Løsninger – Repetisjonsoppgaver

Løsning til Oppgave 1. Vi gjør følgende observasjoner.

(1) Siden 41 er et primtall, følger det fra Fermats lille teorem at

$$8^{40} \equiv 1 \pmod{41}.$$

Da er

$$\left(8^{122}\right) = 8^{3\cdot 40+2} = 8^{3\cdot 40} \cdot 8^2 = \left(8^{40}\right)^3 \cdot 8^2 \equiv 1^3 \cdot 8^2 = 8^2 = 64 \equiv 23 \pmod{41}.$$

Dermed er

$$2 \cdot \left(8^{122}\right) \equiv 2 \cdot 23 = 46 \equiv 5 \pmod{41}.$$

(2) Siden 41 er et primtall, følger det også fra Fermats lille teorem at

$$3^{40} \equiv 1 \pmod{41}.$$

Da er

$$3^{83} = 3^{2\cdot 40+3} = 3^{2\cdot 40} \cdot 3^3 = \left(3^{40}\right)^2 \cdot 3^3 \equiv 1^2 \cdot 3^3 = 3^3 = 27 \pmod{41}.$$

(3) Det følger fra (1) og (2) at

$$2 \cdot \left(8^{122}\right) - 3^{83} - 19 \equiv 5 - 27 - 19 = -41 \equiv 0 \pmod{41}.$$

Vi konkluderer at $2 \cdot \left(8^{122}\right) - 3^{83} - 19$ er delelig med 41.

Løsning til Oppgave 2. Vi gjør følgende observasjoner.

(1) Siden 19 er et primtall, følger det fra Wilsons teorem at

$$18! \equiv -1 \pmod{19}.$$

(2) Vi har:

$$18! = (16!) \cdot 17 \cdot 18 \equiv (16!) \cdot (-2) \cdot (-1) = 2 \cdot (16!) \pmod{19},$$

altså

$$2 \cdot (16!) \equiv 18! \pmod{19}.$$

(3) Det følger fra (1) og (2) at

$$2 \cdot (16!) \equiv -1 \pmod{19}.$$

Da er

$$(6 \cdot (16!))^3 = (3 \cdot 2 \cdot (16!))^3 \equiv (3 \cdot (-1))^3 = (-3)^3 = -27 \equiv 11 \pmod{19}.$$

Vi konkluderer at vi får 11 som rest når vi deler $(6 \cdot (16!))^3$ med 19.

Løsning til Oppgave 3. Vi har:

$$9^2 = 81 \equiv -2 \pmod{83}.$$

Da er

$$9^{12} + 19 = \left(9^2\right)^6 + 19 \equiv (-2)^6 + 19 = 64 + 19 = 83 \equiv 0 \pmod{83}.$$

Dermed er $9^{12} + 19$ delelig med 83.

Løsning til Oppgave 4. Vi gjør følgende observasjoner.

(1) En primtallsfaktorisering til 693 er $3^2 \cdot 7 \cdot 11$.

(2) Det følger fra (1) at

$$\begin{aligned}
\phi(693) &= \phi\left(3^2 \cdot 7 \cdot 11\right) \\
&= \phi\left(3^2\right) \cdot \phi(7) \cdot \phi(11) \\
&= \left(3^2 - 3\right)(7-1)(11-1) \\
&= 6 \cdot 6 \cdot 10 \\
&= 360.
\end{aligned}$$

(3) Ut ifra Eulers teorem er

$$5^{\phi(693)} \equiv 1 \pmod{693}.$$

(4) Det følger fra (2) og (3) at

$$5^{360} \equiv 1 \pmod{693}.$$

(5) Det følger fra (4) at

$$5^{17642} = 5^{49 \cdot 360 + 2} = 5^{49 \cdot 360} \cdot 5^2 = \left(5^{360}\right)^{49} \cdot 5^2 \equiv 1^{49} \cdot 5^2 = 5^2 = 25 \pmod{693}.$$

(6) Det følger fra (5) at

$$32 \cdot \left(5^{17642}\right) - 7 \equiv 32 \cdot 25 - 7 = 793 \equiv 100 \pmod{693}.$$

Løsning til Oppgave 5. Vi gjør følgende observasjoner.

