# 4.4 Lineære kongruenser

Def: En <u>lineær kongruens</u> er en kongruensligning på form

$$ax \equiv b \pmod{n}$$

hvor $x$ er ukjent. En løsning er et tall $x_0 \in \mathbb{Z}$ med $ax_0 \equiv b \pmod{n}$

Eksempler: (1) Kongruensen $14x \equiv 10 \pmod{6}$ er løsbar. En løsning er $x_0 = 2$ siden $14 \cdot 2 \equiv 10 \pmod{6}$ fordi $6 \mid (28-10)$. En annen løsning er $x_1 = 5$ siden $14 \cdot 5 \equiv 10 \pmod{6}$ fordi $6 \mid (70-10)$. Merk at $x_0 \not\equiv x_1 \pmod{6}$, så $x_0$ og $x_1$ er to inkongruente løsn av denne lineære kongruensen. Skal se at disse to løsn representerer alle løsn.

(2) Er kongruensen $14x \equiv 5 \pmod{6}$ løsbar? Hvis ja, så finnes $x_0 \in \mathbb{Z}$ med $14x_0 \equiv 5 \pmod{6}$, dvs $6 \mid (14x_0 - 5)$. Da er $14x_0 - 5 = 6y_0$ for en $y_0 \in \mathbb{Z}$, som gir

$$14x_0 - 6y_0 = 5$$

Siden $\gcd(14,6) = 2$ og $2 \nmid 5$, er dette umulig fra teorien om diofantiske ligninger.

Merk: Anta $ax \equiv b \pmod{n}$ er løsbar, og at $x_0$ er en løsning. Da er alle $z \in \mathbb{Z}$ med $x_0 \equiv z \pmod{n}$ også en løsn. For hvis $x_0 \equiv z \pmod{n}$ er $ax_0 \equiv az \pmod{n}$, og siden $ax_0 \equiv b \pmod{n}$ er da $az \equiv b \pmod{n}$. Det betyr at en løsn $x_0$ representerer uendelig mange løsn av kongruensen, nemlig alle $z$ med $z \equiv x_0 \pmod{n}$, dvs alle

$$x_0 + nt \qquad t \in \mathbb{Z}$$

($z \equiv x_0 \pmod{n} \iff z - x_0 = nt \iff z = x_0 + nt$ for en $t \in \mathbb{Z}$).

Når vi løser en lineær kongruens $ax \equiv b \pmod{n}$, søker vi kun inkongruente løsninger.

Eksempel: Vi så at $x_0 = 2$ og $x_1 = 5$ er to løsn av $14x \equiv 10 \pmod{6}$. Dette er to inkongruente løsn siden $2 \not\equiv 5 \pmod{6}$. Skal se at disse representerer alle løsn. Dvs

$z$ er en løsn $\iff z \equiv 2 \pmod{6}$ eller $z \equiv 5 \pmod{6}$

**Teorem 4.7** Den lineære kongruensen

$$ax \equiv b \pmod{n}$$

er løsbar hvis og bare hvis $\gcd(a,n)$ deler $b$. Hvis $x_0$ er en løsn, så vil de $d$ tallene

$$x_0,\ x_0 + n/d,\ x_0 + 2n/d,\ \dots,\ x_0 + (d-1)n/d$$

representere alle de inkongruente løsn, hvor $d = \gcd(a,n)$.

Bevis: Den er løsbar hvis og bare hvis $\exists\, x_0 \in \mathbb{Z}$ med $ax_0 \equiv b \pmod{n}$, dvs $ax_0 - b = ny_0$ for en $y_0 \in \mathbb{Z}$. Dette skjer hvis og bare hvis den diof. lign $ax - ny = b$ er løsbar, som igjen skjer hvis og bare hvis $ax + ny = b$ er løsbar. Det vet vi skjer hvis og bare hvis $\gcd(a,n)$ deler $b$.

Anta $x_0$ er en løsn, og la $d = \gcd(a,n)$. Da er $x_0 + tn/d$ en løsn for alle $t \in \mathbb{Z}$. Hvorfor? Siden $d$ la er $a = kd$ for en $k$, og siden $ax_0 \equiv b \pmod{n}$ er $ax_0 - b = ny_0$ for en $y_0$. Da får vi

$$a(x_0 + tn/d) - b = (ax_0 - b) + atn/d = ny_0 + kdtn/d = n(y_0 + kt)$$

som betyr at $a(x_0 + tn/d) \equiv b \pmod{n}$. Så $x_0 + tn/d$ er en løsn. Se bok for hvorfor de $d$ tallene

$$x_0,\ x_0 + n/d,\ \dots,\ x_0 + (d-1)n/d$$

er inkongruente modulo $n$, og representerer alle løsn.

Merk: Det at $x_0, x_0 + n/d, \dots, x_0 + (d-1)n/d$ representerer alle løsn betyr at $z$ er en løsn av $ax \equiv b \pmod{n}$ hvis og bare hvis $z \equiv x_0 + tn/d \pmod{n}$ for en $0 \le t \le d-1$.

Strategi: For å løse $ax \equiv b \pmod{n}$:

(1) Finn en løsn $(x_0, y_0)$ av den diof. lign

$$ax + ny \equiv b$$

(2) Da vil

$$x_0,\ x_0 + n/d,\ \dots,\ x_0 + (d-1)n/d$$

representere alle de inkongruente løsn. Skriver da

$$x \equiv x_0, x_0 + n/d, \dots, x_0 + (d-1)n/d \pmod{n}$$

Eksempel: $6X \equiv 15 \pmod{33}$ er løsbar fordi $\gcd(6,33)=3$ og $3 \mid 15$.

Finner en løsn av $6X+33y=15$ v.ha. Euklids alg:

$33 = 5\cdot 6 + 3$ → $3 = 6\cdot(-5)+33\cdot 1$

$6 = 2\cdot 3$ → $\Rightarrow 15 = 5\cdot 3 = 6\cdot(-25)+33\cdot 5$

Så $x_0 = -25$, $y_0 = 5$ er en løsn.

Får 3 inkongruente løsn:

$$-25,\ -25+{}^{33}/_{3},\ -25+{}^{2\cdot 33}/_{3}$$

Så $X \equiv -25, -14, -3 \pmod{33}$

<u>Korollar</u> Hvis $\gcd(a,n)=1$ så har $aX \equiv b \pmod n$ kun én løsn modulo $n$.

Eksempel: $9X \equiv 43 \pmod{34}$ er løsbar fordi $\gcd(9,34)=1$ og har da kun én løsn modulo 34.

Finner en løsn av $9X+34y=43$ v.h.a Euklids alg:

$34 = 3\cdot 9 + 7$

$9 = 1\cdot 7 + 2$

$7 = 3\cdot 2 + 1$

→ noster opp bakover og får

$1 = 9\cdot(-15)+34\cdot 4$

$\Rightarrow 43 = 9\cdot(-645)+34\cdot 172$

Så $x_0 = -645$ er en løsn av $9X \equiv 43 \pmod{34}$. Løsningen av denne lin.kongr er derfor

$$X \equiv -645 \pmod{34}$$