Exercise Sheet 1

Filippo Berta

September 2025

Exercise 1. Let p be a prime number that satisfies $p \equiv 1 \pmod 4$. Explain and verify the assertions of the following *one-sentence proof*[1] of the fact that p can be written as a sum of two squares:

The involution of the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ *defined by*

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ *is odd and the involution by* $(x, y, z) \mapsto (x, z, y)$ *also has a fixed point.*

Exercise 2 (Pell equation)**.** Let $d \geq 2$ be a square-free integer. Let $K = \mathbb{Q}(\sqrt{d})$ and $A = \mathbb{Z}[\sqrt{d}]$. Given an element $z = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ we let $\overline{z} = x - y\sqrt{d}$ and $\mathrm{Nr}(z) = z \cdot \overline{z}$. We also define the Pell equation

$$x^2 - dy^2 = 1 \tag{1}$$

1. Prove that $\mathrm{Nr}(z_1 z_2) = \mathrm{Nr}(z_1)\,\mathrm{Nr}(z_2)$ for every $z_1, z_2 \in K$.
2. Let $A^\times$ be the group of units of the ring A. Show that

   $$A^\times = \{z \in A : \mathrm{Nr}(z) = \pm 1\}.$$

   and show that the set of solutions of (1)

   $$A^{(1)} = \{z = a + b\sqrt{d} \in A : \mathrm{Nr}(z) = 1\}$$

   has index at most two in $A^\times$.
3. Show that the map

   $$A^{(1)} \to (\mathbb{R}, +);\ a + b\sqrt{d} \mapsto \log|a + b\sqrt{d}|$$

   is a group homomorphism with kernel $\{\pm 1\}$ and its image is a *discrete* subgroup of $(\mathbb{R}, +)$.

[1] The proof is due to Don Zagier [Zag90]

4. Show that a discrete subgroup of $(\mathbb{R}, +)$ is cyclic.

5. Conclude that the group of solutions of the Pell equation $A^{(1)}$ satisfies $A^{(1)} = \langle \pm z_0 \rangle$ for some $z_0 \in A^{(1)}$, that is $A^{(1)}$ can be generated by two elements, one of which being -1.

Such a z_0 is call *fundamental solution* of the Pell equation. There exist algorithms to find the fundamental solution, for the moment we will limit ourselves to find non-trivial (that is $(x, y) \neq (\pm 1, 0)$) solutions.

6. Let $\alpha = \mathbb{R} \setminus \mathbb{Q}$ and $n \geq 1$ be an integer. Show that there exist $a \in \mathbb{Z}$ and $b \in \{1, \ldots, n\}$ so that
$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{(n+1)b}.$$
In particular, deduce that there exist infinitely many pairs $(a, b) \in \mathbb{Z}$ $(b \neq 0)$ with $\gcd(a, b) = 1$ and
$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}.$$
Hint: For the first assertion: consider the $n + 2$-number $B = \{\{0\}, \{\alpha\}, \cdots, \{n\alpha\}, 1\} \subset [0, 1]$, where $\{x\} = x - \lfloor x \rfloor$ is the fractional part of x. What can you say about $\min_{x \neq y \in B} |x - y|$?

7. Show that there exists $n \in \mathbb{Z}$ satisfying $1 \leq |n| \leq 2\sqrt{d} + 1$ and so that $x^2 - dy^2 = n$ has infinitely many solutions $(x, y) \in \mathbb{Z}$ with x, y positive. Show also that there exist two distinct solutions (x_1, y_1) and (x_2, y_2) with $x_1 \equiv x_2 \pmod{n}$ and $y_1 \equiv y_2 \pmod{n}$.

8. Let (x_i, y_i), $i = 1, 2$, as in the previous subexercise. Show that $z_0 = \frac{x_1 + \sqrt{d} y_1}{x_2 + \sqrt{d} y_2} \in A^\times$ and it is a non-trivial (that is, $z_0 \neq \pm 1$) solution of the Pell equation.

Exercise 3. Let $j := (-1 + \imath\sqrt{3})/2 = e^{2\imath\pi/3}$.

1. Show that $\mathbb{Z}[j]$ is an Euclidean ring and thus principal.

2. Let $p \geq 2$ be a prime number. Prove that we have a ring isomorphism
$$\mathbb{Z}[j]/(p) \cong \mathbb{F}_p[X]/(X^2 + X + 1).$$

3. Deduce that $p \geq 5$ is not prime in $\mathbb{Z}[j]$ if and only if -3 is a square modulo p.

4. Show that -3 is a square modulo p if and only if $p \equiv 1 \pmod{3}$.
Hint: If -3 is a square mod p, construct an element of order 3 in $\mathbb{F}_p^\times$.