(1) Siden 37 er et primtall, følger det fra Fermats lille teorem at

$$12^{36} \equiv 1 \pmod{37}.$$

Da er

$$12^{289} = 12^{8\cdot 36+1} = 12^{8\cdot 36} \cdot 12 = \left(12^{36}\right)^8 \cdot 12 \equiv 1^8 \cdot 12 = 12 \pmod{37}.$$

(2) Siden 37 er et primtall, følger det fra Wilsons teorem at

$$36! \equiv -1 \pmod{37}.$$

(3) Vi har:

$$36! = (33!) \cdot 34 \cdot 35 \cdot 36 \equiv (33!) \cdot (-3) \cdot (-2) \cdot (-1) = (-6) \cdot (33!) \pmod{37},$$

altså

$$(-6) \cdot (33!) \equiv 36! \pmod{37}.$$

(4) Det følger fra (2) og (3) at

$$(-6) \cdot (33!) \equiv 36! \equiv -1 \pmod{37}.$$

(5) Det følger fra (1) og (4) at

$$(33!)\cdot\left(12^{289}\right)-2 \equiv (33!)\cdot 12-2 = (-2)\cdot(-6)\cdot(33!)-2 \equiv (-2)\cdot(-1)-2 = 2-2 = 0 \pmod{37}.$$

Vi konkluderer at $(33!) \cdot \left(12^{289}\right) - 2$ er delelig med 37.

Løsning til Oppgave 6. En primtallsfaktorisering til 75803 er $7^3 \cdot 13 \cdot 17$.

Løsning til Oppgave 7. Vi gjør følgende observasjoner.

(1) En primtallsfaktorisering til 1043504 er: $2^4 \cdot 7^2 \cdot 11^3$.

(2) En primtallsfaktorisering til 237276 er: $2^2 \cdot 3^3 \cdot 13^3$.

Det følger fra (1) og (2) at

$$\mathsf{sfd}(104304, 237276) = 2^2 = 4.$$

Løsning til Oppgave 8. En primtallsfaktorisering til 3087 er $3^2 \cdot 7^3$. Et resultat fra kurset (Korollar 4.2.23) fastslår da at et hvilket som helst primtall som deler 3087 er likt 3 eller 7.

Løsning til Oppgave 9. En primtallsfaktorisering til 151875 er $3^5 \cdot 5^4$.

Løsning til Oppgave 10. Vi har: $\mathsf{sfd}(40, 16) = 8$. Siden det ikke er sant $8 \mid 9$, har ligningen i oppgaven ingen heltallsløsning.

Løsning til Oppgave 11. Vi benytter Euklids algoritme som følger.

$$\begin{aligned} 138 &= 3 \cdot 42 + 12 \\ 42 &= 3 \cdot 12 + 6 \\ 12 &= 2 \cdot 6. \end{aligned}$$

Dermed er $\mathsf{sfd}(138, 42) = 6$.

Ved å benytte utregningen ovenfor, har vi følgende.

$$\begin{aligned} 12 &= 138 - 3 \cdot 42 \\ 6 &= 42 - 3 \cdot 12 \\ &= 42 - 3 \cdot (138 - 3 \cdot 42) \\ &= (-3) \cdot 138 + 10 \cdot 42. \end{aligned}$$

Ved å gange begge sidene av ligningen

$$138 \cdot (-3) + 42 \cdot 10 = 6$$

med 3, får vi:

$$138 \cdot (-3) \cdot 3 + 42 \cdot 10 \cdot 3 = 18,$$

altså

$$138 \cdot (-9) + 42 \cdot 30 = 18.$$

Dermed er $x = -9$ og $y = 30$ en løsning til ligningen i oppgaven.

For å finne alle løsningene, deler vi 138 og 42 med $\mathsf{sfd}(138, 42)$, altså med 6. Vi har: $138 = 23 \cdot 6$ og $42 = 7 \cdot 6$. Det følger fra teorien for lineære diofantiske ligninger i kurset (Korollar 2.9.25) at alle løsningene til ligningen i oppgaven er: $x = -9 + 7t$ og $y = 30 - 23t$, for et hvilket som helst heltall t.

