Forelesning 12 — torsdag den 25. september

2.10 Delbarhet og Fibonaccitallene

Merknad 2.10.1. Nå skal vi benytte teorien vi har sett på i dette kapittelet for å utforske Fibonaccitallene videre.

Notasjon 2.10.2. La n være et naturlig tall. I resten av dette kapittelet kommer alltid u_n til å betegne det n-te Fibonaccitallet.

Proposisjon 2.10.3. La n være et naturlig tall. Da er $\mathsf{sfd}(u_n, u_{n+1}) = 1$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at $\mathsf{sfd}(u_1, u_2) = 1$. Siden $u_1 = 1$ og $u_2 = 1$, er dette sant.

Anta nå at proposisjonen har blitt bevist for et gitt naturlig tall m. Således har det blitt bevist at $\mathsf{sfd}(u_m, u_{m+1}) = 1$. La c være et naturlig tall slik at:

(i) $c \mid u_{m+1}$;

(ii) $c \mid u_{m+2}$.

Vi gjør følgende observasjoner.

(1) Fra (i) og Proposisjon 2.5.12 følger det at $c \mid -u_{m+1}$.

(2) Ut ifra definisjonen til Fibonaccitallene er $u_{m+2} = u_m + u_{m+1}$. Derfor er $u_m = u_{m+2} - u_{m+1}$.

(3) Fra (ii), (1), (2), og Proposisjon 2.5.24, følger det at $c \mid u_m$.

Fra (3), (i), og antakelsen at $\mathsf{sfd}(u_m, u_{m+1}) = 1$, følger det at $c = 1$.

Dersom $c \mid u_{m+1}$ og $c \mid u_{m+2}$, har vi dermed bevist at $c = 1$. Vi deduserer at $\mathsf{sfd}(u_{m+1}, u_{m+2}) = 1$. Således er proposisjonen sann når $n = m + 1$.

Ved induksjon konkluderer vi at proposisjonen er sann for alle naturlige tall.

□

Eksempel 2.10.4. La n være 5. Da fastslår Proposisjon 2.10.3 at $\mathsf{sfd}(u_5, u_6) = 1$, altså at $\mathsf{sfd}(5, 8) = 1$.

Eksempel 2.10.5. La n være 7. Da fastslår Proposisjon 2.10.3 at $\mathsf{sfd}(u_7, u_8) = 1$, altså at $\mathsf{sfd}(13, 21) = 1$.

Lemma 2.10.6. La n være et naturlig tall. La l være et naturlig tall slik at $l \geq 2$. Da er

$$u_{l+n} = u_{l-1}u_n + u_l u_{n+1}.$$

Bevis. Siden $n \geq 1$, er $n-1 \geq 0$. Siden $l \geq 2$, er $l+1 \geq 3$.Derfor følger det fra Proposisjon 1.14.1 at

$$\begin{aligned} u_{(n-1)+(l+1)} &= u_{(l+1)-1}u_{(n-1)+2} + u_{(l+1)-2}u_{(n-1)+1} \\ &= u_l u_{n+1} + u_{l-1}u_n \\ &= u_{l-1}u_n + u_l u_{n+1}. \end{aligned}$$

Dermed er

$$\begin{aligned} u_{l+n} &= u_{n+l} \\ &= u_{(n-1)+(l+1)} \\ &= u_{l-1}u_n + u_l u_{n+1}. \end{aligned}$$

□

Eksempel 2.10.7. Når $n = 3$ og $l = 7$, fastslår Proposisjon 1.14.1 at

$$u_{10} = u_6 u_3 + u_7 u_4,$$

altså at

$$55 = 8 \cdot 2 + 13 \cdot 3.$$

Eksempel 2.10.8. Når $n = 6$ og $l = 5$, fastslår Proposisjon 1.14.1 at

$$u_{11} = u_4 u_6 + u_5 u_7,$$

altså at

$$89 = 3 \cdot 8 + 5 \cdot 13.$$

Proposisjon 2.10.9. La l og n være naturlige tall. Da har vi: $u_l \mid u_{ln}$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. I dette tilfellet er utsagnet at

$$u_l \mid u_l.$$

Siden $u_l = 1 \cdot u_l$, er dette sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m. Således har det blitt bevist at

$$u_l \mid u_{lm}.$$

Ett av følgende utsagn er sant.

(A) $l = 1$;

(B) $l \geq 2$.

Anta først at (A) er tilfellet. Siden $u_1 = 1$, er det sant at $u_1 \mid u_{m+1}$, altså at $u_1 \mid u_{1\cdot(m+1)}$. Dermed er proposisjonen sann når $n = m + 1$ i dette tilfellet.

