Løsninger – Øving 7

Merknad. I løsningen til Oppgave 1 benytter vi oss av notasjonen i Proposisjon 3.4.16 og Korollar 3.4.36.

Løsning til Oppgave 1. La oss finne løsningene til kongruensen

$$-6x \equiv 15 \pmod{27}.$$

Vi gjør følgende.

(1) Først regner vi ut $\mathsf{sfd}(-6, 27)$. Vi har $\mathsf{sfd}(-6, 27) = 3$. Siden $3 \mid 15$, fastslår Proposisjon 3.4.9 at kongruensen har en løsning.

(2) Nå prøver vi å finne én løsning. Ut ifra (1) og Proposisjon 3.4.13, er x en løsning til kongruensen

$$-6x \equiv 15 \pmod{27}$$

hvis og bare hvis x er en løsning til kongruensen

$$-2x \equiv 5 \pmod{9}.$$

Vi skal prøve å finne én løsning til denne kongruensen.

(3) Hvis vi går gjennom heltallene x slik at $0 \leq x < 9$, ser vi at $x = 2$ er en løsning til kongruensen

$$-2x \equiv 5 \pmod{9}.$$

Vi har nemlig:

$$-2 \cdot 2 - 5 = -9$$

og $9 \mid -9$.

(4) Siden $27 = 9 \cdot 3$, er $k_n = 9$. Da følger det fra (3) og Proposisjon 3.4.16 at:

(I) $x = 2 + 9 \cdot 0$, $x = 2 + 9 \cdot 1$, og $x = 2 + 9 \cdot 2$, altså $x = 2$, $x = 11$, og $x = 20$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 27 til én av disse to;

(III) ikke noe par av disse tre løsningene er ikke kongruent modulo 27 til hverandre.

Istedenfor å argumentere som i (3), kan vi først finne en løsning til kongruensen

$$-2y \equiv 1 \pmod 9.$$

Ved å gå gjennom heltallene y slik at $0 \leq y < 9$, ser vi at $y = 4$ er en løsning. Da følger det fra Proposisjon 3.4.42 at $x = 4 \cdot 5$, altså $x = 20$, er en løsning til kongruensen

$$-2x \equiv 5 \pmod 9.$$

Når vi deler 20 med 9, får vi 2 som resten. Det følger fra Proposisjon 3.4.24 at $x = 2$ er en løsning til kongruensen

$$-2x \equiv 5 \pmod 9.$$

Da kan vi fortsette som ovenfor.

Alternativt kan vi for eksempel benytte algoritmen i Merknad 2.7.15. Vi vet at

$$\mathsf{sfd}(-6, 27) = 3.$$

Vi får:

$$3 = 4 \cdot (-6) + 1 \cdot 27.$$

Siden $15 = 5 \cdot 3$, er $k = 5$. Da fastslår Korollar 3.4.36 at:

(I) $x = 5 \cdot 4 + 9 \cdot 0$, $x = 5 \cdot 4 + 9 \cdot 1$, og $x = 5 \cdot 4 + 9 \cdot 2$, altså $x = 20$, $x = 29$, og $x = 38$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 27 til én av disse to;

(III) ikke noe par av disse tre løsningene er ikke kongruent modulo 27 til hverandre.

Når vi deler 20, 29, og 38 med 27, får vi 20, 2 og 11 som restene. Det følger fra Proposisjon 3.4.24, Proposisjon 3.2.24, og Proposisjon 3.2.33 at

(I) $x = 2 + 9 \cdot 0$, $x = 2 + 9 \cdot 1$, og $x = 2 + 9 \cdot 2$, altså $x = 2$, $x = 11$, og $x = 20$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 27 til én av disse tre;

(III) ikke noe par av disse tre løsningene er ikke kongruent modulo 27 til hverandre.

Flere andre gyldige argumenter kan gis.

La oss nå finne løsningene til kongruensen

$$104x \equiv -56 \pmod{128}.$$

Vi gjør følgende.

(1) Først regner vi ut $\mathsf{sfd}(104, 128)$. Vi har $\mathsf{sfd}(104, 128) = 8$. Siden $8 \mid -56$, fastslår Proposisjon 3.4.9 at kongruensen har en løsning.

