$$n \in \mathbb{N},\ a \in \mathbb{Z}$$

$$n|a \Leftrightarrow \exists q \in \mathbb{Z} : n \cdot q = a$$

n Teiler von a

Division mit Rest

$n \in \mathbb{N},\ a \in \mathbb{Z}$

r ist die kleinste nichtnegative Zahl, so dass es ein $q \in \mathbb{Z}$ mit $r = a - nq$ gibt

$0 \leq r \leq n - 1$

r=Rest der Division von a modulo n

Schreibweise: $\boxed{r = a \ mod \ n}$

$r, s \in \mathbb{Z} \quad r \equiv s \ mod \ n :\Leftrightarrow r \ mod \ n \equiv s \ mod \ n$

(r ist kongruent zu s modulo n)$\Leftrightarrow n|r - s$

$\equiv_n$ ist eine Äquivalenzrelation auf $\mathbb{Z}$

$$\mathbb{Z} = [0] \dot{\cup} [1] \dot{\cup} [2] \dot{\cup} ... \dot{\cup} [n-1]$$

$\rightarrow$ Äquivalenzklassen *mod* n "Restklassen"

0,1,2,...,n-1 sind Repräsentanten der n Äquivalenzklassen *mod* n.

$$\mathbb{Z}_n := \{0, 1, 2, ..., n-1\}$$

$A \cup B =$ Vereinigung von A und B

$A \dot{\cup} B$ für disjukte Vereinigung von A und B ($A \cup B, A \cap B = \emptyset$)

$A_1, ..., A_n, \quad A_i \cap A_j = \emptyset$ für alle $i \neq j$,

so schreiben wir für $A_1 \dot{\cap} ... \dot{\cap} A_n$ auch kurz: $\dot{\bigcup_{i=1}^{n}} A_i$

$a, b \in \mathbb{Z}_n$

$a + b := (a + b) \ mod \ n$

$a \cdot b := (a \cdot b) \ mod \ n$

$\rightarrow$ Operationen auf $\mathbb{Z}_n$ bzw. in $\mathbb{Z}$

$\mathbb{Z}_2$:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\rightarrow (2+2)\ mod\ 3 = 1$

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\rightarrow (2 \cdot 2)\ mod\ 3 = 1$

$\mathbb{Z}_4$:

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

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

$\mathbb{Z}_5$:

+	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

·	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

$4 \cdot 4 \equiv 16\ mod\ 5 = 1 \quad 2 \cdot 3 \equiv 6\ mod\ 5 = 1$

Im Allgemeinen: $\mathbb{Z}_n = \{0, 1, ..., n-1\} \quad n \in \mathbb{Z}$

$+ : \underbrace{\mathbb{Z}_n \times \mathbb{Z}_n}_{\mathbb{Z}_n^2} \rightarrow \mathbb{Z}_n$

$\cdot : \mathbb{Z}_n^2 \rightarrow \mathbb{Z}_n$

$-, /$

Differenz/Subtraktion:

$a, b \in \mathbb{Z}_n$

$a - b := a + y\ mod\ n$, wobei $y + b \equiv 0\ mod\ n \quad y \in \mathbb{Z}_n$

y heißt das zu b inverse Element bezüglich der Addition

Schreibweise: "$-b$" $\boxed{y = n - b\ mod\ n}$

Zum Vergleich in $\mathbb{Z}$:

$10 + -10 = 0$

$n - 10 := n + (-10)$

Ist $b = 0$, so ist $-b = 0$

Ist $b \in \{1, ..., n-1\}$, so ist $\underbrace{-b}_{\text{in } \mathbb{Z}_n} := \underbrace{n - b}_{\text{Differenz in } \mathbb{Z}}$

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

$a/b := a \cdot b^{-1}$, wobei b^{-1} die Lösung $y \in \mathbb{Z}_n$ ist, wobei gilt $y \cdot b = 1$ (in $\mathbb{Z}_n$)

b^{-1} heißt das zu b inverse Element bezüglich der Multiplikation

---

zum Vergleich $\mathbb{Q}$:

$\frac{3}{4} \in \mathbb{Q}$

$\left(\frac{3}{4}\right)^{-1} = \frac{4}{3}$

Durch welche Elemente $a \in \mathbb{Z}_n$ kann man dividieren? Oder äquivalent: Wann existiert a^{-1} für $a \in \mathbb{Z}_n$?

