53. Österreichische Mathematik-Olympiade

Kurs für Internationale „Mathematik macht Freu(n)de“ – Aufgabenblatt für den 9. Oktober 2021

Ablauf

Dieses Aufgabenblatt wurde von Moritz Hiebler zusammengestellt.

Wir freuen uns auf deine Fragen und Lösungsvorschläge per E-Mail.

Am 6. Oktober 2021 wird das Blatt mit Tipps zur Lösung ausgewählter Aufgaben ergänzt. Moritz Hiebler trägt zum Thema im virtuellen Olympiade-Kurs am 9. Oktober 2021 von 10:00–11:45 Uhr vor. Kurz darauf ergänzen wir das Blatt um ausgewählte Lösungsvorschläge und Angaben zu den Quellen der Aufgaben.

Schreibe uns, wenn du bei den virtuellen Kursen dabei sein möchtest. Du bist jederzeit willkommen!

Gauß'sche ganze Zahlen

Einführung

Unter den *Gauß'schen ganzen Zahlen* versteht man die Teilmenge

$$\mathbb{Z}[\mathrm{i}] \coloneqq \{a + b\,\mathrm{i} \mid a, b \in \mathbb{Z}\}$$

der komplexen Zahlen, wobei i die imaginäre Einheit mit $\mathrm{i}^2 = -1$ bezeichnet. Für zwei Elemente z, $w \in \mathbb{Z}[\mathrm{i}]$ liegen auch $z \pm w$ und $z \cdot w$ wieder in $\mathbb{Z}[\mathrm{i}]$.[1]
Wir werden im Folgenden für $\mathbb{Z}[\mathrm{i}]$ Teilbarkeitsuntersuchungen durchführen und am Ende einen Satz über Existenz und Eindeutigkeit der Primfaktorzerlegung beweisen, mit dessen Hilfe wir die Darstellung von natürlichen Zahlen als Summe zweier Quadratzahlen genauer verstehen können.
Zuerst zu dieser zentralen Verbindung eine im Folgenden sehr nützliche

Definition. Für eine Gauß'sche ganze Zahl z sei $\mathrm{N}(z) \coloneqq z \cdot \overline{z} = |z|^2$ die *Norm* von z.

Die Norm ist multiplikativ, d. h. $\mathrm{N}(wz) = wz \cdot \overline{wz} = w\overline{w} \cdot z\overline{z} = \mathrm{N}(w) \cdot \mathrm{N}(z)$. Bei $z = a + b\,\mathrm{i}$ mit a, $b \in \mathbb{Z}$ erhält man $\mathrm{N}(z) = a^2 + b^2 \in \mathbb{Z}_{\geq 0}$, die interessante Summe zweier Quadratzahlen. Wir werden uns neben dem Studium von $\mathbb{Z}[\mathrm{i}]$ an sich vor allem mit der Frage beschäftigen, welche ganzen Zahlen die Norm einer Gauß'schen ganzen Zahl sind.
Mit Hilfe der Norm können wir ein Resultat, analog zur Division mit Rest in $\mathbb{Z}$, formulieren, dessen Beweis wir als Aufgabe führen werden.

Satz 1 (Division mit Rest in $\mathbb{Z}[\mathrm{i}]$)**.** *Seien z, $w \in \mathbb{Z}[\mathrm{i}]$ mit $z \neq 0$. Dann gibt es q, $r \in \mathbb{Z}[\mathrm{i}]$ mit $w = q \cdot z + r$ und $\mathrm{N}(r) < \mathrm{N}(z)$.*

Die Zahlen q und r sind allerdings nicht eindeutig bestimmt, wie man beispielsweise gut bei der Division von $1 + \mathrm{i}$ durch 2 erkennen kann:

$$1 + \mathrm{i} = 0 \cdot 2 + (1 + \mathrm{i}) = \mathrm{i} \cdot 2 + (1 - \mathrm{i}) \qquad \text{und} \qquad 2 = \mathrm{N}(1 + \mathrm{i}) = \mathrm{N}(1 - \mathrm{i}) < \mathrm{N}(2) = 4$$

Widmen wir uns nun der Teilbarkeit, die ganz analog zu der in $\mathbb{Z}$ definiert wird:

Definition. Seien z, $w \in \mathbb{Z}[\mathrm{i}]$. Wir sagen, *$z$ teilt w* oder *w ist (in $\mathbb{Z}[\mathrm{i}]$) durch z teilbar*, falls es ein $q \in \mathbb{Z}[\mathrm{i}]$ mit $w = z \cdot q$ gibt, und schreiben dafür $z \mid w$ (in $\mathbb{Z}[\mathrm{i}]$).

[1] Man sagt in diesem Fall, dass $\mathbb{Z}[\mathrm{i}]$ einen *Unterring* von $\mathbb{C}$ bildet.

Für eine Primfaktorzerlegung braucht es eine Verallgemeinerung des Primzahlbegriffes der natürlichen Zahlen. Leider gibt es im Allgemeinen zwei Möglichkeiten dafür, die nicht zusammenfallen müssen. Wir werden aber bald sehen, dass sie das in $\mathbb{Z}[\mathrm{i}]$ doch tun. Daher genügt uns nur eine weitere

Definition (Primelement)**.** Seien z und w zwei Gauß'sche ganze Zahlen. Ein $\pi \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(\pi) > 1$ heißt ein *Primelement* in $\mathbb{Z}[\mathrm{i}]$, falls aus $\pi \mid z \cdot w$ sogar ($\pi \mid z$ oder $\pi \mid w$) folgt.

