Matematik baskurs, med diskret matematik

SF1671

Föreläsare: Petter Brändén

Föreläsning 11

Moduloräkning

$m > 0$, heltal och $a, b \in \mathbb{Z}$, så säger vi att

$a \equiv b \pmod{m}$ eller $a \equiv_m b$ om

$$m \mid (a-b)$$

alternativt a och b ger samma rest vid division med m

Uttalas: a är kongruent med b modulo m.

$182 = 2 \cdot 90 + 2$ så

$182 \equiv_{90} 2$ men också $182 \equiv_{90} 92$

$\mathbb{Z}_m = \{$ alla möjliga rester vid division med $m\}$
$= \{0, 1, 2, \ldots, m-1\}$

Definierar addition o multiplikation på $\mathbb{Z}_m$

$a+b =$ resten av $a+b$ vid division med m

definition

$a \cdot b =$ — " — $a \cdot b$ — " —

- Exempel. Vad blir resten då 67^{380} divideras med 31.

Vi räknar på i $\mathbb{Z}_{31}$

$67 = 2 \cdot 31 + 5$, så $67 = 5$ i $\mathbb{Z}_{31}$

$67^{380} = 5^{380}$ i $\mathbb{Z}_{31}$

$5^3 = 125 = 4 \cdot 31 + 1$ utnyttja ~~detta~~

$5^3 = 1$ i $\mathbb{Z}_{31}$

$380 = 126 \cdot 3 + 2$, så

$67^{380} = 5^{380} = 5^{126 \cdot 3 + 2} = (5^3)^{126} \cdot 5^2 = 1^{126} \cdot 25 = 25$

i $\mathbb{Z}_{31}$

Svar: Resten är 25

- Definition. Om $a, b \in \mathbb{Z}_n$ och $ab = 1$ i $\mathbb{Z}_n$, så säger vi att a och b är **inverterbara**.

$\mathbb{Z}_5$: $2 \cdot 3 = 6 = 1$, så $2, 3$ är inverterbara.

- Definition. Om $a, b \in \mathbb{Z}_n$ och $ab = 1$ i $\mathbb{Z}_n$, så säger vi att a och b är **inverterbara**.
- Vi skriver $b = a^{-1}$ och b kallas för **inversen** till a .

- **Definition.** Om $a, b \in \mathbb{Z}_n$ och $ab = 1$ i $\mathbb{Z}_n$, så säger vi att a och b är **inverterbara**.
- Vi skriver $b = a^{-1}$ och b kallas för **inversen** till a . det är den alltid
- **Exempel.** Vilka är de inverterbara elementen i $\mathbb{Z}_4$?

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$1 \cdot 1 = 1$ så 1 är inverterbar

$3 \cdot 3 = 1$ så 3 —||—

$3^{-1} = 3$

- **Sats.** Ett element a i $\mathbb{Z}_n$ är inverterbart omm $\mathrm{sgd}(a, n) = 1$.

"a och n är relativt prima"

Bevis: Avgör om a är inverterbart i $\mathbb{Z}_n$

Dvs hitta lösning till ekvation $ax = 1$ i $\mathbb{Z}_n$

dvs $1 - ax = 0$ i $\mathbb{Z}_n$ dvs $n \mid (1 - ax)$

dvs finns $y \in \mathbb{Z}$ s.a. $1 - ax = n \cdot y$

dvs det finns en invers x till a omm vi har

en lösning till $ax + n \cdot y = 1$

$\Longleftrightarrow$ $\mathrm{sgd}(a, n) = 1$

Hur hittar vi inversen till a?

Jo, vi hittar en lösning x till), dvs vi använder Euklides algoritm.

- **Sats**. Ett element a i $\mathbb{Z}_n$ är inverterbart omm $\mathrm{sgd}(a, n) = 1$.
- I $\mathbb{Z}_p$, där p är ett primtal, är alla element förutom 0 inverterbara. $a \in \mathbb{Z}_p$. a inverterbart omm $\mathrm{sgd}(a,p)=1$ $\Leftrightarrow a \neq 0$
- Om a, b är inverterbara så är också ab inverterbart.

