LØSNINGSFORSLAG EKSAMEN MA1301/MA6301/ HØST 2004

Oppgave 1. La x, y, z være hhv antall stipendiater, professorer og administrativt ansatte ved instituttet. Opplysningene gitt er følgende:

$$\begin{aligned} 30x + 70y &= 5060 \\ x + y + z &= 118 \\ x &\geq y + 10 \\ z &\geq 10. \end{aligned}$$

Man må løse den Diofantiske ligningen først. Vi har $\gcd(30, 70) = 10 = 30 \cdot (-2) + 70 \cdot 1$, som gir $5060 = 10 \cdot 506 = 30 \cdot (-1012) + 70 \cdot 506$. Derfor er

$$x_0 = -1012, y_0 = 506$$

en løsning av $30x + 70y = 5060$. Da er alle løsningene gitt ved

$$\begin{aligned} x &= x_0 + \frac{70}{\gcd(30,70)} t = 7t - 1012 \\ y &= y_0 - \frac{30}{\gcd(30,70)} t = 506 - 3t \end{aligned}$$

for $t \in \mathbb{Z}$. Ulikheten $x \geq y + 10$ gir $10t \geq 1528$, dvs $t \geq 152,8$. Ulikheten $z \geq 10$ gir $x + y + z \geq x + y + 10$, dvs $118 \geq x + y + 10$, som gir $614 \geq 4t$, dvs $153,5 \geq t$. Siden t er et heltall må vi da ha $t = 153$. Dette gir

$$\begin{aligned} y &= 506 - 3 \cdot 153 = 47 \\ x &= 7 \cdot 153 - 1012 = 59 \\ z &= 118 - 47 - 59 = 12. \end{aligned}$$

Oppgave 2. Siden $\gcd(3, 100) = 1$ gir Eulers Teorem at $3^{\phi(100)} \equiv 1 (\bmod 100)$. Vi har $100 = 2^2 \cdot 5^2$, så $\phi(100) = 40$, og derfor får vi

$$3^{40} \equiv 1 (\bmod 100).$$

Hvis $n \geq 1$ får vi da $3^{40n} \equiv 1 (\bmod 100)$, som igjen gir

$$3^{40n+1} \equiv 3 (\bmod 100).$$

Da får vi

$$\sum_{n=1}^{10} 3^{40n+1} \equiv 10 \cdot 3 \equiv 30 (\bmod 100),$$

så de to siste sifrene er 30.

Oppgave 3. Vi bruker det Kinesiske Restteorem. Setter

$$m_1 = 6 \cdot 7 = 42, \qquad m_2 = 5 \cdot 7 = 35, \qquad m_3 = 5 \cdot 6 = 30,$$

og løser de tre kongruensene

$$\begin{aligned} m_1 x_1 \equiv 1 (\bmod 5) \quad &\rightarrow \quad 42 x_1 \equiv 1 (\bmod 5) \\ m_2 x_2 \equiv 1 (\bmod 6) \quad &\rightarrow \quad 35 x_2 \equiv 1 (\bmod 6) \\ m_3 x_3 \equiv 1 (\bmod 7) \quad &\rightarrow \quad 30 x_3 \equiv 1 (\bmod 7). \end{aligned}$$

Tre tall som passer inn er $x_1 = 3, x_2 = -1, x_3 = -3$, som gir

$$\begin{aligned}\bar{x} &= m_1x_1 \cdot 2 + m_2x_2 \cdot 1 + m_3x_3 \cdot 1 \\ &= 42 \cdot 3 \cdot 2 + 35 \cdot (-1) \cdot 1 + 30 \cdot (-3) \cdot 1 \\ &= 127.\end{aligned}$$

Løsningen av systemet blir derfor

$$x \equiv 127 \pmod{210}$$

hvor $210 = 5 \cdot 6 \cdot 7$.