Wegen der Multiplikativität der komplexen Konjugation ist mit $\pi \in \mathbb{Z}[\mathrm{i}]$ auch $\overline{\pi}$ ein Primelement in $\mathbb{Z}[\mathrm{i}]$ (Check!). Neben den Primelementen interessieren wir uns auch noch für die Teiler von 1:

Definition. Eine Gauß'sche ganze Zahl e mit $e \mid 1$ heißt *Einheit* von $\mathbb{Z}[\mathrm{i}]$. Die Menge aller Einheiten von $\mathbb{Z}[\mathrm{i}]$ bezeichnen wir mit $\mathbb{Z}[\mathrm{i}]^\times$.

Lemma 1.1 (Charakterisierung von Einheiten)**.** *Sei $e \in \mathbb{Z}[\mathrm{i}]$. Dann sind äquivalent:*

(a) $e \in \mathbb{Z}[\mathrm{i}]^\times$ (b) $\mathrm{N}(e) = 1$ (c) $e \in \{\pm 1, \pm \mathrm{i}\}$ (d) $1/e \in \mathbb{Z}[\mathrm{i}]$

Beweis. Wir zeigen 1.1(a) $\implies$ 1.1(b) $\implies$ 1.1(c) $\implies$ 1.1(d) $\implies$ 1.1(a).
1.1(a) $\implies$ 1.1(b): Sei $f \in \mathbb{Z}[\mathrm{i}]$ mit $ef = 1$. Es folgt $\mathrm{N}(e)\,\mathrm{N}(f) = \mathrm{N}(1) = 1$ und $\mathrm{N}(e) = \mathrm{N}(f) = 1$.
1.1(b) $\implies$ 1.1(c): Schreiben wir $e = a + b\,\mathrm{i}$ mit $a, b \in \mathbb{Z}$, so gilt nach Voraussetzung $a^2 + b^2 = 1$, was auf $a^2 \leq 1$, somit $a \in \{-1, 0, 1\}$ und nach Durchprobieren auf $(a, b) \in \{(0, 1), (0, -1), (1, 0), (-1, 0)\}$ führt. Daher ist e von der behaupteten Form.
1.1(c) $\implies$ 1.1(d): Für diese vier Werte gilt offenbar $1/e = \overline{e} \in \mathbb{Z}[\mathrm{i}]$.
1.1(d) $\implies$ 1.1(a): Wir erhalten mit $1/e \in \mathbb{Z}[\mathrm{i}]$ aus $e \cdot (1/e) = 1$ direkt $e \mid 1$. □

Wir notieren die erwähnte Äquivalenz und führen den Beweis als Aufgabe.

Proposition 1.2. *Seien π, z und w Gauß'sche ganze Zahlen mit $\mathrm{N}(\pi) > 1$. Dann sind äquivalent:*

(a) *π ist ein Primelement.*

(b) *π ist* unzerlegbar*: Aus $\pi = z \cdot w$ folgt $z \in \mathbb{Z}[\mathrm{i}]^\times$ oder $w \in \mathbb{Z}[\mathrm{i}]^\times$.*

Umgekehrt heißt π *zerlegbar*, falls es $z, w \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z), \mathrm{N}(w) > 1$ und $\pi = z \cdot w$ gibt. Unzerlegbare Elemente können also nur in trivialer Weise als Produkt geschrieben werden.
Vor dem Satz über die Existenz und Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[\mathrm{i}]$ benötigen wir noch

Lemma 1.3. *Jede Gauß'sche ganze Zahl z mit $\mathrm{N}(z) > 1$ besitzt ein Primelement in $\mathbb{Z}[\mathrm{i}]$ als Teiler.*

Beweis. Unter allen Teilern von z in $\mathbb{Z}[\mathrm{i}]$ mit Norm größer als 1 gibt es einen Teiler π mit minimaler Norm. Wir behaupten, dass π unzerlegbar und daher nach Proposition 1.2 ein Primelement ist. Angenommen, $\pi = u \cdot w$ für Gauß'sche ganze Zahlen u und w mit Norm größer als 1. Dann folgt $u \mid \pi \mid z$ und $\mathrm{N}(\pi) = \mathrm{N}(u) \cdot \mathrm{N}(w) > \mathrm{N}(u)$, im Widerspruch zur Wahl von π. □

Wir erhalten schließlich den zuvor angekündigten

Satz 2 (Primfaktorzerlegung in $\mathbb{Z}[\mathrm{i}]$)**.** *Jede Gauß'sche ganze Zahl $z \neq 0$ besitzt eine bis auf Reihenfolge und Einheiten eindeutige Darstellung als Produkt von Primelementen in $\mathbb{Z}[\mathrm{i}]$.*
Präziser: Es gibt eine Darstellung $z = e \cdot \pi_1 \cdots \pi_r$ mit ganzem $r \geq 0$, $e \in \mathbb{Z}[\mathrm{i}]^\times$ und Primelementen $\pi_1, \ldots, \pi_r$ in $\mathbb{Z}[\mathrm{i}]$. Für jede weitere Darstellung $z = f \cdot q_1 \cdots q_s$ mit ganzem $s \geq 0$, $f \in \mathbb{Z}[\mathrm{i}]^\times$ und Primelementen $q_1, \ldots, q_s$ in $\mathbb{Z}[\mathrm{i}]$ gilt $r = s$ und es gibt eine Permutation $q_1', \ldots, q_r'$ dieser Elemente mit $q_j'/\pi_j \in \mathbb{Z}[\mathrm{i}]^\times$ für $j = 1, \ldots, r$.

