God Morgon!

BY POPULAR DEMAND

(stark) induktion

invarianter

modulär aritmetik

delbarhet

hur kollar man?

med		
1	-	alla tal
2	-	sista siffran delb. 2
* 3	-	summan av alla siffror delb. 3
4	-	sista 2 siffrorna delb. 4
5	-	sista siffran delb. 5
6	-	delb. 2 och 3
7	-	?
8	-	sista 3 siffrorna delb. 8
* 9	-	summan av alla siffror delb. 9

$10 = 2 \cdot 5$

$10 - 1 = 3 \cdot 3$

$16 = 2 \cdot 2 \cdot 2 \cdot 2$

$16 - 1 = 3 \cdot 5$

$3 \mid 125$ nej eftersom $3 \nmid 8 = 1+2+5$

$3 \mid 225$ ja eftersom $3 \mid 9 = 2+2+5$

vill visa: för alla $n \in \mathbb{N}$: n delb. 3 $\iff$ $S(n)$ delb. 3

visar i stället:

$\forall n \in \mathbb{N}$:

$$n \equiv S(n) \pmod 3$$

$S : \mathbb{N} \to \mathbb{N}$

$S(n) =$ summan av alla siffror av n

ex. $n = 125$

$$125 \overset{?}{\equiv} 8 \pmod 3$$

$$2 \overset{!}{\equiv} 2 \pmod 3$$

---

(1) $S(b) = b$ om $0 \leq b \leq 9$

(2) $S(10a + b) = S(a) + b$ om $0 \leq b \leq 9$

visa: $n \equiv S(n) \pmod 3$ för $n \in \mathbb{N}$

bevis: med stark induktion över n

Låt $P(n) =$ "$n \equiv S(n) \pmod 3$"

basfall: $P(b)$ för $0 \le b \le 9$

$b = S(b)$, alltså $b \equiv S(b) \pmod 3$

stegfall: $(P(0) \wedge \cdots \wedge P(k)) \Rightarrow P(k+1)$, för $k \geq 9$

anta: $P(i)$: "$i \equiv S(i) \pmod 3$", $0 \le i \le k$ (I.H.)

visa: $P(k+1)$: "$k+1 \equiv S(k+1) \pmod 3$"

$$
\begin{aligned}
k+1 &= 10a + b && (\text{för något } a, b \in \mathbb{N},\ 0 \le b \le 9) \\
&\equiv a + b && (10 \equiv 1 \pmod 3)\ * \\
&\equiv S(a) + b && (\text{I.H. } i = a,\ a < k+1) \quad a = \tfrac{k+1-b}{10} \\
&= S(10a + b) && (\text{egenskap } S) \\
&= S(k+1)
\end{aligned}
$$

$\pmod 3$ *

$10 \equiv 1 \pmod 9$

$*$: 3 kan vara 9 också!

2^{29} har 9 siffror, alla olika

<u>fråga:</u> vilken siffra saknas?

$0 \le d \le 9$

(mod 9)

alla siffror i talet spelar roll

(1) $S(2^{29}) = 45 - d$

(2) $2^{29} \equiv S(2^{29}) \pmod{9}$

$$45 = 1+2+3+\dots+9 = \frac{9\cdot 10}{2}$$

$$2^3 = 8 \equiv -1 \pmod{9}$$

$$\begin{aligned}
2^{29} &= 2^{3\cdot 9+2} \\
&= (2^3)^9 \cdot 2^2 \\
&= 8^9 \cdot 2^2 \\
&\equiv (-1)^9 \cdot 4 \\
&= -4 \\
&\equiv 5 \pmod{9} \qquad \equiv 45 - d
\end{aligned}$$

$d \equiv 4 \pmod{9}$

$\Rightarrow$ $5 \equiv -d \pmod{9}$

$d \equiv 4 \pmod{9}$

fusk

$2^{29} =$

536870912

miniräknare

$\boxed{d = 4}$

$1+2+\ldots+3n=$

enkel induktion

$P(k) \Rightarrow P(k+1)$

är mindre användbar än

stark induktion

$(P(0) \wedge \ldots \wedge P(k)) \Rightarrow P(k+1)$

alla naturliga tal kan primfaktoriseras

lika starka

motsägelsebevis + "det minsta motexemplet"

$\sqrt{2}$ inte rationell

<u>visa</u> : $n \equiv S(n) \pmod 3$ för $n \in \mathbb{N}$

<u>bevis</u> : motsägelsebevis. anta att

$N \not\equiv S(N) \pmod 3$ och att N är <u>det minsta</u> sådana motexemplet

① N kan inte bara ha en siffra, eftersom $N = S(N)$ då.

② då har vi $N = 10a + b$, $a, b \in \mathbb{N}$, $0 \le b \le 9$

$$10a + b \not\equiv S(10a+b) \pmod 3$$

③ $$10a + b \not\equiv S(a) + b \pmod 3$$

④ $$10a \not\equiv S(a) \pmod 3$$

$$a \not\equiv S(a) \pmod 3 \qquad (10a \equiv a \pmod 3)$$

<u>men</u> : $a < N$, och $a \not\equiv S(a) \pmod 3$. <u>OMÖJLIGT</u>

invarianter

predikat över tillstånd

sant falsht

- $P(s_0)$ sant
- $\forall s, s'$ $P(s) \Rightarrow P(s')$

steg

steg-system

$\mathbb{N}$

tillstånd

initialtillstånd s_0

0

steg:

tillstånd → nästa tillstånd

+1

då vet vi P måste gälla i alla tillstånd nåbara med steg från initialtillståndet s_0

$\mathbb{N}$ 0 +1

enkel induktion

exempel

talsekvens   Conway   game of life

"look-and-say"

1, 11, 21, 1211, 111221, 312211, 13112221, ...

beskriv siffrorna
i den ordningen:

... k b ...

antalet   siffran

vilka siffror kan finnas med?

svar: 1, 2, 3

---

hitta en invariant

första försök: P(n) = "n har bara siffror 1-3"

P(k) ⇒ P(k') ?   nej: motexempel:
P(111123)
men ¬P(411213)

Låt $P(n)$ = "n innehåller bara siffor 1-3
OCH
n har inga upprepningar fler än 3"

$P(1)$: innehåller bara 1, inga upprepningar fler än 1. ok

$P(k) \Rightarrow P(k')$:

anta : • k innehåller bara 1-3
• k har inga upprepningar > 3

visa : k' innehåller bara 1-3

$k' = \ldots n\, b \ldots$

upprepningar i k 1-3

kommer från k 1-3

k' inga upprepningar > 3

olika

$k' = \ldots n_1 b_1 n_2 b_2 n_3 b_3 \ldots$

olika

$n_1 b_1 n_2 b_2$ kan inte vara lika

$b_1 n_2 b_2 n_3$ kan inte vara lika

alltså, P invariant