1.9 Kongruenzen

1.51 Def: Sei $m \in \mathbb{N}$, $m \geq 2$.
$a, b \in \mathbb{N}$ heißen kongruent modulo m ($a \equiv b \pmod m$ oder $a \equiv b \,(m)$) wenn $m \mid |a-b|$. D.h. a und b ergeben beim Teilen durch m denselben Rest:

$a = q_1 m + r_1$, $0 \leq r_1 \leq m-1$

$b = q_2 m + r_2$, $0 \leq r_2 \leq m-1$

Dann:

$a \equiv b \pmod m \iff m \mid |a-b|$

$\iff m \mid |q_1 m + r_1 - q_2 m + r_2|$

$\iff m \mid \underbrace{|r_1 - r_2|}_{\in \{0,1,\dots,m-1\}}|$

$\iff r_1 - r_2 = 0$

1.52 Satz: $\equiv \pmod m$ ist Äquivalenzrelation auf $\mathbb{N}$

Beweis: 1) reflexiv: $a \equiv a \pmod m$ ✓

2) symmetrisch: $a \equiv b \pmod m \iff m \mid \underbrace{|a-b|}_{=|b-a|}$

$\iff b \equiv a \pmod m$

3) transitiv: $a \equiv b \pmod m \wedge b \equiv c \pmod m$

$\Leftrightarrow m \mid |a-b| \wedge m \mid |b-c|$

$\Rightarrow m \mid |a-b+b-c|$

$\Leftrightarrow m \mid |a-c|$

$\Leftrightarrow a \equiv c \pmod m$ □

1.53 Satz: + und · auf $\mathbb{N}$ sind verträglich mit $\equiv \pmod m$, d.h.

$a \equiv a' \pmod m \wedge b \equiv b' \pmod m$

$\Rightarrow \begin{cases} a+b \equiv a'+b' \pmod m \\ a \cdot b \equiv a' \cdot b' \pmod m \end{cases}$

Beweis: $m \mid |a-a'| \wedge m \mid |b-b'|$

$\Rightarrow m \mid |a \cdot b - a' \cdot b'|$

$= |a \cdot (b-b') + b'(a-a')|$ Addition selber!

durch m teilbar

$\Rightarrow a \cdot b \equiv a' \cdot b' \pmod m$ □

1.54 Rechnen mit Äquivalenzklassen: Die Äquiv.-Rel. $\equiv \pmod m$ besitzt genau m Äquivalenzklassen:

$[1] = \{1, m+1, 2m+1, \dots\}$

$[2] = \{2, m+2, 2m+2, \dots\}$

$\vdots$

$[m] = \{m, 2m, 3m, \dots\}$

$[m+1] = [1]$

die Restklassen modulo m. Definiere

$[a]+[b] := [a+b]$

$[a]\cdot[b] := [a\cdot b]$

wobei a ein bel. El. von $[a]$ ist.

Die Def. ist sinnvoll, denn

$a' \in [a] \wedge b' \in [b]$

letzter Satz $\Rightarrow$
$\begin{cases} a'+b' \equiv a+b \pmod m \\ a'\cdot b' \equiv a\cdot b \pmod m \end{cases}$

$\Rightarrow$
$\begin{cases} [a'+b'] = [a+b] \\ [a'\cdot b'] = [a\cdot b] \end{cases}$

Es gelten:

1) $[a]+([b]+[c]) = [a]+[b+c] = [a+b+c]$

$= [a+b]+[c] = ([a]+[b])+[c]$

(Assoziativgesetz)

2) $[a]+[m] = [a+m] = [a]$ Neutrales Element bezügl. +

3) Für $a \in \{1, \dots, m-1\}$ gilt

$[a]+[m-a] = [a+m-a] = [m]$

$[m-a]$ ist das inverse Element zu $[a]$ bezügl. +

Für $a = [m]$ ist $[m]$ das inverse El.

