpha + q}{r\alpha + s}, \quad p, q, r, s \geq 0, \quad ps - qr = \pm 1.$$

If $r = 0$, then $p = s = 1$ and $\beta = \alpha + q$, $q \geq 0$. Conjugating gives $\beta' = \alpha' + q$. This forces $q = 0$, otherwise we would have $\beta' > 0$, as $\alpha' > -1$. So in that case $\beta = \alpha$ and the assertion is trivially true.

If $s = 0$, we see in the same manner that

$$\beta = \frac{p\alpha + 1}{\alpha} = p + \frac{1}{\alpha}, \quad \lfloor \beta \rfloor = p,$$

that is,

$$\alpha = \frac{1}{\beta - \lfloor \beta \rfloor},$$

so that α is reached in one single step from β.

We now show that we achieve this situation after a finite number of steps in the expansion of β.

Thus let $n = \lfloor \beta \rfloor$. A simple computation shows the relation

$$\frac{1}{\beta - n} = \frac{1}{(\frac{p\alpha + q}{r\alpha + s}) - n} = \frac{r\alpha + s}{(p - rn)\alpha + (q - ns)}$$

between reduced quadratic irrationalities. We are assuming $r, s > 0$, hence the coefficients in the denominator must be non-negative (by the introductory discussion).

If $p - rn = 0$ or $q - ns = 0$ we are through by the above discussion.

Otherwise we continue. Note that we are always obtaining irrationalities > 1.

As each step diminishes the sum of the positive coefficients the process must finally produce a zero coefficient in the denominator, and then we are finished, by the introductory discussion. □

J.III.2 Example. The Theorem says that the reduced irrationalities of the form

$$[P, Q] = \frac{P + \sqrt{D}}{Q}; \quad Q|(D - P^2),$$

fall into disjoint cycles of equivalent irrationalities.

For $D = 19$, there is only one cycle, of length 6:

$$[4,1] \to [4,3] \to [2,5] \to [3,2] \to [3,5] \to [2,3] \to [4,1] \ldots$$

For $D = 29$ there is a cycle of length one, $\alpha = [5,2]$, as

$$\lfloor \alpha \rfloor = \left\lfloor \frac{5 + \sqrt{29}}{2} \right\rfloor = 5; \quad \frac{1}{\alpha - 5} = \frac{2}{\sqrt{29} - 5} = \alpha$$

and one of length five:

$$[5,1] \to [5,4] \to [3,5] \to [2,5] \to [3,4] \to \ldots$$

□

J.III: Exercises

1. Pell's equation revisited.

Consider the reduced quadratic irrationality

$$\alpha = \sqrt{D} + n, \quad n = \lfloor \sqrt{D} \rfloor,$$

D still denoting a positive integer, not a perfect square.

Find the quadratic equation (with integer coefficients) satisfied by α (and its conjugate).

Denoting the period of α by l, deduce a relation

$$\alpha = \alpha_l = \frac{p\alpha + q}{r\alpha + s}; \quad ps - rq = (-1)^l,$$

and, from that, another quadratic equation for α. Deduce

$$(p+s)^2 - 4r^2 D = (-1)^l \cdot 4.$$

How do you deduce a solution to Pell's equation $t^2 - Du^2 = \pm 1$ from that?

2. Using the theory of equivalence, and relations of the form

$$\alpha = \frac{p\alpha + q}{r\alpha + s}, \quad ps - qr = -1,$$

prove that the period of α is odd if and only if $t^2 - Du^2 = -1$ is solvable in integers. (cf. H.III.1, H.III.4.)

3. Let (t, u) be a solution to Pell's equation $t^2 - Du^2 = \pm 1$. Multiply the equation you derived in the first problem above by u; by suitably re-writing the first-degree term, and retracing the steps of the previous problem, derive a relation of the form

$$\alpha = \frac{p\alpha + q}{r\alpha + s}, \quad ps - qr = \pm 1.$$

* J.IV An Alternative Approach

We give here an alternative proof of the equivalence Theorem (J.III.1) looking at the expansion "from the other end". Although the proof will be slightly longer, and perhaps more difficult, we gain a little more information.

We start with a Lemma, providing the base step of a "hidden induction". In the sequel β is always a positive irrational number, and $\alpha > 1$.

J.IV.1 Lemma. *Suppose*

$$\beta = \frac{(rt+1)\alpha + r}{t\alpha + 1},$$

where $r > 0$, $t \geq 1$ are integers. Then $\alpha = \beta_2$ in the expansion of β, and $(rt+1)/t$, $r/1$ are successive convergents.

Proof. Setting

$$\gamma = t + \frac{1}{\alpha} > 1, \quad \alpha = \frac{1}{\gamma - t},$$

we see that t is the floor of γ and that

$$\beta = \frac{rt + 1 + r(\gamma - t)}{t + (\gamma - t)} = \frac{r\gamma + 1}{\gamma} = r + \frac{1}{\gamma}, \quad r = \lfloor \beta \rfloor, \quad \gamma = \frac{1}{\beta - \lfloor \beta \rfloor},$$

whence $\gamma = \beta_1$, $\alpha = \beta_2$.

Furthermore, recalling our vector notation, and the basic recurrence, from G.I.1,

$$\mathbf{v}_{-1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \mathbf{v}_0 = \begin{pmatrix} 1 \\ r \end{pmatrix}, \quad \mathbf{v}_1 = t\begin{pmatrix} 1 \\ r \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} t \\ rt+1 \end{pmatrix},$$

whence

$$\frac{p_1}{q_1} = \frac{rt+1}{t}, \quad \frac{p_0}{q_0} = \frac{r}{1},$$

proving the assertion about convergents. □

Now we look at a more general case.

J.IV.2 Theorem. *Still assuming $\beta > 0$, $\alpha > 1$.This time assume that*

$$\beta = \frac{r\alpha + s}{t\alpha + u}$$

with $ru - st = \pm 1$, $t > u > 0$ (forcing $r, s \geq 0$). Then $\alpha = \beta_k$ for some k, and

$$\frac{r}{t} = \frac{p_k}{q_k}, \quad \frac{s}{u} = \frac{p_{k-1}}{q_{k-1}},$$

so, again, two successive convergents may be read off from the coefficients of the relation expressing β in α.

Proof. If r or s were negative, both would be, as $ru - st = \pm 1$, and $t, u > 0$. But then $\beta < 0$. This contradiction proves the statement in parentheses.

Basically we will perform Euclid on t and u, remembering that $(t, u) = 1$ as $ru - st = \pm 1$. If $u > 1$, the first step is $t = nu + v, u > v > 0$. Introducing

$$\gamma = n + \frac{1}{\alpha}; \quad n = \lfloor \gamma \rfloor, \quad \alpha = \frac{1}{\gamma - \lfloor \gamma \rfloor},$$

the given relation turns into

$$\beta = \frac{r + s(\gamma - n)}{t + u(\gamma - n)} = \frac{s\gamma + (r - ns)}{u\gamma + (t - nu)},$$

where, still, $u > t - nu > 0$. We cannot have $r - ns < 0$ if the determinant is to remain $= \mp 1$, and $\beta > 0$.

We continue in the same manner until arriving at

$$\beta = \frac{a\delta + b}{c\delta + 1}$$

with $c > 1$. We must then have $a = bc \pm 1$ as the determinant will still equal ± 1.

The plus sign is the situation of the Lemma. We see that δ is reached in two steps from β, and, inductively, that α is reached in a number of additional steps. Assuming this proved for γ, by induction (on u) we see that α is reached in the next step.

As for the convergents the Lemma dealt with the base step. Assume $\gamma = \beta_{k-1}$, $\alpha = \beta_k$ and, by way of induction, that

$$\begin{pmatrix} q_{k-1} \\ p_{k-1} \end{pmatrix} = \begin{pmatrix} u \\ s \end{pmatrix}, \quad \begin{pmatrix} q_{k-2} \\ p_{k-2} \end{pmatrix} = \begin{pmatrix} t - nu \\ r - ns \end{pmatrix}.$$

Remembering that $\lfloor \beta_k \rfloor = \lfloor \alpha \rfloor = n$ we then get

$$\begin{pmatrix} q_k \\ p_k \end{pmatrix} = n \cdot \begin{pmatrix} q_{k-1} \\ p_{k-1} \end{pmatrix} + \begin{pmatrix} q_{k-2} \\ p_{k-2} \end{pmatrix} = n \cdot \begin{pmatrix} u \\ s \end{pmatrix} + \begin{pmatrix} t - nu \\ r - ns \end{pmatrix} = \begin{pmatrix} t \\ r \end{pmatrix},$$

proving the statement about convergents.

In the case of *the minus sign* we introduce

$$\omega = (c-1) + \frac{1}{\delta}, \quad \lfloor \omega \rfloor = c - 1, \quad \delta = \frac{1}{\omega - (c-1)},$$

leading to

$$\beta = \frac{a\delta + b}{c\delta + d} = \frac{a + b[\omega - (c-1)]}{c + [\omega - (c-1)]} = \frac{b\omega + (b-1)}{\omega + 1},$$

which is again the situation of the Lemma, and the rest of the proof is as in the previous case. □

We finally give our most general result, an observation due to Australian mathematician Keith Matthews.

J.IV.3 Theorem. *Still assuming $\alpha > 1, \beta > 0$, assume that*

$$\beta = \frac{r\alpha + s}{t\alpha + u}$$

with $r, t, u > 0$, $s \geq 0$, $ru - st = \pm 1$. Then there exists an $m \geq 0$ such that $\alpha + m = \beta_k$ for some k, and at least r/t is a convergent in the continued fractions expansion of β.

Proof. Assume $u \geq t$, else we are in the case of the previous Theorem. Divide: $u = mt + v$, $0 \leq v < t$.

We first deal with the case $v = 0$, $u = mt$. As $(t, u) = 1$ we must have $t = 1$, hence

$$\beta = \frac{r\alpha + s}{\alpha + m}$$

and $s = rm \pm 1$, so that

$$\beta = \frac{r(\alpha + m) \pm 1}{\alpha + m}$$

The plus sign means that $\alpha + m$ is produced from β in one step.

In the case of the minus sign we rewrite thus:

$$\beta = \frac{r(\alpha + m - 1) + (r - 1)}{(\alpha + m - 1) + 1}$$

and the Lemma applies (with $t = 1$, r replaced by $r - 1$, and $\alpha + m - 1$ in place of α).

If $v > 0$, then

$$\beta = \frac{r(\alpha + m) + (s - rm)}{t(\alpha + m) + (u - mt)},$$

with $0 < u - mt < t$. Further $s - rm \geq 0$, as the determinant equals ± 1. Now apply the previous Theorem and its proof (the end) to this situation.

□

J.V Reciprocal Expansions

Let α, β, connected by

$$\beta = \frac{p\alpha + q}{r\alpha + s}, \quad ps - qr = \pm 1,$$

be equivalent quadratic irrationalities. By our previous convention the expansion from β leading to α is afforded by the matrix

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

We have proved its product representation

$$\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} b_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} b_k & 1 \\ 1 & 0 \end{pmatrix},$$

where the b_j are the partial quotients of the expansion:

$$b_0 = \lfloor \beta \rfloor,$$

$$\beta = b_0 + \frac{1}{\beta_1} = \frac{b_0\beta_1 + 1}{\beta_1},$$

and so on.

We proved earlier (H.VII.2) that $-1/\beta'$, $-1/\alpha'$ are reduced as α, β are. Starting from

$$\beta = \frac{p\alpha + q}{r\alpha + s},$$

conjugating,

$$\beta' = \frac{p\alpha' + q}{r\alpha' + s},$$

and inverting:

$$\alpha' = \frac{s\beta' - q}{-r\beta' + p},$$

it is straightforward to prove that

$$-\frac{1}{\alpha'} = \frac{p(\frac{-1}{\beta'}) + r}{q(\frac{-1}{\beta'}) + s},$$

i.e., that transition is afforded by the *matrix transpose*

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} b_k & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} b_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix}$$

with the same factors, but in the opposite order.

Now the matrix

$$\begin{pmatrix} b_k & 1 \\ 1 & 0 \end{pmatrix}$$

performs the transition from the reduced quantity β_k, $b_k = \lfloor \beta_k \rfloor$, to the reduced quantity α:

$$\alpha = \frac{1}{\beta_k - b_k}; \qquad \beta_k = b_k + \frac{1}{\alpha}. \tag{$*$}$$

In an earlier Section (H.VII.2) we proved that then, also:

$$b_k = \left\lfloor \frac{-1}{\alpha'} \right\rfloor. \tag{$**$}$$

This means that the matrix

$$\begin{pmatrix} b_k & 1 \\ 1 & 0 \end{pmatrix}$$

does represent the first step in the expansion of

$$\frac{-1}{\alpha'}.$$

From this we see, inductively, that the last derived matrix product represents the expansion leading

$$\text{from } \frac{-1}{\alpha'} \text{ to } \frac{-1}{\beta'}.$$

If the original expansion is

$$\beta \longrightarrow \beta_1 \longrightarrow \beta_2 \longrightarrow \cdots \longrightarrow \alpha,$$

the derived expansion is

$$\frac{-1}{\alpha'} \longrightarrow \cdots \longrightarrow \frac{-1}{\beta_2'} \longrightarrow \frac{-1}{\beta_1'} \longrightarrow \frac{-1}{\beta'}.$$

We therefore obtain this expansion from that leading from β to α by reversing the order of the partial quotients. We say that the two expansions are *reciprocal* to one another.

In particular, if $\beta = \alpha$, and the given relation represents one period in the expansion of α, the period of $-1/\alpha'$ will be the same running backwards.

A simple example is

$$\alpha = \sqrt{6} + 2 = \overline{[4, 2]}; \quad \frac{-1}{\alpha'} = \frac{\sqrt{6}+2}{2} = \overline{[2, 4]}.$$

Check!

J.VI Selfreciprocity, Partial Quotients

If

$$\alpha = \alpha_0 = \sqrt{D} + n, \quad n = \lfloor \sqrt{D} \rfloor,$$

is reduced, of period l, then

$$\frac{-1}{\alpha_l'} = \frac{-1}{\alpha_0'} = \frac{1}{\sqrt{D} - n} = \alpha_1$$

which means that the expansion in this case is *self-reciprocal.*

Looking at the identical expansions

$$\alpha_1 \to \alpha_2 \to \alpha_3 \to \cdots \to \alpha_l$$
$$\frac{-1}{\alpha'_l} \to \frac{-1}{\alpha'_{l-1}} \to \frac{-1}{\alpha'_{l-2}} \to \cdots \to \frac{-1}{\alpha_1}$$

we conclude that

$$\alpha_k = \frac{-1}{\alpha'_{l+1-k}}, \quad k \geq 1.$$

As (*) and (**) of the previous Section show, α_k and $-1/\alpha'_{k+1}$ have the same floor. Therefore:

$$a_k = \lfloor \alpha_k \rfloor = \left\lfloor \frac{-1}{\alpha'_{k+1}} \right\rfloor = \lfloor \alpha_{l-k} \rfloor = a_{l-k}, \quad k \geq 0,$$

(the case $k = 0$ is covered by periodicity).

Note that in the first identity the index sum is $l + 1$, in the second it is l.

For $\alpha = \sqrt{D}$ the expansion is the same, except for α_0, a_0, so the expansion in this case is "almost" self-reciprocal. The above identities then hold for $k \geq 1$.

For the convenience of the reader we repeat our previous examples to illustrate this symmetry. It is visible in the last row of the two tables. Note again that we were studying the expansion of $\sqrt{D}$, where $a_l = 2a_0$.

$D = 14$:

k	-1	0	1	2	3
p_k	1	3	4	11	$\underline{15}$
q_k	0	1	1	3	$\underline{4}$
P_{k+1}	0	3	2	2	3
$(-1)^{k+1}Q_{k+1}$	1	-5	2	-5	$\underline{1}$
a_{k+1}	3	1	2	1	6

$D = 29$:

k	-1	0	1	2	3	4
p_k	1	5	11	16	27	$\underline{70}$
q_k	0	1	2	3	5	$\underline{13}$
P_{k+1}	0	5	3	2	3	5
$(-1)^{k+1}Q_{k+1}$	1	-4	5	-5	4	$\underline{-1}$
a_{k+1}	5	2	1	1	2	10

Remark 1: An interesting thing happens when the period l is odd, $l = 2m-1$. As we have seen, this is equivalent to the equation $p^2 - Dy^2 = -1$ being solvable in integers.

In this case,

$$\alpha_1 = \frac{-1}{\alpha'_{2m-1}}, \quad \alpha_2 = \frac{-1}{\alpha'_{2m-2}}, \ldots, \alpha_m = \frac{-1}{\alpha'_{2m-l}} = \frac{-1}{\alpha'_m},$$

i.e.,

$$\frac{\sqrt{D}+P_m}{Q_m} = \frac{Q_m}{\sqrt{D}-P_m}$$

so that

$$D = P_m^2 + Q_m^2. \qquad (***)$$

This is illustrated in the example $D = 29$ above, with period 5 and $29 = P_3^2 + Q_3^2 = 2^2 + 5^2$.

Clearly, $(D, Q_m) > 1$ or -1 is a quadratic residue modulo D. We prove below that the first case is impossible.

If D is a prime number $\equiv 1 \pmod 4$ earlier Exercises show that the period is in fact odd, as the equation $p^2 - Dy^2 = -1$ is then shown to be solvable. So we have here a new method for representing p a a sum of squares, (cf. Section E.I), in fact one that does not depend on solving the congruence $x^2 \equiv -1 \pmod p$. In all fairness it should be pointed out that the method explained earlier, using Euclid, is *much* faster (of polynomial, not exponential, complexity).

Remark 2: By the QCF (Section H.I) $D - P_m^2 = Q_m \cdot Q_{m-1}$ so (***) means that $Q_{m-1} = Q_m$. If $D = P_m^2 + Q_m^2$ is odd this entails that $Q = Q_m$ must be the odd term. This is because we have the following situation:

$$p^2 - Dq^2 \equiv \pm Q$$
$$r^2 - Ds^2 \equiv \mp Q$$

where $p/q, r/s$ are successive convergents.

As $ps - qr = \pm 1$, we cannot have all p, q, r, s odd. And if one of p or q is even, the other must be odd; and correspondingly for r, s. This proves that Q must be odd.

Also, we cannot have $d = (Q, D) > 1$. If that were the case, d would divide both p^2 and r^2, which is impossible, as $ps - qr = \pm 1$, so that $(p, r) = 1$.

J.VII Symmetry of the P_k, Q_k

From the examples above it appears that the Q_k exhibit the same symmetry as the a_k, and that the P_k do so with a slight shift. We now explain this.

First recall the QCF recurrence:

$$P_{k+1} = a_k Q_k - P_k, \quad D - P_{k+1}^2 = Q_k Q_{k+1}.$$

Starting from

$$\alpha_k = \frac{\sqrt{D} + P_k}{Q_k}$$

and using the above recurrence (with $k-1$ in place of k) we get

$$\begin{aligned} \frac{\sqrt{D} + P_{l+1-k}}{Q_{l+1-k}} = \alpha_{l+1-k} = \frac{-1}{\alpha'_k} &= \frac{Q_k}{\sqrt{D} - P_k} \\ &= \frac{Q_k(\sqrt{D} + P_k)}{D - P_k^2} = \frac{\sqrt{D} + P_k}{Q_{k-1}}, \quad k \geq 1, \end{aligned}$$

hence, as we hoped to prove:

$$\boxed{P_{l+1-k} = P_k,\ k \geq 1; \quad Q_{l-k} = Q_k,\ k \geq 0.}$$

The examples above (p. 269) give ample illustration.

* J.VIII Moving Forward One Period

We take another look at the relation

$$\sqrt{D} = \frac{p_k(P_{k+1} + \sqrt{D}) + p_{k-1}Q_{k+1}}{q_k(P_{k+1} + \sqrt{D}) + q_{k-1}Q_{k+1}},$$

or

$$\sqrt{D} \cdot \big(q_k(P_{k+1} + \sqrt{D}) + q_{k-1}Q_{k+1}\big) = p_k(P_{k+1} + \sqrt{D}) + p_{k-1}Q_{k+1}.$$

We rewrite it differently this time:

$$(P_{k+1} + \sqrt{D})(q_k\sqrt{D} - p_k) = Q_{k+1}(p_{k-1} - q_{k-1}\sqrt{D})$$

and conjugate:

$$-(P_{k+1} - \sqrt{D})(q_k\sqrt{D} + p_k) = Q_{k+1}(p_{k-1} + q_{k-1}\sqrt{D}).$$

As $(P_{k+1} - \sqrt{D})(P_{k+1} + \sqrt{D}) = -Q_{k+1}Q_k$ by the QCF, we can also rewrite it thus:

$$\boxed{p_k + q_k\sqrt{D} = \frac{P_{k+1} + \sqrt{D}}{Q_k}(p_{k-1} + q_{k-1}\sqrt{D})}$$

or

$$\begin{aligned} p_k + q_k\sqrt{D} &= \frac{Q_{k+1}}{Q_k}\frac{P_{k+1} + \sqrt{D}}{Q_{k+1}}(p_{k-1} + q_{k-1}\sqrt{D}) \\ &= \frac{Q_{k+1}}{Q_k}\alpha_{k+1}(p_{k-1} + q_{k-1}\sqrt{D}), \quad k \geq 0. \end{aligned}$$

Driving this recurrence all the way to the bottom, remembering that $Q_0 = 1$, $p_{-1} + q_{-1}\sqrt{D} = 1$, we arrive at:

$$\begin{aligned} p_k + q_k\sqrt{D} &= \frac{Q_{k+1}}{Q_k} \cdot \alpha_{k+1} \cdot (p_{k-1} + q_{k-1}\sqrt{D}) \\ &= \frac{Q_{k+1}}{Q_k} \cdot \frac{Q_k}{Q_{k-1}} \cdot \alpha_{k+1} \cdot \alpha_k \cdot (p_{k-2} + q_{k-2}\sqrt{D}) \\ &\vdots \\ &= \frac{Q_{k+1}}{Q_k} \cdot \frac{Q_k}{Q_{k-1}} \cdots \frac{Q_1}{Q_0} \cdot \alpha_{k+1} \cdot \alpha_k \cdots \alpha_1, \end{aligned}$$

hence:

J.VIII.1 Theorem (Lagrange's Product Formula).

$$p_k + q_k\sqrt{D} = Q_{k+1} \cdot \alpha_{k+1} \cdot \alpha_k \cdots \alpha_1.$$

□

From the account in Edwards' book it appears that this Product Formula, is already present in the work of Wallis and Brouncker. In fact, their idea was to choose P_{k+1} so as to make both components of $(P_{k+1} + \sqrt{D})(p_{k-1} + q_{k-1}\sqrt{D})$ divisible by Q_k. Among the possible choices they picked the largest $P_{k+1} < \sqrt{D}$. Bhaskara's approach differed from theirs in allowing $P_{k+1} > \sqrt{D}$, i.e., he chose to minimize the absolute value $|D - P_{k+1}^2|$.

Implicit in this discussion is the fact that $x + y\sqrt{D} = p_{k-1} + q_{k-1}\sqrt{D}$ is a solution to the equation $x^2 - Dy^2 = \pm Q_k$ *belonging to* $-P_k$, hence also to $P_{k+1} \equiv -P_k \pmod{Q_k}$, cf. pp. 217 and 240.

We now look at a special case. If the period is l, so that $Q_l = 1$, we get

$$p_{l-1} + q_{l-1}\sqrt{D} = \alpha_l \cdot \alpha_{l-1} \cdots \alpha_1$$

and

$$p_{k+l} + q_{k+l}\sqrt{D} = Q_{k+l+1} \cdot \alpha_{k+l+1} \cdot \alpha_{k+l} \cdots \alpha_{l+1} \cdot \alpha_l \cdots \alpha_1 =$$
$$Q_{k+1} \cdot (\alpha_{k+1} \cdot \alpha_k \cdots \alpha_1) \cdot (\alpha_l \cdots \alpha_1) = (p_k + q_k\sqrt{D})(p_{l-1} + q_{l-1}\sqrt{D}).$$

We have proved:

J.VIII.2 Theorem. *Let $\alpha = \sqrt{D}$, D a positive integer, not a perfect square. Let l be the period of its expansion so that (H.III.3)*

$$p_{l-1}^2 - Dq_{l-1}^2 = (-1)^l.$$

Then it holds that

$$p_{l+k} + q_{l+k}\sqrt{D} = (p_k + q_k\sqrt{D})(p_{l-1} + q_{l-1}\sqrt{D}) \qquad (*)$$

for all $k \geq -1$.

□

The Theorem says that we move one period forward by multiplication with the least positive solution to $x^2 - Dy^2 = \pm 1$.

We have given Examples in an earlier Section, see p. 235.

J.VIII: Exercises

1. Generalize Lagrange's Product Formula to the case $\alpha = (P + \sqrt{D})/Q$ where $Q|(D - P^2)$.

2. Give a new derivation of (*) by noting that the two members (running over a full period) satisfy the same first order recurrence with positive coefficients, and begin and end the same.

* J.IX Running a Period Backwards

Due to self-reciprocity, within a period the solutions to $p_k^2 - Dq_k^2 = \pm Q_k$ appear in pairs, except possibly in the middle. For instance, in the case $D = 29$, we have (look back at the Examples above, p. 269)

$$\begin{aligned} 11^2 - 29 \cdot 2^2 &= 5, \\ 16^2 - 29 \cdot 3^2 &= -5, \end{aligned}$$

corresponding to $k = 1, 2$. How do they relate to one another? The answer is that the respective solutions will differ by a factor $x + y\sqrt{D}$, $x^2 - Dy^2 = \pm 1$, after one of them is conjugated.

In order to prove this we recall the two symmetry relations (J.VII), with a slightly different indexing.

$$Q_{k+1} = Q_{l-k-1}, \quad k \geq -1,$$

and

$$\alpha'_{l-k-1} = \frac{-1}{\alpha_{k+2}}, \quad k \geq -1.$$

Start again with

$$p_k + q_k\sqrt{D} = Q_{k+1} \cdot \alpha_{k+1} \cdot \alpha_k \cdots \alpha_1.$$

Replace k by $l - k - 2$ and conjugate:

$$p_{l-k-2} - q_{l-k-2}\sqrt{D} = Q_{l-k-1} \cdot \alpha'_{l-k-1} \cdot \alpha'_{l-k-2} \cdots \alpha'_1 =$$
$$Q_{k+1} \cdot \alpha'_{l-k-1} \cdot \alpha'_{l-k-2} \cdots \alpha'_1 = Q_{k+1} \cdot \frac{-1}{\alpha_{k+2}} \cdots \frac{-1}{a_l}.$$

Now multiplying this by

$$p_{l-1} + q_{l-1}\sqrt{D} = \alpha_l \cdot \alpha_{l-1} \cdots \alpha_1 = (\alpha_l \cdots \alpha_{k+2}) \cdot (\alpha_{k+1} \cdots \alpha_1)$$

we get

$$\begin{aligned} (p_{l-k-2} - q_{l-k-2}\sqrt{D})(p_{l-1} + q_{l-1}\sqrt{D}) = &\ (-1)^{l-k-1} Q_{k+1} \cdot \alpha_{k+1} \cdot \alpha_k \cdots \alpha_1 \\ &= (-1)^{l-k-1}(p_k + q_k\sqrt{D}), \end{aligned}$$

proving:

J.IX.1 Theorem. *Let $\alpha = \sqrt{D}$, D a positive integer, not a perfect square. Let l be the period of its expansion so that*

$$p_{l-1}^2 - Dq_{l-1}^2 = (-1)^l.$$

Then it holds that

$$p_k + q_k\sqrt{D} = (-1)^{l-k-1}(p_{l-k-2} - q_{l-k-2}\sqrt{D})(p_{l-1} + q_{l-1}\sqrt{D})$$

for $-1 \le k \le l-1$.

□

J.IX.2 Example. In the case $D = 29$, with $k = 2$, the left member is

$$p_2 + q_2\sqrt{D} = 16 + 3\sqrt{29}$$

Here the period is $l = 5$, and $l - k - 2 = 1$, $p_4 + q_4\sqrt{29} = 70 + 13\sqrt{29}$, $p_1 - q_1\sqrt{29} = 11 - 2\sqrt{29}$. And:

$$(70 + 13\sqrt{29}) \cdot (11 - 2\sqrt{29}) = 16 + 3\sqrt{29}.$$

□

J.IX: Exercises

1. If $Q = Q_j = \pm Q_k$ appear within the same period, the corresponding x, y satisfying $x^2 - Dy^2 = \pm Q$ cannot belong (cf. p. 217) to the same P (why not?). Show, by examining the QCF recurrence, that if one belongs to P the other belongs to $-P$.

2. Give an alternative proof along the same lines as the last exercise of the previous Section (comparing recurrences that begin and end the same).

* J.X More on Pell-Like Equations

An intriguing special case is that of $D =$ a prime number, $D \equiv 3 \pmod 4$. In that case the period l must be even, by H.III.1, $l = 2k + 2$. Using that value of k, still setting $z_j = p_j + q_j\sqrt{D}$ for arbitrary j, the general identity (J.IX.1)

$$z_k = (-1)^{l-k-1} z'_{l-k-2} \cdot z_{l-1}$$

becomes:

$$z_k = (-1)^{k+1} z'_k \cdot z_{l-1}.$$

Multiplying by z_k, and remembering

$$z_k \cdot z'_k = p_k^2 - Dq_k^2 = (-1)^{k+1} Q_{k+1},$$

we obtain:

$$(p_k + q_k\sqrt{D})^2 = z_k^2 = Q_{k+1} \cdot (p_{l-1} + q_{l-1}\sqrt{D}).$$

This means that Q_{k+1} must divide $p_k^2 + Dq_k^2$. As it is also plus or minus $p_k^2 - Dq_k^2$, Q_{k+1} must divide both the sum and difference, $2p_k^2$ and $2Dq_k^2$. As $(p_k^2, q_k^2) = 1$ this means that Q_{k+1} divides $2D$. We cannot have $Q_{k+1} = 1$ as that would force a shorter period. And, as $Q_{k+1} < 2\sqrt{D}$, temporarily assuming $D > 3$, it cannot divide the odd prime factor D. Hence $Q_{k+1} = 2$.

So we have proved the solvability of one of the two Diophantine equations

$$x^2 - Dy^2 = \pm 2.$$

We assumed $D > 3$; however, the case $D = 3$ is trivially true ($x = y = 1$).

The sign must be chosen so that ± 2 is a quadratic residue modulo D. Recall that -1 is a non-residue in this case, so exactly one of the two cases holds.

If $D \equiv 3 \pmod 8$, we must take the minus sign, as $(2/D) = -1$. If $D \equiv 7 \pmod 8$, the plus sign holds, as $(2/D) = 1$.

We arrive at the following Theorem:

J.X.1 Theorem. *Let D be an odd prime.*

a) If $D \equiv 3 \pmod 8$, the equation $x^2 - Dy^2 = -2$ is solvable in integers, $x^2 - Dy^2 = 2$ is unsolvable, and the period of the continued fractions expansion of $\sqrt{D}$ is congruent to 2 modulo 4.

b) If $D \equiv 7 \pmod 8$, the equation $x^2 - Dy^2 = 2$ is solvable in integers, $x^2 - Dy^2 = -2$ is unsolvable, and the period of the continued fractions expansion of $\sqrt{D}$ is divisible by 4.

Proof. It remains only to discuss the length of the periods.

The period is $2k+2$, the sign in the right member is $(-1)^{k+1}$ (see the beginning of this Section).

In case a) the sign is -1, hence $k+1$ is odd, k is even, $k = 2m$, and the period is $2k+2 = 4m+2$.

In case b) the sign is $+1$, hence $k+1$ is even, k is odd, $k = 2m-1$, and the period is $2k+2 = 4m$. □

Although this result is of a very classical type, I have not found the explicit statement about the periods in older books.

The solvability in either case can be proved more directly, as previous exercises show, see p. 238.

J.X.2 Example. One example with $D \equiv 3 \pmod 8$ is $D = 19$. We have $13^2 - 19 \cdot 3^2 = -2$ and the period is 6, almost accessible to hand calcuation (the a_k of the first period are 4, 2, 1, 3, 1, 2, the convergents are 4/1, 9/2, 13/3, 48/11, 61/14, 170/39).

An example with $D \equiv 7 \pmod 8$ is $D = 31$, having period 8 and leading (halfway through, of course) to $39^2 - 31 \cdot 7^2 = 2$.

Note that

$$\frac{39 + 7\sqrt{31}}{39 - 7\sqrt{31}} = \frac{1}{2}(39 + 7\sqrt{31})^2 = 1520 + 273\sqrt{31}$$

gives the least positive solution to $x^2 - 31 \cdot y^2 = 1$ according to the discussion in the previous Section.

