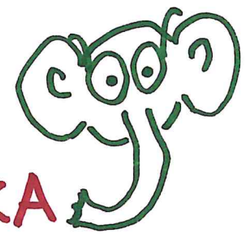
god morgon!

DIOFANTISKA EKVATIONER



ARITMETIKENS FUNDAMENTALSATS

diofantiska ekvationer (diophantine equations)

ekvation där man
bara är intresserad
av heltalslösningar ($\mathbb{Z}$)

$$5x + 7y = 3$$

($x, y \in \mathbb{Z}$)

($x, y \in \mathbb{R}$ eller $\mathbb{Q}$)

$5x = 3 - 7y$

$x = \frac{3-7y}{5}$

$x = \frac{3}{5}, y = 0$

Fermat (1600-talet):

$$a^n + b^n = c^n$$

$a, b, c \in \mathbb{Z}^+$, $n \geq 3$

inga lösningar

"Fermats sista sats"

1990-talet
Andrew Wiles

$10x + 15y = 27$

delb.5 delb.5 ej delb.5

INGA LÖSNINGAR

$\gcd(10,15) = 5$

$5 \nmid 27$

$10x + 15y = 35$

$x=2$
$y=1$

$x, y \in \mathbb{Z}$

MINST 1 LÖSNING

(Bézout / Pulverizer)

OÄNDLIGT MÅNGA LÖSNINGAR

$10 \cdot x + 15 \cdot y = 35$

$10 \cdot (x+15) + 15(y-10) = 35$

$10 \cdot x + \cancel{150} + 15 \cdot y - \cancel{150} =$

$10 \cdot x + 15 \cdot y = 35$

$x = 17$
$y = -9$

ATT LÖSA DIOFANTEN $a \cdot x + b \cdot y = c$ $(x, y \in \mathbb{Z})$

① räkna ut $d = \gcd(a,b)$

② om $d \nmid c$, då INGA LÖSNINGAR

③ dela a, b, c med

$$\left.\begin{aligned} a &\to a/d \\ b &\to b/d \\ c &\to c/d \end{aligned}\right\} \text{"nya" } a, b, c$$

(för den nya a, b : $\gcd(a,b) = 1$)

④ räkna ut u, v sådant att $a \cdot u + b \cdot v = 1$
(Bézout / Pulverizer)

⑤ en lösning är: $x = u \cdot c$, $y = v \cdot c$

⑥ oändligt många lösningar är:

för $k \in \mathbb{Z}$: $x_k = x + k \cdot b$, $y_k = y - k \cdot a$

$10x + 15y = 35$

$d = 5$

$2x + 3y = 7$

$u = -1$, $v = 1$

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

$$\begin{aligned} a \cdot x + b \cdot y &= a \cdot u \cdot c + b \cdot v \cdot c \\ &= c \cdot (a \cdot u + b \cdot v) \\ &= c \cdot 1 \\ &= c \end{aligned}$$

$x = -7$, $y = 7$

$$\begin{aligned} x_k &= -7 + 3 \cdot k \\ y_k &= 7 - 2 \cdot k \end{aligned}$$

$k = 3$:
$x_3 = 2$
$x_3 = 1$

$$a \cdot x + b \cdot y = c$$

$$x = \frac{c - b \cdot y}{a}$$

$$x_k = x + k \cdot b$$

$$y_k = y - k \cdot a$$

$$\begin{aligned} a \cdot x_k + b \cdot y_k &= a \cdot (x + k \cdot b) + b \cdot (y - k \cdot a) \\ &= a \cdot x + \cancel{a \cdot k \cdot b} + b \cdot y - \cancel{b \cdot k \cdot a} \\ &= a \cdot x + b \cdot y \\ &= c \end{aligned}$$

ny y

$$\frac{c - b \cdot (y + a)}{a} =$$

$$\frac{c - b \cdot y - b \cdot a}{a} =$$

$$\frac{c - b \cdot y}{a} - \frac{b \cdot a}{a} =$$

$$\frac{c - b \cdot y}{a} - b$$

$$x - b$$

ARITMETIKENS FUNDAMENTALSATS

+
plus

1, 0

$5 = 1+1+1+1+1$

$2 = 1+1$

gånger

0, 1,
alla primtal
oändligt många!

① är det möjligt att skapa alla naturliga tal med • och primtal?
(bevis?)

$6 = 2 \cdot 3$
$6 = 1 \cdot 2 \cdot 3$
$6 = 1 \cdot 1 \cdot 2 \cdot 3$

② går det på fler än 1 sätt? eller unikt?