4) $[a]+[b] = [a+b] = [b+a] = [b]+[a]$ (Kommutativgesetz)

Man setzt

$\mathbb{Z}/m\mathbb{Z} := \{[1], [2], \ldots, [m]\}$

$(\mathbb{Z}/m\mathbb{Z}, +)$ bildet eine abelsche (oder kommutative) Gruppe (vgl. später)

Wie ist das mit Multiplikation? Z.B. $m = 4$

$\cdot$	[4]	[1]	[2]	[3]
[4]	[4]	[4]	[4]	[4]
[1]	[4]	[1]	[2]	[3]
[2]	[4]	[2]	[4]	[2]
[3]	[4]	[3]	[2]	[1]

Wir sehen: $\cdot$ $[2] \cdot [2] =$ neutrales El. bez. + $= 0$

Es gibt Nullteiler

- Die Gleichung $[2] \cdot x = [2]$ besitzt zwei verschiedene Lösungen $x = [1]$, $x = [3]$
- $[2] \cdot x = [1]$ hat keine Lösung

1.55 Satz: Sei $m \in \mathbb{N}$, $m \geq 2$. Dann

1) $[a]$ besitzt ein inverses Element bezügl. $\cdot$, d.h. die Gl. $[a] \cdot x = [1]$ hat eine Lösung

$\Leftrightarrow$ $ggT(a, m) = 1$

2) $\forall a \in \{1, \dots, m-1\}\ \exists l \in \{1, \dots, m-1\} : [a]\cdot[l]=1$

$\Leftrightarrow$ m ist Primzahl

Beweis: 1) $[a]\cdot[l]=1 \Leftrightarrow$

$\Leftrightarrow [a\cdot l]=[1]$

$\Leftrightarrow a\cdot l \equiv 1 \pmod m$

$\Leftrightarrow m \mid (a\cdot l - 1)$

$\Leftrightarrow \exists y \in \mathbb{N} : a\cdot l - 1 = m\cdot y$

$\Leftrightarrow 1 = a\cdot l - m$

Satz 1.45:

$\{mx+my : x,y \in \mathbb{Z}\} = \mathbb{Z}\cdot ggT(m,n)$

$\Leftrightarrow 1 \in \{mx+ay : x,y \in \mathbb{Z}\}$

$\overset{1.45}{\Leftrightarrow} 1 = ggT(a,m)$

2) "$\Leftarrow$" m Primzahl $\Rightarrow ggT(a,m)=1 \overset{1)}{\Rightarrow} [a]\cdot x=[1]$ hat Lös.

"$\Rightarrow$" Für jedes $a \in \{2, \dots, m-1\}$ hat die Gl. $[a]\cdot x=[1]$ eine Lös.

$\overset{1)}{\Rightarrow} \forall a \in \{2, \dots, m-1\} : ggT(a,m)=1$

$\Rightarrow m$ besitzt keinen Teiler außer 1 und m

$\Rightarrow m$ ist Primzahl. □

1.10 Darstellung natürlicher Zahlen

Zehnersystem: $108 = 1 \cdot 10^2 + 0 \cdot 10^1 + 8 \cdot 10^0$

1.56 Def: Gegeben: Ziffernbasis $g \in \mathbb{N}, g \geq 2$

Ziffern: $Z = \{0, \ldots, g-1\}$ Menge mit g Elementen

Die Darstellung

$$n = (a_N a_{N-1} \ldots a_1 a_0)_g := \sum_{j=0}^{N} a_j g^j$$

heißt g-adische Entwicklung von $n \in \mathbb{N}$.

z.B. $g=2$, $Z = \{0,1\}$: Binärsystem

$1011_2 = (1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0)_{10} = 11_{10}$

Hexadezimalsystem: $g = 16$, $Z = \{0, \ldots, 9, A, B, \ldots, F\}$

wobei A den Wert 10 hat, ...

