Innhold

3 Modulær aritmetikk

3.1 Kongruens

Merknad 3.1.1. Hva er klokka sju timer etter kl. 20? Selvfølgelig er den kl. 3. Vi sier ikke at den er kl. 27!

Etter 24 timer, begynner klokka på 0 igjen: midnatt er både kl. 24 og kl. 0. På en måte er derfor 24 «lik» 0 når vi ser på klokka. Ved å utvide dette litt, kan vi si at 3 er «lik» 27 når vi ser på ei klokke.

Denne måten å telle på kalles «aritmetikk modulo 24». Istedenfor å si at 3 er «lik» 27 når vi teller timene, sier vi at 3 er «kongruent til 27 modulo 24».

Vi kan telle på lignende vis ved å erstatte 24 med et hvilket som helst heltall. I dette kapittelet kommer vi til å studere disse måtene å telle på. Teorien er svært viktig i alle deler av tallteori, og i mange andre områder innen matematikk.

Definisjon 3.1.2. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Da er x og y *kongruent modulo* n dersom $n \mid x - y$.

Merknad 3.1.3. Ut ifra Definisjon 2.5.1 er x og y kongruent modulo n hvis og bare hvis det finnes et heltall k slik at $x - y = kn$.

Terminologi 3.1.4. Hvis x og y er kongruent modulo n, sier vi ofte at x er *kongruent til* y *modulo* n.

Terminologi 3.1.5. «Modulo» forkortes ofte til «mod».

Notasjon 3.1.6. Hvis x og y er kongruent modulo n, skriver vi:

$$x \equiv y \pmod{n}.$$

Eksempel 3.1.7. Siden

$$27 - 3 = 24$$

og $24 \mid 24$, er

$$27 \equiv 3 \pmod{24}.$$

Eksempel 3.1.8. Siden

$$24 - 0 = 24$$

og $24 \mid 24$, er

$$24 \equiv 0 \pmod{24}.$$

Eksempel 3.1.9. Siden

$$53 - 5 = 48$$

og $24 \mid 48$, er

$$53 \equiv 5 \pmod{24}.$$

Eksempel 3.1.10. Siden

$$5 - 3 = 2$$

og $2 \mid 2$ er

$$5 \equiv 3 \pmod{2}.$$

Eksempel 3.1.11. Siden

$$57 - 13 = 44$$

og $2 \mid 44$, er

$$57 \equiv 13 \pmod{2}.$$

Eksempel 3.1.12. Siden

$$21 - 35 = -14$$

og $2 \mid -14$, er

$$21 \equiv 35 \pmod{2}.$$

Eksempel 3.1.13. Siden

$$40 - 124 = -84$$

og $2 \mid -84$, er

$$40 \equiv 124 \pmod{2}.$$

Eksempel 3.1.14. Siden

$$-17 - 21 = -38$$

og $2 \mid -38$, er

$$-17 \equiv 21 \pmod{2}.$$

Eksempel 3.1.15. Siden

$$-22 - (-108) = -22 + 108 = 86$$

og $2 \mid 86$, er

$$-22 \equiv -108 \pmod{2}.$$

Eksempel 3.1.16. Siden

$$-12 - (-4) = -12 + 4 = -8$$

og $2 \mid -8$, er

$$-12 \equiv -4 \pmod{2}.$$

Eksempel 3.1.17. Siden

$$11 - 5 = 6$$

og $3 \mid 6$, er

$$11 \equiv 5 \pmod{3}.$$

Eksempel 3.1.18. Siden

$$0 - 27 = -27$$

og $3 \mid -27$, er

$$0 \equiv 27 \pmod{3}.$$

Eksempel 3.1.19. Siden

$$14 - 17 = -3$$

og $3 \mid -3$, er

$$14 \equiv 17 \pmod{3}.$$

Eksempel 3.1.20. Siden

$$14 - 17 = -3$$

og $3 \mid -3$, er

$$14 \equiv 17 \pmod{3}.$$

Eksempel 3.1.21. Siden

$$-32 - 25 = -57$$

og $3 \mid -57$, er

$$-32 \equiv 25 \pmod{3}.$$

Eksempel 3.1.22. Siden

$$19 - (-59) = 19 + 59 = 78$$

og $3 \mid 78$, er

$$19 \equiv -59 \pmod{3}.$$

Eksempel 3.1.23. Siden

$$-23 - (-11) = -23 + 11 = -12$$

og $3 \mid -12$, er

$$-23 \equiv -11 \pmod{3}.$$

Eksempel 3.1.24. Siden

$$89 - 17 = 72$$

og $-8 \mid 72$, er

$$89 \equiv 17 \pmod{-8}.$$

Eksempel 3.1.25. Siden

$$33 - 25 = 8$$

og $-8 \mid 8$, er

$$33 \equiv 25 \pmod{-8}.$$

Eksempel 3.1.26. Siden

$$14 - 54 = -40$$

og $-8 \mid -40$, er

$$14 \equiv 54 \pmod{-8}.$$

Eksempel 3.1.27. Siden

$$-12 - 36 = -48$$

og $-8 \mid -48$, er

$$-12 \equiv 36 \pmod{-8}.$$

Eksempel 3.1.28. Siden

$$-17 - (-49) = 32$$

og $-8 \mid 32$, er

$$-17 \equiv -49 \pmod{-8}.$$

3.2 Grunnleggende proposisjoner om kongruens

Proposisjon 3.2.1. La n være et naturlig tall. La x være et heltall. Da finnes det et heltall r slik at de følgende er sanne:

(I) $x \equiv r \pmod{n}$;

(II) $0 \leq r < n$.

Bevis. Ut ifra Korollar 2.2.11 finnes det heltall k og r slik at:

(1) $x = kn + r$;

(2) $0 \leq r < n$.

Det følger fra (1) at

$$x - r = kn,$$

altså at

$$n \mid x - r.$$

Dermed er $x \equiv r \pmod{n}$.

□

Merknad 3.2.2. Proposisjon 3.2.1 fastslår at hvert heltall er kongruent modulo n til ett av heltallene 0, 1, 2, ..., $n - 1$.

Merknad 3.2.3. Gitt et naturlig tall n og et heltall x, fastlår beviset for Proposisjon 3.2.1 at vi kan finne r ved å benytte divisjonsalgoritmen: r er resten vi får ved å dele x med n.

Eksempel 3.2.4. Vi har:

$$22 = 7 \cdot 3 + 1,$$

altså $3 \mid 22 - 1$. Dermed er $22 \equiv 1 \pmod{3}$.

Eksempel 3.2.5. Vi har:

$$124 = 7 \cdot 17 + 8,$$

altså $17 \mid 124 - 8$. Dermed er $124 \equiv 8 \pmod{17}$.

Eksempel 3.2.6. Vi har

$$48 = 8 \cdot 6,$$

altså $6 \mid 48 - 0$. Dermed er $48 \equiv 0 \pmod{6}$.

Eksempel 3.2.7. Vi har:

$$-17 = (-4) \cdot 5 + 3,$$

altså $5 \mid -17 - 3$. Dermed er $-17 \equiv 3 \pmod{5}$.

Eksempel 3.2.8. Vi har:

$$-23 = (-6) \cdot 4 + 1,$$

altså $4 \mid -23 - 1$. Dermed er $-23 \equiv 1 \pmod{4}$.

Eksempel 3.2.9. Vi har:

$$-63 = (-9) \cdot 7,$$

altså $7 \mid -63 + 0$. Dermed er $-63 \equiv 0 \pmod{7}$.

Korollar 3.2.10. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da finnes det et heltall r slik at de følgende er sanne:

(I) $x \equiv r \pmod{n}$;

(II) $0 \leq r < |n|$.

Bevis. Ett av følgende utsagn er sant:

(A) $n > 0$;

(B) $n < 0$.

Anta først at (A) er sant. Da følger utsagnet umiddelbart fra Proposisjon 3.2.1.

Anta nå at (B) er sant. Da er $-n$ et naturlig tall. Det følger fra Proposisjon 3.2.1 at det finnes et heltall r slik at:

(1) $x \equiv r \pmod{-n}$;

(2) $0 \leq r < -n$.

Det følger fra (1) og Proposisjon 3.2.19 at

$$x \equiv r \pmod{n}.$$

Siden $n < 0$, er i tillegg $|n| = -n$. Dermed er

$$0 \leq r < |n|.$$

□

Proposisjon 3.2.11. La n være et heltall slik at $n \neq 0$. La r og s være heltall sik at $0 \leq r < |n|$ og $0 \leq s < |n|$. Dersom $r \equiv s \pmod{n}$, er $r = s$.

Bevis. Siden $r \equiv s \pmod{n}$, har vi $n \mid r - s$. Dermed finnes det et heltall k slik at

$$r - s = kn,$$

altså

$$r = kn + s.$$

I tillegg er

$$r = 0 \cdot k + r.$$

Det følger fra Korollar 2.2.20 at $r = s$. □

Merknad 3.2.12. Vi ønsker å manipulere kongruenser på en lignende måte som vi manipulere likheter. I resten av denne delen av kapittelet skal vi bevise at dette er gyldig. Når du leser bevisene, la merke til at vi bygger på de grunnleggende proposisjonene i §2.5 av Kapittel 2.

Proposisjon 3.2.13. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da er $x \equiv 0 \pmod{n}$ hvis og bare hvis $n \mid x$.

Bevis. Vi har: $x \equiv 0 \pmod{n}$ hvis og bare hvis $n \mid x - 0$, altså hvis og bare hvis $n \mid x$. □

Eksempel 3.2.14. Siden $3 \mid 18$, er $18 \equiv 0 \pmod{3}$.

Eksempel 3.2.15. Siden $5 \mid -20$, er $-20 \equiv 0 \pmod{5}$.

Proposisjon 3.2.16. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da er $x \equiv x \pmod{n}$.

Bevis. Siden $x - x = 0$ og $n \mid 0$, er $x \equiv x \pmod{n}$. □

Eksempel 3.2.17. Vi har: $3 \equiv 3 \pmod{5}$.

Eksempel 3.2.18. Vi har: $-11 \equiv -11 \pmod{7}$.

Proposisjon 3.2.19. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Anta at $x \equiv y \pmod{n}$. Da er $x \equiv y \pmod{-n}$.

Bevis. Siden $x \equiv y \pmod{n}$, har vi: $n \mid x - y$. Det følger fra Proposisjon 2.5.9 at $-n \mid x - y$. Dermed er $x \equiv y \pmod{-n}$.

□

Eksempel 3.2.20. Siden

$$32 - 17 = 15$$

og $5 \mid 15$, er

$$32 \equiv 17 \pmod{5}.$$

Derfor fastslår Proposisjon 3.2.19 at

$$32 \equiv 17 \pmod{-5}.$$

Eksempel 3.2.21. Siden

$$-6 - (-36) = 30$$

og $-5 \mid 30$, er

$$-6 \equiv -36 \pmod{-5}.$$

Derfor fastslår Proposisjon 3.2.19 at

$$-6 \equiv -36 \pmod{5}.$$

Korollar 3.2.22. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Da er $x \equiv y \pmod{n}$ hvis og bare hvis $x \equiv y \pmod{-n}$.

Bevis. Følger umiddelbart fra Proposisjon 3.2.19. □

Merknad 3.2.23. Siden Korollar 3.2.22 stemmer, kommer n i de aller fleste eksemplene videre til å bli et naturlig tall.

Proposisjon 3.2.24. La n være et heltall slik at $n \neq 0$. La x og y være heltall. Anta at $x \equiv y \pmod{n}$. Da er $y \equiv x \pmod{n}$.

Bevis. Siden $x \equiv y \pmod{n}$, er $n \mid x-y$. Det følger fra Proposisjon 2.5.12 at $n \mid -(x-y)$, altså at $n \mid y - x$. □

Eksempel 3.2.25. Siden

$$32 - 18 = 14$$

og $7 \mid 14$, er

$$32 \equiv 18 \pmod{7}.$$

Derfor fastslår Proposisjon 3.2.24 at

$$18 \equiv 32 \pmod{7}.$$

Eksempel 3.2.26. Siden

$$3 - 7 = -4$$

og $4 \mid -4$, er

$$3 \equiv 7 \pmod 4.$$

Derfor fastslår Proposisjon 3.2.24 at

$$7 \equiv 3 \pmod 4.$$

Eksempel 3.2.27. Siden

$$-8 - 24 = -32$$

og $16 \mid -32$, er

$$-8 \equiv 24 \pmod{16}.$$

Derfor fastslår Proposisjon 3.2.24 at

$$24 \equiv -8 \pmod{16}.$$

Eksempel 3.2.28. Siden

$$9 - (-11) = 9 + 11 = 20$$

og $5 \mid 20$, er

$$9 \equiv -11 \pmod 5.$$

Derfor fastslår Proposisjon 3.2.24 at

$$-11 \equiv 9 \pmod 5.$$

Eksempel 3.2.29. Siden

$$-5 - (-9) = -5 + 9 = 4$$

og $2 \mid 4$, er

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

Derfor fastslår Proposisjon 3.2.24 at

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

Korollar 3.2.30. La n være et heltall slik at $n \neq 0$. La x være et heltall. Da er $0 \equiv x \pmod n$ hvis og bare hvis $n \mid x$.