The reader might want to try $D = 23$, having period 4, by hand. □

The last Theorem states that one half of the period determines the other half. Can we hope that the first occurence of $Q_{k+1} = 2$ determines the least positive solution to $x^2 - Dy^2 = \pm 1$ as in the Example above? Indeed we can, by the following Theorem.

J.X.3 Theorem. *Still assuming that D is a prime $\equiv 3 \pmod 4$, the situation $Q_{k+1} = 2$ can occur only once every period, i.e., only halfway through it.*

Proof. Let x/y, u/v be convergents to $\sqrt{D}$ satisfying

$$x^2 - Dy^2 = u^2 - Dv^2 = \pm 2.$$

Assume $x + y\sqrt{D} > u + v\sqrt{D}$. Then

$$r + s\sqrt{D} = \frac{x + y\sqrt{D}}{u + v\sqrt{D}} > 1; \quad r^2 - Ds^2 = 1.$$

Let us prove that r, s are integers. Multiplying the numerator and denominator by $u - v\sqrt{D}$ we get

$$r + s\sqrt{D} = \frac{(x + y\sqrt{D})(u - v\sqrt{D})}{\pm 2}.$$

As x, y, u, v must be odd we see that $xu - Dyv$ and $yu - xv$ are even, hence r, s are integers.

As $r + s\sqrt{D} > 1$ it is a positive power of the least solution $p + q\sqrt{D} > 1$ to $p^2 - Dq^2 = 1$ (cf. H.III.6), say $r + s\sqrt{D} = (p + q\sqrt{D})^n$. By an earlier result (cf. Section J.VII) this means that $x + y\sqrt{D}$ is n periods removed from $u + v\sqrt{D}$, hence that they do not belong to the same period. □

As is clear from Edwards' book, the trick of stopping at $Q_{k+1} = 2$, squaring the solution, and dividing by two, was known to Bhaskara.

Now, let us deal with primes $D \equiv 1 \pmod 4$.

J.X.4 Theorem. *Let D be a prime number $\equiv 1 \pmod 4$. Then the equation $x^2 - Dy^2 = \pm 2$ is unsolvable; the period of $\sqrt{D}$ is odd, and $x^2 - Dy^2 = -1$ is thus solvable.*

Proof. The first statement is easy, as $x^2 \equiv 0, 1 \pmod 4$ and also $Dy^2 \equiv 0, 1 \pmod 4$, hence $x^2 - Dy^2 \equiv 0, \pm 1 \not\equiv 2 \pmod 4$.

However, by exactly the same reasoning as in the next to last Theorem, if the period of $\sqrt{D}$ were even, the equation $x^2 - Dy^2 = \pm 2$ would be solvable. Hence the period is odd, and $x^2 - Dy^2 = -1$ is therefore solvable. □

So, of the three Diophantine equations

$$x^2 - Dy^2 = -1, \pm 2$$

for a given odd prime D, one is solvable, the other two not, and all three cases occur.

We conclude this Section by looking at products $D = pq$, where $p \neq q$ are odd prime numbers. We derive two special results.

J.X.5 Theorem. *Assume $p \equiv q \equiv 3 \pmod 4$. Then the period of $\sqrt{pq}$ is even, and the equation $px^2 - qy^2 = \pm 1$ is solvable for exactly one choice of the sign. From this follows one special case of Quadratic Reciprocity, that of $p \equiv q \equiv 3 \pmod 4$.*

Proof. The period is even because $x^2 - pqy^2 = -1$ is unsolvable in integers, -1 being a quadratic non-residue modulo p (and q).

As before (p. 277) we can solve $x^2 - pqy^2 = Q$, $(x, y) = 1$, where Q is a divisor of $2D = 2pq$, hence $Q = \pm 2$, $\pm 2p$, $\pm 2q$, $\pm p$, or $\pm q$.

In the cases with Q even, x, y must be odd. That would give $1 - 1 \equiv 2 \pmod 4$, impossible. Hence, $x^2 - pqy^2 = \pm p$ or $\pm q$, say $\pm p$ (by choice of notation), is solvable. Then x is divisible by p, $x = pz$, hence $pz^2 - qy^2 = \pm 1$ is solvable in relatively prime integers z, y.

We then have

$$\left(\frac{p}{q}\right) = \left(\frac{pz^2}{q}\right) = \left(\frac{\pm 1}{q}\right) = \pm 1,$$

so the sign must be chosen as (p/q).

At the same time

$$\left(\frac{q}{p}\right) = \left(\frac{qy^2}{p}\right) = \left(\frac{\mp 1}{q}\right) = \mp 1 = -\left(\frac{p}{q}\right),$$

giving the special case of Quadratic Reciprocity. □

J.X.6 Example. $p = 7, q = 11$. The period of $\sqrt{77}$ is 6. Halfway through the period (3 steps, easy hand calculation) we arrive at $35^2 - 7 \cdot 11 \cdot 4^2 = -7$, hence $7 \cdot 5^2 - 11 \cdot 4^2 = -1$. □

J.X.7 Theorem. *Assume $p \equiv q \equiv 1 \pmod 4$. If the period of $\sqrt{pq}$ is even, the Diophantine equation $px^2 - qy^2 = \pm 1$ is solvable for at least one choice of the sign. In this case $(p/q) = (q/p) = 1$.*

Hence, if $(p/q) = -1$ (hence, by Quadratic Reciprocity, also $(q/p) = -1$), the period of $\sqrt{pq}$ must be odd, and the Diophantine equation $x^2 - pqy^2 = -1$ is solvable.

Proof. Assume that the period in question is even. Exactly as in the proof of the previous Theorem we can exclude the cases $x^2 - pqy^2 = \pm 2$, $\pm 2p$, $\pm 2q$. (Check!)

So (possibly after changing our notation), the equation $x^2 - pqy^2 = \pm p$ is solvable, and again we conclude that $pz^2 - qy^2 = \pm 1$ is solvable in relatively prime integers z, y. Then

$$\left(\frac{p}{q}\right) = \left(\frac{pz^2}{q}\right) = \left(\frac{\pm 1}{q}\right) = 1,$$

and

$$\left(\frac{q}{p}\right) = \left(\frac{qy^2}{p}\right) = \left(\frac{\mp 1}{p}\right) = 1,$$

and the Theorem follows. □

J.X.8 Example. The smallest example would be $p = 5$, $q = 13$, $(13/5) = (3/5) = -1$; but as $5 \cdot 13 = 8^2 + 1$, $8^2 - 65 \cdot 1^2 = -1$, this example is trivial, of period 1.

The next smallest example, $p = 17$, $q = 29$, $pq = 493$, is quite formidable. The least positive solution is $x = 683982$, $y = 3085$:

$$683982^2 - 493 \cdot 3085^2 = -1,$$

and the period is 9. □

J.X.9 Example. The condition $(p/q) = (q/p) = -1$ is sufficient, but not necessary, for the solvability of $x^2 - pqy^2 = -1$.

A trivial counterexample is $p = 5$, $q = 29$, $(29/5) = (4/5) = 1$, and

$$12^2 - 5 \cdot 29 \cdot 1^2 = -1.$$

□

The following problems partly prepare for the questions to be dealt with in in the next Section. They show, amongst other things, that if $D = 2, 3$, we can restrict our attention to equations $x^2 - Dy^2 = N$ where N is positive.

J.X: Exercises

1. Using the ideas of the first few Theorems of this Section, prove that $x^2 - 2py^2 = -1$ is solvable in integers if the prime number $p \equiv 5 \pmod 8$.

If you have written a QCF routine you will easily find examples of two primes $p \equiv 1 \pmod 8$, with $x^2 - 2py^2 = -1$ solvable or unsolvable.

2. Check that the period of $D = 23$ is in accordance with Theorem J.X.1.

3. Prove that the equation $x^2 - 2y^2 = N$, N an integer, is solvable in relatively prime integers if and only if $x^2 - 2y^2 = -N$ is.

4. (a) Let N be an integer. Prove that the equation $x^2 - 3y^2 = N$ is not solvable in relatively prime integers ("properly solvable") if $4|N$.

(b) Out of the two equations $x^2 - 3y^2 = \pm N$ at most one is properly solvable.

(c) Let N be odd. Then $x^2 - 3y^2 = N$ is properly solvable if and only if $x^2 - 3y^2 = -2N$ is.

J.XI More on $x^2 - Dy^2 = N$

In this Section we discuss the Diophantine equation $x^2 - Dy^2 = N$, where $D > 0$ is not a perfect square. Setting $Q = |N|$ we will deal with the cases $x^2 - Dy^2 = \pm Q$ simultaneously.

There will be one exception: $D = 2, 3$, where we assume $N > 0$ for the time being. Later we will remove that assumption. K Matthews has shown in *Expositiones Mathematicae*, **18** (2000), 323-331, how to avoid this procedure. His treatment leans heavily on a discussion on equivalent quadratic irrationalities that we wished to avoid here. We will sketch his approach at the end of the Section.

Now, if x, y is a solution satisfying $(x, y) = 1$, then also $(y, Q) = 1$, so y is invertible modulo N. Hence there is some integer P, unique modulo Q, such that $x + Py \equiv 0 \pmod{Q}$. Plugging this into $x^2 - Dy^2 = N$ we get $y^2(P^2 - D) \equiv 0 \pmod{Q}$. By invertibility, the factor y^2 cancels, and we are left with $P^2 - D \equiv 0 \pmod{Q}$.

We say that x, y is a solution *produced by*, or *belonging to*, P, (cf. p. 217). Recall from an earlier Section (H.IV) that this amounts to

$$(P + \sqrt{D})(x + y\sqrt{D}) \equiv 0 \pmod{Q}. \qquad (*)$$

Our concern is to find all solutions belonging to any P satisfying $P^2 \equiv D \pmod{N}$. Clearly, if $\pm x, \pm y$ is a solution belonging to P, then $\mp x, \pm y$ is one belonging to $-P$, and conversely. We may assume $-Q/2 < P \leq Q/2$.

In that same Section we showed how to find all solutions belonging to a given P, from one single solution. So we will concentrate on how to find *one* of them, or prove nonexistence.

We precede our algorithm with a Lemma.

J.XI.1 Lemma.

a) Let P be an integer satisfying $P^2 - D \equiv 0 \pmod{Q}$. Let further $x, y \neq 0$ be integers satisfying $x + Py \equiv 0 \pmod{Q}$, and $x^2 - Dy^2 = N$. Then $(x, y) = 1$ (and $(y, N) = 1$). This is also true if $x^2 - Dy^2 = 2N$, with N odd.

b) With x, y, P as in a), put $(x+Py)/Q = p, y = q$. Assume $x, y > 0$. Then $p = p_k, q = q_k$ for some convergent p_k/q_k to the quadratic irrationality $(P+\sqrt{D})/Q$.

c) For every convergent p/q, $(p,q) = 1$, to $(P+\sqrt{D})/Q$,

$$N|\big((Qp-Pq)^2 - Dq^2.\big)$$

Proof.

a) We know that $(x+y\sqrt{D})(x-y\sqrt{D}) = x^2 - Dy^2 = N$. Formula (*) above may be written $(P+\sqrt{D})(x+y\sqrt{D}) = (a+b\sqrt{D})N$, $a, b, \in \mathbf{Z}$. Hence, dividing by $x+y\sqrt{D}$, $P+\sqrt{D} = (a+b\sqrt{D})(x-y\sqrt{D})$, so that $bx-ay = 1$, proving $(x.y) = 1$.

In the second case we similarly find that $(x,y) = 1$ or 2. However, as $x^2 - Dy^2 = 2N$, and N is odd, only the first case can be true.

b) As $(x,y) = 1$, we easily see that $(x+Py)/Q$, y are also relatively prime. We now use the criterion from the Section on Best Approximation, G.IV. Assuming $x^2 - Dy^2 = (x+y\sqrt{D})(x-y\sqrt{D}) = Q$, form the difference:

$$\Big|\frac{(x+Py)/Q}{y} - \frac{P+\sqrt{D}}{Q}\Big| = \Big|\frac{x-y\sqrt{D}}{yQ}\Big| = \Big|\frac{1}{y(x+y\sqrt{D})}\Big|.$$

We need to prove that the denominator is greater than $2y^2$. This is obvious if $D \geq 5$. If $D = 2, 3$ we are assuming $x^2 - Dy^2 > 0$, $x > y\sqrt{D}$, $x+y\sqrt{D} > 2y$ so this case goes through as well.

c) This follows immediately from the fact that $N|(P^2 - D)$. □

The Algorithm

We now have a closer look at the continued fractions expansion of $\alpha_0 = (P+\sqrt{D})/Q$. Setting $\alpha_{k+1} = (R+\sqrt{D})/S$ we have

$$\begin{aligned}\frac{P+\sqrt{D}}{Q} &= \frac{p_k\alpha_{k+1} + p_{k-1}}{q_k\alpha_{k+1} + q_{k-1}} = \\ &= \frac{(Rp_k + Sp_{k-1}) + p_k\sqrt{D}}{(Rq_k + Sq_{k-1}) + q_k\sqrt{D}} = \frac{p_k\sqrt{D} + r_k}{q_k\sqrt{D} + s_k}\end{aligned}$$

with

$$\begin{aligned} p_k s_k - q_k r_k &= p_k(Rq_k + Sq_{k-1}) - q_k(Rp_k + Sq_{k-1}) \\ &= S(p_k q_{k-1} - q_k p_{k-1}) \\ &= (-1)^{k+1} S. \end{aligned}$$

From

$$(P + \sqrt{D})(s_k + q_k\sqrt{D}) = Q(r_k + p_k\sqrt{D})$$

the usual identification yields

$$\begin{aligned} s_k + Pq_k &= Qp_k, \\ Dq_k + Ps_k &= Dq_k. \end{aligned}$$

Multiplying the two equations by s_k, $-q_k$, and adding, we get

$$s_k^2 - Dq_k^2 = (-1)^{k+1} QS. \tag{**}$$

Now if the equation $x^2 - Dy^2 = N$, $x, y > 0$, has a proper solution belonging to P, the solution must be of the form

$$\begin{aligned} x &= Qp_k - Pq_k = s_k \\ y &= q_k \end{aligned}$$

according to the Lemma.

Equation (**) then tells us to look for $|S| = 1$ in the expansion of $(P + \sqrt{D})/Q$. Note that a pre-period S need not be positive.

It can then happen that

I) The pre-period produces an S, $|S| = 1$, and the right sign. Then we have found a solution.

or:

II) Neither the pre-period nor the first period produces $|S| = 1$. Then there are no solutions.

or:

III) The first period produces $S = 1$ with the right sign. Then we have found a solution.

or:

IV) It produces $S = 1$, with the wrong sign, and even period. Then there is no solution.

or, finally,

V) The first period may give $S = 1$, with the wrong sign, and an odd period length. Then the next period will give a solution.

We enter the first period as soon as we obtain a reduced quantity. We enter the second period as soon as the first quantity of the first period is repeated.

The condition for $\alpha > 1$, $0 > \alpha' > -1$ can be stated as a number of suitable inequalities involving only rational integers.

J.XI.2 Example. Let $D = 5$. Suppose 5 is a quadratic residue modulo Q. There are only two reduced quantities of the form $(R + \sqrt{5})/S, S|(5 - R^2)$, namely $\alpha = 2 + \sqrt{5}$, $(1 + \sqrt{5})/2$. They each form a cycle of length 1, i.e., $1/(\alpha - \lfloor\alpha\rfloor) = \alpha$.

Letting $P^2 \equiv 5 \pmod{Q}$, and expanding $(P + \sqrt{5})/Q$, we will sooner or later land in one of the two cycles. However, as $x^2 - 5y^2 = \pm 2$ is impossible (already modulo 4), we can only land in the first cycle.

If one step produces a solution for $x^2 - 5y^2 = \pm Q$, the next step will give a solution to $x^2 - 5y^2 = \mp Q$, as the period is one.

So, if $5 \nmid Q$, the Diophantine equation $x^2 - 5y^2 = \pm Q$ is solvable if and only if 5 is a quadratic residue modulo Q!

Earlier exercises (p. 158) outlined a proof using Thue's Lemma (E.I.1). □

J.XI.3 Example. Let $D = 3$, and Q not divisible by 3 or 2. Assume that 3 is a quadratic residue modulo Q. This means that $p \equiv \pm 1 \pmod{12}$ for each prime dividing Q (exercise). Let $P^2 \equiv D \pmod{Q}$.

There are exactly two reduced irrationalities $(R+\sqrt{3})/S$; $S|(3-R^2)$, namely $1 + \sqrt{3}$ and $(1 + \sqrt{3})/2$, forming one single period. That is, if one is α, and the other is β, then $1/(\alpha - \lfloor\alpha\rfloor) = \beta$.

This means that the denominators $S = 1, 2$ will both appear, at the latest when we enter the first period of $(P + \sqrt{3})/Q$. One will produce a solution to $x^2 - 3y^2 = \pm Q$; the other to $x^2 - 3y^2 = \mp 2Q$.

As $(\pm Q/3) = \pm(Q/3)$ we see that the upper signs hold if and only if Q is a quadratic residue modulo 3. Note that we get solutions belonging to each P. □

J.XI.4 Example. The equations $x^2 - 2y^2 = \pm Q$, Q odd, are even easier, assuming that 2 is a quadratic residue modulo Q, i.e., that $p \equiv \pm 1 \pmod 8$ for all prime factors $p|Q$.

In this case there is only one admissible irrationality, $1 + \sqrt{2}$, with period one. So the algorithm will produce solutions to both equations belonging to any P with $P^2 \equiv 2 \pmod Q$. □

J.XI.5 Example. It could very well happen that $x + Py = 0$, and not just $x + Py \equiv 0 \pmod Q$, for some solution x, y and some P satisfying $-Q/2 < P \leq Q/2$, $P^2 - D \equiv 0 \pmod Q$. That would mean $y = \pm 1, x = \mp P$, as x, y are supposed to be relatively prime, that is $P^2 - D = \pm Q$.

One example is the equation $x^2 - 17y^2 = 19$, where $x = 6, y = 1$ is one solution belonging to $P = -6$, and $6 - 6 \cdot 1 = 0$

This happens because zero is a convergent to $(P + \sqrt{D})/Q$! In fact, as $-1/2 < \beta_0 = (-6 + \sqrt{17})/Q < 0$, $b_0 = -1$, and we get $\beta_1 = 1/(\beta_0 + 1) < 2$, $b_1 = 1$, hence

$$\begin{aligned} \begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \\ \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} &= \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \\ \begin{pmatrix} q_1 \\ p_1 \end{pmatrix} &= b_1 \begin{pmatrix} 1 \\ -1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \end{aligned}$$

The choice $P = 6$, gives a faster solution, $x = -6, y = 1$, because the floor of $(6 + \sqrt{17})/19$ equals zero. The reader might want to check that. □

J.XI.6 Example. Let us try to solve $x^2 - 79y^2 = 97$. 79 and 97 are both prime numbers, and $(79/97) = (18/79) = (2/79) = 1$. The square roots of 79 modulo 97 are $P \equiv \pm 46 \pmod{97}$.

Expanding $(46 + \sqrt{79})/97$ gives the following preperiod:

$$[R, S] = [46, 97] \to [-46, -21] \to [25, 26] \to [1, 3].$$

We then land in a period of reduced quantities, of length 6:

$$[R, S] = [8, 5] \to [7, 6] \to [5, 9] \to [4, 7] \to [3, 10] \to [7, 3].$$

No denominator has absolute value 1, hence the equation $x^2 - 79y^2 = 97$ has no solutions belonging to $P = 46$.

Trying $P \equiv -46 \pmod{97}$, the pre-period again will produce nothing, and we will then land in another cycle of length 6, and no denominator =1. If the elements of the previous cycle are of the form α, the new cycle consists of the various $-1/\alpha'$. The reader who has written a QCF program might want to check this. □

J.XI.7 Example. Let us try $x^2 - 79y^2 = \pm 15$. The square roots of 79 modulo 15 are $P \equiv \pm 2, \pm 7 \pmod{15}$.

Trying $P \equiv \pm 2$ lands in the wrong cycle. $P \equiv 7$ is more successful; we land in the right cycle

$$[7,15] \to [8,1](\to [8,15] \to [7,2])$$

right away. No computation is needed to find the solution $x = 8, y = 1$ to $x^2 - 79y^2 = -15$. As the period is even we will find no solutions to $x^2 - 79y^2 = 15$. □

J.XI.8 Example. Now, let us try $x^2 - 79y^2 = \pm 27 = 3^3$. The values for P are $P \equiv \pm 5 \pmod{27}$.

After the preperiod

$$[5,27] \to [-5,2]$$

producing nothing, we again land in the right cycle,

$$[7,15] \to [8,1](\to [8,15] \to [7,2])$$

The convergents are easily determined:

$$\begin{pmatrix} q_{-1} \\ p_{-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}; \quad \begin{pmatrix} q_0 \\ p_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad \begin{pmatrix} q_1 \\ p_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}; \quad \begin{pmatrix} q_2 \\ p_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix};$$

yielding

$$x = Qp_2 - Pq_2 = 27 \cdot 1 - 5 \cdot 2 = 17; \quad y = q_2 = 2,$$

satisfying $x^2 - 79y^2 = -27$. As the period is even, the equation $x^2 - 79y^2 = 27$ is not solvable. □

J.XI.9 Example. The square roots of 34 modulo 33 are $P \equiv \pm 1$, ± 10.

The equation $x^2 - 34y^2 = -33$ has the obvious solution $x = y = 1$, belonging to $P = -1$.

The equation $x^2 - 34y^2 = 33$ has the less obvious solution $x = 13, y = 2$ belonging to $P = 10 :\ 13 + 2 \cdot 10 = 33$.

That may seem odd, as the period of the reduced quantity $5 + \sqrt{34}$ in this case is even, =4. However, the solution to the second equation appears only in the preperiod of $(10 + \sqrt{34})/33$, in fact, after one step. The reader may wish to check this. □

Remark: **Matthews' Approach**

We begin by recalling the notation. $x, y > 0$ will denote an integer solution to $x^2 - Dy^2 = \pm Q = N$. It is assumed to belong to $P > 0$, where $P^2 \equiv D \pmod{Q}$, and $x + Py \equiv 0 \pmod{Q}$. Then also $Px + Dy \equiv Px + P^2y \equiv 0 \pmod{Q}$.

Matthews' approach starts with the following equivalence between $\sqrt{D}$ and $(P + \sqrt{D})/Q$:

$$\frac{P + \sqrt{D}}{Q} = \frac{(P + \sqrt{D})(x + y\sqrt{D})}{Q(x + y\sqrt{D})} = \frac{(x + Py)/Q)\sqrt{D} + (Px + Dy)/Q}{y\sqrt{D} + x}$$

with determinant $(x(x + Py) - y(Px + Dy))/Q = (x^2 - Dy^2)/Q = \pm 1$. Note that the coefficients are indeed integers.

Then invoking our last result on equivalent irrationalities (J.IV.3) he painlessly, without restriction on the sign of N in the case $D = 2, 3$, infers that the expansion of $(P + \sqrt{D})/Q$ leads to $\sqrt{D}$, and that

$$\frac{(x + Py)/Q}{y}$$

is the corresponding convergent!

The significance of Matthews' proof is that, working directly with $x^2 - Dy^2 = N$, $D = 3$, (i.e., not with $-2N$, if $N < 0$), we are guaranteed to find the *fundamental solution* $x + y\sqrt{D}$ with minimal $y > 0$, in these cases too.

A generalization was later published in K. Matthews, "The Diophantine equation $ax^2 + bxy + cy^2 = N, D = b^2 - 4ac > 0$", *Journal de Théorie des Nombres de Bordeaux*, **14** (2002) 257-270.

It is available on the Internet at `http://www.numbertheory.org/papers.html#patz`.

J.XI: Exercises

1. Write the condition for a quadratic irrationality to be reduced as at most four inequalitites involving rational integers. One possible extension is to write a program determining all admissible reduced quantities $(P+\sqrt{D})/Q$, $Q|(D-P^2)$, for a given integer $D>0$, not a square.

2. If the period of $a+\sqrt{D}$, $a=\lfloor\sqrt{D}\rfloor$, is of even length, then the same holds for the periods of all reduced quantities $(P+\sqrt{D})/Q$, $Q|(D-P^2)$. And conversely. Prove!

3. (Hand calculation possible).

(a) Determine the solutions to $x^2-2y^2=\pm17$. In particular, in either case find those solutions for which $y>0$ is minimal.

(b) Determine the solutions to $x^2-3y^2=\pm13$ (whichever is solvable) and $x^2-3y^2=\pm26$ (whichever is solvable). In particular, in either case find those solutions for which $y>0$ is minimal.

(c) Solve $x^2-3y^2=\pm73,\pm146$, knowing that $21^2\equiv3 \pmod{146}$.

4. **Suggestions for computing:** If you have written a QCF routine, modify, and extend, it to find solutions to the equations

(a)

$$x^2-28y^2=\pm111$$

knowing that $19^2\equiv28 \pmod{37}$.

(b)

$$x^2-237y^2=1009$$

knowing that $674^2\equiv237 \pmod{1009}$. (1009 is a prime number).

Chapter K

$\mathbf{Z}[i]$, Other Number Rings

K.I Preparations

We prepare our discussion on unique factorization in $\mathbf{Z}[i]$ with a few definitions. The first one should be familiar by now.

K.I.1 Definition. A **number ring** is a set R of complex or real numbers, containing zero and one, and closed under addition, subtraction and multiplication.

Closure under the arithmetic operations simply means that they do not lead outside the set, i.e., the sum, difference, and product of two numbers in R belong to R.

K.I.2 Definition. A **number field** is a number ring F where every non-zero element α has its multiplicative inverse $1/\alpha$ in F.

K.I.3 Example. Our number fields will almost invariably be $F = \mathbf{Q}[\sqrt{D}]$ or $F = \mathbf{Q}[i\sqrt{D}]$ where D is a positive integer, not a perfect square.

The latter type of field is often denoted $F = \mathbf{Q}[\sqrt{-D}]$.

The elements are $m + n\sqrt{D}$, $m, n \in \mathbf{Q}$, or $m + in\sqrt{D}$, respectively. Closure under addition and subtraction are obvious. Multiplication is no big issue, e.g., $(m + n\sqrt{D})(s + t\sqrt{D}) = ms + ntD + (ns + mt)\sqrt{D}$.

And the multiplicative inverse of $\alpha = m + n\sqrt{D} \neq 0$ is

$$\alpha^{-1} = (m - n\sqrt{D})/(m^2 - Dn^2).$$

The denominator $m^2 - Dn^2$ is non-zero, cf. p. **??**. Division by α is multiplication by α^{-1}. □

K.I.4 Example. Our number rings will be suitable subrings of the fields just described. We have already encountered $\mathbf{Z}[i]$.

For a less obvious example, take $\mathbf{Z}[\epsilon]$ where $\epsilon =(-1 + i\sqrt{3})/2$, the root to $X^3 = 1$ of least positive argument. The other roots are 1 and $(-1-i\sqrt{3})/2 = \epsilon' = 1/\epsilon = \epsilon^2$.

As $X^3 - 1 = (X - 1)(X^2 + X + 1)$ it also holds that $\epsilon^2 + \epsilon + 1 = 0$.

Closure under addition and subtraction is obvious. Let us have a closer look at multiplication:

$$(m + n\epsilon)(s + t\epsilon) = ms + (mt + ns)\epsilon + nt\epsilon^2 = (ms - nt) + (mt + ns - nt)\epsilon,$$

as $\epsilon^2 + \epsilon + 1 = 0$. The crucial fact is that ϵ satisifies a polynomial equation with leading coefficient 1, and all coefficients integers. It is an *algebraic integer.*

In the same manner one verifies the ring property of $\mathbf{Z}[\omega] = \mathbf{Z}[(1 + \sqrt{D})/2]$ where D is an integer, positive or negative, $|D|$ square-free (not divisible by a square > 1) satisfying $D \equiv 1 \pmod 4$.

The idea is the same, ω is an algebraic integer, satisfying $\omega^2-\omega+(1-D)/4 = 0$.

In fact, all elements of $\mathbf{Z}[\omega]$ are algebraic integers, and all algebraic integers in $\mathbf{Q}[\sqrt{D}]$ lie in $\mathbf{Z}[\omega]$. Exercise.

If $D \not\equiv 1 \pmod 4$, square-free, the corresponding statement is true for the ring $\mathbf{Z}[\sqrt{D}]$. □

When discussing prime factorization in the ring **Z** we achieved uniqueness by insisting on dealing only with positive numbers. Otherwise, we would have had to take signs into account.

When dealing with negative integers as well, the negatives of prime numbers should be given equal status to the primes themselves. Primes and their negatives are the *irreducibles* in **Z**; they still allow only the trivial factors ± 1, $\pm p$. And we will now have unique factorization in irreducibles, up to the signs of the various factors.

What would the "trivial" factors be in more general number rings? What is so trivial about ± 1 is they are the *invertible* elements in **Z**, also known as *units*; in fact they are their own (multiplicative) inverses.

K.I.5 Definition. Let R be a number ring. The element $\alpha \in R$ is a **unit** in (of) R if there is some $\beta \in R$ satisfying $\alpha\beta = 1$.

K.I.6 Definition. Let R be a number ring. The non-unit, non-zero element $\pi \in R$ is **irreducible** in R if the relation $\alpha\beta = \pi$, $\alpha, \beta \in R$, implies that α or β is a unit.

Before we determine the units of some rings it is convenient to introduce the *norm* in certain number fields.

K.I.7 Definition. Let K be a quadratic number field, i.e., $K = \mathbf{Q}[\sqrt{D}]$ or $K = \mathbf{Q}[i\sqrt{D}]$, D positive, not a perfect square. The **norm**, $N(a + b\sqrt{D})$, of $\alpha = a + b\sqrt{D}$, $a, b \in \mathbf{Q}$ is the element $\alpha \cdot \alpha' = a^2 - Db^2$. The norm of $\alpha = a + ib\sqrt{D}$, $a, b \in \mathbf{Q}$ is $\alpha \cdot \alpha' = a^2 + Db^2$.

Recall that α' denotes $a - b\sqrt{D}$ in the real case, and $a - ib\sqrt{D}$ in the complex case.

In the complex case the norm is always ≥ 0, and only 0 has zero norm. In the real (first) case the norm can assume both positive and negative values.

But, again, only 0 is of zero norm. For, if $a^2 - Db^2 = 0$, looking at an arbitrary prime factor $p|D$ we get $v_p(D) = 2(v_p(a) - v_p(b))$, hence all $v_p(D)$ are even, and D would be a square, contrary to assumption.

We have used the following multiplicativity property many times in earlier Chapters.

K.I.8 Lemma. *In any quadratic number field,*

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Proof.

$$(\alpha\beta)(\alpha\beta)' = \alpha\beta\alpha'\beta' = (\alpha\alpha')(\beta\beta').$$

□

We are now ready to determine the units in a few number rings. We start with two complex quadratic rings having more than two units.

K.I.9 Theorem. *The units in $R = \mathbf{Z}[i]$ are ± 1, $\pm i$.*

Proof. Obviously these four elements are invertible.

Assume $m + ni$, $m, n \in \mathbf{Z}$ invertible: $(m + ni)(r + si) = 1$, $r, s \in \mathbf{Z}$. Taking norms we get $(m^2 + n^2)(r^2 + s^2) = 1$ which is possible only if both norms equal 1. This gives us $m + ni = \pm 1, \pm i$ as the only possible units. □

K.I.10 Theorem. *Let $\epsilon = (-1 + i\sqrt{3})/2$. The units in $R = \mathbf{Q}[\epsilon]$ are the six elements $\pm 1 \pm \epsilon$, $\pm\epsilon^2$ (the roots of $X^6 - 1$).*

Proof. We first determine the norm of $m + n\epsilon$ in $\mathbf{Z}[i\sqrt{3}]$. As $m + n\epsilon = (m - n/2) + in\sqrt{3}/2$ we can rewrite the elements as $(r + si\sqrt{3})/2$ where $r = 2m - n$, $s = n$ and r, s are congruent modulo 2, i.e., both even or both odd. The norm is then $(r^2 + 3s^2)/4$ so we are to solve the Diophantine equation $r^2 + 3s^2 = 4$. The solution $r = \pm 2$, $s = 0$ immediately gives the trivial units ± 1.

