Forelesning 18 — mandag den 20. oktober

4.14 Lagranges teorem

Merknad 4.14.1. Fra skolen kjenner du til at en ligning

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

har maksimum to løsninger. Se Merknad 5.1.1 for mer om dette. Kanskje kjenner du dessuten til noe som er mer generell: en ligning

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

har maksimum n løsninger. I denne delen av kapittelet skal vi bevise at det samme er tilfellet i modulær aritmetikk: en kongruens

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0$$

har maksimum n løsninger slik at ikke noe par av disse er kongruent til hverandre modulo p.

Proposisjon 4.14.2. La m være et heltall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. La x være et heltall slik at

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{m}.$$

Ut ifra Proposisjon 3.2.1 finnes det et heltall r slik at:

(1) $0 \leq r < m - 1$;

(2) $x \equiv r \pmod{m}$.

Vi har:

$$a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv 0 \pmod{m}.$$

Bevis. Vi gjør følgende observasjoner.

(1) Ut ifra Proposisjon 3.2.48 er

$$x^i \equiv r^i \pmod{m}$$

for hvert naturlig tall i slik at $i \leq n$.

(2) Det følger fra (1) og Korollar 3.2.45 at

$$a_i x^i \equiv a_i r^i \pmod{m}$$

for hvert naturlig tall i slik at $i \leq n$.

(3) Det følger fra (2) og Korollar 3.2.36 at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x \\ &\equiv a_n r^n + a_{n-1} r^{n-1} + \cdots + a_2 r^2 + a_1 r \pmod{m} \end{aligned}$$

(4) Det følger fra (3) og Korollar 3.2.39 at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ &\equiv a_n r^n + a_{n-1} r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \pmod{m}. \end{aligned}$$

Ut ifra Proposisjon 3.2.24 er da

$$\begin{aligned} &a_n r^n + a_{n-1}r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \\ &\equiv a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{m} \end{aligned}$$

Det følger fra (4), antakelsen at

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{m}$$

og Proposisjon 3.2.33 at

$$a_n r^n + a_{n-1} r^{n-1} + \cdots + a_2 r^2 + a_1 r + a_0 \equiv 0 \pmod{m}.$$

□

Eksempel 4.14.3. Det kan regnes ut at

$$16^2 + 3 \cdot 16 + 4 = 308$$

og at $308 = 44 \cdot 7$, altså at

$$308 \equiv 0 \pmod{7}.$$

Dermed er $x = 16$ en løsning til kongruensen

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

Siden

$$16 \equiv 2 \pmod{7},$$

fastslår Proposisjon 4.14.2 at $x = 2$ er også en løsning til kongruensen. Dette er riktignok sant.

Eksempel 4.14.4. Det kan regnes ut at

$$9^3 + 3 \cdot 9^2 - 16 \cdot 9 + 2 = 830$$

og at $830 = 166 \cdot 5$, altså at

$$830 \equiv 0 \pmod 5.$$

Dermed er $x = 9$ en løsning til kongruensen

$$x^3 + 3x^2 + -16x + 2 \equiv 0 \pmod 5.$$

Siden

$$9 \equiv 4 \pmod 5,$$

fastslår Proposisjon 4.14.2 at $x = 4$ er også en løsning til kongruensen. Dette er riktignok sant.

Lemma 4.14.5. La p være et primtall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. La y være et heltall. Da finnes det et heltall r og, for hvert heltall i slik at $0 \leq i \leq n-1$, et heltall b_i, slik at

$$\begin{aligned} &a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= (x-y)\left(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \end{aligned}$$

for hvert heltall x.

Bevis. Først sjekker vi om lemmaet er sant når $n = 1$. La b_0 være a_1, og la r være $a_1 y + a_0$. Da er:

$$\begin{aligned} (x-y)b_0 + r &= a_1(x-y) + (a_1 y + a_0) \\ &= a_1 x - a_1 y + a_1 y + a_0 \\ &= a_1 x + a_0. \end{aligned}$$

Dermed er lemmaet sant når $n = 1$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. Vi gjør følgende observasjoner.

