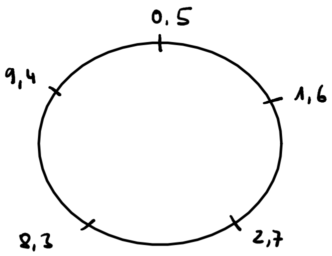
Kongruenz und Restklassen

Kongruenz

Definition:

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

Beispiel: $m = 5$



$1 \equiv 6 \mod 5$

$2 \equiv 7 \equiv 13 \mod 5$

Satz

Folgende Aussagen sind äquivalent:

(1) $a \equiv b \mod m$

(2) $\exists k \in \mathbb{Z}: \; a = b + k \cdot m$

(3) Beim Teilen durch m lassen a und b denselben Rest.

Beweis:

(1) ⇒ (2): $a \equiv b \mod m \Rightarrow m \mid (a-b) \Rightarrow \exists k \in \mathbb{Z}: \; mk = a-b$

$a = b + mk$

(2) ⇒ (3): Sei r der Rest beim Teilen von a durch m.

$$\Rightarrow \exists q \in \mathbb{Z}: \left.\begin{aligned} a &= q \cdot m + r \\ a &= b + km \end{aligned}\right\} \text{ mit } 0 \leq r < m. \Rightarrow b = q \cdot m - k \cdot m + r = (q-k) \cdot m + r$$

Wegen der Eindeutigkeit des Teilens mit Rest folgt: Teilen von b durch m ergibt Rest r

(3) ⇒ (1): $$\left.\begin{aligned} a &= km + r \\ b &= k'm + r \end{aligned}\right\} (a-b) = \underbrace{(k-k')}_{\in \mathbb{Z}} m \Rightarrow m \mid (a-b) \Rightarrow a \equiv b \mod m$$

q.e.d.

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 durch b.

$3 \equiv 7 \mod 2$ – 3 kongruent 7 mod 2 ist wahr

$3 = 7 \bmod 2$ – 3 ist 7 modulo 2 ist falsch

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

Rechenregeln für Kongruenzen

Satz

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

(1) $a \equiv a \mod m$ (Reflexivität)

(2) $a \equiv b \mod m \Rightarrow b \equiv a \mod m$ (Symmetrie)

(3) $a \equiv b \mod m$ und $b \equiv c \mod m \Rightarrow a \equiv c \mod m$ (Transitivität)

Satz

Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann gilt:

(4) $-a \equiv -b \mod m$

(5) $a+c \equiv b+d \mod m$

(6) $ac \equiv bd \mod m$

(7) $a^2 \equiv b^2 \mod m$, $a^3 \equiv b^3 \mod m, \dots$

Beweis (nur (6)):

$$\left.\begin{array}{l} a \equiv b \mod m \Rightarrow \exists k \in \mathbb{Z}: a = b + km \\ c \equiv d \mod m \Rightarrow \exists k' \in \mathbb{Z}: c = d + k'm \end{array}\right\} a \cdot c = (b+km)(d+k'm) = bd + bk'm + kmd + kk'm^2$$

$$= bd + \underbrace{(bk' + kd + kk'm)}_{\in \mathbb{Z}} \cdot m \Rightarrow ac \equiv bd \mod m$$

q.e.d.

Beispiele:

$m = 7$: $73 + 155 \equiv 3 + 1 \equiv 4 \mod 7$

$73 \cdot 155 \equiv 3 \cdot 1 \equiv 3 \mod 7$

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

NR:

$3^1 \equiv 3 \mod 7$

$3^2 \equiv 2$

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

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

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

Beispiel (Wochentag bestimmen)

Der 1.11.2021 ist ein Montag. Welcher Wochentag ist der 24.12.2025?