Beweis. Wir führen einen Beweis durch vollständige Induktion über $n = \mathrm{N}(z)$.
Als Induktionsanfang betrachten wir $\mathrm{N}(z) = 1$. Gemäß Lemma 1.1 bedeutet das $z = e \in \mathbb{Z}[\mathrm{i}]^\times$. Hier liegt obige Darstellung mit $r = 0$ vor. Da Primelemente nach Definition eine Norm größer als 1 haben, muss in jeder weiteren Darstellung wie im Satz $s = 0$ gelten; damit ist hier auch die Eindeutigkeit gezeigt.
Wir dürfen nun für den Induktionsschritt annehmen, dass $n > 1$ gilt und jedes $w \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$ mit $\mathrm{N}(w) < n$ eine im Satz angeführte, bis auf Reihenfolge und Einheiten eindeutige Darstellung besitzt.
Zuerst zur *Existenz:* Wegen $\mathrm{N}(z) = n > 1$ ist Lemma 1.3 anwendbar und liefert ein Primelement π in $\mathbb{Z}[\mathrm{i}]$, das z teilt. Wir schreiben $z = \pi \cdot w$ für ein $w \in \mathbb{Z}[\mathrm{i}] \setminus \{0\}$. Anwendung der Norm liefert $n = \mathrm{N}(z) = \mathrm{N}(\pi) \cdot \mathrm{N}(w) > \mathrm{N}(w)$; laut Induktionsannahme gilt folglich $w = e \cdot \pi_1 \cdots \pi_r$ mit den Bezeichnungen im Satz. Insgesamt erhalten wir $z = w \cdot \pi = e \cdot \pi_1 \cdots \pi_r \pi$.
Nun zur *Eindeutigkeit:* Sei $z = f \cdot q_1 \cdots q_s$ eine weitere Darstellung mit den Bedingungen wie im Satz. Wegen $\pi \mid z$ gibt es (laut Definition nach Induktion) ein ganzes $1 \leq k \leq s$ mit $\pi \mid q_k$.[2] Wir schreiben $q_k = \varepsilon \cdot \pi$ für ein $\varepsilon \in \mathbb{Z}[\mathrm{i}]$. Da q_k nach Proposition 1.2 unzerlegbar ist, folgt $\varepsilon \in \mathbb{Z}[\mathrm{i}]^\times$. Erneutes Einsetzen liefert mit $z/\pi = (f/\varepsilon) \cdot q_1 \cdots q_{k-1} q_{k+1} \cdots q_s$ eine weitere Darstellung von w als Produkt von $s - 1$ Primelementen. Daraus schließen wir nach Induktionsannahme $s - 1 = r$ und die Existenz einer Permutation $q'_1, \ldots, q'_{s-1}$ von $q_1, \ldots, q_{k-1}, q_{k+1}, \ldots, q_s$ mit $q'_j/\pi_j \in \mathbb{Z}[\mathrm{i}]^\times$ für $j = 1, \ldots, r$. Setzen wir schließlich $q'_s \coloneqq q_k$ und beachten $q_k/\pi = \varepsilon \in \mathbb{Z}[\mathrm{i}]^\times$, so beendet dies auch den Beweis der Eindeutigkeit. □

Zum besseren Verständnis dieser Primfaktorzerlegung wollen wir schließlich noch die Primelemente in $\mathbb{Z}[\mathrm{i}]$ charakterisieren und beginnen mit den vielversprechenden Kandidaten, die wir bereits aus $\mathbb{Z}$ kennen:

Proposition 2.1. *Eine Primzahl $p \in \mathbb{Z}_{>0}$ ist genau dann ein Primelement in $\mathbb{Z}[\mathrm{i}]$, wenn es kein $z \in \mathbb{Z}[\mathrm{i}]$ mit $p = \mathrm{N}(z)$ gibt.*

Beweis. Wir beweisen die logische Kontraposition (laut Proposition 1.2):

$$p \text{ ist zerlegbar} \quad \Longleftrightarrow \quad \exists z \in \mathbb{Z}[\mathrm{i}] \colon \mathrm{N}(z) = p$$

„$\Longrightarrow$“: Es gibt z und $w \in \mathbb{Z}[\mathrm{i}]$ mit $p = z \cdot w$ und $\mathrm{N}(z), \mathrm{N}(w) > 1$. Anwendung der Norm liefert $p^2 = \mathrm{N}(p) = \mathrm{N}(z) \cdot \mathrm{N}(w)$. Wegen der Eindeutigkeit der Primfaktorzerlegung von positiven ganzen Zahlen und der Voraussetzung folgt $\mathrm{N}(z) = \mathrm{N}(w) = p$.
„$\Longleftarrow$“: Aus $p > 1$ folgt $p = \mathrm{N}(z) = \mathrm{N}(\overline{z}) > 1$. Nun erhalten wir mit $p = \mathrm{N}(z) = z \cdot \overline{z}$ die gewünschte Zerlegung. □

Das nächste Resultat gibt eine notwendige Bedingung für Primelemente an:

Lemma 2.2. *Jedes Primelement π in $\mathbb{Z}[\mathrm{i}]$ erfüllt $\mathrm{N}(\pi) = p$ oder $\mathrm{N}(\pi) = p^2$ für eine Primzahl $p \in \mathbb{Z}_{>0}$. Bei $\mathrm{N}(\pi) = p^2$ gilt außerdem $\pi = e \cdot p$ für ein $e \in \mathbb{Z}[\mathrm{i}]^\times$.*

Bemerkung. Der Zusatz besagt, dass der zweite Fall nur für Primelemente auf den Achsen der Gauß'schen Zahlenebene eintreten kann.

