Föreläsningar i Talteori

Jan Snellman

MAI, Linköpings Univerrsitet

<2024-01-13 Sat>

Outline

Definition

Heltal, delbarhet

- $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$
- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$

Om inte annat sägs så $a, b, c, x, y, r, s \in \mathbb{Z}$, men $n, m \in \mathbb{Z}_+$.
$a|b$ om finns c så att $b = ac$.
$3|12$ ty $12 = 3 * 4$.

Elementary properties

- $a|0$,
- $0|a \iff a = 0$,
- $1|a$,
- $a|1 \iff a = \pm 1$,
- $a|b \wedge b|a \iff a = \pm b$
- $a|b \iff -a|b \iff a|-b$
- $a|b \wedge a|c \implies a|(b+c)$,
- $a|b \implies a|bc$.

Partial order

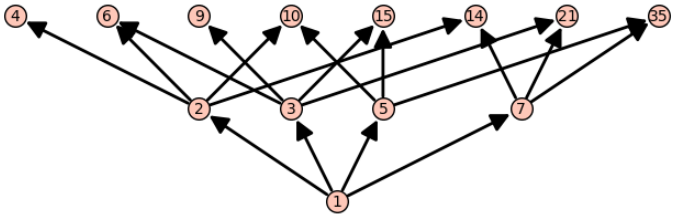

Figure: Heltalen under delbarhet

Begränsad till $\mathbb{Z}_+$ så är delbarhet en partialordning, med ett unikt minimalt element 1.

2 Del av Hasse diagram

Id est,

1. $a|a$,
2. $a|b \wedge b|c \implies a|c$,

Primtal

$n \in \mathbb{Z}_+$ är ett primtal om

- $n > 1$,
- $m|n \implies m \in \{1, n\}$

(positiva delare)

Primtalen börjar

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

Divisionsalgoritmen

Divisionsalgoritmen

$a, b \in \mathbb{Z}$, $b \neq 0$. Då finns unika k, r, *kvot* och *rest*, så att

- $a = kb + r$,
- $0 \leq r < |b|$.

$-27 = (-6) * 5 + 3$.

Bevis, existens

Antag för enkelhets skull att $a, b > 0$. Fixera b, induktion över a, basfall $a < b$. Då

$$a = 0 * b + a.$$

Om $a \geq b$ så

$$a = (a - b) + b$$

och ind. hyp. ger

Största gemensamma delare

Definition

Största gemensamma delare

$a, b \in \mathbb{Z}$. Den största gemensamma delaren till a och b, $c = \gcd(a, b)$, definieras genom

1. $c|a \wedge c|b$,
2. If $d|a \wedge d|b$, then $d \leq c$.

Om vi håller oss till $\mathbb{Z}_+$ kan det sista villkoret ersättas med

1. Om $d|a \wedge d|b$, så $d|c$.

Bezout

Bezouts sats

Låt $d = \gcd(a, b)$. Då finns (ej unika) $x, y \in \mathbb{Z}$ så att

Unique factorization into primes

Some Lemmas

$\gcd(an, bn) = |n| \gcd(a, b)$.
Bevis Antag $a, b, n \in \mathbb{Z}_+$. Induktion över $a + b$. Bas: $a = b = 1$, $\gcd(a, b) = 1$, $\gcd(an, bn) = n$, OK.
Ind. steg: $a + b > 2$, $a \geq b$.

$$a = kb + r, \quad 0 \leq r < b$$

Eftersom $a \geq b$, $k > 0$.
Då

$$\gcd(a, b) = \gcd(b, r)$$
$$\gcd(an, bn) = \gcd(bn, rn)$$

ty

$$an = kbn + rn, \quad 0 \leq rn < bn.$$

Men

Unique factorization into primes

Some Lemmas

$\gcd(an, bn) = |n| \gcd(a, b)$.
Bevis Antag $a, b, n \in \mathbb{Z}_+$. Induktion över $a + b$. Bas: $a = b = 1$, $\gcd(a, b) = 1$, $\gcd(an, bn) = n$, OK.
Ind. steg: $a + b > 2$, $a \geq b$.

$$a = kb + r, \quad 0 \leq r < b$$

Eftersom $a \geq b$, $k > 0$.
Då

$$\gcd(a, b) = \gcd(b, r)$$
$$\gcd(an, bn) = \gcd(bn, rn)$$

ty

$$an = kbn + rn, \quad 0 \leq rn < bn.$$

Men

Unique factorization into primes

Some Lemmas

$\gcd(an, bn) = |n| \gcd(a, b)$.
Bevis Antag $a, b, n \in \mathbb{Z}_+$. Induktion över $a + b$. Bas: $a = b = 1$, $\gcd(a, b) = 1$, $\gcd(an, bn) = n$, OK.
Ind. steg: $a + b > 2$, $a \geq b$.

$$a = kb + r, \quad 0 \leq r < b$$

Eftersom $a \geq b$, $k > 0$.
Då

$$\gcd(a, b) = \gcd(b, r)$$
$$\gcd(an, bn) = \gcd(bn, rn)$$

ty

$$an = kbn + rn, \quad 0 \leq rn < bn.$$

Mer om primtal

Eratosthenes såll

Eratosthenes såll

Algorithm 2

1. Givet N, hitta alla primtal $\leq N$
2. $X = [2, N]$, $i = 1$, $P = \emptyset$
3. $p_i = \min(X)$.
4. Ta bort multipler av p_i från X
5. $P = P \cup \{p_i\}$
6. Om $p_i \geq \sqrt{N}$, terminera, annars $i = i + 1$, goto 3.