Komplexe Zahlen

Konstellation von $\mathbb{C}$:

$R^2 = \{(a,b)|a,b \in \mathbb{R}\}$

$(0,1)^2 = -1$

“imaginäre Einheit:”

$(0,1) = i$

Andere Notation:

$(a,b) \in R^2 = (a,0) + (0,b) = (a,0) + (0,1) \cdot (b,0) = a + i \cdot b$

$\mathbb{C} = \{a + ib|a,b \in \mathbb{R}\}$

Addition:

$(a+ib) + (c+id) = (a+c) + i(b+d)$

Multiplikation:

$(a+ib) \cdot (c+id) = ac + i^2bd + i(ad+bc) = ac - bd + i(ad+bc)$

Begriffe:

$Z = a + ib \in \mathbb{C},\ a,b \in \mathbb{R}$

$a = Re(\mathbb{Z})$

$b = Im(\mathbb{Z})$

wenn $a = 0 \rightarrow Z$ rein imaginär

$Z = a + ib \rightarrow \overline{Z} = a - ib$

$\overline{Z}$ ist die zu Z konjugierte komplexe Zahl

Nützliches:

$Z \cdot \overline{Z} = (a+ib) \cdot (a-ib) = a^2 + b^2$

$|Z| = \sqrt[2]{a^2 + b^2}$

$\overline{Z + W} = \overline{Z} + \overline{W}$

$\overline{Z \cdot W} = \overline{Z} \cdot \overline{W}$

$Re(Z) = \frac{1}{2}(Z + \overline{Z})$

$Im(Z) = \frac{1}{2i}(Z - \overline{Z})$

Dreiecksgleichung:

$Z, W \in \mathbb{C} \Rightarrow |Z + W| \leq |Z| + |W|$

Invertieren: (komplexe Zahl aus Nenner raus bekommen)

$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{ac+bd+i(cb-ad)}{c^2+d^2}$

Polarkoordinaten

Form: $Z = r(\cos\varphi + i\sin\varphi)$

mit Radius $r \in \mathbb{R}$ und Winkel $\varphi \in]-\pi, \pi]$

Umrechnung:

- $Z = a + ib$

1. $r = \sqrt{a^2 + b^2}$
2. $\varphi = \begin{cases} \arccos\frac{a}{r}, b \geq 0 \\ -\arccos\frac{a}{r}, b < 0 \end{cases}$
3. $Z = r \cdot (\cos\varphi + i\sin\varphi)$

- $cos\varphi = \frac{a}{r}$
- $sin\varphi = \frac{b}{r}$

Multiplikation:

$Z_1 = r_1(\cos(\varphi_1) + i\sin(\varphi_1))$

$Z_2 = r_2(\cos(\varphi_2) + i\sin(\varphi_2))$

$Z_1 \cdot Z_2 = r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$

Potenzen:

$Z = r \cdot (\cos(\varphi) + i\sin(\varphi))$

$Z^n = r^n \cdot (\cos(n \cdot \varphi) + i\sin(n \cdot \varphi))$

Wurzeln:

$\sqrt[n]{Z}$ hat genau n Lösungen

$Z_k = \sqrt[n]{r} \cdot (\cos\frac{\varphi+2\pi\cdot k}{n} + i\sin\frac{\varphi+2\pi\cdot k}{n})$

mit $n =$ “Wurzelexponent”,

$r =$ "Radius",

$k =$ "k-te Lösung der Wurzel von 0 bis $n-1$

Lineare Gleichungssysteme

Vereinfachte Schreibweise als Matrix:

$$\overbrace{\begin{matrix} a_{11}x_1 & + & \cdots & + & a_{1n}x_1 & = & b_1 \\ \vdots & + & \ddots & + & \vdots & = & \vdots \\ a_{m1}x_n & + & \cdots & + & a_{mn}x_n & = & b_m \end{matrix}}^{linearesGleichungssystem\ LGS} \Rightarrow \underbrace{\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)}_{(A|b)} \Rightarrow \cdots$$

