Solutions to Exercise Sheet 1

October 10, 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.*

Solution. First, the set S is clearly finite. Second, we show that the map takes values in S. Let $(x, y, z) \in S$. Then

$$\begin{aligned} (x + 2z)^2 + 4z(y - x - z) &= x^2 + 4yz = p \\ (2y - x)^2 + 4y(x - y + z) &= x^2 + 4yz = p \\ (x - 2y)^2 + 4y(x - y + z) &= x^2 + 4yz = p. \end{aligned}$$

Next, we show that the map is in fact an involution. Let $(x, y, z) \in S$ so that $x < y - z$. Then $x + 2z > 2z$ and so

$$(x, y, z) \mapsto (x + 2z, z, y - x - z) \mapsto (x + 2z - 2z, x + 2z - z + y - x - z, z) = (x, y, z).$$

Let $(x, y, z) \in S$ so that $y - z < x < 2y$. Then $y - (x - y + z) = 2y - x - z < 2y - x < 2y$ and so

$$(x, y, z) \mapsto (2y - x, y, x - y + z) \mapsto (2y - (2y - x), y, 2y - x - y + (x - y + z)) = (x, y, z).$$

The last case follows similarly as the first one.

Next, we show that the map has a unique fixed point. Notice that $x - 2y < x < x + 2z$, hence the unique case that can produce a fix point is the middle one.

$$(x, y, z) = (2y - x, y, x - y + z) \Leftrightarrow x = y.$$

Hence we need to show that S contains a unique point of the form (x, x, z). Since $p \equiv 1 \pmod 4$ there exists a unique $k \in \mathbb{Z}$ so that $p = 1 + 4k$. We see so that the tuple $(1, 1, k) \in S$ and it is unique since $(x, x, z) \in S \Rightarrow x | p$ and one easily see that $x = 1$ and so $z = k$.

We conclude that $|S|$ is odd, call the above map ι. Say that $(x, y, z) \sim_\iota (x', y', z')$ if and only if $(x, y, z) = \iota(x', y', z')$. Then $\sim_\iota$ is an equivalence relation and every equivalence class has two elements, except for the equivalence class of $(1, 1, k)$ and so we have

$$|S| = \sum_{[x] \in S/\sim_\iota} |[x]| = 1 + 2 \sum_{[x] \in (S/\sim_\iota) \setminus \{[(1,1,k)]\}} 1,$$

which is odd.

Consider the involution $\eta \colon S \ni (x, y, z) \mapsto (x, z, y)$. As before we define $\sim_\eta$ the equivalence relation $(x, y, z) \sim_\eta (x', y', z') \Leftrightarrow (x, y, z) = \eta(x', y', z')$. This is again an equivalence relation and so

$$|S| = \sum_{[x] \in S/\sim_\eta} |[x]|$$

and if η has no fixed point the latter is even. Hence we deduce that there is a fixed point, that is there exist $x, y \in \mathbb{N}$ so that $(x, y, y) \in S$, that is $x^2 + 4y^2 = p$.

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

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 $(\mathbb{R}, +)$.

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.

Solution. 1. $\mathrm{Nr}(z_1 z_2) = z_1 z_2 \overline{z_1 z_2} = z_1 \overline{z_1}\ z_2 \overline{z_2} = \mathrm{Nr}(z_1)\,\mathrm{Nr}(z_2)$.

2. Suppose $z = a + b\sqrt{d} \in A^\times$. Then there exists $w \in A$ so that $zw = 1$. Taking the norm we see $\mathrm{Nr}(z)\,\mathrm{Nr}(w) = 1$ and $\mathrm{Nr}(z) = a^2 - b^2 d \in \mathbb{Z}$. Hence, $\mathrm{Nr}(z) = \pm 1$.

   Now, suppose that z is so that $\mathrm{Nr}(z) = \pm 1$. Then $z(\pm\overline{z}) = 1$, and $\pm\overline{z} \in A$. That is, $z \in A^\times$.

   Nr induces a map $A^\times / A^{(1)} \simeq \{\pm 1\}$.

