Rational Points on Elliptic Curves

Alexandru Gica[1]

April 8, 2006

[1]Notes, LaTeXimplementation and additional comments by Mihai Fulger

Contents

Chapter 1

Lecture I

Definition 1.0.1. *Let $f \in \mathbb{Q}[X,Y]$ be a polynomial of degree 3 i.e. there exist $a,b,c,\ldots,j \in \mathbb{Q}$ such that $f(X,Y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + j$. The associated set $C \subset \mathbb{Q}^2$ defined as the zero set of f is called an affine rational cubic.*

1.1 Projective Geometry

On the subset of the affine space $\mathbb{A}^3_{\mathbb{R}} \setminus \{(0,0,0)\} = \mathbb{R}^3 \setminus \{(0,0,0)\}$, define the relation " $\sim$ " by $(a,b,c) \sim (a',b',c')$ if and only if there exists $t \neq 0$ such that $t \cdot (a,b,c) = (a',b',c')$ i.e. $a' = ta, b' = tb, c' = tc$. It is easy to see that " $\sim$ " is an equivalence relation. Denote the equivalence class in $\mathbb{A}^3_{\mathbb{R}} \setminus \{(0,0,0)\}$ of the element (a,b,c) by $[a:b:c]$.

Definition 1.1.1. *The factor set $\mathbb{P}^2 = \mathbb{A}^3_{\mathbb{R}} \setminus \{(0,0,0)\}/\sim$ is called the 2-dimensional projective plane.*

The same construction can be applied to any field, not necessarily $\mathbb{R}$, therefore we can define the rational or the complex projective plane.

Definition 1.1.2. *Similarly, for any field K, we define*

$$\mathbb{P}^n_K = \mathbb{A}^{n+1}_K \setminus \{(0,0,\ldots,0)\}/\sim$$

and call it the n-th dimensional projective space over K.

Remark 1.1.3. *Let $K \subset L$ be a field extension. Then the canonical map $\mathbb{P}^n_K \to \mathbb{P}^n_L$ sending $[x_0 : \ldots : x_n] \in \mathbb{P}^n_K$ to $[x_0 : \ldots : x_n] \in \mathbb{P}^n_L$ is well defined and injective.*

1.1.1 Equivalent definitions

Remark 1.1.4. *$\mathbb{P}^n_{\mathbb{R}}$ can be regarded as the set of lines passing through the origin of $\mathbb{A}^{n+1}_{\mathbb{R}}$.*

Notice that $\mathbb{P}^0$ is the set of lines $\mathbb{A}^1$. But $\mathbb{A}^1$ is a line, hence $\mathbb{P}^0$ consists of a single point called the point at infinity of $\mathbb{A}^1$.

Remark 1.1.5. *We can regard $\mathbb{P}^{n+1}$ as $\mathbb{A}^{n+1} \sqcup \mathbb{P}^n$.*

To see this algebraically, notice that $\mathbb{P}^{n+1} = \{[x_0 : x_1 : \ldots : x_{n+1}] | x_0 \neq 0\} \sqcup \{[0 : x_1 : \ldots : x_{n+1}] | x_1, \ldots, x_{n+1}$ are not all zero$\}$. Denote $U_0 = \{[x_0 : x_1 : \ldots : x_{n+1}] | x_0 \neq 0\}$. We can construct a map $\varphi : U_0 \to \mathbb{A}^{n+1}$ by $\varphi([x_0 : x_1 : \ldots : x_{n+1}]) = (\frac{x_1}{x_0}, \ldots, \frac{x_{n+1}}{x_0})$, because $x_0 \neq 0$. We can also construct a map $\psi : \mathbb{A}^{n+1} \to U_0$ by $\psi((x_1, x_2, \ldots, x_{n+1})) = [1 : x_1 : x_2 : \ldots : x_{n+1}]$. It is easy to see that φ and ψ are well defined maps inverse to one another. Therefore we can identify U_0 to $\mathbb{A}^{n+1}$ through φ. Denote $V_0 = \mathbb{P}^{n+1} \setminus U_0$. It is easy to check that the correspondence $V_0 \leftrightarrow \mathbb{P}^n : [0 : x_1 : \ldots : x_{n+1}] \leftrightarrow [x_1 : \ldots : x_{n+1}]$ is well defined and bijective.

