Innhold

4 Primtall

4.1 Primtall

Definisjon 4.1.1. La n være et naturlig tall. Da er n et *primtall* om:

(1) $n \geq 2$;

(2) de eneste naturlige tallene som er divisorer til n er 1 og n.

Eksempel 4.1.2. Siden det ikke er sant at $1 \geq 2$, er 1 ikke et primtall.

Eksempel 4.1.3. De eneste naturlige tallene som er divisorer til 2 er 1 og 2. Derfor er 2 et primtall.

Eksempel 4.1.4. De eneste naturlige tallene som er divisorer til 3 er 1 og 3. Derfor er 3 et primtall.

Eksempel 4.1.5. Siden 2 er en divisor til 4, er 1 og 4 ikke de eneste divisorene til 4. Derfor er 4 ikke et primtall.

Eksempel 4.1.6. De eneste naturlige tallene som er divisorer til 5 er 1 og 5. Derfor er 5 et primtall.

Eksempel 4.1.7. Siden 2 og 3 er divisorer til 6, er 1 og 6 ikke de eneste divisorene til 6. Derfor er 6 ikke et primtall.

Eksempel 4.1.8. De eneste naturlige tallene som er divisorer til 7 er 1 og 7. Derfor er 7 et primtall.

Eksempel 4.1.9. Siden 2 og 4 er divisorer til 8, er 1 og 8 ikke de eneste divisorene til 8. Derfor er 8 ikke et primtall.

Eksempel 4.1.10. Siden 3 er en divisor til 9, er 1 og 9 ikke de eneste divisorene til 9. Derfor er 9 ikke et primtall.

Eksempel 4.1.11. Siden 2 og 45 er divisorer til 10, er 1 og 10 ikke de eneste divisorene til 10. Derfor er 10 ikke et primtall.

Merknad 4.1.12. De første ti primtallene er: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Sjekk om du er enig om dette!

4.2 Grunnleggende proposisjoner om primtall

Proposisjon 4.2.1. La x være et heltall. La p være et primtall. Da er enten $\mathsf{sfd}(p, x) = 1$ eller $\mathsf{sfd}(p, x) = p$.

Bevis. Vi gjør følgende observasjoner:

(1) siden p er et primtall, er 1 og p de eneste divisorene til p;

(2) $\mathsf{sfd}(p, x)$ er en divisor til p.

Det følger fra (1) og (2) at enten $\mathsf{sfd}(p, x) = 1$ eller $\mathsf{sfd}(p, x) = p$.

□

Eksempel 4.2.2. La x være 12, og la p være 5. Da er $\mathsf{sfd}(5, 12) = 1$.

Eksempel 4.2.3. La x være 15, og la p være 5. Da er $\mathsf{sfd}(5, 15) = 5$.

Merknad 4.2.4. Proposisjon 4.2.1 er selvfølgelig ikke sann om vi ikke antar at p er et primtall: ellers hadde begrepet «største felles divisor» ikke vært veldig nyttig! Hvis for eksempel $x = 12$ og $p = 8$, er $\mathsf{sfd}(8, 12) = 4$. Dermed er det ikke sant at $\mathsf{sfd}(8, 12) = 1$ eller $\mathsf{sfd}(8, 12) = 12$.

Korollar 4.2.5. La x være et heltall. La p være et primtall. Hvis $p \mid x$ er $\mathsf{sfd}(p, x) = p$. Ellers er $\mathsf{sfd}(p, x) = 1$.

Bevis. Anta først at det ikke er sant at $p \mid x$. Vi gjør følgende observasjoner:

(1) ut ifra Proposisjon 4.2.1 er enten $\mathsf{sfd}(p, x) = 1$ eller $\mathsf{sfd}(p, x) = p$;

(2) $\mathsf{sfd}(p, x)$ er en divisor til x.

Fra (1), (2), og antakelsen at det ikke er sant at $p \mid x$, følger det at $\mathsf{sfd}(p, x) = 1$.

Anta istedenfor at $p \mid x$. Da følger det fra Proposisjon 2.6.21 at $\mathsf{sfd}(p, x) = p$.

□

Eksempel 4.2.6. La x være 14, og la p være 3. Det er ikke sant at $3 \mid 14$. Da fastslår Korollar 4.2.5 at $\mathsf{sfd}(3, 14) = 1$, som riktignok er sant.

Eksempel 4.2.7. La x være 18, og la p være 3. Det er sant at $3 \mid 18$. Da fastslår Korollar 4.2.5 at $\mathsf{sfd}(3, 18) = 3$, som riktignok er sant.

Merknad 4.2.8. Korollar 4.2.5 er ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x = 15$ og $p = 9$, er det ikke sant at $9 \mid 15$. Imidlertid er $\mathsf{sfd}(9, 15) = 3$, altså er det ikke sant $\mathsf{sfd}(9, 15) = 1$.

Korollar 4.2.9. La p og q være primtall slik at $p \neq q$. La m og n være naturlige tall. Da er $\mathsf{sfd}(p^m, q^n) = 1$.

Bevis. Ut ifra Korollar 4.2.5 er $\mathsf{sfd}(p, q) = 1$. Ved å benytte Proposisjon 2.8.30 og Merknad 2.6.3 gjentatte ganger, følger det at $\mathsf{sfd}(p^m, q^n) = 1$. □

Eksempel 4.2.10. Korollar 4.2.9 fastslår at $\mathsf{sfd}(3^3, 5^2) = 1$, altså at $\mathsf{sfd}(27, 25) = 1$. Dette er riktignok sant.

Eksempel 4.2.11. Korollar 4.2.9 fastslår at $\mathsf{sfd}(2^6, 7^3) = 1$, altså at $\mathsf{sfd}(64, 343) = 1$. Ved å benytte Euklids algoritme, finner vi at dette riktignok er sant.

Proposisjon 4.2.12. La x og y være heltall. La p være et primtall. Anta at $p \mid xy$. Da har vi: $p \mid x$ eller $p \mid y$.

Bevis. Anta at det ikke er sant at $p \mid x$. Fra Korollar 4.2.5 følger det at $\mathsf{sfd}(p, x) = 1$. Fra Proposisjon 2.8.22 deduserer vi at $p \mid y$. □

Eksempel 4.2.13. La p være 3. Vi har: $3 \mid 48$, og $48 = 6 \cdot 8$. Proposisjon 4.2.12 fastslår at enten $3 \mid 6$ eller $3 \mid 8$. Det er riktignok sant at $3 \mid 6$.

Eksempel 4.2.14. La p være 11. Vi har: $11 \mid 66$, og $66 = 3 \cdot 33$. Proposisjon 4.2.12 fastslår at enten $11 \mid 3$ eller $11 \mid 33$. Det er riktignok sant at $11 \mid 33$.

Eksempel 4.2.15. La p være 7. Vi har: $7 \mid 294$, og $294 = 14 \cdot 21$. Proposisjon 4.2.12 fastslår at enten $7 \mid 14$ eller $7 \mid 21$. Det er riktignok sant at $7 \mid 14$, og faktisk også sant at $7 \mid 21$.

Merknad 4.2.16. Proposisjon 4.2.12 er ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x = 4$, $y = 6$, og $p = 12$, har vi: $12 \mid 24$. Imidlertid er det ikke sant at $12 \mid 4$, og heller ikke sant at $12 \mid 6$.

Merknad 4.2.17. Eksempel 4.2.15 viser at det er helt mulig at både $p \mid x$ og $p \mid y$ i Proposisjon 4.2.12.

Merknad 4.2.18. Proposisjon 4.2.12 er avgjørende. Den er kjernen til aritmetikkens fundamentalteoremet, som vi kommer til å se på snart.

Kanskje ser beviset for Proposisjon 4.2.12 lett ut, men Euklids lemma ligger bak det. Euklids lemma var langt fra lett å bevise: vi måtte studere inngående begrepet «største felles divisor» og komme fram til Korollar 2.7.6.

Korollar 4.2.19. La n være et naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq n$, la x_i være et heltall. La p være et primtall. Dersom $p \mid x_1 \cdots x_n$, finnes det et naturlig tall i slik at $1 \leq i \leq n$ og $p \mid x_i$.

Bevis. Først sjekker vi om korollaret er sant når $n = 1$. Dette er tautologisk!

Anta nå at korollaret har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq m + 1$, la x_i være et heltall. Anta at $p \mid x_1 \cdots x_{m+1}$. Vi ønsker å bevise at det finnes et naturlig tall i slik at $1 \leq i \leq m + 1$ og $p \mid x_i$.

La $x = x_1 \cdots x_m$, og la $y = x_{m+1}$. Ut ifra Proposisjon 4.2.12 er ett av følgende sant:

(1) $p \mid x$;

(2) $p \mid y$, altså $p \mid x_{m+1}$.

Anta først at (2) er sant. Da stemmer utsagnet vi ønsker å bevise, ved å la $i = m + 1$.

Anta istedenfor at (1) er sant. Ut ifra antakelsen at korollaret har blitt bevist når $n = m$, finnes det da et naturlig tall i slik at $1 \leq i \leq m$ og $p \mid x_i$. Siden $1 \leq i \leq m$, er $1 \leq i \leq m + 1$. Dermed stemmer utsagnet vi ønsker å bevise.

Således er korollaret sant når $n = m + 1$. Ved induksjon konkluderer vi at korollaret er sant for alle naturlige tall. □

Eksempel 4.2.20. Vi har: $5 \mid 180$ og $180 = 2 \cdot 15 \cdot 6$. Korollar 4.2.19 fastslår at et av følgende er sant: $5 \mid 2$, $5 \mid 15$, $5 \mid 6$. Det er riktignok sant at $5 \mid 15$.

Eksempel 4.2.21. Vi har: $3 \mid 540$ og $540 = 6 \cdot 10 \cdot 9$. Korollar 4.2.19 fastslår at et av følgende er sant: $3 \mid 6$, $3 \mid 10$, $3 \mid 9$. Det er riktignok sant at $3 \mid 6$, og faktisk også sant at $3 \mid 9$.

Merknad 4.2.22. Korollar 4.2.19 er ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x_1 = 8$, $x_2 = 9$, $x_3 = 11$, og $p = 6$, har vi: $6 \mid 792$. Imidlertid er ikke noe av følgende sant: $6 \mid 8$, $6 \mid 9$, eller $6 \mid 11$.

Korollar 4.2.23. La n være et naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq n$, la p_i være et primtall. La p være et primtall. Dersom $p \mid p_1 \cdots p_n$, finnes det et naturlig tall i slik at $1 \leq i \leq n$ og $p = p_i$.

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Korollar 4.2.19 finnes det et naturlig tall i slik at $1 \leq i \leq n$ og $p \mid p_i$.

(2) Siden p_i er et primtall, er 1 og p_i de eneste divisorene til p_i.

Det følger fra (1) og (2) at enten $p = 1$ eller $p = p_i$. Siden p er et primtall, er $p \geq 2$. Vi konkluderer at $p = p_i$.

□

Eksempel 4.2.24. Vi har: $30 = 2 \cdot 3 \cdot 5$. Dersom p er et primtall og $p \mid 30$, fastslår Korollar 4.2.23 at p er lik ett av 2, 3, eller 5.

Eksempel 4.2.25. Vi har: $441 = 3 \cdot 3 \cdot 7 \cdot 7$. Dersom p er et primtall og $p \mid 441$, fastslår Korollar 4.2.23 at p er lik enten 3 eller 7.

Merknad 4.2.26. Korollar 4.2.23 er ikke sant om vi ikke antar at p_i er et primtall for hvert naturlig tall i slik at $1 \leq i \leq n$. Hvis for eksempel $x_1 = 7$, $x_2 = 15$, og $p = 5$, har vi: $7 \cdot 15 = 105$ og $5 \mid 105$. Imidlertid er verken $5 = 7$ eller $5 = 15$.

Merknad 4.2.27. Korollar 4.2.23 er heller ikke sant om vi ikke antar at p er et primtall. Hvis for eksempel $x_1 = 3$, $x_2 = 23$, $x_3 = 5$, og $p = 15$, har vi: $3 \cdot 23 \cdot 5 = 345$ og $15 \mid 345$. Imidlertid er ikke noe av følgende sant: $15 = 3$, $15 = 23$, eller $15 = 5$.

Proposisjon 4.2.28. La p være et primtall. La a og c være heltall. Anta at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da her kongruensen

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

en løsning, og alle løsningene til denne kongruensen er kongruent til hverandre modulo p.

Bevis. Siden det ikke er sant at $a \equiv 0 \pmod{p}$, følger det fra Proposisjon 3.2.13 at det ikke er sant at $p \mid a$. Siden p er et primtall, følger det fra Korollar 4.2.5 at $\mathsf{sfd}(a, p) = 1$. Da følger utsagnet fra Korollar 3.4.39. □

Eksempel 4.2.29. Siden 7 er et primtall og det ikke er sant at

$$4 \equiv 0 \pmod{7},$$

fastslår Proposisjon 4.2.28 at kongruensen

$$4x \equiv 6 \pmod{7}$$

har en løsning. Dette er riktignok sant: $x = 5$ er en løsning. Proposisjon 4.2.28 fastslår i tillegg at enhver annen løsning til kongruensen er kongruent til 5 modulo 7.

Eksempel 4.2.30. Siden 37 er et primtall og det ikke er sant at

$$12 \equiv 0 \pmod{37},$$

fastslår Proposisjon 4.2.28 at kongruensen

$$12x \equiv 28 \pmod{37}$$

har en løsning. Dette er riktignok sant: $x = 27$ er en løsning. Proposisjon 4.2.28 fastslår i tillegg at enhver annen løsning til kongruensen er kongruent til 27 modulo 37.

Proposisjon 4.2.31. La p være et primtall slik at $p > 2$. Da finnes det et naturlig tall k slik at $p - 1 = 2k$.

Bevis. Ut ifra Proposisjon 3.2.1 er ett av følgende utsagn sant:

(A) $p \equiv 0 \pmod{2}$;

(B) $p \equiv 1 \pmod{2}$.

Anta først at (A) er sant. Da har vi: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste divisorene til p. Vi deduserer at $p = 2$. Imidlertid har vi antatt at $p > 2$. Siden antakelsen at (A) er sant fører til motsigelsen at både $p = 2$ og $p > 2$, konkluderer vi at (A) ikke er sant.

Derfor er (B) sant. Da følger det fra Korollar 3.2.39 at

$$p - 1 \equiv 0 \pmod 2,$$

altså

$$2 \mid p - 1.$$

Dermed finnes det et heltall k slik at $p - 1 = 2k$. Siden både 2 og $p - 1$ er naturlige tall, er k et naturlig tall. □

Eksempel 4.2.32. Siden 11 er et primtall og $11 > 2$, fastslår Proposisjon 4.2.31 at det finnes et naturlig tall k slik at $10 = 2k$. Dette er riktignok sant: vi kan la k være 5.

Eksempel 4.2.33. Siden 23 er et primtall og $23 > 2$, fastslår Proposisjon 4.2.31 at det finnes et naturlig tall k slik at $22 = 2k$. Dette er riktignok sant: vi kan la k være 11.

4.3 Aritmetikkens fundamentalteorem I

Merknad 4.3.1. Målet vårt i denne delen av kapittelet er å gi et bevis for Teorem 4.3.3. For å gjøre dette, må vi først endre påstanden i Teorem 4.3.3, for å kunne gjennomføre et bevis ved induksjon. Vi gjorde noe lignende da vi ga et bevis for Korollar 2.7.6 og et bevis for Korollar 2.10.20: se Merknad 2.7.4 og Merknad 2.10.18.

Proposisjon 4.3.2. La n være et naturlig tall slik at $n \geq 2$. La l være et naturlig tall slik at $2 \leq l \leq n$. Da finnes det et naturlig tall t og, for hvert naturlig tall i slik at $i \leq t$, et primtall p_i, slik at $l = p_1 p_2 \cdots p_t$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 2$. Da er $l = 2$, og utsagnet er: det finnes et naturlig tall t og, for hvert naturlig tall i slik at $i \leq t$, et primtall p_i, slik at

$$2 = p_1 p_2 \cdots p_t.$$

Siden 2 er et primtall, er dette sant: vi lar $t = 1$, og lar $p_1 = 2$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall slik at $m \geq 2$. La l være et naturlig tall slik at $2 \leq l \leq m + 1$. Vi ønsker å bevise at det finnes et naturlig tall t og primtall p_i, for hvert naturlig tall i slik at $i \leq t$, slik at $l = p_1 p_2 \cdots p_t$.

Ut ifra definisjonen til et primtall, er ett av følgende sant:

(1) l er et primtall;

(2) det finnes et naturlig tall a slik at $1 < a < l$ og $a \mid l$.

Anta først at (1) er sant. Da rekker vi målet ved å la t være 1 og p_1 være l.

Anta istedenfor at (2) er sant. Da finnes det et naturlig tall k slik at $1 < k < l$ og $l = a \cdot k$. Vi gjør følgende observasjoner.

(1) Siden $l \leq m + 1$ og $a < l$, er $a < m + 1$, altså $a \leq m$.

(2) Siden $l \leq m+1$ og $k < l$, er $k < m+1$, altså $k \leq m$.

(3) Ut ifra antakelsen at proposisjonen er sann når $n = m$, følger det fra (1) at det finnes et naturlig tall s og primtall q_i, for hvert naturlig tall i slik at $i \leq s$, slik at $a = q_1 q_2 \cdots q_s$.

(4) Ut ifra antakelsen at proposisjonen er sann når $n = m$, følger det fra (2) at det finnes et naturlig tall s' og primtall q'_i, for hvert naturlig tall i slik at $i \leq s'$, slik at $k = q'_1 q'_2 \cdots q'_{s'}$.

