

V-04

①

$$\begin{aligned} a) \quad 297 &= 90 \cdot 3 + 27 \\ 90 &= 27 \cdot 3 + 9 \\ 27 &= 9 \cdot 3 \end{aligned}$$

$$\text{Dvs } \gcd(90, 297) = 9$$

$$\begin{aligned} 9 &= 90 - 27 \cdot 3 = 90 - (297 - 90 \cdot 3) \cdot 3 \\ &= 90 \cdot 10 + 297 \cdot (-3) \end{aligned}$$

b) La N være det betalte beløbet. Vi må ha $N = 90 \cdot a + 297 \cdot b$ hvor a er beløjet professorerne må betale og b er beløjet studentene må betale. Denne ligningen har en løsning hvis og bare hvis $\gcd(90, 297) \mid N$. Hvis vi skal ha $2380 \leq N \leq 2390$, er 2385 det eneste tallet som er delelig med 9.

c) Vi har $9 = 90 \cdot 10 + 297 \cdot (-3) \Rightarrow$
(ganger med 265) $2385 = 90 \cdot 2650 + 297 \cdot (-795)$
Dermed er den generelle løsningen gitt
v. $a = 2650 + 33t$, $b = -795 - 10t$ hvor
 $t \in \mathbb{Z}$. Siden både a og b skal være
positive, må $t = 80$, og $a = 10$, $b = 5$.

- ② Vi får $\phi(n) = \phi(5) \cdot \phi(13) = 4 \cdot 12 = 48$.
Vi finner d ved å løse kongruensen
 $ed \equiv 1 \pmod{\phi(n)}$, dvs $11d \equiv 1 \pmod{48}$.
Da må $d \equiv 35 \pmod{48}$. Dermed får
vi $\{n, d\} = \{65, 35\}$.

- ③ a) *Euler gir at $a^{\phi(n)} \equiv 1 \pmod{n}$ når
 $\gcd(a, n) = 1$. Dermed har vi
 $a \cdot a^{\phi(n)-1} \equiv 1 \pmod{n}$, og $a^{\phi(n)-1}$ er en invers
av a modulo n .
* Vi må løse $16x \equiv 1 \pmod{35}$.
 $x \equiv 11 \pmod{35}$ løser denne.

- b) Euler gir $a^{\phi(n)} \equiv 1 \pmod{n}$ når $\gcd(a, n) = 1$.
Siden $\gcd(80, 77) = 1$, får vi da $(\phi(77) = 6 \cdot 10$
 $= 60)$ $80^{241} \equiv (80^{60})^4 \cdot 80 \equiv 80 \equiv 3 \pmod{77}$.

- ④ a) Den er løslbar fordi $\gcd(63, 11) = 1 \nmid 1$.
Kongruensen er ekvivalent med
 $8x \equiv 1 \pmod{11}$. $x \equiv 7 \pmod{11}$ blir
da eneste løsning.

$$b) \begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 2 \pmod{9} \\ x \equiv 1 \pmod{11} \end{cases}$$

Den første kongruensen gir at

$$x = 2 + 7k. \text{ Da må}$$

$$\begin{cases} 2 + 7k \equiv 2 \pmod{9} \\ 2 + 7k \equiv 1 \pmod{11} \end{cases}, \text{ dvs.}$$

$$\begin{cases} 7k \equiv 0 \pmod{9} \\ 7k \equiv 10 \pmod{11} \end{cases}$$

Siden vi kan gange disse kongruensene gjennom med inversen til 7 (med de respektive modulur), 4 i den første og 8 i den andre, får vi

$$\begin{cases} k \equiv 0 \pmod{9} \\ k \equiv 3 \pmod{11} \end{cases}$$

Den første kongruensen gir

$$k = 9l \Rightarrow \text{Vi må ha } 9l \equiv 3 \pmod{11}.$$

Vi ganger gjennom med inversen til 9 mod. 11 (5) og får:

$$l \equiv 4 \pmod{11}, \text{ dvs. } l = 4 + 11m.$$

Dermed får vi

$$\begin{aligned} x &= 2 + 7k = 2 + 7(9l) = 2 + 63l \\ &= 2 + 63(4 + 11m) = 254 + 693m \end{aligned}$$

$$\text{, dvs. } x \equiv 254 \pmod{693}.$$