Universität Karlsruhe
Mathematisches Institut II
Dr. Stefan Kühnlein
Lars Hoffmann

Elementare Zahlentheorie

Sommersemester 2004

12. Übungsblatt

Aufgabe 1 (4 Punkte)
Sei p eine ungerade Primzahl. Zeigen Sie: Sind $a, b \in \mathbb{F}_p^\times$ und $c \in \mathbb{F}_p$, dann ist die Gleichung $ax^2 + by^2 = c$ in $\mathbb{F}_p^2$ lösbar.
Hinweis: Zählen Sie die Elemente der Menge $\{c - by^2 \mid y \in \mathbb{F}_p\}$.

Aufgabe 2 (8 Punkte)

a) Seien $a, b, c, d, w, x, y, z \in \mathbb{Z}$. Zeigen Sie:

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) =$$
$$(aw - bx - cy - dz)^2 + (ax + bw + cz - dy)^2 + (ay + cw - bz + dx)^2 + (az + dw + by - cx)^2.$$

b) Sei p eine Primzahl. Nach Aufgabe 1 gibt es $u, v \in \mathbb{Z}$ mit $u^2 + v^2 \equiv -1 \bmod p$. Weiter sei das Gitter Γ als $\Gamma := A \cdot \mathbb{Z}^4$ definiert, wobei A durch

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ -v & u & 0 & p \end{pmatrix}$$

gegeben sei.
Zeigen Sie, dass für $\epsilon > 0$ und für $r = \sqrt[4]{32}\sqrt{\frac{p}{\pi}} + \epsilon$ die Kugel $B_r(0)$ mit Radius r um den Nullpunkt einen nichttrivialen Gitterpunkt $\gamma \in \Gamma$ enthält. Zeigen Sie weiter, dass sich daraus die Existenz eines $\gamma \in \Gamma$ mit $\| y \|^2 = p$ ergibt.

Hinweis: Sie dürfen ohne Beweis verwenden, dass $B_r(0)$ das Volumen $\frac{\pi^2}{2} r^4$ hat.

c) Folgern Sie, dass jede natürliche Zahl die Summe von vier Quadraten ist.

d) Zeigen Sie außerdem, dass eine Primzahl p mit der Eigenschaft $p \equiv 7 \bmod 8$ nicht Summe von drei Quadraten sein kann.

Aufgabe 3 (4 Punkte)
Zeigen Sie:

$$b_1, \ldots, b_n \in \mathbb{Z}^n \text{ sind Gitterbasis von } \mathbb{Z}^n \iff \det(b_1 \mid \cdots \mid b_n) = \pm 1.$$

ABGABE bis Mittwoch, den **14. Juli 2004, 14:00 Uhr** in den gekennzeichneten Einwurfkästen im Kollegiengebäude Mathematik, 3. OG neben Zimmer 308 oder zu Beginn der Übung.