$\mathbb{Z}_p$ är ett exempel på en ändlig kropp (finite field)

- Sats. Ett element a i $\mathbb{Z}_n$ är inverterbart omm $\mathrm{sgd}(a, n) = 1$.
- I $\mathbb{Z}_p$, där p är ett primtal, är alla element förutom 0 inverterbara.
- Om a, b är inverterbara så är också ab inverterbart. Vi har $(ab)^{-1} = b^{-1}a^{-1}$, ty $a^{-1}b^{-1}$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1.$$

- Sats. Ett element a i $\mathbb{Z}_n$ är inverterbart omm $\mathrm{sgd}(a, n) = 1$.
- I $\mathbb{Z}_p$, där p är ett primtal, är alla element förutom 0 inverterbara.
- Om a, b är inverterbara så är också ab inverterbart. Vi har $(ab)^{-1} = b^{-1}a^{-1}$, ty

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1.$$

- Vi hittar a^{-1} genom att lösa den Diofantiska ekvationen

$$ax + ny = 1$$

- **Exempel.** Bestäm 14^{-1} i $\mathbb{Z}_{45}$. Vi vill alltså lösa

$14x + 45y = 1$, för då $x = 14^{-1}$.

Euklides igen:

$45 = 3 \cdot 14 + 3$

$14 = 4 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

gå baklänges i Euklides

$\text{sgd}(45,14) = 1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (14 - 4 \cdot 3) = 5 \cdot 3 - 1 \cdot 14$

$= 5 \cdot (45 - 3 \cdot 14) - 1 \cdot 14 = 5 \cdot 45 - 16 \cdot 14$

$= 14 \cdot (-16) + 45 \cdot 5$

Svar: $14^{-1} = 29$

$x = -16 = -16 + \underset{0}{\underset{\shortparallel}{45}} = 29$ i $\mathbb{Z}_{45}$

- Lösningar till mer allmänna ekvationer av typen $ax = c$ där x är en obekant i $\mathbb{Z}_n$ kan också lösas genom att lösa en Diofantisk ekvation.

Lös $ax = c$ i $\mathbb{Z}_n$ ($x \in \mathbb{Z}_n$ obekant)

$n \mid (c - ax) \iff$ Finns $y \in \mathbb{Z}$ $c - ax = ny$

Får Diofantiska ekvationen $\boxed{ax + ny = c}$

Löser ekvationen med $(x, y) \in \mathbb{Z} \times \mathbb{Z}$

Sedan hitta vi motsvarand x i $\mathbb{Z}_n$.

- Lösningar till mer allmänna ekvationer av typen $ax = c$ där x är en obekant i $\mathbb{Z}_n$ kan också lösas genom att lösa en Diofantisk ekvation.
- Exempel. Lös $5x = 4$ i $\mathbb{Z}_{11}$.

Alternativ lösning: $5^{-1} = -2 = 9$

$5x = 4 \iff 5^{-1} \cdot 5x = 5^{-1} 4$

$\iff x = 5^{-1} \cdot 4 = 9 \cdot 4 = \ldots = 3$

$11 \mid (4 - 5x) \iff 4 - 5x = 11 \cdot y$ för ngt $y \in \mathbb{Z}$

$$\boxed{5x + 11y = 4}$$

$11 = 2 \cdot 5 + 1$

$1 = (-2) \cdot 5 + 11 \cdot 1$

$1 = 5 \cdot (-2) + 11 \cdot 1$

Multiplicera med 4

$4 = 5 \cdot (-8) + 11 \cdot 4$

$x = -8 = -8 + 11 = 3$ (i $\mathbb{Z}_{11}$)

Svar: $x = 3$

Kan vi ha fler lösningar?

▶ Exempel. Lös $5x = 10$ i $\mathbb{Z}_{15}$.

