LØSNINGSFORSLAG EKSAMEN MA1301 VÅR 2004

Oppgave 1. (a) Euklids algoritme gir

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

Dette gir $\gcd(90, 297) = 9$. Arbeider vi oss bakover får vi

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

Vi kan derfor sette $a = 10$ og $b = -3$.

(b) Siden tallet 9 deler både 90 og 297, må 9 også dele den totale summen som ble betalt inn. Det eneste tallet mellom 2380 og 2390 som er delelig med 9 er 2385 (tverrsumtesten), så det ble betalt inn tilsammen 2385 kroner i inngangspenger.

(c) La x betegne prisen professorene måtte betale, og y prisen studentene måtte betale. Da får vi den Diofantiske ligningen

$$90x + 297y = 2385.$$

Siden $2385 = 9\cdot 265$ får vi fra (a) at

$$2385 = 90\cdot(10\cdot 265) + 297\cdot(-3\cdot 265) = 90\cdot 2650 + 297\cdot(-795),$$

så $x_0 = 2650, y_0 = -795$ er en løsning av ligningen. Da er alle løsningene av ligningen gitt ved

$$\begin{aligned} x &= x_0 + \frac{297}{9}t = 2650 + 33t \\ y &= y_0 - \frac{90}{9}t = -795 - 10t \end{aligned}$$

for $t \in \mathbb{Z}$. Inngangsprisene kan ikke være negative, så løsningen vi er ute etter tilfredsstiller ulikhetene $2650 + 33t \geq 0$ og $-795 - 10t \geq 0$. Den første av disse gir

$$t \geq \frac{-2650}{33} = \frac{-(33\cdot 80 + 10)}{33} \approx -80.3,$$

mens den andre gir

$$t \leq \frac{-795}{10} = -79.5.$$

Siden t skal være et heltall må vi ha $t = -80$, og dette gir

$$\begin{aligned} x &= 2650 + 33\cdot(-80) = 10 \\ y &= -795 - 10\cdot(-80) = 5. \end{aligned}$$

Oppgave 2. Tallet d skal tilfredsstille ulikheten $1 < d < \phi(65)$ og kongruensen $ed \equiv 1 (\bmod \phi(65))$, hvor ϕ er Eulers phi-funksjon. Siden $65 = 5 \cdot 13$ har vi $\phi(65) = (5-1) \cdot (13-1) = 48$, så den lineære kongruensen vi må løse er

$$11x \equiv 1 (\bmod 48).$$

Euklids algoritme gir

$$\begin{aligned} 48 &= 4 \cdot 11 + 4 \\ 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1, \end{aligned}$$

og arbeider vi oss bakover får vi

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (11 - 2 \cdot 4) \\ &= 3 \cdot 4 - 11 \\ &= 3 \cdot (48 - 4 \cdot 11) - 11 \\ &= 3 \cdot 48 - 13 \cdot 11. \end{aligned}$$

Ut i fra dette kan vi slutte at 48 deler $11 \cdot (-13) - 1$, dvs at $11 \cdot (-13) \equiv 1 (\bmod 48)$, så $x_0 = -13$ er en løsning av kongruensen. Da må vi ha $d = -13 + 48 = 35$, slik at den hemmelige dekrypteringsnøkkelen er gitt ved $\{n, d\} = \{65, 35\}$.

Oppgave 3. (a) Siden $\gcd(a, n) = 1$ gir Eulers Teorem at $a^{\phi(n)} \equiv 1 (\bmod n)$. Hvis vi skriver om kongruensen til $a \cdot a^{\phi(n)-1} \equiv 1 (\bmod n)$, ser vi at tallet $b = a^{\phi(n)-1}$ er en invers av a modulo n.

Vi bruker denne fremgangsmåten til å finne en invers av 16 modulo 35. Siden $35 = 5 \cdot 7$ har vi $\phi(35) = 4 \cdot 6 = 24$, så tallet 16^{23} er en invers av 16.

(b) Vi bruker Eulers Teorem nok en gang. Siden $\gcd(77, 80) = 1$ har vi $80^{\phi(77)} \equiv 1 (\bmod 77)$, med $\phi(77) = \phi(11 \cdot 7) = 60$. Dette gir $80^{60} \equiv 1 (\bmod 77)$, og opphøyer vi denne kongruensen i 4 får vi $80^{240} \equiv 1 (\bmod 77)$. Deretter multipliserer vi på begge sider med 80 og får $80^{241} \equiv 80 \equiv 3 (\bmod 77)$, så resten vi får er 3.

