

Kleiner Satz von Fermat

Satz Kleiner Satz von Fermat

Sei $p \in \mathbb{P}$. Dann gilt

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

Beweis:

- Wir führen zunächst eine Induktion für $a \geq 0$ durch.
- **IA** $a = 0$: $0^p \equiv 0 \pmod{p}$.
- **IS** $a \rightarrow a + 1$: Nach vorigem Lemma gilt
$$(a + 1)^p \equiv a^p + 1^p \equiv a + 1 \pmod{p}.$$
- Damit gilt der Satz für alle $a \in \mathbb{N}_0$.
- Für $a < 0$ gilt $(-a)^p \equiv -a \pmod{p}$ mit $-a > 0$.
- Für $p = 2$ ist $-a \equiv -a + 2a = a \pmod{p}$. Daraus folgt die Aussage.
- Für ungerades p folgt

$$-a \equiv (-a)^p = (-1)^p a^p = -a^p \pmod{p}.$$

- Multiplikation mit (-1) liefert die gewünschte Identität.

Kleiner Satz von Fermat

Korollar Kleiner Satz von Fermat (Variante)

Sei $p \in \mathbb{P}$. Dann gilt

$$a^{p-1} \equiv 1 \pmod{p} \text{ f\u00fcr alle } a \in \mathbb{Z} \text{ mit } p \nmid a.$$

Beweis:

- Wir wissen $p \mid a^p - a$ bzw. $p \mid a(a^p - 1)$.
- Da p prim und $p \nmid a$ folgt $p \mid a^p - 1$ und damit $a^{p-1} \equiv 1 \pmod{p}$.

Anwendung:

- Bei Rechnung modulo p reduziere Exponenten modulo $p - 1$.
- Modulo $p = 5$ gilt z.B.

$$2^{99} = 2^{3+96} = 2^3 \cdot (2^4)^{24} \equiv 2^3 \cdot 1^{24} = 2^3 \equiv 3 \pmod{5}.$$

Lemma über Teiler und Vielfache

Für $a, b \in \mathbb{Z}$ und $n, m \in \mathbb{N}$ gilt:

- 1 Falls $a \equiv b \pmod{n}$ und $m|n$, dann ist $a \equiv b \pmod{m}$.
- 2 Es gilt $a \equiv b \pmod{n}$ gdw $ma \equiv mb \pmod{mn}$.

Beweis:

(1) Aus $n|a - b$ und $m|n$ folgt $m|a - b$.

(2) \Rightarrow : Aus $n|a - b$ folgt $mn|m(a - b)$.

\Leftarrow : Aus $nm|m(a - b)$ folgt $nmc = m(a - b)$ und damit $nc = a - b$.

Lösbarkeit linearer Gleichungen

Satz Lösbarkeit linearer Gleichungen

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $ax \equiv b \pmod{n}$. Sei $d = \text{ggT}(a, n)$.

- 1 Falls eine Lösung $x \in \mathbb{Z}$ existiert, so gilt $d \mid b$.
- 2 Sei $d \mid b$. Seien $y, z \in \mathbb{Z}$ mit $ya + zn = \text{ggT}(a, n) = d$.
Ein $x \in \mathbb{Z}$ ist Lösung gdw

$$x \equiv y \frac{b}{d} \pmod{\frac{n}{d}}.$$

Beweis:

- (1) Sei x eine Lösung mit $ax \equiv b \pmod{n}$. Dann gilt $ax = b + kn$ bzw.
 $b = ax - kn$.

$d = \text{ggT}(a, n)$ teilt beide Summanden rechts. Damit gilt $d \mid b$.

- (2) \Leftarrow : Sei $x \equiv y \frac{b}{d} \pmod{\frac{n}{d}}$. Dann gilt

$$ax \equiv ay \cdot \frac{b}{d} \equiv (d - zn) \cdot \frac{b}{d} \equiv b - zn \frac{b}{d} \pmod{\frac{a}{d}n}$$

Damit folgt $ax \equiv b \pmod{n}$, d.h. x ist eine Lösung.

Lösbarkeit linearer Gleichungen

Beweis: (Fortsetzung)

\Rightarrow : Sei x eine Lösung mit $ax \equiv b \pmod{n}$. Dann gilt

$$yax \equiv (d - nz)x \equiv dx \equiv yb \pmod{n}.$$

Aus der letzten Kongruenz folgt $x \equiv y \frac{b}{d} \pmod{\frac{n}{d}}$.

Anmerkung:

Für $\text{ggT}(a, n) = 1$ existiert immer eine Lösung $x \equiv yb \pmod{n}$.

Bsp:

- Berechne die Lösungsmenge von $4x \equiv 2 \pmod{6}$.
- Der Erw. Euklidische Algorithmus liefert $\text{ggT}(4, 6) = -1 \cdot 4 + 6 = 2$.
- Damit gilt $x \equiv -\frac{2}{2} \equiv 2 \pmod{3}$. D.h. die Lösungsmenge ist $2 + 3\mathbb{Z}$.