Bevis. Følger umiddelbart fra Proposisjon 3.2.13 og Proposisjon 3.2.24. □

Eksempel 3.2.31. Siden $7 \mid 21$, er $0 \equiv 21 \pmod 7$.

Eksempel 3.2.32. Siden $6 \mid -48$, er $0 \equiv -48 \pmod 6$.

Proposisjon 3.2.33. La n være et heltall slik at $n \neq 0$. La x, y, og z være heltall. Anta at $x \equiv y \pmod n$, og at $y \equiv z \pmod n$. Da er $x \equiv z \pmod n$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $x \equiv y \pmod{n}$, er $n \mid x - y$.

(2) Siden $y \equiv z \pmod{n}$, er $n \mid y - z$.

Det følger fra (1), (2), og Proposisjon 2.5.24 at $n \mid (x - y) + (y - z)$, altså at $n \mid x - z$. Dermed er $x \equiv z \pmod{n}$. □

Eksempel 3.2.34. Siden

$$19 - (-8) = 27$$

og $3 \mid 27$, er $19 \equiv -8 \pmod{3}$. Siden

$$(-8) - 64 = -72$$

og $3 \mid 72$, er $-8 \equiv 64 \pmod{3}$. Derfor fastslår Proposisjon 3.2.33 at $19 \equiv 64 \pmod{3}$.

Eksempel 3.2.35. Siden

$$-9 - (-59) = 50$$

og $5 \mid 50$, er $-9 \equiv -59 \pmod{5}$. Siden

$$(-59) - 61 = -120$$

og $5 \mid 120$, er $-59 \equiv 61 \pmod{5}$. Derfor fastslår Proposisjon 3.2.33 at $-9 \equiv 61 \pmod{5}$.

Proposisjon 3.2.36. La n være et heltall slik at $n \neq 0$. La x, y, x', og y' være heltall. Anta at $x \equiv y \pmod{n}$, og at $x' \equiv y' \pmod{n}$. Da er $x + x' \equiv y + y' \pmod{n}$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $x \equiv y \pmod{n}$, er $n \mid x - y$.

(2) Siden $x' \equiv y' \pmod{n}$, er $n \mid x' - y'$.

Det følger fra (1), (2), og Proposisjon 2.5.24 at

$$n \mid (x - y) + (x' - y'),$$

altså at

$$n \mid (x + x') - (y + y').$$

Dermed er $x + x' \equiv y + y' \pmod{n}$. □

Eksempel 3.2.37. Siden

$$13 - 5 = 8$$

og $4 \mid 8$, er $13 \equiv 5 \pmod{4}$. Siden

$$23 - (-17) = 40$$

og $4 \mid 40$, er $23 \equiv -17 \pmod{4}$. Derfor fastslår Proposisjon 3.2.36 at

$$13 + 23 \equiv 5 + (-17) \pmod{4},$$

altså at

$$36 \equiv -12 \pmod{4}.$$

Eksempel 3.2.38. Siden

$$(-16) - 17 = -33$$

og $11 \mid -33$, er $-16 \equiv 17 \pmod{11}$. Siden

$$(-34) - (-56) = 22$$

og $11 \mid 22$, er $-34 \equiv -56 \pmod{11}$. Derfor fastslår Proposisjon 3.2.36 at

$$(-16) + (-34) \equiv 17 + (-56) \pmod{5},$$

altså at

$$-50 \equiv -39 \pmod{11}.$$

Korollar 3.2.39. La n være et heltall slik at $n \neq 0$. La x, y, og z være heltall. Anta at $x \equiv y \pmod{n}$. Da er $x + z \equiv y + z \pmod{n}$.

Bevis. Ut ifra Proposisjon 3.2.16 er $z \equiv z \pmod{n}$. Ved å la både x' og y' være z, følger dermed utsagnet umiddelbart fra Proposisjon 3.2.36. □

Eksempel 3.2.40. Siden

$$18 - 12 = 6$$

og $2 \mid 6$, er $18 \equiv 12 \pmod{2}$. Derfor fastslår Korollar 3.2.39 at

$$18 + 15 \equiv 12 + 15 \pmod{2},$$

altså at

$$33 \equiv 27 \pmod{2}.$$

Eksempel 3.2.41. Siden

$$(-8) - (-23) = 15$$

og $5 \mid 15$, er $-8 \equiv -23 \pmod{5}$. Derfor fastslår Korollar 3.2.39 at

$$-8 + 13 \equiv -23 + 13 \pmod{5},$$

altså at

$$5 \equiv -10 \pmod{5}.$$

Proposisjon 3.2.42. La n være et heltall slik at $n \neq 0$. La x, y, x', og y' være heltall. Anta at $x \equiv y \pmod{n}$, og at $x' \equiv y' \pmod{n}$. Da er $x \cdot x' \equiv y \cdot y' \pmod{n}$.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $x \equiv y \pmod{n}$, er $n \mid x - y$. Dermed finnes det et heltall k slik at $x - y = kn$, altså $x = y + kn$.

(2) Siden $x' \equiv y' \pmod{n}$, er $n \mid x' - y'$. Dermed finnes det et heltall k' slik at $x' - y' = k'n$, altså $x' = y' + k'n$.

Det følger fra (1) og (2) at

$$\begin{aligned} x \cdot x' &= (y + kn) \cdot (y' + k'n) \\ &= y \cdot y' + k \cdot k' \cdot n + k' \cdot y \cdot n + k \cdot y' \cdot n \\ &= y \cdot y' + (k \cdot k' + k' \cdot y + k' \cdot y)n. \end{aligned}$$

Dermed er

$$x \cdot x' - y \cdot y' = (k \cdot k' + k' \cdot y + k' \cdot y)n.$$

Siden k, k', y, og y' er heltall, er $k \cdot k' + k' \cdot y + k' \cdot y$ et heltall. Således har vi beviset at

$$n \mid x \cdot x' + y \cdot y'.$$

Vi konkluderer at

$$x \cdot x' \equiv y \cdot y' \pmod{n}.$$

□

Eksempel 3.2.43. Siden

$$20 - (-16) = 36$$

og $3 \mid 36$, er $20 \equiv -16 \pmod{3}$. Siden

$$(-41) - 4 = -45$$

og $3 \mid -45$, er $-41 \equiv 4 \pmod{3}$. Derfor fastslår Proposisjon 3.2.42 at

$$20 \cdot (-41) \equiv (-16) \cdot 4 \pmod{3},$$

altså at

$$-820 \equiv -64 \pmod{3}.$$

Eksempel 3.2.44. Siden

$$(-38) - (-17) = -21$$

og $7 \mid -21$, er $-38 \equiv -17 \pmod{7}$. Siden

$$3 - 10 = -7$$

og $7 \mid -7$, er $3 \equiv 10 \pmod{7}$. Derfor fastslår Proposisjon 3.2.42 at

$$(-38) \cdot 3 \equiv (-17) \cdot 10 \pmod{7},$$

altså at

$$-114 \equiv -170 \pmod{7}.$$

Korollar 3.2.45. La n være et heltall slik at $n \neq 0$. La x, y, og z være heltall. Anta at $x \equiv y \pmod{n}$. Da er $x \cdot z \equiv y \cdot z \pmod{n}$.

Bevis. Ut ifra Proposisjon 3.2.16 er $z \equiv z \pmod{n}$. Ved å la både x' og y' være z, følger dermed utsagnet umiddelbart fra Proposisjon 3.2.42. □

Eksempel 3.2.46. Siden

$$13 - 24 = -11$$

og $11 \mid -11$, er $13 \equiv 24 \pmod{11}$. Derfor fastslår Korollar 3.2.45 at

$$13 \cdot (-3) \equiv 24 \cdot (-3) \pmod{11},$$

altså at

$$-39 \equiv -72 \pmod{11}.$$

Eksempel 3.2.47. Siden

$$17 - (-7) = 24$$

og $6 \mid 24$, er $17 \equiv -7 \pmod{6}$. Derfor fastslår Korollar 3.2.45 at

$$17 \cdot 3 \equiv (-7) \cdot 3 \pmod{6},$$

altså at

$$51 \equiv -21 \pmod{6}.$$

Proposisjon 3.2.48. La n være et heltall slik at $n \neq 0$. La x være et heltall, og la t være et naturlig tall. Anta at $x \equiv y \pmod{n}$. Da er $x^t \equiv y^t \pmod{n}$.

Bevis. Først sjekker vi om proposisjonen er sann når $t = 1$. Ut ifra antakelsen at

$$x \equiv y \pmod{n},$$

er dette sant.

Anta nå at proposisjonen har blitt bevist når $t = m$, hvor m er et gitt naturlig tall. Således har det blitt bevist at

$$x^m \equiv y^m \pmod{n}.$$

Det følger fra dette, antakelsen at

$$x \equiv y \pmod{n},$$

og Proposisjon 3.2.42, at

$$x^m \cdot x \equiv y^m \cdot y \pmod{n},$$

altså at

$$x^{m+1} \equiv y^{m+1} \pmod{n}.$$

Dermed er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for et hvilket som helst naturlig tall n. □

Eksempel 3.2.49. Siden $3 - 5 = -2$ og $2 \mid -2$, er $3 \equiv 5 \pmod 3$. Derfor fastslår Proposisjon 3.2.48 at

$$3^4 \equiv 5^4 \pmod 2,$$

altså at

$$81 \equiv 625 \pmod 2.$$

Eksempel 3.2.50. Siden $(-8) - (-5) = -3$ og $3 \mid -3$, er $-8 \equiv -5 \pmod 3$. Derfor fastslår Proposisjon 3.2.48 at

$$(-8)^2 \equiv (-5)^2 \pmod 3,$$

altså at

$$64 \equiv 25 \pmod 3.$$

Proposisjon 3.2.51. La n være et heltall slik at $n \neq 0$. La x og y være heltall. La l være et heltall slik at $l \neq 0$. Anta at $x \equiv y \pmod n$. Da er $lx \equiv ly \pmod{ln}$.

Bevis. Siden $x \equiv y \pmod n$, har vi: $n \mid x - y$. Dermed finnes det et heltall k slik at $x - y = kn$. Da er

$$l(x - y) = lkn,$$

altså

$$lx - ly = k(ln).$$

Således har vi: $ln \mid lx - ly$. Derfor er

$$lx \equiv ly \pmod{ln}.$$

□

Eksempel 3.2.52. Siden $9 - 23 = -14$ og $7 \mid -14$, er $9 \equiv 23 \pmod 7$. Derfor fastslår Proposisjon 3.2.51 at

$$3 \cdot 9 \equiv 3 \cdot 23 \pmod{3 \cdot 7},$$

altså

$$27 \equiv 69 \pmod{21}.$$

Eksempel 3.2.53. Siden $-11 - (-21) = 20$ og $5 \mid 20$, er $-11 \equiv -21 \pmod 5$. Derfor fastslår Proposisjon 3.2.51 at

$$8 \cdot (-11) \cdot 8 \cdot (-21) \equiv 8 \cdot (-21) \pmod{8 \cdot 5},$$

altså

$$-88 \equiv -168 \pmod{40}.$$

Proposisjon 3.2.54. La n være et heltall slik at $n \neq 0$. La x og y være heltall. La l være et heltall slik at $l \neq 0$, $l \mid y$, og $l \mid n$. Anta at $x \equiv y \pmod n$. Da er $x \equiv 0 \pmod l$.

Bevis. Siden $l \mid y$, finnes det et heltall k slik at $y = kl$. Siden $l \mid n$, finnes det et heltall k' slik at $n = k'l$. Siden $x \equiv y \pmod{n}$, har vi: $n \mid x - y$. Dermed finnes det et heltall k'' slik at $x - y = k''n$. Vi har:

$$\begin{aligned} x &= y + k''n \\ &= kl + k''k'l \\ &= (k + k''k')l. \end{aligned}$$

Siden k, k', og k'' er heltall, er $k+k''k'$ et heltall. Dermed har vi: $l \mid x$. Ut ifra Proposisjon 3.2.13, følger det at $x \equiv 0 \pmod{l}$.

