

Rechenregeln für Kongruenzen

$a \equiv b \pmod{m} \Leftrightarrow a$ und b lassen bei Division durch m den gleichen Rest $\Leftrightarrow m \mid (a - b)$

Für alle $a, b, c, d, r, a_1, b_1 \in \mathbb{Z}; m \in \mathbb{N} \setminus \{1\}$ gilt:

Nr.	Rechenregel	Beispiele	Erläuterung in Kurzform und Beweisskizze
1.	$a \equiv a \pmod{m}$	$6 \equiv 6 \pmod{5}$	Jede Zahl ist zu sich selbst kongruent: $m \mid (a - a)$
2.	$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$	$6 \equiv 11 \pmod{5}$ $\Rightarrow 11 \equiv 6 \pmod{5}$	a und b lassen bei Division durch m den gleichen Rest: $m \mid (a - b) \Rightarrow \dots \Rightarrow m \mid (b - a) \Rightarrow \dots$
3.	$a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$ $\Rightarrow a \equiv c \pmod{m}$	$13 \equiv 27 \pmod{7}$ und $27 \equiv 41 \pmod{7}$ $\Rightarrow 13 \equiv 41 \pmod{7}$	Wenn a und b den gleichen Rest lassen und b und c den gleichen Rest lassen, dann lassen auch a und c den gleichen Rest: $m \mid (a - b)$ und $m \mid (b - c) \Rightarrow m \mid (a - b + b - c) \Rightarrow \dots$
4.	Addition/Subtraktion $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$ $\Rightarrow a \pm c \equiv b \pm d \pmod{m}$	$48 \equiv 27 \pmod{7}$ und $18 \equiv 25 \pmod{7}$ $\Rightarrow 66 \equiv 52 \pmod{7}$ $\Rightarrow 30 \equiv 2 \pmod{7}$	Kongruenzen zum gleichen Modul können addiert und subtrahiert werden: $m \mid (a - b)$ und $m \mid (c - d) \Rightarrow m \mid (a - b) \pm (c - d) \Rightarrow \dots$
5.	$a \equiv b \pmod{m}$ $\Rightarrow a \pm c \equiv b \pm c \pmod{m}$	$31 \equiv 67 \pmod{9}$ $\Rightarrow 33 \equiv 69 \pmod{9}$ $\Rightarrow 20 \equiv 56 \pmod{9}$	Wenn a und b bei Division durch m den gleichen Rest lassen, dann auch $a \pm c$ und $b \pm c$: siehe 4. mit $a \equiv b \pmod{m}$ und $c \equiv c \pmod{m}$
6.	Multiplikation $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$ $\Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$	$15 \equiv 39 \pmod{6}$ und $4 \equiv 16 \pmod{6}$ $\Rightarrow 60 \equiv 624 \pmod{6}$	Kongruenzen zum gleichen Modul können multipliziert werden: $m \mid (a - b)$ und $m \mid (c - d)$ $\Rightarrow m \mid (a - b) \cdot c$ und $m \mid (c - d) \cdot b$ $\Rightarrow m \mid (a - b) \cdot c + (c - d) \cdot b \Rightarrow \dots$
7.	$a \equiv b \pmod{m}$ $\Rightarrow a \cdot c \equiv b \cdot c \pmod{m}$	$6 \equiv 30 \pmod{12}$ $\Rightarrow 24 \equiv 120 \pmod{12}$	Wenn a und b bei Division durch m den gleichen Rest lassen, dann auch $a \cdot c$ und $b \cdot c$: siehe 6. mit $a \equiv b \pmod{m}$ und $c \equiv c \pmod{m}$
8.	Potenzieren $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$ <u>allgemein:</u> $n \in \mathbb{N}$ $a \equiv b \pmod{m} \Rightarrow a^n \equiv b^n \pmod{m}$	$3 \equiv 7 \pmod{4}$ $\Rightarrow 9 \equiv 49 \pmod{4}$ $\Rightarrow 27 \equiv 343 \pmod{4}$	Kongruenzen können potenziert werden: siehe 6. mit $a \equiv b \pmod{m}$ und $c \equiv c \pmod{m}$
9.	Division $\text{ggT}(d, m) = 1$ und $a \equiv b \pmod{m}$ $\Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$	$\text{ggT}(3, 8) = 1$ und $6 \equiv 54 \pmod{8}$ $\Rightarrow 2 \equiv 18 \pmod{8}$ Falls $\text{ggT}(d, m) \neq 1$: $\text{ggT}(4, 8) = 4$ und $12 \equiv 28 \pmod{8}$ aber $3 \not\equiv 7 \pmod{8}$ Division kann aber auch funktionieren: $\text{ggT}(3, 6) = 3$ und $24 \equiv 6 \pmod{6}$ doch $8 \equiv 2 \pmod{6}$	Kongruenzen können durch eine ganze Zahl d geteilt werden, wenn d und der Modul teilerfremd sind (a und b müssen durch d teilbar sein): d ist Teiler von a und von b : $a = a_1 d$; $b = b_1 d$ $a \equiv b \pmod{m} \Rightarrow m \mid (a - b)$ $\Rightarrow m \mid (a_1 d - b_1 d) \Rightarrow m \mid (a_1 - b_1) d$ $\text{ggT}(m, d) = 1 \Rightarrow m$ teilt nicht d $\Rightarrow m \mid (a_1 - b_1) \Rightarrow a_1 \equiv b_1 \pmod{m}$ $\Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$
10.	Übergang zu den Resten $a \equiv m \cdot c + r \pmod{m}$ $\Rightarrow a \equiv r \pmod{m}$	$80 \equiv 20 \pmod{6}$ $80 \equiv 6 \cdot 3 + 2 \pmod{6}$ $\Rightarrow 80 \equiv 2 \pmod{6}$	Bei der Rechnung mit Kongruenzen kann man immer zu den Resten übergehen. $a \equiv m \cdot c + r \pmod{m} \Rightarrow a - r \equiv m \cdot c \pmod{m}$ $m \mid m \cdot c \Rightarrow m \mid (a - r) \Rightarrow a \equiv r \pmod{m}$