$$\cdots \Rightarrow \left(\begin{array}{ccccc|c} \color{orange}{*} & \color{orange}{\cdots} & \color{orange}{\cdots} & \color{orange}{*} & & \color{orange}{*} \\ 0 & \color{orange}{*} & \color{orange}{\cdots} & \color{orange}{*} & & \color{orange}{\vdots} \\ \color{cyan}{\vdots} & 0 & \color{orange}{*} & \color{orange}{*} & & \color{orange}{\vdots} \\ \vdots & \vdots & \vdots & \vdots & & \color{orange}{\vdots} \\ 0 & 0 & \color{cyan}{\cdots} & 0 & & \color{purple}{\star} \end{array}\right) \Rightarrow \cdots \Rightarrow \overbrace{\left(\begin{array}{ccccc|c} 1 & \color{orange}{*} & \color{orange}{\cdots} & \color{orange}{*} & & \color{orange}{*} \\ 0 & 1 & \color{orange}{*} & \color{orange}{*} & & \color{orange}{*} \\ 0 & 0 & 1 & \color{orange}{*} & & \color{orange}{*} \\ \color{cyan}{\vdots} & \color{cyan}{\vdots} & \color{cyan}{\ddots} & \color{orange}{\vdots} & & \color{orange}{\vdots} \\ 0 & 0 & \color{cyan}{\cdots} & 0 & & 0 \end{array}\right)}^{reduzierteZeilenstufenform}$$

$\color{orange}{*}$: unbekannter Wert

$\color{cyan}{*}$: 0

$\color{purple}{\star}$: wenn $\neq 0$ gibt es keine Lösung

Umformen in ZNF:

$$\text{Elementare Zeilenumformungen} \begin{cases} \text{Vertauschen zweier Zeilen} \\ \text{Multiplikation einer Zeile mit } \lambda \neq 0 \\ \text{Addition des } \lambda\text{-fachen eines Zeile zu einer anderen} \end{cases}$$

Rang einer Matrix

Matrix M auf ZSF bringen

$\Rightarrow$ Anzahl an nicht null Zeilen = Rang von $M = rg(M)$

Das Kriterium für Lösbarkeit:

- Das System ist genau dann lösbar, wenn: $rg(A) = rg(A|b)$
- ist das LGS lösbar, so gilt: Anzahl frei wählbaren Vraiablen $= n - r$

$n =$ Anzahl der variablen und $r = rg(A)$

- ist das System (A|b) lösbar, so gilt: $\exists_1$ lsg $\Leftrightarrow n = r$

Matrix

$$A = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_1a \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{ma} \end{pmatrix}}_{n \text{ Spalten}} \left.\vphantom{\begin{pmatrix} a \\ a \\ a \end{pmatrix}}\right\} m \text{ Zeilen}$$

Stelle (i, j) : i-te Zeile | j-te Spalte

$$\underbrace{\begin{matrix} \mathbb{R}^{m\times n} & = \{(a_{ij})_{m,n} | a_{ij} \in \mathbb{R}\} \Rightarrow & \text{"reelle Matrix"} \\ \mathbb{C}^{m\times n} & = \{(a_{ij})_{m,n} | a_{ij} \in \mathbb{C}\} \Rightarrow & \text{"komplexe Matrix"} \end{matrix}}_{\Rightarrow K(k\ddot{o}rper)^{m\times n} = \{(a_{ij})_{m,n} | a_{ij} \in K\}}$$

$A = B \Leftrightarrow$ gleich viele Spalten UND gleich viele Zeilen UND gleiche Einträge an den gleichen Stellen

