Talteori (afsnit 4.1 og 4.3)

Anvendelser: Kryptologi, hash-funktioner, pseudo-tilfældige tal m.m.

↑ DM534 uge 47 ↑ DM534 uge 39

I afsnit 4.1 har I selv læst Def. 1, Sætning 1, Korollar 1 og Sætning 2:

Def 1: Hvis $a,b \in \mathbb{Z}$ og $a \neq 0$, gælder

$$a \mid b \iff \frac{b}{a} \in \mathbb{Z} \iff \exists c \in \mathbb{Z} : b = c \cdot a$$

a går op i b

a er en faktor i b

b er et multiplum af a

Sætning 1 har tre punkter. De to første opsummeres i:

Korollar 1: Lad $a,b,c \in \mathbb{Z}$ og $a \neq 0$. Da gælder

$$a \mid b \wedge a \mid c$$
$$\Downarrow$$
$$\forall k,l \in \mathbb{Z} : a \mid (kb + lc)$$

Sætning 2: (Divisions-algoritmen)

Lad $a \in \mathbb{Z}$ og $d \in \mathbb{Z}^+$. Da gælder

$$\exists! q, r \in \mathbb{Z} : a = dq + r \wedge 0 \leq r < d$$

Def. 2: q = kvotient, r = rest, a = dividend, d = divisor

Eks:

$a = 16 \wedge d = 3$

$\Downarrow$

$q = 5 \wedge r = 1$

$q = a \text{ div } d$

$r = a \text{ mod } d$ ("a modulo d")

↑ skrives som % i mange prg.sprog

Def. 3:

Lad $a, b \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$. Da gælder

$$a \equiv b \pmod{m}$$
$$\Updownarrow$$
$$m \mid (a-b)$$

$a \equiv b \pmod{m}$: a og b er kongruente modulo m

$a \not\equiv b \pmod{m}$: a og b er ikke kongruente modulo m

Eks:

$5 \equiv 15 \pmod{5}$? $\quad 15-5 = 10 = 2 \cdot 5$ ✓

$7 \equiv 16 \pmod{5}$? $\quad 16-7 = 9 = 5+4$ ⅓

$7 \equiv 16 \pmod{3}$? $\quad 16-7 = 3 \cdot 3$ ✓

Kongruens kan defineres på mange måder:

Def. 3 ⇕ $\quad a \equiv b \pmod{m}$

$\quad m \mid (a-b)$ (*)

Sætn. 3 ⇕ $\quad a \bmod m = b \bmod m$

Sætn. 4 ⇕ $\quad \exists k \in \mathbb{Z} : a = b + km$ (**)

Bevis for Sætning 3: Opgave 13

Bevis for Sætning 4:

(**) er en anden skrivemåde af (*):

$m \mid (a-b)$

Def. 1 ⇕ $\quad a-b = km, \quad k \in \mathbb{Z}$

⇕ $\quad a = b + km, \quad k \in \mathbb{Z}$

Sætning 5:

Lad $m \in \mathbb{Z}^+$. Da gælder

$$\begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases}$$

$$\Downarrow$$

$$\begin{cases} a+c \equiv b+d \pmod m \\ ac \equiv bd \pmod m \end{cases}$$

D.v.s. man må addere og gange med det "samme" tal på begge sider.

Eks:

$$5 \equiv 8 \pmod 3$$
$$4 \equiv 10 \pmod 3$$

$$\Downarrow$$

$$\begin{cases} 9 \equiv 18 \pmod 3 & \text{(addr på begge sider)} \\ 20 \equiv 80 \pmod 3 & \text{(mult. ——— " ———)} \end{cases}$$

Bevis:

Som bogen:

$$a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m}$$

Sætn. 4 $\Updownarrow$

$$a = b + km \quad \wedge \quad c = d + \ell m, \quad k, \ell \in \mathbb{Z}$$

$\Downarrow$

$$a + c = (b + km) + (d + \ell m) = (b+d) + (k+\ell)m, \quad k+\ell \in \mathbb{Z}$$

Sætn. 4 $\Updownarrow$

$$a + c \equiv b + d \pmod{m}$$

Eller:

$$a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m}$$

Def. 3 $\Updownarrow$

$$m \mid (a-b) \quad \wedge \quad m \mid (c-d)$$

Sætn. 1(c)(i) $\Downarrow$

$$m \mid (a - b + c - d)$$

$\Updownarrow$

$$m \mid ((a+c) - (b+d))$$

Def. 3 $\Updownarrow$

$$a + c \equiv b + d \pmod{m}$$

$$a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m}$$

Sætn. 4 $\Updownarrow$

$$a = b + km \quad \wedge \quad c = d + \ell m, \quad k, \ell \in \mathbb{Z}$$

$\Downarrow$

$$a \cdot c = (b + km)(d + \ell m), \quad k, \ell \in \mathbb{Z}$$

$\Downarrow$

$$a \cdot c = bd + b\ell m + kmd + k\ell m^2$$

$$= bd + \underbrace{(b\ell + kd + k\ell m)}_{\in \mathbb{Z}} m$$

Sætn. 4 $\Updownarrow$

$$ac \equiv bd \pmod{m}$$

Eller:

$$a \equiv b \pmod{m} \quad \wedge \quad c \equiv d \pmod{m}$$

$\Updownarrow$

$$m \mid (a-b) \quad \wedge \quad m \mid (c-d)$$

$\Downarrow$

$$m \mid (a-b)c \quad \wedge \quad m \mid (c-d)b$$

$\Downarrow$

$$m \mid ((a-b)c + (c-d)b)$$

$\Updownarrow$

$$m \mid (ac - bd)$$

$\Updownarrow$

$$ac \equiv bd \pmod{m}$$

Må man trække det "samme" tal fra på begge sider?

