

Teilbarkeit ganzer Zahlen



MATHEMATIK
macht
FREU(N)DE

a und b sind ganze Zahlen mit $a \neq 0$.

Gibt es eine ganze Zahl k mit $b = a \cdot k$, dann nennen wir a einen **Teiler** von b .

Wir schreiben dafür kurz $a \mid b$.

Gibt es *keine* solche ganze Zahl k , dann schreiben wir $a \nmid b$.

Bei der Division $b : a = k$ bleibt also kein Rest.

$a, b \in \mathbb{Z}, a \neq 0$

Teilbarkeit ganzer Zahlen



MATHEMATIK
macht
FREU(N)DE

Entscheide jeweils, ob \mid oder \nmid stimmt: a) $4 \mid -24$ b) $-5 \mid 20$ c) $6 \nmid -3$ d) $-3 \mid -15$ e) $2 \mid 0$

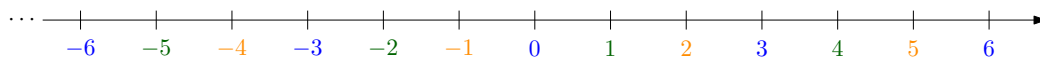
Vielfache & Restklassen



MATHEMATIK
macht
FREU(N)DE

Die **Vielfachen** einer ganzen Zahl m sind alle Zahlen der Form $m \cdot k$ mit $k \in \mathbb{Z}$.

Zum Beispiel: Die ganze Zahl 3 hat die Vielfachen $\{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$.



Dividiert man ein Vielfaches von 3 durch 3, dann bleibt 0 Rest. Wir sagen auch:

Die Zahlenmenge $\bar{0} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$ ist die **Restklasse 0 modulo 3**.

Jede Zahl in der Restklasse 0 können wir in der Form $3 \cdot k + 0$ mit $k \in \mathbb{Z}$ schreiben.

Die Zahlenmenge $\bar{1} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$ ist die **Restklasse 1 modulo 3**.

Jede Zahl in der Restklasse 1 können wir in der Form $3 \cdot k + 1$ mit $k \in \mathbb{Z}$ schreiben.

Die Zahlenmenge $\bar{2} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$ ist die **Restklasse 2 modulo 3**.

Jede Zahl in der Restklasse 2 können wir in der Form $3 \cdot k + 2$ mit $k \in \mathbb{Z}$ schreiben.

Jede Zahl einer Restklasse heißt auch **Repräsentant** dieser Restklasse.

Meistens verwenden wir die m Zahlen $0, 1, 2, \dots, m - 1$ als Repräsentanten ihrer Restklassen modulo m .

Kongruenz



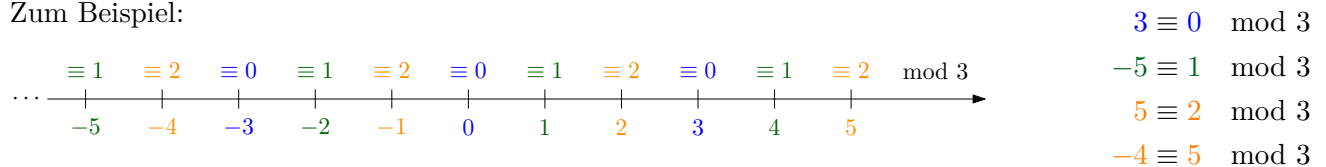
MATHEMATIK
macht
FREU(N)DE

Zwei Zahlen a und b liegen in der gleichen Restklasse modulo m .

Dann sagen wir: „ a und b sind **kongruent** modulo m “ bzw. „ a ist **kongruent** zu b modulo m “

Dann schreiben wir kurz: $a \equiv b \pmod{m}$ Der Ausdruck $a \equiv b \pmod{m}$ ist keine Gleichung, sondern eine **Kongruenz**.

