Delbarhet:

a delar b, $a|b$, om det finns heltal c s.a.

$a \cdot c = b$.

Tex.

$3|9$

$7|42$

$2 \nmid 107$

Om $a \neq 0$ är "$a|b$" samma sak som "$\frac{b}{a}$ är ett heltal".

- Om $a|b$ och $b|c$ så $a|c$.
- Om $a|b$ och $a|c$ så $a|mb+nc$ för alla heltal m, n.

Ofta använd:

- Om $a > 1$ kan vi inte ha både $a|b$ och $a|(b+1)$

(Varför? Detta skulle ge $a|1\cdot(b+1)+(-1)\cdot b = 1$, vilket ej är möjligt ty $a > 1$)

Heltalsdivision "b/a":

Givet a, b där $a > 0$ finns unika heltal q, r s.a.

$b = aq + r, \quad 0 \leq r \leq a-1$.

q – heltalskvot

r – rest

T.ex: 25 delat på 3: $25 = 3 \cdot 7 + 4$
-17 delat på 2: $-17 = 2 \cdot (-9) + 1$
12 delat på 4: $12 = 4 \cdot 3 + 0$.

Primtal

Ett tal $p > 1$ är ett <u>primtal</u> om dess enda delare är ± 1 och $\pm p$.

- (Euklides ~300 f Kr) Det finns oändligt många primtal.

Euklides lemma: Låt p vara ett primtal och a, b heltal. Om $p \mid a \cdot b$ så: $p \mid a$ eller $p \mid b$.

Obs: Om p ej primtal behöver detta inte gälla.
T.ex $4 \mid 6 \cdot 10$, men $4 \nmid 6$ och $4 \nmid 10$.

Aritmetikens fundamentalsats: Varje tal $n > 1$ kan skrivas på ett unikt sätt som produkt av primtal:

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}.$$

Ett tal $n > 1$ som inte är ett primtal är ett <u>sammansatt</u> tal.

- Om n är sammansatt finns tal $1 < a, b < n$ s.a $a \cdot b = n$.
- Ett sammansatt tal n har en primtalsdelare $p \leq \sqrt{n}$.

Detta innebär att vi kan testa om ett tal $n > 1$ är primtal eller sammansatt genom att se om det är delbart med något primtal $\leq \sqrt{n}$.

Exempel: Är 113 och 119 primtal?

Då $10^2 = 100 \leq 113, 119 \leq n^2 = 121$ räcker det att testa primtal upp till 10.

$2 \nmid 113$.

$3 \nmid 113$

$5 \nmid 113$

$7 \mid 113$? $\quad 113 = \underbrace{70}_{7 \mid} + \underbrace{35}_{7 \mid} + \underbrace{8}_{7 \nmid}$ Nej

S: 113 är ett primtal

Dss

$2 \nmid 119$

$3 \nmid 119$ ty $1+1+9 = 11$ $3 \nmid 11$.

$5 \nmid 119$

$7 \mid 119$? $\quad 119 = \underbrace{70}_{7 \mid} + \underbrace{35}_{7 \mid} + \underbrace{14}_{7 \mid}$ Ja.

Sg 119 är ett sammansatt tal. $(119 = 7 \cdot 17)$

Övning 1.2:23: Bevisa eller motbevisa följande påstående: Det finns oändligt många primtal p s.a. både $p+2$ och $p+4$ är primtal!

Enligt divisionsalgoritmen finns q, r s.a

$p = 3q + r$ $\quad r = 0, 1,$ eller 2.

	p	p+2	p+4
r=0:	3q	3q+2	3q+4
r=1:	3q+1	3q+3	3q+5
r=2:	3q+2	3q+4	3q+6

Vi ser att ett av $p, p+2, p+4$ måste vara delbart med 3 så att de skulle vara primtal måste det talet vara 3.

3, 5, 7 ok

~~1~~, 3, 5 ej ok

~~-1~~, ~~1~~, 3 ej ok

Postiendet är en delsekt: Det endast sådana p är 3.

