Elementær Talteori - 2. aflevering

Opgave 1

Antag at a er en primitiv rod modulo p, hvor p er et primtal. Vis at a^k er en primitiv rod modulo p hvis og kun hvis $gcd(k, p-1) = 1$. Brug dette til at bevise {**St**} Prop 2.5.12 når $n = p$.

Vi starter med at vise den første implikation, at hvis $gcd(k, p-1) = 1$ så er a^k en primitiv rod mod p.
Dette vises ved at vise der findes et n således at $a^{k^n} \equiv a \pmod{p}$, da de derfor må generere samme elementer i sættet $\mathbb{Z}/p\mathbb{Z}$ og derved må a^k også være en primitiv rod.
At $gcd(k, p-1) = 1$ betyder at vi kan opstille en ligning $kx + (p-1)y = 1$ da der findes x og y der løser lignignen. Da begge sider er 1 kan vi opløfte begge sider som potens af a, så vi får

$$\begin{aligned} a^{(kx+(p-1)y)} &\equiv a^1 \ (mod\, p) \\ a^{kx}a^{(p-1)y} &\equiv a \ (mod\, p) \\ (a^k)^x(a^{(p-1)})^y &\equiv a \ (mod\, p) \end{aligned}$$

Da $p - 1 = \varphi(p)$ får vi fra Eulers theorem at $a^{\varphi(p)} \equiv 1 \pmod{p}$.

$$\begin{aligned} (a^k)^x(a^{\varphi})^y &\equiv a \ (mod\, p) \\ (a^k)^x(1^y) &\equiv a \ (mod\, p) \\ (a^k)^x &\equiv a \ (mod\, p) \end{aligned}$$

Og vi finder et x som er det n vi ønskede at finde.

Vi skal desuden vise den modsatte implikation, at hvis a^k er en primitiv rod af p, så er $gcd(k, p-1) = 1$.
Vi ved at der må findes et n så $a^{nk} \equiv a \pmod{p}$ eller at $a^{nk-1} \equiv 1 \pmod{p}$.
Vi kan skrive $nk - 1 = m * \varphi(p) + r \pmod{p}$.
Vi vil vise at $r = 0$ da dette betyder vi får $nk - 1 = m * \varphi(p)$ eller $nk + m * \varphi(p) = 1$ som så betyder at $gcd(k, \varphi(p)) = gcd(k, p-1) = 1$.

Ved at sætte begge sider af $nk-1 = m * \varphi(p) + r$ i potens af a får vi

$$a^{nk-1} \equiv a^{m*\varphi(p)+r} \ (mod\, p)$$
$$a^{nk-1} \equiv (a^{\varphi(p)})^m a^r \ (mod\, p)$$

Igen bruger vi Eulers theorem og får så

$$a^{nk-1} \equiv (a^{\varphi(p)})^m a^r \ (mod\, p)$$
$$a^{nk-1} \equiv 1^m a^r \ (mod\, p)$$
$$a^{nk-1} \equiv a^r \ (mod\, p)$$

Vi ved desuden, at $a^{nk-1} \equiv 1 \pmod{p}$. Og får så

$$1 \equiv a^r \ (mod\, p)$$

Dette medfører at $r = 0$ og derfor gælder denne implikation også.

Da alle primitive rødder vil være på formen a^k med et k der er indbyrdes primiske med $p-1$ betyder det at der vil være netop så mange primitive rødder som der er k indbyrdes primiske med $p-1$, hvilket jo netop er $\varphi(p-1)$. Desuden er $\varphi(p) = p-1$ for et primtal p. Altså må {**St**} Prop 2.5.12 gælde.

Opgave 2

Find alle primitive rødder modulo 19.