Besondere Matrizen

- $m \times 1$: S = $\begin{pmatrix} S1 \\ \vdots \\ S_m \end{pmatrix}$ Spaltenvektor
- $1 \times n$: $Z = \begin{pmatrix} Z1 & \cdots & Z_n \end{pmatrix}$ Zeilenvektor
- $m \times n$: $0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ Nullmatrix
- $m = n$: <u>quadratische Matrix</u>

$$\text{Diagonalmatrix: } diag(\lambda_1 \dots \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

$$\text{Einheitsmatrix: } E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

$$\text{Obere } \Delta\text{-Matrix: } O = \begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & * \end{pmatrix}$$

$$\text{Untere } \Delta\text{-Matrix: } U = \begin{pmatrix} * & 0 & \cdots & 0 \\ * & * & \ddots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ * & * & \cdots & * \end{pmatrix}$$

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in K^{m \times n} = \begin{pmatrix} \overrightarrow{S_1}, & \cdots & \overrightarrow{S_n} \end{pmatrix} = \begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix}$$

Rechenoperationen

Transponieren:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}$$

Symmetrische Matrix: $A^T = A$

Addieren:

$A = (a_{ij})_{m,n}$, $B = (b_{ij})_{m,n}$

$A + B = (a_{ij} + b_{ij})_{m,n}$

$A = (a_{ij}) = -(-a_{ij}) = -(-A)$

Skalare Multiplikation (Vervielfachen:)

$A = (a_{ij})_{m,n} \in \mathbb{K}^{m \times n}$

$\lambda \in \mathbb{K}$

$\Rightarrow \lambda A = (\lambda a_{ij})$

Multiplikation:

$$Z = (Z_1, \cdots, Z_n) \quad , \quad S = \begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix}$$

$Z \cdot S = \sum_{i=1}^{n} Z_i S_i$

$$\Downarrow$$

$$A = \begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix} \in \mathbb{K}^{m \times n} \quad , \quad B = \begin{pmatrix} S_1 & \cdots & S_p \end{pmatrix} \in \mathbb{K}^{n \times p}$$

$$A \cdot B := \begin{pmatrix} Z_1 \cdot S_1 & Z_1 \cdot S_2 & \cdots & Z_1 S_p \\ Z_2 \cdot S_1 & Z_2 \cdot S_2 & \cdots & Z_2 S_p \\ \vdots & \vdots & \ddots & \vdots \\ Z_m \cdot S_1 & Z_m \cdot S_2 & \cdots & Z_m \cdot S_p \end{pmatrix} \in K^{m \times p}$$

$A \cdot B \neq B \cdot A \leftarrow$ keine Kommutativität

$A^k = \underbrace{A \cdot A \cdots A}_{k}$

$A^0 := E_n$

<u>Invertieren:</u>

$A \in K^{n \times n} \quad , \quad B = A^{-1}$

$A \cdot B = E_n = B \cdot A$

Nicht jede Matrix invertierbar!

$$B = \begin{pmatrix} \vec{S_1} & \dots & \vec{S_n} \end{pmatrix} \quad , \quad e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

$$A \cdot B = A \cdot \begin{pmatrix} \vec{S_1} & \dots & \vec{S_n} \end{pmatrix} = \begin{pmatrix} A\vec{S_1} \cdots A\vec{S_n} S_n \end{pmatrix} = \begin{pmatrix} e_1 & \cdots & e_n \end{pmatrix} = E_n$$

löse so:

$$(A|E_n) \Rightarrow \cdots \text{el. ZUF} \cdots \Rightarrow (E_n|A^{-1})$$

Elementarmartizen

Permutationsmatrizen (Vertauschen von Zeilen):

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}$$

$$P \cdot A = \begin{pmatrix} 1 & 1 & 1 \\ 3 & 3 & 3 \\ 2 & 2 & 2 \end{pmatrix}$$

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Multiplikation einer Zeile mit $\lambda \neq 0$:

$$D_k(\lambda) = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & 1 & 0 & 0 & \ddots & 0 \\ 0 & \ddots & 0 & \lambda & 0 & \ddots & 0 \\ 0 & \ddots & 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \leftarrow k$$