(5) Det følger fra (4) at:

$$\begin{aligned} n &= ak \\ &= (q_1 \dots q_s)\left(q'_1 \cdots q'_{s'}\right) \\ &= q_1 \dots q_s q'_1 \dots q'_{s'}. \end{aligned}$$

Derfor rekker vi målet ved å la $t = s + s'$ og

$$p_i = \begin{cases} q_i & \text{if } 1 \leq i \leq s, \\ q'_{i-s} & \text{if } s+1 \leq i \leq t. \end{cases}$$

Dermed er proposisjonen sann når $n = m+1$. Ved induksjon konkluderer vi at den er sann for alle de naturlige tallene n slik at $n \geq 2$.

□

Teorem 4.3.3. La n være et naturlig tall slik at $n \geq 2$. Da finnes det et naturlig tall t og primtall p_i, for hvert naturlig tall i slik at $i \leq t$, slik at $n = p_1 p_2 \cdots p_t$.

Bevis. Følger umiddelbart fra Proposisjon 4.3.3 ved å la $l = n$. □

Terminologi 4.3.4. Teorem 4.3.3 og Teorem 4.7.2 kalles *aritmetikkens fundamentalteorem.*

Merknad 4.3.5. Aritmetikkens fundamentalteorem er ett av de vikigste teoremene i hele matematikken. Det er spesielt viktig i tallteori og algebra, og andre deler av matematikk som bygger på disse to, men det dukker opp overalt: til og med i knuteteori!

Eksempel 4.3.6. La n være 24. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \dots, p_t$ slik at $24 = p_1 \cdots p_t$. Det er riktignok sant at

$$24 = 2 \cdot 2 \cdot 2 \cdot 4.$$

Her er $t = 4$, $p_1 = p_2 = p_3 = 2$, og $p_4 = 3$.

Eksempel 4.3.7. La n være 63. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \dots, p_t$ slik at $63 = p_1 \cdots p_t$. Det er riktignok sant at

$$63 = 3 \cdot 3 \cdot 7.$$

Her er $t = 3$, $p_1 = p_2 = 3$, og $p_3 = 7$.

Eksempel 4.3.8. La n være 143. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at $143 = p_1 \cdots p_t$. Det er riktignok sant at

$$143 = 11 \cdot 13.$$

Her er $t = 2$, $p_1 = 11$, og $p_2 = 13$.

Eksempel 4.3.9. La n være 125. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at $125 = p_1 \cdots p_t$. Det er riktignok sant at

$$125 = 5 \cdot 5 \cdot 5.$$

Her er $t = 3$, og $p_1 = p_2 = p_3 = 5$.

Eksempel 4.3.10. La n være 7623. Teorem 4.3.3 fastslår at det finnes et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at $7623 = p_1 \cdots p_t$. Det er riktignok sant at

$$7623 = 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11.$$

Her er $t = 5$, $p_1 = p_2 = 3$, $p_3 = 7$, og $p_4 = p_5 = 11$.

Terminologi 4.3.11. La n være et naturlig tall slik at $n \geq 2$. La t være et naturlig tall. For hvert naturlig tall i slik at $1 \leq i \leq t$, la p_i være et primtall. Anta at

$$n = p_1 \cdots p_t.$$

Vi sier at produktet $p_1 \cdots p_n$ er en *primtallsfaktorisering* av n.

Merknad 4.3.12. Ved å benytte denne terminologien, fastslår Teorem 4.3.3 at hvert naturlig tall har en primtallsfakorisering.

Merknad 4.3.13. Idéen bak beviset for Proposisjon 4.3.2, og dermed beviset for Teorem 4.3.3, er ganske enkel, og fører til en fin metode for å finne en primtallsfaktorisering til et naturlig tall i praksis. For å forklare dette, la oss se igjen på Eksempel 4.3.6.

(1) Vi kan begynne med å observere at $24 = 2 \cdot 12$. Siden 12 er ikke er primtall, har vi ikke rukket en primtallsfaktorisering av 24 ennå.

(2) Vi observerer at $12 = 2 \cdot 6$. Derfor er

$$24 = 2 \cdot 2 \cdot 6.$$

Siden 6 er ikke er primtall, har vi fremdeles rukket en primtallsfaktorisering av 24..

(3) Vi observerer at $6 = 2 \cdot 3$. Derfor er

$$24 = 2 \cdot 2 \cdot 2 \cdot 3.$$

Både 2 og 3 er primtall. Dermed har vi rukket en primtallsfaktorisering av 24: vi kan la t være 4, p_1 være 2, p_2 være 2, p_3 være 2, og p_4 være 3.

Dette er ikke det eneste gyldige argumentet. Istedenfor kan vi gjør følgende.

(1) Begynn med å observere at $24 = 6 \cdot 4$. Siden 6 og 4 ikke er primtall, har vi ikke rukket en primtallsfaktorisering av 24 ennå.

(2) Observer at $6 = 2 \cdot 3$ og at $4 = 2 \cdot 2$. Derfor er

$$24 = 2 \cdot 3 \cdot 2 \cdot 3.$$

Både 2 og 3 er primtall. Dermed har vi rukket en primtallsfaktorisering av 24: vi kan la t være 4, p_1 være 2, p_2 være 3, p_3 være 2, og p_4 være 3.

La merke til at primtallene $p_1, \ldots, p_t$ er de samme som vi fikk tidligere. Det er kun rekkefølgene som er annerledes.

Det er dessuten mulig å begynne med å observere at

$$24 = 8 \cdot 3.$$

Da kan vi fortsette som ovenfor.

La oss oppsummere.

(1) Siden 24 ikke er et primtall, finnes det minst ett par naturlige tall a og k slik at $24 = ak$, $1 < a < 24$, og $1 < k < 24$. For å finne en primtallsfakorisering av 24, er det nok å finne en primtallsfaktorisering av a og en primtallsfaktorisering av b.

(2) Hvis både a og b er primtall, har vi rukket målet. Ellers kan vi uttrykke a eller b, eller begge to, som et produkt av naturlige tall som er større enn 1. Det er nok å finne en primtallsfaktorisering av disse naturlige tallene.

(3) Slik fortsetter vi.

Uansett hvilket produkt $24 = ab$ vi begynner med, viser det seg at vi får den samme primstallsfaktoriseringen til 24, bortsett fra rekkefølgen av primtallene. Den andre delen av aritmetikkens fundamentalteorem, som vi kommer til å gi et bevis for senere, fastslår at dette er tilfellet for et hvilket som helst naturlig tall, ikke kun 24.

Eksempel 4.3.14. La oss gjennomføre metoden i Merknad 4.3.13 for å finne en primtallsfaktorisering til 600. For eksempel kan vi regne som følger:

$$\begin{aligned} 600 &= 50 \cdot 12 \\ &= (10 \cdot 5) \cdot (2 \cdot 6) \\ &= 10 \cdot 5 \cdot 2 \cdot 6 \\ &= (5 \cdot 2) \cdot 5 \cdot 2 \cdot (2 \cdot 3) \\ &= 5 \cdot 2 \cdot 5 \cdot 2 \cdot 2 \cdot 3. \end{aligned}$$

Dermed er

$$5 \cdot 2 \cdot 5 \cdot 2 \cdot 2 \cdot 3$$

en primtallsfaktorisering av 600. Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, får vi

$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5.$$

Vi kan gjennomføre metoden i Merknad 4.3.13 på mange andre måter. For eksempel kan vi regne som følger:

$$\begin{aligned} 600 &= 6 \cdot 100 \\ &= (3 \cdot 2) \cdot (10 \cdot 10) \\ &= 3 \cdot 2 \cdot 10 \cdot 10 \\ &= 3 \cdot 2 \cdot (2 \cdot 5) \cdot (5 \cdot 2) \\ &= 3 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 2. \end{aligned}$$

Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, ser vi at vi har rukket den samme primtallsfaktoriseringen som ovenfor, nemlig

$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5.$$

Eksempel 4.3.15. La oss gjennomføre metoden i Merknad 4.3.13 for å finne en primtallsfaktorisering til 126. Vi kan regne som følger:

$$\begin{aligned} 126 &= 2 \cdot 63 \\ &= 2 \cdot (9 \cdot 7) \\ &= 2 \cdot 9 \cdot 7 \\ &= 2 \cdot (3 \cdot 3) \cdot 7 \\ &= 2 \cdot 3 \cdot 3 \cdot 7 \end{aligned}$$

Dermed er

$$2 \cdot 3 \cdot 3 \cdot 7$$

en primtallsfaktorisering av 126.

Alternativt kan vi for eksempel regne som følger:

$$\begin{aligned} 126 &= 3 \cdot 42 \\ &= 3 \cdot (21 \cdot 2) \\ &= 3 \cdot 21 \cdot 2 \\ &= 3 \cdot (7 \cdot 3) \cdot 2 \\ &= 3 \cdot 7 \cdot 3 \cdot 2. \end{aligned}$$

Dermed er

$$3 \cdot 7 \cdot 3 \cdot 2$$

en primtallsfaktorisering av 126. Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, ser vi at vi har rukket den sammen primtallsfaktoriseringen som ovenfor, nemlig

$$2 \cdot 3 \cdot 3 \cdot 7.$$

For å gjennomføre metoden i Merknad 4.3.13, må vi finne først et naturlig tall som deler 126. I praksis er det sannsynlig at vi hadde først lagt merke til at $2 \mid 126$, og deretter regnet som ovenfor, ved å begynne med produktet

$$126 = 2 \cdot 63.$$

Likevel er alle andre måter å gjennomføre metoden i Merknad 4.3.13 like verdifulle. For eksempel er det usannsynlig at vi først kommer fram til produktet

$$126 = 14 \cdot 9,$$

men om det er tilfellet, kan vi godt regne som følger:

$$\begin{aligned} 126 &= 14 \cdot 9 \\ &= (7 \cdot 2) \cdot (3 \cdot 3) \\ &= 7 \cdot 2 \cdot 3 \cdot 3. \end{aligned}$$

Dermed er

$$7 \cdot 2 \cdot 2 \cdot 3$$

en primtallsfaktorisering av 126. Ved å endre rekkefølgen av primtallene i denne faktoriseringen litt, ser vi at vi har rukket den sammen primtallsfaktoriseringen som ovenfor, nemlig

$$2 \cdot 3 \cdot 3 \cdot 7.$$

Korollar 4.3.16. La n være et naturlig tall. Da finnes det et naturlig tall t, primtall $p_1, p_2, \ldots, p_t$, og naturlige tall $k_1, k_2, \ldots, k_t$ slik at

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_t^{k_t},$$

og slik at $p_i \neq p_j$ om $i \neq j$.

Bevis. Ut ifra Teorem 4.3.3, finnes det et naturlig tall s og primtall $q_1, q_2, \ldots, q_s$ slik at

$$n = q_1 \cdots q_s.$$

La $p_1, p_2, \ldots, p_t$ være de primtallene blant $q_1, q_2, \ldots, q_s$ som forblir etter å ha hevde alle repetisjoner. Da er $q_i \neq q_j$ dersom $i \neq j$.

For hvert naturlig tall i slik at $i \leq t$, la k_i være antall primtall blant $q_1, q_2, \ldots, q_s$ som er like p_i, altså antall ledd i produktet $q_1 \cdots q_s$ som er like p_i. Ved å bytte om rekkefølgen av primtallene i produktet, er da

$$n = \underbrace{p_1 p_1 \cdots p_1}_{k_1 \text{ ganger}} \cdot \underbrace{p_2 p_2 \cdots p_2}_{k_2 \text{ ganger}} \cdots \underbrace{p_s p_s \cdots p_s}_{k_s \text{ ganger}}.$$

Dermed er

$$n = p_1^{k_1} \cdots p_t^{k_t}.$$

□

Eksempel 4.3.17. Ut ifra Eksempel 4.3.14 er $2^3 \cdot 3 \cdot 5^2$ en primtallsfaktorisering til 600.

Eksempel 4.3.18. Ut ifra Eksempel 4.3.15 er $2 \cdot 3^2 \cdot 7$ en primtallsfaktorisering til 126.

Korollar 4.3.19. La n være et naturlig tall slik at $n > 1$. Da finnes det et primtall p slik at $p \mid n$.

Bevis. Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $p_1, p_2, \ldots, p_t$ slik at

$$n = p_1 \cdots p_t.$$

Dersom $t = 1$, er n et primtall. Siden $n \mid n$, er korollaret i dette tilfellet.
Dersom $t > 1$, er

$$n = (p_1 \cdots p_{t-1}) \cdot p_t,$$

altså $p_t \mid n$. □

Merknad 4.3.20. Et hvilket som helst av primtallene $p_1, p_2, \ldots, p_t$ kan benyttes istedenfor p_t i beviset for Korollary 4.3.19.

Eksempel 4.3.21. Korollar 4.3.19 fastslår at det naturlige tallet 231 er delelig med et primtall. Siden $231 = 21 \cdot 11$, har vi riktignok: $11 \mid 231$.

Eksempel 4.3.22. Korollar 4.3.19 fastslår at det naturlige tallet 24843 er delelig med et primtall. Siden $24843 = 1911 \cdot 13$, har vi riktignok: $13 \mid 24843$.

4.4 Det finnes uendelig mange primtall

Merknad 4.4.1. Ved hjelp av aritmetikkens fundamentalteorem kan vi nå bevise et teorem går helt tilbake til Antikkens Hellas, og er ett av de meste berømte teoremene i hele matematikken.

Teorem 4.4.2. La n være et naturlig tall. Da finnes det et primtall p slik at $p > n$.

Bevis. La q være produktet av alle primtallene som er mindre enn eller like n. Ut ifra Teorem 4.3.3, finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$q + 1 = p_1 \cdots p_t.$$

Anta at $p_1 \leq n$. Vi gjør følgende observasjoner.

(1) Ut ifra definisjonen til q og antakelsen at $p_1 \leq n$, følger det at $p_1 \mid q$.

(2) Siden

$$q + 1 = p_1 \cdot (p_2 \cdots p_t),$$

har vi: $p_1 \mid q + 1$.

(3) Det følger fra (1) og Proposisjon 2.5.12 at $p_1 \mid -q$.

(4) Det følger fra (2), (3), og Proposisjon 2.5.24 at $p_1 \mid (q+1) - q$, altså at $p_1 \mid 1$.

Siden p_1 er et primtall, er $p_1 \geq 2$. Det kan ikke være sant at både $p_1 \mid 1$ og $p_1 \geq 2$. Siden antakelsen at $p_1 \leq n$ fører til denne motsigelsen, deduserer vi at det ikke er sant at $p_1 \leq n$. Derfor er $p_1 > n$.

□

Merknad 4.4.3. Det er ikke noe spesielt med p_1 i beviset for Teorem 4.4.2. Det samme argumentet viser at $p_i > n$ for alle primtallene p_1, p_2, …, p_t som dukker opp i primtallsfaktorisingen til $q+1$ i beviset.

Merknad 4.4.4. Teorem 4.4.2 fastslår at det finnes uendelig mange primtall: uansett hvor stort et naturlig tall er, kan vi alltid finne et større primtall.

Eksempel 4.4.5. La oss gå gjennom beviset for Teorem 4.4.2 når $n = 14$. Det finnes seks primtall som er mindre enn eller likt 14, nemlig 2, 3, 5, 7, 11, og 13. La q være produktet av disse primtallene, altså

$$q = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13.$$

Dette produktet er likt 30030. Beviset for Teorem 4.4.2 fastslår at hvert primtall i en primtallsfaktorisering av $q+1$, altså av 30031, er større enn 14. Vi har:

$$30031 = 59 \cdot 509,$$

og både 59 og 509 er primtall. Med andre ord, er primtallet p_1 i beviset for Teorem 4.4.2 likt 59 i dette tilfellet: det er riktignok at $59 > 14$.

Merknad 4.4.6. Ofte er beviset for Teorem 4.4.2 misforstått: det fastslår *ikke* at $q+1$ er et primtall som er større enn n, hvor q er produktet av de primtallene som er mindre enn eller likt n. Det er sant at $q+1 > n$, men det er *ikke* nødvendigvis sant at $q+1$ er et primtall. Som vi så i Eksempel 4.4.5, er $q+1$ ikke et primtall når $n = 14$. Med andre ord, er

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1$$

ikke et primtall: det er delelig med 59 og med 509.

Som vi har sett, fastslår Teorem 4.4.2 heller at hvert primtall i en primtallsfaktorisering av $q+1$ er større enn n.

Eksempel 4.4.7. Noen ganger er imidlertid $q+1$ selv et primtall. La oss gå for eksempel gjennom beviset for Teorem 4.4.2 når $n = 8$. Det finnes fire primtall som er mindre enn eller likt 8, nemlig 2, 3, 5, og 7. La q være produktet av disse primtallene, altså

$$q = 2 \cdot 3 \cdot 5 \cdot 7.$$

Dette produktet er lik 210. Beviset for Teorem 4.4.2 fastslår at hvert primtallene i en primtallsfaktorisering av $q+1$, altså av 211, er større enn 8. Faktisk er 211 et primtall, og derfor er 211 selv en primtallsfaktorisering, med ett ledd i produktet, av 211. Med andre ord, er primtallet p_1 i beviset for Teorem 4.4.2 lik 211 i dette tilfellet: det er riktignok at $211 > 8$.

Merknad 4.4.8. Argumentet bak beviset for Teorem 4.4.2 kan tilpasses for å bevise at andre lignende påstander sanne. La oss se på et eksempel.

Proposisjon 4.4.9. La n være et heltall slik at $n \geq 0$. Da finnes det et primtall p slik at $p \equiv 3 \pmod 4$ og $p > n$.

