Räkning modulo n

April 5 2006

Mängden $\mathbb{Z}_n$

I fortsättningen betecknar n ett fixt heltal ≥ 2.

Definition

Två heltal x och y säges vara **kongruenta modulo** n om

$$n/a - b.$$

I denna situationen skriver vi $a \equiv_n b$, eller $a \equiv b$ (modulo n.)

Anmärkning

Kongruens modulo n är en ekvivalensrelation.

Vi betecknar ekvivalensklassen av x med $[x]_n$:

$$[x]_n = \{y \in \mathbb{Z}, n/x - y\}$$

Mängden $\mathbb{Z}_n$

Enligt divisionalgoritmen kan varrje heltal x entydigt skrivas som:

$$x = nq + r. 0 \leq r \leq n - 1.$$

Det följer att

$$[x]_n = [r]_n, 0 \leq r \leq n - 1$$

och därför finns det totalt $n - 1$ ekvivalensklasser:

$$[0]_n, [1]_n, ..., [n - 1]_n.$$

Definition

Med $\mathbb{Z}_n$ menar vi mämgden av ekvivalensklasser av $\equiv_n$.

$$\mathbb{Z}_n = \{[0]_n, [1]_n, ..., [n - 1]_n\}.$$

Mängden $\mathbb{Z}_n$

Exempel

- $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$, *där:*
  $[0]_2 = \{2n, n = 0, 1, ...\}, [1]_2 = \{2n + 1, n = 0, 1, ...\}.$
- $[110]_5 = [5 \cdot 22]_5 = [0]_5.$
- $[17]_3 = [3 \cdot 5 + 2]_3 = [2]_3.$

Definition

Vi kan införa de följande operationer:

- $[x]_n + [y]_n = [x + y]_n.$
- $[x]_n \cdot [y]_n = [xy]_n.$

Mängden $\mathbb{Z}_n$

Operationerna är väldefinierade, d.v.s att de inte är beroende på representanterna.

- $a \equiv_n x, b \equiv_n y \Rightarrow a + b \equiv_n x + y$.
- $a \equiv_n x, b \equiv_n y \Rightarrow ab \equiv_n xy$.

Exempel

- $10 \equiv_9 1, 10^k \equiv_9 1 \cdot \ldots \cdot 1 = 1$
- $65431 = 6{\cdot}10^4 + 5{\cdot}10^3 + 4{\cdot}10^2 + 3{\cdot}10 + 1 \equiv_9 6+5+4+3+1 \equiv_9 1$.
- *Ett heltal är delbart med* 9 *om summan av alla siffrorna är delbar med* 9.

Mängden $\mathbb{Z}_n$

Vi har sett att om $xy = 0$ där $x, y \in \mathbb{Z}$ då är det $x = 0$ eller $y = 0$.
Notera att detta gäller inte i $\mathbb{Z}_n$.
Till exempel: $[0]_6 \neq [2]_6, [0]_6 \neq [3]_6$, men

$$[2]_6[3]_6 = [6]_6 = [0]_6.$$

Exempel

Hitta lösningar modulo 6 *till* $x^2 - 3x + 2 = 0$
Svar: $x = [2]_6, [1]_6, [4]_6, [5]_6$.

Multiplikationen i $\mathbb{Z}_n$

Definition

Vi säger att $[0] \neq [a] \in \mathbb{Z}_n$ har en **multiplikativ invers** $[b] \neq [0]$ om

$$[a][b] = [1], d.v.s\, ab = 1 \text{ modulo n.}$$

I så fallet betcknar vi $[b]$ med $[a]^{-1}$ och vi säger att a är inverterbar.

Det är klar att:

$$b \text{ är invers till } a \Leftrightarrow a \text{ är invers till } b.$$

Exempel

De inverterbara elementen i $\mathbb{Z}_6$ är:

- $[1], [1]^{-1} = [1]$.
- $[5], [5]^{-1} = [5]$.

Multiplikationen i $\mathbb{Z}_n$

SATS

Ett element $[0] \neq [a] \in \mathbb{Z}_n$ *är inverterbart om och endast om* $(a, n) = 1$.

Exempel

Bestäm $[41]^{-1}$ *i* $\mathbb{Z}_{323}$.

- $[41]$ är inverterbart eftersom är $(41, 323) = 1$.
- Genom divisionsalgoritmen hittar vi x, y sådan att $41x + 323y = 1$:

$$-63 \cdot 41 + 8 \cdot 323 = 1$$

- Då är $-63 \cdot 41 \equiv 1 \bmod 323$ och

$$[41]_{323}^{-1} = [-63]_{323} = [260]_{323}.$$

Multiplikationen i $\mathbb{Z}_n$

Kom ihåg att:

$\phi(n) =$ antalet positiva heltal $1 \leq x \leq n$ som är relativt prima med n.

Då kan vi säga att

$$\phi(n) = \text{ antalet inverterbara element i } \mathbb{Z}_n.$$

Vi betecknar med U_n mängden av inverterbara element i $\mathbb{Z}_n$. Då är $|U_n| = \phi(n)$.

Exempel

- $|U_p| = p - 1$ *för varje primtal* p.
- *Visa att* $[x]_n = [x]_n^{-1} \Rightarrow x^2 - 1 \equiv_n 0$.

Multiplikationen i $\mathbb{Z}_n$

SATS

$x \in U_n \Rightarrow x^{\phi(n)} \equiv_n 1.$

Det följer att: **Little Fermat's theorem**

För varje positivt heltal x och varje primtal p gäller att:

$$x^p \equiv_p x \text{ d.v.s } x^{p-1} \equiv_p 1.$$

Exempel

Beräkna resten då 3^{3374} *divideras med* 17.

Vi vet att $3^{16} \equiv_{17} 1.$

$$3^{3374} = 3^{210 \cdot 16 + 14} = (3^{16})^{210} 3^{14} \equiv_{17} 3^{14} \equiv_{17} 2.$$