Ja: $c \equiv d \pmod m \iff -c \equiv -d \pmod m$

Må man dividere med det samme tal på begge sider, hvis det går op?

Nej, ikke generelt:

$20 \equiv 30 \pmod 5$, men

$4 \not\equiv 6 \pmod 5$

Korollar 2:

Lad $a, b \in \mathbb{Z}$ og $m \in \mathbb{Z}^+$. Da gælder

- $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$
- $ab \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$

Praktisk, da det kan spare en for at regne med store tal.

Bevis:

$a \equiv (a \bmod m) \pmod m$

$b \equiv (b \bmod m) \pmod m$

ifølge Sætning 3

P.V.S.

$a+b \equiv (a \bmod m) + (b \bmod m) \pmod m$, iflg. Sætn. 5

Sætn. 3 ⇕ $(a+b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m$

Og $a \cdot b \equiv (a \bmod m)(b \bmod m) \pmod m$, iflg. Sætn. 5

Sætn. 3 ⇕ $ab \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m$

□

$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$

Primtal (afsnit 4.3)

Def. 1:

Lad $p \in \mathbb{Z}^+ - \{1\}$.

Hvis 1 og p er de eneste tal, der går op i p,
er p et **primtal**.

Ellers er p **sammensat**.

D.v.s.:

Primtal: 2, 3, 5, 7, 11, ...

Sammensat: 4, 6, 8, 9, 10, ...

Mellem 2 og 100 er der 25 primtal.
Men de bliver længere og længere imellem dem. (Hvorfor?)

Eratosthenes si:

Multipla af 2 og multipla af 3:
4 6 8 9 10 12 14 15 16

Alle tal mellem 2 og 15, som ikke er nævnt ovenfor, er primtal.

Hvis et tal n er sammensat, har det nemlig en divisor $\leq \sqrt{n}$. (Sætning 2)

De bliver længere og længere imellem primtallene...
Holder de helt op? D.v.s. er der et største primtal?
Nej:

Sætning 3: Der er uendeligt mange primtal

Bevis-skitse:

Antag til modstrid, at der kun er n primtal $p_1, p_2, \dots, p_n$.
Lad $Q = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$.
Enten er Q et primtal ↯
eller også er der et primtal $q \mid Q$.
Bemærk $q \neq p_1, p_2, \dots, p_n$ (fordi p_i går op i $p_1 p_2 \cdots p_n$ og $p_1 p_2 \cdots p_n + p_i$, men ingen tal derimellem) ↯

Hvis n er meget stor, er der ca. $\frac{n}{\ln(n)}$ primtal mellem 2 og n. (Sætning 4)

Sætning 1: (Aritmetikkens Fundamentalsætning):
Ethvert heltal $n \geq 2$
kan skrives som et produkt af primtal,
og det kan kun gøres på én måde (hvis man sorterer faktorerne efter størrelse).

Eks:

$2 = 2$ $\quad 3 = 3$ $\quad 4 = 2 \cdot 2$

$10 = 2 \cdot 5$ $\quad 12 = 2 \cdot 2 \cdot 3$ $\quad 45 = 3 \cdot 3 \cdot 5$

$100 = 2 \cdot 2 \cdot 5 \cdot 5$

Def. 2:

Lad $a, b \in \mathbb{Z}$, $a \neq 0 \vee b \neq 0$.

$\gcd(a,b) = \max\{d \mid d|a \wedge d|b\}$ kaldes største fælles divisor for a og b

Eks:

$\gcd(18,24) = 6$

$18 = \boxed{2 \cdot 3} \cdot 3$

$24 = 2 \cdot 2 \cdot \boxed{2 \cdot 3}$

$\gcd(12,24) = 12$

$12 = \boxed{2 \cdot 2 \cdot 3}$

$24 = 2 \cdot \boxed{2 \cdot 2 \cdot 3}$

$\gcd(12,25) = 1 \Rightarrow$ 12 og 25 er indbyrdes primiske (Def. 3)

$12 = 2 \cdot 2 \cdot 3$

$25 = 5 \cdot 5$

Def. 5:

Lad $a, b \in \mathbb{Z}^+$.

$\text{lcm}(a,b) = \min\{m \mid a|m \wedge b|m\}$ kaldes mindste fælles multiplum af a og b

Eks:

$\text{lcm}(18, 24) = 72 = \boxed{2 \cdot 3} \cdot (3) \cdot (2 \cdot 2)$

$18 = \boxed{2 \cdot 3} \cdot 3$

$24 = 2 \cdot 2 \cdot \boxed{2 \cdot 3}$

$\text{lcm}(12, 24) = 24$

$12 = \boxed{2 \cdot 2 \cdot 3}$

$24 = 2 \cdot \boxed{2 \cdot 2 \cdot 3}$

$\text{lcm}(12, 25) = 300 = 12 \cdot 25$

$12 = 2 \cdot 2 \cdot 3$

$25 = 5 \cdot 5$

Sætning 5:

Lad $a, b \in \mathbb{Z}^+$. Da gælder

$a \cdot b = \gcd(a, b) \cdot \text{lcm}(a, b)$