Modulo räkning

Def: Om $x_1, x_2 \in \mathbb{Z}$ har samma rest vid division med $m \in \mathbb{N}$ säger vi att x_1 och x_2 är kongruenta modulo m och skriver $x_1 \equiv x_2 \pmod{m}$.

Ett annat sätt att säga detta är att $m \mid (x_1 - x_2)$. Relationen är en ekvivalensrelation.

(reflexiv): $x \equiv x \pmod{m}$

eftersom $m \mid x - x = 0$

(symmetrisk): Om $x \equiv y \pmod{m}$
$\Rightarrow y \equiv x \pmod{m}$

Om $m \mid x-y$ då gäller också
$m \mid (y-x) = -(x-y)$.

(transitiv): Om $x \equiv y \pmod{m}$ och
$y \equiv z \pmod{m} \Rightarrow x \equiv z \pmod{m}$.

Antag $m \mid x-y$ och $m \mid y-z$ då
får vi att $m \mid (x-y)+(y-z) = x-z$.

Vi får en uppdelning av $\mathbb{Z}$ i ekvivalensklasser, t ex

$\mathbb{Z} = \{\text{udda}\} \cup \{\text{jämna}\}$.

$\mathbb{Z} = \{\text{rest } 0 \text{ vid division med } 3\} \cup$

$\cup \{\text{rest } 1 \text{ — " —}\} \cup$

$\cup \{\text{rest } 2 \text{ — " —}\}$

Sats: Om $x_1 \equiv x_2 \pmod m$ och $y_1 \equiv y_2 \pmod m$

då gäller i) $x_1 + y_1 \equiv x_2 + y_2 \pmod m$

ii) $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod m$

OBS! division fungerar ej!!

$2 \equiv 8 \pmod 6$ men $1 \not\equiv 4 \pmod 6$

$2 \cdot 1 \quad 2 \cdot 4$

Ex: Är $12798 \cdot 5463 = 69915574$?

Lösn: Räkning modulo 10:

$12798 \equiv 8 \pmod{10}$

$5463 \equiv 3 \pmod{10}$

$12798 \cdot 5463 \equiv 8 \cdot 3 \equiv 4 \pmod{10}$

$69915574 \equiv 4 \pmod{10}$

Kan stämma!

Räkning modulo 9:

$$12798 = 1\cdot 10^4 + 2\cdot 10^3 + 7\cdot 10^2 + 9\cdot 10 + 8$$

$$10 \equiv 1 \pmod 9$$

$$10^2 \equiv 1\cdot 1 \equiv 1 \pmod 9$$

$$12798 \equiv 1+2+7+9+8 \pmod 9$$

$$\equiv 0 \pmod 9$$

$$12798\cdot 5463 \equiv 0 \pmod 9$$

$$69915574 \equiv 6+9+9+1+5+5+7+4$$

$$\equiv 19 \equiv 1 \pmod 9$$

$$\Rightarrow 12798\cdot 5463 \neq 69915574.$$

Ex: Är 233 256 846 delbart med 3?

V: vill att $233\,256\,846 \equiv 0 \pmod 3$.

$10 \equiv 1 \pmod 3$ så

$233\,256\,846 \equiv 2+3+3+2+5+6+8+4+6$

$\equiv 2+0+0+2+2+0+2+1+0 \equiv 0 \pmod 3$

SVAR: Ja, det är delbart.

$\mathbb{Z}_m$

Mängden av ekvivalensklasser modulo m betecknas $\mathbb{Z}_m$.

Def: Låt oss definiera operationerna $+$ och $\cdot$ på $\mathbb{Z}_m$ genom att låta

$$[x]_m + [y]_m = [x+y]_m$$

$$[x]_m \cdot [y]_m = [x \cdot y]_m$$

Ex: $[0]_2 + [1]_2 = [0+1]_2 = [1]_2$

jämnt + udda udda

$$[2]_2 + [15]_2 = [2+15]_2 = [17]_2 = [1]_2$$
$$= [3]_2$$

Vi måste undersöka om operationerna är väldefinierade, dvs att de inte beror av val av representant. Men det följer från satsen om kongruensräkning. Operationerna har egenskaperna

M_1: $a+b \in \mathbb{Z}_m$, $a \cdot b \in \mathbb{Z}_m$

M_2: $a+b = b+a$ och $a \cdot b = b \cdot a$

M_3: $(a+b)+c = a+(b+c)$ och $(ab)c = a(bc)$

M4: $a+0=a$, $a\cdot 1=a$

M5: $a(b+c)=ab+ac$

M6: För varje $a\in\mathbb{Z}_n$ finns det ett unikt element $(-a)\in\mathbb{Z}_n$ så att $a+(-a)=0$.

