Wilsons teorem

Lemma: Anta at p er et odde primtall. Da er det nøyaktig to elementer i $\mathbb{Z}/(p)$ som er sin egen invers, nemlig $\bar{1}$ og $-\bar{1}$.

Bevis: Siden p er odde, er $\bar{1} \neq -\bar{1}$, så vi har minst to elementer som er sin egen invers. Anta at $\bar{x}$ er et element som er sin egen invers, $\bar{x} \cdot \bar{x} = \bar{1}$, dvs

$$\bar{0} = \bar{x}^2 - \bar{1}^2 = (\bar{x} - \bar{1})(\bar{x} + \bar{1})$$

Siden $\mathbb{Z}/(p)$ ikke har nulldivisorer, må $\bar{x} = \bar{1}$ eller $\bar{x} = -\bar{1}$.

Wilsons teorem: Anta at p er et odde primtall. Da er

$$\underbrace{\overline{(p-1)!}}_{\text{produktet av alle ikke-null elementer i } \mathbb{Z}/(p)} = -\bar{1} \quad \text{i } \mathbb{Z}/(p).$$

Bevis: Alle ikke-null elementer i $\mathbb{Z}/(p)$ har en invers, så vi kan ordne alle elementene i par

$$\{-\bar{1}\}, \{\bar{1}\}, \{\bar{x}_1, \bar{x}_1^{-1}\}, \{\bar{x}_2, \bar{x}_2^{-1}\}, \ldots, \{\bar{x}_k, \bar{x}_k^{-1}\} \leftarrow \text{alle ikke-null elementer}$$

Multipliser sammen alle elementene:

$$\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{p-1} = \underset{-1}{\uparrow}(-1)\underbrace{(1)}_{1}\underbrace{(\bar{x}_1 \cdot \bar{x}_1^{-1})}_{1}\underbrace{(\bar{x}_2 \cdot \bar{x}_2^{-1})}_{1} \cdots \underbrace{(\bar{x}_k \cdot \bar{x}_k^{-1})}_{1} = -\bar{1}$$

$$\boxed{\overline{(p-1)!} = -\bar{1}}$$

Kvadratrester

Vi vet hvordan vi løser første gradsligninger $\bar{a}\bar{x} = \bar{b}$ i $\mathbb{Z}/(p)$.
Hva med annengradsligninger? $\bar{a}\bar{x}^2 + \bar{b}\bar{x} + \bar{c} = \bar{0}$ i $\mathbb{Z}/(p)$

Starter med den enkleste: $\underline{\bar{x}^2 = \bar{a}}$.

Et element $\bar{a}$ i $\mathbb{Z}/(p)$ kalles en <u>kvadratisk rest</u> dersom det finnes en $\bar{x} \in \mathbb{Z}/(p)$ slik at $\bar{x}^2 = \bar{a}$.

<u>Setning</u>: Anta at p er et odde primtall. Hvis $\bar{a} \neq \bar{0}$ er en kvadratisk rest i $\mathbb{Z}/(p)$, så finnes det nøyaktig to elementer $\bar{x}_1$ og $-\bar{x}_1$ som løser ligningen $\bar{x}^2 = \bar{a}$.

<u>Bevis</u>: Siden $\bar{a}$ er en kvadratisk rest, finnes det et element $\bar{x}_1$ slik at $\bar{x}_1^2 = \bar{a}$. Men dermed er også $-\bar{x}_1^2 = \bar{a}$, og siden p er et odde tall, er $-\bar{x}_1 \neq \bar{x}_1$. Anta så at $\bar{x}$ er en tredje løsning: Da er

$$\bar{0} = \underset{\bar{a}}{\bar{x}^2} - \underset{\bar{a}}{\bar{x}_1^2} = (\bar{x} - \bar{x}_1)(\bar{x} + \bar{x}_1)$$

og siden $\mathbb{Z}/(p)$ ikke har nulldivisorer, må $\bar{x} = \bar{x}_1$ og $\bar{x} = -\bar{x}_1$. Så det finnes ikke flere løsninger enn $\bar{x}_1$ og $\bar{x}_2$.