Bevis. La q være produktet av alle primtallene som er mindre enn eller like n, og som er kongruent til 3 modulo 4. Ut ifra Teorem 4.3.3 finnes det et naturlig tall t og primtall $p_1, \ldots, p_t$ slik at

$$4q - 1 = p_1 \cdots p_t.$$

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

(1) $p_i \equiv 0 \pmod 4$;

(2) $p_i \equiv 1 \pmod 4$;

(3) $p_i \equiv 2 \pmod 4$;

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

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

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 4,$$

altså at

$$4q - 1 \equiv 0 \pmod 4.$$

Imidlertid er

$$4q - 1 \equiv 3 \pmod 4.$$

Siden $0 \neq 3$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$4q - 1 \equiv 0 \pmod 4$$

og

$$4q - 1 \equiv 3 \pmod 4.$$

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

Anta nå at (3) er sant for et naturlig tall $i \leq t$. Siden $2 \mid 4$, følger det da fra Proposisjon 3.2.54 at $p_i \equiv 0 \pmod 2$. Da følger det fra Korollar 3.2.45 at

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

altså at

$$4q - 1 \equiv 0 \pmod 2.$$

Imidlertid er

$$4q - 1 \equiv 1 \pmod 2.$$

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

$$4q - 1 \equiv 0 \pmod{2}$$

og

$$4q - 1 \equiv 1 \pmod{4}.$$

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

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

$$p_1 \cdots p_t \equiv 1^t \pmod{4},$$

altså at

$$4q - 1 \equiv 1 \pmod{4}.$$

Imidlertid er

$$4q - 1 \equiv 3 \pmod{4}.$$

Siden $1 \neq 3$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$4q - 1 \equiv 1 \pmod{4}$$

og

$$4q - 1 \equiv 3 \pmod{4}.$$

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

Derfor finnes det et naturlig tall i, hvor $i \leq t$, slik at (4) er sant, altså at $p_i \equiv 3 \pmod{4}$. Anta at $p_i \leq n$. Vi gjør følgende observasjoner.

(1) Siden $p_i \equiv 3 \pmod{4}$, følger det fra definisjonen til q og antakelsen at $p_i \leq n$ at $p_i \mid q$.

(2) Siden

$$4q - 1 = p_i \cdot (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t),$$

har vi: $p_i \mid 4q - 1$.

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

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

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

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

□

Merknad 4.4.10. De første 10 primtallene som er kongruent til 3 modulo 4 er: 3, 7, 11, 19, 23, 31, 43, 47, 59, og 67. Proposisjon 4.4.9 fastslår at det finnes uendelig mange slike primtall: uansett hvor stort et naturlig tall er, finnes det alltid et primtall kongruent til 3 modulo 4 som er større.

Merknad 4.4.11. Beviset for Proposisjon 4.4.9 gir oss en metode for å finne et primtall kongruent til 3 modulo 4 som er større enn et bestemt naturlig tall n: ett av primtallene i en primtallsfaktorisering av $4q - 1$ er et primtall kongruent til 3 modulo 4, hvor q er produktet av alle de primtallene mindre enn eller likt n som er kongruent til 3 modulo 4.

Eksempel 4.4.12. La n være 22. Primtallene som er mindre enn eller likt 22, og som er kongruent til 3 modulo 4, er 3, 7, 11, og 19. La $q = 3 \cdot 7 \cdot 11 \cdot 19$, altså $q = 4389$. Da er $4q - 1 = 17555$. En primtallsfakorisering av 17555 er $5 \cdot 3511$. Beviset for Proposisjon 4.4.9 fastslår at enten 5 eller 3511 er større enn 22 og kongruent til 3 modulo 4. Det er riktignok sant at $3511 > 22$ og $3511 \equiv 3 \pmod 4$.

4.5 Eksempler på bevis for utsagn om primtall hvor kongruenser benyttes

Merknad 4.5.1. I §2.4 av Kapittel 2, så vi at vi kan benytte divisjonsalgoritmen for å dele i tilfeller et bevis for et utsagn om heltallene. I denne delen av kapittelet skal vi se på et par eksempler hvor vi benytter den samme tilnærmingsmetoden, men hvor vi benytter kongruenser istedenfor å benytte divisjonsalgoritmen direkte. Da blir tilnærmingsmetoden mer elegant, og fortere å gjennomføre. I tillegg skal vi se på hvordan en antakelse om primtall kan benyttes når vi gjennomføre et slikt bevis.

Proposisjon 4.5.2. La n være et heltall slik at $n \geq 0$. Da finnes det et heltall $m \geq 0$ slik at $3m + 2$ er et primtall, og $3m + 2 \mid 3n + 2$.

Bevis. Ut ifra Teorem 4.3.3 finnes det et naturlig tall t og, for hvert naturlig tall i slik at $i \leq t$, et primtall p_i, slik at

$$3n + 2 = p_1 \cdots p_t.$$

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

(A) $p_i \equiv 0 \pmod 3$;

(B) $p_i \equiv 1 \pmod 3$;

(C) $p_i \equiv 2 \pmod 3$.

Vi skal gjennomføre beviset i hvert tilfelle hvert for seg.

Anta først at (A) er sant for et naturlig tall i slik at $i \leq t$. Fra Korollar 3.2.45, har vi da:

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv (p_1 \cdots p_{i-1}) \cdot 0 \cdot (p_{i+1} \cdots p_t) \pmod 3,$$

altså

$$(p_1 \cdots p_{i-1}) \cdot p_i \cdot (p_{i+1} \cdots p_t) \equiv 0 \pmod 3.$$

Dermed er

$$3n + 2 \equiv 0 \pmod 3.$$

Imidlertid er

$$3n + 2 \equiv 2 \pmod 3.$$

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

$$3n + 2 \equiv 0 \pmod 3$$

og

$$3n + 2 \equiv 2 \pmod 3.$$

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

Anta nå at (B) er sant for alle de naturlige tallene $i \leq t$. Fra Proposisjon 3.2.42 har vi da:

$$p_1 \cdots p_n \equiv 1^i \pmod 3,$$

altså

$$3n + 2 \equiv 1 \pmod 3.$$

Imidlertid er

$$3n + 2 \equiv 2 \pmod 3.$$

Siden $1 \neq 2$, følger det fra Proposisjon 3.2.11 at det ikke kan være sant at både

$$3n + 2 \equiv 1 \pmod 3$$

og

$$3n + 2 \equiv 2 \pmod 3.$$

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

Derfor finnes det et naturlig tall i, hvor $i \leq t$, slik at (C) er sant, altså at

$$p_i \equiv 2 \pmod 3.$$

Ut ifra definisjonen til denne kongruensen, har vi da: $3 \mid p_i - 2$. Dermed finnes det et heltall m slik at $m \geq 0$ og $p_i = 3m + 2$. Siden

$$3n + 2 = p_i \cdot (p_1 \cdots p_{i-1} p_{i+1} \cdots p_t),$$

har vi i tillegg:

$$p_i \mid 3n + 2.$$

Således er $3m + 2$ et primtall som deler $3n + 2$.

□

Merknad 4.5.3. Med andre ord, fastslår Proposisjon 4.5.2 at hvert naturlig tall som er lik $3n + 2$ for noen heltall $n \geq 0$, er delelig med et primtall som er lik $3m + 2$ for noen heltall $m \geq 0$.

Eksempel 4.5.4. Siden $119 = 3 \cdot 39 + 2$, fastslår Proposisjon 4.5.2 at det finnes et primtall som både deler 119 og er lik $3m + 2$ for noen heltall $m \geq 0$. Riktignok har vi:

(1) $17 \mid 119$;

(2) 17 er et primtall;

(3) $17 = 3 \cdot 5 + 2$.

Med andre ord, kan vi la $m = 5$.

Eksempel 4.5.5. Siden $32 = 3 \cdot 10 + 2$, fastslår Proposisjon 4.5.2 at det finnes et primtall som både deler 32 og er lik $3m + 2$ for noen heltall $m \geq 0$. Riktignok har vi:

(1) $2 \mid 32$;

(2) 2 er et primtall;

(3) $2 = 3 \cdot 0 + 2$.

Med andre ord, kan vi la $m = 0$.

Eksempel 4.5.6. Siden $47 = 3 \cdot 15 + 2$, fastslår Proposisjon 4.5.2 at det finnes et primtall som både deler 47 og er lik $3m + 2$ for noen heltall $m \geq 0$. Faktisk er 47 selv et primtall: vi kan la $m = 15$.

Proposisjon 4.5.7. La p være et primtall slik at $p \geq 5$. Da er $p^2 + 2$ delelig med 3.

Bevis. Ut ifra Proposisjon 3.2.1 er ett av følgende sant:

(A) $p \equiv 0 \pmod 6$;

(B) $p \equiv 1 \pmod 6$;

(C) $p \equiv 2 \pmod 6$;

(D) $p \equiv 3 \pmod 6$;

(E) $p \equiv 4 \pmod 6$;

(F) $p \equiv 5 \pmod 6$.

Anta først at (A) er sant. Fra Proposisjon 3.2.13 har vi da: $6 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 6$. Imidlertid er 6 ikke et primtall. Siden antakelsen at (A) er sant fører til motsigelsen at p både er og er ikke et primtall, konkluderer vi at (A) ikke er sant.

Anta nå at (C) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod 2$. Fra Proposisjon 3.2.13 følger det at: $2 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 2$. Imidlertid er $2 < 5$. Siden antakelsen at (C) er sant fører til motsigelsen at både $p \geq 5$ og $p < 5$, konkluderer vi at (C) ikke er sant.

Anta nå at (D) er sant. Ut ifra Proposisjon 3.2.54 er da $p \equiv 0 \pmod 3$. Fra Proposisjon 3.2.13 følger det at: $3 \mid p$. Siden p er et primtall, er 1 og p de eneste naturlige tallene som deler p. Derfor er $p = 3$. Imidlertid er $3 < 5$. Siden antakelsen at (D) er sant fører til motsigelsen at både $p \geq 5$ og $p < 5$, konkluderer vi at (D) ikke er sant.

Anta nå at (E) er sant. Vi har: $4 \equiv -2 \pmod 6$. Ut ifra Proposisjon 3.2.33 er da

$$p \equiv -2 \pmod 6.$$

Fra Proposisjon 3.2.54 følger det at $p \equiv 0 \pmod{-2}$. Fra Korollar 3.2.22 deduserer vi at $p \equiv 0 \pmod 2$. Ut ifra Proposisjon 3.2.13 har vi da: $2 \mid p$. Som i tilfellet hvor vi antok at (C) var sant, konkluderer vi at (E) ikke er sant.

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

$$p^2 \equiv 1^2 \pmod 6,$$

altså at

$$p^2 \equiv 1 \pmod 6.$$

Da følger det fra Korollar 3.2.39 at

$$p^2 + 2 \equiv 1 + 2 \pmod 6,$$

altså at

$$p^2 + 2 \equiv 3 \pmod 6.$$

Ut ifra Proposisjon 3.2.54 er da

$$p^2 + 2 \equiv 0 \mod 3.$$

Fra Proposisjon 3.2.13 har vi da: $3 \mid p^2 + 2$.

Anta nå at (F) er sant. Vi har: $5 \equiv -1 \pmod 6$. Ut ifra Proposisjon 3.2.33 er da

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

Fra Proposisjon 3.2.48 følger det at

$$p^2 \equiv (-1)^2 \pmod 6,$$

altså at

$$p^2 \equiv 1 \pmod 6.$$

Som i tilfellet hvor vi antok at (B) var sant, følger det at: $3 \mid p^2 + 2$.

□

Merknad 4.5.8. Det følger fra Proposisjon 4.5.7 at, dersom $p \geq 5$ er et primtall, er $p^2 + 2$ ikke et primtall.

Eksempel 4.5.9. La $p = 11$. Proposisjon 4.5.7 fastslår at $11^2 + 2$, altså 123, er delelig med 3. Dette er riktignok sant: $123 = 41 \cdot 3$.

Eksempel 4.5.10. La $p = 17$. Proposisjon 4.5.7 fastslår at $17^2 + 2$, altså 291, er delelig med 3. Dette er riktignok sant: $291 = 97 \cdot 3$.

4.6 Primtallsfaktoriseringer og største felles divisor

Proposisjon 4.6.1. La n og n' være naturlige tall. Anta at

$$n = p_1 \cdots p_t,$$

hvor t er et naturlig tall og, for hvert naturlig tall i slik at $i \leq t$, p_i er et primtall. Anta dessuten at

$$n' = p'_1 \cdots p'_{t'},$$

hvor t' er et naturlig tall og, for hvert naturlig tall i' slik at $i' \leq t'$, $p_{i'}$ er et primtall. La q_1, q_2, …, q_s være alle primtallene slik at, for hvert naturlig tall j slik at $j \leq s$, finnes det naturlige tall i og i' slik at $q_j = p_i$ og $q_j = p'_i$, hvor $i \leq t$ og $i' \leq t'$. Da er

$$\mathsf{sfd}(n, n') = q_1 \cdots q_s.$$

Bevis. La k være produktet av alle primtallene blant p_1, …, p_t som ikke er like q_j for noen naturlig tall j slik at $j \leq s$. Da er

$$n = k \cdot (q_1 \cdots q_s),$$

altså

$$q_1 \cdots q_s \mid n.$$

La k' være produktet av alle primtallene blant p'_1, …, $p'_{t'}$ som ikke er like q_j for noen naturlig tall j slik at $j \leq s$. Da er

$$n' = k' \cdot (q_1 \cdots q_s),$$

altså

$$q_1 \cdots q_s \mid n'.$$

La c være et naturlig tall slik at $c \mid n$ og $c \mid n'$. Ut ifra Teorem 4.3.3, finnes det et naturlig tall u og, for hvert naturlig tall l slik at $l \leq u$, et primtall p_l, slik at

$$c = p_1 \cdots p_u.$$

Vi gjør følgende observasjoner.

(1) For hvert naturlig tall l slik at $l \leq u$, er

$$c = (p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_u) \cdot p_l.$$

Dermed har vi: $p_l \mid c$.

(2) Siden $c \mid n$, følger det fra (1) og Proposisjon 2.5.27 at $p_l \mid n$ for hvert naturlig tall l slik at $l \leq u$.

(3) Det følger fra (2) og Korollar 4.2.23 at, for hvert naturlig tall l slik at $l \leq u$, finnes det et naturlig tall i slik at $i \leq t$ og $p_l = p_i$.

(4) Siden $c \mid n'$, følger det fra (1) og Proposisjon 2.5.27 at $p_l \mid n'$ for hvert naturlig tall l slik at $l \leq u$.

(5) Det følger fra (4) og Korollar 4.2.23 at, for hvert naturlig tall l slik at $l \leq u$, finnes det et naturlig tall i' slik at $i' \leq t'$ og $p_l = p_{i'}$.

(6) Det følger fra (3) og (5) at, for hvert naturlig tall l slik at $l \leq u$, finnes det et naturlig tall j slik at $j \leq s$ og $p_l = q_s$.

La m være produktet av alle primtallene blant $q_1, \ldots, q_s$ som ikke er like p_l for noen naturlig tall l slik at $l \leq u$. Da er

$$q_1 \cdots q_s = m \cdot (p_1 \cdots p_u),$$

altså

$$q_1 \cdots q_s = m \cdot c.$$

Dermed har vi:

$$c \mid q_1 \cdots q_s.$$

Det følger fra Proposisjon 2.5.30 at $c \leq q_1 \cdots q_s$. Således har vi bevist at:

(I) $q_1 \cdots q_s \mid n$;

(II) $q_1 \cdots q_s \mid n'$;

(III) dersom c er et naturlig tall slik at $c \mid n$ og $c \mid n'$, er

$$c \leq q_1 \cdots q_s.$$

Vi konkluderer at

$$\mathsf{sfd}(n, n') = q_1 \cdots q_s.$$

□

Merknad 4.6.2. Proposisjon 4.6.1 gir oss en ny tilnærmingsmetode for å finne den største felles divisoren til et par naturlig tall n og n':

(1) finn en primtallsfaktorisering av n og en primtallsfaktorisering av n';

(2) da er $\mathsf{sfd}(n, n')$ lik produktet av alle primtallene som dukker opp i begge primtallsfaktoriseringene.

Eksempel 4.6.3. La oss benytte oss av denne tilnærmingsmetoden for å finne $\mathsf{sfd}(105, 30)$. En primtallsfaktorisering av 105 er

$$3 \cdot 5 \cdot 7.$$

En primtallsfaktorisering av 30 er

$$2 \cdot 3 \cdot 5.$$

Primtallene som dukker opp i begge primtallsfaktoriseringene er 3 og 5. Proposisjon 4.6.1 fastslår at

$$\mathsf{sfd}(105, 30) = 3 \cdot 5,$$

altså at

$$\mathsf{sfd}(105, 30) = 15.$$

Eksempel 4.6.4. La oss benytte oss av denne tilnærmingsmetoden for å finne $\mathsf{sfd}(180, 216)$. En primtallsfaktorisering av 180 er

$$2 \cdot 2 \cdot 3 \cdot 3 \cdot 5.$$

En primtallsfaktorisering av 216 er

$$2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3.$$

Primtallene som dukker opp i begge primtallsfaktoriseringene er 2 (to ganger) og 3 (to ganger). Proposisjon 4.6.1 fastslår at

$$\mathsf{sfd}(180, 216) = 2 \cdot 2 \cdot 3 \cdot 3,$$

altså at

$$\mathsf{sfd}(180, 216) = 36.$$

Eksempel 4.6.5. La oss benytte oss av denne tilnærmingsmetoden for å finne

$$\mathsf{sfd}(254163, 4952038).$$

En primtallsfaktorisering av 254163 er

$$3 \cdot 7 \cdot 7 \cdot 7 \cdot 13 \cdot 19.$$

En primtallsfaktorisering av 4952038 er

$$2 \cdot 7 \cdot 7 \cdot 13 \cdot 13 \cdot 13 \cdot 23.$$

Primtallene som dukker opp i begge primtallsfaktoriseringene er 7 (to ganger) og 13. Proposisjon 4.6.1 fastslår at

$$\mathsf{sfd}(254163, 4952038) = 7 \cdot 7 \cdot 13,$$

altså i at

$$\mathsf{sfd}(254163, 4952038) = 637.$$

4.7 Aritmetikkens fundamentalteorem II

Merknad 4.7.1. Teorem 4.7.2 fastslår at hvert naturlig tall har en primtallsfaktorisering. I Merknad 4.3.13, Eksempel 4.3.14, og Eksempel 4.3.15, så vi på en metode for å finne en primtallsfaktorisering til et naturlig tall i praksis. Denne metoden kan typisk gjennomføres på flere måter, men vi så at vi alltid får den samme primtallsfaktoriseringen.

