1. Äquivalenzrelation
2. Tischler-Problem
3. Euklidischer Algorithmus
4. Erweiterter euklidischer Algorithmus
5. Lineare diophantische Gleichung
6. Rechnen mit Resten
7. Restklassen
8. $\mathbb{Z}_8$
9. $\mathbb{Z}_8 \times \mathbb{Z}_6$
10. Teilbarkeit in $\mathbb{Z}$
11. Beispiel einer Kongruenzgleichung
12. Chinesischer Restsatz
13. Simultane Kongruenzen
14. Kleiner Satz von Fermat
15. Satz von Euler
16. Eulersche φ-Funktion

↑ Äquivalenzrelation

Nehmen wir die Menge $\mathbb{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, z. B. 9 nummerierte Personen.
Unter Berücksichtigung der Verwandtschaftsbeziehung zerfällt $\mathbb{A}$ in disjunkte Teilmengen (Familien),
z. B. $\{1, 8\}$, $\{3, 5, 6\}$, $\{2, 4, 7\}$, $\{9\}$.
Die Verwandtschaftsbeziehungen tragen wir in eine Tabelle ein, (a, b) für a verwandt mit b.
math. Sprechweise: a äquivalent b, $a \sim b$.
Es gilt hier offensichtlich für a, b, $c \in \mathbb{A}$:
$a \sim a$ Relation ist reflexiv
$a \sim b \implies b \sim a$ symmetrisch
$a \sim b$, $b \sim c \implies a \sim c$ transitiv

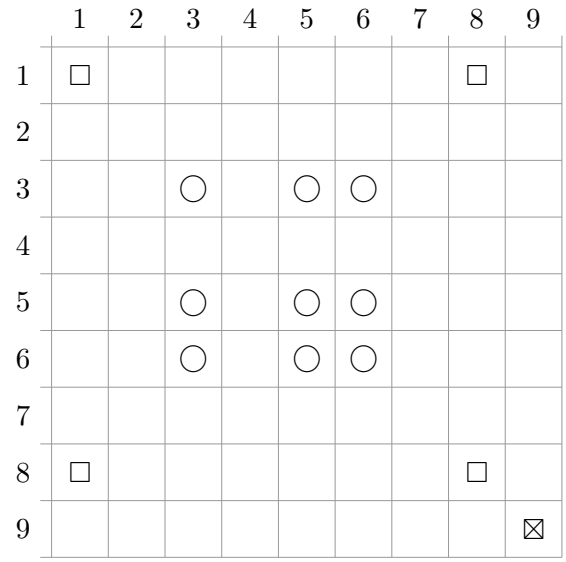
	1	2	3	4	5	6	7	8	9
1	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)	(1,8)	(1,9)
2	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)	(2,8)	(2,9)
3	(3,1)	⋯							
4	(4,1)								
5	(5,1)								
6	(6,1)								
7	(7,1)								
8	(8,1)								
9	(9,1)								

Beginnen wir mit den Teilmengen $\{1, 8\}$ und $\{9\}$.
Symbole statt (a, b) erhöhen die Anschauung.

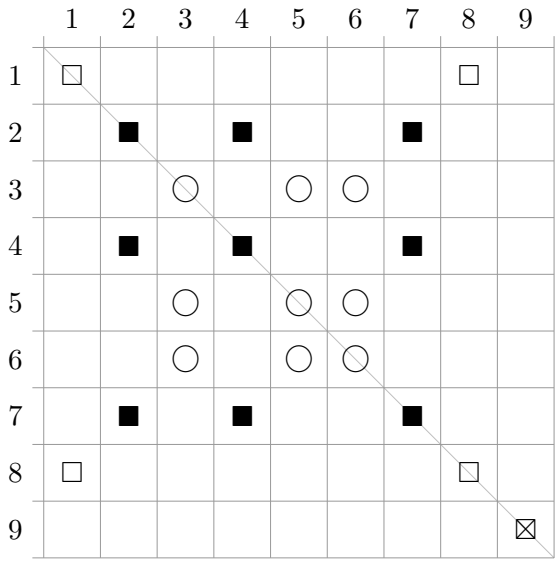
	1	2	3	4	5	6	7	8	9
1	□							□	
2									
3									
4									
5									
6									
7									
8	□							□	
9									⊠

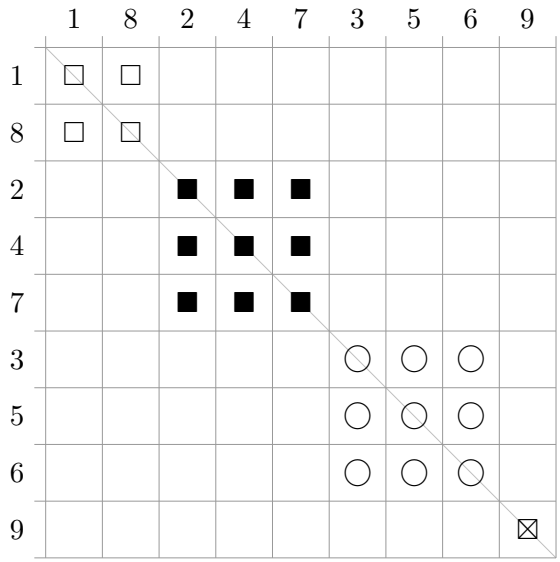
↑ Äquivalenzrelation

Die Beziehungen in der Familie $\{3, 5, 6\}$ werden hinzugefügt,



sowie die der Familie $\{2, 4, 7\}$.





Eine Umordnung der Elemente hebt die Struktur der Relation (Teilmenge von $\mathbb{A} \times \mathbb{A}$) hervor.
Den Teilmengen (Äquivalenzklassen) der Zerlegung von $\mathbb{A}$ (Partition) entsprechen in der Tabelle nicht überlapp Quadrate, die die Diagonale überdecken.
Die Transitivität der Relation garantiert die quadratischen Anordnungen, z. B. $4 \sim 2$, $2 \sim 7 \implies 4 \sim 7$

Eine Partition einer Menge kann dadurch erzeugt werden, dass die Elemente der Menge nach einer Eigenschaft (gehört zur Familie F_k) zusammengefasst werden, oder es wird eine Relation (a ist verwandt mit b) herangezogen, die reflexiv, symmetrisch und transitiv ist.

