Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae, Philipp Wagner, Vera Knüppels

Hausübungen zur Vorlesung

Zahlentheorie

Sommersemester 2012

Blatt 1/2

Abgabe bis 16. April 2012, 12 Uhr (vor der Vorlesung)

AUFGABE 1 F1 **(5 Punkte):**
Beweisen Sie für beliebige Konstanten $a, b, c \in \mathbb{Q}$ und $a > 0$ die Gleichheit

$$an^2 + bn + c = \Theta(n^2).$$

AUFGABE 2 F1 **(6 Punkte):**
Beweisen Sie, dass es unendlich viele Primzahlen der Form $4k - 1$ bzw. $4k + 1$ gibt.

AUFGABE 3 F1 **(4 Punkte):**
Zeigen Sie, dass $\mathbb{Z}[\sqrt{-2}] \subseteq \mathbb{C}$ euklidisch bezüglich der Normfunktion $N(z) = |z|^2$ ist, dies jedoch nicht für $\mathbb{Z}[\sqrt{-5}]$ gilt.

AUFGABE 4 F2 **(8 Punkte):**
Zeigen Sie, folgende Aussagen.

(a) $\pm 1 \in \mathbb{Z}[\sqrt{2}]^*$

(b) $\pm(1 \pm \sqrt{2}) \in \mathbb{Z}[\sqrt{2}]^*$

(c) Ist $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$, dann gilt $a^2 - 2b^2 = \pm 1$.

(d) Ist $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^*$, dann gibt es $n_1, n_2 \in \mathbb{Z}_{\geq 0}$ mit $a + b\sqrt{2} = \pm(1 + \sqrt{2})^{n_1}(1 - \sqrt{2})^{n_2}$.
Hinweis: vollständige Induktion nach $|a|$.

(e) Folgern Sie, dass $\mathbb{Z}[\sqrt{2}]^* = \{\pm(1 + \sqrt{2})^n \mid n \in \mathbb{Z}\}$.

AUFGABE 5 F2 **(6 Punkte):**
Zerlegen Sie die natürlichen Zahlen 101, 103 und 2310 in Primfaktoren innerhalb $\mathbb{Z}[i]$.

AUFGABE 6 F2 **(2 Punkte):**
Bestimmen Sie alle multiplikativen Einheiten im Ring der stetigen, reellen Funktionen $f : \mathbb{R} \to \mathbb{R}$ mit der punktweisen Addition und Multiplikation. Welche Funktionen sind die irreduziblen Elemente?

Hinweis: Alle mit F1 *gekennzeichneten Aufgaben sind im Briefkasten Zahlentheorie Fach 1 abzugeben. Entsprechend sind die mit* F2 *gekennzeichneten Aufgaben im Briefkasten Zahlentheorie Fach 2 abzugeben.*