□

Eksempel 3.2.55. Siden $18 - 6 = 12$ og $12 \mid 12$, er $18 \equiv 6 \pmod{12}$. I tillegg har vi: $12 = 4 \cdot 3$ og $6 = 2 \cdot 3$. Derfor fastslår Proposisjon 3.2.54 at $18 \equiv 0 \pmod{3}$, som er riktignok sant.

Eksempel 3.2.56. Siden $-42 - 6 = -48$ og $24 \mid -48$, er $-42 \equiv 6 \pmod{24}$. I tillegg har vi: $24 = 12 \cdot 2$ og $6 = 3 \cdot 2$. Derfor fastslår Proposisjon 3.2.54 at $-42 \equiv 0 \pmod{2}$, som er riktignok sant.

Proposisjon 3.2.57. La m og n være heltall slik at $m \neq 0$ og $n \neq 0$. Anta at $m \mid n$. La x og y være heltall slik at

$$x \equiv y \pmod{n}.$$

Da er

$$x \equiv y \pmod{m}.$$

Bevis. Siden

$$x \equiv z \pmod{n},$$

har vi: $n \mid x - z$. Siden $m \mid n$, følger det fra Proposisjon 2.5.27 at

$$m \mid x - z.$$

Vi konkluderer at

$$x \equiv z \pmod{m}.$$

□

Eksempel 3.2.58. Siden $64 - 12 = 52$ og $26 \mid 52$, er

$$64 \equiv 12 \pmod{26}.$$

Siden $13 \mid 26$, fastslår Proposisjon 3.2.57 at

$$64 \equiv 12 \mod 13.$$

Siden $64 - 12 = 52$ og $13 \mid 52$, er dette riktignok sant.

Eksempel 3.2.59. Siden $-7-(-19)=12$ og $4 \mid 12$, er

$$-7 \equiv -19 \pmod{4}.$$

Siden $2 \mid 4$, fastslår Proposisjon 3.2.57 at

$$-7 \equiv -19 \mod 2.$$

Siden $-7-(-19)=12$ og $2 \mid 12$, er dette riktignok sant.

Proposisjon 3.2.60. La m og n være heltall slik at $m \neq 0$ og $n \neq 0$. Anta at $m \mid n$. La x, y, og z være heltall. Anta at

$$x \equiv y \pmod{m}.$$

Dersom

$$x \equiv z \pmod{n},$$

finnes det et heltall i slik at

$$z = y + im \pmod{n}.$$

Bevis. Ut ifra Proposisjon 3.2.57 er

$$x \equiv z \pmod{m}.$$

Det følger fra Proposisjon 3.2.24 at

$$z \equiv x \pmod{m}.$$

Siden i tillegg

$$x \equiv y \pmod{m},$$

følger det fra Proposisjon 3.2.33 at

$$z \equiv y \pmod{m}.$$

Da har vi: $m \mid z-y$. Således finnes det et heltall i slik at $z-y=im$, altså slik at $z=y+im$. □

Eksempel 3.2.61. Siden $13-4=9$ og $3 \mid 9$, er

$$13 \equiv 4 \pmod{3}.$$

Siden $13-25=-12$ og $6 \mid -12$, er

$$13 \equiv 25 \pmod{6}.$$

Siden $3 \mid 6$, fastslår Proposisjon 3.2.60 at det er et heltall i slik at $25=4+3i$. Det er riktignok sant at $25=4+3\cdot 7$.

Eksempel 3.2.62. Siden $17 - (-13) = 30$ og $5 \mid 30$, er

$$17 \equiv -13 \pmod{5}.$$

Siden $17 - 67 = -40$ og $20 \mid -40$, er

$$17 \equiv 67 \pmod{20}.$$

Siden $5 \mid 20$, fastslår Proposisjon 3.2.60 at det er et heltall i slik at $67 = -13 + 5i$. Det er riktignok sant at $67 = -13 + 5 \cdot 16$.

Korollar 3.2.63. La m og n være heltall slik at $m \neq 0$ og $n \neq 0$. Anta at $m \mid n$. La x, y, og z være heltall. Anta at

$$x \equiv y \pmod{m}.$$

Dersom

$$x \equiv z \pmod{n},$$

finnes det et heltall i slik at $0 \leq y + im < n$ og

$$z \equiv y + im \pmod{n}.$$

Bevis. Følger umiddelbart fra Proposisjon 3.2.60 og Proposisjon 3.2.1. □

Eksempel 3.2.64. La z være et heltall slik at

$$z \equiv 2 \pmod{5}.$$

Korollar 3.2.63 fastslår at enten

$$z \equiv 2 \pmod{10}$$

eller

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

siden 2 og 7 er de eneste heltallene som er større enn eller like 0, mindre enn 10 og like $2 + 5i$ for noen heltall i. For eksempel er

$$12 \equiv 2 \pmod{5},$$

og

$$12 \equiv 2 \pmod{10}.$$

På en annen side er

$$17 \equiv 2 \pmod{5},$$

og

$$17 \equiv 7 \pmod{10}.$$

Eksempel 3.2.65. La z være et heltall slik at

$$z \equiv 3 \pmod 4.$$

Korollar 3.2.63 fastslår at ett av følgende er sant:

(1) $z \equiv 3 \pmod{16}$;

(2) $z \equiv 7 \pmod{16}$;

(3) $z \equiv 11 \pmod{16}$;

(4) $z \equiv 15 \pmod{16}$.

Heltallene 3, 7, 11, og 15 er nemlig de eneste heltallene som er større enn eller like 0, mindre enn 16 og like $3 + 4i$ for noen heltall i. For eksempel har vi:

(1) $19 \equiv 3 \pmod 4$ og $19 \equiv 3 \pmod{16}$;

(2) $55 \equiv 3 \pmod 4$ og $55 \equiv 7 \pmod{16}$;

(3) $91 \equiv 3 \pmod 4$ og $91 \equiv 11 \pmod{16}$;

(4) $31 \equiv 3 \pmod 4$ og $31 \equiv 15 \pmod{16}$.

Proposisjon 3.2.66. La n være et heltall. La k være et naturlig tall. La x være et heltall slik at

$$x \equiv 0 \pmod n.$$

Da er

$$x^k \equiv 0 \pmod{n^k}.$$

Bevis. Siden

$$x \equiv 0 \pmod n,$$

har vi: $n \mid x$. Det følger fra Proposisjon 2.5.15 at

$$n^k \mid x^k,$$

altså at

$$x^k \equiv 0 \pmod{n^k}.$$

□

Eksempel 3.2.67. Siden

$$12 \equiv 0 \pmod 3,$$

fastlår Proposisjon 3.2.66 at

$$12^2 \equiv 0 \pmod{3^2},$$

altså at

$$144 \equiv 0 \pmod 9.$$

Siden $144 = 16 \cdot 9$ er dette riktignok sant.

Eksempel 3.2.68. Siden

$$-10 \equiv 0 \pmod 5,$$

fastlår Proposisjon 3.2.66 at

$$-10^3 \equiv 0 \pmod{5^3},$$

altså at

$$-1000 \equiv 0 \pmod{125}.$$

Siden $-1000 = -8 \cdot 125$ er dette riktignok sant.

Proposisjon 3.2.69. La n være et heltall. La x og y være heltall slik at

$$x \equiv y \pmod n.$$

La z være et heltall. Da er $\mathsf{sfd}(x, n) = \mathsf{sfd}(y, n)$.

Bevis. Siden

$$x \equiv y \pmod n,$$

har vi: $n \mid x - y.$. Dermed finnes det et heltall k slik at $x - y = kn$, altså $y = kn + x$. Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(y, n) = \mathsf{sfd}(n, x)$, altså $\mathsf{sfd}(y, n) = \mathsf{sfd}(x, n)$. □

Eksempel 3.2.70. Siden

$$18 \equiv 10 \pmod 8,$$

fastslår Proposisjon 3.2.69 at $\mathsf{sfd}(18, 8) = \mathsf{sfd}(10, 8)$. Siden $\mathsf{sfd}(18, 8) = 2$ og $\mathsf{sfd}(10, 8) = 2$, er dette riktignok sant.

Eksempel 3.2.71. Siden

$$56 \equiv -98 \pmod{77},$$

fastslår Proposisjon 3.2.69 at $\mathsf{sfd}(56, 77) = \mathsf{sfd}(-98, 77)$. Siden $\mathsf{sfd}(56, 77) = 7$ og $\mathsf{sfd}(-98, 77) = 7$, er dette riktignok sant.

3.3 Utregning ved hjelp av kongruenser

Merknad 3.3.1. Vi skal nå se at de algebraiske manipulasjonene med kongruenser, som vi nå har hevist er gyldige, kan hjelpe oss å vise at utsagner om store heltall er sanne uten å kruke en kalkulator eller en datamaskin.

Proposisjon 3.3.2. Heltallet $2^{20} - 1$ er delelig med 41.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $32 - (-9) = 41$, og siden $41 \mid 41$, er $32 \equiv -9 \pmod{41}$. Siden $32 = 2^5$, har vi dermed:

$$2^5 \equiv -9 \pmod{41}.$$

(2) Det følger fra (1) og Proposisjon 3.2.48 at

$$\left(2^5\right)^4 \equiv (-9)^4 \pmod{41}.$$

Siden

$$(-9)^4 = 9^4 = (9)^2 \cdot (9)^2 = 81 \cdot 81,$$

har vi dermed:

$$2^{20} \equiv 81 \cdot 81 \pmod{41}.$$

(3) Siden $81 - (-1) = 82$, og siden $41 \mid 82$, er $81 \equiv -1 \pmod{41}$.

(4) Det følger fra (3) og Proposisjon 3.2.42 at $81 \cdot 81 \pmod{}() - 1) \cdot (-1) \pmod{41}$¸ altså at $81 \cdot 81 = 1 \pmod{41}$.

(5) Det følger fra (2), (3), og Proposisjon 3.2.33 at $2^{20} \equiv 1 \pmod{41}$.

(6) Det følger fra (5) og Korollar 3.2.39 at

$$2^{20} - 1 \equiv 1 - 1 \pmod{41},$$

altså at

$$2^{20} - 1 \equiv 0 \pmod{41}.$$

Det følger fra (6) og Proposisjon 3.2.13 at $41 \mid 2^{20} - 1$. □

Proposisjon 3.3.3. Heltallet $111^{333} + 333^{111}$ er delelig med 7.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $111 - (-1) = 112$, og siden $7 \mid 112$, er $111 \equiv -1 \pmod{7}$.

(2) Det følger fra (1) og Proposisjon 3.2.48 at

$$111^{333} \equiv (-1)^{333} \pmod{7},$$

altså at

$$111^{333} \equiv -1 \pmod{7}.$$

(3) Det følger fra (1) og Korollar 3.2.45 at

$$3 \cdot 111 \equiv 3 \cdot (-1) \pmod{7},$$

altså at

$$333 \equiv -3 \pmod{7}.$$

(4) Det følger fra (3) og Proposisjon 3.2.48 at

$$(333)^3 \equiv (-3)^3 \pmod{7},$$

altså at

$$(333)^3 \equiv -27 \pmod{7}.$$

(5) Siden

$$-27 - 1 = -28,$$

og siden $7 \mid 28$, er

$$-27 \equiv 1 \pmod{7}.$$

(6) Det følger fra (4), (5), og Proposisjon 3.2.33 at

$$(333)^3 \equiv 1 \pmod{7}.$$

(7) Det følger fra (7) og Proposisjon 3.2.48 at

$$\left((333)^3\right)^{37} \equiv 1^{37} \pmod{7},$$

altså at

$$333^{111} \equiv 1 \pmod{7}.$$

(8) Det følger fra (2), (7), og Proposisjon 3.2.36 at

$$111^{333} + 333^{111} \equiv (-1) + 1 \pmod{7},$$

altså at

$$111^{333} + 333^{111} \equiv 0 \pmod{7}.$$

Det følger fra (8) og Proposisjon 3.2.13 at $7 \mid 111^{333} + 333^{111}$. □

Proposisjon 3.3.4. Summen

$$1! + 2! + \cdots + 99! + 100!$$

er kongruent til 9 mod 12.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $4! = 4 \times 3 \times 2 \times 1 = 24$, og siden $12 \mid 24$, er $4! \equiv 0 \pmod{12}$.

