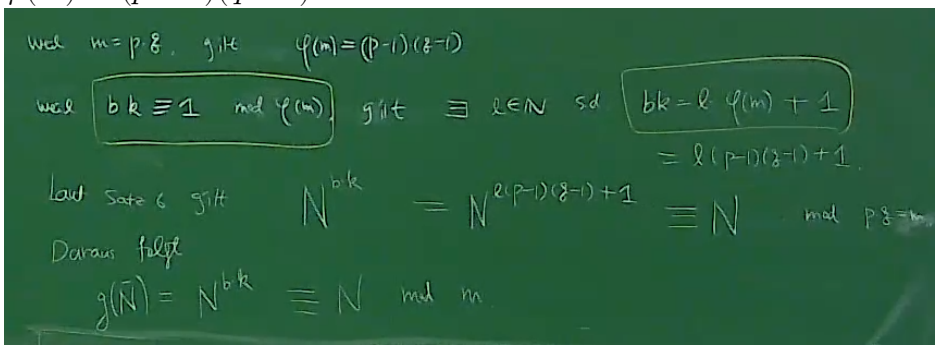
- m,k∈ℕ mit ggT(m,k)=1, m=pq
  - öffentlich
  - p,q sind unterschiedliche Primzahlen
  - N ursprüngliche Nachricht
  - N' verschlüsselte Nachricht
- Alice's Verschlüsselungsfunktion
  - $f : 1, ..., m-1 -> 1, ..., m-1$
  - x –> x^k mod m
- Bob wählt geheime Zahl b∈ℕ mit bk ≡ 1 mod φ(m)
- Bob's Entschlüsselfunktion:
  - $g : 1, ..., m-1 -> 1, ..., m-1$
  - x –> x^b mod m
- [[Satz von Euler-Fermat]]
  - $\varphi(m) = (p-1)(q-1)$
  - 

[[Kryptographie]]