Then there are the solutions $r = \pm 1$, $s = \pm 1$ (independent signs) giving the four solutions $\pm(1 \pm \sqrt{3})/2$. The solutions with $r = -1$ are ϵ, ϵ^2; those with $r = 1$ are $-\epsilon^2, -\epsilon$. □

In the real number ring $\mathbf{Z}[\sqrt{D}]$ the units are the elements of norm $+1$ or -1, i.e., the solutions to $m^2 - Dn^2 = \pm 1$.

We already know, from the theory of continued fractions, that there are infinitely many units of norm $+1$, and we know of cases where units of norm -1 exist, or not.

We should give a final, more exotic, example, of units in a ring.

K.I.11 Example. Let $\omega = (1 + \sqrt{5})/2$. Consider the number ring $\mathbf{Z}[\omega]$. Recall that this is a ring, as ω satisfies the equation $X^2 + X - 1 = 0$ with leading coefficient one.

The elements $m + n(1 + \sqrt{5})/2$ are more conveniently written $(r + s\sqrt{5})/2$ where $r \equiv s \pmod 2$. The units are the elements of norm ± 1, $r^2 - 5s^2 = \pm 4$. The square roots of 5 modulo 4 are, trivially, $P = \pm 1$.

For -4 we immediately find the solutions $(1 \pm \sqrt{5})/2$ belonging to ± 1 respectively. We know from Section H.IV that we get all solutions by multiplying each with all solutions to $x^2 - 5y^2 = \pm 1$. They are $x + y\sqrt{5} = \pm(2 + \sqrt{5})^n$, $n \in \mathbf{Z}$. Their number is infinite. □

We should give a name to the other trivial factor of an irreducible.

K.I.12 Definition. Two elements of a number ring R are **associates** if they differ by a unit factor.

Of course, if $\alpha = \delta\beta$, $\delta\gamma = 1$, then $\beta = \gamma\alpha$, so the situation is totally symmetric. We also see that associates are mutually divisible.

The converse is also true, for if $\alpha = \delta\beta, \beta = \gamma\alpha$, then $(1 - \delta\gamma)\alpha = 0$, hence $\delta\gamma = 1$.

So the only factors of an irreducible element are its associates and the units.

K.I.13 Example. We will presently determine all irreducibles in $\mathbf{Z}[i]$. Here we give just a few examples.

A couple of examples are $\pi = 1+i$, $4+i$, $3+2i$, $5+2i$, $5+4i$ having prime norm 2, 17, 13, 29, 41. Recall that the norm is multiplicative. If $\pi = \alpha\beta$, one of the two factors must then have norm equal to 1, i.e., one factor must be a unit. Hence these five, and in fact all elements of prime norm, are irreducible.

Another class of examples is represented by $\pi = 11$ of norm $11^2 = 121$. Again, if $\pi = \alpha\beta$, neither factor a unit, both factors must be of norm 11. However, a norm is a sum of two squares, and $11 \equiv 3 \pmod 4$ is not such a sum. Recall that this was the *easy* case, accessible by simple computing modulo 4. □

K.II Unique Factorization in $\mathbf{Z}[i]$

As in $\mathbf{Z}$ the key to unique factorization is Euclid and Bézout, so our first task is to establish an analogue to the division algorithm in $\mathbf{Z}[i]$. What should we demand of the remainder on division of $a+bi$ by $m+ni$? It should be in some sense smaller than $m+ni$, and the natural measure of its size is the norm.

K.II.1 Theorem (Complex Division). *Let $a+bi$ and $m+ni \neq 0$ be elements of $R = \mathbf{Z}[i]$. Then there are elements $p+qi$, $r+si \in R$, such that*

$$a+bi = (p+qi)(m+ni) + r+si, \quad 0 \leq N(r+si) < N(m+ni).$$

Proof. We start by exact division in the field $K = \mathbf{Q}[i]$:

$$\frac{a+bi}{m+ni} = t+ui, \quad t,u \in \mathbf{Q}.$$

We then replace the rational numbers t,u by the nearest integers p,q with $|p-t| \leq 1/2$, $|q-u| \leq 1/2$, so that $N((t+ui)-(p+qi)) \leq (1/2)^2+(1/2)^2 = 1/2 < 1$.

Setting $r+si = [(t-p)+i(u-q)](m+ni)$ we then have

$$\begin{aligned} a+bi &= (p+qi)(m+ni) + [(t-p)+i(u-q)](m+ni) \\ &= (p+qi)(m+ni) + (r+si) \end{aligned}$$

and

$$\begin{aligned} N(r+si) &= N[(t-p)+i(u-q)]N(m+ni) \\ &\leq \frac{1}{2}N(m+ni) < N(m+ni). \end{aligned}$$

□

Remark: Students sometimes ask how we can be so sure that the remainder is a complex integer. By its expression it does not exactly look like one. It is the *difference* of two complex integers!

K.II.2 Example. We want to divide $4+7i$ by $3-i$. The exact, rational, quotient is $(4+7i)(3+i)/(3-i)(3+i) = (5+25i)/10 = (1+5i)/2$. Here the real and imaginary parts sit halfway between two integers so we have four choices of a nearest complex integer. We pick $0+2i$, and the result is:

$$4+7i = 2i(3-i)+2+i,$$

where $N(2+i) = 5 < 10 = N(3-i)$. □

We now give the theory of common divisors parallelling that of **Z**. A greatest common divisor would be one of greatest possible norm, but how unique is it? We take a Bézoutian route to it.

K.II.3 Theorem (On the Greatest Common Divisor). *Let the two elements $\alpha_1, \alpha_2 \neq 0$ in $R = Z[i]$ be given. Then among the non-zero elements $\beta_1\alpha_1 + \beta_2\alpha_2$, $\beta_1, \beta_2 \in R$ there is some, δ, of smallest possible norm.*

The number δ is a common divisor of α_1, α_2.

Every common divisor of α_1, α_2 divides δ. It is therefore a common divisor of greatest possible norm. Two such greatest common divisors are mutually divisible, hence associates.

Proof. Only the statement in the second paragraph wants proof.

Suppose, e.g., that δ does not divide α_1. Then perform the division: $\alpha_1 = \kappa\delta + \rho$, with $0 \leq N(\rho) < N(\delta)$. But ρ is of the form $\alpha_1 - \kappa(\beta_1\alpha_1 + \beta_2\alpha_2)=$

$\lambda_1\alpha_1 + \lambda_2\alpha_2$, hence of the same form as δ. As δ was chosen $\neq 0$, and of minimal norm, we must have $\rho = 0$. □

We write $\delta = (\alpha_1, \alpha_2)$, for any greatest common divisor of α_1, α_2 although it is not quite unique. For instance, $(\alpha_1, \alpha_2) = 1$ means that the only common divisors in R are $\pm 1, \pm i$.

K.II.4 Example. We can find the greatest common divisor by Euclid, just as in $\mathbf{Z}$. Let us try $(7+6i, 4+7i)$:

$$\begin{aligned} 7+6i &= 1\cdot(4+7i) + (3-i) \\ 4+7i &= 2i\cdot(3-i) + (2+i) \\ 3-i &= (1-i)(2+i) \end{aligned}$$

so $(7+6i, 4+7i) = 2+i$. □

The two Divisibility Theorems for rational integers (A.II.1, A.II.2) carry over with almost the same proofs, so we omit these.

K.II.5 Theorem (The Two Divisibility Theorems).

a) If α divides $\beta\gamma$, and $(\alpha, \gamma) = 1$, then α divides β.

b) If α, β divide γ, and $(\alpha, \beta) = 1$, then the product $\alpha\beta$ divides γ.

□

K.II.6 Corollary. *If the irreducible element π divides $\alpha\beta$, then it divides one of the factors.*

Proof. If $\pi \nmid \alpha$, then $(\pi, \alpha) = 1$, hence $\pi | \beta$. □

An immediate induction gives

K.II.7 Corollary. *If the irreducible element* π *divides* $\alpha_1\alpha_2\cdots\alpha_d$*, then it divides one of the factors.*

□

So now we can prove the existence and (in some sense) uniqueness of factorization in R.

K.II.8 Theorem. *Every non-zero, non-unit, element of* R *is a product of irreducible elements.*

Proof. Otherwise there is a counterexample α of minimal norm. It is not irreducible, i.e., $\alpha = \beta\gamma$, where neither factor is a unit, hence both factors are of lower norm. By the choice of α they are then products of irreducibles. But then so is their product α, contradiction. □

The next Theorem states that factorization into irreducibles is unique up to unit factors.

K.II.9 Theorem (Unique Factorization). *Suppose*

$$\alpha = \pi_1 \cdot \pi_2 \cdots \pi_d = \epsilon \cdot \pi_1' \cdot \pi_2' \cdots \pi_e', \quad d \leq e,$$

where ϵ *is a unit, the* π_i, π_j' *irreducible.*

Then $d = e$*, and the factors* π_k' *may be reordered in such a way that* π_k *and* π_k' *are associates.*

Proof. The proof is an easy induction on d. If d =1, then obviously $e = 1$, otherwise π_1 would decompose into several non-unit factors.

Now for the step $d - 1 \rightarrow d$. Suppose the Theorem already proved for $d-1 \geq 1$. As π_1 divides the product in the right member, it must divide one of the factors, say π_j', $\pi_j' = \pi_1\kappa$. As π_j' is irreducible, and π_1 is a non-unit, κ

must be a unit, i.e., π_1 and π'_j are associates. We reorder the factors of the right member so that new π'_1 = old π'_j.

We can then divide both members by π_1 and move κ to the unit factor ϵ.

As the product of units, $\epsilon\kappa$, is a unit, the induction step goes through. □

We will refer to the above result as *the Unique Factorization Property* of R.

K.II.10 Example. $13 = (3+2i)(3-2i) = i(3+2i)(-i)(3-2i) = (-2+3i)(-2-3i)$. □

K.II.11 Example. In an earlier Example (K.II.4) we determined $(7+6i, 4+7i) = 2+i$. For hand calculation it might be more convenient to look at the norms first: $N(7+6i) = 85$, $N(4+7i) = 65$. Any common factor must divide the two norms, hence it must divide $(85, 65) = 5$. The gcd cannot be $5 = (2+i)(2-i)$ so it must be one of the two irreducible factors $2+i$ or $2-i$. A simple check gives $2+i$. □

We now finally determine which primes in $\mathbf{Z}$ are reducible or irreducible in R.

K.II.12 Lemma. *The prime number $p \in \mathbf{Z}$ is reducible in R if and only if it is a sum of two squares, i.e., if and only if it is a norm.*

Proof. One direction is immediate: If $p = a^2+b^2$, then $p = (a+ib)(a-ib)$.

In the opposite direction, if $p = (a+bi)(c+di)$, neither factor a unit, then, taking norms, $p^2 = (a^2+b^2)(c^2+d^2)$. As neither factor equals one, both must equal p. □

K.II.13 Corollary. *Primes $p \in \mathbf{Z}$, $p \equiv 3 \pmod 4$ remain irreducible in R.*

Proof.

$$a^2 + b^2 \equiv 0, 1, \text{ or } 2 \pmod 4.$$

□

We can now give a new proof of an old result:

K.II.14 Theorem. *Primes* $p \equiv 1 \pmod 4$ *are reducible in* R*, hence they are sums of two squares.*

Proof. As $(-1/p) = 1$, the congruence

$$x^2 \equiv -1 \pmod p$$

is solvable. So, for some $x \in \mathbf{Z}$, $p|(x^2+1) = (x+i)(x-i)$. If p were irreducible it would have to divide one of the factors. This is impossible as p does not divide the imaginary parts ± 1. Hence p is reducible. □

Note that the prime $2 = (1+i)(1-i)$ is also reducible.

We conclude this Section by determining all the irreducible elements of R.

K.II.15 Theorem. *The irreducible elements are the associates to*

a) $1 + i$

b) prime numbers $p \equiv 3 \pmod 4$

c) $a \pm bi$ *where* $p = a^2 + b^2$ *is a prime number* $\equiv 1 \pmod 4$

Proof. Let the irreducible be $\alpha = a + ib$, of norm $N = N(\alpha) = \alpha \cdot \alpha' = a^2 + b^2$. The number α, being irreducible, must divide some prime factor p of N, $p = \alpha \cdot \gamma$. If γ is a unit, α and p are associates, and we are in case b), as other prime numbers are reducible.

Otherwise $p^2 = N(p) = N(\alpha) \cdot N(\gamma)$ with both factors > 1, $N(\alpha) = \alpha \cdot \alpha' = p$. If $p = 2 = -i(1+i)^2 = (1+i)(1-i)$ we are in case a), as α must be associated to one of the two irreducible factors. If $p \equiv 1 \pmod 4$ we are in case c). □

K.II.16 Example (Computation of $\boldsymbol{\pi}$). From Calculus the reader may know about the series

$$\arctan x = x - \frac{x^3}{3} + \frac{x^5}{5} - \cdots , \quad |x| < 1$$

derived by expanding $1/(1+t^2)$, $|t| < 1$, in a geometric series, and integrating from 0 to x.

Actually, the series converges for $x = \pm 1$ as well, and gives the expected result $\pm\pi/4$. However, it takes a greater effort to prove that sum, and convergence is too slow to be of practical value for the computation of π.

The arctan series is a *Leibniz series*, i.e., it is of the form

$$\sum_{n>0} (-1)^n a_n, \quad a_0 \geq a_1 \geq a_2 \cdots \geq a_{n-1} \geq a_n \cdots \to 0$$

Approximating the sum of such a series with a partial sum, the error is majorized by the absolute value of the first term excluded – these facts are proved in any serious book on Analysis. (If the a_n sequence is convex, i.e., if the (positive) differences $a_n - a_{n+1}$ decrease, one can prove that the error is minorized by half that term).

In our specific example, if the last term included is $(-1)^n x^{2n+1}/(2n+1)$ the error is $\leq |x^{2n+3}|/(2n+3)$. So one would want to substitute as small values as possible for x.

One way to do this is to use the identity

$$\arctan \frac{1}{2} + \arctan \frac{1}{3} = \frac{\pi}{4}$$

and substitute $x = 1/2, 1/3$ in the series. The identity follows directly from $(2+i)(3+i) = 5(1+i)$ on comparing arguments.

It is natural to ask for improvements. We need identities involving products or quotients of numbers of the form $a + i$ resulting in an associate of $1 + i$, or an odd power.

Let us check the factorization of some small numbers:

$$\begin{aligned}
2+i &= 2+i \\
3+i &= (1+i)(2-i) \\
4+i &= 4+i \\
5+i &= (1+i)(3-2i) \\
6+i &= 6+i \\
7+i &= (1-i)(2+i)^2
\end{aligned}$$

Here we see by mere inspection that

$$(7+i)(3+i)^2 = 50 \cdot (1+i)$$

whence

$$\arctan\frac{1}{7} + 2\arctan\frac{1}{3} = \frac{\pi}{4}$$

which is a slight improvement.

The reader may enjoy writing a small program finding numbers of the form a^2+1 that factor over a small base consisting of 2 and a few prime numbers $p \equiv 1 \pmod 4$, then factoring further, and combining to produce the desired multiples of $1 \pm i$.

The numbers $a = 8$, 18, 38, 57, 239, 268 will probably strike the reader as useful. He/she will probably discard findings like $(13+i)(2+i)(4+i) = 85(1+i)$.

□

K.II: Exercises

1. (a) Factor 12 and $6+8i$ into irreducibles in the ring $\mathbf{Z}[i] = R$.

(b) Same ring. Determine the gcd $g = (15, 3+i)$.

(c) g as in the previous item. Find the inverse class of $66 + 171\,i$ modulo g in R (suitably defined).

2. Solve, whenever possible, or prove unsolvability, in complex integers x, y:

(a) $x(1+2i)+y(3+i)=1$

(b) $x \cdot 2+y(3+i)=1-i$

(c) $x(4+i)+y(3+2i)=1$

3. (a) We study the residue classes $m+ni+(2+2i)$, i.e., the sets of complex integers $m+ni+(a+ib)(2+2i)$, $a+ib \in \mathbf{Z}[i]$. Show that each class has a representative $m+ni$, with $|m| \leq 1, -1 \leq n \leq 2$. Find the number of classes.

(b) Then show that each complex integer $m+ni$, of odd norm, is associated to exactly one number $\equiv 1 \pmod{2+2i}$.

4. Show that the equation $x^2+y^2-3t^2-3u^2=0$ is unsolvable in integers.

5. $R=\mathbf{Z}[i]$.

(a) Let q be a prime number, $\equiv 3 \pmod 4$. Show that q divides $m+in$ in R if and only if q divides both m and n. Conclude that the number of residue classes modulo q is $N(q)=q^2$.

(b) Let $p=a^2+b^2$ be a prime number, $\equiv 1 \pmod 4$. Let the integer j satisfy $j^2 \equiv -1 \pmod p$. Show that j can be chosen so that $a+bj \equiv 0$ $\pmod p$.

(c) Show, using the last item, that there is a bijection between the classes modulo p in $\mathbf{Z}$ and the classes modulo $a+ib$ in R. The number of residue classes modulo $a+ib$, therefore, equals $p=N(a+ib)$.

6. A geometric (and more general) approach to the norm. Let $z=a+ib$, $(a,b)=1$. Consider the square with vertices at $0, z, iz, (1+i)z$.

(a) Show that the area of the square is $N(a+ib)=a^2+b^2$.

(b) Convince yourself that the number of lattice points (complex integers) in the interior of the square, plus 0, equals the area a^2+b^2. Hint: Find a suitable set of unit squares that cover the same area.

(c) Show that every complex integer is congruent modulo z to exactly one of the lattice points considered above. Conclude that $N(z)$ equals the number of residue classes modulo z.

(d) Can you modify the above proof to deal with the case $(a,b)>1$ as well?

7. Let K denote the quadratic number field $\mathbf{Q}[\sqrt{D}]$, where D is a positive or negative square-free number (i.e., not divisible by a perfect square > 1).

Show that the set of algebraic integers (p. 292) in K is the ring

(a) $\mathbf{Z}[\sqrt{D}]$ if $D \equiv 2, 3 \pmod 4$.

(b) $\mathbf{Z}[(1+\sqrt{D})/2]$ if $D \equiv 1 \pmod 4$.

8. Suggestions for computing. See the last Example above.

K.III The Number of Representations

Assume that N admits the representation

$$N = x^2 + y^2 = (x + iy)(x - iy)$$

as a sum of two squares. Recall the condition for this: primes $p \equiv 3 \pmod 4$ should only enter the factorization of N with even multiplicity. We now determine the number of *all* representations.

As a byproduct one will be able to determine the number of proper representations, $(x, y) = 1$, very quickly.

We first fix some notation. Assume that

$$N = \prod_{1 \le j \le r} p_j^{e_j} \cdot \prod_{1 \le k \le s} q_k^{f_k} \cdot 2^g$$

where $p_j = a_j^2 + b_j^2 = (a_j + ib_j)(a_j - ib_j) = \pi_j \cdot \pi_j'$ are primes $\equiv 1 \pmod 4$, and q_k are primes $\equiv 3 \pmod 4$.

In $\mathbf{Z}[i]$ the full factorization is

$$\begin{aligned} N = (x + iy)(x - iy) &= \prod_{1 \le j \le r} (\pi_j \pi_j')^{e_j} \cdot \prod_{1 \le k \le s} q_k^{f_k} \cdot (1 + i)^g (1 - i)^g \\ &= \prod_{1 \le j \le r} (\pi_j \pi_j')^{e_j} \cdot \prod_{1 \le k \le s} q_k^{f_k} \cdot (-i)^g (1 + i)^{2g} \end{aligned}$$

We first determine a complete set of non-associate $x + iy$. "Complete" means that each $u + iv, N = (u + iv)(u - iv)$, is to be an associate to (exactly) one member of the set. Note that within the set we do (and must) allow conjugates.

For instance, if $N = 17^2$, then $(4 + i)^2 = 15 + 8i$, $17^2 + 0i$, $(4 - i)^2 = 15 - 8i$ is such a complete set, and the number of representations is $4 \cdot 3 = 12$, the factor 4 coming from the number of units.

First of all, if $q_k^d | (x + iy)$ then also $q_k^d | (x - iy)$ so $x + iy$ and $x - iy$ contain the same number of q_k, and we rediscover the fact that all the f_k are even.

And, as $1 + i$, $1 - i$ are associates, and $1 + i | (x + iy)$ if and only if $1 - i | (x - iy)$ we see that $x + iy$ and $x - iy$ contain the same number of factors $1 + i$.

As for the factors $\pi_j^{e_j} \cdot {\pi'}_j^{e_j}$ we note that $\pi_j^d | x \pm iy$ if and only if ${\pi'}_j^d | x \mp iy$. Therefore we simply have the $e_j + 1$ choices how many factors π_j go into

$x+iy$ and how many go into $x-iy$, determining the corresponding numbers for the π'_j.

Our complete set therefore has

$$\prod_{1\le j\le r}(e_j+1)$$

elements. We then get all possible $x+iy$ by multiplying these with the four units.

We have proved:

K.III.1 Theorem. *Notation as above. Assume that prime numbers* $q\equiv 3 \pmod 4$ *only enter the factorization of* N *with even multiplicity.*

The number or representations $N=x^2+y^2$*, taking the order and sign combinations of* x, y *into account, is then*

$$4\prod_{1\le j\le r}(e_j+1).$$

□

K.III.2 Example. $N=17\cdot 29^3=414613$. Fixing one factor, $4+i$, of 17, gives us the following four possibilities:

$$\begin{aligned}
&(4+i)(5+2i)^3=118+633i\\
&(4+i)(5+2i)^2(5-2i)=29(4+i)(5+2i)=29(18-14i)\\
&(4+i)(5+2i)(5-2i)^2=29(4+i)(5-2i)=29(22-3i)\\
&(4+i)(5-2i)^3=402-503i
\end{aligned}$$

Choosing the factor $4-i$ leads to the conjugates of these four (in the opposite order). Then, finally, we have the choice of four unit factors. That accounts for the $4(1+1)(3+1)=32$ representations of N.

We easily read off the proper representations of N. They are

$$N=414613=118^2+633^2=402^2+503^2.$$

□

We now sketch the result on the number of *proper* representations of an odd number N. We leave $2N$ as an exercise.

K.III.3 Theorem. *Assume that N is the product*

$$\prod_{j=1}^{t} p_j^{e_j}$$

of t prime powers, each prime $p_j \equiv 1 \pmod 4$. Then the number of proper representations $N = x^2 + y^2$, $(x, y) = 1$, taking the order and sign combinations of x, y into account, is 2^{t+2}. Ignoring these, the number is 2^{t-1}.

Proof. (sketch). Refer to the notation of the previous Theorem and its proof. When distributing the π_j, π'_j over the factors $x + iy, x - iy$ the whole power $\pi_j^{e_j}$ must go into one factor and the conjugate power into the other. Otherwise one of them would be divisible by $\pi_j \cdot \pi'_j = p_j$, hence x, y would have the common factor p_j. So for each prime p_j we have two choices which power goes where. That gives 2^t choices, all of them proper (cf. E.II.4).

Then we have counted everything twice, so there are really 2^{t-1} genuinely different representations. Taking order and sign combinations into account we have to multiply by 8, hence the number is 2^{t+2}. □

K.IV $\mathbf{Z}[-\frac{1}{2} + i\frac{\sqrt{3}}{2}]$

Our next example of a quadratic number ring is $\mathbf{Z}[i\sqrt{3}]$. The elements are $m + in\sqrt{3}$, $m, n \in \mathbf{Z}$ and the norm is $m^2 + 3n^2$. The only elements of norm 1 are ± 1, hence these are the only units.

We try to establish a division algorithm as we did for $\mathbf{Z}[i]$. Just as in that case we want to replace an exact quotient $p + iq\sqrt{3}$, $p, q \in \mathbf{Q}$ by the nearest $m + in\sqrt{3}$, $m, n \in \mathbf{Z}$. But taking the norm of the difference $(p-m) + i(q-n)\sqrt{3}$ we only get the estimate

$$(p - m)^2 + 3(q - n)^2 \leq (1/2)^2 + 3(1/2)^2 = 1,$$

and we need strict inequality (cf. the proof of Theorem **??**).

No use trying! If there were a division algorithm we would be able to prove unique factorization the same way as in $\mathbf{Z}[i]$. But the following is a very simple counterexample:

$$4 = 2 \cdot 2 = (1 + i\sqrt{3})(1 - i\sqrt{3}).$$

The numbers entering both factorizations are irreducible. As their norms are =4, any nontrivial factor would have to have norm =2, which is clearly impossible.

And, as the only units are ±1, the number 2 is not associated with $1 + i\sqrt{3}$ or $1 - i\sqrt{3}$.

We are looking at the wrong ring! Look instead at $R = \mathbf{Z}[\epsilon]$, where $\epsilon = (-1 + i\sqrt{3})/2$. In that ring we have shown $(1 \pm i\sqrt{3})/2$ to be units, and in this larger ring $1 \pm i\sqrt{3} = 2 \cdot (1 \pm i\sqrt{3})/2$. Hence, in R the two factorizations differ by unit factors.

So we try to prove the existence of a division algorithm in that ring, instead. We have shown (K.I.10) that the norm of $p + q\epsilon$, $p, q, \in \mathbf{Q}$, is

$$\frac{(2p-q)^2 + 3q^2}{4} = \frac{4p^2 - 4pq + 4q^2}{4} = p^2 - pq + q^2.$$

Let m, n be integers; then

$$N((p-m) + (q-n)\epsilon) = \frac{(2p - q + n - 2m)^2 + 3(q-n)^2}{4}.$$

We first choose n so that $|q - n| \leq 1/2$. We then choose m so that $|p - q/2 + n/2 - m| \leq 1/2$. Then

$$N((p-m)+(q-n)\epsilon) = \frac{(2p - q + n - 2m)^2 + 3(q-n)^2}{4} \leq \frac{1 + 3/4}{4} = \frac{7}{16} < 1.$$

So now the whole theory goes through, and

K.IV.1 Theorem. *R has the Unique Factorization Property (cf. K.II.9).*

□

Remark: A more direct proof would have been to look at the expression $(p-m)^2-(p-m)(q-n)+(q-n)^2$ and choosing m, n to be nearest integers to p, q. This gives the inequality $(p-m)^2-(p-m)(q-n)+(q-n)^2 \leq 3/4$. The above procedure gives a sharper estimate and therefore covers more cases, e.g., where 3 is replaced by 7 or 11.

The following results are analogous to those on $\mathbf{Z}[i]$ and admit similar proofs.

K.IV.2 Theorem. $R = \mathbf{Z}[\epsilon]$, *where* $\epsilon = (-1+i\sqrt{3})/2$.

a) The prime number 3 is reducible. Its factorization into irreducibles is

$$3 = -\epsilon^2(1-\epsilon)^2.$$

b) A rational prime is reducible in R if and only if it is the norm of an element in R.

c) Primes $p \equiv 2 \pmod 3$ *remain irreducible in R.*

d) Primes $p \equiv 1 \pmod 3$ *are reducible in R. They are the norms* $m^2 - mn + n^2$ *of irreducible elements* $m + n\epsilon$, *or, stated differently ,* $p = (m+n\epsilon)(m+n\epsilon') = m^2 - mn + n^2$.

Proof. Part a) is a simple computation, taking into account that $\epsilon^2+\epsilon+1 = 0$. The number $1-\epsilon = (3-i\sqrt{3})/2$ is irreducible, as its norm, 3, is prime.

For part b), simply note that $N(m+n\epsilon) = (m+n\epsilon)(m+n\epsilon') = N(m+n\epsilon')$, where both factors have the same norm. So if p is a norm it is the product of two non-unit factors.

Conversely, suppose $p = \alpha \cdot \beta$, where neither factor is a unit. Then $N(p) = p^2 = N(\alpha)N(\beta)$ where the factors are ordinary positive integers > 1. Therefore $p = N(\alpha) = N(\beta)$.

For part c) we use b). If $p = N(m+n\epsilon) = m^2 - mn + n^2$ then $4p = (2m-n)^2 + 3n^2$. Modulo 3 we get $2 \equiv 0$ or $1 \pmod 3$, contradiction.

For part d) we note that $(-3/p) = 1$ by an early Example on Quadratic Reciprocity (Ex. D.I.13). Let $x^2 \equiv -3 \pmod p$, so that $p|(x+i\sqrt{3})(x-i\sqrt{3})$.

If p were irreducible it would have to divide $x+i\sqrt{3}$ or $x-i\sqrt{3}$, impossible. So p is a norm, by part b). □

And, now, in a manner very similar to $\mathbf{Z}[i]$ we can prove the following Theorem.

K.IV.3 Theorem. *The irreducible elements in R are the associates of*

a) $1-\epsilon = (3+i\sqrt{3})/2$;

b) prime numbers $p \equiv 2 \pmod 3$;

c) $m+n\epsilon, m+n\epsilon' = m+n\epsilon^2$, $m,n \in \mathbf{Z}$; *satisfying* $m^2-mn+n^2 = p$ *where p is a prime number* $\equiv 1 \pmod 3$.

Proof. Let the irreducible be α, of norm $N = N(\alpha) = \alpha \cdot \alpha'$. The number α, being irreducible, must divide some prime factor p of N, $p = \alpha \cdot \gamma$. If γ is a unit, α and p are associates, and we are in case b), as other prime numbers are reducible.

Otherwise $p^2 = N(p) = N(\alpha)\cdot N(\gamma)$ with both factors > 1, $N(\alpha) = \alpha\cdot\alpha' = p$. If $p = 3 = -\epsilon^2(1-\epsilon)^2$ we are in case a). If $p \equiv 1 \pmod 3$ we are in case c). □

Remark: In Section E.III we proved that all primes $p \equiv 1 \pmod 3$ can be written in the form $p = x^2+3y^2$ and derived the form $m^2 \pm mn + n^2$ from that.

Going in the opposite direction is easy if n (or m) is even, $n = 2s$, because then $m^2-2ms+4s^2 = (m-s)^2+3s^2$. If both m and n are odd, then $m^2-mn+n^2 = ((m+n)/2)^2 + 3((m-n)/2)^2$ (cf. old exercise, page 20).

In the exercises you are invited to study further number rings using the techniques just established.

K.IV: Exercises

1. The norm. Refer to the last problem on p. 304.

We are in the ring R studied in this Section. Let $z = (m+in\sqrt{3})/2 \in R$, with m, n of equal parity. Form the parallellogram with vertices in $0, z, \theta z, (1+\theta)z$, where $\theta = (1+i\sqrt{3})/2$.

Relate its area, and the number of ring elements inside the parallellogram to the norm of z, and the number of residue classes modulo z, copying the ideas of the cited problem as closely as possible.

2. In the ring $R = \mathbf{Z}[i\sqrt{5}]$, show that that $2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$ are two factorizations of 6 into irreducible factors (check the norms) showing that R does not possess the Unique Factorization Property.

3. (You may have worked this problem before, in the context of Thue's Lemma, E.I.1.)

(a) Let $\theta = (1+\sqrt{5})/2$ and let R denote the number ring $\mathbf{Z}[\theta]$ (check the ring property!). Copy the theory for the ring $\mathbf{Z}[\epsilon]$ as closely as possible to show that R has the Unique Factorization Property.

(b) Let $p \neq 2, 5$ be a prime number representable as $p = x^2 + xy - y^2$, x, y integers. Show that $p \equiv 1$ or $4 \pmod 5$.

(c) Show that $(5/p) = 1$ if and only if $p \equiv 1$ or $4 \pmod 7$. Copying the theory for $\mathbf{Z}[\epsilon]$, show that p is representable as $p = x^2 + xy - y^2$, x, y integers (the norm in R).

(d) Conclude that $p = u^2 - 5v^2$ for suitable integers u, v. The case where x, y are both odd is solved by setting $y = x - 2z$.

4. (a) Let $\theta = (1+i\sqrt{7})/2$ and let R denote the number ring $\mathbf{Z}[\theta]$ (check the ring property!). Copy the theory for the ring $\mathbf{Z}[\epsilon]$ as closely as possible to show that R has the Unique Factorization Property.

(b) Let $p \neq 2, 7$ be a prime number representable as $p = x^2 + xy + 2y^2$, x, y integers. Show that $p \equiv 1, 2$ or $4 \pmod 7$.

(c) Show that $(-7/p) = 1$ if and only if $p \equiv 1, 2,$ or $4 \pmod 7$. Copying the theory for $\mathbf{Z}[\epsilon]$, show that p is representable as $p = x^2 + xy + 2y^2$, x, y integers (the norm in R).

(d) Determine the parities of x, y in that representation and conclude that $p = u^2 + 7v^2$ for suitable integers u, v.

5. An algorithm for solving $x^2 + xy + y^2 = p$, $p = 3 \cdot n + 1$, a prime. Fill in the details, comparing to the algorithm given previously (E.I.5) for $x^2 + y^2 = p$.

