H23-T3-A4

a) Seien p eine ungerade Primzahl und $n \geq 1$. Zeigen Sie, dass die Gleichung $x^2 = 1$ in $R = \mathbb{Z}/p^n\mathbb{Z}$ genau zwei Lösungen hat.

b) Betsimmen Sie alle Lösungen der Gleichung $x^2 = 1$ im Ring $\mathbb{Z}/2023\mathbb{Z}$
Hinweis: $2023 = 7 \cdot 17^2$.

Lösung

a) Da p ungerade ist, ist $1 \neq -1 \in R$, daher sind -1 und 1 Lösungen für $x^2 = 1$. Wir müssen nun noch zeigen, dass das die einzigen beiden Lösungen sind. Wir erinnern zunächst an das folgende Resultat aus der Zahlentheorie:

$$\text{Für } n = p^k \text{mit } p \text{ ungerade gilt } ((\mathbb{Z}/n\mathbb{Z})^\times, \cdot) \cong (\mathbb{Z}/\phi(n), +),$$

wobei ϕ die eulersche Phi-Funktion ist. Nehmen wir nun an es existiert $\alpha \in R - \{\pm 1\}$ mit $\alpha^2 = 1$, dann folgt $\alpha \in R^\times$. Zudem folgt aus $\alpha \neq 1$ und $\alpha^2 = 1$, dass $\text{ord}(\alpha) = 2$. Da jedoch $\text{ord}(-1) = 2$ folgt aus der Tatsache, dass es für jeden Teiler d der Ordnung einer zyklischen Gruppe genau eine Untergruppe der Ordnung d gibt, dass $\alpha = -1$ ist - ein Widerspruch.

b) Nach dem Hinweis gilt $2023 = 7 \cdot 17^2$ und da $\text{ggT}(17^2, 7) = 1$ folgt aus dem chinesischem Restsatz:

$$\mathbb{Z}/2023\mathbb{Z} \overset{\Phi}{\cong} \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/17^2\mathbb{Z}.$$

In $\mathbb{Z}/7\mathbb{Z}$ sowie $\mathbb{Z}/17^2\mathbb{Z}$ gibt es für $x^2 = 1$ nach Teil a) genau zwei Lösungen. Woraus folgt, dass es in $\mathbb{Z}/2023\mathbb{Z}$ genau vier Lösungen gibt. Wir berechnen diese wie folgt:
Zunächst berechnet man mittels des euklidischen Algorithmus die Bézout-Darstellung des größten geimensamen Teilers von 7 und 17^2 nämlich $1 = 124 \cdot 7 - 3 \cdot 17^2$. Aus dieser wird wie folgt die Umkehrabbildung Φ^{-1} konstruiert:

$$\Phi^{-1} : \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/17^2\mathbb{Z} \to \mathbb{Z}/2023\mathbb{Z}, \quad ([x], [y]) \mapsto [-3 \cdot 17^2 \cdot x + 124 \cdot 7 \cdot y].$$

Nun genügt es $([1], [1]), ([1], [-1]), ([-1], [1])$ und $([-1], [-1])$ in Φ^{-1} einzusetzen. Man erhält $[1], [-1], [288]$ und $[1735]$.