Section 3: Gaussian Integers

We have seen the number i pop up in a couple of previous examples, but we have been hesitant to actually deal with complex numbers. Number theory, as a field of mathematics, generally deals with real numbers. But complex numbers do have their place in number theory as well, and in this section we open ourselves to fully explore their place in this branch of mathematics.

We have seen various classes of numbers grow from rejection by mathematicians to general acceptance. The number 0, negatives numbers, and irrational numbers all went through this same progression. Imaginary numbers, and more generally complex numbers, were the latest to emerge from intellectual banishment and enjoy general acceptance. This transformation took place in the 19th century. That is not to say that imaginary numbers were not used prior to the 1800's, only that they were looked upon with great suspicion and discomfort. As early as the mid 16th century, mathematicians began using negative integers and, more to the point, roots of negative integers in solving equations. In *Ars Magna*, published in 1540, the Italian mathematician Girolamo Cardano refuses to consider equations of the type $x^2 - 3x = 40$ because of the negative coefficient. Instead he considers the equivalent $x^2 = 3x + 40$. Yet even with this heightened sensitivity to negatives, Cardano was the first to venture into the world of imaginary numbers. He posed the following problem in *Ars Magna*:

> "Someone says to you, divide 10 into two parts, one of which multiplied into the other shall produce 40. This is impossible to solve. Nevertheless, we shall solve it in this fashion..."

He then produced the equation $x(10 - x) = 40$ and correctly solved it noting that the two numbers $5 + \sqrt{-15}$ and $5 - \sqrt{-15}$ were the two required numbers. However, Cardano called this solution "puzzling" and said it was "as subtle as it is useless."

It wasn't until the latter half of the 16th century that imaginary numbers started to gain more widespread usage. Rafael Bombelli in 1572 used imaginary numbers, but only temporarily during a problem. Consider the cubic equation $x^3 - 78x = 220$. If Cardano's cubic formula is applied to this equation, we come across the number $\sqrt{-5476}$. For Cardano, this stopped all calculations, and rendered this equation "unsolvable." However, paradoxically for mathematicians at that time, this equations actually has three real solutions, namely 10, $-5 + \sqrt{3}$, and $-5 - \sqrt{3}$. Bombelli noticed this and allowed himself to use imaginary numbers to find the real solutions. He was perplexed about how that worked though, and said he found the solution by "magic."

Imaginary numbers remained on the fringe of acceptance, but clearly outside of it. In 1637, when René Descartes published *La Geometrie*, he referred to numbers such as $\sqrt{-9}$ as "imaginary," and in the 18th century, Leonhard Euler introduced the symbol i for $\sqrt{-1}$. It took

the great Carl Gauss to embrace imaginary numbers at the end of the 18th century for them to become fully accepted.

In his doctoral dissertation published in 1797 (at the age of twenty), Gauss gave the first solid proof of the Fundamental Theorem of Algebra. This theorem states that every equation has a root in the complex numbers. The proof of this important theorem is rather formidable, so we won't go through it here. But we will (finally) begin to discuss the number theory of the complex numbers.

Let $a+bi$ and $c+di$ be two complex numbers. You undoubtedly recall the rules for adding and subtracting such numbers. Multiplication is just as easy,

$$(a+bi)(c+di) = ac+adi+bci+bdi^2 = (ac-bd)+(ad+bc)i\,.$$

For division, we must do a trick similar to rationalizing the denominator. Instead of making the denominator rational, we want it to be real, so I guess we should call this "realizing" the denominator. Namely, if we divide $a+bi$ by $c+di$, we get

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di}\cdot\frac{c-di}{c-di} = \frac{(ac+bd)+(-ad+bc)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2}+\frac{-ad+bc}{c^2+d^2}i\,.$$

The ***Gaussian integers*** are the complex numbers $a+bi$, where a and b are integers. These numbers have many properties in common with ordinary integers. Namely, the sum, difference, and/or product of two Gaussian integers is again a Gaussian integer. However, this may not be true for quotients (just as it often fails to be true for ordinary integers).

Example 3.3.1 Notice that

$\frac{3+2i}{1-6i} = -\frac{9}{37}+\frac{20}{37}i$ is not a Gaussian integer, but

$\frac{16-11i}{3+2i} = \frac{26-65i}{13} = 2-5i$ is a Gaussian integer.

This suggests that we can define divisibility in the Gaussian integers just as we did in the ordinary integers.

Definition 3.3.2 We say that the Gaussian integer $a+bi$ ***divides*** the Gaussian integer $c+di$ if there exists a Gaussian integer $e+fi$ such that $c+di = (a+bi)(e+fi)$.

