Universität Konstanz
Fachbereich
Mathematik und Statistik
Prof. Dr. Salma Kuhlmann
Dr. Lorna Gregory

Algebraische Zahlentheorie
Übungsblatt 11

Alle Ringe seien kommutativ mit Eins.

Aufgabe 11.1

Sei p eine Primzahl mit $p \equiv 1$ mod 4.

(a) Zeigen Sie, dass $u \in \mathbb{Z}$ mit
$$u^2 \equiv -1 \text{ mod } p$$
existiert.

(b) Sei
$$L := \{(a, b) \in \mathbb{Z}^2 \mid b \equiv au \text{ mod } p\}.$$
Zeigen Sie, dass das Volumen eines Fundamentalparallelotops von L gleich p ist.

(c) Verwenden Sie den Minkowskischen Gitterpunktsatz um zu zeigen, dass $(a, b) \in L$ mit
$$0 < a^2 + b^2 < 2p$$
existiert.

(d) Folgern Sie, dass jede Primzahl mit $p \equiv 1$ mod 4 als Summe von zwei Quadraten geschrieben werden kann.

Aufgabe 11.2

Sei p eine ungerade Primzahl.

(a) Zeigen Sie, dass die Gleichung
$$x^2 + y^2 + 1 \equiv 0 \text{ mod } p$$
eine Lösung hat.

Hinweis: Schubfachprinzip.

(b) Seien $u, v \in \mathbb{Z}$ mit $u^2 + v^2 + 1 \equiv 0$ mod p. Sei
$$L := \{(a, b, c, d) \in \mathbb{Z}^4 \mid c \equiv ua + vb \text{ mod } p\ ,\ d \equiv ub - va \text{ mod } p\}.$$
Zeigen Sie, dass das Volumen eines Fundamentalparallelotops von L gleich p^2 ist.

(c) Verwenden Sie den Minkowskischen Gitterpunktsatz um zu zeigen, dass $(a, b, c, d) \in L$ mit
$$0 < a^2 + b^2 + c^2 + d^2 < 2p$$
existiert.

Hinweis: Das Volumen einer Kugel in $\mathbb{R}^4$ mit Radius r ist $\pi^2 r^4/2$.

(d) Folgern Sie, dass jede Primzahl als Summe von vier Quadraten geschrieben werden kann.

(e) Benutzen Sie, die Identität

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)$$
$$= (aA - bB - cC - dD)^2 + (aB + bA + cD - dC)^2$$
$$+(aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2$$

um zu zeigen, dass jedes $n \in \mathbb{N}$ als Summe von vier Quadraten geschrieben werden kann.

Aufgabe 11.3
Seien K ein Zahlkörper und $0 \neq I \lhd \mathcal{O}_K$.
Zeigen Sie:
(a) Ist $N(I)$ prim, so ist auch I prim.

(b) Ist I prim, so existiert eine Primzahl $p \in \mathbb{N}$ mit

$$N(I) = p^m,$$

für ein $m \leq [K : \mathbb{Q}]$.

Aufgabe 11.4
Seien $\mathcal{O}_K := \mathbb{Z}[\sqrt{-17}]$, $\mathfrak{p}_1 := \langle 2, 1+\sqrt{-17}\rangle$, $\mathfrak{p}_2 := \langle 3, 1+\sqrt{-17}\rangle$ und $\mathfrak{p}_3 := \langle 3, 1-\sqrt{-17}\rangle$.
(a) Berechnen Sie $N(\mathfrak{p}_1)$, $N(\mathfrak{p}_2)$ und $N(\mathfrak{p}_3)$.

(b) Zeigen Sie, dass
$$\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2 = \langle 18\rangle.$$

(c) Finden Sie alle ideale $I \lhd \mathcal{O}_K$ mit $N(I) = 18$.

Abgabe **Montag, 15.07.2013** bis 12.00 Uhr in die Briefkästen bei F 411.
