Übungen zur Algebraischen Zahlentheorie I

Wintersemester 2010/11

Universität Heidelberg
Mathematisches Institut
Prof. A. Schmidt
Dr. A. Holschbach

Blatt 3
Abgabetermin: Mittwoch, 03.11.2010, 16.15 Uhr

Aufgabe 1. Zeigen Sie: Eine ungerade Primzahl p ist genau dann von der Form $p = x^2+2y^2$ mit ganzen Zahlen x und y, wenn p kongruent 1 oder 3 modulo 8 ist.
Hinweis: Man benutze die Äquivalenz $\left(\frac{-2}{p}\right) = +1 \Leftrightarrow p \equiv 1, 3 \bmod 8$.

Aufgabe 2. Sei m eine natürliche Zahl. In Verallgemeinerung der Notation aus der Vorlesung bezeichnen wir $a \in \mathbb{Z}$ als *quadratischen Rest modulo* m, wenn a teilerfremd zu m ist und ein $x \in \mathbb{Z}$ existiert mit $x^2 \equiv a \bmod m$. Wegen Aufgabe 2 von Blatt 2 kann man sich bei der Untersuchung der quadratischen Reste auf den Fall beschränken, dass m eine Primzahlpotenz ist. Sei also $m = p^e$ mit einer Primzahl p und $e \geq 1$; der Einfachheit halber sei $p \neq 2$. Zeigen Sie: a ist genau dann ein quadratischer Rest modulo m, wenn $\left(\frac{a}{p}\right) = 1$.
Hinweis: Für die schwierigere Richtung zeige man: Gilt $x^2 \equiv a \bmod p^e$, so gibt es ein $k \in \mathbb{Z}$ mit $(x + kp^e)^2 \equiv a \bmod p^{e+1}$.

Aufgabe 3. Sei $n \in \mathbb{Z}$ und m eine ungerade natürliche Zahl mit Primfaktorzerlegung $m = p_1^{e_1} \cdots p_r^{e_r}$. Als Verallgemeinerung des Legendre-Symbols definiert man das *Jacobi-Symbol* $\left(\frac{n}{m}\right)$ folgendermaßen:

$$\left(\frac{n}{m}\right) := \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)^{e_i},$$

wobei auf der rechten Seite Legendre-Symbole stehen. Zeigen Sie: Das Jacobi-Symbol $\left(\frac{n}{m}\right)$ ist multiplikativ bzgl. m und n, und für teilerfremde ungerade natürliche Zahlen m, n gilt das quadratische Reziprozitätsgesetz

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}. \tag{1}$$

Hinweis: Zeigen Sie zunächst für beliebige ungerade $u, v \in \mathbb{Z}$:

$$uv - 1 \equiv (u-1) + (v-1) \bmod 4,$$

und folgern Sie damit (1) aus dem QRG für das Legendre-Symbol.

Aufgabe 4. Es sei n eine ungerade und quadratfreie natürliche Zahl, die sich als Summe zweier Quadratzahlen schreiben läßt. Zeigen Sie: Diese Darstellung ist (bis auf Vertauschung der Summanden) genau dann eindeutig, wenn n eine Primzahl ist.

Zusatzaufgabe: Seien a, b natürliche Zahlen. Wir wollen zeigen: Lässt sich eine Primzahl p in der Form $ax^2 + by^2$ mit $x, y \in \mathbb{Z}$ darstellen, so ist diese Darstellung (bis auf die offensichtlichen Symmetrien) eindeutig.

(a) Angenommen, es gilt $p = ax^2 + by^2 = a\tilde{x}^2 + b\tilde{y}^2$ mit $x, y, \tilde{x}, \tilde{y} \in \mathbb{Z}$. Zeigen Sie: $-ab$ ist ein quadratischer Rest modulo p, und es gilt $x\tilde{y} \equiv \pm\tilde{x}y \bmod p$.

(b) Zeigen Sie, dass unter den obigen Voraussetzungen gilt:

$$|x\tilde{y} \mp \tilde{x}y| \leq \frac{p}{\sqrt{ab}};$$

und folgern Sie die obige Behauptung.