For $\mathbb{P}^0$ this construction is obviously impossible so we define $\mathbb{P}^0$ by using the previous remark.

We now give geometric meaning to the algebraic view above. We can regard U_0 as the set of directions in $\mathbb{A}^{n+2}$, passing through the origin, that cut the hyperplane $x_0 = 1$. Because a line not included in a hyperplane cuts the hyperplane in at most one point, U_0 identifies to $\mathbb{A}^{n+1}$. V_0 can be regarded as the set of directions in $\mathbb{A}^{n+2}$, passing through the origin, which are parallel to $x_0 = 1$. But this are exactly the lines in the hyperspace $x_0 = 0$ and this hyperspace obviously identifies to $\mathbb{A}^{n+1}$. Therefore V_0 is the set of lines in $\mathbb{A}^{n+1}$ passing through the origin, $\mathbb{P}^n$.

V_0 is called the hyperplane at infinity of $\mathbb{A}^{n+1}$, or the set of points at infinity.

1.1.2 The Geometry of the Projective Plane

Let K be an arbitrary field. In this subsection, denote $\mathbb{A}^n = \mathbb{A}^n_K$ and $\mathbb{P}^n = \mathbb{P}^n_k$.

Definition 1.1.6. *Let $\pi \subset \mathbb{A}^{n+1}$ be a hyperplane passing through the origin of $\mathbb{A}^{n+1}$. The image $[\pi]$ of $\pi \setminus \{(0, \ldots, 0)\}$ in $\mathbb{P}^n$ is called a hyperplane of the projective space.*

If $n = 3$, $[\pi]$ is called a line in the projective plane.

Remark 1.1.7. *If $v, w \in \mathbb{A}^3$ generate a plane π, then $[\pi] = \{[\alpha \cdot v + \beta \cdot w] | \alpha, \beta \in K, (\alpha, \beta) \neq (0, 0)\}$.*

Remark 1.1.8. *Let $F \in K[X_0, \ldots, X_n]$ be a homogeneous polynomial of degree m. Then $F(t \cdot x_0, \ldots, t \cdot x_n) = t^m F(x_0, \ldots, x_n)$ $\forall t \in K, (x_0, \ldots, x_n) \in \mathbb{A}^{n+1}_K$. Let $[a_0 : \ldots : a_n] \in \mathbb{P}^n_K$. Notice that $F(a_0, \ldots, a_n) = 0 \Leftrightarrow F(ta_0, \ldots, ta_n) = 0$ $\forall t \neq 0$.*

Definition 1.1.9. *Under the assumptions of the previous remark, $[a_0 : a_1 : \ldots : a_n] \in \mathbb{P}^n_K$ is called a zero of F, if $F(a_0, \ldots, a_n) = 0$. The remark above proves that the definition is consistent.*

Proposition 1.1.10. *Let H be a subset of $\mathbb{P}^n$. Then H is a hyperplane if and only if H is the zero set of a homogeneous polynomial of degree 1 in $K[X_0, \ldots, X_n]$.*

Proof: If H is a hyperplane, then there exists π a hyperspace of $\mathbb{A}^{n+1}$ such that H is the image of π in $\mathbb{P}^n$. Then π is the zero set of a homogeneous polynomial F of degree 1 in $K[X_0, \ldots, X_n]$. It is easy to see that H is the zero set of F in $\mathbb{P}^n$.

Conversely, if H is the zero set in $\mathbb{P}^n$ of a homogenous polynomial of degree 1 in $K[X_0, \ldots, X_n]$, let π be the hyperspace in $\mathbb{A}^{n+1}$ determined by F. It is easy to see that the image of π in $\mathbb{P}^n$ is H, so H is a hyperplane. ■

Proposition 1.1.11. *Any two lines $l1$ and $l2$ in $\mathbb{P}^2$ intersect.*

Proof: Let π and τ be the two planes in $\mathbb{A}^3$, passing through the origin, that generate $l1$ and $l2$. If $l1 \neq l2$, then $\pi \neq \tau$. We know that any two distinct planes in $\mathbb{A}^3$ that have at least one common point intersect on a line. The image of this line in $\mathbb{P}^2$ is the intersection point of $l1$ and $l2$. ■

1.2 The Group Law of a Cubic

Definition 1.2.1. *A rational cubic is the zero set in $\mathbb{P}^2_{\mathbb{Q}}$ of a homogeneous polynomial of degree 3 in $\mathbb{Q}[X, Y, Z]$.*

Analogously we can define a real or a complex cubic.