(1) Vi har:

$$\begin{aligned} &a_{m+1}x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= x\left(a_{m+1}x^m + a_m x^{m-1} + \cdots + a_2 x + a_1\right) + a_0. \end{aligned}$$

(2) Ut ifra antakelsen at lemmaet er sant når $n = m$, finnes det et heltall r' og, for hvert heltall i slik at $0 \leq i \leq m-1$, et heltall b'_i, slik at

$$\begin{aligned} &a_{m+1}x^m + a_m x^{m-1} + \cdots + a_2 x + a_1 \\ &= (x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'. \end{aligned}$$

(3) La b_0 være r'. For hvert heltall i slik at $1 \leq i \leq m$, la b_i være b'_{i-1}. La r være $yr' + a_0$. Da er

$$\begin{aligned}
&(x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \\
&= (x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x\right) + (x-y)b_0 + r \\
&= x(x-y)\left(b_m x^{m-1} + b_{m-1}x^{m-2} + \cdots + b_2 x + b_1\right) + xb_0 - yb_0 + r \\
&= x\Big((x-y)\left(b_m x^{m-1} + b_{m-1}x^{m-2} + \cdots + b_2 x + b_1\right) + b_0\Big) - yb_0 + r \\
&= x\Big((x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'\Big) - yr' + \left(yr' + a_0\right) \\
&= x\Big((x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'\Big) + a_0.
\end{aligned}$$

(4) Det følger fra (2) at

$$\begin{aligned}
&x\Big((x-y)\left(b'_{m-1}x^{m-1} + b'_{m-2}x^{m-2} + \cdots + b'_1 x + b'_0\right) + r'\Big) + a_0 \\
&= x\left(a_{m+1}x^m + a_m x^{m-1} + \cdots + a_2 x + a_1\right) + a_0.
\end{aligned}$$

Det følger fra (1), (3), og (4) at

$$\begin{aligned}
&a_{m+1}x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\
&= (x-y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r.
\end{aligned}$$

Dermed er lemmaet sant når $n = m + 1$.

Ved induksjon konkluderer vi at lemmaet er sant når n er et hvilket som helst naturlig tall.

□

Eksempel 4.14.6. La y være 3. Da fastslår Lemma 4.14.5 at det finnes et heltall r og et heltall b_0 slik at

$$11x + 8 = (x-3) \cdot b_0 + r,$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være 11, og r være 41: det stemmer at

$$11x + 8 = (x-3) \cdot 11 + 41.$$

Eksempel 4.14.7. La y være -7. Lemma 4.14.5 fastslår at det finnes et heltall r og heltall b_0 og b_1 slik at

$$5x^2 + 2x - 3 = \big(x - (-7)\big)\left(b_1 x + b_0\right) + r,$$

altså at

$$5x^2 + 2x - 3 = (x+7)\left(b_1 x + b_0\right) + r,$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være -33, b_1 være 5, og r være 228: det stemmer at

$$5x^2 + 2x - 3 = (x+7)\left(5x - 33x\right) + 228.$$

Eksempel 4.14.8. La y være 6. Lemma 4.14.5 fastslår at det finnes et heltall r og heltall b_0, b_1, og b_2 slik at

$$2x^3 - 8x^2 + 5x - 7 = (x - 6)\left(b_2x^2 + b_1x + b_0\right) + r$$

for hvert heltall x. Dette er riktigknok sant, ved å la b_0 være 2, b_1 være 4, b_2 være 29, og r være 167: det stemmer at

$$2x^3 - 8x^2 + 5x - 7 = (x - 6)\left(2x^2 + 4x + 29\right) + 167.$$

Merknad 4.14.9. Utsagnet i Lemma 4.14.5 er: det finnes et heltall r og, for hvert heltall i slik at $0 \leq i \leq n$, et heltall b_i, slik at

$$\begin{aligned} &a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 \\ &= (x - y)\left(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2x^2 + b_1x + b_0\right) + r \end{aligned}$$

for *hvert* heltall x. Dette er ikke det samme som å si: gitt et heltall x, finnes det et heltall r og, for hvert heltall i slik at $0 \leq i \leq n$, et heltall b_i, slik at denne ligningen stemmer.

Den andre påstanden holder muligheten åpen for at heltallet r og heltallene b_i varierer avhengig av x. Heltallet r og heltallene b_i i Lemma 4.14.5 varierer ikke avhengig av x.

Gitt et heltall x, er for eksempel

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 2x.$$

Ved å la b_0 være 1, b_1 være 2, og r være $2x$, får vi med andre ord at

$$2x^2 + x - 1 = (x - 1)\left(b_1x + b_0\right) + r.$$

Imidlertid varierer da r avhengig av x. Hvis for eksempel $x = 1$, er $r = 2$, og vi har:

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 2.$$

Hvis $x = 2$, er $r = 4$, og vi har:

$$2x^2 + x - 1 = (x - 1)(2x + 1) + 4.$$

Istedenfor kan vi la b_0 være 1, b_1 være 2, og r være 3: da har vi

$$2x^2 + x - 1 = (x - 1)(2x + 3) + 2.$$

I dette tilfellet varierer r ikke avhengig av x: uansett hvilket heltall x vi velger, er $r = 3$.