↑ Äquivalenzrelation

Etwas allgemeiner ergibt sich folgendes Bild:

	1	2	3	4	5	6	7	8	9
1	×							×	
2		×		×			×		
3			×		×	×			
4		×		×			×		
5			×		×	×			
6			×		×	×			
7		×		×			×		
8	×							×	
9									×

	1	8	2	4	7	3	5	6	9
1	×	×							
8	×	×							
2			×	×	×				
4			×	×	×				
7			×	×	×				
3						×	×	×	
5						×	×	×	
6						×	×	×	
9									×

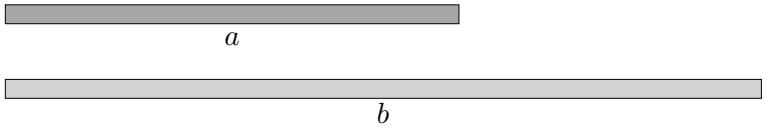
Teilen wir die Zahlen der Menge $\mathbb{M} = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ durch 3 und fassen die Zahlen nach den möglichen Teilerresten 0, 1, 2 zusammen: $\mathbb{M} = \{3, 6, 9\} \cup \{1, 4, 7\} \cup \{2, 5, 8\}$

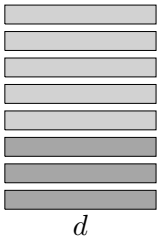
	3	6	9	1	4	7	2	5	8
3	0	0	0						
6	0	0	0						
9	0	0	0						
1				1	1	1			
4				1	1	1			
7				1	1	1			
2							2	2	2
5							2	2	2
8							2	2	2

Die Partition kann auch durch eine Äquivalenzrelation erzeugt werden.
Betrachten wir hierzu die Teilmenge $\{1, 4, 7\}$.
Es gilt: $1 = 0 \cdot 3 + 1$, $4 = 1 \cdot 3 + 1$, $7 = 2 \cdot 3 + 1$.
Die Differenz zweier Zahlen ist durch 3 teilbar (der Rest 1 fällt raus).
$b - a$ ist genau dann durch 3 teilbar, wenn a und b denselben Teilerrest haben.
$a \sim b \iff 3$ teilt $b - a$ andere Bezeichnung $a \equiv b \mod 3$, a kongruent b modulo 3
Das Vorzeichen von $b-a$ spielt keine Rolle, möglich wäre auch $a \sim b \iff 3$ teilt $|\, b-a \,|$.

↑ Tischler-Problem

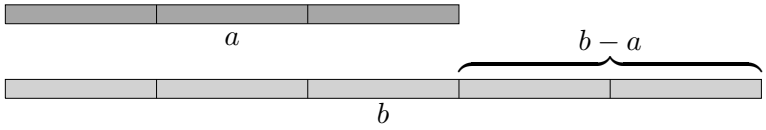
Stell Dir vor, du hast zwei Stäbe der Länge a und b, wobei a und b natürliche Zahlen sind.
Du möchtest die Stäbe in gleichgroße Stücke zersägen und zwar so, dass die Länge d der Stücke möglichst groß.

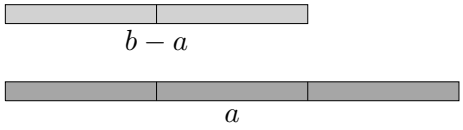




↑ Tischler-Problem

Stell Dir vor, du hast zwei Stäbe der Länge a und b, wobei a und b natürliche Zahlen sind.
Du möchtest die Stäbe in gleichgroße Stücke zersägen und zwar so, dass die Länge d der Stücke möglichst groß.





1. Wenn $a = b$, dann ist die gesuchte Länge a.
2. Wenn b größer ist als a, dann ist die gesuchte Länge für a und b dieselbe wie die gesuchte Länge für $b - a$ und a.

↑ Euklidischer Algorithmus

1. Welche Zahlen sind durch 3 teilbar?

Lösung: Alle Zahlen, die mit 3er-Schritten erreichbar sind, d. h. alle Vielfachen von 3, nämlich: 3, 6, 9, 12, 15, ...

2. Ist 7063 durch 7 teilbar?

Lösung: 7063 = 7000 + 63
Mit 1000 und anschließend 9 7er-Schritten ist die Zahl erreichbar.

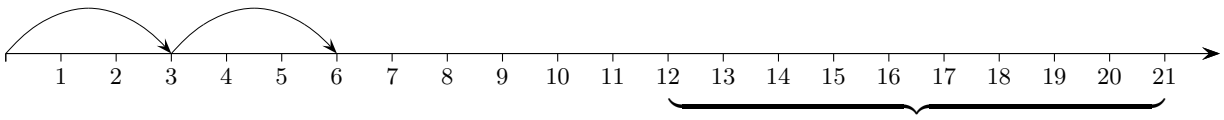
3. Ist 582 durch 3 teilbar?

Lösung: Um dies zu erkennen, gibt es eine einfache Regel. Hierzu zerlegen wir 582 geschickt:
$582 = 100 \cdot 5 + 10 \cdot 8 + 2$
$582 = 99 \cdot 5 + 1 \cdot \underline{5} + 9 \cdot 8 + 1 \cdot \underline{8} + \underline{2}$
Da 99 und 9 durch 3 teilbar sind, muss lediglich untersucht werden, ob dies auch für $\underbrace{5 + 8 + 2}$ *zutrifft.*
Dies ist die Quersumme von 582.

Eine Zahl ist durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.

Die Zerlegung liefert auch eine Begründung für:
Eine Zahl ist durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.

4. Wie lauten alle gemeinsamen Teiler von 12 und 21?



Wenn 12 mit einer bestimmten Schrittweite erreichbar ist und auch 21 mit dieser Schrittweite, dann trifft dies auch für die Differenz $21 - 12 = 9$ zu (beachte die Schritte von 12 bis 21).
Statt die Teiler von 12 und 21 zu suchen, können daher auch die Teiler von 12 und 9 ermittelt werden. Offensichtlich gibt es nur den gemeinsamen Teiler 3. Die Bildung der Differenz kann wiederholt werden. Mit diesem Verfahren kann der größte gemeinsame Teiler (ggT) gefunden werden.

$\text{ggT}(52, 30) = 2$

$52 = 1 \cdot 30 + 22$
$30 = 1 \cdot 22 + 8$
$22 = 2 \cdot 8 + 6$
$8 = 1 \cdot 6 + 2$
$6 = 3 \cdot 2 + 0$

Von unten nach oben gelesen erhält man daraus die Darstellung:

$2 = 3 \cdot 30 - 4 \cdot (52 - 30) = 7 \cdot 30 - 4 \cdot 52$
$= 3 \cdot (30 - 22) - 22 = 3 \cdot 30 - 4 \cdot 22$
$= 8 - (22 - 2 \cdot 8) = 3 \cdot 8 - 22$
$2 = 8 - 6$

Mit der vorletzten Zeile beginnen.

$\text{ggT}(48,5) = 1$

$48 = 9 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Von unten nach oben gelesen erhält man daraus die Darstellung:

$1 = 2 \cdot (48 - 9 \cdot 5) - 5 = 2 \cdot 48 - 19 \cdot 5$

$= 3 - (5 - 3) \qquad = 2 \cdot 3 - 5$

$1 = 3 - 2$

Damit ist gezeigt, dass

$$1 = 2 \cdot 48 - 19 \cdot 5$$

gilt, woraus

$$-19 \cdot 5 \mod 48 = 1$$

folgt.