Løsning til Oppgave 12. Vi benytter Euklids algoritme som følger.

$$\begin{aligned} 50 &= 3 \cdot 15 + 5 \\ 15 &= 3 \cdot 5 \end{aligned}$$

Dermed er $\mathsf{sfd}(15, 50) = 5$.

Ved å benytte utregningen ovenfor, er

$$5 = 50 - 3 \cdot 15.$$

Dermed er

$$15 \cdot (-3) - 5 = 50 \equiv 0 \pmod{50}.$$

Det følger at

$$15 \cdot (-3) \equiv 5 \pmod{50}.$$

Ved å gange begge sidene av denne kongruensen med 4, får vi at

$$15 \cdot (-3) \cdot 4 \equiv 5 \cdot 4 \pmod{50},$$

altså at

$$15 \cdot (-12) \equiv 20 \pmod{50}.$$

Således er $x = -12$ en løsning til kongruensen i oppgaven.

For å få alle løsningene, deler vi 50 med $\mathsf{sfd}(15, 50)$, altså med 5. Vi får: $50 = 10 \cdot 5$. Det følger fra teorien for lineære kongruenser i kurset (Korollar 3.4.36) at alle løsningene slik at $0 \leq x < 50$ er: $x = -12 + 10t$, hvor t er et hvilket som helst heltall slik at $0 \leq -12 + 10t < 50$. Dermed er alle løsningene som oppfyller kravet i oppgaven: 8, 18, 28, 38, og 48.

Løsning til Oppgave 13. Først regner vi ut diskriminanten. Vi får:

$$(-20)^2 - 4 \cdot 4 \cdot 25 = 0.$$

Det følger fra teorien for kvadratiske kongruenser i kurset (Korollar 5.2.30) at det finnes ett heltall x slik at x er en løsning til kongruensen i oppgaven og slik at $0 \leq x < 137$.

Siden

$$0^2 \equiv 0 \pmod{137},$$

følger det fra teorien for kvadratiske kongruenser i kurset (Proposisjon 5.1.9) at vi kan komme fram til x ved å løse kongruensen

$$(2 \cdot 4)x \equiv 0 - (-20) \pmod{137},$$

altså kongruensen

$$8x \equiv 20 \pmod{137}.$$

For å gjøre dette, benytter vi Euklids algoritme.

$$137 = 17 \cdot 8 + 1$$
$$8 = 8 \cdot 1$$

Fra den første ligningen i denne utregningen, får vi:

$$8 \cdot 17 + 1 = 137 \equiv 0 \pmod{127},$$

altså

$$8 \cdot 17 \equiv -1 \pmod{137}.$$

Ved å gange begge sidene av denne kongruensen med -20, får vi:

$$8 \cdot 17 \cdot (-20) \equiv (-1) \cdot (-20) \pmod{137},$$

altså

$$8 \cdot (-340) \equiv 20 \pmod{137}.$$

Dermed er $x = -340$ en løsning til kongruensen

$$8x \equiv 20 \pmod{137}.$$

Siden

$$-340 \equiv 71 \pmod{137},$$

følger det at $x = 71$ er en løsning til kongruensen

$$8x \equiv 20 \pmod{137},$$

og dermed til kongruensen i oppgaven. I tillegg oppfyller x kravet at

$$0 \leq x < 137.$$

Løsning til Oppgave 14. Vi regner ut $\mathbb{L}_{189437}^{589}$ som følger. Vi refererer til reglene (A) – (G) i oversikten over kvadratiske kongruenser og Legendresymboler som følger.

