Elementare Zahlentheorie

Abgabetermin: Donnerstag, 02/07/2008, 12:00

Fernstudenten reichen alle Aufgaben ein und ersetzen den hier angegebenen Abgabetermin durch den ihnen mitgeteilten. Für alle anderen Studenten ist die Aufgabe 24 eine Präsenzaufgabe, deren Lösung nicht eingereicht werden muß. Für die Lösung der Aufgaben 22 und 23 benötigt man aus der Vorlesung vom 30.6. die Aussage: $x \in \mathbb{Z}[\omega_m]^* \iff |N(x)| = 1$, und für die Aufgabe 23 benötigt man aus dieser Vorlesung ferner, daß es für $m > 0$ eine Einheit ungleich ± 1 in $\mathbb{Z}[\omega_m]$ gibt.

Aufgabe 21: Es sei $p \in \mathbb{P}$ eine ungerade Primzahl und $k, m \in \mathbb{Z}$ mit $\mathrm{ggt}(p, km) = 1$. Falls die diophantische Gleichung

$$x^2 - m \cdot y^2 = k \cdot p$$

eine Lösung hat, dann ist das Legendre-Symbol $\left(\frac{m}{p}\right) = 1$.

Aufgabe 22: Es sei $m \in \mathbb{Z}$ eine quadratfreie ganze Zahl und $x \in \mathbb{Z}[\omega_m]$.

a. Ist $N(x)$ irreduzibel in $\mathbb{Z}$, so ist x irreduzibel in $\mathbb{Z}[\omega_m]$.

b. Jedes Element in $\mathbb{Z}[\omega_m]$ läßt sich als Produkt von endlich vielen irreduziblen Elementen schreiben.

Hinweis: in Teil b. betrachte man die Menge M aller $0 \neq x \in \mathbb{Z}[\omega_m] \setminus \mathbb{Z}[\omega_m]^*$, die nicht Produkt endlich vieler irreduzibler Elemente sind, sowie die Menge N der $|N(x)|$ für $x \in M$. Ist M nicht leer, so besitzt N ein Minimum. Dies führe man zum Widerspruch.

Aufgabe 23: Es sei $m \in \mathbb{Z}_{>0}$ eine quadratfreie Zahl.

a. Das Minimum $\varepsilon = \min\left\{x \in \mathbb{Z}[\omega_m]^* \;\middle|\; x > 1\right\}$ existiert.

b. $\mathbb{Z}[\omega_m]^*_{>0} := \left\{x \in \mathbb{Z}[\omega_m]^* \;\middle|\; x > 0\right\} = \langle \varepsilon \rangle$.

c. $\mathbb{Z}[\omega_m]^* = \left\{ \pm \varepsilon^n \;\middle|\; n \in \mathbb{Z}\right\} = \{1, -1\} \cdot \mathbb{Z}[\omega_m]^*_{>0}$.

Anmerkung: Man nennt ε die *Fundamentaleinheit* von $\mathbb{Z}[\omega_m]$. Teil c. zeigt, daß $\mathbb{Z}[\omega_m]$ isomorph zu $\mathbb{Z}_2 \times \mathbb{Z}$ ist.

Aufgabe 24: Es sei $m \in \mathbb{Z}_{<0}$ eine negative quadratfreie ganze Zahl. Dann gilt

$$\mathbb{Z}[\omega_m]^* = \begin{cases} \{1, -1, i, -i\}, & \text{falls } m = -1, \\ \{1, -1, \omega_m, -\omega_m, \omega_m^2, -\omega_m^2\}, & \text{falls } m = -3, \\ \{1, -1\}, & \text{sonst.} \end{cases}$$