Week 4 Summary

Lecture 7

The *least common multiple* of two nonzero integers a and b is a positive integer m with the following two properties:

(i) $a|m$ and $b|m$;

(ii) for all $c \in \mathbb{Z}$, if $a|c$ and $b|c$ then $m|c$.

In words, Property (i) says that m is a multiple of both a and b, while Property (ii) says that every integer that is a multiple of both a and b is a multiple of m.

In the first question of the homework assignment you are asked to show that $\text{lcm}(a, b) = ab/d$, where $d = \gcd(a, b)$.

If a, b and c are given integers then the Diophantine equation $xa + yb = c$ has no solution unless $d|c$, where $d = \gcd(a, b)$. If this condition is satisfied then a solution x_0, y_0 can be found via the Euclidean Algorithm, as explained last time. The general solution is then

$$x = x_0 + t(b/d)$$
$$y = y_0 - t(a/d)$$

where t is a parameter that can take arbitrary integer values.

Whilst on the topic of gcd's and lcm's, there are three more properties we should note. First of all, let a and b be fixed positive integers, and consider the following two sets:

$$S = \{\, n \in \mathbb{Z}^+ \mid n|a \text{ and } n|b \,\},$$
$$T = \{\, n \in \mathbb{Z}^+ \mid n = pa + qb \text{ for some } p,\, q \in \mathbb{Z} \,\}.$$

Every element of S is a divisor of every element of T, and so every element of S is less than or equal to every element of T. The gcd of a and b is in both sets: it is the largest element of S and the smallest element of T.

You should be able to prove the following two elementary propositions.

***Proposition** Let a, b be integers, not both zero, and let $d = \gcd(a, b)$. Then $\frac{a}{d}$ and $\frac{b}{d}$ are integers, and $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

***Proposition** If $n|ab$ and $\gcd(n, a) = 1$ then $n|b$.

We wish to investigate some problems to do with expressing integers as sums of two squares. For example, it is well known that $3^2 + 4^2 = 5^2$. Is it possible to find the general solution of the Diophantine equation $x^2 + y^2 = z^2$? More generally, given any integer a, can we solve the Diophantine equation $x^2 + y^2 = a$?

It turns out to be very useful to use complex numbers when discussing these problems. The basic reason for this is that, using complex numbers, we can write $x^2 + y^2$ as $(x + iy)(x - iy)$. This enables us to view the problem of solving $x^2 + y^2 = a$ as being concerned with factorization of a. Although the original problem appeared to have nothing to do with complex numbers, and although its final solution can be stated without mentioning complex numbers, nevertheless the easiest way to get to the solution is via complex numbers.

We define $\mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \}$, a subset of $\mathbb{C}$, the field of all complex numbers. As is well known, elements of $\mathbb{C}$ can be represented as points in the plane, the point with Cartesian coordinates (x, y) corresponding to the complex number $x + iy$. (This is called the *Argand diagram*, or complex plane.) The set $\mathbb{Z}[i]$ consists of the points with integer coordinates (forming a square lattice in the complex plane); it is called the *ring of Gaussian integers*. People who have not done the Rings and Fields course need not be concerned about the word "ring" here: all that it means is that the sum of two Gaussian integers is a Gaussian integer, and the product of two Gaussian integers is a Gaussian integer.

Gaussian integers are very much the complex analogue of ordinary integers, and we shall see that $\mathbb{Z}[i]$ has many properties that are similar to properties of $\mathbb{Z}$. Most importantly, we shall see that the Euclidean Algorithm (suitably modified) works in $\mathbb{Z}[i]$, and from this it follows that a unique factorization theorem holds in $\mathbb{Z}[i]$.

If $\alpha = a + bi \in \mathbb{C}$, where a is the real part of α and b the imaginary part, we define $N(\alpha) = a^2 + b^2$. This is called the *norm* of α. It is the same as the square of the modulus of α.

We shall prove that if $x, y \in \mathbb{Z}[i]$ with $y \neq 0$, then there exist $q, r \in \mathbb{Z}[i]$ with $x = qy + r$, and $N(r) \leq \frac{1}{2}N(y)$. Here is an example of how to do this. Suppose that $x = 7 - 5i$ and $y = 2 + 3i$. The aim is to divide y into x and get a quotient q which is a whole (complex) number and a remainder r that is, in some sense, small compared to y. So we do the obvious thing: we work out x/y as a complex number, finding the real and imaginary parts, and then find an element of $\mathbb{Z}[i]$ whose real and imaginary parts are as close to those of x/y as we can make them.

$$\frac{7-5i}{2+3i} = \frac{(7-5i)(2-3i)}{(2+3i)(2-3i)} = \frac{(14-15)+(-10-21)i}{13} = -\frac{1}{13} - \frac{31}{13}i.$$

the closest integer to $-1/13$ is zero, and the closest integer to $-31/13$ is -2. So we define $q = 0 - 2i$. The remainder r is

$$x - qy = (7-5i) - (-2i)(2+3i) = (7-5i) - (6-4i) = 1 - i.$$

We can check that $N(r) \leq \frac{1}{2}N(y)$. Indeed, $N(r) = 1^2 + (-1)^2 = 2$, and $N(y) = 2^2 + 3^2 = 13$.