Den <u>största gemensamma delaren</u> (a,b), av heltal a,b är det största tal d så att $d|a$ och $d|b$.

Om $(a,b)=1$ är a och b <u>relativt prima</u>.

Största gemensamma delare kan beräknas med Euklides algoritm.

Tag t.ex $a=147$ $b=56$:

$147 = 2\cdot 56 + 35$
$56 = 1\cdot 35 + 21$
$35 = 1\cdot 21 + 14$
$21 = 1\cdot 14 + 7$
$14 = 2\cdot 7 + 0$

Vi får: $(147,56)=7$.

Bezouts identitet: Givet a,b finns m,n så att $ma+nb=(a,b)$.

Vi kan utöka Euklides algoritm så att vi hittar m,n som uppfyller detta

Fortsättning på exempel:

$$7 = 21 - 14 = 21 - (35 - 21) = 2 \cdot 21 - 35$$

$$= 2 \cdot (56 - 35) - 35 = 2 \cdot 56 - 3 \cdot 35$$

$$= 2 \cdot 56 - 3 \cdot (147 - 2 \cdot 56) = \underbrace{8}_{n} \cdot 56 \underbrace{- 3}_{m} \cdot 147.$$

Övning 1.3:9 3a) Låt a, b, c vara positiva heltal s.a $(a,b) = 1$. Visa att om $a \mid c$ och $b \mid c$ så: $ab \mid c$.

Enligt Bezouts identitet finns m, n s.a

$$ma + nb = 1.$$

Mult med c ger

$$mac + nbc = c.$$

Vi får att

$$\frac{c}{ab} = \frac{mac}{ab} + \frac{nbc}{ab} = m \cdot \frac{c}{b} + n \cdot \frac{c}{a} = \text{heltal},$$

så: $c \mid ab$, som önskat.

Alternativt kan vi använda AFS. Hur?

Övn 1.5:71. Låt a, b, n vara positiva heltal s.a $ab = n^2$. Om $(a,b) = 1$, visa att det finns heltal c och d s.a $a = c^2$ och $b = d^2$.

a och b har primtalsfaktoriseringar

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$
$$b = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}.$$

D: $(a,b) = 1$ har a och b inga gemensamma primtalsdelare, så $p_i \neq q_j$ för alla i, j.

Detta innebär att $n^2 = ab$ har primtalsfaktoriseringen

$$ab = n^2 = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_m^{b_m}.$$

D: n^2 är en kvadrat måste då alla $a_1, \ldots a_k, b_1, \ldots b_m$ vara jämna. (Om $n = r_1^{n_1} r_2^{n_2} \cdots$ så har n^2 primtalsfaktoriseringen $n^2 = r_1^{2n_1} r_2^{2n_2} \cdots$)

Det följer att

$$c = p_1^{a_1/2} p_2^{a_2/2} \cdots$$

och

$$d = q_1^{b_1/2} q_2^{b_2/2} \cdots$$

är heltal. Dessa uppfyller $c^2 = a$ och $d^2 = b$, som önskat.

Exempel: Finns heltal x, y som löser ...

a) $30x + 18y = 12$?

b) $30x + 18y = 2$?

Vi beräknar $(30, 18)$.

$30 = 1 \cdot 18 + 12$

$18 = 1 \cdot 12 + 6$

$12 = 2 \cdot 6 + 0$

$(30, 18) = 6$

Då $6 \mid 30$ och $6 \mid 18$ måste $6 \mid 30x + 18y$

för alla val av x, y, men $6 \nmid 2$ så

b) saknar lösning.

För a) använder vi Euklides algoritm

alg.

$6 = 18 - 12 = 18 - (30 - 18) = 2 \cdot 18 - 30$

$30 \cdot (-1) + 18 \cdot 2 = 6$

Multiplicerat med 2 ger

$30 \cdot (-2) + 18 \cdot 4 = 12$

$x = -2$, $y = 4$ är en lösning till a).

