Gaussian Integers

Project on Gaussian Integers.

The following problems are from *Number Theory: A Lively Introduction with Proofs, Applications, and Stories* by Erica Flapan, Tim Marks, and James Pommersheim.

Read the scanned notes on Moodle. Present as much as necessarily for classmates to follow.

Rubric. Present as much as necessarily for classmates to follow: 4 points if individual, 3 points if pair.

Exploration 1 *Here I will use slightly more standard notation, which will match iwth the $\mathbb{Z}[\sqrt{d}]$ topic and complex analysis.*

Definition 1. *The set of* Gaussian integers*, denoted $\mathbb{Z}[i]$ (read "$\mathbb{Z}$ adjoin i") is defined by*

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\},$$

where $i^2 = -1$.

Let $z = a + bi$ be a Gaussian integer. The complex conjugate of z *is $\overline{z} = a - bi$. Define the* norm of z, *as*

$$N(z) = |z| = z\overline{z} = (a + bi)(a - bi) = a^2 + b^2.$$

Lemma (Lemma 13.1.4)**.** *Let r and s be Gaussian integers. Then*

$$N(rs) = N(r)N(s).$$

Problem 1.1 *Prove Lemma 13.1.4*

Rubric. 4 points if individual, 3 points if pair.

Problem 1.2 *Let d and z be Gaussian integers.*

(a) *Prove that if $d \mid z$, then $|d| \mid |z|$.*

(b) *Prove or provide a counterexample for if $|d| \mid |z|$, then $d \mid z$.*

Rubric. 4 points if individual, 3 points if pair.

Definition 2. *Let $p \in \mathbb{Z}[i]$ such that p is not a unit. We say p is* prime *if for every $a, b \in \mathbb{Z}[i]$, $p = ab$ implies that a is a unit or b is a unit.*

Learning outcomes:
Author(s): Claire Merriman

Lemma (Lemma 13.2.6)**.** *Let z be a Gaussian integer. If $N(z)$ is a prime in the (regular) integers, then z is a prime as a Gaussian integer.*

Problem 1.3 *Prove Lemma 13.2.6.*

Rubric. 4 points if individual, 3 points if pair.

Definition 3. *Let $a, d \in \mathbb{Z}[i]$. We say a and b are* relatively prime *if for all $d \in \mathbb{Z}[i]$, $d \mid a$ and $d \mid b$ implies that d is a unit.*

Theorem (Division Theorem for Gaussian Integers)**.** *Let $a, d \in \mathbb{Z}[i]$ with $b \neq 0$. Then there exist Gaussian integers q and r such that $a = qb + r$ with $N(r) < N(b)$*

Problem 1.4 *(If presenting as a pair) Prove Division Theorem for Gaussian Integers using Exercises 15-17 in the scanned notes.*

Rubric. 5 points.

Theorem (Theorem 13.5.4)**.** *Suppose $p \in \mathbb{Z}$ is prime. Then p is a prime in $\mathbb{Z}[i]$ if and only if $p \equiv 3 \pmod 4$.*

Theorem (Theorem 13.5.5)**.** *Let $z \in \mathbb{Z}[i]$. Then z is a prime Gaussian integer if and only if one of the following conditions holds:*

- *$N(z) = 2$,*
- *$N(z)$ is a prime integer congruent to 1 modulo 4,*
- *z is a unit times a prime integer congruent to 3 modulo 4.*

Problem 1.5 *Prove Theorem 13.5.5*

Rubric. 4 points if individual, 3 points if pair.
