

# Zahlentheorie

Zahlentheorie (Mathematik der ganzen Zahlen)

$$\mathbb{Z} = \{ \dots -2, -1, 0, 1, 2, \dots \}$$

$$\mathbb{N} = \{ 1, 2, 3, \dots \}$$

## Diophantische Gleichungen

Gegeben:  $a, b, c \in \mathbb{N}$ , gesucht  $x, y$  mit

$$ax + by = c$$

Wir schreiben Lösungen als Zahlenpaar  $(x/y)$

Beispiele:  $x + 3y = 10 \quad (x/y) = (7/1), (4/2), (1/3)$

$$3x + 7y = 1 \quad (x/y) = (-2/1), (5/-2)$$

$$5x + 5y = 1 \quad \text{keine Lösung, linke Seite ist durch 5 teilbar, rechte nicht.}$$

## Teiler und Primzahlen

**Definition:** 1) Seien  $x \in \mathbb{Z}, k \in \mathbb{N}$ .  $k$  heißt Teiler von  $x$ , geschrieben  $k|x$ , falls es ein  $q \in \mathbb{Z}$  gibt, so dass:  $x = k \cdot q$

2) Seien  $a, b \in \mathbb{N}$ : Dann ist der größte gemeinsame Teiler von  $a, b$  definiert durch:

$$\text{ggT}(a, b) = \max \{ k \in \mathbb{N} : k|a \wedge k|b \}$$

Beispiel:  $\underset{k|x}{3|12}$ , denn  $12 = 3 \cdot 4$ ,  $\underset{k|q}{2|-8}$ , denn  $-8 = 2 \cdot -4$

$$a = 70, b = 98$$

$a$  hat die Teiler  $1, 2, 5, 7, 10, 14, 35, 70$

$b$  hat die Teiler  $1, 2, 7, 14, 49, 98$

Menge der gemeinsamen Teiler:  $\{1, 2, 7, 14\}$        $\text{ggT}(70, 98) = 14$

**Definition:** Eine natürliche Zahl  $p > 1$  heißt Primzahl oder prim, wenn sie genau zwei Teiler besitzt: die 1 und sich selbst:

Beispiele:  $2, 3, 5, 7, 11, 13, 17, \dots$

## Hauptsatz der elementaren Zahlentheorie.

Jede natürliche Zahl  $n > 1$  lässt sich, bis auf die Reihenfolge der Faktoren, eindeutig als Produkt von Primzahlen darstellen.

Beispiel:  $70 = 2 \cdot 5 \cdot 7$        $\text{ggT}(70, 98) = 2 \cdot 7 = 14$   
 $98 = 2 \cdot 7 \cdot 7$

$$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \quad \text{ggT}(360, 756) = 2 \cdot 2 \cdot 3 \cdot 3 = 36$$
 $756 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7$

**Folgerung:** Jeder gemeinsame Teiler von  $a$  und  $b$  ist auch Teiler von  $\text{ggT}(a, b)$

**Satz:** Seien  $a, b, k \in \mathbb{N}, x, y \in \mathbb{Z}$

Aus  $k|a$  und  $k|b$  folgt  $k|(ax + by)$

Beweis:  $k|a \Rightarrow a = q_1 \cdot k$        $k|b \Rightarrow b = q_2 \cdot k$        $\left. \begin{array}{l} ax + by = q_1 \cdot kx + q_2 \cdot ky = k(\underbrace{q_1 x + q_2 y}_{q' \in \mathbb{Z}}) \Rightarrow k|(ax + by) \end{array} \right\}$

**Satz:** Besitzt die Gleichung  $ax + by = c$  eine Lösung  $(x/y)$ , so folgt:  $\text{ggT}(a, b) | c$

Beweis:  $\left. \begin{array}{l} \text{ggT}(a, b) | a \\ \text{ggT}(a, b) | b \end{array} \right\} \Rightarrow \text{ggT}(a, b) | ax + by$   
 Letzte Sch

