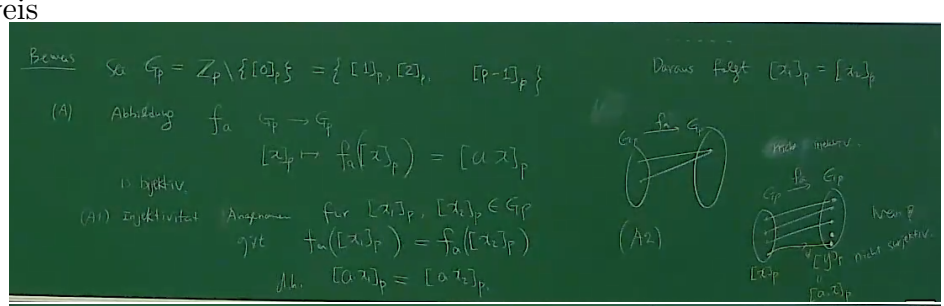
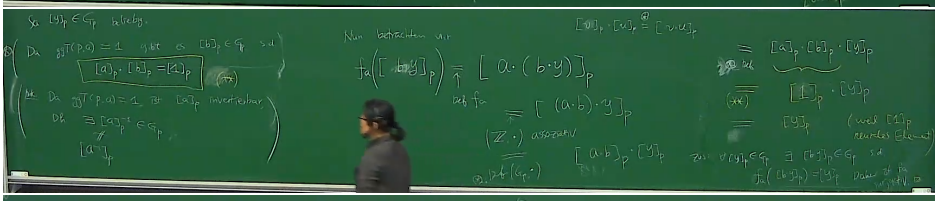
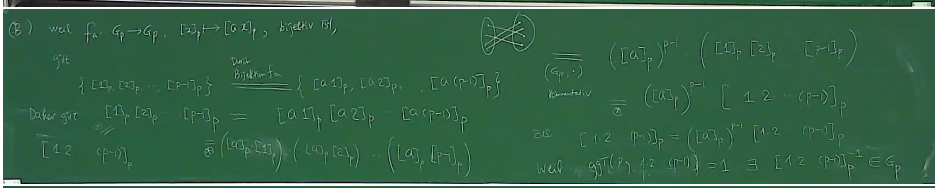
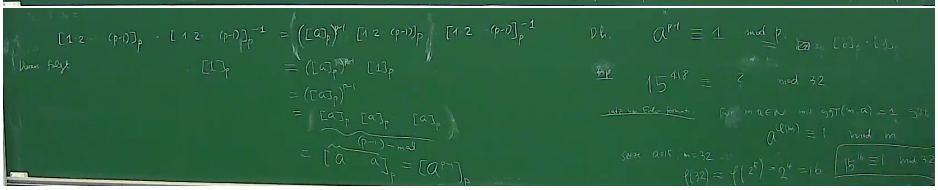
- $G_m := [x_m] \in Z_m : ggT(x,m) = 1$
  - Repräsentantensystem $R := 0, 1, ..., m-1$ ### Eulersche Phi-Funktion
- $\varphi(m) := |G_m| = |k \in R : ggT(k,m) = 1|$
- p∈P ==> $ggT(k,p) = 1$ für alle k ==> $\varphi(p) = p-1$
- Laut Primfaktorzerlegung gilt für m∈ℕ, m≥2
  - $m = p_1^{k_1} ... p_r^{k_r}$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

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]]