Forelesning 16 — mandag den 13. oktober

5.1 Kvadratiske kongruenser

Merknad 5.1.1. Fra skolen vet du at en ligning

$$ax^2 + bx + c = 0$$

har 0, 1, eller 2 løsningner. Hvis $\sqrt{b^2 - 4ac} < 0$, har ligningen 0 løsninger. Hvis $\sqrt{b^2 - 4ac} = 0$, har ligningen 1 løsning. Hvis $\sqrt{b^2 - 4ac} > 0$, har ligningen 2 løsninger.

Hvis $\sqrt{b^2 - 4ac} \geq 0$, vet dessuten en formell for å finne disse løsningene:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Imidlertid er disse ligningne ofte ikke heltall. Løsningene til ligningen

$$x^2 - 2 = 0$$

er for eksempel $x = \pm\sqrt{2}$.

I dette kapittelet kommer vi til å se på heltallsløsninger til kongruenser

$$ax^2 + bx + c \equiv 0 \pmod{n}.$$

Terminologi 5.1.2. La n være et heltall slik at $n \neq 0$. La a, b, og c være heltall. La x være et heltall slik at

$$ax^2 + bx + c \equiv 0 \pmod{n}.$$

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

Terminologi 5.1.3. La n være et heltall slik at $n \neq 0$. La a, b, og c være heltall. Når vi er interessert i heltall x som er løsninger til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{n},$$

kalles

$$ax^2 + bx + c \equiv 0 \pmod{n}$$

en *kvadratisk kongruens*.

Merknad 5.1.4. Vi skal fokusere på kongruenser

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

hvor p er et primtall og $p > 2$.

Merknad 5.1.5. Nå har vi blitt fortrolig med algebraiske manipulasjoner med kongruenser. Heretter skal vi derfor gi referansen til proposisjonen eller korollaret i §3.2 som fastslår at en algebraisk manipulasjon vi benytter er gydlig kun når dette er uklart.

Lemma 5.1.6. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

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

Da er det ikke sant at

$$2a \equiv 0 \pmod{p}.$$

Bevis. Anta at

$$2a \equiv 0 \pmod{p}.$$

Fra Proposisjon 3.2.13 har vi da: $p \mid 2a$. Siden p er et primtall, følger det fra Proposisjon 4.2.12 at enten $p \mid 2$ eller $p \mid a$. Imidlertid fastslår følgende observasjoner at verken $p \mid 2$ eller $p \mid a$ er sant.

(1) Siden det ikke er sant at

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

følger det fra Proposisjon 3.2.13 at det ikke er sant at $p \mid a$.

(2) Det eneste primtallet som deler 2 er 2. Siden $p > 2$, er det derfor ikke sant at $p \mid 2$.

Således fører antakelsen at $2a \equiv 0 \pmod{p}$ til en motsigelse. Vi konkluderer at det ikke er sant $2a \equiv 0 \pmod{p}$. □

Lemma 5.1.7. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at

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

Da er det ikke sant at

$$4a \equiv 0 \pmod{p}.$$

Bevis. Siden det ikke er sant at

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

følger det fra Lemma 5.1.6 at det ikke er sant at

$$2a \equiv 0 \pmod{p}.$$

Dermed følger det fra Lemma 5.1.6 at det ikke er sant at

$$2(2a) \equiv 0 \pmod{p},$$

altså at det ikke er sant at

$$4a \equiv 0 \pmod{p}.$$

□

Lemma 5.1.8. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at $a \equiv 0 \pmod{p}$. Da er x en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

hvis og bare hvis x er en løsning til kongruensen

$$(4a)\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Bevis. Anta først at

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Ut ifra Korollar 3.2.45 er da

$$(4a)\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Anta istedenfor at

$$(4a)\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Siden det ikke er sant at

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

følger det fra Lemma 5.1.7 at det ikke er sant at

$$4a \equiv 0 \pmod{p}.$$

Da følger det fra Proposisjon 4.8.28 at

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

□

Proposisjon 5.1.9. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

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

La y være et heltall slik at

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

La x være et heltall slik at

$$2ax \equiv y - b \pmod{p}.$$

Da er

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned}(2ax + b)^2 - (b^2 - 4ac) &= \left(4a^2x^2 + 4abx + b^2\right) - b^2 + 4ac \\ &= 4a\left(ax^2 + bx + c\right).\end{aligned}$$

Dermed er

$$4a\left(ax^2 + bx + c\right) = (2ax + b)^2 - (b^2 - 4ac).$$

(2) Siden

$$2ax \equiv y - b \pmod{p},$$

er

$$2ax + b \equiv y \pmod{p}.$$

Det følger at

$$(2ax+b)^2 - (b^2 - 4ac) \equiv y^2 - (b^2 - 4ac) \pmod{p}.$$

(3) Siden

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

er

$$y^2 - (b^2 - 4ac) \equiv 0 \pmod{p}.$$

Det følger fra (1) – (3) at

$$4a\left(ax^2 + bx + c\right) \equiv 0 \pmod{p}.$$

Ut ifra Lemma 5.1.8 er da

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

□

Eksempel 5.1.10. La oss se på kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Vi har:

$$7^2 - 4 \cdot 1 \cdot 10 = 49 - 40 = 9.$$

La oss således se på kongruensen

$$y^2 \equiv 9 \pmod{11}.$$

Vi har: $y = 3$ er en løsning til denne kongruensen.

