EKSAMEN MA1301 HØST 2018
LØSNINGSFORSLAG

Oppgave 1. Euklids algoritme anvendt på 68 og 504 gir

$$\begin{aligned} 504 &= 7\cdot 68 + 28 \\ 68 &= 2\cdot 28 + 12 \\ 28 &= 2\cdot 12 + 4 \\ 12 &= 3\cdot 4 + 0 \end{aligned}$$

Det betyr at $\gcd(68,504) = 4$, og siden 4 deler 336 er kongruensen løsbar (og har 4 inkongruente løsninger). Ved å jobbe oss bakover får vi

$$\begin{aligned} 4 &= 28 - 2\cdot 12 \\ &= 28 - 2\cdot(68 - 2\cdot 28) \\ &= 28\cdot 5 - 2\cdot 68 \\ &= (504 - 7\cdot 68)\cdot 5 - 2\cdot 68 \\ &= 504\cdot 5 + 68\cdot(-37) \end{aligned}$$

Siden $336 = 4\cdot 84$, multipliserer vi med 84 og får

$$336 = 4\cdot 84 = 504\cdot 5\cdot 84 + 68\cdot(-37)\cdot 84 = 504\cdot 420 + 68\cdot(-3108)$$

Altså er $x_0 = -3108$ en spesifikk løsning av kongruensen. De fire tallene

$$x_0,\ x_0 + 504/4,\ x_0 + 2\cdot 504/4,\ x_0 + 3\cdot 504/4$$

representerer derfor alle løsningene, dvs løsningen er

$$x \equiv -3108, -2982, -2856, -2730 \pmod{504}$$

Minste positive løsning er minste positive tall på formen $-3108 + k\cdot(504/4)$, dvs $-3108 + 126k$. Det er tallet 42.

Oppgave 2. Siden 47 er et primtall er $46! \equiv -1 \pmod{47}$ fra Wilsons teorem. Det gir

$$46! \equiv -1 \equiv 46 \pmod{47}$$

og siden $\gcd(46,47) = 1$ kan vi dele ut 46 og få $45! \equiv 1 \pmod{47}$. Siden $45 \equiv -2 \pmod{47}$ og $1 \equiv 48 \equiv 2\cdot 24 \pmod{47}$ får vi da

$$2\cdot 24 \equiv 1 \equiv 45! \equiv (-2)\cdot(44!) \pmod{47}$$

Nå kan vi dele ut -2, siden $\gcd(-2,47) = 1$, og få $44! \equiv -24 \pmod{47}$. Det gir

$$5\cdot(44!) \equiv 5\cdot(-24) \equiv -120 \equiv 21 \pmod{47}$$

Vi får altså 21 til rest.

Oppgave 3. Siden modulusene $7, 9, 13$ er parvis relativt primiske, garanterer det kinesiske restteoremet at systemet er løsbart og har en unik løsning modulo $7 \cdot 9 \cdot 13$, det vil si modulo 819. Vi setter

$$N_1 = 9 \cdot 13 = 117, \qquad N_2 = 7 \cdot 13 = 91, \qquad N_3 = 7 \cdot 9 = 63$$

og ser på følgende tre lineære kongruenser hver for seg:

$$\begin{aligned} 1 &\equiv 117x \equiv 5x \pmod 7 \\ 1 &\equiv 91x \equiv x \pmod 9 \\ 1 &\equiv 63x \equiv 11x \pmod{13} \end{aligned}$$

Tre løsninger som passer er $x_1 = 3, x_2 = 1, x_3 = 6$, så vi får

$$\begin{aligned} x_0 &= (-2) \cdot N_1 \cdot x_1 + 6 \cdot N_2 \cdot x_2 + 8 \cdot N_3 \cdot x_3 \\ &= (-2) \cdot 117 \cdot 3 + 6 \cdot 91 \cdot 1 + 8 \cdot 63 \cdot 6 \\ &= 2868 \end{aligned}$$

Løsningen på systemet blir altså

$$x \equiv 2868 \pmod{819}$$

Oppgave 4. **(a)** La a være et heltall med $\gcd(a, n) = 1$. Da er ordenen til a modulo n det minste tallet $k \geq 1$ med $a^k \equiv 1 \pmod n$. Ordenen er ikke definert dersom $\gcd(a, n) \neq 1$.

