Motivasjon
Eulers phi-funksjon

$$\varphi(n) = \left|\{ i \mid 1 \le i \le n,\ \gcd(i,n) = 1\}\right|, \quad 1 \le n \in \mathbb{Z}.$$

Har: $\cdot$ $\varphi(p) = p-1$, $\quad p$ primtall

$\cdot$ $\varphi(p^n) = p^n - p^{n-1}$ $\quad (\gcd(i,p^n)=1 \Leftrightarrow \gcd(i,p)=1)$

$\cdot$ $\varphi(mn) = \varphi(m)\varphi(n)$, når $\gcd(m,n)=1$.

Dette gir: $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, p_i primtall, $p_i \neq p_j$, $i \neq j$.

$$\varphi(n) = \varphi(p_1^{n_1}) \cdots \varphi(p_t^{n_t})$$
$$= (p_1^{n_1} - p_1^{n_1-1}) \cdots (p_t^{n_t} - p_t^{n_t-1}).$$

$(\mathbb{Z}_n, +)$ gruppe, men har også multiplikasjon.
Men, $(\mathbb{Z}_n, \cdot)$ er det ikke en gruppe.

Vet: $\langle \bar{r} \rangle = \mathbb{Z}_n \Longleftrightarrow \gcd(r,n) = 1 \leftarrow$ antall slike er lik $\varphi(n)$.

$\Updownarrow$

$\exists s$ slik at $s\bar{r} = \bar{1} \Longleftrightarrow \bar{r}$ invertibel mhp. $\cdot$

$s\bar{r} = \bar{s}\cdot\bar{r}$

Har sett: $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ når $\gcd(m,n)=1$
som grupper.
Samme avbilding bevarer multiplikasjon.

$x = (\bar{x}_1, \bar{x}_2) \in \mathbb{Z}_m \times \mathbb{Z}_n$ invertibel $\Leftrightarrow$ $\bar{x}_1$ og $\bar{x}_2$ invertible.

$$\Big[\underset{\substack{\uparrow \\ \text{Antall invert.} \\ \text{elem. } \varphi(m)}}{\mathbb{Z}_m} \times \underset{\substack{\uparrow \\ \text{Antall invert} \\ \text{elem } \varphi(n)}}{\mathbb{Z}_n} \simeq \mathbb{Z}_{mn}\Big]$$

Antall invert. elem $\varphi(m)\varphi(n) = \varphi(mn)$.