Remark 1.2.2. *Let $F \in \mathbb{Q}[X, Y, Z]$ be a homogeneous polynomial of degree 3. Let $\mathbb{Q} \subset K \subset \mathbb{C}$ be a field extension. The coefficients of F are rational, but they are also complex numbers, so it makes sense to consider the complex cubic C defined by F. It also makes sense to consider the cubic $C(K)$ that is the zero set of F in $\mathbb{P}^2_K$.*

If $\mathbb{Q} \subset K \subset L \subset \mathbb{C}$ are field extensions, then the canonical injective map $\mathbb{P}^2_K \hookrightarrow \mathbb{P}^2_L$ allows us to see $C(K)$ as a subset of $C(L)$.

Definition 1.2.3. *Let C be the affine rational cubic determined by $f(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + j$. Denote $f^*(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3$. f^* is called the homogenized polynomial of f. Denote by $\bar{C}$ the rational cubic defined by f^*. In algebraic geometry language, $\bar{C}$ is called the projective closure of C.*

Definition 1.2.4. *Let K be a field and let $F \in K[X, Y, Z]$ be a homogeneous polynomial of degree 3. Let C be the associated cubic. Let $P = [a : b : c]$ be a point on C i.e. $F(a, b, c) = 0$ and $(a, b, c) \in \mathbb{A}^3_K$, not all zero. C is called nonsingular at P if $\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) \neq (0, 0, 0)$.*

If P is a nonsingular point for C, then the line of $\mathbb{P}^2_K$ given by $\frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y + \frac{\partial F}{\partial Z}(P) \cdot Z = 0$ is called the tangent line to C at P and is denoted $T_P C$.

C is called nonsingular or smooth if it is nonsingular at every point.

Exercise 1.2.5. *Let C be the complex cubic defined by the degree 3 homogeneous polynomial F. Then C is smooth if and only if F is irreducible.*

Theorem 1.2.6 (Bezout). *: Let $F_1, F_2 \in \mathbb{C}[X,Y,Z]$ be homogeneous polynomials of degrees m and n respectively. The zero sets of F_1 and F_2 are called projective curves of degrees m and n respectively. If F_1 and F_2 have no common factors ($\mathbb{C}[X,Y,Z]$ is factorial), then C_1 and C_2 are said to have no common component, and then $C_1 \cap C_2$ is a set of mn points counted with multiplicities.*

Corollary 1.2.7. *Two complex cubics with no common component intersect in exactly 9 points counted with multiplicities.*

Theorem 1.2.8 (9 Points Theorem). *Let C_1 and C_2 be two cubics with no common components. Denote the nine points of intersection of C_1 and C_2 by $A_1, A_2, \ldots, A_9$. Assume C is a cubic that contains $A_1, \ldots, A_8$. Then $A_9 \in C$.*

Proof: The last 3 statements are powerful results of Algebraic Geometry, and their proofs or the complete explanation of the multiplicity of intersection of two curves in the projective plane exceed the level of this course.

However, what you can accept is that two projective curves of degrees m and n intersect in at most mn distinct points.

