Goethe-Universität Frankfurt
Institut für Mathematik
Summer term 2020
6. Mai 2020

Elementare Zahlentheorie
Prof. Dr. Martin Möller
Dr. Jonathan Zachhuber
M.Sc. Riccardo Zuffetti

Übungsblatt 3

Aufgabe 1 (2 Punkte)

Prove that there are infinitely many primes $p \equiv 1 \bmod 4$ and infinitely many primes $p \equiv 3 \bmod 4$.

Aufgabe 2 (4 Punkte)

(i) Write 5 and 13 as sums of squares of two integers and as sums of squares of two non-integer rational numbers.

(ii) Let r be a rational number. Write it as $r = \frac{p}{q}$, for some $p, q \in \mathbb{Z}$ with $q \neq 0$. Prove that r can be represented as the sum of the squares of two rational numbers if and only if pq can be represented as the sum of the squares of two integers.

Aufgabe 3 (4 Punkte)

Let a and m be integers, with a odd and $m \geq 1$. We want to study the squares which are congruent to a modulo 2^m, i.e. the solutions of

$$X^2 \equiv a \mod 2^m. \tag{1}$$

(i) For $m \in \{1, 2\}$ and a odd, find *all* possible solutions of (1).

(ii) Let $m \geq 3$ and $a = 1$. Compute the four solutions (mod 2^m) of (1).

(iii) Let $m \geq 3$ and a odd. Prove that if (1) admits a solution, then $a \equiv 1 \bmod 8$.

Aufgabe 4 (6 Punkte)

Let n be a positive integer greater than 1. We denote by $S(n)$ the number of ways n can be represented as

$$n = x^2 + y^2, \quad \text{for some integer } 0 < y \leq x.$$

In this guided exercise, we find an explicit formula for $S(n)$.

(i) Suppose that n is even. Prove that

$$S(n) = \begin{cases} S(n/2) - 1, & \text{if } n \text{ is a square,} \\ S(n/2) + 1, & \text{if } n/2 \text{ is a square,} \\ S(n/2), & \text{otherwise.} \end{cases}$$

For this reason, from now on we suppose n to be odd.

(ii) The ring of the *Gaussian integer* is defined as

$$\mathbb{Z}[i] \coloneqq \{a + ib \,:\, a, b \in \mathbb{Z}\},$$

with ordinary addition and multiplication. The norm of a Gaussian integer $a + ib$ is $N(a + ib) = a^2 + b^2$. An element of $\mathbb{Z}[i]$ in a *unit* if it is invertible. Prove that the units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Fact: It is known that $\mathbb{Z}[i]$ is an Euclidean domain. This implies that every non-zero non-unit Gaussian integer factors uniquely (up to permutations) as a product of a unit and prime first-quadrant Gaussian integers. With *prime Gaussian integer*, we mean a non-unit $\eta \neq 0$ in $\mathbb{Z}[i]$ such that if $\eta | \xi_1 \xi_2$ with $\xi_j \in \mathbb{Z}[i]$, then $\eta | \xi_j$ for some j. If $N(\eta)$ is odd in $\mathbb{Z}$, then $N(\eta)$ is either a prime $\equiv 1 \bmod 4$ or a square of a prime $\equiv 3 \bmod 4$. We say that $a + ib$ is a *first-quadrant Gaussian integer* if $a > 0$ and $b \geq 0$.

(iii) Let $S'(n)$ be the number of first-quadrant Gaussian integers ξ with norm $N(\xi) = n$. Prove that

$$S'(n) = \begin{cases} 2S(n), & \text{if } n \text{ is not a square,} \\ 2S(n) + 1, & \text{if } n \text{ is a square.} \end{cases}$$

(iv) Write $n = n_1 \cdot n_2$ for some positive coprime integers n_1 and n_2. Prove that every Gaussian integer ξ such that $N(\xi) = n$ factors uniquely as $\xi = u \cdot \xi_1 \cdot \xi_2$, where u is a unit, ξ_1 and ξ_2 are first-quadrant Gaussian integers, and $N(\xi_j) = n_j$ for $j = 1, 2$.

(v) Let $n = n_1 \cdot n_2$. Prove that if n_1 and n_2 are coprime integers greater than 1, then

$$S'(n_1 \cdot n_2) = S'(n_1) \cdot S'(n_2).$$

(vi) Decompose n as

$$n = p_1^{a_1} \cdots p_r^{a_r} \cdot q_1^{b_1} \cdots q_\ell^{b_\ell},$$

where the p_j (respectively q_j) are distinct primes such that $p_j \equiv 1 \bmod 4$ (resp. $q_j \equiv 3 \bmod 4$). Prove that if some b_j is odd, then $S(n) = 0$. Prove that if all b_j are even, then

$$S(n) = \begin{cases} (a_1 + 1) \cdots (a_r + 1)/2, & \text{if } n \text{ is not a square,} \\ \big((a_1 + 1) \cdots (a_r + 1) - 1\big)/2, & \text{if } n \text{ is a square.} \end{cases}$$

Please, upload your solutions on the Olat page of this course, by **14:00** on **Wednesday, 13.5.2020**.