LØSNINGSFORSLAG EKSAMEN MA1301/MA6301/MNFMA104
HØST 2003

Oppgave 1. (a) Euklids algoritme gir

$$\begin{aligned} 675 &= 2 \cdot 285 + 105 \\ 285 &= 2 \cdot 105 + 75 \\ 105 &= 1 \cdot 75 + 30 \\ 75 &= 2 \cdot 30 + 15 \\ 30 &= 2 \cdot 15 \end{aligned}$$

Dette gir $\gcd(675, 285) = 15$.

(b) Siden $\gcd(675, 285)$ deler 30 er ligningen løsbar. Ved å arbeide oss bakover i Euklids algoritme får vi

$$\begin{aligned} 15 &= 75 - 2 \cdot 30 \\ &= 75 - 2(105 - 75) \\ &= 3 \cdot 75 - 2 \cdot 105 \\ &= 3(285 - 2 \cdot 105) - 2 \cdot 105 \\ &= 3 \cdot 285 - 8 \cdot 105 \\ &= 3 \cdot 285 - 8(675 - 2 \cdot 285) \\ &= 675 \cdot (-8) + 285 \cdot 19 \end{aligned}$$

Ved å multiplisere med 2 får vi da

$$30 = 15 \cdot 2 = 675 \cdot (-16) + 285 \cdot 38,$$

og derfor er $x_0 = -16, y_0 = 38$ en løsning av den diofantiske ligningen $675x + 285y = 30$. Da er alle løsningene gitt ved

$$\begin{aligned} x &= x_0 + \frac{285}{15}t = -16 + 19t \\ y &= y_0 - \frac{675}{15}t = 38 - 45t \end{aligned}$$

hvor t er et heltall.

Oppgave 2. Alle heltall x som gir rest $1, 2$ og 3 ved divisjon med henholdsvis $5, 7$ og 8 er gitt ved systemet

$$\begin{aligned} x &\equiv 1 (\mathrm{mod}\, 5) \\ x &\equiv 2 (\mathrm{mod}\, 7) \\ x &\equiv 3 (\mathrm{mod}\, 8) \end{aligned}$$

Siden $5, 7$ og 8 er innbyrdes primiske, bruker vi det Kinesiske Restteorem. Vi setter $m_1 = 7 \cdot 8 = 56, m_2 = 5 \cdot 8 = 40, m_3 = 5 \cdot 7 = 35$ og løser de tre kongruensene

$$\begin{aligned} m_1 x_1 &\equiv 1 (\mathrm{mod}\, 5) \leftrightarrow 56x_1 \equiv 1 (\mathrm{mod}\, 5) \\ m_2 x_2 &\equiv 1 (\mathrm{mod}\, 7) \leftrightarrow 40x_2 \equiv 1 (\mathrm{mod}\, 7) \\ m_3 x_3 &\equiv 1 (\mathrm{mod}\, 8) \leftrightarrow 35x_3 \equiv 1 (\mathrm{mod}\, 8) \end{aligned}$$

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

$$\begin{aligned} \overline{x} &= 1 \cdot m_1 x_1 + 2 \cdot m_2 x_2 + 3 \cdot m_3 x_3 \\ &= 1 \cdot 56 \cdot 1 + 2 \cdot 40 \cdot 3 + 3 \cdot 35 \cdot 3 \\ &= 611 \end{aligned}$$

Løsningen er derfor alle heltallene gitt ved $x \equiv 611 (\mathrm{mod}\, 5 \cdot 7 \cdot 8)$, dvs

$$x \equiv 611 (\mathrm{mod}\, 280)$$

Det minste positive tallet som tilfredsstiller dette må være det tallet i intervallet $[0, 279]$ som er kongruent med 611 modulo 280. Siden vi har $611 - 2 \cdot 280 = 51$ er dette tallet 51.

Oppgave 3. (a) Eulers Teorem sier at for alle $n \in \mathbb{N}$ og $a \in \mathbb{Z}$ med $\gcd(n, a) = 1$ gjelder

$$a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$$

hvor ϕ er Eulers phi-funksjon.

