Kleiner Satz FERMAT:

i) $a^p =_p a$; ii) $a^{p-1} =_p 1$

Binomischer Lehrsatz

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^n$

$\rightsquigarrow (a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

RSA

① $n = pq$; $\varphi = (p-1)(q-1)$, $ggT(e, \varphi) = 1$

② d: erweitert. EUKLID: $de =_\varphi 1$

③ $S_o = (e, n)$, $S_p = (d, n)$

④ encr.: $C = M^e \bmod n$

decr.: $M = C^d \bmod n$

GEOMETRIE

$\cos(\alpha) = \frac{|\langle a|b\rangle|}{\|a\| \cdot \|b\|}$

! $\cos(\alpha + \frac{\pi}{2}) = \sin(\alpha)$

Abstände

$d(p, g) = \|u \times (q - p)\|$, iff $\|u\| = 1$

Konstruktion ONB

$a \nparallel b$, $\mathcal{B} = \{a, \|a\|^2 b - \langle a|b\rangle b, a \times b\}$

ADDITIONSSÄTZE

$\sin(\alpha+\beta) = \cos(\alpha)\sin(\beta) + \cos(\beta)\sin(\alpha)$

$\cos(\alpha+\beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$

$\tan(\alpha+\beta) = \frac{\tan(\alpha) + \tan(\beta)}{1 - \tan(\alpha)\tan(\beta)}$

$\sin^2(\alpha) + \cos^2(\alpha) = 1$

$\mathbb{C}$ $z := a + bi$, $w := c + di$

Division DF: $\frac{z}{w} = \frac{z\overline{w}}{|w|}$

$\overline{w}w = |w|$, $|w| = \sqrt{c^2 + d^2} \in \mathbb{R}$

$\overline{z} = a - bi = |z| e^{-i\varphi}$

Polardarstellung

$z = |z| e^{i\varphi} = |z|(\cos(\varphi) + i\sin(\varphi))$

$\varphi = v(b) \cos\left(\frac{a}{|z|}\right)$, $v(b) \hat{=}$ Vorzeichen(b)

$\mathrm{Re}(z) = \cos(\varphi) = \frac{1}{2}(e^{i\varphi} + e^{-i\varphi})$

$\mathrm{Im}(z) = \sin(\alpha) = \frac{1}{2i}(e^{i\varphi} + e^{-i\varphi})$

n-te Wurzel in $\mathbb{C}$

Einheitswurzeln: $u_k = e^{i\frac{k}{\pi} 2\pi}$, $0 < k < n-1$

$w_0 = \sqrt[n]{|z|} \cdot e^{i\frac{\varphi}{n}}$

$w_k = u_k \cdot w_0$

Quadratwurzel $(z)^{\frac{1}{2}}$ in $\mathbb{C}$

$w_0 = \sqrt{\frac{1}{2}(|z| + a)} + i v(b) \sqrt{\frac{1}{2}(|z| - a)}$

CARDANISCHE FORMELN

$x^3 + bx^2 + cx + d = 0$

① $x = y - \frac{b}{3} \rightsquigarrow y^3 + px + q = 0$

$p := c - \frac{b^2}{3}$, $q = \frac{2}{27} b^3 - \frac{1}{3} bc + d$

② $\Delta := \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$

(3.1) $\Delta > 0$: 1 Lösung $\in \mathbb{R}$

$y = \sqrt[3]{\sqrt{\Delta} - \frac{q}{2}} - \sqrt[3]{\sqrt{\Delta} + \frac{q}{2}}$

(3.2) $\Delta = 0$: 2 Lösungen $\in \mathbb{R}$

$y_1 = \frac{3q}{p}$, $y_{2/3} = \frac{3q}{2p}$

(3.3) $\Delta < 0$: 3 Lösungen $\in \mathbb{R}$

$\varphi = \frac{1}{3} \arccos\left(-\frac{q}{2} \cdot \frac{27}{|p|^3}\right)$

!! φ auf mind. 4 Nachkommastellen genau!!

$y_1 = 2\sqrt{\frac{|p|}{3}} \cdot \cos(\varphi)$

$y_{2/3} = -2\sqrt{\frac{|p|}{3}} \cdot \cos\left(\varphi \pm \frac{\pi}{3}\right)$

VEKTORRÄUME

$\langle a|b\rangle = \sum_{k=1}^{n} \overline{a}_k b_k$, $\langle ta + sb|c\rangle = \overline{t}\langle a|c\rangle - \overline{s}\langle b|c\rangle$

$\|a\| = \sqrt{\langle a|a\rangle}$

MATRIZEN

$A = [a_1, a_2, \dots a_n] = \begin{bmatrix} a_1^t \\ a_2^t \\ \vdots \\ a_n^t \end{bmatrix}$

$n \times m \rightsquigarrow n \updownarrow, \overset{m}{\leftrightarrow}$

Kippregel: $Ax = \sum_{k=1}^{n} x_k a_k = \begin{bmatrix} \langle a_1^t|x\rangle \\ \langle a_2^t|x\rangle \\ \vdots \\ \langle a_n^t|x\rangle \end{bmatrix}$

Operationen

$BA = [Ba_1, Ba_2, \dots, Ba_n] \neq AB$; $AA^{-1} = \mathbb{1}$

$A^* = \overline{A^t}$, A^t Spiegelung an Diagonale

Inverse: $\mathbb{K}^n$: GAUSS $\boxed{A \mid \mathbb{1}} \longrightarrow \boxed{\mathbb{1} \mid A^{-1}}$

$\mathbb{R}^3$: $A^{-1} = \frac{1}{\det(A)} [a_2^t \times a_3^t, a_3^t \times a_1^t, a_1^t \times a_2^t]$

Determinante

$\det(AB) = \det(A) \cdot \det(B) \rightsquigarrow \det(A^{-1}) = \frac{1}{\det(A)}$

SARRUSsche Regel: $\searrow = \oplus$, $\nearrow = \ominus$

$\det(A) \neq 0 \Leftrightarrow A$ bijektiv $\Leftrightarrow \{a_1, a_2, \dots a_n\}$ lin. unabhängig

$\det(A) > 0 \Leftrightarrow$ positiv orientiert (ist gut)

$\det(A) < 0 \Leftrightarrow$ negativ orientiert (ist blöd)

Matrizen als ONB

$B^{-1} = B^*$

$x_B = B^* x$; $x = B x_B$

DREHUNG

$D_{1\alpha} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{bmatrix}$ $D_{2\alpha}$ sucked → nicht benötigt

$x' = B D_{n\alpha} B^* x$