First, find x, y, such that $a_0 = x^n \not\equiv 1 \pmod p$, $b_0 = y^n \equiv 1 \pmod p$. Using $a_0^3 - b_0^3 \equiv 0 \pmod p$, prove that $a_0^2 + a_0 b_0 + b_0^2 = r_0 \cdot p$. By division, find A_0, B_0, such that $A_0^2 + A_0 B_0 + B_0^2 = r_1 r_0$, with $r_1 < r_0$. Prove that $a_1 - b_1\epsilon = (a_0 - \epsilon b_0)(A_0 - \epsilon^2 B_0)/r_0$ is an integral linear combination of 1 and ϵ, and proceed inductively from there.

Chapter L

Primality and Factorization

L.I Introduction

In this Section we present some of the primality tests and factorization methods in use up until the early 80's. There are several reasons for presenting these apparently outmoded algorithms.

First, they are still useful in finding small factors of a number. Second, they are for the most part easy to program, and therefore invite some instructive experimentation and toying with the concepts and the basic theory. Third, several of the modern methods elaborate on the classical methods so that the latter are still of didactical value as an introduction to the former.

The running times given should be taken with a grain of salt. For all the examples I used a 1.83 GHz 32–bit computer, and all of the programs were written in the high-level language Python 2.5. They would run several times faster if written and run in C.

No serious effort was spent on optimizing the programs. While it is certainly essential to minimize, e.g., the number of multiplications at each turn of a loop, my main concern was the programming effort involved.

Perhaps the inclusion of the now-defunct CFRAC algorithm wants justification. I am assuming that the reader has already devised a QCF routine and wants to put it to further use. The least he can do is "wait-for-a square" that requires very little additional programming.

Also, several of the techniques involved, among them Gaussian elimination mod 2, large prime variation, and the Brillhart-Morrison square-rooting process, are essential to the Quadratic Sieve algorithm, as is the earlier discussion on prime generation.

The early abort strategy is useful in other algorithms involving trial division over lists, e.g., the Index Calculus algorithm (p. 100) for discrete logarithms. Therefore, CFRAC could serve as a gentle introduction to these algorithms. It is also easier to illustrate in small examples.

So here we are, back in the 70's, but with the computer power of the 21st century. Hopefully, this Chapter will urge the reader to study the comprehensive texts listed under "Computational" in the Bibliography, and the surveys by Montgomery and Bernstein listed in the Web section there.

L.II Special Numbers, Special Factors

Numbers of the form $a^n \pm 1$ have attracted a lot of attention through the years. In order to study them we recall the geometric sum identity:

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

For odd n, replacing x by $-x$, and multiplying by -1, we also have

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \cdots - x + 1).$$

L.II.1 Theorem. *Let a, n be integers, a even, $n \geq 2$. If $a^n + 1$ is a prime, then n is a power of two.*

Proof. Suppose $n = t \cdot u$ where $u > 1$ is odd. Then, putting $x = a^t$ in the last identity above, we get

$$a^n + 1 = (a^t)^u + 1 = x^u + 1 = (x+1)(x^{u-1} - x^{u-2} + \cdots - x + 1)$$

with the first factor strictly between 1 and $a^n + 1$, showing $a^n + 1$ to be composite. Hence n has no odd factors. □

L.II.2 Theorem. *Let n, a be integers, $a > 1$, $n \geq 1$. If $(a^n - 1)/(a - 1)$ is a prime, then n is prime, too.*

Suppose n is composite, $n = t \cdot u$, where $t, u > 1$. Then, putting $x = a^t$ in the first identity above,

$$\begin{aligned}\frac{a^n - 1}{a - 1} = \frac{x^u - 1}{a - 1} = \frac{x - 1}{a - 1}(x^{u-1} + x^{u-2} + \cdots + x + 1)\\ = (a^{t-1} + a^{t-2} + \cdots + 1)(x^{u-1} + x^{u-2} + \cdots + x + 1),\end{aligned}$$

showing $(a^n - 1)/(a - 1)$ to be composite. Hence n is a prime. □

Numbers of the form $F_n = 2^{2^n} + 1$ are known as *Fermat numbers.* The first five of them, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$, are prime numbers. No further Fermat primes are known. We will later (L.VII.6) give a necessary and sufficient condition for a Fermat number to be a prime.

Numbers of the form $M_p = 2^p - 1$ are known as *Mersenne numbers.* Numbers of the form $(10^p - 1)/(10 - 1)$ are called (decimal) *repunits.*

In September 2008 46 Mersenne primes were known. The prime number

$$2^{43\,112\,609} - 1$$

was announced on August 23, 2008. Most prime number records have been Mersenne primes.

The prime decimal repunits known as of this writing are those with exponents 2, 19, 23, 317, 1031. A few more repunits have been found to be "probable" primes.

We can say something about the possible prime factors of either kind.

L.II.3 Theorem (Factors of Mersenne Numbers). *Let $p \geq 3$ be a prime, and q a prime factor of $2^p - 1$. Then $q \equiv 1 \pmod{2p}$, also $q \equiv \pm 1 \pmod{8}$.*

Proof. By assumption, $2^p \equiv 1 \pmod{q}$, and by Little Fermat, $2^{q-1} \equiv 1 \pmod{q}$. So $\mathrm{ord}_q(2)$ divides both the prime number p and $q - 1$. It cannot be 1, so it must equal p, whence $p|(q-1)$, $q = 1 + mp$. As q and p are odd, m must be even, $m = 2k$, $q = 1 + 2kp$.

So p divides $(q-1)/2$. As $2^p \equiv 1 \pmod{q}$, also $2^{(q-1)/2} \equiv 1 \pmod{q}$. By Euler's Criterion, $(2/q) = 1$, and by the Ergänzungssatz (D.I.11) $q \equiv \pm 1 \pmod{8}$. □

L.II.4 Theorem (Factors of Fermat Numbers). *If* $N = 2^{2^n} + 1$, $n \geq 2$, *and* p *is prime factor of* N, *then* $p \equiv 1 \pmod{2^{n+2}}$.

Proof. As $2^{2^n} \equiv -1 \pmod{p}$, $2^{2^{n+1}} \equiv 1 \pmod{p}$, and 2 is the only prime factor of 2^{n+1}, we see that $\mathrm{ord}_p(2) = 2^{n+1}$, for any prime factor p (cf. A.V.6). By Little Fermat, this implies that $p-1$ is divisible by 8, as $n \geq 2$.

Further, as $p \equiv 1 \pmod{8}$, 2 must be a quadratic residue modulo p. By Euler's Criterion that means that $\mathrm{ord}_p(2)|(p-1)/2$, so that, in fact, $p \equiv 1 \pmod{2^{n+2}}$. □

L.II.5 Example. A simple but classic example. The factors of the Fermat number

$$N = F_5 = 2^{32} + 1$$

must be of the form $1 + k \cdot 128$. In fact, the prime factorization is

$$N = 641 \cdot 6\,700\,417 = (5 \cdot 128 + 1) \cdot (52\,347 \cdot 128 + 1).$$

N is a ten-digit number, accessible by trial division, to be discussed below.

A quick way to verify the factor 641 is:

$$641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$$

Hence,

$$\begin{aligned} 5^4 \cdot 2^{28} &\equiv 1 \pmod{641}, \\ -2^4 \cdot 2^{28} &\equiv 1 \pmod{641}, \\ 2^{32} &\equiv -1 \pmod{641}. \end{aligned}$$

□

Riesel's book has lots of material on numbers of special algebraic forms.

L.III Trial Division

Almost the only method that factors a number and simultaneously verifies the primality of the factors is *trial division.* It is all but useless, however, when dealing with, say, 15-16-digit-numbers composed of two primes of similar size.

Let the number be N. We set a ceiling at its square root. We then keep dividing N by 2, 3, $6-1$, $6+1$, $2\cdot 6-1, 2\cdot 6+1, \ldots$ The first time the division leaves no remainder we have found a prime factor p. We check the multiplicity k of p and list these numbers. Then we set $N = N/p^k$ and lower the ceiling to the square root of *that* number. We continue in this manner. When we hit the ceiling possibly one factor remains. It is determined by yet another division.

This method verifies the primality of

$$N = 45122\,73113$$

in perhaps 0.2 seconds. An 11-digit-number like

$$N = 4\,13369\,70097$$

requires slightly more, but well less than a second.

Factoring

$$N = 31\ 61907\ 57417\ 40159 = 39\,229\,207 \cdot 806\,008\,537$$

even today takes about half a minute, way too slow!

Therefore the practical use of trial division is limited to perhaps finding the smallest prime factors up to, say, $5\cdot 10^5$ or even smaller.

If trial division is required on several numbers it might be profitable to create a list of prime numbers once and for all, using the Sieve of Eratosthenes.

L.IV Lists of Primes

Some factoring algorithms require a list of prime numbers of moderate size. The classical way to create such a list is the *Sieve of Eratosthenes.* Say we want to list all prime numbers from 2 to 150. We start by making a list of all odd numbers from 3 to 149:

$$\begin{array}{l}
[3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,\\
33,35,37,39,41,43,45,47,49,51,53,55,57,59,\\
61,63,65,67,69,71,73,75,77,79,81,83,85,87,89,\\
91,93,95,97,99,101,103,105,107,109,111,113,115,117,119,\\
121,123,125,127,129,131,133,135,137,139,141,143,145,147,149]
\end{array}$$

Starting with the 3 in position 0 we run through the list in steps of 3 and replace each following multiple of 3 by a zero:

$$\begin{array}{l}
[3,5,7,0,11,13,0,17,19,0,23,25,0,29,31,\\
0,35,37,0,41,43,0,47,49,0,53,55,0,59,\\
61,0,65,67,0,71,73,0,77,79,0,83,85,0,89,\\
91,0,95,97,0,101,103,0,107,109,0,113,115,0,119,\\
121,0,125,127,0,131,133,0,137,139,0,143,145,0,149]
\end{array}$$

Next we look at the 5 in position 1, and replace the numbers $5 \cdot 5$, $7 \cdot 5$, etc., i.e., the numbers in positions $1+m \cdot 5$, $m \geq 2 = (5-1)/2$, by zeros. We need not look at multiples below the square, as they have already been zeroed. The starting position for any given p in the list is $(p^2-3)/2$, in this case $(5^2-3)/2 = 11$.

$$\begin{array}{l}
[3,5,7,0,11,13,0,17,19,0,23,0,0,29,31,\\
0,0,37,0,41,43,0,47,49,0,53,0,0,59,\\
61,0,0,67,0,71,73,0,77,79,0,83,0,0,89,\\
91,0,0,97,0,101,103,0,107,109,0,113,0,0,119,\\
121,0,0,127,0,131,133,0,137,139,0,143,0,0,149]
\end{array}$$

We proceed similarly with the 7 in position 2, zeroing all numbers in positions $2+m \cdot 7$, $m \geq 3 = (7-1)/2$ (21 and 35 already zeroed):

$$\begin{array}{l}
[3,5,7,0,11,13,0,17,19,0,23,0,0,29,31,\\
0,0,37,0,41,43,0,47,0,0,53,0,0,59,\\
61,0,0,67,0,71,73,0,0,79,0,83,0,0,89,\\
0,0,0,97,0,101,103,0,107,109,0,113,0,0,0,\\
121,0,0,127,0,131,0,0,137,139,0,143,0,0,149]
\end{array}$$

Next in line is a zero in position 3. We simply skip that position and proceed to the 11 in position 4. This time only the numbers 121 and 143 are zeroed.

$$\begin{aligned}&[3, 5, 7, 0, 11, 13, 0, 17, 19, 0, 23, 0, 0, 29, 31,\\&0, 0, 37, 0, 41, 43, 0, 47, 0, 0, 53, 0, 0, 59,\\&61, 0, 0, 67, 0, 71, 73, 0, 0, 79, 0, 83, 0, 0, 89,\\&0, 0, 0, 97, 0, 101, 103, 0, 107, 109, 0, 113, 0, 0, 0,\\&0, 0, 0, 127, 0, 131, 0, 0, 137, 139, 0, 0, 0, 0, 149]\end{aligned}$$

Next in line would be 13. However, $13^2 = 169 > 150$, and we have already zeroed all the lower multiples of 13, so we stop here. It only remains to put in the number 2 and throw out the zeros:

$$\begin{aligned}&[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31,\\&37, 41, 43, 47, 53, 59,\\&61, 67, 71, 73, 79, 83, 89,\\&97, 101, 103, 107, 109, 113,\\&127, 131, 137, 139, 149]\end{aligned}$$

One time- and space-saving device is to start with a list of ones, and work with the positions rather than the numbers. Sieving will produce a list of ones and zeros, indicating the positions of the odd primes and composites.

With limited storage one will have to sieve in blocks. For instance, my computer readily sieves out the prime positions up to 10^8 in a matter of seconds, but resists sieving out the primes beyond $3 \cdot 10^7$.

Here is one possible solution. Fix the upper limit $= n$, and a blocklength B, say 10^6. Use an ordinary sieve to find all primes up to $r = \sqrt{n}$. Use only these to sieve beyond that limit. Let p_{max} be the largest prime $\leq \sqrt{n}$.

Imagine the odd numbers from $T = 2 + p_{max}$ to n divided into blocks, each, except the last, of length B. We sieve each block for positions. Initialize each block with all 1's. After sieving, for each remaining 1 output the prime corresponding to that position, and append it to your list, or whatever.

For each prime p you will need to know where to start sieving within a block. Suppose its left endpoint is L, odd (it is of the form $T + 2kB$). It is in position 0. Where is the nearest multiple of p located? If the position is y, we have to solve

$$L + 2y = (2m + 1)p$$

with $0 \leq y < p$, i.e., $2y = (p - L) + 2mp$, $y = (p - L)/2 + mp$. In other words, y is the least non-negative remainder of $(p - L)/2$ on division by p. We zero the ones in positions y, $y + p$, $y + 2p \cdots < B$. From one block to the next each y is simply updated as the remainder of $y - B$ on division by the corresponding prime number p.

This suggestion is an adaption of algorithm 3.2.1 in Crandall-Pomerance, designed to find primes in a given interval.

That book, and that of Bach-Shallit, suggest further improvements.

L.V Fast Exponentiation

Many tests and algorithms require the computation of high powers of some given number modulo a positive number, $a^n \equiv ? \pmod{m}$. Just multiplying one factor at a time is far too slow. The fast algorithm to be explained can be shown to be quadratic in (the bitlength of) the modulus, and linear in the exponent.

It is a built-in function in Python, Maple, and Mathematica.

Say we are supposed to compute $a^{55} \pmod{m}$. We determine the binary representation $55 = 2^5 + 2^4 + 2^2 + 2 + 1 = (110111)_2$ (cf. Section L.XII) which we read from left to right,

$$\begin{aligned} & & 1 &= 1 \\ (11)_2 &= & 2 \cdot 1 + 1 &= 3, \\ (110)_2 &= & 2 \cdot 3 + 0 &= 6, \\ (1101)_2 &= & 2 \cdot 6 + 1 &= 13, \\ (11011)_2 &= & 2 \cdot 13 + 1 &= 27, \\ (110111)_2 &= & 2 \cdot 27 + 1 &= 55. \end{aligned}$$

Here the ones and zeros in the left members are the bits of 55.

Each step in our algorithm consists of a squaring, followed by a multiplication by a (always a) if there is a one in the left member:

$$\begin{aligned} & a \to a^2 \cdot a = a^3 \to (a^3)^2 \cdot a^0 = a^6 \to \\ & \quad \to (a^6)^2 \cdot a = a^{13} \to (a^{13})^2 \cdot a = a^{27} \to \\ & \quad \to (a^{27})^2 \cdot a = a^{55}. \end{aligned}$$

All operations are of course to be taken modulo m.

Another, slower, variant, proceeds from right to left: $a^{55} = (a^2)^{27} \cdot a = (a^4)^{13} \cdot a^2 \cdot a = (a^8)^6 \cdot a^4 \cdot a^2 \cdot a = (a^{16})^3 \cdot a^4 \cdot a^2 \cdot a$ etc. Here we need not establish the binary representation of the exponent beforehand. What is computed at each stage is the product of all factors except the first. Each time the base is squared.

In the last step indicated above, corresponding to a zero in the binary representation, the base is squared, but not multiplied to the product.

A recursive variant starts with $55 = 27 + 28$, then splits these two exponents, and so on.

L.VI Primality: Fermat and Miller-Rabin

There are mainly two types of primality tests. Here we deal with negative, or probabilistic, tests that declare a number either composite or probably prime. Some prefer the term "compositeness tests". Later we will deal with some deterministic tests.

For numbers of some special form, e.g., Fermat or Mersenne numbers, there are simple necessary and sufficient conditions for their primality. We will deal with those too. The practicality of these tests when applied to very large numbers is a different matter, of course. We start with the contrapositive to Little Fermat:

$$\boxed{\textit{The number } N \textit{ is composite if, for some } a,\ (a,N)=1,\ a^{N-1} \not\equiv 1 \pmod{N}.}$$

Unfortunately, there are composite numbers N such that *no* $a, (a, N) = 1$, falsifies Little Fermat. They are known as *Carmichael numbers* (see p. 90). One such number is $1729 = 7 \cdot 13 \cdot 19$. The reason for the failure of the Fermat test is that $7 - 1$, $13 - 1$, $19 - 1$ all divide $1729 - 1$. Therefore, if a is not divisible by 7, 13, or 19, $a^{1728} \equiv 1$ modulo 7, 13, and 19, hence also modulo their product.

An improvement is offered by the *Miller-Rabin- test,* which rests on the following simple, but extremely useful observation:

$$\boxed{\begin{array}{l}\textit{N is certainly composite if there are } x, y \textit{ such that } x \not\equiv \pm y \pmod{N}, \\ \textit{but } x^2 \equiv y^2 \pmod{N}.\end{array}}$$

For, if N is prime, and $N|(x - y)(x + y)$, then N must divide one of the two factors.

The Miller-Rabin test applies this observation for $y = 1$. Assuming N odd (of course), write $N - 1 = 2^d u$ where $d > 0$, and u is odd. We find the factor u by repeatedly dividing $N - 1$ by 2, until the result is odd (division by 2 is a shift, checking parity is a bitwise "and" with 1).

If $a^u \equiv \pm 1 \pmod N$ no conclusion is possible.

If $a^u \not\equiv \pm 1 \pmod N$ we keep squaring. If it happens that $x = a^{2^k u} \not\equiv -1 \pmod N$ while $x^2 \equiv 1 \pmod N$, then N is composite. The same holds, of course, if $a^{N-1} \not\equiv 1 \pmod N$.

If N is composite, at least 3/4 of the possible a will reveal it (for the proof see Bressoud-Wagon, Childs, Rosen). The strategy of the Miller-Rabin test is, of course, to test several bases.

The estimate 3/4 is, on the average, *very* pessimistic. The analytically minded reader will find some results in Damgard-Landrock-Pomerance: "Average Case Error for the Strong Probable Prime Test", *Mathematics of Computation,* Vol.**61**, 1993, No. 203, pp. 177-194.

L.VI.1 Example. Let us look at the Carmichael number $N = 1729$. We easily find $N - 1 = 2^6 \cdot 27$. Now

$$x = 2^{54} \equiv 1065 \not\equiv -1 \pmod{1729},$$

and

$$x^2 = 2^{108} \equiv 1 \pmod{1729}.$$

This proves that N is composite.

We were lucky in not reaching the highest level, the Fermat test. That fact gives us a factorization for free. From

$$(1065 - 1)(1065 + 1) \equiv 0 \pmod{1729}$$

we find the factors

$$(1064, 1729) = 133$$

and

$$(1066, 1729) = 13,$$

whence $1729 = 133 \cdot 13$. □

The Miller-Rabin test can fail in two ways. Either already $a^u \equiv 1 \pmod N$, or there is some k, $0 \le k \le d - 1$, such that $a^{2^k u} \equiv -1 \pmod N$. If N is composite, in either case we say that N is a *strong pseudoprime* to the base a. Cf. the weaker concept “pseudoprime”, introduced in earlier exercises, p. 31.

If the choice of several bases a fails to expose N as composite the time is ripe to try some deterministic test.

Prime Generation

Sometimes one wants to create large (probable) primes, e.g., for use in an RSA cipher (see page 33). For the multipolynomial version of the Quadratic Sieve, or for the purpose of creating examples, one may want whole lists of moderately-sized primes.

We suggest here a number of simple algorithms for finding the smallest prime number $\geq$ than a given odd integer N.

Consider the arithmetic progression N, $N+2$, $N+4$, ... Before subjecting any of these numbers to a Miller-Rabin test we want to throw out those having small factors. There are basically three strategies.

We start by creating a list of small odd primes using a basic Eratosthenes routine. The optimal upper bound of this list depends on the number N. It could be as low as 10 for small N (no Eratosthenes required!) or several thousand for N with a few hundred digits.

The first strategy begins by trial-dividing the candidate $N + 2 \cdot k$ against the list. As soon as we find a prime dividing $N + 2 \cdot k$ it is discarded. With the bound 10 (primes 3, 5, 7) we will exclude about one half of all the odd numbers; with the bound 1000 we will keep approximately 1/6 of them.

If $N + 2 \cdot k$ is not divisible by any prime in the list we apply Miller-Rabin to it. For smaller N it seems faster to take the product P of all the primes in the list and then compute the gcd $g = (P, N + 2 \cdot k)$. If $g = 1$ the candidate is tested.

The second strategy is to use a sieve. We compute for each p_k in the list the least positive remainders q_k of $(p_k - N)/2$, modulo p_k We decide on a sieving interval, say from N to $N + 1022$; for smaller N that is more than we need, but that seems to matter very little. We start with a list of 512 ones, and change each of these in positions $\equiv q_k \pmod{p_k}$ to zero. For each remaining one, say in position j, the number $N + 2 \cdot j$ is tested for primality.

Sieving seems to be fastest alternative for larger numbers.

The third strategy is to list the residues of N modulo all the p_k. If at least one of these is zero we update N to $N+2$, simultaneously augmenting the residues by 2, and reducing modulo p_k (preferably by subtraction, not division). As soon as we have created a list without zeros we continue with a Miller-Rabin test as above.

As an indication of the significance of the parameters involved, I have experimented with the number $N = \lfloor\sqrt{10^{519}}\rfloor$, a 260-digit odd number. With primes up to 1000, after 67 trials I finally found a candidate, $N + 782$, that passed the Miller-Rabin test. With primes up to 8167 (1024 primes) this number was reduced to 50. Going up to 50 000 reduced the number of candidates further, to 36, but the over-all performance was slowed down by the greater number of divisions.

Sieving, by contrast, profited from the use of more primes.

L.VI: Exercises

1. Let $N = 1105$. Show that N is Carmichael number (p. 90). Find the factorization $1105 - 1 = 2^t \cdot u$, with u odd. Then show how to find numbers a, b, such that $a^u b^u \not\equiv a^{2u} \equiv b^{2u} \equiv -1 \pmod{1105}$, and conclude that 1105 is a strong pseudoprime to the bases a, b, but not to their product.

(You may even be able to solve the resulting Chinese congruence system by hand.)

The bases a, b are perhaps not the first ones you would try!

2. Using a powering routine of your own (or one built in your favorite programming language), write a program that Miller-Rabin-tests a given number to a given base, or a list of bases.

As a warmup, expose the numbers 7 418 629, 564 651 361 as composite. Check that the number 25 326 001 passes the test to the bases $2, 3, 5$. Also check that $N = 1502\,40184\,97471\,76241$, is a strong pseudoprime to the bases 2, 3, 4, 6 but not to the base 12.

(Miller-Rabin-testing to the base 12 will factor N, and there is a very simple relationship between the two factors. Explore!)

3. (a) Find the smallest base exposing the number

$$6\,85286\,63395\,04691\,22442\,23605\,90273\,83567\,19751\,08278\,43866\,81071$$

as composite.

(b) D Bleichenbacher, who constructed this example may have wanted to make the test look bad. The penalty for this is that the Miller-Rabin test finds a factor (this is rare)! Does your program find it?

4. Prime power detection. Let $n = p^k$, an odd prime power.

(a) Let a, $(a, n) = 1$, be an integer. Show that $p|(a^{n-1} - 1, n)$

(b) If $n|a^{2s} - 1$, then either $n|a^s - 1$ or $n|a^s + 1$.

(c) Assume now that n is revealed as composite by a Miller-Rabin-test, base a. Show that $g = (a^{n-1} - 1, n)$ is a proper factor of n, i.e., a factor satisfying $1 < g < n$. Hint: Let $n - 1 = 2^t \cdot u$, u odd, and consider the smallest f such that $a^{2^f \cdot u} \equiv 1 \pmod{n}$.

(d) Now devise a test that with high probability determines whether the odd number n is a prime power or not.

(e) If you want examples of $(a^{n-1} - 1, n) \neq p$, try $n = p^3$, $a = 2$, where $p = 1093$, 3511, the two known so-called Wieferich primes, satisfying $2^{p-1} \equiv 1 \pmod{p^2}$.

5. This exercise connects with the RSA cryptographic scheme, discussed briefly in Section A.VI. It uses the ideas behind the Miller-Rabin Test. Let $p \neq q$ be two large prime integers, $n = pq$ their product, and $\phi(n) = (p-1)(q-1)$. Assume that d and e are inverses of one another modulo $\phi(n)$. The purpose of the exercise is to show that with great probability the factorization $n = pq$ may be found from the knowledge of d and e.

(a) Let $de - 1 = 2^t \cdot u$, where $t \geq 1$ (why?), and u odd. Assume that a^u, $(a, n) = 1$, is of greater order modulo p than modulo q (the orders are powers of 2, prove this). Then show that, for some $s < t$,

$$(a^{2^s \cdot u} - 1, n) = q.$$

(b) We now need to prove that, for a substantial portion of the invertible classes modulo $a + (n)$, a^u has different orders modulo p and q. In fact, at least $\phi(n)/2$ of them have this property. Let g be a primitive root modulo both p and q (existence by CRT, prove it). Now study the Chinese congruence system:

$$a \equiv \begin{cases} g^x \pmod{p} \\ g^y \pmod{q} \end{cases}$$

First, if g^u is of higher order modulo p than modulo q, choosing x odd, and y arbitrary, show that the solution a is of higher order modulo p than modulo q.

> Next, if the two orders are the same, let x, y be of opposite parities, but otherwise arbitrary, and show that the solution a is of different order modulo p and q.

Now devise a probabilistic algorithm determining the factors p, q from the knowledge of d, e.

L.VII Lehmer, Lucas, Pocklington

We now turn to positive, or deterministic, tests. Such a test will reveal with absolute certainty that N is prime, or it will reveal N as probably composite. Of course, we never test for primality without doing a Miller-Rabin test first.

The following Theorem, due to French mathematician E. Lucas (1842-1891), is the simplest converse to Little Fermat.

L.VII.1 Theorem (Primitive Root Criterion). *If, for some a,*

$$a^{N-1} \equiv 1 \pmod{N},$$

and, for all prime numbers q dividing N,

$$a^{(N-1)/q} \not\equiv 1 \pmod{N},$$

then N is a prime, and a is a primitive root modulo N.

Proof. The assumption means that the order of a modulo N is $N-1$. That order is also a factor in $\phi(N)$, so $N-1 \le \phi(N)$.

But modulo a composite number there are always non-zero non-invertible classes, so in that case $\phi(N) < N-1$.

The only possibility left is that N is a prime. □

If N is really prime, then there is a 50% chance of a being a quadratic residue modulo N. Euler's Criterion then gives $a^{(N-1)/2} \equiv 1 \pmod{N}$, so quite probably the base first chosen will reveal nothing.

L.VII.2 Example. We exemplify with

$$N = 1\,02233\,38353\,29657$$

Here is the result of the test, using the base 3. The Fermat test is superfluous if the number has already been subjected to the Miller-Rabin test.

$$\begin{aligned}
N-1 &= 2\cdot 2\,957\cdot 146\,063\cdot 295\,877\\
3^{N-1} &\equiv 1 \pmod N\\
3^{(N-1)/2} &\equiv 1\,02233\,38353\,29656 \pmod N\\
3^{(N-1)/2957} &\equiv 32422\,47673\,63906 \pmod N\\
3^{(N-1)/146063} &\equiv 69730\,26463\,21792 \pmod N\\
3^{(N-1)/295877} &\equiv 73678\,57524\,08036 \pmod N
\end{aligned}$$

All the results, except the first, being $\not\equiv 1 \pmod N$, this proves N prime.

The factors of $N-1$ were found by trial division, which should really be combined with some other method. Determining the primality of N by complete trial division is slower, but feasible. □

Here is a variant due to H.C. Pocklington (1870-1952).

L.VII.3 Theorem (Pocklington). *Let p be a prime factor of N, and q one of $N-1$, $v_q(N-1)=k$, so that $q^k|(N-1)$. If, for some a,*

$$(a^{(N-1)/q}-1, N) = 1,$$

and

$$a^{N-1} \equiv 1 \pmod N,$$

then $p \equiv 1 \pmod{q^k}$.

If q is not too small, we might use trial division, over the sparse sequence $1+m\cdot q^k$, $m\geq 1$, in order to determine the primality of N. The larger q is, the fewer divisions will be required.

If $q>\sqrt{N}$ no division at all is required! In that case, all prime factors of N must be larger than its square root, which is possible only if N is a prime number.

Further, one could lump together several of the q (all taken with their proper multiplicity) satisfying the conditions of the Theorem, possibly with different bases, thus producing an even sparser sequence.

And, again, if their product exceeds $\sqrt{N}$, we have proved the primality of N.

We will give a more systematic approach later, in Example L.IX.3.

Here is the proof of the Theorem:

Proof. The second part of the assumption means that

$$\mathrm{ord}_p(a)|(N-1).$$

The first part of the assumption implies that

$$p \nmid a^{(N-1)/q} - 1 \text{ so that } \mathrm{ord}_p(a) \nmid \frac{N-1}{q}.$$

We spell things out. Write $d = \mathrm{ord}_p(a) = q^\ell \cdot s$, $N-1 = q^k \cdot t$, where q divides neither s nor t. Then $d|(N-1)$ gives $\ell \leq k$, $s|t$, and $d \nmid (N-1)/q$ gives $\ell \nleq k-1$. Hence $\ell = k$, so that the full power q^k dividing $N-1$ must divide $\mathrm{ord}_p(a)$.

By Little Fermat we conclude that $q^k|\ \mathrm{ord}_p(a)|(p-1)$. □

L.VII.4 Example. Just to illustrate what the Theorem says, we take the following example:

$$N = 61\,89700\,19642\,69013\,74495\,62111.$$

Luckily, $N-1$ has many small prime factors, and easily cracks on trial division:

$$N - 1 = 2 \cdot 3 \cdot 5 \cdot 17 \cdot 23 \cdot 89 \cdot 353 \cdot 397 \cdot 683 \cdot 2113 \cdot 29315\,42417$$

Note that the largest prime factor q is much smaller than the square root of N:

$$\lfloor\sqrt{N}\rfloor = 2487\,91080\,95803.$$

We cannot use the base 2, as

$$2^{(N-1)/q} \equiv 1 \pmod{N}.$$

In fact, this relation holds for all the prime factors, except 89 (which happens to be the order of 2 modulo N).

So we test the base 3:

$$m = 3^{(N-1)/q} - 1 \equiv 18\,05910\,65836\,31708\,35540\,66745 \pmod{N} \qquad (*)$$

and, indeed,

$$(m, N) = 1.$$

The possible factors therefore are of the form $1 + k \cdot q$, where we need only look at $1 < 1 + k \cdot q < \sqrt{N}$, i.e., $0 < k \leq 8486$. Trialdividing against these candidates reveals N to be prime in no time at all.

We could have done without trial division by verifying (*) for the three largest prime factors 683, 2113, 29315 42417, the product of which exceeds the square root of N. The base 3 works for all three of them. □

L.VII.5 Example. We have mentioned Mersenne numbers (L.II.3) like

$$N = 2^{127} - 1$$

(note that 127 is a prime). Later we will give a necessery and sufficient condition for their primality. Let us see how Pocklington applies to this number.

