# ALGEBRAIC NUMBER THEORY
# PART I (EXERCISES)

**Exercise 1.**

(1) If $a, b$ are coprime positive integers and $ab = c^2$ for some integer $c$, show that $a = t^2$ and $b = s^2$ for some integers $t$ and $s$.
(2) Show that for any integer $x$ the numbers $x$ and $x^2 + 1$ are coprime.
(3) Numbers $0, 1, 2^2 = 4, 3^2 = 9, \ldots$ are called **squares**. Show that the distance between $k^2$ and $(k+1)^2$ is equal to $2k+1$. When is this distance equal to 1?
(4) Use the previous results to conclude that the equation $y^2 = x^3 + x$ has no solutions in **positive** integers $x$ and $y$.

## 1. Gaussian Integers

**Exercise 2.** Let $a + bi, c + di$ be Gaussian integers. Prove the following:

(1) Every rational integer is a Gaussian integer;
(2) $(a + bi) + (c + di)$ is a Gaussian integer;
(3) $(a + bi) - (c + di)$ is a Gaussian integer;
(4) $(a + bi)(c + di)$ is a Gaussian integer.

**Exercise 3.** Prove that $1 + 2i$ divides 5 but does not divide 7.

**Exercise 4.** Let $\alpha, \beta$ be Gaussian integers. Prove the following:

(1) $N(\alpha\beta) = N(\alpha)N(\beta)$; Show that $N(\alpha) \geq 0$ for all Gaussian integers and $N(\alpha) = 0$ if and only if $\alpha = 0$. Thus the norm is **non-negative**.

**Exercise 5.**

(1) Show that if $\alpha$ is a Gaussian unit then $N(\alpha) = 1$.
(2) Prove that the units of $\mathbb{Z}[i]$ are $1, -1, i$ and $-i$.

**Exercise 6.** Find Gaussian primes among the integers $2, 3, 5, 7$.

## 2. Sums of Two Squares

In this exercise we will investigate which numbers $n$ can be written as the sum of two squares. That is, $n = a^2 + b^2$ for some integers $a$ and $b$.

**Exercise.** Compute first 10 numbers that are sums of two squares.

**Step 1.** Let $m$ and $n$ be positive integers that are sums of two squares. Prove that $mn$ is also a sum of two squares. **Hint:** use the fact that the norm $N$ is multiplicative.

**Step 2.** Prove that every integer that is a sum of two squares is of the form $4k$, $4k+1$ or $4k+2$ for some integer $k$. Conclude that every rational prime $p$ of the form $4k+3$ is not a sum of two squares, and so it is a Gaussian prime.

**Step 3.** Let $p$ be a rational prime of the form $4k+1$. In this exercise, we will use the fact that there always exists an integer $x$ such that $p \mid x^2 + 1$.

(1) Show that $p$ does not divide neither $x+i$ nor $x-i$. Conclude that it is not prime, so $p = \alpha\beta$ for some Gaussian integers $\alpha, \beta$.
(2) Prove that neither $\alpha$ nor $\beta$ are units. Conclude that $N(\alpha) = p$, so $p$ is a sum of two squares.

**Step 4.** Show that 2 is a sum of 2 squares. Conclude that every number of the form

$$2^t p_1^{e_1} \dots p_k^{e_k} q_1^{2f_1} \dots q_\ell^{2f_\ell}$$

is a sum of two squares, where $p_i$ are primes of the form $4k+1$ and $q_i$ are primes of the form $4k+3$.