Prof. Dr. M. Helbig
Mathematik – Übung

Hochschule Rosenheim
University of Applied Sciences

Kongruenzen und Restklassen

* **Modulo.** Berechnen Sie den Rest modulo 6 der Zahlen 25, -25, 2 und 12.

Lösung. Division mit Rest:

$25 = 4 \cdot 6 + \boxed{1}$ $\quad 25 \bmod 6 = 1$

$-25 = (-5) \cdot 6 + \boxed{5}$ $\quad -25 \bmod 6 = 5$

$2 = 0 \cdot 6 + \boxed{2}$ $\quad 2 \bmod 6 = 2$

$12 = 2 \cdot 6 + \boxed{0}$ $\quad 12 \bmod 6 = 0 \iff 6 \mid 12$

Div mit Rest am TR: ÷R
25 ÷R 6 = 4; R1

in C: 12%6==0

⚠ Div. m. Rest ist nicht:
$-25 = (-4) \cdot 6 - 1$, da $0 \leq r < 6$

Eigener Lösungsversuch.

* **Kongruenzen, Teil 1.** Welche der Aussagen ist wahr?

1. $65 \equiv 117 \pmod{13}$
2. $111 \equiv 1001 \pmod{11}$
3. $71 \equiv 157 \pmod{17}$
4. $12 \equiv 117 \pmod{21}$
5. $-35 \equiv 74 \pmod{17}$

$-(a-b) = b-a$

Lösung.

Wdh: $a \equiv b \pmod{m} \overset{\text{Def.}}{:\Longleftrightarrow} a \bmod m = b \bmod m \overset{\text{Satz}}{\Longleftrightarrow} m \mid a-b \Longleftrightarrow m \mid b-a$

1. $65 \bmod 13 = 0$, $117 \bmod 13 = 0$ ✓ ODER: $13 \mid 9 \cdot 13 = 52 = 117 - 65$ ✓
2. $111 \bmod 11 = 1$, $1001 \bmod 11 = 0$ ✗ ($AQ(111) = 1-1+1 = 1$, $AQ(1001) = 1-0+0-1 = 0$)
   (Bei mod 11 gilt: $a \equiv AQ(a) \pmod{11}$ (alternierende Quersumme), d.h. $a \bmod 11 = AQ(a) \bmod 11$)
3. $71 \equiv 3 \not\equiv 4 \equiv 157 \pmod{17}$ ✗
4. $12 \equiv 12 \equiv 117 \pmod{21}$ ✓
5. $-35 \equiv 16 \not\equiv 6 \equiv 74 \pmod{17}$ ✗

Eigener Lösungsversuch.

ISBN-10.

1. Zeigen Sie, dass 0-817-64176-9 eine gültige ISBN-10 ist.
2. Ein Fehler passiert an der zweiten Stelle, und es wird daher statt der Nummer in a) 0-117-64176-9 eingegeben. Wird der Fehler erkannt?

Lösung.

Prüfziffer

Wdh: $z_{10} \equiv 1 \cdot z_1 + 2 \cdot z_2 + \ldots + 9 \cdot z_9 \pmod{11}$

$\Leftrightarrow \underbrace{(-1)}_{10} \cdot z_1 + \underbrace{(-2)}_{9} z_2 + \ldots + \underbrace{(-9)}_{2} \cdot z_9 + 1 \cdot z_{10} \equiv 0 \pmod{11}$

$\Leftrightarrow 10 z_1 + 9 z_2 + \ldots + 2 \cdot z_9 + 1 \cdot z_{10} \equiv 0 \pmod{11}$

1. $\underbrace{1 \cdot 0}_{0} + \underbrace{2 \cdot 8}_{16 \equiv 5} + \underbrace{3 \cdot 1}_{3} + \underbrace{4 \cdot 7}_{\equiv 6} + \underbrace{5 \cdot 6}_{\equiv 8} + \underbrace{6 \cdot 4}_{\equiv 2} + \underbrace{7 \cdot 1}_{\equiv 7} + \underbrace{8 \cdot 7}_{\equiv 1} + \underbrace{9 \cdot 6}_{\equiv 10}$

