Euclidischer Algorithmus

$a, b \in \mathbb{N}_0 \quad a \geq b \geq 0$

Ziel: berechne $ggT(a, b)$

Algo: Ist $b = 0$, dann gib a als $ggT(a, b)$ aus

sonst: gib $ggT(b, a \; mod \; b)$ aus

Beispiel:

$a = 2406, \quad b = 654$

$$\begin{aligned}\boxed{ggT(2406, 654)} &= ggT(654, \underbrace{2406 \; mod \; 654}_{444}) \\ &= ggT(654, 444) = ggT(\underset{"a"}{444}, \underset{"b"}{210}) \\ &= ggT(210, 24) = ggT(24, 18) \\ &= ggT(18, 6) = ggT(6, 0) = \boxed{6}\end{aligned}$$

Satz:

$$ggT(a, b) = min\{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$$

D.h. auf unser Beispiel: $\exists x, y \in \mathbb{Z}$ mit:

$$6 = 2406x + 654y$$

Wie finden wir x und y?

$$\begin{aligned}\overset{a_1}{2406} &= 3 \cdot \overset{b_1}{654} + \overset{r_1}{444} \\ \overset{a_2}{654} &= 1 \cdot \overset{b_2}{444} + \overset{r_2}{210} \\ \overset{a_3}{444} &= 2 \cdot \overset{b_3}{210} + \overset{r_3}{24} \\ \overset{a_4}{210} &= 8 \cdot \overset{b_4}{24} + \overset{r_4}{18} \\ \overset{a_5}{24} &= 1 \cdot \overset{b_5}{18} + \overset{r_5}{6} \\ \overset{a_6}{18} &= 3 \cdot \overset{b_6}{6} + \overset{r_6}{0}\end{aligned}$$

Ziel: $6 = 2406 \cdot x + 654 \cdot y$

$$
\begin{aligned}
6 &= 24 - 1 \cdot 18 \\
18 &= 210 - 8 \cdot 24 \\
\hline
6 &= 24 - 1 \cdot (210 - 8 \cdot 24) \\
&= 9 \cdot 24 - 1 \cdot 210 \\
&= 9 \cdot (\underbrace{444 - 2 \cdot 210}_{24}) - 1 \cdot 210 \\
&= 9 \cdot 444 - 19 \cdot 210 \\
&= 9 \cdot 444 - 19 \cdot (654 - 1 \cdot 444) \\
&= 28 \cdot 444 - 19 \cdot 654 \\
&= 28 \cdot (2406 - 3 \cdot 654) - 19 \cdot 654 \\
&= 28 \cdot 2406 - 84 \cdot 654 - 19 \cdot 654 \\
&= \underbrace{28}_{=x} \cdot 2406 - \underbrace{(-103)}_{=y} \cdot 654
\end{aligned}
$$

$ggT(3.8) = 1$

$$
\begin{aligned}
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 2 = 3 - (8 - 2 \cdot 3) \\
&= \underset{x}{3} \cdot 3 + \underset{y}{(-1)} 8
\end{aligned}
$$

In $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ rechnen wir modulo n.

Frage: Gegeben $x \in \mathbb{Z}_n$

Ist x bez. der Multiplikation invertierbar?

Antwort: x invertierbar $\Leftrightarrow ggT(x, n) = 1$

Spezialfall: Ist n eine Primzahl, so ist jedes Element $x \in \mathbb{Z}_n,\ x \neq 0$, invertierbar (bez. der Mult.)

Für n prim/Primzahl:

es gibt genau $n - 1$ invertierbare Elemente in $\mathbb{Z}_n$

Fall n keine Primzahl:

Wie viele invertierbare Elemente gibt es in $\mathbb{Z}_n$ dann?

Kominatorik: Abzählprinzipien/-tricks

Im Folgenden befassen wir uns mit endlichen Mengen.

Für eine Menge X, steht $|X|$ für die Anzahl der Elemente in X.

Regeln:

1) Bijektionsregel: Zwei endlichen Mengen A und B haben dieselbe Anzahl der Elemente ($|A| = |B|$) genau dann, wenn es eine Bijektion $\varphi : A \to B$ gibt.

