

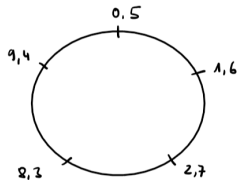
# Vertiefungskurs Mathematik

Zahlentheorie - Kongruenz und Restklassen

# Kongruenz

Definition: Seien  $a, b \in \mathbb{Z}, m \in \mathbb{N}$ . Dann heißt  $a$  *kongruent zu  $b$  modulo  $m$*  geschrieben:  $a \equiv b \pmod{m}$ , falls  $a - b$  durch  $m$  teilbar ist.

Beispiel:  $m = 5$



$$\begin{aligned} 1 &\equiv 6 \pmod{5} \\ 2 &\equiv 7 \equiv 12 \pmod{5} \end{aligned}$$

Satz: Folgende Aussagen sind äquivalent:

- (1)  $a \equiv b \pmod{m}$
- (2)  $\exists k \in \mathbb{Z} : a = b + km$
- (3) Beim Teilen durch  $m$  lassen  $a$  und  $b$  denselben Rest.

Beweis:

(1)  $\Rightarrow$  (2):  $a \equiv b \pmod{m}$  heißt nach Definition  $m \mid (a - b)$ . Also gibt ein  $k \in \mathbb{Z}$  mit  $km = a - b$ . Damit gilt:  $a = b + km$ .

(2)  $\Rightarrow$  (3): Sei  $r$  der Rest beim Teilen von  $a$  durch  $m$ . Nach dem Satz vom Teilen mit Rest gibt es ein eindeutig bestimmtes  $q \in \mathbb{Z}$  mit  $a = qm + r$  und  $0 \leq r < m$ . Damit ist  $b = a - km = qm + r - km = (q - k)m + r$ . Also lässt auch  $b$  beim Teilen durch  $m$  den Rest  $r$ .

(3)  $\Rightarrow$  (1): Es gilt  $a = k_1m + r$  und  $b = k_2m + r$  mit eindeutig bestimmten  $k_1, k_2, r \in \mathbb{Z}$  und  $0 \leq r < m$ . Also ist  $a - b = (k_1 - k_2)m$  und damit gilt  $m \mid (a - b)$ . □

## Doppelte Verwendung von 'mod'

'mod' wird auch als *modulo-Operator* verwendet.

$r = a \bmod b$  bedeutet: r ist der Rest bei der Division von a und b.

Beispiel:

$3 = 7 \bmod 2$  bedeutet: 3 ist Rest von  $7 : 2$  (das ist falsch)

$3 \equiv 7 \bmod 2$  bedeutet: 3 ist kongruent zu  $7 \bmod 2$  (das ist wahr)

Es gilt:  $a \bmod m = b \bmod m \Leftrightarrow a \equiv b \bmod m$

## Rechenregeln für Kongruenzen

Satz: Die Relation 'kongruent modulo  $m$ ' ist eine Äquivalenzrelation auf  $\mathbb{Z}$ .

- (1)  $a \equiv a \pmod{m}$  (Reflexivität)
- (2)  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$  (Symmetrie)
- (3)  $a \equiv b \pmod{m}$  und  $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$  (Transitivität)

Satz: Wenn  $a \equiv b \pmod{m}$  und  $c \equiv d \pmod{m}$ , dann gilt:

- (4)  $-a \equiv -b \pmod{m}$
- (5)  $a + c \equiv b + d \pmod{m}$
- (6)  $a \cdot c \equiv b \cdot d \pmod{m}$
- (7)  $a^2 \equiv b^2 \pmod{m}$ ,  $a^3 \equiv b^3 \pmod{m}$ , ...

Beweis (nur 6): Aus der Voraussetzung folgt, es gibt  $k_1, k_2 \in \mathbb{Z}$  mit  $a = b + k_1m$  und  $c = d + k_2m$ . Dann ist  $ac = (b + k_1m)(d + k_2m) = bd + bk_2m + k_1md + k_1k_2m^2 = bd + (bk_2 + k_1d + k_1k_2m) \cdot m$ .

