Der Chinesische Restsatz und die Euler'sche φ-Funktion

Erklärung

Der Chinesische Restsatz

Es seien $m_1, m_2, \ldots, m_k \in \mathbb{N}$ paarweise teilerfremd und $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Dann gibt es eine Lösung $a \in \mathbb{Z}$, welche alle Kongruenzen des folgenden Systems erfüllt:

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \\ x &\equiv a_k \mod m_k \end{aligned}$$

a ist eindeutig modulo $m := m_1 m_2 \cdots m_k$.
Die Lösungsmenge ist somit

$$\{a + k \cdot m : k \in \mathbb{Z}\}.$$

Erklärung

Die Lösung a hat die Form

$$a = a_1 \cdot e_1 + a_2 \cdot e_2 + \cdots + a_k \cdot e_k \ ,$$

wobei für die $e_1, \ldots, e_m$, gilt:

$$e_i \equiv \begin{cases} 1 & \mod m_i \\ 0 & \mod m_j, \text{ für alle } j \neq i. \end{cases}$$

Berechnung von e_i: Finde mit dem Erweiterten Euklidischen Algorithmus $s, t \in \mathbb{Z}$, sodass

$$s \cdot m_i + \underbrace{t \cdot \frac{m}{m_i}}_{= e_i} = 1.$$

Sind die Moduln $m_1, m_2, \ldots, m_k$ nicht teilerfremd, so kann es Lösungen geben, muss es aber nicht. In dem Fall existiert eine Lösung genau dann, wenn für alle $i \neq j$ gilt: $a_i \equiv a_j \mod \mathrm{ggT}(m_i, m_j)$.

Erklärung

Die Euler'sche φ-Funktion

Die Euler'sche φ-Funktion $\varphi(n)$ zählt die zu $n \in \mathbb{N}$ teilerfremden Zahlen:

$$\varphi(n) = |\{m \in \{1, \ldots, n\} : \mathrm{ggT}(m, n) = 1\}|$$

Rechenregeln:

- $\varphi(p) = p - 1$, falls p eine Primzahl ist.
- $\varphi(p^k) = p^{k-1}(p - 1)$, falls p eine Primzahl ist.
- $\varphi(m_1 \cdot m_2) = \varphi(m_1)\varphi(m_2)$, falls $\mathrm{ggT}(m_1, m_2) = 1$.

Aufgaben

Chinesischer Restsatz

Aufgabe 1. Lösen Sie das folgende System simultaner Kongruenzen mithilfe des Chinesischen Restsatzes:

$$\begin{aligned} x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 7 \\ x &\equiv 3 \mod 11 \end{aligned}$$

Lösung

Aufgabe 2. Oma Meier gießt ihre Blumen alle 3 Tage und leert das Katzenklo alle 5 Tage. Heute ist Dienstag und am folgenden Mittwoch bzw. Donnerstag sind die Blumen bzw. das Katzenklo an der Reihe. Wann fallen beide Tätigkeiten zum ersten Mal auf einen Freitag?

Eulersche φ-Funktion

Aufgabe 3. Berechnen Sie $\varphi(n)$ für die folgenden Werte von n:

a) $n = 7$ b) $n = 27$ c) $n = 80$ d) $n = 100$ e) $n = 132$

Lösung