Addition des λ-fachen der l-ten Zeile zur k-ten Zeile:

$$N_{kl}(\lambda) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \lambda & \vdots \\ 0 & \ddots & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \leftarrow \lambda \text{ an der } k\text{-ten Zeile und } l\text{-ten Spalte}$$

Rechenregeln Matrizen

Addition:

$A + B = B + A$	Kommutativität
$(A+B)+C = (A+B)+C$	Assoziativität
$(\mu \cdot \lambda)A = \mu(\lambda \cdot A)$	
$0 + A = A = A = 0$	Neutrales Element
$E_n A = A$	
$\forall A \exists B : A + B = 0$	Inverses Element
$B = -A$	
$\lambda(A+B) = \lambda A + \lambda B$	Distributivität

Transposition:

$(A+B)^T = A^T + B^T$	Summe
$(\lambda A)^T = \lambda A^T$	Skalarmultiplikation
$(A^T)^T = A$	Zweifache Transposition
$(AB)^T = B^T A^T$	Produkt
$(A^{-1})^T = (A^T)^{-1}$	Inverses

Multiplikation:

$\exists A, B : AB \neq BA$	nicht kommutativ!
$(AB)C = A(BC)$	Assoziativität
$\exists E \in E_n : EA = A$	Neutrales Element
$A(B+C) = AB + AC$	Distributivität
$(B+C)A = BA + CA$	
$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$	Inverses

Gruppen

G nichtleere Menge mit innerer Verknüpfung $\cdot$

$\cdot : G \times G \to G$

$(G, \cdot)$ heißt Gruppe, wenn:

$$\begin{array}{r||l} \forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c) & \text{Assoziativgesetz} \\ \exists e \in G : e \cdot a = a = a \cdot e \quad \forall a \in G & \text{neutrales Element} \\ \forall a \in G \exists b \in G : a \cdot b = e = b \cdot a & \text{inverses Element} \end{array}$$

G nennt man <u>abelsch</u> (=kommutativ) falls:

- $ab = ba \quad \forall a, b \in G$

Untergruppen

$(G, \cdot)$ sei eine Gruppe mit neutralem Element e

$U \subseteq G$ mit:

$$\left.\begin{array}{r||l} e \in U & \text{neutrales Element} \\ u, v \in U \Rightarrow u \cdot v \in U & \text{abgeschlossen} \\ u \in U \Rightarrow u^{-1} \in U & \text{inverses Element} \end{array}\right\} \Rightarrow \begin{cases} U \text{ ist Untergruppe} \\ U \leq G \end{cases}$$

Von Elementen erzeugten Untergruppen

$\langle a \rangle = \{a^k \mid a \in G,\ k \in \mathbb{Z}\}$

- $e \in \langle a \rangle$
- $a^k, a^l \in \langle a \rangle \Rightarrow a^k \cdot a^l = a^{k+l} \in \langle a \rangle$
- $a^k a^{-k} = a^0 = e$

Ordnung eines Elements

$(G, \cdot)$ Gruppe $\to a \in G$

$\to O(a) = |\langle a\rangle| = \begin{cases} n \in \mathbb{N}, & \#\{a^k \mid k \in \mathbb{Z}\} \\ \infty, & sonst. \end{cases}$

$O(a) =$ kleinste Zahl n mit $a^n = e$

$\langle a\rangle = \{e, a, \ldots, a^{n-1}\}$

$O(a) = n$

<u>Satz über die Ordnung von Gruppenelementen:</u>

Es sei G eine Gruppe mit neutralem Element e, und es sei $a \in G$:

(a) Falls $O(a) = \infty$, dann: $a^i \neq a^j \ , \ i \neq j$.

(b) Falls $O(a) \in \mathbb{N}$, so gilt: $O(a) = u =$ kleinste natürliche Zahl, für die $a^n = e$ gilt.