Def.:

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen teilerfremd (oder: relativ prim), falls sie keinen gemeinsamen Teiler außer 1 besitzen.

D.h.

a, b teilerfremd $:\Leftrightarrow$

$\forall x \in \mathbb{N} : (x|a) \wedge (x|b) \rightarrow x = 1$

Satz:

Sei $n \in \mathbb{N},\ n \geq 2$.

$a \in \mathbb{Z}_n$ besitzt a^{-1}(das multiplikative Inverse Element)$\Leftrightarrow$ a und n sind teilerfremd.

Beweis: etwas später

Bem.

$\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n : a \neq 0, a \text{ und } n \text{ sind teilerfremd}\}$

Definition (ggT)

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

Der größte gemeinsame Teiler (ggT)von a und b ist definiert als

$$max \underbrace{\{d \in \mathbb{N} : d|a \text{ und } d|b\}}_{\text{Menge aller gemeinsamen Teiler von } a \text{ und } b}$$

(wobei $max\ A :=$ das größte Element aus A)

Bem.:

a und b sind teilerfremd $:\Leftrightarrow ggT(a, b) = 1$

Def.:

Eine ganzzahlige Linearkombination von zwei Zahlen $a, b \in \mathbb{Z}$ ist eine Zahl der Form $\boxed{ax + by}$, wobei $x, y \in \mathbb{Z}$.

Diese Linearkombination $ax + by$ heißt positiv, falls $ax + by \geq 1$ gilt.

Satz

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

Dann gilt:

$ggT(a, b)$ ist die kleinste positive Linearkombination von a und b.

Beweis:

Sei $d := ggT(a, b)$

Sei $t :=$ die kleinste positive ganzzahlige Linearkombination von a und b

$$= min\left(\{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}\right)$$

Da $d = ggT(a, b)$, folgt: $d|a, d|b$.

Daher folgt: $d|t$ (insbesondere: $d \leq t$)

(da d jede ganzzahlige Linearkombination von a und b teilt)

Es bleibt zu zeigen: $t \leq d$

Sei $r := a \ mod \ t$

d.h. es gibt ein $q \in \mathbb{Z} : r = a - qt,\ 0 \leq r < t$

Wir wissen es gibt $x, y \in \mathbb{Z} : t = ax + by$

$r = a - q(ax + by) = \boxed{a(1 - qx) + by(-q)} \geq 0$

Wir sehen: r ist auch eine ganzzahlige Linearkombination von a und b. Weil t aber die kleinste ganzzahlige positive Linearkombination von a und b ist, muss gelten: $\boxed{r = 0} \Rightarrow t|a$

Analog können wir zeigen: $t|b$

Also ist $t \leq ggT(a, b) = d$.

Also muss gelten: $t = d$ $\square$

Lemma

Für alle $a, b \in \mathbb{Z},\ b \neq 0$, und alle $n \in \mathbb{N}$ gilt:

$$ggT(a_n, b_n) = n \cdot ggT(a, b)$$

Beweis: nach dem Satz davor:

$$ggT(a_n, b_n) = min\{a_n x + b_n y : x, y \in \mathbb{Z}, a_n x + b_n y \geq 1\}$$

$$= n \cdot min\{ax + by : q, y \in \mathbb{Z}, ax - by \geq 1\}$$

$$= n \cdot ggT(a, b) \quad \square$$

Lemma

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

Sei $n \in \mathbb{N}$. Gelten $n|ab$ und $ggT(n, a) = 1$, so folgt: $n|b$.

