Eulers teorem

Har: $U(\mathbb{Z}/n\mathbb{Z}) = \{r + n\mathbb{Z} \mid r \in \{1, 2, \ldots, n\} \text{ med } \gcd(r, n) = 1\}$

Eulers phi-funksjon

$\varphi(n) = |\{r \in \mathbb{Z} \mid 1 \leq r \leq n \text{ med } \gcd(r, n) = 1\}|$

Merk: $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$

- $\varphi(p) = p - 1$ $\quad$ p primtall
- $\varphi(p^n) = p^n - p^{n-1}$
- $\varphi(mn) = \varphi(m)\varphi(n)$, $\gcd(m, n) = 1$

Setning 67 (Eulers teorem 20.8)

La $n > 1$, $a \in \mathbb{Z}$ med $\gcd(a, n) = 1$. Da er

$$a^{\varphi(n)} \equiv 1 \mod n.$$

Bevis: La $a \in \mathbb{Z}$ slik at $a + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$, (orden $\varphi(n)$)

Da er

$$(a + n\mathbb{Z})^{\varphi(n)} = a^{\varphi(n)} + n\mathbb{Z} = 1 + n\mathbb{Z},$$

siden $|U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$ (Lagrange teorem)

dvs, $a^{\varphi(n)} \equiv 1 \mod n$

Bruker: $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$

$\Rightarrow$ $a + n\mathbb{Z} \in U(\mathbb{Z}/n\mathbb{Z})$

$\Updownarrow$

$\bar{a} \in \mathbb{Z}_n$ sa er $\bar{a} \in U(\mathbb{Z}_n)$

$\Updownarrow$

$\gcd(a, n) = 1$. $\square$