Nå skal vi bevise at dette er nødvendigvis sant: hvert naturlig tall har kun én primtallsfaktorisering. Det er kun rekkefølgen av primtallene i faktoriseringen som kan være ulik. Med andre ord, har hvert naturlig tall kun én primtallsfaktorisering slik at primtallene i faktoriseringen går fra lavest på venstre side til høyest på høyre side.

Teorem 4.7.2. La n være et naturlig tall. La s og t være naturlige tall. Anta at det finnes, for hvert naturlig tall i slik at $i \leq s$, og hvert naturlig tall j slik at $j \leq t$, primtall p_i og p'_j slik at

$$n = p_1 \cdots p_s$$

og

$$n = p'_1 \cdots p'_t.$$

Anta dessuten at

$$p_1 \leq p_2 \leq \cdots \leq p_s$$

og at

$$p'_1 \leq p'_2 \leq \cdots \leq p'_t.$$

Da har vi:

(I) $s = t$;

(II) $p_i = p'_i$ for hvert naturlig tall i slik at $i \leq s$.

Bevis. Først sjekker vi om proposisjonen er sann når $s = 1$. Da er $n = p_1$, hvor p_1 er et primtall. La t være et naturlig tall. Anta at det finnes, for hvert naturlig tall j slik at $j \leq t$, primtall p'_j slik at

$$p_1 = p'_1 \cdots p'_t,$$

hvor

$$p'_1 \leq p'_2 \leq p'_t.$$

Vi ønsker å bevise at vi da har: $t = 1$ og $p_1 = p'_1$. Siden

$$p_1 = p'_1 \cdots p'_t,$$

har vi: $p'_1 \mid p_1$. Siden p_1 er et primtall, følger det fra Korollar 4.2.23 at $p'_1 = p_1$. Anta at $t > 1$. Da har vi:

$$p_1 = p_1 \cdot \left(p'_2 \cdots p'_t\right).$$

Det følger fra Proposisjon 2.2.25 at

$$1 = p'_2 \cdots p'_t.$$

Siden p'_j er, for hvert naturlig tall j slik at $j \leq t$, et primtall, er $p'_j \geq 2$. Derfor er

$$p'_2 \cdots p'_t \geq 2.$$

Det kan ikke være sant at både

$$p'_2 \cdots p'_t = 1$$

og

$$p'_2 \cdots p'_t \geq 2.$$

Siden antakelsen at $t > 1$ fører til denne motsigelsen, konkluderer vi at det ikke er sant at $t > 2$. Dermed er $t = 1$. Således har vi bevist at proposisjonen er sann når $s = 1$.

Anta nå at proposisjonen har blitt bevist når $s = m$, hvor m er et gitt naturlig tall. Vi ønsker å bevise at det følger at proposisjonen er sann når $s = m + 1$. Anta at det finnes et naturlig tall t slik at, for hvert naturlig tall slik at $i \leq m + 1$, og hvert naturlig tall j slik at $j \leq t$, primtall p_i og p_j slik at

$$n = p_1 \cdots p_s$$

og

$$n = p'_1 \cdots p'_t.$$

Anta dessuten at

$$p_1 \leq p_2 \leq \cdots \leq p_{m+1}$$

og at

$$p'_1 \leq p'_2 \leq \cdots \leq p'_t.$$

Vi gjør følgende observasjoner.

(1) Siden

$$p'_1 \ldots p'_t = (p_1 \cdots p_m) \cdot p_{m+1},$$

har vi:

$$p_{m+1} \mid p'_1 \cdots p'_t.$$

Siden p_{m+1} er et primtall, følger det fra Korollar 4.2.23 at det finnes et naturlig tall j slik at $j \leq t$ og $p_{m+1} = p'_j$. Siden $p'_j \leq p'_t$, deduserer vi at $p_{m+1} \leq p'_t$.

(2) Siden

$$p_1 \ldots p_{m+1} = \left(p'_1 \cdots p'_{t-1}\right) \cdot p'_t,$$

har vi:

$$p'_t \mid p_1 \cdots p_{m+1}.$$

Siden p'_t er et primtall, følger det fra Korollar 4.2.23 at det finnes et naturlig tall i slik at $i \leq m + 1$ og $p'_t = p_i$. Siden $p_i \leq p_{m+1}$, deduserer vi at $p'_t \leq p_{m+1}$.

(3) Fra (1) og (2) har vi: $p_{m+1} \leq p'_t$ og $p'_t \leq p_{m+1}$. Det følger at $p_{m+1} = p'_t$.

(4) Ut ifra (3) og ligningen

$$p_1 \cdots p_{m+1} = p'_1 \cdots p'_t$$

er

$$(p_1 \cdots p_m) \cdot p_{m+1} = \left(p'_1 \cdots p'_{t-1}\right) \cdot p_{m+1}.$$

Det følger fra Proposisjon 2.2.25 at

$$p_1 \cdots p_m = p'_1 \cdots p'_{t-1}.$$

Fra antakelsen at proposisjonen er sann når $n = m$, følger det fra (4) at:

(I) $m = t - 1$;

(II) $p_i = p'_i$ for hvert naturlig tall i slik at $1 \leq i \leq m$.

Ut ifra (I) er $m + 1 = t$. Ut ifra (3) og (II) er $p_i = p'_i$ for hvert naturlig tall i slik at $1 \leq i \leq m + 1$. Således er proposisjonen sann når $n = m + 1$.

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

□

Merknad 4.7.3. Teorem 4.7.2 er ikke sant om vi ikke antar at p_i er et primtall for hvert naturlig tall i slik at $i \leq s$, og at p'_j er et primtall for hvert naturlig tall j slik at $j \leq t$. For eksempel har vi: $12 = 3 \cdot 4$ og $12 = 2 \cdot 6$. Det er ikke sant at $3 = 2$ og at $4 = 6$.

Merknad 4.7.4. Antakelsen at

$$p_1 \leq p_2 \leq \cdots \leq p_s$$

og

$$p'_1 \leq p'_2 \leq \cdots \leq p'_t$$

er harmløs: vi kan bytte om rekkefølgen av primtallene i en hvilken som helst primtallsfaktorisering for å oppfylle dette kravet. Dermed kan Teorem 4.7.2 formuleres som i det andre avsnittet av Merknad 4.7.1.

Merknad 4.7.5. Når vi så på divisjonsalgoritmen i §2.2, var det både en proposisjon som sa noe om eksistens (Proposisjon 2.2.6) og en proposisjon sa noe om entydighet (Proposisjon 2.2.15): se Merknad 2.2.17. På lignende vis er Teorem 4.3.3 et teorem om *eksistensen* av en primtallsfaktorisering til et naturlig tall, mens Teorem 4.7.2 er et teorem om *entydigheten* av primtallsfakoriseringene til et naturlig tall.

4.8 Inverser modulo et primtall

Merknad 4.8.1. Fra skolen kjenner du godt til at ligningen

$$3x = 1$$

har en løsning: $x = \frac{1}{3}$. Vi skriver ofte $\frac{1}{3}$ som 3^{-1}. For et hvilket som helst heltall a slik at $a \neq 0$, er $x = \frac{1}{a}$, altså $x = a^{-1}$, en løsning til ligningen

$$ax = 1.$$

Brøkene a^{-1} er svært viktige. De gir oss muligheten til å definere begrepet «dele med a»: gang med a^{-1}.

Bortsett fra når $a = 1$ eller $a = -1$, er a^{-1} aldri et heltall. Det vil si ligningen

$$ax = 1$$

har en heltallsløsning kun når a er lik enten 1 eller -1. Vi kan ikke dele i verdenen av heltall: vi må jobbe i den større verdenen av brøk.

La n være et naturlig tall. Hva om vi istedenfor ser på kongruensen

$$ax \equiv 1 \pmod{n}?$$

Når n er et primtall p, følger det resultater om linære kongruenser som vi har sett på at denne kongruensen har en heltallsløsning for et hvilket som helst a som ikke delelig med p.

Når vi jobber modulo et primtall, finnes det dermed et heltall som spiller rollen av brøket a^{-1}. Dette heltallet gir oss muligheten til å dele i aritmetikk modulo et primtall.

Således finnes det et forhold mellom aritmetikk modulo p og aritmetikk med brøk. Dette forholdet er på mange måter nærere enn forholdet mellom aritmetikk modulo p og aritmetikk med heltall.

At vi kan dele i aritmetikk modulo et primtall er svært viktig. Vi kommer til å benytte oss av dette ofte!

Definisjon 4.8.2. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. En *invers* til a modulo p er et heltall x slik at $ax \equiv 1 \pmod{p}$.

Notasjon 4.8.3. Vi betegner en invers x til a modulo p slik at $0 \leq x < p$ som a^{-1}.

Eksempel 4.8.4. Siden $2 \cdot 3 = 6$ og $6 \equiv 1 \pmod{5}$, er 3 en invers til 2 modulo 5. Med andre ord er $2^{-1} = 3$ i aritmetikk modulo 5.

Eksempel 4.8.5. Siden $3 \cdot 5 = 15$ og $15 \equiv 1 \pmod{7}$, er 5 en invers til 3 modulo 7. Med andre ord er $3^{-1} = 5$ i aritmetikk modulo 7.

Eksempel 4.8.6. Siden $2 \cdot 2 = 4$ og $4 \equiv 1 \pmod{3}$, er 2 en invers til 2 modulo 3. Med andre ord er $2^{-1} = 2$ i aritmetikk modulo 3.

Merknad 4.8.7. Eksempel 4.8.4 og Eksempel 4.8.6 viser at inversen til et heltall modulo et primtall p avhenger av p. Hvis vi med andre ord har to ulike primtall p og q, kan en invers til et heltall a modulo p være ulik en invers til a modulo q.

Proposisjon 4.8.8. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. Ut ifra Proposisjon 3.2.1 finnes det at heltall r slik at:

(1) $a \equiv r \pmod{p}$.

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

Da er et heltall x en invers til a modulo p hvis og bare hvis x er en invers til r modulo p.

Bevis. Ut ifra (1) og Korollar 3.2.45 er

$$ax \equiv rx \pmod{p}.$$

Ut ifra Proposisjon 3.2.24 og Proposisjon 3.2.33 er da

$$rx \equiv 1 \pmod{p}$$

hvis og bare hvis

$$ax \equiv 1 \pmod{p}.$$

□

Eksempel 4.8.9. Siden $12 \cdot 3 = 36$ og

$$36 \equiv 1 \pmod{5},$$

er 3 en invers til 12 modulo 5. Vi har:

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

Proposisjon 4.8.8 fastslår at 3 er da en invers til 2 modulo 5. Fra Eksempel 4.8.4 vet vi at dette er riktignok sant.

Eksempel 4.8.10. Siden $38 \cdot 5 = 190$ og

$$190 \equiv 1 \pmod{7},$$

er 5 en invers til 38 modulo 7. Vi har:

$$38 \equiv 3 \pmod{7}.$$

Proposisjon 4.8.8 fastslår at 5 er da en invers til 3 modulo 7. Fra Eksempel 4.8.5 vet vi at dette er riktignok sant.

Proposisjon 4.8.11. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. La x være en invers til a modulo p. Da finnes det et heltall r slik at:

(1) r er en invers til a modulo p;

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

(3) $x \equiv r \pmod{p}$.

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

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

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

Vi gjør følgende observasjoner.

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

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

Fra Proposisjon 3.2.24 følger det at

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

(2) Siden x er en invers til a modulo p, er

$$ax \equiv 1 \pmod{p}.$$

Fra (1), (2), og Proposisjon 3.2.33 følger det at

$$ar \equiv 1 \pmod{p},$$

altså at r er en invers til a modulo p.

□

Eksempel 4.8.12. Siden $3 \cdot 7 = 21$ og

$$21 \equiv 1 \pmod{5},$$

er 7 en invers til 3 modulo 5. Siden $3 \cdot 2 = 6$ og

$$6 \equiv 1 \pmod{5},$$

er 2 i tillegg en invers til 3 modulo 5. Proposisjon 4.8.11 fastslår at

$$7 \equiv 2 \pmod{5}.$$

Dette er riktignok sant.

Eksempel 4.8.13. Siden $4 \cdot 25 = 100$ og

$$100 \equiv 1 \pmod{11},$$

er 25 en invers til 4 modulo 11. Siden $4 \cdot 3 = 12$ og

$$12 \equiv 1 \pmod{11},$$

er 3 i tillegg en invers til 4 modulo 11. Proposisjon 4.8.11 fastslår at

$$25 \equiv 3 \pmod{11}.$$

Dette er riktignok sant.

Proposisjon 4.8.14. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. Da finnes det et heltall x som er en invers til a modulo p, og enhver annet heltall som er en invers til a er kongruent til x modulo p.

Bevis. Følger umiddelbart fra Proposisjon 4.2.28, ved å la c være 1. □

Korollar 4.8.15. La p være et primtall. La a være et heltall slik at det ikke er sant at $a \equiv 0 \pmod{p}$. Da finnes det et heltall r slik at:

(1) r er en invers til a modulo p;

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

(3) enhver annet heltall som er en invers til a er kongruent til r modulo p.

Bevis. Følger umiddelbart fra Proposisjon 4.8.14, Proposisjon 4.8.11, Proposisjon 3.2.33, og Proposisjon 3.2.24. □

Merknad 4.8.16. Korollar 4.8.15 fastslår at, for et hvilket som helst heltall a, finnes det et heltall x som kan betegnes a^{-1} ifølge Notasjon 4.8.3. Dessuten er x det eneste heltallet som kan betegnes slikt.

Eksempel 4.8.17. La p være 2. Siden $1 \cdot 1 = 1$ og

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

er $1^{-1} = 1$ modulo 2. Ut ifra Proposisjon 4.8.8 er inversen til 1 nok å konstatere en invers modulo 2 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 2.

Eksempel 4.8.18. La p være 3. Siden $1 \cdot 1 = 1$ og

$$1 \equiv 1 \pmod{3},$$

er $1^{-1} = 1$ modulo 3. Siden $2 \cdot 2 = 4$ og

$$4 \equiv 1 \pmod{3},$$

er $2^{-1} = 2$ modulo 3. Ut ifra Proposisjon 4.8.8 er inversene til 1 og 2 nok å konstatere en invers modulo 3 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 3.

Eksempel 4.8.19. La p være 5. Ut ifra Proposisjon 4.8.8 er inversene til de naturlige tallene 1, 2, 3, og 4 nok å konstatere en invers modulo 5 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 5. Disse inversene vises i tabellene.

Naturlig tall	Invers modulo 5
1	1
2	3
3	2
4	4

For eksempel er $4^{-1} = 4$ modulo 5, siden $4 \cdot 4 = 16$ og

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

Eksempel 4.8.20. La p være 7. Ut ifra Proposisjon 4.8.8 er inversene til de naturlige tallene 1, 2, ..., 6 nok å konstatere en invers modulo 7 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 7. Disse inversene vises i tabellene.

Naturlig tall	Invers modulo 7
1	1
2	4
3	5
4	2
5	3
6	6

For eksempel er $2^{-1} = 4$ modulo 7, siden $2 \cdot 4 = 8$ og

$$8 \equiv 1 \pmod{7}.$$

Eksempel 4.8.21. La p være 11. Ut ifra Proposisjon 4.8.8 er inversene til de naturlige tallene 1, 2, ..., 10 nok å konstatere en invers modulo 7 til et hvilket som helst heltall som ikke er kongruent til 0 modulo 11. Disse inversene vises i tabellene.

Naturlig tall	Invers modulo 11
1	1
2	6
3	4
4	3
5	9
6	2
7	8
8	7
9	5
10	10

For eksempel er $7^{-1} = 8$ modulo 11, siden $7 \cdot 8 = 56$ og

$$56 \equiv 1 \pmod{11}.$$

Proposisjon 4.8.22. La p være et primtall. Da er $(p-1)^{-1} = p - 1$.

Bevis. Siden $p - 1 \equiv -1 \pmod{p}$, følger det fra Proposisjon 3.2.42 at

$$(p-1) \cdot (p-1) \equiv (-1) \cdot (-1) \pmod{p}.$$

Dermed er

$$(p-1)\cdot(p-1) \equiv 1 \pmod{p}.$$

□

Eksempel 4.8.23. Proposisjon 4.8.22 fastlår at $12^{-1} = 12$ modulo 13. Siden

$$12 \cdot 12 = 144$$

og

$$144 \equiv 1 \pmod{13},$$

er dette riktignok sant.

Eksempel 4.8.24. Proposisjon 4.8.22 fastlår at $16^{-1} = 16$ modulo 17. Siden

$$16 \cdot 16 = 256$$

og

$$256 \equiv 1 \pmod{17},$$

er dette riktignok sant.

Merknad 4.8.25. La p være et primtall. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Ut ifra Proposisjon 3.2.13 er det da ikke sant at $p \mid a$. Fra Korollar 4.2.5 følger det at $\mathsf{sfd}(a, p) = 1$.

Korollar 3.4.39 gir oss derfor en tilnærmingsmetode for å finne a^{-1} modulo p. Ved å benytte algoritmen i Merknad 2.7.15, får vi heltall u og v slik at $1 = au + vp$. Da fastslår Korollar 3.4.39 at $x = u$ er en løsning til kongruensen

$$ax \equiv 1 \pmod{p}.$$

Eksempel 4.8.26. Ved å benytte algoritmen i Merknad 2.7.15, får vi at

$$1 = 9 \cdot 17 + (-8) \cdot 19.$$

Da fastslår Korollar 3.4.39 at $x = 9$ er en løsning til kongruensen

$$17x \equiv 1 \pmod{19},$$

altså at $17^{-1} = 9$ modulo 19.

