# LEKTION 03-08

## Modulär aritmetik

Klockan är nu 9 : 00. Hur mycket kommer klockan om 16 timmar? Man kan ta $9+16=25$ men eftersom en dygn bara har 24 timmar blir det $kl:01$. Vi sägar då att vi räcknar "modulo 24". Det betyder att :

- vi delar tal med 24
- vi tar resten. Vi säger att två tal är "ekvivalenta" (lika modulo 24) om de har samma resten. Om $a$ och $b$ är ekvivalenta skriver vi: $a \equiv b$.

Vi har att $25 = 24+1$ och $1 = 0 \cdot 24 + 1$, dvs $25 \equiv 1$.

**Definition 0.1.** Två tal är eqvivalenta *modulo* $n$, $a \equiv_n b$ om

$$a = kn + b \text{ där } k \in \mathbb{Z}$$

Vi ska tänka på $a$ och $b$ som "samma tal modulo n" . Till exampel modulo 2 har vi:

$$\ldots -6 \equiv_2 -4 \equiv_2 -2 \equiv_2 0 \equiv_2 2 \equiv_2 4 \equiv_2 6 \ldots$$

$$\ldots -5 \equiv_2 -3 \equiv_2 -1 \equiv_2 1 \equiv_2 3 \equiv_2 5 \equiv_2 7 \ldots$$

Alla jämna heltal är ekvivalenta till 0 modulo 2 och alla udda heltal är ekvivalenta till 1 modulo 2. Så vi kan beteckna alla jämna tal med [0] och alla udda heltal med [1] och bilda en ny mängd (mängden av heltal modulo 2):

$$\mathbb{Z}_2 = \{[0], [1]\}$$

*Exempel.* Räkna $26 + 32$ modulo 2.

Eftersom $26 + 32 = 58$ och $58 \equiv_2 [0]$ säger man att $26 + 32 = 0$ modulo 2.

På samma sätt kan man bilda mängen av heltal modulo n:

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

där $[k]$ representerar alla heltal på formen $tn + k$ där $t \in \mathbb{Z}$, dvs $[k] = \{tn + k \text{ där } t \in \mathbb{Z}\}$. Vi säger att $k$ är ekvilansklassen av $k$ modulo $n$ och $\mathbb{Z}_n$ är mängden av ekvilensklasser modulo $n$.

En multipel av $n$ blir alltid [0] modulo $n$.

*Notera att:* om $a \equiv_n c$ och $b \equiv_n d$ då $a = kn + c$ och $b = hn + d$ där $k, h \in \mathbb{Z}$. Det följer att $a + b = (k + h)n + (d + c)$ och $ab = (khn + kd + ch)n + dc$. Detta visar att

- $a + b \equiv_n c + d$, dvs att $[a] + [c] = [a + c]$.

- $ac \equiv_n cd$, dvs att $[a] \cdot [c] = [a \cdot c]$

*Exempel.*

- Beräkna $27 \cdot 35$ modulo 4.
  $27 \cdot 35 = (6 \cdot 4 + 3) \cdot (4 \cdot 8 + 3) \equiv_4 3 \cdot 3 = 4 \cdot 2 + 1 \equiv_4 1$
- Beräkna 65432 modulo 9.
  $65432 = 6 \cdot 10^4 + 5 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 2 \equiv_9 6 \cdot 1^4 + 5 \cdot 1^3 + 4 \cdot 1^2 + 3 \cdot 1 + 2 = 20 \equiv_9 2$

Man kan sammafattar resultatet av addition och multliplication modulo n i en tabel. Till exempel, modulo 6:

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 2 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| · | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

*Notera* kancelleringslagen gäller inte. Till example i $\mathbb{Z}_6$ har vi

$$2 \cdot 2 = 2 \cdot 5 \text{ men } 2 \neq 5$$

Kancelleringslagen gäller om elemnt är INVERTERBARA.

**Definition 0.2.** Ett element $a \in \mathbb{Z}_n$ är inverterbara om det finns $b \in \mathbb{Z}_n$ sådan att:

$$a \cdot b = b \cdot a = 1$$

Elementet $b$ kallas *inversen* av $a$.

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

*BEVIS.* Antag först att $sgd(a, n) = 1$. Det Finns heltal $x, y$ sådan att $1 = ax + yn$ och därmed är $1 \equiv_n ax$. Det betyder att:

$$[1] = [ax] = [a] \cdot [x].$$

Antag nu att $a$ är invertebar, dvs det finns $b$ sådan att $[ab] = [1]$. Det följer att

$$ab = kn + 1, \text{ och därmed } 1 = ab - kn$$

Det betyder att $a$ och $n$ är relativt prima.

*Exempel.* Bestäm inversen till 41 i $\mathbb{Z}_{323}$.

Inversen existerar eftersom $sgd(41, 323) = 1$. Vi beräkna den med hjälp av Euklides algoritm:

$$\begin{array}{rcrcr} 323 & = & 8 \cdot 41 & - & 5 \\ 41 & = & 8 \cdot 5 & + & 1 \end{array}$$

Därmed gäller $1 = -63 \cdot 41 + 8 \cdot 323 \equiv_{323} -63 \cdot 41$. Inversen är alltså $[-63] = [260]$.

Man kan lösa ekvationer modulo $n$. Vi ska lösa

$$6x \equiv_{17} 8$$

Vi vill hitta (alla) $x \in \mathbb{Z}_{17}$ sådan att $6x \equiv_{17} 8$.

Eftersom $6x \equiv_{17} 8$ om och endast om $6x = 17y+8$ ska vi lösa den diofantiska ekvationen

$$6x - 17y = 8.$$

Heltalen 6 och 17 är relatvt prima och Euklides algoritm ger:

$$\begin{array}{rcrcr} 17 & = & 2 \cdot 6 & + & 5 \\ 6 & = & 5 \cdot 1 & + & 1 \end{array}$$

Då blir $1 = 6 - 5 = 5 - 16 + 2 \cdot 6 = 3 \cdot 6 - 17$. Det följer att $x = 24 + 17k$ och $y = 8 + 6k$ är den allmänna lösning. Nu ska vi beräkna den modulo 17.

- $x = 24 + 17k \equiv_{17} 7$;
- $y = 8 + 6k$;

Svaret är $x = 7$ (vi menar att $x = [7] \in \mathbb{Z}_{17}$).

*Exempel* Lös ekvationen $6x \equiv_{16} 8$.

Vi ska lösa ekvationen $6x - 16y = 8$. Vi ser direkt att $gcd(6, 16) = 2$ och Euklides algoritm ger $2 = 3 \cdot 6 - 16$ (man kan beräkna det direkt!). Vidare vet vi att $lcd(6, 16) = 16 \cdot 3$. Den allmänna lösning blir:

- $x = 12 + 8k \equiv_{16} 8 + 8k$; vi har då två möjliga fall, nämlingen $x = 4$ $(k = -1)$ eller $x = 12$ $(k = 0)$.
- $y = 4 + 3k$;

Svaret är $x = 4$ och $x = 12$ (vi menar $x = [4], [12] \in \mathbb{Z}_{16}$).