La oss da se på kongruensen

$$(2 \cdot 1)x \equiv 3 - 7 \pmod{11},$$

altså kongruensen

$$2x \equiv -4 \pmod{11}.$$

Siden

$$-4 \equiv 7 \pmod{11},$$

er et heltall x er en løsning til denne kongruensen hvis og bare hvis det finnes en løsning til kongruensen

$$2x \equiv 7 \pmod{11}.$$

Siden $x = 9$ er en løsning til denne kongruensen, er derfor $x = 9$ en løsning til kongruensen

$$2x \equiv -4 \pmod{11}.$$

Da fastslår Proposisjon 5.1.9 at $x = 9$ er en løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden

$$9^2 + 7 \cdot 9 + 10 = 81 + 63 + 10 = 154$$

og

$$154 \equiv 0 \pmod{11},$$

er dette riktignok sant.

Eksempel 5.1.11. La oss se på kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

Vi har:

$$6^2 - 4 \cdot 4 \cdot 2 = 36 - 32 = 4.$$

La oss således se på kongruensen

$$y^2 \equiv 4 \pmod{7}.$$

Vi har: $y = 2$ er en løsning til denne kongruensen.

La oss da se på kongruensen

$$(2 \cdot 4)x \equiv 2 - 6 \pmod{7},$$

altså kongruensen

$$8x \equiv -4 \pmod{7}.$$

Siden

$$-4 \equiv 3 \pmod{7}$$

og

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

er et heltall x er en løsning til denne kongruensen hvis og bare hvis det finnes en løsning til kongruensen

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

Siden $x = 3$ er en løsning til denne kongruensen, er derfor $x = 3$ en løsning til kongruensen

$$8x \equiv -4 \pmod{7}.$$

Da fastslår Proposisjon 5.1.9 at $x = 3$ er en løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

Siden

$$4 \cdot (3^2) + 6 \cdot 3 + 2 = 36 + 18 + 2 = 56$$

og

$$56 \equiv 0 \pmod 7,$$

er dette riktignok sant.

Korollar 5.1.12. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

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

La y være et heltall slik at

$$y^2 \equiv b^2 - 4ac \pmod p.$$

La z være et heltall slik at

$$2az \equiv y - b \pmod p.$$

La z' være et heltall slik at

$$2az' \equiv -y - b.$$

Da er $x = z$ og $x = z'$ løsninger til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p.$$

Dersom det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod p,$$

er det ikke sant at

$$z \equiv z' \pmod p.$$

Bevis. Vi gjør følgende observasjoner.

(1) Det følger ummidelbart fra Proposisijon 5.1.9 at $x = z$ er en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p.$$

(2) Siden $(-y)^2 = y^2$ og

$$y^2 \equiv b^2 - 4ac \pmod p,$$

er

$$(-y)^2 \equiv b^2 - 4ac \pmod p.$$

(3) Det følger umiddelbart fra (2) og Proposisjon 5.1.9 at $x = z'$ er en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p.$$

Anta at

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

Da er

$$2az \equiv 2az' \pmod{p}.$$

Det følger at

$$y - b \equiv -y - b \pmod{p},$$

altså at

$$2y \equiv 0 \pmod{p}.$$

Siden $p > 2$, er det, ut ifra Proposisjon 2.5.30, ikke sant at $p \mid 2$, altså er det ikke sant at

$$2 \equiv 0 \pmod{p}.$$

Det følger fra Proposisjon 4.8.28 at

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

Da er

$$y^2 \equiv 0 \pmod{p}.$$

Derfor er

$$b^2 - 4ac \equiv 0 \pmod{p}.$$

Således har vi bevist at, dersom

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

er

$$b^2 - 4ac \equiv 0 \pmod{p}.$$

Vi konkluderer at, dersom det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod{p},$$

er det ikke sant at

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

□

Eksempel 5.1.13. La oss se igjen på kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

I Eksempel 5.1.10 fant vi at $x = 9$ er en løsning til denne kongruensen. Nå skal vi finne en annen løsning.

