Eulersches Theorem (siehe Skript S. 11.3/54)

Fermat's kleines Theorem:

Sei p eine Primzahl.

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

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

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

Eulersches Theorem:

Seien p und q verschiedene Primzahlen.

1. Ist a relativ prim zu pq , dann gilt für alle $k \in \mathbb{Z}$:

$$a^{k(p-1)(q-1)} \equiv 1 \pmod{pq}$$

2. Für alle $a \in \mathbb{Z}$ gilt:

$$a^{k(p-1)(q-1)+1} \equiv a \pmod{pq}$$

wobei $k \in \mathbb{N}$.

Das Theorem kann sehr einfach aus Fermat's kleinem Theorem abgeleitet werden (siehe Skript S. 11.3/55-56)

Das Produkt zweier Primzahlen $p \cdot q$ wird verwendet, um einen Exponenten $e \cdot d$ durch eine Folge von Faktoren auszudrücken:

$$e \cdot d = k \cdot (p-1) \cdot (q-1) + 1$$

Hat man zwei Primzahlen p und q , so kann man damit Zahlen $e \cdot d = k \cdot (p-1) \cdot (q-1) + 1$ erzeugen, so dass das Eulersche Theorem erfüllt ist.

Mit Hilfe zweier Primzahlen p und q kann man nun Exponenten erzeugen, die das Eulersche Theorem erfüllen.

Beispiel

$$p = 5, q = 7, p \cdot q = 35$$

$$\Rightarrow 145 = 6 \cdot (p-1) \cdot (q-1) + 1 = 6 \cdot 4 \cdot 6 + 1 = 144 + 1$$

$$\Rightarrow x^{145} \equiv x \pmod{35}$$

Kennt man die Primfaktoren von 145, sie lauten $e=5$ und $d=29$, so kann man wegen Eulers Theorem schreiben:

$$x^{e \cdot d} = x^{145} = (x^5)^{29} = x^{5 \cdot 29} \equiv x \pmod{35}$$

Aus $y = x^5 \pmod{35}$ und $y^{29} \pmod{35}$ kann x mit Hilfe des Eulerschen Theorems zurückberechnet werden:

$$y^{29} \equiv (x^5)^{29} = x^{5 \cdot 29} = x^{145} \equiv x \pmod{35}$$

Wichtig: wähle Exponenten wie 145, die das Eulersche Theorem erfüllen!