Forelesning 15 — torsdag den 9. oktober

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 §1.2, var det både en proposisjon som sa noe om eksistens (Proposisjon 1.2.6) 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 1.2.11 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.

Oppgaver

O4.1 Oppgaver i eksamens stil

Oppgave O1.1.1. 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 O3.1.2. Løs Oppgave 2 i Øving 4 ved å benytte kongruenser istedenfor å benytte divisjonsalgoritmen direkte.

Oppgave O3.1.3. 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 O3.1.4. Finn en invers til 6 modulo 13.

Oppgave O3.1.5. Benytt Fermats lille teorem for å vise at $6^{146} + 2$ er delelig med 19.

Oppgave O3.1.6. La x være et heltall. Anta at $\mathsf{sfd}(x, 21) = 1$. Vis at $8x^6 + 55$ er delelig med 63.

Oppgave O3.1.7. 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.