$15 \mid (10 - 5x) \Leftrightarrow$ Finns $y \in \mathbb{Z}$ s.a. $10 - 5x = 15y$

$$\begin{cases} x = x_0 - k\frac{b}{d} \\ y = y_0 + k\frac{a}{d} \end{cases}$$

$k \in \mathbb{Z}$. sedan reducera mod n

$\boxed{5x + 15y = 10} \Leftrightarrow \boxed{x + 3y = 2 \quad \star}$

dividera med 5

Samtliga lösningar till $\star$ ges av

$$\begin{cases} x = 2 - 3y \\ y \in \mathbb{Z} \text{ (godtyckligt)} \end{cases}$$

Bara intresserade av $x \in \mathbb{Z}_{15}$

y	0	-1	-2	-3	-4	-5	-6	...
$x \in \mathbb{Z}_{15}$	2	5	8	11	14	17 = 2	5	

upprepas

Svar: 2, 5, 8, 11, 14

- Fermats lilla sats. Låt p vara ett primtal och a ett heltal s.a. $p \nmid a$. Då är
$$a^{p-1} \equiv_p 1.$$
- Pierre de Fermat (1607–1665).

- **Fermats lilla sats.** Låt p vara ett primtal och a ett heltal s.a. $p \nmid a$. Då är
$$a^{p-1} \equiv_p 1.$$

Bevis: Räcker att visa att $a^{p-1} = 1$ i $\mathbb{Z}_p$ då $a \neq 0$. Bilda funktion

$f : \{1, 2, \dots, p-1\} \to \{1, 2, \dots, p-1\}$. $f(x) = ax$.

f är injektion dvs (1-1), $f(x) \neq f(y)$ då $x \neq y$.

Varför? Om $f(x) = f(y)$ så $ax = ay$ (multiplicera med a^{-1})

$a^{-1}ax = a^{-1}ay$ så $x = y$. Olika $\to$ olika

$$V_f = \{1, 2, \dots, p-1\} = D_f$$
$$= \{a\cdot 1, a\cdot 2, a\cdot 3, \dots, a\cdot(p-1)\}$$

Produkten av talen är lika

$\Rightarrow$ $(a\cdot 1)\cdot(a\cdot 2)\cdot(a\cdot 3)\cdots(a\cdot(p-1)) = 1\cdot 2\cdot 3\cdot\dots\cdot(p-1)$

$\Rightarrow$ $a^{p-1}\cdot(\underbrace{1\cdot 2\cdot\dots\cdot(p-1)}_{=b}) = \underbrace{1\cdot 2\cdot 3\cdot\dots\cdot(p-1)}_{=b}$. Mult. med b^{-1}

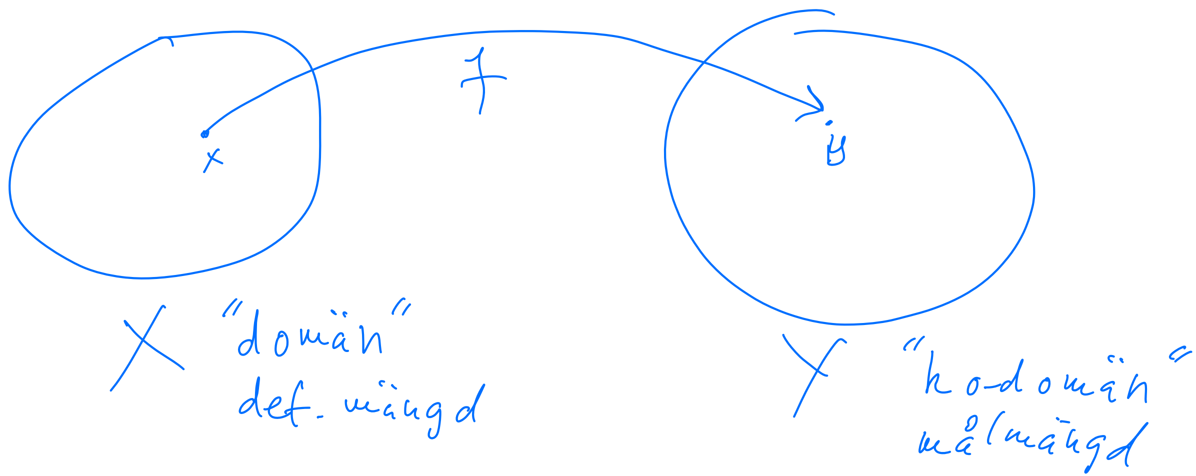
$\Rightarrow$ $a^{p-1}b = b$ $\Rightarrow$ $\boxed{a^{p-1} = 1}$ $\square$

Funktioner

Definition

Låt X och Y vara mängder. En **funktion** f från X till Y är en regel som till varje x i X associerar precis ett element $y = f(x)$ i Y.

