

Elementare Zahlentheorie

Sommersemester 2017

Übungsblatt 9

20. Juni 2017

Aufgabe 40. (Nochmals zweiter Ergänzungssatz)

Sei p eine ungerade Primzahl.

- Berechnen Sie $-i(1+i)^2$.
- Berechnen Sie $2^{(p-1)/2}$ modulo p mittels (a) durch eine Rechnung in $\mathbb{Z}[i]$, und zwar koeffizientenweise modulo p .

Weisen Sie so den zweiten Ergänzungssatz für alle ungeraden Primzahlen p nach.

Aufgabe 41.

- Bestimmen Sie den ggT von $23 + 17i$ und $11 - 3i$.
Hinweis: Überlegen Sie sich, wie Sie eine Variante des Euklidischen Algorithmus formulieren können. Beweisen Sie, daß der Algorithmus terminiert und korrekt ist.
- Gilt eine analoge Version des Lemma von Bezout auf für $\mathbb{Z}[i]$ anstelle von \mathbb{Z} ?

Aufgabe 42. (Primfaktorzerlegung in $\mathbb{Z}[i]$)

- Aus der Vorlesung ist bekannt, dass der Ring $\mathbb{Z}[i]$ der ganzen Gauß'schen Zahlen faktoriell ist. Daher können wir, wie in \mathbb{Z} , zu jedem Primelement $\pi \in \mathbb{Z}[i]$ die Bewertung

$$v_\pi : \mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}_0$$

definieren, und zwar für jedes $x \in \mathbb{Z}[i]$, $x \neq 0$, durch

$$v_\pi(x) := \text{Anzahl der Faktoren } \pi \text{ in der Primfaktorzerlegung von } x = \max\{v \in \mathbb{N}_0 : \pi^v \mid x\}.$$

Darauf basierend können wir $v_{1+i}(10)$ auf folgende zwei verschiedenen Weisen bestimmen:

- In der Primfaktorzerlegung $10 = 2 \cdot 5 = (1+i)(1-i)(1+2i)(1-2i)$ kommt $1+i$ genau einmal vor, d.h. $v_{1+i}(10) = 1$.
- Aus $(1+i)^2 \mid 10$ und $(1+i)^3 \nmid 10$, folgt aber $v_{1+i}(10) = 2$!?!!

Wo liegt der Fehler?

- Bestimmen Sie die Primfaktorzerlegung von $7 + 74i \in \mathbb{Z}[i]$.

Aufgabe 43. (Pythagoräisches Tripel mittels $\mathbb{Z}[i]$)

- Zeigen Sie, daß ein $z \in \mathbb{Q}(i)$ genau dann Norm $N(z) = 1$ hat, wenn es ein $w \in \mathbb{Q}(i)$, $w \neq 0$ gibt mit $z = w/\bar{w}$.
- Sei $a^2 + b^2 = c^2$ ein Pythagoräisches Tripel. Wenden Sie (a) auf $z = (a+bi)/c$ an. Leiten Sie daraus eine Parametrisierung Pythagoräischer Tripel mit a, b, c teilerfremd und $2 \mid b$ ab.

Abgabe: Am kommenden Montag, den **26. Juni 2017**, bis zur Vorlesung in den Kasten im 3. Stock, Institut für Mathematik, Robert-Mayer-Straße 6-8. Downloads von Übungsblättern und Informationen zur Vorlesung unter

http://www.uni-frankfurt.de/65113368/17_SS_Elementare-Zahlentheorie