Anta nå at (B) er tilfellet. Vi gjør følgende observasjoner.

(1) Vi har:
$$u_{l(m+1)} = u_{lm+l}.$$

(2) Siden $l \geq 2$, følger det fra Lemma 2.10.6 at
$$u_{lm+l} = u_{lm-1}u_l + u_{lm}u_{l+1}.$$

(3) Ut ifra antakelsen at $u_l \mid u_{lm}$ finnes det et heltall k slik at $u_{lm} = k \cdot u_l$.

(4) Det følger fra (2) og (3) at
$$\begin{aligned} u_{lm+l} &= u_{lm-1}u_l + ku_lu_{l+1} \\ &= (u_{lm-1} + ku_{l+1})\, u_l. \end{aligned}$$

(5) Siden hvert Fibonaccitall er et naturlig tall og k er et heltall, er $u_{lm-1} + ku_{l+1}$ et heltall.

(6) Det følger fra (4) og (5) at $u_l \mid u_{lm+l}$.

Dermed har vi bevist at $u_l \mid u_{l(m+1)}$. Således er proposisjonen sann når $n = m + 1$.

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

□

Eksempel 2.10.10. Når $l = 3$ og $n = 5$, fastslår Proposisjon 2.10.9 at $u_3 \mid u_{15}$, altså at $2 \mid 610$.

Eksempel 2.10.11. Når $l = 4$ og $n = 3$, fastslår Proposisjon 2.10.9 at $u_4 \mid u_{12}$, altså at $3 \mid 144$.

Korollar 2.10.12. La l og k være naturlige tall slik at $l \mid n$. Da er $u_l \mid u_n$.

Bevis. Siden l og n er naturlige tall, finnes det da et naturlig tall k slik at $n = kl$. Det fra Proposisjon 2.10.9 at $u_l \mid u_{kl}$, altså at $u_l \mid u_n$. □

Eksempel 2.10.13. Vi har: $3 \mid 9$. Derfor er $u_3 \mid u_9$, altså $2 \mid 34$.

Eksempel 2.10.14. Vi har: $6 \mid 12$. Derfor er $u_6 \mid u_{12}$, altså $8 \mid 144$.

Lemma 2.10.15. La k, l, n, og r være naturlige tall slik at $n = kl+r$. Da er $\mathsf{sfd}(u_n, u_l) = \mathsf{sfd}(u_r, u_l)$.

Bevis. Ett av følgende utsagn er sant:

(A) $k = 1$ og $l = 1$;

(B) $kl \geq 2$.

Anta først at (A) er tilfellet. Da er utsagnet at $\mathsf{sfd}(u_n, u_1) = \mathsf{sfd}(u_r, u_1)$. Siden $u_1 = 1$, har vi:

$$\mathsf{sfd}(u_n, u_1) = \mathsf{sfd}(u_n, 1) = 1$$

og

$$\mathsf{sfd}(u_r, u_1) = \mathsf{sfd}(u_r, 1) = 1.$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (B) er tilfellet. Vi skal først bevise at $\mathsf{sfd}(u_{kl-1}, u_l) = 1$. La c være et naturlig tall slik at:

(i) $c \mid u_{kl-1}$;

(ii) $c \mid u_l$.

Vi gjør følgende observasjoner.

(1) Fra Proposisjon 2.10.9 har vi: $u_l \mid u_{kl}$.

(2) Det følger fra (ii), (1), og Proposisjon 2.5.27 at $c \mid u_{kl}$.

(3) Fra (i), (2), og Proposisjon 2.10.3 følger det at $c = 1$.

Dersom $c \mid u_{kl-1}$ og $c \mid u_l$, har vi dermed bevist at $c = 1$. Derfor er $\mathsf{sfd}(u_{kl-1}, u_l) = 1$.

Nå gjør vi følgende observasjoner.

(1) Siden $kl \geq 2$, følger det fra Lemma 2.10.6 at

$$u_{kl+r} = u_{kl-1}u_r + u_{kl}u_{r+1}.$$

(2) Ut ifra Proposisjon 2.10.9 er $u_l \mid u_{kl}$.

(3) Det følger fra (2) og Korollar 2.5.18 at $u_l \mid u_{r+1}u_{kl}$, altså at $u_l \mid u_{kl}u_{r+1}$.