Lösung von simultanen Kongruenzen

Ziel:

- Bestimme alle Lösungen des Kongruenzsystems

$$\begin{cases} cx \equiv a \pmod{n} \\ dx \equiv b \pmod{m} \end{cases}$$

- Falls $c \neq 1$ löse nach x auf (voriger Satz), ersetze n durch $\frac{n}{\text{ggT}(c,n)}$.
- D.h. wir können oBdA annehmen, dass $c = d = 1$.

Satz Chinesischer Restsatz (CRT, Version 1)

Seien $a, b \in \mathbb{Z}$ und $n, m \in \mathbb{N}$. Sei $d = \text{ggT}(n, m) = yn + zm$, $y, z \in \mathbb{Z}$.

1 Falls das System $\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$ lösbar ist, gilt $a \equiv b \pmod{d}$.

2 Sei $a \equiv b \pmod{d}$. Ein $x \in \mathbb{Z}$ ist eine Lösung gdw

$$x \equiv a - yn \frac{a-b}{d} \pmod{\frac{nm}{d}}.$$

Beachte: Für teilerfremde n, m ist das System *immer* lösbar.

Chinesischer Restsatz

Beweis:

(1) Sei x eine Lösung mit $x \equiv a \pmod{n}$ und $x \equiv b \pmod{m}$.

Da $d \mid n$ und $d \mid m$ folgt $\left| \begin{array}{l} x \equiv a \pmod{d} \\ x \equiv b \pmod{d} \end{array} \right|$. Damit gilt $a \equiv b \pmod{d}$.

(2) \Leftarrow : Sei $x \equiv a - yn \frac{a-b}{d} \pmod{\frac{nm}{d}}$.

- Wegen $d \mid n$ und $d \mid m$ können wir x modulo n und m betrachten.
- Modulo n gilt $x \equiv a - yn \frac{a-b}{d} \equiv a \pmod{n}$ und modulo m gilt $x \equiv a - yn \frac{a-b}{d} \equiv a - (d - zm) \frac{a-b}{d} \equiv a - (a-b) + zm \frac{a-b}{d} \equiv b \pmod{m}$.
- Damit ist x eine Lösung des simultanen Kongruenzsystems.

\Rightarrow : Seien x, x' Lösungen. Wir zeigen, dass dann $x \equiv x' \pmod{\frac{nm}{d}}$.

- Wegen $x \equiv a \equiv x' \pmod{n}$ und $x \equiv b \equiv x' \pmod{m}$ folgt $n \mid x - x'$ und $m \mid x - x'$. D.h. $x - x'$ ist gemeinsames Vielfaches von n und m .
- $\text{kgV}(n, m)$ ist *kleinstes* gemeinsames Vielfaches von n und m , d.h.

$$\text{kgV}(n, m) \mid x - x'.$$

- Wegen $\text{kgV}(n, m) = \frac{nm}{\text{ggT}(n, m)} = \frac{nm}{d}$ folgt $x \equiv x' \pmod{\frac{nm}{d}}$.

Chinesischer Restsatz

Bsp: Löse das folgende System simultaner Kongruenzen

$$\left| \begin{array}{l} x \equiv 3 \pmod{6} \\ x \equiv 7 \pmod{10} \end{array} \right|.$$

- Es gilt $d = \text{ggT}(6, 10) = -3 \cdot 6 + 2 \cdot 10 = 2$.
- Lösung existiert wegen $3 \equiv 7 \pmod{2}$ und besitzt die Form
$$x \equiv 3 + 3 \cdot 6 \cdot \frac{3-7}{2} \equiv 3 + (-6) \equiv 27 \pmod{30}.$$
- D.h. alle Lösungen sind von der Gestalt $27 + 30\mathbb{Z}$.

Chinesischer Restsatz für mehr Gleichungen

Satz Chinesischer Restsatz

Die Lösungsmenge des Systems von simultanen Kongruenzen

$$a_i x \equiv b_i \pmod{n_i} \quad \text{für } i = 1, \dots, n$$

kann induktiv berechnet werden.

Beweis:

- Löse zunächst alle linearen Gleichungen nach x auf. Dies liefert

$$x \equiv c_i \pmod{n'_i} \quad \text{für } c_i \in \mathbb{Z}, n'_i \in \mathbb{N}.$$

- Löse mittels Chinesischem Restsatz die Kongruenzen

$$\left| \begin{array}{l} x \equiv c_1 \pmod{n'_1} \\ x \equiv c_2 \pmod{n'_2} \end{array} \right|.$$

- Die Lösungen kombinieren wir mit $x \equiv c_3 \pmod{n'_3}$, usw.
- D.h. wir fassen jeweils zwei Kongruenzen zusammen, bis nur noch eine Kongruenz verbleibt.

Übung: Geben Sie eine explizite Formel für x falls $n = 3$.