Eksempel 4.8.27. Ved å benytte algoritmen i Merknad 2.7.15, får vi at

$$1 = (-10) \cdot 26 + 9 \cdot 29.$$

Da fastslår Korollar 3.4.39 at $x = -10$ er en løsning til kongruensen

$$26x \equiv 1 \pmod{29},$$

altså at -10 er en invers til 26 modulo 29. Siden

$$-10 \equiv 19 \mod 29,$$

konkluderer vi at $26^{-1} = 19$ modulo 29.

Proposisjon 4.8.28. La p være et primtall. La x, y, og z være heltall slik at

$$xz \equiv yz \pmod{p}.$$

Anta at det ikke er sant at

$$z \equiv 0 \pmod{p}.$$

Da er

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

Bevis. Siden p er et primtall og det ikke er sant at

$$z \equiv 0 \pmod{p},$$

fastslår Korollar 4.8.15 at det finnes et heltall z^{-1} som er en invers til z modulo p. Dermed er

$$zz^{-1} \equiv 1 \pmod{p}.$$

Vi gjør følgende observasjoner.

(1) Fra Korollar 3.2.45 og kongruensen

$$zz^{-1} \equiv 1 \pmod{p}$$

følger det at

$$xzz^{-1} \equiv x \pmod{p}.$$

Fra Proposisjon 3.2.24 følger det at

$$x \equiv xzz^{-1} \pmod{p}.$$

(2) Fra Korollar 3.2.45 og kongruensen

$$zz^{-1} \equiv 1 \pmod{p}$$

følger det at

$$yzz^{-1} \equiv y \pmod{p}.$$

(3) Fra Korollar 3.2.45 og kongruensen

$$xz \equiv yz \pmod{p},$$

følger det at

$$xzz^{-1} \equiv yzz^{-1} \pmod{p}.$$

Fra (1) – (3) og Proposisjon 3.2.33, følger det at

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

□

Eksempel 4.8.29. Vi har:

$$42 \equiv 72 \pmod{5},$$

altså

$$3 \cdot 14 \equiv 8 \cdot 14 \pmod{5}.$$

Proposisjon 4.8.28 fastslår da at

$$3 \equiv 8 \pmod{5},$$

som er riktignok sant.

Eksempel 4.8.30. Vi har:

$$30 \equiv 96 \pmod{11},$$

altså

$$5 \cdot 6 \equiv 16 \cdot 6 \pmod{11}.$$

Proposisjon 4.8.28 fastslår da at

$$5 \equiv 16 \pmod{11},$$

som er riktignok sant.

Merknad 4.8.31. Siden det ikke er sant at

$$z \equiv 0 \pmod{p},$$

er det ikke sant at $p \mid z$. Ut ifra Korollar 4.2.5 er da $\mathsf{sfd}(z, p) = 1$. Derfor kan Proposisjon 4.8.28 også bevises ved å benytte Proposisjon 3.4.13.

4.9 Binomialteoremet modulo et primtall

Merknad 4.9.1. La n være et naturlig tall. La k være et heltall slik at $0 \leq k \leq n$. Ut ifra Proposisjon 1.9.29, er $\binom{n}{k}$ et naturlig tall. Ut ifra Proposisjon 3.2.1, er $\binom{n}{k}$ kongruent modulo n til et heltall r slik at $0 \leq r < n$. Hva er r? Når n er et primtall, sier følgende proposisjon at r er alltid lik 0. Denne observasjonen er veldig nyttig, som vi kommer til å se.

Proposisjon 4.9.2. La p være et primtall. La k være et heltall slik at $0 < k < p$. Da er

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Bevis. Ut ifra definisjonen til $\binom{p}{k}$, er

$$p! = \binom{p}{k} \cdot \big(k! \cdot (p-k)!\big).$$

Ut ifra definisjonen til $p!$ er dermed

$$\binom{p}{k} \cdot k! \cdot (p-k)! = (p-1)! \cdot p,$$

altså

$$\binom{p}{k} \cdot k! \cdot (p-k)!$$

er delelig med p. Siden p er et primtall, følger det fra Korollar 4.2.19 at ett av følgende er sant.

(A) Vi har:

$$p \mid \binom{p}{k}.$$

(B) Vi har:

$$p \mid k!.$$

(C) Vi har:

$$p \mid (p-k)!.$$

Anta først at (C) er sant. Ut ifra Korollar 4.2.19 og definisjonen til $(p-k)!$, finnes det da et naturlig tall i slik at $p \mid i$ og $i \leq p-k$. Siden $k > 0$, er $p-k < p$. Dermed er $i < p$. Siden $p \mid i$, følger det imidlertid fra Proposisjon 2.5.30 at $p \leq i$. Det kan ikke være sant at både $i < p$ og $p \leq i$. Siden antakelsen at (C) er sant fører til denne motsigelsen, deduserer vi at (C) ikke er sant.

Anta nå at (B) er sant. Ut ifra Korollar 4.2.19 og definisjonen til $k!$, finnes det da et naturlig tall i slik at $p \mid i$ og $i \leq k$. Siden $k < p$, er da $i < p$. Siden $p \mid i$, følger det imidlertid fra Proposisjon 2.5.30 at $p \leq i$. Dermed har vi: $p < p$. Dette kan ikke være sant! Siden antakelsen at (B) er sant fører til denne motsigelsen, deduserer vi at (B) ikke er sant.

Således er (A) sant. Ut ifra Proposisjon 3.2.13, er da

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

□

Eksempel 4.9.3. La p være 5. Proposisjon 4.9.2 fastslår at

$$\binom{5}{k} \equiv 0 \pmod{5}$$

for hvert naturlig tall k slik at $k < 5$. Tabellen viser $\binom{5}{k}$ for hvert naturlig tall k slik at $k < 5$.

k	$\binom{5}{k}$
1	5
2	10
3	10
4	5

Det er riktignok sant at hvert naturlig tall i den andre kolonnen er kongruent til 0 modulo 5.

Eksempel 4.9.4. La p være 7. Proposisjon 4.9.2 fastslår at

$$\binom{7}{k} \equiv 0 \pmod{7}$$

for hvert naturlig tall k slik at $k < 7$. Tabellen viser $\binom{5}{k}$ for hvert naturlig tall k slik at $k < 5$.

k	$\binom{7}{k}$
1	7
2	21
3	35
4	35
5	21
6	7

Det er riktignok sant at hvert naturlig tall i den andre kolonnen er kongruent til 0 modulo 7.

Merknad 4.9.5. Proposisjon 4.9.2 er ikke nødvendigvis sant om vi ikke antar at p er et primtall. For eksempel er $\binom{4}{2} = 2$, og det er ikke sant at $2 \equiv 0 \pmod{4}$.

Proposisjon 4.9.6. La p være et primtall. La x og y være heltall. Da er

$$(x + y)^p \equiv x^p + y^p \pmod{p}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 1.9.30 er

$$(x + y)^p = \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i.$$

(2) Ut ifra Proposisjon 4.9.2 er $\binom{p}{i} \equiv 0 \pmod{p}$ når $1 \leq i \leq p - 1$.

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

$$\binom{p}{i} x^{p-i} y^i \equiv 0 \pmod{p}$$

når $1 \leq i \leq n$.

(4) Det følger fra (3), Proposisjon 3.2.36, og Proposisjon 3.2.16 at

$$\sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i \equiv x^p + y^p \pmod{p}.$$

Fra (1) og (4) konkluderer vi at

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

□

Eksempel 4.9.7. La p være 2. Da fastslår Proposisjon 4.9.6 at

$$(3+8)^2 \equiv 3^2 + 8^2 \pmod{2}.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$(3+8)^2 = 11^2 = 121$$

og

$$121 \equiv 1 \pmod{2}.$$

(2) Vi har:

$$3^2 + 8^2 = 9 + 64 = 73$$

og

$$73 \equiv 1 \pmod{2}.$$

Dermed er

$$121 \equiv 73 \pmod{2},$$

altså Proposisjon 4.9.6 riktignok stemmer.

Eksempel 4.9.8. La p være 3. Da fastslår Proposisjon 4.9.6 at

$$(6+2)^3 \equiv 6^3 + 2^3 \pmod{3}.$$

Vi gjør følgende observasjoner.

(1) Vi har:

$$(6+2)^3 = 8^3 = 512$$

og

$$512 \equiv 2 \pmod{3}.$$

(2) Vi har:

$$6^3 + 2^3 = 216 + 8 = 224$$

og

$$224 \equiv 2 \pmod 3.$$

Dermed er

$$512 \equiv 224 \pmod 2,$$

altså Proposisjon 4.9.6 riktignok stemmer.

Merknad 4.9.9. Proposisjon 4.9.6 er binomialteoremet i aritmetikk modulo et primtall. Det har blitt mye enklere! Alle de elevene i årenes løp som har gjort feilen at $(x+y)^2 = x^2 + y^2$ hadde hatt det riktig om de hadde sagt at de jobber modulo 2!

Proposisjon 4.9.6 er svært nyttig. Vi kommer ummidelbart til å benytte oss av det for å bevise Proposisjon 4.10.1, som er svært viktig: vi skal benytte oss av denne proposisjonen igjen og igjen.

4.10 Fermats lille teorem

Proposisjon 4.10.1. La p være et primtall. La x være et heltall slik at $x \geq 0$. Da er

$$x^p \equiv x \pmod p.$$

Bevis. Siden $0^p \equiv 0 \pmod p$, er proposisjonen sann når $x = 0$. Anta at proposisjonen har blitt bevist når $x = m$, hvor m er et gitt heltall slik at $m \geq 0$. Ut ifra Proposisjon 4.9.6 er

$$(m+1)^p \equiv m^p + 1^p \pmod p,$$

altså

$$(m+1)^p \equiv m^p + 1 \pmod p.$$

Ut ifra antakelsen at proposisjonen er sann når $x = m$, er

$$m^p \equiv m \pmod p.$$

Da følger det fra Korollar 3.2.39 og Proposisjon 3.2.33 at

$$(m+1)^p \equiv m + 1 \pmod p.$$

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

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

Eksempel 4.10.2. Proposisjon 4.10.1 fastslår at

$$9^2 \equiv 9 \pmod 2.$$

Vi gjør følgende observasjoner.

(1) Vi har: $9^2 = 81$, og

$$81 \equiv 1 \pmod{2}.$$

(2) Vi har:

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

Dermed er utsagnet riktignok sant.

Eksempel 4.10.3. Proposisjon 4.10.1 fastslår at

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

Vi gjør følgende observasjoner.

(1) Vi har: $4^3 = 64$ og

$$64 \equiv 1 \pmod{3}.$$

(2) Vi har:

$$4 \equiv 1 \pmod{3}.$$

Dermed er utsagnet riktignok sant.

Eksempel 4.10.4. Proposisjon 4.10.1 fastslår at

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

Siden $3^5 = 243$ og $243 \equiv 3 \pmod{5}$, er dette riktignok sant.

Korollar 4.10.5. La p være et primtall. La x være et heltall. Da er

$$x^p \equiv x \pmod{p}.$$

Bevis. Ett av følgende er sant:

(A) $x \geq 0$;

(B) $x < 0$.

Anta først at (A) er sant. Da følger korollaret umiddelbart fra Proposisjon 4.10.1.
Anta istedenfor at (B) er sant. Ut ifra Korollar 2.2.11 er ett av følgende sant.

(I) $p = 2$;

(II) p er et oddetall.

Anta først at (I) er sant. Ut ifra Proposisjon 3.2.1 er da enten

$$-x \equiv 0 \pmod 2$$

eller

$$-x \equiv 1 \pmod 2.$$

Anta først at

$$-x \equiv 0 \pmod 2.$$

Ut ifra Proposisjon 3.2.48 er da $(-x)^p \equiv 0 \pmod 2$. Dermed er

$$(-x)^p \equiv -x \pmod 2.$$

Anta istedenfor at

$$-x \equiv 1 \pmod 2.$$

Ut ifra Proposisjon 3.2.48 er da $(-x)^p \equiv 1 \pmod 2$. Dermed er

$$(-x)^p \equiv -x \pmod 2.$$

Således er korollaret sant når (I) stemmer.

Anta nå at (II) er sant. Da er $-x \geq 0$. Ut ifra Proposisjon 4.10.1 er da

$$(-x)^p \equiv -x \pmod p.$$

Siden p er et oddetall, er $(-1)^p = -1$. Dermed er $(-x)^p = -x^p$. Siden

$$(-x)^p \equiv -x \pmod p,$$

følger det at

$$-x^p \equiv -x \pmod p.$$

Ut ifra Korollar 3.2.45 følger det at

$$(-1) \cdot -x^p \equiv (-1) \cdot -x \pmod p,$$

altså at

$$x^p \equiv x \pmod p.$$

Således er korollaret sant når (II) stemmer.

□

Eksempel 4.10.6. Proposisjon 4.10.1 fastslår at

$$(-7)^2 \equiv -7 \pmod 2.$$

Vi gjør følgende observasjoner.

(1) Vi har: $(-7)^2 = 49$, og

$$49 \equiv 1 \pmod 2.$$

(2) Vi har:

$$-7 \equiv 1 \pmod{2}.$$

Dermed er utsagnet riktignok sant.

Eksempel 4.10.7. Proposisjon 4.10.1 fastslår at

$$(-5)^3 \equiv -5 \pmod{3}.$$

Vi gjør følgende observasjoner.

(1) Vi har: $(-5)^3 = -125$ og

$$-125 \equiv 1 \pmod{3}.$$

(2) Vi har:

$$-5 \equiv 1 \pmod{3}.$$

Dermed er utsagnet riktignok sant.

Korollar 4.10.8. La p være et primtall. La x være et heltall slik at det ikke er sant at

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

Da er

$$x^{p-1} \equiv 1 \pmod{p}.$$

Bevis. Ut ifra Korollar 4.10.5 er

$$x^p \equiv x \pmod{p}.$$

Siden det ikke er sant at

$$x \equiv 0 \pmod{p},$$

følger det fra Proposisjon 4.8.28 at

$$x^p \cdot x^{-1} \equiv x \cdot x^{-1} \pmod{p},$$

altså at

$$x^{p-1} \equiv 1 \pmod{p}.$$

□

Terminologi 4.10.9. Både Korollar 4.10.5 og Korollar 4.10.8 kalles *Fermats lille teorem.*

Merknad 4.10.10. Flere andre bevis for Korollar 4.10.8 kan gis. Disse bevisene er typisk av kombinatorisk art: vi finner to forskjellige måter å navngi heltallene r slik at $0 \leq r \leq p-1$. Slike «telleargumentene» er ikke enkle å uttrykke rigorøst kun ved hjelp av de begrepene vi utforsker i dette kurset.

Hvis vi først hadde gitt et bevis for Korollar 4.10.8, kunne vi ha dedusert at Korollar 4.10.5 er sant ved å gange begge sidene av kongruensen

$$x^{p-1} \equiv 1 \pmod{p}$$

med x.

Eksempel 4.10.11. Korollar 4.10.8 fastslår at

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

Siden $4^4 = 256$ og

$$256 \equiv 1 \pmod{5},$$

er dette riktignok sant.

Eksempel 4.10.12. Korollar 4.10.8 fastslår at

$$2^6 \equiv 1 \pmod{7}.$$

Siden $2^6 = 64$ og

$$64 \equiv 1 \pmod{7},$$

er dette riktignok sant.

Merknad 4.10.13. En formodning som ikke ble besvart i flere hundreår var at den motsatte til Korollar 4.10.8 stemmer: dersom det finnes et heltall x slik at

$$x^{n-1} \equiv 1 \pmod{n},$$

er n et primtall. Denne formodningen er faktisk gal! La oss se på at moteksempel.

La x være 2, og la n være 341. Vi har: $2^{10} = 1024$. Siden $1023 = 3 \cdot 341$, er

$$341 \mid 1023.$$

Derfor er

$$1024 \equiv 1 \pmod{341},$$

altså

$$2^{10} \equiv 1 \pmod{341}.$$

Ut ifra Proposisjon 3.2.48, er da

$$\left(2^{10}\right)^{34} \equiv 1^{34} \pmod{341},$$

altså

$$2^{340} \equiv 1 \pmod{341}.$$

Imidlertid er $341 = 11 \cdot 31$, det vil si er 341 ikke et primtall.

4.11 Eksempler på bevis hvor Fermats lille teorem benyttes

Proposisjon 4.11.1. Det naturlige tallet $7^{104}+1$ er delelig med 17.

Bevis. Vi har:

$$104 = 6 \cdot 16 + 8.$$

Dermed er

$$7^{104} = 7^{6\cdot 16+8} = 7^{6\cdot 16} \cdot 7^8 = \left(7^{16}\right)^6 \cdot 7^8.$$

Siden 17 er et primtall, følger det fra Korollar 4.10.8 at

$$7^{16} \equiv 1 \pmod{17}.$$

Ut ifra Proposisjon 3.2.48 er da

$$\left(7^{16}\right)^6 \equiv 1^6 \pmod{17},$$

altså

$$\left(7^{16}\right)^6 \equiv 1 \pmod{17}.$$

Siden $49 + 2 = 51$, og $17 \mid 51$, har vi i tillegg:

$$7^2 \equiv -2 \pmod{17}.$$

Ut ifra Proposisjon 3.2.48 er da

$$\left(7^2\right)^4 \equiv (-2)^4 \pmod{17},$$

altså

$$7^8 \equiv 16 \pmod{17}.$$

Siden

$$16 \equiv -1 \pmod{17},$$

er dermed

$$7^8 \equiv -1 \pmod{17}.$$

Det følger fra Proposisjon 3.2.42 at

$$\left(7^{16}\right)^6 \cdot 7^8 \equiv 1 \cdot (-1) \pmod{17},$$

altså at

$$7^{104} \equiv -1 \pmod{17}.$$

Således er $7^{104}+1$ delelig med 17.

□

Merknad 4.11.2. Følgende proposisjon behøves i løpet av vårt neste eksempel på et bevis hvor Fermats lille teorem benyttes. Proposisjonen er viktig i seg selv.