(1) Vi har:

$$\begin{aligned} \mathbb{L}_{189437}^{589} &= \mathbb{L}_{189437}^{19\cdot 31} && (19 \cdot 31 \text{ er en primtallsfaktorisering til } 589) \\ &= \mathbb{L}_{189437}^{19} \cdot \mathbb{L}_{189437}^{31} && \text{(A)} \end{aligned}$$

(2) Vi har:

$$\begin{aligned} \mathbb{L}_{189437}^{19} &= \mathbb{L}_{19}^{189437} && (\text{G, } 189437 \equiv 1 \pmod 4) \\ &= \mathbb{L}_{19}^{7} && (\text{B, } 189437 \equiv 7 \pmod{19}) \\ &= -\mathbb{L}_{7}^{19} && (\text{G, } 19 \equiv 3 \pmod 4 \text{ og } 7 \equiv 3 \pmod 4) \\ &= -\mathbb{L}_{7}^{5} && (\text{B, } 19 \equiv 5 \pmod 7) \\ &= -\mathbb{L}_{5}^{7} && (\text{G, } 5 \equiv 1 \pmod 4) \\ &= -\mathbb{L}_{5}^{2} && (\text{B, } 7 \equiv 2 \pmod 5) \\ &= -(-1) && (\text{F, } 5 \equiv 5 \pmod 8) \\ &= 1 \end{aligned}$$

(3) Vi har:

$$\begin{aligned} \mathbb{L}_{189437}^{31} &= \mathbb{L}_{31}^{189437} && (\text{G, } 189437 \equiv 1 \pmod 4) \\ &= \mathbb{L}_{31}^{27} && (\text{B, } 189437 \equiv 27 \pmod{31}) \\ &= \mathbb{L}_{31}^{3^3} && (3^3 \text{ er en primtallsfaktorisering til } 27) \\ &= \mathbb{L}_{31}^{3^2} \cdot \mathbb{L}_{31}^{3} && \text{(A)} \\ &= 1 \cdot \mathbb{L}_{31}^{3} && \text{(D)} \\ &= \mathbb{L}_{31}^{3} \\ &= -\mathbb{L}_{3}^{31} && (\text{G, } 3 \equiv 3 \pmod 4 \text{ og } 31 \equiv 3 \pmod 4) \\ &= -\mathbb{L}_{3}^{1} && (\text{B, } 31 \equiv 1 \pmod 3) \\ &= -1 && \text{(C)} \end{aligned}$$

Det følger fra (1) – (3) at

$$\mathbb{L}_{189437}^{589} = \mathbb{L}_{189437}^{19} \cdot \mathbb{L}_{189437}^{31} = 1 \cdot (-1) = -1.$$

Vi konkluderer at 589 ikke er en kvadratisk rest modulo 189437.

Løsning til Oppgave 15. Først regner vi ut diskriminanten. Vi får:

$$56^2 - 4 \cdot 301 \cdot 2 = 728.$$

Nå regner vi ut $\mathbb{L}_{839}^{728}$ som følger. Igjen refererer vi til reglene (A) – (G) i oversikten over kvadratiske kongruenser og Legendresymboler.

(1) Vi har:

$$\begin{aligned}
\mathbb{L}_{839}^{728} &= \mathbb{L}_{839}^{2^3 \cdot 7 \cdot 13} && (2^3 \cdot 7 \cdot 13 \text{ er en primtallsfaktorisering til } 728) \\
&= \mathbb{L}_{839}^{2^2} \cdot \mathbb{L}_{839}^{2} \cdot \mathbb{L}_{839}^{7} \cdot \mathbb{L}_{839}^{13} && \text{(A)} \\
&= 1 \cdot \mathbb{L}_{839}^{2} \cdot \mathbb{L}_{839}^{7} \cdot \mathbb{L}_{839}^{13} && \text{(D)} \\
&= \mathbb{L}_{839}^{2} \cdot \mathbb{L}_{839}^{7} \cdot \mathbb{L}_{839}^{13} \\
&= 1 \cdot \mathbb{L}_{839}^{7} \cdot \mathbb{L}_{839}^{13} && \text{(F) og } 839 \equiv 7 \pmod 8 \\
&= \mathbb{L}_{839}^{7} \cdot \mathbb{L}_{839}^{13}
\end{aligned}$$

