Homework 1

Deadline: 24th October (23:55 JST), 2021

Exercise 1. Recall some algebra. For this show the following basic facts for rings:

(i) In an integral domain, every prime element is irreducible.

(ii) In a unique factorization domain, every irreducible element is prime.

(iii) Any Euclidean ring is factorial.

Exercise 2. Prove Wilson's theorem, i.e. show that for any prime number p we have

$$(p-1)! \equiv -1 \mod p\,.$$

Exercise 3. Show the following facts for the Gaussian integers $\mathbb{Z}[i]$:

(i) The group of units is $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$. For this show that an element $\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$, where N is the norm defined by $N(\alpha) = |\alpha|^2$.

(ii) Show that, in the ring $\mathbb{Z}[i]$, the relation $\alpha\beta = e\gamma^n$, for relatively prime[1] numbers $\alpha, \beta \in \mathbb{Z}[i]$ and a unit $e \in \mathbb{Z}[i]^\times$ implies $\alpha = e_1 a^n$ and $\beta = e_2 b^n$ with $a, b \in \mathbb{Z}[i]$ and units $e_1, e_2 \in \mathbb{Z}[i]^\times$.

Exercise 4. Find all pythagorean triples, i.e. find all integers $a, b, c \in \mathbb{Z}$ satisfying

$$a^2 + b^2 = c^2\,.$$

For this proceed as follows:

(i) First focus on the case where $a, b, c > 0$ and $\gcd(a, b, c) = 1$ and then explain afterwards how you can obtain the remaining solutions from this.

(ii) Show that in this case, up to permutation, the solutions are all given by

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2\,,$$

where $u, v \in \mathbb{Z}$, $u > v > 0$, $\gcd(u, v) = 1$ and u, v are not both odd. To show that these are indeed all solutions, factor $a^2 + b^2$ in $\mathbb{Z}[i]$ and then use Exercise 3 (ii).

[1] Relatively prime here means that there exists no irreducible element which divides both of them.