## Der Euklidische Algorithmus

### Letzte Sch

#### Der Euklidsche Algorithmus

**Satz** (Teilen mit Rest): Seien  $a, b \in \mathbb{N}$ . Dann gibt es eindeutig bestimmte Zahlen  $q, r \in \mathbb{N}_0 = \{0, 1, 2, \dots\}$  so dass gilt:  $a = q \cdot b + r$  mit  $0 \leq r \leq b-1$

Beispiele:  $13 : 4 = 3$  Rest 1 bedeutet  $13 = 3 \cdot 4 + 1$   
 $223 : 25 = 8$  Rest 23 "  $223 = 8 \cdot 25 + 23$

**Satz:** Sei  $a = q \cdot b + r$ . Dann gilt:  $\text{ggT}(a, b) = \text{ggT}(b, r)$

$$\left. \begin{array}{l} \text{ggT}(b, r) \mid b \\ \text{ggT}(b, r) \mid r \end{array} \right\} \xrightarrow{\text{Satz}} \left. \begin{array}{l} \text{ggT}(b, r) \mid q \cdot b + 1 \cdot r = a \\ \text{ggT}(b, r) \mid b \end{array} \right\} \xrightarrow{\text{Dagl.}} \left. \begin{array}{l} \text{ggT}(b, r) \leq \text{ggT}(a, b) \\ \text{ggT}(b, r) \mid b \end{array} \right\} \Rightarrow \text{ggT}(a, b) = \text{ggT}(b, r)$$

$$\left. \begin{array}{l} \text{ggT}(a, b) \mid a \\ \text{ggT}(a, b) \mid b \end{array} \right\} \xrightarrow{\text{Satz}} \left. \begin{array}{l} \text{ggT}(a, b) \mid a - q \cdot b = r \\ \text{ggT}(a, b) \mid b \end{array} \right\} \Rightarrow \text{ggT}(a, b) \leq \text{ggT}(b, r)$$

Der Euklidsche Algorithmus zur Bestimmung des ggT:

1.  $a = 126, b = 98$

$$\begin{array}{r} 126 \quad 98 \\ 98 \quad 28 \quad \text{Rest von } 126:98 \\ 28 \quad 14 \\ 14 \quad 0 \end{array}$$

$\text{ggT}(126, 98) = 14$

2.  $a = 28, b = 52$

$$\begin{array}{r} 28 \quad 52 \\ 52 \quad 28 \\ 28 \quad 24 \\ 24 \quad 4 \\ 4 \quad 0 \end{array}$$

$\text{ggT}(28, 52) = 4$

3.  $a = 1000, b = 999$

$$\begin{array}{r} 1000 \quad 999 \\ 999 \quad 1 \\ 1 \quad 0 \end{array}$$

$\text{ggT}(1000, 999) = 1$

#### Erweiterter Euklidschen Algorithmus

**Satz:** Zu beliebig gewählten natürlichen Zahlen  $a, b$  gibt es ganze Zahlen  $x, y$  so dass

$$ax + by = \text{ggT}(a, b)$$

Beispiel:  $a = 110, b = 32$

$$\begin{array}{ll} 110 = 3 \cdot 32 + 14 & 2 = -3 \cdot 32 + 7(110 - 3 \cdot 32) = 7 \cdot 110 - 24 \cdot 32 \\ 32 = 2 \cdot 14 + 4 & 2 = 14 - 3(32 - 2 \cdot 14) = -3 \cdot 32 + 7 \cdot 14 \\ 14 = 3 \cdot 4 + 2 & 2 = 14 - 3 \cdot 4 \\ 4 = 2 \cdot 2 + 0 & \end{array}$$

$\text{ggT}(110, 32) = 2$

$(x, y) = (7, -24)$

Tabellenschreibweise:

$a$	$b$	$q$	$r$	$x$	$y$
110	32	3	14	7	$-3 - (7 \cdot 3) = -24$
32	14	2	4	-3	$1 - (-3 \cdot 2) = 7$
14	4	3	2	1	$0 - 1 \cdot 3 = -3$
4	2	2	0	0	1
					immer
					Ende