$\equiv 14 \equiv 3$ $\quad \equiv 17 \equiv 6$ $\quad \equiv 0$

$\equiv 9 \equiv z_{10} \pmod{11}$ ✓

2. $\underbrace{1 \cdot 0}_{0} + \underbrace{2 \cdot 8}_{16 \equiv 5} + \underbrace{3 \cdot 1}_{3} + \underbrace{4 \cdot 7}_{\equiv 6} + \underbrace{5 \cdot 6}_{\equiv 8} + \underbrace{6 \cdot 4}_{\equiv 2} + \underbrace{7 \cdot 1}_{\equiv 7} + \underbrace{8 \cdot 7}_{\equiv 1} + \underbrace{9 \cdot 6}_{\equiv 10} \equiv 17 \equiv 6$

$\equiv 14 \equiv 3$ $\quad \equiv 17 \equiv 6$ $\quad \equiv 0$

$\not\equiv 9 \equiv z_{10} \pmod{11}$ Ja, es wird erkannt!

Eigener Lösungsversuch.

EAN. Die Europäische Artikelnummer ist eine 13 stellige Ziffernfolge *abcd efgh ikmn p*. ~~Die ersten beiden Ziffern geben das Herkunftsland an, die folgenden fünf stehen für den Hersteller und die nächsten fünf für das Produkt~~. Die Prüfziffer p erfüllt die Gleichung → Wikipedia

$$a + 3b + c + 3d + e + 3f + g + 3h + i + 3k + m + 3n + p \equiv 0 \pmod{10}.$$

1. Wie lautet die Prüfziffer der „Penne Rigate“: 8076 8020 8573-p?
2. Statt der richtigen Artikelnummer 8076 8020 8573-p wird die falsche Artikelnummer 8076 8028 0573-p angegeben, bei der zwei aufeinander folgende Ziffern vertauscht wurden. Wird der Fehler erkannt?

Lösung.

z.B. Wikipedia:

Prüfziffer

1. $1\cdot 8 + 3\cdot 0 + 1\cdot 7 + 3\cdot 6 + 1\cdot 8 + 3\cdot 0 + 1\cdot 2 + 3\cdot 0 + 1\cdot 8 + 3\cdot 5 + 1\cdot 7 + 3\cdot 3 + 1\cdot p$

$8 \quad 0 \quad 7 \quad \equiv 8 \quad 8 \quad 0 \quad 2 \quad 0 \quad 8 \quad \equiv 5 \quad 7 \quad 9$

$5 \quad \equiv 6 \quad 0 \quad \equiv 6$

$\equiv 1 \quad \equiv 1$

$\equiv 2 + p \overset{!}{\equiv} 0 \pmod{10} \iff p \equiv -2 \equiv 8 \pmod{10}$

2. $1\cdot 8 + 3\cdot 0 + 1\cdot 7 + 3\cdot 6 + 1\cdot 8 + 3\cdot 0 + 1\cdot 2 + 3\cdot \cancel{0}\,8 + 1\cdot \cancel{8}\,0 + 3\cdot 5 + 1\cdot 7 + 3\cdot 3 + 1\cdot 8$

$8 \quad 0 \quad 7 \quad \equiv 8 \quad 8 \quad 0 \quad 2 \quad \cancel{0}\,4 \quad \cancel{8}\,0 \quad \equiv 5 \quad 7 \quad 9$

$5 \quad \equiv 6 \quad \cancel{0}\,6 \quad \equiv 6$

$\equiv 1 \quad \equiv 1$

$\equiv \cancel{2}\,8 + 8 \equiv 16 \equiv 6 \not\equiv 0 \pmod{10}$. Es wird erkannt!

Eigener Lösungsversuch.

skript

Q(n)

Quersumme. Es sei S_n die Quersumme der natürlichen Zahl n (z.B. $n = 395$, $S_n = 3 + 9 + 5 = 17$). Zeigen Sie

$$\boxed{n \equiv S_n \pmod 3.}$$

D.h. n und S_n lassen beim Teilen durch 3 den gleichen Rest. *Hinweis:* $10 \equiv 1 \pmod 3$. Wie kann man also leicht feststellen, ob eine Zahl durch 3 teilbar ist?