(2) For hvert naturlig tall m slik at $4 < m \leq 100$, følger det fra (1) og Korollar 3.2.45 at

$$4! \cdot (5 \times \cdots \times m) \equiv 0 \cdot (5 \times \cdots \times m) \pmod{12},$$

altså at

$$m! \equiv 0 \pmod{12}.$$

(3) Fra (2) og Proposisjon 3.2.36 følger det at

$$1! + 2! + 3! + 4! + 5! + \cdots + 99! + 100! \equiv 1! + 2! + 3! + 0 + 0 + \cdots + 0 + 0 \pmod{12},$$

altså at

$$1! + 2! + \cdots + 99! + 100! \equiv 1! + 2! + 3! \pmod{12}.$$

(4) Siden

$$1! + 2! + 3! = 1 + 2 + 6 = 9$$

følger det fra (3) at

$$1! + 2! + \cdots + 99! + 100! \equiv 9 \pmod{12}.$$

□

Proposisjon 3.3.5. La t være et naturlig tall. Da er $3^{t+2} + 4^{2t+1}$ delelig med 13.

Bevis. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned} 3^{t+2} + 4^{2t+1} &= 3^t \cdot 9 + 4^{2t} \cdot 4 \\ &= 3^t \cdot 9 + \left(4^2\right)^t \cdot 4 \\ &= 3^t \cdot 9 + 16^t \cdot 4. \end{aligned}$$

(2) Siden $16 - 3 = 13$ og $13 \mid 13$, er $16 \equiv 3 \pmod{13}$.

(3) Det følger fra (2) og Proposisjon 3.2.48 at

$$16^t \equiv 3^t \pmod{13}.$$

(4) Det følger fra (3) og Korollar 3.2.45 at

$$16^t \cdot 4 \equiv 3^t \cdot 4 \pmod{13}.$$

(5) Det følger fra (4) og Korollar 3.2.39 at

$$3^t \cdot 9 + 16^t \cdot 4 \equiv 3^t \cdot 9 + 3^t \cdot 4 \pmod{13},$$

altså at

$$3^t \cdot 9 + 16^t \cdot 4 \equiv 3^t \cdot 13 \pmod{13}.$$

(6) Siden $13 \mid 3^t \cdot 13$, følger det fra Proposisjon 3.2.13 at $3^t \cdot 13 \equiv 0 \pmod{13}$.

(7) Det følger fra (5), (6), og Proposisjon 3.2.33 at

$$3^t \cdot 9 + 16^t \cdot 4 \equiv 0 \pmod{13}.$$

Det følger fra (1) og (7) at

$$3^{t+2} + 4^{2t+1} \equiv 0 \pmod{13}.$$

Det følger fra Proposisjon 3.2.13 at $13 \mid 3^{t+2} + 4^{2t+1}$.

□

Proposisjon 3.3.6. La x være et naturlig tall. Anta at det finnes et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $x_i \geq 0$. Da er x delelig med 9 hvis og bare hvis summen

$$x_0 + x_1 + \cdots + x_{n-1} + x_n$$

er delelig med 9.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $10 - 1 = 9$ og $9 \mid 9$, er $10 \equiv 1 \pmod 9$.

(2) La i være et heltall slik at $0 \leq i \leq n$. Det følger fra (1) og Proposisjon 3.2.48 at $10^i \equiv 1^i \pmod 9$, altså at
$$10^i \equiv 1 \pmod 9.$$

(3) Det følger fra (2) og Korollar 3.2.45 at $x_i \cdot 10^i \equiv x_i \cdot 1 \pmod 9$, altså at
$$x_i \cdot 10^i \equiv x_i \pmod 9.$$

(4) Det følger fra (3) og Proposisjon 3.2.36 at
$$\begin{aligned} &x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0 \\ &\equiv x_n + x_{n-1} + \cdots + x_1 + x_0 \pmod 9, \end{aligned}$$
altså at
$$x \equiv x_0 + x_1 + \cdots + x_{n-1} + x_n \pmod 9.$$

Anta at $9 \mid x$. Det følger fra Korollar 3.2.30 at $0 \equiv x \pmod 9$. Da følger det fra (4) og Proposisjon 3.2.33 at

$$0 \equiv x_0 + x_1 + \cdots + x_{n-1} + x_n \pmod 9.$$

Fra Proposisjon 3.2.13 deduserer vi at

$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n.$$

Dersom $9 \mid x$, har vi dermed bevist at

$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n.$$

Anta istedenfor at
$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n.$$

Det følger fra Proposisjon 3.2.13 at

$$x_0 + x_1 + \cdots + x_{n-1} + x_n \equiv 0 \pmod 9.$$

Da følger det fra (4) og Proposisjon 3.2.33 at

$$x \equiv 0 \pmod 9.$$

Fra Korollar 3.2.30 deduserer vi at $9 \mid x$. Dersom

$$9 \mid x_0 + x_1 + \cdots + x_{n-1} + x_n,$$

har vi dermed bevist at $9 \mid x$.

□

Merknad 3.3.7. Når vi skriver et heltall, skriver vi akkurat heltall x_0, …, x_n for noe heltall n, slik at ligningen i Proposisjon 3.3.6 stemmer. For eksempel har vi:

$$1354 = 1 \cdot 1000 + 3 \cdot 100 + 5 \cdot 10 + 4 \cdot 1,$$

altså

$$1354 = 1 \cdot 10^3 + 3 \cdot 10^2 + 5 \cdot 10^1 + 4 \cdot 10^0.$$

Med andre ord er x_i det i-te heltallet fra høyre, ved å telle fra 0.

Merknad 3.3.8. Ved å benytte divisjonsalgoritmen, kan det bevises formelt at, for hvert heltall x, finnes det et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $0 \leq x_i \leq 9$. Med andre ord, gjelder Proposisjon 3.3.6 for et hvilket som helst heltall x.

Det kan også bevises at heltallene n og x_0, x_1, …, x_n er de *eneste* slik at ligningen i Proposisjon 3.3.6 stemmer, og slik at $0 \leq x_i \leq 9$ for hvert i.

Imidlertid er disse bevisene ikke spesielt viktige fra et teoretisk synspunkt. Derfor skal vi hoppe over dem, og nøye oss med Proposisjon 3.3.6.

Terminologi 3.3.9. La x være et heltall. La n være et heltall slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $0 \leq x_i \leq 9$. La i være et heltall slik at $0 \leq i \leq n$. Vi sier at x_i er et *siffer* av x.

Eksempel 3.3.10. Siden summen av sifrene i 72 er

$$7 + 2 = 9,$$

og siden $9 \mid 9$, fastslår Proposisjon 3.3.6 at $9 \mid 72$.

Eksempel 3.3.11. Siden summen av sifrene i 154872 er

$$1 + 5 + 4 + 8 + 7 + 2 = 27,$$

og siden $9 \mid 27$, fastslår Proposisjon 3.3.6 at $9 \mid 154872$.

Eksempel 3.3.12. Siden summen av sifrene i 76253 er

$$7 + 6 + 2 + 5 + 3 = 23,$$

og siden det ikke er sant at $9 \mid 23$, fastslår Proposisjon 3.3.6 at det ikke er sant at $9 \mid 76253$.

Eksempel 3.3.13. Siden summen av sifrene i 849 er

$$8 + 4 + 9 = 21,$$

og siden det ikke er sant at $9 \mid 21$, fastslår Proposisjon 3.3.6 at det ikke er sant at $9 \mid 849$.

Proposisjon 3.3.14. La x være et naturlig tall. Anta at det finnes et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $x_i \geq 0$. Da er x delelig med 11 hvis og bare hvis summen

$$x_0 - x_1 + \cdots + (-1)^{n-1} \cdot x_{n-1} + (-1)^n x_n$$

er delelig med 11.

Bevis. Vi gjør følgende observasjoner.

(1) Siden $10 - (-1) = 11$ og $11 \mid 11$, er $10 \equiv -1 \pmod{11}$.

(2) La i være et heltall slik at $0 \leq i \leq n$. Det følger fra (1) og Proposisjon 3.2.48 at $10^i \equiv (-1)^i \pmod{11}$.

(3) Det følger fra (2) og Korollar 3.2.45 at $x_i \cdot 10^i \equiv x_i \cdot (-1)^i \pmod{11}$, altså at

$$x_i \cdot 10^i \equiv (-1)^i \cdot x_i \pmod{11}.$$

(4) Det følger fra (3) og Proposisjon 3.2.36 at

$$\begin{aligned} &x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0 \\ &\equiv (-1)^n \cdot x_n + (-1)^{n-1} x_{n-1} + \cdots + (-1)^1 \cdot x_1 + (-1)^0 \cdot x_0 \pmod{11}, \end{aligned}$$

altså at

$$x \equiv x_0 - x_1 + \cdots + (-1)^{n-1} x_{n-1} + (-1)^n x_n \pmod{11}.$$

Anta at $11 \mid x$. Det følger fra Korollar 3.2.30 at $0 \equiv x \pmod{11}$. Da følger det fra (4) og Proposisjon 3.2.33 at

$$0 \equiv x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n \pmod{11}.$$

Fra Proposisjon 3.2.13 deduserer vi at

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n.$$

Dersom $11 \mid x$, har vi dermed bevist at

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n.$$

Anta istedenfor at

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n.$$

Det følger fra Proposisjon 3.2.13 at

$$x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n \equiv 0 \pmod{11}.$$

Da følger det fra (4) og Proposisjon 3.2.33 at

$$x \equiv 0 \pmod{11}.$$

Fra Korollar 3.2.30 deduserer vi at $11 \mid x$. Dersom

$$11 \mid x_0 - x_1 + \cdots + (-1)^{n-1}x_{n-1} + (-1)^n x_n,$$

har vi dermed bevist at $11 \mid x$.

□

Eksempel 3.3.15. Siden

$$1 - 2 + 1 = 0,$$

og siden $11 \mid 0$, fastslår Proposisjon 3.3.6 at $11 \mid 121$.

Eksempel 3.3.16. Siden

$$3 - 5 + 7 - 0 + 6 = 11,$$

og siden $11 \mid 11$, fastslår Proposisjon 3.3.6 at $11 \mid 60753$.

Eksempel 3.3.17. Siden

$$2 - 1 + 8 - 2 + 9 - 1 + 7 = 22,$$

og siden $11 \mid 22$, fastslår Proposisjon 3.3.6 at $11 \mid 7192812$.

Eksempel 3.3.18. Siden

$$9 - 1 + 3 - 7 + 4 = 8,$$

og siden det ikke er sant at $11 \mid 8$, fastslår Proposisjon 3.3.6 at det ikke er sant at $11 \mid 47319$.

Eksempel 3.3.19. Siden

$$7 - 3 + 8 = 12,$$

og siden det ikke er sant at $11 \mid 12$, fastslår Proposisjon 3.3.6 at det ikke er sant at $11 \mid 837$.

3.4 Lineære kongruenser

Terminologi 3.4.1. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La x være et heltall slik at

$$ax \equiv c \pmod{n}.$$

Da sier vi at x er en *løsning* til denne kongruensen.

Terminologi 3.4.2. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Når vi er interessert i heltall x som er løsninger til kongruensen

$$ax \equiv c \pmod{n},$$

kalles

$$ax \equiv c \pmod{n}$$

en *lineær kongruens*.

