Intro to Gaussian Primes

William Kraft

July 21, 2023

1 Gaussian Integers

Definition 1.1 (Gaussian integer)**.** A complex number $z \in \mathbb{C}$ is a Gaussian integer if

$$\Re(z), \Im(z) \in \mathbb{Z}$$

where $\Re$ and $\Im$ represent the real and imaginary parts respectively. Let

$$\mathbb{Z}[i]$$

represent the set of all Gaussian integers.

Definition 1.2 (Norm)**.** The norm of a Gaussian integer, $z = a + bi$ where $a, b \in \mathbb{Z}$, has norm

$$N(z) = a^2 + b^2.$$

Problem 1.3. Calculate $N(3+i)$.

Problem 1.4. Let $z, w \in \mathbb{Z}[i]$. Show that

$$N(z \cdot w) = N(z) \cdot N(w).$$

Note! This property will be of the utmost importance in the next section.

Problem 1.5. Calculate $N((3+i) \cdot (4-i))$.

Definition 1.6 (Divisibillity)**.** A Gaussian integer, z, is divisible by another Gaussian integer, w, if there exists a third Gaussian integer, d, such that

$$z = d \cdot w.$$

Problem 1.7. Is 2 divisible by any Gaussian integer z with $1 < N(z) < 4$?

2 Gaussian Primes

Definition 2.1 (Units)**.** A unit is an element with a multilicative inverse. In the Gaussian integers the units are

$$1, i, -1, -i.$$

Definition 2.2 (Gaussian prime)**.** A non-unit Gaussian integer is a prime if it is only divisible by units or unit multiples of itself.

Problem 2.3. Prove that not all primes in $\mathbb{Z}$ are primes in $\mathbb{Z}[i]$.

Problem 2.4. Prove that all Gaussian integers with prime norms are Gaussian primes.

Theorem 2.5 (Fermat's theorem on sums of squares)**.** A prime $p > 2$ can be written as the sum $a^2 + b^2$ where $a, b \in \mathbb{Z}$ iff $p \equiv 1 \mod 4$.

Problem 2.6. Show that for all primes, p, in $\mathbb{Z}$ with $p \equiv 1 \mod 4$, there exists a Gaussian integer with norm p.

Problem 2.7. Prove that if p is a prime in $\mathbb{Z}$ and $p \equiv 3 \mod 4$, it is a Gaussian prime.

Corollary 2.8 (Categories of Gaussian primes)**.** For each prime, p, in the integers, it falls under one of the following categories:

- If $p \equiv 1 \mod 4$, then there exists a Gaussian prime, z, such that $N(z) = p$.
- If $p \equiv 3 \mod 4$, then p is itself a Gaussian prime.
- If $p = 2$, then $p = (1 + i)(1 - i)$;

Theorem 2.9 (Euclid's Lemma for Gaussian Primes)**.** Let p be a Gaussian prime and $a, b, \in \mathbb{Z}[i]$. If p divides $a \cdot b$ then p divides one of a or b.

Problem 2.10. Show that all Gaussian primes are in fact unit multples of the previously mentioned categories.

Theorem 2.11 (Lagrange's Lemma)**.** If a prime in the integers, p, is congruent to 1 mod 4, then there exists an n such that $p|n^2 + 1$.

Problem 2.12. Without using anything proven by Fermat's theorem on sums of squares, prove it.

Problem 2.13. Show that if an integer can be written as the sum of two squares in more than one way, then it is not prime.