Lecture 6

The following result is revision of first year mathematics.

***Proposition** Let $\alpha, \beta \in \mathbb{C}$. Then $N(\alpha\beta) = N(\alpha)N(\beta)$.

We wish to investigate factorization in $\mathbb{Z}[i]$. First, we define a *unit* of $\mathbb{Z}[i]$ to be an element $\alpha \in \mathbb{Z}[i]$ such that $1/\alpha \in \mathbb{Z}[i]$. It is fairly easy to see—and it is a question in Tutorial 4—that $\mathbb{Z}[i]$ has just four units: 1, -1, i and $-i$. These are exactly the Gaussian integers with norm 1. Two Gaussian integers are said to be

associates of each other if you can get from to the other by multiplying by a unit. The associates of α are thus α itself, $-\alpha$, $i\alpha$ and $-i\alpha$.
We define a Gaussian integer α to be *reducible* if it can be expressed as a product, $\alpha = \beta\gamma$, where β, $\gamma \in \mathbb{Z}[i]$ and neither β nor γ is a unit. A Gaussian integer that is not reducible and not a unit is said to be *irreducible*. The irreducible elements of $\mathbb{Z}[i]$ are the complex analogue of prime numbers.

***Proposition** Suppose that $\alpha \in \mathbb{Z}[i]$ has the property that $N(\alpha)$ is a prime integer. Then α is irreducible.

This is quite easy to prove: a factorization $\alpha = \beta\gamma$ in $\mathbb{Z}[i]$ would lead to a factorization $N(\alpha) = N(\beta)N(\gamma)$ in $\mathbb{Z}$, contrary to the fact that $N(\alpha)$ is prime.

Example: $N(4+i) = 4^2 + 1^1 = 17$ is prime; so $4+i$ is irreducible.

Although the integer 17 cannot be factorized as a product of two integers, apart from the trivial factorizations $17 = 1 \times 17$ and $17 = (-1) \times (-17)$, it can be factorized nontrivially in $\mathbb{Z}[i]$ as $(4+i)(4-i)$. (These two factors areboth irreducible, by the proposition above.) By contrast, the integer 3, which also has no nontrivial factorization in $\mathbb{Z}$, cannot be factorized nontrivially in $\mathbb{Z}[i]$. (This is another question in Tutorial 4.) The prime integer 2, like 17, can be factorized in $\mathbb{Z}[i]$: indeed, $2 = (1+i)(1-i)$. The prime 11, like 3, cannot. The following theorem, which we shall prove in due course, says exactly what is happening.

Theorem (a) Let $p \in \mathbb{Z}$ be a prime such that $p \equiv 3 \pmod 4$. Then p is irreducible as an element of $\mathbb{Z}[i]$.
(b) Let $p \in \mathbb{Z}$ be a prime such that $p \not\equiv 3 \pmod 4$, so that either $p = 2$ or $p \equiv 1 \pmod 4$. Then there exist integers x and y such that $p = x^2 + y^2$, and in $\mathbb{Z}[i]$ we have the factorization $p = (x+yi)(x-yi)$, both factors being irreducible.
(c) If $\alpha \in \mathbb{Z}[i]$ is irreducible then so are its associates ($-\alpha$, $i\alpha$ and $-i\alpha$). Furthermore, α is either of the form p, $-p$, ip or $-ip$ for some prime integer p that is congruent to 3 modulo 4, or else $p = x + yi$ for some integers x and y such that $x^2 + y^2$ is prime.

For example, the prime number 113 is congruent to 1 modulo 4; so it must be the sum of two squares. Indeed, it is $49 + 64$. Correspondingly there are eight irreducible Gaussian integers, $\pm 7 \pm 8i$ and $\pm 8 \pm 7i$ (which fall into two sets of 4 associates). The prime number 107 is congruent to 3 modulo 4; so 107, -107, $107i$ and $-107i$ are irreducible Gaussian integers.

***Proposition** Let x, $y \in \mathbb{Z}[i]$ with $y \neq 0$. There exist q, $r \in \mathbb{Z}[i]$ with $x = qy + r$ and $N(r) \leq \frac{1}{2}N(y)$.

To prove this, note first that given any real number θ there exists at least one integer n with $|\theta - n| \leq \frac{1}{2}$. So, writing $\frac{x}{y}$ as $\theta_1 + \theta_2 i$, we can define $q = n_1 + n_2 i$, where n_1 and n_2 are chosen such that $|\theta_1 - n_1|$ and $|\theta_2 - n_2|$ are both at most $\frac{1}{2}$. Then $N(\frac{x}{y} - q) \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$, and it follows easily that $r = x - qy = (\frac{x}{y} - q)y$ satisfies $N(r) \leq \frac{1}{2}N(y)$.