Gaussian Integers

The concepts of divisibility, primality and factoring are actually more general than the discussion so far. For the moment, we have been working in the integers, which we denote by $\mathbb{Z}$ with the familiar notions of addition and multiplication. Now we generalize these notions to include non-integers, and especially, complex numbers. Before we give definitions, here is a motivation from the theory of Diophantine equations. We spent quite a bit of time manipulating algebraic expressions to solve the Diophantine equation

$$x^2 + y^2 = z^2$$

It was shown that all solutions with $(x, y, z) = 1$ and $x, y, z > 0$ and y even had the form

$$x = u^2 - v^2, y = 2uv, z = u^2 + v^2$$

where $(u, v) = 1$ and exactly one of u and v is even. We also saw that for certain types of Diophantine equations it was helpful to factor part of the equation, for instance

$$x^3 - y^3 = 2$$

is the same as $(x - y)(x^2 + xy + y^2) = 2$ and this leads to

$$x - y = 1$$
$$x^2 + xy + y^2 = 2$$

and then $x = y + 1$ and so $3y^2 + 3y + 1 = 2$ but the latter is impossible so there is no solution. Here is an informal way we could combine the two approaches. Suppose we allow complex numbers when factoring the equation. This then allows

$$x^2 + y^2 = (x + \mathbb{i}y)(x - \mathbb{i}y)$$

and if this is to be a square, we might think $x + \mathbb{i}y$ and $x - \mathbb{i}y$ should be squares:

$$x - \mathbb{i}y = (u - \mathbb{i}v)^2$$

for some integers u and v. Expanding it out we get

$$x - \mathbb{i}y = u^2 - v^2 + 2\mathbb{i}uv$$

and in the complex numbers this means $x = u^2 - v^2$ and $y = 2uv$. This agrees with what we proved in class. One point of the Gaussian integers is to make this rigorous.

1. Ring of Gaussian Integers

Definition 1.1. The *ring of Gaussian integers*, denoted $\mathbb{Z}[\mathbb{i}]$ consists of the set of complex numbers of the form $x + \mathbb{i}y$ where x and y are integers and the usual rules of complex addition and multiplication.

Clearly the product and sum of Gaussian integers is again a Gaussian integer. We can assign to each Gaussian integer the modulus or length of the corresponding complex number:

Definition 1.2. [Norm] If $z = x + \mathbb{i}y$ is a Gaussian integer then the *norm* of z is $\mathsf{N}(z) = |z| = x^2 + y^2$. A *unit* is a Gaussian integer with norm 1.

Definition 1.3. [Divisors] If w, z are Gaussian integers, then we write $w \mid z$, or w *divides* z, if there is a Gaussian integer v such that $z = vw$, and w is called a *divisor* of z.

A very useful fact about norms is their *multiplicativity*:

Lemma 1.

If $a, b \in \mathbb{Z}[\mathbb{i}]$, *then* $\mathsf{N}(ab) = \mathsf{N}(a) \cdot \mathsf{N}(b)$. *In particular if* $a \mid b$ *then* $\mathsf{N}(a) \mid \mathsf{N}(b)$.

Proof. Suppose $a = a_1 + a_2\mathbb{i}, b = b_1 + b_2\mathbb{i}$. Then

$$\begin{aligned}\mathsf{N}(ab) &= \mathsf{N}((a_1 + \mathbb{i}a_2)(b_1 + \mathbb{i}b_2)) = \mathsf{N}(a_1b_1 - a_2b_2 + \mathbb{i}(a_2b_1 + a_1b_2)) \\ &= (a_1b_1 - a_2b_2)^2 + (a_2b_1 + a_1b_2)^2 \\ &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) = \mathsf{N}(a) \cdot \mathsf{N}(b)\end{aligned}$$

This proves the lemma. ■

The only Gaussian integers with norm 1 are $\pm 1, \pm\mathbb{i}$ since these are the four points in the complex plane on the unit circle with integer co-ordinates.

2. Gaussian Primes

Definition 2.1. [Gaussian Primes] If a Gaussian integer z is not a unit and the only divisors of z are units and z times a unit, then z is called a *Gaussian prime.*

Example. If n is an integer that is not prime, then of course n cannot be a Gaussian prime. If p is an integer prime, then is p a Gaussian prime? The answer is no, because $(1+i)(1-i) = 2$ so 2 is not a prime. However, 3 is a prime since $(x+iy)(a+ib) = 3$ means $xa - by = 3$ and $ay + xb = 0$. This means $x(a^2+b^2) = 3$ but then since $a+ib$ is not a unit, meaning $a^2+b^2 \neq 1$, we must have $a^2+b^2 = 3$ and we already know this is impossible. So 3 is a prime. This example was instructive, since it already suggest which primes are Gaussian primes: they are the primes p such that $x^2+y^2 = p$ has no solution:

