Mattehjälpen

Crash Course

TATA82 Diskret matematik

VT2019 – CC #1

Induktionsbevis

- Alltid en uppgift på tenta
- Standardiserad lösningsgång

Metod

1) Visa att påståendet gäller för basfallet, ex. $n=1$
2) Antag att påståendet gäller för något tal, ex. $n=p$
3) Visa att, givet (2) så gäller påståendet för $n=p+1$
4) Induktionsprincipen ger då att påståendet gäller för alla n

Exempel Visa att $1+2+\dots+n = \frac{n(n+1)}{2}$, $n \geq 1$

Lösning

1) Visa för basfall, $n=1$:

$$VL = 1$$
$$HL = \frac{1(1+1)}{2} = \frac{2}{2} = 1$$
$$VL = HL \quad \text{VSV} \blacksquare$$

Smidigt att dela upp i VL och HL!

2) Antag att det gäller för $n=p$, $p \geq 1$

$$1+2+\dots+p = \frac{p(p+1)}{2} \qquad (*)$$

3) Visa för $n=p+1$

Vill visa $1+2+\dots+p+p+1 = \frac{(p+1)[(p+1)+1]}{2}$

$$VL = 1+2+\dots+p+p+1$$
$$= / 1+2+\dots+p = \frac{p(p+1)}{2} \text{ enligt } (*) /$$
$$= \frac{p(p+1)}{2} + p+1$$
$$= \frac{p^2+3p+2}{2}$$

Här används induktionsantagandet

Viktigt steg!

3) forts.

$$HL = \frac{(p+1)[(p+1)+1]}{2}$$

$$= \frac{(p+1)(p+2)}{2}$$

$$= \frac{p^2+3p+2}{2}$$

$VL = HL$ VSV ■

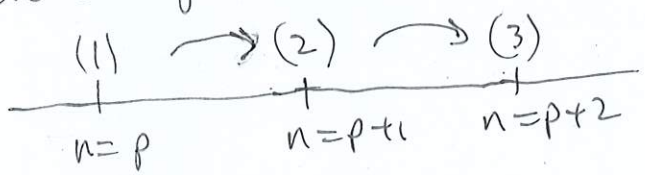
4) Enligt Induktionsprincipen (IP) har vi visat att

$$1+2+\dots+n = \frac{n(n+1)}{2} \quad \text{för } n \geq 1.$$

<u>Anmärkning</u>

Vi visar att det gäller för $n=p \Rightarrow$ gäller för $n=p+1$

Men då gäller också för $n=p+1 \Rightarrow$ gäller för $n=p+2$ osv.



$\boxed{\text{Exempel}}$ 2017-10-28 #1

Visa att $\displaystyle\sum_{k=1}^{n} (k+1)k^2 = \frac{n(n+1)(n+2)(3n+1)}{12}$, $n \geq 1$

<u>Lösning</u>

1) Visa för basfall, $n=1$:

$$VL = \sum_{k=1}^{1} (k+1)k^2 = (1+1)1^2 = 2$$

summa med endast 1 term

$$HL = \frac{1(1+1)(1+2)(3\cdot 1+1)}{12} = \frac{1\cdot 2\cdot 3\cdot 4}{12} = 2$$

$VL = HL$ VSV ■

2) Antag att det gäller för $n=p+1$

$$\sum_{k=1}^{p}(k+1)k^2 = \frac{p(p+1)(p+2)(3p+1)}{12}, \quad p \geq 1 \qquad (*)$$

3) Visa för $n=p+1$:

Vill visa $\displaystyle\sum_{k=1}^{p+1}(k+1)k^2 = \frac{(p+1)[(p+1)+1][(p+1)+2][3(p+1)+1]}{12}$

$$VL = \sum_{k=1}^{p+1}(k+1)k^2 = \underbrace{\sum_{k=1}^{p}(k+1)k^2}_{\text{"ursprunglig summa"}} + \underbrace{\sum_{k=p+1}^{p+1}(k+1)k^2}_{\text{"summa av k+1:te termen"}}$$

Dela upp summor är användbart!

$$= \left| \sum_{k=1}^{p}(k+1)k^2 = \frac{p(p+1)(p+2)(3p+1)}{12} \right|$$

enligt $(*)$

Här används induktionsantagandet viktigt steg!