<u>Setning</u>: Hvis p er et odde primtall, så er nøyaktig halvparten av de ikke-null elementene i $\mathbb{Z}/(p)$ kvadratiske rester. Det vil si at $\frac{p-1}{2}$ kvadratiske rester i $\mathbb{Z}/(p)$.

<u>Bevis</u>: Vi grupperer elementene $\neq \bar{0}$ i $\mathbb{Z}/(p)$ sammen:

$$\underbrace{(\bar{x}_1, -\bar{x}_1)}_{\text{kvadrat } \bar{a}_1}, \underbrace{(\bar{x}_2, -\bar{x}_2)}_{\bar{a}_2}, \ldots\ldots \underbrace{(\bar{x}_{\frac{p-1}{2}}, -\bar{x}_{\frac{p-1}{2}})}_{\bar{a}_{\frac{p-1}{2}}} \leftarrow \frac{p-1}{2} \text{ kvadratiske rester.}$$

p et odde primtall

<u>Lemma</u>: Anta at $\bar{a}$ er en ikke-null rest i $\mathbb{Z}/(p)$. Da er enten $\bar{a}^{\frac{p-1}{2}} = \bar{1}$ eller $\bar{a}^{\frac{p-1}{2}} = -\bar{1}$.

<u>Bevis</u>: Sett $\bar{x} = \bar{a}^{\frac{p-1}{2}}$. Da $\bar{x}^2 = \left(\bar{a}^{\frac{p-1}{2}}\right)^2 = \bar{a}^{p-1} = \bar{1}$ (lille Fermat). Dette viser at $\bar{x}$ er en "kvadratrot" av $\bar{1}$, og $\bar{1}$ har bare to kvadratrøtter, nemlig $\bar{1}$ og $-\bar{1}$.

<u>Eulers kriterium</u>: Hvis p er et odde primtall, så er $\bar{a} \neq \bar{0}$ en kvadratisk rest i $\mathbb{Z}/(p)$ hvis og bare hvis $\bar{a}^{\frac{p-1}{2}} = 1$.

<u>Bevis</u>: Anta at $\bar{a}$ er en kvadratisk rest. Da finnes det en $\bar{x} \neq \bar{0}$ slik at $\bar{x}^2 = \bar{a}$. Opphøyer i $\frac{p-1}{2}$ på begge sider

$$1 = \bar{x}^{p-1} = (\bar{x}^2)^{\frac{p-1}{2}} = \bar{a}^{\frac{p-1}{2}} \quad \text{ved lille Fermat.}$$

Anta så at $\bar{a}$ <u>ikke</u> er en kvadratisk rest. For hver $\bar{x}$ i $\mathbb{Z}/(p)$ finnes det nøyaktig én $\bar{x}'$ slik at $\bar{x} \cdot \bar{x}' = \bar{a}$. (fordi lineære løsninger har en entydig løsning i $\mathbb{Z}/(p)$)

Grupperer elementene i par:

$$\{\bar{x}_1, \bar{x}_1'\}, \{\bar{x}_2, \bar{x}_2'\}, \ldots, \{\bar{x}_{\frac{p-1}{2}}, \bar{x}'_{\frac{p-1}{2}}\}$$

(legg merke til at $\bar{x} \neq \bar{x}'$ siden $\bar{a}$ ikke er en kvadratisk rest)

$$\bar{a}^{\frac{p-1}{2}} = \underbrace{(\bar{x}_1\bar{x}_1')}_{a}\underbrace{(\bar{x}_2\bar{x}_2')}_{a} \cdots \underbrace{(\bar{x}_{\frac{p-1}{2}}\bar{x}'_{\frac{p-1}{2}})}_{a} = \underbrace{\bar{x}_1\bar{x}_1'\bar{x}_2\bar{x}_2' \cdots \bar{x}_{\frac{p-1}{2}}\bar{x}'_{\frac{p-1}{2}}}_{\text{alle ikke-null elementer i } \mathbb{Z}/(p)} = -1$$

ved Wilsons teorem.

