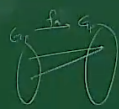
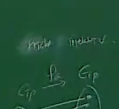


- $G_m := [x_m] \in Z_m : ggT(x, m) = 1$ 
  - Repräsentantensystem  $R := 0, 1, \dots, m - 1$  ### Eulersche Phi-Funktion
- $\varphi(m) := |G_m| = |\{k \in R : ggT(k, m) = 1\}|$
- $p \text{ Prim} \Rightarrow ggT(k, p) = 1 \text{ für alle } k \Rightarrow \varphi(p) = p - 1$
- Laut Primfaktorzerlegung gilt für  $m$ ,  $m \geq 2$ 
  - $m = p_1^{k_1} \dots p_r^{k_r}$
  - $\varphi(p) = p_1^{k_1-1}(p_1 - 1) \dots p_r^{k_r-1}(p_r - 1)$
  - \*  $\varphi(p) = \prod_{i=1}^k p_i^{l_i-1}(p_i - 1)$
- 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  $f_a: G_p \rightarrow G_p$   
 $[x]_p \mapsto f_a([x]_p) = [ax]_p$   
 1. bijektiv  
 (A1) Injektivität: Angenommen für  $[x]_p, [y]_p \in G_p$   
 gilt  $f_a([x]_p) = f_a([y]_p)$   
 d.h.  $[ax]_p = [ay]_p$

(A2)   


Sei  $[y]_p \in G_p$  beliebig.  
 Da  $\exists! (p, a) = 1$  gilt es  $[y]_p \in G_p$  s.d.  
 $[ay]_p = [x]_p$  (A2)  
 d.h.  $\exists! (p, a) = 1$  ist  $[ay]_p$  invertierbar  
 d.h.  $\exists [a]_p^{-1} \in G_p$   
 $[a]_p^{-1} \cdot [ay]_p = [x]_p$

Nun betrachten wir  
 $f_a([a \cdot b]_p) = [a \cdot (b \cdot y)]_p$   
 $\stackrel{\text{def } f_a}{=} [a \cdot (b \cdot y)]_p$   
 $\stackrel{(\mathbb{Z}, \cdot) \text{ assoziativ}}{=} [(a \cdot b) \cdot y]_p$   
 $\stackrel{(\mathbb{Z}, \cdot) \text{ assoziativ}}{=} [a \cdot b]_p \cdot [y]_p$  zu  $[y]_p \in G_p \exists [y]_p^{-1} \in G_p$  s.d.  
 $f_a([a \cdot b]_p) = [a]_p \cdot [y]_p$

(B) weil  $f_a: G_p \rightarrow G_p$ ,  $[x]_p \mapsto [ax]_p$ , bijektiv ist,  
 gilt  
 $\{[1]_p, [2]_p, \dots, [p-1]_p\} \xrightarrow{\text{bijektiv}} \{[a \cdot 1]_p, [a \cdot 2]_p, \dots, [a \cdot (p-1)]_p\}$   
 Daher gilt  
 $[1]_p \cdot [2]_p \cdot \dots \cdot [p-1]_p = [a \cdot 1]_p \cdot [a \cdot 2]_p \cdot \dots \cdot [a \cdot (p-1)]_p$   
 $[1 \cdot 2 \cdot \dots \cdot (p-1)]_p = [a^p \cdot (1 \cdot 2 \cdot \dots \cdot (p-1))]_p$   
 $[1 \cdot 2 \cdot \dots \cdot (p-1)]_p = [a^p \cdot (1 \cdot 2 \cdot \dots \cdot (p-1))]_p$   
 $[1 \cdot 2 \cdot \dots \cdot (p-1)]_p \cdot [1 \cdot 2 \cdot \dots \cdot (p-1)]_p^{-1} = [a^p \cdot (1 \cdot 2 \cdot \dots \cdot (p-1))]_p \cdot [1 \cdot 2 \cdot \dots \cdot (p-1)]_p^{-1}$   
 Dann folgt  
 $[1]_p = [a^p]_p$   
 $[1]_p = [a^p]_p$   
 $[1]_p = [a^p]_p$   
 $[1]_p = [a^p]_p$

Daraus folgt  $[a^p]_p = [1]_p$  und  $p \mid a^p - 1$   
 also  $a^p \equiv 1 \pmod p$   
 für  $m \in \mathbb{N}$  mit  $\text{ggT}(m, p) = 1$   
 $a^{(m)} \equiv 1 \pmod m$   
 somit gilt  $a^m \equiv 1 \pmod m$   
 (1.2)  $f(x) = x^m = 1 \pmod m$

## 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]]