Lösung. Bsp: $n = 395 = 5 \cdot \underbrace{10^0}_{\equiv 1} + 9 \cdot \underbrace{10^1}_{\equiv 1} + 3 \cdot \underbrace{10^2}_{\equiv 1} \equiv 5 + 9 + 3 = S_n \pmod 3$

Ziffern $0, \dots, 9$ — Summe der Ziffern = Quersumme

Beweis: $n = \sum_{i=0}^{k} a_i \underbrace{10^i}_{\equiv 1} \equiv \sum_{i=0}^{k} a_i \cdot \underbrace{1^i}_{1} = \sum_{i=0}^{k} a_i = S_n \pmod 3.$

Also gilt: $3 \mid n \iff n \equiv 0 \pmod 3 \iff S_n \equiv 0 \pmod 3 \iff 3 \mid S_n$

d.h. „3 teilt n" g.d.w. 3 teilt Quersumme n

~~**Eigener Lösungsversuch.**~~

Beu: Es gilt auch:

$$\boxed{n \equiv S_n \pmod 9}$$

$$n = \sum_{i=0}^{k} a_i \underbrace{10^i}_{\equiv 1} \equiv \sum_{i=0}^{k} a_i = S_n \pmod 9$$

Also auch

$$\boxed{9 \mid n \iff 9 \mid S_n}$$

alternierende Quersumme!

$$\boxed{n \equiv AQ(n) \pmod{11}}$$

$$n = \sum_{i=0}^{k} a_i \underbrace{10^i}_{\equiv (-1)^i} = \sum_{i=0}^{k} (-1)^i a_i = AQ(n)$$

$10 \equiv -1 \bmod 11 \Rightarrow 10^i \equiv (-1)^i \bmod 11$

Also auch $\boxed{11 \mid n \iff 11 \mid AQ(n)}$

Bsp: $n = 3.485.921$

$3 \mid n$? $S_n = 1+2+9+5+8+4+3 = 32$, $S_{32} = 2+3 = 5$, $3 \nmid 5 \Rightarrow \underline{3 \nmid n}$

$9 \mid n$? — n — $9 \nmid 5 \Rightarrow \underline{9 \nmid n}$

$11 \mid n$? $AQ(n) = 1-2+9-5+8-4+3 = 10$, $11 \nmid 10 \Rightarrow \underline{11 \nmid n}$

Lineare Kongruenzgleichungen. Lösen Sie die folgenden Gleichungen und geben Sie alle Lösungen $0 \leq x < m$ an (m der jeweilige Modul).

1. $5 + x \equiv 3 \pmod 7$
2. $5 + x \equiv 4 \pmod 7$
3. $3 \cdot x \equiv 4 \pmod 7$
4. $4 \cdot x \equiv 5 \pmod 6$
5. $4 \cdot x \equiv 6 \pmod{10}$

Lösung.

1. $5+x \equiv 3 \pmod 7 \overset{-5}{\Rightarrow} x \equiv \underbrace{3-5}_{-2 \equiv 5} \pmod 7 \Rightarrow x \equiv 5 \pmod 7$

$\Rightarrow x = 5 + k \cdot 7 \overset{0 \leq x < 7}{\Rightarrow} \underline{x = 5}.$

2. $5+x \equiv 4 \pmod 7 \overset{-5}{\Rightarrow} x \equiv \underbrace{4-5}_{-1 \equiv 6} \pmod 7 \Rightarrow x = 6 + k \cdot 7 \overset{0 \leq x < 7}{\Rightarrow} \underline{x = 6}.$

3. $3 \cdot x \equiv 4 \pmod 7 \overset{\cdot 3^{-1} \equiv 5}{\Rightarrow} \underbrace{5 \cdot 3}_{15 \equiv 1} \cdot x \equiv \underbrace{5 \cdot 4}_{20 \equiv 6} \pmod 7 \Rightarrow x = 6 + k \cdot 7 \overset{0 \leq x < 7}{\Rightarrow} \underline{x = 6}.$

(Raten: 1,2,3,4,5,6: $3 \cdot 5 \equiv 1$)

ODER: $3 \cdot x = 4 + k \cdot 7 \Leftrightarrow \underbrace{3x + 7\underbrace{(-k)}_{y} = 4}_{\text{diophant. Gl.}}$

(1.) EEA mit a = 3 und b = 7 :

a =	q *	b +	r	x	y	ggT =	a *	x +	b *	y
3 =	0 *	7 +	3	-2	1	1 =	3 *	-2 +	7 *	1
7 =	2 *	3 +	1	1	-2	1 =	7 *	1 +	3 *	-2
3 =	3 *	1 +	0	0	1	1 =	3 *	0 +	1 *	1

ggT = 1 | 4 ($\cdot 4$)