Altså er $\bar{a}^{\frac{p-1}{2}} = -\bar{1}$ når $\bar{a}$ ikke er en kvadratisk rest.

Når er $\overline{-1}$ en kvadratisk rest?

$p=2$

Setning: $\overline{-1}$ er en kvadratisk rest i $\mathbb{Z}/(p)$ hvis $p \equiv 2 \pmod 4$ eller $p \equiv 1 \pmod 4$

Bevis: Hvis $p=2$, så $\overline{-1} = \overline{1} = \overline{1}\cdot\overline{1}$ er en kvadratisk.

$p \equiv 1 \pmod 4$: Da er $p = 4k+1$, så $(\overline{-1})^{\frac{p-1}{2}} = (\overline{-1})^{\frac{4k+1-1}{2}} = (\overline{-1})^{2k} = \overline{1}$

Ved Eulers kriterium er dermed (-1) en kvadratisk rest.

$p \equiv 3 \pmod 4$ Da er $p = 4k+3$, så $(\overline{-1})^{\frac{p-1}{2}} = (\overline{-1})^{\frac{4k+3-1}{2}} = (\overline{-1})^{2k+1} = -\overline{1}$

Ved Eulers kriterium er dermed (-1) ikke en kvadratisk rest

Teorem: Det finnes uendelig mange primtall som er kongruente med 1 $\pmod 4$

Bevis: Anta at det kun finnes endelig mange primtall som kong. med 1 $\pmod 4$: $p_1, p_2, \ldots, p_n$

La $$N = (2p_1p_2\cdots p_n)^2 + 1$$

Vi ser at N ikke er delelig med $2, p_1, p_2, \ldots, p_n$. Hvis p er en primfaktor i N, må altså $p \equiv 3 \pmod 4$. Siden $p \mid N$, er $\overline{N} = \overline{0}$ i $\mathbb{Z}/(p)$.

$$\overline{0} = \overline{N} = \underbrace{\overline{(2p_1p_2\cdots p_n)}}_{\overline{x}}{}^2 + \overline{1} = \overline{x}^2 + \overline{1} \quad \text{i } \mathbb{Z}/(p).$$

Altså $\overline{x}^2 = -\overline{1}$ i $\mathbb{Z}/(p)$. Dette er en selvmotsigelse siden $\overline{-1}$ ikke er en kvadratisk rest i $\mathbb{Z}/(p)$ når $p \equiv 3 \pmod 4$.

Annengradsligninger i $\mathbb{Z}/(p)$

Gitt: $\bar{a}\bar{x}^2 + \bar{b}\bar{x} + \bar{c} = \bar{0}$ i $\mathbb{Z}/(p)$, $\bar{a} \neq \bar{0}$

Løser: Ganger ligningen med $\bar{4}\bar{a}$:

$$\underbrace{\bar{4}\bar{a}^2\bar{x}^2 + \bar{4}\bar{a}\bar{b}\bar{x}} + \bar{4}\bar{a}\bar{c} = \bar{0} \qquad (\bar{2}\bar{a}\bar{x} + \bar{b})^2 = \bar{4}\bar{a}^2\bar{x}^2 + \bar{4}\bar{a}\bar{x}\bar{b} + \bar{b}^2$$

Fullstendig kvadrat:

$$\underbrace{\bar{4}\bar{a}^2\bar{x}^2 + \bar{4}\bar{a}\bar{b}\bar{x} + \bar{b}^2} - \bar{b}^2 + \bar{4}\bar{a}\bar{c} = \bar{0}$$

$$(\bar{2}\bar{a}\bar{x} + \bar{b})^2 = \bar{b}^2 - \bar{4}\bar{a}\bar{c}$$

(kun mulig hvis $\bar{b}^2 - \bar{4}\bar{a}\bar{c}$ er en kvadratisk rest i $\mathbb{Z}/(p)$. Anta det heretter.)

