

Lineare Algebra

Skalarprodukt

$$\langle \vec{x} | \vec{y} \rangle = \|\vec{x}\| * \|\vec{y}\| * \cos \angle(\vec{x}, \vec{y})$$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} * \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = x_1 y_1 + x_2 y_2 + x_3 y_3$$

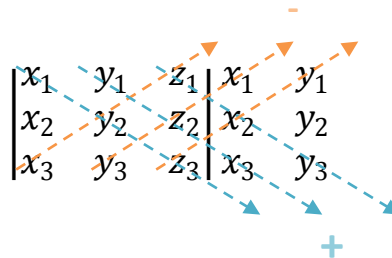
Kreuzprodukt

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \times \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_2 y_3 - x_3 y_2 \\ x_3 y_1 - x_1 y_3 \\ x_1 y_2 - x_2 y_1 \end{pmatrix}$$

Spatprodukt

$$(\vec{x} \times \vec{y}) * \vec{z}$$

Regel von Sarrus



$$x_1 y_2 z_3 + y_1 z_2 x_3 + z_1 x_2 y_3 - x_3 y_2 z_1 - y_3 z_2 x_1 - z_3 x_2 y_1$$

Nur $R^3!$

Determinante Entwickeln

$$\sum_{j=1}^n (-1)^{k+j} a_{kj} \det(\tilde{A}_{k,j})$$

Matrixprodukt

$$\begin{bmatrix} -1 & 2 \\ 2 & -3 \\ 2 & -2 \end{bmatrix} * \begin{bmatrix} 2 & -4 & 1 \\ 3 & 0 & -1 \end{bmatrix} = \begin{bmatrix} -3 & -4 & -3 \\ -7 & -4 & 4 \\ -4 & -4 & 3 \end{bmatrix}$$

$3 * \boxed{2 \quad 2} * 3 \qquad \qquad \qquad 3 * 3$

Kern/Rang/Dimension

$$\ker(A) = \{ \vec{x} : A\vec{x} = \vec{0} \}$$

$$\dim(A) = m * n$$

Wenn Matrix m x n

$$Rg(A) = \dim(\text{im}(A))$$

Maximale Anzahl linear unabhängiger Spalten von A
 (Gauß bis Ende, übrig gebliebene)

$$Rg(A) + \dim(\ker(A)) = n$$

n = Zahl der Variablen

Lineare Optimierung

Simplex -Algorithmus

1. Zielfunktion z=...
 - a. z-...=0
2. Nebenfunktionen => Schlupfvariablen
3. Negativsten Koeffizienten
4. Pivot Zeile
5. Rest Nullen

Diskrete Mathematik

Erweiterter euklidischer Algorithmus

$ggT(721,448)$:

$$\begin{aligned} 721 &= 1 \cdot 448 + 273 \\ 448 &= 1 \cdot 273 + 175 \\ 273 &= 1 \cdot 175 + 98 \\ 175 &= 1 \cdot 98 + 77 \\ 98 &= 1 \cdot 77 + 21 \\ 77 &= 3 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

$$\Rightarrow ggT(721,448) = 7$$

$$d = a \cdot m + b \cdot n$$

siehe Aufzeichnungen hinten

$$mx + my = k - \text{analog}$$

Primzahlen

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Primzahlen:

2	3	5	7
11	13	17	19
23	29	31	37
41	43	47	53
59	61	67	71
73	79	83	89
97	101	103	107
109	113		