Oppgave 4. Wilsons Teorem: for alle primtall p gjelder $(p-1)! \equiv -1 \pmod p$. Siden 37 er et primtall får vi da at $36! \equiv -1 \pmod{37}$, og fra denne og kongruensen $-1 \equiv 36 \pmod{37}$ fås kongruensen

$$36! \equiv 36 \pmod{37}.$$

Her er 36 en felles faktor på begge sider, og siden $\gcd(36, 37) = 1$ kan vi dele ut og få $35! \equiv 1 \pmod{37}$. Trekker vi fra 35 på begge sider får vi da

$$35! - 35 \equiv 1 - 35 \equiv 3 \pmod{37},$$

så vi får 3 til rest.

Oppgave 5. (a) Vi må finne tallet d som tilfredsstiller $1 < d < \phi(n)$ og $ed \equiv 1 \pmod{\phi(n)}$. Nå er $\phi(n) = \phi(5 \cdot 17) = 4 \cdot 16 = 64$, så kravene til d blir

$$1 < d < 64$$

$$15d \equiv 1 \pmod{64}.$$

Euklids algoritme gir

$$\begin{aligned}64 &= 4 \cdot 15 + 4 \\ 15 &= 3 \cdot 4 + 3 \\ 4 &= 3 + 1,\end{aligned}$$

og jobber vi oss bakover får vi

$$\begin{aligned}1 &= 4 - 3 \\ &= 4 - (15 - 3 \cdot 4) = 4 \cdot 4 - 15 \\ &= 4 \cdot (64 - 4 \cdot 15) - 15 = 15 \cdot (-17) + 64 \cdot 4.\end{aligned}$$

Derfor er $d \equiv -17 \pmod{64}$, som gir $d = -17 + 64 = 47$. Den hemmelige dekrypteringsnøkkelen er derfor *tallparet*

$$\{n, d\} = \{85, 47\}.$$

(b) Vi må finne tallet $E(M)$ som tilfredsstiller $0 \leq E(M) < n$ og $E(M) \equiv M^e \pmod n$, dvs

$$0 \leq E(M) < 85$$

$$E(M) \equiv 7^{15} \pmod{85}.$$

Siden $7^3 = 343$ og $85 \cdot 4 = 340$ er $7^3 \equiv 3 \pmod{85}$, og dette gir

$$7^{15} \equiv 3^5 \equiv 243 \equiv 73 \pmod{85}.$$

Derfor er $E(M) = 73$.

Oppgave 6. Vi må finne minste positive b slik at

$$31b \equiv 1 (\mathrm{mod}\, 131),$$

så i praksis må vi løse en lineær kongruens. Euklids algoritme gir

$$\begin{aligned} 131 &= 4 \cdot 31 + 7 \\ 31 &= 4 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1, \end{aligned}$$

og jobber vi oss bakover får vi

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (31 - 4 \cdot 7) = 9 \cdot 7 - 2 \cdot 31 \\ &= 9 \cdot (131 - 4 \cdot 31) - 2 \cdot 31 = 31 \cdot (-38) + 131 \cdot 9. \end{aligned}$$

Derfor er $b \equiv -38 (\mathrm{mod}\, 131)$, så vi får

$$b = -38 + 131 = 93.$$

Oppgave 7. (a) Anta k deler t. Da er $t = ks$ for et tall s, og siden $a^k \equiv 1 (\mathrm{mod}\, n)$ kan vi opphøye i s og få $a^{ks} \equiv 1 (\mathrm{mod}\, n)$, dvs $a^t \equiv 1 (\mathrm{mod}\, n)$.