(2) Nå prøver vi å finne én løsning. Ut ifra (1) og Proposisjon 3.4.13, er x en løsning til kongruensen

$$104x \equiv -56 \pmod{128}$$

hvis og bare hvis x er en løsning til kongruensen

$$13x \equiv -7 \pmod{16}.$$

Vi kan godt gå gjennom alle heltallene x slik at $0 \leq x < 16$ for å finne én løsning, eller prøve å finne først en løsning til kongruensen

$$13x \equiv -7 \mod 16.$$

Imidlertid ser dette litt slitsomme ut: i dette tilfellet kan vi sannsynligvis finne løsningene til kongruensen

$$104x \equiv -56 \pmod{128}$$

fortere om vi benytter algoritmen i Merknad 2.7.15.

(3) Hvis vi gjør dette, får vi:

$$8 = 5 \cdot 104 + (-4) \cdot 128.$$

Siden $-56 = (-7) \cdot 8$, er $k = -7$. Siden $128 = 16 \cdot 8$, er $k_n = 8$. Da fastslår Korollar 3.4.36 at:

(I) $x = (-7) \cdot 5 + 16 \cdot r$ er en løsning til kongruensen for hvert heltall r slik at $0 \leq r < 8$, altså $x = -35$, $x = -19$, $x = -3$, $x = 13$, $x = 29$, $x = 45$, $x = 61$, $x = 77$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 128 til én av disse to;

(III) ikke noe par av disse åtte løsningene er ikke kongruent modulo 128 til hverandre.

(4) Når vi deler -35, -19, -3, 13, 29, 45, 61, og 77 med 128, får vi 13, 29, 45, 61, 77, 93, 109, og 125 som restene. Det følger fra Proposisjon 3.4.24, Proposisjon 3.2.24, og Proposisjon 3.2.33 at

(I) $x = 13$, $x = 29$, $x = 45$, $x = 61$, $x = 77$, $x = 93$, $x = 109$, og $x = 125$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 128 til én av disse åtte;

(III) ikke noe par av disse åtte løsningene er ikke kongruent modulo 128 til hverandre.

Flere andre gyldige argumenter kan gis.

La oss nå finne løsningene til kongruensen

$$7x \equiv 2 \pmod{50}.$$

Vi gjør følgende.

(1) Først regner vi ut $\mathsf{sfd}(7, 50)$. Vi har $\mathsf{sfd}(7, 50) = 1$. Siden $1 \mid 2$, fastslår Proposisjon 3.4.9 at kongruensen har en løsning.

(2) Nå prøver vi å finne én løsning. Vi har: $y = -7$ er en løsning til kongruensen

$$7y \equiv 1 \pmod{50},$$

siden

$$7 \cdot (-7) - 1 = -50$$

og $50 \mid -50$. Det følger fra Proposisjon 3.4.42 at $x = (-7) \cdot 2$, altså $x = -14$, er en løsning til kongruensen

$$7x \equiv 2 \pmod{50}.$$

(3) Når vi deler -14 med 50, får vi 36 som resten. Det følger fra Proposisjon 3.4.24 at $x = 36$ er en løsning til kongruensen

$$7x \equiv 2 \pmod{50}.$$

Ut ifra Proposisjon 3.4.16, er enhver annen løsning kongruent modulo 50 til denne.

Alternativt kan vi benytte algoritmen i Merknad 2.7.15. Vi får:

$$1 = (-7) \cdot 7 + 1 \cdot 50.$$

Siden $2 = 2 \cdot 1$, er $k = 2$. Da fastlår Korollar 3.4.36 at $x = 2 \cdot (-7)$, altså $x = -14$, er en løsning til kongruensen, og enhver annen løsning er kongruent modulo 50 til denne. Som ovenfor, får vi 36 som resten når vi deler -14 med 50. Da følger det fra Proposisjon 3.4.24, Proposisjon 3.2.24, og Proposisjon 3.2.33 at $x = 36$ er en løsning til kongruensen, og enhver annen løsning er kongruent modulo 50 til denne.

Flere andre gyldige argumenter kan gis.

Løsning til Oppgave 2. De naturlige tallene x slik at $30 \leq x \leq 45$ som er primtall er: 31, 37, 41, og 43.

Løsning til Oppgave 3. Anta først at

$$p \equiv 7 \pmod{10}.$$

Vi gjør følgende observasjoner.

