Binomische Formel mod p

Lemma Binomische Formel mod p

Seien $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$. Dann gilt

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

Beweis:

- Nach Binomischer Formel gilt
$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$
- Wir wollen zeigen, dass $p \mid \binom{p}{i}$ für $1 \leq i < p$. Daraus folgt
$$(a+p)^p \equiv a^p + b^p \bmod p.$$
- Es gilt $\binom{p}{i} \cdot i! = \frac{p!}{(p-i)!} = \prod_{j=0}^{i-1}(p-j)$.
- Wegen $i \geq 1$ teilt p die rechte Seite der Gleichung.
- Da p die rechte Seite teilt, muss p auch die linke Seite teilen.
- Wegen $i < p$ und p prim gilt aber $p \nmid i!$. Damit folgt $p \mid \binom{p}{i}$.

Anmerkung: Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto x^p \bmod p$ ist linear, d.h.

$$f(a+b) \equiv f(a) + f(b) \bmod p \text{ . } (f \text{ heißt } \textit{Frobenius}.)$$

Kleiner Satz von Fermat

Satz Kleiner Satz von Fermat

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

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

Beweis:

- Wir führen zunächst eine Induktion für $a \geq 0$ durch.
- **IA** $a = 0$**:** $0^p \equiv 0 \bmod p$.
- **IS** $a \to a + 1$**:** Nach vorigem Lemma gilt
$$(a+1)^p \equiv a^p + 1^p \equiv a + 1 \bmod p.$$
- Für $a < 0$ gilt $(-a)^p \equiv -a \bmod p$ mit $-a > 0$.
- Für $p = 2$ ist $-a = -a + 2a \equiv a \bmod 2$. Daraus folgt die Aussage.
- Für ungerades p folgt
$$-a \equiv (-a)^p = (-1)^p a^p = -a^p \bmod p.$$
- Multiplikation mit (-1) liefert die gewünschte Identität.

Kleiner Satz von Fermat

Korollar Kleiner Satz von Fermat (Variante)

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

$$a^{p-1} \equiv 1 \bmod p \text{ für alle } a \in \mathbb{Z} \text{ mit } p \nmid a.$$

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 $a^{p-1} \equiv 1 \bmod p$.

Anwendung:

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

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

Teiler und Vielfache

Lemma über Teiler und Vielfache

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

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

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 $ax \equiv b \bmod n$. Sei $d = \mathrm{ggT}(a, n)$.

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 $ya + zn = \mathrm{ggT}(a, n) = d$.
   Ein $x \in \mathbb{Z}$ ist Lösung gdw
   $$x \equiv y\frac{b}{d} \bmod \frac{n}{d}.$$

Beweis:

(1) Sei x eine Lösung mit $ax \equiv b \bmod n$. Dann gilt $ax = b + kn$ bzw.
$$b = ax - kn.$$
$d = \mathrm{ggT}(a, n)$ teilt beide Summanden rechts. Damit gilt $d \mid b$.

(2) $\Leftarrow$: Sei $x \equiv y\frac{b}{d} \bmod \frac{n}{d}$. Dann gilt
$$ax \equiv \frac{ay}{d} \cdot b \equiv \frac{d - zn}{d} \cdot b \equiv b - zn\frac{b}{d} \bmod \frac{a}{d}n$$
Damit folgt $ax \equiv b \bmod n$, d.h. x ist eine Lösung.

Lösbarkeit linearer Gleichungen

Beweis: (Fortsetzung)

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

$$yax \equiv (d - nz)x \equiv dx \equiv yb \bmod n.$$

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

Anmerkung:
Für $\mathrm{ggT}(a, n) = 1$ existiert stets genau eine Lösung $x \equiv yb \bmod n$.

Bsp:

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

Lösung von simultanen Kongruenzen

Ziel:

- Bestimme alle Lösungen des Kongruenzensystems

$$\left| \begin{array}{ll} cx \equiv a & \mod n \\ dx \equiv b & \mod m \end{array} \right|$$

- Falls $c \neq 1$ löse nach x auf (voriger Satz), ersetze n durch $\frac{n}{\mathrm{ggT}(c,n)}$.
- 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 $d = \mathrm{ggT}(n, m) = yn + zm,\ y, z \in \mathbb{Z}$.

1. Falls das System $\left| \begin{array}{ll} x \equiv a & \mod n \\ x \equiv b & \mod m \end{array} \right|$ lösbar ist, gilt $a \equiv b \mod d$.
2. Sei $a \equiv b \mod d$. Ein $x \in \mathbb{Z}$ ist eine Lösung gdw

$$x \equiv a - yn\tfrac{a-b}{d} \mod \tfrac{nm}{d}.$$

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

Chinesischer Restsatz

Beweis:

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

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

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

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

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

- Wegen $x \equiv a \equiv x' \bmod n$ und $x \equiv b \equiv x' \bmod m$ folgt $n \mid x - x'$ und $m \mid x - x'$. D.h. $x - x'$ ist gemeinsames Vielfaches von n und m.
- $\mathrm{kgV}(n, m)$ ist *kleinstes* gemeinsames Vielfaches von n und m, d.h.
$$\mathrm{kgV}(n, m) \mid x - x'.$$
- Wegen $\mathrm{kgV}(n, m) = \frac{nm}{\mathrm{ggT}(n,m)} = \frac{nm}{d}$ folgt $x \equiv x' \bmod \frac{nm}{d}$.

Chinesischer Restsatz

Bsp: Löse das folgende System simultaner Kongruenzen

$$\left| \begin{array}{ll} x \equiv 3 & \mod 6 \\ x \equiv 7 & \mod 10 \end{array} \right| .$$

- Es gilt $d = \mathrm{ggT}(6, 10) = -3 \cdot 6 + 2 \cdot 10 = 2$.
- Lösung existiert wegen $3 \equiv 7 \mod 2$ und besitzt die Form
$$x \equiv 3 + 3 \cdot 6 \cdot \frac{3-7}{2} \equiv 3 + (-6) \equiv 27 \mod 30.$$
- 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

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

kann berechnet werden.

Beweis:

- Löse zunächst alle linearen Gleichungen nach x auf. Dies liefert
$$x \equiv c_i \bmod n_i' \quad \text{für } c_i \in \mathbb{Z}, n_i' \in \mathbb{N}.$$
- Löse mittels Chinesischem Restsatz die Kongruenzen
$$\left| \begin{array}{ll} x \equiv c_1 & \bmod n_1' \\ x \equiv c_2 & \bmod n_2' \end{array} \right|.$$
- Die Lösungen kombinieren wir mit $x \equiv c_3 \bmod n_3'$, usw.
- D.h. wir fassen jeweils zwei Kongruenzen zusammen, bis nur noch eine Kongruenz verbleibt.

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