Exercise Sheet 1

This sheet is due in the lecture on Tuesday 7th October, and will be discussed in the exercise class on Friday 10th October.

Exercise 1.1. *Review of highest common factors.*

(1) Use Euclidean algorithm to compute $\mathrm{hcf}(963, 657)$ and find a pair of integers m, n satisfying $963m + 657n = \mathrm{hcf}(963, 657)$.

(2) For non-zero integers a and b, let $d = \mathrm{hcf}(a, b)$, $a = da'$ and $b = db'$. Show that $\mathrm{hcf}(a', b') = 1$. (Hint: write $d = am + bn$ for some $m, n \in \mathbb{Z}$.)

Exercise 1.2. *Examples of arithmetic functions.*

(1) Compute the values of $\nu(n)$, $\sigma(n)$, $\mu(n)$, $\phi(n)$ for $n = 360$ and $n = 429$.

(2) For any integer $n \geqslant 3$, show that $\phi(n)$ is even.

(3) For any integer $n \geqslant 2$, show that the sum of all elements in the set $\{m \in \mathbb{Z} \mid 1 \leqslant m \leqslant n, \mathrm{hcf}(m, n) = 1\}$ is $\frac{1}{2}n\phi(n)$.

Exercise 1.3. *Applications of Möbius inversion.*

(1) Show that $\sum_{d \mid n} \mu(\frac{n}{d})\nu(d) = 1$ for any $n \in \mathbb{Z}^+$;

(2) Show that $\sum_{d \mid n} \mu(\frac{n}{d})\sigma(d) = n$ for any $n \in \mathbb{Z}^+$.

Exercise 1.4. *Unique factorisation in the ring of Gaussian integers.*

Consider the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ and the function $\nu : \mathbb{Z}[i] \to \{0, 1, 2, \cdots\}$ given by $\nu(a + bi) = a^2 + b^2$ (the absolute value as a complex number).

(1) Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, $\nu(\alpha\beta) = \nu(\alpha)\nu(\beta)$. (Hint: either compute it directly, or use the fact that $\nu(\alpha) = \alpha \cdot \overline{\alpha}$.)

(2) Show that the function ν is a Euclidean valuation. (Hint: for $\alpha, \beta \in \mathbb{Z}[i]$, consider $\frac{\alpha}{\beta}$ as a complex number. Choose q to be the Gaussian integer which is the nearest to $\frac{\alpha}{\beta}$ in the complex plane.)

(3) Conclude that unique factorisation holds for $\mathbb{Z}[i]$.

(4) Show that $\alpha \in \mathbb{Z}[i]$ is a unit iff $\nu(\alpha) = 1$. Conclude that the only units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

(5) For $\alpha \in \mathbb{Z}[i]$, suppose $\nu(\alpha)$ is a prime in $\mathbb{Z}$. Show that α is irreducible in $\mathbb{Z}[i]$.

(6) Show that $(2 + i)(2 - i) = 5 = (1 + 2i)(1 - 2i)$ are two factorisations of 5 into irreducible elements in $\mathbb{Z}[i]$. How is this consistent with unique factorisation?