Universität Karlsruhe
Mathematisches Institut II
Dr. Stefan Kühnlein
Lars Hoffmann

Elementare Zahlentheorie

Sommersemester 2004

9. Übungsblatt

Aufgabe 1 (4 Punkte)
Sei $n \in \mathbb{N}$ und mit p immer eine Primzahl bezeichnet. Zeigen Sie, dass

$$\#\{(x,y) \in \mathbb{Z}^2 \mid x^2 + y^2 = n\} = 4 \cdot \prod_{p|n,\, p\equiv 1 \bmod 4} (1 + v_p(n)) \cdot \prod_{p|n,\, p \equiv 3 \bmod 4} \frac{1 + (-1)^{v_p(n)}}{2}.$$

Aufgabe 2 (4 Punkte)
Schreiben Sie, falls möglich, 1105 und 2002 als Summe zweier natürlicher Quadratzahlen.

Aufgabe 3 (4 Punkte)
Zeigen Sie, dass $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ euklidisch ist (bezüglich der Norm $N(a + b\frac{1+\sqrt{-3}}{2}) = a^2 + ab + b^2$).

Aufgabe 4 (4 Punkte)
Sei $F(x) = \frac{(4x+1-i)^4}{4}\Phi_5(\frac{4x+1+i}{4x+1-i})$. Zeigen Sie:

a) Es ist $F(x) \in \mathbb{Z}[x]$, und wenn für ein $a \in \mathbb{Z}$ gilt, dass $F(a) \neq -1$ ist, so gibt es einen Primteiler $p \equiv -1 \bmod 4$ von $F(a)$.

b) Die Primzahl aus a) erfüllt die Bedingung $p \equiv -1 \bmod 5$.
Hinweis: Verwenden Sie ohne Beweis $\mathbb{F}_{p^2} = \mathbb{F}_p(i) = \mathbb{F}_p[X]/(X^2 + 1)$.

c) Es gibt unendlich viele Primzahlen p der Form $p \equiv -1 \bmod 5$.

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.