Beispiel2:

$$\begin{array}{r} a \quad b \quad q \quad r \quad x \quad y \\ \hline 99 \quad 78 \quad 1 \quad 21 \quad -11 \quad 3+11 = 14 \\ 78 \quad 21 \quad 3 \quad 15 \quad 3 \quad -2-9 = -11 \end{array}$$

$$-11 \cdot 99 + 14 \cdot 78 = 3$$

$$\begin{array}{r}
 21 \quad 15 \quad 1 \quad 6 \quad -2 \quad 1 - (-2) = 3 \\
 15 \quad 6 \quad 2 \quad 3 \quad 1 \quad 0 - 2 = -2 \\
 6 \quad 3 \quad 2 \quad 0 \quad 0 \quad 1
 \end{array}$$

**Satz (Existenzsatz):** Seien  $a, b, c \in \mathbb{N}$  gegeben, so dass  $\text{ggT}(a, b) \mid c$ .

Dann hat  $ax + by = c$  mindestens eine Lösung  $(x, y)$  mit  $x, y \in \mathbb{Z}$ .

Beweis: ex.  $k \in \mathbb{N}$ :  $c = k \cdot \text{ggT}(a, b)$

$$\begin{aligned}
 \text{Letzter Satz} \Rightarrow & \text{ ex. } x, y : ax + by = \text{ggT}(a, b) \\
 \Rightarrow & akx + bky = \text{ggT}(a, b) \cdot k = c \\
 \Rightarrow & (kx, ky) \text{ ist Lösung.}
 \end{aligned}$$

$$3x + 2y = 1 \quad (x, y) = (1, -1) \text{ ist Lösung}$$

$$3(1) + 2(-1) = 1$$

$$3(1+2) + 2(-1-3) = 1$$

$$3(1+2k) + 2(-1-3k) = 1$$

Weitere Lösungen:

$$\begin{array}{r}
 \vdots \\
 5 \quad -7 \\
 3 \quad -4 \quad \uparrow -3 \\
 1 \quad -1 \\
 -1 \quad 2 \quad \downarrow +3 \\
 -3 \quad 5 \\
 \vdots
 \end{array}$$

**Satz:** Ist  $(x_0, y_0)$  eine Lösung von  $ax + by = c$ , dann sind alle Zahlenpaare  $(x, y) = (x_0 + kb, y_0 - ka)$  mit  $k \in \mathbb{Z}$

Lösungen. Gilt  $\text{ggT}(a, b) = 1$ , dann sind dadurch alle Lösungen gegeben.

Beweis:  $ax + by = a(x_0 + kb) + b(y_0 - ka) = ax_0 + akb + by_0 - bka = ax_0 + by_0 = c \quad \checkmark$

Sei  $(x, y)$  irgendeine Lösung von  $ax + by = c$  und  $\text{ggT}(a, b) = 1$ .

$$a(x - x_0) + b(y - y_0) = ax + by - (ax_0 + by_0) = c - c = 0$$

$\Rightarrow a(x - x_0) = -b(y - y_0) \Rightarrow a \text{ ist Teiler der rechten Seite, da } \text{ggT}(a, b) = 1 \text{ muss } a \text{ Teiler von } y - y_0 \text{ sein.}$

$\Rightarrow a \mid (y - y_0) \Rightarrow y - y_0 = k \cdot a \text{ mit geeignetem } k.$