Merknad 4.14.10. Lemma 4.14.5 kan generaliseres. Et uttrkk

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0,$$

hvor a_i er et heltall for hvert heltall i slik at $0 \leq i \leq n$, og x er en variabel, kalles et *polynom*. Det finnes en divisjonsalgoritme for polynom som bygger på divisjonsalgoritmen for heltall: vi kan dele et polynom med et annet polynom, og får en kvotient som er et polynom og en rest som er et heltall. Lemma 4.14.5 følger umiddelbart fra dette.

Imidlertid kommer vi ikke til å trenge et annet sted divisjonsalgoritmen for polynom. Dessuten må begrepet ≪ ≪polynom≫ defineres formelt, og dette er heller ikke noe vi kommer et annet sted til å trenge. Derfor skal vi nøye oss med det direkte beviset vi ga for Lemma 4.14.5.

Proposisjon 4.14.11. La p være et primtall. La n være et naturlig tall. For hvert heltall i slik at $0 \leq i \leq n$, la a_i være et heltall. Anta at det ikke er sant at

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

Enten har kongruensen

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

ingen løsning, eller så er der et naturlig tall l slik at $l \leq n$, og heltall x_1, x_2, …, x_l, slik at følgende er sanne.

(I) For hvert naturlig tall i slik at $i \leq l$, er

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}.$$

(II) La z være et heltall slik at

$$a_n z^n + a_{n-1} z^{n-1} + \cdots + a_2 z^2 + a_1 z + a_0 \equiv 0 \pmod{p}.$$

Da finnes det et naturlig tall i slik at $i \leq l$ og $z \equiv x_i \pmod{p}$.

Bevis. Først sjekker vi om proposisjonen er sann når $n = 1$. La a_0 og a_1 være heltall. Siden p er et primtall og det ikke er sant at

$$a_1 \equiv 0 \pmod{p},$$

følger det fra Proposisjon 4.2.28 at det finnes et heltall x slik at følgende er sanne.

(1) Vi har: $a_1 x \equiv -a_0 \pmod{p}$.

(2) La y være et heltall slik at $a_1 y \equiv -a_0 \pmod{p}$. Da er $x \equiv y \pmod{p}$.

Det følger fra (1) og Korollar 3.2.39 at

$$a_1 x + a_0 \equiv 0 \pmod{p}.$$

Således er proposisjonen sann når $n = 1$, ved å la $l = 1$ og $x_1 = x$.

Anta nå at proposisjonen har blitt bevist når $n = m$, hvor m er et gitt naturlig tall. For hvert heltall i slik at $0 \leq i \leq m + 1$, la a_i være et heltall. Hvis kongruensen

$$a_{m+1} x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har ingen løsning, er proposisjonen sann. Ellers finnes det et heltall y slik at

$$a_{m+1} y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p}.$$

Ut ifra Lemma 4.14.5 finnes det et heltall r og, for hvert naturlig tall i slik at $0 \leq i \leq m$, et heltall b_i, slik at

$$\begin{aligned} &a_{m+1} x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &= (x - y)\left(b_m x^m + b_{m-1} x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) + r \end{aligned}$$

for hvert heltall x. Ved å la $x = y$, får vi:

$$a_{m+1}y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 = r.$$

Siden

$$a_{m+1}y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p},$$

følger det at

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

Ut ifra Korollar 3.2.39 er dermed

$$\begin{aligned} &a_{m+1}x^{m+1} + a_m x^m + \cdots + a_2 x^2 + a_1 x + a_0 \\ &\equiv (x - y)\left(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0\right) \pmod{p} \end{aligned}$$

for hvert heltall x.

Anta først at kongruensen

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \equiv 0 \pmod{p}$$

har ingen løsning. Da er proposisjonen sann når $n = m + 1$, ved å la l være 1 og x_1 være y.

Anta istedenfor at kongruensen

$$b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2 x^2 + b_1 x + b_0 \equiv 0 \pmod{p}$$

har minst én løsning. Siden det ikke er sant at

$$a_{m+1} \equiv 0 \pmod{p},$$

er det ikke sant at

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

Ut ifra antakelsen at proposisjonen er sann når $n = m$, finnes det derfor et naturlig tall l' og, for hvert naturlig tall i slik at $i \leq l'$, et heltall y_i, slik at følgende er sanne.

(A) For hvert naturlig tall i slik at $i \leq l'$, er

$$b_m y_i^m + b_{m-1}y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0 \equiv 0 \pmod{p}.$$

(B) La z være et heltall slik at

$$b_m z^m + b_{m-1}z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0 \equiv 0 \pmod{p}.$$

Da finnes det et naturlig tall i slik at $i \leq l'$ og $z \equiv y_i \pmod{p}$.

La da l være $l' + 1$. For hvert naturlig tall i slik at $i \leq l'$, la x_i være y_i. La x_l være y. Vi gjør følgende observasjoner.