Ut ifra Eksempel 5.1.10 er $y = 3$ en løsning til kongruensen

$$y^2 \equiv 7^2 - 4 \cdot 1 \cdot 10.$$

Vi fant løsningen $x = 9$ til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}$$

ved å løse kongruensen

$$(2 \cdot 1)x \equiv 3 - 7 \pmod{11}.$$

Korollar 5.1.12 fastlår at vi kan finne en annen løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}$$

ved å løse kongruensen

$$(2 \cdot 1)x \equiv -3 - 7 \pmod{11},$$

altså kongruensen

$$2x \equiv -10 \pmod{11}.$$

Vi har: $x = -5$ er en løsning til denne kongruensen. Derfor er $x = -5$ en løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden

$$-5 \equiv 6 \pmod{11},$$

følger det fra Proposisjon **??** at $x = 6$ er en løsning til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden

$$6^2 + 7 \cdot 6 + 10 = 88$$

og $11 \mid 88$, er dette riktignok sant.

Således har vi: $x = 9$ og $x = 6$ er løsninger til kongruensen

$$x^2 + 7x + 10 \equiv 0 \pmod{11}.$$

Siden $7^2 - 4 \cdot 1 \cdot 10 = 9$, og det ikke er sant at

$$9 \equiv 0 \pmod{11},$$

fastslår i tillegg Korollar 5.1.12 at disse to løsningene ikke er kongruent til hverandre modulo 11. Ut ifra Proposisjon 3.2.11, er dette riktignok sant.

Eksempel 5.1.14. La oss se igjen på kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod{7}.$$

I Eksempel 5.1.11 fant vi at $x = 3$ er en løsning til denne kongruensen. Nå skal vi finne en annen løsning.

Ut ifra Eksempel 5.1.11 er $y = 2$ en løsning til kongruensen

$$y^2 \equiv 6^2 - 4 \cdot 4 \cdot 2.$$

Vi fant løsningen $x = 3$ til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod 7$$

ved å løse kongruensen

$$(2 \cdot 4)x \equiv 2 - 6 \pmod 7.$$

Korollar 5.1.12 fastslår at vi kan finne en annen løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod 7$$

ved å løse kongruensen

$$(2 \cdot 4)x \equiv -2 - 6 \pmod 7,$$

altså kongruensen

$$8x \equiv -8 \pmod 7.$$

Vi har: $x = -1$ er en løsning til denne kongruensen. Derfor er $x = -1$ en løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod 7.$$

Siden

$$-1 \equiv 6 \pmod 7,$$

følger det fra Proposisjon **??** at $x = 6$ er en løsning til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod 7.$$

Siden

$$4 \cdot 6^2 + 6 \cdot 6 + 2 = 182$$

og $7 \mid 182$, er dette riktignok sant.

Således har vi: $x = 3$ og $x = 6$ er løsninger til kongruensen

$$4x^2 + 6x + 2 \equiv 0 \pmod 7.$$

Siden $6^2 - 4 \cdot 4 \cdot 2 = 4$, og det ikke er sant at

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

fastslår i tillegg Korollar 5.1.12 at disse to løsningene ikke er kongruent til hverandre modulo 7. Ut ifra Proposisjon 3.2.11, er dette riktignok sant.

Terminologi 5.1.15. La a, b, og c være heltall. Heltallet $b^2 - 4ac$ kalles *diskriminanten* til a, b, og c.

Notasjon 5.1.16. La a, b, og c være heltall. Diskriminanten til a, b, og c betegnes ofte som Δ, det greske bokstavet som tilsvarer til bokstavet «d».

Merknad 5.1.17. La p være et primtall slik at $p > 2$. Proposisjon 5.1.9 gir muligheten til å gjøre enklere teorien til kvadratisk kongruenser modulo p. Tidligere i kurset har vi rukket en veldig god forståelse for hvordan løse lineære kongruenser. Dermed forstår vi hvordan kongruensen

$$2ax \equiv y - c \pmod{p}$$

i Proposisjon 5.1.9 kan løses.

For å finne en løsning til en hvilken som helst kvadratisk kongruens, fastslår således Proposisjon 5.1.9 at vi kan fokusere på kongruenser

$$y^2 \equiv \Delta \pmod{p},$$

hvor Δ er et heltall.