$$= \frac{p(p+1)(p+2)(3p+1)}{12} + [(p+1)+1](p+1)^2$$

$$= \frac{p(p+1)(p+2)(3p+1)}{12} + \frac{12(p+2)(p+1)^2}{2}$$

Bryt ut gemensamma faktorer för tydlighet

$$= \frac{(p+1)(p+2)}{12}\left[p(3p+1) + 12(p+1)\right]$$

$$= \frac{(p+1)(p+2)}{12}\left[3p^2 + 13p + 12\right]$$

$$HL = \frac{(p+1)[(p+1)+1][(p+1)+2][3(p+1)+1]}{12} =$$

$$= \frac{(p+1)(p+2)(p+3)(3p+4)}{12} = \frac{(p+1)(p+2)}{12}\left[(p+3)(3p+4)\right]$$

$$= \frac{(p+1)(p+2)}{12}\left[3p^2 + 13p + 12\right]$$

Bryt ut samma gemensamma faktorer som ovan

$VL = HL$ vsv ∎

4) Enligt induktionsprincipen (IP) har vi visat att

$$\sum_{k=1}^{n} (k+1)k^2 = \frac{n(n+1)(n+2)(3n+1)}{12}, \quad n \geq 1$$

Modulo räkning

i) $a \equiv b \mod m \iff ax = bx \mod m$, $x \in$ heltal

modulo "skalar" med multiplikation

ii) $a \equiv b \mod m \iff (a \mod m) \equiv b \mod m$

"reducering" modulo m för ändrar inte modulo m

iii) $a \equiv b \mod m \iff a^n \equiv b^n \mod m$, $n \in$ heltal

modulo "bevaras" vid exponentiation

iv) $a^n \equiv b \mod m \iff (a \mod m)^n \equiv b \mod m$

Exempel 2017-10-28 #6

Visa att $(1^2)^n + (3^2)^n + (5^2)^n + (7^2)^n + (9^2)^n + (11^2)^n + (13^2)^n + (15^2)^n \equiv 0 \mod 8$

Lösning

Reducera alla termer mod 8, ty iv) ger att

- $a^n \equiv b \mod 8 \iff (a \mod 8)^n \equiv b \mod 8$
- $1^2 \equiv 1 \mod 8 \iff (1^2)^n \equiv 1^n \mod 8$
- $3^2 \equiv 9 \equiv 1 \mod 8 \iff (3^2)^n \equiv 1^n \mod 8$
- $5^2 \equiv 25 \equiv 1 \mod 8 \iff (5^2)^n \equiv 1^n \mod 8$
- p.s.s för 7^2, 9^2, 11^2, 13^2, 15^2 ... $\equiv 1^n \mod 8$
- $(1^2)^n + (3^2)^n + (5^2)^n + (7^2)^n + (9^2)^n + (11^2)^n + (13^2)^n + (15^2)^n$

$\equiv 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 \equiv 8 \equiv 0 \mod 8$

VSV ∎

Modulo räkning, forts

Exempel 2015-08-20 #6

Hitta minsta positiva heltalet x som uppfyller:

$$x^2+x \equiv 1 \mod 5$$
$$x^2+x \equiv 5 \mod 7$$
$$x^2+x \equiv 3 \mod 13$$

Lösning

- $x^2+x \equiv 1 \mod 5$ $\Rightarrow$ behöver endast testa $x = 0, 1, 2, 3, 4$ ty

  $x = 5 \equiv 0 \mod 5$

  $x = 6 \equiv 1 \mod 5$

  x^2+x där $x=6$ ger enligt i(v)) och ii)

  $\underbrace{(x \bmod 5)^2}_{\equiv 1^2} + \underbrace{(x \bmod 5)}_{\equiv 1}$ dvs "$x=1$"

- Löser $x^2+x \equiv 1 \mod 5$

  $0^2+0 \equiv 0 \not\equiv 1 \mod 5$

  $1^2+1 \equiv 2 \not\equiv 1 \mod 5$

  $2^2+2 \equiv 6 \equiv 1 \mod 5$ $\Rightarrow$ $x \equiv 2 \mod 5$

- Löser $x^2+x \equiv 5 \mod 7$ Här behöver vi testa $x = 0, \dots, 6$

  $0^2+0 \equiv 0 \not\equiv 5 \mod 7$

  $\vdots$

  $3^2+3 \equiv 12 \equiv 5 \mod 7$ $\Rightarrow$ $x \equiv 3 \mod 7$

- Löser $x^2+x \equiv 3 \mod 13$ Här behöver vi testa $x = 0, \dots, 12$

  $0^2+0 \equiv 0 \not\equiv 3 \mod 13$

  $\vdots$

  $6^2+6 \equiv 42 \equiv 3 \mod 13$ $\Rightarrow$ $x \equiv 6 \mod 13$

- Vi får att x ska uppfylla

$$\begin{cases} x \equiv 2 \mod 5 \\ x \equiv 3 \mod 7 \\ x \equiv 6 \mod 13 \end{cases} \Rightarrow \text{Lös med KRS !}$$