Låt $m > 0$. Vi säger att a är kongruent med b modulo m, $a \equiv b \bmod m$, om $m \mid a - b$.

Om $a \equiv b \bmod m$ och $c \equiv d \bmod m$ så:

- $a + c \equiv b + d \bmod m$
- $a \cdot c \equiv a \cdot c \bmod m$.
- $a^n \equiv b^n \bmod m$. för $n > 0$.

$a \equiv b \bmod m \iff a, b$ har samma rest vid div med m.

Kongruens mod m delar upp heltalen i m kongruensklasser

$[0] = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$

$[1] = \{\ldots -2m+1, -m+1, 1, m+1, 2m+1, \ldots\}$

$\vdots$

$[m-1] = \{\ldots -m-1, -1, m-1, 2m-1, 3m-1, \ldots\}$

$a \equiv b \bmod m \iff a, b$ ligger i samma kongruensklass mod m.

Exempel: Visa att $4^{75}+6^{75}$ är delbart med 5.

$5 \mid 4^{75}+6^{75}$

IH

$4^{75}+6^{75} \equiv 0 \mod 5$

$4 \equiv -1 \mod 5$

$6 \equiv 1 \mod 5$

Så:

$4^{75}+6^{75} \equiv (-1)^{75} + 1^{75} = -1+1 = 0 \mod 5.$

Exempel: Låt p vara ett primtal. Visa att om $a \cdot b \equiv 0 \mod p$ så är $a \equiv 0 \mod p$ eller $b \equiv 0 \mod p$.

$ab \equiv 0 \mod p \iff p \mid a \cdot b$

Vilket enligt Euklides lemma ger $p \mid a$ eller $p \mid b$, dvs $a \equiv 0 \mod p$ eller $b \equiv 0 \mod p$.

Vi söger att b är en modulär invers till a mod m om

$$a \cdot b \equiv 1 \mod m.$$

Invers existerar om $(a, m) = 1$.

Exempel: Finn en invers till 7 mod 19.

Vi använder Euklides stöhade alg

$$19 = 2 \cdot 7 + 5$$
$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$$1 = 5 - 2 \cdot 2$$
$$= 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7$$
$$= 3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 = 3 \cdot 19 - 8 \cdot 7$$
$$\equiv (-8) \cdot 7 \mod 19$$

-8 är en invers till 7 mod 19.

Kinesiska restsatsen:

$$\begin{cases} x \equiv b_1 \mod m_1 \\ x \equiv b_2 \mod m_2 \\ \vdots \\ x \equiv b_n \mod m_n \end{cases}$$

har en lösning x_0. Den allmänna lösningen ges av $x \equiv x_0 \mod m_1 m_2 \cdots m_n$.

Vi kan beräkna x_0 som följer:

$M = m_1 \cdot m_2 \cdots m_n$

$M_i = M/m_i$ för $1 \le i \le n$.

Finn x_i $1 \le i \le n$ s.a

$M_i x_i \equiv 1 \mod m_i$, t.ex med Euklides algoritm

Då är

$x_0 = M_1 x_1 b_1 + M_2 x_2 b_2 + \cdots + M_n x_n b_n$ en lösning.

Exempel:

$$\begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 2 \bmod 5 \end{cases}$$

$M = 15$

$M_1 = 5 \quad b_1 = 1$

$M_2 = 3 \quad b_2 = 2$

$M_1 x_1 = 5x_1 \equiv 1 \bmod 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 3 - 2$

$= 3 - (5 - 3) = 2 \cdot 3 - 5$

$\equiv (-1)5 \bmod 3$

Vi kan ta $x_1 = -1$

$M_2 x_2 = 3x_2 \equiv 1 \bmod 5$

Vi kan ta $x_2 = 2$.

$x_0 = 5 \cdot (-1) \cdot 1 + 3 \cdot 2 \cdot 2 = -5 + 12 = 7.$

Allmänna lösningen ges av $x \equiv 7 \bmod 15$.