Merknad 5.1.18. Sammenlign Proposisjon 5.1.9 med formellen for løsningene til en kvadratisk ligning som du kjenner til fra skolen, nevnt i Merknad 5.1.1. Å si at

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

er det samme som å si at x er en løsning til ligningen

$$2ax = y - b,$$

hvor y er én av de to mulige løsningene til ligningen

$$y^2 = b^2 - 4ac,$$

det vil si enten

$$y = \sqrt{b^2 - 4ac}$$

eller

$$y = -\sqrt{b^2 - 4ac}.$$

Proposisjon 5.1.9 og Korollar 5.1.12 sier at vi kan finne en løsning til en kvadratisk kongruens modulo p på akkurat den samme måten. Den eneste forskjellen er at vi ikke alltid kan ta kvadratroten av et heltall og få et heltall. Med andre ord er det ikke så lett å løse kongruensen

$$y^2 \equiv b^2 - 4ac \pmod{p}$$

som å løse ligningen

$$y^2 = b^2 - 4ac,$$

fordi vi er kun interessert i heltallsløsninger til kongruenser. Dermed må vi studere når i modulær aritmetikk et heltall «har en kvadratrot» som er et heltall. La oss begunne med dette med en gang!

5.2 Kvadratiske rester

Definisjon 5.2.1. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at
$$a \equiv 0 \pmod{p}.$$
Da er a en *kvadratisk rest* modulo p dersom det finnes et heltall x slik at
$$x^2 \equiv a \pmod{p}.$$

Eksempel 5.2.2. Siden $3^2 = 9$ og
$$9 \equiv 2 \pmod{7},$$
er 2 en kvadratisk rest modulo 7.

Eksempel 5.2.3. Siden $4^2 = 16$ og
$$16 \equiv 5 \pmod{11},$$
er 5 en kvadratisk rest modulo 11.

Merknad 5.2.4. Å si at a er en kvadratisk rest modulo p er det samme som å si: «a har en kvadratrot modulo p».

Proposisjon 5.2.5. La p være et primtall slik at $p > 2$. La a være et heltall slik at det ikke er sant at
$$a \equiv 0 \pmod{p}.$$
Da er a en *kvadratisk rest* modulo p hvis og bare hvis det finnes et heltall r slik at $1 \leq r \leq p-1$ og
$$r^2 \equiv a \pmod{p}.$$

Bevis. Anta først at det finnes et heltall r slik at $1 \leq r \leq p-1$ og
$$r^2 \equiv a \pmod{p}.$$
Da er a en kvadratisk rest modulo p: la x være r i Definisjon 5.2.1.

Anta istedenfor at a er en kvadratisk rest modulo p. Da finnes det et heltall x slik at
$$x^2 \equiv a \pmod{p}.$$
Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at $0 \leq r \leq p-1$ og
$$x \equiv r \pmod{p}.$$
Anta først at $r = 0$. Da er
$$x \equiv 0 \pmod{p}.$$

Dermed er

$$x^2 = 0 \pmod{p}.$$

Siden

$$x^2 \equiv a \pmod{p},$$

følger det at

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

Imidlertid har vi antatt at dette ikke er sant. Siden antakelsen at $r = 0$ fører til denne motsigelsen, deduserer vi at det ikke er sant at $r = 0$. Dermed er $1 \leq r \leq p - 1$.

Siden

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

er

$$x^2 \equiv r^2 \pmod{p}.$$

Siden

$$x^2 \equiv a \pmod{p},$$

følger det at

$$r^2 \equiv a \pmod{p}.$$

□

Eksempel 5.2.6. Siden $7^2 = 49$ og

$$49 \equiv 4 \pmod{5},$$

er 4 en kvadratisk rest modulo 5. Proposisjon 5.2.5 fastslår at det da er et heltall r slik at:

(1) $1 \leq r \leq 4$;

(2) $7 \equiv r \pmod{5}$;

(3) $r^2 \equiv 4 \pmod{5}$.

Dette er riktignok sant: vi kan velge r til å være 2.

Eksempel 5.2.7. Siden $17^2 = 289$ og

$$289 \equiv 3 \pmod{11},$$

er 3 en kvadratisk rest modulo 11. Proposisjon 5.2.5 fastslår at det da er et heltall r slik at:

(1) $1 \leq r \leq 10$;

(2) $17 \equiv r \pmod{11}$;

(3) $r^2 \equiv 3 \pmod{11}$.

Dette er riktignok sant: vi kan velge r til å være 6.

Proposisjon 5.2.8. La p være et primtall slik at $p > 2$. 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 da et heltall r slik at $1 \leq r \leq p-1$ og
$$a \equiv r \pmod{p}.$$
Da er a en kvadratisk rest modulo p hvis og bare hvis r er en kvadratisk rest modulo p.

Bevis. Siden
$$a \equiv r \pmod{p},$$
finnes det et heltall x slik at
$$x^2 \equiv a \pmod{p}$$
hvis og bare hvis det finnes et heltall x slik at
$$x^2 \equiv r \pmod{p}.$$
□

Eksempel 5.2.9. Siden $6^2 = 36$ er 36 en kvadratisk rest modulo et hvilket helst primtall p slik at $p > 2$. Siden
$$36 \equiv 1 \pmod{5},$$
fastslår Proposisjon 5.2.8 at 1 er kvadratisk rest modulo 5.