(2.) $x = 4 \cdot (-2) = -8$

(3.) Allg. Lösung: $x = -8 + z\frac{7}{1} \overset{0 \leq x < 7}{\Rightarrow} \underline{x = 6}$

4. $4x \equiv 5 \pmod 6$ (Inverses von 4 existiert nicht, da $ggT(4,6) = 2 \neq 1$)

$\Leftrightarrow 4x = 5 + k \cdot 6 \Leftrightarrow \underline{4}x + \underline{6}\underbrace{(-k)}_{y} = \underline{5}$ diophant. Gl. nicht lösbar, da $ggT(4,6) = 2 \nmid 5$.

d.h. keine Lösung!

~~Eigener Lösungsversuch.~~

5. $4x \equiv 6 \pmod{10} \iff 4x + 10y = 6$ lösbar da $ggT(4,10) = 2 \mid 6$ (·3)

1. EEA mit a = 4 und b = 10 :

a =	q *	b +	r |	x |	y |	ggT =	a *	x +	b *	y
4 =	0 *	10 +	4 |	-2 |	1 |	2 =	4 *	-2 +	10 *	1
10 =	2 *	4 +	2 |	1 |	-2 |	2 =	10 *	1 +	4 *	-2
4 =	2 *	2 +	0 |	0 |	1 |	2 =	4 *	0 +	2 *	1

2. $x = -2 \cdot 3 = -6$

3. Alg. Lsg: $x = -6 + z\underbrace{\frac{10}{2}}_{5} = -6 + z \cdot 5 \implies x = 4 \vee x = 9$ $\quad 0 \le x < 10$

(nicht eindeutig lösbar!)

Allgemein: $ax \equiv b \pmod{n}$ lösbar?

$\iff ax = b + k \cdot n \iff ax + n\underbrace{(-k)}_{y} = b$

1. Fall: $ggT(a,n) \nmid b$: keine Lösung

2. Fall: $ggT(a,n) \mid b$: es gibt eine Lösung $\rightarrow$ EEA: $x = x_0 + z\frac{n}{ggT(a,n)}$

Es gibt genau $ggT(a,n)$ verschiedene Lösungen $0 \le x < n$:

$$\iff \quad 0 \le x_0 + z\frac{n}{ggT(a,n)} < n$$

$$\overset{-x_0}{\iff} \quad -x_0 \le z\frac{n}{ggT(a,n)} < n - x_0$$

$$\overset{\cdot \frac{ggT}{n}}{\iff} \quad \underbrace{-x_0\frac{ggT}{n}}_{=:\alpha} \le z < \underbrace{\frac{ggT}{n}(n - x_0)}_{ggT - \underbrace{\frac{ggT}{n}x_0}_{=:\alpha}}$$

$$\iff \quad \alpha \le z < \alpha + ggT$$

da $z \in \mathbb{Z}$ gibt es dafür ggT verschiedene Mgl.!

Restklassen, Teil 1. Geben Sie die Restklassen in $\mathbb{Z}_7$ und $\mathbb{Z}_8$. Bestimmen Sie für $\mathbb{Z}_8$ & $\mathbb{Z}_7$ die Verknüpfungstabelle für die Addition und Multiplikation. Welche Elemente von $\mathbb{Z}_8$ besitzen multiplikativ Inverse? Welche Elemente von $\mathbb{Z}_7$ besitzen multiplikative Inverse?

Lösung.

$\mathbb{Z}_7$:

+	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

·	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

$\bar{1}^{-1} = \bar{1}$, $\bar{2}^{-1} = \bar{4}$, $\bar{3}^{-1} = \bar{5}$
$\bar{4}^{-1} = \bar{2}$, $\bar{5}^{-1} = \bar{3}$, $\bar{6}^{-1} = \bar{6}$.

} jede Restklasse $\bar{a} \neq \bar{0}$ ist invertierbar (7 prim!)

Wieviele? $\varphi(7) = 7 - 1 = 6$

$\mathbb{Z}_8$:

+	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

·	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

invertiert sind alle teilerfremd zu 8:

$\bar{1}^{-1} = \bar{1}$, $\bar{3}^{-1} = \bar{3}$, $\bar{5}^{-1} = \bar{5}$, $\bar{7}^{-1} = \bar{7}$

Wieviele? $\varphi(8) = \varphi(2^3) = \underbrace{2^3}_{8} - \underbrace{2^2}_{4} = 4$

Eigener Lösungsversuch.