Låt p vara ett primtal.

Wilsons sats: $(p-1)! \equiv -1 \mod p$

Fermats lilla sats:

- För alla a är $a^p \equiv a \mod p$
- Om $a \not\equiv 0 \mod p$ är $a^{p-1} \equiv 1 \mod p$.

Exempel: Är $54^{103} + 69^{67}$ delbart med 13?

$13 \mid 54^{103} + 69^{67}$ är samma som att

$54^{103} + 69^{67} \equiv 0 \mod 13$.

Vi delar exponenterna med $13-1$.

$103 = 8 \cdot 12 + 7$

$67 = 5 \cdot 12 + 7$

$$54^{103} + 69^{67} \equiv \left(54^{12}\right)^8 \cdot 54^7 + \left(69^{12}\right)^5 \cdot 69^7$$

$$\equiv 54^7 + 69^7 \mod 13$$

$54 = 4 \cdot 13 + 2 \equiv 2 \mod 13$

$69 = 5 \cdot 13 + 4 \equiv 4 \mod 13$

$54^7 + 69^7 \equiv 2^7 + 4^7 = 2^7 + 2^{2\cdot 7} \equiv 2^7 + 2^{12}\cdot 2^2 \equiv$

$= 128 + 4 = 134 \equiv 4 \mod 13.$

Nej, det är ej delbart med 13.

Övrig: Bestäm den minsta resten då

$33!^2$ divideras med 67.

67 är ett primtal, så enligt Wilsons sats är

$66! = 1\cdot 2\cdot 3\cdot \ldots \cdot 66 \equiv -1 \mod 67.$

$66! = 1\cdot 2\cdot 3\cdot \ldots \cdot 33\cdot (67-1)\cdot (67-2)\cdot \ldots \cdot (67-33)$

$\equiv 1\cdot 2\cdot 3\cdot \ldots \cdot 33\cdot -1\cdot -2\cdot \ldots \cdot -33 \mod 67$

$= (-1)^{33}\cdot 33!^2$

Vi ser att $-1\cdot 33!^2 \equiv -1 \mod 67$

$33!^2 \equiv 1 \mod 67,$

så $33!^2$ har rest 1 vid division med 67.

Definition: Eulers φ-funktion av $m > 0$ ges av

$\varphi(m)$ = antal $x = 0, 1, \ldots m-1$ s.a $(x, m) = 1$.

Sats: Om m har primtalsfaktorisering

$m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ ges $\varphi(m)$ av

$$\varphi(m) = (p_1 - 1) p_1^{a_1 - 1} (p_2 - 1) p_2^{a_2 - 1} \cdots (p_n - 1)^{a_n - 1}$$

I ord: φ-funktionen beräknas genom att primtalsfaktorisera m och ersätta en primtalsfaktor p av varje sort med $p - 1$.

Exempel:

- $\varphi(10) = \varphi(2 \cdot 5) = (2-1)(5-1) = 4$
- $\varphi(18) = \varphi(2 \cdot 3^2) = (2-1)(3-1)3 = 1 \cdot 2 \cdot 3 = 6$.
- $\varphi(25) = \varphi(5^2) = (5-1) \cdot 5 = 20$.
- $\varphi(p) = p - 1$ för p primtal.

Eulers sats: Om $m > 0$ och $(a, m) = 1$ är

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Exempel: Finn resten av 41^{200} vid division med 18.

$\varphi(18) = \varphi(2 \cdot 3^2) = (2-1)(3-1) \cdot 3 = 6$

$41 = 2 \cdot 18 + 5 \equiv 5 \mod 18$

$200 = 6 \cdot 33 + 2$

$41^{200} \equiv 6^{200} = 5^{6 \cdot 33 + 2} = \left(5^6\right)^{33} \cdot 5^2$

Eulers sats $\equiv 1^{33} \cdot 25 = 25 \equiv 7 \mod 18.$

41^{200} har rest 7 vid division med 18.