Theorem 2.1. *The integer primes that are Gaussian primes are integer primes p such that $x^2+y^2 = p$ has no solution.*

Proof. If p is an integer prime with a solution (a,b) to $x^2+y^2 = p$ then

$$(a - \mathbb{i}b)(a + \mathbb{i}b) = a^2 + b^2 = p$$

So p is not a Gaussian prime. Now if p is not a Gaussian prime, then

$$(x + \mathbb{i}y)(a + \mathbb{i}b) = p$$

for some Gaussian integers $x+\mathbb{i}y$, $a+\mathbb{i}b$. As in the example, this means $xa - by = p$ and $ay + xb = 0$. This means $x(a^2+b^2) = p$ but then since $a+ib$ is not a unit, meaning $a^2+b^2 \neq 1$, we must have $a^2+b^2 = p$ and so the equation has a solution. ■

Lemma 2.1. *Let $z \in \mathbb{Z}[\mathbb{i}]$. If $\mathsf{N}(z)$ is an integer prime, then z is a Gaussian prime.*

Proof. Suppose z is not a Gaussian prime, so there are non-units a and b with $z = ab$. By Lemma 1, $\mathsf{N}(z) = \mathsf{N}(ab) = \mathsf{N}(a) \cdot \mathsf{N}(b)$, and since $\mathsf{N}(a) \neq 1 \neq \mathsf{N}(b)$, $\mathsf{N}(z)$ is conjugate. ■

Soon we shall see that the only Gaussian integers that are Gaussian primes are the ones which are integer primes as in Theorem 2.1, or the ones whose norm is a prime.

Fundamental Theorem of Arithmetic for Gaussian Primes.

Let $z \in \mathbb{Z}[\mathbb{i}]$. Then up to reordering and multiplication by units, there exist unique Gaussian primes $z_1, z_2, \ldots, z_k$ such that $z = z_1 z_2 \ldots z_k$.

We cannot prove this theorem yet, but we can show already that every Gaussian integer is a product of Gaussian primes, using the norm:

Prime Factorization Theorem.

Let $z \in \mathbb{Z}[\mathbb{i}]$. Then there exist Gaussian primes $z_1, z_2, \ldots, z_k$ such that $z = z_1 z_2 \ldots z_k$.

Proof. If z is itself a Gaussian prime, then we are done. Now we proceed by induction on the norm. If $z = ab$ where $\mathsf{N}(a) > 1, \mathsf{N}(b) > 1$. Since $\mathsf{N}(z) = \mathsf{N}(ab) = \mathsf{N}(a)\mathsf{N}(b)$ we have $\mathsf{N}(a), \mathsf{N}(b) < \mathsf{N}(z)$. By induction, a and b have prime factorizations and therefore so does z. ■

The extra steps needed to go from this to the fundamental theorem involve the definition of greatest common divisors and the Euclidean algorithms. The main step we used to prove unique factorization in the integers is that if p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$. The same turns out to hold in the Gaussian integers, but we have to prove it.

3. Euclidean Algorithms

The Euclidean division theorem in the integers says that for any non-zero integers n and m, there exist unique non-negative integers q, r such that $r < |m|$ and $n = qm + r$. A Euclidean division theorem exists for Gaussian integers just as it exists for the integers.

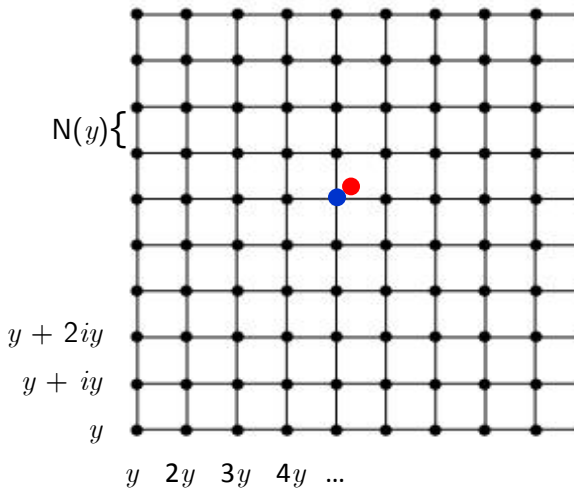
Euclidean Division Theorem,

For any non-zero Gaussian integers x, y, there exist Gaussian integers q, r such that $\mathsf{N}(r) < \mathsf{N}(x)$ *and $x = qy + r$. We have $y \mid x$ if and only if $r = 0$.*

Proof. The Gaussian multiples of the complex number y make a square lattice whose squares have side length $\mathsf{N}(y)$. Now x (red point below) lies in one of the squares of the lattice, so x is at distance less than $\mathsf{N}(y)$ from the closest corner qy (blue point below). That means for some Gaussian integer r with $\mathsf{N}(r) < \mathsf{N}(x)$, $x = qy + r$. For the second part, if $r = 0$ then clearly $y \mid x$. If $y \mid x$, say $x = wy$, then by Lemma 1 (multiplicativity),

$$\mathsf{N}(y) > \mathsf{N}(r) = \mathsf{N}(x - qy) = \mathsf{N}(y(w - q)) = \mathsf{N}(y)\mathsf{N}(w - q)$$

This is impossible unless $\mathsf{N}(w - q) = 0$. Then $w = q$ and $r = x - qy = wy - wy = 0$. ■



There is one important difference relative to the integers, and that is the absence of the word unique: the Gaussian integers are not unique in this theorem. We call r a *remainder* and q a *quotient*. The key point is that the norm of r is less than the norm of y.

