$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Euklidscher Algorithmus EUKLID

Eingabe: Zahlen $m, n \in \mathbb{N}$ mit $m \leq n$

Ausgabe: Grösster gemeinsamer Teiler ggT(m, n)

if m teilt n **then**

    return m

else

    return EUKLID$(n \bmod m, m)$

Erweiterter Euklidscher Algorithmus ERWEITERTER-EUKLID

Eingabe: Zahlen $m, n \in \mathbb{N}$ mit $m \leq n$

Ausgabe: Zahlen $x, y \in \mathbb{Z}$ mit ggT$(m, n) = mx + ny$

if m teilt n **then**

  return $(1, 0)$

else

  $(x', y') \leftarrow$ ERWEITERTER-EUKLID$(n \bmod m, m)$

  $x \leftarrow y' - x' \cdot \lfloor \frac{n}{m} \rfloor; y \leftarrow x'$

  return (x, y)

Chinesischer Restsatz – Einfache Version

Für alle natürlichen Zahlen $m, n \in \mathbb{N}$ mit ggT$(m, n) = 1$ und alle $a \in \mathbb{Z}_m$ und $b \in \mathbb{Z}_n$ gibt es ein eindeutig bestimmtes $t \in \mathbb{Z}_{mn}$ so dass

$$\begin{aligned} t &\equiv a \mod m \qquad \text{und} \\ t &\equiv b \mod n. \end{aligned}$$

Chinesischer Restsatz – Allgemeine Version

Wenn $b_1, \ldots, b_k$ und $m_1, \ldots, m_k$ natürliche Zahlen sind mit ggT$(m_i, m_j) = 1$ für alle $1 \leq i < j \leq k$, dann gibt es genau ein $x \in \mathbb{Z}_{m_1 \cdot \ldots \cdot m_k}$ mit

$$x \equiv b_i \mod m_i \qquad \text{für alle } i = 1, \ldots, k.$$

Satz von Euler

Für alle $n \in \mathbb{N}$, $n \geq 2$ gilt:

$$a^{\phi(n)} \equiv 1 \pmod{n} \qquad \text{für alle } a \in \mathbb{Z}_n^*. \tag{1}$$

Satz von Fermat

Für alle $n \in \mathbb{N}$, $n \geq 2$ gilt:

$$n \text{ Primzahl} \qquad \Longleftrightarrow \qquad a^{n-1} \equiv 1 \bmod n \quad \text{für alle } a \in \mathbb{Z}_n \setminus \{0\}. \tag{2}$$