Fermat's kleines Theorem (siehe Skript S. 11.3/45)

Sei p eine Primzahl.

1. Ist **a relativ prim zu p**, dann gilt:

$$\mathbf{a^{p-1} \equiv 1 \pmod{p}}$$

2. $a^p \equiv a \pmod{p}$ für **alle a ∈ Z**.

Frage: Was bedeutet Aussage 1?

Antwort: Jede große Zahl a^{p-1} kann durch 1 ersetzt werden.

Beispiel

a = 2, p = 7 $\Rightarrow$ a und p sind relativ prim

Berechne 2^{25} mod 7 unter Benutzung von Fermat's Theorem.

Versuche, den Exponent e = 25 so zu zerlegen, dass er Terme der Form $a^{p-1} = 2^6$ enthält. Das ist einfach:

$$2^{25} = 2^6 \cdot 2^6 \cdot 2^6 \cdot 2^6 \cdot 2^1$$

Nach Fermat's Theorem kann jeder Term 2^6 durch 1 ersetzt werden, so dass statt 2^{25} nur noch 2^1 (mod p) berechnet werden muss.

Rechnung: $2^{25} = 2^6 \cdot 2^6 \cdot 2^6 \cdot 2^6 \cdot 2^1 \pmod 7 = 2^1 \pmod 7 \equiv 2$

Probe: $2^{25} = 33554432 \pmod 7 \equiv 2$

Das bedeutet, der Exponent e = 25 wird modulo 6 reduziert

Nach Fermat's kleinem Theorem gilt somit für a mod p ≠ 0:

$$a^e \bmod p = a^{e \bmod (p-1)} \bmod p$$

Damit lassen sich sehr große Zahlen extrem stark durch Anwendung von modulo (p-1) reduzieren.