(1.1) Gruppen

Wichtige Regeln für $\mathbb{Z}$ mit „+" und „·"

(0) Für $a, b \in \mathbb{Z}$ ist $a+b \in \mathbb{Z}$ | Abgeschlossen

(i) Es gibt eine Zahl $e \in \mathbb{Z}$ mit $a+e=a$ für alle $a \in \mathbb{Z}$ | neutrales Element $e=0$

(ii) Für alle $a \in \mathbb{Z}$ gibt es ein Element $a' \in \mathbb{Z}$ mit $a+a'=e$ | Inverses Element $a=5 \Rightarrow a'=-5$

(iii) Für alle $a, b, c \in \mathbb{Z}$ gilt $(a+b)+c = a+(b+c)$ | Assoziativ.

Es sei M eine Menge und $\circ$ ein Operator (zweistellig) auf M.

Es gelte:

(o) $\circ$ ist auf M abgeschlossen

(i) Es gibt ein $e \in M$ mit $a \circ e = a$ für alle $a \in M$

(ii) Für alle $a \in M$ gibt es ein a' mit $a \circ a' = e$

(iii) Für alle $a, b, c \in M$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$

Dann ist $(M, \circ)$ eine Gruppe

$(\mathbb{N}, +)$ ist keine Gruppe

$(\mathbb{Z}, +)$ ist Gruppe

$(\mathbb{Q}, +)$ ist Gruppe

$(\mathbb{R}, +)$ ist Gruppe

$(\mathbb{Z}, \cdot)$ ist keine Gruppe

$(\mathbb{Q} - \{0\}, \cdot)$ ist Gruppe

$(\mathbb{R} - \{0\}, \cdot)$ ist Gruppe

$$G = \{7 \cdot a \mid a \in \mathbb{Z}\} = \{\dots, -14, -7, 0, 7, 14, \dots\}$$

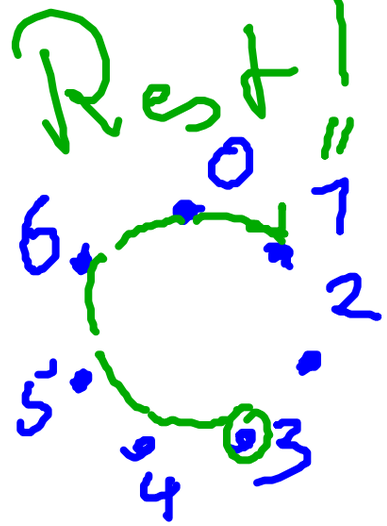
$(7\mathbb{Z}, +)$ ist Gruppe $= 7\mathbb{Z}$

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$

$$a \oplus_7 b = (a+b) \bmod 7$$

$3 + 5$ ← 7ner Rest

$$3 \oplus_7 5 = 1$$



$(\mathbb{Z}_7, \oplus_7)$

a	0	1	2	3	4	5	6
a'	0	6	5	4	3	2	1

$3 + 5$

$e = 0$

$a \odot_7 b = (a \cdot b) \bmod 7$

$3 \odot_7 5 = 1$

$(\mathbb{Z}_7 - \{0\}, \odot_7)$ ist Gruppe

$e = 1$

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Allgemein: $(\mathbb{Z}_p, \oplus_p)$ ist Gruppe für für alle $p \in \mathbb{N} - \{0\}$

$(\mathbb{Z}_p - \{0\}, \odot_p)$ ist Gruppe g.d.w p ist Primzahl

Satz $(\mathbb{Z}_p, \oplus_p)$ ist Gruppe für alle $p \in \mathbb{N} - \{0\}$

Bew 0) Abgeschlossenheit von $a \oplus_p b$
Bildbereich von $\oplus_p$ ist $\{0,1,2,\ldots,p-1\} = \mathbb{Z}_p$

i) Neutrales Element:
Sei $a \in \mathbb{Z}_p$ $\quad a \oplus_p 0 = (a+0) \bmod p$
0 ist neutr. El. $\quad = a \bmod p = a$

ii) Inverses Element
Sei $a \in \mathbb{Z}_p$ wähle $a' = (p-a) \bmod p$
$a \oplus_p a' = (a + (p-a)) \bmod p = p \bmod p = 0$

iii) Assoziativität: Sei $a, b, c \in \mathbb{Z}_p$
$(a \oplus_p b) \oplus_p c = ((a+b) \bmod p) + c) \bmod p = ((a+b)+c) \bmod p$
$= (a + (b+c)) \bmod p = \ldots \ldots = a \oplus_p (b \oplus_p c)$

Satz: $(\mathbb{Z}_p - \{0\}, \odot_p)$ ist Gr. wenn p Primzahl

Bew 0) Abgeschlossenheit: Bildbereich von $\odot_p$ ist $\mathbb{Z}_p - \{0\}$

zu zeigen $a \cdot b \neq k \cdot p$, $a, b \in \mathbb{Z}_p - \{0\}$, $k \in \mathbb{Z}$

wegen p ist Primzahl (Eindeutigkeit Primfaktorzerlegung)

i) neutrales Element sei $a \in \mathbb{Z}_p - \{0\}$

$a \odot_p 1 = (a \cdot 1) \bmod p = a$

! ii) Inverses El. Später ...!