Modulo 15 er ethvert tall kongruent med ett av tallene $0, 1, 2, \ldots, 14$. Så dersom a er et heltall med $\gcd(a, 15) = 1$, så er a kongruent med ett av tallene $1, 2, 4, 7, 8, 11, 13, 14$ modulo 15. Vi må derfor finne ordenen til hver av disse åtte tallene modulo 15. Vi har et resultat som sier at ordenen må dele $\phi(15)$, så siden $\phi(15) = 8$, vil ordenen til et tall a være enten $1, 2, 4$ eller 8. Vi har

$$\begin{array}{lllll} 1^1 \equiv 1 & & & & \\ 2^1 \equiv 2 & \Rightarrow & 2^2 \equiv 4 & \Rightarrow & 2^4 \equiv 16 \equiv 1 \\ 4^1 \equiv 4 & \Rightarrow & 4^2 \equiv 16 \equiv 1 & & \\ 7^1 \equiv 7 & \Rightarrow & 7^2 \equiv 49 \equiv 4 & \Rightarrow & 7^4 \equiv 16 \equiv 1 \\ 8^1 \equiv 8 & \Rightarrow & 8^2 \equiv 64 \equiv 4 & \Rightarrow & 8^4 \equiv 16 \equiv 1 \\ 11^1 \equiv 11 & \Rightarrow & 11^2 \equiv 121 \equiv 1 & & \\ 13^1 \equiv 13 \equiv -2 & \Rightarrow & 13^2 \equiv 4 & \Rightarrow & 13^4 \equiv 16 \equiv 1 \\ 14^1 \equiv 14 \equiv -1 & \Rightarrow & 14^2 \equiv 1 & & \end{array}$$

hvor alt er modulo 15. Det betyr:

$$\begin{aligned} a = 1 &\Rightarrow a \text{ har orden } 1 \\ a \in \{4, 11, 14\} &\Rightarrow a \text{ har orden } 2 \\ a \in \{2, 7, 8, 13\} &\Rightarrow a \text{ har orden } 4 \end{aligned}$$

(b) La a være et heltall med $\gcd(a, n) = 1$. Da er a en primitiv rot av n dersom ordenen til a modulo n er $\phi(n)$.

Siden $\phi(18) = 6$, vil det si at en primitiv rot av 18 er et tall som har orden 6. La oss prøve med $a = 5$, som er laveste positive tall (bortsett fra 1) som er relativt primisk med 18. Nok en gang: siden ordenen til et tall modulo 18 må dele $\phi(18) = 6$, må ordenen være $1, 2, 3$ eller 6. Vi har

$$5^1 \equiv 5 \Rightarrow 5^2 \equiv 25 \equiv 7 \Rightarrow 5^3 \equiv 35 \equiv 17$$

hvor alt er modulo 18. Det betyr at tallet 5 ikke har orden $1, 2$ eller 3, og må derfor ha orden 6. Altså er 5 en primitiv rot av 18. (Siden 18 har en primitiv rot, har den $\phi(\phi(18)) = \phi(6) = 2$ stykker. Den ene er altså 5, og man kan vise at den andre er $5^5 \equiv 11 \pmod{18}$.)

For at et tall skal være en primitiv rot av 15, må det ha orden $\phi(15) = 8$. Men vi så i (a) at ingen tall har orden 8 modulo 15. Det betyr at tallet 15 ikke har noen primitive røtter. Det kan vises (men vi har ikke gjort det i kurset) at de positive heltallene som har primitive røtter er

$$2, 4, p^k, 2p^k$$

for odde primtall p og $k \geq 1$. Tallet 15 er ikke på denne listen, mens 18 er det.

Oppgave 5. Vi ser på Legendresymbolet $\left(\frac{43}{19}\right)$. Siden $43 \equiv 5 \pmod{19}$ gir regnereglene at

$$\left(\frac{43}{19}\right) \equiv \left(\frac{5}{19}\right) \equiv 5^{(19-1)/2} \equiv 5^9 \equiv 1953125 \equiv 1 \pmod{19}$$

Verdien av et Legendresymbol er ± 1, så det betyr at $\left(\frac{43}{19}\right) = 1$. Derfor er kongruensen $x^2 \equiv 43 \pmod{19}$ løsbar (løsningene er $x_1 = 9$ og $x_2 = 19 - 9 = 10$).

For å finne ut om den «motsatte» kongruensen er løsbar, bruker vi loven om kvadratisk resiprositet:

$$\left(\frac{43}{19}\right)\left(\frac{19}{43}\right) = (-1)^{\frac{43-1}{2} \cdot \frac{19-1}{2}} = -1$$

Siden $\left(\frac{43}{19}\right) = 1$, betyr det at $\left(\frac{19}{43}\right)$ må være lik -1. Følgelig er kongruensen $x^2 \equiv 19 \pmod{43}$ ikke løsbar.

