Lektion 4

Theorem 4.1 *Let x, y, z be positive integers such that $SGD(x, y, z) = 1$. Then the following two statements are equivalent :*

(i) x is even and $x^2 + y^2 = z^2$,
(ii) there exist positive integers $a < b$ such that $SGD(a, b) = 1$ and

$$x = 2ab, \quad y = b^2 - a^2, \quad z = b^2 + a^2.$$

PROOF : Left as an exercise.

A triple of relatively prime integers satisfying the equivalent conditions of Theorem 4.1 is called a *primitive Pythagorean triple.*

Theorem 4.2 *Let x, y, z be integers such that $x^4 + y^4 = z^4$. Then $xyz = 0$.*

PROOF : We consider more generally the equation

$$x^4 + y^4 = z^2 \tag{1}$$

and show that it has no integer solutions such that $xyz \neq 0$. The proof is by contradiction and makes use of Fermat's technique of *infinite descent.* More precisely, the idea is as follows : we suppose there exists a solution (x, y, z) of (1) for which $xyz \neq 0$. Then there must be a solution for which, in addition, $\mathrm{SGD}(x, y, z) = 1$. Given any such 'primitive' solution, we then show how one may construct a new one (X, Y, Z) such that $|Z| < |z|$. But since there must be, among all primitive solutions, one in which $|z|$ is minimised, we thereby obtain the desired contradiction.

So let (x, y, z) be a primitive solution to (1). Then (x^2, y^2, z) is a primitive Pythagorean triple so, by Theorem 4.1, if we assume WLOG that x is even and y odd, then there exist relatively prime integers a, b such that

$$x^2 = 2ab, \tag{2}$$
$$y^2 = b^2 - a^2, \tag{3}$$
$$z = b^2 + a^2. \tag{4}$$

We can rewrite (3) as

$$y^2 + a^2 = b^2,$$

and so (y, a, b) is also a primitive Pythagorean triple. Since y is odd, so must a be even, and there exist relatively prime integers p, q such that

$$a = 2pq, \tag{5}$$
$$y = q^2 - p^2, \tag{6}$$
$$b = q^2 + p^2. \tag{7}$$

Substituting (5) and (7) into (2) yields

$$x^2 = 4pq(p^2 + q^2). \tag{8}$$

Now p and q are relatively prime, hence one sees easily that both are relatively prime to $p^2 + q^2$. Thus, the three numbers p, q and $p^2 + q^2$ are pairwise relatively prime. Since their product is, by (8), a perfect square, it follows from the Fundamental Theorem of Arithmetic that each is a perfect square. In other words, there exist pairwise relatively prime integers X, Y, Z such that

$$p = X^2, \quad q = Y^2, \quad p^2 + q^2 = Z^2.$$

Substituting the first two of these relations into the third yields the relation

$$X^4 + Y^4 = Z^2,$$

so we have constructed the desired new primitive solution to (1). It remains to check that $|Z| < |z|$. But, using (7) and (4), we have

$$Z^2 = p^2 + q^2 = b < b^2 + a^2 = z \leq z^2,$$

as required.

Lecture 5

Theorem 5.1 *The only integers x, y such that*

$$y^2 + 2 = x^3 \tag{9}$$

are $x = 3, y = \pm 5$.

'PROOF' : Write (9) as

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3. \tag{10}$$

We shall first verify that, for any integer y, the numbers $y + \sqrt{-2}$ and $y - \sqrt{-2}$ have no common factor in

$$\mathbf{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbf{Z}\}.$$

For suppose $z := a + b\sqrt{-2}$ is a common factor. Then z divides

$$(y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2},$$

and, taking squares of absolute values (as complex numbers), we conclude that

$$a^2 + 2b^2 \mid 8,$$

as ordinary integers. The only possibilities are thus

(i) $a = \pm 1,\ b = 0.$
(ii) $a = \pm 2,\ b = 0.$
(iii) $a = 0,\ b = \pm 1.$
(iv) $a = 0,\ b = \pm 2.$

In case (i), $z = \pm 1$, and hence not a proper factor. In all other cases, there must exist integers c, d such that

$$y + \sqrt{-2} = (a + b\sqrt{-2})(c + d\sqrt{-2}).$$

From this it follows, by equating the real and imaginary parts, that

$$y = ac - 2bd, \tag{11}$$
$$1 = ad + bc. \tag{12}$$

Now (12) immediately rules out (ii) and (iv), since in both cases the rhs of (12) is even. But from (9) it follows already that y must be odd (otherwise the lhs of (9) will be even, but not divisible by 4), and then (11) also eliminates (iii).

Hence, we have proven that $y \pm \sqrt{-2}$ have no common factor in $\mathbf{Z}[\sqrt{-2}]$.

By (10), this implies that each of them must be a cube in $\mathbf{Z}[\sqrt{-2}]$.