Proposisjon 4.11.3. La x og r være heltall. La m og n være heltall. Anta at $m \neq 0$, $n \neq 0$, og $\mathsf{sfd}(m, n) = 1$. Anta at

$$x \equiv r \pmod{m}$$

og at

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

Da er

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

Bevis. Vi gjør følgende observasjoner.

(1) Siden

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

har vi:

$$m \mid x - r.$$

(2) Siden

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

har vi:

$$n \mid x - r.$$

Siden $\mathsf{sfd}(m, n) = 1$, følger det fra Proposisjon 2.8.17 at $mn \mid x - r$. Dermed er

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

□

Eksempel 4.11.4. Vi har:

$$49 \equiv 1 \pmod{3}$$

og

$$49 \equiv 1 \pmod{4}.$$

Siden $\mathsf{sfd}(3, 4) = 1$, fastlsår Proposisjon 4.11.3 at

$$49 \equiv 1 \pmod{3 \cdot 4},$$

altså

$$49 \equiv 1 \pmod{12}.$$

Dette er riktignok sant.

Eksempel 4.11.5. Vi har:

$$89 \equiv 5 \pmod{7}$$

og

$$89 \equiv 5 \pmod{6}.$$

Siden $\mathsf{sfd}(7, 6) = 1$, fastlsår Proposisjon 4.11.3 at

$$89 \equiv 5 \pmod{7 \cdot 6},$$

altså

$$89 \equiv 5 \pmod{42}.$$

Dette er riktignok sant.

Korollar 4.11.6. La x og r være heltall. La p og q være et primtall slik at $p \neq q$. Anta at

$$x \equiv r \pmod{p}$$

og at

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

Da er

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

Bevis. Siden q er et primtall, er 1 og q de eneste divisorene til q. Siden $p \neq q$, følger det at q ikke er delelig med p. Det følger fra Korollar 4.2.5 at $\mathsf{sfd}(p, q) = 1$. Da følger korollaret umiddelbart fra Proposisjon 4.11.3. □

Eksempel 4.11.7. Vi har:

$$32 \equiv 2 \pmod{3}$$

og

$$32 \equiv 2 \pmod{5}.$$

Korollar 4.11.6 fastslår at

$$32 \equiv 2 \pmod{3 \cdot 5},$$

altså

$$32 \equiv 2 \pmod{15}.$$

Dette er riktignok sant.

Eksempel 4.11.8. Vi har:

$$237 \equiv 6 \pmod{11}$$

og

$$237 \equiv 6 \pmod{7}.$$

Korollar 4.11.6 fastslår at

$$237 \equiv 6 \pmod{7 \cdot 11},$$

altså

$$237 \equiv 6 \pmod{77}.$$

Dette er riktignok sant.

Merknad 4.11.9. Utsagnet i Proposisjon 4.11.3 er ikke nødvendigvis sant om vi ikke antar at p er et primtall. La for eksempel p være 4, og la q være 6. Vi har:

$$14 \equiv 2 \pmod{4}$$

og

$$14 \equiv 2 \pmod{6}.$$

Imidlertid er det ikke sant at

$$14 \equiv 2 \pmod{24}.$$

Utsagnet i Proposisjon 4.11.3 er heller ikke nødvendigvis sant om $p \mid q$. La for eksempel p være 3, og la q være 6. Vi har:

$$8 \equiv 2 \pmod{3}$$

og

$$8 \equiv 2 \pmod{6}.$$

Imidlertid er det ikke sant at

$$8 \equiv 3 \pmod{18}.$$

Proposisjon 4.11.10. La x være et heltall. Anta at $\mathsf{sfd}(x, 30) = 1$. Da er $x^4 + 59$ delelig med 60.

Bevis. Siden $\mathsf{sfd}(x, 30) = 1$, er x ikke delelig med 2, 3, eller 5. Da fastslår Korollar 4.10.8 at alle de tre følgende utsagnene er sanne:

(A) $x \equiv 1 \pmod{2}$;

(B) $x^2 \equiv 1 \pmod{3}$;

(C) $x^4 \equiv 1 \pmod{5}$.

Det følger fra (A) og Korollar 3.2.63 at enten

$$x \equiv 1 \pmod{4}$$

eller

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

Hvis

$$x \equiv 1 \pmod{4},$$

følger det fra Proposisjon 3.2.48 at

$$x^4 \equiv 1^4 \pmod{4},$$

altså at

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

Hvis

$$x \equiv 3 \pmod 4,$$

følger det fra Proposisjon 3.2.48 at

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

altså at

$$x^2 \equiv 9 \pmod 4.$$

Siden

$$9 \equiv 1 \pmod 4,$$

følger det fra Proposisjon 3.2.33 at

$$x^2 \equiv 1 \pmod 4.$$

Da følger det fra Proposisjon 3.2.48 at

$$\left(x^2\right)^2 \equiv 1^2 \pmod 4,$$

altså at

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

Således er

$$x^4 \equiv 1 \pmod 4$$

både om

$$x \equiv 1 \pmod 4$$

og om

$$x \equiv 3 \pmod 4,$$

altså i begge de mulige tilfellene.

I tillegg følger det fra (B) og Proposisjon 3.2.48 at

$$\left(x^2\right)^2 \equiv 1^2 \pmod 3,$$

altså at

$$x^4 \equiv 1 \pmod 3.$$

Dermed er følgende sanne.

(1) $x^4 \equiv 1 \pmod 4$;

(2) $x^4 \equiv 1 \pmod 3$;

(3) $x^4 \equiv 1 \pmod 5$.

Ved å la p være 3 og q være 4, følger det fra (1), (2), og Proposisjon 4.11.3 at

$$x^4 \equiv 1 \pmod{3 \cdot 4},$$

altså at

$$x^4 \equiv 1 \pmod{12}.$$

Ved å la p være 5 og q være 12, følger det fra denne kongruensen, (3), og Proposisjon 4.11.3 at

$$x^4 \equiv 1 \pmod{5 \cdot 12},$$

altså at

$$x^4 \equiv 1 \pmod{60}.$$

Da følger det fra Korollar 3.2.39 at

$$x^4 + 59 \equiv 1 + 59 \pmod{60},$$

altså at

$$x^4 \equiv 60 \pmod{60}.$$

Siden

$$60 \equiv 0 \pmod{60},$$

følger det fra Proposisjon 3.2.33 at

$$x^4 + 59 \equiv 0 \pmod{60}.$$

Fra Proposisjon 3.2.13 konkluderer vi at

$$x^4 + 59$$

er delelig med 60.

□

Eksempel 4.11.11. Proposisjon 4.11.10 fastslår at

$$7^4 + 59$$

er delelig med 60. Siden $7^4 + 59 = 2460$ og $2460 = 41 \cdot 60$ er dette riktignok sant.

Eksempel 4.11.12. Proposisjon 4.11.10 fastslår at

$$11^4 + 59$$

er delelig med 60. Siden $11^4 + 59 = 14700$ og $14700 = 245 \cdot 60$ er dette riktignok sant.

Proposisjon 4.11.13. La p være et primtall. La a være et heltall slik at det ikke er sant at

$$a \equiv 0 \pmod{p}.$$

Da er

$$x = a^{p-2}c$$

en løsning til kongruensen

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

Enhver annen løsning til denne kongruensen er kongruent til x modulo p.

Bevis. Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

følger det fra Korollar 4.10.8 at

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ut ifra Korollar 3.2.45 er da

$$a^{p-1}c \equiv c \pmod{p}.$$

Siden

$$a \cdot \left(a^{p-2}c\right) = a^{p-1}c,$$

deduserer vi at

$$a \cdot \left(a^{p-2}c\right) \equiv c \pmod{p}.$$

Med andre ord er $x = a^{p-2}c$ en løsning til kongruensen

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

Siden det ikke er sant at

$$a \equiv 0 \pmod{p},$$

er det ikke sant at $p \mid a$. Siden p er et primtall, følger det fra Korollar 4.2.5 at $\mathsf{sfd}(a, p) = 1$. Ut ifra Korollar 3.4.39, Proposisjon 3.2.33, og Proposisjon 3.2.24, er da en hvilken som helst løsning x til kongruensen

$$ax \equiv 0 \pmod{p}$$

kongruent modulo p til $a^{p-2}c$. □

Eksempel 4.11.14. Proposisjon 4.11.13 fastslår at $x = 3^3 \cdot 2$, altså $x = 54$, er en løsning til kongruensen

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

Siden

$$162 \equiv 2 \pmod{5},$$

er dette riktignok sant.

Eksempel 4.11.15. Proposisjon 4.11.13 fastslår at $x = 2^5 \cdot 5$, altså $x = 160$, er en løsning til kongruensen

$$2x \equiv 5 \pmod{7}.$$

Siden

$$320 \equiv 5 \pmod{7},$$

er dette riktignok sant.

4.12 Orden modulo et primtall

Definisjon 4.12.1. La p være et primtall. La x være et heltall slik at det ikke er sant at

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

Et naturlig tall t er *ordenen* til a modulo p dersom t er det minste naturlige tallet slik at:

(1) $x^t \equiv 1 \pmod{p}$;

(2) $0 \leq t < p$.

Merknad 4.12.2. La x være et heltall slik at det ikke er sant at

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

Ut ifra Korollar 4.10.8 er

$$x^{p-1} \equiv 1 \pmod{p}.$$

Derfor har x en orden, og denne ordenen er mindre enn eller likt $p - 1$.

Merknad 4.12.3. For å finne ordenen til et heltall x modulo et primtall p, kan vi gå gjennom heltallene x, x^2, x^3, ..., x^{p-1}. Den første potensen i slik at

$$x^i \equiv 1 \pmod{p}$$

er ordenen til x modulo p.

Notasjon 4.12.4. La p være et primtall. La x være et heltall slik at det ikke er sant at $x \equiv 0 \pmod{p}$. Vi betegner ordenen til x modulo p som $\mathsf{ord}_p(x)$.

Eksempel 4.12.5. Siden $1^1 = 1$, er ordenen til 1 lik 1 for et hvilket som helst primtall p.

Eksempel 4.12.6. For å finne ordenen til 2 modulo 3, gjør vi følgende. Kongruensen i den andre raden er modulo 3.

i	2^i
1	2
2	$4 \equiv 1$

Dermed er ordenen til 2 modulo 3 lik 2.

Således har vi følgende ordener modulo 3.

x	Ordenen til x modulo 3
1	1
2	2

Eksempel 4.12.7. Alle kongruenser i dette eksempelet er modulo 5. For å finne ordenen til 2 modulo 5, gjør vi følgende.

i	2^i
1	2
2	4
3	$8 \equiv 3$
4	$2^4 = 2^2 \cdot 2^2 \equiv 4 \cdot 4 = 16 \equiv 1$

Dermed er ordenen til 2 modulo 5 lik 4.

For å finne ordenen til 3 modulo 5, gjør vi følgende.

i	3^i
1	3
2	$9 \equiv 4$
3	$3^3 = 3^2 \cdot 3^1 \equiv 4 \cdot 3 = 12 \equiv 2$
4	$3^4 = 3^3 \cdot 3^1 \equiv 2 \cdot 3 = 6 \equiv 1$

Dermed er ordenen til 3 modulo 5 lik 4.

For å finne ordenen til 4 modulo 5, gjør vi følgende.

i	4^i
1	4
2	$16 \equiv 1$

Dermed er ordenen til 4 modulo 5 lik 2.

Således har vi følgende ordener modulo 5.

x	Ordenen til x modulo 5
1	1
2	4
3	4
4	2

Merknad 4.12.8. Utregningene i Eksempel 4.12.7 er ikke de eneste mulige. For å vise at

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

kan vi også for eksempel regne som følger:

$$2^4 = 2^3 \cdot 2^1 \equiv 3 \cdot 2 = 6 \equiv 1 \pmod{5}.$$

Alternativt følger det fra Korollar 4.10.8.

Det samme gjelder i neste eksempel.

Eksempel 4.12.9. Alle kongruenser i dette eksempelet er modulo 7. For å finne ordenen til 2 modulo 7, gjør vi følgende.

i	2^i
1	2
2	4
3	$8 \equiv 1$

Dermed er ordenen til 2 modulo 7 lik 3.

For å finne ordenen til 3 modulo 7, gjør vi følgende.

i	3^i
1	3
2	$9 \equiv 2$
3	$3^3 = 3^2 \cdot 3^1 \equiv 2 \cdot 3 = 6$
4	$3^4 = 3^2 \cdot 3^2 \equiv 2 \cdot 2 = 4$
5	$3^5 = 3^3 \cdot 3^2 \equiv 6 \cdot 2 = 12 \equiv 5$
6	$3^6 = 3^4 \cdot 3^2 \equiv 4 \cdot 2 = 8 \equiv 1$

Dermed er ordenen til 4 modulo 7 lik 6.

For å finne ordenen til 4 modulo 7, gjør vi følgende.

i	4^i
1	4
2	$16 \equiv 2$
3	$4^3 = 4^2 \cdot 4^1 \equiv 2 \cdot 4 = 8 \equiv 1$

Dermed er ordenen til 4 modulo 7 lik 3.

For å finne ordenen til 5 modulo 7, gjør vi følgende.

i	5^i
1	5
2	$25 \equiv 4$
3	$5^3 = 5^2 \cdot 5^1 \equiv 4 \cdot 5 = 20 \equiv -1$
4	$5^4 = 5^3 \cdot 5^1 \equiv (-1) \cdot 5 = -5 \equiv 2$
5	$5^5 = 5^3 \cdot 5^2 \equiv (-1) \cdot 4 = -4 \equiv 3$
6	$5^6 = 5^3 \cdot 5^3 \equiv (-1) \cdot (-1) = 1$

Dermed er ordenen til 5 modulo 7 lik 6.

For å finne ordenen til 6 modulo 7, gjør vi følgende.

i	6^i
1	6
2	$36 \equiv 1$

Dermed er ordenen til 6 modulo 7 lik 2.

Således har vi følgende ordener modulo 7.

x	Ordenen til x modulo 7
1	1
2	3
3	6
4	3
5	6
6	2

Proposisjon 4.12.10. La p være et primtall. La x være et heltall slik at x det ikke er sant at

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

La s være ordenen til x. La t være et naturlig tall. Da er

$$x^t \equiv 1 \pmod{p}$$

hvis og bare hvis $s \mid t$.

Bevis. Anta først at $x^t \equiv 1 \pmod{p}$. Ut ifra Proposisjon 2.2.6 finnes det naturlige tall k og r slik at $t = ks + r$. Da er:

$$\begin{aligned} x^t &= x^{ks+r} \\ &= x^{ks} x^r \\ &= (x^s)^k \, x^r. \end{aligned}$$

Ut ifra definisjonen til s er

$$x^s \equiv 1 \pmod{p}.$$

Dermed er

$$x^t \equiv 1^k \cdot x^r,$$

alts

$$x^t \equiv x^r \pmod{p}.$$

Ut ifra antakelsen at

$$x^t \equiv 1 \pmod{p}$$

og Proposisjon 3.2.24, er da

$$x^r \equiv 1 \pmod{p}.$$

Ut ifra definisjonen til s, er s det minste naturlige tallet slik at $x^s \equiv 1 \pmod{p}$. Siden $0 \leq r < s$ og

$$x^r \equiv 1 \pmod{p},$$

følger det at $r = 0$. Dermed er $t = ks$. Vi konkluderer at $s \mid t$.

Anta istedenfor at $s \mid t$. Da finnes det et naturlig tall k slik at $t = ks$. Ut ifra definisjonen til s, er $x^s \equiv 1 \pmod{p}$. Derfor er

$$(x^s)^k \equiv 1^k \pmod{p},$$

altså er

$$x^{sk} \equiv 1 \pmod{p}.$$

Siden

$$sk = ks = t,$$

konkluderer vi at

$$x^t \equiv 1 \pmod{p}.$$

□

Eksempel 4.12.11. Siden $2^6 = 64$ og

$$64 \equiv 1 \pmod{7},$$

fastslår Proposisjon 4.12.10 at ordenen til 2 modulo 7 deler 6. Ut ifra Eksempel 4.12.9 er ordenen til 2 modulo 7 lik 3. Det er riktignok sant at $3 \mid 6$.

Eksempel 4.12.12. Siden $3^8 = 6561$ og

$$6561 \equiv 1 \pmod{5},$$

fastslår Proposisjon 4.12.10 at ordenen til 3 modulo 4 deler 8. Ut ifra Eksempel 4.12.7 er ordenen til 3 modulo 5 lik 4. Det er riktignok sant at $4 \mid 8$.

4.13 Primitive røtter modulo et primtall

Definisjon 4.13.1. La p være et primtall. La x være et heltall slik at det ikke er sant at

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

Da er x en *primitiv rot* modulo p dersom ordenen til x modulo p er $p - 1$.

Eksempel 4.13.2. Siden ordenen til 1 er $2 - 1 = 1$, er 1 en primitiv rot modulo 2.

Eksempel 4.13.3. Ut ifra tabellen på slutten av Eksempel 4.12.6 har vi følgende.

x	Primitiv rot modulo 3?
1	✗
2	✓

Eksempel 4.13.4. Ut ifra tabellen på slutten av Eksempel 4.12.7 har vi følgende.

x	Primitiv rot modulo 5?
1	✗
2	✓
3	✓
4	✗

Eksempel 4.13.5. Ut ifra tabellen på slutten av Eksempel 4.12.9 har vi følgende.

x	Primitiv rot modulo 7?
1	✗
2	✗
3	✓
4	✗
5	✓
6	✗

Proposisjon 4.13.6. La p være et primtall. La x være en primitiv rot modulo p. La a være et heltall. Da finnes det et heltall r slik at $0 \leq r < p$ og

$$x^r \equiv a \pmod{p}.$$

Bevis. Kommer snart! □

Merknad 4.13.7. Proposisjon 4.13.6 er grunnen for at primitive røtter er viktige. Å kunne uttrykke et hvilket som helst heltall modulo p som en potens av ett heltall er noe er spesielt med aritmetikk modulo p, og svært viktig fra et teoretisk synspunkt. Det er langt fra tilfellet at det finnes et heltall x slik at hvert naturlig tall er *likt* x opphøyd i noe. Når $x = 2$, får vi for eksempel heltallene 2, 4, 8, 16, ..., men får vi ikke de negative heltallene, og heller ikke de naturlige tallene 1, 3, 5, 6, 7, 9, ...

