

- $G_m := [x_m] \in Z_m : ggT(x, m) = 1$
 - Repräsentantensystem $R := 0, 1, \dots, m-1$ ### Eulersche Phi-Funktion
- $\varphi(m) := |G_m| = |\{k \in R : ggT(k, m) = 1\}|$
- $p \in P \implies ggT(k, p) = 1$ für alle $k \implies \varphi(p) = p-1$
- Laut Primfaktorzerlegung gilt für $m \in \mathbb{N}, m \geq 2$
 - $m = p_1^{k_1} \dots p_r^{k_r}$
 - $\varphi(p) = p_1^{k_1-1}(p_1-1) \dots p_r^{k_r-1}(p_r-1)$
 - * $\varphi(p) = \prod_{i=1}^k p_i^{l_i-1}(p_i-1)$
- für $ggT(p, n) = 1$ gilt
 - $a^{p-1} \equiv_p 1$
 - Beweis

Beweis Sei $G_p = \mathbb{Z}_p \setminus \{[0]_p\} = \{[1]_p, [2]_p, \dots, [p-1]_p\}$ Daraus folgt $[x]_p = [x]_p$

(A) Abbildung $f_a: G_p \rightarrow G_p$
 $[x]_p \mapsto f_a([x]_p) = [ax]_p$
 (A1) Injektivität: Angenommen für $[x]_p, [y]_p \in G_p$
 $f_a([x]_p) = f_a([y]_p) \implies [ax]_p = [ay]_p$
 D.h. $[a(x-y)]_p = [0]_p$
 Da $a \in G_p$ ist $a \cdot (x-y) \equiv 0 \pmod p$
 Da a invertierbar ist $x-y \equiv 0 \pmod p$
 D.h. $[x]_p = [y]_p$

(A2) Surjektivität: Sei $[y]_p \in G_p$. Dann existiert $[x]_p \in G_p$ mit $[ax]_p = [y]_p$.
 (A3) Assoziativität: $[a(bx)]_p = [(ab)x]_p = [a]_p \cdot [bx]_p = [a]_p \cdot [b]_p \cdot [x]_p = [ab]_p \cdot [x]_p$

(B) Sei $a \in G_p$. Dann ist f_a bijektiv. Wir betrachten f_a^{-1} .
 $f_a^{-1}([a]_p) = [1]_p$
 $f_a^{-1}([2]_p) = [a^{-1} \cdot 2]_p$
 \vdots
 $f_a^{-1}([p-1]_p) = [a^{-1} \cdot (p-1)]_p$
 D.h. f_a^{-1} ist eine Permutation von G_p .
 Die Abbildung f_a^{-1} ist assoziativ.
 $f_a^{-1} \circ f_a = \text{id}$
 $f_a \circ f_a^{-1} = \text{id}$
 D.h. f_a^{-1} ist die Umkehrabbildung von f_a .
 Da f_a assoziativ ist, gilt auch f_a^{-1} assoziativ.
 D.h. f_a^{-1} ist ein Element der Gruppe (G_p, \cdot) .
 D.h. $a^{-1} \in G_p$.
 D.h. $a \cdot a^{-1} = 1$ in G_p .
 D.h. $a^{p-1} = 1$ in G_p .
 D.h. $a^{p-1} \equiv 1 \pmod p$.

Satz von Euler-Fermat

- $a^{\varphi(m)} \equiv_m 1$
- $a^{l(p-1)(q-1)+1} \equiv_{pq} a$
 - p, q unterschiedliche Primzahlen

[[Kryptographie]]