Week 5 Summary

Lecture 9

Let α, $\beta \in \mathbb{Z}[i]$. We shall that α *divides* β, which we write as $\alpha|\beta$, if $\beta = \alpha\gamma$ for some $\gamma \in \mathbb{Z}[i]$. If $\alpha|\beta$ and $\beta|\alpha$ then α and β are associates; we write $\alpha \sim \beta$ to indicate this. It is easily seen that if $\alpha \sim \alpha'$ and $\beta \sim \beta'$ then $\alpha|\beta$ if and only if $\alpha'|\beta'$.

Definition: Let a, b, $d \in \mathbb{Z}[i]$. We say that d is a greatest common divisor of a and b if

(1) $d|a$ and $d|b$;

(2) for all $c \in \mathbb{Z}[i]$, if $c|a$ and $c|b$ then $c|d$.

If d is a gcd of a and b then d' is a gcd of a and b if and only if d' is an associate of d. So if a and b have a gcd then they have exactly four gcd's. We shall write $\mathrm{GCD}(a, b)$ for the set of all gcd's of a and b.

To prove the existence of gcd's we use the Euclidean Algorithm. Suppose that r_0, $r_1 \in \mathbb{Z}[i]$, not both zero. The notation is chosen so that $N(r_1) \le N(r_0)$. Starting with $j = 1$, repeat the following steps as often as possible:

- If $r_j \neq 0$, find a_j, $r_{j+1} \in \mathbb{Z}[i]$ satisfying $r_{j-1} = a_j r_j + r_{j+1}$ and $N(r_{j+1}) \le (1/2)N(r_j)$.
- Advance j by 1.

If $N(r_j) > 0$ then $r_j \neq 0$, and the process can be continued; furthermore, $N(r_j) > N(r_{j+1}) \ge 0$. In a finite number of steps the sequence $N(r_1)$, $N(r_2)$, $N(r_3)$, $\ldots$ reaches zero, and the process stops. So for some k we have

$$\begin{aligned} r_0 &= a_1 r_1 + r_2 && 0 < N(r_2) < N(r_1) \\ r_1 &= a_2 r_2 + r_3 && 0 < N(r_3) < N(r_2) \\ &\vdots \\ r_{k-2} &= a_{k-1} r_{k-1} + r_k && 0 < N(r_k) < N(r_{k-1}) \\ r_{k-1} &= a_k r_k. \end{aligned}$$

(Thus $r_{k+1} = 0$.) From the first of these equations it follows that $c \in \mathbb{Z}[i]$ is a common divisor of r_0 and r_1 if and only if it is a common divisor of r_1 and r_2; the second equation similarly shows that c is a common divisor of r_1 and r_2 if and only if it is a common divisor of r_2 and r_3; the next equation shows that the common divisors of r_2 and r_3 are the same as the common divisors of r_3 and r_4, and so on. So

$$\{\, c \in \mathbb{Z}[i] \bigm| c|r_0 \text{ and } c|r_1 \,\} = \{\, c \in \mathbb{Z}[i] \bigm| c|r_{k-1} \text{ and } c|r_k \,\}.$$

But the last equation shows that $r_k|r_{k-1}$, and hence every divisor of r_k is also a divisor of r_{k-1}. So the set of common divisors of r_{k-1} and r_k is just the set of divisors of r_k. We conclude that the set of common divisors of r_0 and r_1 is precisely the set of divisors of r_k. In particular, this shows that r_k is a gcd of r_0 and r_1.

As for $\mathbb{Z}$, we can work backwards through the equations obtained in the Euclidean Algorithm, or use a Magic Table, to express the last nonzero remainder, r_k, in the form $pr_1 + qr_0$ (for some p, $q \in \mathbb{Z}[i]$). And multiplying through by an arbitrary Gaussian integer shows that every multiple of r_k can also be expressed in this form. (This includes, in particular, every gcd of r_0 and r_1, since they are obtained from r_k by multiplying by units.)

It is a corollary of the existence of gcd's that a unique factorization theorem holds in $\mathbb{Z}[i]$. Observe first that if a Gaussian integer has norm greater than 1 and is not irreducible, then it can be expressed as a product of two Gaussian integers with smaller norms; if either factor is not irreducible, then it in turn can be factorized as a product of Gaussian integers whose norms are smaller again. Since the norms are always positive integers, they cannot continue decreasing indefinitely; so eventually a stage must be reached when all the factors are irreducible. So it is clear that any nonzero Gaussian integer that is not a unit can be expressed as a product of irreducibles. Using properties of gcd's, we can prove that such factorizations are essentially unique.

Lecture 10

***Proposition:** Let a, $b \in \mathbb{Z}[i]$ with b irreducible. Then either $b \in \mathrm{GCD}(a, b)$, and then $b|a$, or else $1 \in \mathrm{GCD}(a, b)$.

This follows readily from the fact that any gcd of a and b, being a divisor of b, must either be a unit or an asssociate of b (since b has no other divisors).

