Humboldt-Universität zu Berlin
Institut für Mathematik
Dr. D. Agostini, M. Sc. L. Lerer
L. Mädje

Zahlentheorie

SoSe 2019

Exercise Sheet 2

If you want your solutions to be corrected, you should hand them in by Monday, April 29.
Please write your name and immatriculation number on top of every exercise.

Exercise 2.1 (2 points) Let $d \in \mathbb{Z}$ be an integer with $d \equiv 1 \pmod 4$. Show that $\frac{1 \pm \sqrt{d}}{2}$ is integral over $\mathbb{Z}$.

Exercise 2.2 (1+2+2+2=7 points) Let R be an integral domain and $a, b \in R$. A *common divisor* of a and b is an element $c \in R$ such that $c|a$ and $c|b$. A *greatest common divisor* of a and b is an element d such that, if c is a common divisor of a and b then $c|d$.

a) Let $a, b \in R$. Show that if a greatest common divisor of a and b exists then it is unique up to multiplication by a unit.

From now on we assume that R is a UFD.

b) Show that for any $a, b \in R$ there exists a greatest common divisor.

c) Let d be a gcd of a, b. Is it true that there exist $x, y \in R$ such that $ax + by = d$?

d) Let $a, b, c \in R$ such that $\gcd(a, b) = 1$ and $ab = c^n$, for some integer $n \geq 1$. Prove that $a = ua_1^n$ and $b = vb_1^n$ for some $a_1, b_1 \in R$ and units $u, v \in R^\times$.

Exercise 2.3 (1+3+2+3+1+2=12 points) Let $\alpha = \frac{1+i\sqrt{11}}{2} \in \mathbb{C}$. The goal of the exercise is to prove that the ring $\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is Euclidean, with respect to the norm function $N : \mathbb{Z}[\alpha] \to \mathbb{Z}_{\geq 0}$ given by $N(a + b\alpha) = a^2 + ab + 3b^2$.

a) Check that $N(x) = |x|^2$ for all $x \in \mathbb{Z}[\alpha]$, where $|\cdot|$ is the complex absolute value.

b) Consider the parallelogram P with vertices $0, \alpha, \alpha + 1, 1$. Let $z \in \mathbb{C}$ be a point lying in the interior or on the perimeter of P. Prove that there exist a vertex v of P such that $|z - v| < 1$.

c) Deduce that for all $z \in \mathbb{C}$, we have

$$\min_{x \in \mathbb{Z}[\alpha]} |z - x| < 1.$$

d) Let $x, y \in \mathbb{Z}[\alpha], x \neq 0$. Show that there exists $q \in \mathbb{Z}[\alpha]$ such that $N(y - qx) < N(x)$.

e) Conclude that $\mathbb{Z}[\alpha]$ is Euclidean.

f) *(Extra)* Prove, using the norm, that the units of $\mathbb{Z}[\alpha]$ are $\{1, -1\}$.

Exercise 2.4 (3+3+2+3=11 points) The goal of the exercise is to find all integer solutions to the Diophantine equation $x^2 + 11 = y^3$. We will use results of the previous exercises.

a) Let $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ be a solution. Reduce the equation modulo 8 and prove that y must be odd.

b) Factorize the equation as $(x + \sqrt{-11})(x - \sqrt{-11}) = y^3$ inside the ring $\mathbb{Z}[\alpha]$ of Exercise 2.3. Prove that $\gcd(x + \sqrt{-11}, x - \sqrt{-11}) = 1$. (Use also the previous point).

c) Deduce using 2.2.d and 2.3.f that $x + \sqrt{-11} = u^3$ for some $u \in \mathbb{Z}[\alpha]$.

d) Find all solutions.