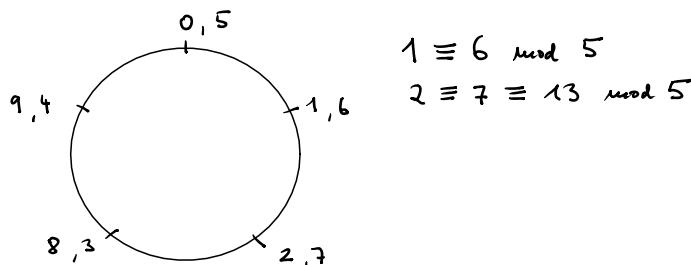
$$y = y_0 + ka$$

$$a(x - x_0) = -b(y_0 + ka - y_0) = -bka$$

$$\Rightarrow x - x_0 = -bk$$

$$x = x_0 - bk \quad \checkmark$$

## Kongruenz



**Definition:** Seien  $a, b \in \mathbb{Z}$ ,  $m \in \mathbb{N}$ . Dann heißt  $a$  kongruent zu  $b$  modulo  $m$ , geschrieben

$$a \equiv b \pmod{m}, \text{ falls } a - b \text{ durch } m \text{ teilbar ist.}$$

**Satz:** Folgende Aussagen sind äquivalent:

- (1)  $a \equiv b \pmod{m}$
- (2) Es gibt  $k \in \mathbb{Z}$ , so dass  $a = b + km$
- (3) Beim Teilen mit Rest  $a$  durch  $m$ ,  $b$  durch  $m$  bleibt derselbe Rest.

Beweis: (1)  $\Rightarrow$  (2):

$$a \equiv b \pmod{m} \Rightarrow m | (a-b) \Rightarrow \exists k \in \mathbb{Z}: (a-b) = km \Rightarrow \exists k \in \mathbb{Z}: a = b + km$$

(2)  $\Rightarrow$  (3):

Sei  $R$  der Rest beim Teilen von  $a$  durch  $m \Rightarrow \exists k' \in \mathbb{Z}: a = k'm + R$

$$(2) \Rightarrow b = a - km = k'm - km + R = (\underbrace{k'-k}_{\in \mathbb{Z}})m + R \Rightarrow \text{Teilen von } b \text{ durch } m \text{ ergibt Rest } R$$

(3)  $\Rightarrow$  (1):

$$\left. \begin{array}{l} a = km + R \\ b = k'm + R \end{array} \right\} a - b = \underbrace{(k - k')}_{\in \mathbb{Z}} m \Rightarrow m | (a-b) \Rightarrow a \equiv b \pmod{m}$$

Doppelte Verwendung von 'mod'

'mod' wird auch als Modulo Operator verwendet:  $r = a \bmod b$   $r$  ist der Rest bei der Division von  $a$  durch  $b$ .

$$\begin{array}{ll} 3 \equiv 7 \pmod{2} & \checkmark \quad \text{ist wahr} \\ 3 = 7 \pmod{2} & \times \quad \text{ist falsch} \end{array}$$

Zusammenhang der beiden Verwendungsweisen:  $a \bmod m = b \bmod m \Leftrightarrow a \equiv b \pmod{m}$

### Rechenregeln für Kongruenzen

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

(1)  $a \equiv a \pmod{m}$  Reflexivität

(2)  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$  Symmetrie

(3)  $a \equiv b \pmod{m}$  und  $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$  Transitivität

Satz: Wenn  $a \equiv b \pmod{m}$  und  $c \equiv d \pmod{m}$ , dann:

(4)  $-a \equiv -b \pmod{m}$

(5)  $a+c \equiv b+d \pmod{m}$

(6)  $ac \equiv bd \pmod{m}$

(7)  $a^2 \equiv b^2 \pmod{m}, a^3 \equiv b^3 \pmod{m}$

Beweis: (nur (6))

$$\begin{aligned} a \equiv b \pmod{m} &\Rightarrow \exists k \in \mathbb{Z}: a = b + km \quad \left. \begin{array}{l} a \cdot c = (b + km)(d + k'm) = bd + bkm + knd + kk'm^2 \\ = bd + \underbrace{(bkm + knd + kk'm^2)}_{\in \mathbb{Z}} \cdot m \Rightarrow ac \equiv bd \pmod{m} \end{array} \right\} \\ c \equiv d \pmod{m} &\Rightarrow \exists k' \in \mathbb{Z}: c = d + k'm \end{aligned}$$