An intuitive proof can be provided for the 9 Points Theorem if the 9 points are all distinct (algebraic geometry translation: the multiplicity of intersection of the two cubics at each point of intersection is 1). A cubic over a field K is given by a degree three homogeneous polynomial. It is obvious that multiplication of the 10 coefficients of the degree 3 polynomial by a nonzero constant does not change the zero set of the polynomial. This gives a bijective correspondence between the set of cubics over K and $\mathbb{P}^9_K$. The condition that a point $[X : Y : Z]$ belongs to a cubic given by $aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0$ is, by considering $a, b, c, d, e, f, g, h, i, j$ as indeterminates, equivalent to that $[a : b : \ldots : j]$ belongs to a certain hyperplane in $\mathbb{P}^9_K$. So the set of cubics passing through the distinct 8 points $A_1, \ldots, A_8$ corresponds to the intersection of 8 hyperplane in $\mathbb{P}^9_K$. This intersection is a line l in $\mathbb{P}^9_K$. This line passes though the two distinct points corresponding to the two cubics C_1 and C_2. C contains the 8 points $A_1, \ldots, A_8$ if and only if the corresponding point of C in $\mathbb{P}^9_K$ belongs to l. It can be proved that this happens if and only if $F = \alpha F_1 + \beta F_2$, where F, F_1, F_2 are the polynomials corresponding to C, C_1 and C_2 respectively, and α, β are in K. $F(A_9) = \alpha F_1(A_9) + \beta F_2(A_9) = 0 \Rightarrow A_9 \in C$. ■

Definition 1.2.9. *Let C be a complex nonsingular cubic. Let $P, Q \in C$. If $P \neq Q$ then by Bezout, the line passing through P and Q cuts C in 3 points with multiplicities. Let $P * Q$ be the third point of intersection of the line PQ with C. It is possible that this point is one of the points P or Q. If $P = Q$, then $T_P C$ cuts the cubic twice in P. By Bezout it must intersect C again in a point $P * P$. It is possible that this point is again P.*

Remark 1.2.10. *" $*$ " is not a group operation on C. To see this, we prove that this operation has no neutral element. Assume $P * O = P \ \forall P \in C$. Then the line PO cuts C twice in P for all $P \in C$. This means that PO is tangent to C at P for all $P \in C$. Let F be the homogeneous polynomial of degree 3 that defines C and let $O = [a : b : c]$. We have $O \in T_P C$ if and only if $\frac{\partial F}{\partial X}(P)a + \frac{\partial F}{\partial Y}(P)b + \frac{\partial F}{\partial Z}(P)c = 0$. Let $G(X, Y, Z) = \frac{\partial F}{\partial X}(X, Y, Z)a + \frac{\partial F}{\partial Y}(X, Y, Z)b + \frac{\partial F}{\partial Z}(X, Y, Z)c = 0$. G is a degree 2 polynomial which defines a conic in P^2. By Bezout we get that $gcd(G, F) \neq 1$ or else the intersection of the zero set of G and C is a finite set which contradicts $O \in T_P C \ \forall P \in C$. But $gcd(G, F) \neq 1$ contradicts the irreducibility of F.*

Definition 1.2.11. *Let C be a complex nonsingular cubic and fix a point $O \in C$. For arbitrary $P, Q \in C$, define $P + Q = O * (P * Q)$.*

Theorem 1.2.12. *In the conditions of the definition above, $(C, +)$ is an abelian group.*

Proof: Commutativity of " $+$ " is implied by the commutativity of " $*$ " which is obvious.

Let $P \in C$. Then $P + O = O * (P * O)$. The line PO cuts C at O, P and $O * P$. This line is obviously the same as the line $O(O * P)$ which intersects C in $O, O * P$ and P. Therefore $O * (O * P) = P$. This proves that O is a neutral element for " $+$ " on C.

Let $Q \in C$, $S = O * O$ and $Q' = Q * S$. Then $Q * Q' = S$ and $Q + Q' = O * S = O$, hence Q' is an inverse for Q.