Das bedeutet:  $ac \equiv bd \pmod{m}$



## Beispiel

$$m = 7$$

$$73 + 155 \equiv 3 + 1 \equiv 4 \pmod{7}$$

$$73 \cdot 155 \equiv 3 \cdot 1 \equiv 3 \pmod{7}$$

$$73^{155} \equiv 3^{155} \equiv 5 \pmod{7}$$

Nebenrechnung (alles mod 7):

$$3^1 \equiv 3$$

$$3^2 \equiv 2$$

$$3^4 \equiv 4 \equiv 3^{16} \equiv 3^{64}$$

$$3^8 \equiv 2 \equiv 3^{32} \equiv 3^{128}$$

$$3^{155} = 3^{128+16+8+2+1} \equiv 2 \cdot 4 \cdot 2 \cdot 2 \cdot 3 \equiv 32 \cdot 3 \equiv -3 \cdot 3 \equiv -9 \equiv 5$$

## Teilbarkeitsregeln

Satz: Sei  $n \in \mathbb{N}$ . Dann gilt:

$2|n \Leftrightarrow$  die letzte Ziffer ist gerade.

$3|n \Leftrightarrow$  die Quersumme ist durch 3 teilbar.

$4|n \Leftrightarrow$  die Zahl aus den letzten beiden Ziffern ist durch 4 teilbar.

$5|n \Leftrightarrow$  die letzte Ziffer ist 5 oder 0.

$6|n \Leftrightarrow 2|n$  und  $3|n$ .

$7|n \Leftrightarrow$  die Zahl, die entsteht, wenn man das doppelte der letzten Ziffer von der Zahl ohne die letzte Ziffer abzieht, ist durch 7 teilbar.

$8|n \Leftrightarrow$  die Zahl aus den letzten drei Ziffern ist durch 8 teilbar.

$9|n \Leftrightarrow$  die Quersumme ist durch 9 teilbar.

$10|n \Leftrightarrow$  die letzte Ziffer ist eine 0.

$11|n \Leftrightarrow$  die alternierende Quersumme ist durch 11 teilbar.

$12|n \Leftrightarrow 3|n$  und  $4|n$ .

## Beispiele Teilbarkeitsregeln

Teilbarkeit durch 7:

$$35881 \rightarrow 3586 \rightarrow 346 \rightarrow 22 \Rightarrow 7 \text{ kein Teiler von } 35881$$

Teilbarkeit durch 11:

$$355971 : 1 - 7 + 9 - 5 + 5 - 3 = 0 \Rightarrow 11 \mid 355971$$



## Beweis der Teilbarkeitsregeln (für 3,9,11,7)

Es sei  $n = a_k a_{k-1} \dots a_2 a_1 a_0$  die Dezimaldarstellung von  $n \in \mathbb{N}$  mit  $a_i \in \{0, 1, \dots, 9\}$  für  $0 \leq i \leq k$ . Dann gilt

$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k$$

Teilbarkeit durch 3:  $n \equiv a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k$   
 $\equiv a_0 + a_1 + a_2 + \dots + a_k \equiv \text{Quersumme}(n) \pmod{3}$

Teilbarkeit durch 9 ebenso.

Teilbarkeit durch 11:  $n \equiv a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k$   
 $\equiv a_0 - a_1 + a_2 - a_3 + a_4 \dots \equiv \text{alternierende Quersumme}(n) \pmod{11}$

Teilbarkeit durch 7: Es sei  $m$  die Zahl  $n$  ohne die letzte Ziffer. Dann gilt  $n = 10 \cdot m + a_0$ . Also gilt auch:  $2n = 20m + 2a_0$ . Und damit gilt:

$2n = 21m - m + 2a_0$ . Daraus folgt:  $2n \equiv -m + 2a_0 \pmod{7}$ . Insgesamt gilt:  
 $7|n \Leftrightarrow 7|2n \Leftrightarrow -m + 2a_0 \equiv 0 \pmod{7} \Leftrightarrow m - 2a_0 \equiv 0 \pmod{7} \Leftrightarrow 7|(m - 2a_0) \square$

## Restklassen

Betrachte alle Zahlen, die beim Teilen durch eine Zahl  $m \in \mathbb{N}$  denselben Rest lassen. Diese Zahlen werden zu einer Menge zusammengefasst, der Restklasse.