(2) Vi har:

$$\begin{aligned}
\mathbb{L}_{839}^{7} &= -\mathbb{L}_{7}^{839} && (\text{G, } 7 \equiv 3 \pmod 4 \text{ og } 839 \equiv 3 \pmod 4) \\
&= -\mathbb{L}_{7}^{6} && (\text{B, } 839 \equiv 6 \pmod 7) \\
&= -\mathbb{L}_{7}^{2 \cdot 3} && (2 \cdot 3 \text{ er en primtallsfaktorisering til } 6) \\
&= -\mathbb{L}_{7}^{2} \cdot \mathbb{L}_{7}^{3} && \text{(A)} \\
&= -1 \cdot \mathbb{L}_{7}^{3} && (\text{F, } 7 \equiv 7 \pmod 8) \\
&= -\mathbb{L}_{7}^{3} \\
&= -(-\mathbb{L}_{3}^{7}) && (\text{G, } 7 \equiv 3 \pmod 7 \text{ og } 3 \equiv 3 \pmod 4) \\
&= \mathbb{L}_{3}^{7} \\
&= \mathbb{L}_{3}^{1} && (\text{B, } 7 \equiv 1 \pmod 3) \\
&= 1 && \text{(C)}
\end{aligned}$$

(3) Vi har:

$$\begin{aligned}
\mathbb{L}_{839}^{13} &= \mathbb{L}_{13}^{839} && (\text{G, } 13 \equiv 1 \pmod 4) \\
&= \mathbb{L}_{13}^{7} && (\text{B, } 839 \equiv 7 \pmod{13}) \\
&= \mathbb{L}_{7}^{13} && (\text{G, } 13 \equiv 1 \pmod 4) \\
&= \mathbb{L}_{7}^{6} && (\text{B, } 13 \equiv 6 \pmod 7) \\
&= -1 && \text{som i (2)}
\end{aligned}$$

Det følger fra (1) – (3) at

$$\mathbb{L}_{839}^{728} = \mathbb{L}_{839}^{7} \cdot \mathbb{L}_{839}^{13} = 1 \cdot (-1) = -1.$$

Dermed er 728 ikke en kvadratisk rest modulo 839. Det følger fra teorien fra kvadratiske kongruenser i kurset (Korollar 5.2.30) at kongruensen i oppgaven har ingen løsning.

En alternativ måte å regne ut $\mathbb{L}_7^6$ er:

$$\begin{aligned}
\mathbb{L}_7^6 &= \mathbb{L}_7^{-1} && (\text{B}, 6 \equiv -1 \pmod 7)\\
&= (-1)^{\frac{7-1}{2}} && (\text{E})\\
&= (-1)^3\\
&= -1
\end{aligned}$$

Løsning til Oppgave 16. Først regner vi ut diskriminanten. Vi får:

$$(-54)^2 - 4 \cdot 49 \cdot 1 = 2720.$$

Nå regner vi ut $\mathbb{L}_{4027}^{2720}$ som følger. Igjen refererer vi til reglene (A) – (G) i oversikten over kvadratiske kongruenser og Legendresymboler.

(1) Vi har:

$$\begin{aligned}
\mathbb{L}_{4027}^{2720} &= \mathbb{L}_{4027}^{2^5 \cdot 5 \cdot 17} && (2^5 \cdot 5 \cdot 17 \text{ er en primtallsfaktorisering til } 2720)\\
&= \mathbb{L}_{4027}^{\left(2^2\right)^2} \cdot \mathbb{L}_{4027}^{2} \cdot \mathbb{L}_{4027}^{5} \cdot \mathbb{L}_{4027}^{17} && (\text{A})\\
&= 1 \cdot \mathbb{L}_{4027}^{2} \cdot \mathbb{L}_{4027}^{5} \cdot \mathbb{L}_{4027}^{17} && (\text{D})\\
&= \mathbb{L}_{4027}^{2} \cdot \mathbb{L}_{4027}^{5} \cdot \mathbb{L}_{4027}^{17}\\
&= (-1) \cdot \mathbb{L}_{4027}^{5} \cdot \mathbb{L}_{4027}^{17} && (\text{F}) \text{ og } 4027 \equiv 3 \pmod 8\\
&= -\mathbb{L}_{4027}^{5} \cdot \mathbb{L}_{4027}^{17}
\end{aligned}$$

