# 8.1 Ordenen til et tall

Eulers teorem: Hvis $\gcd(a,n)=1$ er $a^{\phi(n)} \equiv 1 \pmod{n}$. Men det kan finnes eksponenter $1 \leq k < \phi(n)$ med $a^k \equiv 1 \pmod{n}$.

Def: La $a \in \mathbb{Z}$ og $n \geq 1$ med $\gcd(a,n)=1$

(1) Ordenen til $a$ modulo $n$ er det minste tallet $k \geq 1$ med $a^k \equiv 1 \pmod{n}$

(2) Hvis ordenen til $a$ er $\phi(n)$ kalles $a$ en primitiv rot av $n$.

Eksempler: (1) Ordenen til 4 modulo 9:

$$4^1 \equiv 4 \pmod{9}$$
$$4^2 \equiv 7 \pmod{9}$$
$$4^3 \equiv 1 \pmod{9}$$

Så 4 har orden 3 modulo 9. Merk at $\phi(9)=6$, så 4 er ikke en primitiv rot av 9.

(2) Ordenen til 3 modulo 10:

$$3^1 \equiv 3 \pmod{10}$$
$$3^2 \equiv 9 \pmod{10}$$
$$3^3 \equiv 7 \pmod{10}$$
$$3^4 \equiv 1 \pmod{10}$$

Så 3 har orden 4 modulo 10. Siden $\phi(10)=4$ er 3 en pr. rot av 10.

(3) Ordenen til 1 modulo $n$ er 1.

Merk: (1) Definisjonen gir kun mening når $\gcd(a,n)=1$, for hvis $\gcd(a,n) \neq 1$ kan ikke $a^k \equiv 1 \pmod{n}$ for noen $k \geq 1$ (hvorfor?).

(2) Hvis $a$ har orden $k$ modulo $n$ og $a \equiv b \pmod{n}$, så har $b$ også orden $k$ modulo $n$, siden $a^i \equiv b^i \pmod{n}$ $\forall\, i \geq 1$.

(3) For å finne eventuelle primitive røtter av $n$ trenger vi fra (2) bare å sjekke de $a \in \{1,2,\ldots,n-1\}$ med $\gcd(a,n)=1$.

Eksempel: Har $n=8$ noen primitive røtter? Trenger da bare å sjekke de $a \in \{1,2,\ldots,7\}$ med $\gcd(a,8)=1$, dvs $a=1,3,5,7$:

$$1^1 \equiv 1 \pmod{8} \Rightarrow 1 \text{ har orden } 1$$
$$3^2 \equiv 1 \pmod{8} \Rightarrow 3 \text{ har orden } 2$$
$$5^2 \equiv 1 \pmod{8} \Rightarrow 5 \text{ har orden } 2$$
$$7^2 \equiv 1 \pmod{8} \Rightarrow 7 \text{ har orden } 2$$

Siden $\phi(8)=4$ har 8 ingen pr. røtter.

**Teorem 8.1** Anta $a$ har orden $k$ modulo $n$. Da gjelder

$$a^t \equiv 1 \pmod{n} \iff k \mid t$$

Spesielt vil $k \mid \phi(n)$

Bevis: Anta $k \mid t$, dvs $t = km$ for en $m \geq 1$. Siden $a^k \equiv 1 \pmod{n}$ er da

$$a^t \equiv a^{km} \equiv (a^k)^m \equiv 1^m \equiv 1 \pmod{n}$$

Anta motsatt at $k \nmid t$. Da er $t = mk + r$ hvor $1 \leq r \leq k-1$ ($r \neq 0$ siden $k \nmid t$). Siden $a^k \equiv 1 \pmod{n}$ får vi da

$$a^t \equiv a^{mk+r} \equiv a^{mk} \cdot a^r \equiv (a^k)^m \cdot a^r \equiv a^r \pmod{n}.$$

Dersom da $a^t \equiv 1 \pmod{n}$, vil $a^r \equiv 1 \pmod{n}$, umulig (hvorfor?) □

Merk: For å finne ordenen til $a$ modulo $n$ trenger vi bare å lete blant divisorene til $\phi(n)$.

Eksempel: Siden $\phi(9) = 6$ vil et tall $a$ med $\gcd(a,9) = 1$ har orden 1, 2, 3 eller 6 modulo 9. For $a = 5$:

$$5^1 \equiv 5 \pmod{9}$$
$$5^2 \equiv 7 \pmod{9}$$
$$5^3 \equiv 8 \pmod{9}$$

Det betyr at 5 må ha orden 6 modulo 9. Spesielt er 5 en pr. rot av 9.

**Teorem 8.2 / 83**

Anta $a$ har orden $k$ modulo $n$

(1) $a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{k}$

(2) $a^t$ har orden $k/\gcd(k,t)$ modulo $n$ (viktig i gruppeteori)

Korollar: Hvis $a$ har orden $k$ modulo $n$, så er tallene

$$a, a^2, \ldots, a^k$$

inkongruente modulo $n$.

Bevis: Anta $a^i \equiv a^j \pmod{n}$ med $i, j \in \{1, 2, \ldots, k\}$. Fra Teorem 8.2 er da $i \equiv j \pmod{k}$, dvs $k \mid (i-j)$. Da må $i = j$. □

Eksempel: Så at 5 har orden 6 modulo 9 (så 5 er en pr. rot av 9 siden $\phi(9) = 6$).

Da sier korollaret at $5, 5^2, 5^3, 5^4, 5^5, 5^6$ er inkongr modulo 9. Stemmer, siden

$5 \equiv 5 \pmod{9}$ $\quad 5^4 \equiv 4 \pmod{9}$

$5^2 \equiv 7 \pmod{9}$ $\quad 5^5 \equiv 2 \pmod{9}$

$5^3 \equiv 8 \pmod{9}$ $\quad 5^6 \equiv 1 \pmod{9}$

Merk at $\{1, 2, 4, 5, 7, 8\}$ er de tallene $a \in \{1, 2, \ldots, 9\}$ med $\gcd(a,9) = 1$.

**Teorem 8.4** La $\gcd(a,n)=1$ og $n_1, n_2, \ldots, n_{\phi(n)}$ være elementene i $\{1,2,\ldots,n\}$ relativt primiske med $n$. Hvis $a$ er en pr.rot av $n$, så er tallene

$$a, a^2, \ldots, a^{\phi(n)}$$

kongr med

$$n_1, n_2, \ldots, n_{\phi(n)}$$

modulo $n$ i en eller annen rekkefølge.

**Korollar:** Hvis $n$ har en primitiv rot, så har den $\phi(\phi(n))$ stykker (modulo $n$)

**Eksempel:** Vi så at 9 har en pr.rot, nemlig 5. Da har 9 $\phi(\phi(9))=\phi(6)=2$ primitive rotter (modulo 9). Så to av tallene $\{1,2,\ldots,8\}$ er primitive røtter av 9. Den ene er 5, finn den andre.

**Skal se:** $p$ primtall $\Rightarrow$ $p$ har primitive røtter (og da $\phi(\phi(p)) = \phi(p-1)$ stykker fra korollaret).

**Formodning** (Artin)

La $a$ være et tall som ikke er et kvadrat og $a \neq 1, -1$. Da er $a$ en primitiv rot for $\infty$ mange primtall.

Altså sier formodningen at det skal finnes $\infty$ mange primtall $p$ slik at $a$ har orden $p-1$ modulo $p$. Status: uløst problem. Faktisk har ingen klart å finne et eneste tall $a$ som er en pr.rot for $\infty$ mange primtall.