Talteori, Föreläsning 1

Heltal, Delbarhet, Primtal

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan `http://courses.mai.liu.se/GU/TATA54/`

Summary

Delbarhet
- Definition
- Elementära egenskaper
- Partial order
- Primtal
- Divisionsalgoritmen

Största gemensamma delare
- Definition
- Bezout
- Euklides algoritm
- Euklides utvidgade algoritm

Unik primfaktorisering
- Några Lemman
- En viktig primtalsegenskap
- Euklides igen
- Aritmetikens fundamentalsats
- Exponentvektorer
- Minsta gemensamma multipel

Mer om primtal
- Eratostenes såll
- Primtal i aritmetisk progression

Summary

Delbarhet
- Definition
- Elementära egenskaper
- Partial order
- Primtal
- Divisionsalgoritmen

Största gemensamma delare
- Definition
- Bezout
- Euklides algoritm
- Euklides utvidgade algoritm

Unik primfaktorisering
- Några Lemman
- En viktig primtalsegenskap
- Euklides igen
- Aritmetikens fundamentalsats
- Exponentvektorer
- Minsta gemensamma multipel

Mer om primtal
- Eratostenes såll
- Primtal i aritmetisk progression

Summary

Delbarhet
- Definition
- Elementära egenskaper
- Partial order
- Primtal
- Divisionsalgoritmen

Största gemensamma delare
- Definition
- Bezout
- Euklides algoritm
- Euklides utvidgade algoritm

Unik primfaktorisering
- Några Lemman
- En viktig primtalsegenskap
- Euklides igen
- Aritmetikens fundamentalsats
- Exponentvektorer
- Minsta gemensamma multipel

Mer om primtal
- Eratostenes såll
- Primtal i aritmetisk progression

Summary

Delbarhet
- Definition
- Elementära egenskaper
- Partial order
- Primtal
- Divisionsalgoritmen

Största gemensamma delare
- Definition
- Bezout
- Euklides algoritm
- Euklides utvidgade algoritm

Unik primfaktorisering
- Några Lemman
- En viktig primtalsegenskap
- Euklides igen
- Aritmetikens fundamentalsats
- Exponentvektorer
- Minsta gemensamma multipel

Mer om primtal
- Eratostenes såll
- Primtal i aritmetisk progression

Definition

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

Om inte annat sägs så $a, b, c, x, y, r, s \in \mathbb{Z}$, men $n, m \in \mathbb{Z}_+$.

Definition

$a|b$ om finns c så att $b = ac$.

Exempel

$3|12$ ty $12 = 3 * 4$.

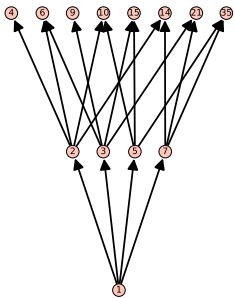
Lemma

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

Teorem

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

Del av Hasse diagram



Id est,

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

Definition

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

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

Primtalen börjar

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

Divisionsalgoritmen

Teorem

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

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

Exempel

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

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

$$a - b = k'b + r', \quad 0 \leq r' < b$$

så

$$a = b + k'b + r' = (1 + k')b + r'.$$

Ta $k = 1 + k'$, $r = r'$.

Bevis, unikhet

Om

$$a = k_1 b + r_1 = k_2 b + r_2, \quad 0 \leq r_1, r_2 < b$$

så

$$0 = a - a = (k_1 - k_2)b + r_1 - r_2$$

varför

$$(k_1 - k_2)b = r_2 - r_1$$

$|RHS| < b$, så $|LHS| < b$, alltså $k_1 = k_2$. Men då är $r_1 = r_2$.

Exempel

$a = 23, b = 5$.

$$\begin{aligned} 23 &= 5 + (23 - 5) = 5 + 18 \\ &= 5 + 5 + (18 - 5) = 2 * 5 + 13 \\ &= 2 * 5 + 5 + (13 - 5) = 3 * 5 + 8 \\ &= 3 * 5 + 5 + (8 - 5) = 4 * 5 + 3 \end{aligned}$$

$k = 4,\ r = 3$.

Definition

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

1. $c|a \wedge c|b$,
2. Om $d|a \wedge d|b$, så $d \leq c$.

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

2' Om $d|a \wedge d|b$, så $d|c$.

Teorem (Bezout)

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

$$ax + by = d.$$

Bevis.

