Ordningar och primitiva rötter

Låt $m > 0$ och $(a, m) = 1$.

Ordningen av a mod m, $\text{ord}_m a$, är det minsta positiva heltal k s.a $a^k \equiv 1 \mod m$.

Exempel: Tag $m = 15$, $a = 2$. $(a, m) = (2, 15) = 1$, så $\text{ord}_{15} 2$ existerar.

$2^1 = 2 \not\equiv 1 \mod 15$

$2^2 = 4 \not\equiv 1 \mod 15$

$2^3 = 8 \not\equiv 1 \mod 15$

$2^4 = 16 \equiv \underline{1} \mod 15$

Så $\text{ord}_{15} 2 = 4$.

Ordning har egenskaperi:

- $a^n \equiv 1 \mod m \iff \text{ord}_m a \mid n$, dvs $n = k \cdot \text{ord}_m a$ för något k.
- $a^i \equiv a^j \mod m \iff i \equiv j \mod \text{ord}_m a$
- $\text{ord}_m a^i = \dfrac{\text{ord}_m a}{(i, \text{ord}_m a)}$.
- $\text{ord}_m a \mid \varphi(m)$ I synnerhet $\text{ord}_m a \leq \varphi(m)$.

Låt $(r, m) = 1$.

r är en primitiv rot mod m om $\text{ord}_m r = \varphi(m)$.

Exempel: Tag $m=5$. Vi har

$2^1 = 2 \not\equiv 1 \mod 5$

$2^2 = 4 \not\equiv 1 \mod 5$

$2^3 = 8 \equiv 3 \not\equiv 1 \mod 5$

$2^4 = 16 \equiv 1 \mod 5$

$\operatorname{ord}_5 2 = 4 = \varphi(5)$

Så 2 är en primitiv rot mod 5.

Tag $m=8$. Talen a s.a $(a,8)=1$ ges upp till kongruens är 1, 3, 5, 7.

$1^1 \equiv 1 \mod 8$

$\operatorname{ord}_8 1 = 1$

$3^1 = 3 \not\equiv 1 \mod 8$

$3^2 = 9 \equiv 1 \mod 8$

$\operatorname{ord}_8 3 = 2$

$5^1 = 5 \not\equiv 1 \mod 8$

$5^2 = 25 \equiv 1 \mod 8$

$\operatorname{ord}_8 5 = 2$

$7^1 = 7 \not\equiv 1 \mod 8$

$7^2 = 49 \equiv 1 \mod 8$

$\operatorname{ord}_8 7 = 2.$

Finns inget a s.a $\operatorname{ord}_8 a = \varphi(8) = 4$, så det finns inga primitiva rötter mod 8.

- r är en primitiv rot mod m $\iff$ för varje a s.a. $(a,m)=1$ finns ett i s.a $a \equiv r^i \bmod m$.
Då $r^i \equiv r^j \bmod m \iff i \equiv j \bmod \operatorname{ord}_m r = \varphi(m)$ kan vi alltid välja i ovan bland $0,1,2,\dots,\varphi(m)-1$.

- r är en primitiv rot $\iff r^{\varphi(m)/q} \not\equiv 1 \bmod m$ för alla primtal $q \mid \varphi(m)$.

Satsen om primitiva rötter: Primitiva rötter mod m existerar omm $m = 1, 2, 4, p^n, 2p^n$ där p är ett udda primtal och $n \geq 1$.

- I synnerhet: Det finns alltid primitiva rötter mod ett primtal.
- Om primitiva rötter existerar mod m finns det $\varphi(\varphi(m))$ till kongruens mod m exakt primitiva rötter.
- Om r är en primitiv rot mod m ges de återstående sådana rötterna av r^i där $1 \leq i < \varphi(m)$ och $(i, \varphi(m)) = 1$.

Existens av primitiv rot mod m innebär att "multiplikation mod m beter sig som addition mod $\varphi(m)$".

Ett sätt att göra denna intuition konkret är med index:

Låt $(a,m)=1$ och låt r vara en primitiv rot mod m. Indexet av a relativt r, ind$_r a$, är det lägsta positiva heltal k s.a. $a \equiv r^k \bmod m$.

Index har egenskaper liknande de för logaritmer:

Låt $(a,m)=(b,m)=1$.

- $a \equiv b \mod m \iff ind_r a \equiv ind_r b \mod \varphi(m)$
- $ind_r 1 \equiv 0 \mod \varphi(m)$
- $ind_r r \equiv 1 \mod \varphi(m)$
- $ind_r(a \cdot b) \equiv ind_r a + ind_r b \mod \varphi(m)$
- $ind_r(a^n) \equiv n \cdot ind_r a \mod \varphi(m)$.

Obs: Indexräkning görs mod $\varphi(m)$! istället för mod m.