Eksempel 3.4.3. Siden

$$6 \cdot 3 - 8 = 18 - 8 = 10$$

og $5 \mid 10$, er

$$6 \cdot 3 \equiv 8 \pmod{5}.$$

Dermed er 3 en løsning til kongruensen

$$6x \equiv 8 \pmod{5}.$$

Eksempel 3.4.4. Siden

$$(-8) \cdot (-5) - 12 = 40 - 12 = 28$$

og $7 \mid 28$, er

$$(-8) \cdot (-5) \equiv 12 \pmod{7}.$$

Dermed er -5 en løsning til kongruensen

$$-8x \equiv 12 \pmod{7}.$$

Proposisjon 3.4.5. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Da er x en løsning til kongruensen

$$ax \equiv c \pmod{n}$$

hvis og bare hvis det finnes et heltall y slik at x og y er en løsning til ligningen

$$ax - ny = c.$$

Bevis. Anta først at x er en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Da har vi: $n \mid ax - c$. Dermed finnes det et heltall y slik at

$$ax - c = yn.$$

Således er

$$ax - yn = c.$$

Anta istedenfor at det finnes et heltall y slik at

$$ax - yn = c.$$

Da er

$$ax - c = yn,$$

altså $n \mid ax - c$. Vi deduserer at $ax \equiv c \pmod{n}$. □

Eksempel 3.4.6. Fra Eksempel 3.4.3 vet vi at 3 er en løsning til kongruensen

$$6x \equiv 8 \pmod{5}.$$

Derfor fastslår Proposisjon 3.4.5 at det finnes et heltall y slik at $x = 3$ og y er en løsning til ligningen

$$6x - 5y = 8.$$

Vi har nemlig at $x = 3$ og $y = 2$ er en løsning til ligningen

$$6x - 5y = 8.$$

Eksempel 3.4.7. Fra Eksempel 3.4.4 vet vi at -5 er en løsning til kongruensen

$$-8x \equiv 12 \pmod{7}.$$

Derfor fastslår Proposisjon 3.4.5 at det finnes et heltall y slik at $x = -5$ og y er en løsning til ligningen

$$-8x - 7y = 12.$$

Vi har nemlig at $x = -5$ og $y = 4$ er en løsning til ligningen

$$-8x - 7y = 12.$$

Merknad 3.4.8. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Proposisjon 3.4.5 fastslår at det finnes et nært forhold mellom heltallsløsninger til lineære kongruenser og løsninger til lineære diofantiske ligninger.

Dermed kan vi bygge på den gode forståelsen vår for lineære diofantiske ligninger for å få en like god forståelse for heltallsløsninger til lineære kongruenser, som vi nå kommer til å se.

Proposisjon 3.4.9. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Da har kongruesen

$$ax \equiv c \pmod{n}$$

en løsning hvis og bare hvis $\mathsf{sfd}(a, n) \mid c$.

Bevis. Følger umiddelbart fra Proposisjon 3.4.5 og Korollar 2.9.12. □

Eksempel 3.4.10. Vi har: $\mathsf{sfd}(12, 15) = 3$. Siden $3 \mid 6$, fastslår Proposisjon 3.4.9 at kongruensen

$$12x \equiv 6 \pmod{15}$$

har en løsning.

Proposisjon 3.4.9 sier ikke hvordan man finner den, men det kan sjekkes at for eksempel $x = 13$ er en løsning.

Eksempel 3.4.11. Vi har: $\mathsf{sfd}(-14, 21) = 7$. Siden $7 \mid 35$, fastslår Proposisjon 3.4.9 at kongruensen

$$-14x \equiv 35 \pmod{21}$$

har en løsning.

Proposisjon 3.4.9 sier ikke hvordan man finner den, men det kan sjekkes at for eksempel $x = 5$ er en løsning.

Merknad 3.4.12. Etter å ha gjort noen forbedredelser, skal vi nå se på *hvordan* man finner en løsning til en kongruens

$$ax \equiv c \pmod{n}.$$

Proposisjon 3.4.13. La n være et heltall slik at $n \neq 0$. La a, x, og y være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Siden $d \mid n$, finnes det et heltall k_n slik at $n = k_n d$. Vi har:

$$ax \equiv ay \pmod{n}$$

hvis og bare hvis

$$x \equiv y \pmod{k_n}.$$

Bevis. Anta først at

$$ax \equiv ay \pmod{n}.$$

Vi gjør følgende observasjoner.

(1) Siden

$$ax \equiv ay \pmod{n},$$

har vi: $n \mid ax - ay$, altså $n \mid a(x - y)$. Dermed finnes det et heltall k slik at

$$a(x - y) = kn.$$

(2) Siden $\mathsf{sfd}(a, n) = d$, har vi: $d \mid a$. Dermed finnes det et heltall k_a slik at $a = k_a a$.

(3) Fra (1), (2), og antakelsen at $n = k_n d$, følger det at

$$k_a d(x - y) = k k_n d,$$

altså at

$$d k_a (x - y) = d k k_n.$$

(4) Fra (3) og Proposisjon 2.2.25 følger det at

$$k_a (x - y) = k k_n.$$

Dermed har vi:

$$k_n \mid k_a (x - y).$$

(5) Ut ifra Proposisjon 2.8.13 er

$$\mathsf{sfd}(k_a, k_n) = 1,$$

altså

$$\mathsf{sfd}(k_n, k_a) = 1.$$

(6) Fra (4), (5), og Proposisjon 2.8.22 følger det at

$$k_n \mid x - y.$$

Dermed er

$$x \equiv y \pmod{k_n}.$$

Således har vi bevist at, dersom

$$ax \equiv ay \pmod{n},$$

er

$$x \equiv y \pmod{k_n}.$$

Anta istedenfor at

$$x \equiv y \pmod{k_n}.$$

Da følger det fra Proposisjon 3.2.51 at

$$ax \equiv ay \pmod{n}.$$

□

Eksempel 3.4.14. Siden $6 \cdot 14 - 6 \cdot 23 = -54$, og siden $9 \mid -54$, er

$$6 \cdot 14 \equiv 6 \cdot 23 \pmod{9}.$$

Vi har: $\mathsf{sfd}(6, 9) = 3$, og $9 = 3 \cdot 3$. Derfor fastslår Proposisjon 3.4.13 at

$$14 \equiv 23 \pmod{3}.$$

Eksempel 3.4.15. Siden $8 \cdot 12 - 8 \cdot 5 = 56$, og siden $28 \mid 56$, er

$$8 \cdot 12 \equiv 8 \cdot 5 \pmod{28}.$$

Vi har: $\mathsf{sfd}(8, 28) = 4$, og $28 = 7 \cdot 4$. Derfor fastslår Proposisjon 3.4.13 at

$$12 \equiv 5 \pmod{7}.$$

Proposisjon 3.4.16. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Anta at

$$ax \equiv c \pmod{n}.$$

La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Ut ifra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid n$, altså at det finnes heltall k_n slik at $n = k_n d$. Da er følgende sanne.

(I) For hvert heltall r slik at $0 \leq r < d$, er

$$x' = x + k_n r$$

en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

(II) La x' være et heltall slik at

$$ax' \equiv c \pmod{n}.$$

Da finnes det et heltall r, hvor $0 \leq r < d$, slik at

$$x' \equiv x + k_n r \pmod{n}.$$

(III) La r og s være heltall slik at $0 \leq r < d$ og $0 \leq s < d$. La

$$x' = x + k_n r$$

og

$$x'' = x + k_n s$$

Hvis

$$x' \equiv x'' \pmod{n}$$

er $r = s$.

Bevis. La oss først bevise at (I) er sant. La t være et heltall slik at $0 \leq t < d$, Fra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid a$, altså at det finnes heltall k_a slik at $a = k_a d$. Ut ifra Korollar 2.9.24 er

$$x' = x + k_n t$$

og

$$y' = x - k_a t$$

en løsning til ligningen

$$ax + ny = c.$$

Derfor er

$$x' = x + k_n t$$

og

$$y' = -(x - k_a t) = k_a t - x$$

en løsning til ligningen

$$ax - ny = c.$$

Fra Proposisjon 3.4.5 deduserer vi at

$$x' = x + k_n t$$

er en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

La oss nå bevise at (II) er sant. La x' være et heltall slik at

$$ax' \equiv c \pmod{n}.$$

Fra Proposisjon 3.4.5 følger det at det finnes et heltall y' slik at

$$ax' - ny' = c.$$

Da er

$$ax' + n(-y') = c.$$

Det følger fra Korollar 2.9.25 at det da er et heltall t slik at

$$x' = x + k_n t.$$

Ut ifra Korollar 2.2.11 finnes det heltall k_t og r slik at:

(1) $t = k_t d + r$;

(2) $0 \leq r < d$;

Da er

$$\begin{aligned} x' &= x + k_n t \\ &= x + k_n \left(k_t d + r\right) \\ &= x + k_n r + (k_n d) k_t \\ &= x + k_n r + n k_t. \end{aligned}$$

Derfor er

$$x' - (x + k_n r) = k_t n,$$

altså $n \mid x' - (x + k_n r)$. Dermed er

$$x' \equiv x + k_n r \pmod{n}.$$

La oss nå bevise at (III) er sant. Anta at

$$x' \equiv x'' \pmod{n},$$

altså at

$$x + k_n r \equiv x + k_n s \pmod{n}.$$

Vi gjør følgende observasjoner.

(1) Det følger fra Korollar 3.2.39 at

$$x + k_n r - x \equiv x + k_n s - x \pmod{n},$$

altså at

$$k_n r \equiv k_n s \pmod{n}.$$

(2) Siden $k_n \mid n$, følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(k_n, n) = k_n$.

Fra (1), (2), og Proposisjon 3.4.13 følger det at

$$r \equiv s \pmod{d}.$$

Siden $0 \leq r < d$ og $0 \leq s < d$, følger det fra Proposisjon 3.2.11 at $r = s$.

□

Merknad 3.4.17. La a og c være heltall, og la $d = \mathsf{sfd}(a, c)$. Proposisjon 3.4.16 fastslår at kongruensen

$$ax \equiv c \pmod{n}$$

har akkurat d løsninger slik at ikke noe par av disse er kongruent modulo n. Gitt én løsning x, er disse løsningene: x, $x + k_n$, $x + 2k_n$, $x + 3k_n$, …, $x + (d-1)k_n$.

Eksempel 3.4.18. La oss se på kongruensen

$$4x \equiv 6 \pmod{10}.$$

Siden

$$4 \cdot 4 - 6 = 10$$

og $10 \mid 10$, er

$$4 \cdot 4 \equiv 6 \pmod{10}.$$

Dermed er $x = 4$ en løsning til kongruensen. Vi har: $\mathsf{sfd}(4, 10) = 2$. Siden $10 = 5 \cdot 2$, er $k_n = 5$. Proposisjon 3.4.16 fastslår at:

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

(II) enhver annen løsning til kongruensen er kongruent modulo 10 til én av disse to;

(III) disse to løsningene er ikke kongruent modulo 10 til hverandre.

Eksempel 3.4.19. La oss se på kongruensen

$$12x \equiv 51 \pmod{21}.$$

Siden

$$12 \cdot 6 - 51 = 21$$

og $21 \mid 21$, er

$$12 \cdot 6 \equiv 51 \pmod{21}.$$

Dermed er $x = 6$ en løsning til kongruensen. Vi har: $\mathsf{sfd}(12, 21) = 3$. Siden $21 = 7 \cdot 3$, er $k_n = 7$. Proposisjon 3.4.16 fastslår at:

(I) $x = 6 + 7 \cdot 0$, $x = 6 + 7 \cdot 1$, og $x = 6 + 7 \cdot 2$, altså $x = 6$, $x = 13$, og $x = 20$, er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse to;

(III) ikke noe par av disse tre løsningene er kongruent modulo 21 til hverandre.

Merknad 3.4.20. La merke til at (II) i Proposisjon 3.4.16 sier ikke at hver løsning til kongruensen

$$ax \equiv c \pmod{n}$$

er *lik* $x + k_n r$ for et heltall r slik at $0 \leq r < d$. På lignende vis sier ikke (II) i Eksempel 3.4.18 at hver løsning x til kongruensen

$$4x \equiv 6 \pmod{10}$$

er *lik* enten 4 eller 9. For eksempel er $x = 14$ en løsning: siden

$$4 \cdot 14 - 6 = 50$$

og $10 \mid 50$, er

$$4 \cdot 14 \equiv 6 \pmod{10}.$$

For et annet eksempel er $x = -1$ en løsning: siden

$$4 \cdot (-1) - 6 = -10$$

og $10 \mid -10$, er

$$4 \cdot (-1) \equiv 6 \pmod{10}.$$

Merknad 3.4.21. Imidlertid sier Proposisjon 3.4.16 at, dersom kongruensen

$$ax \equiv c \pmod{n}$$

har én løsning, finnes det akkurat d løsninger slik at ikke noe par av disse er kongruent modulo n til hverandre. Det er ikke viktig at vi beskriver disse d løsningene som i (I) i Proposisjon 3.4.16. Hver liste over d løsninger, slik at ikke noe par av disse er kongruent modulo n, er like verdifull.

For eksempel i Eksempel 3.4.18, etter å ha observert at $x = 4$ er en løsning til kongruensen

$$4x \equiv 6 \pmod{10},$$

fikk vi lista $x = 4$ og $x = 9$ ved å benytte (I) i Proposisjon 3.4.16. Følgende lister er like verdifulle:

(1) $x = 14$ og $x = 9$;

(2) $x = 4$ og $x = -1$;

(3) $x = 14$ og $x = -1$.

Det finnes uendelig mange andre lister som er like verdifulle!