$a^s = e \Leftrightarrow O(a)\Big|s$

Sätze von Lagrange und Euler

<u>Satz von Lagrange:</u>

G sei eine endliche Gruppe, $U \leq G$

Dann:

$$|U|\Big||G|$$

<u>Satz von Euler:</u>

$$a^{|G|} = e \quad \forall a \in G$$

Die Restklassen modulo n:

Gegeben: $n \in \mathbb{N}$

Betrachte: wähle $a \in \mathbb{Z}$

$$\overline{a} = \{a + nz \mid z \in \mathbb{Z}\}$$

<u>Wir schließen</u> $a, b \in \mathbb{Z}$:

$a \equiv b(mod \ \ n)$, falls a, b den gleichen Rest bei Div durch n haben:

Es gilt:

$$\left.\begin{array}{l} a = qn + r \\ b = \tilde{q}n + r \end{array}\right\} \Leftrightarrow \left\{\begin{array}{ll} a - b & = (q - \tilde{q})n \\ & \Leftrightarrow n|(a-b) \\ & \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \\ & \Leftrightarrow \overline{a} = \overline{b} \end{array}\right.$$

Menge der Restklassen $\rightarrow \mathbb{Z}\Big|n\mathbb{Z} = \mathbb{Z}\Big|n = \mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

$|\mathbb{Z}_n| = n$

<u>Addition:</u>

$\overline{k}, \overline{l} \in \mathbb{Z}$

$\rightarrow \overline{k} = \overline{l} = \overline{k+l}$

Ringe

Eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$ heißt ein Ring falls gilt:

- $(R, +)$ ist abelsche Gruppe
- $\cdot$ ist assoziativ
- Distributivgesätze $a(b+c) = ab + ac$ und $(a+b)c = ac + bc \forall a, b, c \in R$
- $\exists$ Einselement: $1 \in R$: $1 \cdot a = a = a \cdot 1 \quad \forall a \in R$

Einheitengruppe (= Gruppe der invertierbaren Elemente)

Gegeben: Ring $(R, +, \cdot)$

$R^\times = \{a \in R \,|\, a \text{ ist invertierbar}\} = \{a \in R \,|\, \exists b \in R : ab = 1 = ba\}$

$R^\times$ ist die Einheitengruppe von R

Prime Restklassengruppen

$$\begin{aligned} n \in \mathbb{N} \to \mathbb{Z}_n^\times &= \{\overline{a} \text{ ist invertierbar}\} \\ &= \{\overline{a} \in \mathbb{Z}_n \,\big|\, \exists j \in \mathbb{Z}_n : \overline{a}j = 1\} \\ &= \{\overline{a} \in \mathbb{Z}_n \mid ggt(a, n) = 1\} \end{aligned}$$

$$a, b \text{ sind relativ prim/teilerfremd} \Leftrightarrow ggT(a, b) = 1$$

$(\mathbb{Z}_n, +, \cdot)$ ist körper $\Leftrightarrow n \in (\mathbb{P})$

$$\begin{array}{lll} \overline{a} \text{ invertierbar} & \Leftrightarrow \exists \overline{b} \in \mathbb{Z}_n & : \overline{a}\overline{b} = \overline{1} \\ & \Leftrightarrow \exists b \in \mathbb{Z} & : (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \\ & \Leftrightarrow \exists b \in \mathbb{Z} & : n \big| ab - 1 \\ & \Leftrightarrow \exists b \in \mathbb{Z}\ \exists x \in \mathbb{Z} & : ab - 1 = nx \\ & \Leftrightarrow \exists b \in \mathbb{Z}\ \exists x \in \mathbb{Z} & : ab - nx = 1 \\ & \Rightarrow & ggT(a, n) = 1 \end{array}$$