Beweis. Ist $\mathrm{N}(\pi)$ eine Primzahl, bleibt nichts zu zeigen. Sonst gibt es positive ganze Zahlen $a, b > 1$ mit $\mathrm{N}(\pi) = ab$. Aus $\mathrm{N}(\pi) = \pi\overline{\pi} = ab$ ergibt sich $\pi \mid a$ oder $\pi \mid b$ in $\mathbb{Z}[\mathrm{i}]$, o. B. d. A. $\pi \mid a$. Wir schreiben $a = \pi e$ für ein $e \in \mathbb{Z}[\mathrm{i}]$ und erhalten daraus $\pi\overline{\pi} = ab = \pi e b$, d. h. $\overline{\pi} = eb$. Nachdem mit π auch $\overline{\pi}$ ein Primelement (und nach Proposition 1.2 unzerlegbar) ist, gilt $e \in \mathbb{Z}[\mathrm{i}]^\times$ oder $b \in \mathbb{Z}[\mathrm{i}]^\times$. Da Letzteres im Widerspruch zu $b > 1$ steht, bleibt nur $e \in \mathbb{Z}[\mathrm{i}]^\times$ zu untersuchen. Dann gilt aber

[2] Die Möglichkeit $\pi \mid f$ kann durch Anwendung der Norm ausgeschlossen werden.

$a^2 = \mathrm{N}(a) = \mathrm{N}(\pi) \cdot \mathrm{N}(e) = ab \cdot 1$, also $a = b$. Jede Zerlegung von $\mathrm{N}(\pi)$ in zwei positive ganze Faktoren größer als 1 führt also zur Gleichheit dieser beiden Faktoren. Folglich kann $\mathrm{N}(\pi)$ nur einen Primfaktor $p \in \mathbb{Z}_{>0}$ und diesen nur mit Vielfachheit 2 haben. Notwendigerweise gilt $a = p$ in dieser Zerlegung, was auch den Zusatz beweist. □

Abschließend formulieren wir noch den anfangs erwähnten Satz über die Darstellbarkeit natürlicher Zahlen als Summe zweier Quadratzahlen:

Satz 3. *Eine positive ganze Zahl n ist genau dann die Norm einer Gauß'schen ganzen Zahl, wenn in der Primfaktorzerlegung von n über $\mathbb{Z}$ alle in $\mathbb{Z}[\mathrm{i}]$ unzerlegbaren Primzahlen nur in gerader Vielfachheit vorkommen.*

Beweis. Wir zeigen die beiden Implikationen einzeln:
„$\Longrightarrow$“: Sei $n = \mathrm{N}(z)$ für ein $z \in \mathbb{Z}[\mathrm{i}]$. Laut Satz 2 gibt es eine Primfaktorzerlegung $z = e \cdot \pi_1 \cdots \pi_r$ in $\mathbb{Z}[\mathrm{i}]$ mit den Bezeichnnungen wie dort. Folglich ist $n = \mathrm{N}(z) = \mathrm{N}(\pi_1) \cdots \mathrm{N}(\pi_r)$. Sei nun $p \in \mathbb{Z}_{>0}$ eine in $\mathbb{Z}[\mathrm{i}]$ unzerlegbare Primzahl. Nach Proposition 2.1 kann $\mathrm{N}(\pi_j) = p$ nicht gelten, laut Lemma 2.2 ist $\mathrm{v}_p(\mathrm{N}(\pi_j))$ für alle $j = 1, \ldots, r$ entweder 0 oder 2, insbesondere gerade. Folglich muss auch

$$\mathrm{v}_p(n) = \mathrm{v}_p(\mathrm{N}(\pi_1)) + \cdots + \mathrm{v}_p(\mathrm{N}(\pi_r))$$

gerade sein.
„$\Longleftarrow$“: Alle in $\mathbb{Z}[\mathrm{i}]$ unzerlegbaren Primteiler von n mögen in gerader Vielfachheit vorkommen. Sei $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s}$ die Primfaktorzerlegung von n in $\mathbb{Z}$, wobei $r, s \in \mathbb{Z}_{\geq 0}$, $p_1, \ldots, p_r$ paarweise verschiedene, in $\mathbb{Z}[\mathrm{i}]$ unzerlegbare Primzahlen, $q_1, \ldots, q_s$ paarweise verschiedene, in $\mathbb{Z}[\mathrm{i}]$ zerlegbare Primzahlen, $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s$ positive ganze Zahlen und $\alpha_1, \ldots, \alpha_r$ sämtlich gerade seien. Gemäß Proposition 2.1 gibt es $z_1, \ldots, z_s \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z_j) = q_j$ für alle ganzen $1 \leq j \leq s$. Dann ist

$$z \coloneqq p_1^{\alpha_1/2} \cdots p_r^{\alpha_r/2} z_1^{\beta_1} \cdots z_s^{\beta_s}$$

eine Gauß'sche ganze Zahl mit Norm n. □

Aufgaben

Aufgabe 1. Führe Dir die Einleitung zu Gemüte.

Aufgabe 2. Beweise Satz 1.

Aufgabe 3. Beweise Proposition 1.2.

Aufgabe 4. Sei $z = a + b\,\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ mit $a, b \in \mathbb{Z}$ und $\mathrm{ggT}(a, b) = 1$. Zeige, dass jeder ungerade Primteiler (in $\mathbb{Z}$) von $\mathrm{N}(z)$ kongruent zu 1 modulo 4 ist.

Aufgabe 5. Beweise den *Satz von Wilson*: Eine ganze Zahl $n \geq 2$ ist genau dann eine Primzahl, wenn $(n-1)! \equiv -1 \pmod{n}$ gilt.

Aufgabe 6. Sei $p \in \mathbb{Z}_{>0}$ eine Primzahl mit $p \equiv 1 \pmod{4}$. Dann gilt

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}.$$

Aufgabe 7. Wir beweisen, dass jede Primzahl $p \equiv 1 \pmod{4}$ die Norm einer Gauß'schen ganzen Zahl ist:

1. Sei $0 < x < p$ eine ganze Zahl mit $x^2 \equiv -1 \pmod{p}$ (konstruiert z. B. wie in Aufgabe 6) und betrachte das *Gitter*
$$G \coloneqq \{a + b\,\mathrm{i} \mid ax \equiv b \pmod{p}\}.$$
Die *Fundamentalzelle* von G sei das Parallelogramm mit den Eckpunkten 0, $1+x\,\mathrm{i}$, $1+(p+x)\,\mathrm{i}$ und $p\,\mathrm{i}$. Um jeden der Eckpunkte wird ein Kreis mit Fläche $F > p$ gezeichnet. Man beweise, dass sich mindestens zwei Kreise schneiden.