Aus (5) und (6) folgt z.B.:

$$10 + x \equiv 4 + x \equiv -1 + x \pmod{5}$$

$$10^2 \equiv 9 \pmod{91} \Rightarrow 10^4 \equiv 81 \equiv -10 \pmod{91}$$

### Quersummenregeln

$$\begin{aligned} 2781 &\equiv 2 \cdot 1000 + 7 \cdot 100 + 8 \cdot 10 + 1 \pmod{9} \\ &= 2 \cdot 1 + 7 \cdot 1 + 8 \cdot 1 + 1 \pmod{9} \\ &= \text{Quersumme (2781)} \pmod{9} \end{aligned}$$

$$\begin{aligned} 10 &\equiv 1 \pmod{9} \\ 10 \cdot 10 &\equiv 1 \cdot 1 \pmod{9} \dots \end{aligned}$$

Ist die Quersumme einer Zahl durch 9 teilbar, dann auch die Zahl.

$$\begin{aligned} 46354 &\equiv 4 \cdot 10000 + 6 \cdot 1000 + 3 \cdot 100 + 5 \cdot 10 + 4 \cdot 1 \pmod{11} \\ &\equiv 4 - 6 + 3 - 5 + 4 \pmod{11} \\ &= \text{alternierende Quersumme (46354)} \end{aligned}$$

$$\begin{aligned} 1 &\equiv 1 \pmod{11} \\ 10 &\equiv -1 \pmod{11} \\ 100 &\equiv (-1)^2 \equiv 1 \pmod{11} \\ 1000 &\equiv 1 \pmod{11} \dots \end{aligned}$$

Ist die alternierende Quersumme einer Zahl durch 11 teilbar, dann auch die Zahl.

### Restklassen

Betrachte alle Zahlen, die beim Teilen durch eine Zahl  $m \in \mathbb{N}$  den selben Rest lassen. Diese Zahlen werden zu einer Menge zusammengefaßt, der Restklasse.

Definition: Die Restklasse  $\bar{a}$  von  $a$  modulo  $m$ :

$$-\quad r_1 \quad r_2 \quad \dots \quad r_m \quad \dots \quad \Gamma_{m-1}$$

Menge zusammengefaßt, der Restklasse.

**Definition:** Die Restklasse  $\bar{a}$  von  $a$  modulo  $m$ :

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

Beispiel: Die Restklassen modulo 5:

$$\begin{aligned}\bar{0} &= \{\dots, -10, -5, 0, 5, 10, \dots\} = \overline{5} = \overline{10} \dots \\ \bar{1} &= \{\dots, -9, -4, 1, 6, 11, \dots\} = \overline{6} = \overline{11} \dots \\ \bar{2} &= \{\dots, -8, -3, 2, 7, 12, \dots\} = \overline{7} = \overline{12} \dots \\ \bar{3} &= \{\dots, -7, -2, 3, 8, 13, \dots\} = \overline{8} = \overline{13} \dots \\ \bar{4} &= \{\dots, -6, -1, 4, 9, 14, \dots\} = \overline{9} = \overline{14} \dots\end{aligned}$$

**Definition:** Die Menge aller Restklassen heißt Restklassenring modulo  $m$ , geschrieben:  $\mathbb{Z}_m$

$$\text{Beispiel: } \mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

### Rechnen im Restklassenring

**Definition:** Seien  $a, b \in \mathbb{Z}$

$$\begin{aligned}\bar{a} + \bar{b} &:= \overline{a+b} \\ \bar{a} \cdot \bar{b} &:= \overline{a \cdot b}\end{aligned}$$

$$\text{Beispiel: in } \mathbb{Z}_5: \quad \begin{array}{rcl} \overline{2} + \overline{2} &=& \overline{4} \\ \overline{7} + \overline{12} &=& \overline{19} \end{array} \quad \text{Es ist egal, welche Darstellung von } \bar{a} \text{ und } \bar{b} \text{ für die Berechnung verwendet wird.}$$

