Assignment 1

Arithmetic, Zorn's Lemma.

1. (a) Using the Euclidean division, determine $\gcd(1602, 399)$.
   (b) Find $m_0, n_0 \in \mathbb{Z}$ such that $\gcd(1602, 399) = 1602m_0 + 399n_0$. [*Hint:* Write the steps of the euclidean algorithm and compute 'backwards'.]
   (c) Similarly, determine $\gcd(123456, 876)$ and find $m_0, n_0 \in \mathbb{Z}$ such that

   $$\gcd(123456, 876) = 123456m_0 + 876n_0.$$

   (d) Determine $\gcd(\ell^2 + \ell + 1, 3\ell^2 + 4\ell + 5)$ for each $\ell \in \mathbb{Z}$.

2. A *Pythagorean triple* is an ordered triple (a, b, c) of positive integers for which $a^2 + b^2 = c^2$. It is called *primitive* if a, b and c are *coprime*, that is, if there is no integer $d > 1$ which divides a, b and c.

   (a) Let $1 \leqslant x < y$ be odd integers. Prove that

   $$\left(xy, \frac{y^2 - x^2}{2}, \frac{y^2 + x^2}{2}\right) \tag{1}$$

   is a Pythagorean triple.
   (b) Suppose that x and y are also coprime. Prove that the Pythagorean triple (1) is primitive.
   *(c) Prove that all primitive Pythagorean triples are of the form (1) with coprime odd integers $1 \leqslant x < y$, up to switching the first two entries. [*Hint:* Reduce to the case in which a is odd. Prove that $\frac{c+b}{a}\frac{c-b}{a} = 1$ and write down $\frac{c+b}{a} = \frac{u}{t}$ and $\frac{c-b}{a} = \frac{t}{u}$ for coprime positive integers $u > t$. Find $\frac{c}{a}$ and $\frac{b}{a}$ in terms of t and u.]

3. In this exercise we give a famous proof by Zagier of Fermat's theorem on sums of two squares. For $m, n, r \in \mathbb{Z}$ we say that m is *congruent to r modulo n*, and write $m \equiv r \pmod{n}$, if $m - r \in n\mathbb{Z}$.

   Theorem 0.1 (Fermat)**.** *Let p be an odd prime number. Then it is possible to express $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 (mod\ 4)$.*

   Let X be a set. An *involution* of X is a map $\varphi : X \longrightarrow X$ such that $\varphi \circ \varphi = \mathrm{id}_X$.

(a) Prove: if X is finite and has odd cardinality, then every involution of X has a fixed point.

(b) Prove: if X is finite and an involution of X has a unique fixed point, then $|X|$ is odd.

In parts (c)-(f), suppose that $p \equiv 1 \pmod 4$ is a prime number. Let

$$X_p := \{(x, y, z) \in \mathbb{Z}^3_{\geqslant 0} : x^2 + 4yz = p\}.$$

(c) Show that X_p is finite and non-empty.

(d) Show that the maps $f, g : X_p \longrightarrow X_p$ sending

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

$$g : (x, y, z) \longmapsto (x, z, y)$$

are well defined involutions.

(e) Let $A = \{(x, y, z) \in X_p : x < y - z\}$, $B = \{(x, y, z) \in X_p : y - z < x < 2y\}$ and $C = \{(x, y, z) \in X_p : x > 2y\}$. Prove that $f(A) \subseteq C$ and $f(C) \subseteq A$. Deduce that $f(B) \subseteq B$ and use this to prove that f has a unique fixed point.

(f) Deduce that $|X_p|$ is odd and conclude that the "if" statement holds.

(g) Prove that if $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$, then $p \equiv 1 (\text{mod } 4)$.

4. Let S be a set. A *well-order* on S is a total order on S such that every non-empty subset S has a minimal element. For example, the natural order in $\mathbb{N}$ is a well-order.

(a) Define a well-order on $\mathbb{Z}$.

(b) Define a well-order on $\mathbb{Q}$.

(c) Using Zorn's lemma, prove that every set S admits a well-order. [*Hint:* Consider the partially ordered set

$$\mathcal{S} := \{(A, R) : A \subseteq S,\ R \text{ is a well-order on } A\}$$

endowed with the partial order defined by

$$(A, R) \leqslant (A', R') \overset{\text{def.}}{\iff} \left(\begin{array}{c} A \subseteq A'; \forall x, y \in A, xRy \iff xR'y \\ \text{and } \forall a \in A, \forall a' \in A', a'R'a \implies a' \in A \end{array} \right).$$

Check that $(\mathcal{S}, \leqslant)$ satisfies the hypotheses of Zorn's lemma and get a maximal element (M, R_0). Prove that $M = S$.]