2. Folgere daraus, dass es ein $z \in G \setminus \{0\}$ mit Abstand kleiner oder gleich $2 \cdot \sqrt{F/\pi}$ gibt. (Hier bezeichnet π die Kreiszahl.)

3. Wähle F hierin passend und beweise schließlich $\mathrm{N}(z) = p$.

Aufgabe 8. Sei $p \in \mathbb{Z}_{>0}$ eine Primzahl. Zeige: Genau dann ist p ein Primelement in $\mathbb{Z}[\mathrm{i}]$, wenn $p \equiv 3 \pmod{4}$ gilt.

Aufgabe 9. Sei $p \in \mathbb{Z}_{>0}$ eine Primzahl mit $p \equiv 1 \pmod{4}$. Wir untersuchen noch, wie viele im Wesentlichen verschiedene Darstellungen von p als Summe zweier Quadratzahlen möglich sind. Seien dazu $p = a^2 + b^2 = x^2 + y^2$ mit a, b, x, $y \in \mathbb{Z}$.

1. Definiere *im Wesentlichen verschiedene* Darstellungen als Summe zweier Quadratzahlen.

2. Zeige, dass $a^2y^2 - b^2x^2$ durch p teilbar ist.

3. Beweise, dass sich p im Wesentlichen nur auf eine Art als Summe zweier Quadratzahlen darstellen lässt (bei sinnvoller Definition).

Tipps zu ausgewählten Aufgaben

Aufgabe 1. Einfach über den eigenen Schatten springen! ;)

Aufgabe 2. Nähere w/z durch eine möglichst nahe liegende Zahl $q \in \mathbb{Z}[\mathrm{i}]$ an und verwende die Multiplikativität des Absolutbetrages in $\mathbb{C}$.

Aufgabe 3. Um unzerlegbare Elemente als Primelemente nachzuweisen, gehe von $\pi \mid zw$, $\pi \nmid z$ aus, betrachte alle Gauß'schen ganzen Zahlen $\zeta \neq 0$ der Form $\lambda\pi + \mu z$ und zeige durch Division mit Rest (Satz 1), dass eine Zahl e unter ihnen mit kleinster Norm alle anderen ζ teilt.

Aufgabe 4. Verwende quadratische Reste.

Aufgabe 5. Zerlege bei primem n die Menge $\{1, \ldots, n-1\}$ in Teilmengen $\{a, b\}$, sodass $ab \equiv 1 \pmod{n}$ gilt. Wann kann das nicht funktionieren? Zeige in die andere Richtung $(n-1)! \equiv 0 \pmod{n}$ für zusammengesetzte Zahlen $n > 4$.

Aufgabe 6. Verwende den Satz von Wilson (Aufgabe 5).

Aufgabe 7. Ad 7.1: Betrachte die Zerteilung des Kreises um den Ursprung durch das Gitter und verschiebe alle „Schnipsel“ in die Fundamentalzelle. Aufgrund ihrer Gesamtfläche können sie nicht alle disjunkt sein. Ad 7.2: Nutze 7.1 durch Translation aus. Ad 7.3: Wähle F klein genug, dass $\mathrm{N}(z) < 2p$ ist, und zeige $p \mid \mathrm{N}(z)$.

Aufgabe 8. Verwende Proposition 2.1 und Aufgabe 7.

Aufgabe 9. Setze $z \coloneqq a + b\,\mathrm{i}$, $w \coloneqq x + y\,\mathrm{i}$ und berechne zum Beweis von 9.3 nach Verwendung der binomischen Formel in 9.2 entweder $\mathrm{N}(z \cdot w)$ oder $\mathrm{N}(\overline{z} \cdot w)$ auf zwei verschiedene Arten.

Lösungsvorschläge zu ausgewählten Aufgaben

Lösungsvorschläge von Moritz Hiebler

Aufgabe 1. Unlösbar.

Aufgabe 2. Sei $a \coloneqq \lfloor \Re(w/z) \rceil$, $b \coloneqq \lfloor \Im(w/z) \rceil$, $q \coloneqq a + b\,\mathrm{i}$ und $r \coloneqq w - qz$.[3] Nach Definition gilt

$$\left|\frac{r}{z}\right| = \left|\frac{w}{z} - q\right| \leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \sqrt{\frac{1}{2}}$$

und daraus folgt wegen $\mathrm{N}(z) > 0$ auch

$$w = qz + r \qquad \text{mit} \qquad \mathrm{N}(r) = |r|^2 \leq \frac{|z|^2}{2} = \frac{\mathrm{N}(z)}{2} < \mathrm{N}(z).$$

