Universität Konstanz
Fachbereich Mathematik und Statistik
Sommersemester 2019

Alexander Taveira Blomenhofer
Markus Schweighofer

Übungsblatt 12 zur Zahlentheorie

Aufgabe 1. Sei $d \in \not\square$. Betrachte die folgende Aussage:

> Die diophantische Gleichung
>
> $$(*) \qquad y^2 = x^3 + d$$
>
> besitzt genau dann eine Lösung $(x, y) \in \mathbb{Z}^2$, wenn es ein $a \in \mathbb{N}_0$ gibt mit
>
> $$d \in \{-3a^2 - 1, -3a^2 + 1\}.$$
>
> In diesem Fall gibt es genau ein solches a und für dieses a sind genau
>
> $$(a^2 - d, \pm a(a^2 + 3d))$$
>
> die beiden (nicht notwendig verschiedenen) Lösungen von $(*)$ in $\mathbb{Z}^2$.

(a) Zeige, dass es höchstens ein $a \in \mathbb{N}_0$ mit $d \in \{-3a^2 - 1, -3a^2 + 1\}$ gibt.

(b) Zeige: Ist $a \in \mathbb{Z}$ mit $d \in \{-3a^2 - 1, -3a^2 + 1\}$, so sind $(a^2 - d, \pm a(a^2 + 3d))$ Lösungen von $(*)$.

Wegen (a) und (b) reduziert sich die obige Aussage offensichtlich zu der folgenden:

> Seien $x, y \in \mathbb{Z}$ mit
>
> $$(*) \qquad y^2 = x^3 + d.$$
>
> Dann gibt es ein $a \in \mathbb{Z}$ mit $3a^2 + d \in \mathbb{Z}^\times$ und
>
> $$x = a^2 - d \qquad \text{sowie} \qquad y = a(a^2 + 3d).$$

Betrachte folgenden vermeintlichen Beweis für diese letztere Aussage:

Im Zahlring $\mathcal{O}_d$ von $\mathbb{Q}(\sqrt{d})$ kann $(*)$ geschrieben werden als

$$(**) \qquad (y - \sqrt{d})(y + \sqrt{d}) = x^3.$$

Hilfsbehauptung: Es gibt kein Primelement p von $\mathcal{O}_d$, welches sowohl $y - \sqrt{d}$ als auch $y + \sqrt{d}$ teilt.

Begründung: Angenommen, p wäre so ein Primelement von $\mathcal{O}_d$. Setzt man $N := N_{\mathbb{Q}(\sqrt{d})|\mathbb{Q}}$, so gilt $p \mid x$ in $\mathcal{O}_d$ und daher $N(p) \mid x^2$ in $\mathbb{Z}$. Durch Betrachtung der Gleichung $(*)$ modulo 8 sieht man, dass $N(p)$ ungerade sein muss, denn sonst wäre 2 in $\mathbb{Z}$ ein Teiler von x^2 und damit 8 ein Teiler von x^3, so dass die Restklasse von d im Ring $\mathbb{Z}/(8)$ ein Quadrat wäre. Weiter gilt $p \mid 2y$ in $\mathcal{O}_d$ und daher $N(p) \mid 4y^2$ in $\mathbb{Z}$. Da $N(p)$ ungerade ist, folgt sogar $N(p) \mid y^2$. Wegen $(*)$ folgt $N(p) \mid d$ in $\mathbb{Z}$. Da d quadratfrei ist, folgt $N(p) \in \mathbb{Z}^\times$ (wenn eine Primzahl $N(p)$ teilen würde, so würde ihr Quadrat sowohl x^2 als auch y^2 teilen und damit gemäß $(*)$ auch d). Es folgt $p \in \mathcal{O}_d^\times$. Widerspruch!

Die Existenz und Eindeutigkeit der Primfaktorzerlegung in $\mathcal{O}_d$ liefert ein $z \in \mathcal{O}_d$ und eine Einheit $\varepsilon \in \mathcal{O}_d$ mit $y + \sqrt{d} = \varepsilon z^3$. Offensichtlich gilt $\varepsilon \in \{-1, 1\}$ und daher $\varepsilon = \varepsilon^3$, so dass wir Œ davon ausgehen können, dass

$$y + \sqrt{d} = z^3.$$

Schreibe $z = a + b\sqrt{d}$ mit $a, b \in \mathbb{Z}$. Dann gilt

$$y + \sqrt{d} = (a + b\sqrt{d})^3 = (a^3 + 3ab^2d) + (3a^2b + b^3d)\sqrt{d}$$

was gleichbedeutend mit $y = a^3 + 3ab^2d$ und $1 = 3a^2b + b^3d = b(3a^2 + b^2d)$ ist. Es folgt $b \in \mathbb{Z}^\times$ und daher $3a^2 + d = 3a^2 + b^2d \in \mathbb{Z}^\times$ wie gewünscht. Weiter folgt $y = a^3 + 3ab^2d = a^3 + 3ad = a(a^2 + 3d)$ wie ebenfalls gewünscht. Die Gleichung $(**)$ kann man jetzt umschreiben zu

$$(***) \qquad (a + \sqrt{d})^3(a - \sqrt{d})^3 = x^3.$$

Es folgt $x^3 = (a^2 - d)^3$ und daher $x = a^2 - d$.

(c) Identifiziere Stellen in obigem „Beweis“, die Dir nicht unmittelbar klar sind oder die Dir sogar faul vorkommen. Führe jeweils aus, warum Dir die jeweilige Begründung nicht gefällt (zum Beispiel weil sie zu kurz ist oder weil ein unzulässiges Argument angeführt wird).

(d) Ändere und ergänze den obigen „Beweis“ so, dass er für den Fall $d = -1$ richtig wird.

(e) Modifiziere den obigen „Beweis“ so, dass er zulässig wird, wenn $d < -1$, $d \in \not\square_{2,3}$ und $\mathcal{O}_d$ faktoriell ist.

(f) Sei A ein Dedekindring, dessen Klassenzahl nicht durch 3 teilbar ist, und I ein Ideal von A derart, dass I^3 ein Hauptideal ist. Zeige, dass dann auch I ein Hauptideal ist.

(g) Rette den obigen „Beweis“ für den Fall, dass $d < -1$, $d \in \not\square_{2,3}$ und die Klassenzahl von $\mathcal{O}_d$ nicht durch 3 teilbar ist.

Abgabe bis Mittwoch, den 10. Juli 2019, um 11:44 Uhr in die Zettelkästen neben F411.