Goethe-Universität Frankfurt
Institut für Mathematik
Summer term 2020
23. Juni 2020

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

Übungsblatt 10

Aufgabe 1 (4 Punkte)

Let Λ be a lattice in $\mathbb{R}^n$, for some $n \geq 1$. In this guided exercise, we want to prove that there exists a basis $\mathcal{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ of $\mathbb{R}^n$ such that every element of Λ can be written in a unique way as an *integral* combination (i.e. with coefficients in $\mathbb{Z}$) of elements of $\mathcal{B}$.

(i) Let $\mathbf{v}_1, \dots, \mathbf{v}_n$ be linearly independent vectors of Λ. For every $i = 1, \dots, n$, we define

$$S_i \coloneqq \{x_i \in (0,1] \,:\, \exists x_j \in \mathbb{R} \text{ s.t. } \sum_{j=1}^{i} x_j \mathbf{v}_j \in \Lambda\}.$$

Prove that S_i is *non empty* and *finite* for every i.

(ii) Let $u_{i,i}$ be the minimum of S_i. We denote by $u_{i,j}$ the real numbers such that

$$\mathbf{b}_i \coloneqq \sum_{j=1}^{i} u_{i,j} \mathbf{v}_j \in \Lambda,$$

whose existence is ensured by the previous point. Prove that $\mathcal{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n)$ satisfies the desired condition.

Aufgabe 2 (5 Punkte)

Let $a, b, m, d \in \mathbb{Z}_{>0}$, with d not a square.

(i) Suppose that (x_1, y_1) and (x_2, y_2) are solutions of Pell's equations $X^2 - dY^2 = a$ and $X^2 - dY^2 = b$, respectively. Prove that

$$(x_1, y_1) \cdot (x_2, y_2) \coloneqq (x_1 x_2 + d y_1 y_2, x_1 y_2 + y_1 x_2)$$

is a solution of Pell's equation $X^2 - dY^2 = ab$.

(ii) Prove that if Pell's equation $X^2 - dY^2 = m$ admits a solution, then it has *infinitely many* solutions.

(iii) Compute at least 3 *positive* solutions of $X^2 - 3Y^2 = 6$.

Aufgabe 3 (7 Punkte)

(i) Let $(G, \bullet)$ be an abelian group, and let 1_G be its neutral element. Prove that the subset of G of the n-torsion elements

$$\mathrm{Tor}_n(G) \coloneqq \{g \in G \,:\, g^n = 1_G\}, \qquad \text{with } n \geq 1,$$

endowed with the operation $\bullet$, is a subgroup of $(G, \bullet)$.

(ii) Prove that if G is a finite cyclic group of even cardinality, then $\#\operatorname{Tor}_2(G) = 2$.

(iii) Let $G_1, \dots, G_n$ be abelian groups and let $G = G_1 \times \cdots \times G_n$. Prove that

$$\operatorname{Tor}_2(G) = \operatorname{Tor}_2(G_1) \times \cdots \times \operatorname{Tor}_2(G_n).$$

(iv) Compute $\#\operatorname{Tor}_2\left(\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^*\right)$ and $\#\operatorname{Tor}_2\left(\left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^*\right)$.

(v) Prove that $\#\operatorname{Tor}_2\left(\left(\frac{\mathbb{Z}}{2^k\mathbb{Z}}\right)^*\right) = 4$, for every $k \geq 3$.

(vi) Let p be an odd prime. Prove that $\#\operatorname{Tor}_2\left(\left(\frac{\mathbb{Z}}{p^k\mathbb{Z}}\right)^*\right) = 2$, for every $k \geq 1$.

(vii) Let $m \geq 2$ be an integer and $p(m)$ the number of prime divisors of m. Prove that

$$\#\{a \in \mathbb{Z}/2m\mathbb{Z} : a^2 \equiv 1 \bmod 4m\} = 2^{p(m)}.$$

Please, upload your solutions on the Olat page of this course, by **14:00** on **Wednesday, 01.07.2020**.