Definition: Die *Restklasse*  $\bar{a}$  von  $a$  modulo  $m$  ist definiert durch:  
 $\bar{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{m}\}.$

Andere Schreibweise:  $[a]$  statt  $\bar{a}$ .

Beispiel: Die Restklassen modulo 5 sind

$$\bar{0} = \{\dots, -10, -5, 0, 5, 10, \dots\}$$

$$\bar{1} = \{\dots, -9, -4, 1, 6, 11, \dots\}$$

$$\bar{2} = \{\dots, -8, -3, 2, 7, 12, \dots\}$$

$$\bar{3} = \{\dots, -7, -2, 3, 8, 13, \dots\}$$

$$\bar{4} = \{\dots, -6, -1, 4, 9, 14, \dots\}$$

## Rechnen im Restklassenring

Die Menge aller Restklassen modulo  $m$  heißt *Restklassenring modulo  $m$*  geschrieben  $\mathbb{Z}_m$ .

Beispiel:  $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

Definition: Seien  $a, b \in \mathbb{Z}$ .

$$\bar{a} + \bar{b} := \overline{a + b}$$

$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

Beispiel in  $\mathbb{Z}_5$ :  $\bar{2} + \bar{3} = \bar{5} \quad \bar{7} + \bar{8} = \overline{15} = \bar{5}$

Es spielt keine Rolle, welcher Repräsentant der Restklasse für die Berechnung genommen wird. Addition und Multiplikation sind ‘wohldefiniert’.

## Verknüpfungstabellen

Die Verknüpfungstabelle für Addition und Multiplikation in  $\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Subtraktion:  $\bar{a} - \bar{b} := \bar{a} + \overline{-b}$ . Dann gilt:  $\bar{a} - \bar{a} = \bar{a} + \overline{-a} = \overline{a - a} = \bar{0}$

Hilfsfrage für negative Restklassen: Wieviel fehlt vom Absolutbetrag zum nächsten Vielfachen von  $m$ ? Beispiel in  $\mathbb{Z}_7$ :  $\overline{-25} = \bar{3}$

Division in  $\mathbb{Z}_5$  :

$$\frac{\bar{1}}{\bar{2}} = x \Leftrightarrow \bar{1} = \bar{2} \cdot x \Leftrightarrow x = \bar{3}$$

$$\frac{\bar{2}}{\bar{3}} = x \Leftrightarrow \bar{2} = \bar{3} \cdot x \Leftrightarrow x = \bar{4}$$

Problem bei der Division in  $\mathbb{Z}_4$  :

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$$\frac{\overline{1}}{\overline{2}} = x \Leftrightarrow \overline{1} = \overline{2} \cdot x, \quad \text{es gibt kein } x.$$

$$\frac{\overline{2}}{\overline{2}} = x \Leftrightarrow \overline{2} = \overline{2} \cdot x, \quad x = \overline{1} \text{ oder } x = \overline{3}, \text{ d.h. } x \text{ ist nicht eindeutig.}$$

## Existenz von Brüchen in $\mathbb{Z}_m$

$$\frac{\bar{a}}{\bar{b}} = \bar{x} \Leftrightarrow \bar{a} = \bar{b} \cdot \bar{x} = \overline{b \cdot x} \Leftrightarrow a \equiv bx \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z} : km = a - bx$$

In der letzten Gleichung sind  $a, b, m$  vorgegeben  $k$  ist unbekannt und  $x$  ist gesucht. Wir müssen also die diophantische Gleichung  $bx + km = a$  lösen.

Falls  $m$  Primzahl, dann ist  $\text{ggT}(m, b) = 1$ . Dann hat die Gleichung für jedes  $a$  eine Lösung  $x_0$  und alle anderen Lösungen sind gegeben durch  $x_0 + t \cdot m, t \in \mathbb{Z}$ . Dies sind die Elemente von  $\overline{x_0}$ .