Merknad 3.4.22. Likevel beskriver skriver vi oftest ei liste hvor alle løsningene x til kongruensen

$$ax \equiv c \pmod{n}$$

oppfyller: $0 \leq x < n$. Proposisjon 3.2.1 fastslår at det alltid er mulig å finne ei slik liste.

For eksempel skriver vi oftest $x = 4$ og $x = 9$ som lista over løsningene til kongruensen

$$4x \equiv 6 \pmod{10}$$

vi så på i Eksempel 3.4.18.

Merknad 3.4.23. For å finne løsningene til kongruensen

$$ax \equiv c \pmod{n},$$

følger det fra Proposisjon 3.4.16 at det viktigste er å finne én løsning. Som vi snart kommer til å se, kan dette alltid gjøres, om det *er* en løsning, ved å benytte Euklids algoritme,

Imidlertid kan en løsning ofte finnes fortere i prakis ved å benytte andre metoder. For å hjelpe oss med dette, er følgende proposisjon svært nyttig.

Proposisjon 3.4.24. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Anta at

$$ax \equiv c \pmod{n}.$$

Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at:

(1) $x \equiv r \pmod{n}$;

(2) $0 \leq r < n$.

Vi har:

$$ar \equiv c \pmod{n}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Proposisjon 3.2.1 fastslår at det finnes et heltall r slik at:
   (i) $x \equiv r \pmod{n}$;
   (ii) $0 \leq r < n$.

(2) Det følger fra (i) og Korollar 3.2.45 at

$$ax \equiv ar \pmod{n}.$$

(3) Fra (2) og Proposisjon 3.2.24 følger det at

$$ar \equiv ax \pmod{n}.$$

(4) Fra (3), antakelsen at

$$ax \equiv c \pmod{n},$$

og Proposisjon 3.2.33, følger det at

$$ar \equiv c \pmod{n}.$$

□

Eksempel 3.4.25. La oss se på kongruensen

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

Siden

$$6 \cdot 53 - (-27) = 345$$

og $15 \mid 345$, er

$$6 \cdot 53 \equiv -27 \pmod{15}.$$

Proposisjon 3.4.24 fastslår at det finnes en løsning r til kongruensen slik at:

(1) $53 \equiv r \pmod{15}$;

(2) $0 \leq r < 15$.

Beviset for Proposisjon 3.4.24 fastslår at r er resten vi får når vi deler 53 med 15, altså $r = 8$. Siden

$$6 \cdot 8 - (-27) = 75$$

og $15 \mid 75$, er det riktignok sant at

$$6 \cdot 8 \equiv -27 \pmod{15}.$$

Eksempel 3.4.26. La oss se på kongruensen

$$4x \equiv 18 \pmod{14}.$$

Siden

$$4 \cdot (-69) - 18 = -294$$

og $14 \mid -294$, er

$$4 \cdot (-69) \equiv 18 \pmod{14}.$$

Proposisjon 3.4.24 fastslår at det finnes en løsning r til kongruensen slik at:

(1) $-69 \equiv r \pmod{15}$;

(2) $0 \leq r < 14$.

Beviset for Proposisjon 3.4.24 fastslår at r er resten vi får når vi deler -69 med 14, altså $r = 1$. Siden

$$4 \cdot 1 - 18 = -14$$

og $14 \mid -14$, er det riktignok sant at

$$4 \cdot 1 \equiv 18 \pmod{14}.$$

Merknad 3.4.27. Dersom det finnes en løsning til kongruensen

$$ax = c \pmod{n},$$

følger det fra Proposisjon 3.4.24 at det finnes en løsning x slik at $0 \leq x < n$. For å finne én løsning til kongruensen, kan vi derfor ganske enkelt sjekke om

$$ar \equiv c \pmod{n}$$

for heltallene r slik at $0 \leq x < n$. Da kan vi benytte (I) i Proposisjon 3.4.16 for å finne de andre løsningene.

Eksempel 3.4.28. La oss se på kongruensen

$$8x \equiv -12 \pmod{20}.$$

For å finne én løsning, er det nok å sjekke om kongruensen stemmer når $x = 0$, $x = 1$, $x = 2$, ..., $x = 19$.

(1) Det er ikke sant at

$$8 \cdot 0 \equiv -12 \pmod{20},$$

siden det ikke er sant at

$$0 \equiv 3 \pmod{20}.$$

(2) Det er sant at

$$8 \cdot 1 \equiv -12 \pmod{20},$$

siden

$$8 - (-12) = 20$$

og $20 \mid 20$.

Siden vi nå har funnet én løsning, er det ikke nødvendig å se på $x = 2$, $x = 3$, ..., $x = 19$.

Nå benytter vi (I) i Proposisjon 3.4.16 for å finne de andre løsningene. Vi har: $\mathsf{sfd}(8, 20) = 4$, og $20 = 5 \cdot 4$. Derfor fastslår Proposisjon 3.4.16 at:

(I) $x = 1 + 5r$ er en løsning for alle heltallene r slik at $0 \leq r < 4$, altså $x = 1$, $x = 6$, $x = 11$, og $x = 16$ er løsninger;

(II) enhver annen løsning er kongruent modulo 20 til én av disse;

(III) ikke noe par av disse fire løsningene er kongruent modulo 20 til hverandre.

Eksempel 3.4.29. La oss se på kongruensen

$$14x \equiv 7 \pmod{63}.$$

For å finne én løsning, er det nok å sjekke om kongruensen stemmer når $x = 0$, $x = 1$, $x = 2$, ..., $x = 62$.

(1) Det er ikke sant at

$$14 \cdot 0 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$0 \equiv 7 \pmod{63}.$$

(2) Det er ikke sant at

$$14 \cdot 1 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$14 \equiv 7 \pmod{63}.$$

(3) Det er ikke sant at

$$14 \cdot 2 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$28 \equiv 7 \pmod{63}.$$

(4) Det er ikke sant at

$$14 \cdot 3 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$42 \equiv 7 \pmod{63}.$$

(5) Det er ikke sant at

$$14 \cdot 4 \equiv 7 \pmod{63},$$

siden det ikke er sant at

$$56 \equiv 21 \pmod{63}.$$

(6) Det er sant at

$$14 \cdot 5 \equiv 7 \pmod{63},$$

siden

$$14 \cdot 5 - 7 = 63$$

og $63 \mid 63$.

Siden vi nå har funnet én løsning, er det ikke nødvendig å se på tilfellet når $x = 6$, $x = 7$, ..., $x = 62$.

Nå benytter vi (I) i Proposisjon 3.4.16 for å finne de andre løsningene. Vi har: $\mathsf{sfd}(14, 63) = 7$ og $63 = 9 \cdot 7$. Derfor fastslår Proposisjon 3.4.16 at:

(I) $x = 5 + 9r$ er en løsning for alle heltallene r slik at $0 \leq r < 7$, altså $x = 5$, $x = 14$, $x = 23$, $x = 32$, $x = 41$, $x = 50$, og $x = 59$ er løsninger;

(II) enhver annen løsning er kongruent modulo 63 til én av disse;

(III) ikke noe par av disse fire løsningene er kongruent modulo 63 til hverandre.

Merknad 3.4.30. Proposisjon 3.4.13 kan også være til stor hjelp når vi ønsker å finne en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

La $d = \mathsf{sfd}(a, n)$. Anta at $d \mid c$. Proposisjon 3.4.13 fastslår at x er en løsning til kongruensen hvis og bare hvis x er en løsning til kongruensen

$$k_a x \equiv k_c \pmod{k_n},$$

hvor:

(1) k_a er heltallet slik at $a = k_a \cdot d$;

(2) k_c er heltallet slik at $c = k_c \cdot d$;

(3) k_n er heltallet slik at $n = k_n \cdot d$.

Det kan være mange færre tilfeller å se på når vi gjennomfører metoden i Merknad 3.4.27 for kongruensen

$$k_a x \equiv k_c \pmod{k_n},$$

sammenlignet med når vi gjennomfører denne metoden for kongruensen

$$ax \equiv c \pmod{n}.$$

Med andre ord, kan vi ofte finne en løsning til kongruensen

$$k_a x \equiv k_c \pmod{k_n}$$

mye fortere enn en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Eksempel 3.4.31. La oss se igjen på kongruensen

$$8x \equiv -12 \pmod{20}$$

fra Eksempel 3.4.28. Vi har: $\mathsf{sfd}(8, 20) = 4$. Derfor er $k_a = 2$, $k_c = -3$, og $k_n = 5$. Proposisjon 3.4.13 fastslår at x er en løsning til kongruensen hvis og bare hvis x er en løsning til kongruensen

$$2x \equiv -3 \pmod{5}.$$

For å finne en løsning til denne kongruensen, er det nok å sjekke om den stemmer når $x = 0$, $x = 1$, $x = 2$, ..., $x = 4$.

(1) Det er ikke sant at

$$2 \cdot 0 \equiv -3 \pmod{5},$$

siden det ikke er sant at

$$0 \equiv -3 \pmod{5}.$$

(2) Det er sant at

$$2 \cdot 1 \equiv -3 \pmod{5},$$

siden

$$2 \cdot 1 - (-3) = 5$$

og $5 \mid 5$.

Nå kan vi fortsette som i Eksempel 3.4.28, ved å benytte løsningen $x = 1$ for å finne de andre løsningene til kongruensen

$$8x \equiv -12 \pmod{20}.$$

Eksempel 3.4.32. La oss se igjen på kongruensen

$$14x \equiv 7 \pmod{63}$$

fra Eksempel 3.4.29. Vi har: $\mathsf{sfd}(14, 63) = 7$. Derfor er $k_a = 2$, $k_c = 1$, og $k_n = 9$. Proposisjon 3.4.13 fastslår at x er en løsning til kongruensen hvis og bare hvis x er en løsning til kongruensen

$$2x \equiv 1 \pmod{9}.$$

For å finne en løsning til denne kongruensen, er det nok å sjekke om den stemmer når $x = 0$, $x = 1$, $x = 2$, …, $x = 8$.

(1) Det er ikke sant at

$$2 \cdot 0 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$0 \equiv 1 \pmod{9}.$$

(2) Det er ikke sant at

$$2 \cdot 1 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$2 \equiv 1 \pmod{9}.$$

(3) Det er ikke sant at

$$2 \cdot 2 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$4 \equiv 1 \pmod{9}.$$

(4) Det er ikke sant at

$$2 \cdot 3 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$6 \equiv 1 \pmod{9}.$$

(5) Det er ikke sant at

$$2 \cdot 4 \equiv 1 \pmod{9},$$

siden det ikke er sant at

$$8 \equiv 1 \pmod{9}.$$

(6) Det er sant at

$$2 \cdot 5 \equiv 1 \pmod{9},$$

siden

$$2 \cdot 5 - 1 = 9$$

og $9 \mid 9$.

Nå kan vi fortsette som i Eksempel 3.4.29, ved å benytte løsningen $x = 5$ for å finne de andre løsningene til kongruensen

$$14x \equiv 7 \pmod{63}.$$

Proposisjon 3.4.33. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vn$. Ut ifra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid n$, altså at det finnes heltall k_n slik at $n = k_n d$. Anta at $d \mid c$, altså at det et heltall k slik at $c = kd$. Da er

$$x = ku$$

en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Bevis. Ut ifra Proposisjon 2.9.4 er

$$a(ku) + n(kv) = c.$$

Dermed er

$$a(ku) - n \cdot (-kv) = c.$$

Fra Proposisjon 3.4.5 deduserer vi at

$$a(ku) \equiv c \pmod{n}.$$

□

Eksempel 3.4.34. La oss se på kongruensen

$$12x \equiv 57 \pmod{21}.$$

Vi har: $\mathsf{sfd}(12, 21) = 3$. Siden $3 \mid 57$, vet vi fra Proposisjon 3.4.9 at kongruensen har en løsning. Ved å benytte algoritmen i Merknad 2.7.15, får vi:

$$3 = 2 \cdot 12 + (-1) \cdot 21.$$

Siden $57 = 19 \cdot 3$, er $k = 19$. Derfor fastslår Korollar 3.4.36 at $x = 19 \cdot 2$ er en løsning til kongruensen, altså at $x = 38$ er en løsning til kongruensen.

Når vi deler 38 med 21 får vi 17 som resten. Det følger fra Proposisjon 3.4.24 at $x = 17$ er en løsning til kongruensen.