Zum Beispiel:



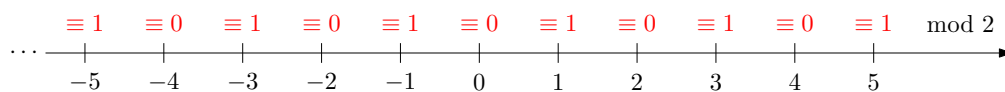
Kongruenz



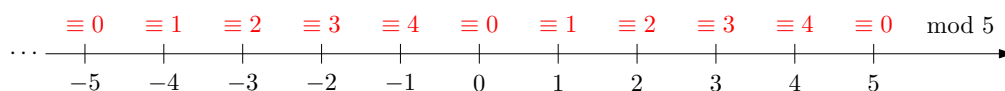
MATHEMATIK
macht
FREU(N)DE

Fülle in die Lücke jeweils jene Zahl aus $\{0, 1, 2, \dots, m - 1\}$, zu der die Zahl modulo m kongruent ist.

a) $m = 2$



b) $m = 5$



Kongruenz?



MATHEMATIK
macht
FREU(N)DE

Entscheide, ob die Zahlen kongruent (\equiv) oder nicht kongruent ($\not\equiv$) sind.

- a) $27 \equiv 42 \pmod{5}$ b) $-3 \equiv 39 \pmod{7}$ c) $981273 \not\equiv 48276 \pmod{2}$ d) $846 \equiv 14322 \pmod{3}$

Äquivalente Aussagen



MATHEMATIK
macht
FREU(N)DE

Zwei Zahlen a und b liegen genau dann in der gleichen Restklasse modulo m , wenn $a = b + k \cdot m$ mit einer passenden ganzen Zahl k gilt. a und b unterscheiden sich um ein Vielfaches von m . Erkläre damit die folgende Aussage:

$$a \equiv b \pmod{m} \iff m \mid a - b$$

a und b liegen genau dann in der gleichen Restklasse modulo m , wenn m ein Teiler von $a - b$ ist.

$$a \equiv b \pmod{m} \iff a = b + k \cdot m \iff a - b = k \cdot m \iff m \mid a - b$$

Rechenregeln für Kongruenzen



MATHEMATIK
macht
FREU(N)DE

Erkläre die folgenden Rechenregeln für Kongruenzen:

$$1) \left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$

Wir dürfen zwei Kongruenzen modulo m addieren.

$$\left. \begin{array}{l} a_1 - b_1 = k_1 \cdot m \\ a_2 - b_2 = k_2 \cdot m \end{array} \right\} \implies (a_1 + a_2) - (b_1 + b_2) = \underbrace{(k_1 + k_2)}_{\in \mathbb{Z}} \cdot m \implies a_1 + a_2 \equiv b_1 + b_2 \pmod{m} \checkmark$$

$$2) a \equiv b \pmod{m} \implies a \cdot c \equiv b \cdot c \pmod{m}$$

Wir dürfen beide Seiten einer Kongruenz mit der gleichen ganzen Zahl multiplizieren.

$$m \mid a - b \implies m \mid \underbrace{(a - b) \cdot c}_{a \cdot c - b \cdot c} \checkmark$$

$$3) \left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$$

Wir dürfen zwei Kongruenzen modulo m multiplizieren.

$$\left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \implies a_1 \cdot a_2 \equiv b_1 \cdot a_2 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \implies b_1 \cdot b_2 \equiv b_1 \cdot a_2 \pmod{m} \end{array} \right\} \implies a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$$

Division



MATHEMATIK
macht
FREU(N)DE

Wir dürfen beide Seiten einer Kongruenz *nicht* einfach durch einen gemeinsamen Teiler dividieren.

Zum Beispiel: $\underbrace{18}_{=3 \cdot 6} \equiv \underbrace{30}_{=5 \cdot 6} \pmod{4}$, aber $3 \not\equiv 5 \pmod{4}$.