Oppgave 6. Modulusen 35 er produktet av 5 og 7. La oss derfor vise at kongruensen holder modulo disse to faktorene.

Hvis 5 deler a, så er begge sidene av kongruensen delelig med 5, så da er $a^{24n+1} \equiv 0 \equiv a \pmod{5}$. Hvis 5 ikke deler a, så er $a^4 \equiv 1 \pmod{5}$ fra Fermats teorem, som gir $a^{24} \equiv (a^4)^6 \equiv 1 \pmod{5}$, og videre da $a^{24n} \equiv 1 \pmod{5}$ for alle $n \geq 1$. Da er $a^{24n+1} \equiv a \pmod{5}$.

Hvis 7 deler a, så er begge sidene av kongruensen delelig med 7, så da er $a^{24n+1} \equiv 0 \equiv a \pmod{7}$. Hvis 7 ikke deler a, så er $a^6 \equiv 1 \pmod{7}$ fra Fermats teorem, som gir $a^{24} \equiv (a^6)^4 \equiv 1 \pmod{7}$, og videre da $a^{24n} \equiv 1 \pmod{7}$ for alle $n \geq 1$. Da er $a^{24n+1} \equiv a \pmod{7}$.

Vi har nå vist at for alle a og $n \geq 1$, så er $a^{24n+1} \equiv a \pmod{5}$ og $a^{24n+1} \equiv a \pmod{7}$. Det betyr at både 5 og 7 deler $a^{24n+1} - a$. Siden $\gcd(5,7) = 1$, vil da også $5 \cdot 7 = 35$ dele $a^{24n+1} - a$, dvs $a^{24n+1} \equiv a \pmod{35}$.

Oppgave 7. Koeffisientene foran variablene er $3a+7$ og $2a+5$. Se på likheten

$$(3a+7) \cdot (-2) + (2a+5) \cdot 3 = 1$$

Dette viser at tallet 1 er en lineærkombinasjon av de to koeffisientene, og da har vi et resultat som sier at $\gcd(3a+7, 2a+5) = 1$. Da er den diofantiske ligningen alltid løsbar, uansett hva b er, siden 1 deler b.

Ved å multiplisere likheten over med b, får vi

$$(3a+7) \cdot (-2b) + (2a+5) \cdot 3b = b$$

Det betyr at $x_0 = -2b, y_0 = 3b$ er en spesiell løsning av ligningen. Da er alle løsningene gitt ved

$$\begin{aligned} x &= x_0 + \tfrac{2a+5}{1} t &&= (2a+5)t - 2b \\ y &= y_0 - \tfrac{3a+7}{1} t &&= 3b - (3a+7)t \end{aligned}$$

for $t \in \mathbb{Z}$.

Oppgave 8. **(a)** Anta n er delelig med et odde primtall p. Da er $n = mp^k$ hvor $k \geq 1$ og p ikke deler m, dvs $\gcd(m, p^k) = 1$. Siden ϕ er multiplikativ får vi da

$$\phi(n) = \phi(p^k)\phi(m) = (p^k - p^{k-1})\phi(m) = p^{k-1}(p-1)\phi(m)$$

Primtallet p er odde, så 2 deler $p-1$ og derfor $\phi(n)$.

Anta nå at n ikke er delelig med noen odde primtall. Da er $n = 2^k$, og siden $n \geq 3$ er $k \geq 2$. Det gir

$$\phi(n) = 2^k - 2^{k-1} = 2(2^{k-1} - 2^{k-2})$$

så 2 deler $\phi(n)$ også i dette tilfellet. Dette viser at 2 deler $\phi(n)$ for alle $n \geq 3$.

(b) Fra Eulers teorem (som vi kan bruke siden $\gcd(a, n) = 1$) har vi $a^{\phi(n)} \equiv 1 \pmod{n}$, som betyr at n deler $a^{\phi(n)} - 1$. Hvis p er et primtall som deler n, vil da p også dele $a^{\phi(n)} - 1$.

Fra (a) er $\phi(n)$ et partall, så vi kan skrive

$$a^{\phi(n)} - 1 = \left(a^{\phi(n)/2} - 1\right)\left(a^{\phi(n)/2} + 1\right)$$

Siden p er et primtall, må da p dele en av disse faktorene, dvs at p må dele enten $a^{\phi(n)/2} - 1$ eller $a^{\phi(n)/2} + 1$. Det betyr at en av de to kongruensene

$$a^{\phi(n)/2} \equiv 1 \pmod{p}, \qquad a^{\phi(n)/2} \equiv -1 \pmod{p}$$

gjelder.