"Wenn n und a teilerfremd und n ab teilt, so muss n auch b teilen."

Beweis:

Weil $ggT(n, a) = 1$, gilt es $x, y \in \mathbb{Z} : 1 = nx + ay$

Multiplikation beider Seiten mit b:

$$b = bnx + bay$$

Da n sowohl bnx, als auch bay teilt, muss n auch b teilen. $\square$

Notation:

$n \in \mathbb{N},\ a \in \mathbb{Z}_n$

Wir schreiben $a \cdot \mathbb{Z}_n : a \cdot \mathbb{Z}_n := \{ax\ mod\ n : x \in \mathbb{Z}_n\}$

D.h. $a\mathbb{Z}_n$ ist die Menge verschiedener Repräsentanten von Zahlen $xa\ mod\ n$ $(0 \leq x \leq n-1)$

Satz:

Sei $n \in \mathbb{N}$, sei $a \in \mathbb{Z}_n$.

Ist $ggT(a, n) = 1$, so gilt $a\mathbb{Z}_n = \mathbb{Z}_n$

Insbesondere hat die Gleichung $ax \equiv b\ mod\ n$ genau eine Lösung in $\mathbb{Z}_n$.

Beweis:

Seien $x, y \in \mathbb{Z}_n,\ x \neq y$ mit $ax \equiv ay\ mod\ n$. (oder: $ax = ay$ (in $\mathbb{Z}_n$))

Also muss n $\underbrace{ax - ay}_{a(x-y)}$ teilen.

Weil $ggT(n, a) = 1$, folgt nach dem Lemma davor: $n|(x - y)$

Das ist aber unmöglich, denn aus $0 \leq x, y \leq n-1$ und $n|(x-y)$ folgt: $x = y$.

Deswegen gilt: alle $ax\ mod\ n$ (für $x \in \mathbb{Z}_n$) sind verschieden.

Also folgt: $a\mathbb{Z}_n = \mathbb{Z}_n$

"Insbesondere..." Wir müssen zeigen:

Für $a, b \in \mathbb{Z}_n$ gibt es ein eindeutiges (einziges) $x \in \mathbb{Z}_n$ mit $ax = b$ (in $\mathbb{Z}_n$)

Weil $a\mathbb{Z}_n = \mathbb{Z}_n$ gilt, gibt es ein $x \in \mathbb{Z}_n$ mit $ax = b$ (in $\mathbb{Z}_n$)

Es kann kein weiteres $y \in \mathbb{Z}_n$ mit $ay = b$ (in $\mathbb{Z}_n$) geben wegen des obiges Arguments. $\square$

Bemerkung:

$n \in \mathbb{N},\ a \in \mathbb{Z}_n,\ ggT(a, n) = 1$

gilt:

$$\varphi : \begin{cases} \mathbb{Z}_n \to \mathbb{Z}_n = a\mathbb{Z}_n \\ x \mapsto ax \end{cases} \text{ ist eine Bijektion.}$$

Def:

Sei S eine Menge, eine Bijektion $\varphi : S \to S$ heißt Permutation .

Also ist die Abbildung

$$\begin{cases} \mathbb{Z}_n \to \mathbb{Z}_n \\ x \mapsto ax \end{cases}$$

eine Permutation (falls die Voraussetzungen des Satzes erfüllt sind)

Satz:

$n \in \mathbb{N},\ n \geq 2 \quad a \in \mathbb{Z}_n$.

a besitzt $a^{-1} \Leftrightarrow ggT(a, n) = 1$

Bis jetzt:

Ist $ggT(a, n) = 1$, so hat die Gleichung $ax = 1$ in $\mathbb{Z}_n$ genau eine Lösung. Deren Lösung $x \in \mathbb{Z}_n$ ist genau a^{-1}.

("$\Leftarrow$" ✓)

"$\Rightarrow$" $ggT(a, n) \neq 1 \Rightarrow a$ besitzt kein a^{-1}