Logik
Induktion
Talteori
(paus)

God morgon!

talteori (number theory)

- primtal
- delbarhet
- modulär aritmetik

delbarhet

för $a, b \in \mathbb{Z}$

skriver vi $a \mid b$

"b är en multipel av a"

"a delar b"

"b är delbart med a"

$2 \mid 8$ sant

$3 \mid 7$ falskt

$5 \mid 10$ sant

$0 \mid 5$ ~~sant~~/falskt?

vill: undvika att prata om "dela med"

$$a \mid b \iff \exists c \in \mathbb{Z}.\ b = a \cdot c$$

$0 \mid 5$?

$\exists c \in \mathbb{Z}.\ 5 = 0 \cdot c$ – falskt

egenskaper av $|$

- $0 \mid a$ — falskt för $a \neq 0$; sant för $a = 0$ — $(0 \mid 0)$
- $1 \mid a$ — sant — $1 \cdot a = a$
- $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$ (transitivitet)

  $b = d_1 \cdot a$, $c = d_2 \cdot b$

  $c = (d_1 \cdot d_2) \cdot a$
- $(a \mid b \wedge a \mid c) \Rightarrow a \mid b+c$

  $b = d_1 \cdot a$, $c = d_2 \cdot a$

  $b+c = d_1 \cdot a + d_2 \cdot a = (d_1 + d_2) \cdot a$

$\mathbb{N}^+ = \mathbb{Z}^+ \neq \mathbb{N}$

mängden av alla delare

a $\quad\quad$ $\{d \in \mathbb{N} \mid d \mid a\}$

primtal $p \in \mathbb{N}$: $\quad p \geq 2 \quad \wedge \quad$ delare av p är $\{1, p\}$

$$p \geq 2 \quad \wedge \quad \neg \exists a, b \in \mathbb{N} . (a \geq 2 \wedge b \geq 2 \wedge p = a \cdot b)$$

15 $\quad\quad$ 12

$\{1,3,5,15\}$ $\quad\quad$ $\{1,2,4,3,6,12\}$

$\{1,3\}$

vilka delare har 2 tal gemensamt?

→ räkna ut den största gemensamma delaren

gcd(a,b) - den största gemensamma delaren av a och b
(sgd(a,b) på svenska)

Euklides
"Elementa"
(axiom + logik)

- gcd(a,b) = gcd(b,a)
- gcd(0,a) = a , om a≠0
- gcd(1,a) = 1
- gcd(a,a) = a , om a≠0
- gcd(a+b, b) = gcd(a,b)

gcd(0,0)?
- =0
- odefinierat
- jag undviker bestämma mig

$\gcd_{=10+15}(25,10) = \gcd(15,10)$

$d|a,\ d|b \Rightarrow d|a+b$

$d|a+b,\ d|b \Rightarrow d|a$

$a+b=c_1\cdot d \quad b=c_2\cdot d \Rightarrow a=a+b-b=c_1\cdot d-c_2\cdot d=(c_1-c_2)\cdot d$

gcd (25, 10) = 5

25	10
15	10
5	10
5	5

gcd (18, 12) = 6

18	12
6	12
6	6

gcd (11, 17)

11	17
11	6
5	6
5	1

algoritm =
metod för att
räkna ut något

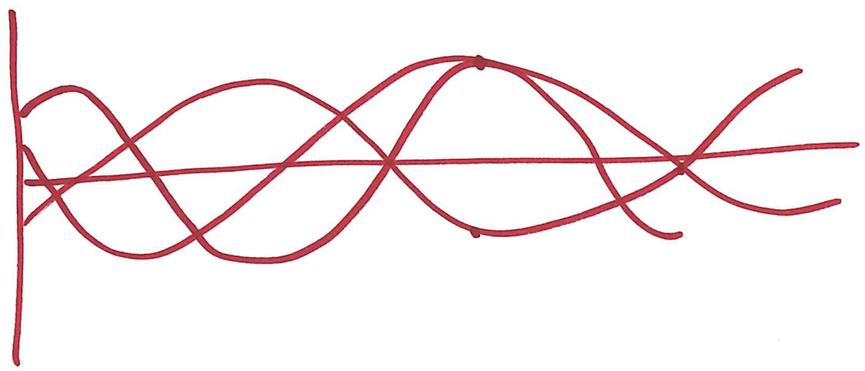
biorytm — populärt på 70- 80-talet

"horoskop"