5. Conclude that a prime $p \geq 5$ is of the form $a^2 - ab + b^2$ with $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 3$.

Exercise 4. Let $\mathbb{F}$ be a field of characteristic $\neq 2$. We define the ring of quaternions over $\mathbb{F}$, denoted by $\mathbb{H}_{\mathbb{F}}$, as the vector space over $\mathbb{F}$ given by

$$\mathbb{H}_{\mathbb{F}} = \mathbb{F} \oplus \mathbb{F}\mathrm{i} \oplus \mathbb{F}\mathrm{j} \oplus \mathbb{F}\mathrm{k},$$

together with the ring structure given by

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1, \quad \mathrm{ij} = -\mathrm{ji} \quad \text{and} \quad \mathrm{k} = \mathrm{ij}.$$

1. For $q = x + y\mathrm{i} + z\mathrm{j} + w\mathrm{k}$, we define $\overline{q} := x - y\mathrm{i} - z\mathrm{j} - w\mathrm{k}$. Prove that

$$\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2} \qquad \text{and} \qquad \overline{q_1 q_2} = \overline{q_2 q_1}.$$

2. For $q \in \mathbb{H}_{\mathbb{F}}$, we define the norm of q as $\mathrm{Nr}(q) := q\overline{q}$. Prove that

$$\mathrm{Nr}(q) = x^2 + y^2 + z^2 + w^2 \in \mathbb{F} \qquad \text{and} \qquad \mathrm{Nr}(q_1 q_2) = \mathrm{Nr}(q_1)\,\mathrm{Nr}(q_2).$$

3. Show that $\mathbb{H}_{\mathbb{F}}$ is a division ring if and only if the norm map $\mathrm{Nr} : \mathbb{H}_{\mathbb{F}} \to \mathbb{F}$ is non-degenerate, i.e. if $\mathrm{Nr}(q) = 0 \Leftrightarrow q = 0$.

4. Let $p \neq 2$ be a prime. Show that $\mathbb{H}_{\mathbb{F}_p}$ is not a division ring.
Hint: Prove that the two sets $A = \{x^2 + 1 : x \in \mathbb{F}_p\}$ and $B = \{-z^2 : z \in \mathbb{F}_p\}$ satisfy $A \cap B \neq \emptyset$.

Exercise 5. Let $\mathbb{H} \subset \mathbb{H}_{\mathbb{Q}}$ be defined by

$$\mathbb{H} := \{(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k})/2 : a, b, c, d \in \mathbb{Z},\ a \equiv b \equiv c \equiv d \bmod 2\}.$$

1. Show that $\mathbb{H}$ is a subring of $\mathbb{H}_{\mathbb{Q}}$ and that $\mathrm{Nr}(\mathbb{H}) \subset \mathbb{N}$. This ring is called Hurwitz's ring.

2. Prove that $\mathbb{H}$ is a (non-commutative) Euclidean ring: For every $x, y \in \mathbb{H}$ with $y \neq 0$, there exists $z, w \in \mathbb{H}$ such that $x = yz + w$ and $\mathrm{Nr}(w) < \mathrm{Nr}(y)$. (This implies in particular that every left/right ideal is principal.)

3. For every $z \in \mathbb{H}$, we have $\mathrm{Nr}(z) = 1 \Leftrightarrow z \in \mathbb{H}^\times$.

4. Let $p \neq 2$ be a prime. Prove that there is a ring isomorphism

$$\mathbb{H}/p\mathbb{H} \cong \mathbb{H}_{\mathbb{F}_p},$$

and conclude that there exists $x \in \mathbb{H}$ such that $\mathrm{Nr}(x) = p$. [*Hint:* Use 4(d) to conclude that $p\mathbb{H}$ is not a right maximal ideal in $\mathbb{H}$.]

5. Let p be an arbitrary prime. First prove that $4p$ can be written as a sum of four squares, and then use this to show that also $2p$ can be written as a sum of four squares.

   Hint:

$$\frac{1}{2}(a^2+b^2+c^2+d^2) = \left((\frac{a+b}{2})^2 + (\frac{a-b}{2})^2 + (\frac{c+d}{2})^2 + (\frac{c-d}{2})^2 \right)$$

6. Prove that every prime p is a sum of four squares. Conclude that for every positive integer n there exist a, b, c, d such that

$$n = a^2 + b^2 + c^2 + d^2.$$

References

[Zag90] D. Zagier. A one-sentence proof that every prime $p \equiv 1(\mod 4)$ is a sum of two squares. *The American Mathematical Monthly*, 97(2):144–144, 1990. URL: http://www.jstor.org/stable/2323918.