Universität Karlsruhe
Mathematisches Institut II
Dr. Stefan Kühnlein
Lars Hoffmann

Elementare Zahlentheorie

Sommersemester 2004

10. Übungsblatt

Aufgabe 1 (4 Punkte)
Zeigen Sie, ohne einen Teiler zu berechnen, dass 1729 keine Primzahl ist.

Aufgabe 2 (4 Punkte)
Sei $d \not\equiv 1 \bmod 4$, $K = \mathbb{Q}(\sqrt{d})$ und $\mathcal{O}$ der Ganzheitsring in K. Zeigen Sie:

a) Es ist $I := \{z \in \mathcal{O} \mid \mathcal{N}(z) \in 2\mathbb{Z}\}$ ein Ideal in $\mathcal{O}$.

b) Falls $d < -2$ ist, ist I kein Hauptideal.

Aufgabe 3 (4 Punkte)
Seien $\mathcal{O} = \mathbb{Z}[\sqrt{3}]$, $\epsilon = 2 + \sqrt{3}$ (*Hinweis:* $2 + \sqrt{3}$ ist eine Einheit in $\mathcal{O}$) und $r_k := \epsilon^{2^{k-1}} + \kappa(\epsilon)^{2^{k-1}}$.

Zeigen Sie:

a) Es gilt $r_1 = 4$ und $r_{k+1} = r_k^2 - 2$.

Sei nun p eine ungerade Primzahl und $M_p = 2^p - 1$. Der *Lucas-Lehmer-Test* für Mersenne-Primzahlen besagt nun, dass M_p eine Primzahl ist, falls $M_p \mid r_{p-1}$ gilt. Um ihn zu beweisen, zeigen wir, dass M_p keinen Primteiler l mit der Eigenschaft $l \leq \sqrt{M_p}$ haben kann, falls M_p ein Teiler von r_{p-1} ist.
Nehmen wir also zunächst an, dass es ein $R \in \mathbb{N}$ gibt mit $r_{p-1} = \epsilon^{2^{p-2}} + \kappa(\epsilon)^{2^{p-2}} = R \cdot M_p$.

b) Zeigen Sie: $\epsilon^{2^{p-1}} = RM_p\epsilon^{2^{p-2}} - 1$ und $\epsilon^{2^p} = (RM_p\epsilon^{2^{p-2}} - 1)^2$.

Nun sei M_p außerdem keine Primzahl, habe also einen Primteiler $l \in \mathbb{N}$ mit der Eigenschaft $l \leq \sqrt{M_p}$. Zeigen Sie:

c) Die Ordnung von ϵ in $(\mathcal{O}/l\mathcal{O})^\times$ ist 2^p.

d) Aus c) folgt, dass $2^p \leq l^2 - 1$ ist.

Aufgabe 4 (4 Punkte)
Es sei $f \in \mathbb{Z}[X]$ und $\alpha \in \mathbb{Q}$ eine Nullstelle von f. Zeigen Sie: Ist die Darstellung $\alpha = \frac{z}{n}$ vollständig gekürzt, so teilt n den Leitkoeffizienten von f.

ABGABE bis Mittwoch, den **23. Juni 2004, 14:00 Uhr** in den gekennzeichneten Einwurfkästen im Kollegiengebäude Mathematik, 3. OG neben Zimmer 308 oder zu Beginn der Übung.