(1) Det følger fra (A) og Korollar 3.2.45 at, for hvert naturlig tall i slik at $i \leq l'$, er

$$(y_i - y)\left(b_m y_i^m + b_{m-1} y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0\right) \equiv (x - y) \cdot 0 \pmod{p},$$

altså

$$(y_i - y)\left(b_m y_i^m + b_{m-1} y_i^{m-1} + \cdots + b_2 y_i^2 + b_1 y_i + b_0\right) \equiv 0 \pmod{p}.$$

Dermed er

$$(x_i - y)\left(b_m x_i^m + b_{m-1} x_i^{m-1} + \cdots + b_2 x_i^2 + b_1 x_i + b_0\right) \equiv 0 \pmod{p}$$

for hvert naturlig tall i slik at $i \leq l - 1$. Siden

$$\begin{aligned} &a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \\ &\equiv (x_i - y)\left(b_m x_i^m + b_{m-1} x_i^{m-1} + \cdots + b_2 x_i^2 + b_1 x_i + b_0\right) \pmod{p}, \end{aligned}$$

følger det fra Korollar 3.2.33 at

$$a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

for hvert naturlig tall i slik at $i \leq l - 1$.

(2) Siden

$$a_{m+1} y^{m+1} + a_m y^m + \cdots + a_2 y^2 + a_1 y + a_0 \equiv 0 \pmod{p},$$

er

$$a_{m+1} x_l^{m+1} + a_m x_l^m + \cdots + a_2 x_l^2 + a_1 x_l + a_0 \equiv 0 \pmod{p}.$$

For hvert naturlig tall i slik at $i \leq l$, er således

$$a_{m+1} x_i^{m+1} + a_m x_i^m + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}.$$

Dermed er (I) sant.

La nå z være et heltall slik at

$$a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \equiv 0 \pmod{p}.$$

Siden

$$\begin{aligned} &a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \\ &= (z - y)\left(b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0\right) \end{aligned}$$

er da

$$(z - y)\left(b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0\right) \equiv 0 \pmod{p}.$$

Anta at det ikke er sant at

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

Ut ifra Korollar 3.2.39 er det da ikke sant at

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

Det følger da fra Proposisjon 4.8.28 at

$$b_m z^m + b_{m-1} z^{m-1} + \cdots + b_2 z^2 + b_1 z + b_0 \equiv 0 \pmod{p}.$$

Fra denne kongruensen og (B) deduserer vi at det finnes et naturlig tall i slik at $i \leq l'$ og

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

altså slik at $i \leq l - 1$ og

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

Vi har således bevist: dersom

$$a_{m+1} z^{m+1} + a_m z^m + \cdots + a_2 z^2 + a_1 x + a_0 \equiv 0 \pmod{p},$$

er enten

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

altså

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

eller så finnes det et naturlig tall i slik at $i \leq l - 1$ og

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

Dermed er (II) er sant.

Således er proposisjonen sann når $n = m + 1$. Ved induksjon konkluderer vi at proposisjonen er sann for et hvilket som helst naturlig tall n.

□

Terminologi 4.14.12. Proposisjon 4.14.11 kalles *Lagranges teorem.*

Merknad 4.14.13. Med andre ord fastslår Proposisjon 4.14.11 at, dersom det ikke er sant at

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

finnes det maksimum n løsninger til kongruensen

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

slik at ikke noe par av disse løsningene er kongruent til hverandre modulo p, og slik at enhver annen løsning er kongruent modulo p til én av disse løsningene.

Terminologi 4.14.14. Anta at kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har m løsninger, hvor m er et heltall slik at $0 \leq m \leq n$, slik at ikke noe par av disse m løsningene er kongruent til hverandre modulo p, og slik at enhver annen løsning er kongruent modulo p til én av disse m løsningene. Da sier vi at kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}$$

har *m løsninger modulo p.*

Merknad 4.14.15. Ved å benytte denne terminologien, fastslår Proposisjon 4.14.11 at, dersom det ikke er sant at

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

finnes det maksimum n løsninger modulo p til kongruensen

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod{p}.$$

Eksempel 4.14.16. Proposisjon 4.14.11 fastslår at kongruensen

$$-3x^2 + 7x - 17 \equiv 0 \pmod{5}$$

har maksimum to løsninger p. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 4 er løsninger.

Vi har følgende. Alle kongruensene er modulo 5.

x	$-3x^2 + 7x - 17$	Løsning modulo 5?
1	$-13 \equiv 2$	✗
2	$-15 \equiv 0$	✓
3	$-23 \equiv 2$	✗
4	$-37 \equiv 3$	✗

Således har kongruensen

$$-3x^2 + 7x - 17 \equiv 0 \pmod{5}$$

én løsning modulo 5.