Siden
$$36 \equiv 3 \pmod{11},$$
fastslår Proposisjon 5.2.8 at 3 er kvadratisk rest modulo 11.

Siden
$$36 \equiv 2 \pmod{17},$$
fastslår Proposisjon 5.2.8 at 2 er kvadratisk rest modulo 17.

Eksempel 5.2.10. Siden $8^2 = 64$ er 64 en kvadratisk rest modulo et hvilket helst primtall p slik at $p > 2$. Siden
$$64 \equiv 4 \pmod{5},$$
fastslår Proposisjon 5.2.8 at 4 er kvadratisk rest modulo 5.

Siden
$$64 \equiv 1 \pmod{7},$$
fastslår Proposisjon 5.2.8 at 1 er kvadratisk rest modulo 7.

Siden
$$64 \equiv 9 \pmod{11},$$
fastslår Proposisjon 5.2.8 at 9 er kvadratisk rest modulo 11.

Merknad 5.2.11. La oss avgjøre hvilke heltall er kvadratiske rester modulo noen bestemte primtall. Det følger fra Proposisjon 5.2.5 og Proposisjon 5.2.8 at det er nok å gå gjennom heltallene 1^2, 2^2, ..., $(p-1)^2$ og sjekke hvilke heltall blant 1, 2, ..., $p-1$ de er kongruent til modulo p.

Eksempel 5.2.12. La p være 3. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 2$ og $x^2 \equiv r \pmod 3$
1	1	1
2	4	1

Dermed er 1 en kvadratisk rest modulo 3, og enhver annen kvadratisk rest modulo 3 er kongruent til 1 modulo 3.

Eksempel 5.2.13. La p være 5. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 4$ og $x^2 \equiv r \pmod 5$
1	1	1
2	4	4
3	9	4
4	16	1

Dermed er 1 og 4 kvadratiske rester modulo 5, og enhver annen kvadratisk rest modulo 5 er kongruent til enten 1 eller 4 modulo 5.

Eksempel 5.2.14. La p være 7. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 6$ og $x^2 \equiv r \pmod 7$
1	1	1
2	4	4
3	9	2
4	16	2
5	25	4
6	36	1

Dermed er 1, 2, og 4 kvadratiske rester modulo 7, og enhver annen kvadratisk rest modulo 7 er kongruent til én av disse tre naturlige tallene modulo 7.

Eksempel 5.2.15. La p være 11. Vi regner som følger.

x	x^2	r slik at $1 \leq r \leq 10$ og $x^2 \equiv r \pmod{11}$
1	1	1
2	4	4
3	9	9
4	16	5
5	25	3
6	36	3
7	49	5
8	64	9
9	81	4
10	100	1

Dermed er 1, 3, 4, 5, og 9 kvadratiske rester modulo 11, og enhver annen kvadratisk rest modulo 11 er kongruent til én av disse fem naturlige tallene modulo 11.

Merknad 5.2.16. Følgende proposisjon er motsatt til Proposisjon 5.1.9.

Proposisjon 5.2.17. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. La x være en løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}.$$

La $y = 2ax + b$. Da er y en løsning til kongruensen

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

Bevis. Vi regner som følger.

$$\begin{aligned} y^2 &= (2ax + b)^2 \\ &= 4a^2x^2 + 4abx + b^2 \\ &= b^2 + 4a\left(ax^2 + bx\right) \\ &= b^2 + 4a\left(ax^2 + bx + c - c\right) \\ &= b^2 + 4a\left(ax^2 + bx + c\right) - 4ac. \end{aligned}$$

Siden

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

er

$$b^2 + 4a\left(ax^2 + bx + c\right) - 4ac \equiv b^2 - 4ac \pmod{p}.$$

Dermed er

$$y^2 \equiv b^2 - 4ac \pmod{p}.$$

□

Eksempel 5.2.18. Siden

$$2 \cdot \left(5^2\right) - 5 + 4 = 49$$

og

$$49 \equiv 0 \pmod 7,$$

er $x = 5$ en løsning til kongruensen

$$2x^2 - x + 4 \equiv 0 \pmod 7.$$

Da fastslår Proposisjon 5.2.17 at $y = 2 \cdot 2 \cdot 5 + (-1)$, altså $y = 19$, er en løsning til kongruensen

$$y^2 \equiv (-1)^2 - 4 \cdot 2 \cdot 4 \pmod 7,$$

altså til kongruensen

$$y^2 \equiv -31 \pmod 7.$$

Siden

$$19 \equiv 5 \pmod 7,$$

, er

$$y^2 \equiv 25 \equiv 4 \pmod 7.$$

I tillegg har vi:

$$-31 \equiv 4 \pmod 7.$$

Dermed er det riktignok sant at

$$19^2 \equiv -31 \pmod 7.$$

Eksempel 5.2.19. Siden

$$3 \cdot \left(4^2\right) + 7 \cdot 4 + 1 = 77$$

og

$$77 \equiv 0 \pmod{11},$$

er $x = 3$ en løsning til kongruensen

$$3x^2 + 7x + 1 \equiv 0 \pmod{11}.$$

Da fastslår Proposisjon 5.2.17 at $y = 2 \cdot 3 \cdot 4 + 7$, altså $y = 31$, er en løsning til kongruensen

$$y^2 \equiv 7^2 - 4 \cdot 3 \cdot 1 \pmod{11},$$

altså til kongruensen

$$y^2 \equiv 37 \pmod{11}.$$

Siden

$$31 \equiv -2 \pmod{11},$$

, er

$$y^2 \equiv 4 \pmod{11}.$$

I tillegg har vi:

$$37 \equiv 4 \pmod{11}.$$

Dermed er det riktignok sant at

$$31^2 \equiv 37 \pmod{11}.$$

Lemma 5.2.20. La p være et primtall slik at $p > 2$. La a og b være heltall. Anta at det ikke er sant at

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

Da har kongruensen

$$2ax \equiv y - b \pmod{p}$$

en løsning for et hvilket som helst heltall y.

Bevis. Siden det ikke er sant at

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

følger det fra Lemma 5.1.6 at det ikke er sant at

$$2a \equiv 0 \pmod{p}.$$

Fra Proposisjon 3.2.13 deduserer vi at det ikke er sant at $p \mid 2a$. Da følger det fra Proposisjon 4.2.28 at kongruensen

$$2ax \equiv y - b \pmod{p}$$

har en løsning når $y - b$ er et hvilket som helst heltall, altså når y er et hvilket som helst heltall. □

Eksempel 5.2.21. Siden det ikke er sant at

$$5 \equiv 0 \pmod{3},$$

fastslår Lemma 5.2.20 at kongruensen

$$10x \equiv y - 6 \pmod{3}$$

har en løsning for et hvilket som helst heltall y. Når for eksempel $y = 2$, er det riktignok sant at $x = 2$ er en løsning til kongruensen

$$10x \equiv -4 \pmod{3}.$$

Når for eksempel $y = 6$, er det riktignok sant at $x = 0$ er en løsning til kongruensen

$$10x \equiv 0 \pmod{3}.$$

Når for eksempel $y = 19$, er $x = 1$ en løsning til kongruensen

$$10x \equiv 13 \pmod{3}.$$

Korollar 5.2.22. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

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

Da har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

en løsning om og bare om $b^2 - 4ac$ er en kvadratisk rest modulo p.

Bevis. Anta først at kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

har en løsning. Da følger det fra Proposisjon 5.2.17 at $b^2 - 4ac$ er en kvadratisk rest modulo p.

Anta istedenfor at $b^2 - 4ac$ er en kvadratisk rest modulo p. Vi gjør følgende observasjoner.

(1) Ut ifra Lemma 5.2.20, har kongruensen

$$2ax \equiv y - b \pmod{p}$$

en løsning for et hvilket som helst heltall y.

(2) Siden det ikke er sant at

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

følger det fra Lemma 5.1.6 at det ikke er sant at

$$4a \equiv 0 \pmod{p}.$$

Det følger fra (1), (2), og Proposisjon 5.1.9 at, dersom $b^2 - 4ac$ er en kvadratisk rest modulo p, altså finnes det et heltall y slik at

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

en løsning. □

Terminologi 5.2.23. Med andre ord har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

en løsning hvis og bare hvis $b^2 - 4ac$ «har en kvadratiskrot» som er et heltall modulo p.

Eksempel 5.2.24. La oss se på kongruensen

$$3x^2 + 5x + 4 \equiv 0 \pmod 7.$$

Vi har:

$$5^2 - 4 \cdot 4 \cdot 3 = 25 - 48 = -23,$$

og

$$-23 \equiv 5 \pmod 7.$$

Imidlertid vet vi fra Eksempel 5.2.14 at 5 ikke er an kvadratisk rest modulo 7. Da følger det fra Proposisjon 5.2.17 at kongruensen

$$3x^2 + 5x + 4 \equiv 0 \pmod 7$$

har ingen løsning.

Eksempel 5.2.25. La oss se på kongruensen

$$2x^2 - 3x - 7 \equiv 0 \pmod{11}.$$

Vi har:

$$(-3)^2 - 4 \cdot 2 \cdot (-7) = 9 + 56 = 65,$$

og

$$65 \equiv 10 \pmod{11}.$$

Imidlertid vet vi fra Eksempel 5.2.15 at 10 ikke er an kvadratisk rest modulo 11. Da følger det fra Proposisjon 5.2.17 at kongruensen

$$2x^2 - 3x - 7 \equiv 11 \pmod 7$$

har ingen løsning.