The most interesting part of the proof is associativity. Let $P, Q, R \in C$. To prove $P + (Q + R) = (P + Q) + R$, it suffices to prove $P * (Q + R) = (P + Q) * R$. Let S be the intersection of the lines $[P, Q + R]$ and $[R, P + Q]$. We have to prove $S \in C$. Define C_1 as the union of the lines $(P, Q, P * Q)$, $(Q * R, O, Q + R)$ and $(P + Q, S, R)$. Let C_2 be the union of the lines $(Q, R, Q * R)$, $(O, P * Q, P + Q)$ and $(P, S, Q + R)$. Then C_1 and C_2 are cubics and their intersection is the set of 9 points $O, P, Q, R, P * Q, Q * R, P + Q, Q + R, S$. The cubic C passes through $O, P, Q, R, P * Q, Q * R, P + Q, Q + R$, thus through S by the 9 point theorem. ∎

Proposition 1.2.13. *If C is a complex nonsingular cubic defined by a polynomial $F \in \mathbb{Q}[X, Y, Z]$ and if C has a rational point O (i.e. $\exists a, b, c \in \mathbb{Q}$ such that $[a : b : c] = O$), then " $+$ " is well defined on $C(\mathbb{Q})$ and $(C(\mathbb{Q}), +)$ is an abelian group.*

Proof: To prove that " + " is well defined it suffices to prove that $P, Q \in C(Q) \Rightarrow P + Q \in C(Q)$. It suffices to prove that $P, Q \in C(Q) \Rightarrow P * Q \in C(Q)$. Basically, this is a consequence of the fact that a degree 3 polynomial in one indeterminate with rational coefficients and 2 rational roots has all its roots rational. ■

1.2.1 The choice of origin

In theorem 1.2.12 we have seen that the choice of a point O on a nonsingular complex cubic defines a group operation " + " on C such that $(C, +)$ is an abelian group.

Let O and O' be points on the nonsingular complex cubic C and let "+" and " $\perp$ " be the abelian group operation they define. Denote $G = (C, +)$ and $G' = (C, \perp)$. For any $P \in C$, denote by $-P$ and by TP the inverse of P in G and G' respectively.

Theorem 1.2.14. *G and G' are isomorphic as abelian groups.*

Proof: Let $P, Q \in C$ be arbitrary points. We prove that $P \perp Q = (P + Q) - O'$. This is equivalent to $O' * (P * Q) = O * (P * Q) - O' \Leftrightarrow O' + O' * (P * Q) = O * (P * Q) \Leftrightarrow O * (O' * (O' * (P * Q))) = O * (P * Q)$, which follows from the easy observation that $X * (X * Y) = Y \ \forall X, Y \in C$.

Let $f : G \to G'$, $f(P) = P + O_1$. We have $f(P + Q) = P + Q + O' = (P + O') + (Q + O') - O' = (P + O') \perp (Q + O') = f(P) \perp f(Q)$, therefore f is a group homomorphism. It is easy to check that $g : G' \to G$ defined by $g(P) = P - O'$ is a homomorphism that is an inverse for f, hence f and g are isomorphisms. ■

1.3 The Weierstrass Normal Form

Let $F(X, Y) = Y^2 - f(X)$ where $f(X) = X^3 + aX^2 + bX + c$ and $a, b, c \in \mathbb{Q}$. Let C be the affine complex cubic determined by F.

Definition 1.3.1. *The affine rational curve $C(\mathbb{Q})$ defined by $F(X, Y) = 0$, is called an elliptic curve.*

Remark 1.3.2. *The projective closure $\bar{C}(\mathbb{Q})$ of $C(\mathbb{Q})$ is given by $F^*(X, Y, Z) = Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3$.*

In 1.1.5 we have defined the hyperplane at infinity of $\mathbb{P}^n_K$ for any field K by working in the first variable X_0. It is clear that nothing changes if we work with any other variable. In particular, when working in $\mathbb{P}^2$, we will be working with points at infinity with respect to the last variable, Z.

The points at infinity of $\bar{C}$ are given by $F^*(X, Y, 0) = 0 \Leftrightarrow X^3 = 0 \Leftrightarrow X = 0$. This means that the only point at infinity of $\bar{C}$ is $O = [0 : 1 : 0]$

because $[0 : Y : 0] = [0 : 1 : 0]\ \forall Y \neq 0$. Notice that O is also a point of $\bar{C}(\mathbb{Q})$.

O is a nonsingular point for $\bar{C}$. This is because $\frac{\partial F^*}{\partial Y}((0,1,0)) = 2 \neq 0$.

We will usually identify $C(\mathbb{Q})$ and its projective closure $\bar{C}(\mathbb{Q})$.

