

---

Übungsblatt 3 zur Zahlentheorie

---

**Aufgabe 1.** (Normdarstellung)

Beweise die folgende Verallgemeinerung von Satz 1.4.12: Sei  $n = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$  mit  $p_i \in \mathbb{P}$  und  $e_i > 0$  für alle  $i \in \{1, \dots, r\}$ . Dann sind äquivalent:

- (a)  $n$  ist in der Form  $a^2 + 3b^2$  mit  $a, b \in \mathbb{Z}$  darstellbar.
- (b) Gibt es ein  $i \in \{1, \dots, r\}$  mit  $p_i \equiv 2 \pmod{3}$ , so ist  $e_i$  gerade.

**Hinweis** zu (a)  $\Rightarrow$  (b): Handle den Fall  $p_i = 2$  gesondert und unterscheide gerade und ungerade.

Für  $p_i > 2$  benutze  $a^2 + 3b^2 \equiv 0 \pmod{p_i}$  und unterscheide, ob  $b \equiv 0$  oder  $b \not\equiv 0 \pmod{p_i}$  ist. Im zweiten Fall ist  $-3 = -1 \cdot 3$  ein quadratischer Rest modulo  $p_i$  und man kann mit dem quadratischen Reziprozitätsgesetz und anderen Aussagen über das Legendre-Symbol einen Widerspruch erzeugen.

**Aufgabe 2.** (Einheitengruppen von euklidischen Ringen)

Zeige, dass einer der Ringe  $\mathbb{Z}[\sqrt{d}]$  mit  $d \in \{-2, 2\}$  euklidisch ist (sie sind es beide, aber bei einem ist es einfach) und dass

- (a)  $\mathbb{Z}[\sqrt{-2}]^\times$  endlich ist.
- (b)  $\mathbb{Z}[\sqrt{2}]^\times$  unendlich ist.

**Aufgabe 3.** (Dirichlet, angewandt)

Seien  $q_1, \dots, q_r$  paarweise verschiedene ungerade Primzahlen und  $e_1, \dots, e_r \in \{-1, 1\}$ . Zeige, dass die folgenden Mengen unendlich sind:

- (a)  $P_1 := \{p \in \mathbb{P} \mid \forall i \in \{1, \dots, r\} : \left(\frac{p}{q_i}\right) = e_i\}$
- (b)  $P_2 := \{p \in \mathbb{P} \mid \forall i \in \{1, \dots, r\} : \left(\frac{q_i}{p}\right) = e_i\}$

**Hinweis:** Finde jeweils eine unendliche Teilmenge.

**Abgabe bis Mittwoch, den 4. Mai** um 10:00 Uhr in die Zettelkästen neben F411.