(2) Vi har:

$$\begin{aligned}
\mathbb{L}_{4027}^{5} &= \mathbb{L}_{5}^{4027} && (\text{G}, 5 \equiv 1 \pmod 4)\\
&= \mathbb{L}_{5}^{2} && (\text{B}, 4027 \equiv 2 \pmod 5)\\
&= -1 && (\text{F}, 5 \equiv 5 \pmod 8)
\end{aligned}$$

(3) Vi har:

$$\begin{aligned}
\mathbb{L}_{4027}^{17} &= \mathbb{L}_{17}^{4027} && (\text{G}, 17 \equiv 1 \pmod 4)\\
&= \mathbb{L}_{17}^{15} && (\text{B}, 4027 \equiv 15 \pmod{17})\\
&= \mathbb{L}_{17}^{3 \cdot 5} && (3 \cdot 5 \text{ er en primtallsfaktorisering til } 15)\\
&= \mathbb{L}_{17}^{3} \cdot \mathbb{L}_{17}^{5}
\end{aligned}$$

(4) Vi har:

$$\begin{aligned}
\mathbb{L}_{17}^{3} &= \mathbb{L}_{3}^{17} && (\text{G, } 17 \equiv 1 \pmod 4)\\
&= \mathbb{L}_{3}^{2} && (\text{B, } 17 \equiv 2 \pmod 3)\\
&= -1 && (\text{F, } 3 \equiv 3 \pmod 8).
\end{aligned}$$

(5) Vi har:

$$\begin{aligned}
\mathbb{L}_{17}^{5} &= \mathbb{L}_{5}^{17} && (\text{G, } 17 \equiv 1 \pmod 4)\\
&= \mathbb{L}_{5}^{2} && (\text{B, } 17 \equiv 2 \pmod 5)\\
&= -1 && (\text{F, } 5 \equiv 5 \pmod 8).
\end{aligned}$$

(6) Det følger fra (3) – (5) at

$$\mathbb{L}_{4027}^{17} = \mathbb{L}_{17}^{3} \cdot \mathbb{L}_{17}^{5} = (-1) \cdot 1 = 1.$$

Det følger fra (1), (2), og (6) at

$$\mathbb{L}_{4027}^{2720} = -\mathbb{L}_{4027}^{5} \cdot \mathbb{L}_{4027}^{17} = -(-1) \cdot 1 = 1.$$

Dermed er 2720 en kvadratisk rest modulo 4027. Det følger fra teorien fra kvadratiske kongruenser i kurset (Korollar 5.2.30) at det finnes to heltall x slik at x er en løsning til kongruensen i oppgaven og slik at $0 \leq x < 4027$.

En alternativ måte å regne ut $\mathbb{L}_{17}^{15}$ er:

$$\begin{aligned}
\mathbb{L}_{17}^{15} &= \mathbb{L}_{17}^{-2} && (\text{B, } 15 \equiv -2 \pmod{17})\\
&= \mathbb{L}_{17}^{(-1)\cdot 2}\\
&= \mathbb{L}_{17}^{-1} \cdot \mathbb{L}_{17}^{2} && (\text{A})\\
&= \mathbb{L}_{17}^{-1} \cdot 1 && (\text{F, } 17 \equiv 1 \pmod 8)\\
&= \mathbb{L}_{17}^{-1}\\
&= (-1)^{\frac{17-1}{2}} && (\text{E})\\
&= (-1)^{8}\\
&= 1
\end{aligned}$$

Løsning til Oppgave 17. Først oversetter vi meldingen fra symboler til heltall ved å benytte Tabell 6.1. Vi får:

$$9\ \ 11\ \ 11\ \ 5\ \ 0\ \ 19\ \ 29\ \ 14\ \ 20\ \ 42.$$

Nå opphøyer vi alle disse heltallene i 11. Vi får:

$$9^{11}\ \ 11^{11}\ \ 11^{11}\ \ 5^{11}\ \ 0^{11}\ \ 19^{11}\ \ 29^{11}\ \ 14^{11}\ \ 20^{11}\ \ 42^{11}.$$