(1) Siden

$$p \equiv 7 \pmod{10},$$

følger det fra Proposisjon 3.2.48 at

$$p^2 \equiv 7^2 \pmod{10},$$

altså at

$$p^2 \equiv 49 \pmod{10}.$$

(2) Siden $49 - (-1) = 50$ og $10 \mid 50$, er

$$49 \equiv -1 \pmod{10}.$$

Det følger fra (1), (2), og Proposisjon 3.2.33 at

$$p^2 \equiv -1 \pmod{10}.$$

Således har vi bevist at, dersom

$$p \equiv 7 \pmod{10},$$

er

$$p^2 \equiv -1 \pmod{10}.$$

Anta nå at $p \equiv 4 \pmod{10}$. Siden $2 \mid 4$ og $2 \mid 10$, følger det fra Proposisjon 3.2.54 at $p \equiv 0 \pmod{2}$. Fra Proposisjon 3.2.13 har vi da: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Det følger at $p = 2$. Imidlertid vet vi at $p > 2$. Det kan ikke være sant at både $p = 2$ og $p > 2$. Siden antakelsen at $p \equiv 4 \pmod{10}$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $p \equiv 4 \pmod{10}$.

La oss nå bevise at enten $p^2 - 1$ er delelig med 10 eller $p^2 + 1$ er delelig med 10. Ut ifra Proposisjon 3.2.1 er ett av følgende sant:

(A) $p \equiv 0 \pmod{10}$;

(B) $p \equiv 1 \pmod{10}$;

(C) $p \equiv 2 \pmod{10}$;

(D) $p \equiv 3 \pmod{10}$;

(E) $p \equiv 4 \pmod{10}$;

(F) $p \equiv 5 \pmod{10}$.

(G) $p \equiv 6 \pmod{10}$;

(H) $p \equiv 7 \pmod{10}$;

(I) $p \equiv 8 \pmod{10}$;

(J) $p \equiv 9 \pmod{10}$.

Anta først at (A) er sant. Fra Proposisjon 3.2.13 har vi da: $10 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 10$. Imidlertid er 10 ikke et primtall. Siden antakelsen at (A) er sant fører til motsigelsen at p både er og er ikke et primtall, konkluderer vi at (A) ikke er sant.

Anta nå at (B) er sant. Da følger det fra Proposisjon 3.2.48 at

$$p^2 \equiv 1^2 \pmod{10},$$

altså at

$$p^2 \equiv 1 \pmod{10}.$$

Da følger det fra Korollar 3.2.39 at

$$p^2 - 1 \equiv 1 - 1 \pmod{10},$$

altså at

$$p^2 - 1 \equiv 0 \pmod{10}.$$

Fra Proposisjon 3.2.13 følger det at

$$10 \mid p^2 - 1.$$

Anta nå at (C) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod{2}$. Fra Proposisjon 3.2.13 følger det at: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 2$. Imidlertid vet vi at $p > 2$. Siden antakelsen at (C) er sant fører til motsigelsen at både $p = 2$ og $p > 2$, konkluderer vi at (C) ikke er sant.

Vi beviste ovenfor at (D) ikke er sant. Anta nå at (E) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod{5}$. Fra Proposisjon 3.2.13 følger det at: $5 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 5$. Imidlertid vet vi at $p \neq 5$. Siden antakelsen at (E) er sant fører til motsigelsen at både $p = 5$ og $p \neq 5$, konkluderer vi at (E) ikke er sant.

Anta nå at (F) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod{2}$. Ved å benytte det samme argumentet som i tilfellet hvor vi antok at (C) var sant, følger det at (F) ikke er sant.

Anta nå at (G) er sant. Vi beviste ovenfor at vi da har:

$$p^2 \equiv -1 \pmod{10}.$$

Da følger det fra Korollar 3.2.39 at

$$p^2 + 1 \equiv -1 + 1 \pmod{10},$$

altså at

$$p^2 + 1 \equiv 0 \pmod{10}.$$

Fra Proposisjon 3.2.13 følger det at

$$10 \mid p^2 + 1.$$

Anta nå at (H) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod 2$. Ved å benytte det samme argumentet som i tilfellet hvor vi antok at (C) var sant, følger det at (H) ikke er sant.

Anta nå at (I) er sant. Vi gjør følgende observasjoner.

(1) Siden

$$p \equiv 9 \pmod{10},$$

følger det fra Proposisjon 3.2.48 at

$$p^2 \equiv 9^2 \pmod{10},$$

altså at

$$p^2 \equiv 81 \pmod{10}.$$

(2) Siden $81 - 1 = 80$ og $10 \mid 80$, er

$$81 \equiv 1 \pmod{10}.$$

Det følger fra (1), (2), og Proposisjon 3.2.33 at

$$p^2 \equiv 1 \pmod{10}.$$

Da følger det fra Korollar 3.2.39 at

$$p^2 - 1 \equiv 1 - 1 \pmod{10},$$

altså at

$$p^2 - 1 \equiv 0 \pmod{10}.$$

Fra Proposisjon 3.2.13 følger det at

$$10 \mid p^2 - 1.$$

Således har vi bevist: i alle tilfellene som er mulige, har vi enten

$$10 \mid p^2 - 1$$

eller

$$10 \mid p^2 + 1.$$

Løsning til Oppgave 4. De første 10 primtallene p slik at

$$p \equiv 5 \pmod 6$$

er 5, 11, 17, 23, 29, 41, 47, 53, 59, 71.