└ 3 olika : fysiska : 23 dagar = 23

känslomässig : 28 dagar = 2·2·7

intellektuell : 33 dagar = 3·11



"beviset"

du kan få vilket resultat som helst

$23 \cdot a + 28 \cdot b + 33 \cdot c = ??$

$a, b, c \in \mathbb{Z}$

kan vi nå alla element i $\mathbb{Z}$? $u, v \in \mathbb{Z}$

$10 \cdot u + 25 \cdot v = \ldots$ ↑ delb. 5

$\gcd(10,25) = 5$

$7 \cdot u + 11 \cdot v = 1$

$\gcd(7,11) = 1$

$u = -3$
$v = 2$

algoritm?

$a \cdot u + b \cdot v = \ldots$ ↖ kan bli vilket element i $\mathbb{Z}$ som helst om $\gcd(a,b) = 1$

titta på $\boxed{a \cdot u + b \cdot v = 1}$ lösbart om $\gcd(a,b) = 1$

Bézout / Pulverizer

$1 \cdot a + 0 \cdot b = a$

$0 \cdot a + 1 \cdot b = b$

	u	v	a	b	u	v
	1	0	7	11	0	1
	1	0	7	4	-1	1
	2	-1	3	4	-1	1
	2	-1	3	(1)	-3	2

t.ex. $-1 \cdot a + 1 \cdot b =$
$-1 \cdot 7 + 1 \cdot 11 = 4$

$2 \cdot a - 1 \cdot b =$
$2 \cdot 7 - 1 \cdot 11 = 3$

$-3 \cdot a + 2 \cdot b = 1$

leta efter
u, v

$a \cdot u + b \cdot v = 1$

u	v	a	b	u	v
1	0	13	18	0	1
		13	5	-1	1
2	-1	8	5		
3	-2	3	5		
		3	2	-4	3
7	-5	1	2		

$3 \cdot 13 - 2 \cdot 18 = 3!$ →

$7 \cdot 13 - 5 \cdot 18 = 1$?

$91 - 90 = 1$! ☺

pulverizer / Bézouts metod:

om $\gcd(a,b) = 1$

då finns $u, v \in \mathbb{Z}$

sådant att $a \cdot u + b \cdot v = 1$

Euklides sats: för $a, b \in \mathbb{Z}$, och p prim:

$$p \mid a \cdot b \Rightarrow (p \mid a \vee p \mid b)$$

$$3 \mid 6 \cdot 5 \Rightarrow (3 \mid 6 \vee 3 \mid 5)$$

$$6 \mid 4 \cdot 15 \Rightarrow (6 \mid 4 \vee 6 \mid 15)$$ NEJ

6 ej prim

$2 \cdot 3 \mid 4 \cdot 15$

$2 \mid 4$

$3 \mid 15$

visa: $p \mid a \cdot b \Rightarrow (p \mid a \vee p \mid b)$ för $a, b \in \mathbb{Z}$, p primtal

bevis: anta $p \mid a \cdot b$.

falluppdelning

$p \mid a$, då vet vi $(p \mid a \vee p \mid b)$

□

$p \nmid a$ ("är inte delare av")

$\gcd(p, a) = 1$ (eftersom svaret bara kan vara 1 eller p)

↓ (Pulverizer)

vi har $u, v \in \mathbb{Z}$ sådant att:

$u \cdot p + v \cdot a = 1$

multiplicera med b:

$u \cdot p \cdot b + v \cdot a \cdot b = b$

$u \cdot p \cdot b$: delb. p

$v \cdot a \cdot b$: delb. p

b: delb. p!

$p \mid b$

□