9.1 Eulers kriterium

Problem: Gitt en kongruens $ax^2+bx+c \equiv 0 \pmod p$ hvor p er prim, er den løsbar? Hvis ja, finn alle løsn.

Merk: (1) Vi antar pta, for hvis ikke er det jo kongruensen $bx+c \equiv 0 \pmod p$, som er lineær.

(2) $p=2$: lett å løse

(3) Fra (1) og (2) kan vi anta at p er odde og at pta. Da kan problemet reduseres (se bok) til følgende problem:

Problem: Løs kongruenser på formen

$$x^2 \equiv a \pmod p$$

Merk: (1) Hvis pla blir kongruensen $x^2 \equiv 0 \pmod p$, som er ekv med $x \equiv 0 \pmod p$, dvs $p \mid x$. Så vi antar pta.

(2) Hvis x_0 er en løsn av $x^2 \equiv a \pmod p$, så er også $p-x_0$ en løsn (sjekk dette), og $x_0 \not\equiv p-x_0 \pmod p$ (sjekk dette også). Så x_0 og $p-x_0$ er to inkongr. løsn. Fra Lagranges teorem er da x_0 og $p-x_0$ alle løsningene modulo p

(3) Hvis pta a kongr modulo p med ett av tallene $\{1,2,\dots,p-1\}$. Så vi reduserer til følgende problem:

Problem: For hvilke $a \in \{1,2,\dots,p-1\}$ er kongr

$$x^2 \equiv a \pmod p$$

løsbar? Hvis løsbar, finn løsn.

Eksempel: Ta $p=5$. For hvilke $a \in \{1,2,3,4\}$ er $x^2 \equiv a \pmod 5$ løsbar?

$x^2 \equiv 1 \pmod 5 \longrightarrow 1$ og $5-1=4$ er løsn

$x^2 \equiv 2 \pmod 5 \longrightarrow$ ikke løsbar

$x^2 \equiv 3 \pmod 5 \longrightarrow$ ikke løsbar

$x^2 \equiv 4 \pmod 5 \longrightarrow 2$ og $5-2=3$ er løsn.

Merk: (1) For å sjekke om $x^2 \equiv a \pmod p$ er løsbar, trenger vi bare å sjekke om $x = 1,2,\dots,p-1$ er en løsn.

(2) Eksempelet antyder at for halvparten av alle $a \in \{1,\dots,p-1\}$ er $x^2 \equiv a \pmod p$ løsbar, og for halvparten ikke løsbar. Slik er det, skal se.

Def: La p være et odde primtall og a et tall med $p \nmid a$. Da er a en kvadratisk rest av p dersom

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

er løsbar.

Eksempel: 1 og 4 er kv. rester av $p=5$. Det samme er da alle $a \in \mathbb{Z}$ med $a \equiv 1, 4 \pmod 5$. Tallene 2, 3 er ikke kv.-rester, så det er heller ikke $a \in \mathbb{Z}$ med $a \equiv 2, 3 \pmod 5$.

Teorem 9.1 (Eulers kriterium)

La p være et odde primtall og $a \in \mathbb{Z}$ et tall med $p \nmid a$. Da gjelder

$$a \text{ kv. rest av } p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Bevis: Anta a er en kv.-rest, dvs $\exists\, x_0$ med $x_0^2 \equiv a \pmod p$. Siden $p \nmid a$ har vi $p \nmid x_0$ (sjekk), så Fermats teorem gir $x_0^{p-1} \equiv 1 \pmod p$. Det gir

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod p.$$

Anta motsatt at $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Fra Seksjon 8.2 vet vi at det finnes en primitiv rot b av p, dvs $b^{p-1} \equiv 1 \pmod p$ og $p-1$ er den minste eksponenten k med $b^k \equiv 1 \pmod p$. Fra Seksjon 8.1 er de $p-1$ tallene

$$b, b^2, \ldots, b^{p-1}$$

inkongr modulo p, så de må representere alle tall som ikke er delelig med p. Derfor er

$$a \equiv b^t \pmod p$$

for en $t \in \{1, 2, \ldots, p-1\}$. Har nå

$$1 \equiv a^{\frac{p-1}{2}} \equiv (b^t)^{\frac{p-1}{2}} \equiv b^{\frac{t(p-1)}{2}} \pmod p$$

så fra Seksjon 8.1 må da $p-1$ dele $\frac{t(p-1)}{2}$. Da må $2 \mid t$ (sjekk), så $t = 2m$ for en $m \geq 1$. Har da

$$(b^m)^2 \equiv b^{2m} \equiv b^t \equiv a \pmod p$$

så $x_0 = b^m$ er en løsn av $x^2 \equiv a \pmod p$. □

Korollar Samme forutsetn som før:

$$a \text{ kv rest av } p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

$$a \text{ ikke kv rest av } p \iff a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Bevis: Siden $p \nmid a$ gir Fermat at $a^{p-1} \equiv 1 \pmod p$, dvs p deler $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$. Men da må p dele en av faktorene, så en av kongruensene

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p, \quad a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

må gjelde. Ikke begge kan gjelde samtidig (hvorfor?) □

Eksempel: (1) For $p=5$ så vi at 1 og 4 er kv. rester, mens 2 og 3 ikke er det.

$$1^{\frac{5-1}{2}} \equiv 1 \pmod 5$$
$$2^{\frac{5-1}{2}} = 2^2 \equiv -1 \pmod 5$$
$$3^{\frac{5-1}{2}} = 3^2 \equiv -1 \pmod 5$$
$$4^{\frac{5-1}{2}} \equiv 4^2 \equiv 1 \pmod 5$$

(2) For $p=7$ er $\frac{p-1}{2} = 3$, så vi får

$$1^3 \equiv 1 \pmod 7$$
$$2^3 \equiv 8 \equiv 1 \pmod 7$$
$$3^3 \equiv 27 \equiv -1 \pmod 7$$
$$4^3 \equiv (-3)^3 \equiv -27 \equiv 1 \pmod 7$$
$$5^3 \equiv (-2)^3 \equiv -8 \equiv -1 \pmod 7$$
$$6^3 \equiv (-1)^3 \equiv -1 \pmod 7$$

Det betyr at 1, 2, 4 er kvadratiske rester av 7, mens 3, 5, 6 ikke er det.