La n være et naturlig tall. La oss nå bevise at det er et primtall p slik at

$$p \equiv 5 \pmod 6$$

og $p > n$. La q være produktet av alle primtallene som er mindre enn eller like n, og som er kongruent til 5 modulo 6. Ut ifra Teorem 4.3.3 er det et naturlig tall t og primtall p_1, ..., p_t slik at

$$6q - 1 = p_1 \cdots p_t.$$

Ut ifra Proposisjon 3.2.1 er, for hvert naturlig tall i slik at $i \leq t$, ett av følgende sant:

(1) $p_i \equiv 0 \pmod 6$;

(2) $p_i \equiv 1 \pmod 6$;

(3) $p_i \equiv 2 \pmod 6$;

(4) $p_i \equiv 3 \pmod 6$;

(5) $p_i \equiv 4 \pmod 6$;

(6) $p_i \equiv 5 \pmod 6$;

Anta først at (1) er sant for et naturlig tall $i \leq t$.. Da følger det fra Korollar 3.2.45 at

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 6,$$

altså at

$$6q - 1 \equiv 0 \pmod 6.$$

Imidlertid er

$$6q - 1 \equiv 5 \pmod 6.$$

Siden $0 \neq 5$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$6q - 1 \equiv 0 \pmod 6$$

og

$$6q - 1 \equiv 5 \pmod 6.$$

Siden antakelsen at (1) er sant fører til denne motigelsen, konkluderer vi at (1) ikke er sant.

Anta nå at (3) er sant for et naturlig tall $i \leq t$. Da følger det fra Proposisjon 3.2.54 at $p_i \equiv 0 \pmod 2$. Ut ifra Korollar 3.2.45 er da

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 2,$$

altså

$$6q - 1 \equiv 0 \pmod 2.$$

Imidlertid er

$$6q - 1 \equiv 1 \pmod 2.$$

Siden $0 \neq 1$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$6q - 1 \equiv 0 \pmod 2$$

og

$$6q - 1 \equiv 1 \pmod 2.$$

Siden antakelsen at (3) er sant fører til denne motigelsen, konkluderer vi at (3) ikke er sant.

Anta nå at (4) er sant for et naturlig tall $i \leq t$. Da følger det fra Proposisjon 3.2.54 at $p_i \equiv 0 \pmod 3$. Ut ifra Korollar 3.2.45 er da

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 2,$$

altså

$$6q - 1 \equiv 0 \pmod 3.$$

Imidlertid er

$$6q - 1 \equiv 2 \pmod 3.$$

Siden $0 \neq 2$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$6q - 1 \equiv 0 \pmod 3$$

og

$$6q - 1 \equiv 2 \pmod 3.$$

Siden antakelsen at (4) er sant fører til denne motigelsen, konkluderer vi at (4) ikke er sant.

Anta nå at (5) er sant for et naturlig tall $i \leq t$. Da følger det fra Proposisjon 3.2.54 at $p_i \equiv 0 \pmod 2$. Som i tilfellet da vi antok at (3) er sant, fører dette til en motsigelse. Vi konkluderer at (5) ikke er sant.

Anta nå at (2) er sant for alle de naturlige tallene i slik at $i \leq t$. Da følger det fra Proposisjon 3.2.42 at

$$p_1 \cdots p_t \equiv 1^t \pmod 6,$$

altså at

$$6q - 1 \equiv 1 \pmod 6.$$

Imidlertid er

$$6q - 1 \equiv 5 \pmod 5.$$

Siden $1 \neq 5$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$6q - 1 \equiv 1 \pmod 6$$

og

$$6q - 1 \equiv 5 \pmod 6.$$

Siden antakelsen at (2) er sant fører til denne motigelsen, konkluderer vi at (2) ikke er sant for alle de naturlige tallene i slik at $i \leq t$.

Derfor finnes det et naturlig tall i, hvor $i \leq t$, slik at (6) er sant, altså at $p_i \equiv 5 \pmod 6$. Anta at $p_i \leq n$. Vi gjør følgende observasjoner.

