Hochschule RheinMain
Prof. Dr. Steffen Reith

10. Übung

1. Sei $\mathcal{R} = (R, +, \cdot)$ ein beliebiger kommutativer Ring mit dem Nullelement $0_\mathcal{R}$. Zeigen Sie, dass für ein beliebiges Ringelement $x \in R$ dann $x \cdot 0_\mathcal{R} = 0_\mathcal{R}$ gilt. Wir nennen ein Ringelement $a \neq 0_\mathcal{R}$ *Nullteiler*, wenn es ein $b \neq 0_\mathcal{R}$ mit $a \cdot b = 0_\mathcal{R}$ gilt. Zeigen Sie, dass jeder Körper keine Nullteiler besitzt.

2. Zeigen Sie, dass $\mathbb{Z}_n$ genau dann ein Körper ist, wenn n eine Primzahl ist.

3. Wir definieren die Funktion $\Phi\colon \mathbb{N} \to \mathbb{N}$ 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:

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

4. Berechnen Sie (oder Ihr Rechner) $\text{ggT}(235, 124)$ und die Lineardarstellung mit Hilfe des erweiterten euklidischen Algorithmus oder von Hand (überlegen Sie sich evtl. eine eigene systematische Vorgehensweise).

   Für den erweiterten Euklidischen Algorithmen definieren wir zunächst zwei Folgen $(x_k)_{k\in\mathbb{N}} = x_0, x_1, x_2, \ldots$ und $(y_k)_{k\in\mathbb{N}} = y_0, y_1, y_2, \ldots$ 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 $r_0, r_1, r_2, \ldots$, das ungleich 0 ist. Dann ergibt sich die Lineardarstellung zu

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

5. Verwenden Sie den kleinen Satz von Fermat, um das Inverse von 2 in Z_{31} zu berechnen.

Besprechung in der Übung am 17. Februar 2018.