Definition 1.3.3. *Call a point of $P(x,y)$ of C nonsingular if $\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P)\right) \neq (0,0)$. A point that is not nonsingular is called a singular point.*

If $P(x,y)$ is a nonsingular point for C, then the tangent line to C at P, T_PC is the line given by the equation $\frac{\partial F}{\partial X}(P)(X-x) + \frac{\partial F}{\partial Y}(P)(Y-y) = 0$.

Proposition 1.3.4. *C is smooth if and only if all the complex roots of f are distinct.*

Proof: Assume $P(x,y)$ is a singular point for C. Then $\frac{\partial F}{\partial X}(x,y) = -f'(x) = 0$ and $\frac{\partial F}{\partial Y}(x,y) = 2y = 0 \Rightarrow f(x) = y^2 = 0$. These imply $f(x) = f'(x) = 0$, which happens if and only if x is a multiple root of f. ■

1.3.1 Explicit formulas for the group operation on $\bar{C}(\mathbb{Q})$

Assume C is nonsingular i.e. all the complex roots of f are distinct. By 1.2.13 there is a well defined group operation "+" on $\bar{C}(\mathbb{Q})$ with neutral element O, the point at infinity of C, such that $(\bar{C}(\mathbb{Q}), +)$ is an abelian group.

Lets look more deeply into the structure of $\bar{C}$. Let $U = \{[x : y : 1] \in \mathbb{P}^2_{\mathbb{C}}\}$. Let $\varphi : U \to \mathbb{A}^2_{\mathbb{C}}$ be the map defined by $\varphi([x : y : 1]) = (x, y)$. We know that φ is bijective and we can see $\mathbb{P}^2_{\mathbb{C}}$ as the union of $\varphi(U) = \mathbb{A}^2_{\mathbb{C}}$ and a line at infinity which corresponds to a copy of $\mathbb{P}^1_{\mathbb{C}}$. We have seen that $O = [0 : 1 : 0]$ is the only point at infinity of $\bar{C}$. It follows easily from the equations of $\bar{C}$ and C that $\varphi(\overline{C} \cap U) = C$. Let $\psi : \mathbb{A}^2_{\mathbb{C}} \to U$ be the inverse map of φ given by $\psi((x,y)) = [x : y : 1]$. It is not hard to prove that if l is a line in $\mathbb{A}^2_{\mathbb{C}}$, then there exists a unique line $\bar{l} \in \mathbb{P}^2_{\mathbb{C}}$ such that $\psi(l) = \bar{l} \cap U$ (the idea is to homogenize the equation of l with respect to Z). $\bar{l}$ is called the projective closure of l.

The point of all these observations was to prove that if we restrict the geometry of $\mathbb{P}^2_{\mathbb{C}}$ to U, then we find the geometry of the affine plane $\mathbb{A}^2_{\mathbb{C}}$. We use this to find affine formulas for the group operation on $\bar{C}$ for which we have given only a projective definition.

With this in mind, consider C as a subset of $\bar{C}$. We actually have $\bar{C} = C \cup O$ because the only point at infinity of $\bar{C}$ is O. For any line l in the affine plane, $\bar{l} = l \cup l_\infty$, where l_∞ is the only point at infinity of $\bar{l}$. For ergonomic reasons, we agree to say the O is the point at infinity of C and l_∞ is the point at infinity of l.