Aufgabe 3. 1.2(a) $\implies$ 1.2(b): Sei π ein Primelement in $\mathbb{Z}[\mathrm{i}]$ und $1 \cdot \pi = z \cdot w$. Daher gilt $\pi \mid z \cdot w$ und nach Voraussetzung $\pi \mid z$ oder $\pi \mid w$, o. B. d. A. $\pi \mid z$. Schreibe $z = \pi u$ für ein $u \in \mathbb{Z}[\mathrm{i}]$. Einsetzen liefert $\pi = (\pi u)w \iff 1 = uw$ und Lemma 1.1 ergibt $w \in \mathbb{Z}[\mathrm{i}]^\times$.
1.2(a) $\implies$ 1.2(b): Sei nun π unzerlegbar und es gelte $\pi \mid z \cdot w$ sowie $\pi \nmid z$. Wir müssen $\pi \mid w$ beweisen. Dazu zeigen wir zuerst, dass es s, $t \in \mathbb{Z}[\mathrm{i}]$ mit $s\pi + tz \in \mathbb{Z}[\mathrm{i}]^\times$ gibt.
Unter allen Zahlen ζ aus $\mathbb{Z}[\mathrm{i}] \setminus \{0\}$ der Form $\lambda\pi + \mu z$ mit λ, $\mu \in \mathbb{Z}[\mathrm{i}]$ sei $e \coloneqq s\pi + tz$ (s, $t \in \mathbb{Z}[\mathrm{i}]$) eine mit kleinster Norm. Wir behaupten $e \mid \zeta$ und dividieren dazu ζ durch e mit Rest (vgl. Satz 1): Es gibt q, $r \in \mathbb{Z}[\mathrm{i}]$ mit $\zeta = qe + r$ und $\mathrm{N}(r) < \mathrm{N}(e)$. Aus $r = \zeta - qe = (\lambda - qs)\pi + (\mu - qt)z$ und der Voraussetzung, dass e unter allen diesen Zahlen $\neq 0$ minimale Norm hat, folgt $r = 0$; d. h. ζ ist durch e teilbar. Für $\zeta = 1 \cdot \pi + 0 \cdot z$ erhalten wir $e \mid \pi$, also ein $v \in \mathbb{Z}[\mathrm{i}]$ mit $\pi = e \cdot v$. Da π unzerlegbar ist, folgt $e \in \mathbb{Z}[\mathrm{i}]^\times$ oder $v \in \mathbb{Z}[\mathrm{i}]^\times$. In letzterem Fall ergibt sich für $\zeta = 0 \cdot \pi + 1 \cdot z = z$ der Widerspruch $\pi \mid \pi \cdot v^{-1} = e \mid z$ zur Annahme $\pi \nmid z$. Also bleibt nur $e \in \mathbb{Z}[\mathrm{i}]^\times$ übrig.
Wir schließen $w = (se^{-1}w)\pi + (e^{-1}t)zw$ durch Multiplikation von $e = s\pi + tz$ mit $e^{-1}w$. Nun teilt π beide Summanden rechts, also auch w.

Aufgabe 4. Sei p ein ungerader Primteiler von $\mathrm{N}(z) = a^2 + b^2$. Wäre b durch p teilbar, so auch $a^2 = \mathrm{N}(z) - b^2$ und folglich a, im Widerspruch zu $\mathrm{ggT}(a, b) = 1$. Damit gibt es eine Lösung $y \in \mathbb{Z}$ der linearen Kongruenz $by \equiv 1 \pmod{p}$. Multiplikation von $a^2 \equiv -b^2 \pmod{p}$ mit y^2 liefert $(ay)^2 \equiv -(by)^2 \equiv -1 \pmod{p}$ und -1 ist somit ein quadratischer Rest modulo p. Nach dem quadratischen Reziprozitätsgesetz gilt schließlich

$$\left(\frac{-1}{p}\right) = 1 \quad \iff \quad (-1)^{(p-1)/2} = 1 \quad \iff \quad 2 \mid (p-1)/2 \quad \iff \quad p \equiv 1 \pmod{4}.$$

Aufgabe 5. Für $n = 2$ stimmt die Aussage. Sei von nun an $n > 2$ eine Primzahl. Zu jedem ganzen $1 \leq k \leq n-1$ gibt es wegen $\mathrm{ggT}(k, n) = 1$ eine eindeutige ganze Zahl $1 \leq \ell \leq n-1$ mit $k\ell \equiv 1 \pmod{n}$. Dabei ist $k = \ell$ äquivalent zu

$$k^2 \equiv 1 \pmod{n} \quad \iff \quad n \mid (k-1)(k+1) \quad \iff \quad (n \mid k-1 \quad \text{oder} \quad n \mid k+1),$$

was im angegebenen Intervall nur für $k = 1$ und $k = n-1$ auftritt. Unterschiedlichen Zahlen $1 \leq k \leq n-1$ entsprechen dabei unterschiedliche Zahlen $1 \leq \ell \leq n-1$ und dem so definierten ℓ wird umgekehrt k zugewiesen. Im Produkt $1 \cdot \dots \cdot (n-1) = (n-1)!$ bleiben daher modulo n nach

[3] Dabei steht $\lfloor x \rceil$ bei $x \in \mathbb{R}$ für die ganze Zahl mit dem kleinsten Abstand zu x. Bei gleichem Abstand zu zwei ganzen Zahlen werde aufgerundet (*kaufmännisches Runden*).

Gruppierung der zusammengehörigen Faktoren nur 1, weitere $(n-3)/2$ Einser und $n-1 \equiv -1 \pmod{n}$ stehen und wir erkennen $(n-1)! \equiv -1 \pmod{n}$.
Umgekehrt sei $n = ab$ zusammengesetzt mit $1 < a \leq b < n$. Bei $a < b$ kommen die beiden Zahlen a und b in $(n-1)!$ als Faktoren vor, und n teilt die Zahl $(n-1)!$, d. h. $(n-1)! \equiv 0 \not\equiv -1 \pmod{n}$. Ist n nicht das Quadrat einer Primzahl, können wir a als den kleinsten Primteiler von n und b als dessen Komplementärteiler wählen. Bei $n = 2^2 = 4$ gilt $(4-1)! = 6 \not\equiv -1 \pmod{4}$, bei $p \geq 3$ kommen in $(p^2-1)!$ zumindest p und $2p < p^2$ als Faktoren vor und es gilt wieder $(n-1)! \equiv 0 \not\equiv -1 \pmod{n}$. Dies beschließt den Beweis, dass $(n-1)! \not\equiv -1 \pmod{n}$ für alle zusammengesetzten $n \geq 2$.