Die Verknüpfungstabelle für die Addition und Multiplikation in  $\mathbb{Z}_5$  (ohne Oberstrich)

+ 0 1 2 3 4	*	0 1 2 3 4
0 0 1 2 3 4	0	0 0 0 0 0
1 1 2 3 4 0	1	0 1 2 3 4
2 2 3 4 0 1	2	0 2 4 1 3
3 3 4 0 1 2	3	0 3 1 4 2
4 4 0 1 2 3	4	0 4 3 2 1

$$\text{Subtraktion: } \bar{1} - \bar{2} = \bar{1} + (-\bar{2}) = \bar{1} + \bar{3} = \bar{4}$$

(Hilfsregel für negative Zahlen: wieviel fehlt vom Absolutbetrag zum nächsten Vielfachen)

$$\text{Division: } \frac{\bar{1}}{\bar{2}} = \bar{x} \Leftrightarrow \bar{1} = \bar{2} \cdot \bar{x} \Rightarrow \bar{x} = \bar{3}$$

Tabelle

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

Die Verknüpfungstabelle für die Multiplikation in  $\mathbb{Z}_4$

0 1 2 3	$\frac{1}{2} = \bar{x}$	$\bar{1} = \bar{2} \cdot \bar{x}$	es gibt kein $x$
0 0 0 0 0			
1 0 1 2 3			
2 0 2 0 2	$\frac{1}{2} = \bar{x} \Leftrightarrow \bar{2} = \bar{2} \cdot \bar{x} \quad \bar{x} = \bar{1} \text{ oder } \bar{x} = \bar{3}$	$\bar{2} = \bar{2} \cdot \bar{x} \quad \bar{x} = \bar{1} \text{ oder } \bar{x} = \bar{3}$	$\Rightarrow \bar{x}$ ist nicht eindeutig
3 0 3 2 1			

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

$$\begin{aligned}\frac{\bar{a}}{\bar{b}} = \bar{x} &\Leftrightarrow \bar{a} = \bar{x} \cdot \bar{b} = \overline{bx} \\ &\Leftrightarrow bx \equiv a \pmod{m} \\ &\Leftrightarrow bx - a = km \quad \text{für ein } k \in \mathbb{Z} \\ &\Leftrightarrow bx + (-k)m = a \quad (\text{diophantische Gleichung}) \\ &\quad \begin{matrix} \text{gesucht} & \text{unbekannt} \end{matrix}\end{aligned}$$

Falls  $\text{ggT}(b, m) \mid a$ : die Gleichung hat Lösung

Falls  $m$  Primzahl: die Gleichung hat für jedes  $a$  Lösung  $x_0$   
und alle anderen Lösungen sind gegeben durch  $x_0 + lm$  ( $l \in \mathbb{Z}$ )  
Dies sind die Elemente von  $\bar{x}_0$

**Satz vom Dividieren:** Ist  $p$  eine Primzahl und sind  $a, b \in \mathbb{Z}$ ,  $b \neq 0$   
 $a \in \mathbb{Z}$ ,  $b \in \{1, \dots, p-1\}$

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

### Der kleine Satz von Fermat

Anmerkung: Großer Satz von Fermat = Fermatsche Vermutung: Die Gleichung  $x^n + y^n = z^n$  besitzt für  $n \in \mathbb{N}, n \geq 3$  keine Lösung mit  $x, y, z \in \mathbb{N}$  (erst 1994 bewiesen).

