

Umkehrung des Kleinen Satzes von Fermat

Kleiner Satz von Fermat:

Ist $a \in \mathbb{N}$ kein Vielfaches der Primzahl p , so ist $a^{p-1} \equiv 1 \pmod{p}$.

Die folgende Umkehrung des Kleinen Satzes von Fermat gilt **nicht**:

Gilt für alle Zahlen $a \in \mathbb{N}$ mit $\text{ggT}(a, n) = 1$: $a^{n-1} \equiv 1 \pmod{n}$, dann ist n eine Primzahl.

Bei einem möglichen Primzahltest reicht es, alle Zahlen $a \in \mathbb{N}$ mit $1 < a < n - 1$ zu überprüfen:

- $a = 1$ muss nicht überprüft werden: $1^{n-1} \equiv 1 \pmod{n}$
- $a = n - 1$ muss nicht überprüft werden: $(n - 1)^{(n-1)} \equiv 1 \pmod{n}$
 - $n - 1 \equiv n - 1 \pmod{n}$
 - $(n - 1)^2 \equiv n^2 - 2n + 1 \equiv n \cdot (n - 2) + 1 \equiv 1 \pmod{n}$
 - $(n - 1)^3 \equiv 1 \cdot (n - 1) \equiv n - 1 \pmod{n}$
 - $(n - 1)^4 \equiv (n - 1)^2 \equiv 1 \pmod{n}$
 - ...
 - $(n - 1)^{\text{ungerade}} \equiv n - 1 \pmod{n}$
 - $(n - 1)^{\text{gerade}} \equiv 1 \pmod{n}$

n *gerade* $\Rightarrow \text{ggT}(2, n) = 2$

\Rightarrow Test sollte schon eher entscheiden: n *zusammengesetzt*

n *ungerade* ($n - 1$ ist dann gerade): $(n - 1)^{(n-1)} \equiv 1 \pmod{n}$

- $a = n$ muss nicht überprüft werden: $\text{ggT}(n, n) = n$

- **$a > n$ muss nicht überprüft werden:** **Es entstehen keine neuen Reste.**

$a > n$ und $\text{ggT}(a, n) = 1 \Rightarrow$ Es gibt Zahlen $b, c \in \mathbb{N}$
und $1 \leq c < n$, so dass **$a = bn + c$**

Es gilt: $\text{ggT}(bn + c, n) = 1 \Rightarrow (bn + c)^{(n-1)} \equiv c^{n-1} \pmod{n}$

$$bn + c \equiv c \pmod{n}$$

$$(bn + c)^2 \equiv b^2n^2 + 2bnc + c^2 \equiv c^2 \pmod{n}$$

$$(bn + c)^3 \equiv c^3 \pmod{n}$$

$$(bn + c)^4 \equiv c^4 \pmod{n}$$

...

$$(bn + c)^{n-1} \equiv c^{n-1} \pmod{n}$$

***Es gilt schon: Für alle $a \in \mathbb{N}$ ($1 < a < n - 1$) mit $\text{ggT}(a, n) = 1$:
 $a^{n-1} \equiv 1 \pmod{n}$***

\Rightarrow Die Zahlen $c \in \{1, 2, \dots, n - 1\}$ wurden schon getestet:
 $\text{ggT}(c, n) = 1 \Rightarrow c^{n-1} \equiv 1 \pmod{n}$

\Rightarrow **Wenn schon für alle $a < n$ alle Potenzen bei Division durch n den Rest 1 lassen, so auch alle Potenzen mit $a > n$.**