**Satz vom Dividieren:** Sei  $p$  Primzahl,  $a \in \mathbb{Z}$ ,  $b \in \{1, \dots, p-1\}$ , dann besitzt die Gleichung  $\overline{b} \cdot \overline{x} = \overline{a}$  in  $\mathbb{Z}_p$  genau eine Lösung  $\overline{x}$ , d.h.  $\frac{\overline{a}}{\overline{b}} := \overline{x}$  ist definiert.

Merkregel: Wenn wir  $\frac{\overline{1}}{\overline{a}}$  in  $\mathbb{Z}_p$  suchen, dann lösen wir die Gleichung  $ax + py = 1$ . Es gilt dann:  $\frac{\overline{1}}{\overline{a}} = \overline{x}$ .

Beispiel: Bestimme  $\frac{\overline{1}}{\overline{7}}$  in  $\mathbb{Z}_{11}$ . Wir lösen die Gleichung  $7x + 11y = 1$ . Eine Lösung ist  $x = -3, y = 2$ . Also gilt:  $\frac{\overline{1}}{\overline{7}} = \overline{-3} = \overline{8}$ .



## Kleiner Satz von Fermat:

Sei  $p$  Primzahl,  $a \in \mathbb{N}$  kein Vielfaches von  $p$ .

Dann gilt:  $\overline{a}^{p-1} = \overline{1}$  in  $\mathbb{Z}_p$  bzw.  $a^{p-1} \equiv 1 \pmod{p}$ .

Beispiel in  $\mathbb{Z}_5$ :  $2^4 \equiv 16 \equiv 1$ ,  $3^4 \equiv 81 \equiv 1$ ,  $4^4 \equiv (-1)^4 \equiv 1$

Beweis: Setze  $A = \{\overline{0a}, \overline{1a}, \overline{2a}, \dots, \overline{(p-1)a}\} \subseteq \mathbb{Z}_p$ . Wir zeigen zunächst  $A = \mathbb{Z}_p$ , indem wir zeigen, dass alle Elemente in  $A$  verschieden sind.

Annahme:  $\overline{ja} = \overline{ka}$  für ein  $k > j$ . Dann gilt:

$\overline{0} = \overline{ja} - \overline{ka} = \overline{ja - ka} = \overline{(j-k)a}$ . Da  $j - k \neq 0$  können wir dividieren und erhalten  $\overline{a} = \frac{\overline{0}}{\overline{j-k}}$ . Damit ist  $a$  ein Vielfaches von  $p$ , im Widerspruch zur

Annahme. Also gilt  $A = \mathbb{Z}_p$ . Wir entfernen  $\overline{0a}$  aus  $A$  und  $\mathbb{Z}_p$ . Das Produkt der restlichen Elemente muss gleich sein.

$\overline{1a} \cdot \overline{2a} \cdot \dots \cdot \overline{(p-1)a} = \overline{1} \cdot \overline{2} \cdot \dots \cdot \overline{p-1}$ . Wir dividieren durch  $\overline{1}, \overline{2}, \dots$  und erhalten:  $\overline{a}^{p-1} = \overline{1}$  □

## Primitivwurzeln:

Definition: Ein Element  $\bar{g} \in \mathbb{Z}_m$  heißt *Primitivwurzel*, falls durch  $\bar{g}^k$  alle Elemente von  $\mathbb{Z}_m$  außer  $\bar{0}$  dargestellt werden können.

Beispiel:

$$2^0 \equiv 1 \pmod{7} \qquad 3^0 \equiv 1 \pmod{7}$$

$$2^1 \equiv 2 \qquad 3^1 \equiv 3$$

$$2^2 \equiv 4 \qquad 3^2 \equiv 2$$

$$2^3 \equiv 1 \qquad 3^3 \equiv 6$$

$$2^4 \equiv 2 \qquad 3^4 \equiv 4$$

$$2^5 \equiv 4 \qquad 3^5 \equiv 5$$

$$2^6 \equiv 1 \qquad 3^6 \equiv 1$$

$\bar{3}$  ist Primitivwurzel in  $\mathbb{Z}_7$ ,  $\bar{2}$  nicht.

Tritt bei  $\bar{g}^k$  vor  $\bar{g}^{p-1}$  die Restklasse  $\bar{1}$  auf, so wiederholen sich die Restklassen. Es kann keine Primitivwurzel vorliegen.