Solution to Exercise Sheet 2
Algebraic Number Theory

October 10, 2025

Exercises 1, 2, 3 are from Exercise Sheet 1 and they are still relevant for the second week.
Exercise 4 is new.

Exercise 1. 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 2. 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 $A \cap B \neq \emptyset$.

Exercise 3. 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

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

Exercise 4. The goal of this exercice is to prove Fermat's Theorem for $n = 4$: if $(x, y, z) \in \mathbb{Z}^3$ is a solution of

$$X^4 + Y^4 = Z^4, \tag{1}$$

then $xyz = 0$. We do this by contradiction: suppose that (x, y, z) is a solution of (1) and $x, y, z \neq 0$.

1. Show that we can assume that $0 < x, y, z$, $(x, y) = 1$, x odd and y is even.

2. Show that there exist integers $0 < n < m$ such that $(m, n) = 1$, $x^2 = m^2 - n^2$, $y^2 = 2mn$ and n is even.

3. Show that both m and $\frac{n}{2}$ are square numbers.

4. Show that there exist r, s with $(r, s) = 1$, $m = r^2 + s^2$ and $n = 2rs$. Conclude that both r, s are square numbers and that there exist u, v, w such that

$$w^2 = u^4 + v^4$$

and $0 < w < z$.

5. Deduce the desired contradiction.

Solution. Let (x, y, z) a solution of (1) so that $xyz \neq 0$.

1. After substituting x (resp. y, z) with $-x$ (resp. $-y$,$-z$) we may assume that $0 < x, y, z$. Suppose $\gcd(x, y) > 1$. Let p^m (p prime, m positive integer) so that $p^m | x$, $p^m | y$. Then $p^{4m} | z^4$, and so by uniqueness of the factorization $p^m | z$. In particular, we deduce that $\gcd(x, y) | z$. Then $x' = \frac{x}{\gcd(x,y)}$, $y' = \frac{y}{\gcd(x,y)}$, $z' = \frac{z}{\gcd(x,y)}$ also solves (1). One of the two triples (x', y', z') or (y', x', z') has the desired properties. In fact, x' and y' can't be both even as they are coprime. Suppose they are both odd. Then we will have $z'^4 \equiv 2 \pmod 4$, but this impossible. Hence x' or y' is even.

   After eventually substituting (x, y, z) with (x', y', z') or (y', x', z') we may assume that $0 < x, y$, x is odd y is even and x, y are coprime.

2. The triple (x^2, y^2, z^2) is a Pythagorean triple. Hence there exists coprime $m, n \in \mathbb{Z}$ so that $x^2 = m^2 - n^2$, $y^2 = 2mn$ and $z^2 = m^2 + n^2$ (if either m or n even), or $x^2 = \frac{m^2 - n^2}{2}$, $y^2 = mn$ if both m, n are odd. The latter case can not happen, since y is even and so we are in the first case. If m is even, then $1 \equiv x^2 \equiv -n^2 \equiv -1 \pmod 4$, which is absurd, and so we deduce that n is even.

3. Since y is even we see that $m\frac{n}{2} = (\frac{y}{2})^2$ is a square. Since m and $\frac{n}{2}$ are coprime we see that both m and $\frac{n}{2}$ must be square numbers.

4. The triple (x, n, m) is a Pythagorean triple. Hence, there exists r, s coprime so that $m = r^2 + s^2$, and $n = 2rs$ (if either r or s is even) or $m = \frac{r^2+s^2}{2}$, $n = rs$ (if both r, s are odd). The second case can not happen since n is even and so we are in the first case. Since $\frac{n}{2}$ is a square and r and s are coprime we deduce that r and s are square numbers, say $r = u^2$, $s = v^2$. Then we have $m = u^4 + v^4$, but since m is a square itself we can write $m = w^2$ for some positive integer w. Hence we see that
$$w^2 = u^4 + v^4.$$
Recall that $m^2 + n^2 = z^2$. Hence $m^2 < z^2$ and so $0 < w^4 < z^2$, so $0 < w < z$.

5. Using $w^2 = u^4 + v^4$ we can produce another triple (u', v', w') so that $w'^2 = u'^4 + v'^4$ and $0 < w' < w$. In fact, notice that we actually used that $x^4 + y^4 = (z')^2$ for $z' = z^2$, but we did not use the fact the z' is a square (check the details).

   Iterating this process a finite number of times produces the desired contradiction.