Addieren wir auf der linken Seite noch $48 \cdot 5$ (was auf der rechten Seite nichts ändert, da wir modulo 48 rechnen) erhalten wir

$$29 \cdot 5 \mod 48 = 1$$

Satz von Bézout
Seien $a, b \in \mathbb{N}_0$. Der größte gemeinsame Teiler $\text{ggT}(a,b)$ lässt sich als ganzzahlige Linearkombination von a und b darstellen:

$$\text{ggT}(a,b) = u \cdot a + v \cdot b \quad \text{mit } u, v \in \mathbb{Z}.$$

Die Darstellung ist nicht eindeutig,
die Gleichung wird durch verschiedene Zahlenpaare u, v erfüllt.

$\text{ggT}(16,6) = 2 = -1 \cdot 16 + 3 \cdot 6$

$= \quad 2 \cdot 16 - 5 \cdot 6$

Folgende Anordnung erleichtert beim rückwärtigen Einsetzen den Überblick zu behalten.

$48 = 9 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = \quad 2 \cdot 48 - 19 \cdot 5$

$= -1 \cdot \quad 5 + \quad 2 \cdot 3$

$1 = \qquad 3 - \quad 1 \cdot 2$

Das rückwärtige Einsetzen kann vereinfacht werden.
Die Werte für u und v werden von unten nach oben schrittweise ermittelt.

$48 = \quad 9 \quad \cdot 5 + 3$

$5 = \quad 1 \quad \cdot 3 + 2$

$3 = \quad 1 \quad \cdot 2 + 1$

$2 = \quad 2 \quad \cdot 1 + 0$

u	v	
2	-19	$= -1 - 9 \cdot 2$
-1	2	$= 1 - 1 \cdot (-1)$
1	-1	

↑ Erweiterter euklidischer Algorithmus

Das rückwärtige Einsetzen kann vereinfacht werden.
Die Werte für u und v werden von unten nach oben schrittweise ermittelt.

$$
\begin{aligned}
48 &= 9 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}
$$

u	v	
2	-19	$= -1 - 9 \cdot 2$
-1	2	$= 1 - 1 \cdot (-1)$
1	-1	

Zur Begründung gehen wir zu einer allgemeineren Schreibweise über.

$$
\begin{aligned}
a &= q_1 \cdot b + r_1 \\
(b =)\ r_0 &= q_2 \cdot r_1 + r_2 \\
r_1 &= q_3 \cdot r_2 + r_3 \\
r_2 &= q_4 \cdot r_3 + r_4 \\
r_3 &= q_5 \cdot r_4
\end{aligned}
$$

u	v
$\dots$	$\dots$
v	$u - q_2 \cdot v$
u	v
1	$-q_4$
0	1

$r_4 = ur_1 + v(r_0 - q_2 r_1) = vr_0 + (u - q_2 v)r_1$

d. h. $\mathrm{ggT}(a, b) = r_4 = ur_1 + vr_2$

Mit der vorletzten Zeile kann begonnen werden.

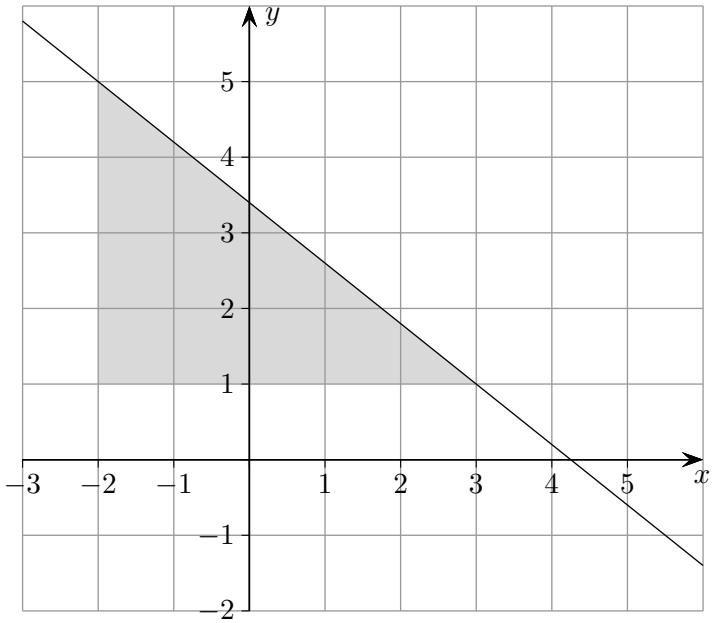
↑ Lineare diophantische Gleichung

$$ax + by = c$$

Gesucht sind die ganzzahligen Lösungen x und y mit vorgegebenen ganzen Zahlen a, b und c.
$ax + by = c$ kann als Geradengleichung gelesen werden. Die Frage lautet daher:
Durch welche Gitterpunkte verläuft die Gerade?

$4x + 5y = 17$

$y = -\frac{4}{5}x + \frac{17}{5}$



Hier liegt die für lineare Probleme typische Lösungsstruktur vor.
Alle Lösungen der zugehörigen homogenen Gleichung

$$4x + 5y = 0$$

unseres Beispiel werden durch $(5k \mid -4k)$, $k \in \mathbb{Z}$ erfasst.
Eine einzige (partikuläre) Lösung der inhomogenen Gleichung $4x + 5y = 17$ ist z. B. $(-2 \mid 5)$.
Die allgemeine Lösung der diophantischen Gleichung setzt sich nun aus dieser partikulären (speziellen) Lösung und der allgemeinen Lösung der homogenen Gleichung zusammen, hier

$$(x \mid y) = (-2 \mid 5) + (5k \mid -4k).$$

Zur Begründung ist wichtig:
Mit zwei Lösungen einer inhomogenen Gleichung ist die Differenz eine Lösung der zugehörigen homogenen Gleichung.

Eine einzelne Lösung von

$$ax + by = c$$

kann für $c = \text{ggT}(a, b)$ mit dem erweiterten euklidischen Algorithmus erhalten werden.
Falls c ein Vielfaches des ggTs ist, wäre die erhaltene Lösung noch zu multiplizieren.
In allen anderen Fällen ist die Gleichung nicht lösbar. Hierzu ist lediglich zu beachten, dass der $\text{ggT}(a, b)$ die linke Seite der Gleichung teilt und damit auch die Rechte.