Eksempel 4.14.17. Proposisjon 4.14.11 fastslår at kongruensen

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

har maksimum to løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 6 er løsninger. Vi har følgende. Alle kongruensene er modulo 7.

x	$2x^2+3x+5$	Løsning modulo 7?
1	$10 \equiv 3$	✗
2	$19 \equiv 5$	✗
3	$32 \equiv 4$	✗
4	$49 \equiv 0$	✓
5	$70 \equiv 0$	✓
6	$95 \equiv 4$	✗

Således har kongruensen

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

to løsninger modulo 7.

Eksempel 4.14.18. Proposisjon 4.14.11 fastslår at kongruensen

$$5x^2+7x+6 \equiv 0 \pmod{13}$$

har maksimum to løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 12 er løsninger.

Vi har følgende. Alle kongruensene er modulo 13.

x	$5x^2+7x+6$	Løsning modulo 13?
1	$18 \equiv 5$	✗
2	$40 \equiv 1$	✗
3	$72 \equiv 7$	✗
4	$114 \equiv 10$	✗
5	$166 \equiv 10$	✗
6	$228 \equiv 7$	✗
7	$300 \equiv 1$	✗
8	$382 \equiv 5$	✗
9	$474 \equiv 6$	✗
10	$576 \equiv 4$	✗
11	$688 \equiv 12$	✗
12	$810 \equiv 4$	✗

Således har kongruensen

$$5x^2+7x+6 \equiv 0 \pmod{13}$$

ingen løsning modulo 13.

Eksempel 4.14.19. Proposisjon 4.14.11 fastslår at kongruensen

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

har maksimum tre løsninger. For å vise om dette er sant, er det, ut ifra Proposisjon 4.14.2, nok å sjekke hvilke av heltallene 1, 2, ..., 10 er løsninger.

Vi har følgende. Alle kongruensene er modulo 11.

x	$x^3 - x^2 + x + 1$	Løsning modulo 11?
1	2	✗
2	7	✗
3	$22 \equiv 0$	✓
4	$53 \equiv 9$	✗
5	$106 \equiv 7$	✗
6	$187 \equiv 0$	✓
7	$302 \equiv 5$	✗
8	$457 \equiv 6$	✗
9	$658 \equiv 9$	✗
10	$911 \equiv 7$	✗

Således har kongruensen

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

to løsninger modulo 11.

Merknad 4.14.20. Hvis vi ikke jobber modulo p, og se istedenfor på ligningen

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 = 0,$$

fører akkurat det samme argumentet som i beviset for Proposisjon 4.14.11 til et bevis for faktumet nevnt i Merknad 4.14.1: at denne ligningen har maksimum n løsninger.

Merknad 4.14.21. Proposisjon 4.14.11 er ikke nødvendigvis sann om vi ikke antar at p er et primtall. La oss se for eksempel på kongruensen

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

Vi har følgende. Alle kongruensene er modulo 10.

x	$x^2 + x - 2$	Løsning modulo 10?
1	0	✓
2	4	✗
3	$10 \equiv 0$	✓
4	$18 \equiv 8$	✗
5	$28 \equiv 8$	✗
6	$40 \equiv 0$	✓
7	$54 \equiv 4$	✗
8	$70 \equiv 0$	✓
9	$88 \equiv 8$	✗

Således har kongruensen

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

fire løsninger modulo 10.

4.15 Wilsons teorem

Merknad 4.15.1. Kanskje ser Lagranges teorem temmelig unøyaktig ut. Det sier ikke hvor mange løsninger kongruensen

$$a_n x_i^n + a_{n-1} x_i^{n-1} + \cdots + a_2 x_i^2 + a_1 x_i + a_0 \equiv 0 \pmod{p}$$

har, og sier ikke hvordan eventuelle løsninger kan finnes.

Derfor er det lett å tro at Lagranges teorem derfor ikke er så nyttig. Imidlertid kommer vi nå til å se at Lagranges teorem kan benyttes for å gi et bevis for Proposisjon 4.15.8, som er både konkret og eksakt. Beviset for Proposisjon 4.15.8 benytter altså, på en interessant måte, et overslag vi får ved å benytte Lagranges teorem som et steg mot å fastslå at den nøyaktige kongruensen i proposisjonen stemmer.

Først må vi gjøre noen forberedelser.

Lemma 4.15.2. La n være et naturlig tall slik at $n \geq 2$. La x være et heltall. Det finnes heltall a_0, a_1, …, a_{n-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)\\&= x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

Bevis. Først sjekker vi om lemmaet er sant når $n = 2$. I dette tilfellet er utsagnet at det finnes et heltall a_0 slik at

$$x - 1 = x - a_0.$$

Ved å la a_0 være 1, ser vi at dette riktignok er sant.