Anta nå at k ikke deler t. Da er $t = ks + r$ hvor resten r tilfredsstiller $1 \leq r < k$ (vi kan jo ikke ha $r = 0$ siden $k \nmid t$). Siden $a^k \equiv 1 (\mathrm{mod}\, n)$ kan vi opphøye i s og få $a^{ks} \equiv 1 (\mathrm{mod}\, n)$, og denne siste kan vi multiplisere med a^r og få $a^{ks+r} \equiv a^r (\mathrm{mod}\, n)$, dvs $a^t \equiv a^r (\mathrm{mod}\, n)$. Hvis det nå var slik at $a^t \equiv 1 (\mathrm{mod}\, n)$ ville vi hatt $a^r \equiv 1 (\mathrm{mod}\, n)$, men dette er umulig siden $r < k$ og k er det minste positive tallet som er slik at $a^k \equiv 1 (\mathrm{mod}\, n)$. Derfor er $a^t \not\equiv 1 (\mathrm{mod}\, n)$.

(b) La k være ordenen til 7 modulo 11. Vi må undersøke om $k = \phi(11)$, dvs om $k = 10$. Fra (a) vet vi at k må dele 10, siden $7^{\phi(11)} \equiv 1 (\mathrm{mod}\, 11)$ ifølge Eulers Teorem. Vi må med andre ord sjekke divisorene til 10:

$$\begin{aligned} 7^1 &\equiv 7 (\mathrm{mod}\, 11) \\ 7^2 &\equiv 5 (\mathrm{mod}\, 11) \\ 7^5 &\equiv 7^2 \cdot 7^2 \cdot 7 \equiv 5 \cdot 5 \cdot 7 \equiv 10 (\mathrm{mod}\, 11). \end{aligned}$$

Siden vi nå har funnet ut at k ikke kan være $1, 2$ eller 5, må vi ha at $k = 10$. Derfor er 7 en primitiv rot av 11.

Tallet 37 er et primtall, og har derfor primitive røtter. Ifølge et teorem har det da

$$\phi(\phi(37)) = \phi(36) = \phi(2^2 \cdot 3^2) = 12$$

primitive røtter.

Oppgave 8. Induksjon på n. Vi har

$$S_2 = \sum_{i=1}^{2} \frac{1}{i} = 1 + \frac{1}{2} \geq \frac{1}{2} + 1,$$

så påstanden stemmer for $n = 1$. La nå $n \geq 1$ og anta

$$S_{2^n} \geq \frac{n}{2} + 1.$$

Vi må vise at da stemmer påstanden også for $n + 1$, dvs at

$$S_{2^{n+1}} \geq \frac{n+1}{2} + 1.$$

Vi har

$$\begin{aligned}
S_{2^{n+1}} &= \sum_{i=1}^{2^{n+1}} \frac{1}{i} \\
&= \sum_{i=1}^{2\cdot 2^n} \frac{1}{i} \\
&= \sum_{i=1}^{2^n} \frac{1}{i} + \sum_{i=2^n+1}^{2^n+2^n} \frac{1}{i} \\
&= S_{2^n} + \sum_{i=2^n+1}^{2^n+2^n} \frac{1}{i} \\
&\geq \left(\frac{n}{2}+1\right) + \sum_{i=2^n+1}^{2^n+2^n} \frac{1}{i}.
\end{aligned}$$

Se nå på den siste summen som går fra $i = 2^n + 1$ til $i = 2^n + 2^n$. Der er det 2^n ledd, og alle er større enn eller lik det siste leddet som er $\frac{1}{2^n+2^n} = \frac{1}{2\cdot 2^n}$. Derfor har vi

$$\sum_{i=2^n+1}^{2^n+2^n} \frac{1}{i} \geq 2^n \cdot \frac{1}{2\cdot 2^n} = \frac{1}{2},$$

som gir

$$\begin{aligned}
S_{2^{n+1}} &\geq \left(\frac{n}{2}+1\right) + \sum_{i=2^n+1}^{2^n+2^n} \frac{1}{i} \\
&\geq \left(\frac{n}{2}+1\right) + \frac{1}{2} \\
&= \frac{n+1}{2} + 1.
\end{aligned}$$