Kinesiska restsatsen (KRS)

Givet system av kongruenser

$$x \equiv b_1 \mod n_1$$
$$x \equiv b_2 \mod n_2$$
$$\vdots$$
$$x \equiv b_k \mod n_k$$

och $N = n_1 \times n_2 \times \dots \times n_k$

samt $N_i = \frac{N}{n_i}$, $i = 1, \dots, k$

samt $\underbrace{x_i \text{ lösningar}}_{\text{kallas multiplikativa inverser}}$ till $N_i x_i \equiv 1 \mod n_i$, $i = 1, \dots, k$

då är $x = b_1 N_1 x_1 + b_2 N_2 x_2 + \dots + b_k N_k x_k$ en lösning till systemet

Metod

1) Faktorisera N till n_i
2) Använd n_i för att bestämma N_i
3) Ta fram system av kongruenser
4) Beräkna b_i
5) Beräkna x_i
6) Sätt ihop delresultat för att lösa ut x

Exempel 2016-08-18 #5

Bestäm $73^{1567} \mod 990$, dvs $x = 73^{1567} \mod 990$

Lösning

I stället för att beräkna mod 990 (för stort!), beräkna rester för faktorerna till 990 mha KRS → sätt ihop
→ få svaret mod 990

Lösning, forts.

1) Låt $N = 990$, Faktorisera N till n_i

$$990 = 9 \cdot 110$$
$$= \underbrace{9}_{n_1} \cdot \underbrace{5}_{n_2} \cdot \underbrace{2}_{n_3} \cdot \underbrace{1}_{n_4}$$

Eftersom $N = n_1 \times n_2 \times n_3 \times n_4$

2) Använd n_i till att bestämma N_i

$$\begin{cases} n_1 = 9 \\ n_2 = 5 \\ n_3 = 2 \\ n_4 = 11 \end{cases} \Rightarrow \begin{cases} N_1 = N/n_1 = 990/9 = 110 \\ N_2 = N/n_2 = 990/5 = 198 \\ N_3 = N/n_3 = 990/2 = 495 \\ N_4 = N/n_4 = 990/11 = 90 \end{cases}$$

3) Ta fram system av kongruenser

Låt $x = 73^{1567}$

För KRS ska systemet vara
$$\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ x \equiv b_3 \bmod n_3 \\ x \equiv b_4 \bmod n_4 \end{cases} \Rightarrow \begin{cases} x \equiv b_1 \bmod 9 \\ x \equiv b_2 \bmod 5 \\ x \equiv b_3 \bmod 2 \\ x \equiv b_4 \bmod 11 \end{cases}$$

4) Beräkna b_i

$\underline{b_1}$: Vi har $x = 73^{1567}$ och $x \equiv b_1 \bmod 9$

$$\Rightarrow 73^{1567} \equiv b_1 \bmod 9$$

$$73^{1567} \equiv (73 \bmod 9)^{1567} \equiv 1^{1567} \equiv 1 \bmod 9$$

$$\therefore b_1 = 1 \quad \blacksquare$$

Lösning, forts

b_2: $73^{1567} \equiv b_2 \mod 5$

$73^{1567} \equiv (73 \mod 5)^{1567} \equiv 3^{1567} \mod 5$

Vi ser att $3^2 \equiv 9 \equiv -1 \mod 5$

Idé: "ersätt basen"

$3^{1567} \equiv (3^2)^{783} \cdot 3^1 \equiv (-1)^{783} \cdot 3^1 \equiv (-1) \cdot 3 \equiv -3 \equiv 2 \mod 5$

$\therefore b_2 = 2$ ∎

b_3: $73^{1567} \equiv b_3 \mod 2$

$73^{1567} \equiv (73 \mod 2)^{1567} \equiv 1^{1567} \equiv 1 \mod 2$

$\therefore b_3 = 1$ ∎

b_4: $73^{1567} \equiv b_4 \mod 11$

$73^{1567} \equiv (73 \mod 11)^{1567} \equiv 7^{1567} \mod 11$

Vi ser att $7^2 \equiv 49 \equiv 5 \mod 11$

$7^3 \equiv 5 \cdot 7 \equiv 35 \equiv 2 \mod 11$

$7^4 \equiv 2 \cdot 7 \equiv 14 \equiv 3 \mod 11$

$7^5 \equiv 3 \cdot 7 \equiv 21 \equiv -1 \mod 11$

Ersätt basen!