   Erinnerung (Übung):

   Sind $|A| = |B| < \infty$ dann gilt:

   Jede Injektion $\varphi : A \to B$ ist auch eine Surjektion und somit eine Bijektion.

2) Summenregel: Sind $A_1, ..., A_n$ endliche, paarweise disjunkte Mengen

   (d.h. für alle $a \neq j : A_i \cap A_j = \emptyset$) dann gilt

$$\left| \dot{\bigcup_{i=1}^{n}} A_i \right| = \sum_{i=1}^{n} |A_i|$$

   Erinnerung an die Schreibweise:

   $\dot{\bigcup}_{i=1}^{n} A_i$ für Vereinigung paarweise disjunkter Mengen

3) Produktregel: Sind $A_1, ..., A_n$ endliche Mengen, so gilt:

$$\left| \prod_{i=1}^{n} A_i \right| = \prod_{i=1}^{n} |A_i|$$

   wobei

$$\prod_{i=1}^{n} A_i := \{(a_1, a_2, ..., a_n) : \forall i \in \{1, ..., n\} \text{ gilt: } a_i \in A_i\}$$

   das kartesische Produkt von $A_1, ..., A_n$

Beispiele:

1.) $A_1 = A_2 = ... = A_n = \{0, 1\}$

$$\prod_{i=1}^{n} A_i = \prod_{i=1}^{n} \{0, 1\} = \{0, 1\}^n$$

   (Erinnerung: sind alle $A_i = A$, so schreiben wir kurz A^n für $\prod_{i=1}^{n} A_i$)

   $|\{0, 1\}^n| = 2^n$

2.) X endliche Menge, $|X| = n \in \mathbb{N}$

(per Induktion: $|P(x)| = 2^{|X|} = 2^n$)

Im Folgenden geben wir eine Bijektion zwischen $P(X)$ und $\{0,1\}^n$ an und folgern wieder: $|P(X)| = |\{0,1\}^n| = 2^n$

$|X| = n,\ X = \{x_1, ..., x_n\}$

$$\varphi : \begin{cases} P(X) \to \{0,1\}^n \\ A \mapsto (a_1, ..., a_n) \end{cases}$$

wobei $a_i = 1 \Leftrightarrow x_i \in A \qquad \forall i \in \{1, ..., n\}$

Falls $X = \{\underset{x_1}{1}, \underset{x_2}{2}, \underset{x_3}{3}, \underset{x_4}{4}\}$

$\varphi(\{2,3\}) = (0,1,1,0)$

Beh: φ ist bijektiv

i) φ injektiv: $A, B \in P(X)$

$\varphi(A) = \varphi(B) = (a_1, ..., a_n)$ d.h. für jedes $i \in \{1, ..., n\}$ gilt:

$$a_i = 1 \Leftrightarrow x_i \in A$$

$$\Updownarrow$$

$$x_i \in B$$

Also: $\forall i \in \{1, ..., n\} : x_i \in A \Leftrightarrow x_i \in B$

d.h. $A = B$

ii) φ surjektiv:

Zu jeder $a = (a_1, ..., a_n) \in \{0,1\}^n$

$$A := \{x_i : a_i = 1\}$$

X, Y Mengen (endlich)

$X = \{x_1, ..., x_m\} \quad Y = \{y_1, ..., y_n\} \quad m, n \in \mathbb{N}$

$S \subseteq X \times Y$

Ziel: $|S| = ?$

Prinzip vom Doppelten Abzählen

	y_1	y_2	y_3	...	y_j	y_n
x_1						
x_2				0		
...						
x_i				1		
x_m						

Wir schreiben in die Tabelle 1 in die Zeile x_i und Spalte y_j genau dann, wenn $(x_i, y_j) \in S$. (Sonst schrebien wir 0)

Beispiel:

$X = \{a, b\}, \quad Y = \{1, 2, 3\}, \quad S = \{(a, 1), (a, 3), (b, 2)\}$

	1	2	3
a	1	0	1
b	0	1	0

Für $x \in X$ schreiben wir

$$r_x(S) := |\{y : y \in Y, (x, y) \in S\}|$$

= Anzahl der 1'en in der Zeile x

$$\begin{pmatrix} r_a(S) = 2 \\ r_b(S) = 1 \end{pmatrix} \quad r =' row'$$

Für $y \in Y$ schreiben wir:

$$c_y(S) := |\{x : x \in X, (x, y) \in S\}|$$

= Anzahl der 1'en in der Spalte y

$c =' column'$

$c_1(S) = 1$

$c_2(S) = 1$

$c_3(S) = 1$

Prinzip des doppelten Abzählens:

$$|S| = \overset{\text{Summe über alle Zeilen der Tabelle}}{\sum_{x \in X} r_x(S)} = \overset{\text{Summe über alle Spalten}}{\sum_{y \in Y} c_y(S)}$$