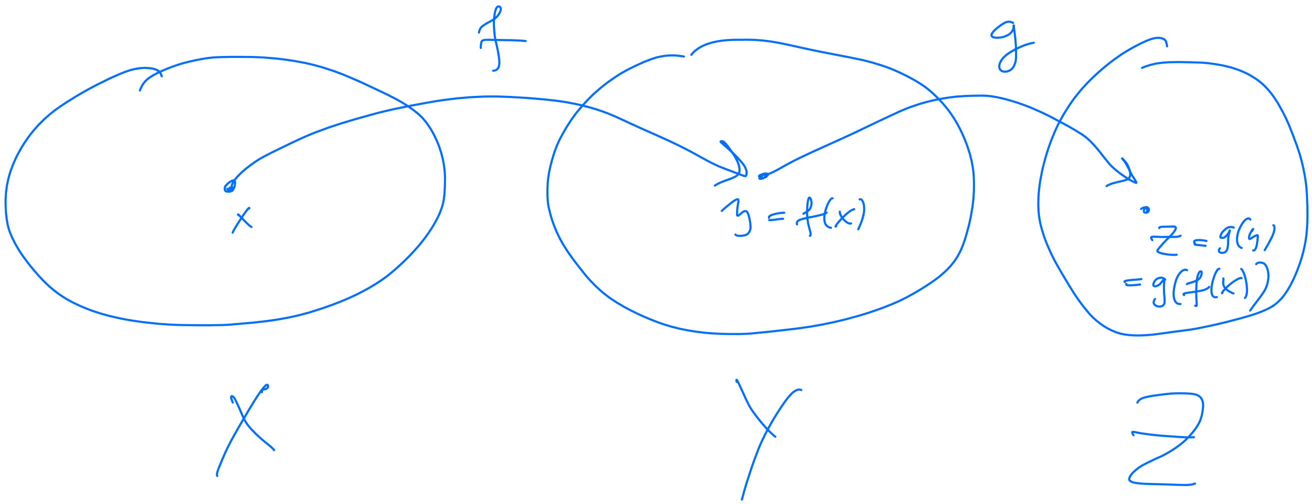
- Vi skriver $f : X \to Y$.
- X kallas **domän** (definitionsmängd).
- Y kallas **kodomän** (målmängd).



Funktioner

Definition

Om $f : X \to Y$ och $g : Y \to Z$ så kan vi definiera en funktion $(g \circ f) : X \to Z$ genom $(g \circ f)(x) = g(f(x))$.



Viktiga typer av funktioner

- Injektion (1–1): $f : X \to Y$ är en injektion om

$$x_1 \neq x_2 \quad \Longrightarrow \quad f(x_1) \neq f(x_2).$$

Viktiga typer av funktioner

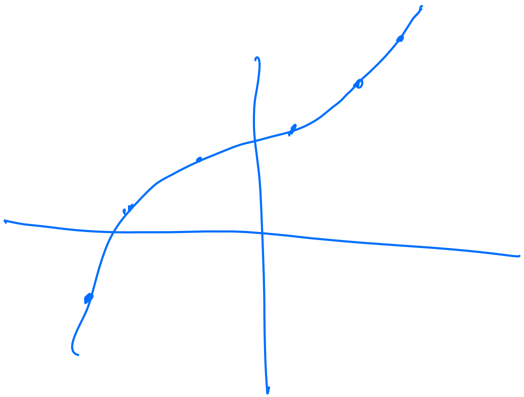
- Injektion (1–1): $f : X \to Y$ är en injektion om

olika på olika

(f är injektiv)

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

- Exempel. $X = Y = \mathbb{Z}$, $f(x) = 2x$ och $f(x) = x^3 + 3$.