Restklassen, Teil 2. Berechnen Sie möglichst geschickt ohne Taschenrechner:

1. $\overline{8}+\overline{9}$ in $\mathbb{Z}_{16}$
2. $\overline{7}-\overline{9}$ in $\mathbb{Z}_{16}$
3. $\overline{48}+\overline{57}$ in $\mathbb{Z}_{64}$
4. $\overline{48}-\overline{57}$ in $\mathbb{Z}_{64}$
5. $\overline{7}\cdot\overline{9}$ in $\mathbb{Z}_{16}$
6. $\overline{13}\cdot\overline{5}$ in $\mathbb{Z}_{16}$
7. $\overline{48}\cdot\overline{6}$ in $\mathbb{Z}_{64}$
8. $\overline{8}\cdot\overline{57}$ in $\mathbb{Z}_{64}$
9. $\overline{423}\cdot\overline{191}+\overline{212}\cdot\overline{348}+\overline{110}\cdot\overline{317}$ in $\mathbb{Z}_5$
10. $\overline{423}\cdot\overline{191}-\overline{212}\cdot\overline{348}+\overline{110}\cdot\overline{317}$ in $\mathbb{Z}_5$

Lösung.

1. $\overline{8}+\overline{9} \overset{\text{Def.}}{=} \overline{8+9} = \overline{17} = \overline{1}$
2. $7-9 = -2 = 14.$
3. $48+\underbrace{57}_{-7} = 41$ (Trick: $a \approx n \rightarrow a = a-n$)
4. $48-\underbrace{57}_{(-7)} = 48+7 = 55$
5. $7\cdot\underbrace{9}_{3\cdot3} \equiv \underbrace{21}_{5}\cdot 3 = 15$
6. $\underbrace{13}_{-3}\cdot 5 = -15 = 1$ (d.h. $13^{-1}=5$)
7. $48\cdot\underbrace{6}_{2\cdot3} = \underbrace{96}_{32}\cdot 3 = 96 = 32.$

   $\underbrace{48}_{-16}\cdot 6 = -96 = 32$
8. $8\cdot\underbrace{57}_{-7} = -56 = 8$
9. $\underbrace{\underbrace{423}_{3}\cdot\underbrace{191}_{1}}_{3} + \underbrace{\underbrace{212}_{2}\cdot\underbrace{348}_{3}}_{6} + \underbrace{\underbrace{110}_{0}\cdot\underbrace{317}_{2}}_{0} = 4$

   $\underbrace{\quad\quad}_{1}$
10. $\underbrace{\underbrace{423}_{3}\cdot\underbrace{191}_{1}}_{3} - \underbrace{\underbrace{212}_{2}\cdot\underbrace{348}_{3}}_{6} + \underbrace{\underbrace{110}_{0}\cdot\underbrace{317}_{2}}_{0} = 2$

   $\underbrace{\quad\quad}_{1}$

Eigener Lösungsversuch.

Restklassen, Teil 3. Berechnen Sie die multiplikativ Inversen, sofern möglich:

1. $\overline{5}$ in $\mathbb{Z}_{26}$
2. $\overline{11}$ in $\mathbb{Z}_{256}$
3. $\overline{178}$ in $\mathbb{Z}_{80189}$
4. $\overline{97}$ in $\mathbb{Z}_{80189}$
5. $\overline{234}$ in $\mathbb{Z}_{1024}$

Lösung. Invertierbarkeitskriterium: $\bar{a} \in \mathbb{Z}_n$ inv. $\iff ggT(a,n) = 1$ (teilerfremd)

1. $ggT(5, \underbrace{26}_{2\cdot 13}) = 1$ ✔ (inv.)

