Diskret matematik 2018-03-26 #4

Vad är 3/2? Den unika lösningen x till $2x=3$
Ingen lösning i $\mathbb{Z}_6$. $5x=1$ har en lösning i $\mathbb{Z}_6$: $x=5$.

<u>Sats</u> Låt a & b vara heltal.

Ekvationen $ax=d$ har åtminstone en lösning i $\mathbb{Z}_n$ omm $\gcd(a,n)\mid d$.

Obs! Det kan finnas flera.

<u>Bevis</u> Enl. def$^n$ av modulär aritmetik håller $ax=d$ i $\mathbb{Z}_n$ omm det finns ett heltal y sådant att $ax+ny=d$.

Enl. tidigare sats har denna ekvation en lösn. omm $\gcd(a,n)\mid d$. ∎

Så varför hade $2x=3$ ingen lösning i $\mathbb{Z}_6$?

För det motsvarar att lösa $2x+6y=3$ och att vänsterled är delbara med $\gcd(2,6)=2$, men 3 är inte det.

<u>Ex</u> Ekvationen $3x=3$ har tre lösningar i $\mathbb{Z}_6$: $x=1, 3, 5$

<u>Def$^n$</u> Ett tal a kallas inverterbart i $\mathbb{Z}_n$ om det finns ett tal x så att $ax=1$ i $\mathbb{Z}_n$.

<u>Sats</u> Talet a är inverterbart i $\mathbb{Z}_n$ omm a&n är relativt prima, dvs. $\gcd(a,n)=1$.

Om a är inverterbart, då är lösningen x till $ax=1$ i $\mathbb{Z}_6$ <u>unik</u>; den kallas a:s invers (multiplikativa invers) och skrivs $a^{-1}$.

T.ex. är $5^{-1}=5$ i $\mathbb{Z}_6$.

<u>Bevis</u> Enl. den tidigare satsen har $ax=1$ en lösning i $\mathbb{Z}_n$ omm $\gcd(a,n)\mid 1$, vilket är omm $\gcd(a,n)=1$.

För att se unik:

Om $ax_1=1$ & $ax_2=1$ i $\mathbb{Z}_n$

då är

$$\begin{array}{lr} & ax_1 = 1 \\ (\text{gånger } x_2) & ax_1x_2 = x_2 \\ (\text{skriv om}) & (ax_2)x_1 = x_2 \\ (ax_2=1) & 1\cdot x_1 = x_2 \\ & x_1 = x_2 \end{array}$$

Ex. Vad är 3:s invers ($3^{-1}$) i $\mathbb{Z}_{13}$?

Vi provar oss fram t.ex.:

1) $x = 1, 2, 3, 4$

$3x = 1$
$3 \cdot 1 = 3 \neq 1$
$3 \cdot 2 = 6 \neq 1$
$3 \cdot 3 = 9 \neq 1$
$3 \cdot 4 = 12 \neq 1$ men $3 \cdot 4 = -1$
så $3 \cdot (-4) = 1$
så $3^{-1} = -4 = 9$.

2) Se anteckningar på Canvas.

Så $3^{-1} = 9$ i $\mathbb{Z}_{13}$

Ex. Lös $3x = 5$ i $\mathbb{Z}_{13}$

Svar Eftersom 3 är inverterbart så kan jag multiplicera med $3^{-1}$ ($=9$)

$3x = 5$

$x = \underbrace{(3^{-1} \cdot 3)}_{1} x = 3^{-1} \cdot 3x = 3^{-1} \cdot 5 = 9 \cdot 5 = 45 = 6$

"Vi delar med 3"

Sats. Om $p$ är ett primtal, då är alla talen $1, 2, \ldots, p-1$ inverterbara i $\mathbb{Z}_p$.

Bevis $\gcd(a, p) = 1$ om $a$ inte är en multipel av $p$.

Ex Bestäm inversen till 28 i $\mathbb{Z}_{103}$ ← Ett primtal (räcker att kolla om delbart med 2, 3, 5 eller 7.)

Vi vill lösa $28x = 1$ i $\mathbb{Z}_{103}$
Omvandla till diof. ekv.

$28x + 103y = 1$.

Euklides:

$103 = 3 \cdot 28 + 19$
$28 = 1 \cdot 19 + 9$
$19 = 2 \cdot 9 + 1$

Läs baklänges:

$1 = \boxed{19} - 2\boxed{9}$
$= \boxed{19} - 2(\boxed{28} - \boxed{19})$
$= 3\boxed{19} - 2\boxed{28}$
$= 3(\boxed{103} - 3\boxed{28}) - 2\boxed{28}$
$= \underbrace{3}_{y}\boxed{103} \underbrace{-11}_{x}\boxed{28}$ $\quad x = -11$

Så $28^{-1} = -11 = 92$ i $\mathbb{Z}_{103}$

**Ex.** Lös $6x = 8$ i $\mathbb{Z}_{16}$

**Svar** Här är $\gcd(6, 16) = 2$, dvs inte 1, så 6 är inte inverterbart. Men det finns lösningar till ekvationen eftersom $\gcd(6,16) = 2 \mid 8$ = högerledet.
(Det kommer finnas precis 2 lösningar)

Hur hitta?