Nå erstatter vi disse heltallene med heltall som er kongruent til dem modulo 62, men som er mindre enn 62 og større enn eller like 0. Vi får:

$$45\ \ 55\ \ 55\ \ 25\ \ 0\ \ 41\ \ 29\ \ 40\ \ 38\ \ 24.$$

Løsning til Oppgave 18. Siden 5 og 11 er primtall og $55 = 5 \cdot 11$, er $(5, 11)$ den private nøkkelen til person B. For å dekryptere meldingen, finner vi først en invers til 7 modulo $(5-1)(11-1)$, altså modulo 40. Det vil si: vi finner først et naturlig tall x slik at

$$7x \equiv 1 \pmod{40}.$$

For å gjøre dette, benytter vi Euklids algoritme som følger.

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

Ved å benytte utregningen ovenfor, har vi følgende.

$$\begin{aligned} 5 &= 40 - 5 \cdot 7 \\ 2 &= 7 - 1 \cdot 5 \\ &= 7 - 1 \cdot (40 - 5 \cdot 7) \\ &= (-1) \cdot 40 + 6 \cdot 7 \\ 1 &= 5 - 2 \cdot 2 \\ &= (40 - 5 \cdot 7) - 2 \cdot ((-1) \cdot 40 + 6 \cdot 7) \\ &= 3 \cdot 40 + (-17) \cdot 7. \end{aligned}$$

Dermed er

$$7 \cdot (-17) - 1 = (-3) \cdot 40 \equiv 0 \pmod{40},$$

altså

$$7 \cdot (-17) \equiv 1 \pmod{40}.$$

Således er $x = -17$ en løsning til kongruensen

$$7x \equiv 1 \pmod{40}.$$

Vi har:

$$-17 \equiv 23 \pmod{40}.$$

Derfor er $x = 23$ en løsning til kongruensen

$$7x \equiv 1 \pmod{40}.$$

I tillegg er 23 et naturlig tall. Dermed er 23 inversen til 7 modulo 40.

Nå opphøyer vi alle heltallene i den krypterte meldingen i 23. Vi får:

$$2^{23}\ 21^{23}\ 17^{23}\ 17^{23}\ 1^{23}\ 48^{23}.$$

Nå erstatter vi disse heltallene med heltall som er kongruent til dem modulo 55, og som er større enn eller like 0 og mindre enn 55. Vi får:

$$8\ 21\ 18\ 18\ 1\ 42.$$

Nå oversetter vi fra heltall til symboler ved å benytte Tabell 6.1. Vi får: «Hurra!».

Løsning til Oppgave 19. Vi må finne et heltall x slik at følgende er sanne:

(1) $x \equiv 5 \pmod 8$;

(2) $x \equiv 2 \pmod{13}$.

Vi gjør følgende observasjoner.

(1) Vi har: $x = 5$ er en løsning til kongruensen

$$13x \equiv 1 \pmod 8.$$

Vi kan komme fram til denne løsningen ved å gå gjennom 0, 1, ..., 7 til vi når en løsning. Alternativt kan vi benytte Euklids algoritme.

(2) Vi har: $x = 5$ er en løsning til kongruensen

$$8x \equiv 1 \pmod{13}.$$

Igjen kan vi komme fram til denne løsningen ved å gå gjennom 0, 1, ..., 12 til vi når en løsning. Alternativt kan vi benytte Euklids algoritme.

Det følger fra (1), (2), og det kinesiske restteoremet at

$$x = 13 \cdot 5 \cdot 5 + 8 \cdot 5 \cdot 2,$$

altså $x = 405$, er en løsning både til $x \equiv 5 \pmod 8$ og $x \equiv 2 \pmod{13}$.

Alle heltallene som er en løsning til disse to kongruensene er: $x = 405 + (8 \cdot 13)t$, altså $x = 405 + 104t$, hvor t er et hvilket som helst heltall.

Løsning til Oppgave 20. Først løser vi (1) og (2). Vi gjør følgende observasjoner.

(1) Vi har: $x = 1$ er en løsning til kongruensen

$$9x \equiv 1 \pmod 4.$$

(2) Vi har: $x = 7$ er en løsning til kongruensen

$$4x \equiv 1 \pmod 9.$$

Vi kan komme fram til denne løsningen ved å gå gjennom 0, 1, ..., 8 til vi når en løsning. Alternativt kan vi benytte Euklids algoritme.