(1) Siden $p_i \equiv 5 \pmod 6$, følger det fra definisjonen til q og antakelsen at $p_i \leq n$ at $p_i \mid q$.

(2) Siden

$$6q - 1 = p_i \cdot (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t),$$

har vi: $p_i \mid 6q - 1$.

(3) Det følger fra (1) og Korollar 2.5.18 at $p_i \mid 6q$.

(4) Det følger fra (2) og Korollar 2.5.18 at $p_i \mid -(6q - 1)$.

(5) Det følger fra (3), (4), og Proposisjon 2.5.24 at $p_i \mid 6q - (6q - 1)$, altså at $p_i \mid 1$.

Siden p_i er et primtall, er $p_i \geq 2$. Det kan ikke være sant at både $p_i \mid 1$ og $p_i \geq 2$. Siden antakelsen at $p_i \leq n$ fører til denne motsigelsen, deduserer vi at det ikke er sant at $p_i \leq n$. Derfor er $p_i > n$.

Løsning til Oppgave 5. Ut ifra Proposisjon 3.2.1 er ett av følgende sant:

(A) $n \equiv 0 \pmod 5$;

(B) $n \equiv 1 \pmod 5$;

(C) $n \equiv 2 \pmod 5$;

(D) $n \equiv 3 \pmod 5$;

(E) $n \equiv 4 \pmod 5$.

Anta først at (A) er sant. Ut ifra Proposisjon 3.2.48 er da

$$n^4 \equiv 0^4 \pmod 5,$$

altså

$$n^4 \equiv 0 \pmod 5.$$

Fra Proposisjon 3.2.13 deduserer vi at $5 \mid n^4$, altså at det er et heltall m slik at $n^4 = 5m$.

Anta nå at (B) er sant. Ut ifra Proposisjon 3.2.48 er da

$$n^4 \equiv 1^4 \pmod 5,$$

altså

$$n^4 \equiv 1 \pmod 5.$$

Fra Proposisjon 3.2.13 deduserer vi at $5 \mid n^4 - 1$. Dermed er det et heltall m slik at $n^4 - 1 = 5m$, altså at $n^4 = 5m + 1$.

Anta nå at (C) er sant. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.48 er da

$$n^4 \equiv 2^4 \pmod 5,$$

altså

$$n^4 \equiv 16 \pmod 5.$$

(2) Siden $16 - 1 = 15$ og $5 \mid 15$, er

$$16 \equiv 1 \pmod 5.$$

Det følger fra (1), (2), og Proposisjon 3.2.33 at

$$n^4 \equiv 1 \pmod 5.$$

Fra Proposisjon 3.2.13 deduserer vi at $5 \mid n^4 - 1$. Dermed er det et heltall m slik at $n^4 - 1 = 5m$, altså at $n^4 = 5m + 1$.

Anta nå at (D) er sant. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.48 er da

$$n^4 \equiv 3^4 \pmod 5,$$

altså

$$n^4 \equiv 81 \pmod 5.$$

(2) Siden $81 - 1 = 80$ og $5 \mid 80$, er

$$81 \equiv 1 \pmod 5.$$

Det følger fra (1), (2), og Proposisjon 3.2.33 at

$$n^4 \equiv 1 \pmod 5.$$

Fra Proposisjon 3.2.13 deduserer vi at $5 \mid n^4 - 1$. Dermed er det et heltall m slik at $n^4 - 1 = 5m$, altså at $n^4 = 5m + 1$.

Anta nå at (E) er sant. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.48 er da

$$n^4 \equiv 4^4 \pmod 5.$$

(2) Siden $4^2 - 1 = 16 - 1 = 15$ og $5 \mid 15$, er

$$4^2 \equiv 1 \pmod{5}.$$

Da følger det fra Proposisjon 3.2.48 at

$$\left(4^2\right)^2 \equiv 1^2 \pmod{5},$$

altså at

$$4^4 \equiv 1 \pmod{5}.$$

Det følger fra (1), (2), og Proposisjon 3.2.33 at

$$n^4 \equiv 1 \pmod{5}.$$

Fra Proposisjon 3.2.13 deduserer vi at $5 \mid n^4 - 1$. Dermed er det et heltall m slik at $n^4 - 1 = 5m$, altså at $n^4 = 5m + 1$.

Således har vi bevist: i alle mulige tilfeller, er det et heltall m slik at $n^4 = 5m$ eller $n^4 = 5m + 1$.