Noen løsninger

Fredrik Meyer

Her er noen løsningsforslag til oppgaver jeg gjorde dårlig i plenumen.

Oppgave 1 (Oppgave 5.7)**.** La p være et odde primtall. Vi har sett i kapittel 5 at dersom $x^2 \equiv -1 \pmod{p}$ er løsbar, så er $p \equiv 1 \pmod{4}$. Her er noen generaliseringer:

a) Vis at dersom $x^4 \equiv -1 \pmod{p}$ er løsbar så er $p \equiv 1 \pmod{8}$.

b) Vis at dersom $x^8 \equiv -1 \pmod{p}$ er løsbar, så er $p \equiv 1 \pmod{16}$.

c) Formuler og bevis en naturlig generalisering av a) og b).

■

a) La x være en løsning av $x^4 \equiv -1 \pmod{p}$. La først $u = x^2$. Da ser vi at ligningen $u^2 \equiv -1 \pmod{4}$ har en løsning. Dette impliserer at $p - 1 \equiv 1 \pmod{4}$, så $4 \mid p - 1$.

   Vi har da følgende kjede av likheter:

$$1 \equiv x^{p-1} \equiv x^{\frac{4}{4}(p-1)} \equiv (x^4)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}.$$

   Merk at ingen av eksponentene er ekte brøker, så alt er veldefinert.

   For at dette skal være mulig, må $\frac{1}{4}(p-1)$ være partall. Men dette gir at $\frac{1}{4}(p-1) = 2k$, altså $p - 1 = 8k$, altså $p \equiv 1 \pmod{8}$.

b) Igjen, la $u = x^2$. Dermed har $u^4 \equiv -1 \pmod{p}$ en løsning. Fra a) impliserer det at $p - 1 \equiv 0 \pmod{8}$. Dermed kan vi skrive

$$1 \equiv x^{p-1} \equiv x^{\frac{8}{8}(p-1)} \equiv (x^8)^{\frac{p-1}{8}} \equiv (-1)^{\frac{p-1}{8}} \pmod{p}.$$

   Dermed må $\frac{1}{8}(p-1)$ være partall, så $p - 1 = 16k$, så $p \equiv 1 \mod 16$.

c) Den naturlige generaliseringen er selvsagt: om $x^{2^{k-1}} \equiv -1 \pmod{p}$, så er $p \equiv 1 \pmod{2^k}$ for $k \geq 2$.

Dette kan vi bevise med induksjon. Vi har allerede sett at dette er sant for $k = 2$. Anta nå at påstanden stemmer for $k = l$. Vi skal vise at den holder for $k = l + 1$.

Anta at $x^{2^k} \equiv -1 \pmod{p}$ har en løsning x. Sett først $u = x^2$. Da er $x^{2^k} = u^{2^{k-1}} \equiv -1 \pmod{p}$, så ved induksjonshypotesen har vi at $p - 1 \equiv 0 \pmod{2^k}$. Dermed kan vi skrive (som over)

$$1 \equiv x^{p-1} \equiv x^{\frac{2^k}{2^k}(p-1)} \equiv (x^{2^k})^{\frac{p-1}{2^k}} \equiv (-1)^{\frac{p-1}{2^k}} \pmod{p}.$$

Dermed må $(p-1)/2^k$ være partall, så vi kan skrive $(p-1)/2^k = 2l$ for en $l \in \mathbb{Z}$. Dermed er $p - 1 = 2^{k+1}l$, så $p \equiv 1 \pmod{2^{k+1}}$, som var det vi skulle vise.

Det følger ved induksjonsprinsippet at påstanden holder for alle k.

Oppgave 2 (Oppgave 5.8)**.** La p være et primtall med $p \equiv 3 \pmod{4}$. Vis at

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1 \pmod{p}.$$

■

Merk at venstresiden er produktet av den første halvparten tall i $\mathbb{Z}/(p)$. De resterende tallene i $\mathbb{Z}/(p)$ er $-1, -2, -3....$ Dermed kan vi skrive

$$(p-1)! \equiv \left(\frac{p-1}{2}\right)! \left(\frac{p-1}{2}\right)!(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Men siden $p \equiv 3 \pmod{4}$, er $(-1)^{\frac{p-1}{2}} = -1$. Sett $x = \left(\frac{p-1}{2}\right)!$. Da har vi at

$$x^2 \equiv 1 \pmod{p},$$

så $x \equiv \pm 1 \pmod{p}$ (ved oppgave 2a) i obligen).

Her er et eksempel på hva vi gjør for $p = 7$:

$$-1 \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 2 \cdot 3 \cdot (-3) \cdot (-2) \cdot (-1) \equiv \left(\frac{6}{2}\right)!^2 (-1)^3 \pmod{7}.$$

Så $3!^2 \equiv 1 \pmod{7}$, så $3! \equiv \pm 1 \pmod{7}$ (som stemmer).

Oppgave 3 (Oppgave 6.3)**.** a) Vis at dersom $k \equiv 7 \pmod 8$, så kan ikke k skrives som en sum av tre kvadrater.

b) Vis at dersom $4a$ kan skrives som en sum av tre kvadrater, så kan også a det.

c) Vis at ingen tall på formen $4^m(8k+7)$ aldri kan skrives som en sum av tre kvadrater. Dette er den enkle delen av Gauss' resultat.

■

a) Vi skriver opp kvadratene modulo 8. Disse er $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 1$, $4^2 \equiv 0$, $5^2 \equiv 1$, $6^2 \equiv 4$, $7^2 \equiv 1$ og $0^2 \equiv 0$. Så kvadratene modulo 8 er $0, 1, 4$. Vi sjekker at det ikke er mulig å legge sammen noen tre av disse tallene og få 7. Dette betyr at om $a = k_1^2 + k_2^2 + k_3^2$, så kan ikke $a \equiv 7 \pmod 8$.

b) Vi ser på ligningen $4a = k_1^2 + k_2^2 + k_3^2$ modulo 4. Modulo 4 er kvadratene enten 0 eller 1. Men vi har at $k_1^2 + k_2^2 + k_3^2 = 4a \equiv 0 \pmod 4$. For at dette skal gå, må hvert ledd være lik 0 modulo 4. Men dette skjer kun hvis alle k_i er partall.

Dermed, om $4a = k_1^2 + k_2^2 + k_3^2$, kan vi skrive $k_i = 2m_i$ for $m_i \in \mathbb{N}$ og få

$$4a = (2m_1)^2 + (2m_2)^2 + (2m_3)^2 = 4m_1^2 + 4m_2^2 + 4m_3^2.$$

Vi kan dermed dele på 4 på begge sider, og ser at a også kan skrives som en sum av tre kvadrater.

c) Anta gitt et tall $r = 4^m(8k+7)$ og anta for motsigelse at det kan skrives som en sum av tre kvadrater.

Da følger det fra *b*) at $r' = 4^{m-1}(8k+7)$ også kan skrives som en sum av tre kvadrater. Vi kan fortsette, og ser at da må også $r'' = 4^{m-2}(8k+7)$ kunne skrives som en sum av tre kvadrater.

Til slutt ender vi opp med at $8k+7$ kan skrives som en sum av tre kvadrater. Men dette motsier a), da $8k + 7 \equiv 7 \pmod 8$.