Rechenregeln für Kongruenzen

$a \equiv b \pmod{m} \Leftrightarrow a$ und b lassen bei Division durch m den gleichen Rest $\Leftrightarrow m \mid (a - b)$

Für alle $a, b, c, d, r, a_1, b_1 \in \mathbb{Z}; m \in \mathbb{N} \setminus \{1\}$ gilt:

Nr.	Rechenregel	Beispiele	Erläuterung in Kurzform und Beweisskizze
1.	$a \equiv a \pmod{m}$	$6 \equiv 6 \pmod{5}$	Jede Zahl ist zu sich selbst kongruent: $m \mid (a - a)$
2.	$a \equiv b \pmod{m}$ $\Rightarrow b \equiv a \pmod{m}$	$6 \equiv 11 \pmod{5}$ $\Rightarrow 11 \equiv 6 \pmod{5}$	a und b lassen bei Division durch m den gleichen Rest: $m \mid (a - b) \Rightarrow \dots \Rightarrow m \mid (b - a) \Rightarrow \dots$
3.	$a \equiv b \pmod{m}$ und $b \equiv c \pmod{m}$ $\Rightarrow a \equiv c \pmod{m}$	$13 \equiv 27 \pmod{7}$ $27 \equiv 41 \pmod{7}$ \Rightarrow $13 \equiv 41 \pmod{7}$	Wenn a und b den gleichen Rest lassen und b und c den gleichen Rest lassen, dann lassen auch a und c den gleichen Rest: $m \mid (a - b)$ und $m \mid (b - c)$ $\Rightarrow m \mid (a - b + b - c) \Rightarrow \dots$
4.	<u>Addition/Subtraktion</u> $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$ $\Rightarrow a \pm c \equiv b \pm d \pmod{m}$	$48 \equiv 27 \pmod{7}$ $18 \equiv 25 \pmod{7}$ \Rightarrow $66 \equiv 52 \pmod{7}$ $30 \equiv 2 \pmod{7}$	Kongruenzen zum gleichen Modul können addiert und subtrahiert werden: $m \mid (a - b)$ und $m \mid (c - d)$ $\Rightarrow m \mid (a - b) \pm (c - d)$ $\Rightarrow \dots$
5.	$a \equiv b \pmod{m}$ $\Rightarrow a \pm c \equiv b \pm c \pmod{m}$	$31 \equiv 67 \pmod{9}$ \Rightarrow $33 \equiv 69 \pmod{9}$ $20 \equiv 56 \pmod{9}$	Wenn a und b bei Division durch m den gleichen Rest lassen, dann auch $a \pm c$ und $b \pm c$: siehe 4. mit $a \equiv b \pmod{m}$ und $c \equiv c \pmod{m}$
6.	<u>Multiplikation</u> $a \equiv b \pmod{m}$ und $c \equiv d \pmod{m}$ \Rightarrow $a \cdot c \equiv b \cdot d \pmod{m}$	$15 \equiv 39 \pmod{6}$ $4 \equiv 16 \pmod{6}$ \Rightarrow $60 \equiv 624 \pmod{6}$	Kongruenzen zum gleichen Modul können multipliziert werden: $m \mid (a - b)$ und $m \mid (c - d)$ $\Rightarrow m \mid (a - b) \cdot c$ und $m \mid (c - d) \cdot b$ $\Rightarrow m \mid (a - b) \cdot c + (c - d) \cdot b$ $\Rightarrow \dots$
7.	$a \equiv b \pmod{m}$ $\Rightarrow a \cdot c \equiv b \cdot c \pmod{m}$	$6 \equiv 30 \pmod{12}$ \Rightarrow $24 \equiv 120 \pmod{12}$	Wenn a und b bei Division durch m den gleichen Rest lassen, dann auch $a \cdot c$ und $b \cdot c$: siehe 6. mit $a \equiv b \pmod{m}$ und ...