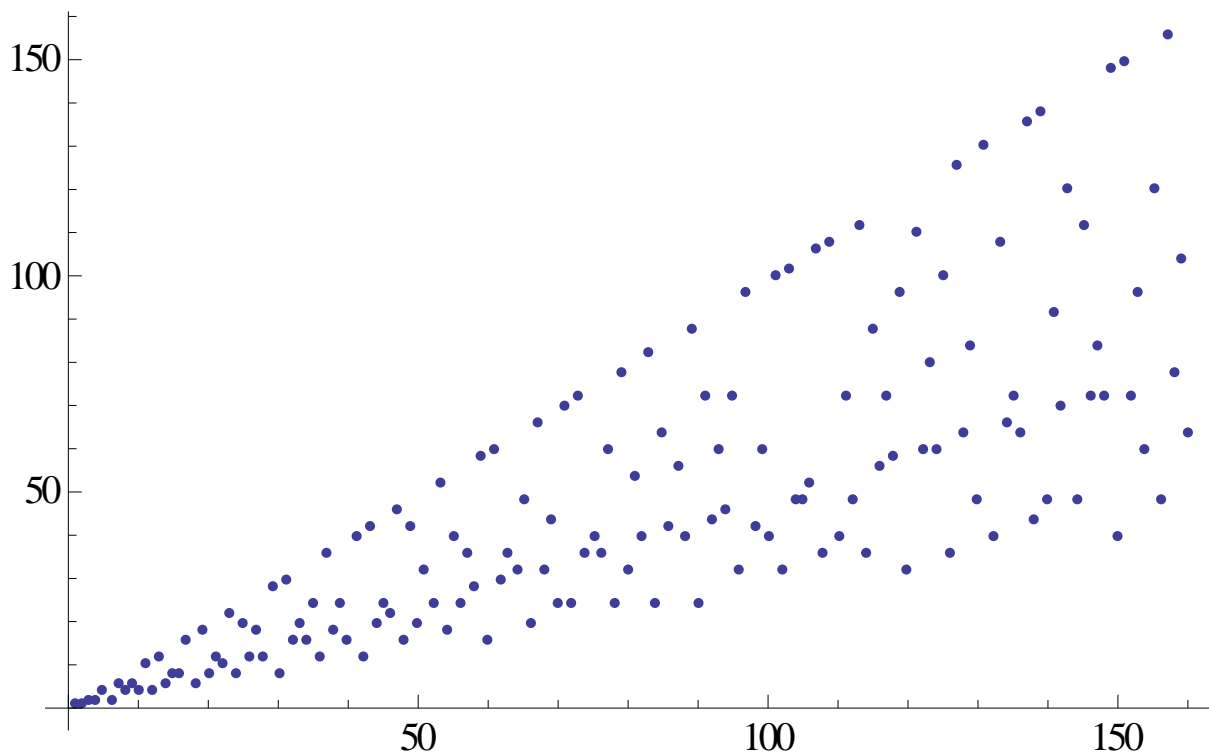
$p = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541\}$

Primfaktorzerlegung

Zur Gewinnung der Primfaktorzerlegung geht man gewöhnlich die Primzahlen von unten (d.h. 2, 3, 5, 7...) durch und prüft, ob die zu zerlegende Zahl durch sie ohne Rest glatt teilbar ist. In diesem Fall schreibt man die Primzahl auf, teilt die zu zerlegende Zahl durch die Primzahl und macht mit dem Ergebnis (dem Quotienten) weiter, bis am Schluß nur noch eine Primzahl übrig bleibt.

Eulersche φ -Funktion

$$\varphi(n) = n * \left(1 - \frac{1}{p_1}\right) * \dots * \left(1 - \frac{1}{p_k}\right)$$



RSA-Algorithmus

Erzeugung des Schlüsselpaares

1. 2 Primzahlen ($p = 11, q = 13$)
2. RSA Modul: $N = p * q = 143$
3. $\varphi(N) = \varphi(143) = 120$
4. Zahl e muss zu 120 teilerfremd sein. Hier $e = 23 \Rightarrow$ Öffentlicher Schlüssel: $e = 23, N = 143$
5. Berechnung der Inversen zu e :

$$e * d + k * \varphi = 1 = \text{ggT}(e, \varphi(N))$$

$$23 * d + k * 120 = 1 = \text{ggT}(23, 120)$$

6. Mit euklidischen Algorithmus d und k berechnen, d privater Schlüssel, k nicht benötigt

Verschlüsseln von Nachrichten

$$C = K^e \text{ mod } N$$

Entschlüsseln

$$K = C^d \text{ mod } N$$