Week 6 Summary

Lecture 11

We have shown that if $a$ and $b$ are integers such that $a^2 + b^2$ is prime then $a + bi$ is an irreducible element of $\mathbb{Z}[i]$, and we have also shown that that if $p$ is a prime that is not a sum of two squares then $\pm p$ and $\pm pi$ are irreducible in $\mathbb{Z}[i]$.

*Proposition:* Every irreducible element of $\mathbb{Z}[i]$ has one or other of these two forms.

Suppose that $(x, y, z)$ is a basic Pythagorean triple. Any prime that is a divisor of both $x$ and $z$ is a divisor of $z^2 - x^2 = y^2$, and hence a divisor of $y$. But since our Pythagorean triple $(x, y, z)$ is basic, there is no integer greater than 1 dividing all three of $x$, $y$ and $z$. So gcd($x, z$) = 1. Since $x$ is odd and $y$ even it follows that $z$ is odd. So gcd($4x^2, z^2$) = 1. Now suppose that $\gamma \in \mathbb{Z}[i]$ is a gcd of $x + iy$ and $x - iy$. Then $\gamma$ divides $(x + iy) + (x - iy) = 2x$. Taking complex conjugates, we deduce that also $\overline{\gamma} \mid 2x$. So $\gamma \overline{\gamma} \mid (2x)^2$. That is, $N(\gamma) \mid 4x^2$. Also, since $\gamma \mid (x + iy)$ and $\overline{\gamma} \mid (x - iy)$ it follows that $\gamma \overline{\gamma} \mid (x + iy)(x - iy) = x^2 + y^2 = z^2$. So $N(\gamma) \mid z^2$, and therefore $N(\gamma) \mid \gcd(4x^2, z^2) = 1$. Hence $\gamma$ is a unit: we have shown that $x + iy$ and $x - iy$ are coprime Gaussian integers. But their product is a square (since $(x + iy)(x - iy) = z^2$), and it follows from the unique factorization theorem for $\mathbb{Z}[i]$ that if the product of two coprime Gaussian integers is a square then they are each squares, up to unit factors. So $x + iy = u_1 \zeta_1^2$ and $x - iy = u_2 \zeta_2^2$ for some units $u_1, u_2$ and some $\zeta_1, \zeta_2 \in \mathbb{Z}[i]$.

Writing $\zeta_1 = a + bi$, and noting that $u_1$ must be 1, $-1$, $i$ or $-i$, we have $x + iy = \pm((a^2 - b^2) + 2abi)$ or $x + iy = \pm(-2ab + (a^2 - b^2)i)$. Since $x$ is odd, we must have the former case rather than the latter. Interchanging $a$ and $b$ if necessary, we see that $x = a^2 - b^2$ and $y = 2ab$ for some integers $a$ and $b$.

We turn next to an investigation of powers in $\mathbb{Z}_n$. When $n = 7$, for example, the successive powers of 3 are 3, 2, 6, 4, 5, and 1, repeating in a periodic sequence of period six. The powers of 2 form a sequence of period three, and the powers of 6 a sequence of period two. It turns out that if gcd($a, n$) = 1 then there is always a positive integer $k$ such that $a^k \equiv 1 \pmod{n}$. The least such $k$ is called the order of $a$ modulo $n$, denoted by ord$_n(a)$. The sequence of powers of $a$ in $\mathbb{Z}_n$ has period ord$_n(a)$. One can check easily that ord$_7(a)$ is a divisor of six in each case; this is a special case of a result known as the Fermat-Euler Theorem.

Lecture 12

We adopt the convention that if $S$ is any finite set then $|S|$ denotes the number of elements of $S$.

The Euler phi function is the function $\varphi: \mathbb{Z}^+ \to \mathbb{Z}^+$ defined as follows: $\varphi(n)$ is the number of positive integers $a$ with $1 \leq a \leq n$ and gcd($a, n$) = 1. That is, $\varphi(n) = |\{a \in \mathbb{Z} | 1 \leq a \leq n \text{ and } \gcd(a, n) = 1\}|$. 

−1−
Recall that \( \gcd(a, n) = 1 \) if and only if \( a \) has an inverse in \( \mathbb{Z}_n \). In other words, \( \gcd(a, n) = 1 \) if and only if \( a \) is a unit in \( \mathbb{Z}_n \). Denote the set of units of \( \mathbb{Z}_n \) by \( \mathbb{Z}_n^* \). The definition of \( \varphi(n) \) can then be restated as \( \varphi(n) = |\mathbb{Z}_n^*| \).

For example, \( \mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\} \), and so \( \varphi(15) = 8 \). Similarly one can check that \( \varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6, \varphi(8) = 4, \varphi(9) = 6 \). There is a formula for \( \varphi(n) \) in terms of the prime factorization of \( n \); we shall come to this later.

**Fermat-Euler Theorem:** Let \( a, n \in \mathbb{Z}^+ \) with \( \gcd(a, n) = 1 \). Then \( a^{\varphi(n)} \equiv 1 \pmod{n} \). Moreover, \( \text{ord}_n(a) \) is a divisor of \( \varphi(n) \).

(The proof can be found in Walters, or indeed any elementary text.)

A *primitive root* modulo \( n \) is an integer \( a \) coprime to \( n \) having the property that \( \text{ord}_n(a) = \varphi(n) \). For example, since \( \text{ord}_7(3) = 6 = \varphi(7) \), we see that 3 is a primitive root modulo 7. When \( a \) is a primitive root modulo \( n \), the powers of \( a \) in \( \mathbb{Z}_n^* \), which has only \( \varphi(n) \) elements altogether, it follows that all elements of \( \mathbb{Z}_n^* \) are powers of \( a \). For example, the powers of 2 in \( \mathbb{Z}_{25}^* \), from \( 2^1 \) to \( 2^{20} \), are as follows: 2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 18, 11, 22, 19, 13 and 1. We exhausted all 20 elements of \( \mathbb{Z}_{25}^* \) before reaching the point at which the sequence repeats. So 2 is a primitive root modulo 25.

Primitive roots modulo \( n \) do not exist for all values of \( n \). They exist when \( n \) is prime or the square of a prime, or twice a prime, but not otherwise. They are not easy to find: basically, one just uses trial and error to find them.

Consider the decimal representation of a rational number \( p/q \), where \( p \) and \( q \) are coprime positive integers with \( p < q \). As is well known, this has the form \( 0.a_1a_2...a_na_{n+1}a_{n+2}...a_{n+r} \), where the overline notation indicates a repeating block. The values of \( n \) and \( r \) for a given decimal expansion of \( p/q \) are not unique: for example, 0.23154 can also be written as 0.231541541. To avoid this, we insist on choosing \( n \) and \( r \) to be as small as possible. We then call \( n \) and \( r \), respectively, the lengths of the non-periodic and periodic parts of the decimal expansion.

**Proposition:** If \( q = 2^a5^bm \), where \( \gcd(m, 10) = 1 \), then the non-periodic part of the decimal expansion of \( p/q \) has length \( \max(a, b) \), and the periodic part has length \( \text{ord}_m(10) \). (Note that it is assumed that \( \gcd(p, q) = 1 \) and \( 0 < p < q \).)