Aflevering 2

Jonas Trepiakas - hvn548@alumni.ku.dk

Vi beviser først et lemma:

Lemma 1: Lad g være en primitiv rod modulo p. Da har vi

$$g^l \equiv -1 \pmod p \iff l \equiv \frac{p-1}{2} \pmod{p-1}.$$

Bevis: Da vi for $k \in \mathbb{Z}$ har $p \mid k^2 - 1 \iff p \mid (k-1)(k+1) \iff k \equiv 1 \vee k \equiv -1 \pmod p$ følger, at $g^{\frac{p-1}{2}} \equiv -1 \pmod p$ (hvis $g^{\frac{p-1}{2}} \equiv 1 \pmod p$ ville det stride imod, at g er en primitiv rod modulo p). Så hvis $l \equiv \frac{p-1}{2} \pmod{p-1}$ fås

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

Antag nu modsat, at $g^l \equiv -1 \pmod p$. Da har vi

$$g^l \equiv -1 \equiv g^{\frac{p-1}{2}} \pmod p \implies g^{l-\frac{p-1}{2}} \equiv 1 \pmod p \implies p-1 = \mathrm{ord}(g) \mid l - \frac{p-1}{2} \implies l \equiv \frac{p-1}{2} \pmod{p-1}.$$

Hvormed resultatet følger.

Opgave 1. Antag først, at $a = -1$ er en primitiv rod modulo $p > 3$, hvor p er et primtal. Da $a^2 \equiv 1 \pmod p$, fås $\mathrm{ord}(a) \mid 2 < p - 1 = \varphi(p)$, hvormed a ikke er en primitiv rod modulo p.
Antag nu, at a er et perfekt kvadrat, altså $a = k^2, k \in \mathbb{Z}_+$, og antag, at a er en primitiv rod modulo $p > 3$, hvor p er et primtal. Skriv da $p - 1 = 2l$. Idet a er en primitiv rod, må $\gcd(a, p) = 1$, hvormed $\gcd(k, p) = 1$, så vi får

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

Dermed har vi $\mathrm{ord}(a) \mid l \implies \mathrm{ord}(a) \leq l < 2l = p - 1$, så a er ikke en primitiv rod modulo p.

Antag nu, at $p = 3$. Da $\varphi(p) = 2 = \mathrm{ord}(-1)$, er $-1 \equiv 2$ en primitiv rod modulo 3.
Da samtlige kvadratiske rødder modulo 3 desuden er $0, 1$, følger alle perfekte kvadrater har orden 1 eller ∞, så ingen perfekte kvadrater er primitive rødder modulo 3.

Opgave 2: Lad $p - 1 = 2l$. Per Lemma 1 fås $(aa')^l \equiv a^l (a')^l \equiv (-1)(-1) \equiv 1 \pmod p$, så $\mathrm{ord}(aa') | l \implies \mathrm{ord}(aa') \leq l < 2l = p - 1$, så aa' er ikke en primitiv rod modulo p.

Opgave 3: Antag, at $-a$ er en primitiv rod, og at $p \equiv 3 \pmod 4$. Da har vi $4l = p - 3$ for et $l \in \mathbb{Z}$, hvormed $p - 1 = 2k$, hvor $k \in \mathbb{Z}$ er ulige. Per Lemma 1 fås nu

$$(-a)^k \equiv (-1)^k a^k \equiv (-1)(-1) \equiv 1 \pmod p.$$

Hvormed $\mathrm{ord}(-a) \mid k$, så $\mathrm{ord}(-a) \leq k < 2k = p - 1$, så $-a$ er ikke en primitiv rod. Da $p > 3$ er et primtal, er den specielt ulige, så p er enten 1 eller 3 modulo 4, hvormed vi får, at hvis $-a$ er en primitiv rod, må $p \equiv 1 \pmod 4$.

Antag nu i stedet, at $p \equiv 1 \pmod 4$. Vi har, at $\mathrm{ord}(-a) \leq p - 1$ ifølge Fermats lille sætning.
Antag nu, at $\mathrm{ord}(-a) = d < p - 1 = 4k$ for $k \in \mathbb{Z}$. Hvis d er lige, fås $1 \equiv (-a)^d \equiv a^d \pmod p$ i modstrid med, at a er en primitiv rod modulo p. Men hvis d er ulige fås $1 \equiv (-a)^d \equiv -a^d \iff a^d \equiv -1 \pmod p$, hvormed Lemma 1 giver $d \equiv \frac{p-1}{2} \pmod{p-1}$, så $4k \mid d - 2k$, så d er lige, som er en modstrid. Dermed er $-a$ en primitiv rod modulo p.

Opgave 4: Vi har først, at $2 \equiv 11 \equiv x^2 - 3y^3 \equiv x^2 \pmod 3$, men da 2 ikke er en kvadratisk rest modulo 3, eksisterer ingen heltallige løsninger til ligningen.
Til gengæld har vi i $\mathbb{R}$, at

$$\begin{aligned} 11 &= x^2 - 3y^3 \\ \iff y^3 &= \frac{x^2 - 11}{3} \\ \iff y &= \sqrt[3]{\frac{x^2 - 11}{3}},. \end{aligned}$$

og da $\sqrt[3]{\frac{x^2-11}{3}} \in \mathbb{R}$ for alle $x \in \mathbb{R}$, følger at alle $x, y \in \mathbb{R}$ af formen

$$(x, y) = \left(x, \sqrt[3]{\frac{x^2-11}{3}}\right)$$

løser ligningen.