

Beweis des Kleinen Satzes von Fermat

Kleiner Satz von Fermat:

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

Voraussetzung: $a \in \mathbb{N}$ und $\text{ggT}(a, p) = 1$ (a und p sind teilerfremd)

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

Beweis:

Bei Division einer zu p teilerfremden Zahl durch p können nur die Reste

$$1, 2, 3, 4, \dots, p-1$$

aufzutreten.

(Rest 0 würde bedeuten, dass die Zahl ein Vielfaches von p ist.)

Menge aller von Null verschiedenen Reste bei Division durch p : $\{1, 2, 3, 4, \dots, p-1\}$

Alle diese $p-1$ Reste sind **kleiner** als p . Außerdem ist p eine **Primzahl**.

\Rightarrow Die Zahlen $1, 2, 3, 4, \dots, p-1$ sind alle **teilerfremd zu p** .

äquivalent: $\text{ggT}(1, p) = 1$; $\text{ggT}(2, p) = 1$; ... ; $\text{ggT}(p-1, p) = 1$

Deswegen und da a kein Vielfaches von p ist, gilt mit

$$r_i \in \{1, 2, 3, 4, \dots, p-1\} \quad (i = 1, 2, \dots, p-1)$$

$$\begin{aligned} 1a \text{ kein Vielfaches von } p &\Rightarrow 1a \text{ lässt bei Division durch } p \text{ einen Rest ungleich Null} \\ &\Rightarrow \mathbf{1a \equiv r_1 \pmod{p}} \end{aligned}$$

$$\begin{aligned} 2a \text{ kein Vielfaches von } p &\Rightarrow 2a \text{ lässt bei Division durch } p \text{ einen Rest ungleich Null} \\ &\Rightarrow \mathbf{2a \equiv r_2 \pmod{p}} \end{aligned}$$

$$\begin{aligned} 3a \text{ kein Vielfaches von } p &\Rightarrow 3a \text{ lässt bei Division durch } p \text{ einen Rest ungleich Null} \\ &\Rightarrow \mathbf{3a \equiv r_3 \pmod{p}} \end{aligned}$$

...

$$\begin{aligned} (p-1)a \text{ kein Vielfaches von } p &\Rightarrow (p-1)a \text{ lässt bei Division durch } p \text{ einen Rest ungleich Null} \\ &\Rightarrow \mathbf{(p-1)a \equiv r_{p-1} \pmod{p}} \end{aligned}$$

Man kann nicht sagen, dass z.B. bei Division von $3a$ durch p genau der Rest 3 entsteht, aber:

Bei Division der Zahlen $a, 2a, 3a, \dots, (p-1)a$ durch p tritt jeder Rest

$$1, 2, 3, 4, \dots, p-1$$

genau einmal auf:

(Auf der rechten Seite der Kongruenzen stehen alles verschiedene Zahlen.)

Angenommen zwei Reste der rechten Seite der Kongruenzen wären gleich:

$$r_i = r_j \text{ mit } i \neq j \quad i, j \in \{1, 2, 3, 4, \dots, p-1\}$$

$$ia \equiv r_i \pmod{p} \quad \text{und} \quad ja \equiv r_j \pmod{p} \Rightarrow ia \equiv ja \pmod{p}$$

(siehe Kongruenzen 3. Rechenregel)

$$\text{ggT}(a, p) = 1 \quad \Rightarrow \quad \text{man kann durch } a \text{ teilen} \quad \Rightarrow \quad i \equiv j \pmod{p}$$

(siehe Kongruenzen 9. Rechenregel)

$$i \text{ und } j \text{ sind } \textit{kleiner} \text{ als } p \quad \Rightarrow \quad i = j \quad \Rightarrow \quad \textit{Widerspruch}$$

\Rightarrow *Auf der rechten Seite der Kongruenzen tritt jeder Rest*
1, 2, 3, 4, ..., p-1 genau einmal auf.

$$1a \equiv r_1 \pmod{p}$$

$$2a \equiv r_2 \pmod{p}$$

$$3a \equiv r_3 \pmod{p}$$

...

$$(p-1)a \equiv r_{p-1} \pmod{p}$$

Kongruenzen kann man multiplizieren: *(siehe Kongruenzen 6. Rechenregel)*

$$1a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv r_1 \cdot r_2 \cdot r_3 \cdot \dots \cdot r_{p-1} \pmod{p}$$

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$$

(jeder Rest genau einmal vorhanden)

Da die Reste $1, 2, 3, 4, \dots, p-1$ alle zu p teilerfremd sind, kann man durch $1, 2, 3, 4, \dots, p-1$ teilen: *(siehe Kongruenzen 9. Rechenregel)*

$$\Rightarrow \quad \mathbf{a^{p-1} \equiv 1 \pmod{p}} \quad \textit{q.e.d.}$$