3. Call the map ϕ. The facts that ϕ is a group homomorphism and $\ker(\phi) = \{\pm 1\}$ are clear . We show now that the image of ϕ is discrete. Since $\mathrm{Im}(\phi)$ is a group, to show that it is discrete it is sufficent to produce a open ball $B_r(0)$ around the identity element in $0 \in \mathbb{R}$ so that $B_r(0) \cap \mathrm{Im}(\phi) = \{0\}$. Then, with the same r we will have $B_r(\phi(z)) \cap \mathrm{Im}(\phi) = \{\phi(z)\}$.

   Let $B_r(0)$ be an open ball of radius $r > 0$. We claim that $\mathbb{A}^{(1)} \cap \phi^{-1}(B_r(0))$ is finite. Suppose the claim is true, then with $r' = \frac{1}{2}\min\{|\phi(z_1) - \phi(z_2)| \ |z_1, z_2 \in \mathbb{A}^{(1)} \cap \phi^{-1}(B_r(0)), \ \phi(z_1) \neq \phi(z_2)\}$ we see that $B_{r'}(0) \cap \mathrm{Im}(\phi) = \{0\}$ which is what we want to show.

   Let us prove the claim. The condition $a + b\sqrt{d} \in \phi^{-1}(B_r(0))$ is equivalent to $\left|\log|a + b\sqrt{d}|\right| < r$, which is equivalent to

$$e^{-r} < |a + b\sqrt{d}| < e^r \tag{2}$$

   . Since $a + b\sqrt{d} \in \mathbb{A}^{(1)}$ we have that

$$e^{-r}|a - b\sqrt{d}| \leq 1 = |(a + b\sqrt{d})(a - b\sqrt{d})| \leq e^r|a + b\sqrt{d}|.$$

   In particular,

$$e^{-r} \leq |a - b\sqrt{d}| \leq e^r. \tag{3}$$

   Fixed $r > 0$, there are only finitely many $a, b \in \mathbb{Z}$ satisfying (2) and (3): this can be done by case distinction. Suppose $a + b\sqrt{d}$ and $a - b\sqrt{d}$ are both positive. Then (2) and (3) imply together that

$$2e^{-r} \leq 2a \leq 2e^r, \quad e^{-r} - e^r \leq 2b\sqrt{d} \leq e^r - e^{-r}.$$

   The other cases are similar.

4. Let $G \subset (\mathbb{R}, +)$ a discrete subgroup. If G is trivial there is nothing to show. So suppose $G \neq \{0\}$. Let $x \in G$ be an element so that $|x| = \min\{|y|, \ y \in G \setminus \{0\}\}$. After changing x with $-x$ if necessary we may assume that $x > 0$. We claim that $G = \langle x \rangle$. Let $y \in G$. Then there exists $m \in \mathbb{Z}$ so that

$$mx < y \leq (m + 1)x.$$

   Then $G \ni r = (m+1)x - y < x$ and $r \geq 0$. By minimality of x we have $r = 0$ and $y = (m+1)x$.

5. $A^{(1)}/\{\pm 1\} \simeq \mathrm{Im}(\phi)$. Hence the claim.

6. We follow the hint. Let B be as in the hint. We have $r = \min_{x \neq y \in B}|x - y| \leq \frac{1}{n+1}$, otherwise order order the elements of B in ascending order $0 = a_0 \leq a_1 \leq \cdots \leq a_{n+1} = 1$. Then

$$1 = \sum_{j=0}^{n} a_{j+1} - a_j > \sum_{j=0}^{n+1} \frac{1}{n+1} \geq 1.$$

   The equality $r = \frac{1}{n+1}$ happens if and only if $a_i = \frac{i}{n+1}$, $0 \leq i \leq n+1$, but if this is the case, then $\alpha \in \mathbb{Q}$, which we are excluding. Hence $r < \frac{1}{n+1}$. Let $l_1 > l_2$ be so that $r = |\{l_1\alpha\} - \{l_2\alpha\}|$. Notice that $|\alpha(l_1 - l_2) - (\lfloor l_1\alpha \rfloor - \lfloor l_2\alpha \rfloor)| = |\{l_1\alpha\} - \{l_2\alpha\}| = r < \frac{1}{n+1}$, hence the statement is true with $a = \lfloor l_1\alpha \rfloor - \lfloor l_2\alpha \rfloor$ and $b = l_1 - l_2$.