Anta nå at lemmaet har blitt bevist når $n = m$, hvor m er et gitt naturlig tall slik at $m \geq 2$. Således har det blitt bevist at det finnes heltall b_0, b_1, …, b_{m-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(m-1)\big)\\&= x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0.\end{aligned}$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&= \Big((x-1)(x-2)\cdots\big(x-(m-1)\big)\Big)\cdot(x-m)\\&= \big(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\big)\cdot(x-m).\end{aligned}$$

Produktet

$$\big(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\big)\cdot(x-m)$$

er likt summen av

$$x\left(x^{m-1} + b_{m-2}x^{m-2} + b_{m-3}x^{m-3} + \cdots + b_2x^2 + b_1x + b_0\right)$$

og

$$-m\left(x^{m-1}+b_{m-2}x^{m-2}+b_{m-3}x^{m-3}+\cdots+b_2x^2+b_1x+b_0\right),$$

altså summen av

$$\left(x^m+b_{m-2}x^{m-1}+b_{m-3}x^{m-2}+\cdots+b_2x^3+b_1x^2+b_0x\right)$$

og

$$-\left(mx^{m-1}+mb_{m-2}x^{m-2}+mb_{m-3}x^{m-3}+\cdots+mb_2x^2+mb_1x+mb_0\right).$$

Denne summen er lik

$$x^m+(b_{m-2}+m)\,x^{m-1}+(b_{m-3}+mb_{m-2})\,x^{m-2}+\cdots+(b_1+mb_2)\,x^2+(b_0+mb_1)\,x+mb_0.$$

Dermed har vi vist at

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&=x^m+(b_{m-2}+m)\,x^{m-1}+(b_{m-3}+mb_{m-2})\,x^{m-2}+\cdots+(b_1+mb_2)\,x^2+(b_0+mb_1)\,x+mb_0.\end{aligned}$$

La a_0 være mb_0. For hvert naturlig tall i slik at $i\leq m-2$, la a_i være $b_{i-1}+mb_i$. La a_{m-1} være $b_{m-2}+m$. Da er

$$\begin{aligned}&(x-1)(x-2)\cdots(x-m)\\&=x^m+a_{m-1}x^{m-1}+a_{m-2}x^{m-2}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

Dermed er lemmaet sant når $n=m+1$.

Ved induksjon konkluderer vi at lemmaet er sant for alle de naturlige tallene n slik at $n\geq 2$.

□

Eksempel 4.15.3. Lemma 4.15.2 fastslår at det finnes heltall a_0 og a_1 slik at

$$(x-1)(x-2)=x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)=x^2-3x+2,$$

altså kan vi la a_0 være 2 og a_1 være -3.

Eksempel 4.15.4. Lemma 4.15.2 fastslår at det finnes heltall a_0, a_1, a_2 slik at

$$(x-1)(x-2)(x-3)=x^3+a_2x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)(x-3)=x^3-6x^2+11x-6,$$

altså kan vi la a_0 være -6, a_1 være 11, og a_2 være -6.

Korollar 4.15.5. La n være et naturlig tall slik at $n \geq 2$. La x være et heltall. Det finnes heltall a_0, a_1, …, a_{n-2} slik at:

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=a_{n-2}x^{n-2}+a_{n-3}x^{n-3}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

Bevis. Ut ifra Lemma 4.15.2 finnes det heltall b_0, b_1, …, b_{n-1} slik at

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)\\&=x^{n-1}+b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0.\end{aligned}$$

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=\big(x^{n-1}+b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0\big)-x^{n-1}+1\\&=b_{n-2}x^{n-2}+b_{n-3}x^{n-3}+\cdots+b_2x^2+b_1x+b_0+1.\end{aligned}$$

La $a_0 = b_0 + 1$. For hvert naturlig tall i slik at $i \leq n-2$, la $a_i = b_i$. Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(n-1)\big)-\big(x^{n-1}-1\big)\\&=a_{n-2}x^{n-2}+a_{n-3}x^{n-3}+\cdots+a_2x^2+a_1x+a_0.\end{aligned}$$

□

Eksempel 4.15.6. Korollar 4.15.5 fastslår at det finnes heltall a_0 og a_1 slik at

$$(x-1)(x-2)-\big(x^2-1\big)=a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)-\big(x^2-1\big)=-3x+3,$$

altså kan vi la a_0 være -3 og a_1 være 3.

Eksempel 4.15.7. Korollar 4.15.5 fastslår at det finnes heltall a_0, a_1, a_2 slik at

$$(x-1)(x-2)(x-3)-\big(x^3-1\big)=a_2x^2+a_1x+a_0.$$

Dette er riktignok sant:

$$(x-1)(x-2)(x-3)=-6x^2+11x-5,$$

altså kan vi la a_0 være -6, a_1 være 11, og a_2 være -5.