***Proposition:** Suppose that $b|a_1a_2$ and $1 \in \mathrm{GCD}(a_1, b)$. Then $b|a_2$.

The proof of this for $\mathbb{Z}[i]$ is just the same as its proof for $\mathbb{Z}$.

It is an immediate corollary of the above two propositions that if b is irreducible and divides a_1a_2 then either $b|a_1$ or $b|a_2$. And then an easy induction shows that if $b|a_1a_2\cdots a_m$ and b is irreducible then $b|a_j$ for some j. This enables us to prove the unique factorization theorem.

Theorem: If $a_1a_2\cdots a_m \sim b_1b_2\cdots b_k$, where all the a_j's and b_j's are irreducible Gaussian integers, then $k = m$, and we can renumber a_1, a_2, ... , a_m so that $a_j \sim b_j$ for $j = 1, 2, \ldots, k$.

The proof goes like this. Since b_1 is irreducible and divides $b_1b_2\cdots b_k$, which is an associate of $a_1a_2\cdots a_m$, it follows that $b_1|a_j$ for some j. Since a_j is also irreducible it follows that a_j and b_1 are associates. After renumbering, we can assume that $j = 1$; that is, a_1 and b_1 are associates. So

$$b_1a_2a_3\cdots a_m \sim a_1a_2a_3\cdots a_m \sim b_1b_2b_3\cdots b_k$$

and, cancelling, it follows that $a_2a_3\cdots a_m \sim b_2b_3\cdots b_k$. We can now repeat the argument to get $a_2 \sim b_2$, cancel these factors away, then deduce that $a_3 \sim b_3$, and so on until no factors are left.

The theorem says that, up to associates and reordering factors, factorization into irreducibles is unique in $\mathbb{Z}[i]$.

***Proposition:** Let $p \in \mathbb{Z}$ be a prime. If $p = a^2 + b^2$ for some integers a and b, then $a + bi$ and $a - bi$ are irreducible in $\mathbb{Z}[i]$, and p is not irreducible in $\mathbb{Z}[i]$ (since $p = (a + bi)(a - bi)$). If p cannot be written as a sum of two squares then p is irreducible as an element of $\mathbb{Z}[i]$.

The first part of this follows from the fact, proved earlier, that a Gaussian integer whose norm is prime must be irreducible. For the second part, suppose that p cannot be expressed as the sum of two squares, and suppose $p = (a + bi)(c + di)$ in $\mathbb{Z}[i]$. Taking norms gives $p^2 = (a^2 + b^2)(c^2 + d^2)$. Since p is prime the only ways p^2 can be factorized in $\mathbb{Z}^+$ are as the product of p^2 and 1 or as the product of p and p. But $a^2 + b^2 = p = c^2 + d^2$ is impossible here because of our assumption about p. So we must have either $a^2 + b^2 = 1$ or $c^2 + d^2 = 1$; that is, one of the factors $a + bi$ or $c + di$ must be a unit. Thus p is irreducible.

Since $0^2 \equiv 2^2 \equiv 0 \pmod 4$ and $1^2 \equiv 3^2 \equiv 1 \pmod 4$, it follows that if a and b are any integers then $a^2 + b^2$ is congruent modulo 4 to either 0, 1 or 2. It is impossible to have $a^2 + b^2 \equiv 3 \pmod 4$. So primes that are congruent to 3 modulo 4 cannot be expressed as the sum of two squares, and hence they are irreducible in $\mathbb{Z}[i]$. It turns out that primes congruent to 1 modulo 4 can be expressed as sums of two squares, but we are not ready to prove this yet.

We can apply our knowledge of unique factorization in $\mathbb{Z}[i]$ to the study of Pythagorean triples. These are solutions of the Diophantine equation $x^2 + y^2 = z^2$. Notice that if (x, y, z) is a Pythagorean triple then so is (dx, dy, dz) for any integer d. Similarly, if (x, y, z) is a Pythagorean triple such that some integer d is a factor of all of x, y and z, then $(x/d, y/d, z/d)$ is also a Pythagorean triple. So to classify all Pythagorean triples, it will be sufficient to classify those that have no common factor bigger than 1. Now it is fairly easy to see that in any such Pythagorean triple, one of x or y must be odd and the other even. For if they were both even then $z^2 = x^2 + y^2$ would also be even, forcing z to be even, contradicting the assumption that x, y and z have no common factor; on the other hand, if x and y were both odd then x^2 and y^2 would both be congruent to 1 modulo 4, giving $z^2 \equiv x^2 + y^2 \equiv 2 \pmod 4$, which is impossible.

In view of this we define a *basic Pythagorean triple* to be a triple (x, y, z) of positive integers, with no common factor, such that x is odd and y is even, and $x^2 + y^2 = z^2$. We shall show that for every basic Pythagorean triple (x, y, z) there exist positive integers a and b such that $x = a^2 - b^2$, $y = 2ab$ and $z = a^2 + b^2$. (It is trivial to check that these formulas always yield a Pythagorean triple, for any integer values of a and b.)