Euklidischer Algorithmus

$a_1 = a,\ a_2 = b \mid b > 0$

Sukzessive Division mit Rest:

$$\begin{array}{rcccll} a_1 & = & q_1 a_2 & + & a_3 & , 0 < a_3 < a_2 \\ a_2 & = & q_2 a_3 & + & a_4 & , 0 < a_4 < a_3 \\ \vdots & = & \vdots & + & \vdots & \quad \vdots \\ a_{n-2} & = & q_{n-2} a_{n-1} & + & a_n & , 0 < a_n < a_{n-1} \\ a_{n-1} & = & q_{n-1} a_n & + & 0 & \nwarrow \underline{a_n = ggT(a_1, a_2)} \end{array}$$

$\exists r, s \in \mathbb{Z} : ra + sb = a_n \quad \Leftarrow$ erweiterter euklidischer Algorithmus

Eulersche φ-Funktion:

Man nennt $\varphi(n) = \#\{a \in \{1, \ldots, n\} \mid ggT(a, n) = 1\}$

$\varphi(n) = \left|\mathbb{Z}_n^\times\right|$

$\varphi(p) = p - 1 \quad \forall p \in \mathbb{P}$

kleiner Satz von Fermat

Es sei $p \in \mathbb{P}$ dann gilt: $\forall a \in \mathbb{Z} : a^p \equiv a(mod\, p)$

Das Pohlig Hellman Verfahren

$$\underline{p = \text{(große) Primzahl} \;\Big\|\; \mathcal{N} = \text{ Klartext} \mid \mathcal{N} \in \mathbb{Z}_p^\times \;\Big\|\; e, d = \text{ Schlüssel}}$$

Wähle $e \in \mathbb{N}$ mit $ggT(e, p-1) = 1$

Bestimme d mit:

$$\begin{aligned} ed &\equiv 1(mod\, p-1) \\ ed &= 1 + r(p-1) \\ 1 &= ed - r(p-1) \end{aligned}$$

$$\Rightarrow \text{euklidischer Algorithmus}$$

Verschlüsseln:

$$\mathcal{C} = \mathcal{N}^e$$

Entschlüsseln:

$$\mathcal{C}^d = (\mathcal{N}^e)^d = \mathcal{N}^{ed} = \mathcal{N}^{1+r(p-1)} = \mathcal{N}^1 \cdot (\mathcal{N}^{(p-1)})^r \overset{\text{Satz von Euler - Fermat}}{\equiv} N$$

Wähle p am besten mit $\frac{p-1}{2}$ auch prim $\leftarrow$ sichere Primzahl

RSA-Verfahren:

Vorbereitung des Empfängers (Erzeugers der Schlüssel):

1. wähle große $p, q \in \mathbb{P} \;:\; p \neq q$ und $p \pm 1, q \pm 1$ müssen große Primteiler haben
2. setze $n = p \cdot q$
3. $\left|\mathbb{Z}_n^\times\right| = \left|\{a \in \{1, \ldots, n\} \mid ggT(a, n) = 1\}\right| = \varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$
4. wähle $e \in \{1, \ldots, n\} \;:\; ggT(e, \varphi(n)) = 1$

5. berechne $d\ :\ e \cdot d \equiv 1 (mod\ \varphi(n))$
6. veröffentliche Schlüssel (n, e)

Verschlüsselung des Senders:

$$\mathcal{C} \equiv \mathcal{N}^e\ (mod\ n)$$

Entschlüsselung des Empfängers:

$$\mathcal{N} \equiv \mathcal{C}^d\ (mod\ n)$$

Vektorräume

Körper

Ein Ring K $(K, +, \cdot)$ mit:

1. K ist kommutativ
2. $\exists$ Einselement $1\ :\ 1 \cdot \lambda = \lambda = \lambda \cdot 1 \quad \forall \lambda \in K$
3. Jedes $\lambda \neq 0$ ist invertierbar $\Leftrightarrow\ K^\times = K \setminus \{0\}$