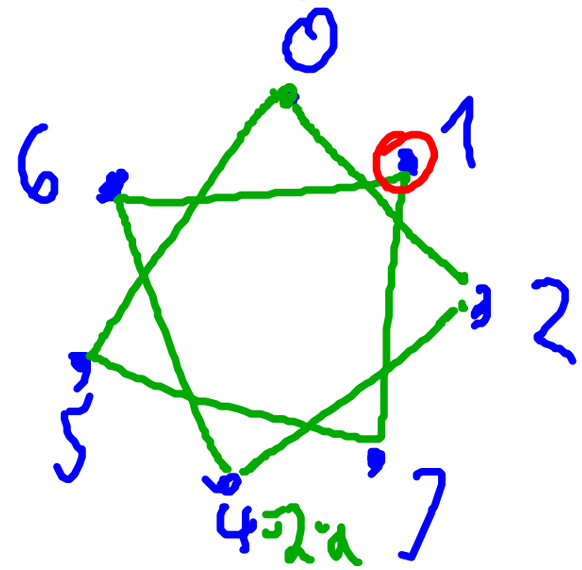
iii) Abschluss zu $(\mathbb{Z}_p, \oplus_p)$

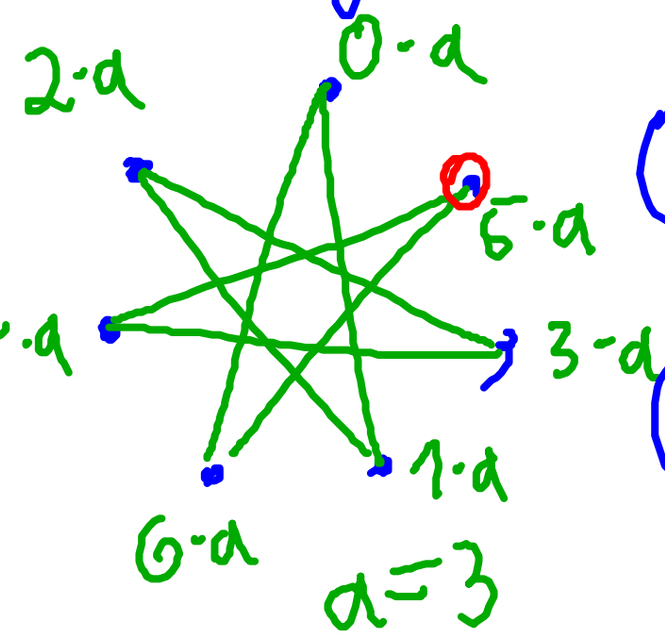
Die eigentliche Schwierigkeit:

Sei p eine Primzahl und $a \in \mathbb{Z}_p - \{0\}$

Zeige: es gibt ein $b \in \mathbb{Z}_p$ mit $(a \cdot b) \bmod p = 1$

Bildhaftes Diagrammhaftes Verstehen $p = 7$





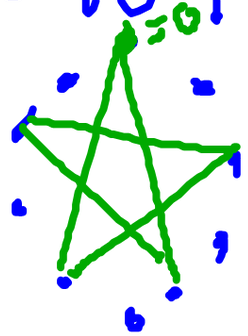
Beobachtungen:

(i) jede getroffene Ecke sieht gleichaus

(ii) alle Ecken werden getroffen insb die Ecke 1

---

p keine P2 $p = 10$ $a = 4$



Etwas Formeln:

Es sei p Primzahl und $a < p$

Betrachte: $\{0 \odot_p a, 1 \odot_p a, 2 \odot_p a \ldots\ldots (p-1) \odot_p a\} = M_a$

Ann $M_a \neq \mathbb{Z}_p$ $\Rightarrow$ Es exist. $i, j < p$ mit

$i \odot_p a = j \odot_p a \qquad i > j$

$\Leftrightarrow (i \cdot a) \bmod p = (j \cdot a) \bmod p$

$\Leftrightarrow (i \cdot a - j \cdot a) \bmod p = 0$

$\Leftrightarrow (i - j) \cdot a = k \cdot p$ Widerspruch

$= p \quad < p$

$\neq 0 \quad \neq 0$

zu p ist Primzahl