Vi bruger algoritme 2.5.16 i {**St**} til at finde de primitive rødder. Vi starter med at finde primtals faktoriseringen af $\varphi(p) = p - 1 = 18$.
Denne er $2*3^2$, altså er faktorene $p_i = \{2, 3\}$ og der er $\varphi(18) = 18(1-\frac{1}{2})(1-\frac{1}{3}) = 6$ primitive rødder.
Der skal altså gælde, at et tal a er en primitiv rod, hvis der gælder $a^{(p-1)/p_i} \not\equiv 1 \pmod{p}$ for alle p_i, hvor vi kigger på $2 \leq a \leq 18$. Følgende udregninger er modulo 19.

$$
\begin{array}{ll}
2^{18/2} = 18 & 2^{18/3} = 7 \\
3^{18/2} = 18 & 3^{18/3} = 7 \\
4^{18/2} = 1 & \\
5^{18/2} = 1 & \\
6^{18/2} = 1 & \\
7^{18/2} = 1 & \\
8^{18/2} = 18 & 8^{18/3} = 1 \\
9^{18/2} = 1 & \\
10^{18/2} = 18 & 10^{18/3} = 11 \\
11^{18/2} = 1 & \\
12^{18/2} = 18 & 12^{18/3} = 1 \\
13^{18/2} = 18 & 13^{18/3} = 11 \\
14^{18/2} = 18 & 14^{18/3} = 7 \\
15^{18/2} = 18 & 15^{18/3} = 11 \\
16^{18/2} = 1 & \\
17^{18/2} = 1 & \\
18^{18/2} = 18 & 18^{18/3} = 1
\end{array}
$$

Hvoraf de 6 tal der ikke giver 1 (mod 19) er nogle af tilfældende er tallene 2,3,10,13,14 og 15, som altså er de primiske rødder modulo 19.

Opgave 3

Antag at $a = -1$ eller a er en perfekt kvadrat. Vis at a ikke er en primitiv rod modulo p for noget primtal $p > 3$. Bemærk at dette forklarer antagelsen i Artins formodning ({**St**} Conjecture 2.5.14). Afgør desuden hvorvidt a er en primitiv rod modulo 3.

Hvis $a = -1$ set det let, at a ikke kan generere hele den multiplikative gruppe da den kun danner elementerne 1 og $p - 1$. Så hvis $p > 3$ kan den ikke være en primitiv rod. Hvis $p = 3$ vil $a = -1$ kunne være en primitiv rod, idet den genererer både 1 og $-1 = p - 1 = 2$.

Hvis a er et perfekt kvadrat. For at a er en primitiv rod, betyder det altså, at $a, a^2, a^3, .., a^{(p-1)}$ genererer alle tal $1, 2, 3, .., p-1$. Der gælder desuden at $a^{(p-1)} \equiv 1 \pmod{p}$.
For at vise at et perfekt kvadrat ikke er en primitiv rod, skal vi blot finde et modeksempel. Hvis 2 potenser af a giver samme rest mod p betyder det at hele den multiplikative gruppe $\mathbb{Z}/p\mathbb{Z}$ ikke bliver genereret.
Vi ser at $(a^2)^{(p-1)/2} = a^{p-1} \equiv 1 \pmod{p}$. Men vi ved allerede at $(a^2)^{(p-1)} \equiv 1 \pmod{p}$. Altså giver disse to potenser ($p-1$ og $\frac{p-1}{2}$) det samme resultat og hele den multiplikative gruppe bliver ikke genereret og dermed kan et perfekt kvadrat ikke være en primitiv rod.
Hvis $p = 3$ holder dette stadig ikke af samme argumentering da $(b^2)^{(p-1)/2} = (b^2)^{(p-1)}$ hvor vi ved disse to potenser er forskellige da $p - 1 = 2$.

Opgave 4

Vis den modsatte implikation af Miller-Rabin sætningen. Altså at hvis der for alle $a \not\equiv 0$ mod p gælder sætning (1) så er p et primtal.

Vi starter med at vise den første betingelse holder.

$$a^m \equiv 1 \, (mod \, p)$$

Ikke lavet.
Ide: At vise det ved hjælp af Fermats theorem, hvor $a^{p-1} \equiv 1 \pmod{p}$ og derved konkludere at i tilfælde hvor m kan skrives som sådan er p et primtal.

Og herefter, at den anden betingelse holder

$$a^{2^r m} \equiv -1 \, (mod \, p), 0 \leq r < k$$

Ikke lavet.
Ide: Vis at venstre side vil kunne skrives som $p-1$ i tilfælde hvor første betingelse ikke viste noget.