Die richtige Rechenregel zum Kürzen gemeinsamer Teiler ist am Ende des Arbeitsblatts.

Division mit Rest



MATHEMATIK
macht
FREU(N)DE

Gegeben sind zwei ganze Zahlen z und m .

Gesucht ist jene Zahl r aus $\{0, 1, 2, \dots, m - 1\}$, für die $z \equiv r \pmod{m}$ gilt.

Zum Beispiel: $z = 208, m = 12$

1) Wir führen die Division mit Rest $z : m$ durch.

$$208 : 12 = 17 + \frac{4}{12}$$

„Wie oft geht 12 in 208? 17 Mal, 4 Rest“

2) Wir multiplizieren die Gleichung mit m .

$$208 = 17 \cdot 12 + 4$$

3) Aus den Rechenregeln für Kongruenzen folgt, dass der Rest $r = 4$ die gesuchte Zahl ist.

$$208 = \underbrace{17 \cdot 12}_{\equiv 0 \pmod{12}} + 4 \implies 208 \equiv 4 \pmod{12}$$

Division mit Rest



MATHEMATIK
macht
FREU(N)DE

Ermittle jene Zahl r aus $\{0, 1, 2, \dots, m - 1\}$, für die $z \equiv r \pmod{m}$ gilt, und fülle die Lücken aus.

a) $42 = 5 \cdot 8 + 2 \implies 42 \equiv 2 \pmod{8}$

c) $129 = 64 \cdot 2 + 1 \implies 129 \equiv 1 \pmod{2}$

b) $96 = 13 \cdot 7 + 5 \implies 96 \equiv 5 \pmod{7}$

d) $358 = 59 \cdot 6 + 4 \implies 358 \equiv 4 \pmod{6}$

Einerziffer entscheidet



MATHEMATIK
macht
FREU(N)DE

a) „Jede natürliche Zahl ist modulo 10 in der gleichen Restklasse wie ihre Einerziffer.“

Wir erklären die Aussage anhand der Zahl $4723 = 4 \cdot 1000 + 7 \cdot 100 + 2 \cdot 10 + 3 \cdot 1$:

$$4723 = \underbrace{4 \cdot 100 \cdot 10}_{\equiv 0 \pmod{10}} + \underbrace{7 \cdot 10 \cdot 10}_{\equiv 0 \pmod{10}} + \underbrace{2 \cdot 10}_{\equiv 0 \pmod{10}} + \underbrace{3 \cdot 1}_{\equiv 3 \pmod{10}} \equiv 3 \pmod{10}$$

Eine natürliche Zahl ist also genau dann durch 10 teilbar, wenn ihre Einerziffer 0 ist.

b) „Jede natürliche Zahl ist modulo 5 in der gleichen Restklasse wie ihre Einerziffer.“

Erkläre die Aussage anhand der Zahl 4723:

$$4723 = \underbrace{4 \cdot 200 \cdot 5}_{\equiv 0 \pmod{5}} + \underbrace{7 \cdot 20 \cdot 5}_{\equiv 0 \pmod{5}} + \underbrace{2 \cdot 2 \cdot 5}_{\equiv 0 \pmod{5}} + \underbrace{3 \cdot 1}_{\equiv 3 \pmod{5}} \equiv 3 \pmod{5}$$

Eine natürliche Zahl ist also genau dann durch 5 teilbar, wenn ihre Einerziffer 0 oder 5 ist.

c) „Jede natürliche Zahl ist modulo 2 in der gleichen Restklasse wie ihre Einerziffer.“

Erkläre die Aussage anhand der Zahl 4723:

$$4723 = \underbrace{4 \cdot 500 \cdot 2}_{\equiv 0 \pmod{2}} + \underbrace{7 \cdot 50 \cdot 2}_{\equiv 0 \pmod{2}} + \underbrace{2 \cdot 5 \cdot 2}_{\equiv 0 \pmod{2}} + \underbrace{3 \cdot 1}_{\equiv 3 \pmod{2}}$$