Viktiga typer av funktioner

- Injektion (1–1): $f : X \to Y$ är en injektion om

$$x_1 \neq x_2 \quad \Longrightarrow \quad f(x_1) \neq f(x_2).$$

- Exempel. $X = Y = \mathbb{Z}$, $f(x) = 2x \quad$ och $\quad f(x) = x^3 + 3$.
- Surjektion (På): $f : X \to Y$ är en surjektion om det för alla $y \in Y$ finns minst ett $x \in X$ s.a. $f(x) = y$.

$\Leftrightarrow$ värdemängd = målmängd

Viktiga typer av funktioner

- Injektion (1–1): $f : X \to Y$ är en injektion om

$$x_1 \neq x_2 \implies f(x_1) \neq f(x_2).$$

- Exempel. $X = Y = \mathbb{Z}$, $f(x) = 2x$ och $f(x) = x^3 + 3$.
- Surjektion (På): $f : X \to Y$ är en surjektion om det för alla $y \in Y$ finns minst ett $x \in X$ s.a. $f(x) = y$.
- Exempel.

• $X = \mathbb{R}$, $Y = [-1, 1]$, $f(x) = \sin x$
surjektiv.

• $X = \mathbb{Z}$, $Y = \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

$f(x) =$ "resten av x vid division mod m"
surjektion.

Bijektioner och inverser

- Bijektion $f : X \to Y$ är en bijektion om f är både en injektion och en surjektion.

Bijektioner och inverser

- Bijektion $f : X \to Y$ är en bijektion om f är både en injektion och en surjektion.

  pos. reella talen

- Exempel. $X = Y = \mathbb{R}_+$, $f(x) = x^2$
  $X = \mathbb{Z}$, $Y = \{\text{jämna talen}\}$, $f(x) = 2x$.

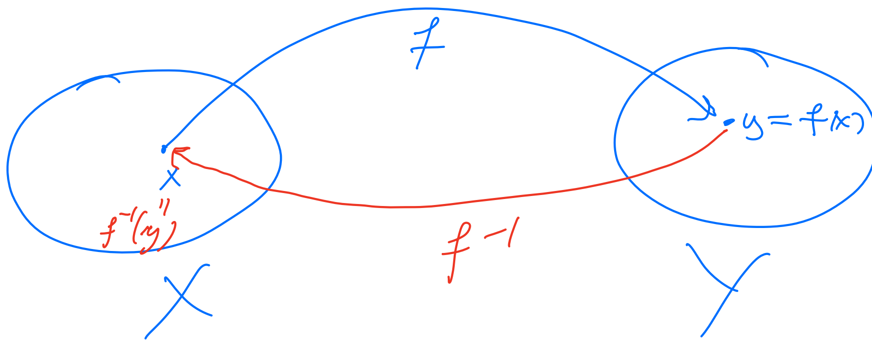
Bijektioner och inverser

- Bijektion $f : X \to Y$ är en bijektion om f är både en injektion och en surjektion.
- Exempel. $X = Y = \mathbb{R}_+$, $f(x) = x^2$
  $X = \mathbb{Z}$, $Y = \{\text{jämna talen}\}$, $f(x) = 2x$.
- Invers Om $f : X \to Y$ är en bijektion så definierar vi inversen till f, $f^{-1} : Y \to X$ genom att "vända på pilarna"

injektiviteten

$$f^{-1}(y) = \text{“det unika } x \text{ s.a. } f(x) = y\text{”}$$

existensen av y fås från surjektivitet,



Bijektioner och inverser

- Bijektion $f : X \to Y$ är en bijektion om f är både en injektion och en surjektion.
- Exempel. $X = Y = \mathbb{R}_+$, $f(x) = x^2$
  $X = \mathbb{Z}$, $Y = \{\text{jämna talen}\}$, $f(x) = 2x$.
- Invers Om $f : X \to Y$ är en bijektion så definierar vi inversen till f, $f^{-1} : Y \to X$ genom att "vända på pilarna"

$$f^{-1}(y) = \text{"det unika } x \text{ s.a. } f(x) = y\text{"}$$

- Kom ihåg: Förut krävde vi bara att f skulle vara injektiv för att definiera inversen till $f : X \to Y$, men då är $f^{-1} : \mathcal{V}_f \to X$.