Eksempel 3.4.35. La oss se på kongruensen

$$-8x \equiv 20 \pmod{44}.$$

Vi har: $\mathsf{sfd}(-8, 44) = 4$. Siden $4 \mid 20$, vet vi fra Proposisjon 3.4.9 at kongruensen har en løsning. Ved å benytte algoritmen i Merknad 2.7.15, får vi:

$$4 = 5 \cdot (-8) + 1 \cdot 44.$$

Siden $20 = 5 \cdot 4$, er $k = 4$. Derfor fastslår Korollar 3.4.36 at $x = 5 \cdot 5$ er en løsning til kongruensen, altså at $x = 25$ er en løsning til kongruensen.

Korollar 3.4.36. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La d være et naturlig tall slik at $\mathsf{sfd}(a, n) = d$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vn$. Ut ifra definisjonen til $\mathsf{sfd}(a, n)$ vet vi at $d \mid n$, altså at det finnes heltall k_n slik at $n = k_n d$. Anta at $d \mid c$, altså at det et heltall k slik at $c = kd$. Da er følgende sanne.

(I) For hvert heltall r slik at $0 \leq r < d$, er

$$x = ku + k_n r$$

en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

(II) La x være et heltall som er en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Da finnes det et heltall r, hvor $0 \leq r < d$, slik at

$$x \equiv ku + k_n r \pmod{n}.$$

(III) La r og s være heltall slik at $0 \leq r < d$ og $0 \leq s < d$. La

$$x = ku + k_n r$$

og

$$x' = ku + k_n s$$

være to av løsningene i (I) til kongruensen

$$ax \equiv c \pmod{n}.$$

Dersom

$$x \equiv x' \pmod{n},$$

er $r = s$.

Bevis. Følger umiddelbart fra Proposisjon 3.4.33 og Proposisjon 3.4.16. □

Eksempel 3.4.37. La oss se på kongruensen

$$12x \equiv 57 \pmod{21}.$$

Som i Eksempel 3.4.34, er $\mathsf{sfd}(12, 57) = 3$ og $ku = 38$. Siden $21 = 7 \cdot 3$, er $k_n = 7$. Derfor fastslår Korollar 3.4.36 at:

(I) $x = 38 + 7r$ er en løsning til kongruensen for alle heltallene r slik at $0 \leq r < 3$, altså $x = 38$, $x = 45$, og $x = 52$ er løsninger til kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) Ikke noe par av disse tre løsningene er kongruent til hverandre modulo 21.

Når vi deler 38, 45, og 52 med 21, får vi restene 17, 3, og 10. Dermed følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 3$, $x = 10$, og $x = 17$ er løsninger til kongruensen.

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 21.

Etter at vi fant løsningen $x = 38$, kunne vi alternativt hatt først dedusert, som i Eksempel 3.4.34, at $x = 17$ er en løsning. Da kan vi benytte Proposisjon 3.4.16 for å få:

(I) $x = 17 + 7r$ er en løsning til kongruensen for alle heltallene r slik at $0 \leq r < 3$, altså $x = 17$, $x = 24$, og $x = 31$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) ikke noe par av disse tre løsningene er kongruent til hverandre modulo 21.

Når vi deler 24 og 31 med 21, får vi restene 3 og 10. Dermed følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 3$, $x = 10$, og $x = 17$ er løsninger til kongruensen.

(II) enhver annen løsning til kongruensen er kongruent modulo 21 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 21.

Eksempel 3.4.38. La oss se på kongruensen

$$-8x \equiv 20 \pmod{44}.$$

Som i Eksempel 3.4.35, er $\mathsf{sfd}(-8, 44) = 4$ og $ku = 25$. Siden $44 = 11 \cdot 4$, er $k_n = 11$. Derfor fastslår Korollar 3.4.36 at:

(I) $x = 25 + 11r$ er en løsning til kongruensen for alle heltallene r slik at $0 \leq r < 4$, altså $x = 25$, $x = 36$, $x = 47$, og $x = 58$ er løsninger til kongruensen;

(II) enhver annen løsning til kongruensen er kongruent modulo 44 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 44.

Når vi deler 25, 36, 47, og 58 med 44, får vi restene 25, 36, 3, og 14. Dermed følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 3$, $x = 14$, $x = 25$, og 36 er løsninger til kongruensen.

(II) enhver annen løsning til kongruensen er kongruent modulo 44 til én av disse løsningene.

(III) ikke noe par av disse fire løsningene er kongruent til hverandre modulo 44.

Korollar 3.4.39. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Anta at $\mathsf{sfd}(a, n) = 1$. Fra Korollar 2.7.20 vet vi at det finnes heltall u og v slik at $d = ua + vn$. Da er $x = cu$ en løsning til kongruensen

$$ax \equiv c \pmod{n},$$

og enhver annen løsning er kongruent modulo n til denne løsningen.

Bevis. Følger umiddelbart fra Korollar 3.4.36. □

Eksempel 3.4.40. La oss se på kongruensen

$$7x \equiv 16 \pmod{23}.$$

Vi har: $\mathsf{sfd}(7, 23) = 1$. Siden $1 \mid 16$, vet vi fra Proposisjon 3.4.9 at kongruensen har en løsning. Ved å benytte algoritmen i Merknad 2.7.15, får vi:

$$1 = 10 \cdot 7 + (-3) \cdot 23.$$

Derfor fastslår Korollar 3.4.36 at:

(1) $x = 16 \cdot 10$ er en løsning til kongruensen, altså $x = 160$ er en løsning til kongruensen;

(2) enhver annen løsning til kongruensen er kongruent modulo 23 til denne løsningen.

Når vi deler 160 med 23, får vi 22 som resten. Det følger fra Proposisjon 3.4.24 at $x = 22$ er en løsning til kongruensen. Da fastslår (II) i Proposisjon 3.4.16 at enhver annen løsning er kongruent til denne modulo 23.

Merknad 3.4.41. I Merknad 3.4.27 og Merknad 3.4.30 har vi sett to metoder som kan hjelpe oss å finne en løsning til kongruensen

$$ax \equiv c \pmod{n}$$

fortere i praksis enn å benytte Euklids algoritme og Merknad 2.7.15. Følgende proposisjon kan også være til hjelp.

Proposisjon 3.4.42. La n være et heltall slik at $n \neq 0$. La a og c være heltall. La y være et heltall slik at

$$ay \equiv 1 \pmod{n}.$$

Da er $x = yc$ en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Bevis. Siden

$$ay \equiv 1 \pmod{n},$$

følger det fra Korollar 3.2.45 at

$$ayc \equiv c \pmod{n}.$$

□

Eksempel 3.4.43. La oss se på kongruensen

$$5x \equiv 17 \pmod{19}.$$

Siden

$$5 \cdot 4 - 1 = 19$$

og $19 \mid 19$, er $y = 4$ en løsning til kongruensen

$$5y = 1 \pmod{19}.$$

Da fastslår Proposisjon 3.4.42 at

$$x = 4 \cdot 17,$$

altså $x = 68$, er en løsning til kongruensen.

Når vi deler 68 med 19 får vi resten 11. Det følger fra Proposisjon 3.4.24 at $x = 11$ er en løsning til kongruensen. Siden $\mathsf{sfd}(5, 19) = 1$, er alle andre løsninger kongruent modulo 19 til denne løsningen.

Eksempel 3.4.44. La oss se på kongruensen

$$6x \equiv -24 \pmod{9}.$$

Vi har: $\mathsf{sfd}(6, 9) = 3$. Da fastslår Proposisjon 3.4.13 at et heltall x er en løsning til denne kongruensen hvis og bare hvis det finnes en løsning til kongruensen

$$2x \equiv -8 \pmod{3}.$$

Siden

$$2 \cdot 2 - 1 = 3$$

og $3 \mid 3$, er $x = 2$ en løsning til kongruensen

$$2x \equiv 1 \pmod{3}.$$

Da fastslår Proposisjon 3.4.42 at

$$x = 2 \cdot (-8),$$

altså $x = -16$, er en løsning til kongruensen

$$2x \equiv -8 \pmod{3},$$

altså til kongruensen

$$6x \equiv -24 \pmod{9}.$$

Nå kan vi benytte Proposisjon 3.4.16 for å finne de andre løsningene. Siden $9 = 3 \cdot 3$, er $k_n = 3$. Da fastslår Proposisjon 3.4.16 at:

(I) $x = -16 + 3r$ er en løsning til kongruensen

$$6x \equiv -24 \pmod 9$$

for alle heltallene r slik at $0 \leq r < 3$, altså $x = -16$, $x = -13$, og $x = -10$, er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 9 til én av disse løsningene.

(III) Ikke noe par av disse tre løsningene er kongruent til hverandre modulo 9.

Når vi deler -16, -13, og -10 med 9, får vi restene 2, 5, og 8. Da følger det fra Proposisjon 3.4.24, (I) – (III) ovenfor, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 2$, $x = 5$, og $x = 8$ er løsninger til kongruensen

$$6x \equiv -24 \pmod 9.$$

(II) Enhver løsning til kongruensen er kongruent modulo 9 til én av disse løsningene.

(III) Ikke noe par av disse tre løsningene er kongruent til hverandre modulo 9.

Merknad 3.4.45. Følgende proposisjon kan spare oss litt arbeid når vi ønsker å finne løsningene til en kongruens.

Proposisjon 3.4.46. La n være et heltall slik at $n \neq 0$. La a, c, og x være heltall. Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at:

(1) $c \equiv r \pmod n$;

(2) $0 \leq r < n$.

Da er

$$ax \equiv c \pmod n$$

hvis og bare hvis

$$ax \equiv r \pmod n.$$

Bevis. Anta først at

$$ax \equiv c \pmod n.$$

Siden

$$c \equiv r \pmod n,$$

følger det fra Proposisjon 3.2.33 at

$$ax \equiv r \pmod n.$$

Anta istedenfor at

$$ax \equiv r \pmod n.$$

Siden $c \equiv r \pmod{n}$, følger det fra Proposisjon 3.2.24 at

$$r \equiv c \pmod{n}.$$

Da følger det fra Proposisjon 3.2.33 at

$$ax \equiv c \pmod{n}.$$

□

Eksempel 3.4.47. Vi har: $87 \equiv 3 \pmod{12}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$9x \equiv 87 \pmod{12}$$

hvis og bare hvis x er en løsning til kongruensen

$$9x \equiv 3 \pmod{12}.$$

Eksempel 3.4.48. Vi har: $-102 \equiv 18 \pmod{20}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$12x \equiv -102 \pmod{20}$$

hvis og bare hvis x er en løsning til kongruensen

$$12x \equiv 18 \pmod{20}.$$

Merknad 3.4.49. La n være et heltall slik at $n \neq 0$. La a og c være heltall. Vi har nå rukket en komplett forståelse for kongruensen

$$ax \equiv c \pmod{n},$$

og har i tillegg sett flere metoder for å finne fort dens løsninger. For å oppsummere, har vi følgende oppskrift.

(1) Regn ut $\mathsf{sfd}(a, n)$. La oss betegne $\mathsf{sfd}(a, n)$ som d. Dersom $d \mid c$, har kongruensen en løsning: gå da videre til (3), eller valgfritt til (2). Ellers har kongruensen ikke en løsning.

(2) Dersom $c > n$, finn et heltall r slik at $c \equiv r \pmod{n}$ og $0 \leq r < n$. Gå da videre til (3) ved å erstatte c med r.

(3) Prøv å finne én løsning. For å gjøre dette, kan vi gå videre til ett av (4), (5), (6), eller (7). Dersom $\mathsf{sfd}(a, n) > 1$, er det typisk best å gå videre til (5).

(4) Ved å benytte algoritmen i Merknad 2.7.15, finn heltall u og v slik at $d = ua + vn$. Finn heltallet k slik at $c = kd$. Da er $x = ku$ en løsning. Gå videre til (8).

(5) Dersom $\mathsf{sfd}(a, n) > 1$, finn heltallet k_a slik at $a = k_a \cdot d$, heltallet k_c slik at $c = k_c d$, og heltallet k_n slik at $n = k_n \cdot d$. Prøv å finne én løsning til kongruensen

$$k_a \equiv k_c \pmod{k_n}$$

ved å gå videre til (4), (6) eller (7), og ved å erstatte a med k_a, c med k_c, og n med k_n. Ofte er det i praksis best å gå videre til (6) eller (7).

(6) Sjekk om x er en løsning til kongruensen for alle heltallene x slik at $0 \leq x < n$. Stopp når en løsning er blitt funnet. Gå videre til (8).

(7) Finn en løsning til kongruensen

$$ay \equiv 1 \pmod{n}.$$

Da er yc en løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

Gå videre til (8).