Proposisjon 4.15.8. La p være et primtall. Da er

$$(p-1)!\equiv -1 \pmod{p}.$$

Bevis. Anta først at $p = 2$. Vi har:

$$(2-1)! - (-1) = 1! - (-1) = 1 + 1 = 2.$$

Siden $2 \mid 2$, deduserer vi at

$$(2-1)! \equiv -1 \pmod{2}.$$

Dermed er proposisjonen sann i dette tilfellet.

Anta nå at $p > 2$. La x være et heltall. Ut ifra Korollar 4.15.5 finnes det heltall a_0, a_1, ..., a_{p-2} slik at

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &= a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

Anta at det ikke er sant at

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$. La da m være det største heltallet slik at:

(i) $0 \leq m \leq p-2$;

(ii) det ikke er sant at

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

Da er

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &= a_mx^m + a_{m-1}x^{m-1} + \cdots + a_2x^2 + a_1x + a_0.\end{aligned}$$

For hvert naturlig tall r slik at $r \leq p-1$ er følgende sanne.

(1) Siden $(r-r) = 0$, er

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) = 0.$$

(2) Ut ifra Korollar 4.10.8 er

$$r^{p-1} \equiv 1 \pmod{p}.$$

Dermed er

$$r^{p-1} - 1 \equiv 1 - 1 \pmod{p},$$

altså

$$r^{p-1} - 1 \equiv 0 \pmod{p}.$$

(3) Det følger fra (1) og (2) at

$$(r-1)(r-2)\cdots\big(r-(p-1)\big) - \big(r^{p-1}-1\big) \equiv 0 \pmod{p}.$$

For hvert naturlig tall r slik at $r \leq p-1$, er dermed $x = r$ en løsning til kongruensen

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big) \equiv 0 \pmod{p},$$

altså til kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}.$$

Således har kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

minst $p-1$ løsninger.

Siden det ikke er sant at

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

følger det på en annen side fra Proposisjon 4.14.11 at kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

har maksimum m løsninger. Vi har: $m \leq p-2$. Dermed har vi en motsigelse: kongruensen

$$a_m x^m + a_{m-1}x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \pmod{p}$$

kan ikke ha både minst $p-1$ løsninger og maksimum $p-2$ løsninger.

Vi har således bevist at antakelsen at det ikke er sant at

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$ fører til en motsigelse. Derfor er

$$a_i \equiv 0 \pmod{p}$$

for alle heltallene i slik at $0 \leq i \leq p-2$.

Det følger fra Korollar 3.2.45 og Proposisjon 3.2.36 at, for et hvilket som helst heltall x, er da

$$\begin{aligned}&(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big)\\ &\equiv 0\cdot x^{p-2} + 0\cdot x^{p-3} + \cdots + 0\cdot x^2 + 0\cdot x + 0 \pmod{p},\end{aligned}$$

altså

$$(x-1)(x-2)\cdots\big(x-(p-1)\big) - \big(x^{p-1}-1\big) \equiv 0 \pmod{p}.$$

La $x = 0$. Ut ifra den foregående proposisjonen er

$$(0-1)(0-2)\cdots\big(0-(p-1)\big) - \big(^{p-1}-1\big) \equiv 0 \pmod{p},$$

altså

$$(-1)^{p-1}\big(1\cdot 2\cdots(p-1)\big) + 1 \equiv 0 \pmod{p}.$$

Ut ifra Korollar 3.2.39 er dermed

$$(-1)^{p-1}(p-1)! \equiv -1 \pmod{p}.$$

Ut ifra Proposisjon 4.2.31, finnes det et naturlig tall k slik at $p-1=2k$. Derfor er

$$(-1)^{p-1} = (-1)^{2k} = \left((-1)^2\right)^k = 1^k = 1.$$

Vi konkluderer at

$$(p-1)! \equiv -1 \pmod{p}.$$

□

Terminologi 4.15.9. Proposisjon 4.15.8 kalles *Wilsons teorem.*

Eksempel 4.15.10. Siden 3 er et primtall og $3 > 2$, fastslår Proposisjon 4.15.8 at

$$(3-1)! \equiv -1 \pmod{3}.$$

Siden $(3-1)! = 2! = 2$ og

$$2 \equiv -1 \pmod{3},$$

er dette riktignok sant.

Eksempel 4.15.11. Siden 5 er et primtall og $5 > 2$, fastslår Proposisjon 4.15.8 at

$$(5-1)! \equiv -1 \pmod{5}.$$

Siden $(5-1)! = 4! = 24$ og

$$24 \equiv -1 \pmod{5},$$

er dette riktignok sant.