Potenzen in  $\mathbb{Z}_5$ :

0 1 2 3 4	0	1	2	3	4
0 0 0 0 0	0	0	0	0	0
1 0 1 2 3 4	1	0	1	2	3
2 0 2 4 1 3	2	0	2	4	1
3 0 3 1 4 2	3	0	3	1	4
4 0 4 3 2 1	4	0	4	3	2

k	1	2	3	4
$\bar{2}^k$	$\bar{2}$	$\bar{4}$	$\bar{3}$	$\bar{1}$
$\bar{3}^k$	$\bar{3}$	$\bar{1}$	$\bar{3}$	$\bar{1}$
$\bar{4}^k$	$\bar{4}$	$\bar{1}$	$\bar{4}$	$\bar{1}$

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

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

Beispiel:  $2^{40} \equiv ? \pmod{19}$   $2^{40} = 2^{19-1} \cdot 2^{19-1} \cdot 2^4 \equiv 1 \cdot 1 \cdot 16 \equiv 16 \pmod{19}$

Beweis:  $A = \{\bar{0a}, \bar{1a}, \bar{2a}, \dots, (\bar{p-1}a)\} \subseteq \mathbb{Z}_p$ .

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

Annahme  $\bar{j}a = \bar{k}a$  für  $k > j \Rightarrow \bar{0} = \bar{j}a - \bar{k}a = \bar{j}a - \bar{k}a = \bar{(j-k)a}$  mit  $j-k \neq 0$

$\Rightarrow \frac{\bar{0}}{\bar{(j-k)}} = \bar{a} \Rightarrow \bar{0} = \bar{a} \Rightarrow a \text{ Vielfaches von } p \quad \square$

Also  $A = \mathbb{Z}_p$ . Wir entfernen  $\bar{0a}$  aus  $A$  und  $\bar{0}$  aus  $\mathbb{Z}_p$ . Das Produkt der restlichen Elemente muss gleich sein.

$$\bar{a} \cdot \bar{1a} \cdot \bar{2a} \cdot \dots \cdot \bar{(p-1)a} = \bar{1} \cdot \bar{2} \cdot \bar{3} \cdot \dots \cdot \bar{(p-1)}$$

$$\Rightarrow \bar{a}^{p-1} = 1$$

### Primivwurzel

**Definition:** Ein Element  $\bar{g} \in \mathbb{Z}_m$  heißt Primivwurzel, falls durch  $\bar{g}^k$  alle Elemente von  $\mathbb{Z}_m$  außer 0 dargestellt werden können.

Spalte hoch Zeile	in $\mathbb{Z}_7$					
1 2 3 4 5 6	1	2	3	4	5	6
1 1 2 3 4 5 6	1	2	3	4	5	6
2 1 4 2 2 4 1	2	1	4	9	5	3
3 1 ① 6 ① 6 6	3	1	8	5	9	4
4 1 2 4 4 2 1	4	1	5	4	3	9
5 1 4 5 2 3 6	5	1	10	① ① ①	10	10 ① 10
6 1 1 1 1 1 1	6	1	9	3	4	5

Spalte hoch Zeile	in $\mathbb{Z}_{10}$									
1 2 3 4 5 6 7 8 9 10	1	2	3	4	5	6	7	8	9	10
1 1 2 3 4 5 6	1	1	2	3	4	5	6	7	8	9
2 1 4 2 2 4 1	2	1	4	9	5	3	3	5	9	4
3 1 ① 6 ① 6 6	3	1	8	5	9	4	7	2	6	3
4 1 2 4 4 2 1	4	1	5	4	3	9	9	3	4	5
5 1 4 5 2 3 6	5	1	10	① ① ①	10	10	10 ①	10	10	10
6 1 1 1 1 1 1	6	1	9	3	4	5	5	4	3	9
7 1 7 9 5 3 8 6 2 4	7	1	7	9	5	3	8	6	2	4
8 1 3 5 9 4 4 9 5 3	8	1	3	5	9	4	4	9	5	3
9 1 6 4 3 9 2 8 7 5	9	1	6	4	3	9	2	8	7	5
10 1 1 1 1 1 1 1 1 1	10	1	1	1	1	1	1	1	1	1

### Primivwurzel

Tritt zwischendrin die Restklasse 1 auf, so wiederholen sich die Einträge, es kann also keine Primivwurzel vorliegen.