Die allgemeine Lösung von $6x + 4y = 0$ ist nicht $(4k \mid -6k)$, $k \in \mathbb{Z}$, es fehlt z. B. $(2 \mid -3)$.

$$ax + by = 0$$

wird also durch $(\frac{b}{\text{ggT}(a,b)}\,k \mid -\frac{a}{\text{ggT}(a,b)}\,k)$, $k \in \mathbb{Z}$, vollständig gelöst.

↑ Rechnen mit Resten

1 €-Gutscheine im Gesamtwert von 318 € sollen auf 7 Personen gleichmäßig verteilt werden.
Wie viele Gutscheine bleiben übrig?

$318 = 45 \cdot 7 + 3$, 3 Gutscheine bleiben übrig. Schreibweise: $318 \mod 7 = 3$

Der Rest verändert sich nicht, wenn ein Vielfaches von 7 von 318 subtrahiert wird.
Das kann einem Zwischenstand beim Verteilen entsprechen.

Wenn im Übereifer 7 Gutscheine zuviel verteilt werden, $318 = 46 \cdot 7 - 4$, entsteht ein Defizit von -4.
Es kann durch Rücknahme von 7 Gutscheinen in einen positiven Rest umgewandelt werden.

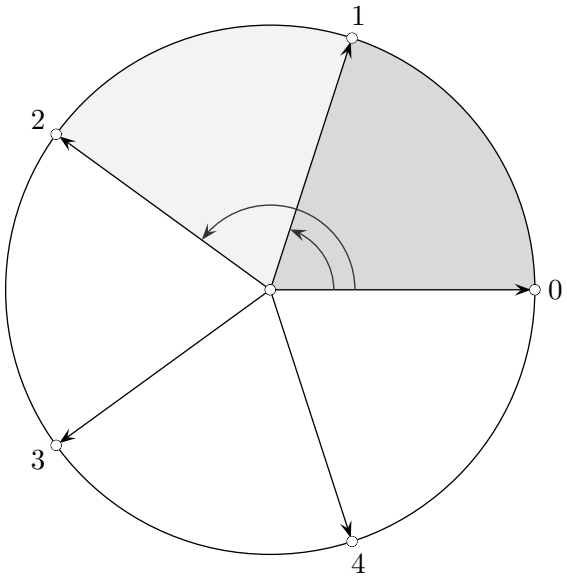
$$(4 + 25 \cdot 7) \cdot (2 + 34 \cdot 7) = 8 + 7 \cdot (\quad) \equiv 8 \equiv 1 \mod 7$$

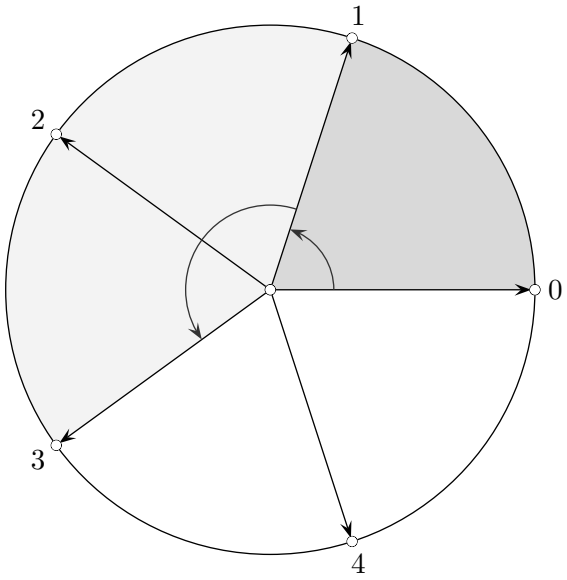
$$(-2 + 28 \cdot 7) \cdot (5 + 31 \cdot 7) = -10 + 7 \cdot (\quad) \equiv -3 \equiv 4 \mod 7$$

$$\begin{aligned} & 9^{10} \mod 7 \\ \equiv\ & 2^{10} \\ \equiv\ & 2^3 \cdot 2^3 \cdot 2^3 \cdot 2 \\ \equiv\ & 1 \cdot 1 \cdot 1 \cdot 2 \\ \equiv\ & 2 \end{aligned}$$

$$\begin{aligned} & 4^{10} \mod 7 \\ \equiv\ & (-3)^{10} \\ \equiv\ & (-3)^3 \cdot (-3)^3 \cdot (-3)^3 \cdot (-3) \\ \equiv\ & (-27) \cdot (-27) \cdot (-27) \cdot (-3) \\ \equiv\ & 1 \cdot 1 \cdot 1 \cdot (-3) \\ \equiv\ & 4 \end{aligned}$$

↑ Rechnen mit Resten





Wir rechnen in den natürlichen Zahlen $\mathbb{N}_0$ (einschließlich 0) und betrachten die Reste, die bei der Division durch 5 entstehen. Auf der Menge $\{0, 1, 2, 3, 4\}$ können zwei Verknüpfungen in naheliegender Weise definiert werden.
$1 + 2 = 3$ bedeutet, dass ein Rest von 3 verbleibt, wenn zwei Zahlen mit den Resten 1 und 2 addiert werden. Was ergibt $3 + 4$.

Fülle die Verknüpfungstafeln aus und überprüfe an einigen Beispielen, ob $a \circ (b + c) = a \circ b + a \circ c$ gilt.

+	0	1	2	3	4
0					
1					
2					
3					
4					

∘	0	1	2	3	4
0					
1					
2					
3					
4					

Was ist unter $2 - 3$ zu verstehen? Ist $\frac{1}{3}$ sinnvoll?

↑ Restklassen

Wir fassen die Zahlen aus $\mathbb{N}_0$ zu Restklassen zusammen, deren Elemente bei Division mit 4 jeweils denselben Rest ergeben.

$\overline{0} = \{0, 4, 8, 12, \ldots\} = 4\mathbb{N}_0$
$\overline{1} = \{1, 5, 9, 13 \ldots\} = 1 + 4\mathbb{N}_0$
$\overline{2} = \{2, 6, 10, 14 \ldots\} = 2 + 4\mathbb{N}_0$
$\overline{3} = \{3, 7, 11, 15 \ldots\} = 3 + 4\mathbb{N}_0$

Durch eine Betrachtung der Reste wird Folgendes klar:

$$a \equiv b,\ c \equiv d \quad \Longrightarrow \quad a + c \equiv b + d \pmod 4$$

$a = n \cdot 4 + r_1$
$c = m \cdot 4 + r_2$
Wenn a und b den Rest r_1 ergeben und c und d den Rest r_2, so ist der Rest für $a + c$ und $b + d$ jeweils $(r_1 + r_2)$ mod 4 (eventuell muss 4 subtrahiert werden).

$$a \equiv b,\ c \equiv d \quad \Longrightarrow \quad ac \equiv bd \pmod 4$$

$ac = 4 \cdot (\ldots) + r_1 r_2$
$bd = 4 \cdot (\ldots) + r_1 r_2$
Es entsteht derselbe Rest $r_1 r_2$ mod 4.