The Euclidean division theorem can be turned into an algorithm for finding quotient and remainder.

Euclidean Division Algorithm, *For any non-zero Gaussian integers x, y, a quotient q and remainder r can be found by writing $x/y = u + iv$, rounding u and v to their nearest integers U and V, and letting $q = U + iV$ and $r = x - qy$.*

Example. Find a quotient, remainder when $3 + 2\mathbb{i}$ is divided by $y = -1 + 3\mathbb{i}$. First we write

$$\frac{3 + 2\mathbb{i}}{-1 + 3\mathbb{i}} = \frac{3}{10} + \mathbb{i}\frac{-11}{10}.$$

The nearest integer to $\frac{3}{10}$ is 0 and the nearest integer to $\frac{-11}{10}$ is -1.

Therefore we may take the quotient to be $q = -\mathbb{i}$ and write

$$3 + 2\mathbb{i} = -\mathbb{i}(-1 + 3\mathbb{i}) + \mathbb{i}$$

and a remainder is $\mathbb{i}$. Note again that the quotient and remainder are not unique, we could just as well have taken them to be 1 - $\mathbb{i}$ and $1 + 2\mathbb{i}$, as long as the norm of the remainder is less than the norm of y.

Definition 3.1. [GCD] A *common divisor* of Gaussian integers w and z is a Gaussian integer y that divides w and z. A *greatest common divisor* of w, z is a common divisor of w and z with greatest norm. If the norm is 1, then the Gaussian integers are *relatively prime.*

Two Gaussian integers in general have many gcds. Let (z, w) be the set of gcds of w and z. Gcds are found as in the Euclidean gcd algorithm: if N(z) ≥ N(w) write $z = qw + r$ as in the Euclidean division theorem. If g is a gcd of w and r, then $g \in (z, w)$ but we have reduced the norm, so we can repeat until the remainder is zero. This is a Euclidean gcd algorithm.

Example. Find a gcd of $3 + 2\mathbb{i}$ and $1 + \mathbb{i}$. First we apply the division algorithm:

$$\frac{3+2\mathbb{i}}{1+\mathbb{i}} = \frac{5}{2} - \mathbb{i}\frac{1}{2}$$

and so a quotient is $2 - \mathbb{i}$. Therefore $3 + 2\mathbb{i} = (2 - \mathbb{i})(1 + \mathbb{i}) + \mathbb{i}$. We know a gcd of $3 + 2\mathbb{i}$ and $1 + \mathbb{i}$ is a gcd of $1+\mathbb{i}$ and $\mathbb{i}$. Now $1 + \mathbb{i} = (1 - \mathbb{i}).\mathbb{i} + 0$, and we stop. So we know a gcd is $\mathbb{i}$, which is a unit, and this tells us the two numbers are relatively prime.

A consequence of the gcd algorithm, working backwards as in the integers, is the following:

GCD Property *Any gcd of two Gaussian integers is a linear combination of them.*

Prime Divisor Property *If p is a Gaussian prime and $p \mid wz$ then $p \mid w$ or $p \mid z$.*

Proof. Suppose p doesn't divide w. Then every gcd of p and w is a unit u. By the GCD property, $u = rp + sw$ for some Gaussian integers r, s, and so $uz = rpz + swz$. But p is a divisor of everything on the left, so $p \mid uz$ and that means (check it) $p \mid z$. ■

Proof of Fundamental Theorem of Arithmetic for Gaussian Primes.

We already saw that each $z \in \mathbb{Z}[\mathbb{i}]$ has a prime factorization $z = z_1 z_2 ... z_k$. The unique factorization theorem is clearly true for units i.e. Gaussian integers of norm 1. Now proceed by induction on the norm. If $\mathsf{N}(z) > 1$ and z is a Gaussian prime we are done. Otherwise, if $p \mid z$ is a prime divisor of largest norm, then by the prime divisor property, p is one of $z_1, z_2, ..., z_k$. Then $\mathsf{N}(z/p) < \mathsf{N}(z)$ so by induction z/p has a prime factorization that is unique. Then clearly adding p gives the unique factorization of z. ■

We have concluded that while gcds are not unique in the Gaussian integers, they still enjoy unique factorization as in the integers. Now we are going to put this property to work, and in the end, to solve some Diophantine equations.