

12. Übung

1. Wir definieren die Funktion $\Phi: \mathbb{N} \rightarrow \mathbb{N}$ durch $\Phi(n) =_{\text{def}} \#\{1 \leq a \leq n \mid \text{ggT}(a, n) = 1\}$ (Mit $\#$ wird wieder die Anzahl der Elemente in einer Menge bezeichnet).

Sei $k \geq 1$ und p eine Primzahl. Zeigen Sie, dass dann für Funktion Φ gilt:

$$\Phi(p^k) = p^{k-1}(p-1).$$

Verwenden Sie die Tatsache, dass $\Phi(n \cdot m) = \Phi(n) \cdot \Phi(m)$, wenn $\text{ggT}(n, m) = 1$, um die folgende Aussage zu beweisen:

$$\Phi(n) = n \prod_{\substack{p|n \\ p \text{ prim}}} \left(1 - \frac{1}{p}\right)$$

2. Berechnen Sie (oder Ihr Rechner) $\text{ggT}(235, 124)$ und die Lineardarstellung mit Hilfe des erweiterten euklidischen Algorithmus oder von Hand mit der in der Übung vorgestellten Methode.

Für den erweiterten Euklidischen Algorithmus definieren wir zunächst zwei Folgen $(x_k)_{k \in \mathbb{N}} = x_0, x_1, x_2, \dots$ und $(y_k)_{k \in \mathbb{N}} = y_0, y_1, y_2, \dots$ wie folgt induktiv:

(IA) $x_0 = 1, x_1 = 0, y_0 = 0$ und $y_1 = 1$

(IS)

$$\begin{aligned}x_{k+1} &= q_k x_k + x_{k-1} \\ y_{k+1} &= q_k y_k + y_{k-1}\end{aligned}$$

für $1 \leq k \leq n$, wobei $q_k = \lfloor r_{k-1}/r_k \rfloor$, $r_{k+1} = r_{k-1} \bmod r_k$, $r_0 = |a|$ und $r_1 = |b|$. Mit r_n bezeichnen wir das letzte Glied der Folge r_0, r_1, r_2, \dots , das ungleich 0 ist. Dann ergibt sich die Lineardarstellung zu

$$\text{ggT}(a, b) = (-1)^n a x_n + (-1)^{n+1} b y_n$$

3. In dieser Aufgabe betrachten wir die Restklassenringe $\mathbb{Z}_n, n \geq 2$ und die Menge aller *Quadrate* $\mathbb{S}_n \subseteq \mathbb{Z}_n \setminus \{0\}$, die wie folgt definiert ist:

$$\mathbb{S}_n = \{a \in \mathbb{Z}_n \setminus \{0\} \mid \text{es gibt ein } x \in \mathbb{Z}_n, \text{ sodass } x^2 \equiv a \pmod{n}\}$$

Analog definieren wir die Menge der Nichtquadrate:

$$\mathbb{T}_n = \{a \in \mathbb{Z}_n \setminus \{0\} \mid \text{es gibt kein } x \in \mathbb{Z}_n, \text{ sodass } x^2 \equiv a \pmod{n}\}$$

- i) Geben Sie die Mengen \mathbb{S}_{11} und \mathbb{T}_{11} explizit an.

- ii) Zeigen Sie: Das Produkt zweier Quadrate in \mathbb{Z}_n ist wieder ein Quadrat in \mathbb{Z}_n .
 - iii) Ist das Produkt zweier Nichtquadrate wieder ein Nichtquadrat? Belegen Sie Ihre Aussage!
 - iv) Sei p eine Primzahl. Überprüfen Sie, dass (\mathbb{S}_p, \cdot) eine kommutative Gruppe bildet, wobei „ \cdot “ die normale Restklassenmultiplikation ist.
4. Diese Aufgabe sollte durch „einfaches Hinsehen“ lösbar sein. Sei die folgenden Rekurrenz $T: \mathbb{N} \rightarrow \mathbb{N}$ gegeben:

$$\begin{aligned} T(0) &=_{\text{def}} 1 \\ T(n) &=_{\text{def}} T(n-1) + (2n+1) \end{aligned}$$

Geben Sie die Werte von $T(1)$, $T(2)$, $T(3)$ und $T(4)$ direkt an, und bestimmen Sie eine Funktion $f(n)$, die das Funktionensymbol T nicht enthält, so dass $T(n) = f(n)$ gilt. Beweisen Sie die Korrektheit Ihrer Vermutung.

Besprechung in der Übung am 4. Februar 2016.