$\mathbb{Z}/m\mathbb{Z}$ ist ein Körper $\Leftrightarrow$ m ist eine Primzahl

$\mathbb{Z}/p\mathbb{Z}$

Bsp: $\mathbb{Z}/8\mathbb{Z}$ kein Körper

multiplikativ invertierbar: $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ (weil ggT mit 8 = 1 ist.)

$\mathbb{Z}/5\mathbb{Z}$ ist ein "

$\mathbb{Z}/27\mathbb{Z}$ ist kein Körper

$\mathbb{Z}/101\mathbb{Z}$ ist ein Körper $\Rightarrow \{\bar{1}, \dots, \overline{100}\}$ sind multiplikativ invertierbar!

(101 ↑ Primzahl)

$\overline{13}^{-1} = \overline{70}$ → bekommt man mit dem erweiterten Euklid. Alg.

$ggT(13, 101) = 1 \rightarrow \exists\, s, t \in \mathbb{Z}$, s.d.

$s \cdot 13 + t \cdot 101 = 1 \rightarrow$ in $\mathbb{Z}/101\mathbb{Z}$: $\bar{s} \odot \overline{13} = \bar{1}$

$\Rightarrow \bar{s}$ ist das multiplikative Inverse von $\overline{13}$!

$101 = 7 \cdot 13 + 10$

$a = 7 \cdot b + r_1 \Rightarrow r_1 = a - 7b$

$13 = 1 \cdot 10 + 3$

$b = 1 \cdot r_1 + r_2 \Rightarrow r_2 = b - r_1 = b - (a - 7b) = 8b - a$

$10 = 3 \cdot 3 + 1$

$r_1 = 3 \cdot r_2 + r_3 \Rightarrow r_3 = r_1 - 3 \cdot r_2 = (a - 7b) - 3(8b - a) = 4a - 31b$

$3 = 3 \cdot 1 + 0$

ggT

$1 = 4 \cdot 101 - 31 \cdot 13 \Rightarrow s = -31 \Rightarrow (\overline{13})^{-1} = \overline{-31} = \overline{70}$

Beh: Ist p prim, dann gilt $\forall\, \bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\} : \bar{a}^{p-1} = \bar{1}$

(das Inverse von $\bar{a}$ ist:

$$\bar{b} \odot \bar{a} = \bar{1} \Rightarrow \bar{b} = \bar{a}^{p-2}$$

$$\bar{1} = \underbrace{\bar{a} \odot \bar{a} \odot \ldots \odot}_{p-1}$$

Bew: Sei $\bar{a} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$.

$$\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\} = \{\underbrace{\bar{1}, \ldots, \overline{p-1}}_{p-1 \text{ viele}}\} \qquad \{\bar{1}, \ldots, \bar{4}\}$$

$$\bar{a} \cdot \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\} = \{\underbrace{\bar{a}, \bar{2} \odot \bar{a}, \ldots, \overline{(p-1)} \odot \bar{a}}_{p-1 \text{ viele}}\} \subset \mathbb{Z}/p\mathbb{Z} \qquad \{\bar{a}, \bar{2} \odot \bar{a}, \bar{3} \odot \bar{a}, \bar{4} \odot \bar{a}\}$$

Beh: all diese ~~Zahlen~~ Restklassen sind untereinander und ungleich $\bar{0}$.

Bew: mit Widerspruch angenommen, $\bar{i} \odot \bar{a} = \bar{j} \odot \bar{a}$ für $\bar{i} \neq \bar{j} \in \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$

$\Leftrightarrow (\bar{i} \oplus -\bar{j}) \odot \bar{a} = \bar{0} \quad / \cdot \bar{a}^{-1}$

$\Leftrightarrow (\bar{i} \oplus -\bar{j}) = \bar{0}$

$\Leftrightarrow \bar{i} = \bar{j}$. ↯

$\left(\bar{a} \odot \bar{i} = \bar{0} \quad / \cdot \bar{a}^{-1} \right.$
$\left. \bar{i} = \bar{0} \right)$

$$\Rightarrow \bar{a} \cdot \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\} = \{\bar{1}, \ldots, \overline{p-1}\}$$

$$\Rightarrow \underbrace{\bar{1} \odot \bar{2} \odot \ldots \odot \overline{p-1}}_{=: \bar{x}} = \bar{a} \odot \bar{1} \odot \bar{a} \odot \bar{2} \odot \ldots \odot \overline{(p-1)} \odot \bar{a}$$

$$= \bar{a}^{p-1} \odot \underbrace{\bar{1} \odot \bar{2} \odot \ldots \odot \overline{p-1}}_{\bar{x}}. \qquad / \cdot \bar{x}^{-1}$$

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

RSA - Algorithmus

A → B

Text/Ziffer → Zahl M . . . . . >

↓

wähle große Primzahlen p, q

Berechne: $n = p \cdot q$ → B

$m = (p-1) \cdot (q-1)$.