(4) Det følger fra (3) og Proposisjon 2.6.27 at

$$\mathsf{sfd}(u_{kl-1}u_r + u_{kl}u_{r+1}, u_l) = \mathsf{sfd}(u_{kl-1}u_r, u_l).$$

(5) Vi vet at $\mathsf{sfd}(u_{kl-1}, u_l) = 1$, altså at $\mathsf{sfd}(u_l, u_{kl-1}) = 1$. Det følger fra Proposisjon 2.8.26 at $\mathsf{sfd}(u_l, u_{kl-1}u_r) = \mathsf{sfd}(u_l, u_r)$, altså at $\mathsf{sfd}(u_{kl-1}u_r, u_l) = \mathsf{sfd}(u_r, u_l)$.

Fra (1), (4), og (5) følger det at $\mathsf{sfd}(u_{kl+r}, u_l) = \mathsf{sfd}(u_r, u_l)$, altså at $\mathsf{sfd}(u_n, u_l) = \mathsf{sfd}(u_r, u_l)$.

□

Eksempel 2.10.16. Vi har: $7 = 2 \cdot 3 + 1$. Lemma 2.10.15 fastslår at $\mathsf{sfd}(u_7, u_3) = \mathsf{sfd}(u_3, u_1)$, altså at $\mathsf{sfd}(13, 2) = \mathsf{sfd}(2, 1)$.

Eksempel 2.10.17. Vi har: $13 = 2 \cdot 5 + 3$. Lemma 2.10.15 fastslår at $\mathsf{sfd}(u_{13}, u_5) = \mathsf{sfd}(u_5, u_3)$, altså at $\mathsf{sfd}(233, 5) = \mathsf{sfd}(5, 2)$.

Merknad 2.10.18. Målet vårt er Korollar 2.10.20. Imidlertid skal vi først bevise Proposisjon 2.10.19. Da skal vi observere at Korollar 2.10.20 følger fra Proposisjon 2.10.19.

Sammenlign med Merknad 2.7.4. For hvert par naturlige tall l og s slik at $s < l$, beviser vi på en måte at $\mathsf{sfd}(u_l, u_s) = u_d$ mange ganger: en gang for hvert naturlig tall større enn eller likt l.

Likevel viser det seg at påstanden i Proposisjon 2.10.19 er bedre for å gjennomføre et bevis ved induksjon enn påstanden i Korollar 2.10.20.

Proposisjon 2.10.19. La n være et naturlig tall slik at $n \geq 2$. La s og l være naturlige tall slik at $s < l \leq n$. La $d = \mathsf{sfd}(l, s)$. Da er $\mathsf{sfd}(u_l, u_s) = u_d$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 2$. La l og s være naturlige tall slik at $s < l \leq 2$. La $d = \mathsf{sfd}(l, s)$. Vi må sjekke om

$$\mathsf{sfd}(u_l, u_s) = u_d.$$

Et par naturlige tall l og s oppfyller kravet $s < l \leq 2$ hvis og bare hvis $s = 1$ og $l = 2$. Derfor må vi sjekke om

$$\mathsf{sfd}(u_2, u_1) = u_{\mathsf{sfd}(2,1)}.$$

Vi har: $\mathsf{sfd}(2, 1) = 1$. Siden $u_1 = 1$ og $u_2 = 1$, har vi i tillegg: $\mathsf{sfd}(u_2, u_1) = \mathsf{sfd}(1, 1) = 1$. Dermed er utasgnet sant.

Anta nå at proposisjonen har blitt bevist når n er et gitt naturlig tall m slik at $m \geq 2$. La s og l være naturlige tall slik at $s < l \leq m + 1$. Ut ifra Proposisjon 1.2.6 finnes det heltall k og r slik at $l = ks + r$, $k \geq 0$, og $0 \leq r < s$. Siden $r < s$ og $s < l$, er $r < l$. Derfor er det faktisk ikke sant at $k = 0$, altså k er et naturlig tall. Ett av følgende utsagn er sant:

(A) $r = 0$;

(B) r er et naturlig tall.

Anta først at (A) er tilfellet. Da er $l = ks$, altså $s \mid l$. Vi gjør følgende observasjoner.

(1) Det følger fra Proposisjon 2.6.21 at $\mathsf{sfd}(l, s) = s$.

(2) I tillegg følger det fra Korollar 2.10.12 at $u_l \mid u_s$.

(3) Det følger fra (2) og Proposisjon 2.6.21 at $\mathsf{sfd}(u_l, u_s) = u_s$.

Det følger fra (1) og (3) at $\mathsf{sfd}(u_l, u_s) = \mathsf{sfd}(l, s)$. Dermed er proposisjonen sann i dette tilfellet.

Anta nå at (B) er tilfellet. Vi gjør følgende observasjoner.