It is easy to find all factors of $N - 1$ below a million, by trial division. Their product is

$$Q = 2 \cdot 3^3 \cdot 7^2 \cdot 19 \cdot 43 \cdot 73 \cdot 127 \cdot 337 \cdot 5419 \cdot 92\,737 \cdot 649\,657.$$

Removing all factors ≤ 73 we still get

$$P = 127 \cdot 337 \cdot 5419 \cdot 92\,737 \cdot 649\,657 > \sqrt{N}.$$

Here we give the results of a computer run using the base 3. Base 2 does not work at all.

```
base= 3
prime factors to be used  are
[649657, 92737, 5419, 337, 127, 73, 43, 19, 7, 3, 2]
fermat test: 3 **(N-1)=1 modulo N
factor= 649657 , multiplicity= 1
acc. product= 649657
power= 3 **((N-1)/ 649657 )=
534069447239129308145638487248213335530 modulo N
gcd(power-1,N)= 1
```

```
factor= 92737 , multiplicity= 1
acc. product= 60247241209
power= 3 **((N-1)/ 92737 )=
150550836351600033767904108065981737908 modulo N
gcd(power-1,N)= 1
factor= 5419 , multiplicity= 1
acc. product= 326479800111571
power= 3 **((N-1)/ 5419 )=
26695659649525653566430798996420549056 modulo N
gcd(power-1,N)= 1
factor= 337 , multiplicity= 1
acc. product= 110023692637599427
power= 3 **((N-1)/ 337 )=
95859789961691791874930359127846942304 modulo N
gcd(power-1,N)= 1
factor= 127 , multiplicity= 1
acc. product= 13973008964975127229
power= 3 **((N-1)/ 127 )=
1237940039285380274899124224 modulo N
gcd(power-1,N)= 1
acc. product now exceeds sqrt(N)
```

The Primitive Root Criterion could also be put to work. One has the choice of stepping up the base from 2 and upwards, until a primitive root is found, or finding candidates by a random process. In this case the latter approach would probably be faster, as the least positive primitive root is 43.

The original test, by E Lucas, is based on the factorization of $N + 1$, which is not *that* hard to determine. See the end of the Chapter, L.XV. □

Remark: Dividing out the prime factors of $N - 1 = 2^{127} - 2$ that we found, leaves the quotient $M = 7\,71586\,73929$. We easily see that it is less than the square of the last prime factor that we found, $q = 649\,657$ ($q^2 > 10^{11} > M$).

But this means that M cannot be composite, as all of its prime factors must be larger than q. So, without further effort, we find the complete factorization of N.

This idea is also exploited in the so-called “large prime variation” of the Continued Fractions and Quadratic Sieve methods, for factoring.

Our next Example is elevated to the status of a Theorem.

L.VII.6 Theorem (Pépin's Test for Fermat Numbers). *Let N be the* Fermat number

$$F_m = 2^{2^m} + 1, \quad m \geq 1.$$

Then N is a prime if and only if

$$3^{(N-1)/2} \equiv -1 \pmod{N}.$$

Proof. For the "if" part we note that $q = 2$ is the only prime factor of $N-1$, that $2^{2^m}|(N-1)$, and that $(N-1)/2 > \sqrt{N}$. The condition of the Theorem yields that

$$(3^{(N-1)/2} - 1, N) = (-2, N) = 1,$$

which proves the "if" part.

The "only if" part follows at once from Euler's Criterion and the simple fact that

$$\left(\frac{3}{N}\right) = \left(\frac{2^{2^m}+1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

□

L.VII.7 Example. The only known Fermat primes so far are $F_k, 0 \leq k \leq 4$: 3, 5, 17, 257, 65537. The smallest composite F_k is $N = F_5 = 2^{32} + 1 = 28633\,11531$, as we have seen above. For that number,

$$3^{(N-1)/2} \equiv 10\,324\,303 \not\equiv -1 \pmod{N}.$$

Fermat numbers are a popular testing ground for factorization algorithms.□

Proth's test gives a primality criterion for another restricted class of numbers:

L.VII.8 Theorem (Proth's Test). *Let $N = k \cdot 2^m + 1$, $m \geq 1$, where k is odd, and $k < 2^m$. Suppose, for some base a, that*

$$a^{(N-1)/2} \equiv -1 \pmod{N}.$$

Then N is a prime.

Proof. Again $(a^{(N-1)/2} - 1, N) = (-2, N) = 1$, and $2^m > \sqrt{N}$, yielding the result. □

Proth's test reveals nothing if N is prime and a is a quadratic residue modulo N. In that case

$$a^{(N-1)/2} \equiv +1 \pmod{N}$$

by Euler's Criterion.

If, however,

$$a^{(N-1)/2} \not\equiv \pm 1 \pmod{N},$$

then, of course, N is composite.

A variant, then, is the folllowing:

L.VII.9 Theorem. *Assumptions as in the previous Theorem. Suppose the Jacobi symbol*

$$\left(\frac{a}{N}\right) = -1.$$

Then N is prime if and only if

$$a^{(N-1)/2} \equiv -1 \pmod{N}.$$

The proof is really the same as for Pépin's test. □

Trial and error will produce an a satisfying

$$\left(\frac{a}{N}\right) \neq 1$$

in a very short time.

L.VII: Exercises

1. Using little more than fast powering and a gcd routine, verify (interactively) that the following numbers are primes:

(a) $1 + 2 \cdot 3 \cdot 5^{278}$

(b) $934(2^{127} - 1) + 1$

(c) $N = 180 \cdot (2^{127} - 1)^2 + 1$ (a 78 digit number).

In the last two examples, assume known that $2^{127} - 1$ is a prime.

2. By a combination of Miller-Rabin and Proth tests, determine which of the following numbers are prime:

(a) $199 \cdot 2^{854} + 1$

(b) $409\,116\,489 \cdot 2^{87} + 1$

(c) $1\,205\,1351 \cdot 2^{96} + 1$

L.VIII Factoring: Pollard $p-1$

We now turn to factoring algorithms, and begin with one by British mathematician J. Pollard, from the early 70's. Its historic importance is that it inspired the powerful Elliptic Curves Method of factorization. It is therefore given in all texts as an introduction to the ideas of the latter algorithm.

Suppose the number N to be factored has a prime factor p, such that all the prime factors of $p-1$ are small. $p-1$ then divides $k!$, $k! = (p-1)q$, where k is not too large. By Little Fermat we get, for a such that $p \nmid a$,

$$a^{k!} = (a^{p-1})^q \equiv 1 \pmod{p}$$

so that

$$(a^{k!} - 1, N) \geq p > 1.$$

With luck we get a factor $< N$.

One can make this procedure more efficient by instead taking inductively the lcm $M(k)$ of all numbers up to k. If $k+1$ is not a prime power, then $M(k+1) = M(k)$. If $k+1$ is a prime power p^d then $M(k+1) = pM(k)$.

A more direct approach to this variant, perhaps easier to program, would be to create a prime list up to a suitable limit B, using Eratosthenes. Then for each prime $q \leq B$ determine the highest power $q^e \leq B^2$. Then we take one prime q at a time and raise our base to the power q e times.

To save time one does not compute the gcd at every turn of the loop, but does so at intervals, e.g., at every 100 turns of the loop.

A simple variant of the $p-1$ method inputs a list of bases a, the number to be factored, N, a period for taking gcd's (see the previous paragraph), and a ceiling for k, indicating when to change the base.

L.VIII.1 Example. Let $N = 540143$. We compute $b = 2^{6!} \equiv 518\,077 \pmod{N}$, however $(b-1, N) = 1$. Next turn is $b = 2^{7!} \equiv 167\,138 \pmod{N}$, giving $(b-1, N) = 421$ and $N = 421 \cdot 1283$. □

L.VIII.2 Example. The $p-1$-method, with base 2, cannot handle $14\,111 = p \cdot q = 103 \cdot 137$.

This is because $p-1$ and $q-1$ have the same largest prime factor, 17, and the orders of 2 modulo 103 and 137 are 51 and 68, both divisible by 17. So the lowest k giving

$$(2^{k!} - 1, N) > 1,$$

is $k = 17$. And then

$$N | 2^{k!} - 1,$$

as *both* 51 and 68 divide 17!.

The probability for something similar happening for large N is negligible. Also, really small factors should be found by trial-division before attempting anything else. □

L.VIII.3 Example. Factoring

$$N = 83910\,72126\,67598\,13859 = 45456\,46757 \cdot 1\,84595\,78087,$$

using the base 2, and a gcd-period of 100, takes little more than a second on my machine, in fact much less, when using the lcm approach. This is because one of the prime factors minus one has small prime factors:

$$45456\,46757 - 1 = 2^2 \cdot 7 \cdot 8837 \cdot 18371.$$

$N = 31\,61907\,57417\,40159 = 806\,008\,537 \cdot 39\,229\,207$ takes longer. Here is the reason:

$$806\,008\,537 - 1 = 2 \cdot 3 \cdot 3\,731\,521,$$

$$39\,229\,207 - 1 = 2 \cdot 3 \cdot 6\,538\,201.$$

Using the naive $k!$ approach is at least ten times slower than using a prime list as indicated above.

There are further improvements ("phase two", "stage two") see, e.g., Crandall-Pomerance. Without these refinements, the Pollard rho algorithm, to be presented below, usually wins. □

L.IX Factoring, Pollard rho

The rho method, another invention of Pollard's, is very easy to program. It does not depend on exponentiations, but does require Euclid. Each turn of the loop requires three polynomial evaluations, and half of the values are computed twice, a waste we can live with. Richard Brent has proposed a variant avoiding this, see the end of this Section.

N is the number we want to factor. The number p is an unknown prime factor, e.g., the smallest one. We already know, by a Miller-Rabin test (Section L.VI), that N is composite.

We try to create a sequence of numbers $x_0, x_1, x_2, \ldots$ which appears to exhibit a random distribution modulo N, such that eventually two of them are congruent modulo p. One does this by repeated application of a simple polynomial function f – often $f(X) = X^2 + c$, $c \neq 0, -2$, or $f(X) = X^2 + X + 1$ will do the trick. The optimal number of iterations is some moderate multiple of $N^{1/4}$, which we set as the ceiling for the number of turns of the loop.

We then choose some x_0 and form $x_0, x_1 = f(x_0), x_2 = f(x_1), \ldots$

If $x_j - x_i \equiv 0 \pmod{p}$ then also $f(x_j) - f(x_i) \equiv 0 \pmod{p}$. Therefore it seems reasonable to form $x_{2k} - x_k$ so that the distance keeps increasing. So we work with the two sequences $x_k, y_k = x_{2k}$ in parallel, which means three evaluations for each iteration, as the y-sequence is updated twice.

In our quest for factors, at each turn of the loop we compute the gcd $d = (x_{2k} - x_k, N)$ and output $d, N/d$ if i $d \neq 1, N$ (and then Miller-Rabin-test the factors and continue). If we do not achieve a factorization before hitting the ceiling we repeat with a different function. A recursive program (starting by trialdividing out all factors below, say, 10^4) will handle at least any 30-digit number in a few minutes, with reasonable confidence. The worst case is a number composed of two primes of similar size.

This particular iteration scheme is due to the American computer scientist Robert Floyd (1936-2001).

L.IX.1 Example. $N = 540143$.

Using $f(x) = x^2 + 1$ and $x_0 = y_0 = 1$ we get

$$x_1 = 2, y_1 = 5, \quad (5 - 2, N) = 1$$

$$x_2 = 5, y_2 = 677, \quad (677 - 5, N) = 1$$

$$x_3 = 26, y_3 = 455\,057, \quad (455\,057 - 26, N) = 1$$

$$\ldots$$

$$x_{24} = 26\,630, y_{24} = 174\,822, \quad y_{24} - x_{24} = 148\,192, \quad (148\,192, N) = 421.$$

□

One should not take gcd's at every turn of the loop. Better to assign a period and multiply that number of differences (modulo N, of course) before taking the gcd. In order not to miss small factors, we trial-divide as already mentioned.

The optimal period would depend on the expected number of iterations. Already a period of 100 makes the time spent on Euclid relatively negligible.

L.IX.2 Example. In the Sections on trial division and Pollard $p-1$ we studied the factorization of the number $N = 31\,61907\,57417\,40159 = 39\,229\,207 \cdot 806\,008\,537$, Using $f(X) = X^2 + X + 1, x_0 = 1$, gives a factorization within a fraction of a second. Taking gcd's at intervals of 100 speeds things up by a factor 10.

Using $f(X) = X^2 + 1, x_0 = 1$, is about 8 times as slow. The performance may vary greatly and unpredictably with the choice of the iterating function f. □

The expected number of iterations lies somewhere around a moderate multiple of the square root of the smallest prime factor, assuming random behavior.

Suppose we randomly pick one out of p objects numbered $0, 1, \ldots, p-1$. (In our application the objects are the classes modulo the smallest prime factor p.) Suppose we do so m times, repeats allowed.

For each j, $0 \le j \le p-1$, we let X_j denote the stochastic variable defined by $X_j = 1$ if the j:th element is picked at least once, $X_j = 0$ otherwise.

Consider the sum

$$X = X_0 + X_1 + \cdots + X_{p-1}.$$

$X = k$ if k different objects are picked. The expected number $q(m,p)$ of different outcomes on m trials therefore equals the expected value of X.

The expectation of any X_j obviously equals the probability that element j is picked. The probability that it is *not* picked is $(1 - 1/p)^m$, the probability that it is picked therefore equals $1-(1-1/p)^m$. From this we see, by summing the expectations, that

$$q(m,p) = p \cdot \left(1 - (1 - \frac{1}{p})^m\right).$$

Applying Taylor's Theorem to $f(x) = (1+x)^m$ gives

$$f(x) = 1 + mx + \frac{m(m-1)}{2}x^2 + \text{ error}$$

where the absolute value of the error term is less than $m(m-1)(m-2)|x|^3/6$.

Substituting $x = -1/p$ we obtain the following approximation for $q(m,p)$:

$$q(m,p) = m - \frac{m(m-1)}{2p} + \text{ error}$$

with error term less than $m(m-1)(m-2)/(6p^2)$. So $q(m,p)$ is less than m by a couple of units if m is a small multiple of $\sqrt{p}$, in other words, for such a choice of m the expected number of repeats is positive.

More on this topic, with explicit calculations of probabilities can be found in elementary textbooks on probability, under the heading “birthday paradox”.

Brent’s Modification

We give here a modified approach by Australian mathematician R Brent (1946-). Let the iterates be x_m, y_n. We update m, n and x, y according to the following scheme:

$$\begin{aligned}(m,n) =&(1,\mathbf{2})\\ &(\mathbf{2},\mathbf{4})\\ &(\mathbf{4},7),(4,\mathbf{8})\\ &(\mathbf{8},13),(8,14),(8,15),(8,\mathbf{16})\\ &(\mathbf{16},25),(16,26),(16,27),(16,28),(16,29),(16,30),(16,31),(16,\mathbf{32})\\ &\dots\end{aligned}$$

The number of pairs in each row is a power of 2. Note how the index difference increases by one unit in each step, and only y is iterated on. Try to see the whole of the pattern before reading further.

One could program this scheme as follows. Initialize $m = 1, n = 2$, and the iterates $x = x_1$ (input value) and $y = x_2 = f(x_1)$. Suppose we have reached $(m,n) = (2^{k-1}, 2^k)$, $x = x_m$, $y = y_n$. We then put $r = n$, $x = y$, $n = m + n + 1$, and y is iterated on $m + 1$ times. Then put $m = r$, and iterate on y, update n, until $n = 2 \cdot m = 2^{k+1}$. Simultaneously form the differences $x - y$ and multiply them to the product. Take gcd’s at intervals, as indicated above.

Clearly higher iterates will be formed than with the Floyd method, but there will be fewer evaluations, about $2/3$ as many. The actual gain in speed is about $20 - 25\%$. Riesel’s book discusses the mathematics involved in this estimate, at least for $f(X) = X^2 + a$.

L.IX.3 Example (A Pratt Certificate). Wishing once to factor the repunit $(10^{41} - 1)/9$ completely, I trial divided to the limit 10^6 (again, we should really combine this with some other factoring method) and Miller-

Rabin-tested (to several bases) the cofactor:

$$\frac{10^{41}-1}{9} = 83 \cdot 1231 \cdot 53897 \cdot 20176\,37099\,00322\,80374\,86579\,42361.$$

Here the large cofactor N is a strongly suspected prime. We need to know with absolute certainty that it is prime. Hoping to expose it with Pocklington's method (L.VII.3) I tried to factor $N-1$, again trialdividing to the limit 10^6, and Miller-Rabin-testing the cofactor:

$$N-1 = 2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 41 \cdot 9661 \cdot 3\,85889\,69828\,15807\,76323.$$

The cofactor $M = 3\,85889\,69828\,15807\,76323$ is again a strong suspect, and is subjected to the same procedure:

$$M-1 = 2 \cdot 13 \cdot 947 \cdot 15\,67255\,69929\,97351.$$

This time a Miller-Rabin test shows that the large cofactor

$$L = 15\,67255\,69929\,97351$$

is composite. Pollard rho finds the factors $L = 271\,58563 \cdot 5770\,76077$. These factors are so small that full trial division will expose their primality. If instead we stick to trialdividing only up to 10^6, we find $271\,58562 = 2 \cdot 3^2 \cdot 19 \cdot 79411$ and $5770\,76077 - 1 = 2^2 \cdot 3^4 \cdot 17\,81099$, with $1781099 - 1 = 2 \cdot 11 \cdot 19 \cdot 4261$.

I could now work from the bottom up, verifying the primality of 1718099, 577076077, 27158563, L, M, and, finally, N, using Pocklington. Obviously this test lends itself splendidly to recursive programming.

Note that one need not really use all prime factors of $N-1$. For instance, we can always exclude the factor 2.

In our example, the smallest base b for which

$$(b^{(N-1)/2} - 1, N) = 1$$

is 19 (a primitive root, in fact), and we do not need that step at all.

One could of course work with the factors of $N-1$ in descending order, until their product exceeds $\sqrt{N}$. Problems arise, of course, when the second largest prime factor is so large that we cannot even achieve a tentative factorization.

This certification scheme due to V. Pratt, combines equally well with the Primitive Root Test. The primality proof achieved goes under the name of **Pratt certificate**. □

L.IX: Exercises

1. (H W Lenstra, J Pintz, W L Steiger, E Szemeredi). Prove the following statements.

(a) Suppose n is a positive integer satisfying $n \leq 3^{3m}$. If there is a positive integer a such that

$$a^{3^m} \equiv 1 \pmod{n}, \qquad (a^{3^m-1} - 1, n) = 1,$$

then n is a prime or a product of two primes $\equiv 1 \pmod{3^m}$.

(b) Suppose $n = (x \cdot 3^m + 1)(y \cdot 3^m + 1) \leq 3^{3m}$ and

$$n = A \cdot 3^{2m} + B \cdot 3^m + 1, \quad 0 < A < 3^m, \quad 0 < B \leq 3^m.$$

Then $xy = A$, $x + y = B$.

(c) Suppose $n = A \cdot 3^{2m} + B \cdot 3^m + 1$, $0 < A < 3^m$, $0 < B \leq 3^m$. Then n is a prime if and only if

i. there is a positive integer a such that

$$a^{3^m} \equiv 1 \pmod{n}, \qquad (a^{3^m-1} - 1, n) = 1,$$

and

ii. $B^2 - 4A$ is a square

Hint: $(X - x)(X - y) = X^2 - (x + y)X + xy$.

2. Use the rho method with $f(X) = X^2 + 1$ to factorize

(a) 36563 94819 17866 84703 into two factors, and

(b) 3245 64576 76789 98977 into three. Miller-Rabin-test the factors to several bases (if you have a program for complete trial division, you can use that as a deterministic primality test.)

3. A more ambitious project would be to write a full recursive factoring program trialdividing out the factors below 10^5 or 10^4, then using rho to find further factors, returning a full set of Miller-Rabin-tested factors. Ideally, if running too long, it should output the factors it found, along with the cofactor, certified to be composite.

Your program should be able to handle

(a) 526 31814 39815 23188 28920 59893

(b) $12051351 \cdot 2^{96} + 1$

(c) $2^{109} - 2^{55} + 1$

(d) $(10^{37} - 1)/9$

(e) $(10^{47} - 1)/9$

(f) $2^{136} + 1$

(g) $5^{93} + 1$

(h) 34 56456 45675 75787 68689 79790 808113

(i) $3^{225} - 1$ (This one will take some time, possibly 15 minutes).

4. The performance of the rho method varies greatly with the input. The same holds for the $p-1$ method of the previous section, but, as indicated there, for other reasons. You may enjoy writing a similar program as in the previous exercise and testing the same numbers.

A number that $p-1$, but not rho, will easily crack is $10^{53} - 1$. Find, and at least Miller-Rabin-test, the factors. Then use that same program to explain the success of the $p-1$ method.

5. A natural continuation of the previous exercises would be to find Pratt certificates for the large factors.

6. You may also like to try the Fermat number $F_8 = 2^{2^8} + 1$ which was cracked in 1980, by Brent and Pollard, using a somewhat special iteration function, $x^{2^{10}} + 1$, and initial value $x_0 = 3$. You can find the explanation in Riesel's book or in the original article, "Factorization of the Eighth Fermat Number", *Mathematics of Computation*, Vol. **36**, No. 154, (Apr., 1981), pp. 627-630.

Today, a standard rho routine will find two factors, P, Q (in about twice the time). Surprisingly, even the larger factor Q (62 digits) can be Pratt-certified in "reasonable" time, a couple of minutes. The smaller factor P can (today) be certified by full trial division.

You may then be able to explain Brent and Pollard's conclusion: "I am now entirely persuaded to employ the method, a handy trick, on gigantic composite numbers".

Needless to say, perhaps, modern factorization routines and primality tests crack F_8 in just a second or two. You should not try this exercise on a slow computer. If you wish to try $F_7 = 2^{2^7} + 1$ you should definitely use the special iteration function $f(x) = x^{2^9} + 1$, intitial value $x_0 = 3$, which runs about six times as fast as a standard iteration.

Brent-Pollard's general idea was to use the iteration function $x^m + 1$ if the required prime factors were known to be congruent to 1 modulo m.

7. Further suggestions for computing:

(a) Find primitive roots for some of the primes p you have encountered. Their computation relies on fast exponentiation (Section L.V) and factoring $p - 1$.

(b) A possible extension then is computing Discrete Logarithms, using, preferably, Pohlig-Hellman plus rho, as described in Section C.VII.

L.X “Waiting For a Square”

We now look at the crudest algorithm using continued fractions. Expanding $\sqrt{N}$, using the QCF (Section H.I), leads to the following relations:

$$p_k^2 - Nq_k^2 = (-1)^{k+1} Q_{k+1},$$

where p_k, q_k are steadily increasing, and $0 < Q_{k+1} < 2\sqrt{N}$.

For some even $k+1$ it might occur that Q_{k+1} is a perfect square $=R^2$, say. It then holds that $N|(p_k - R)(p_k + R)$. With bad luck one factor is divisible by N, otherwise one of the gcd’s $(p_k - R, N)$ and $(p_k + R, N)$ produces a genuine factor of N.

If we are unlucky we continue until we register success. Perhaps one should have a ceiling for the number of iterations; some moderate multiple of $N^{1/4}$ will usually do.

L.X.1 Example. We have tried trial division, Pollard $p-1$, and Pollard rho on the number 31 61907 57417 40159. The method just described cracks that number in less than 0.1 seconds, after 7294 iterations, using not much more than 20 lines of code.

The right member Q_{k+1} is $33\,235\,225 = 5765^2 = R^2$. The corresponding p_k (reduced modulo N of course) is 18 92398 34711 35378. And we get:

$$\begin{aligned}(p_k + R, N) &= 806\,008\,537,\\ (p_k - R, N) &= 39\,229\,207.\end{aligned}$$

□

Note that only the p_k, not the q_k, need be computed. And one should perhaps reduce them to their least absolute value remainders.

The reasonable range for this method seems to be up to about 25 digits.

L.X.2 Example. Unlike our previous examples, the following,

$$\begin{aligned}N &= 203\,80237\,72101\,12418\,68065\,58119\\ &= 14060\,51123 \cdot 20292\,56729 \cdot 714\,284\,357\end{aligned}$$

has three prime factors. The rho method finds the factors about 10 times as fast as “wait for a square” (using a gcd-period of 100). The main gain is in finding the first factor.

The reason is that Pollard rho is more sensitive to the size of the smallest prime factor. For a given iteration function, and initial value, the number of steps producing a certain factor depends only on that factor. The time spent on each step depends on the cofactor, however. □

For larger numbers one may have to write a routine for finding the floor of a square root.

Morrison-Brillhart, who published the CFRAC method in 1975, suggest a Newton method. Start with some $a_0 > \sqrt{N}$, for instance,

$$a_0 = 2^{\lfloor B(N)/2 \rfloor + 1},$$

where $B(N)$ is the number of bits in N. Then iterate:

$$a_{n+1} = \left\lfloor (a_n + \lfloor \frac{N}{a_n} \rfloor)/2 \right\rfloor.$$

As soon as $a_n^2 < N$, or as soon as $a_{n+1} >= a_n$, we have found $\lfloor \sqrt{N} \rfloor = a_n$.

Some of the drawbacks of this method should be evident. The p_k are very soon of the same order as N. It may be long before a square turns up – maybe never! We are dependent on a fairly long period. For instance, Fermat numbers are of the form $n^2 + 1$ having the shortest possible period, one!

A partial solution is *multipliers*, expanding $\sqrt{kN}$ for several low values of k.

The method will rapidly detect a square, as that leads to division by zero:

$$\begin{aligned} 0 = \lfloor \sqrt{N} \rfloor &= \sqrt{N} = \alpha_0 \\ \alpha_1 &= \frac{1}{\alpha_0 - a_0} = \frac{1}{0}. \end{aligned}$$

It will not factor the cube of a prime $p \geq 5$. Suppose $p_k^2 - p^3 q_k^2 = Q_{k+1} = R^2$. If we achieve a factorization, then p must divide both $p_k - R$ and $p_k + R$.

Hence p must divide their difference, $2R$, i.e., p must divide R. But then, by the standard inequality $Q_k < 2\sqrt{D}$, $2\sqrt{p^3} > R^2 \geq p^2$, i.e., $p < 4$, impossible.

L.X: Exercises

1. If you have already written a QCF routine, use "Wait for a Square" to factor the numbers

(a) 36563 94819 17866 84703

(b) 5038 40507 49619 52087 41373

(c) 35419 05253 35205 94597 94529

(On the last number, Pollard rho will be much slower).

You should at least Miller-Rabin-test the factors. However, they are so small that full trial division will expose their primality in reasonable time.

L.XI CFRAC

The idea behind CFRAC, published in the early 70's, is one does not wait for squares, one creates them.

We start by creating a list of primes, by Eratosthenes. We have checked that the number to be factored, N is composite, after extracting small factors, using trial division and/or the Pollard methods. N is odd, of course.

Note that $p_k^2 - Nq_k^2 = (-1)^{k+1}Q_{k+1}$, $(p_k, q_k) = 1$; so if p is an odd prime factor of Q_{k+1}, we must have $(N/p) = 1$. We therefore throw out all the odd primes for which N is not a quadratic residue. We augment the list by the sign -1.

Then we run QCF. Each $(-1)^{k+1}Q_{k+1}$, k odd or even, is trialdivided against the factor base. If $(-1)^{k+1}Q_{k+1}$ factors completely, the exponents (taken modulo 2) are stored in one list each, for every successful Q_{k+1}. The exponent of -1 will be 1, if k is even, 0, if k is odd. At the same time the Q_{k+1} and p_k are listed.

By Gaussian elimination mod 2 (to be explained in Section L.XII) we find a complete set of independent relations modulo 2 among the exponent vectors. For each relation we multiply those $(-1)^{k+1}Q_{k+1}$ whose exponent vectors enter the relation with coefficient 1. The product of these will be a square. At the same time we multiply the corresponding p_k.

We call the resulting products $Q = R^2$, and p. Multiplying the relations

$$p_k^2 - Nq_k^2 = (-1)^{k+1}Q_{k+1}, \quad p_k^2 \equiv (-1)^{k+1}Q_{k+1}$$

shows that

$$p^2 \equiv R^2 \pmod{N},$$

and one can only hope that $(p + R, N)$ or $(p - R, N)$ produces a non-trivial factor of N (it suffices to study one of them).

This method was first used with success by Brillhart and Morrison, in 1970, to factor $F_7 = 2^{128} + 1$, a 39-digit number. They used a multiplier, 257, after some experimentation, to get a reasonably long period, and an optimal factor base. The factorization took several hours. Note that, unlike Pollard rho, the CFRAC method is insensitive to the size of the smallest prime factor.

The prime factorization of F_7 is

$$59\,64958\,91274\,97217 \cdot 57\,04689\,20068\,51290\,54721.$$

A modern algorithm, run on a modern computer, finds the factors in less than a second.

There are a number of refinements.

One is "early abort". The bigger the factor base, the more Q_k's factor over it. However, expanding the factor base also means that many unsuccessful factoring attempts last longer. The strategy then is to interrupt trial divisions that seem to last too long. At one or two cuts of the factor base one checks whether the unfactored portion of Q_k exceeds a prescribed fraction of $2\sqrt{N}$. If so, the factoring process is interrupted and the next Q_k is examined.

Another is "large prime variation" . If a number fails to factor completely over the factor base, the remaining factor R is seen to be a prime number if it is less than the square p_{max}^2 of the last prime of the factor base.

It is then saved. If Q_k and Q_l, $l > k$, have R as their largest prime divisor, then $Q_k Q_l / R^2$ factors over the factor base. At the same time we have to match this with $p_k p_l \cdot R^{-1} \pmod{N}$.

(One will actually have to lower the limit quite a bit below p_{max}^2, to increase the frequency of repeats. A moderate multiple kp_{max}, say $100 \leq k \leq 200$, seems to work well).

If $m > 1$ different Q_k contain the same large prime factor R, then $m - 1$ factorizations are created.

The inversion and division step in the next to last paragraph, although often indicated in the literature, is not really needed.

Fix the first Q_k having the large prime factor R. Consider each succeeding Q_l having that same large prime factor R. $Q'_l = Q_k Q_l$ is then of the form $Q''_l R^2$ where Q''_l factors over the factor base. Knowing the exponent vectors of Q_k, Q_l (ignoring the large prime factor R) we add these to get the exponent vector of Q''_l

We then find the relations between the exponent vectors of the Q's after replacing each of the Q_l by Q''_l.

Finally , for each relation (modulo 2) between the exponent vectors, multiply the Q's entering the relation, with each of the Q_l replaced by Q'_l, and extract the square root of that product (which is a perfect square, by construction). That can be done using an algorithm by Brillhart and Morrison to be presented later. In this procedure we can determining the exponents modulo 2 right away when trial dividing, at the cost of having to keep the Q's.

An alternative is to sum the corresponding nonreduced exponent vectors and halve the sum, much as in the Example below.

The result is then matched against the product of the p's with each p_l replaced by $p_k p_l$. This variant appears to be slower.

Including a large prime variation in a CFRAC program requires a great deal of extra programming effort, including a sort. One stores triples consisting of Q_k, preceded by their factor lists (headed by the large prime or 1), and the corresponding p_k. The triples are sorted, and collisions of first elements > 1 (the large prime) are handled as indicated above.

More details can be found in Riesel.

Finally, there are faster alternatives to the standard Gaussian algorithm for determining the dependencies, requiring, however, a much greater programming effort. These are of even greater importance in the more modern algorithms, such as the Quadratic and Number Field Sieves.

Without any of these refinements the reasonable range for using CFRAC (as a pastime) seems to be up to 35 digits. It has been supplanted by the Quadratic Sieve.

L.XI.1 Example. We illustrate a simple variant of the method on $N = 12007001$ (cf. the discussion in Riesel's book). Like most didactical examples it is really too small to illustrate the advantages of CFRAC over, e.g., trial division.

We use a factor base of nine elements, -1, and the eight smallest primes such that $(N/p) = 1$. The base is

$$-1, 2, 5, 23, 31, 43, 53, 59, 61.$$

We run QCF and make lists of the 10 first $k, p_k, (-1)^{k+1}Q_{k+1}$, such that $(-1)^{k+1}Q_{k+1}$ factors completely over the factor base. The p_k are reduced modulo N. We arrive at the following table:

k	p_k	$\pm Q_{k+1}$
5	2 228 067	40
9	668 093	1475
17	20	400
20	10 806 646	−976
23	7 209 052	2360
26	11 477 859	−155
27	6 764 708	2048
29	10 273 669	4000
31	4 333 614	1891
32	7 018 490	−2440

The matrix of exponent vectors, written as a list of lists, is

$$\begin{gathered}
[[0,3,1,0,0,0,0,0,0],\\
[0,0,2,0,0,0,0,1,0],\\
[0,4,2,0,0,0,0,0,0],\\
[1,4,0,0,0,0,0,0,1],\\
[0,3,1,0,0,0,0,1,0],\\
[1,0,1,0,1,0,0,0,0],\\
[0,11,0,0,0,0,0,0,0],\\
[0,5,3,0,0,0,0,0,0],\\
[0,0,0,0,1,0,0,0,1],\\
[1,3,1,0,0,0,0,0,1]]
\end{gathered}$$

For instance, $-976 = (-1)\cdot 2^4 \cdot 61$, accounting for the fourth row. The matrix is typically sparse.