Mit Kongruentem kann ausgetauscht werden:

$$a \equiv bc,\quad c \equiv d \quad \Longrightarrow \quad a \equiv bd \pmod 4$$

Begründung:
Aus $c \equiv d$ folgt $bc \equiv bd$ und mit der Voraussetzung erhalten wir $a \equiv bd$

Nun sollte verständlich sein, dass z. B. 3^{98} bei Division mit 8 den Rest 1 ergibt:

$$3^{98} \equiv 9^{49} \equiv 1^{49} \equiv 1 \pmod 8$$

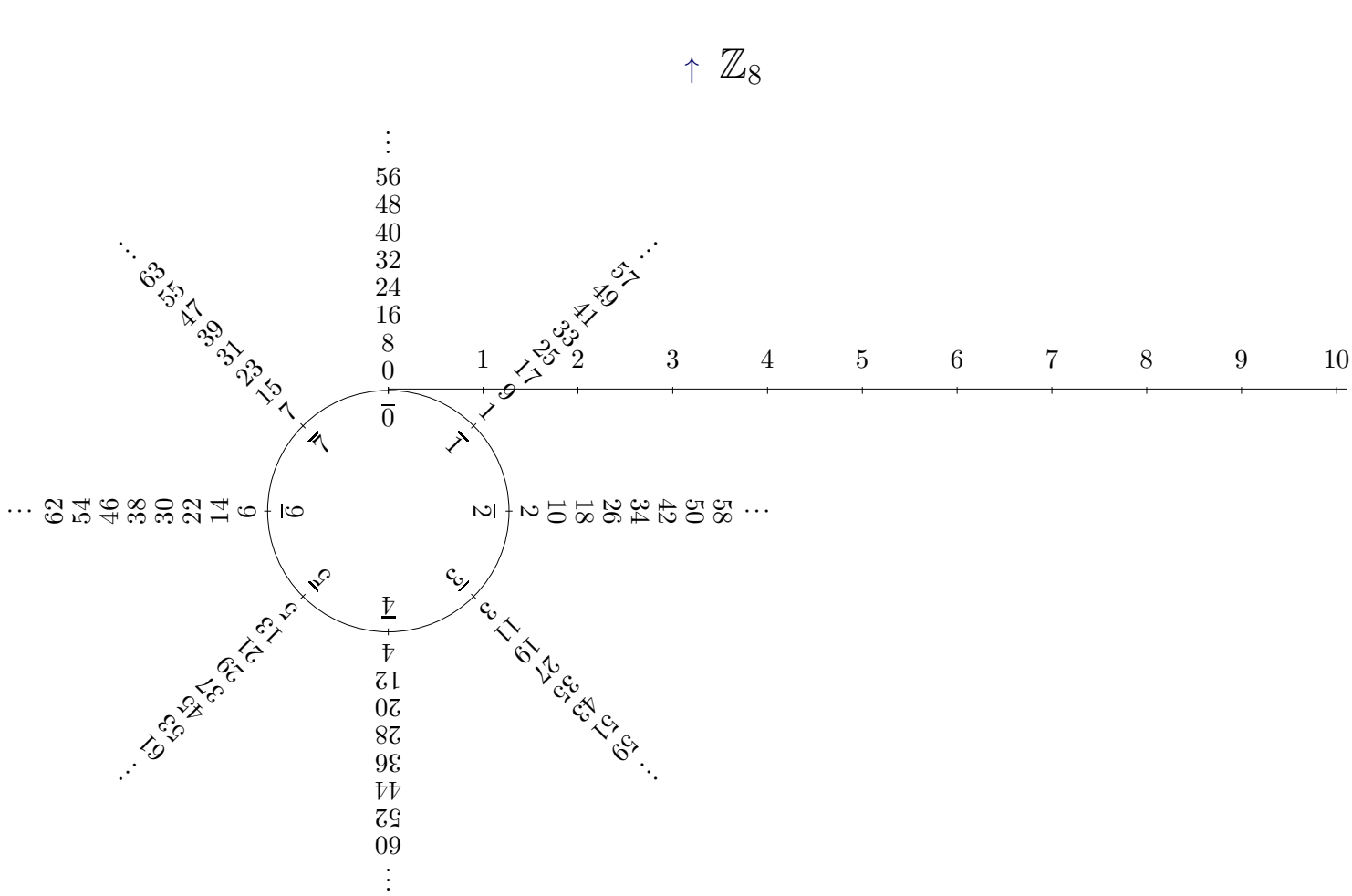
Damit eine Rechnung wie

$$7^{98} \equiv 2^{98} \equiv 4^{49} \equiv (-1)^{49} \equiv -1 \equiv 4 \pmod 5$$

möglich wird, müssen die Restklassen auf $\mathbb{Z}$ erweitert werden.

Für die Division mit 4 erhalten wir

$\overline{0} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\} = 4\mathbb{Z}$
$\overline{1} = \{\ldots, -11, -7, -3, 1, 5, 9, 13 \ldots\} = 1 + 4\mathbb{Z}$
$\overline{2} = \{\ldots, -10, -6, -2, 2, 6, 10, 14 \ldots\} = 2 + 4\mathbb{Z}$
$\overline{3} = \{\ldots, -9, -5, -1, 3, 7, 11, 15 \ldots\} = 3 + 4\mathbb{Z}$



Der Zahlenstrahl wird hier aufgerollt. Es entstehen die acht Restklassen derjenigen Zahlen, die sich nur um ein Vielfaches von $n = 8$ unterscheiden.

$(\mathbb{Z}_8, +)$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$(\mathbb{Z}_8, \circ)$

∘	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

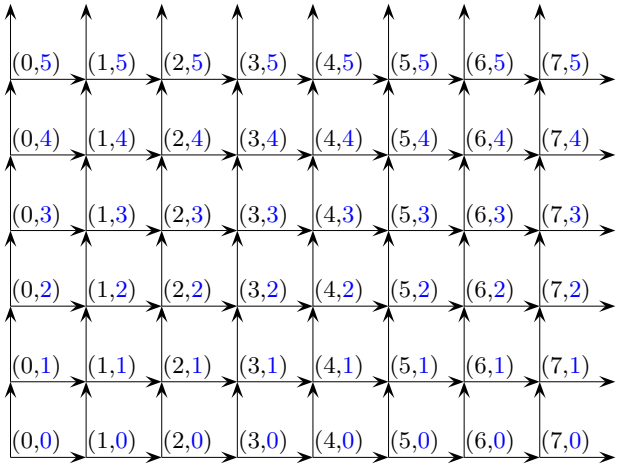
$(\mathbb{Z}_8^*, \circ)$

∘	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

statt z. B. $\overline{4}$ vereinfacht 4
In Excel wird lediglich eine Anweisung wie $= \mathrm{REST}(\$A5 + B\$4; 8)$ kopiert.

