GAUSSIAN INTEGERS

1. Basic Definitions

A Gaussian integer is a complex number $z = x + yi$ for which x and y, called respectively the real and imaginary parts of z, are integers. In particular, since either or both of x and y are allowed to be 0, every ordinary integer is also a Gaussian integer. We recall that the complex conjugate of z is defined by $\overline{z} = x - iy$ and satisfies, for arbitrary complex numbers z and w, $\overline{z+w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$. We remark that sums, products, and complex conjugates of Gaussian Integers are again Gaussian integers.

For any complex number z, we define the norm of z by $N(z) = z\overline{z} = x^2 + y^2$, where x and y are the respectively the real and imaginary parts of z. It follows that $N(zw) = N(z)N(w)$. We remark that the norm of any complex number is a non-negative real number, the norm of a Gaussian integer is a non-negative integer, and only 0 has norm 0. We observe further that only ± 1 and $\pm i$ have norm 1. These are called unit Gaussian integers, or units, and two Gaussian integers are called associates if they can be obtained from one another by multiplication by units. Note that, in general, $\overline{z}$ and its associates are distinct from z and its associates. The exceptions to this rule occur when the real and imaginary parts of z have the same absolute value, and when the real or imaginary part of z is 0.

We defined divisibility for the Gaussian integers exactly as for integers. We say $z|w$ if w is the product of z and some Gaussian integer. A Gaussian integer is called irreducible if its only divisors are units and its associates. Notice that if $N(z)$ is a prime, then z is irreducible since if $z = w_1 w_2$, it follows that $N(z) = N(w_1)N(w_2)$, from which it follows that either w_1 or w_2 is a unit. For example $1 + i$ and $2 + i$ are irreducible, since they have norms 2 and 5 respectively. We do not claim the converse of this proposition. For example, we will see that 3 is irreducible as a Gaussian integer, but $N(3) = 9$, which is not prime. Notice that we have just proved that 2 and 5 are not irreducible as Gaussian integers.

2. The Division Algorithm and gcd's for Gaussian Integers

The division algorithm for Gaussian integers states that if z and d are Gaussian integers, then there are Gaussian integers q and r with $N(r) \leq \frac{1}{2}N(d)$ and $z = qd + r$. We do not assert the uniquenss of r, for reasons that will become clear in the proof.

The basic idea is that if we represent complex numbers in the plane in the usual way with the real and imaginary parts as coordinates, then the distance between z and w is $SqrtN(z - w)$. We will choose q to be a Gaussian integer whose distance from the complex number $\frac{z}{d}$ is as small as possible. We can always choose q with $N(q - \frac{c}{d}) \leq \frac{1}{2}$, but there may be up to four such choices possible. Since $r = z - qd = d(q - \frac{c}{d})$ it follows both that r is a Gaussian integer and that $N(r) \leq \frac{1}{2}N(d)$. This completes the proof.

We now define d to be a greatest common divisor of z and w if d has the form $\alpha z + \beta w$ with α and β Gaussian integers, and $N(d)$ takes the smallest positive value for Gaussian integers of that form. It now follows from the division algorithm that d divides both z and w. It also follows, as in the case of linear combinations of integers, that any common divisor of z and w divides d. It follows that all greatest common divisors of z and w are associates of one another.

It now follows precisely as it did for ordinary integers that if α, z and w are Gaussian integers, $\alpha | zw$ and 1 is a greatest common divisor of α and z, then α divides w. It also follows precisely as for ordinary integers that if α is an irreducible Gaussian integer, then either $\alpha | z$ or 1 is a greatest common divisor of α and z. It is similarly easy to prove that every Gaussian integer that is neither a unit nor irreducible is a product of irreducible factors. Uniqueness is slightly more awkward to prove, simply because it is more awkward to state; we will not require the details.