4.14 Lagranges teorem

Merknad 4.14.1. Fra skolen kjenner du til at en ligning

$$ax^2 + bx + c = 0$$

har maksimum to løsninger. Se Merknad 5.1.1 for mer om dette. Kanskje kjenner du dessuten til noe som er mer generell: en ligning

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

har maksimum n løsninger. I denne delen av kapittelet skal vi bevise at det samme er tilfellet i modulær aritmetikk: en kongruens

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

har maksimum n løsninger slik at ikke noe par av disse er kongruent til hverandre modulo p.

Proposisjon 4.14.2. La m være et heltall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. La x være et heltall slik at

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{m}.$$

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

(1) $0 \leq r < m - 1$;

(2) $x \equiv r \pmod{m}$.

Vi har:

$$a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv 0 \pmod{m}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.48 er

$$x^i \equiv r^i \pmod{m}$$

for hvert naturlig tall i slik at $i \leq n$.

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

$$a_i x^i \equiv a_i r^i \pmod{m}$$

for hvert naturlig tall i slik at $i \leq n$.

(3) Det følger fra (2) og Korollar 3.2.36 at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x \\ &\equiv a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r \pmod{m} \end{aligned}$$

(4) Det følger fra (3) og Korollar 3.2.39 at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ &\equiv a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \pmod{m}. \end{aligned}$$

Ut ifra Proposisjon 3.2.24 er da

$$\begin{aligned} &a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \\ &\equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{m} \end{aligned}$$

Det følger fra (4), antakelsen at

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{m}$$

og Proposisjon 3.2.33 at

$$a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv 0 \pmod{m}.$$

□

Eksempel 4.14.3. Det kan regnes ut at

$$16^2 + 3 \cdot 16 + 4 = 308$$

og at $308 = 44 \cdot 7$, altså at

$$308 \equiv 0 \pmod{7}.$$

Dermed er $x = 16$ en løsning til kongruensen

$$x^2 + 3x + 4 \equiv 0 \pmod{7}.$$

Siden

$$16 \equiv 2 \pmod{7},$$

fastslår Proposisjon 4.14.2 at $x = 2$ er også en løsning til kongruensen. Dette er riktignok sant.

Eksempel 4.14.4. Det kan regnes ut at

$$9^3 + 3 \cdot 9^2 - 16 \cdot 9 + 2 = 830$$

og at $830 = 166 \cdot 5$, altså at

$$830 \equiv 0 \pmod{5}.$$

Dermed er $x = 9$ en løsning til kongruensen

$$x^3 + 3x^2 + -16x + 2 \equiv 0 \pmod{5}.$$

Siden

$$9 \equiv 4 \pmod{5},$$

fastslår Proposisjon 4.14.2 at $x = 4$ er også en løsning til kongruensen. Dette er riktignok sant.

Lemma 4.14.5. La p være et primtall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. La y være et heltall. Da finnes det et heltall r og, for hvert heltall i slik at $0 \leq i \leq n-1$, et heltall b_i, slik at

$$\begin{aligned}&a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0\\ &= (x-y)\left(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r\end{aligned}$$

for hvert heltall x.

Bevis. Først sjekker vi om lemmaet er sant når $n = 1$. La b_0 være a_1, og la r være $a_1 y + a_0$. Da er:

$$\begin{aligned}(x-y)b_0 + r &= a_1(x-y) + (a_1 y + a_0)\\ &= a_1 x - a_1 y + a_1 y + a_0\\ &= a_1 x + a_0.\end{aligned}$$

Dermed er lemmaet sant når $n = 1$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned}&a_{m+1}x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0\\ &= x\left(a_{m+1}x^m + a_m x^{m-1} + \cdots + a_2 x + a_1\right) + a_0.\end{aligned}$$

(2) Ut ifra antakelsen at lemmaet er sant når $n = m$, finnes det et heltall r' og, for hvert heltall i slik at $0 \leq i \leq m-1$, et heltall b'_i, slik at

$$\begin{aligned}&a_{m+1}x^m + a_m x^{m-1} + \cdots + a_2 x + a_1\\ &= (x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'.\end{aligned}$$

(3) La b_0 være r'. For hvert heltall i slik at $1 \leq i \leq m$, la b_i være b'_{i-1}. La r være $yr' + a_0$. Da er

$$\begin{aligned}&(x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r\\ &= (x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x\right) + (x-y)b_0 + r\\ &= x(x-y)\left(b_m x^{m-1} + b_{m-1}x^{m-2} + \cdots + b_2 x + b_1\right) + xb_0 - yb_0 + r\\ &= x\Big((x-y)\left(b_m x^{m-1} + b_{m-1}x^{m-2} + \cdots + b_2 x + b_1\right) + b_0\Big) - yb_0 + r\\ &= x\Big((x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'\Big) - yr' + \left(yr' + a_0\right)\\ &= x\Big((x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'\Big) + a_0.\end{aligned}$$

(4) Det følger fra (2) at

$$\begin{aligned} &x\Big((x-y)\left(b'_{m-1}x^{m-1}+b'_{m-2}x^{m-2}+\cdots+b'_1x+b'_0\right)+r'\Big)+a_0\\ &=x\left(a_{m+1}x^m+a_mx^{m-1}+\cdots+a_2x+a_1\right)+a_0. \end{aligned}$$

Det følger fra (1), (3), og (4) at

$$\begin{aligned} &a_{m+1}x^{m+1}+a_mx^m+\cdots+a_2x^2+a_1x+a_0\\ &=(x-y)\left(b_mx^m+b_{m-1}x^{m-1}+\cdots+b_2x^2+b_1x+b_0\right)+r. \end{aligned}$$

Dermed er lemmaet sant når $n=m+1$.

Ved induksjon konkluderer vi at lemmaet er sant når n er et hvilket som helst naturlig tall.

□

Eksempel 4.14.6. La y være 3. Da fastslår Lemma 4.14.5 at det finnes et heltall r og et heltall b_0 slik at

$$11x+8=(x-3)\cdot b_0+r,$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være 11, og r være 41: det stemmer at

$$11x+8=(x-3)\cdot 11+41.$$

Eksempel 4.14.7. La y være -7. Lemma 4.14.5 fastslår at det finnes et heltall r og heltall b_0 og b_1 slik at

$$5x^2+2x-3=\big(x-(-7)\big)\left(b_1x+b_0\right)+r,$$

altså at

$$5x^2+2x-3=(x+7)\left(b_1x+b_0\right)+r,$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være -33, b_1 være 5, og r være 228: det stemmer at

$$5x^2+2x-3=(x+7)\left(5x-33x\right)+228.$$

Eksempel 4.14.8. La y være 6. Lemma 4.14.5 fastslår at det finnes et heltall r og heltall b_0, b_1, og b_2 slik at

$$2x^3-8x^2+5x-7=(x-6)\left(b_2x^2+b_1x+b_0\right)+r$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være 2, b_1 være 4, b_2 være 29, og r være 167: det stemmer at

$$2x^3-8x^2+5x-7=(x-6)\left(2x^2+4x+29\right)+167.$$

Merknad 4.14.9. Utsagnet i Lemma 4.14.5 er: det finnes et heltall r og, for hvert heltall i slik at $0 \leq i \leq n$, et heltall b_i, slik at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= (x - y)\left(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \end{aligned}$$

for *hvert* heltall x. Dette er ikke det samme som å si: gitt et heltall x, finnes det et heltall r og, for hvert heltall i slik at $0 \leq i \leq n$, et heltall b_i, slik at denne ligningen stemmer.

Den andre påstanden holder muligheten åpen for at heltallet r og heltallene b_i varierer avhengig av x. Heltallet r og heltallene b_i i Lemma 4.14.5 varierer ikke avhengig av x.

Gitt et heltall x, er for eksempel

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 2x.$$

Ved å la b_0 være 1, b_1 være 2, og r være $2x$, får vi med andre ord at

$$2x^2 + x - 1 = (x - 1)\left(b_1 x + b_0\right) + r.$$

Imidlertid varierer da r avhengig av x. Hvis for eksempel $x = 1$, er $r = 2$, og vi har:

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 2.$$

Hvis $x = 2$, er $r = 4$, og vi har:

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 4.$$

Istedenfor kan vi la b_0 være 1, b_1 være 2, og r være 3: da har vi

$$2x^2 + x - 1 = (x - 1)(2x + 3) + 2.$$

I dette tilfellet varierer r ikke avhengig av x: uansett hvilket heltall x vi velger, er $r = 3$.

Merknad 4.14.10. Lemma 4.14.5 kan generaliseres. Et uttrkk

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

hvor a_i er et heltall for hvert heltall i slik at $0 \leq i \leq n$, og x er en variabel, kalles et *polynom*. Det finnes en divisjonsalgoritme for polynom som bygger på divisjonsalgoritmen for heltall: vi kan dele et polynom med et annet polynom, og får en kvotient som er et polynom og en rest som er et heltall. Lemma 4.14.5 følger umiddelbart fra dette.

Imidlertid kommer vi ikke til å trenge et annet sted divisjonsalgoritmen for polynom. Dessuten må begrepet « «polynom» defineres formelt, og dette er heller ikke noe vi kommer et annet sted til å trenge. Derfor skal vi nøye oss med det direkte beviset vi ga for Lemma 4.14.5.

Proposisjon 4.14.11. La p være et primtall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. Anta at det ikke er sant at

$$a_n \equiv 0 \pmod{p}.$$

Enten har kongruensen

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

ingen løsning, eller så er der et naturlig tall l slik at $l \leq n$, og heltall x_1, x_2, …, x_l, slik at følgende er sanne.

(I) For hvert naturlig tall i slik at $i \leq l$, er

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}.$$

(II) La z være et heltall slik at

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_2 z^2 + a_1 z + a_0 \equiv 0 \pmod{p}.$$

Da finnes det et naturlig tall i slik at $i \leq l$ og $z \equiv x_i \pmod{p}$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. La a_0 og a_1 være heltall. Siden p er et primtall og det ikke er sant at

$$a_1 \equiv 0 \pmod{p},$$

følger det fra Proposisjon 4.2.28 at det finnes et heltall x slik at følgende er sanne.

(1) Vi har: $a_1 x \equiv -a_0 \pmod{p}$.

(2) La y være et heltall slik at $a_1 y \equiv -a_0 \pmod{p}$. Da er $x \equiv y \pmod{p}$.

Det følger fra (1) og Korollar 3.2.39 at

$$a_1 x + a_0 \equiv 0 \pmod{p}.$$

Således er proposisjonen sann når $n = 1$, ved å la $l = 1$ og $x_1 = x$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. For hvert heltall i slik at $0 \leq i \leq m + 1$, la a_i være et heltall. Hvis kongruensen

$$a_{m+1} x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har ingen løsning, er proposisjonen sann. Ellers finnes det et heltall y slik at

$$a_{m+1} y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p}.$$

Ut ifra Lemma 4.14.5 finnes det et heltall r og, for hvert naturlig tall i slik at $0 \leq i \leq m$, et heltall b_i, slik at

$$\begin{aligned} &a_{m+1} x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= (x - y)\left(b_m x^m + b_{m-1} x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \end{aligned}$$

for hvert heltall x. Ved å la $x = y$, får vi:

$$a_{m+1}y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 = r.$$

Siden

$$a_{m+1}y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p},$$

følger det at

$$r \equiv 0 \pmod{p}.$$

Ut ifra Korollar 3.2.39 er dermed

$$\begin{aligned} &a_{m+1}x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &\equiv (x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) \pmod{p} \end{aligned}$$

for hvert heltall x.

Anta først at kongruensen

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \equiv 0 \pmod{p}$$

har ingen løsning. Da er proposisjonen sann når $n = m+1$, ved å la l være 1 og x_1 være y.

Anta istedenfor at kongruensen

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \equiv 0 \pmod{p}$$

har minst én løsning. Siden det ikke er sant at

$$a_{m+1} \equiv 0 \pmod{p},$$

er det ikke sant at

$$b_m \equiv 0 \pmod{p}.$$

Ut ifra antakelsen at proposisjonen er sann når $n = m$, finnes det derfor et naturlig tall l' og, for hvert naturlig tall i slik at $i \leq l'$, et heltall y_i, slik at følgende er sanne.

(A) For hvert naturlig tall i slik at $i \leq l'$, er

$$b_m y_i^m + b_{m-1}y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0 \equiv 0 \pmod{p}.$$

(B) La z være et heltall slik at

$$b_m z^m + b_{m-1}z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0 \equiv 0 \pmod{p}.$$

Da finnes det et naturlig tall i slik at $i \leq l'$ og $z \equiv y_i \pmod{p}$.

La da l være $l'+1$. For hvert naturlig tall i slik at $i \leq l'$, la x_i være y_i. La x_l være y. Vi gjør følgende observasjoner.

(1) Det følger fra (A) og Korollar 3.2.45 at, for hvert naturlig tall i slik at $i \leq l'$, er

$$(y_i - y)\left(b_m y_i^m + b_{m-1} y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0\right) \equiv (x - y) \cdot 0 \pmod{p},$$

altså

$$(y_i - y)\left(b_m y_i^m + b_{m-1} y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0\right) \equiv 0 \pmod{p}.$$

Dermed er

$$(x_i - y)\left(b_m x_i^m + b_{m-1} x_i^{m-1} + \cdots + b_2 x_i^2 + b_1 x_i + b_0\right) \equiv 0 \pmod{p}$$

for hvert naturlig tall i slik at $i \leq l - 1$. Siden

$$\begin{aligned} &a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \\ &\equiv (x_i - y)\left(b_m x_i^m + b_{m-1} x_i^{m-1} + \cdots + b_2 x_i^2 + b_1 x_i + b_0\right) \pmod{p}, \end{aligned}$$

følger det fra Korollar 3.2.33 at

$$a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

for hvert naturlig tall i slik at $i \leq l - 1$.

(2) Siden

$$a_{m+1} y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p},$$

er

$$a_{m+1} x_l^{m+1} + a_m x_l^m + \cdots + a_2 x_l^2 + a_1 x_l + a_0 \equiv 0 \pmod{p}.$$

For hvert naturlig tall i slik at $i \leq l$, er således

$$a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}.$$

Dermed er (I) sant.

La nå z være et heltall slik at

$$a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \equiv 0 \pmod{p}.$$

Siden

$$\begin{aligned} &a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \\ &= (z - y)\left(b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0\right) \end{aligned}$$

er da

$$(z - y)\left(b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0\right) \equiv 0 \pmod{p}.$$

Anta at det ikke er sant at

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

Ut ifra Korollar 3.2.39 er det da ikke sant at

$$z - y \equiv 0 \pmod{p}.$$

Det følger da fra Proposisjon 4.8.28 at

$$b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0 \equiv 0 \pmod{p}.$$

Fra denne kongruensen og (B) deduserer vi at det finnes et naturlig tall i slik at $i \leq l'$ og

$$z \equiv y_i \pmod{p},$$

altså slik at $i \leq l - 1$ og

$$z \equiv x_i \pmod{p}.$$

Vi har således bevist: dersom

$$a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \equiv 0 \pmod{p},$$

er enten

$$z \equiv y \pmod{p},$$

altså

$$z \equiv x_l \pmod{p},$$

eller så finnes det et naturlig tall i slik at $i \leq l - 1$ og

$$z \equiv x_i \pmod{p}.$$

Dermed er (II) er sant.

Således er proposisjonen sann når $n = m + 1$. Ved induksjon konkluderer vi at proposisjonen er sann for et hvilket som helst naturlig tall n.

□

Terminologi 4.14.12. Proposisjon 4.14.11 kalles *Lagranges teorem.*

Merknad 4.14.13. Med andre ord fastslår Proposisjon 4.14.11 at, dersom det ikke er sant at

$$a_n \equiv 0 \pmod{p},$$

finnes det maksimum n løsninger til kongruensen

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

slik at ikke noe par av disse løsningene er kongruent til hverandre modulo p, og slik at enhver annen løsning er kongruent modulo p til én av disse løsningene.

Terminologi 4.14.14. Anta at kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har m løsninger, hvor m er et heltall slik at $0 \leq m \leq n$, slik at ikke noe par av disse m løsningene er kongruent til hverandre modulo p, og slik at enhver annen løsning er kongruent modulo p til én av disse m løsningene. Da sier vi at kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har *m løsninger modulo p.*

Merknad 4.14.15. Ved å benytte denne terminologien, fastslår Proposisjon 4.14.11 at, dersom det ikke er sant at

$$a_n \equiv 0 \pmod{p},$$

finnes det maksimum n løsninger modulo p til kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}.$$

Eksempel 4.14.16. Proposisjon 4.14.11 fastslår at kongruensen

$$-3x^2 + 7x - 17 \equiv 0 \pmod{5}$$

har maksimum to løsninger p. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 4 er løsninger.

Vi har følgende. Alle kongruensene er modulo 5.

x	$-3x^2 + 7x - 17$	Løsning modulo 5?
1	$-13 \equiv 2$	✗
2	$-15 \equiv 0$	✓
3	$-23 \equiv 2$	✗
4	$-37 \equiv 3$	✗

Således har kongruensen

$$-3x^2 + 7x - 17 \equiv 0 \pmod{5}$$

én løsning modulo 5.