(auch Raten: $k=-1$)

$\overline{5} \cdot \overline{x} = \overline{1} \iff 5 \cdot x = 1 + k \cdot 26 \iff 5x + 26\underbrace{(-k)}_{y} = 1$

EEA mit a = 5 und b = 26 :

a =	q *	b +	r	x	y	ggT =	a *	x +	b *	y
5 =	0 *	26 +	5	-5	1	1 =	5 *	-5 +	26 *	1
26 =	5 *	5 +	1	1	-5	1 =	26 *	1 +	5 *	-5
5 =	5 *	1 +	0	0	1	1 =	5 *	0 +	1 *	1

$\Rightarrow x = -5 = 21$

Alternativ mit Satz von Euler:

$ggT(5,26) = 1 \overset{\text{Euler}}{\Rightarrow} 5^{\varphi(26)} \equiv 1 \mod 26$, $\varphi(26) = \varphi(2)\varphi(13) = 1 \cdot 12 = 12$

$5^{-1} \equiv \underbrace{1}_{5^{\varphi(26)}} \cdot 5^{-1} \equiv 5^{\varphi(26)-1} = 5^{12-1} = 5^{11} = 5 \cdot \underbrace{(5^2)}_{\equiv -1}^{5} \equiv -5 \equiv 21 \pmod{26}$

(11 = q; Schnelles Potenz.)

Merke: $\boxed{ggT(a,n) = 1 \overset{\text{Euler}}{\Rightarrow} a^{-1} \equiv a^{\varphi(n)-1} \pmod n}$ (siehe GDI-Folien)

2. $ggT(\underbrace{11, 256}_{2^8}) = 1$: $\overline{11} \cdot \overline{x} = \overline{1} \iff 11x + 256y = 1$

EEA mit a = 11 und b = 256 :

a =	q *	b +	r	x	y	ggT =	a *	x +	b *	y
11 =	0 *	256 +	11	-93	4	1 =	11 *	-93 +	256 *	4
256 =	23 *	11 +	3	4	-93	1 =	256 *	4 +	11 *	-93
11 =	3 *	3 +	2	-1	4	1 =	11 *	-1 +	3 *	4
3 =	1 *	2 +	1	1	-1	1 =	3 *	1 +	2 *	-1
2 =	2 *	1 +	0	0	1	1 =	2 *	0 +	1 *	1

$x = -93 = 163$.

$\varphi(256) - 1 = 2^8 - 2^7 - 1$

ODER mit Euler: $ggT(11,256) = 1 \Rightarrow 11^{-1} \equiv 11^{127} \equiv \ldots \equiv 163$.

3. $ggT(178, 80189) = ?$ $\quad 178 = 2 \cdot 89$ & $89 \mid 80189$ (= $89 \cdot 901$)

~~Eigener Lösungsversuch~~. $\Rightarrow ggT(178, 80189) \geq 89 \neq 1 \Rightarrow$ nicht inv.

ODER: ggT mit EA bestimmen!

4. $\overline{97} \cdot \overline{x} = \overline{1} \iff 97x + 80189y = 1$

EEA mit a = 97 und b = 80189 :

a =	q *	b +	r	x	y	ggT =	a *	x +	b *	y
97 =	0 *	80189 +	97	-34721	42	1 =	97 *	-34721 +	80189 *	42
80189 =	826 *	97 +	67	42	-34721	1 =	80189 *	42 +	97 *	-34721
97 =	1 *	67 +	30	-29	42	1 =	97 *	-29 +	67 *	42
67 =	2 *	30 +	7	13	-29	1 =	67 *	13 +	30 *	-29
30 =	4 *	7 +	2	-3	13	1 =	30 *	-3 +	7 *	13
7 =	3 *	2 +	1	1	-3	1 =	7 *	1 +	2 *	-3
2 =	2 *	1 +	0	0	1	1 =	2 *	0 +	1 *	1

$x = -34721 = 45468$

5. $ggT(234, 1024) \geq 2 \Rightarrow$ nicht invertierbar!

2... 2...

(Halb-)Gruppe. Es sei $G = \{e, x, y\}$ eine Menge mit drei Elementen und $\circ$ die Verknüpfung mit

$\circ$	e	x	y
e	e	x	y
x	x	e	y
y	y	x	e

Bildet $(G, \circ)$ eine kommutative (Halb-)Gruppe?

Lösung.

Prüfe zuerst Halbgruppe:

(Abg): In der Tabelle kommen nur e, x, y vor ✓

(Ass): $\forall a,b,c \in G: (a \circ b) \circ c = a \circ (b \circ c)$ ← 27 Mgl.

nicht erfüllt: ✗

$$(\underbrace{x \circ y}_{y}) \circ x = x \neq e = x \circ (\underbrace{y \circ x}_{x})$$

keine Halbgruppe (auch keine Gruppe)

eee
eex
eey
exe
exx
exy
eye
⋮

Eigener Lösungsversuch.