   We construct a sequence $(\frac{a_l}{b_l})_l \subset \mathbb{Q}$ so that

$$|\alpha - \frac{a_{l+1}}{b_{l+1}}| < |\alpha - \frac{a_l}{b_l}|, \qquad |\alpha - \frac{a_l}{b_l}| < \frac{1}{b_l^2}.$$

   The induction base is given by what we have done before. Notice that in the construction above $\frac{1}{(n+1)b} < \frac{1}{b^2}$. Now suppose we have constructed $\frac{a_1}{b_1}, \ldots, \frac{a_l}{b_l}$. Let m be an integer so that $\frac{1}{m+1} < |\alpha - \frac{a_l}{b_l}|$. Use what we have done before to find a_{l+1}, $b_{l+1} > 0$ so that $|\alpha - \frac{a_{l+1}}{b_{l+1}}| < \frac{1}{(m+1)b_{l+1}} < |\alpha - \frac{a_l}{b_l}|$. This shows the induction step.

7. Since $\sqrt{d}$ is irrational, there exist infinitely many coprime pairs (x, y) so that

$$|\sqrt{d} - \frac{x}{y}| < \frac{1}{y^2}.$$

Notice that

$$0 < |x^2 - dy^2| = |(x - \sqrt{d}y)||x + \sqrt{d}y| < \frac{1}{y}|x + \sqrt{d}y| \leq \sqrt{d} + |\frac{x}{y}| \leq 2\sqrt{d} + 1$$

In particular, by pigeonhole principle there exists $1 \leq n \leq 2\sqrt{d} - 1$ so that infinitely many pairs $(x, y) \in \mathbb{Z}^2$, with x and y coprime, satisfy $x^2 - y^2 d = n$. Notice that we may always substitute x with $-x$ and y with $-y$ to assume that both are positive. Again, by pigeonhole principle, since there are only finitely many congruence class modulo n there will be infinitely many, and hence at least two, distinct solutions that are congruent modulo n.

8. We have
$$z_0 = \frac{(x_1 + \sqrt{d}y_1)(x_2 - \sqrt{d}y_2)}{n} = \frac{x_1x_2 - dy_1y_2 + \sqrt{d}(x_2y_1 - x_1y_2)}{n}.$$
We have $x_1x_2 - dy_1y_2 \equiv x_2^2 - dy^2 \equiv 0 \,(\mathrm{mod}\, n)$ and $x_2y_1 - x_1y_2 \equiv x_1y_1 - x_1y_1 \equiv 0 \,(\mathrm{mod}\, n)$, hence $z_0 \in A$. Since $N(z_0) = 1$ we deduce $z_0 \in A^\times$. By construction we have $z_0 \neq \pm 1$.

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 $p \equiv 1 \,(\mathrm{mod}\, 3)$.
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 $p \equiv 1 \,(\mathrm{mod}\, 3)$.

Solution. 1. Let $z, q \in \mathbb{Z}[j]$, $q \neq 0$. Then $\frac{z}{q} \in \mathbb{Q}(j)$ and we can write it as $\frac{z}{q} = x + yi\sqrt{3}$. Let $a, b \in \mathbb{Z}$ so that $|x - a| \leq 1/2$ and $|y - b| \leq 1/2$. If at least one of the two inequalities is strict, then
$$|(\frac{z}{q} - (a + ib\sqrt{3}))|^2 = (x - a)^2 + 3(y - b)^2 < 1,$$
hence $z = q(a + ib\sqrt{3}) + r$ with $|r| < |q|$.
If both $|x - a| = 1/2$ and $|y - b| = 1/2$ it follows that $x \in \frac{1}{2} + \mathbb{Z}$ and $y \in \frac{1}{2} + \mathbb{Z}$, hence $\frac{z}{q} \in \mathbb{Z}[j]$ and we can take $r = 0$.

2. Consider the following map
$$\mathbb{Z}[X] \to \mathbb{F}_p[X] \to \mathbb{F}_p[X]/(X^2 + X + 1),$$
where the first arrow is the reduction $\mod p$ of the coefficients and the second arrow is the canonical projection. This map is clearly surjective and its kernel is $(p, X^2 + X + 1)$.
We also have
$$\mathbb{Z}[j]/(p) \simeq (\mathbb{Z}[X]/(X^2 + X + 1))/(p) \simeq \mathbb{Z}[X]/(p, X^2 + X + 1),$$
hence the claim

