Kongruenser: (1) $a \equiv b \pmod{n}$ hvis n deler $(a-b)$

(2) Eksempel: $7 \equiv -13 \pmod 4$ siden $4 \mid (7-(-13))$, og $8 \not\equiv 5 \pmod 2$ siden $2 \nmid (8-5)$

(3) $a \equiv b \pmod n \iff a$ og b gir samme rest når vi deler på n

(4) Egenskaper:

(a) $a \equiv a \pmod n$

(b) $a \equiv b \pmod n \iff b \equiv a \pmod n$

(c) $a \equiv b \pmod n,\ b \equiv c \pmod n \implies a \equiv c \pmod n$

(d) $a \equiv b \pmod n,\ c \equiv d \pmod n \implies \begin{cases} a+c \equiv b+d \pmod n \\ ac \equiv bd \pmod n \end{cases}$

(e) $a \equiv b \pmod n \implies \begin{cases} a+c \equiv b+c \pmod n \\ ac \equiv bc \pmod n \end{cases}$

(f) $a \equiv b \pmod n \implies a^t \equiv b^t \pmod n \quad \forall\ t \geq 1$

Eksempler: (1) $42 \equiv 3 \pmod{13}$ siden $13 \mid (42-3)$, og $4 \equiv 30 \pmod{13}$ siden $13 \mid (4-30)$
Fra (d) får vi da
$42+4 \equiv 3+30 \pmod{13}$ dvs $46 \equiv 33 \pmod{13}$
$42 \cdot 4 \equiv 3 \cdot 30 \pmod{13}$ dvs $168 \equiv 90 \pmod{13}$

(2) $15 \equiv 3 \pmod 6$, så fra (f) får vi at $15^t \equiv 3^t \pmod 6\ \forall\ t \geq 1$. For eksempel er $15^{2018} \equiv 3^{2018} \pmod 6$.

(3) Implikasjonen $a \equiv b \pmod n \implies a^t \equiv b^t \pmod n$ kan generelt ikke reverseres: $5^2 \equiv 3^2 \pmod 8$ siden $8 \mid (25-9)$, men $5 \not\equiv 3 \pmod 8$ siden $8 \nmid (5-3)$.

(4) $28 \equiv 3 \pmod 5$, så fra (e) får vi $28c \equiv 3c \pmod 5\ \forall\ c \in \mathbb{Z}$. For eksempel er $28 \cdot 4 \equiv 3 \cdot 4 \pmod 5$, dvs $112 \equiv 12 \pmod 5$.

(5) Implikasjonen $a \equiv b \pmod n \implies ac \equiv bc \pmod n$ kan generelt ikke reverseres: $5 \cdot 2 \equiv 2 \cdot 2 \pmod 6$ fordi $6 \mid (10-4)$, men $5 \not\equiv 2 \pmod 6$. Vi kan altså ikke kansellere en felles faktor i en kongruens sånn uten videre.

Teorem 4.3 $ac \equiv bc \pmod n \implies a \equiv b \pmod{n/\gcd(c,n)}$

Korollar 1 Hvis $ac \equiv bc \pmod n$ og $\gcd(c,n)=1$, så er $a \equiv b \pmod n$.

Bevis: Følger fra Teorem 4.3, men siden vi ikke beviste det så beviser vi dette korollaret uten hjelp av teoremet.
Kongruensen $ac \equiv bc \pmod n$ betyr at $n \mid (ac-bc)$, dvs $n \mid c(a-b)$. Siden $\gcd(n,c)=1$ gir Euklids lemma at da må $n \mid (a-b)$, dvs $a \equiv b \pmod n$. □

Eksempler: (1) $8 \cdot 7 \equiv 2 \cdot 7 \pmod 6$ fordi $6 \mid (56-14)$. Siden $\gcd(7,6)=1$ får vi $8 \equiv 2 \pmod 6$

(2) Hvis $ac \equiv bc \pmod p$ og p er prim med $p \nmid c$, er $a \equiv b \pmod p$.