Oppgave 4. (a) Siden $\gcd(63, 11) = 1$ er kongruensen løsbar. Ved å bruke Euklids algoritme på tallene 63 og 11 for så å arbeide oss bakover, får vi $1 = 23 \cdot 11 - 4 \cdot 63$. Dette betyr at 11 deler $63 \cdot (-4) - 1$, dvs at $63 \cdot (-4) \equiv 1 (\bmod 11)$, så $x_0 = -4$ er en løsning av kongruensen. Da er alle løsningene gitt ved $x \equiv -4 (\bmod 11)$.

(b) Siden $7, 9$ og 11 er innbyrdes primiske, bruker vi det Kinesiske Restteorem. Vi setter $m_1 = 9 \cdot 11 = 99$, $m_2 = 7 \cdot 11 = 77$, $m_3 = 7 \cdot 9 = 63$ og løser

$$\begin{aligned} m_1 x_1 &\equiv 1 (\bmod 7) \leftrightarrow 99 x_1 &\equiv 1 (\bmod 7) \\ m_2 x_2 &\equiv 1 (\bmod 9) \leftrightarrow 77 x_2 &\equiv 1 (\bmod 9) \\ m_3 x_3 &\equiv 1 (\bmod 11) \leftrightarrow 63 x_3 &\equiv 1 (\bmod 11). \end{aligned}$$

Vi ser direkte at vi kan sette $x_1 = 1, x_2 = 2$, og fra (a) har vi at vi kan sette $x_3 = -4$. Dette gir

$$\overline{x} = 2 \cdot m_1 x_1 + 2 \cdot m_2 x_2 + 1 \cdot m_3 x_3 = 2 \cdot 99 \cdot 1 + 2 \cdot 77 \cdot 2 + 1 \cdot 63 \cdot (-4) = 254,$$

så alle løsningene av systemet er gitt ved $x \equiv 254 (\bmod 7 \cdot 9 \cdot 11)$, dvs $x \equiv 254 (\bmod 693)$.

Oppgave 5. (a) Vi benytter oss av induksjonsprinsippet. Siden $\frac{\alpha - \beta}{\alpha - \beta} = 1$ og $\frac{\alpha^2 - \beta^2}{\alpha - \beta} = \frac{(\alpha - \beta)(\alpha + \beta)}{\alpha - \beta} = \alpha + \beta = 1$, stemmer påstanden for $n = 1$ og $n = 2$. La nå $n \geq 3$, og anta påstanden er vist for alle $n < 3$. Da har vi

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \\ &= \frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + \frac{\alpha^{n-2} - \beta^{n-2}}{\alpha - \beta} \\ &= \frac{(\alpha^{n-1} + \alpha^{n-2}) - (\beta^{n-1} + \beta^{n-2})}{\alpha - \beta}. \end{aligned}$$

Siden α og β er røtter i polynomet $x^2 - x - 1$ har vi $\alpha^2 = \alpha + 1$ og $\beta^2 = \beta + 1$, og multipliserer vi disse likhetene med henholdsvis α^{n-2} og β^{n-2} får vi $\alpha^n = \alpha^{n-1} + \alpha^{n-2}$ og $\beta^n = \beta^{n-1} + \beta^{n-2}$. Derfor gjelder

$$f_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

og påstanden er derfor vist.

(b) Siden $\frac{\alpha^0 - \beta^0}{\alpha - \beta} = 0 = f_0$ har vi

$$\begin{aligned} \sum_{i=0}^{n} \binom{n}{i} f_i &= \sum_{i=0}^{n} \binom{n}{i} \frac{\alpha^i - \beta^i}{\alpha - \beta} \\ &= \frac{1}{\alpha - \beta} \left(\sum_{i=0}^{n} \binom{n}{i} \alpha^i - \sum_{i=0}^{n} \binom{n}{i} \beta^i \right) \\ &= \frac{1}{\alpha - \beta} \left(\sum_{i=0}^{n} \binom{n}{i} 1^{n-i} \alpha^i - \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} \beta^i \right) \\ &= \frac{(1+\alpha)^n - (1+\beta)^n}{\alpha - \beta}, \end{aligned}$$

hvor den siste likheten kommer fra binomialformelen. Men $1+\alpha = \alpha^2$ og $1+\beta = \beta^2$, og dette gir

$$\begin{aligned} \sum_{i=0}^{n} \binom{n}{i} f_i &= \frac{(\alpha^2)^n - (\beta^2)^n}{\alpha - \beta} \\ &= \frac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta} \\ &= f_{2n}. \end{aligned}$$