A Menge: endlich, falls A endlich viele Elemente enthält (Schreibweise: $|A| < \underset{\text{"unendlich"}}{\infty}$)

Ist A nicht endlich, so heißt A unendlich.

Def.

Sei A eine Menge. A heißt abzählbar, falls es eine Bijektion $f : \mathbb{N} \to A$ gibt oder A endlich ist.

Mengen, die nicht abzählbar sind, heißen überabzählbar.

Beispiele: (abz. Mengen): $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$

Bsp (überabzählbare Menge): $\mathbb{R}$

$$(0,1) := \{x \in \mathbb{R} : 0 < x < 1\}$$

"offenes Intervall $(0,1)$"

$a, b \in \mathbb{R} \quad a < b$:

$$(a,b) := \{x \in \mathbb{R} : a < x < b\}$$

$$[a,b] := \{x \in \mathbb{R} : a \leq x \leq b\}$$

$$[a,b) := \{x \in \mathbb{R} : a \leq x < b\}$$

$$(a,b] := \{x \in \mathbb{R} : a < x \leq b\}$$

Satz:

$(0,1)$ ist überabzählbar. (d.h. es gibt keine (!) Bijektion von $\mathbb{N}$ nach $(0,1)$)

Beweis:

$a \in (0,1)$:

$$a = 0, a_1 a_2 a_3 ..., \quad \text{wobei } a_i \in \{0, 1, ..., 9\} \qquad \text{Dezimaldarstellung}$$

Beweis durch Widerspruch:

sei $f : \mathbb{N} \to (0,1)$ eine Bijektion

$$\varphi(1) = 0, s_{11} s_{12} s_{13} ...$$

$$\varphi(2) = 0, s_{21} s_{22} s_{23} ...$$

$$\varphi(3) = 0, s_{31} s_{32} s_{33} ...$$

$$\vdots$$

$$\varphi(n) = 0, s_{n1}s_{n2}s_{n3}...s_{nn}s_{n(n+1)}s_{n(n+2)}\cdots$$

$$\varphi(n+1) = 0, ...$$

$$\vdots$$

Wir definieren, ausgehend von der Diagonalen $(s_{11}, s_{22}, s_{33}, ...)$ eine Zahl $a \in (0,1)$, welche in der Aufzählung nicht vorkommt, d.h. für alle $n \in \mathbb{N}$ gilt: $\varphi(n) \neq a$

$$a = 0, a_1a_2a_3...a_n...$$

$$a_i := \begin{cases} 4, \text{ falls } s_{ii} \neq 4 \\ 5, \text{ falls } s_{ii} = 4 \end{cases}$$

Beispiel:

$$\varphi(1) = 0, 123...$$
$$\varphi(2) = 0, 143...$$
$$\varphi(3) = 0, 144...$$

$a = 0, 455...$

Da a in der Aufzählung $\varphi(1), \varphi(2), ...$ von $(0,1)$ nicht vorkommt, erhalten wir einen Widerspruch zur Annahme (,dass $(0,1)$ abzählbar). Also muss $(0,1)$ überabzählbar sein. $\square$

Erinnerung:

Aufzählung einer Menge A ist eine surjektive Abbildung $\psi : \mathbb{N} \to A$.

Erinnerung:

Zwei Mengen A und B sind gleichmächtig, falls es eine Bijektion zwischen A und B gibt.

Beispiele:

$\mathbb{N}$ und $\mathbb{Q}$ sind gleichmächtig.

$\mathbb{Q}$ und $\mathbb{R}$ sind nicht gleichmächtig.

Sind A und B endlich, so gilt:

A und B sind gleichmächtig $\Leftrightarrow |A| = |B|$

Deswegen:

$|A|$ Mächtigkeit von A oder: Kardinalität von A

Beispiele:

$$M := \{x \in \mathbb{R} : x \geq 1\}$$

$$N := \{x \in \mathbb{R} : x \geq 2\}$$

M und N sind gleichmächtig, denn:

$$\varphi : \begin{cases} M \to N \\ x \mapsto x + 1 \end{cases} \quad \text{ist eine Bijektion}$$

Andere Schreibweise für M und N:

$M = [1, \infty) = \{x \in \mathbb{R} : 1 \leq x < \infty\}$

$N = [2, \infty)$

$$L = \{x \in \mathbb{R} : x < 1\} = (-\infty, 1) = \{x \in \mathbb{R} : -\infty < x < 1\}$$

$$L' = \{x \in \mathbb{R} : -\infty < x \leq 1\} = (-\infty, 1]$$

$$g : \begin{cases} L' \to M \\ x \mapsto -x + 2 \end{cases}$$

$L'' := [-1, \infty)$

Bem.:

L und M sind gleichmächtig (Aufgabe)

$\mathbb{Q} : \boxed{(K1) - (K5)}$ Körperaxiome:

$K = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

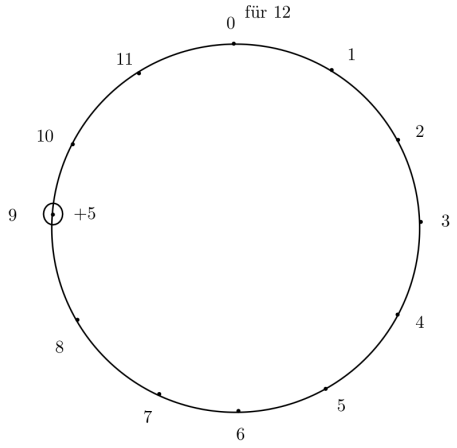
$\cdot$	0	1
0	0	0
1	0	1

0 entspricht einer geraden Zahl

1 entspricht einer ungeraden Zahl

Bsp.

Uhr



$'9 + 5' =' 2'$

Modulare Arithmetik.

Division mit Rest

Sei $a \in \mathbb{N}_0,\ n \in \mathbb{N}$

Wir können a durch n teilen, indem wir mehrfach von a die Zahl n abziehen (subtrahieren), bis eine Zahl r mit $0 \leq r < n$ übrig bleibt. Die Zahl r nennen wir den Rest der Division von a durch n und bezeichnen mit $\boxed{a \ mod \ n}$

Wir sagen: r ist der Rest von a modulo n.

$a \in \mathbb{Z}, \quad a < 0$

$a \ mod \ n$ erhalten wir, wenn wir zu a n solange addieren, bis wir eine nichtnegative Zahl erhalten.

Def.

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

Wir definieren $\boxed{a \ mod \ n}$ als die kleinste ganze Zahl $r \geq 0$, so dass es ein $q \in \mathbb{Z}$ mit $\boxed{r = a - q \cdot n}$ gibt.

Def.

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

Die Zahl n heißt ein Teiler von a, falls es ein $q \in \mathbb{Z}$ gibt, so dass gilt: $\boxed{a = n \cdot q}$

Wir schreiben in diesem Fall: $n|a$

Sprechweise: n teilt a oder n ist ein Teiler von a

Bemerkung:

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

$$\Leftrightarrow a \; mod \; n = 0$$

Lemma:

Seien $a, b, c \in \mathbb{Z}$

1.) Aus $a|b$ folgt $a|bc$

2.) Aus $a|b$ und $b|c$ folgt $a|c$

3.) Aus $a|b$ und $a|c$ folgt $a|(sb + ct)$ für alle $s, t \in \mathbb{Z}$

4.) Ist $c \neq 0$, so gilt $a|b \Leftrightarrow ac|bc$

Beweis:

Wir zeigen nur (2), der Rest ist Übung.

(2) Aus $a|b$ folgt (nach der Def.):

es gibt ein $s \in \mathbb{Z} : \boxed{as = b}$

Aus $b|c$ folgt: $\exists t \in \mathbb{Z}$ mit $\boxed{bt = c}$.

Setzt man für $b = as$ ein $bt = c$ ein, so erhalten wir: $\boxed{ast = c} \quad s, t \in \mathbb{Z}$

d.h. $a|c$.

Def.

Seien $a, b \in \mathbb{Z}$, sei $n \in \mathbb{N}$.

Sei $a \; mod \; n = b \; mod \; n$, so nennen wir a und b kongruent modulo n, und schreiben dazu:

$$\boxed{a \equiv b \; mod \; n}$$

KONGRUENT modulo n

! $a \equiv b \; mod \; n \Leftrightarrow$

a und b besitzen denselben Rest modulo n

$a = b \; mod \; n \Leftrightarrow$

a ist der Rest von b modulo n

Lemma

Für $a, b \in \mathbb{Z}, \quad n \in \mathbb{N}$ gilt $a \equiv b \; mod \; n$ genau dann, wenn $a|(a-b)$.

Beweis: (genau dann, wenn: $\boxed{\Leftrightarrow}$)

Sei $r_a \in \mathbb{Z}$ mit $0 \leq r_a < n$ der Rest von $a \; mod \; n$.

D.h. $\exists q_a \in \mathbb{Z} : \boxed{r_a = a - q_a \cdot n}$

Analog: $r_b \in \mathbb{Z}$ mit $0 \leq r_b < n$

$\exists q_b : \boxed{r_b = b - q_b \cdot n}$

"$\Rightarrow$" $a \equiv b \; mod \; n$ heißt: $r_a = r_b$

D.h.:

$$\begin{aligned} a - q_a n &= b - q_b n \\ a - b &= q_a n - q_b n = (q_a - q_b) \cdot k \end{aligned}$$

D.h.:

$$n|(a-b)$$

$$\begin{aligned} \text{" } \Leftarrow \text{ "} \quad a &= a_a + q_a n \\ b &= r_b + q_b n \\ a - b &= r_a - r_b + (q_a - q_b) \cdot n \end{aligned}$$

Da $n|(q_a - q_b)n$, und $n|(a-b)$ teilt (Vor.), muss n auch $r_a - r_b$ teilen.

$$\begin{aligned} 0 \leq r_a &< n \\ 0 \leq r_b &< n \\ \text{d.h.} \quad 0 \leq |r_a - r_b| &< n \end{aligned}$$

Also muss $|r_a - r_b| = 0$ sein, daher gilt: $r_a = r_b$.