$D2A_{16} = (13 \cdot 16^2 + 2 \cdot 16^1 + 10 \cdot 16^0)_{10} = 3370_{10}$

1.57 Satz: Seien g, Z fest. Jede Zahl $n \in \mathbb{N}$ besitzt eine eindeutige g-adische Entwicklung

Beweis der Existenz (Konstruktiv!):

Euklid. Algorithmus:

$n = q_1 \cdot g + r_1 \Rightarrow a_0 = r_1$

$q_1 = q_2 \cdot g + r_2 \Rightarrow a_1 = r_2$

$$\vdots$$

$q_{N-2} = q_{N-1} \cdot g + r_{N-1} \Rightarrow a_{N-2} := r_{N-1}$

$q_{N-1} = q_N \cdot g + r_N \Rightarrow a_{N-1} := r_N$

$q_N = 0 \cdot g + r_{N+1} \Rightarrow a_N := r_{N+1} = q_N$

Rückwärts hochgehen:

$q_{N-1} = a_N g + a_{N-1}$

$q_{N-2} = a_N \cdot g^2 + a_{N-1} g + a_{N-2}$

$$\vdots$$

$n = a_N \cdot g^N + a_{N-1} g^{N-1} + \ldots + a_0 \cdot g^0$

z.B: 2018 mit $g = 6$:

$2018 = 336 \cdot 6 + 2 \Rightarrow a_0 = 2$

$336 = 56 \cdot 6 + 0 \Rightarrow a_1 = 0$.

$56 = 9 \cdot 6 + 2 \Rightarrow a_2 = 2$

$9 = 1 \cdot 6 + 3 \Rightarrow a_3 = 3$

$1 = 0 \cdot 6 + 1 \Rightarrow a_4 = 1$

$\Rightarrow 2018_{10} = 13202_6$

1.11 Mächtigkeit von Mengen

1.58 Def: Zwei Mengen A, B heißen gleich groß oder gleich mächtig, falls es eine bijektive Abb. $f: A \to B$ gibt.

Bsp: 1) $f: \{1,2,3\} \to \{a,b,c\}$

$f(1) := a$, $f(2) = b$, $f(3) := c$ $\Rightarrow$ f bijektiv

2) $f:]-\infty, -3] \to]-\infty, -1] : x \mapsto x+2$

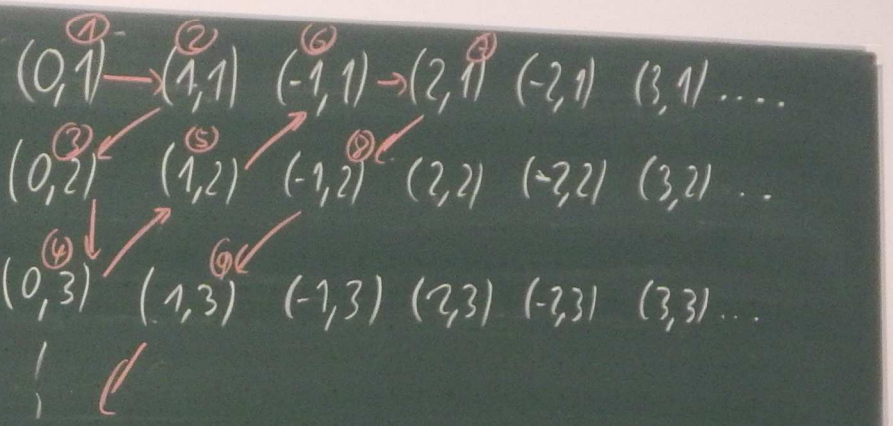
d.h. $]-\infty, -3] \subsetneq]-\infty, -1[$, aber trotzdem gleich groß

3) $D := \{3n : n \in \mathbb{N}\}$

$f: \mathbb{N} \to D : n \mapsto 3n$ ist bijektiv

4) $\mathbb{Z} \times \mathbb{N}$ ist gleich mächtig wie $\mathbb{N}$.

Cantorsches Diagonalverfahren:



Die Nummerierung definiert die bijektive Abb $f: \mathbb{Z} \times \mathbb{N} \to \mathbb{N}$

Interpretiere die Zahlenpaare als Brüche: $(a,l) \triangleq \frac{a}{l}$

Lasse alle Brüche weg, deren Wert bereits vorkam

$\Rightarrow f: \mathbb{Q} \to \mathbb{N}$ bijektiv

$\mathbb{Q}$ ist gleich mächtig wie $\mathbb{N}$.