Proposition 1.3.5. *Let $P(x,y) \in C$. Then $\overline{T_PC} = T_P\bar{C}$.*

Proof: The equation of $\overline{T_PC}$ is obtained by homogenizing the equation of T_PC. T_PC is given by $\frac{\partial F}{\partial X}(x,y)(X-x)+\frac{\partial F}{\partial Y}(x,y)(Y-y)=0 \Leftrightarrow -f'(x)(X-x)+2y(Y-y)=0$. By homogenizing, we find the equation of $\overline{T_PC}$, $-f'(x)(X-xZ)+2y(Y-yZ)=0$ **[1]**. The equation of $T_P\bar{C}$ is $\frac{\partial F^*}{\partial X}(x,y,1)X+\frac{\partial F^*}{\partial Y}(x,y,1)Y+\frac{\partial F^*}{\partial Z}(x,y,1)Z=0 \Leftrightarrow -f'(x)X+2yY+(y^2-ax^2-2bx-3c)Z=0$ **[2]**. [1] and [2] are the same thing if and only if $f'(x)x-2y^2=y^2-ax^2-2bx-3c \Leftrightarrow f'(x)x+ax^2+2bx+3c=3y^2$. Because $P\in C$, $y^2=f(x)$. So [1]=[2] if and only if $(3x^2+2ax+b)x+ax^2+2bx+3c=3y^2=3(x^3+ax^2+bx+c)$. And the last is obviously true. ∎

Definition 1.3.6. *Denote by $x:\mathbb{A}^2_{\mathbb{C}}\to\mathbb{C}$ and by $y:\mathbb{A}^2_{\mathbb{C}}\to\mathbb{C}$ the projections on the x and y coordinates respectively.*

Remark 1.3.7. *The point at infinity of C, $O=[0:1:0]$ is the point at infinity of the line $x=0$.*

Remark 1.3.8. *If $P\in C$, then $O*P$ is obtained by taking the line OP and intersecting it again to C. The line OP and the projective closure of $x=0$ intersect in O, so restricted to the affine, they are parallel. Therefore $O*P$ is obtained by taking the other point of intersection of the parallel through P to $x=0$ and C.*

Notice that the curve C is symmetric with respect to the x axis. If $P(x,y)\in C$, then $x(O*P)=x(P)$ and $y(O*P)=-y(P)$. Let $P'(x,-y)=O*P$ be the symmetric of P with respect to the x-axis. $P+P'=O*(P*P')=O*O$. If $O*O\neq O$, then, because O is the only point at infinity of C, $O*O=X\in C$. Let X' be the symmetric of X with respect to the x-axis. $X'\in C$. But $O=O+O=O*(O*O)=O*X=X'$ contradicts $X'\in C$. Therefore $P+P'=O\Rightarrow P'=-P$.

Let $P(x_1,y_1)$ and $Q(x_2,y_2)$ be points on $C(\mathbb{Q})$. We have seen in 1.2.13 that $P+Q$ is an element of $\overline{C}(\mathbb{Q})$. So either $P+Q=O$, or $P+Q\in C(\mathbb{Q})$. We look, if possible, for formulas for $x(P+Q)$ and $y(P+Q)$.

If $x_1=x_2$ and $P\neq Q$, then P and Q lie on a parallel to $x=0$ and so $P*Q=O\Rightarrow P+Q=O*(P*Q)=O*O=O$.

Assume $x_1\neq x_2$. Then the line PQ is the line of equation $y=\lambda\cdot x+\nu$, where $\lambda=\frac{y_1-y_2}{x_1-x_2}$ and $\nu=y_1-\lambda x_1=y_2-\lambda x_2$. The intersection of PQ and C is described by the equations

$$\begin{cases} (\lambda\cdot x+\nu)^2=x^3+ax^2+bx+c \Leftrightarrow x^3+(a-\lambda^2)x^2+(b-2\lambda\nu)x+(c-\nu^2)=0 \\ y=\lambda\cdot x+\nu \end{cases}.$$

We know that P and Q are solutions of this system. The third solution is $P*Q$. By Viete, $x(P*Q)=\lambda^2-a-x_1-x_2$. Plunging this into the equation of PQ yields $y(P*Q)=\lambda^3-\lambda a-\lambda x_1-\lambda x_2+\nu$. From these we get the formulas:

$$\begin{cases} x(P+Q)=\lambda^2-a-x_1-x_2 \\ y(P+Q)=-\lambda^3+\lambda a+\lambda x_1+\lambda x_2-\nu \end{cases}. \tag{1.3.1}$$