This is the same thing as saying that the quotient $\frac{c+di}{a+bi}$ is a Gaussian integer. So from Example 3.3.1, we see that $3+2i$ divides $16-11i$, but $1-6i$ does not divide $3+2i$. Now that we can talk about divisibility, we can talk about factorizations and primality. Consider the Gaussian integer $1238-1484i$. This number factors (with some effort) as

$$1238 - 1484i = (2+3i)^3 \cdot (-1+4i) \cdot (3+i)^2 .$$

But to get this factorization, we must have a solid idea of what constitutes a prime Gaussian integer. Even ordinary integers may have, and indeed do have, different prime factorizations over the Gaussian integers. For example, the ordinary integer 600, which we know factors as $2^3 \cdot 3 \cdot 5^2$ over the integers, has a different prime factorization over the Gaussian integers. Its factorization over the Gaussians is

$$600 = -i \cdot (1+i)^6 \cdot 3 \cdot (2+i)^2 \cdot (2-i)^2 .$$

So our present goal is to determine what Gaussian integers are prime.

For the ordinary integers, we think of the prime numbers as the basic building blocks because they cannot be factored any further. However, technically this isn't true. The prime 7 can be "factored" as $7 \cdot 1$, $7 \cdot (-1) \cdot (-1)$, or even $7 \cdot (1)^3 \cdot (-1)^4$. Clearly, we recognize that these are not really different factorizations. What is it about the numbers 1 and –1 that makes them special? The answer is that they are the only two integers with multiplicative inverses. Namely,

$$1 \cdot 1 = 1 \text{ and } (-1) \cdot (-1) = 1 .$$

No other ordinary integer has a multiplicative inverse. This motivates the following definition.

Definition 3.3.3 An ordinary integer is a ***unit*** if it has a multiplicative inverse. Similarly, a Gaussian integer is a unit if it has a multiplicative inverse in the Gaussian integers. Stated another way, a Gaussian integer is a unit if it divides 1.

So what we have already stated is that 1 and –1 are the only ordinary units. The Gaussian integers are blessed with more units that the ordinary integers.

Exercise 3.3.4 Find four Gaussian units.

Definition 3.3.5 A Gaussian integer $a+bi$ is ***prime*** if its only divisors are units and units times $a+bi$.

Now that we know what Gaussian primes are, can we identify them? To do this easily, we move to the complex plane. Given a Gaussian integer $a+bi$, we can associate a point in the plane (a,b). We can then talk about the distance between this point and the origin, which is $\sqrt{a^2+b^2}$, or more specifically, the square of that distance. We call this the norm of the number.

Definition 3.3.6 The ***norm*** of a Gaussian integer $a+bi$ is a^2+b^2. We denote this by $N(a+bi)$.

Example 3.3.7 The norm of $3+2i$ is $(3)^2+(2)^2=13$ and the norm of $-4+6i$ is $(-4)^2+(6)^2=52$.

Theorem 3.3.8 Let α and β be Gaussian integers. Then $N(\alpha\beta)=N(\alpha)N(\beta)$.

Exercise 3.3.9 Prove Theorem 3.3.8.

One useful aspect of norms is that they associate an ordinary integer to each Gaussian integer. We can then use our knowledge of ordinary integers to help us with questions about Gaussian integers.

Theorem 3.3.10 There are only four Gaussian units.

Proof: Let $a+bi$ be a unit. Then there exists a Gaussian integer $c+di$ such that $(a+bi)(c+di)=1$. So $1=N(1)=N((a+bi)(c+di))=N(a+bi)N(c+di)$. Therefore we see that $N(a+bi)=a^2+b^2$ must divide 1. Since all variables are integers, we see that the only possibilities are $a=\pm1, b=0$ or $a=0, b=\pm1$. This yields the four units we have already seen (Exercise 3.3.4).

We are now ready to state which Gaussian integers are prime. The proof of parts (a) and (b) of this theorem are left as an exercise. Part (c) is beyond the scope of these notes.

Theorem 3.3.11 The Gaussian prime numbers can be described as follows:

(a) $1+i$ is a Gaussian prime.
(b) If p be an ordinary prime that is congruent to 1 modulo 4, it can be shown that p can be written as the sum of two squares, say $p=u^2+v^2$. Then $u+vi$ is a Gaussian prime.
(c) Let p be an ordinary prime that is congruent to 3 modulo 4. Then p is also a Gaussian prime.

All other Gaussian prime numbers are equal to a unit multiplied by one of these numbers.

Exercise 3.3.12 Prove Theorem 3.3.11 (a) and (b).