$29 + 24 + 365 + 365 + 366 + 365 \equiv 1+3+1+1+2+1 \equiv 9 \equiv 2 \mod 7$

↑ vom 1.11. ausgehend sind es noch 29 weitere Tage bis Ende November

↑ Schaltjahr 2024

$\Rightarrow$ 24.12.2025 ist ein Mittwoch

Satz (Teilbarkeitsregeln)

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

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

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

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

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

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

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

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

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

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

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

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

Beispiele:

$n|7$: $n = 35881 \to 3586 \to 357 \to 21 \Rightarrow 7|n$

$n|11$: $n = 355971 \to 1-7+9-5+5-3 = 0 \Rightarrow 11|n$

Beweis (für 3, 9, 7, 11)
Es sei $n = a_k a_{k-1} \dots a_2 a_1 a_0$ die Dezimaldarstellung von n mit $a_i \in \{0,1,..9\}$ für $0 \le i \le k$.
Dann gilt: $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k$
$n|3$: $n \equiv a_0 + a_1 \cdot 1 + a_2 \cdot 1 + \dots + a_k \cdot 1 \equiv$ Quersumme(n) mod 3
$n|9$: $n \equiv a_0 + a_1 \cdot 1 + a_2 \cdot 1 + \dots + a_k \cdot 1 \equiv$ Quersumme (n) mod 9
$n|11$: $n \equiv a_0 + a_1 \cdot (-1) + a_2 \cdot 1 + a_3 \cdot (-1) + \dots \equiv$ alternierende Quersumme (n) mod 11
$n|7$: Es sei m die Zahl n ohne die letzte Ziffer, d.h. $n = m \cdot 10 + a_0$
$\Rightarrow n = 10 \cdot m + a_0 \Rightarrow 2n = 20m + 2a_0 = 21m - m + 2a_0 \equiv -m + 2a_0 \mod 7$
Also: $n|7 \Leftrightarrow 2n|7 \Leftrightarrow -m+2a_0 \equiv 0 \mod 7 \Leftrightarrow m - 2a_0 \equiv 0 \mod 7 \Leftrightarrow m - 2a|7$ q.e.d.

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:
$\bar{a} := \{ b \in \mathbb{Z} : b \equiv a \mod m \}$ (andere Schreibweise: $[a]$ statt $\bar{a}$)

Beispiel:
Die Restklassen modulo 5:
$\bar{0} = \{ \dots, -10, -5, 0, 5, 10, \dots \} = \bar{5} = \overline{10} \dots$
$\bar{1} = \{ \dots, -9, -4, 1, 6, 11, \dots \} = \bar{6} = \overline{11} \dots$
$\bar{2} = \{ \dots, -8, -3, 2, 7, 12, \dots \} = \bar{7} = \overline{12} \dots$
$\bar{3} = \{ \dots, -7, -2, 3, 8, 13, \dots \} = \bar{8} = \overline{13} \dots$
$\bar{4} = \{ \dots, -6, -1, 4, 9, 14, \dots \} = \bar{9} = \overline{14} \dots$

Definition
Die Menge aller Restklassen heißt Restklassenring modulo m, geschrieben $\mathbb{Z}_m$
Beispiel: $\mathbb{Z}_5 = \{ \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4} \}$

Rechnen im Restklassenring

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 $\mathbb{Z}_5$
$\bar{2} + \bar{2} = \bar{4}$
$\overset{\shortparallel}{\bar{7}} + \overset{\shortparallel}{\overline{12}} = \overset{\shortparallel}{\overline{19}}$

Es ist egal, welche Darstellung von $\bar{a}$ und $\bar{b}$ für die Berechnung verwendet wird. Die Addition auf Restklassen ist "wohldefiniert"

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 $\bar{a} - \bar{a} = \bar{a} + \overline{(-a)} = \overline{a-a} = \bar{0}$

in $\mathbb{Z}_5$: $\bar{1} - \bar{2} = \bar{1} + \overline{-2} = \bar{1} + \bar{3} = \bar{4}$

Hilfsfrage für negative Restklassen: wieviel fehlt vom Absolutbetrag zum nächsten Vielfachen von m?