$S = \{\, ax + by | x, y \in \mathbb{Z} \,\}$, $d = \min S \cap \mathbb{Z}_+$. Om $t \in S$, så $t = kd + r$, $0 \leq r < d$.
Alltså $r = t - kd \in S \cap \mathbb{N}$. Minimialitet av d, $r < d$ ger $r = 0$. Så $d|t$.
Men $a, b \in S$, så $d|a$, $d|b$, och om ℓ är en annan gemensamm delare så $a = \ell u$, $b = \ell v$, och

$$d = ax + by = \ell ux + \ell vy = \ell(ux + vy)$$

varför $\ell|d$. Det följer att d är den **största** gemensamma delaren. □

Étienne Bézout

Fundamentalt lemma

Lemma

Om $a = kb + r$ *så* $\text{sgd}(a, b) = \text{sgd}(b, r)$.

Bevis.

Om $c|a$, $c|b$ så $c|r$.
Om $c|b$, $c|r$ så $c|a$. □

Euklides utvidgade algoritm, exempel

$$
\begin{aligned}
27 &= 3 * 7 + 6 \\
7 &= 1 * 6 + 1 \\
6 &= 6 * 1 + 0
\end{aligned}
$$

$$
\begin{aligned}
6 &= 1 * 27 - 3 * 7 \\
1 &= 7 - 1 * 6 \\
&= 7 - (27 - 3 * 7) \\
&= (-1) * 27 + 4 * 7
\end{aligned}
$$

Algorithm

1. Initialisering: Sätt $x = 1, y = 0, r = 0, s = 1$.
2. Terminering?: Om $b = 0$, sätt $d = a$ och terminera.
3. Kvot och rest: Divisionsalg ger $a = qb + c$ med $0 \leq c < b$.
4. Shift: Sätt $(a, b, r, s, x, y) = (b, c, x - qr, y - qs, r, s)$ och gå till steg 2.
5. Slut: $\text{sgd}(a, b) = d = rx + sy$

Lemma

$\text{sgd}(an, bn) = |n| \, \text{sgd}(a, b)$.

Bevis

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

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

Eftersom $a \geq b$, $k > 0$.

Då

$$\operatorname{sgd}(a, b) = \operatorname{sgd}(b, r)$$
$$\operatorname{sgd}(an, bn) = \operatorname{sgd}(bn, rn)$$

ty

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

Men

$$b + r = b + (a - kb) = a - b(k - 1) \leq a < a + b,$$

så ind. hyp. ger

$$n \operatorname{sgd}(b, r) = \operatorname{sgd}(bn, rn).$$

Men $LHS = n \operatorname{sgd}(a, b)$, $RHS = \operatorname{sgd}(an, bn)$.

Lemma

Om $a|bc$ *och* $\text{sgd}(a,b) = 1$ *så* $a|c$.

Bevis.

$$1 = ax + by,$$

så

$$c = axc + byc.$$

Eftersom $a|RHS$, $a|c$. □

Lemma

p prime, $p|ab$. Då $p|a$ eller $p|b$.

Bevis.

Om $p \not| a$ så $\text{sgd}(p, a) = 1$. Tidigare lemmat ger nu att $p|b$. □

Teorem (Euklides)

Varje $n \in \mathbb{Z}_+$ kan skrivas som en produkt av primtal. Det finns oändligt många primtal.

Bevis.

1 är tomma produkten. Ind över n. Om n primtal, OK. Annars, $n = ab$, $a, b < n$. Så a, b produkt av primtal. Sätt ihop.
Antag $p_1, p_2, \ldots, p_s$ lista på alla kända primtal. Sätt

$$N = p_1 p_2 \cdots p_s + 1,$$

då är $N = kp_i + 1$ för alla kända primtal, så inget känt primtal delar N. Men N är en produkt av primtal, så antingen är det självt ett (okänt) primtal, eller så är det en produkt av okända primtal. □

Exempel

$$2 * 3 * 5 + 1 = 31$$

$$2 * 3 * 5 * 7 + 1 = 211$$

$$2 * 3 * 5 * 7 * 11 * 13 + 1 = 59 * 509$$

Exempel

$$2 * 3 * 5 + 1 = 31$$

$$2 * 3 * 5 * 7 + 1 = 211$$

$$2 * 3 * 5 * 7 * 11 * 13 + 1 = 59 * 509$$

Exempel

$$2 * 3 * 5 + 1 = 31$$
$$2 * 3 * 5 * 7 + 1 = 211$$
$$2 * 3 * 5 * 7 * 11 * 13 + 1 = 59 * 509$$

Teorem

Varje $n \in \mathbb{Z}_+$ kan unikt (upp till omordning av faktorer) skrivas

$$n = p_1 p_2 \cdots p_s, \qquad p_i \text{ primtal}.$$

Bevis.