Aufgabe 6. Sei $t \coloneqq (p-1)/2$. Wir ersetzen für $1 \leq k \leq t$ bei dem Satz von Wilson in $(p-1)!$ die Faktoren $p-k$ modulo p durch $-k$ und erhalten wegen $t+1 = p-t$ und der Voraussetzung, dass $(p-1)/2$ gerade ist, die Kongruenz

$$-1 \equiv (p-1)! = 1 \cdots t(p-t) \cdots (p-1) \equiv 1 \cdots t(-t) \cdots (-1) = (-1)^{(p-1)/2}(t!)^2 = (t!)^2 \pmod{p},$$

was zu zeigen war.

Aufgabe 7. Wir beweisen zuerst, dass man im Gitter G translieren kann: Aus u, $w \in G$ folgt $u - w \in G$.
Schreiben wir nämlich $u = a + b\,\mathrm{i}$, $w = c + d\,\mathrm{i}$ mit a, b, c, $d \in \mathbb{Z}$ mit $ax \equiv b \pmod{p}$ und $cx \equiv d \pmod{p}$, so gilt $u - w = (a-c) + (b-d)\,\mathrm{i}$ und $(a-c)x \equiv (b-d) \pmod{p}$ laut den Rechenregeln für Kongruenzen. Nun zu den Aufgaben:

7.1: Als Parallelogramm beträgt die Fläche der Fundamentalzelle $p \cdot 1 = p$ (Seite auf der imaginären Achse der Länge p, Höhe vom Betrag 1). Der Kreis k um 0 wird durch die „Gitterlinien“ $\Re z = n$, $n \in \mathbb{Z}$, bzw. $\Im z = x\Re z + np$, $n \in \mathbb{Z}$ in „Bruchstücke“ zerlegt, die wir alle in die Fundamentalzelle verschieben. Da dieser Kreis Fläche $F > p$ hat, können die verschobenen Bruchstücke nicht alle disjunkt sein (andernfalls wäre die Summe ihrer Flächen kleiner oder gleich der der Fundamentalzelle). Seien A und B zwei translierte Bruchstücke (in der Fundamentalzelle) mit gemeinsamen Punkten. Wir verschieben k so auf Kreise mit Mittelpunkten $u' \neq w'$ von G, dass diese mit der Fundamentalzelle genau A bzw. B als Schnittmenge haben. Daher schneiden sich zwei verschobene Kreise um Punkte $u' \neq w'$ von G. Der Abstand von u' und w' – der alleinige Parameter, ob sich die Kreise schneiden (der Radius ist fixiert) – ist aber größer oder gleich dem Abstand von u' zu einem der Nachbarn innerhalb einer angrenzenden Zelle, weswegen sich zwei dieser Kreise schneiden. Transliert man diese Zelle zurück in die Fundamentalzelle, erhält man das Gewünschte.

7.2: Somit sind (mindestens) zwei Eckpunkte $u \neq w \in G$ der Fundamentalzelle höchstens das Doppelte des Radius $\sqrt{F/\pi}$ der Kreise voneinander entfernt. Dann ist $z \coloneqq u - w \in G \setminus \{0\}$ mit der gewünschten Abschätzung für den Betrag.

7.3: Für $F \coloneqq (\pi/3)p$ folgt $\mathrm{N}(z) = |z|^2 \leq (2\sqrt{F/\pi})^2 = 4p/3 < 2p$.[4] Schreiben wir $z = s + t\,\mathrm{i}$ mit s, $t \in \mathbb{Z}$ und $sx \equiv t \pmod{p}$, so ergibt sich

$$\mathrm{N}(z) = s^2 + t^2 \equiv s^2 + (sx)^2 = s^2(1+x^2) \equiv 0 \pmod{p},$$

woraus zusammen mit $0 < \mathrm{N}(z) < 2p$ zwingend $\mathrm{N}(z) = p$ folgt.

Aufgabe 8. Laut Proposition 2.1 ist p genau dann ein Primelement in $\mathbb{Z}[\mathrm{i}]$, wenn es kein $z \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z) = p$ gibt. Wegen $\mathrm{N}(1+\mathrm{i}) = 2$ ($\not\equiv 3 \pmod{4}$) müssen wir nur mehr ungerade Primzahlen

[4] F kann auf viele Arten gewählt werden, bei $F = cp$ muss nur $1 < c < \pi/2$ gelten. Die Wahl hier ist nur getroffen, um konkret zu bleiben.

p betrachten. Das Endresultat von Aufgabe 7 zeigt, dass alle Primzahlen $p \equiv 1 \pmod 4$ zerlegbar sind. Als einzige Kandidaten bleiben somit nur $p \equiv 3 \pmod 4$ übrig
Es bleibt noch zu beweisen, dass es zu Primzahlen $p \equiv 3 \pmod 4$ kein $z \in \mathbb{Z}[\mathrm{i}]$ mit $\mathrm{N}(z) = p$ gibt. Wir wählen den Ansatz $z = a + b\,\mathrm{i}$ mit $a, b \in \mathbb{Z}$. Für $d \coloneqq \mathrm{ggT}(a, b)$ gilt $d^2 \mid \mathrm{N}(z)$, d. h. bei $d > 1$ kann nicht $\mathrm{N}(z) = p$ gelten. Bei $d = 1$ kommt jedoch Aufgabe 3 zu greifen, wonach $p \equiv 3 \pmod 4$ kein Primteiler der Norm einer solchen Gauß'schen ganzen Zahl sein kann.

Aufgabe 9. Wir verwenden durchgehend die Gauß'schen ganzen Zahlen $z \coloneqq a+b\,\mathrm{i}$ und $w \coloneqq x+y\,\mathrm{i}$.