3. p is not prime in $\mathbb{Z}[j]$ if and only if $Z[j]/(p)$ is not an integral domain. The latter happens, by the above isomorphism, if and only if $X^2 + X + 1 \in \mathbb{F}_p[X]$ is reducible. The polynomial $X^2 + X + 1 \in \mathbb{F}_p[X]$ is reducible if and only if it has a root in $\mathbb{F}_p[X]$ and this happens if any only if $1 - 4 = -3$ is a square in $\mathbb{F}_p$

4. Now suppose that $p \geq 5$. Suppose first that -3 is a square modulo p. Hence there exists $a \in \mathbb{F}_p^\times$ so that $a^2 + a + 1 = 0$. Then $a^2 = -a - 1$ and $a^3 = -a^2 - a = a + 1 - a = 1$. Since $a, a^2 \neq 1$ ($p \geq 5$) we see that a has order 3. Hence, $3|p-1$.

   Suppose on the other hand that $p \equiv 1 \mod 3$. Since $\mathbb{F}_p^\times$ is cyclic, there exists $a \in \mathbb{F}_p^\times$ so that $\mathrm{ord}(a) = 3$. Then
   $$0 = a^3 - 1 = (a-1)(a^2 + a + 1)$$
   and so a is a root of $X^2 + X + 1$ and so -3 is a square $(\mathrm{mod}\, p)$.

5. First notice that
   $$a^2 - ab + b^2 = (a + jb)(a + j^2 b) = |a + jb|^2$$
   In particular if $p = a^2 - ab + b^2$, $a, b \in \mathbb{Z}$, then p is not prime in $\mathbb{Z}[j]$ and so $p \equiv 1 \mod 3$. Suppose $p \equiv 1 \mod 3$, then p is not prime in $\mathbb{Z}[j]$ and so there exists $q_1, q_2 \in \mathbb{Z}[j] \smallsetminus \mathbb{Z}[j]^\times$ so that $p = q_1 q_2$. Then $p^2 = |p|^2 = |q_1 q_2|^2 = |q_1|^2 |q_2|^2$. Since $|q_i|^2 \in \mathbb{Z}$ and q_i are non-units we see that $|q_1|^2 = p$, hence p is of the desired form.

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

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 $A \cap B \neq \emptyset$.

Solution. First notice that $\mathrm{ki} = \mathrm{j}$ and $\mathrm{jk} = \mathrm{i}$.

1. Skipped.

2. For $q = x + y\mathrm{i} + z\mathrm{j} + w\mathrm{k}$ we have
   $$\begin{aligned}
   \mathrm{Nr}(q) &= q\overline{q} \\
   &= (x + y\mathrm{i} + z\mathrm{j} + w\mathrm{k})(x - y\mathrm{i} - z\mathrm{j} - w\mathrm{k}) \\
   &= x^2 + y^2 + z^2 + w^2 + \mathrm{i}(yx - xy - zw - (-wz)) + \\
   &+ \mathrm{j}(-xz + zx - (-yw) + (-wy)) + \mathrm{k}(-xw + wx + (-zy) - (-zj)) \\
   &= x^2 + y^2 + z^2 + w^2.
   \end{aligned}$$

   For the second statement notice that $\mathbb{F}$ commutes (with respect to the multiplication) with every element of $\mathbb{H}$. Therefore
   $$\mathrm{Nr}(q_1 q_2) = \overline{q_1 q_2}\ q_1 q_2 = \overline{q_2}\ \ \mathrm{Nr}(q_1) q_2 = \mathrm{Nr}(q_1)\,\mathrm{Nr}(q_2).$$

3. Suppose $\mathbb{H}_\mathbb{F}$ is a division ring. Let $q \neq 0$. Then there exists $q' \in \mathbb{H}_\mathbb{F}$ so that $q'q = 1$. Then $1 = \mathrm{Nr}(q'q) = \mathrm{Nr}(q')\,\mathrm{Nr}(q)$, hence $\mathrm{Nr}(q) \neq 0$. This shows that Nr is non degenerate. Suppose that Nr is non degenerate. Let $q \neq 0$. Then $\mathrm{Nr}(q) \neq 0$ and we have $q \cdot \frac{\overline{q}}{\mathrm{Nr}(q)} = 1$. Hence q has an inverse.

4. Suppose that the claim in the Hint is true. Then there are $x, z \in \mathbb{F}_p$ so that $x^2 + z^2 + 1 = 0$, hence $\mathrm{Nr}(x + z\mathrm{i} + \mathrm{j}) = 0$ and so the norm is degenerate.