Gaussian elimination produces the following five (not just one!) linear relations (modulo 2) among the exponent vectors:

$$\begin{gathered}
[[0,0,1,0,0,0,0,0,0,0],\\
[1,1,0,0,1,0,0,0,0,0],\\
[1,0,0,0,0,0,0,1,0,0],\\
[1,0,0,1,0,1,1,0,1,0],\\
[1,0,0,1,0,0,0,0,0,1]]
\end{gathered}$$

The single 1 in the first relation reflects the fact that the corresponding $Q = 400$ is a square.

Let us have a closer look at the fourth relation. Numbering from 0 to 9, it expresses that the product of number 0,3,5,6,8 of the $\pm Q$ above is a perfect square. Indeed, the sum of the corresponding exponent vectors is $[2, 18, 2, 0, 2, 0, 0, 0, 2]$ with all exponents even. Halving them gives

$$[1, 9, 1, 0, 1, 0, 0, 1].$$

Ignoring the sign (the first component) we see that $Q = R^2$ where $R = 2^9 \cdot 5 \cdot 31 \cdot 61 = 4840960$.

The product of the corresponding p_k is

$$p \equiv 2\,228\,067{\cdot}10\,806\,646{\cdot}11\,477\,859{\cdot}6\,764\,708{\cdot}4\,333\,614 \equiv 10\,842\,960 \pmod{N}.$$

A little bit of Euclid then yields the (prime) factors

$$(p \pm R, N) = 3001,\ 4001,$$

and, indeed, $N = 3001 \cdot 4001$.

The other four relations turn out to lead to only the trivial factors, on taking the gcd's.

We are still in the range where wait-for-a-square is faster (trial division is faster yet). The first square Q_{2k} is $Q_{68} = 1024 = 32^2$ and the corresponding p_{67} is $\equiv 11\,238\,777 \pmod{N}$, and $(11\,238\,777 - 32, N) = 3001$, $(11\,238\,777 + 32, N) = 4001$.

The period of $\sqrt{N}$, should you wonder, is 870. □

L.XI.2 Example. We sketch here Brillhart-Morrison's alternative method for finding the (modular) square root of a product, *known to be a square.* It is useful also in the context of the Quadratic Sieve.

Suppose the product is $Q_1 Q_2 \cdots Q_n$. Suppose, for $k < n$, we have achieved the factorization $Q_1 Q_2 \cdots Q_k = d_1 d_2 \cdots d_k e^2$ where $d_i | Q_i$, $i = 1, 2, \dots k$ and are relatively prime in pairs (initially, $Q_1 = Q_1 \cdot 1$).

We store $r = d_1 d_2 \cdots d_k$, the "reduced product", and e, the "free factor" (reduced modulo N). We find the gcd, $g = (r, Q_{k+1})$.

g contributes the factor g^2 to the total product, and is therefore multiplied to the free factor. It has the form $g = d''_1 d''_2 \cdots d''_k$, where d''_i divides d_i; $d_i = d'_i d''_i$, $i = 1, 2, \dots k$.

The quotient $d_{k+1} = Q_{k+1}/g$ is relatively prime to r/g, which now has the form $d'_1 d'_2 \cdots d'_k$. We have achieved

$$Q_1 Q_2 \cdots Q_{k+1} = (d'_1 d'_2 \cdots d'_k \cdot d_{k+1})(ge)^2$$

where the factor in the first pair of parentheses is our new reduced product, and the product ge is our new free factor (to be reduced modulo N).

When $k + 1 = n$, the reduced product must itself be a a square, since the whole product is, by assumption, The final step is to multiply its square root to the free factor, modulo N.

In the Example above, the factors are 40, 976, 155, 2048, 1891. The first gcd is $(40, 976) = 8$, giving our first reduced product $= 5 \cdot 122 = 610$, and free factor $= 8$.

Next, $(610, 155) = 5$, so our new reduced product is $(610/5) \cdot (155/5) = 3782$, and the new free factor is $5 \cdot 8 = 40$.

We now look at the fourth factor, 2048. This time we get $(3782, 2048) = 2$, new reduced product $1891 \cdot 1024 = 1936384$, and free factor $2 \cdot 40 = 80$.

The last factor is 1891, $(1\,936\,384, 1\,891) = 1\,891$, giving the reduced product $1\,936\,384/1891 = 1024$ and free factor $1891 \cdot 80 = 151280$. $1024 = 32^2$ so the desired square root is $32 \cdot 151\,280 = 4\,840\,960$.

□

L.XI.3 Example. The following example

$$N = 6589\,68977\,39494\,03132\,93285\,74193\,88201$$

has 34 digits. The factorization is

$$N = 474\,64739\,77078\,59989 \cdot 13\,88333\,69903\,04709.$$

Using a very simple program, and a factor base of 300 primes, led to 21 relations, (the typical proportion seems to be 5-10% of the length of the factor base).

Typically (for the case of two prime divisors), about half of them, 11 to be exact, led to factorizations. For, e.g., three primes, a greater portion factors, and generally, any factorization will occur.

The whole process took me 267 seconds, 0.12 of which were spent on row reduction. In the example above, I also tried a smaller base, of 200 primes, looking for 200+a few extra factorizations (the extras are usually not necessary, the system will be singular anyway).

That choice cut the running time by 50 seconds. A simple early abort stategy, stopping at the 50th prime, if the unfactored portion exceeded $2\sqrt{N}/100$, cut the time by another 75 seconds.

I have also tried a crude large prime variant, with a factor base of 100 primes bringing the running time down to 80 seconds.

A more sophisticated program combines the two tricks. With the same basis, moving the cut down to 15th prime, and lowering the limit for the unfactored portion to $2\sqrt{N}/500$, I brought the running time down to 40 seconds (for larger numbers, the divisor 1000 seems more appropriate). Introducing cuts at the 10th and 30th primes, with divisors 500 and 10^5 brought the running time down to 20 seconds. Clearly, early aborts produce great effects given the scant extra programming effort.

My method of dealing with the large primes was to set a negative number of extras, **extra**$= -k \cdot L$, where k lies somewhere between 0.4 and 0.6. The desirable number of factorizations was set to L+**extra**. The large prime limit was set at 200 times the largest prime in the factor base, and should possibly be set lower for a number this size. Each time a large prime was detected the variable **extra**, hence also the target number of factorizations, was augmented by one. The number of large primes in this case was around 1000, and there were about 75 repeats, yielding enough factorizations.

Denoting by FF the number of full factorizations over the factor base, and FL the number of factorizations including a large prime, a more orthodox procedure is to go on factoring until $FF + k \cdot FL$ exceeds the size of the factor base. k is a constant < 1, something like $0.6 - 0.7$ will do.

The number $257 \cdot F_7 = 257 \cdot (2^{128} + 1)$ is a historically interesting example as it was first cracked using CFRAC (the multiplier 257, found by experimentation, was introduced in order to achieve a reasonably long period).

Using a base of 200 primes and large prime variation with -120 "extras", my program ran for about 15 minutes, a 50% improvement over the basic algorithm.

An early abort at the 15th prime, with divisor 1000 took 5 minutes off that. A second cut, at the 50th prime, with divisor 10^6, produced an even more drastic reduction, to less than 4 minutes.

Keeping the first divisor, raising the second one to $4 \cdot 10^7$, and moving the cuts back to positions 10 and 30, reduced the running time even further, to 138 seconds. I have not made any further experiments on numbers of this size.

S Wagstaff and C Pomerance experimented a lot with these parameters in the 80's, but with much larger numbers and on a base of 959 primes. They recommended a second cut at the 95th prime, with divisor $4 \cdot 10^7$.

These running times are not very impressive in comparison with newer methods. There are more devices for speeding up a CFRAC program. However, given the greater efficiency of the newer methods, it is doubtful whether anyone would like to spend his energy on such efforts. Already a single-polynomial Quadratic Sieve, *without* large prime variation, is as fast, or even faster than CFRAC when we go beyond 35 digits.

A simple Elliptic Curves program of mine, comprising maybe 120 lines of code, cracks F_7 in a second. That method , like Pollard rho, is sensitive to the size of the smallest prime factor, which in this case has 17 decimal digits.

CFRAC was developed and implemented by Brillhart and Morrison in 1970. Their original article, “A Method of Factoring and the Factorization of F_7” was published in *Mathematics of Computation*, Vol. **29**, No. 129, Jan., 1975, pp. 183-205, and is yet today a very delightful and historically interesting read.

□

L.XII Elimination Modulo 2

Here we exemplify a standard algorithm for Gaussian elimination modulo 2.

We want to determine the dependencies among the rows of the matrix

$$\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{array}$$

We want to eliminate from right to left. Therefore we augment the matrix by an identity matrix *to the left*:

$$\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}$$

From elementary Linear Algebra you will recall that the elimination process creates zero rows to the right of the vertical line. The rows to the left of the zero rows will then give a complete set of linear relations among the the rows – they record the total row operation that produced the zero row.

"Complete" means every linear relation is a (unique) linear combination of these rows.

Looking at the last column we already have a zero in the first position. In the next position there is a one, and adding that row to the two rows below it creates zeros in their places:

$$\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{array}$$

We now delete the row we used, and the last column:

$$\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

Next we add the first row to the third:

$$\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{array}$$

Again we delete the row we used, and the last column:

$$\begin{array}{cccc|c} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{array}$$

Finally we add the first row to the second:

$$\begin{array}{cccc|c} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{array}$$

Deleting the first row, and the last column now leaves us with the coefficients of the relations between the four rows:

$$1 \quad 0 \quad 1 \quad 1$$

Each row in the matrix is a list (or whatever) of binary numbers that happen to equal 0 or 1, with lots of zero bits. The procedure is made more efficient by converting the list of binary numbers to one number, or one string of bits, using the shift and “bitwise or” operators. In Python the construction might look like this:

```
def pack(v):
    n=0L
    for k in v:
         n=(n<<1)|k
    return n
```

where v is the list representing a row in the matrix. The shift, $<<$, represents multiplication by 2, and the “or” operator (the vertical) adds in the bit k to the last place of n.

It pays to work in blocks by shifting n to the left ($n << 32$) repeatedly and packing segments of 32 elements of the list v. An alternative is to pack into several 32-bit words, and do the elimination in blocks.

The list of the four given rows will look like this on the screen, in decimal notation:

$$[6, 5, 1, 7].$$

Augmenting to the left with an identity matrix will look like adding $64 = 2^6$, $32 = 2^5$, 16, 8 to these numbers. The 2-powers are represented by left shifts of 1. The additions again are “bitwise or” operators.

The additions modulo 2 used in creating zeros are bitwise exclusive-or operators. Deletion of a zero column is division by two, represented by a shift operator (the routine can be arranged so as to save these shifts for last).

The “unpacking” is executed by “bitwise and” and shifts. In Python it might look like:

```
def unpack(n):
     v=[]
```

```
    while n>0:
         v=v.append(n&1)
         n=n>>1
    v.reverse()
    return v
```

v is a list, and we start with an empty list. The "and" operation reduces n modulo 2, i.e., it extracts the last bit from n, and the result is included in the list. The shift represents the removal of that bit.

If the number is very large, as may happen in other contexts, the conversion will have to be performed in blocks of, say, 32 bits. A "bitwise and" with $2^{32}-1 = 4294967295$ isolates the last 32 bits, a 32-fold shift, $n >> 32$, throws them away. (A really fast solution uses Python's built-in function hex.)

In a simple CFRAC program, the elimination modulo 2 contributes perhaps one half of the code and a tiny portion of the execution time!

L.XII: Exercises

1. (a) If you can muster the energy to write a full CFRAC program, you might like to try $(10^{37}-1)/9$, although CFRAC is slower than Pollard rho in this case (why?).
Another test example is

$$10\,11220\,07784\,34797\,33361\,71115\,62199.$$

The optimal size of the factor base seems to lie somewhere around 100. Experiment! (Pollard rho will crack it, too, but more slowly).
Miller-Rabin-test the factors.

(b) If you Miller-Rabin-tested (p. 325) the number

$$6\,85286\,63395\,04691\,22442\,23605\,90273\,83567\,19751\,08278\,43866\,81071,$$

and found a factor, CFRAC will crack the cofactor in reasonable time.

L.XIII Quadratic Sieve

Orientation

The most important modern factoring algorithms are the Elliptic Curves Method (ECM), the Multiple Polynomial Quadratic Sieve (MPQS), and the Number Field Sieve (NFS). Of these the first and the third depend on extensive theoretical preparations beyond the scope of this text. The Quadratic Sieve is very elementary in comparison. The analysis of its performance is less elementary, of course.

NFS is responsible for some recent spectacular factoring records, although its practicality has been questioned. ECM is best suited for finding prime factors of 20-30 digits, even in very large numbers. It is remarkable in its minimal storage requirements and the modest programming effort that goes into it.

As an introduction to the full Quadratic Sieve algorithm, as described in, e.g., Crandall-Pomerance, I will first outline a simple version of the single polynomial Quadratic Sieve. Even in this simple form, requiring a few pages of code, the QS outdoes CFRAC (even with large prime variation and early aborts) at least from 35 digits upwards. It is not nearly as fast as the MPQS or ECM, but it will crack 40-digit numbers while you check your email and 45-digit numbers while you prepare a meal.

The number we wish to factor is denoted N. It is odd and has been proven composite. By trivial division (up to, say, $5 \cdot 10^5$) and, e.g., a standard rho routine (with, say, 10^6 turns of the loop) we have removed all smaller factors, perhaps up to 10 digits. A more serious program would remove even larger factors, using the ECM.

We let m denote the floor of $\sqrt{N}$. We will use a *sieving polynomial* $f(X) = (X+m)^2 - N$. We are looking for X-values in a symmetric interval $|X| \leq M$, M much smaller than m (the *sieving interval*), for which $f(X)$ factors over a *factor base*. Such a base consists of the sign -1 and prime numbers p below a prescribed *smoothness bound* B. Of these we need only keep the prime 2 (if $N \equiv 1 \pmod 8$) and those odd p for which $(N/p) = 1$, of course.

The factorizations determine exponent vectors modulo 2. By Gaussian elimination we can find combinations of vectors that sum to zero modulo 2. Multiplying the corresponding polynomial values $f(X)$ on the one hand, and the corresponding $(X + m)^2$ on the other hand, we arrive at congruences of the form $a^2 \equiv b^2 \pmod{N}$. Hopefully one or both of the gcd's $(a \pm b, N)$ will then reveal a proper factor of N.

The product a of the $X + m$ modulo N is easy to determine if we store the $(X + m)$-values in a list as we go along. Storing the corresponding $f(X)$-values, and using Brillhart–Morrison's algorithm, we find the value for b.

We cannot afford to trial-divide all the values of $f(X)$ over the factor base. We must have some crude method of selection of the X to try.

The basic idea, soon to be modified, is the following. For each prime p there are two square-roots of N modulo p. Let us call them $\pm r$. For each number of the form $X = k \cdot p \pm r$ in the sieving interval the prime number p divides $f(X)$. If we start with a list of ones we could multiply in those factors p in their respective locations. Doing this for all p, we would find which $f(X)$ factor completely.

There is however one error and several flaws in this procedure. We are forgetting multiple factors – small primes frequently are. For instance, if $N \equiv 1 \pmod{8}$, half of the values are divisible by 8. Sieving over small primes is also very time-consuming. It is furthermore too time-consuming to compute all the polynomial values. The modified idea is to first find out which polynomial values are reasonably close to factoring, and only then perform the trial division.

In dealing with approximations we also replace multiplication by the faster operation addition, i.e., we work with (approximate) logarithms, e.g., the integers closest to the various 2-logarithms. I found it expedient to exclude several small primes, when sieving.

Also we do not check whether the logarithms, in the location corresponding to X, sum approximately to $\log(|f(X)|)$. Instead we choose a constant *target*, the log of the average of $|f(X)|$. As m^2 approximates N, and X^2 is small compared to N, $|(X + m)^2 - N| \approx |2mX|$, the average of which is mM. Our target is therefore taken as an approximation of $\log(m) + \log(M) \approx \log(N)/2 + \log(M)$.

We will have to subtract a small error term d to compensate for the fact that we leave out small primes and ignore prime powers. In case we introduce the large prime variation, described in the context of CFRAC, a common choice is to subtract $d = 2 \cdot p_{max}$ where $p_{max]}$ is the largest prime of the factor base.

Those X that produce a sum of logarithms exceeding $\log(N)/2 + \log(M) - d$ are those for which we trialdivide $f(X)$ over the factor base. That saves a *lot* of work. Only perhaps a few hundred values in a million are tested – or even computed! – and a substantial portion of these yield full factorizations. This portion will depend on details of the program, such as the choice of error term and the number of primes (or prime powers!) excluded from sieving.

With limited storage we are forced to work in blocks, i.e., we process intervals of a given length L, from the center outwards: $[0, L)$ $[-L, 0)$, $[L, 2L)$ .... On my machine the ideal seems to be $L = 10^6$.

The number of blocks need not be specified in the single polynomial version; we could check the accumulated number of exponent vectors after each block and quit sieving as soon as it exceeds the size F of the factor base (in all my runs $0.97 * F$ sufficed).

With large prime variation it is not quite that easy. We must attach some weight to the number of large prime factorizations as we did with the CFRAC, and go on sieving until the weighted sum exceeds the length of the factor base (or slightly less). A suggestion of Silverman's is to stop when $FF+(1-R)FL > R\cdot$ the length of the factor base, where R is slightly less than 1, say $R = 0.96$. FF again denotes the number of fully factored polynomial values, FL the number of those values including one large prime outside the factor base.

For 39 digits the expected number of blocks is maybe 100, for 49 digits several thousand –working with multiple polynomials reduces the sieving interval drastically. The smoothness bound could be 45 000-50 000 for 39-40 digits, maybe 110 000-120 000 for 45-46 digits. These bounds are again smaller in the full multiple polynomial algorithm, and smaller yet with large prime variation - which in this case requires more storage than in CFRAC. The elimination stage is also more of an issue in QS as the factor bases for numbers of a given size are much larger.

If the quantities $a + b, a - b$, hence also a, b, have an odd prime factor in common it must belong to the factor base. As we have already weeded out small factors this means that QS will never crack a prime power. If you get 100 relations in the elimination step and none of them leads to a factorization you will know why. Should you enter a square (prime or not), your factor base would be about twice the expected size. It would probably make some of your parameter choices far from optimal.

But a serious factoring program should check this pathology at the beginning. The Newton procedure we have explained earlier for finding the floor of a square root, is easily modified to find exact square roots, cubic roots, etc.

Multiple Polynomials

Anyone who has written a basic QS program will have noticed how the number of fully factored reports diminish as we travel away from the origin. Peter Montgomery's ingenious idea was to introduce several sieving polynomials of the form $(aX + b)^2 - N$, and sieve each over a shorter interval. By choosing a, b so that $a \mid (b^2 - N)$, the polynomial can be written in the form $a(aX^2 + 2bX + c) = ag(X)$, i.e., all its values are divisible by a.

By a skillful choice of a we can achieve that the values of $g(X)$ are on the average of the same magnitude as those of $(X + m)^2 - N$, or even slightly smaller. We assume $0 < b < a/2$. Then the minimum of $ag(X)$ is close to $X = 0$, so we sieve over a symmetric interval, $|X| \leq M$. The minimum value is $-N$. The greatest values are assumed at the endpoints, and are approximately $a^2M^2 - N$. It is reasonable to make these two equal in absolute value, i.e., $a^2M^2 \approx 2N$, $a \approx \sqrt{2N}/M$. The approximate maximum of $|g(X)|$ is $N/a \approx M\sqrt{N}/\sqrt{2}$.

Classical MPQS now chooses a to be the square of a prime number q. b is then to be taken as a square root of N modulo q^2, available by, e.g. Berlekamp (+Hensel), or the *Lucas sequences* to be introduced in the next Section. The square rooting routine can be avoided by choosing $q \equiv 3 \pmod 4$. In that case the solution to $x^2 \equiv b \pmod q$ is, as we have noted before, $x \equiv \pm b^{(q+1)/4}$ $\pmod q$.

There are two roots between 0 and a and we can choose the one closest to 0. q can be generated by the methods introduced earlier. Note that we need not determine $c = (b^2 - N)/a$.

The sieving proceeds much as in the single polynomial case, only we have to the factor a into account when trial dividing. Also, the average of $|g(X)|$ is more like $\sqrt{2N}M/3$. Note that the factor base is the same as in the single polynomial case – we are looking for primes p that divide $(aX + b)^2 - N$, hence we still require that $(N/p) = 1$.

The most time-consuming step when initializing a new polynomial is to invert a modulo each prime p in the factor base (or at least those used in sieving) so as to determine the roots of $ag(X)$ modulo p. The square roots of N modulo p are computed at the beginning of the program and reused when determining the roots of a new sieving polynomial.

The extra effort in expanding a single polynomial routine to one using multiple polynomials is surprisingly small, especially in comparison with large prime variation. One should attempt the former first, as it brings down the length of the lists involved.

The‘self-intializing” QS, known as SIQS, chooses a to be the product of several prime numbers in the factor base. If a is composed of 5 prime factors, say, there are 32 square roots b of N modulo a, but as $\pm b$ yield the same polynomial values we keep only half of them. Nonetheless, that means that we need only one inversion step to produce the roots of 16 polynomials, which is a considerable saving when factoring large numbers.

For very clear accounts of the details I refer to Bressoud and Crandall-Pomerance (the Quadratic Sieve is Pomerance’s invention). The latter book also explains SIQS.

A very full, practical, account of SIQS is Scott Contini’s MSc thesis, downloadable from his website, `http://www.crypto-world.com/Contini.html`.

The QS originated with Pomerance. Multiple polynomials is Peter Montgomery’s idea. The classical reference is Robert D Silverman: “The Multiple Polynomial Quadratic Sieve”, *Mathematics of Computation*, **48**, No 177 (1987), 329-339.

A reader with experience in the C programming language might enjoy studying the code in `http://www.friedspace.com/QS/` (by William Hart, 28 pages) or `http://www.boo.net/~jasonp/qs.html` (by Jason Papadoupolos, 99 pages).

L.XIV Lucas Sequences and Primality

Some earlier methods have relied on factoring $N-1$ easily. Maybe we do not get enough factors that way. Then perhaps $N+1$ might prove more successful. The tool is *Lucas sequences.* For more details on these, see the books by Riesel and Bressoud-Wagon.

We study the linear recurrence

$$S_{n+2} - PS_{n+1} + QS_n = 0; \quad n \geq 0; \qquad S_0, S_1 \text{ given.}$$

P, Q are integers. A popular choice is $P = Q = 5$ or $P = 1$, $Q = \pm 2, \pm 3, \ldots$ – the theoretical reason for this is explained in Bressoud-Wagon.

The sequence $S_0, S_1, S_2, \ldots$ then also consists of integers, uniquely determined by the conditions. We will consider the same sequence taken modulo the odd number N, the primality of which we wish to investigate. It has already been subjected to a Miller-Rabin test, of course.

We let p denote an arbitrary prime factor of N. We hope to prove that $p = N$.

The recurrence may be written in matrix form:

$$\begin{pmatrix} S_{n+2} \\ S_{n+1} \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} S_{n+1} \\ S_n \end{pmatrix} = M \begin{pmatrix} S_{n+1} \\ S_n \end{pmatrix}$$

whence:

$$\begin{pmatrix} S_{n+1} \\ S_n \end{pmatrix} = M^n \begin{pmatrix} S_1 \\ S_0 \end{pmatrix}.$$

For n fixed we easily find S_n modulo a given positive integer, using binary exponentiation of the matrix M. Another, more efficient, scheme will be presented in the last Section.

Now assume that the discriminant $D = P^2 - 4Q$ satisfies $(D/N) = -1$. Then also $(D/p) = -1$ for some prime factor $p|N$. Of course, D is then not a perfect square in itself. We further assume that $(N, Q) = 1$, so that Q is invertible modulo N, and also, a fortiori, modulo every prime factor of N.

The roots of the quadratic equation

$$X^2 - PX + Q = 0$$

are then the irrational numbers

$$a = \frac{P + \sqrt{D}}{2}, \quad b = a' = \frac{P - \sqrt{D}}{2}$$

(note that 2 is invertible modulo N).

The sequences $S_n = a^n, b^n$, satisfy the recurrence, e.g.,

$$a^{n+2} - Pa^{n+1} + Qa^n = a^n(a^2 - Pa + Q) = 0,$$

and so do all linear combinations of the two sequences.

We will concentrate on two special solution sequences,

$$U_n = \frac{a^n - b^n}{a - b}, \quad V_n = a^n + b^n.$$

Their initial values are $U_0 = 0, U_1 = 1$ and $V_0 = 1 + 1 = 2, V_1 = a + b = P$.

From the identity

$$2(a^{n+1} - b^{n+1}) = (a+b)(a^n - b^n) + (a-b)(a^n + b^n)$$

we conclude (dividing by $a - b$) that

$$2U_{n+1} = PU_n + V_n.$$

Another useful formula is the *doubling formula*:

$$U_{2n} = U_n V_n,$$

which follows directly from the conjugate rule

$$a^{2n} - b^{2n} = (a^n - b^n)(a^n + b^n),$$

again by division.

Now suppose $U_n \equiv 0$, $U_{n+1} \equiv m \pmod{N}$, where m is some integer. That is m times the initial values $U_0 \equiv 0$, $U_1 \equiv 1 \pmod{N}$. This means that the sequence will repeat from n on, but multiplied by m. Hence also $U_{2n} = U_{3n} = \cdots = 0$.

There is a shortest period $k > 0$ satisfying $U_0 = U_k = U_{2k} = \cdots = 0$. We now prove that every other period is a multiple of k.

L.XIV.1 Lemma. *Let $M > 0$ be a positive modulus, satisfying $(Q, M) = 1$. Let further k be the smallest positive index for which $U_k \equiv 0 \pmod{M}$, and $n > 0$ an arbitrary index satisfying $U_n \equiv 0 \pmod{M}$. Then k divides n.*

Proof. We first note that if two irrationalities of the form $r + s\sqrt{D}$, $r, s \in \mathbf{Z}$, are (componentwise) divisible by M, then so is their product.

We next recall that $ab = Q$, so the invertibility of Q entails that of a and b modulo M.

We then have the following equivalence:

$$\begin{aligned} U_n \equiv 0 \pmod{M} &\iff a^n \equiv b^n \pmod{M} \\ &\iff a^{2n} \equiv (ab)^n = Q^n \pmod{M}, \end{aligned}$$

where we get from the rightmost member to the middle member on multiplication by the the inverse to a^n modulo M. And from the first to the second on multiplication by $a - b = \sqrt{D}$.

Letting $QR \equiv 1 \pmod{M}$, and multiplying the last congruence by R^n, we get

$$U_n \equiv 0 \pmod{M} \iff (a^2R)^n \equiv 1 \pmod{M}.$$

k is by assumption the least $n > 0$ having that property. Hence it is the order of a^2R modulo M, and the Lemma follows by the general theory of orders of invertible classes, (A.V.5), readily generalizable to this case (exercise!). □

The number k is not the period of the sequence U_n, properly speaking, only of the zeros appearing in it. Bressoud calls it the “rank” of the U-sequence.

Now consider the sequence taken modulo p, where p is a prime number such that $(D/p) = -1$. We will need to generalize Little Fermat. First we state yet another version of “Freshman’s Dream”.

We let x and y denote integers or quadratic irrationalities of the form

$$c + d\sqrt{D},$$

where $c = r/s$, $d = t/u$ are rational numbers, with r, u relatively prime to p, hence invertible modulo p. Hence it is meaningful to speak of r/s, t/u modulo p. Then:

L.XIV.2 Lemma (Freshman’s Dream).

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

□

We are still assuming that D is not a quadratic residue modulo p, hence not a perfect square. We will use the first part of the following Corollary to Freshman’s Dream. Applied to the situation above, and the two roots a, b, it implies $a^p \equiv b$, $b^p \equiv a \pmod{p}$.

L.XIV.3 Corollary.

$$\left(\frac{D}{p}\right) = -1 \Rightarrow (c + d\sqrt{D})^p \equiv c - d\sqrt{D} \pmod{p},$$

$$\left(\frac{D}{p}\right) = 1 \Rightarrow (c + d\sqrt{D})^p \equiv c + d\sqrt{D} \pmod{p}.$$

Proof.

$$(c + d\sqrt{D})^p \equiv c^p + d^p D^{(p-1)/2}\sqrt{D} \equiv c^p + d^p\left(\frac{D}{p}\right)\sqrt{D} \equiv c + d\left(\frac{D}{p}\right)\sqrt{D}$$

Here we used Euler's Criterion and Little Fermat. □

With our previous notation, and the chosen p, it then holds that

$$U_p \equiv \frac{a^p - b^p}{a - b} \equiv \frac{b - a}{a - b} \equiv -1 \pmod{p},$$

and

$$\begin{aligned} U_{p+1} &\equiv \frac{a^{p+1} - b^{p+1}}{a - b} \\ &\equiv \frac{a \cdot b - b \cdot a}{a - b} \equiv 0 \pmod{p}. \end{aligned}$$

This shows that $U_k \equiv 0 \pmod{p}$ occurs with period $p+1$ or a factor of $p+1$, if $(D/p) = -1$, and with period $p - 1$, or a factor of $p - 1$, otherwise.

So at least we have a pseudoprime test:

L.XIV.4 Theorem. *Assumptions and notation as above. If*

$$U_{N+1} \not\equiv 0 \pmod{N},$$

then N is composite.

L.XIV.5 Example. $N = 450\,74455\,37641$. With $P = 1, Q = 3, D = -11$, $(D/N) = -1)$ one obtains $U_{N+1} \equiv 72\,44374\,53394 \not\equiv 0 \pmod{N}$, and N is composite. It is a Carmichael number (cf. p. 90), $N = pqr = 9091 \cdot 18181 \cdot 27271$, with $p - 1, q - 1, r - 1$ dividing $N - 1$, resisting a simple Fermat test. (Note that the factors are of the form $t + 1, 2t + 1, 3t + 1$.) □

One can prove the following *sufficient* condition for primality, in analogy with the Primitive Root test (L.VII.1):

L.XIV.6 Theorem. *Assumptions as above. Suppose* $U_{N+1} \equiv 0 \pmod{N}$*, but* $U_{(N+1)/q} \not\equiv 0 \pmod{N}$ *for each prime factor* $q|(N+1)$*. Then* N *is prime.*

□

The proof depends on an investigation into the relevant analogue of Carmichael's λ function (C.V.3), the maximal order function $\omega(N)$. One can prove $\omega(N) \leq 0.8N < N+1$ if N has at least two different prime factors.

In the case of of a prime power $N = p^t$ one proves that $\omega(N)$ divides $p^t \pm p^{t-1}$ (generally), and equals $p^t \pm 1$ (from the assumption). However, $p^t \pm 1 \nmid p^t \pm p^{t-1}$ except when $t = 1$.

The details are given in Bressoud-Wagon and Riesel.

The following is the Lucas analogue of Pocklington's Theorem. It was first discovered by Swedish mathematician and computer scientist Hans Riesel (1929-), later rediscovered and published by Michael Morrison.

L.XIV.7 Theorem (Riesel-Morrison). *Assumptions as above. Suppose* $U_{N+1} \equiv 0 \pmod{N}$*, but* $(U_{(N+1)/q}, N) = 1$ *for some of the prime factors* $q|N$*. Let* F *be the product of the corresponding prime powers* q^k *dividing* N*. Then every prime factor* $p|N$ *is congruent to* $+$ *or* -1 *modulo* F*.*

Proof. Let p be a prime factor of N, and let d be the order of the U-sequence modulo p.

The assumptions say that d divides $N+1$, but none of the $(N+1)/q$. In the same manner as in the proof of Pocklington (see L.VII.3) we infer that $F|d$.

Further, by the general theory, d divides $p+1$ or $p-1$, so F divides one of these numbers. □

L.XIV.8 Example. Let us have a look at

$$N = 59\,64958\,91274\,97217,$$

a factor of the Fermat number F_7. The prime factorization of $N+1$ is $2 \cdot 3 \cdot 733 \cdot 1356\,28897\,51591$.