In $\mathbb{Z}$ gibt es keine Nullteiler, denn aus $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.
In $(\mathbb{Z}_8, \circ)$ finden wir $2 \circ 4 = 0$, $4 \circ 6 = 0$.
$\mathrm{ggT}(a, 8) = k > 1 \implies a \circ (8/k) = 0$. In a ist der Faktor k enthalten.
Werden aus $(\mathbb{Z}_8, \circ)$ alle Nullteiler und 0 entnommen, verbleibt die Gruppe $(\mathbb{Z}_8^*, \circ)$.
Die Abbildung $x \to a \circ x$, $(\mathbb{Z}_8, \circ) \to (\mathbb{Z}_8, \circ)$ ist injektiv.
$a \circ x = a \circ y \implies a \circ (x - y) = 0 \quad (x > y),\ (x - y) = 0,\ x = y$

$\uparrow\ \mathbb{Z}_8 \times \mathbb{Z}_6$

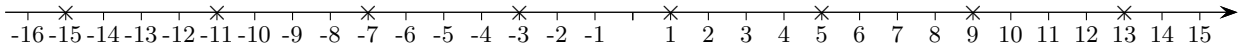


Zu zwei Gruppen kann eine Produktgruppe mit elementweiser Verknüpfung von Paaren gebildet werden, $\mathbb{Z}_8 \times \mathbb{Z}_6 = \{(a, b) \mid a \in \mathbb{Z}_8, b \in \mathbb{Z}_6\}$.

$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

$\mathbb{Z}_8 \times \mathbb{Z}_6$ weist anschaulich eine doppelt in sich zurückgebogene Struktur auf.
$(a, 5) + (0, 1) = (a, 0),\ (7, a) + (1, 0) = (0, a)$
Durch das Verkleben von oberer und unterer Kante entsteht ein Schlauch. Seine beiden Enden können zu einer Art Schwimmring (Torus) verbunden werden.

↑ Teilbarkeit in $\mathbb{Z}$



Die Rechnungen zur Restklasse $\overline{1}$

$$\begin{aligned}
13 &= 3 \cdot 4 &&+ 1\\
9 &= 2 \cdot 4 &&+ 1\\
5 &= 1 \cdot 4 &&+ 1\\
1 &= 0 \cdot 4 &&+ 1\\
-3 &= (-1) \cdot 4 &&+ 1\\
-7 &= (-2) \cdot 4 &&+ 1\\
-11 &= (-3) \cdot 4 &&+ 1\\
-15 &= (-4) \cdot 4 &&+ 1
\end{aligned}$$

verdeutlichen den Sachverhalt:

Für alle $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gibt es $q \in \mathbb{Z}$ (eindeutig) mit

$$a = q \cdot b + r, \quad 0 \leq r < b$$

Die Kongruenz-Rechenregeln bleiben erhalten.

$$17^{88} \equiv (-7)^{88} \equiv 49^{44} \equiv 1^{44} \equiv 1 \pmod{24}$$

Teilbarkeit durch 11
Eine Zahl ist durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.
61259
alternierende Quersumme: $6 - 1 + 2 - 5 + 9 = 11$
$(5569 \cdot 11 = 61259)$

$61259 = 6 \cdot 10000 + 1 \cdot 1000 + 2 \cdot 100 + 5 \cdot 10 + 9$

durch 11 teilbar: 11, 99, 1001, 9999, 100001, 999999, ...

$$\begin{aligned}
10 &\equiv -1 \pmod{11}\\
100 &\equiv 1\\
1000 &\equiv -1\\
10000 &\equiv 1\\
&\ldots
\end{aligned}$$

$61259 \equiv 6 \cdot 1 + 1 \cdot (-1) + 2 \cdot 1 + 5 \cdot (-1) + 9 \pmod{11}$

↑ Beispiel einer Kongruenzgleichung

Wir suchen eine Lösung x (ohne Probieren) für:

$$7x \equiv 1 \mod 19$$

$$\iff 19 \mid (7x-1)$$

$$\iff \exists\, q \quad 19q = 7x - 1$$

Es ist also die diophantische Gleichung

$$7x - 19q = 1$$

oder $(q = -y)$

$$7x + 19y = 1$$

zu lösen. Man beachte: $\mathrm{ggT}(7, 19) = 1$

Wir verwenden den erweiterten euklidischen Algorithmus.

a	b	q	r	x	y
7	19	0	7	-8	3
19	7	2	5	3	-8
7	5	1	2	-2	3
5	2	2	1	1	-2
2	1	2	0	0	1

Ergebnis:

$$7 \cdot (-8) + 19 \cdot 3 = 1$$

Die Lösung (Restklasse) der Gleichung lautet daher: $x = -8$ (oder in anderer Darstellung $x = 11$)

Probieren hätte möglicherweise ergeben:

$$\underbrace{7 \cdot 8}_{56,\ 3\cdot 19 = 57} \equiv -1 \mod 19$$

$$\iff 7 \cdot (-8) \equiv 1 \mod 19$$

Man reflektiere die Umformungen.

$$4x + 3 \equiv 1 \mod 7$$

$$\iff 4x \equiv -2$$

$$\iff 4x \equiv 5$$

$$\iff 8x \equiv 10$$

$$\iff x \equiv 3$$

↑ Simultane Kongruenzen, Beispiel für den chinesischen Restsatz

$$\begin{aligned} x &\equiv 2 \mod 8 \\ x &\equiv 4 \mod 5 \end{aligned}$$

Um das System zu lösen, liegt folgender Ansatz nahe:

$$x = 2 \cdot \underbrace{\big(5 \cdot u\big)}_{1} + 4 \cdot \underbrace{\big(8 \cdot v\big)}_{0} \mod 8$$

$$\underbrace{}_{0} \qquad \underbrace{}_{1} \mod 5$$

u und v sind so zu wählen, dass gilt:

$$\begin{aligned} 5u &\equiv 1 \mod 8 \\ 8v &\equiv 1 \mod 5 \end{aligned}$$

$u = 5$, $v = 2$ (leicht zu sehen)

$$x = 2 \cdot \big(5 \cdot 5\big) + 4 \cdot \big(8 \cdot 2\big) = 114$$

$$x \equiv 114 \mod 40 \qquad 40 = \mathrm{kgV}(8, 5)$$

↑ Simultane Kongruenzen, Beispiel für den chinesischen Restsatz

$$
\begin{aligned}
x &\equiv 2 \mod 3 \\
x &\equiv 3 \mod 5 \\
x &\equiv 4 \mod 7
\end{aligned}
$$