(b) Her må vi finne det minste ikke-negative tallet som er kongruent med 63^{81} modulo 10. Siden $\gcd(63, 81) = 1$ sier Eulers Teorem at $63^{\phi(10)} \equiv 1 (\mathrm{mod}\, 10)$, dvs

$$63^4 \equiv 1 (\mathrm{mod}\, 10)$$

Ved å opphøye kongruensen i 20 får vi da $63^{80} \equiv 1 (\mathrm{mod}\, 10)$, som gir $63^{81} \equiv 63 (\mathrm{mod}\, 10)$. Nå er $63 \equiv 3 (\mathrm{mod}\, 10)$, så derfor har vi

$$63^{81} \equiv 3 (\mathrm{mod}\, 10)$$

Det siste sifferet i tallet 63^{81} er derfor 3.

(c) La a være et heltall og p et primtall som ikke deler a. Da må vi ha $\gcd(p, a) = 1$, og Eulers Teorem gir derfor

$$a^{\phi(p)} \equiv 1 (\mathrm{mod}\, p)$$

Funksjonen ϕ er definert ved at $\phi(n)$ er antall elementer i mengden $\{1, \ldots, n\}$ relativt primiske med n, og siden tallene $1, \ldots, (p-1)$ ikke deles av p må vi derfor ha $\phi(p) = p - 1$. Da får vi

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

Oppgave 4. (a) Siden $\gcd(7, 40) = 1$ er denne lineære kongruensen løsbar, og den har én løsning modulo 40. Euklids algoritme gir

$$\begin{aligned} 40 &= 5 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

og ved å arbeide oss bakover får vi

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(7 - 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3(40 - 5 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 40 - 17 \cdot 7 \end{aligned}$$

Så skriver vi om og får $7 \cdot (-17) - 1 = 40 \cdot (-3)$, som betyr at $x_0 = -17$ er en løsning av kongruensen $7x \equiv 1 (\mathrm{mod}\, 40)$. Da er alle løsningene gitt ved

$$x \equiv -17 (\mathrm{mod}\, 40)$$

(b) Vi har $\phi(55) = 4 \cdot 10 = 40$, slik at d er det unike tallet som tilfredsstiller $1 < d < 40$ og $ed \equiv 1 (\mathrm{mod}\, 40)$. Når vi setter inn for e i kongruensen får vi

$$7d \equiv 1 (\mathrm{mod}\, 40)$$

Fra (a) vet vi at da må d tilfredsstille $d \equiv -17 (\mathrm{mod}\, 40)$, og vi får derfor $d = 23$. Den hemmelige nøkkelen blir da

$$\{n, d\} = \{55, 23\}$$

(c) Vi må finne tallet $E(13)$ som tilfredsstiller $0 \leq E(13) < 55$ og $13^e \equiv E(13) (\mathrm{mod}\, 55)$, dvs

$$13^7 \equiv E(13) (\mathrm{mod}\, 55)$$

Siden $13^2 \equiv 4 (\mathrm{mod}\, 55)$ er $13^6 \equiv 4^3 \equiv 9 (\mathrm{mod}\, 55)$, som gir $13^7 \equiv 13 \cdot 9 \equiv 7 (\mathrm{mod}\, 55)$. Derfor har vi

$$E(13) = 7$$

Oppgave 5. Siden p og q er tvillingprimtall kan vi uten tap av generalitet sette $q = p - 2$. Fra Wilsons Teorem vet vi at vi har

$$(p-1)! \equiv -1 (\mathrm{mod}\, p)$$

og siden $-1 \equiv p - 1 (\mathrm{mod}\, p)$ får vi da

$$(p-1)! \equiv p - 1 (\mathrm{mod}\, p)$$

Her er $p-1$ en faktor på begge sidene i kongruensen, og siden $\gcd(p, p-1) = 1$ kan vi dele og få $(p-2)! \equiv 1 (\mathrm{mod}\, p)$, dvs

$$q! \equiv 1 (\mathrm{mod}\, p)$$