Mathematisches Institut
der Universität Paderborn
Prof. I. Burban und H. Herr

SS 2019
Mittwoch, 26.06.2019
Blatt 11

Übungen zur Algebra

Aufgabe 64.[4 Punkte] Beweisen Sie, dass der Ring

$$R = \mathbb{Z}[\sqrt{-2}] = \left\{ a + b\sqrt{-2} \,\middle|\, a, b \in \mathbb{Z} \right\} \subset \mathbb{C},$$

versehen mit der Normfunktion

$$R \setminus \{0\} \xrightarrow{N} \mathbb{N},\ a + b\sqrt{-2} \mapsto a^2 + 2b^2,$$

Euklidisch ist. Bestimmen Sie die Gruppe der Einheiten von R.

Aufgabe 65.[4 Punkte] Sei R ein Ring und $e \in R$ ein Element mit $e^2 = e$ (ein solches Elemente heißt *Idempotent*). Zeigen Sie, dass dann auch $1 - e$ ein Idempotent ist, und dass die Abbildung

$$R \longrightarrow R/(e) \times R/(1-e),\ \ x \mapsto \big(x + eR, x + (1-e)R\big)$$

ein Ringisomorphismus ist.
Hinweis: Zeigen Sie zuerst, dass $\big(\overline{1}, \overline{0}\big)$ und $\big(\overline{0}, \overline{1}\big)$ im Bild dieser Abbildung liegen.

Aufgabe 66.[3 Punkte] Sei R ein kommutativer Ring. Ein Element $x \in R$ nennt man *nilpotent*, wenn es ein $k \in \mathbb{N}$ gibt mit $x^k = 0$. Zeigen Sie, dass die nilpotenten Elemente ein Ideal von R bilden.

Aufgabe 67.[3 Punkte] Berechnen Sie $2^{100000} \bmod 91$.

Aufgabe 68.[2+3+4 Punkte] Bestimmen Sie alle Lösungen der folgenden Kongruenzgleichungen für $x \in \mathbb{Z}$:

(1) $27x \equiv 25 \bmod 257$.
(2) $60x \equiv b \bmod 272$ in Abhängigkeit von $b \in \mathbb{Z}$.
(3) $x^{11} \equiv 3 \bmod 20$. Begründen Sie, warum x modulo 20 eindeutig bestimmt ist.

Aufgabe 69.[4 Punkte] Alice sendet Bob eine geheime Botschaft nach dem RSA Verfahren. Bob wählt dazu die geheimen Primzahlen 101 und 103. Danach teilt er Alice deren Produkt $n = 10403$ sowie die zu $\varphi(n)$ teilerfremde Zahl 2051 mit. Was sendet Alice, wenn ihre Botschaft 1000 lautet, und wie rechnet Bob, um die empfangene Nachricht zu entschlüsseln?

Bitte wenden!

Aufgabe 70 (Bonus).[12 Punkte] Um das Jahr 1650 hat der französische Mathematiker Pierre Fermat seine englische Rivalen mit dem folgenden Problem herausgefordert:

Seien $x, y \in \mathbb{Z}$, so dass gilt: $y^2 = x^3 - 2$.
Beweisen Sie, dass $(x, y) = (3, \pm 5)$.

Historischer Hintergrund. Es gibt keine Belege, dass Fermat selbst eine korrekte Lösung seines Problems hatte. Die erste im Jahr 1730 von Leonhard Euler veröffentlichte Lösung der Fermatschen Herausforderung hatte unbehebbare Lücken. Der erste vollständige Beweis wurde erst im 19. Jahrhundert erzielt.

Kontern Sie die Fermatsche Herausforderung durch eine Lösung, in dem die Eindeutigkeit der Primfaktorzerlegung im Euklidischen Ring $\mathbb{Z}[\sqrt{-2}]$ die entscheidende Rolle spielt.

Hinweis: Man kann in folgenden Schritten vorgehen:

(1) Begründen Sie, dass sowohl x als auch y ungerade sein müssen.
(2) Betrachten Sie die Gleichung im Ring $\mathbb{Z}[\sqrt{-2}]$ und zeigen Sie
$$\text{ggT}\left(y - \sqrt{-2},\ y + \sqrt{-2}\right) = 1.$$
(3) Schreiben Sie x als Produkt aus Primfaktoren und folgern Sie $y + \sqrt{-2} = (p_1^{m_1} ... p_t^{m_t})^3$ und $y - \sqrt{-2} = (q_1^{l_1} .... q_s^{l_s})^3$ für Primelemente $p_1,\ ...,\ p_t,\ q_1,\ ...,\ q_s$ mit $p_i \neq q_j$ für alle i und j.
(4) Zeigen Sie, dass für $a,\ b \in \mathbb{Z}$ mit $y + \sqrt{-2} = (a + b\sqrt{-2})^3$ gilt $b = 1$ und $a \in \{+1,\ -1\}$.

Abgabe: Dienstag, 02.07.2019, 9:00 Uhr.