   Consider the group homomorphism $\mathbb{F}_p^\times \ni z \mapsto z^2$. Its kernel is ± 1 and so its image has cardinality $\frac{p-1}{2}$. Adding $0 = 0^2$ we get that $|\{x^2 \mid x \in \mathbb{F}_p\}| = \frac{p+1}{2}$. Hence $|A| = |B| = \frac{p+1}{2}$. In particular, they must intersect.

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

Solution. Let $\mathbb{H}_0 = \{a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \mid a, b, c, d \in \mathbb{Z}\}$. It is clear that $\mathbb{H}_0$ is a ring.

1. Every element $x \in \mathbb{H}$ can be written as a sum $x = y + \frac{\epsilon}{2}(1 + \mathrm{i} + \mathrm{j} + \mathrm{k})$ with $y \in \mathbb{H}_0$ and $\epsilon \in \{0, 1\}$. In particular to show that $\mathbb{H}$ is a ring it suffices to show that $(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}) \cdot \frac{1}{2}(1 + \mathrm{i} + \mathrm{j} + \mathrm{k}) \in \mathbb{H}$ for every $y \in \mathbb{H}_0$ and $(\frac{1}{2}(1 + \mathrm{i} + \mathrm{j} + \mathrm{k}))^2 \in \mathbb{H}$. For the latter we have

   $$(\frac{1}{2}(1 + \mathrm{i} + \mathrm{j} + \mathrm{k}))^2 = \frac{1}{4}(-2 + 2\mathrm{i} + 2\mathrm{j} + 2\mathrm{k}) = \frac{1}{2}(-1 + \mathrm{i} + \mathrm{j} + \mathrm{k}) \in \mathbb{H}.$$

   For the former, with $y = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$, we have

   $$y \cdot \frac{1}{2}(1 + \mathrm{i} + \mathrm{j} + \mathrm{k}) = \frac{1}{2}(a - b - c - d + \mathrm{i}(a + b + c - d) + \mathrm{j}(a + c + d - b) + \mathrm{k}(a + b + d - c)).$$

   Since $1 \equiv -1 \pmod 2$ one sees that

   $$a - b - c - d \equiv a + b + c - d \equiv a + c + d - b \equiv a + b + d - c \pmod 2$$

   and so the desired result.

   Let $x = \frac{1}{2}(a + \mathrm{i} + \mathrm{j} + \mathrm{k}) \in \mathbb{H}$, $a \equiv b \equiv c \equiv d \pmod 2$. If a, b, c, d are all even, then a^2, b^2, c^2, d^2 are all $0 \pmod 4$. If a, b, c, d are odd. Then $a^2, b^2, c^2, d^2 \equiv 1 \pmod 4$ and so in each case we see that

   $$N(x) = \frac{1}{4}(a^2 + b^2 + c^2 + d^2) \in \mathbb{N} \cup \{0\}.$$

2. From Exercise 4 we know that $\mathbb{H}_{\mathbb{Q}}$ is a division ring. In particular, given $z, q \in \mathbb{H}$, $q \neq 0$, we consider $z \cdot q^{-1}$ (which exists since $\mathbb{H}_{\mathbb{Q}}$ is a division ring). Write $z \cdot q^{-1} = \frac{x}{2} + \frac{y}{2}\mathrm{i} + \frac{z}{2}\mathrm{j} + \frac{w}{2}\mathrm{k}$. Let $a, b, c, d \in \mathbb{Z}$, *all of the same parity*, so that $|x-a|, |y-b|, |z-c|, |w-d| \leq 1$. Then

$$N(z \cdot q^{-1} - \frac{1}{2}(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k})) = \frac{1}{4}((x-a)^2 + (y-b)^2 + (z-c)^2) \leq 1.$$

If the inequality is strict we set $r = z - q\frac{1}{2}(a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}))$, otherwise we see that $x = a \pm 1, y = b \pm 1, z = c \pm 1, w = d \pm 1$, that is $z \cdot q^{-1} \in \mathbb{H}$ already and we set $r = 0$.