V heißt ein K-Vektorraum falls $\forall \lambda, \mu \in K\ ,\ \forall u, v, w \in V\ :$

$$\left.\begin{array}{l} 1.\ v + w \in V\ ,\ \lambda \cdot v \in V \\ 2.\ u + (v + w) = (u + v) + w \\ 3.\ \exists 0 \in V\ :\ 0 + v = v \\ 4.\ \exists v' \in V\ :\ v + v' = 0 \\ 5.\ u + v = v + u \end{array}\right\} (V, +)\ :\ \text{abelsche Gruppe}$$

$$\left.\begin{array}{l} 6.\ \lambda(u + v) = \lambda u + \lambda v \\ 7.\ (\lambda + \mu)v = \lambda v + \mu v \\ 8.\ (\lambda\mu)v = \lambda(\mu v) \\ 9.\ 1v = v \end{array}\right\} \quad \text{Verträglichkeitsgesetze}$$

Sprechweisen und Regeln

Vektor: Element eines Vektorraumes

Nullvektor: 0-Element des Vektorraumes

Entgegengesetzte Vektoren (Negative): $-v \quad \rightarrow w + (-v) = w - v$

$K = \mathbb{R}$: reeller Vektorraum

$K = \mathbb{C}$: komplexer Vektorraum

$\lambda \in K$: Skalare

3 Regeln:

$0 \cdot v = (0+0) \cdot v = 0 \cdot v + 0 \cdot v \ \big| - (0v)$

$0 = 0 \cdot v$

$\lambda \cdot 0 = \lambda(0+0) = \lambda \cdot 0 + \lambda \cdot 0$

$0 = \lambda \cdot 0$

$\lambda \cdot v = 0 \iff \lambda = 0 \vee v = 0$

Untervektorräume

V sei ein K-Vektorraum

$U \subseteq$ heißt Untervektorraum, falls U wieder ein K-Vektorraum ist

d.h.

- $0 \in U$
- $u, v \in U \Rightarrow u + v \in U$
- $\lambda \in K, u \in U \Rightarrow \lambda u \in U$

Linearkombinationen

$v_1, \ldots, v_n \in V \ , \ \lambda_1, \ldots, \lambda_n \in K$

wenn gilt:

$$v = \lambda_1 v_1 + \ldots + \lambda_n v_n = \sum_{i=1}^{n} \lambda_i v_i \in V$$

ist v eine Linearkombination von $v_1, \ldots, v_n$

Das Erzeugnis von X

Geg.: V : K-Vektorraum $\quad x \subseteq V$

$$\begin{array}{rcl} Setze: \langle X \rangle & = & lin(X) = span(X) \\ & = & \left\{ \sum_{i=1}^{n} \lambda_i v_i \,\middle|\, \lambda_i \in K,\ v_i \in X,\ n \in \mathbb{N} \right\} \\ & = & Kv_1 + \ldots + Kv_n \\ & = & \text{Menge aller endlichen Linearkombinationen von Elementen aus } X \\ & = & \text{Erzeugnis von } X \\ & = & \text{lineare Hülle von } X \end{array}$$

- $\langle X \rangle \leq V \leftrightarrow \langle X \rangle$ ist ein Untervektorraum von V

Definition:

$X = \emptyset \to \langle \emptyset \rangle = \{0\}$

Lineare Unabhängigkeit:

Geg.: K-Vektorraum V

$v_1, \ldots, v_n \in V$ heißen linear unabhängig, falls:

$\forall T \subsetneq \{v_1, \ldots, v_n\} \Rightarrow \langle T \rangle \subsetneq \langle v_1, \ldots, v_n \rangle \leftarrow$ "keins unnötig"

Das Kriterium für lineare Unabhängigkeit:

Gegeben: $v_1, \ldots, v_n \in V$, $0_v \in V$

Ansatz:

$$\lambda_1 v_1 + \ldots + \lambda_n v_n = 0_v$$

Falls:

$$\exists_1 \text{Lsg.} \Rightarrow v_1, \ldots, v_n \text{ linear unabhängig}$$