God Morgon!

POPULAR DEMAND

fredag? kl. 10:00 - 11:00

"övning"

maila om ni vill att detta händer!

talteori

- primtal
- moduloräkning

induktion

- enkel induktion med $\leq$
- stark induktion

sannolikhet (lite)

extra övning LV4

finns det $n \in \mathbb{N}$ så att $\{n, n+1, n+2, n+3, n+4, n+5\}$

kan delas upp i 2 mängder A och B

så att produkten av alla tal i A

är lika med produkten av alla tal i B?

t."ex." $15 \cdot 13 = 11 \cdot 12 \cdot 14 \cdot 10$ (n=10)

fungerar ej tyvärr

t.ex. n=2

2, 3, 4, 5, 6, 7

A vs. B → omöjligt p.g.a. 7

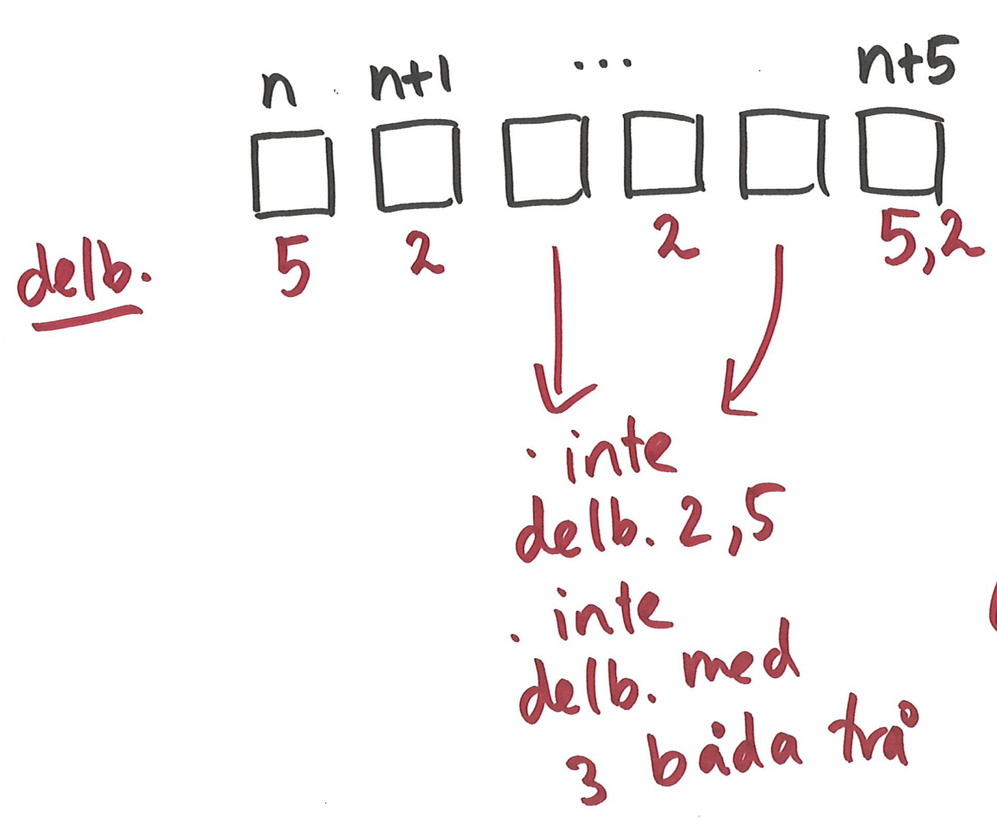
detta går inte

svar: nej

bevis?

bevis: • inget tal i $\{n, \dots, n+5\}$ kan ha en primfaktor 7 eller större. (I så fall skulle det talet vara det enda talet med den faktorn).

$\Rightarrow$ alla tal i $\{n, \dots, n+5\}$ får bara ha primfaktorer 2, 3, 5.



· precis 3 tal jämna (primfaktor 2)

· precis 2 tal ~~udda~~ primfaktor 3

1 dubbelt (delbart med 2 och 3)

OMÖJLIGT

RSA - krypto

$N = p \cdot q$ $\quad p, q$ primtal $\quad p \neq q$

om $\quad a \equiv b \pmod{p}$ och $a \equiv b \pmod{q}$ **då** $\quad a \equiv b \pmod{N}$, $N = p \cdot q$

bevis. vi vet $\quad a - b = k_1 \cdot p$ för något k_1

$a - b = k_2 \cdot q$ för något k_2

$p \mid (a-b)$, dvs. $p \mid k_2 \cdot q$ som betyder att

– eller –

$p \mid k_2$ $\quad$ $p \mid q$

$k_2 = k_3 \cdot p$ (för något k_3) $\quad$ går ej, $p \neq q$

$a - b = k_2 \cdot q = k_3 \cdot p \cdot q$, m.a.o. $a \equiv b \pmod{p \cdot q}$ $\square$

induktion ex. 1

visa: $3^n \leq n!$ för $n \geq 7$

bevis: med induktion över n

Låt $P(n) =$ "$3^n \leq n!$"

basfall: $P(7)$: $3^7 = 2187 \leq 5040 = 7!$ ok

$3^6 = 729$
$6! = 720$

stegfall: $P(k) \Rightarrow P(k+1)$, för $k \geq 7$

anta: $P(k)$: $3^k \leq k!$ (I.H.)