$7^{1567} \equiv (7^5)^{313} \cdot 7^2 \equiv (-1)^{313} \cdot 7^2$

$\equiv -1 \cdot 7^2 \equiv -49 \equiv 6 \mod 11$

$\therefore b_4 = 6$ ∎

Sammanfattningsvis vet vi:

$$\begin{cases} x \equiv 1 \mod 9 & , N_1 = 110 \\ x \equiv 2 \mod 5 & , N_2 = 198 \\ x \equiv 1 \mod 2 & , N_3 = 495 \\ x \equiv 6 \mod 11 & , N_4 = 90 \end{cases}$$

Söker nu x_i →

Lösning, forts

5) Beräkna x_i från $N_i x_i \equiv 1 \mod n_i$

x_1: $\begin{cases} N_1 = 110 \\ n_1 = 9 \end{cases}$ $\Rightarrow$ $110 x_1 \equiv 1 \mod 9$

$\Leftrightarrow (110 \mod 9) x_1 \equiv 1 \mod 9$

$\Leftrightarrow 2 x_1 \equiv 1 \mod 9$

Här kan man använda Euklides algoritm (men vi gör inte det)

"Skala upp" med lämpligt heltal så att VL $\equiv 1 \mod 9$

$\Leftrightarrow 5 \cdot 2 \, x_1 \equiv 1 \cdot 5 \mod 9$

$\Leftrightarrow \underbrace{10}_{\equiv 1 \mod 9} x_1 \equiv 5 \mod 9$

$\Leftrightarrow x_1 \equiv 5 \mod 9$ ∎

x_2: $\begin{cases} N_2 = 198 \\ n_2 = 5 \end{cases}$ $\Rightarrow$ $198 x_2 \equiv 1 \mod 5$

$\Leftrightarrow (198 \mod 5) x_2 \equiv 1 \mod 5$

$\Leftrightarrow 3 x_2 \equiv 1 \mod 5$

$\Leftrightarrow 2 \cdot 3 \, x_2 \equiv 1 \cdot 2 \mod 5$

$\Leftrightarrow 6 x_2 \equiv 2 \mod 5$

$\Leftrightarrow x_2 \equiv 2 \mod 5$ ∎

x_3: $\begin{cases} N_3 = 495 \\ n_3 = 2 \end{cases}$ $\Rightarrow$ $495 x_3 \equiv 1 \mod 2$

$\Leftrightarrow (495 \mod 2) x_3 \equiv 1 \mod 2$

$x_3 \equiv 1 \mod 2$ ∎

x_4: $\begin{cases} N_4 = 90 \\ n_4 = 11 \end{cases}$ $\Rightarrow$ $90 x_4 \equiv 1 \mod 11$

$\Leftrightarrow (90 \mod 11) x_4 \equiv 1 \mod 11$

$\Leftrightarrow 2 x_4 \equiv 1 \mod 11$

$\Leftrightarrow 6 \cdot 2 \, x_4 \equiv 1 \cdot 6 \mod 11$

$\Leftrightarrow x_4 \equiv 6 \mod 11$ ∎

Lösning, forts

6) Sätt ihop delresultat

Vi vet $x \equiv b_1 N_1 x_1 + b_2 N_2 x_2 + b_3 N_3 x_3 + b_4 N_4 x_4$ lösning till $x \equiv 73^{1567} \bmod 990$

Vi vet:

$b_1 = 1$	$N_1 = 110$	$x_1 = 5$
$b_2 = 2$	$N_2 = 198$	$x_2 = 2$
$b_3 = 1$	$N_3 = 495$	$x_3 = 1$
$b_4 = 6$	$N_4 = 90$	$x_4 = 6$

$$\therefore x = 1 \cdot 110 \cdot 5 + 2 \cdot 198 \cdot 2 + 1 \cdot 495 \cdot 1 + 6 \cdot 90 \cdot 6$$

$$= 5077 \equiv 127 \bmod 990$$

Glöm ej reducera till minsta lösning modulo 990!