## Der kleine Fermat

Sei p prim und sei $a \in \mathbb{Z}$, sodass p kein Teiler von a ist, dann:
$a^{p-1} \equiv 1 (mod\ p)$

**Beweis:** $|\mathbb{Z}_p^*| = p - 1$
b:=(a mod p)$\in |\mathbb{Z}_p^*|$
$b^{|\mathbb{Z}_p^*|}$=1
$a^{p-1} \equiv 1 (mod\ p)$

## Der Satz von Euler-Fermat

Der kleine Fermat nur ohne die Bedingung, dass $|\mathbb{Z}_p^*|$, mit p prim.
**Satz:** Sei nun b beliebig und ggT(a,n)=1
Dann: $a^{\phi(n)} \equiv 1 (mod\ n)$
$|\mathbb{Z}_n^*| = \phi(n)$
b:= (a mod n)$\in |\mathbb{Z}_n^*|$
$b^{\phi(n)} = 1$
$a^{\phi(n)} \equiv 1 (mod\ n)$
Der Satz findet Anwendung innerhalb des Verschlüsselungsverfahren RSA.