ELEMENTARE ZAHLENTHEORIE
12. Übungsblatt

Julia Sauter, Andrew Hubery

Aufgabe 1.

Sei $p \geq 3$ eine Primzahl betrachten Sie die Menge

$$A(p) = \{1 < k < p \mid k-1 \text{ und } k \text{ sind beide quadratische Reste modulo } p\}.$$

Das heißt, für $k \in A(p)$ gibt es $x, y \in \mathbb{Z}$ mit $x^2 \equiv k-1 \pmod{p}$ und $y^2 \equiv k \pmod{p}$. Es folgt, dass $(y+x)(y-x) \equiv 1 \pmod{p}$.

(a) Sei $1 \equiv ab \pmod{p}$ und setzen Sie $y \coloneqq \frac{1}{2}(a+b) \pmod{p}$. Für welche $a, b \in \mathbb{F}_p^\times$ gilt $y^2 \notin A(p)$?

(b) Beweisen Sie, dass

$$|A(p)| = \begin{cases} (p-5)/4 & \text{falls } p \equiv 1 \pmod{4}. \\ (p-3)/4 & \text{falls } p \equiv 3 \pmod{4}. \end{cases}$$

(2+2 Punkte)

Aufgabe 2.

Sei $\zeta \coloneqq \frac{1}{2}(1+\sqrt{-3}) \in \mathbb{C}$. Wir wollen zeigen, dass $\mathbb{Z}[\zeta] \subset \mathbb{C}$ ein euklidische Ring ist. Wir schreiben $\bar{\alpha} = a - bi$ für das komplex konjugierte Zahl von $\alpha = a + bi \in \mathbb{C}$.

(a) Zeigen Sie, dass $\mathbb{Z}[\zeta] = \{a + b\zeta \mid a, b \in \mathbb{Z}\}$ ein Ring ist, und dass $\mathbb{Z}[\zeta] = \mathbb{Z}[\bar{\zeta}]$.

(b) Für $\alpha = a + b\zeta \in \mathbb{Z}[\zeta]$ gilt $N(\alpha) \coloneqq \alpha\bar{\alpha} = a^2 + ab + b^2$. Zeigen Sie, dass $N(\alpha) \geq 0$, und finden Sie alle Einheiten in $\mathbb{Z}[\zeta]$, also alle $\alpha \in \mathbb{Z}[\zeta]$ mit $N(\alpha) = 1$.

(c) Seien $\alpha, \beta \in \mathbb{Z}[\zeta]$ mit $\alpha \neq 0$ und schreiben Sie $\beta/\alpha = \bar{\alpha}\beta/N(\alpha) = x + y\zeta$ mit $x, y \in \mathbb{Q}$. Sei nun $q = c + d\zeta \in \mathbb{Z}[\zeta]$ mit $|x-c|, |y-d| \leq \frac{1}{2}$. Zeigen Sie, dass für $r \coloneqq \beta - q\alpha \in \mathbb{Z}[\zeta]$ gilt $N(r) \leq \frac{3}{4}N(\alpha)$. Es folgt, dass $\mathbb{Z}[\zeta]$ ein euklidische Ring ist.

(2+2+2 Punkte)

Aufgabe 3.

Sei $\zeta \coloneqq \frac{1}{2}(1+\sqrt{-3}) \in \mathbb{C}$.

(a) Mit Hilfe Aufgabe (2) finden Sie $g \coloneqq \mathrm{ggT}(1-17\zeta, 3-12\zeta)$.

(b) Berechnen Sie

$$\zeta g, \quad \zeta^2 g, \quad (1-17\zeta)/g, \quad (3-12\zeta)/g.$$

(c) Schreiben Sie $g = (1-17\zeta)x + (3-12\zeta)y$ mit $x, y \in \mathbb{Z}[\zeta]$.

(3+2+1 Punkte)

Abgabe: Montag 8. Juli, bis 12 Uhr in die Postfächer der Tutoren im V3–126

Aufgabe 4.

Sei $\zeta := \frac{1}{2}(1+\sqrt{-3}) \in \mathbb{C}$ und $N(\alpha) = \alpha\bar{\alpha}$. Eine $\alpha \in \mathbb{Z}[\zeta]$ heißt irreduzibel, falls für $\alpha = \beta_1\beta_2$ mit $\beta_i \in \mathbb{Z}[\zeta]$ ist eine von β_1 oder β_2 eine Einheit.

(a) Für $\alpha = a + b\zeta \in \mathbb{Z}$ schreiben Sie $4N(\alpha)$ in der Form $x^2 + my^2$. Benutzen Sie ihre Antwort um zu zeigen, dass für eine Primzahl $p \in \mathbb{Z}$ mit $p \equiv 2 \pmod 3$ gibt es kein $\alpha \in \mathbb{Z}[\zeta]$ mit $N(\alpha) = p$.

(b) Sei nun $p \in \mathbb{Z}$ eine Primzahl mit $p \equiv 1 \pmod 3$. Zeigen Sie, dass es eine $n \in \mathbb{Z}$ gibt, sodass p ein Teiler von n^2+3 ist. Finden Sie jetzt eine $\alpha \in \mathbb{Z}[\zeta]$ mit $N(\alpha) = n^2+3$. Zeigen Sie, dass p kein Teiler von α oder $\bar{\alpha}$ ist. Schließen Sie daraus, dass $p \in \mathbb{Z}[\zeta]$ nicht irreduzibel ist. Folgern Sie, dass es $\pi \in \mathbb{Z}[\zeta]$ gibt mit $N(\pi) = p$.

(2+2 Punkte)