1 är inget primtal, 2 är ett primtal

givet $p \in \mathbb{N}$.

p är ett <u>primtal</u> $\iff$

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

givet två primtal p, q

<u>om</u> $p \mid q$ <u>då måste</u> $p = q$

delarna:
1 och q
alltså $p = 1$ eller $p = q$
↓
omöjligt

primtalsfaktorisering: att skriva ett tal som en multiplikation av 1 eller flera primtal

$5 = 5$

$15 = 3 \cdot 5$

$12 = 2 \cdot 2 \cdot 3$

$25 = 5 \cdot 5$

alla naturliga tal ≥ 2 kan primtalsfaktoriseras

visa: Alla $n \in \mathbb{N}$, $n \geq 2$ kan primtalsfaktoriseras

bevis: med STARK induktion över n

Låt $P(n)$ = "n kan primtalsfaktoriseras".

basfall: $P(2)$: $2 = 2$ är redan prim. **OK**

stegfall: $(P(2) \wedge \cdots \wedge P(k)) \Rightarrow P(k+1)$, $k \geq 2$

anta: $P(i)$: "i kan primfaktoriseras" $(2 \leq i \leq k)$ (I.H.)

visa: $P(k+1)$: "$k+1$ kan primfaktoriseras"

falluppdelning:

$k+1$ är prim

färdiga eftersom $k+1$ är primtal

$k+1$ ej prim

då har vi $a, b \geq 2$

och $k+1 = a \cdot b$, $a, b \leq k$

I.H (i=a): a kan primfaktoriseras

$a = p_1 \cdot \ldots \cdot p_n$ (alla p_i prim)

I.H. (i=b): b kan primfaktoriseras

$b = q_1 \cdot \ldots \cdot q_m$ (alla q_i prim)

alltså $k+1 = a \cdot b = p_1 \cdot \ldots \cdot p_n \cdot q_1 \cdot \ldots \cdot q_m$

□

alla naturliga tal ≥ 2 kan bara skrivas som en multiplikation av primtal på 1 UNIKT sätt

$12 = 2 \cdot 2 \cdot 3$
$= 2 \cdot 3 \cdot 2$
$= 3 \cdot 2 \cdot 2$

vilka primtal används

• associativ kommutativ

~~$42 = 3 \cdot 5$~~
~~$42 = 2 \cdot 2 \cdot 7$~~

Euklides sats: $p \mid a \cdot b \Rightarrow (p \mid a \vee p \mid b)$

för $a, b \in \mathbb{Z}$, p prim

Lemma: om p prim och $q_1, \dots, q_n$ prim:

om $p \mid q_1 \cdot \dots \cdot q_n$ **då** $p = q_i$ för något i

bevis: induktion över n

Låt $P(n)$: "**om** $p \mid q_1 \cdots q_n$ **då** $p = q_i$ för något i"

basfall: $P(1)$: $p \mid q_1$, då måste $p = q_1$ **ok**.

stegfall: $P(k) \Rightarrow P(k+1)$, $k \geq 1$

anta: $P(k)$: **om** $p \mid q_1 \cdot \dots \cdot q_k$ **då** $p = q_i$ för något i (I.H.)

visa: $P(k+1)$: **om** $p \mid q_1 \cdot \dots \cdot q_{k+1}$ **då** $p = q_i$ för något i

anta $p \mid q_1 \cdot q_2 \cdot \dots \cdot q_k \cdot q_{k+1}$

Euklides sats:

$p \mid q_1 \cdot \dots \cdot q_k$

↓ I.H.

$p = q_i$

$p \mid q_{k+1}$

↓ både prim

$p = q_{k+1}$

□

sats = teorem

hjälpsats = lemma

↑

sanna, bevisade saker

visa: det finns 1 unikt sätt att primfaktorisera tal ≥ 2

bevis: motsägelsebevis. Anta att det finns tal ≥ 2 som kan primfaktoriseras på 2 sätt.

Låt N vara det minsta talet som har 2 sätt.

$$N = p_1 \cdot \ldots \cdot p_n \qquad N = q_1 \cdot \ldots \cdot q_m$$

inte likadana

då: $p_1 \mid N$, $p_1 \mid q_1 \cdot \ldots \cdot q_m$, $p_1 = q_i$ för något i

"descente infini"

$$\frac{N}{p_1} = p_2 \cdot \ldots \cdot p_n \qquad \frac{N}{p_1} = q_1 \cdot \ldots \cdot q_m$$

(q_i utan)

inte likadana

$\frac{N}{p_1} < N$, som motsäger att N var minst! $\square$