(3) Det følger fra (1), (2), og det kinesiske restteoremet at

$$x = 9 \cdot 1 \cdot 3 + 4 \cdot 7 \cdot 8,$$

altså $x = 251$, er en løsning både til $x \equiv 3 \pmod 4$ og $x \equiv 8 \pmod 9$. Alle heltallene som er en løsning til disse to kongruensene er: $x = 251 + (4 \cdot 9)t$, altså $x = 251 + 36t$, hvor t er et hvilket som helst heltall.

Nå løser vi kongruensene

$$x \equiv 251 \pmod{36}$$

og

$$x \equiv 2 \pmod{11}.$$

Vi finner først en løsning til kongruensen

$$11x \equiv 1 \pmod{36}$$

og til kongruensen

$$36x \equiv 1 \pmod{11}.$$

For å gjøre dette, benytter vi Euklids algoritme som følger.

$$\begin{aligned} 36 &= 3 \cdot 11 + 3 \\ 11 &= 3 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Fra disse ligningene får vi følgende.

$$\begin{aligned} 3 &= 36 - 3 \cdot 11 \\ 2 &= 11 - 3 \cdot 3 \\ &= 11 - 3 \cdot (36 - 3 \cdot 11) \\ &= (-3) \cdot 36 + 10 \cdot 11 \\ 1 &= 3 - 1 \cdot 2 \\ &= (36 - 3 \cdot 11) - 1 \cdot ((-3) \cdot 36 + 10 \cdot 11) \\ &= 4 \cdot 36 + (-13) \cdot 11 \end{aligned}$$

Vi gjør følgende observasjoner.

(1) Det følger at

$$11 \cdot (-13) - 1 = (-4) \cdot 36 \equiv 0 \pmod{36},$$

altså at

$$11 \cdot (-13) \equiv 1 \pmod{36}.$$

Således er $x = -13$ en løsning til kongruensen

$$11x \equiv 1 \pmod{36}.$$

(2) I tillegg følger det at

$$36 \cdot 4 - 1 = 13 \cdot 11 \equiv 0 \pmod{11},$$

altså at

$$36 \cdot 4 \equiv 1 \pmod{11}.$$

Således er $x = 4$ en løsning til kongruensen

$$36x \equiv 1 \pmod{11}.$$

Det følger fra (1), (2), og det kinesiske restteoremet at

$$x = 11 \cdot (-13) \cdot 251 + 36 \cdot 4 \cdot 2,$$

altså $x = -35605$, er en løsning både til $x \equiv 251 \pmod{36}$ og $x \equiv 2 \pmod{11}$. Vi konkluderer at $x = -35605$ er en løsning til alle de tre kongruensene i oppgaven.

Alle heltallene som er en løsning til disse tre kongruensene er: $x = -35605 + (36 \cdot 11)t$, altså $x = -35606 + 396t$, hvor t er et hvilket som helst heltall.

Løsning til Oppgave 21. Vi gjør følgende observasjoner.

(1) Vi har: $x = 6$ er en løsning til kongruensen

$$13x \equiv 1 \pmod{7}.$$

Vi kan komme fram til denne løsningen ved å gå gjennom 0, 1, ..., 6 til vi når en løsning. Alternativt kan vi benytte Euklids algoritme.

(2) Vi har: $x = 5$ er en løsning til kongruensen

$$21x \equiv 1 \pmod{13},$$

altså til kongruensen

$$7 \cdot (3x) \equiv 1 \pmod{13}.$$

Igjen kan vi komme fram til denne løsningen ved å gå gjennom 0, 1, ..., 12 til vi når en løsning. Alternativt kan vi benytte Euklids algoritme.

Det følger fra (1), (2), og et argument som ligner på beviset for del (I) av det kinesiske restteoremet at

$$x = 13 \cdot 6 \cdot 2 + 7 \cdot 5 \cdot 5,$$

altså $x = 331$, er en løsning både til $x \equiv 2 \pmod{7}$ og $3x \equiv 5 \pmod{13}$.