1) Euklides på $6x + 16y = 8$
eller $3x + 8y = 4$ ⊛

$$8 = 2 \cdot \boxed{3} + \boxed{2}$$
$$\boxed{3} = 1 \cdot \boxed{2} + \boxed{1}$$

2) Baklänges
$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) \\ &= -8 + 3 \cdot 3 \end{aligned}$$
så $x, y = (3, -1)$ ger oss en lösn. till $3x + 8y = 1$

3) Multiplicera med $\frac{\text{högerled}}{\gcd} = \frac{4}{1}$ för att få en lösn. till ⊛
$$3 \cdot 12 + 8 \cdot (-4) = 4$$
Så $(x, y) = (12, -4)$ är en lösning till ⊛

4) Använd formen för lösn. till diof. ekv:
$$x = x_p - \frac{b}{\gcd(a,b)} \cdot k = 12 - 8k \text{ för godtyckliga heltal } k.$$

5) Vilka lösningar ger detta i $\mathbb{Z}_{16}$?

$k = 0$ ger $x = 12$
$k = 1$ ger $x = 4$ } Detta är samtliga lösningar.
$k = 2$ ger $x \equiv 12 \pmod{16}$
⋮

**Potenser** $2^{22} \bmod 23$? Är detta $2^{-1}$? NEJ! $2^{-1} = 12$ i $\mathbb{Z}_{23}$.
$$\underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{22 \text{ ggr}}$$

**Metod 1** (Repeterad förenkling)

Vad är $2^{20} \pmod 7$?
$$2^{20} = (2^3)^6 \cdot 2^2 \equiv 1^6 \cdot 2^2 \pmod 7 = 4$$

**Metod 2**

**Sats** (Fermads lilla sats)
Låt $p$ vara ett primtal och låt $a$ vara ett tal som är relativt primt med $p$ (dvs $p \nmid a$)

Då är $a^{p-1} \equiv 1 \pmod p$

Ex. I $\mathbb{Z}_{11}$ gäller $1^{10} \equiv 2^{10} \equiv 3^{10} \equiv 4^{10} \equiv \ldots \equiv 9^{10} \equiv 10^{10} \equiv 1 \pmod{11}$

Bevis

Nyckeln: i $\mathbb{Z}_p$ är talen $a, 2a, 3a, \ldots, (p-1)a$
precis $1, 2, 3, \ldots p-1$ i någon ordning

T.ex. i $\mathbb{Z}_{11}$, $a=2$

| $j$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $ja$ | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 |
| $ja$ mod 11 | 2 | 4 | 6 | 8 | 10 | 1 | 3 | 5 | 7 | 9 |

Varför? Alla talen $ja$ är olika i $\mathbb{Z}_p$:

om $j_1 a = j_2 a$
då är $j_1 a a^{-1} = j_2 a a^{-1} \Rightarrow j_1 = j_2$ (för $j = 1, 2, \ldots, p-1$)

Inget av talen $ja$ är 0 i $\mathbb{Z}_p$:

om $ja = 0$ Då är $j \cdot a \cdot a^{-1} = j = 0$

Därför är de $(p-1)$ talen $a, 2a, \ldots, (p-1)a$
precis $1, 2, \ldots, p-1$ i någon ordning.

Om vi multiplicerar ihop dem:

$a \cdot (2a) \cdot (3a) \ldots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}$

$\parallel$

$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \ldots (p-1)$

Multiplicera med $(p-1)^{-1}, (p-2)^{-1}, \ldots, 3^{-1}, 2^{-1}$
så får vi att $a^{p-1} \equiv 1 \pmod{p}$ $\blacksquare$

Talbaser (Hoppas över. Står ev. i anteckningar på Canvas)

## Delbarhet med 9

Ett tal $x$ är delbart med 9 omm dess siffersumma är det.

**Bevis** Skriv $x$ i decimal form som

$$x = 10^n a_n + 10^{n-1} a_{n-1} + \dots + 10^2 a_2 + 10 a_1 + a_0$$

där $a_n a_{n-1} \cdots a_2 a_1 a_0$ är bas-10 rep. av $x$.

Mod 9 är
$$\begin{aligned} x &\equiv a_n 10^n + a_{n-1} 10^{n-1} + \dots + 10 a_1 + a_0 \\ &\equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod 9. \end{aligned}$$