Looking for a recurrence

$$U_{n+2} - PU_{n+1} + QU_n = 0,$$

with $(D/N) = (P^2 - 4Q/N) = -1$, we fix $P = 1$, and step up $Q = \pm 2, \pm 3 \ldots$. The choice $Q = 3$, giving $D = -11$, is the first that works. A computer run produced the following:

```
P, Q, D = 1 2 -7 , (D/N) = 1
P, Q, D = 1 -2 9 , (D/N) = 1
P, Q, D = 1 3 -11 , (D/N) = -1
prime factors of 59649589127497218 :
[13562889751591L, 733, 3, 2]
testing the factor q= 13562889751591
U((N-J)/q): 11132979547214806
gcd with N: 1
testing the factor q= 733
U((N-J)/q): 7106250345218906
gcd with N: 1
testing the factor q= 3
U((N-J)/q): 57414734989485274
gcd with N: 1
testing the factor q= 2
U((N-J)/q): 9394399751895754
gcd with N: 1
```

proving the primality of Q without the slightest doubt. (The J stands for the Jacobi symbol $(D/N) = -1$.) □

L.XIV.9 Example. Next we look at $R = 407477800048937789623$. Is it prime? $R+1 = 2^3$ times a product of simple factors. The same procedure gives

```
P, Q, D = 1 2 -7 , (D/N) = 1
P, Q, D = 1 -2 9 , (D/N) = 1
```

```
P, Q, D = 1 3 -11 , (D/N) = 1
P, Q, D = 1 -3 13 , (D/N) = 1
P, Q, D = 1 4 -15 , (D/N) = -1
prime factors of 407477800048937789624 :
[12040620145783L, 71699, 59, 2]
testing the factor q= 12040620145783
U((N-J)/q): 193977511718274844669
gcd with N: 1
testing the factor q= 71699
U((N-J)/q): 373867674101395430255
gcd with N: 1
testing the factor q= 59
U((N-J)/q): 198619893718259475088
gcd with N: 1
testing the factor q= 2
U((N-J)/q): 0
gcd with N: 407477800048937789623
```

So, according to Riesel-Morrison, every prime factor of R is congruent to $+$ or -1 modulo $F = 59 \cdot 71\,699 \cdot 1\,204\,06201\,45783 = (R+1)/8$, hence there is room for only one, i.e., R is prime.

Remark: The reader wishing to program this test should of course stop when the accumulated product of prime factors exceeds the square root, as we did in the case of Pocklington.

If we try the other factor of F_7, $M = 57\,04689\,20068\,51290\,54721$, it turns out that $M+1 = 2\cdot 7\cdot R$, which makes the Lucas method a bit awkward compared to, e.g., Pocklington, or the Primitive Root Test. The largest prime factor of $M-1$ has 12 digits, so $M-1$ cracks easily, and M then yields to a Primitive Root test, base, e.g., =21, the smallest positive primitive root. Pocklington, base 3, also works.

The success of either algorithm depends on the efficiency of your factoring algorithm, and on the size of the factors found. A combination of the two methods may be optimal. See the books already cited. □

The U-sequence test should really be accompanied by a computation of the corresponding V-value – see the exercises at the end of the Chapter.

An intriguing application of Lucas sequences (with polynomial parameters) is given in Section 49 of Nagell's book, where he proves that there are infinitely many primes $\equiv -1$ modulo any given integer $n \geq 2$ (cf. F.VIII.9). The periods of U-sequences plays a decisive role. Beware that his V are our U, and his U are half our V.

L.XIV: Exercises

1. Explain why the choices $P = \pm 1$ and $Q = 1$ make for a very poor pseudoprimetest.

2. Express V_{m+n} in terms of V_m, V_n, and V_{m-n}, $m \geq n$. Then do the same for the U-sequence.

3. Let a, b be the roots of $X^2 - PX + Q = 0$ (possibly modulo some positive integer). What is the equation satisified by a^2, b^2? Express the sequence V_{2m}, $m = 0, 1, 2, 3, \ldots$ belonging to the parameters P, Q, as a V_m-sequence belonging to other parameters.

Then generalize to k in place of 2.

4. Let q be a prime number. Suppose $U_{2m} \equiv 0 \pmod q$. Show that either $U_m \equiv 0$ or $V_m \equiv 0 \pmod q$. Use this observation to devise the Lucas analog of the Miller-Rabin test, starting with the factorization $n - (D/n) = 2^t \cdot u$.

L.XV Mersenne Numbers

We now give a criterion for the primality of the Mersenne number $N = M_p = 2^p - 1$, where p is a prime number ≥ 3. It is due to E. Lucas, and American mathematician Derrick Lehmer (1905-1991).

We study the special recurrence

$$S_{n+2} - 4S_{n+1} + S_n = 0; \quad n \geq 0.$$

The roots of the equation $x^2 - 4x + 1 = 0$ are $a = 2 + \sqrt{3}$, $b = 2 - \sqrt{3}$. The discriminant of the equation is $D = 4^2 - 4 \cdot 1 \cdot 1 = 12 = 2^2 \cdot 3$.

As $N \equiv -1 \pmod 8$, the Jacobi symbol $(2/N) = 1$. Further $N \equiv 3 \pmod 4$, $N \equiv 1 \pmod 3$, so $(3/N) = -(N/3) = -1$. This means that the corresponding relation holds for at least one prime factor of N.

We have already shown that the sequences

$$U_n = \frac{a^n - b^n}{a - b}, \quad n \geq 0,$$

and

$$V_n = a^n + b^n,$$

with initial values $U_0 = 0$, $U_1 = 1$ and $V_0 = 2, V_1 = 4$ satisfy the recurrence.

We also have

$$U_{2n} = U_n V_n \quad \text{and} \quad V_{2n} = V_n^2 - 2(a^n b^n) = V_n^2 - 2.$$

Setting

$$T_k = V_{2^{k-1}}$$

we have

$$T_{k+1} = T_k^2 - 2, \quad T_1 = V_1 = 4.$$

As $D = (a - b)^2$ we also have the following identity:

$$V_n^2 - DU_n^2 = (a^n + b^n)^2 - (a^n - b^n)^2 = 4a^n b^n = 4Q^n. \qquad (*)$$

We prove the sufficiency part of the Lucas(-Lehmer) criterion first.

L.XV.1 Theorem. *If*

$$T_{p-1} = V_{(N+1)/4} \equiv 0 \pmod{N},$$

then N is a prime.

Proof. Let q be a prime factor of N. Obviously then

$$U_{(N+1)/2} = U_{(N+1)/4}V_{(N+1)/4} \equiv 0 \pmod{q}.$$

As $V_{(N+1)/4} \equiv 0 \pmod{q}$, and $Q = 1$, the identity (*) shows that $(U_{(N+1)/4}, q) = 1$.

This means that the exact order of the U-sequence, modulo q, equals $(N+1)/2$. It is also a factor of $q \pm 1$. So $(N+1)/2 \le q \pm 1$, $q|N \le 2q+1 < 3q$. That leaves room for only one prime factor, hence $N = q$. □

L.XV.2 Example. Here are the numbers (modulo N), produced by the algorithm, proving $2^{17} - 1$ to be a prime number:

$$\begin{array}{llll}
T_1 = 4, & T_2 = 14 & T_3 = 194 & T_4 = 37634, \\
T_5 = 95799, & T_6 = 119121, & T_7 = 66179, & T_8 = 53645, \\
T_9 = 122218, & T_{10} = 126220, & T_{11} = 70490, & T_{12} = 69559, \\
T_{13} = 99585, & T_{14} = 78221, & T_{15} = 130559, & \\
T_{16} = 0. & & &
\end{array}$$

The last prime record verified by hand was $2^{127} - 1$. The Lucas-Lehmer test verifies this on my 1.83 GHz computer in about 0.001 seconds.

Riesel's record from 1957-1961, $2^{3217} - 1$, a 969 digit number, takes about 2 seconds.

The first record of the 1970's, $2^p - 1$, $p = 19937$, a 6002 digit number, originally took 35 minutes to verify.

A straightforward application of the Lucas criterion on my computer would take something like 7 minutes! Simply too much time is spent on squaring numbers and reducing them modulo a large number only afterwards.

The books of Riesel and Crandall-Pomerance describe some strategies for fast squaring and algorithms for computing modulo large numbers of special construction. □

We now turn to the necessity part.

L.XV.3 Theorem. *If $q = 2^p - 1$ is a prime, then $T_{p-1} \equiv 0 \pmod{q}$.*

Proof. As

$$T_p = T_{p-1}^2 - 2,$$

it suffices to prove that

$$T_p = V_{2^{p-1}} \equiv -2 \pmod{q}.$$

Recall the facts $(2/q) = 1, (3/q) = -1$ derived above. We will use the Corollary to Freshman's Dream (L.XIV.3) above. Also $(1+\sqrt{3})^2 = 4+2\sqrt{3} = 2a$.

First we recall the definition:

$$T_p = a^{(q+1)/2} + b^{(q+1)/2},$$

as $q + 1 = 2^p$.

We are finished if we can prove that both terms are $\equiv -1 \pmod{q}$.

Now

$$\begin{aligned} 2^{(q+1)/2}a^{(q+1)/2} &= (1+\sqrt{3})^{q+1} = (1+\sqrt{3}) \cdot (1+\sqrt{3})^q \equiv \\ &\equiv (1+\sqrt{3}) \cdot (1+\sqrt{3})^q \equiv (1+\sqrt{3}) \cdot (1-\sqrt{3}) \equiv -2 \pmod{q}. \end{aligned}$$

We applied the Corollary just mentioned to $m + n\sqrt{3} = 1 + \sqrt{3}$.

At the same time

$$2^{(q+1)/2} = 2 \cdot 2^{(q-1)/2} \equiv 2 \cdot \left(\frac{2}{q}\right) \equiv 2 \pmod{q}$$

by Euler's Criterion. We plug this into the congruence above, and then multiply by the inverse to 2 modulo q, yielding

$$a^{(q+1)/2} \equiv -1 \pmod{q},$$

and, by conjugation,

$$b^{(q+1)/2} \equiv -1 \pmod{q},$$

whence the desired result, by addition. □

L.XVI Lucas and Modular Square Roots

Modular square roots, i.e., solutions to quadratic congruences of the type

$$x^2 \equiv Q \pmod{p}, \quad p \text{ prime},$$

are essential to performing, e.g., Cornacchia's Algorithm. They also appear in the context of certain factoring algorithms, such as the Quadratic Sieve. We have already given an algorithm due to Berlekamp (see Section E.IV). Here we give another one, using Lucas sequences.

As we have already seen, the case $p \equiv 3 \pmod 4$ is particularly simple, just take $x \equiv \pm Q^{(p+1)/4} \pmod p$. So we now assume that $p \equiv 1 \pmod 4$. Just like the previous algorithm this one depends on knowing a quadratic non-residue modulo p.

We again study recurrences with characteristic polynomial $X^2 - PX + Q$, having the zeros a, b. We assume P chosen so that

$$D = (a-b)^2 = P^2 - 4Q$$

is a quadratic non-residue modulo p.

The letters U, V keep their old meaning.

Let $m = (p+1)/2$. Then

$$V_m = a^m + b^m; \quad V_m^2 = a^{p+1} + b^{p+1} + 2(ab)^m = a^{p+1} + b^{p+1} + 2Q^m.$$

By Euler's Criterion, $Q^{(p-1)/2} \equiv 1 \pmod p$, as $(Q/p) = 1$. Hence $Q^{(p+1)/2} \equiv Q \pmod p$.

We also know, by L.XIV.3, that $a^p \equiv b$, $b^p \equiv a \pmod p$, hence $a^{p+1} + b^{p+1} \equiv 2ab \equiv 2Q \pmod p$.

Putting these observations together we arrive at:

$$V_m^2 \equiv 4Q \pmod{p}.$$

Using $m \cdot 2 \equiv 1 \pmod p$, and multiplying by m^2, we obtain the following:

L.XVI.1 Theorem. *Notation and assumptions as above. The solution to the congruence* $x^2 \equiv Q \pmod p$ *is* $x \equiv \pm m V_m \pmod p$, *where* $m = (p+1)/2$.

□

Remark: An alternative is: if V_m is even, then divide by two; if V_m is odd, add p, then divide.

Before we give an Example we express the result in terms of the U-sequence as well.

L.XVI.2 Theorem. *Notation and assumptions as above. The solution to the congruence* $x^2 \equiv Q \pmod{p}$ *is* $x \equiv \pm U_{m+1} \pmod{p}$*, where* $m = (p+1)/2$*.*

Proof. As $U_m V_m = U_{2m} = U_{p+1} \equiv 0 \pmod{p}$, by the general theory, and $V_m \not\equiv 0 \pmod{p}$, $U_m \equiv 0 \pmod{p}$, $a^m \equiv b^m \pmod{p}$.

Further, we proved in the beginning that $2U_{m+1} - PU_m = V_m$, so, multiplying by $m = (p+1)/2$ we see that $U_{m+1} \equiv mV_m \pmod{p}$, thereby finishing the proof. □

L.XVI.3 Example. For our example we take the prime number $p = 479255977$ and $Q = 2$. Certainly $(Q/p) = 1$ as $p \equiv 977 \equiv 1 \pmod{8}$.

By trial and error we find a small P such that $P^2 - 4Q$ is a quadratic nonresidue modulo p. A simple Jacobi routine leads (e.g., by stepping up P) to the choice $P = 7$.

We compute U_{m+1}, modulo p, $m = (p+1)/2$ using, e.g., binary exponentiation of the matrix M introduced in the beginning. (The most efficient method is to use the scalar recursive formula for the U_n given in the last Section of this Chapter.)

We get $x \equiv \pm 103\,530\,344 \pmod{p}$. □

Remark:

As $U_m \equiv 0 \pmod{p}$, that is, $a^m \equiv b^m \pmod{p}$, we also get $b^{m+1} \equiv ba^m \pmod{p}$ whence

$$U_{m+1} = \frac{a^{m+1} - b^{m+1}}{a-b} \equiv \frac{aa^m - ba^m}{a-b} \equiv a^{(p+1)/2} \pmod{p}.$$

Quite reasonable, as

$$(a^{(p+1)/2})^2 \equiv a^{p+1} \equiv ab \equiv Q \pmod{p}.$$

With a little bit of Algebra we could prove more directly that $a^{(p+1)/2}$ is indeed congruent to an ordinary integer modulo p. Those who know some "Abstract" Algebra will realize that the classes $m + n\sqrt{D}$ modulo p form a *finite field*, i.e., all non-zero classes are invertible. (This is because the polynomial $X^2 - D$ is *irreducible* modulo p, D being a quadratic non-residue.)

The really important issue is the lack of zero-divisors. For, suppose $(m + n\sqrt{D})(r + s\sqrt{D}) \equiv 0 \pmod{p}$, with the first factor incongruent to 0 modulo p. Multiplying by the conjugate of the first factor gives $(m^2 - Dn^2)(r + s\sqrt{D}) \equiv 0 \pmod{p}$, where the first factor is a rational integer incongruent to zero, as $(D/p) = -1$, and $p \nmid m, n$. This forces the second factor to be congruent to zero modulo p.

Lagrange's Theorem on polynomial congruences easily generalizes to this case. Hence the congruence $x^2 \equiv Q \pmod{p}$ can have only two solutions, those known to exist, as $(Q/p) = 1$, with irrational part $n = 0$

By this token the Lucas sequence solution connects with the so-called Cipolla Algorithm, given in, e.g., Crandall-Pomerance, and Bach-Shallit.

L.XVI: Exercises

1. Write a simple routine checking the primality of some Mersenne numbers, e.g., those mentioned in the texts, further $2^{107} - 1, 2^{277} - 1, 2^{719} - 1$.

2. Using the scalar fomulas in the next Section, and the U-sequence algorithm, compute some modular square roots, e.g., solve $x^2 \equiv y \pmod{p}$ for

(a) $y = -1, 17, 29, 41$; $p = 45122\,73113$

(b) $y = 17$, $p = 2^{127} - 1$

or the examples in Section E.IV.

L.XVII Scalar Formulas

I have chosen the matrix approach above for ease of presentation. In practice it is much more efficient to deal with the U_n and V_n directly. According to the fast exponentiation scheme (Section L.V)) we need formulas for passing from n to $2n$, and from n to $n+1$.

One scheme is to work with the pair U_n, V_n. Recall that $a+b=P$, $ab=Q$, $a-b=\sqrt{D}$.

Doubling is easy. We have already seen that

$$U_{2n} = U_n V_n.$$

And V_{2n} is almost as easy:

$$V_{2n} = a^{2n} + b^{2n} = (a^n + b^n)^2 - 2a^n b^n = V_n^2 - 2Q^n.$$

(of course, Q^n is not computed each time, but updated according to the binary exponentiation scheme).

As for passing from n to $n+1$, we have the following two identities, the first of which we have already derived.

$$\begin{aligned} U_{n+1} &= \frac{1}{2}(V_n U_1 + U_n V_1) = \frac{1}{2}(PU_n + V_n), \\ V_{n+1} &= \frac{1}{2}(V_n V_1 + DU_n U_1) = \frac{1}{2}(DU_n + PV_n). \end{aligned}$$

(Working modulo the odd number N, the $1/2$ is to be interpreted as $(N+1)/2$.)

One quick way to establish these formulas is to check that both members satisfy the second order recurrence $S_{n+1} - PS_{n+1} + QS_n = 0$ and have the same initial values S_0, S_1.

In matrix form, the identities read:

$$\begin{pmatrix} U_{n+1} \\ V_{n+1} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} P & 1 \\ D & P \end{pmatrix} \begin{pmatrix} U_n \\ V_n \end{pmatrix}.$$

Another scheme is to work with the pair U_{n+1}, U_n. We then need identities enabling the step to U_{2n+2}, U_{2n+1} (doubling and one-step) or to U_{2n+1}, U_{2n} (doubling).

For instance, starting with the matrix

$$M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix},$$

an easy induction proves that

$$M^n = \begin{pmatrix} U_{n+1} & -QU_n \\ U_n & -QU_{n-1} \end{pmatrix} = \begin{pmatrix} U_{n+1} & -QU_n \\ U_n & U_{n+1} - PU_n \end{pmatrix},$$

$$M^{n+1} = \begin{pmatrix} U_{n+2} & -QU_{n+1} \\ U_{n+1} & -QU_n \end{pmatrix} = \begin{pmatrix} PU_{n+1} - QU_n & -QU_{n+1} \\ U_{n+1} & -QU_n \end{pmatrix}.$$

The matrix powers in both members also satisfy the recurrence, so really all that is necessary is to check the two initial values, $n = 0, 1$.

Taking the first column of $M^n \cdot M^n$ then gives the column $(U_{2n+1}\ U_{2n})^t$, which is the first column of M^{2n}. And the first column of $M^{n+1} \cdot M^n$ similarly gives the column $(U_{2n+2}\ U_{2n+1})^t$. We arrive at the following doubling rules, where always the first two or the last two are to be taken together:

$$\begin{aligned} U_{2n+2} &= PU_{n+1}^2 - 2QU_{n+1}U_n, \\ U_{2n+1} &= U_{n+1}^2 - QU_n^2, \\ U_{2n} &= 2U_{n+1}U_n - PU_n^2. \end{aligned}$$

This approach is faster than the U, V method above. Any V_n can then easily be found from the U-recurrence, as $V_n = 2U_{n+1} - PU_n$.

L.XVII.1 Example. The following is a computer run of the example $N = 127$, $P = 3$, $Q = 1$, $n = 91$, $n + 1 = 92$, i.e., we are finding U_{92}, U_{91} from the recurrence $U_{j+2} - 3U_{j+2} + U_j \equiv 0 \pmod{N}$, with initial conditions $U_1 = 1$, $U_0 = 0$. The binary representation of 91 given below has the highest bit to the left. A zero bit means that the lower index of the pair is doubled. A non-zero bit means that the lower index is doubled, and then augmented by one unit. Or, equivalently, that the higher index is doubled.

Please check the first few values.

```
U1, U0= 1 , 0
binary repr. of 91 : [1, 0, 1, 1, 0, 1, 1]
next bit = 1 : j= 2 , 1 ; U= 3 , 1
next bit = 0 : j= 3 , 2 ; U= 8 , 3
next bit = 1 : j= 6 , 5 ; U= 17 , 55
next bit = 1 : j= 12 , 11 ; U= 13 , 58
next bit = 0 : j= 23 , 22 ; U= 107 , 52
next bit = 1 : j= 46 , 45 ; U= 105 , 109
next bit = 1 : j= 92 , 91 ; U= 25 , 33
```

□

An alternative route to these, and many other, identities is to note that $a - b = \sqrt{D}$, $U_n\sqrt{D} = a^n - b^n$, so that:

$$\begin{aligned} 2a^n &= (a^n + b^n) + (a^n - b^n) = V_n + U_n\sqrt{D}, \\ a^n &= \frac{1}{2}(V_n + U_n\sqrt{D}). \end{aligned}$$

For instance:

$$a^{n+1} = \frac{1}{2}(V_{n+1} + U_{n+1}\sqrt{D}) = a^n \cdot a = \frac{V_n + U_n\sqrt{D}}{2} \cdot \frac{V_1 + U_1\sqrt{D}}{2}.$$

As the U_n and V_n are rational integers, we may identify the rational and irrational parts, and we find again

$$\begin{aligned} U_{n+1} &= \frac{1}{2}(V_nU_1 + U_nV_1) = \frac{1}{2}(V_n + PU_n), \\ V_{n+1} &= \frac{1}{2}(V_nV_1 + U_nU_1) = \frac{1}{2}(PV_n + U_n). \end{aligned}$$

Details and more identities can also be found in the books of Riesel and Bressoud-Wagon. Crandall-Pomerance also give an account, but they use more Algebra.

L.XVII: Exercises

1. Check the derivation of the update formulas for the (U_{n+1}, U_n)-pairs above from the matrix products.

2. Derive as many identities as you possibly can from the relation

$$a^n = \frac{1}{2}(V_n + U_n\sqrt{D}).$$

3. (a) Denote the V-sequence belonging to the parameters P, Q by $V_n(P,Q)$. Prove the identity:

$$V_n(V_k(P,1),1) = V_{nk}(P,1)$$

(b) Can you generalize to the case where the first and third 1 are replaced by Q?

(c) Assuming that $((P^2-4)/N) = -1$, so that $((P^2-4)/p) = -1$ for at least one prime factor p of N, that k is a product of prime powers, and n a prime, do you see how the ideas of Pollard's $p-1$ factoring algorithm (L.VIII) translate to this situation?

(d) A more direct approach to the factoring problem would be to raise one root a of the equation $X^2 - PX + 1 = 0$ to high powers modulo N, again assuming $((P^2-4)/N) = -1$, Discuss the connection. You may derive inspiration from the ideas of Berlekamp's algorithm, E.IV.

4. Suggestions for computing Write a program that computes $U_q \pmod{p}$ for given parameters P, Q.

Show that $n = 323 = 17 \cdot 19$ is a *Lucas pseudoprime* for the parameters $P = 1$, $Q = -1$, i.e., n is composite, and $U_N \equiv 0 \pmod{n}$ for $N = n + (D/n)$.

5. Let q be a prime number. Determine $V_{q-(D/n)}$, where D is the discriminant $P^2 - 4Q$. How does this apply to the previous problem?

Compare these results to the case $N = 5777 = 53 \cdot 109$.

6. Suppose that $(D/n) = -1$, but also $(Q/n) = +1$. Further suppose that $U_{n+1} \equiv 0 \pmod{n}$, and $V_{n+1} \equiv 2Q \pmod{n}$. Let $m = (n+1)/2$. Show that the irrational part of a^m (the term involving $\sqrt{D}$) is congruent to zero modulo n if and only if $U_m \equiv 0$.

How can this observation be included in a Lucas primality test?

You may want to express both the assumptions and the conclusion in terms of the power sequence a^n. Cf. the paper by Jon Grantham, "A Probable Prime Test with High Confidence", *Journal of Number Theory*, **72**, 32-47 (1998), `http://www.rni.net/~pseudoprime/jgpapers.html`

7. Under the assumptions of the previous problem, show that $U_{m+1}^2 \equiv Q \pmod{n}$, even if n is composite.

Bibliography

Elementary

Of the books below Rosen is the most comprehensive, the most consistently elementary, and the richest in applications.

Nagell's book (translated from Swedish) is a very well-organized and well-written account of the elements from a time when the largest known prime number was $2^{127} - 1$.

Mollin gives the fundaments, but advances to the beginnings of Algebraic Number Theory. The book is slanted towards his interests in Pell-type Diophantine equations.

Stillwell's book gives a *very* gentle introduction to some concepts in Algebraic Number Theory.

Childs, L., *A Concrete Introduction to Higher Algebra*, Springer-Verlag, UTM, 2nd ed., 1995.

Jones, G.A., Jones, J. M., *Elementary Number Theory*, Springer SUMS, 1998.

Mollin, R. A., *Fundamental Number Theory with Applications*, CRC Press, 1998.

Nagell, T., *Introduction to Number Theory*, Almqvist & Wicksell, Wiley, 1951.

Niven, I., Zuckerman, H., Montgomery H., *An Introduction to the Theory of Numbers*, Wiley.

Rosen, K. H., *Elementary Number Theory and its applications*, Pearson International, 5th ed, 2005.

Schumer, P., *Introduction to Number Theory*, PWS Publishing Co.

Stillwell, J., *Elements of Number Theory*, Springer-Verlag UTM, 2003.

Computational

The book by Bressoud alone is out of print. It has a good introduction to elliptic curves, and gives most of the background material as it goes along.

The more comprehensive books by Riesel and Crandall-Pomerance complement one another. Riesel's book gives most of the theoretical background in numerous appendices, and lots of Pascal code. Crandall-Pomerance naturally covers more of recent developments. They give the algorithms in C-like pseudocode.

Bach-Shallit gives careful foundations of complexity theory, the theory of finite fields, and a survey of methods assuming the as yet unproved "Generalized Riemann Hypthesis"

Bressoud-Wagon is not purely computational, has lots of entertaining and original material.

Cohen's book contains lots of elementary material despite its title.

Bach, E., Shallit, J., *Algorithmic Number Theory, Vol. 1*, MIT Press, 1996.

Bressoud, D. M., *Factorization and Primality Testing*, Springer, 1988.

Bressoud, D.,Wagon, S., *A Course in Computational Number Theory*, Key College Publishing/Springer, 2000.

Cohen, H., *A Course in Computational Algebraic Number Theory*, Springer Graduate Texts in Mathematics, 138, 1995.

Crandall, R., Pomerance, C., *Prime Numbers - A Computational Perspective* Springer, 2005.

Riesel, H., *Prime Numbers and Computer Methods for Factorization*, Birkhäuser Progress in Mathematics, vol. 126, 1994.

Applied

Books on Cryptography usually include most of the background material from Number Theory. The two books listed below include discussions on several Discrete Logarithm algorithms, for instance. Trappe-Washington is the more comprehensive book, also includes some Coding Theory.

The third book covers an astonishing range of applications, but does not exactly prove everything.

Buchmann, J., *Introduction to Cryptography*, Springer UTM 2003.

Trappe, W., Washington, L., *Introduction to Cryptography with Coding Theory*, Prentice Hall, 2002.

Schroeder, M.R., *Number Theory in Science and Communication*, Springer, 1986.

Advanced

The two books listed deal with various advanced topics still mostly outside the realm of Algebraic Number Theory. There is very little overlap between the two. Ireland-Rosen presupposes some Abstract Algebra, Rose demands more in the way of Analysis.

Ireland, K., Rosen, M., *A Classical Introduction to Modern Number Theory*, Springer Graduate Texts 82, 1982.

Rose, H. E., *A Course in Number Theory*, Oxford Science Publications, 1994.

Historic

Scharlau, W., Opolka, H., *From Fermat to Minkowski, Lectures on the Theory of Numbers and its Historic Development*, Springer Undergraduate Texts, 1984.

Edwards, H. M., *Fermat's Last Theorem, A Genetic Introduction to Algebraic Number Theory*, Springer Graduate Texts in Mathematics 50, 1977.

Analytic

The first title below is an *extremely* well-written introduction, with full coverage of the elementary parts. The second title goes more deeply into the analytic parts.

Apostol, T., *Introduction to Analytic Number Theory*, Springer Undergraduate Texts, 1976.

Brüdern, J., *Einführung in die analytische Zahlentheorie*, Springer-Lehrbuch, 1995.

Elliptic

The books on elliptic curves that seem to require the least preparation are

Silverman, J., Tate, J., *Rational Points on Elliptic Curves*, Springer Undergraduate Texts, 1992.

Washington, L., *Elliptic Curves, Number Theory and Cryptography*, Chapman & Hall, 2003.

Algebraic

The textbooks below inevitably require some “Abstract” Algebra, but are among the most concrete and clearly written accounts of the foundations. The essay by R Dedekind has a long and very interesting introduction by J. Stillwell.

Dedekind, R., *Theory of Algebraic Integers*, Cambridge University Press, in the series “Cambridge Mathematical Library”, 1996 , translated and introduced by J. Stillwell.

Holzer, L., *Zahlentheorie*, Teubner, 1958.

Stewart, I.N., Tall, D.O., *Algebraic Number Theory*, Chapman and Hall, 1979.

Articles cited in the text

R. Brent, J. Pollard. “Factorization of the Eighth Fermat Number”. *Mathematics of Computation*, Vol. **36**, No. 154 (Apr., 1981), pp. 627-630.

J. Brillhart, M. Morrison. “A Method of Factoring and the Factorization of F_7”. *Mathematics of Computation*, Vol. **29**, No. 129 (Jan. 1975), 183-205,

I. Damgard, P. Landrock, C. Pomerance. “Average Case Error for the Strong Probable Prime Test”. *Mathematics of Computation,* Vol.**61** (1993), No. 203, pp. 177-194.

M. Gerstenhaber. “The 152nd proof of the law of quadratic reciprocity”. *Am. Math. Monthly*, **70** (1963), 397-398.

J. Grantham. “A Probable Prime Test with High Confidence”, *Journal of Number Theory*, **72**, (1998), 32-47.

Or: `http://www.rni.net/~pseudoprime/jgpapers.html`

K. Matthews. “The Diophantine Equation $x^2 - Dy^2 = N, D > 0$”, *Expositiones Mathematicae*, **18** (2000), 323-331.

For complements and corrections, refer to `http://www.numbertheory.org/papers.html#patz`

K.Matthews, “The Diophantine equation $ax^2+bxy+cy^2 = N, D = b^2-4ac > 0$”, *Journal de Thorie des Nombres de Bordeaux*, **14** (2002) 257-270.

Available at the url above.

K. Matthews, “Thue’s theorem and the diophantine equation $x^2 - Dy^2 = \pm N$”, *Mathematics of Computation*, **71** No. 239 (2001), 1281-1286.

A. Nitaj. “L’algorithme de Cornacchia”, *Expositiones Mathematicae* **13**, (1995), 358-365.

R. Silverman: “The Multiple Polynomial Quadratic Sieve”, *Mathematics of Computation*, **48**, No 177 (1987), 329-339.

Web

Dario Alpern's Site. Factoring and Discrete Logarithms with open source code in Java. For Spanish version, delete "ENGLISH.HTM".

`http://www.alpertron.com.ar/ENGLISH.HTM`

D. J. Bernstein's Notes. A set of notes on integer factorization. Bernstein's website has lots of interesting material, not all of it related to mathematics or computer science.

`http://cr.yp.to/2006-aws/notes-20060309.pdf`

J. Brillhart et al., *Factorizations of* $b^n \pm 1, b = 2$, 3, 5, 6, 7, 10, 11, 12, *Up to High Powers.* Apart from the tables (nice for checking your own results) this book has a very concise resumé of the theory and techniques involved, and some fascinating historical comments on the hardware.

`http://www.ams.org/online_bks/conm22/`

S. Contini. Has Contini's MSc thesis on the "self-initializing" Quadratic Sieve, downloadable in pdf:

`http://www.crypto-world.com/Contini.html`

W. Hart. Source code for **SIMPQS**. `http://www.friedspace.com/QS/`

Ikenaga's Notes. Conceived as companion notes to Rosen's text. The solution to $x^2 - 1141y^2 = 1$ was still wrong in December 2006.

`http://marauder.millersville.edu/~bikenaga/numth/numnote.html`

Lenstra, H.W., Jr., *Solving the Pell Equation.*

`http://www.ams.org/notices/200202/fea-lenstra.pdf`

The MacTutor History of Mathematics Archive.

`http://www-history.mcs.st-andrews.ac.uk/history/Indexes/Number_Theory.html`

The Mathematical Atlas.