Existens, Euklides. Unikhet: antag

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdot q_r.$$

Eftersom $p_1 | n$, har vi att $p_1 | q_1 q_2 \cdots q_r$, vilket mha tidigare lemma ger $p_1 | q_j$ något q_j, alltså $p_1 = q_j$. Kancellera och fortsätt. □

Exponentvektorer

- Numrera primtalen i växande ordning, $p_1 = 2, p_2 = 3, p_3 = 5$, et cetera.
- Då $n = \prod_{j=1}^{\infty} p_j^{a_j}$, med bara ändligt många a_j noll-skilda.
- Låt $v(n) = (a_1, a_2, a_3, \dots)$ vara denna heltalsföljd.
- Då $v(nm) = v(n) + v(m)$.
- Ordna komponentvis, då $n|m \iff v(n) \leq v(m)$.
- Vi har $v(\text{sgd}(n, m)) = \min(v(n), v(m))$.

Exempel

$$\begin{aligned}
\text{sgd}(100, 130) &= \text{sgd}(2^2 * 5^2, 2 * 5 * 13) \\
&= 2^{\min(2,1)} * 5^{\min(2,1)} * 13^{\min(0,1)} \\
&= 2^1 * 5^1 * 13^0 \\
&= 10
\end{aligned}$$

Definition

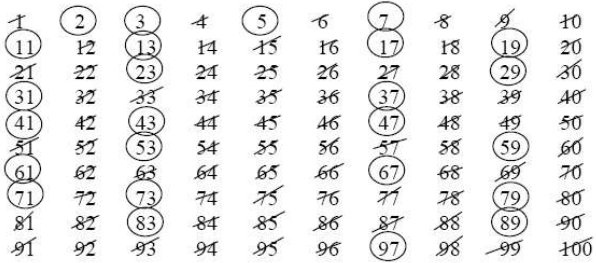
- $a, b \in \mathbb{Z}$
- $m = \text{mgm}(a, b)$ minsta gemensamma multipel om
  1. $m = ax = by$ (gemensam multipel)
  2. Om n gemensam multipel till a, b så $m|n$

Lemma

- $a, b \in \mathbb{Z}_+$, $c, d \in \mathbb{Z}$
- $\text{mgm}(\prod_j p_j^{a_j}, \prod_j p_j^{b_j}) = \prod_j p_j^{\max(a_j, b_j)}$
- $ab = \text{sgd}(a, b)\,\text{mgm}(a, b)$
- *Om* $a|c$ *och* $b|c$ *så* $\text{mgm}(a, b)|c$
- *Om* $c \equiv d \mod a$ *och* $c \equiv d \mod b$ *så* $c \equiv d \mod \text{mgm}(a, b)$

Algorithm

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.



- Varje heltal har rest 0,1,2, eller 3, modulo 4
- Bortsett från 2 så är alla primtal udda
- Så primtal > 2 är antingen på formen $4n + 1$ eller $4n + 3$
- $4n + 3 = 4(n + 1) - 1 = 4m - 1$.

Teorem

Det finns oändligt många primtal på formen $4m - 1$.

Bevis.

Låt $q_1, \ldots, q_r$ vara de kända primtalen, sätt

$$N = 4q_1q_2 \cdots q_r - 1$$

Då N udda, ej delbar med någon q_j. Primtalsfaktorisera N:

$$N = u_1u_2 \cdots u_s$$

Om alla $u_i = 4m_i + 1$ så

$$N = (4m_1 + 1)(4m_2 + 1) \cdots (4m_s + 1) = 4m + 1,$$

en motsägelse!. Så någon $u_j = 4m_j - 1$, $u_j | N$ så $u_j \notin \{q_1, \ldots, q_r\}$, alltså tidigare okänd. □

Teorem (Dirichlet)

$a, b \in \mathbb{Z}$, $\text{sgd}(a, b) = 1$. Då innehåller $a\mathbb{Z} + b$ oändligt många primtal.

Exempel

Uppenbarligen så har $6\mathbb{Z} + 3$ bara ett primtal, 3, så villkoret nödvändigt.

Dirichlet