

3.53 a

$$1 \cdot x + 1 \cdot y = 17 \quad (*)$$

a) lös ekv. med den vanliga metoden.

$$1 = \underbrace{0}_{x} \cdot 1 + \underbrace{1}_{y} \cdot 1$$

Partikulära lösningen är
 $x = 0, y = 17$

$$x + y = 0$$

homogena
ekv.

$$x = k$$
$$y = -k, \quad k \in \mathbb{Z}$$

$$\begin{aligned} x &= k \\ y &= 17 - k \end{aligned}$$

allmänna
lösningen
till (*)

b) på ett annat sätt

skriv

$$y = 17 - x,$$

x väljs fritt från $\mathbb{Z}$.

4.45 sid 98

visa att

$$\sum_{k=1}^m (-k)^3 = -\frac{m^2(m+1)^2}{4}$$

$(-k)^3$ är inget annat än $-k^3$
dvs

$$-\sum k^3 = -\frac{m^2(m+1)^2}{4}$$

eller

$$\sum_{k=1}^m k^3 = \frac{m^2(m+1)^2}{4}$$

m=1: $1^3 = \frac{(1+1)^2 \cdot 1}{4}$

m=2: $1^3 + 2^3 = \frac{2^2 \cdot 3^2}{4}$

m=3: $1^3 + 2^3 + 3^3 = \frac{3^2 \cdot 4^2}{4}$

...

} oändligt
många påståen.
den.

$$1^3 + 2^3 + \dots + (m-1)^3 + m^3 = \frac{1}{4} \cdot m^2 \cdot (m+1)^2.$$

IND. BAS $m=1$; $1^3 = \frac{1^2 \cdot 2^2}{4}$ RÄTT.

IND. HYPOTES:

Sant för något p :

$$VL_p = 1^3 + 2^3 + \dots + p^3 = \frac{1}{4} \cdot p^2 \cdot (p+1)^2 = HL_p$$

undersök $p+1$:

$$VL_{p+1} = \boxed{1^3 + 2^3 + \dots + p^3} + (p+1)^3 = \frac{1}{4} p^2 (p+1)^2 + (p+1)^3$$

$VL_p = HL_p$ enligt indhyp.

$$\begin{aligned}
& \frac{1}{4} p^2 (p+1)^2 + (p+1)^3 = \\
& = (p+1)^2 \left(\frac{p^2}{4} + (p+1) \right) = \\
& = \frac{(p+1)^2 (p+2)^2}{4} = H_{p+1}
\end{aligned}$$

enligt ind. principen är vi klara.

3.40 sid 66, bok 2

$$n = 91, e = 5. \text{ hitta } d.$$

$$n = 13 \cdot 7 \text{ alltså } p = 13, q = 7$$

$$m = (p-1)(q-1) = 12 \cdot 6 = 72.$$

$$ed \equiv 1 \pmod{72};$$

$$ed - 1 = 72 \cdot k \text{ för något } k.$$

$$1 = ed - 72k; \quad 1 = 5d - 72k;$$

$$\boxed{\begin{matrix} k=2 \\ d=29 \end{matrix}}$$

$$n = 35, e = 7$$

$$p \cdot q = 7 \cdot 5 = 35$$

$$m = (p-1)(q-1) = 24$$

↓ löses ut

$$ed = 7d \equiv 1 \pmod{24}$$

$$d = 7 \text{ funger}$$

$$7d + 24k = 1$$

Euklides
på 24 och 7

och
Euklides
baktvängs
sen.

Elektronisk signatur från A
till B

$$A \xrightarrow{\text{Skickar}} e_B(d_A(m)) = k$$

B dekrypterar

$$e_A(d_B(k)) = m$$

B skickar 23 till A

$$e_A(d_B(23)) = (23^7 \bmod 35)^5 \bmod 91$$

$$23^7 = 23^{4+2+1} = 23^4 \cdot 23^2 \cdot 23$$

$$23 \bmod 35 = 23$$

$$(23)^2 = 529 = 4 \bmod 35$$

$$(23)^4 \equiv 4^2 = 16 \bmod 35$$

$$\begin{array}{r} 529 \overline{) 35} \\ \underline{35} \\ 179 \\ \underline{175} \\ 4 \end{array}$$

$$23^7 \equiv 16 \cdot 4 \cdot 23 = 1472 \equiv 2 \bmod 35$$

$$2^5 \bmod 91 \text{ är } 32.$$