(8) Etter at vi har funnet én løsning, benytt Proposisjon 3.4.16 for å finne de andre. Gå valgfritt videre til (8).

(9) Benytt Proposisjon 3.4.24, Proposisjon 3.2.24, og Proposisjon 3.2.33, for å finne alle løsningene x slik at $0 \leq x < n$.

Eksempel 3.4.50. La oss se på kongruensen

$$16x \equiv 56 \pmod{24}.$$

Vi gjør følgende.

(1) Først regner vi ut $\mathsf{sfd}(16, 24)$. Vi får: $\mathsf{sfd}(16, 24) = 8$. Siden $8 \mid 56$, fastslår Proposisjon 3.4.9 at kongruensen har en løsning. Da har vi fullført Steg (1) i Merknad 3.4.49.

(2) Siden $56 - 8 = 48$ og $24 \mid 48$, er $56 \equiv 8 \pmod{24}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$16x \equiv 56 \pmod{24}$$

hvis og bare hvis x er en løsning til kongruensen

$$16x \equiv 8 \pmod{24}.$$

Nå skal vi prøve å finne løsningene til denne kongruensen. Dette fullfører Steg (2) i Merknad 3.4.49.

(3) For å finne løsningene til kongruensen

$$16x \equiv 8 \pmod{24},$$

skal vi først prøve å finne én løsning. Dette fullfører Steg (3) i Merknad 3.4.49.

(4) Ut ifra Proposisjon 3.4.30, er x en løsning til kongruensen

$$16x \equiv 8 \pmod{24}$$

hvis og bare hvis x er en løsning til kongruensen

$$2x \equiv 1 \pmod{3}.$$

Nå skal vi prøve å finne én løsning til denne kongruensen. Dette fullfører Steg (5) i Merknad 3.4.49.

(5) Nå sjekker vi om x er en løsning til kongruensen

$$2x \equiv 1 \pmod{3}$$

for hvert heltall x slik at $0 \leq x < 3$. Siden

$$2 \cdot 2 - 1 = 3$$

og $3 \mid 3$, får vi at $x = 2$ er en løsning. Dette fullfører Steg (6) i Merknad 3.4.49.

(6) Vi har:

$$24 = 3 \cdot 8.$$

Da fastslår Proposisjon 3.4.16 at:

(I) $x = 2 + 3r$ er en løsning til kongruensen

$$16x \equiv 56 \pmod{24}$$

for alle heltallene r slik at $0 \leq r < 8$, altså $x = 2$, $x = 5$, $x = 8$, $x = 11$, $x = 14$, $x = 15$, $x = 18$, $x = 21$ er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 24 til én av disse løsningene.

(III) Ikke noe par av disse åtte løsningene er kongruent til hverandre modulo 24.

Dette fullfører Steg (8) i Merknad 3.4.49.

(7) Siden alle løsningene x i (7) oppfyller $0 \leq x < 24$, er det ikke noe å gjøre i Steg (9) i Merknad 3.4.49.

Vi kunne alternativt har gjort ett av følgende.

(1) Vi kunne har benyttet algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$16x \equiv 56 \pmod{24}$$

og da benyttet Proposisjon 3.4.16 for å finne de andre løsningene. Dermed hadde vi gått fra Steg (1) til Steg (3) til Steg (4) til Steg (8) i Merknad 3.4.49.

(2) Vi kunne har benyttet algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$16x \equiv 8 \pmod{24}$$

og da benyttet Proposisjon 3.4.16 for å finne de andre løsningene. Dermed hadde vi gått fra Steg (1) til Steg (2) til Steg (3) til Steg (4) til Steg (8) i Merknad 3.4.49.]

(3) Vi kunne har benyttet algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$2x \equiv 1 \pmod{3}$$

og da benyttet Proposisjon 3.4.16 for å finne de andre løsningene. Dermed hadde vi gått fra Steg (1) til Steg (2) til Steg (3) til Steg (5) til Steg (4) til Steg (8) i Merknad 3.4.49.

I tillegg kunne vi har benyttet metoden i (7) i Merknad 3.4.49 på flere steder. For eksempel kunne vi har funnet en løsning til kongruensen

$$16x \equiv 1 \pmod{24},$$

og benyttet dette heltallet for å finne en løsning til kongruensen

$$16x \equiv 8 \pmod{24}.$$

Imidlertid rekker vi en løsning fortere ved å følge stegene (1) – (7) ovenfor.

Eksempel 3.4.51. La oss se på kongruensen

$$-27x \equiv -99 \pmod{45}.$$

Vi gjør følgende.

(1) Først regner vi ut $\mathsf{sfd}(-27, 45)$. Vi får: $\mathsf{sfd}(-27, 45) = 9$. Siden $9 \mid -99$, fastslår Proposisjon 3.4.9 at kongruensen har en løsning. Da har vi fullført Steg (1) i Merknad 3.4.49.

(2) Siden $-99 - 36 = -135$ og $45 \mid -135$, er $-99 \equiv 36 \pmod{45}$. Da fastslår Proposisjon 3.4.46 at x er en løsning til kongruensen

$$-27x \equiv -99 \pmod{45}$$

hvis og bare hvis x er en løsning til kongruensen

$$-27x \equiv 36 \pmod{45}.$$

Nå skal vi prøve å finne løsningene til denne kongruensen. Dette fullfører Steg (2) i Merknad 3.4.49.

(3) For å finne løsningene til kongruensen

$$-27x \equiv 36 \pmod{45},$$

skal vi først prøve å finne én løsning. Dette fullfører Steg (3) i Merknad 3.4.49.

(4) Ut ifra Proposisjon 3.4.30, er x en løsning til kongruensen

$$-27x \equiv 36 \pmod{45}$$

hvis og bare hvis x er en løsning til kongruensen

$$-3x \equiv 4 \pmod{5}.$$

Nå skal vi prøve å finne én løsning til denne kongruensen. Dette fullfører Steg (5) i Merknad 3.4.49.

(5) Nå prøver vi å finne en løsning til kongruensen

$$-3y \equiv 1 \pmod{5}.$$

Siden

$$(-3) \cdot (-2) - 1 = 5$$

og $5 \mid 5$, er $y = -2$ en løsning til denne kongruensen. Da fastslår Proposisjon 3.4.42 at $x = (-2) \cdot 4$, altså $x = -8$ er en løsning til kongruensen

$$-3x \equiv 4 \pmod{5}.$$

Dette fullfører Steg (7) i Merknad 3.4.49.

(6) Vi har:

$$45 = 5 \cdot 9.$$

Da fastslår Proposisjon 3.4.16 at:

(I) $x = -8 + 5r$ er en løsning til kongruensen

$$-18x \equiv -99 \pmod{45}$$

for alle heltallene r slik at $0 \leq r < 9$, altså $x = -8$, $x = -3$, $x = 2$, $x = 7$, $x = 12$, $x = 17$, $x = 22$, $x = 27$, og $x = 32$ er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 45 til én av disse løsningene.

(III) Ikke noe par av disse ni løsningene er kongruent til hverandre modulo 45.

Dette fullfører Steg (8) i Merknad 3.4.49.

(7) Når vi deler $x = -8$ og $x = -3$ med 45, får vi restene 37 og 42. Derfor fastslår Proposisjon 3.4.24, Proposisjon 3.2.24, og Proposisjon 3.2.33 at:

(I) $x = 2$, $x = 7$, $x = 12$, $x = 17$, $x = 22$, $x = 27$, $x = 32$, $x = 37$, og $x = 42$ er løsninger til denne kongruensen.

(II) Enhver løsning til kongruensen er kongruent modulo 45 til én av disse løsningene.

(III) Ikke noe par av disse ni løsningene er kongruent til hverandre modulo 45.

Dette fullfører Steg (9) i Merknad 3.4.49.

Alternativt kunne vi har gjort følgende.

(1) For å finne en løsning til kongruensen

$$-3x \equiv 4 \pmod{5},$$

kunne vi har sjekket om x er en løsning for hvert heltall x slik at $0 \leq x < 4$. Siden

$$(-3) \cdot 2 - 4 = -10$$

og $5 \mid --10$, får vi at $x = 2$ er en løsning. Dette fullfører Steg (6) i Merknad 3.4.49. Da hadde vi gått videre til Steg (8) i Merknad 3.4.49.

(2) Som i Eksempel 3.4.50, kunne vi har benyttet algoritmen i Merknad 2.7.15 istedenfor ett av (2), (4), eller (5) ovenfor, og så gått videre til Steg (8) i Merknad 3.4.49.

I tillegg, som i Eksempel 3.4.50, kunne vi har benyttet metoden i (7) i Merknad 3.4.49 på flere steder. Imidlertid rekker vi en løsning fortere ved å følge stegene (1) – (7) ovenfor.

Merknad 3.4.52. Generelt sett er det best å benytte algoritmen i Merknad 2.7.15 for å finne en løsning til kongruensen

$$ax \equiv c \pmod{n}$$

når n er ganske stort, og det er ikke mulig å benytte Proposisjon 3.4.30 for å se istedenfor på en kongruens hvor n er mindre.

Merknad 3.4.53. Mange andre gyldige metoder kan benyttes for å finne én løsning til kongruensen

$$ax \equiv c \pmod{n}.$$

For eksempel kan vi argumentere på en lignende måte som i Proposisjon 3.4.42, med for eksempel -1 istedenfor 1, og $-yc$ istedenfor yc. Vær kreativ!

O3 Oppgaver – Modulær aritmetikk

O3.1 Oppgaver i eksamens stil

Oppgave O3.1.1. Hvilke av de følgende er sanne?

(1) $123 \equiv 155 \pmod 4$?

(2) $-5 \equiv 18 \pmod 7$?

(3) $36 \equiv -8 \pmod{11}$?

Begrunn svarene dine.

Oppgave O3.1.2. Gjør følgende.

(1) Vis at $53 \equiv 14 \pmod{39}$ og at $196 \equiv 1 \pmod{39}$. Deduser at

$$53^2 \equiv 1 \pmod{39}.$$

(2) Vis at $103 \equiv -14 \pmod{39}$. Deduser fra dette og kongruensen $196 \equiv 1 \pmod{39}$ at $103^2 \equiv 1 \pmod{39}$.

(3) Benytt (1) og (2) for å vise at

$$53^{103} + 103^{53}$$

er delelig med 39.

Oppgave O3.1.3. Gjør følgende.

(1) Vis at $32 \equiv 5 \pmod{27}$.

(2) La t være et naturlig tall. Benytt (1) for å vise at

$$2^{5t+1} + 5^{t+2}$$

er delelig med 27. *Tips*: Observer at $2^{5t} = 32^t$.

Oppgave O3.1.4. La x være et naturlig tall. Anta at det er et heltall n slik at $n \geq 0$ og

$$x = x_n \cdot 10^n + x_{n-1} \cdot 10^{n-1} + \cdots + x_2 \cdot 10^2 + x_1 \cdot 10^1 + x_0 \cdot 10^0,$$

hvor, for hvert heltall i slik at $0 \leq i \leq n$, er x_i et heltall slik at $x_i \geq 0$. Gjør følgende.

(1) Vis at $10 \equiv 4 \pmod 6$.

(2) La i være et naturlig tall. Vis at $10^i \equiv 4 \pmod 6$. *Tips*: Benytt (1) og induksjon.

(3) Benytt (2) for å vise at x er delelig med 6 hvis og bare hvis summen

$$x_0 + 4x_1 + 4x_2 + \cdots + 4x_{n-1} + 4x_n$$

er delelig med 6.

(4) Er 1321473 delelig med 6? Benytt (3) i løpet av svaret ditt.

Oppgave O3.1.5. Benytt algoritmen i Merknad 2.7.15 i minst én del av oppgaven, men ikke i alle de tre delene.

(1) Finn løsninger til kongruensen

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

slik at alle løsningene til denne kongruensen er kongruent modulo 27 til ett av heltallene i lista di, og slik at ikke noe par av heltallene i lista di er kongruent til hverandre modulo 27.

(2) Finn løsninger til kongruensen

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

slik at alle løsningene til denne kongruensen er kongruent modulo 128 til ett av heltallene i lista di, og slik at ikke noe par av heltallene i lista di er kongruent til hverandre modulo 128.

(3) Finn løsninger til kongruensen

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

slik at alle løsningene til denne kongruensen er kongruent modulo 50 til ett av heltallene i lista di, og slik at ikke noe par av heltallene i lista di er kongruent til hverandre modulo 50.