3. Skipped.

4. Since $p \neq 2$ we have a well defined ring homomorphism

$$\mathbb{H} \to \mathbb{H}_{\mathbb{F}_p}; \frac{a}{2} + \frac{b}{2}\mathrm{i} + \frac{c}{2}\mathrm{j} + \frac{d}{2}\mathrm{k} \mapsto a2^{-1} \pmod p + b2^{-1} \pmod p\mathrm{i} + c2^{-1} \pmod p\mathrm{j} + d2^{-1} \pmod p\mathrm{k}$$

that projects each coefficient to its congruence class $\mod p$.

The fact that it is a ring homorphism is a computation that we skip.

First, we show that the map is surjective. Let $z \in \mathbb{H}_{\mathbb{F}_p}$. Let $a, b, c, d \in \mathbb{Z}$ be so that $x = a2^{-1} \pmod p + b2^{-1} \pmod p\mathrm{i} + c2^{-1} \pmod p\mathrm{j} + d2^{-1} \pmod p\mathrm{k}$. After substituting a (resp. b, c, d) with $a + p$ (which has opposite parity of a) we may assume that a, b, c, d have same parity. This shows that the map is surjective.

The ker of this map is the subset (of $\mathbb{H}$) of elements whose coefficients are all divisible by p, that is $(p)\mathbb{H}$. Hence the desired isomorphism.

Since $\mathbb{H}_{\mathbb{F}_p}$ is not a division ring, we see that $p\mathbb{H}$ is not a right maximal ideal. In fact, there exists $y \in \mathbb{H}_{\mathbb{F}_p} \setminus \{0\}$ that does not have an inverse[2]. Let $0 \neq x \cdot p\mathbb{H} \in \mathbb{H}/p\mathbb{H}$ be the inverse image of y. Then we have that $x \notin p\mathbb{H}$ and $(x, p)\mathbb{H} \neq \mathbb{H}$. That is (p) is not maximal. Since $\mathbb{H}$ is a (non-commutative) PID and (p) is non maximal, there exists $q_1, q_2 \in \mathbb{H} \setminus \mathbb{H}^\times$ so that $q_1 q_2 = p$. Then $N(q_1 q_2) = N(p) = p^2$. Hence $N(q_1) = p$.

5. Let $p \neq 2$. Let $x = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} \in \mathbb{H}$ so that $N(x) = p$, then

$$4p = a^2 + b^2 + c^2 + d^2.$$

We use the Hint and see that

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

and each $a + b, a - b, c + d, c - d \equiv 0 \pmod 2$. For $p = 2$ we have $4p = 2^3 = 2^2 + 2^2$ and $2p = 2^2$.

6. By previous point we have

$$2p = a^2 + b^2 + c^2 + d^2,$$

for some $a, b, c, d \in \mathbb{Z}$. Suppose first $p \neq 2$. Then $2p \equiv 2 \mod 4$ and so we claim that $\{a, b, c, d\}$ must contain exactly 2 even numbers and 2 odd numbers. Suppose that $\{a, b, c, d\}$ contains no even number. Then $a^2 + b^2 + c^2 + d^2 \equiv 1 + 1 + 1 + 1 \equiv 0 \pmod 4$. If a, b, c, d are all even, then $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod 4$. Suppose that $\{a, b, c, d\}$ contains 1 (resp. 3 even numbers), then $a^2 + b^2 + c^2 + d^2 \equiv 3 \pmod 4$ (resp. $\equiv 1 \pmod 4$). Hence the claim.

Without loss of generality we can say that a, b are both even and that c, d are both odd. Then, using the Hint of the previous subexercise, we have

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

is a sum of four squared integers.

For $p = 2$ we have $2 = 1^2 + 1^2$.

Now consider $n \in \mathbb{N}$ any positive integer. Write $n = p_1^{l_1} \cdots p_m^{l_m}$. Write $p_h = a_h^2 + b_h^2 + c_h^2 + d_h^2 = N(q_h)$, for $q_h = a_h + b_h\mathrm{i} + c_h\mathrm{j} + d_h\mathrm{k} \in \mathbb{H}_0$ (see definition at the beginning of solutions). Then by multiplicativity of the norm we have $n = N(q_1^{l_1}) \cdots N(q_m^{l_m}) = N(x)$ for some $x \in \mathbb{H}_0$. That is, n is a sum of four squares.

[2]Here I am vague with left and right inverse. But you can show that given any associative operation with double sided neutral element, then to have a left inverse is equivalent to have a right inverse, hence generically an inverse.

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.

mp