Thus, there exist integers a, b such that

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3. \tag{13}$$

Multiplying out the rhs of (13) and equating the real and imaginary parts yields the two equations

$$y = a^3 - 6ab^2, \tag{14}$$

$$1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2). \tag{15}$$

Immediately, (14) implies that

$$b = 3a^2 - 2b^2 = \pm 1.$$

Since a, b are integers, the only possibility is $b = 1,\ a = \pm 1$. Substituting these possibilities into (13) gives $y = \pm 5$, v.s.v.

OBS !! There is a major gap in the proof, namely the part in italics. What I state there is correct, but it requires a proof. What one would actually like to prove is a generalisation of the Fundamental Theorem of Arithmetic to the ring $\mathbf{Z}[\sqrt{-2}]$. We will return to this issue later in the course. But, for the moment, it is worth remarking that the F.T.A. does not hold in, for example, the ring $\mathbf{Z}[\sqrt{-5}]$.

Lektion 6 (?)

NOTATION : $\mathbf{C}^\times$ denotes the group of non-zero complex numbers under multiplication.

DEFINITION 6.1 : Let G be a finite abelian group. A *character* of G is a group homomorphism

$$\chi : G \to \mathbf{C}^\times.$$

Note that, since G is finite, $\chi(g)$ must be a root of unity for any $g \in G$ and any character χ. Indeed, if $n \cdot g = 0_G$, then $\chi(0) = 1 = \chi(ng) = [\chi(g)]^n$, so $\chi(g)$ is an n:th root of unity.

Given two characters χ_1, χ_2 of a group G, we can define a third character $\chi_1 \cdot \chi_2$, called the 'product' of χ_1 and χ_2, as follows :

$$(\chi_1 \cdot \chi_2)(g) := \chi_1(g) \cdot \chi_2(g), \qquad \forall\, g \in G. \tag{16}$$

It is easy to check that $\chi_1 \cdot \chi_2$ is also a character.

NOTATION : The set of characters of an abelian group G is denoted by $\hat{G}$.

Theorem 6.2 *Let G be a finite abelian group. Under the multiplication of characters defined by (16), $\hat{G}$ becomes a finite abelian group isomorphic to G.*

PROOF : The details were given in class. To show that $\hat{G}$ is a group (that the multiplication is associative, and that an identity element and inverses exist) is easy. That this group is isomorphic to G is the interesting part. The idea for showing this was as follows : Let

$$G = C_1 \oplus C_2 \oplus \cdots \oplus C_k$$

be any decomposition of G as a direct sum of cyclic groups. Let n_i denote the order of C_i and let e_i be any group element which generates C_i. We think of the set $\{e_1, ..., e_k\}$ as a 'basis' for G. Then there is a canonical 'dual basis' $\{\chi_1, ..., \chi_k\}$ for $\hat{G}$ given by

$$\chi_i(e_j) = \begin{cases} e^{2\pi i/n_i}, & \text{if } i = j, \\ 1, & \text{if } i \neq j. \end{cases}$$

NOTATION/TERMINOLOGY : The identity element of the character group $\hat{G}$ is denoted χ_0. It is called the *trivial character* and is the mapping given by

$$\chi_0(g) = 1, \quad \forall\, g \in G.$$

The following proposition will prove useful in our study of Dirichlet L-functions.

Proposition 6.3 *Let G be a finite abelian group, $g^* \in G$ and $\chi^* \in \hat{G}$. Then*

(i)

$$\sum_{\chi \in \hat{G}} \chi(g^*) = \begin{cases} |G|, & \text{if } g^* = 0, \\ 0, & \text{if } g^* \neq 0. \end{cases}$$

(ii)

$$\sum_{g \in G} \chi^*(g) = \begin{cases} |G|, & \text{if } \chi^* = \chi_0, \\ 0, & \text{if } \chi^* \neq \chi_0. \end{cases}$$

PROOF : (i) was done in class, and (ii) left as an exercise. For (i), the argument is as follows : if $g \neq 0$ then there exists at least one character - let's pick one and denote it χ_g - with the property that $\chi_g(g) \neq 1$. This follows from the proof of Theorem 6.2, as outlined above.

Then, since $\hat{G}$ is a group, we have that

$$\sum_{\chi} \chi(g) = \sum_{\chi} (\chi \cdot \chi_g)(g) = \chi_g(g) \cdot \sum_{\chi} \chi(g).$$

Since $\chi_g(g) \neq 1$, it follows that the sum must be zero, v.s.v.

Lecture 10 (?)

I gave a second proof of Gauss' reciprocity law, as an alternative to the one in Baker. A handout from the book [1], containing the proof, was given. The idea was to use Gauss sums. The relevant preparatory information on Gauss sums is contained in my old lecture notes, on pages 38-39 (specifically, Proposition 24).

Reference

[1] N. Koblitz, A course in numebr theory and cryptography, Springer 1987 (GTM Series, No. 114).