Eksempel 4.15.12. Siden 7 er et primtall og $7 > 2$, fastslår Proposisjon 4.15.8 at

$$(7-1)! \equiv -1 \pmod{7}.$$

Siden $(7-1)! = 6! = 720$ og

$$720 \equiv -1 \pmod{7},$$

er dette riktignok sant.

Proposisjon 4.15.13. Det naturlige tallet

$$2 \cdot (26!) + 1$$

er delelig med 29.

Bevis. Vi gjør følgende observasjoner.

(1) Vi har: $2 = (-1) \cdot (-2)$. Derfor er

$$2 \cdot (26!) = (-1) \cdot (-2) \cdot (26!).$$

(2) Vi har:

$$-1 \equiv 28 \pmod{29}$$

og

$$-2 \equiv 27 \pmod{29}.$$

(3) Det følger fra (2) og Proposisjon 3.2.42 at

$$(-1) \cdot (-2) \equiv 28 \cdot 27 \pmod{29}.$$

(4) Det følger fra (3) og Korollar 3.2.45 at

$$(-1) \cdot (-2) \cdot (26!) \equiv 28 \cdot 27 \cdot 26! \pmod{29}.$$

Siden $28 \cdot 27 \cdot (26!) = 28!$, er dermed

$$(-1) \cdot (-2) \cdot (26!) \equiv 28! \pmod{29}.$$

(5) Siden 29 er et primtall, følger det fra Proposisjon 4.15.8 at

$$28! \equiv -1 \pmod{29}.$$

(6) Det følger fra (4), (5), og Proposisjon 3.2.33 at

$$(-1) \cdot (-2) \cdot (26!) \equiv -1 \pmod{29}.$$

Det følger fra (1) og (6) at

$$2 \cdot (26!) \equiv -1 \pmod{29}.$$

Ut ifra Korollar 3.2.39 er da

$$2 \cdot (26!) + 1 \equiv -1 + 1 \pmod{29},$$

altså

$$2 \cdot (26!) + 1 \equiv 0 \pmod{29}.$$

Vi konkluderer at $29 \mid 2 \cdot (26!) + 1$. □

Merknad 4.15.14. Det er naturlig å se først på Wilsons teorem som er artig, men ikke så viktig fra et teoretisk synspunkt. Imidlertid kommer til å benytte Wilsons teorem i løpet av vårt bevis for det dypeste teoremet i kurset, Teorem **??**!

5.3 Legendresymbolet

Definisjon 5.3.1. La p være et primtall slik at $p > 2$. La a være et heltall. *Legendresymbolet* til a og p er: 1 dersom a er en kvadratisk rest modulo p; 0 dersom $a \equiv 0 \pmod{p}$; og -1 ellers.

Notasjon 5.3.2. La p være et primtall slik at $p > 2$. La a være et heltall. Vi betegner Legendresymbolet til a og p som $\mathbb{L}_p^a$.

Merknad 5.3.3. La p være et primtall slik at $p > 2$. La a være et heltall. Ved å benytte Notasjon 5.3.2, har vi:

$$\mathbb{L}_p^a = \begin{cases} 1 & \text{dersom } a \text{ er en kvadratisk rest til } p, \\ 0 & \text{dersom } a \equiv 0 \pmod{p}, \\ -1 & \text{ellers.} \end{cases}$$

Merknad 5.3.4. Legendresymbolet til a og p betegnes typisk (a/p), $\left(\frac{a}{p}\right)$, eller $(a \mid p)$. Imidlertid har det ingenting å gjøre med brøk, og ingenting å gjøre med delbarhet med p. For å unngå forvirring, skal vi derfor følge Notasjon 5.3.2.

Eksempel 5.3.5. Fra Eksempel 5.2.12 har vi følgende.

a	$\mathbb{L}_3^a$
0	0
1	1
2	-1

Eksempel 5.3.6. Fra Eksempel 5.2.13 har vi følgende.

a	$\mathbb{L}_5^a$
0	0
1	1
2	-1
3	-1
4	1

Eksempel 5.3.7. Fra Eksempel 5.2.14 har vi følgende.

a	$\mathbb{L}_7^a$
0	0
1	1
2	1
3	-1
4	1
5	-1
6	-1

Eksempel 5.3.8. Fra Eksempel 5.2.15 har vi følgende.

a	$\mathbb{L}_{11}^{a}$
0	0
1	1
2	-1
3	1
4	1
5	1
6	-1
7	-1
8	-1
9	1
10	-1

Oppgaver

O4.1 Oppgaver i eksamens stil

Oppgave O4.1.11. Vis uten å regne ut at $18 \cdot (33!) - 3$ er delelig med 37.

Oppgave O5.1.2. Skriv ned Legendresymbolene $\mathbb{L}_{11}^{a}$ for alle de heltallene a slik at $0 \leq a \leq 10$. *Tips*: Benytt svaret ditt på Oppgave O4.1.10.