Um das System zu lösen, liegt folgender Ansatz nahe:

$$
\begin{aligned}
x = 2 \cdot \underbrace{\big(5 \cdot 7 \cdot u\big)}_{1} + 3 \cdot \underbrace{\big(3 \cdot 7 \cdot v\big)}_{0} + 4 \cdot \underbrace{\big(3 \cdot 5 \cdot w\big)}_{0} &\mod 3 \\
\underbrace{\qquad}_{0} \qquad \underbrace{\qquad}_{1} \qquad \underbrace{\qquad}_{0} &\mod 5 \\
\underbrace{\qquad}_{0} \qquad \underbrace{\qquad}_{0} \qquad \underbrace{\qquad}_{1} &\mod 7
\end{aligned}
$$

u, v und w sind so zu wählen, dass gilt:

$$
\begin{aligned}
35u &\equiv 1 \mod 3 \\
21v &\equiv 1 \mod 5 \\
15w &\equiv 1 \mod 7
\end{aligned}
$$

Mit dem erweiterten euklidischen Algorithmus erhalten wir:

$$
\begin{aligned}
1 &= \ 12 \cdot 3 - 1 \cdot 35 \\
1 &= -4 \cdot 5 + 1 \cdot 21 \\
1 &= -2 \cdot 7 + 1 \cdot 15
\end{aligned}
$$

$$
\Longrightarrow \quad u = -1,\ v = 1,\ w = 1
$$

$$
x = 2 \cdot \big(5 \cdot 7 \cdot u\big) + 3 \cdot \big(3 \cdot 7 \cdot v\big) + 4 \cdot \big(3 \cdot 5 \cdot w\big) = 53
$$

$$
x \equiv 53 \mod 105 \qquad\qquad 105 = \mathrm{kgV}(3, 5, 7)
$$

↑ Chinesischer Restsatz

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ x &\equiv a_3 \mod m_3 \end{aligned}$$

m_i paarweise teilerfremd

Ansatz:

$$x = a_1 \cdot \underbrace{\left(m_2 \cdot m_3 \cdot u\right)}_{1} + a_2 \cdot \underbrace{\left(m_1 \cdot m_3 \cdot v\right)}_{0} + a_3 \cdot \underbrace{\left(m_1 \cdot m_2 \cdot w\right)}_{0} + k \cdot m_1 m_2 m_3$$

$$\underbrace{}_{0} \quad \underbrace{}_{1} \quad \underbrace{}_{0} \mod m_2$$

$$\underbrace{}_{0} \quad \underbrace{}_{0} \quad \underbrace{}_{1} \mod m_3$$

u, v und w sind so zu wählen (erweiterter euklidischer Algorithmus), dass gilt:

$$\begin{aligned} m_2 m_3 u &\equiv 1 \mod m_1 \\ m_1 m_3 v &\equiv 1 \mod m_2 \\ m_1 m_2 w &\equiv 1 \mod m_3 \end{aligned}$$

↑ Simultane Kongruenzen

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ x &\equiv a_3 \mod m_3 \end{aligned}$$

Der chinesischer Restsatz kann nur angewandt werden, wenn die Moduln m_i paarweise teilerfremd sind.

1. $$\begin{aligned} x &\equiv 3 \mod 5 \\ x &\equiv 3 \mod 25 \end{aligned}$$

   Die 1. Gleichung ist redundant. $x = k \cdot 25 + 3$

2. $$\begin{aligned} x &\equiv 1 \mod 4 \\ x &\equiv 5 \mod 8 \end{aligned}$$

   Die 1. Gleichung ist äquivalent zu $x \equiv 5 \mod 4$ und redundant. $x = k \cdot 8 + 5$

3. $$\begin{aligned} x &\equiv a \mod p \\ x &\equiv b \mod p^2 \\ x &\equiv c \mod p^3 \end{aligned}$$

   Das System ist nur lösbar, wenn die ersten beiden Gleichungen redundant sind. $x = k \cdot p^3 + c$

4. $$\begin{aligned} x &\equiv a \mod m \qquad \text{ggT}(m,n) = 1 \\ x &\equiv a \mod n \end{aligned}$$

   Die beiden Gleichungen sind äquivalent zu $x \equiv a \mod mn$

5. $$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ x &\equiv a_3 \mod m_3 \end{aligned}$$

   Liegen keine paarweise teilerfremden Moduln vor, wird man die m_i in Primzahlpotenzen zerlegen und gemäß 4. ein äquivalentes System aufstellen. Gemäß 3. werden alle redundanten Gleichungen gestrichen. Wenn nur teilerfremde Moduln übrigbleiben, haben wir die Voraussetzung des chinesischen Restsatzes erreicht.

6. $x \equiv a \mod m \qquad \mathrm{ggT}(m,n) = 1 = u \cdot m + v \cdot n$
$x \equiv b \mod n$

$$x \equiv v \cdot n \cdot a + u \cdot m \cdot b \mod mn$$

Die Lösung kann unmittelbar angegeben werden, wenn die Linearkombination des ggTs vorliegt. Die Probe bestätigt die Korrektheit, z. B. (1. Zeile)

$v \cdot n \cdot a + u \cdot m \cdot b \equiv a \mod m$, weil aus der Linearkombination $v \cdot n \equiv 1 \mod m$ folgt.

7. $x \equiv 4 \mod 7 \qquad \mathrm{ggT}(7,30) = 1 = 13 \cdot 7 - 3 \cdot 30$
$x \equiv 19 \mod 30$

$$x \equiv \underbrace{-3 \cdot 30 \cdot 4 + 13 \cdot 7 \cdot 19}_{1369} \mod 210 \iff x \equiv 109 \mod 210$$

8. $3x \equiv 1 \mod 4 \mid \cdot 4 \iff x \equiv 3 \mod 4 \iff x \equiv 11 \mod 12$
$5x \equiv 1 \mod 6 \mid \cdot 6 \qquad x \equiv 5 \mod 6 \qquad x \equiv 4 \mod 7$
$3x \equiv 5 \mod 7 \mid \cdot 7 \qquad x \equiv 4 \mod 7$

$$\mathrm{ggT}(12,7) = 1 = 3 \cdot 12 - 7 \cdot 7 \implies x \equiv 11 \mod 84$$

9. $x \equiv a \mod m$ $\quad$ $\mathrm{ggT}(m,n) = d = u \cdot m + v \cdot n$
$x \equiv b \mod n$

Voraussetzung $a \equiv b \mod d$

$$x \equiv v \cdot \frac{n}{d} \cdot a + u \cdot \frac{m}{d} \cdot b \mod \mathrm{kgV}(m,n) \quad (= \frac{mn}{d})$$

Die Lösung kann unmittelbar angegeben werden, wenn die Voraussetzung erfüllt ist und die Linearkombination des ggTs vorliegt.