4.3 Tallsystemer

Titallsystemet: Vi bruker titallsystemet:

$$8205 = 8\cdot 10^3 + 2\cdot 10^2 + 0\cdot 10 + 5$$

Et tall $a_t a_{t-1} \cdots a_1 a_0$, hvor a_i er et siffer med $0 \le a_i \le 9$, representerer tallet

$$a_t \cdot 10^t + a_{t-1} 10^{t-1} + \cdots + a_1 \cdot 10 + a_0$$

b-tallsystemet: Gitt et positivt tall $b > 1$. I b-tallsystemet er tallene på form

$$(a_t a_{t-1} \cdots a_1 a_0)_b \quad 0 \le a_i \le b-1$$

og er notasjon for

$$a_t \cdot b^t + a_{t-1} b^{t-1} + \cdots + a_1 \cdot b^1 + a_0 \cdot b^0$$

(For titallsystemet skriver vi 8205 istedet for $(8205)_{10}$). Hvert $n \ge 1$ kan uttrykkes på en unik slik måte (se bok).

Eksempler: (1) Når $b=2$ har vi det binære tallsystemet:

$$(11001)_2 = 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 = 25$$

Alle tall $n \ge 1$ kan uttrykkes unikt som

$$n = a_t \cdot 2^t + a_{t-1} \cdot 2^{t-1} + \cdots + a_1 \cdot 2^1 + a_0 \cdot 2^0$$
$$= (a_t a_{t-1} \cdots a_1 a_0)_2$$

hvor $a_i \in \{0,1\}$. For å uttrykke et tall binært, trekk fra så høye potenser av 2 som mulig:

$$106 = 64 + 42$$
$$= 64 + 32 + 10$$
$$= 64 + 32 + 8 + 2$$
$$= 2^6 + 2^5 + 2^3 + 2$$
$$= 1\cdot 2^6 + 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 1\cdot 2^1 + 0\cdot 2^0$$
$$= (1101010)_2$$

(2) Tallet 17 i 3-tallsystemet:

$$17 = 1\cdot 3^2 + 2\cdot 3^1 + 2\cdot 3^0 = (122)_3$$

(3)

$$(20311)_4 = 2\cdot 4^4 + 0\cdot 4^3 + 3\cdot 4^2 + 1\cdot 4^1 + 1\cdot 4^0 = 565$$

Teorem 4.4 La $f(x) = c_t x^t + \cdots + c_1 x + c_0$ være et polynom med $c_i \in \mathbb{Z}$. Da gjelder:

$$a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n}$$

Bevis: Hvis $a \equiv b \pmod{n}$ er $a^i \equiv b^i \pmod{n}$ $\forall\, i \geq 0$, og da $c_i a^i \equiv c_i b^i \pmod{n}$ $\forall\, 0 \leq i \leq t$, som gir

$$\sum_{i=0}^{t} c_i a^i \equiv \sum_{i=0}^{t} c_i b^i \pmod{n} \qquad \square$$

Teorem 4.5 (Divisjon med 3 og 9)

La $n = (a_t a_{t-1} \cdots a_1 a_0)_{10}$ være et tall i 10-tallsystemet. Da:

$$3 \mid n \Leftrightarrow 3 \mid (a_t + \cdots + a_1 + a_0)$$
$$9 \mid n \Leftrightarrow 9 \mid (a_t + \cdots + a_1 + a_0)$$

(tverrsumtesten).

Bevis: Har $n = a_t \cdot 10^t + \cdots + a_1 \cdot 10 + a_0$. La $f(x) = a_t x^t + \cdots + a_1 x + a_0$. Da er $n = f(10)$ og $a_t + \cdots + a_0 = f(1)$. Siden

$$10 \equiv 1 \pmod{3}$$
$$10 \equiv 1 \pmod{9}$$

gir Teorem 4.4 at

$$f(10) \equiv f(1) \pmod{3}$$
$$f(10) \equiv f(1) \pmod{9}$$

dvs $n \equiv (a_t + \cdots + a_0) \pmod{3}$ og $n \equiv (a_t + \cdots + a_0) \pmod{9}$. $\square$

Eksempel: $3 \mid 462$ siden $3 \mid (4+6+2)$ mens $3 \nmid 514$ siden $3 \nmid (5+1+4)$.
$9 \mid 2340$ siden $9 \mid (2+3+4+0)$.

Teorem 4.6 (Divisjon med 11)

$$11 \mid (a_t \cdots a_1 a_0)_{10} \Leftrightarrow 11 \mid (a_0 - a_1 + a_2 - \cdots + (-1)^t a_t)$$

Bevis: Som over, start med $10 \equiv -1 \pmod{11}$ $\square$

Eksempel: $11 \mid 8152914$ siden $11 \mid (4-1+9-2+5-1+8)$