Nr.	Rechenregel	Beispiele	Erläuterung in Kurzform und Beweisskizze
8.	<p><u>Potenzieren</u> $a \equiv b \pmod{m}$ $\Rightarrow a^2 \equiv b^2 \pmod{m}$</p> <p><u>allgemein: $n \in \mathbb{N}$</u> $a \equiv b \pmod{m}$ $\Rightarrow a^n \equiv b^n \pmod{m}$</p>	$3 \equiv 7 \pmod{4}$ \Rightarrow $9 \equiv 49 \pmod{4}$ $27 \equiv 343 \pmod{4}$	<p>Kongruenzen können potenziert werden: siehe 6. mit $a \equiv b \pmod{m}$ und ...</p>
9.	<p><u>Division</u> $\text{ggT}(d, m) = 1$ und $a \equiv b \pmod{m}$ $\Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$</p>	$\text{ggT}(3, 8) = 1$ $6 \equiv 54 \pmod{8}$ $\Rightarrow 2 \equiv 18 \pmod{8}$ <p>Falls $\text{ggT}(d, m) \neq 1$: $\text{ggT}(4, 8) = 4$ $12 \equiv 28 \pmod{8}$ aber $3 \not\equiv 7 \pmod{8}$</p> <p>Division kann funktionieren: $\text{ggT}(3, 6) = 3$ $24 \equiv 6 \pmod{6}$ doch $8 \equiv 2 \pmod{6}$</p>	<p>Kongruenzen können durch eine ganze Zahl d geteilt werden, wenn d und der Modul teilerfremd sind (a und b müssen durch d teilbar sein):</p> <p>d ist ein Teiler von a und von b: $a = a_1 d ; b = b_1 d$ $a \equiv b \pmod{m}$ $\Rightarrow m (a - b) \Rightarrow m (a_1 d - b_1 d)$ $\Rightarrow m (a_1 - b_1) d$</p> <p>$\text{ggT}(m, d) = 1 \Rightarrow m$ teilt nicht d $\Rightarrow m (a_1 - b_1)$ $\Rightarrow a_1 \equiv b_1 \pmod{m}$ $\Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$</p>
10.	<p><u>Übergang zu den Resten</u> $a \equiv m \cdot c + r \pmod{m}$ $\Rightarrow a \equiv r \pmod{m}$</p>	$80 \equiv 20 \pmod{6}$ $80 \equiv 6 \cdot 3 + 2 \pmod{6}$ $\Rightarrow 80 \equiv 2 \pmod{6}$	<p>Bei der Rechnung mit Kongruenzen kann man immer zu den Resten übergehen: $a \equiv m \cdot c + r \pmod{m}$ $\Rightarrow a - r \equiv m \cdot c \pmod{m}$ $m m \cdot c \Rightarrow m (a - r)$ $\Rightarrow a \equiv r \pmod{m}$</p>