Division in $\mathbb{Z}_5$: $\frac{\bar{1}}{\bar{2}} = \bar{x} \Leftrightarrow \bar{1} = \bar{2} \cdot \bar{x} \underset{\text{Tabelle}}{\Rightarrow} \bar{x} = \bar{3}$

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

Aber betrachte $\mathbb{Z}_4$:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\frac{\bar{1}}{\bar{2}} = \bar{x} \Leftrightarrow \bar{1} = \bar{2} \cdot \bar{x}$, es gibt kein $\bar{x}$

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

$\Rightarrow \bar{x}$ ist nicht eindeutig

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

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

$\Leftrightarrow \exists k \in \mathbb{Z}: bx - km = a$ } diophantische Gleichung

$x \in \mathbb{Z}$ gesucht, $k \in \mathbb{Z}$ unbekannt, $a, b, m \in \mathbb{N}$ gegeben

Falls m Primzahl gilt: $ggT(m, b) = 1$. Dann hat diese Gleichung für jedes a eine Lösung x_0 und alle anderen Lösungen sind gegeben durch $x_0 + l \cdot m$ $(l \in \mathbb{Z})$. 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 $\bar{b} \cdot \bar{x} = \bar{a}$ in $\mathbb{Z}_p$ genau eine Lösung $\bar{x}$, d.h. $\frac{\bar{a}}{\bar{b}} := x$ ist definiert.

Merkregel: Wenn wir $\frac{\bar{1}}{\bar{a}}$ in $\mathbb{Z}_m$ suchen, dann lösen wir $ax + my = 1$. Dann gilt: $\frac{\bar{1}}{\bar{a}} = \bar{x}$

Der kleine Satz von Fermat:

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

$\bar{a}^{p-1} = \bar{1}$ in $\mathbb{Z}_p$ bzw. $a^{p-1} \equiv 1 \mod p$

Beispiel in $\mathbb{Z}_5$

$1^4 \equiv 1 \mod 5$, $2^4 \equiv (4)^2 \equiv (-1)^2 \equiv 1 \mod 5$

$3^4 \equiv (9)^2 \equiv (-1)^2 \equiv 1 \mod 5$, $4^4 \equiv (-1)^4 \equiv 1 \mod 5$

Beweis (kleiner Satz von Fermat):

$A = \{ \overline{0a}, \overline{1a}, \overline{2a}, \dots, \overline{(p-1)\cdot a} \} \subseteq \mathbb{Z}_p$

Wir zeigen zunächst $A = \mathbb{Z}_p$, indem wir zeigen, dass alle Elemente in A verschieden sind.

Annahme: $\overline{ja} = \overline{ka}$ für ein $k > j$. $\Rightarrow \overline{0} = \overline{ja} - \overline{ka} = \overline{ja - ka} = \overline{(j-k) \cdot a}$

$\Rightarrow \overline{(j-k)} \cdot \overline{a} = \overline{0}$ mit $j - k \neq 0 \Rightarrow \frac{\overline{0}}{\overline{(j-k)}} = \overline{a} \Rightarrow \overline{0} = \overline{a} \Rightarrow a$ ist Vielfaches von p. $\lightning$

Also $A = \mathbb{Z}_p$. Wir entfernen $\overline{0a}$ aus A und $\overline{0}$ aus $\mathbb{Z}_p$. Das Produkt der restlichen Elemente muss gleich sein. $\overline{a} \cdot \overline{2a} \cdot \overline{3a} \cdot \ldots \cdot \overline{(p-1)a} = \overline{1} \cdot \overline{2} \cdot \overline{3} \cdot \ldots \cdot \overline{(p-1)} \Rightarrow \overline{a}^{p-1} = \overline{1}$ q.e.d.

Definition:

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

Beispiel

$2^0 \equiv 1 \mod 7$	$3^0 \equiv 1 \mod 7$
$2^1 \equiv 2$	$3^1 \equiv 3$
$2^2 \equiv 4$	$3^2 \equiv 2$
$2^3 \equiv 1$	$3^3 \equiv 6$
$2^4 \equiv 2$	$3^4 \equiv 4$
$2^5 \equiv 4$	$3^5 \equiv 5$
$2^6 \equiv 1$	$3^6 \equiv 1$
2 ist keine Primitivwurzel,	3 ist Primitivwurzel in $\mathbb{Z}_7$.

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