OBS! motsvarigheten till I7 gäller ej.

Ex: I $\mathbb{Z}_2=\{0,1\}$ är $-1=1$.

$\mathbb{Z}_m$ $0, 1, 2, 3, \ldots (m-1)$.

Inverterbara element i $\mathbb{Z}_m$

I $\mathbb{Z}$ saknar alla tal utom $1, -1$ en multiplikativ invers, men i $\mathbb{Z}_m$ kan det finnas flera.

Def: $r \in \mathbb{Z}_m$ sägs vara inverterbart om det finns ett tal $x \in \mathbb{Z}_m$ så att $r \cdot x = 1$ i $\mathbb{Z}_m$. ($x = r^{-1}$)

Ex: Finn alla inverterbara element i $\mathbb{Z}_{10}$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$.

Lösn: $\mathbb{Z}_{10}$: $3 \cdot 7 \equiv 21 \equiv 1 \quad 7 = 3^{-1}$

$(-1)^2 \equiv 9^2 \equiv 81 \equiv 1 \quad 3 = 7^{-1}$

$1^2 = 1$

$\mathbb{Z}_{11}$: alla tal utom 0.

(Övn: visa det!)

$\mathbb{Z}_{12}$: $5^2 = 25 = 1$, $7^2 = 49 = 1$

$(-1)^2 = 11^2 = 121 = 1$, $1^2 = 1$

Sats: r är inverterbar i $\mathbb{Z}_m$ om och endast om $SGD(r,m)=1$.
Speciellt i $\mathbb{Z}_p$ (p primtal) så är alla element, utom 0, inverterbara.

Bevis: Om $r\cdot k=1$ i $\mathbb{Z}_m$ då finns l så att $r\cdot k - 1 = m\cdot l \Rightarrow 1 = rk - ml$
$\Rightarrow SGD(r,m)=1$.

Om $SGD(r,m)=1$ så finns $k', l' \in \mathbb{Z}$ så att $1 = rk' + ml' \Rightarrow r\cdot k = 1$ i $\mathbb{Z}_m$.

Följdsats: Antalet inverterbara element i $\mathbb{Z}_m$ är $\phi(m)$ st.

Låt U_n betecknа mängden av inverterbara element i $\mathbb{Z}_n$.

Om $y \in U_n$ så får vi att $yU_n = U_n$, för funktionen $f: U_n \to U_n$; $f(x) = yx$ är bijektiv.

Ex: $U_3 = \{1, 2\}$ och $2U_3 = \{2 \cdot 1, 2 \cdot 2\} = \{2, 1\}$

Ex: $U_8 = \{1, 3, 5, 7\}$ $3U_8 = \{3 \cdot 1, 3 \cdot 3, 3 \cdot 5, 3 \cdot 7\} =$

$= \{3, 1, 7, 5\} = U_8$

Sats: Om $y \in U_m$ så är $y^{\phi(m)} \equiv 1 \pmod{m}$

Ex: $3^4 \equiv 1 \pmod 8$ $(3^4 = 81 \equiv 1 \pmod 8)$

bevis: Låt $U_m = \{u_1, \ldots, u_{\phi(m)}\}$

och sätt $u = u_1 \cdots u_{\phi(m)}$. Då

$y \in U_m$, $yU_m = U_m$ har vi att

$$u = u_1 \cdots u_{\phi(m)} = (yu_1)(yu_2)\cdots(yu_{\phi(m)})$$

$$= y^{\phi(m)} \cdot u_1 u_2 \cdots u_{\phi(m)} = y^{\phi(m)} u$$

Multiplicera bägge sidor med u^{-1} ger

$$1 = y^{\phi(m)}$$

Eulers sats: Om $SGD(y, m) = 1$ så är $y^{\phi(m)} \equiv 1 \pmod{m}$.

Fermats lilla sats: Om p primtal och $p \nmid y$ så är $y^{p-1} \equiv 1 \pmod{p}$

$\Updownarrow$

$SGD(p, y) = 1$

Ex: Visa att $n^p \equiv n \pmod{p}$ för alla $n \in \mathbb{Z}$.

Lösn: Om $p \nmid n$ har vi $n^{p-1} \equiv 1 \Rightarrow n^p \equiv n \pmod{p}$

Om $p \mid n \Rightarrow n \equiv 0 \pmod{p}$ så $n^p \equiv n \pmod{p}$

$0 \equiv 0$