(SKETCHES OF) SOLUTIONS, NUMBER THEORY, TATA 54, 2016-03-21

(1) It can be seen from the prime factorization of n, if n can be written as the sum of two squares of integers.

(a) $1098 = 2 \cdot 549 = 2 \cdot 3^2 \cdot 61$. Since no prime of the form $4k+3$ occurs with an odd power in 1098, the number 1098 can be written as the sum of two squares.

(b) $4067 = 7 \cdot 581 = 7^2 \cdot 83$, and here there is a prime number of the form $4k+3$, namely 83, which occurs to an odd power. Hence 4067 cannot be written as the sum of two squares.

ANSWER: (a): Yes (b): No.

(2) (a) $\alpha = [8; \overline{16}] = 8 + \dfrac{1}{\beta}$, where β, where $\beta = 16 + \dfrac{1}{\beta}$. We get the equation $\beta^2 - 16\beta - 1 = 0$ and its positive solution is $\beta = 8 + \sqrt{65}$.

(b) The positive solutions of the diophantine equation $x^2 - 65y^2 = 1$ are given by $(x_j, y_j) = (p_{2j-1}, q_{2j-1})$ for $j = 1, 2, 3, \ldots$. The least one is obtained from $\frac{p_1}{q_1} = [8; 16] = 8 + \frac{1}{16} = \frac{129}{16}$. Even if you do not remeber the exact formula, you can find the smallest solution, because every solution is given by a convergent of the continued fraction expansion of $\sqrt{65}$.

ANSWER: (b): The smallest solution is $(x, y) = (129, 16)$.

(3) $45 + 60i = 15(3 + 4i) = 3 \cdot 5 \cdot (3 + 4i)$. The prime number 3 is a gaussian prime, since it is congruent 3 (mod 4). Moreover $5 = (2 + i)(2 - i)$ and $2 + i$ and $2 - i$ are gaussian primes, since their norms are the prime number 5. Now the norm of $3 + 4i = 25$. Since $2 + i$ is a gaussian prime with norm 5, let us try if $(2 + i)|(3 + i)$: $\frac{3+4i}{2+i} = \frac{(3+4i)(2-i)}{5} = 2 + i$. Hence $3 + 4i = (2 + i)^2$.

ANSWER: $3(2 - i)(2 + i)^3$

(4) Let $f(x) = x^3 + 2x^2 + x + 1$. Solve first the congruence $f(x) \equiv 0 \pmod 5$. Computing we get $f(x) \equiv 1, 0, 1, -1, -1 \pmod 5$ for respectively $x \equiv 0, 1, -1, 2, -2 \pmod 5$. Hence $f(x) \equiv 0 \pmod 5$ has the solutions $x = 1 + 5t$ for $t \in \mathbb{Z}$. We determine next those t such that $f(1+5t) \equiv 0 \pmod{5^2}$. Now $f(1+5t) = (1 + 5t)^3 + 2(1 + 5t)^2 + 1 + 5t + 1 \equiv 5 + 3 \cdot 5t + 2 \cdot 2 \cdot 5t + 5t \equiv$

$5 + 8 \cdot 5t \equiv 5 + (2 \cdot 5 - 2)5t \equiv 5(1 - 2t) \pmod{5^2}$. Hence $f(1+5t) \equiv 0 \pmod{5^2} \iff 5(1-2t) \equiv 0 \pmod{5^2} \iff 1-2t \equiv 0 \pmod{5} \iff 2t \equiv 1 \pmod{5} \iff t \equiv 3 \pmod{5} \iff t = 3 + 5n, t \in \mathbb{Z}$.

Thus $x = 1 + 5t = 1 + 5(3 + 5n) = 16 + 25n$.

ANSWER: $x = 16 + 25n$, where $n \in \mathbb{Z}$.

(5) (a) Since $\operatorname{ord}_{11} 2 | 10$ and $2^5 = 32 \equiv -1 \pmod{11}$, $\operatorname{ord}_{11} 2 = 10$ and therefore 2 is a primitive root of 11.

(b)

x	1	2	3	4	5	6	7	8	9	10
$\operatorname{ind}_2 x$	10	1	8	2	4	9	7	3	6	5

(c)

$$7^x \equiv 3 \pmod{11}$$
$$\iff$$
$$\operatorname{ind}_2 7^x \equiv \operatorname{ind}_2 3 \pmod{10}$$
$$\iff$$
$$x \operatorname{ind}_2 7 \equiv \operatorname{ind}_2 3 \pmod{10}$$
$$\iff$$
$$7x \equiv 8 \pmod{10}$$
$$\iff$$
$$3 \cdot 7x \equiv 3 \cdot 8 \pmod{10}$$
$$\iff$$
$$x \equiv 4 \pmod{10}.$$

ANSWER: (a): For example 2 is a primitive root modulo 11. (b): See the table above. (c): $x = 4+10n$, for $n = 0, 1, 2, \ldots$

(6) $3x^2 + x + 6 \equiv 0 \pmod{59} \iff 20(3x^2 + x + 6) \equiv 0 \pmod{59} \iff x^2 + 20x + 120 \equiv 0 \pmod{59} \iff (x + 10)^2 \equiv -20 \pmod{59}$. Our congruence has therefore a solution if and only if $(\frac{-20}{59}) = 1$ Now $(\frac{-20}{59}) = (\frac{-1}{59})(\frac{2}{59})^2(\frac{5}{59})$. Here $(\frac{-1}{59}) = -1$, since $59 \equiv 3 \pmod{4}$ and by the law of quadratic reciprocity (observe that $5 \equiv 1 \pmod{4}$), $(\frac{5}{59}) = (\frac{59}{5}) = (\frac{4}{5}) = 1$. Hence $(\frac{-20}{59}) = (-1) \cdot 1 \cdot 1 = -1$ and the congruence therefore has no solutions.

ANSWER: No solutions