Merknad 5.2.26. I Merkand 5.1.18 lot vi merke til at finnes noen likheter mellom teorien for kvadratiske ligninger og teorien for kvadratiske kongruenser. Nå skal vi nærmere å disse likhetene.

Lemma 5.2.27. La p være et primtall. La y være et heltall slik at

$$y^2 \equiv 0 \pmod p.$$

Da er

$$y \equiv 0 \pmod p.$$

Bevis. Siden

$$y^2 \equiv 0 \pmod p,$$

har vi: $p \mid y^2$. Siden p er et primtall, følger det fra Proposisjon 4.2.12 at $p \mid y$. Dermed er

$$y \equiv 0 \pmod p.$$

□

Eksempel 5.2.28. Siden

$$64 \equiv 0 \pmod{2},$$

er $y = 8$ en løsning til kongruensen

$$y^2 \equiv 0 \pmod{2}.$$

Lemma 5.2.27 fastslår da at

$$8 \equiv 0 \pmod{2}.$$

Dette er riktignok sant.

Eksempel 5.2.29. Siden

$$81 \equiv 0 \pmod{3},$$

er $y = 9$ en løsning til kongruensen

$$y^2 \equiv 0 \pmod{3}.$$

Lemma 5.2.27 fastslår da at

$$9 \equiv 0 \pmod{3}.$$

Dette er riktignok sant.

Korollar 5.2.30. La p være et primtall slik at $p > 2$. La a, b, og c være heltall. Anta at det ikke er sant at

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

Da er følgende sanne.

(A) Dersom $b^2 - 4ac$ ikke er en kvadratisk rest modulo p, har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

ingen løsning.

(B) Dersom

$$b^2 - 4ac \equiv 0 \pmod{p},$$

har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

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

(C) Dersom $b^2 - 4ac$ er en kvadratisk rest modulo p, og det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod{p},$$

har kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

to løsninger som ikke er kongruent til hverandre modulo p, og slik at enhver annen løsning til kongruensen er kongruent til én av disse to modulo p.

Bevis. Dersom b^2-4ac ikke er en kvadratisk rest modulo p, følger det fra Korollar 5.2.22 at kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p$$

ikke har en løsning. Dermed er (A) sant.

Anta nå at

$$b^2 - 4ac \equiv 0 \pmod p.$$

Da er $y = 0$ en løsning til kongruensen

$$y^2 \equiv b^2 - 4ac \pmod p,$$

altså b^2-4ac er en kvadratisk rest modulo p. Det følger fra Korollar 5.2.22 at kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p$$

har en løsning.

La z være et heltall slik at

$$az^2 + bz + c \equiv 0 \pmod p.$$

La z' være et heltall slik at

$$a(z')^2 + bz' + c \equiv 0 \pmod p.$$

Ut ifra antakelesen at

$$b^2 - 4ac \equiv 0 \pmod p,$$

følger det fra Proposisjon 5.2.17 at

$$(2az + b)^2 \equiv 0 \pmod p$$

og

$$(2az' + b)^2 \equiv 0 \pmod p.$$

Ut ifra Lemma 5.2.27 er da

$$2az + b \equiv 0 \pmod p$$

og

$$2az' + b \equiv 0 \pmod p.$$

Med andre ord er både $x = z$ og $x = z'$ løsninger til kongruensen

$$2ax = -b \pmod p.$$

Da følger det fra Proposisjon 4.2.28 at

$$z \equiv z' \pmod p.$$

Dermed har vi bevist at, dersom

$$b^2 - 4ac \equiv 0 \pmod p,$$

er følgende sanne:

(1) kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

har en løsning;

(2) alle løsningene til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

er kongruent til hverandre modulo p.

Således er (B) sant.

Anta nå at $b^2 - 4ac$ er en kvadratisk rest modulo p, og at det ikke er sant at

$$b^2 - 4ac \equiv 0 \pmod{p}.$$

Ut ifra Korollar 5.1.12 er da både $x = z$ og $x = z'$ løsninger til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

og det er ikke sant at

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

Det følger fra Proposisjon **??** at enhver annen løsning til kongruensen

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

er kongruent modulo p til enten z eller z'. Således er (C) sant. □

Eksempel 5.2.31. La oss se på kongruensen

$$3x^2 - 2x + 2 \equiv 0 \pmod{5}.$$

Vi har:

$$(-2)^2 - 4 \cdot 3 \cdot 2 = 4 - 24 = -20$$

og

$$-20 \equiv 0 \pmod{5}.$$

Derfor er $y = 0$ en løsning til kongruensen

$$y^2 \equiv (-2)^2 - 4 \cdot 3 \cdot 2 \pmod{5}.$$

Vi har: $x = 2$ er en løsning til kongruensen

$$6x \equiv 2 \pmod{5},$$

altså til kongruensen

$$(2 \cdot 3)x \equiv 0 - (-2) \pmod{5}.$$

Det følger fra Proposisjon 5.1.9 at $x = 2$ er en løsning til kongruensen

$$3x^2 - 2x + 2 \equiv 0 \pmod 5.$$

Siden

$$(-2)^2 - 4 \cdot 3 \cdot 2 \equiv 0 \pmod 5,$$

fastslår Korollar 5.2.30 (B) at alle løsningene til kongruensen

$$3x^2 - 2x + 2 \equiv 0 \pmod 5$$

er kongruent til 2 modulo 5.

Eksempel 5.2.32. La oss se på kongruensen

$$5x^2 + 3x + 3 \equiv 0 \pmod 7.$$

Vi har:

$$3^2 - 4 \cdot 5 \cdot 3 = 9 - 60 = -51$$

og

$$-51 \equiv 5 \pmod 7.$$

Ut ifra Eksempel 5.2.14 er 5 ikke en kvadratisk rest modulo 7. Da fastslår Korollar 5.2.30 (A) at kongruensen

$$5x^2 + 3x + 3 \equiv 0 \pmod 7$$

har ingen løsning.

Eksempel 5.2.33. La oss se på kongruensen

$$6x^2 + 2x + 5 \equiv 0 \pmod{11}.$$

Vi har:

$$2^2 - 4 \cdot 6 \cdot 5 = 4 - 120 = -116$$

og

$$-116 \equiv 5 \pmod{11}.$$

Vi har: $y = 4$ er en løsning til kongruensen

$$y^2 \equiv 5 \pmod{11}.$$

Vi har: $x = 2$ er en løsning til kongruensen

$$12x \equiv 2 \pmod{11},$$

altså til kongruensen

$$(2 \cdot 6)x \equiv 4 - 2 \pmod{11}.$$

I tillegg har vi: $x = 5$ er en løsning til kongruensen

$$12x \equiv -6 \pmod{11},$$

altså til kongruensen

$$(2 \cdot 6)x \equiv -4 - 2 \pmod{11}.$$

Da fastslår Korollar 5.1.12 at $x = 2$ og $x = 5$ er løsninger til kongruensen

$$6x^2 + 2x + 5 \equiv 0 \pmod{11}$$

som ikke er kongruent modulo 11 til hverandre.

Siden det ikke er sant at

$$5 \equiv 0 \mod 11,$$

fastslår Korollar 5.2.30 (C) at enhver annen løsning til kongruensen

$$6x^2 + 2x + 5 \equiv 0 \pmod{11}$$

er kongruent modulo 11 til én av disse to.

Merknad 5.2.34. La oss oppsummere. La p være et primtall slik at $p > 2$. Korollar 5.2.30 fastslår at diskriminanten avgjør hvor mange løsninger en kvadratisk kongruens modulo p har, akkurat som diskriminanten avgjør hvor mange løsninger en kvadratisk ligning her. Det vil si følgende.

(A) Dersom diskriminanten ikke er en kvadratisk rest modulo p, har kongruensen ingen løsning. Med andre ord, dersom diskriminanten ikke har en ≪kvadratrot≫ modulo p, har kongruensen ingen løsning.

(B) Dersom diskriminanten er 0, finnes det akkurat én løsning til kongruensen fra synspunktet av aritmetikk modulo p, altså enhver annen løsning er kongruent modulo p til denne løsningen.

(C) Dersom diskriminanten har en kvadratisk rest og ikke er 0, finnes det akkurat to løsninger til kongruensen fra synspunktet av aritmetikk modulo p, altså disse to løsningenen ikke er kongruent til hverandre modulo p, og enhver annen løsning er kongruent modulo p til én av disse to.

I tillegg fastslår Proposisjon 5.1.9 og Korollar 5.1.12 at, i tilfeller (B) og (C), *finnes* løsningene på en tilsvarende måte som løsningene til en kvadratisk ligning finnes når diskriminanten er 0, og når diskriminanten er større enn 0.

Oppgaver

O5.1 Oppgaver i eksamens stil

Oppgave O5.1.1. Gjør følgende.

(1) Vis at 12 er en kvadratisk rest modulo 13.

(2) Benytt (1) for å finne en løsning til kongruensen

$$3x^2 + 7x - 11 \equiv 0 \pmod{13}.$$

Oppgave O5.1.2. Har kongruensen

$$4x^2 + 2x + 1 \equiv 0 \pmod{5}$$

en løsning?