

Methoden der elementaren Zahlentheorie II

1. Kongruenzen

Definition:

Sei $n \in \mathbb{N}$. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo n*,

$$a \equiv b \pmod{n},$$

wenn n die Differenz $a-b$ teilt, also $a-b = kn$ für $k \in \mathbb{Z}$. n ist Modul der Kongruenz.

Beispiel: $27:6 = 4$ Rest 3

$$33:6 = 5 \text{ Rest } 3$$

$$\rightarrow 27 \equiv 33 \pmod{6}, 33-27=6$$

➤ Gilt dies nicht, so sind a und b inkongruent modulo n

Beispiel: $28:6 = 4$ Rest 4

$$33:6 = 5 \text{ Rest } 3$$

$$\rightarrow 28 \not\equiv 33 \pmod{6}, 33-28=5$$

➤ Zwei ganze Zahlen sind immer kongruent modulo 1 $\rightarrow n > 1$

Rechenregeln:

(a) $a \equiv a \pmod{k}$

(b) $a \equiv b \pmod{k} \rightarrow b \equiv a \pmod{k}$

(c) $a \equiv b \pmod{k}$ und $b \equiv c \pmod{k} \rightarrow a \equiv c \pmod{k}$

(d) $a \equiv b \pmod{k}$ und $c \equiv d \pmod{k}$

$$\rightarrow a+c \equiv b+d \pmod{k} \text{ und } ac \equiv bd \pmod{k}$$

(e) $a \equiv b \pmod{k} \rightarrow a+c \equiv b+c \pmod{k}$ und $ac \equiv bc \pmod{k}$

(f) $a \equiv b \pmod{k} \rightarrow a^n \equiv b^n \pmod{k}$ für $n \in \mathbb{N}$

2. Äquivalenzklassen

Definition:

Es sei $q \geq 2$ eine natürliche Zahl. Für jedes $n \in \mathbb{Z}$ nennen wir die Menge $n^* := \{ n+kq : q \in \mathbb{Z} \}$ die Äquivalenzklasse der Zahl n modulo q . Wir bezeichnen sie mit n^* oder $n^*(q)$.

Beispiel:

$$n = 7:$$

$$2^* = \{ \dots, -5, 2, 9, 16, 23, \dots \}$$

3. Der Chinesische Restsatz

Definition:

Sind $n_1, n_2, n_3, \dots, n_r$ paarweise teilerfremde natürliche Zahlen, so hat das Kongruenzensystem

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \dots, x \equiv a_r \pmod{n_r}$$

eine Lösung, die eindeutig modulo $n_1 \cdot n_2 \cdot \dots \cdot n_r$ ist.

Literaturverzeichnis:

- Grinberg, N.(2008): Lösungsstrategien. Mathematik für Nachdenker. Frankfurt am Main: Harri Deutsch Verlag.
- Burton, D.;Dalkowski, H.(2005): Handbuch der elementaren Zahlentheorie. Lemgo: Helderermann Verlag.
- Padberg, F.(2008):Elementare Zahlentheorie. 3.Auflage. Heidelberg: Spektrum Akademischer Verlag.