Übungen zur Vorlesung

Algebra

Prof. Dr. Jürgen Hausen
Justus Springer

Sommersemester 2023

Blatt 7

Abgabe: 15.06.2023, 10:00 Uhr (Postfach im C-Bau, 3. Stock)

⊛ **Aufgabe 1.** Bestimme mittels euklidischem Algorithmus einen größten gemeinsamen Teiler für die Polynome

$$f := 6T^5 - 15T^4 + 13T^3 - 3T^2 - 6T + 4, \qquad g := 3T^4 - 3T^3 + 2T^2 + T - 1.$$

Aufgabe 2. Es seien $p \in \mathbb{Z}$ eine Primzahl und $c \in \mathbb{Z}$ mit $\mathrm{ggT}(p, c) = 1$, sodass $cp = m^2 + n^2$ mit ganzen Zahlen m, n gilt. Zeige:

(i) $p = p + i \cdot 0$ ist kein Primelement in dem Ring $\mathbb{Z}[i]$ der ganzen Gaußschen Zahlen.

(ii) Es gibt ganze Zahlen a, b mit $p = a^2 + b^2$.

Aufgabe 3. Es sei $p \in \mathbb{Z}_{\geq} 1$ eine Primzahl. Zeige:

(i) Es gilt $(p-1)! \equiv -1 \mod p$. *Hinweis:* Betrachte das entsprechende Produkt im Körper $\mathbb{Z}/p\mathbb{Z}$ und nutze, dass 1 und $(p-1)$ in $\mathbb{Z}/p\mathbb{Z}$ die einzigen zu sich selbst inversen Elemente sind.

(ii) Gilt $p = 4m + 1$ mit $m \in \mathbb{Z}_{\geq 0}$, so gibt es ein $c \in \mathbb{Z}$ mit $c^2 \equiv -1 \mod p$. *Hinweis:* Betrachte $c := (2m)!$.

Aufgabe 4. Es sei $p \in \mathbb{Z}$ eine Primzahl der Form $p = 4m + 1$ mit einem $m \in \mathbb{Z}$. Zeige: Es gibt ganze Zahlen a, b mit $p = a^2 + b^2$. *Hinweis:* Es gibt ein $x \in \mathbb{Z}$ mit $|x| \leq p/2$, sodass $x^2 \equiv -1 \mod p$ gilt. Verwende dann Aufgaben 3 und 2.

Die mit ⊛ gekennzeichneten Aufgaben sind zur besonders sorgfältigen schriftlichen Ausarbeitung vorgesehen und werden mit 0–4 Punkten bewertet. Zu den restlichen Aufgaben erhalten Sie Feedback von Ihrer Tutorin/Ihrem Tutor.