visa: $P(k+1)$: $3^{k+1} \leq (k+1)!$

$$
\begin{aligned}
3^{k+1} &= 3 \cdot 3^k && \\
&\leq 3 \cdot k! && \text{(I.H.)} \\
&\leq (k+1) \cdot k! && \text{(eftersom } k \geq 7\text{)} \\
&= (k+1)! && \text{(def. !)}
\end{aligned}
$$

□

induktion ex.2

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

$$f(n) = \begin{cases} 0 & , \text{om } n \leq 1 \\ 1 + f(n-2) & , \text{om } n \geq 2 \end{cases}$$

{ $\lfloor x \rfloor$ = runda ner x }

n	f(n)
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3
8	4
9	4
⋮	⋮

visa : $f(n) = \lfloor \frac{n}{2} \rfloor$, för $n \in \mathbb{N}$

bevis : med STARK induktion över n

Låt $P(n) =$ " $f(n) = \lfloor \frac{n}{2} \rfloor$ "

basfall : $P(0)$: $f(0) = 0 = \lfloor \frac{0}{2} \rfloor$ ok

$P(1)$: $f(1) = 0 = \lfloor \frac{1}{2} \rfloor$ ok

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

.... $f(k+1) = 1 + f(k-1)$ ...

behöver något starkare

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

anta: $P(i)$: $f(i) = \lfloor \frac{i}{2} \rfloor$ för $0 \leq i \leq k$ (I.H.)

visa: $P(k+1)$: $f(k+1) = \lfloor \frac{k+1}{2} \rfloor$

$$f(k+1) = 1 + f(k+1-2) \quad \text{(def. } f\text{, } k+1 \geq 2\text{)}$$

$$= 1 + f(k-1)$$

$$= 1 + \lfloor \frac{k-1}{2} \rfloor \quad \text{(I.H. } i = k-1\text{)}$$

(falluppdelning)

k-1 jämn

$$= 1 + \frac{k-1}{2}$$

$$= \frac{2}{2} + \frac{k-1}{2}$$

$$= \frac{k+1}{2}$$

$$= \lfloor \frac{k+1}{2} \rfloor \quad \text{(k+1 jämn)}$$

k-1 udda

$$= 1 + \frac{k-1}{2} - \frac{1}{2}$$

$$= \frac{k}{2}$$

$$= \frac{k+1}{2} - \frac{1}{2}$$

$$= \lfloor \frac{k+1}{2} \rfloor \quad \text{(k+1 udda)}$$

□

$$1 + \left\lfloor \frac{k-1}{2} \right\rfloor = \frac{2}{2} + \left\lfloor \frac{k-1}{2} \right\rfloor$$

$$\stackrel{?}{=} \left\lfloor \frac{k+1}{2} \right\rfloor$$

STRAFF(k-1)

$$1 + \left\lfloor \frac{k-1}{2} \right\rfloor = 1 + \frac{k-1}{2} - \text{STRAFF}(k-1)$$

$$= \frac{2}{2} + \frac{k-1}{2} - \text{STRAFF}(k-1)$$

$$= \frac{k+1}{2} - \text{STRAFF}(k-1)$$

$$= \frac{k+1}{2} - \text{STRAFF}(k+1)$$

$$= \left\lfloor \frac{k+1}{2} \right\rfloor$$

alternativt bevis: kortare, men (kanske) svårare att förstå?

Sannolikhet

$$p = \frac{G}{T}$$

G ← antalet "fall" man är intresserad av

T ← totala antalet "fall"

slå tärning:

sannolikhet att slå 6?

$G = 1$ $\quad T = 6$

$p = \frac{1}{6}$

2 möjligheter

slå sexa — slå ingen sexa

$T = 2$

$G = 1$

$p = \frac{1}{2}$

FEL!!!

exempel sannolikhet

3 kort:

blå + blå	blå + röd	röd + röd

väljs 1 kort slumpmässigt

visar 1 sida: röd

sannolikheten att andra sidan är blå?

finns 6 olika sidor, lika sannolika

röd, alltså 3 fall kvar:

1. röd - röd
2. röd - röd
3. röd - blå

$p = \frac{2}{3}$ för röd

50% förstås? NEJ!

G/T

Monty Hall

- 3 dörrar, mycket pengar bakom 1 dörr
  A B C — de andra 2 är tomma
- du väljer en dörr A — sannolikheten att du valt rätt? $\frac{1}{3}$
- nu öppnar de en annan dörr, som är tom
- får erbjudandet att byta dörr. **ska du?**

$\frac{1}{3}$ rätt dörr — inte byta

$\frac{2}{3}$ fel dörr — A ~~B~~ C — alltid byta

du vinner!