3. Which Primes are Irreducible Gaussian Integers ?

Let p be an odd prime. If p is not an irreducible Gaussian integer then p has a factor of the form $x + yi$ and then $N(x + yi) | N(p) = p^2$. If $x + yi$ is neither a unit nor an associate of p, we must have $N(x + yi) = (x + yi)(x - yi) = x^2 + y^2 = p$. This establishes that an odd prime is an irreducible Gaussian integer if and only if it is not the sum of two squares.

We notice next that if x and y have opposite parity, then $x^2 + y^2 \equiv 1 \pmod 4$. This is true because all even squares are congruent to $0 \pmod 4$ and all odd squares are congruent to $1 \pmod 4$. It follows that all primes congruent to 3 $\pmod 4$ are irreducible Gaussian integers.

We will now show that all primes congruent to 1 $\pmod 4$ have the form $N(x+yi) = x^2+y^2$ and therefore are not irreducible Gaussian integers. We begin by recalling that -1 is a quadratic residue, for such a prime. Thus there exists an integer x with $x^2+1 \equiv 0 \pmod p$. Moreover, by choosing a least residue, and replacing x by $p-x$ if necessary, we can be certain that $0 < x \le \frac{p-1}{2}$. This gives

$$(x+i)(x-i) = x^2+1 = kp \le \frac{(p-1)^2}{4} + 1 < p^2.$$

If p is an irreducible Gaussian integer, it must divide at least one of the factors on the left. But then it must divide both, and the product must be divisible by p^2, which is impossible, since it is less than p^2. The conclusion is that p is not an irreducible Gaussian integer if $p \equiv 1 \pmod 4$.

Now, we observe that if $p \equiv 1 \pmod 4$, and $N(x+yi) = p$ then any Gaussian integer whose norm is p must be irreducible, must divide p, and therefore must divide either $x+yi$ or $x-yi$. It follows that any such Gaussian integer is an associate of either $x+yi$ or $x-yi$.

It now follows that the irreducible Gaussian integers are the following and their associates:

- Primes congruent to 3 $\pmod 4$.
- $1+i$
- $x+yi$ and $x-yi$ where x and y are positive integers such that x^2+y^2 is a prime congruent to 1 $\pmod 4$.

4. Sums of two squares

Clearly, an integer is the sum of two squares if and only if it is the norm of some Gaussian integer. If we factor a Gaussian integer into irreducible factors, the norms of the factors are primes not not congruent to 3 $\pmod 4$ and the squares of primes congruent to 3 $\pmod 4$. It follows that the norms of Gaussian integers are precisely those numbers for which all primes congruent to 3 $\pmod 4$ have even multiplicity.

5. Problems

1. Apply the Euclidean algorithm for Gaussian integers to express $8+7i$ in the form $qd+r$ where $d = 1+2i$ and q and r are Gaussian integers with $N(r) \le \frac{1}{2}N(d)$.

Solution: We have

$$\frac{8+7i}{1+2i} = \frac{(8+7i)(1-2i)}{5} = \frac{22}{5} - \frac{9}{5}i.$$

The nearest Gaussian integer is $4-2i$, so that the remainder is given by

$$r = 8+7i-(1+2i)(4-2i) = i.$$

2. Why is $1-i$ not on the list of irreducible Gaussian integers?

   Answer: $1-i$ is an associate, as well as the conjugate, of $1+i$.

3. Prove that the hypotenuse of a fundamental Pythagorean triple is not divisible by any prime congruent to $3 \pmod 4$.

   Proof: The hypotenuse of a fundamental Pythagorean triple has the form $z\overline{z}$ where $z = m+ni$, and m and n are relatively prime. If p is a prime congruent to $3 \pmod 4$, and divides $z\overline{z}$, then p divides at least one of the factors. From this, it follows that m and n are not relatively prime, as is required for fundamental Pythagorean triples.

4. Find the smallest integer that is the hypotenuse of eight different fundamental Pythagorean triples.

   Solution: Such an integer must be divisible by four distinct primes, each congruent to $1 \pmod 4$. The smallest is $5{\cdot}13{\cdot}17{\cdot}29 = 32045$.