Bem:

1)

$$\sum_{x \in X} r_x(S) = \sum_{i=1}^{m} r_{x_i}(S)$$

$$\sum_{y \in Y} c_y(S) = \sum_{j=1}^{n} c_{y_j}(S)$$

2) Stehen in jeder Zeile r Einsen und in jeder Spalte c Einsen, so gilt:

$$r \cdot |X| = c \cdot |Y|$$

Eulersche Funktion

Leonard Euler (1707-1783)

Für $n \in \mathbb{N}$ definieren wir

$$\varphi(n) := (\{x : x \in \{1, ..., n\} \text{ und } ggT(x, n) = 1\})$$

= Anzahl der Elemente x, $1 \leq x \leq n$ mit $ggT(x, n) = 1$

n	1	2	3	4	5	6	7	8
$\varphi(n)$	1 1	1 1	2 1,2	2 1,3	4 1,2,3,4	2 1,5	6 1,2,3,4,5,6	4 1,3,5,7

Beobachtung:

$\varphi(n) = n - 1$, falls n Primzahl

$$\varphi(n) = |\{x \in \mathbb{Z}_n : x \text{ ist invertierbar bez. Multiplikation in } \mathbb{Z}_n \text{ modulo } n'\}|$$

$$\begin{aligned}
8 &= \overset{\varphi(8)}{4} + \overset{\varphi(4)}{2} + \overset{\varphi(2)}{1} + \overset{\varphi(1)}{1} \\
7 &= 6 + 1 \\
6 &= \overset{\varphi(6)}{2} + \overset{\varphi(3)}{2} + \overset{\varphi(2)}{1} + \overset{\varphi(1)}{1} \\
5 &= 4 + 1 \\
4 &= 2 + 1 + 1 \\
3 &= 2 + 1 \\
2 &= 1 + 1 \\
1 &= 1
\end{aligned}$$

Satz:

Sei $n \in \mathbb{N}$. Dann gilt:

$$\sum_{d : d|n,\ d \in \mathbb{N}} \varphi(d) = n$$

$$\sum_{d : P(d)}$$

$\rightarrow$ die Summe wird über alle Werte d gebildet, welche die Eigenschaft $P(d)$ besitzen.

Beweis:

Wir stellen eine Tabelle für die Menge $S \subseteq X \times Y$ auf, wobei:

$X := \{d : d \in \mathbb{N},\ d|n\}$= Teiler von n'

$Y := \{1, ..., n\} (=: [n])$

$S := \{(d, f) : d, f \in \mathbb{N}, d|n, d \leq f, ggT(f, d) = 1\}$

	1	2	...	d_i		n	
d_1							
d_2							
...							
d_i				1	0	0...	0
d_m							

$ggT(f, d_i) > 1$

Bsp: $n = 8$

"f"

"d"		1	2	3	4	5	6	7	8
	1	1	0	0	0	0	0	0	0
	2	1	0	0	0	0	0	0	0
	4	1	0	1	0	0	0	0	0
	8	1	0	1	0	1	0	1	0

Zeile: dort stehen alle Teiler von n

Spalte: $1, ..., n$

S besteht aus Paaren (d, f) mit $d \leq f$

$ggT(d, f) = 1$

$$|S| = \sum_{d \in X} r_{\substack{d \\ \varphi(d)}}(S)$$

Ziel:

Wir geben eine Bijektion von S in die Menge $[n] = \{1, 2, ..., n\}$an.

$\overset{\text{Bij.regel}}{\Rightarrow} \quad |S| = n = \sum_{d|n} \varphi(d)$

$$\varphi : \begin{cases} S \to [n] \\ (d, f) \mapsto \frac{nf}{d} \in [n], \text{ denn } f \leq d,\ d|n \end{cases}$$