Eksempel 4.14.17. Proposisjon 4.14.11 fastslår at kongruensen

$$2x^2 + 3x + 5 \equiv 0 \pmod{7}$$

har maksimum to løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 6 er løsninger. Vi har følgende. Alle kongruensene er modulo 7.

x	$2x^2+3x+5$	Løsning modulo 7?
1	$10 \equiv 3$	✗
2	$19 \equiv 5$	✗
3	$32 \equiv 4$	✗
4	$49 \equiv 0$	✓
5	$70 \equiv 0$	✓
6	$95 \equiv 4$	✗

Således har kongruensen

$$2x^2+3x+5 \equiv 0 \pmod 7$$

to løsninger modulo 7.

Eksempel 4.14.18. Proposisjon 4.14.11 fastslår at kongruensen

$$5x^2+7x+6 \equiv 0 \pmod{13}$$

har maksimum to løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 12 er løsninger.

Vi har følgende. Alle kongruensene er modulo 13.

x	$5x^2+7x+6$	Løsning modulo 13?
1	$18 \equiv 5$	✗
2	$40 \equiv 1$	✗
3	$72 \equiv 7$	✗
4	$114 \equiv 10$	✗
5	$166 \equiv 10$	✗
6	$228 \equiv 7$	✗
7	$300 \equiv 1$	✗
8	$382 \equiv 5$	✗
9	$474 \equiv 6$	✗
10	$576 \equiv 4$	✗
11	$688 \equiv 12$	✗
12	$810 \equiv 4$	✗

Således har kongruensen

$$5x^2+7x+6 \equiv 0 \pmod{13}$$

ingen løsning modulo 13.

Eksempel 4.14.19. Proposisjon 4.14.11 fastslår at kongruensen

$$x^3-x^2+x+1 \equiv 0 \pmod{11}$$

har maksimum tre løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 10 er løsninger.

Vi har følgende. Alle kongruensene er modulo 11.

x	$x^3 - x^2 + x + 1$	Løsning modulo 11?
1	2	✗
2	7	✗
3	$22 \equiv 0$	✓
4	$53 \equiv 9$	✗
5	$106 \equiv 7$	✗
6	$187 \equiv 0$	✓
7	$302 \equiv 5$	✗
8	$457 \equiv 6$	✗
9	$658 \equiv 9$	✗
10	$911 \equiv 7$	✗

Således har kongruensen

$$x^3 - x^2 + x + 1 \equiv 0 \pmod{11}$$

to løsninger modulo 11.

Merknad 4.14.20. Hvis vi ikke jobber modulo p, og se istedenfor på ligningen

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0,$$

fører akkurat det samme argumentet som i beviset for Proposisjon 4.14.11 til et bevis for faktumet nevnt i Merknad 4.14.1: at denne ligningen har maksimum n løsninger.

Merknad 4.14.21. Proposisjon 4.14.11 er ikke nødvendigvis sann om vi ikke antar at p er et primtall. La oss se for eksempel på kongruensen

$$x^2 + x - 2 \equiv 0 \pmod{10}.$$

Vi har følgende. Alle kongruensene er modulo 10.

x	$x^2 + x - 2$	Løsning modulo 10?
1	0	✓
2	4	✗
3	$10 \equiv 0$	✓
4	$18 \equiv 8$	✗
5	$28 \equiv 8$	✗
6	$40 \equiv 0$	✓
7	$54 \equiv 4$	✗
8	$70 \equiv 0$	✓
9	$88 \equiv 8$	✗

Således har kongruensen

$$x^2 + x - 2 \equiv 0 \pmod{10}$$

fire løsninger modulo 10.

4.15 Wilsons teorem

Merknad 4.15.1. Kanskje ser Lagranges teorem temmelig unøyaktig ut. Det sier ikke hvor mange løsninger kongruensen

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

har, og sier ikke hvordan eventuelle løsninger kan finnes.

Derfor er det lett å tro at Lagranges teorem derfor ikke er så nyttig. Imidlertid kommer vi nå til å se at Lagranges teorem kan benyttes for å gi et bevis for Proposisjon 4.15.8, som er både konkret og eksakt. Beviset for Proposisjon 4.15.8 benytter altså, på en interessant måte, et overslag vi får ved å benytte Lagranges teorem som et steg mot å fastslå at den nøyaktige kongruensen i proposisjonen stemmer.

Først må vi gjøre noen forberedelser.

Lemma 4.15.2. La n være et naturlig tall slik at $n \geq 2$. La x være et heltall. Det finnes heltall a_0, a_1, …, a_{n-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)\\&= x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

Bevis. Først sjekker vi om lemmaet er sant når $n = 2$. I dette tilfellet er utsagnet at det finnes et heltall a_0 slik at

$$x - 1 = x - a_0.$$

Ved å la a_0 være 1, ser vi at dette riktignok er sant.

Anta nå at lemmaet har blitt bevist når $n = m$, hvor m er et gitt naturlig tall slik at $m \geq 2$. Således har det blitt bevist at det finnes heltall b_0, b_1, …, b_{m-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(m-1)\big)\\&= x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0.\end{aligned}$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&= \Big((x-1)(x-2)\cdots\big(x-(m-1)\big)\Big)\cdot(x-m)\\&= \big(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\big)\cdot(x-m).\end{aligned}$$

Produktet

$$\big(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\big)\cdot(x-m)$$

er likt summen av

$$x\left(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\right)$$

og

$$-m\left(x^{m-1}+b_{m-2}x^{m-2}+b_{m-3}x^{m-3}+\cdots+b_2x^2+b_1x+b_0\right),$$

altså summen av

$$\left(x^m+b_{m-2}x^{m-1}+b_{m-3}x^{m-2}+\cdots+b_2x^3+b_1x^2+b_0x\right)$$

og

$$-\left(mx^{m-1}+mb_{m-2}x^{m-2}+mb_{m-3}x^{m-3}+\cdots+mb_2x^2+mb_1x+mb_0\right).$$

Denne summen er lik

$$x^m+(b_{m-2}+m)\,x^{m-1}+(b_{m-3}+mb_{m-2})\,x^{m-2}+\cdots+(b_1+mb_2)\,x^2+(b_0+mb_1)\,x+mb_0.$$

Dermed har vi vist at

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&=x^m+(b_{m-2}+m)\,x^{m-1}+(b_{m-3}+mb_{m-2})\,x^{m-2}+\cdots+(b_1+mb_2)\,x^2+(b_0+mb_1)\,x+mb_0.\end{aligned}$$

La a_0 være mb_0. For hvert naturlig tall i slik at $i\leq m-2$, la a_i være $b_{i-1}+mb_i$. La a_{m-1} være $b_{m-2}+m$. Da er

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&=x^m+a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

Dermed er lemmaet sant når $n=m+1$.

Ved induksjon konkluderer vi at lemmaet er sant for alle de naturlige tallene n slik at $n\geq 2$.

□

Eksempel 4.15.3. Lemma 4.15.2 fastslår at det finnes heltall a_0 og a_1 slik at

$$(x-1)(x-2)=x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)=x^2-3x+2,$$

altså kan vi la a_0 være 2 og a_1 være -3.

Eksempel 4.15.4. Lemma 4.15.2 fastslår at det finnes heltall a_0, a_1, a_2 slik at

$$(x-1)(x-2)(x-3)=x^3+a_2x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)(x-3)=x^3-6x^2+11x-6,$$

altså kan vi la a_0 være -6, a_1 være 11, og a_2 være -6.

Korollar 4.15.5. La n være et naturlig tall slik at $n \geq 2$. La x være et heltall. Det finnes heltall a_0, a_1, …, a_{n-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=a_{n-2}x^{n-2}+a_{n-3}x^{n-3}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

Bevis. Ut ifra Lemma 4.15.2 finnes det heltall b_0, b_1, …, b_{n-1} slik at

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)\\&=x^{n-1}+b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0.\end{aligned}$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=\big(x^{n-1}+b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0\big)-x^{n-1}+1\\&=b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0+1.\end{aligned}$$

La $a_0 = b_0 + 1$. For hvert naturlig tall i slik at $i \leq n-2$, la $a_i = b_i$. Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=a_{n-2}x^{n-2}+a_{n-3}x^{n-3}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

□

Eksempel 4.15.6. Korollar 4.15.5 fastslår at det finnes heltall a_0 og a_1 slik at

$$(x-1)(x-2)-\big(x^2-1\big)=a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)-\big(x^2-1\big)=-3x+3,$$

altså kan vi la a_0 være -3 og a_1 være 3.

Eksempel 4.15.7. Korollar 4.15.5 fastslår at det finnes heltall a_0, a_1, a_2 slik at

$$(x-1)(x-2)(x-3)-\big(x^3-1\big)=a_2x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)(x-3)=-6x^2+11x-5,$$

altså kan vi la a_0 være -6, a_1 være 11, og a_2 være -5.

Proposisjon 4.15.8. La p være et primtall. Da er

$$(p-1)!\equiv -1 \pmod{p}.$$

Bevis. Anta først at $p = 2$. Vi har:

$$(2-1)! - (-1) = 1! - (-1) = 1 + 1 = 2.$$

Siden $2 \mid 2$, deduserer vi at

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

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at $p > 2$. La x være et heltall. Ut ifra Korollar 4.15.5 finnes det heltall a_0, a_1, …, a_{p-2} slik at

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &= a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

Anta at det ikke er sant at

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$. La da m være det største heltallet slik at:

(i) $0 \leq m \leq p-2$;

(ii) det ikke er sant at

$$a_m \equiv 0 \pmod{p}.$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &= a_mx^m + a_{m-1}x^{m-1} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

For hvert naturlig tall r slik at $r \leq p-1$ er følgende sanne.

(1) Siden $(r-r) = 0$, er

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) = 0.$$

(2) Ut ifra Korollar 4.10.8 er

$$r^{p-1} \equiv 1 \pmod{p}.$$

Dermed er

$$r^{p-1} - 1 \equiv 1 - 1 \pmod{p},$$

altså

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

(3) Det følger fra (1) og (2) at

$$(r-1)(r-2)\cdots\big(r-(p-1)\big) - \big(r^{p-1}-1\big) \equiv 0 \pmod{p}.$$

For hvert naturlig tall r slik at $r \leq p-1$, er dermed $x = r$ en løsning til kongruensen

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big) \equiv 0 \pmod{p},$$

altså til kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}.$$

Således har kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

minst $p-1$ løsninger.

Siden det ikke er sant at

$$a_m \equiv 0 \pmod{p},$$

følger det på en annen side fra Proposisjon 4.14.11 at kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

har maksimum m løsninger. Vi har: $m \leq p-2$. Dermed har vi en motsigelse: kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

kan ikke ha både minst $p-1$ løsninger og maksimum $p-2$ løsninger.

Vi har således bevist at antakelsen at det ikke er sant at

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$ fører til en motsigelse. Derfor er

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$.

Det følger fra Korollar 3.2.45 og Proposisjon 3.2.36 at, for et hvilket som helst heltall x, er da

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &\equiv 0\cdot x^{p-2} + 0\cdot x^{p-3} + \cdots + 0\cdot x^2 + 0\cdot x + 0 \pmod{p},\end{aligned}$$

altså

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big) \equiv 0 \pmod{p}.$$

La $x = 0$. Ut ifra den foregående proposisjonen er

$$(0-1)(0-2)\cdots\big(0-(p-1)\big) - \big({}^{p-1}-1\big) \equiv 0 \pmod{p},$$

altså

$$(-1)^{p-1}\big(1\cdot 2\cdots(p-1)\big) + 1 \equiv 0 \pmod{p}.$$

Ut ifra Korollar 3.2.39 er dermed

$$(-1)^{p-1}(p-1)! \equiv -1 \pmod{p}.$$

Ut ifra Proposisjon 4.2.31, finnes det et naturlig tall k slik at $p-1=2k$. Derfor er

$$(-1)^{p-1} = (-1)^{2k} = \left((-1)^2\right)^k = 1^k = 1.$$

Vi konkluderer at

$$(p-1)! \equiv -1 \pmod{p}.$$

□

Terminologi 4.15.9. Proposisjon 4.15.8 kalles *Wilsons teorem.*

Eksempel 4.15.10. Siden 3 er et primtall og $3 > 2$, fastslår Proposisjon 4.15.8 at

$$(3-1)! \equiv -1 \pmod{3}.$$

Siden $(3-1)! = 2! = 2$ og

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

er dette riktignok sant.

Eksempel 4.15.11. Siden 5 er et primtall og $5 > 2$, fastslår Proposisjon 4.15.8 at

$$(5-1)! \equiv -1 \pmod{5}.$$

Siden $(5-1)! = 4! = 24$ og

$$24 \equiv -1 \pmod{5},$$

er dette riktignok sant.

Eksempel 4.15.12. Siden 7 er et primtall og $7 > 2$, fastslår Proposisjon 4.15.8 at

$$(7-1)! \equiv -1 \pmod{7}.$$

Siden $(7-1)! = 6! = 720$ og

$$720 \equiv -1 \pmod{7},$$

er dette riktignok sant.

Proposisjon 4.15.13. Det naturlige tallet

$$2 \cdot (26!) + 1$$

er delelig med 29.

Bevis. Vi gjør følgende observasjoner.

(1) Vi har: $2 = (-1) \cdot (-2)$. Derfor er

$$2 \cdot (26!) = (-1) \cdot (-2) \cdot (26!).$$

(2) Vi har:

$$-1 \equiv 28 \pmod{29}$$

og

$$-2 \equiv 27 \pmod{29}.$$

(3) Det følger fra (2) og Proposisjon 3.2.42 at

$$(-1) \cdot (-2) \equiv 28 \cdot 27 \pmod{29}.$$

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

$$(-1) \cdot (-2) \cdot (26!) \equiv 28 \cdot 27 \cdot 26! \pmod{29}.$$

Siden $28 \cdot 27 \cdot (26!) = 28!$, er dermed

$$(-1) \cdot (-2) \cdot (26!) \equiv 28! \pmod{29}.$$

(5) Siden 29 er et primtall, følger det fra Proposisjon 4.15.8 at

$$28! \equiv -1 \pmod{29}.$$

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

$$(-1) \cdot (-2) \cdot (26!) \equiv -1 \pmod{29}.$$

Det følger fra (1) og (6) at

$$2 \cdot (26!) \equiv -1 \pmod{29}.$$

Ut ifra Korollar 3.2.39 er da

$$2 \cdot (26!) + 1 \equiv -1 + 1 \pmod{29},$$

altså

$$2 \cdot (26!) + 1 \equiv 0 \pmod{29}.$$

Vi konkluderer at $29 \mid 2 \cdot (26!) + 1$. □

Merknad 4.15.14. Det er naturlig å se først på Wilsons teorem som er artig, men ikke så viktig fra et teoretisk synspunkt. Imidlertid kommer til å benytte Wilsons teorem i løpet av vårt bevis for det dypeste teoremet i kurset, Teorem 5.8.30!

O4 Oppgaver – Primtall

O4.1 Oppgaver i eksamens stil

Oppgave O4.1.1. Hvilke naturlige tall x slik at $30 \leq x \leq 45$ er primtall?

Oppgave O4.1.2. La p være et primtall slik at $p > 2$ og $p \neq 5$. Gjør følgende.

(1) Dersom $p \equiv 7 \pmod{10}$, vis at $p^2 \equiv -1 \pmod{10}$.

(2) Vis at det ikke er sant at $p \equiv 4 \pmod{10}$. *Tips*: Benytt Proposisjon 3.2.54.

(3) Vis at enten $p^2 - 1$ er delelig med 10 eller $p^2 + 1$ er delelig med 10.

Oppgave O4.1.3. Gjør følgende.

(1) Skriv ned de første 10 primtallene p slik at $p \equiv 5 \pmod{6}$.

(2) La n være et naturlig tall. Bevis at det er et primtall p slik at $p \equiv 5 \pmod{6}$ og $p > n$. Med andre ord, bevis at det er uendelig mange primtall som er kongruent til 5 modulo 6. *Tips*: Se på $6q - 1$, hvor q er produktet av alle primtallene som er mindre enn eller like n og som er kongruent til 5 modulo 6.

Oppgave O4.1.4. Løs Oppgave 2 i Øving 4 ved å benytte kongruenser istedenfor å benytte divisjonsalgoritmen direkte.

Oppgave O4.1.5. Gjør følgende.

(1) Finn en primtallsfaktorisering til 7623.

(2) Finn en primtallsfaktorisering til 2352.

(3) Benytt (1) og (2) for å finne den største felles divisoren til 7623 og 2352.

Oppgave O4.1.6. Finn en invers til 6 modulo 13.

Oppgave O4.1.7. Benytt Fermats lille teorem for å vise at $6^{146} + 2$ er delelig med 19.

Oppgave O4.1.8. La x være et heltall. Anta at $\mathsf{sfd}(x, 21) = 1$. Vis at $8x^6 + 55$ er delelig med 63.

Oppgave O4.1.9. Finn uten å benytte Euklids algoritme og uten gå gjennom alle heltallene 0, 1, ..., 28 en løsning x til kongruensen

$$3x \equiv 8 \pmod{29},$$

slik at $0 \leq x < 29$. Forklar hvorfor enhver annen løsning er kongruent modulo 29 til løsningen du har funnet.

Oppgave O4.1.10. Skriv ned ordenene modulo 11 til alle de naturlige tallene 1, 2, ..., 10. Hvilke av 1, 2, ..., 10 er primitive røtter modulo 11?

Oppgave O4.1.11. Vis uten å regne ut at $18 \cdot (33!) - 3$ er delelig med 37.

O4.2 Oppgaver for å hjelpe med å forstå kapittelet

Oppgave O4.2.1. Gå gjennom beviset for Teorem 4.3.3 når $n = 18$. Hva er det minste primetall større enn 18 som vi får? *Tips*: 510511 er delelig med 277 og 97, og både 277 og 97 er primtall.

Oppgave O4.2.2. La p være 11. Regn ut de første ti naturlige tallene i sekvensen i Definisjon **??**. Ved å benytte svaret ditt på Oppgave O4.1.10, sjekk om det tiende naturlige tallet i sekvensen er en primitiv rot modulo 11.