9.1: Da $\mathrm{N}(z) = \mathrm{N}(ez) = \mathrm{N}(e\overline{z})$ für alle Einheiten $e \in \mathbb{Z}[\mathrm{i}]^\times$ gilt, entschließen wir uns wie folgt:

Zwei Paare (a, b) und (x, y) ganzer Zahlen mit $n = a^2 + b^2 = x^2 + y^2$ nennen wir *im Wesentlichen verschiedene* Darstellungen von $n \in \mathbb{Z}_{\geq 0}$ als Summe zweier Quadratzahlen, falls

$$w \notin \{ez \mid e \in \mathbb{Z}[\mathrm{i}]^\times\} \cup \{e\overline{z} \mid e \in \mathbb{Z}[\mathrm{i}]^\times\}$$

für die zugeordneten Gauß'schen ganzen Zahlen z und w gilt.

Ohne die Verwendung von $\mathbb{Z}[\mathrm{i}]$ kann man äquivalent formulieren: $a \notin \{\pm x, \pm y\}$ (und $b \notin \{\pm x, \pm y\}$).

9.2: Das folgt direkt aus $a^2y^2 - b^2x^2 = (a^2 + b^2)y^2 - b^2(x^2 + y^2) = py^2 - pb^2$.

9.3: Laut 9.2 gilt $p \mid (ay)^2 - (bx)^2 = (ay - bx)(ay + bx)$ und somit $p \mid ay - bx$ oder $p \mid ay + bx$. Wir betrachten im ersten Fall

$$p^2 = \mathrm{N}(z)\,\mathrm{N}(w) = \mathrm{N}(zw) = \mathrm{N}((ax - by) + (ay + bx)\,\mathrm{i}) = (ax - by)^2 + (ay + bx)^2$$

und im zweiten

$$p^2 = \mathrm{N}(\overline{z})\,\mathrm{N}(w) = \mathrm{N}(\overline{z}w) = \mathrm{N}((ax + by) + (ay - bx)\,\mathrm{i}) = (ax + by)^2 + (ay - bx)^2.$$

In beiden Fällen teilt p die linke Seite und eine der beiden Quadratzahlen auf der rechten Seite; folglich auch die andere sowie deren Basis. Division durch p^2 liefert nun $1 = c^2+d^2$ für $c, d \in \mathbb{Z}$, wobei $(c, d) = (\frac{1}{p}(ax - by), \frac{1}{p}(ay + bx))$ im ersten Fall und $(c, d) = (\frac{1}{p}(ax + by), \frac{1}{p}(ay - bx))$ im zweiten. Wegen $c^2 \leq 1$ erhalten wir nach Durchprobieren die Lösungen $(\pm 1, 0)$ und $(0, \pm 1)$. Wenn allerdings beispielsweise $(\frac{1}{p}(ax - by), \frac{1}{p}(ay + bx)) = (0, \pm 1)$ gilt, d. h. $ax = by$ und $ay + bx = \pm p$, so ergibt sich durch Multiplikation der zweiten Gleichung mit y

$$pa = a(x^2 + y^2) = ay^2 + (ax)x = ay^2 + (by)x = \pm py \qquad \Longrightarrow \qquad a = \pm y,$$

und die beiden Darstellungen sind im Wesentlichen gleich. Auf ähnliche Weise ergibt sich im zweiten Fall $a = \pm x$ und wieder Im-Wesentlichen-Gleichheit.

Einen weiteren, viel ansprechenderen Beweis für 9.3, den ich erst beim Lösungsschreiben gefunden habe, möchte ich nicht vorenthalten:
Zuerst zeigen wir, dass z und w unzerlegbar und daher laut Proposition 1.2 Primelemente sind. Aus $z = u \cdot v$ für $u, v \in \mathbb{Z}[\mathrm{i}]$ folgt nämlich $\mathrm{N}(u)\,\mathrm{N}(v) = \mathrm{N}(z) = p$ und wegen der eindeutigen Primfaktorzerlegung in $\mathbb{Z}_{>0}$ entweder $\mathrm{N}(u) = 1$ oder $\mathrm{N}(v) = 1$, laut Lemma 1.1 erhalten wir entweder $u \in \mathbb{Z}[\mathrm{i}]^\times$ oder $v \in \mathbb{Z}[\mathrm{i}]^\times$. Analog weist man w als Primelement nach.
Jetzt ergibt sich mit $z\overline{z} = \mathrm{N}(z) = p = w\overline{w}$ aber $z \mid w\overline{w}$ und folglich $z \mid w$ oder $z \mid \overline{w}$. In der Primfaktorzerlegung von w bzw. $\overline{w}$ in $\mathbb{Z}[\mathrm{i}]$ gemäß Satz 2 kann aber nur ein Faktor vorkommen, weil w bzw. $\overline{w}$ selbst Primelemente sind. Also gilt $w = ez$ oder $w = e\overline{z}$ für ein $e \in \mathbb{Z}[\mathrm{i}]^\times$ und die beiden Darstellungen sind im Wesentlichen gleich.

Quellenangaben zu den Aufgaben

Aufgabe 1. –

Aufgabe 2. aus [2], §59, Beispiel 5

Aufgabe 3. aus [2], §59, Lemma 59.2

Aufgabe 4. nach [1], Aufgabe 214.b)

Aufgabe 5. aus [1], Aufgabe 210

Aufgabe 6. aus [1], Aufgabe 248.a)

Aufgabe 7. nach [1], Aufgabe 259

Aufgabe 8. nach [2], §59, Lemma 59.16

Aufgabe 9. aus [1], Aufgabe 260

Literatur

[1] A. Bartholomé, J. Rung, and H. Kern. *Zahlentheorie für Einsteiger*. Vieweg+Teubner, 7th edition, 2010.

[2] G. Scheja and U. Storch. *Lehrbuch der Algebra*, volume 2. B. G. Teubner Stuttgart, 1st edition, 1988.