D.h. $a \equiv b \; mod \; n \quad \square$

Lemma

Seien $x, y, a, b \in \mathbb{Z}$

Sei $n \in \mathbb{N}$ Gelten: $x \equiv y \; mod \; n$ und $a \equiv b \; mod \; n$, so gelten:

1) $x + a \equiv y + b \; mod \; n$

2) $x - a \equiv y - b \; mod \; n$

3) $xa \equiv yb \ mod \ n$

4) $x^d \equiv y^d \ mod \ n$ für alle $d \in \mathbb{N}$

Beweis: Übung:

(3) $x \equiv y \ mod \ n$ folgt: $\exists q \in \mathbb{Z} : (x-y) = q \cdot n$

$a \equiv b \ mod \ n$ folgt: $\exists s \in \mathbb{Z} : (a-b) = s \cdot n$

$x = y + qn$

$a = b + sn$

$\boxed{xa = yb + bqn + ysn + qsn^2}$

$xa - yb = (bq + ys + qsn)n$

Also, nach dem Lemma davor gilt:

$$xa \equiv yb \ mod \ n$$

Lemma:

Die Kongruenzrelation modulo n ist eine Äquivalenzrelation.

Beweis:

Sei $n \in \mathbb{N}$

$a \equiv b \ mod \ n$

$$\{(a,b) \in \mathbb{Z}^2 : a \equiv b \ mod \ n\} =: " \equiv " \leq \mathbb{Z}^2$$

reflexiv: $a \equiv a \ mod \ n \forall a \in \mathbb{Z}$

symmetrisch: $a \equiv b \ mod \ n \Rightarrow b \equiv a \ mod \ n$

transitiv: $a \equiv b \ mod \ n : n|(a-b)$

$b \equiv c \ mod \ n : n|(b-c)$

Also $n"((a-b)+(b-c)) = (a-c)$

$\Rightarrow a \equiv c \ mod \ n.$

Mit $\equiv_n$ bezeichnen wir also auch die Äquivalenzrelation auf $\mathbb{Z}$.

- $\equiv_n \subseteq \mathbb{Z}^2 := \{(a,b) \in \mathbb{Z}^2 : a \equiv b \ mod \ n\}$

$a \in \mathbb{Z}$ Äquivalenzklasse von a:

$$[a]_{\equiv_n} := \{b \in \mathbb{Z} : a \equiv b \ mod \ n\} = \{b \in \mathbb{Z} : n|(a-b)\}$$

Die Menge $[a]_{\equiv_n}$ wird eine Restklasse von a modulo n genannt.

kurze Schreibweise: $[a]$

Beispiel: $n = 2$:

$[0]_{\equiv_2} = \{$ gerade ganze Zahlen$\} = \{2k : k \in \mathbb{Z}\}$

$[1]_{\equiv_2} = \{$ ungerade ganze Zahlen$\} = \{2k + 1 : k \in \mathbb{Z}\}$

$n = 5$:

(n) fünf Restklassen:

(jede Restklasse entspricht einem Rest zwischen $0, 1, ..., n - 1$ bei der Division modulo n)

$$
\begin{aligned}
[0] &= \{5k : k \in \mathbb{Z}\} \\
[1] &= \{5k + 1 : k \in \mathbb{Z}\} \\
[2] &= \{5k + 2 : k \in \mathbb{Z}\} \\
[3] &= \{5k + 3 : k \in \mathbb{Z}\} \\
[4] &= \{5k + 4 : k \in \mathbb{Z}\} \\
[5] &= [0]
\end{aligned}
$$

Bem.

Restklasse von modulo n = Äquivalenzklasse von a bez. $\equiv_n$.

Def.

Jede Restklasse $[a]_{\equiv_n}$ enthält genau eine Zahl $r \in \{0, 1, ..., n-1\}$ mit $[r]_{\equiv_n} = [a]_{\equiv_n}$. Und wir nennen r den Repräsentanten dieser Restklasse.

Def.

Die Menge aller Repräsentanten bezeichnen wir mit

$\mathbb{Z}_n := \{0, 1, ..., n - 1\}$ für $n \in \mathbb{N}$

Additon und Multiplikation in $\mathbb{Z}_n$:

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

$$
\underset{\text{Summe in } \mathbb{Z}_n}{a + b} := \overset{\text{Summe in } \mathbb{Z}}{(a + b)} \ mod\ n
$$

$$
\underset{\text{Produkt/Mult. in } \mathbb{Z}_n}{a \cdot b} := \overset{\text{Multiplikation in } \mathbb{Z}}{(a \cdot b)} \ mod\ n
$$