Forelesning 14 — torsdag den 2. oktober

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 $3511 \equiv 3 \pmod 4$.

Oppgaver

O4.1 Oppgaver i eksamens stil

Oppgave O4.1.1. Hvilke naturlige tall x slik at $30 \leq x \leq 45$ er primtall?

Oppgave O2.1.2. 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.

O2.2 Oppgaver for å hjelpe med å forstå forelesningen

Oppgave O2.2.1. 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.