(1) Ut ifra Lemma 2.7.3 er $\mathsf{sfd}(l, s) = \mathsf{sfd}(s, r)$.

(2) Siden $s < l \leq m+1$, er $s < m$. La $d = \mathsf{sfd}(s, r)$. Ut ifra antakelsen at proposisjonen er sann når $n = m$, følger det at $\mathsf{sfd}(u_s, u_r) = u_d$.

(3) Ut ifra Lemma 2.10.15 er $\mathsf{sfd}(u_l, u_s) = \mathsf{sfd}(u_s, u_r)$.

Det følger fra (1), (2), og (3) at $\mathsf{sfd}(u_l, u_s) = \mathsf{sfd}(l, s)$. Dermed er proposisjonen sann i dette tilfellet.

□

Korollar 2.10.20. La l og n være naturlige tall. La $d = \mathsf{sfd}(l, n)$. Da er $\mathsf{sfd}(u_l, u_n) = u_d$.

Bevis. Ett av følgende utsagn er sant:

(1) $n = 1$;

(2) $n \geq 2$.

Anta først at $n = 1$. Da er utsagnet at $\mathsf{sfd}(u_l, u_1) = u_{\mathsf{sfd}(l,1)}$. Siden $u_1 = 1$, har vi:

$$\mathsf{sfd}(u_l, u_1) = \mathsf{sfd}(u_l, 1) = 1.$$

I tilleg har vi:

$$u_{\mathsf{sfd}(l,1)} = u_1 = 1.$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at $n \geq 2$. Da følger det umiddelbart fra Proposisjon 2.10.19, ved å la l i proposisjonen være n og s i proposisjonen være l, at utsagnet er sant. □

Merknad 2.10.21. La d være den største felles divisoren til det l-te Fibonaccitallet og det n-te Fibonaccitallet. Proposisjon 2.10.19 fastlår at d er også et Fibonaccitall, nemlig det d-te!

Eksempel 2.10.22. Vi har: $\mathsf{sfd}(6, 9) = 3$. Korollar 2.10.20 fastslår at $\mathsf{sfd}(u_6, u_9) = u_3$, altså at $\mathsf{sfd}(8, 34) = 2$.

Eksempel 2.10.23. Vi har: $\mathsf{sfd}(8, 12) = 4$. Korollar 2.10.20 fastslår at $\mathsf{sfd}(u_8, u_{12}) = u_4$, altså at $\mathsf{sfd}(21, 144) = 3$.

Korollar 2.10.24. La l og n være naturlige tall slik at $l \geq 3$ Da er u_n delelig med u_l hvis og bare hvis n er delelig med l.

Bevis. Anta først at u_n er delelig med u_l. Vi gjør følgende observasjoner.

(1) Siden u_n er delelig med u_l, følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(u_l, u_n) = u_l$.

(2) Ut ifra Korollar 2.10.20 er $\mathsf{sfd}(u_l, u_n) = u_{\mathsf{sfd}(l,n)}$.

(3) Det følger fra $u_l = u_{\mathsf{sfd}(l,n)}$.

(4) De eneste naturlige tallene $i \neq j$ slik at $u_i = u_j$ er $i = 1$ og $j = 2$.

(5) Siden $l \geq 3$, følger det fra (3) og (4) at $l = \mathsf{sfd}(l, n)$.

Fra definisjonen til $\mathsf{sfd}(l, n)$ har vi: $\mathsf{sfd}(l, n) \mid n$. Dermed har vi: $l \mid n$.

Anta istedenfor at $l \mid n$. Korollar 2.10.12 fastslår at $u_l \mid u_n$.

□

Eksempel 2.10.25. Siden 10 er ikke delelig med 4, følger det fra Korollar 2.10.24 er u_{10} er ikke delelig med u_4, altså er 55 ikke delelig med 3.

Eksempel 2.10.26. Siden 54 er ikke delelig med 23, følger det fra Korollar 2.10.24 er u_{54} er ikke delelig med u_{23}.

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 1.2.11 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 $11 \mid 837$.

Oppgaver

O2.1 Oppgaver i eksamens stil

Oppgave O2.1.13. For et hvilket som helst naturlig tall r, la u_r betegne det r-te Fibonaccitallet. Finn $\mathsf{sfd}(u_{2793}, u_{462})$.

Oppgave O2.1.14. For et hvilket som helst naturlig tall r, la u_r betegne det r-te Fibonaccitallet. La l og n være naturlige tall. Anta at $\mathsf{sfd}(l, n) = 1$. Bevis at $u_l u_n \mid u_{ln}$.

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.