Eine natürliche Zahl ist also genau dann durch 2 teilbar, wenn ihre Einerziffer 0, 2, 4, 6 oder 8 ist.

a) „Jede natürliche Zahl ist modulo 9 in der gleichen Restklasse wie ihre Ziffernsumme.“

Wir erklären die Aussage anhand der Zahl $4723 = 4 \cdot (999 + 1) + 7 \cdot (99 + 1) + 2 \cdot (9 + 1) + 3 \cdot 1$:

$$4723 = \underbrace{4 \cdot 9 \cdot 111}_{\equiv 0 \pmod 9} + \underbrace{4}_{\equiv 4 \pmod 9} + \underbrace{7 \cdot 9 \cdot 11}_{\equiv 0 \pmod 9} + \underbrace{7}_{\equiv 7 \pmod 9} + \underbrace{2 \cdot 9 \cdot 1}_{\equiv 0 \pmod 9} + \underbrace{2}_{\equiv 2 \pmod 9} + \underbrace{3 \cdot 1}_{\equiv 3 \pmod 9} \equiv 4 + 7 + 2 + 3 \pmod 9$$

Eine natürliche Zahl ist also genau dann durch 9 teilbar, wenn ihre Ziffernsumme durch 9 teilbar ist.

b) „Jede natürliche Zahl ist modulo 3 in der gleichen Restklasse wie ihre Ziffernsumme.“

Erkläre die Aussage anhand der Zahl 4723:

$$4723 = \underbrace{4 \cdot 3 \cdot 333}_{\equiv 0 \pmod 3} + \underbrace{4}_{\equiv 4 \pmod 3} + \underbrace{7 \cdot 3 \cdot 33}_{\equiv 0 \pmod 3} + \underbrace{7}_{\equiv 7 \pmod 3} + \underbrace{2 \cdot 3 \cdot 3}_{\equiv 0 \pmod 3} + \underbrace{2}_{\equiv 2 \pmod 3} + \underbrace{3 \cdot 1}_{\equiv 3 \pmod 3} \equiv 4 + 7 + 2 + 3 \pmod 3$$

Eine natürliche Zahl ist also genau dann durch 3 teilbar, wenn ihre Ziffernsumme durch 3 teilbar ist.



1) Fülle in den beiden Tabellen die Reste bei Division durch 4 aus.

Rest von $(\square + \square) : 4$				
+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Rest von $(\square \cdot \square) : 4$				
·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2) Ermittle jene Zahl r aus $\{0, 1, 2, 3\}$, für die $23 \equiv r \pmod 4$ gilt, und fülle die Lücken aus.

$$23 = 5 \cdot 4 + 3 \implies 23 \equiv 3 \pmod 4$$

Ermittle jene Zahl r aus $\{0, 1, 2, 3\}$, für die $42 \equiv r \pmod 4$ gilt, und fülle die Lücken aus.

$$42 = 10 \cdot 4 + 2 \implies 42 \equiv 2 \pmod 4$$

3) Berechne $23 + 42 \pmod 4$ und $23 \cdot 42 \pmod 4$.

$$23 + 42 \equiv 3 + 2 \equiv 1 \pmod 4$$

$$23 \cdot 42 \equiv 3 \cdot 2 \equiv 2 \pmod 4$$

4) Wie viele Lösungen hat die Kongruenz $2 \cdot x \equiv 2 \pmod 4$ über der Grundmenge $\{0, 1, 2, 3\}$?

2 Lösungen: $x = 1$ und $x = 3$

5) Wie viele Lösungen hat die Kongruenz $2 \cdot x \equiv 1 \pmod 4$ über der Grundmenge $\{0, 1, 2, 3\}$?

Keine Lösung.



1) Fülle in den beiden Tabellen die Reste bei Division durch 5 aus.