`http://www.math.niu.edu/~rusin/known-math/index/11-XX.html`

Montgomery Survey. A very good survey of modern factorization methods. Downloadable in postscript.

http://citeseer.ist.psu.edu/montgomery94survey.html

Number Theory Web.

http://www.numbertheory.org/ntw/

J. Papadoupolos. Source code for **msieve**, http://www.boo.net/~jasonp/qs.html

PARI. Computer algebra system designed for fast computations in number theory.

http://pari.math.u-bordeaux.fr/

The Prime Pages.

http://primes.utm.edu/

Python Programming Language.

http://www.python.org/

Wikipedia. Often a surprisingly accurate *first* source (e.g., follow the external links).

http://www.wikipedia.org

Wolfram MathWorld.

http://mathworld.wolfram.com/

Tables

$x^2 - Dy^2 = \pm 1$

Lists $D : (x, y, \pm 1, \text{period})$

$2 : (1, 1, -1, 1)$	$3 : (2, 1, 1, 2)$	$5 : (2, 1, -1, 1)$
$6 : (5, 2, 1, 2)$	$7 : (8, 3, 1, 4)$	$8 : (3, 1, 1, 2)$
$10 : (3, 1, -1, 1)$	$11 : (10, 3, 1, 2)$	$12 : (7, 2, 1, 2)$
$13 : (18, 5, -1, 5)$	$14 : (15, 4, 1, 4)$	$15 : (4, 1, 1, 2)$
$17 : (4, 1, -1, 1)$	$18 : (17, 4, 1, 2)$	$19 : (170, 39, 1, 6)$
$20 : (9, 2, 1, 2)$	$21 : (55, 12, 1, 6)$	$22 : (197, 42, 1, 6)$
$23 : (24, 5, 1, 4)$	$24 : (5, 1, 1, 2)$	$26 : (5, 1, -1, 1)$
$27 : (26, 5, 1, 2)$	$28 : (127, 24, 1, 4)$	$29 : (70, 13, -1, 5)$
$30 : (11, 2, 1, 2)$	$31 : (1520, 273, 1, 8)$	$32 : (17, 3, 1, 4)$
$33 : (23, 4, 1, 4)$	$34 : (35, 6, 1, 4)$	$35 : (6, 1, 1, 2)$
$37 : (6, 1, -1, 1)$	$38 : (37, 6, 1, 2)$	$39 : (25, 4, 1, 2)$
$40 : (19, 3, 1, 2)$	$41 : (32, 5, -1, 3)$	$42 : (13, 2, 1, 2)$
$43 : (3482, 531, 1, 10)$	$44 : (199, 30, 1, 8)$	$45 : (161, 24, 1, 6)$
$46 : (24335, 3588, 1, 12)$	$47 : (48, 7, 1, 4)$	$48 : (7, 1, 1, 2)$
$50 : (7, 1, -1, 1)$	$51 : (50, 7, 1, 2)$	$52 : (649, 90, 1, 6)$
$53 : (182, 25, -1, 5)$	$54 : (485, 66, 1, 6)$	$55 : (89, 12, 1, 4)$
$56 : (15, 2, 1, 2)$	$57 : (151, 20, 1, 6$	$58 : (99, 13, -1, 7)$
$59 : (530, 69, 1, 6)$	$60 : (31, 4, 1, 4)$	$61 : (29718, 3805, -1, 11)$
$62 : (63, 8, 1, 4)$	$63 : (8, 1, 1, 2)$	$65 : (8, 1, -1, 1)$
$66 : (65, 8, 1, 2)$	$67 : (48842, 5967, 1, 10)$	$68 : (33, 4, 1, 2)$
$69 : (7775, 936, 1, 8)$	$70 : (251, 30, 1, 6)$	$71 : (3480, 413, 1, 8)$
$72 : (17, 2, 1, 2)$	$73 : (1068, 125, -1, 7)$	$74 : (43, 5, -1, 5)$
$75 : (26, 3, 1, 4)$	$76 : (57799, 6630, 1, 12)$	$77 : (351, 40, 1, 6)$
$78 : (53, 6, 1, 4)$	$79 : (80, 9, 1, 4)$	$80 : (9, 1, 1, 2)$
$82 : (9, 1, -1, 1)$	$83 : (82, 9, 1, 2)$	$84 : (55, 6, 1, 2)$
$85 : (378, 41, -1, 5)$	$86 : (10405, 1122, 1, 10)$	$87 : (28, 3, 1, 2)$
$88 : (197, 21, 1, 6)$	$89 : (500, 53, -1, 5)$	$90 : (19, 2, 1, 2)$
$91 : (1574, 165, 1, 8)$	$92 : (1151, 120, 1, 8)$	$93 : (12151, 1260, 1, 10)$
$94 : (2143295, 221064, 1, 16)$	$95 : (39, 4, 1, 4)$	$96 : (49, 5, 1, 4)$
$97 : (5604, 569, -1, 11)$	$98 : (99, 10, 1, 4)$	$99 : (10, 1, 1, 2)$

$101 : (10, 1, -1, 1)$	$102 : (101, 10, 1, 2)$	$103 : (227528, 22419, 1, 12)$
$104 : (51, 5, 1, 2)$	$105 : (41, 4, 1, 2)$	$106 : (4005, 389, -1, 9)$
$107 : (962, 93, 1, 6)$	$108 : (1351, 130, 1, 8)$	$109 : (8890182, 851525, -1, 15)$

A Table Of Primitive Roots

For every odd prime ≤ 5009 the least positive primitive root is listed. Format: $[prime, leastprimitiveroot]$. **1-1019**

[3, 2],	[5, 2],	[7, 3],	[11, 2],	[13, 2],
[17, 3],	[19, 2],	[23, 5],	[29, 2],	[31, 3],
[37, 2],	[41, 6],	[43, 3],	[47, 5],	[53, 2],
[59, 2],	[61, 2],	[67, 2],	[71, 7],	[73, 5],
[79, 3],	[83, 2],	[89, 3],	[97, 5],	[101, 2],
[103, 5],	[107, 2],	[109, 6],	[113, 3],	[127, 3],
[131, 2],	[137, 3],	[139, 2],	[149, 2],	[151, 6],
[157, 5],	[163, 2],	[167, 5],	[173, 2],	[179, 2],
[181, 2],	[191, 19],	[193, 5],	[197, 2],	[199, 3],
[211, 2],	[223, 3],	[227, 2],	[229, 6],	[233, 3],
[239, 7],	[241, 7],	[251, 6],	[257, 3],	[263, 5],
[269, 2],	[271, 6],	[277, 5],	[281, 3],	[283, 3],
[293, 2],	[307, 5],	[311, 17],	[313, 10],	[317, 2],
[331, 3],	[337, 10],	[347, 2],	[349, 2],	[353, 3],
[359, 7],	[367, 6],	[373, 2],	[379, 2],	[383, 5],
[389, 2],	[397, 5],	[401, 3],	[409, 21],	[419, 2],
[421, 2],	[431, 7],	[433, 5],	[439, 15],	[443, 2],
[449, 3],	[457, 13],	[461, 2],	[463, 3],	[467, 2],
[479, 13],	[487, 3],	[491, 2],	[499, 7],	[503, 5],
[509, 2],	[521, 3],	[523, 2],	[541, 2],	[547, 2],
[557, 2],	[563, 2],	[569, 3],	[571, 3],	[577, 5],
[587, 2],	[593, 3],	[599, 7],	[601, 7],	[607, 3],
[613, 2],	[617, 3],	[619, 2],	[631, 3],	[641, 3],
[643, 11],	[647, 5],	[653, 2],	[659, 2],	[661, 2],
[673, 5],	[677, 2],	[683, 5],	[691, 3],	[701, 2],
[709, 2],	[719, 11],	[727, 5],	[733, 6],	[739, 3],
[743, 5],	[751, 3],	[757, 2],	[761, 6],	[769, 11],
[773, 2],	[787, 2],	[797, 2],	[809, 3],	[811, 3],
[821, 2],	[823, 3],	[827, 2],	[829, 2],	[839, 11],
[853, 2],	[857, 3],	[859, 2],	[863, 5],	[877, 2],
[881, 3],	[883, 2],	[887, 5],	[907, 2],	[911, 17],
[919, 7],	[929, 3],	[937, 5],	[941, 2],	[947, 2],
[953, 3],	[967, 5],	[971, 6],	[977, 3],	[983, 5],
[991, 6],	[997, 7],	[1009, 11],	[1013, 3],	[1019, 2]

1021-2579

[1021, 10], [1031, 14], [1033, 5], [1039, 3], [1049, 3],
[1051, 7], [1061, 2], [1063, 3], [1069, 6], [1087, 3],
[1091, 2], [1093, 5], [1097, 3], [1103, 5], [1109, 2],
[1117, 2], [1123, 2], [1129, 11], [1151, 17], [1153, 5],
[1163, 5], [1171, 2], [1181, 7], [1187, 2], [1193, 3],
[1201, 11], [1213, 2], [1217, 3], [1223, 5], 1229, 2],
[1231, 3], [1237, 2], [1249, 7], [1259, 2], [1277, 2],
[1279, 3], [1283, 2], [1289, 6], [1291, 2], [1297, 10],
[1301, 2], 1303, 6], [1307, 2], [1319, 13], [1321, 13],
[1327, 3], [1361, 3], [1367, 5], [1373, 2], [1381, 2],
[1399, 13], [1409, 3], [1423, 3], [1427, 2], [1429, 6],
[1433, 3], [1439, 7], [1447, 3], [1451, 2], [1453, 2],
[1459, 3], [1471, 6], [1481, 3], [1483, 2], [1487, 5],
[1489, 14], [1493, 2], [1499, 2], [1511, 11], [1523, 2],
[1531, 2], [1543, 5], [1549, 2], [1553, 3], [1559, 19],
[1567, 3], [1571, 2], [1579, 3], [1583, 5], [1597, 11],
[1601, 3], [1607, 5], [1609, 7], [1613, 3], [1619, 2],
[1621, 2], [1627, 3], [1637, 2], [1657, 11], [1663, 3],
[1667, 2], [1669, 2], [1693, 2], [1697, 3], [1699, 3],
[1709, 3], [1721, 3], [1723, 3], [1733, 2], [1741, 2],
[1747, 2], [1753, 7], [1759, 6], [1777, 5], [1783, 10],
[1787, 2], [1789, 6], [1801, 11], [1811, 6], [1823, 5],
[1831, 3], [1847, 5], [1861, 2], [1867, 2], [1871, 14],
[1873, 10], [1877, 2], [1879, 6], [1889, 3], [1901, 2],
[1907, 2], [1913, 3], [1931, 2], [1933, 5], [1949, 2],
[1951, 3], [1973, 2], [1979, 2], [1987, 2], [1993, 5]
[1997, 2], [1999, 3], [2003, 5], [2011, 3], [2017, 5],
[2027, 2], [2029, 2], [2039, 7], [2053, 2], [2063, 5],
[2069, 2], [2081, 3], [2083, 2], [2087, 5], [2089, 7],
[2099, 2], [2111, 7], [2113, 5], [2129, 3], [2131, 2],
[2137, 10], [2141, 2], [2143, 3], [2153, 3], [2161, 23],
[2179, 7], [2203, 5], [2207, 5], [2213, 2], [2221, 2],
[2237, 2], [2239, 3], [2243, 2], [2251, 7], [2267, 2],
[2269, 2], [2273, 3], [2281, 7], [2287, 19], [2293, 2],
[2297, 5], [2309, 2], [2311, 3], [2333, 2], [2339, 2],
[2341, 7], [2347, 3], [2351, 13], [2357, 2], [2371, 2],
[2377, 5], [2381, 3], [2383, 5], [2389, 2], [2393, 3],
[2399, 11], [2411, 6], [2417, 3], [2423, 5], [2437, 2],
[2441, 6], [2447, 5], 2459, 2], [2467, 2], [2473, 5],
[2477, 2], [2503, 3], [2521, 17], [2531, 2], [2539, 2],
[2543, 5], [2549, 2], [2551, 6], [2557, 2], [2579, 2],

2591-4001

[2591, 7], [2593, 7], [2609, 3], [2617, 5], [2621, 2],
[2633, 3], [2647, 3], [2657, 3], [2659, 2], [2663, 5],
[2671, 7], [2677, 2], [2683, 2], [2687, 5], [2689, 19],
[2693, 2], [2699, 2], [2707, 2], [2711, 7], [2713, 5],
[2719, 3], [2729, 3], [2731, 3], [2741, 2], [2749, 6],
[2753, 3], [2767, 3], [2777, 3], [2789, 2], [2791, 6],
[2797, 2], [2801, 3], [2803, 2], [2819, 2], [2833, 5],
[2837, 2], [2843, 2], [2851, 2], [2857, 11], [2861, 2],
[2879, 7], [2887, 5], 2897, 3], [2903, 5], [2909, 2],
[2917, 5], [2927, 5], [2939, 2], [2953, 13], [2957, 2],
[2963, 2], [2969, 3], [2971, 10], [2999, 17], [3001, 14]
[3011, 2], [3019, 2], [3023, 5], [3037, 2], [3041, 3],
[3049, 11], [3061, 6], [3067, 2], [3079, 6], [3083, 2],
[3089, 3], [3109, 6], [3119, 7], [3121, 7], [3137, 3],
[3163, 3], [3167, 5], [3169, 7], [3181, 7], [3187, 2],
[3191, 11], [3203, 2], [3209, 3], [3217, 5], [3221, 10],
[3229, 6], [3251, 6], [3253, 2], [3257, 3], [3259, 3],
[3271, 3], [3299, 2], [3301, 6], [3307, 2], [3313, 10],
[3319, 6], [3323, 2], [3329, 3], [3331, 3], [3343, 5],
[3347, 2], [3359, 11], [3361, 22], [3371, 2], [3373, 5],
[3389, 3], [3391, 3], [3407, 5], [3413, 2], [3433, 5],
[3449, 3], [3457, 7], [3461, 2], [3463, 3], [3467, 2],
[3469, 2], [3491, 2], [3499, 2], [3511, 7], [3517, 2],
[3527, 5], [3529, 17], [3533, 2], [3539, 2], [3541, 7],
[3547, 2], [3557, 2], [3559, 3], [3571, 2], [3581, 2],
[3583, 3], [3593, 3], [3607, 5], [3613, 2], [3617, 3],
[3623, 5], [3631, 15], [3637, 2], [3643, 2], [3659, 2],
[3671, 13], 3673, 5], [3677, 2], [3691, 2], [3697, 5],
[3701, 2], [3709, 2], [3719, 7], [3727, 3], [3733, 2],
[3739, 7], [3761, 3], [3767, 5], [3769, 7], [3779, 2],
[3793, 5], [3797, 2], [3803, 2], [3821, 3], [3823, 3],
[3833, 3], [3847, 5], [3851, 2], [3853, 2], [3863, 5],
[3877, 2], [3881, 13], [3889, 11], [3907, 2], [3911, 13],
[3917, 2], [3919, 3], [3923, 2], [3929, 3], [3931, 2],
[3943, 3], [3947, 2], [3967, 6], [3989, 2], [4001, 3],

4003-5009

[4003, 2], [4007, 5], [4013, 2], [4019, 2], [4021, 2],
[4027, 3], [4049, 3], [4051, 10], [4057, 5], [4073, 3],
[4079, 11], [4091, 2], [4093, 2], [4099, 2], [4111, 12],
[4127, 5], [4129, 13], [4133, 2], [4139, 2], [4153, 5],
[4157, 2], [4159, 3], [4177, 5], [4201, 11], [4211, 6],
[4217, 3], [4219, 2], [4229, 2], [4231, 3], [4241, 3],
[4243, 2], [4253, 2], [4259, 2], [4261, 2], [4271, 7],
[4273, 5], [4283, 2], [4289, 3], [4297, 5], [4327, 3],
[4337, 3], [4339, 10], [4349, 2], [4357, 2], [4363, 2],
[4373, 2], [4391, 14], [4397, 2], [4409, 3], [4421, 3],
[4423, 3], [4441, 21], [4447, 3], [4451, 2], [4457, 3],
[4463, 5], [4481, 3], [4483, 2], [4493, 2], [4507, 2],
[4513, 7], [4517, 2], [4519, 3], [4523, 5], [4547, 2],
[4549, 6], [4561, 11], [4567, 3], [4583, 5], [4591, 11],
[4597, 5], [4603, 2], [4621, 2], [4637, 2], [4639, 3],
[4643, 5], [4649, 3], [4651, 3], [4657, 15], [4663, 3],
[4673, 3], [4679, 11], [4691, 2], [4703, 5], [4721, 6],
[4723, 2], [4729, 17], [4733, 5], [4751, 19], [4759, 3],
[4783, 6], [4787, 2], [4789, 2], [4793, 3], [4799, 7],
[4801, 7], [4813, 2], [4817, 3], [4831, 3], [4861, 11],
[4871, 11], [4877, 2], [4889, 3], [4903, 3], [4909, 6],
[4919, 13], [4931, 6], [4933, 2], [4937, 3], [4943, 7],
[4951, 6], [4957, 2], [4967, 5], [4969, 11], [4973, 2],
[4987, 2], [4993, 5], [4999, 3], [5003, 2], [5009, 3].

A Table of Discrete Logarithms

Primitive root =2, unless otherwise noted.

```
prime=3
[1, 2], [2, 1]

prime=5
[1, 4], [2, 1], [3, 3], [4, 2]

prime=7, primitive root = 3
[1, 6], [2, 2], [3, 1], [4, 4], [5, 5], [6, 3]
```

```
prime=11, primitive root  =2
[1, 10], [2, 1], [3, 8], [4, 2], [5, 4], [6, 9], [7, 7], [8, 3],
[9,6], [10, 5]


prime=13
[1, 12], [2, 1], [3, 4], [4, 2], [5, 9], [6, 5], [7, 11], [8, 3], [9,
8], [10, 10], [11, 7], [12, 6]

prime=17, primitive root =3
[1, 16], [2, 14], [3, 1], [4, 12], [5, 5], [6, 15], [7, 11], [8, 10],
[9, 2], [10, 3], [11, 7], [12, 13], [13, 4], [14, 9], [15, 6], [16,
8]

prime=19
[1, 18], [2, 1], [3, 13], [4, 2], [5, 16], [6, 14], [7, 6], [8, 3],
[9, 8], [10, 17], [11, 12], [12, 15], [13, 5], [14, 7], [15, 11],
 [16,4], [17, 10], [18, 9]

prime=23, primitive root = 5
[1, 22], [2, 2], [3, 16], [4, 4], [5, 1], [6, 18], [7, 19], [8, 6],
[9, 10], [10, 3], [11, 9], [12, 20], [13, 14], [14, 21], [15, 17],
[16, 8], [17, 7], [18, 12], [19, 15], [20, 5], [21, 13], [22, 11]

prime=29
[1, 28], [2, 1], [3, 5], [4, 2], [5, 22], [6, 6], [7, 12], [8, 3],
[9, 10], [10, 23], [11, 25], [12, 7], [13, 18], [14, 13], [15, 27],
[16, 4], [17, 21], [18, 11], [19, 9], [20, 24], [21, 17], [22, 26],
[23, 20], [24, 8], [25, 16], [26, 19], [27, 15], [28, 14]

prime=31, primitive root =3
[1, 30], [2, 24], [3, 1], [4, 18], [5, 20], [6, 25], [7, 28],
[8,12], [9, 2], [10, 14], [11, 23], [12, 19], [13, 11], [14, 22],
[15,21], [16, 6], [17, 7], [18, 26], [19, 4], [20, 8], [21, 29], [22, 17],
[23, 27], [24, 13], [25, 10], [26, 5], [27, 3], [28, 16], [29, 9],
[30, 15]

prime=37
[1, 36], [2, 1], [3, 26], [4, 2], [5, 23], [6, 27], [7, 32], [8, 3],
[9, 16], [10, 24], [11, 30], [12, 28], [13, 11], [14, 33], [15, 13],
[16, 4], [17, 7], [18, 17], [19, 35], [20, 25], [21, 22], [22, 31],
[23, 15], [24, 29], [25, 10], [26, 12], [27, 6], [28, 34], [29, 21],
[30, 14], [31, 9], [32, 5], [33, 20], [34, 8], [35, 19], [36, 18]

prime=41, primitive root =6
[1, 40], [2, 26], [3, 15], [4, 12], [5, 22], [6, 1], [7, 39],
[8,38], [9, 30], [10, 8], [11, 3], [12, 27], [13, 31], [14, 25],
[15,37], [16, 24], [17, 33], [18, 16], [19, 9], [20, 34], [21, 14],
[22,29], [23, 36], [24, 13], [25, 4], [26, 17], [27, 5], [28, 11],
[29,7], [30, 23], [31, 28], [32, 10], [33, 18], [34, 19], [35, 21],
[36,2], [37, 32], [38, 35], [39, 6], [40, 20]


prime=43, primitive root =3
[1, 42], [2, 27], [3, 1], [4, 12], [5, 25], [6, 28], [7, 35],
[8,39], [9, 2], [10, 10], [11, 30], [12, 13], [13, 32], [14, 20],
[15,26], [16, 24], [17, 38], [18, 29], [19, 19], [20, 37], [21, 36],
[22,15], [23, 16], [24, 40], [25, 8], [26, 17], [27, 3], [28, 5],
[29,41], [30, 11], [31, 34], [32, 9], [33, 31], [34, 23], [35, 18],
[36,14], [37, 7], [38, 4], [39, 33], [40, 22], [41, 6], [42, 21]


prime=47, primitive root =5
[1, 46], [2, 18], [3, 20], [4, 36], [5, 1], [6, 38], [7, 32], [8, 8],
[9, 40], [10, 19], [11, 7], [12, 10], [13, 11], [14, 4], [15, 21],
[16, 26], [17, 16], [18, 12], [19, 45], [20, 37], [21, 6], [22, 25],
[23, 5], [24, 28], [25, 2], [26, 29], [27, 14], [28, 22], [29, 35],
[30, 39], [31, 3], [32, 44], [33, 27], [34, 34], [35, 33], [36, 30],
[37, 42], [38, 17], [39, 31], [40, 9], [41, 15], [42, 24], [43, 13],
[44, 43], [45, 41], [46, 23]

prime=53
[1, 52], [2, 1], [3, 17], [4, 2], [5, 47], [6, 18], [7, 14], [8, 3],
[9, 34], [10, 48], [11, 6], [12, 19], [13, 24], [14, 15], [15, 12],
[16, 4], [17, 10], [18, 35], [19, 37], [20, 49], [21, 31], [22, 7],
[23, 39], [24, 20], [25, 42], [26, 25], [27, 51], [28, 16], [29, 46],
[30, 13], [31, 33], [32, 5], [33, 23], [34, 11], [35, 9], [36, 36],
[37, 30], [38, 38], [39, 41], [40, 50], [41, 45], [42, 32], [43, 22],
[44, 8], [45, 29], [46, 40], [47, 44], [48, 21], [49, 28], [50, 43],
[51, 27], [52, 26]
```

```
prime=59
[1, 58], [2, 1], [3, 50], [4, 2], [5, 6], [6, 51], [7, 18], [8, 3],
[9, 42], [10, 7], [11, 25], [12, 52], [13, 45], [14, 19], [15, 56],
[16, 4], [17, 40], [18, 43], [19, 38], [20, 8], [21, 10], [22, 26],
[23, 15], [24, 53], [25, 12], [26, 46], [27, 34], [28, 20], [29, 28],
[30, 57], [31, 49], [32, 5], [33, 17], [34, 41], [35, 24], [36, 44],
[37, 55], [38, 39], [39, 37], [40, 9], [41, 14], [42, 11], [43, 33],
[44, 27], [45, 48], [46, 16], [47, 23], [48, 54], [49, 36], [50, 13],
[51, 32], [52, 47], [53, 22], [54, 35], [55, 31], [56, 21], [57, 30],
[58, 29]

prime=61
[1, 60], [2, 1], [3, 6], [4, 2], [5, 22], [6, 7], [7, 49], [8, 3],
[9, 12], [10, 23], [11, 15], [12, 8], [13, 40], [14, 50], [15, 28],
[16, 4], [17, 47], [18, 13], [19, 26], [20, 24], [21, 55], [22, 16],
[23, 57], [24, 9], [25, 44], [26, 41], [27, 18], [28, 51], [29, 35],
[30, 29], [31, 59], [32, 5], [33, 21], [34, 48], [35, 11], [36, 14],
[37, 39], [38, 27], [39, 46], [40, 25], [41, 54], [42, 56], [43, 43],
[44, 17], [45, 34], [46, 58], [47, 20], [48, 10], [49, 38], [50, 45],
[51, 53], [52, 42], [53, 33], [54, 19], [55, 37], [56, 52], [57, 32],
[58, 36], [59, 31], [60, 30]

prime=67
[1, 66], [2, 1], [3, 39], [4, 2], [5, 15], [6, 40], [7, 23], [8, 3],
[9, 12], [10, 16], [11, 59], [12, 41], [13, 19], [14, 24], [15, 54],
[16, 4], [17, 64], [18, 13], [19, 10], [20, 17], [21, 62], [22, 60],
[23, 28], [24, 42], [25, 30], [26, 20], [27, 51], [28, 25], [29, 44],
[30, 55], [31, 47], [32, 5], [33, 32], [34, 65], [35, 38], [36, 14],
[37, 22], [38, 11], [39, 58], [40, 18], [41, 53], [42, 63], [43, 9],
[44, 61], [45, 27], [46, 29], [47, 50], [48, 43], [49, 46], [50, 31],
[51, 37], [52, 21], [53, 57], [54, 52], [55, 8], [56, 26], [57, 49],
[58, 45], [59, 36], [60, 56], [61, 7], [62, 48], [63, 35], [64, 6],
[65, 34], [66, 33]


prime=71, primitive root =7
[1, 70], [2, 6], [3, 26], [4, 12], [5, 28], [6, 32], [7, 1], [8, 18],
[9, 52], [10, 34], [11, 31], [12, 38], [13, 39], [14, 7], [15, 54],
[16, 24], [17, 49], [18, 58], [19, 16], [20, 40], [21, 27], [22, 37],
[23, 15], [24, 44], [25, 56], [26, 45], [27, 8], [28, 13], [29, 68],
[30, 60], [31, 11], [32, 30], [33, 57], [34, 55], [35, 29], [36, 64],
[37, 20], [38, 22], [39, 65], [40, 46], [41, 25], [42, 33], [43, 48],
[44, 43], [45, 10], [46, 21], [47, 9], [48, 50], [49, 2], [50, 62],
[51, 5], [52, 51], [53, 23], [54, 14], [55, 59], [56, 19], [57, 42],
[58, 4], [59, 3], [60, 66], [61, 69], [62, 17], [63, 53], [64, 36],
[65, 67], [66, 63], [67, 47], [68, 61], [69, 41], [70, 35]

prime=73, primitive root = 5
[1, 72], [2, 8], [3, 6], [4, 16], [5, 1], [6, 14], [7, 33], [8, 24],
[9, 12], [10, 9], [11, 55], [12, 22], [13, 59], [14, 41], [15, 7],
[16, 32], [17, 21], [18, 20], [19, 62], [20, 17], [21, 39], [22, 63],
[23, 46], [24, 30], [25, 2], [26, 67], [27, 18], [28, 49], [29, 35],
[30, 15], [31, 11], [32, 40], [33, 61], [34, 29], [35, 34], [36, 28],
[37, 64], [38, 70], [39, 65], [40, 25], [41, 4], [42, 47], [43, 51],
[44, 71], [45, 13], [46, 54], [47, 31], [48, 38], [49, 66], [50, 10],
[51, 27], [52, 3], [53, 53], [54, 26], [55, 56], [56, 57], [57, 68],
[58, 43], [59, 5], [60, 23], [61, 58], [62, 19], [63, 45], [64, 48],
[65, 60], [66, 69], [67, 50], [68, 37], [69, 52], [70, 42], [71, 44],
[72, 36]

prime=79, primitive root  =3
[1, 78], [2, 4], [3, 1], [4, 8], [5, 62], [6, 5], [7, 53], [8, 12],
[9, 2], [10, 66], [11, 68], [12, 9], [13, 34], [14, 57], [15, 63],
[16, 16], [17, 21], [18, 6], [19, 32], [20, 70], [21, 54], [22, 72],
[23, 26], [24, 13], [25, 46], [26, 38], [27, 3], [28, 61], [29, 11],
[30, 67], [31, 56], [32, 20], [33, 69], [34, 25], [35, 37], [36, 10],
[37, 19], [38, 36], [39, 35], [40, 74], [41, 75], [42, 58], [43, 49],
[44, 76], [45, 64], [46, 30], [47, 59], [48, 17], [49, 28], [50, 50],
[51, 22], [52, 42], [53, 77], [54, 7], [55, 52], [56, 65], [57, 33],
[58, 15], [59, 31], [60, 71], [61, 45], [62, 60], [63, 55], [64, 24],
[65, 18], [66, 73], [67, 48], [68, 29], [69, 27], [70, 41], [71, 51],
[72, 14], [73, 44], [74, 23], [75, 47], [76, 40], [77, 43], [78, 39]

prime=83
[1, 82], [2, 1], [3, 72], [4, 2], [5, 27], [6, 73], [7, 8], [8, 3],
[9, 62], [10, 28], [11, 24], [12, 74], [13, 77], [14, 9], [15, 17],
[16, 4], [17, 56], [18, 63], [19, 47], [20, 29], [21, 80], [22, 25],
[23, 60], [24, 75], [25, 54], [26, 78], [27, 52], [28, 10], [29, 12],
[30, 18], [31, 38], [32, 5], [33, 14], [34, 57], [35, 35], [36, 64],
[37, 20], [38, 48], [39, 67], [40, 30], [41, 40], [42, 81], [43, 71],
[44, 26], [45, 7], [46, 61], [47, 23], [48, 76], [49, 16], [50, 55],
[51, 46], [52, 79], [53, 59], [54, 53], [55, 51], [56, 11], [57, 37],
[58, 13], [59, 34], [60, 19], [61, 66], [62, 39], [63, 70], [64, 6],
[65, 22], [66, 15], [67, 45], [68, 58], [69, 50], [70, 36], [71, 33],
[72, 65], [73, 69], [74, 21], [75, 44], [76, 49], [77, 32], [78, 68],
[79, 43], [80, 31], [81, 42], [82, 41]

prime=89, primitive root = 3
[1, 88], [2, 16], [3, 1], [4, 32], [5, 70], [6, 17], [7, 81],
[8,48], [9, 2], [10, 86], [11, 84], [12, 33], [13, 23], [14, 9],
[15,71], [16, 64], [17, 6], [18, 18], [19, 35], [20, 14], [21, 82],
[22,12], [23, 57], [24, 49], [25, 52], [26, 39], [27, 3], [28, 25],
[29,59], [30, 87], [31, 31], [32, 80], [33, 85], [34, 22], [35, 63],
[36,34], [37, 11], [38, 51], [39, 24], [40, 30], [41, 21], [42, 10],
[43,29], [44, 28], [45, 72], [46, 73], [47, 54], [48, 65], [49, 74],
[50,68], [51, 7], [52, 55], [53, 78], [54, 19], [55, 66], [56, 41],
[57,36], [58, 75], [59, 43], [60, 15], [61, 69], [62, 47], [63, 83],
[64,8], [65, 5], [66, 13], [67, 56], [68, 38], [69, 58], [70, 79],
[71,62], [72, 50], [73, 20], [74, 27], [75, 53], [76, 67], [77, 77],
[78,40], [79, 42], [80, 46], [81, 4], [82, 37], [83, 61], [84, 26],
[85,76], [86, 45], [87, 60], [88, 44]

prime=97, primitive root =5
[1, 96], [2, 34], [3, 70], [4, 68], [5, 1], [6, 8], [7, 31], [8, 6],
[9, 44], [10, 35], [11, 86], [12, 42], [13, 25], [14, 65], [15, 71],
[16, 40], [17, 89], [18, 78], [19, 81], [20, 69], [21, 5], [22, 24],
[23, 77], [24, 76], [25, 2], [26, 59], [27, 18], [28, 3], [29, 13],
[30, 9], [31, 46], [32, 74], [33, 60], [34, 27], [35, 32], [36, 16],
[37, 91], [38, 19], [39, 95], [40, 7], [41, 85], [42, 39], [43, 4],
[44, 58], [45, 45], [46, 15], [47, 84], [48, 14], [49, 62], [50, 36],
[51, 63], [52, 93], [53, 10], [54, 52], [55, 87], [56, 37], [57, 55],
[58, 47], [59, 67], [60, 43], [61, 64], [62, 80], [63, 75], [64, 12],
[65, 26], [66, 94], [67, 57], [68, 61], [69, 51], [70, 66], [71, 11],
[72, 50], [73, 28], [74, 29], [75, 72], [76, 53], [77, 21], [78, 33],
[79, 30], [80, 41], [81, 88], [82, 23], [83, 17], [84, 73], [85, 90],
[86, 38], [87, 83], [88, 92], [89, 54], [90, 79], [91, 56], [92, 49],
[93, 20], [94, 22], [95, 82], [96, 48]
```

Index