Set 4

(A) Division algorithm in $\mathbb{Z}[i]$

(1) In the complex plane, draw a few of the $\mathbb{Z}[i]$-multiples of $2+i$. What pattern do they make?

(2) Prove the following about the norm on $\mathbb{Z}[i]$:

(i) We have $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

(ii) We have $N(1) = 1$.

(3) (*HW*) Show that, for $\alpha \in \mathbb{Z}[i]$, we have $N(\alpha) = 1$ if and only if[1] α is a unit.

(4) Do (Set 1 (A) (4)) again, now by using the previous problem.

(5) We want to now start exploring the division algorithm in $\mathbb{Z}[i]$. To fix ideas, let's say we want to divide $\alpha = 4 - i$ by $\beta = 2 + i$; that is, we want to express $\alpha = \gamma\beta + \rho$ where $\gamma, \beta \in \mathbb{Z}[i]$ and ρ is "small". Begin by drawing all the multiples of β: this gives a tiling of the plane by squares. Show that the area of each square is $N(\beta)$; convince yourself that this works for any β, and not just $\beta = 2 + i$.

(6) Prove the division algorithm for $\mathbb{Z}[i]$, stated below.

Theorem 2. *Given $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$, there exist $\gamma, \rho \in \mathbb{Z}[i]$ such that $\alpha = \gamma\beta + \rho$ and $N(\rho) < N(\beta)$.*

(7) Find γ and ρ for the following pairs (α, β): $(10 + 2i, 2 - i)$, $(8 + 8i, 3 + 2i)$, $(7 + 5i, 1 + i)$.

(8) Even though Theorem 2 looks a lot like the division algorithm for $\mathbb{Z}$, there are some key differences. For example, show that γ and ρ need not be uniquely determined.

(9) Given $\alpha, \beta \in \mathbb{Z}[i]$ nonzero, what should "the" greatest common divisor of α and β be? Is it unique? If not, can you say something about "how unique" it is?

(10) (*HW*) Prove the following theorem. [Hint: adapt the proofs from (Set 2)].

Theorem 3. *Let $\alpha, \beta \in \mathbb{Z}[i]$ be nonzero, and let $g \in \mathbb{Z}[i]$ be a greatest common divisor of α and β. Then $z \in \mathbb{Z}[i]$ can be written as $z = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[i]$ if and only if z is a multiple of g.*

In set-theoretic notation, this statement is written as:

$$\{\alpha x + \beta y \mid x, y \in \mathbb{Z}[i]\} = \mathbb{Z}[i] \cdot g.$$

(11) How is the above fact similar, or different, from Theorem 1 in Set 2?

(B) In a commutative ring, an element x is a *square* whenever $x = y^2$ for some y.

(1) List all the squares in $\mathbf{U}_3$. How many are there? Do the same for $\mathbf{U}_5$, $\mathbf{U}_7$, $\mathbf{U}_{11}$, $\mathbf{U}_{13}$, and $\mathbf{U}_{17}$. Any conjectures? Is your conjecture true in $\mathbf{U}_9$ or $\mathbf{U}_{15}$? What could be different about these?

(2) Write down multiplication tables for $\mathbf{U}_7$, $\mathbf{U}_8$, and $\mathbf{U}_9$. What do you notice about the rows and columns of your tables? Can you account for this?

(3) Plot the Gaussian integer multiples of $3 + i$ in the complex plane. What does this set look like geometrically? Now plot the following Gaussian integers on the same graph: $0, 2 - i, -6, 1 + i, -3 - 4i, 3 - i, -4 + 2i$. How far away is each from the closest multiple of $3 + i$?

(4) Can you find $q, r \in \mathbb{Z}[i]$ such that $10 - 7i = (4 + 3i)q + r$ and $N(r) < N(4 + 3i)$? Are such q and r unique?

(5) (*HW*) State and prove your conjecture from (1). [Hint: if $x^2 = y^2$ then $(x - y)(x + y) = 0$; what happens then when our commutative ring has no nonzero zerodivisors? And why does our commutative ring have no nonzero zerodivisors?]

[1] If P and Q are statements, The sentence "P if and only if Q", sometimes written "P iff Q", or $P \iff Q$ in symbols, means that P implies Q and that Q implies P. In other words, if one of them is true, both must be true, and if one of them is false, both must be false. In the context of this problem, this means you need to prove two things: that α is a unit $\implies N(\alpha) = 1$, and that $N(\alpha) = 1 \implies \alpha$ is a unit

(C) As on Set 3, solve these problems by justifying each step with one of the axioms of the integers (or more primitive logical principles not particular to the study of integer arithmetic).

(1) If a is a positive integer (an element of $\mathbb{Z}_{>0}$) and b and c are integers satisfying $b < c$, then $ab < ac$.

(2) If a and b are positive integers and $a|b$, then $a \leq b$.

(3) $-1 \cdot -1 = 1$.

(4) $d|a$ and $d|b$ implies $d|(ar + bs)$ for every r and s.