Rest von $(\square + \square) : 5$					
+	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

Rest von $(\square \cdot \square) : 5$					
·	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

2) Was fällt dir in der Tabelle zum Multiplizieren auf?

Bis auf in der ersten Zeile enthält jede Zeile alle Zahlen aus $\{0, 1, 2, 3, 4\}$ genau einmal.

3) a und b sind jeweils Zahlen aus $\{1, 2, 3, 4\}$.

Wie viele Lösungen hat die Kongruenz $a \cdot x \equiv b \pmod{5}$ über der Grundmenge $\{0, 1, 2, 3, 4\}$?

Genau eine Lösung.



1) Fülle in den beiden Tabellen die Reste bei Division durch 6 aus.

Rest von $(\square + \square) : 6$						
+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Rest von $(\square \cdot \square) : 6$						
·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2) Welche Zeilen in der Multiplikations-Tabelle enthalten alle Zahlen aus $\{0, 1, 2, 3, 4, 5\}$ genau einmal?

Es gibt einen Zusammenhang mit dem Divisor 6. Hast du eine Vermutung?

Die Zeile $1 \cdot x$ und die Zeile $5 \cdot x$.

1 und 5 sind genau die Zahlen aus $\{1, 2, 3, 4, 5\}$, die zu 6 teilerfremd sind.



Wir dürfen beide Seiten einer Kongruenz modulo m durch einen gemeinsamen Teiler c dividieren. Bei der neuen Kongruenz müssen wir aber modulo $\frac{m}{\text{ggT}(c,m)}$ rechnen:

$$a \cdot c \equiv b \cdot c \pmod m \stackrel{(*)}{\iff} a \equiv b \pmod{\frac{m}{\text{ggT}(c,m)}}$$

Zum Beispiel: $\underbrace{18}_{=3 \cdot 6} \equiv \underbrace{30}_{=5 \cdot 6} \pmod 4 \iff 3 \equiv 5 \pmod 2$, weil $\text{ggT}(6,4) = 2$.

Auf dem **AB – Fundamentalsatz der Arithmetik** haben wir $m \mid c \cdot N \iff \frac{m}{\text{ggT}(c,m)} \mid N$ gezeigt. Damit können wir $(*)$ begründen:

$$\begin{aligned} a \cdot c \equiv b \cdot c \pmod m &\iff \underbrace{a \cdot c - b \cdot c}_{c \cdot (a-b)} \equiv 0 \pmod m \iff \\ &\iff m \mid c \cdot (a-b) \stackrel{N=a-b}{\iff} \\ &\iff \frac{m}{\text{ggT}(c,m)} \mid a-b \iff \\ &\iff a-b \equiv 0 \pmod{\frac{m}{\text{ggT}(c,m)}} \iff \\ &\iff a \equiv b \pmod{\frac{m}{\text{ggT}(c,m)}} \end{aligned}$$



1) Fülle in den beiden Tabellen die Reste bei Division durch 7 aus.

Rest von $(\square + \square) : 7$							
+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Rest von $(\square \cdot \square) : 7$							
·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

2) c ist eine Zahl aus $\{1, 2, 3, 4, 5, 6\}$.

Die Spalte $x \cdot c \pmod 7$ enthält jede der Zahlen $\{0, 1, 2, 3, 4, 5, 6\}$ genau einmal. Begründe, warum das aus der Rechenregel für die Division folgt.

7 ist eine Primzahl, also ist $\text{ggT}(c, 7) = 1$

Aus $a \cdot c \equiv b \cdot c \pmod 7$ folgt mit der Rechenregel $a \equiv b \pmod 7$.

Die Zahlen $\{0, 1, 2, 3, 4, 5, 6\}$ sind in verschiedenen Restklassen modulo 7.

Also müssen $0 \cdot c, 1 \cdot c, 2 \cdot c, \dots, 6 \cdot c$ in verschiedenen Restklassen modulo 7 sein.