Beweis:

Die angegebene Lösung ist äquivalent (Umformung mit der Linearkombination des ggTs) zu

$$x \equiv a - u \cdot m \cdot \frac{a-b}{d}, \qquad \text{was wiederum äquivalent ist zu}$$

$$x \equiv b - v \cdot n \cdot \frac{b-a}{d}.$$

Aus diesen beiden Darstellungen ist die Korrektheit der Lösung offensichtlich.
Ein System aus Kongruenzen lässt sich durch wiederholtes Anwenden des Satzes lösen.

10. $x \equiv 3 \mod 25$ $\quad$ $\mathrm{ggT}(25,10) = 5 = 1 \cdot 25 - 2 \cdot 10, \quad 3 \equiv 8 \mod 5$
$x \equiv 8 \mod 10$

$$x \equiv \underbrace{-2 \cdot 2 \cdot 3 + 1 \cdot 5 \cdot 8}_{28} \mod 50$$

↑ Kleiner Satz von Fermat

Für alle Primzahlen p und alle natürlichen Zahlen a, die kein Vielfaches von p sind gilt:

$$a^{p-1} \equiv 1 \mod p$$

z. B. $4^6 \equiv 1 \pmod 7$

Wir betrachten die 6 Zahlen: 1, 2, 3, 4, 5, 6,
multiplizieren sie mit 4 (z. B.) und schreiben die Teilerreste mod 7 auf.
Dies ergibt: 4, 1, 5, 2, 6, 3

Allgemein:
Werden die Teilerreste mod p: 1, 2, 3, ... , $(p-1)$
mit a multipliziert, so ergeben sich mod p dieselben Teilerreste. Die Reihenfolge ist unerheblich.

Zur Begründung:

$$\begin{aligned}
& b \not\equiv c \\
\iff \quad & p \nmid (b-c) \\
\iff \quad & p \nmid a(b-c) \qquad p \text{ nicht in } a \text{ enthalten} \\
\iff \quad & p \nmid (ab-ac) \\
\iff \quad & ab \not\equiv ac
\end{aligned}$$

Damit erhalten wir:

$$\begin{aligned}
& 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv 1a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \\
\iff \quad & 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv a^{p-1}(1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)) \\
\iff \quad & (p-1)! \equiv a^{p-1}(p-1)! \\
\iff \quad & p \mid (p-1)!\,(a^{p-1}-1) \\
\iff \quad & p \mid (a^{p-1}-1) \qquad \text{Behauptung}
\end{aligned}$$

↑ Satz von Euler

Der kleine Satz von Fermat lässt sich verallgemeinern.
Statt p nehmen wir eine natürliche Zahl n.
Für eine Primzahl p sind die $(p-1)$ Zahlen 1, 2, 3, …, $(p-1)$ teilerfremd.
Für n treten an ihre Stelle die zu n teilerfremden Zahlen r_1, r_2, …, $r_{\varphi(n)}$ die kleiner als n sind (Teilerreste, $r_1 = 1$), für sie gilt also $\mathrm{ggT}(r_i, n) = 1$.
Die Anzahl sei $\varphi(n)$, z. B. $\varphi(8) = |\{1,3,5,7\}| = 4$

Der Satz von Euler besagt nun:

$$a^{\varphi(n)} \equiv 1 \mod n \qquad \text{unter der Bedingung } \mathrm{ggT}(a,n) = 1$$

Begründung:

$$\begin{aligned}
& b \not\equiv c \\
\iff \quad & n \nmid (b-c) \\
\iff \quad & n \nmid a(b-c) \qquad \mathrm{ggT}(a,n) = 1 \\
\iff \quad & n \nmid (ab-ac) \\
\iff \quad & ab \not\equiv ac
\end{aligned}$$

Damit erhalten wir:

$$\begin{aligned}
& r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{\varphi(n)} \equiv a r_1 \cdot a r_2 \cdot a r_3 \cdot \ldots \cdot a r_{\varphi(n)} \\
\iff \quad & \equiv a^{\varphi(n)}\, r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{\varphi(n)} \\
\iff \quad & n \mid (a^{\varphi(n)} - 1) \cdot r_1 \cdot r_2 \cdot r_3 \cdot \ldots \cdot r_{\varphi(n)} \\
\iff \quad & n \mid (a^{\varphi(n)} - 1) \qquad \text{Behauptung}
\end{aligned}$$

↑ Eulersche φ-Funktion

Beispiele:

$\varphi(5) = |\{1,2,3,4\}| = 4$ Diese Zahlen haben mit 5 den ggT 1.

$\varphi(7) = |\{1,2,3,4,5,6\}| = 4$

Für Primzahlen p gilt offensichtlich $\varphi(p) = p - 1$.

$\varphi(3^2) = |\{1,2,3,4,5,6,7,8,9\} \setminus \{3,6,9\}| = 6$

$\varphi(5^2) = |\{1,2,3,\ \ldots\ ,24,25\} \setminus \{5,10,15,20,25\}| = 20$

$\varphi(7^3) = |\{1,2,3,\ \ldots\ ,7^3\} \setminus \{1\cdot 7,\ 2\cdot 7,\ 3\cdot 7,\ \ldots\ ,7^2\cdot 7\}| = 7^3 - 7^2$

Wir erkennen, dass für Primzahlpotenzen gilt $\varphi(p^n) = p^n - p^{n-1} = p^n(1 - \frac{1}{p})$.

Die Funktion ist auch multiplikativ: $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ für teilerfremde Zahlen m, n.

Diese Eigenschaft ermöglicht uns, $\varphi(a)$ für beliebiges a zu ermittelt.

Anhand des Zahlenbeispiels $m = 9$, $n = 4$ wird die Beweisidee deutlich.
$\varphi(9) = 6$, $\varphi(4) = 2$, z.z. $\varphi(9 \cdot 4) = 12$.

In der obersten Zeile sind die zu 9 teilerfremden Zahlen grau unterlegt.

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36

Nur die Zahlen in den grau unterlegten Spalten ergeben 1 als ggT mit 9. Unter ihnen sind diejenigen Zahlen, die mit $9 \cdot 4$ den ggT 1 bilden. Es sind gerade die Zahlen, die auch zu 4 teilerfremd sind.

mod 4

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

Die Spalten haben alle die Stuktur:

$k + 0 \cdot 9$
$k + 1 \cdot 9$
$k + 2 \cdot 9$
$k + 3 \cdot 9$

In jeder Spalte sind alle Teilerreste mod 4 vorhanden,
$i \not\equiv j \implies k + i \cdot 9 \not\equiv k + j \cdot 9$, beachte $\text{ggT}(4,9) = 1$,
darunter jeweils $\varphi(4) = 2$ Teilerfremde zu 4.
Nun sollte $\varphi(9 \cdot 4) = 6 \cdot 2$ einleuchten.