$(\mathbb{Z}/m\mathbb{Z})^x = \{\bar{x} \text{ mit } ggT(x,m) = 1\}$

kein Körper

Wähle eine zufällige Restklasse

$[\bar{e}] \in (\mathbb{Z}/m\mathbb{Z})^x \Rightarrow$ encryption key → B

Berechne

$\bar{e}^{-1} = \bar{d} \in (\mathbb{Z}/m\mathbb{Z})^x$

mit dem erweiterten euklid. Algorithmus

A:

p, q → $n = p \cdot q$

$m = (p-1)(q-1)$

$\bar{e} \in (\mathbb{Z}/m\mathbb{Z})^x$

Berechne $\bar{d} = \bar{e}^{-1}$

Verschlüsseln mit $\bar{e}$:

$S = M^e \bmod n$ = Verschlüsselung von M

B

n, $\bar{e}$ öffentlich

$\bar{d}$ private key hat nur B, niemand von außen

Entschlüsseln:

$S^d \bmod n = M$

weil $M^{e \cdot d} = M \bmod n$

$(\mathbb{Z}/p\mathbb{Z})^3$ $\quad$ $\mathbb{R}^3$ $\quad$ $\mathbb{Q}^3$ $\quad$ $\mathbb{C}^2$

$\mathbb{R}$ $\quad$ $\mathbb{Q}$ $\quad$ $\mathbb{C}$

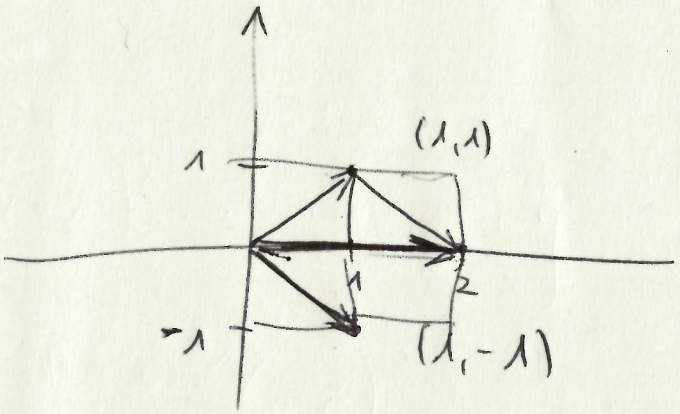
$\bar{2}\cdot\begin{pmatrix}\bar{1}\\ \bar{0}\\ \bar{2}\end{pmatrix} = \begin{pmatrix}\bar{2}\\ \bar{0}\\ \bar{1}\end{pmatrix}$ im $(\mathbb{Z}/3\mathbb{Z})^3$

$\mathbb{R}\times\mathbb{R}\times\mathbb{R}$ $\quad$ $\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}$ $\quad$ $\mathbb{C}\times\mathbb{C}$

(x,y,z) $\quad$ (x,y,z) $\quad$ $(a+ib,\ c+id)$

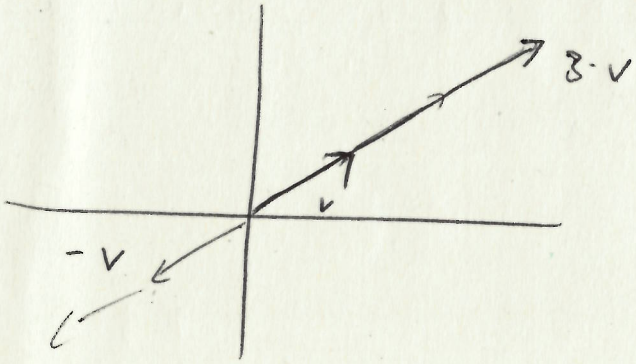
$\lambda\cdot\begin{pmatrix}x\\ y\\ z\end{pmatrix} = \begin{pmatrix}\lambda\cdot x\\ \lambda\cdot y\\ \lambda\cdot z\end{pmatrix}$

z.B. : $2\cdot\begin{pmatrix}1\\ 0\\ 1\end{pmatrix} = \begin{pmatrix}2\\ 0\\ 2\end{pmatrix}$ im $\mathbb{R}^3$.



$\mathbb{R}^2$

$\begin{pmatrix}1\\ 1\end{pmatrix} + \begin{pmatrix}1\\ -1\end{pmatrix} = \begin{pmatrix}1+1\\ 1-1\end{pmatrix} = \begin{pmatrix}2\\ 0\end{pmatrix}$



$\mathbb{R}^n$ $\quad \begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}$

$\mathbb{Q}^n$ $\quad$ $\mathbb{C}^n$ $\quad$ $(\mathbb{Z}/p\mathbb{Z})^n$ Vektorraum ~~hat~~ mit p^n vielen Punkten

$(\mathbb{Z}/2\mathbb{Z})^2$ $\quad$ $(\bar{0},\bar{0})$ $\quad$ $(\bar{0},\bar{1})$

$(\bar{1},\bar{0})$ $\quad$ $(\bar{1},\bar{1})$

Beispiele:

$$\mathbb{C}^{(2)} = \left\{ \begin{pmatrix} a+ib \\ c+id \end{pmatrix} \mid a,b,c,d \in \mathbb{R} \right\}.$$

$$(\mathbb{Z}/5\mathbb{Z})^3 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} = \left\{ \begin{pmatrix} \bar{a} \\ \bar{b} \\ \bar{c} \end{pmatrix} \mid \bar{a},\bar{b},\bar{c} \in \mathbb{Z}/5\mathbb{Z} \right\}$$

5^3 Elemente

z.B. $\begin{pmatrix} \bar{2} \\ \bar{3} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{4} \\ \bar{1} \\ \bar{2} \end{pmatrix}$

$$\begin{pmatrix} \bar{2} \\ \bar{3} \\ \bar{0} \end{pmatrix} + \begin{pmatrix} \bar{4} \\ \bar{1} \\ \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{2} \oplus \bar{4} \\ \bar{3} \oplus \bar{1} \\ \bar{0} \oplus \bar{2} \end{pmatrix} = \begin{pmatrix} \bar{1} \\ \bar{4} \\ \bar{2} \end{pmatrix}.$$

$$\bar{2} \odot \begin{pmatrix} \bar{2} \\ \bar{3} \\ \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{4} \\ \bar{1} \\ \bar{0} \end{pmatrix}$$