$$\bar{2}\bar{a}\bar{x} + \bar{b} = \text{"}\pm\sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}}\text{"}$$

$$\bar{2}\bar{a}\bar{x} = -\bar{b} \pm \sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}} \qquad | (\bar{2}\bar{a})^{-1}$$

$$\bar{x} = (\bar{2}\bar{a})^{-1}(-\bar{b} \pm \sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}}) = \frac{-\bar{b} \pm \sqrt{\bar{b}^2 - \bar{4}\bar{a}\bar{c}}}{\bar{2}\bar{a}}$$

Setning: Annengradsligningen
$\bar{a}\bar{x}^2 + \bar{b}\bar{x} + \bar{c} = \bar{0}$ der $\bar{a} \neq \bar{0}$.
har løsninger i $\mathbb{Z}/(p)$ hvis og bare hvis $\bar{b}^2 - \bar{4}\bar{a}\bar{c}$ er en kvadratisk rest i $\mathbb{Z}/(p)$.
I så fall er løsningene gitt ved

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

Eksempel: $\bar{2}\bar{x}^2 + \bar{6}\bar{x} + \bar{3} = \bar{0}$ i $\mathbb{Z}/(13)$

Løsningene er gitt ved:

$$\bar{x} = \frac{-\bar{6} \pm \sqrt{\bar{6}^2 - \bar{4}\cdot\bar{2}\cdot\bar{3}}}{\bar{2}\cdot\bar{2}} = \frac{-\bar{6} \pm \sqrt{\overline{12}}}{\bar{2}\cdot\bar{2}} = \frac{-\bar{6} \pm \sqrt{\overline{25}}}{\bar{2}\cdot\bar{2}}$$

(36 − 24)

$$= \frac{-\bar{6} \pm \bar{5}}{\bar{2}\cdot\bar{2}} = \begin{cases} -\frac{\bar{1}}{\bar{4}} = -\frac{\overline{14}}{\bar{4}} = -\frac{\bar{7}}{\bar{2}} = -\frac{\overline{20}}{\bar{2}} = -\overline{10} = \underline{\underline{\bar{3}}} \\ \frac{-\overline{11}}{\bar{4}} = \frac{\bar{2}}{\bar{4}} = \frac{\bar{1}}{\bar{2}} = \frac{\overline{14}}{\bar{2}} = \underline{\underline{\bar{7}}} \end{cases}$$

Ekstra eksempel: Eulers kriterium: Er $\bar{9}$ en kvadratisk rest i $\mathbb{Z}/(17)$?

Kriteriet: $\bar{a}^{\frac{p-1}{2}} = \begin{cases} 1 & \bar{a} \text{ er kvadratisk rest} \\ -1 & \bar{a} \text{ ikke er kvadratisk rest.} \end{cases}$

Test

$$\bar{9}^8 = \bar{9}^2\cdot\bar{9}^2\cdot\bar{9}^2\cdot\bar{9}^2 = (\bar{-4})(\bar{-4})(\bar{-4})(\bar{-4}) = \overline{16}\cdot\overline{16} = (\bar{-1})(\bar{-1}) = \bar{1}$$

$9^2 = 81 = \underbrace{5\cdot 17}_{85} - 4$

$\bar{9}^2 = -\bar{4}$

Så $\bar{9}$ er en kvadratisk rest i $\mathbb{Z}/(17)$

Kvadratsummer. 2, 3, 5, 7, 11, 13, 17

$5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$

$p \equiv 1 \pmod 4$ kvadrsum

$p \equiv 3 \pmod 4$ – " –

Neste forelesning fredag!