If $P = Q$, then T_PC is given by $-f'(x_1)(x - x_1) + 2y_1(y - y_1) = 0$. If $y_1 = 0$, then, because C is smooth, $f'(x_1) \neq 0$ and T_PC is parallel to $x = 0$, hence $P * P = O \Rightarrow P + P = O$. If $y_1 \neq 0$, then T_PC is the line of equation $y = \lambda \cdot x + \nu$, where $\lambda = \frac{f'(x_1)}{2y_1}$ and $\nu = y_1 - \lambda \cdot x_1$. Just as in the case $x_1 \neq x_2$, we get the formulas:

$$\begin{cases} x(2P) = \lambda^2 - a - 2x_1 \\ y(2P) = -\lambda^3 + \lambda a + 2\lambda x_1 - \nu \end{cases} . \tag{1.3.2}$$

We have seen that the inverse of $P(x, y) \in C$ is $P'(x, -y)$. This also holds in $C(\mathbb{Q})$.

Remark 1.3.9. *These formulas can be used to give complete proofs for Theorem 1.2.12 and Proposition 1.2.13 without any prior knowledge of Algebraic Geometry, but only if the affine cubic has the particular form $y^2 = x^3 + ax^2 + bx + c$ i.e. the cubic is an elliptic curve.*

Example 1.3.10. *Let $C(\mathbb{Q})$ be the affine rational cubic of equation $y^2 = x^3 - 43x + 166$. Prove that $P(3, 8) \in C(\mathbb{Q})$. Compute $P, 2P, 3P, 4P, 8P$. Compare P to $8P$.*

Solution: $P \in C(\mathbb{Q}) \Leftrightarrow 8^2 = 3^3 - 43 \cdot 3 + 166 \Leftrightarrow 64 = 27 - 129 + 166$.

We apply the formula 1.3.2 to find the coordinates of $2P$. We have $\lambda = \frac{f'(3)}{2 \cdot 8} = \frac{3 \cdot 9 - 43}{16} = -1$. $\nu = 8 - \lambda \cdot 3 = 11$. $x(2P) = (-1)^2 - 2 \cdot 3 = -5$. $y(2P) = -(\lambda \cdot x(2P) + \nu) = -(-(-5) + 11) = -16$.

We now compute $4P$. $\lambda = \frac{f'(-5)}{2(-16)} = \frac{3(-5)^2 - 43}{-32} = -1$. $\nu = (-16) - (-1)(-5) = -21$. $x(4P) = (-1)^2 - 2(-5) = 11$. $y(4P) = -((-1) \cdot 11 - 21) = 32$.

For $8P$, we have: $\lambda = \frac{f'(11)}{2 \cdot 32} = \frac{3 \cdot 11^2 - 43}{64} = 5$. $\nu = 32 - 5 \cdot 11 = -23$. $x(8P) = 5^2 - 2 \cdot 11 = 3$. $y(8P) = -(5 \cdot 3 - 23) = 8$.

We notice that $8P = P \Rightarrow 7P = 0 \Rightarrow 3P = -4P$. So $x(3P) = x(-4P) = x(4P) = 11$ and $y(3P) = y(-4P) = -y(4P) = -32$. ■

Exercise 1.3.11. *Let $C(\mathbb{Q})$ be the elliptic curve defined by $y^2 = x^3 + 17$. Prove that $P_1(-2, 3), P_2(-1, 4), P_3(2, 5), P_4(4, 9), P_5(8, 23) \in C(\mathbb{Q})$.*

Find integers m, n such that $P_2 = mP_1 + nP_3$. Write P_4 and P_5 in terms of P_1 and P_3.

Prove that $P_6 = -P_1 + 2P_3$ and $P_7 = 3P_1 - P_3$ have integer coordinates with $y(P_i) > 0$, $i = \overline{6, 7}$.

Find a point on $C(\mathbb{Q})$, different from $(P_i)_{i=\overline{1,7}}$, with integer coordinates.

Example 1.3.12. *Let $C(\mathbb{Q})$ be the affine rational cubic defined by $x^3 + y^3 = \alpha$ with $\alpha \in \mathbb{Z}^*$. Let $C'(\mathbb{Q})$ be the elliptic curve $v^2 = u^3 - 432\alpha^2$. There is a rational bijective application $\varphi : C(\mathbb{Q}) \to C'(\mathbb{Q})$ defined by $\varphi(x, y) = (12\alpha \cdot \frac{1}{x+y}, 36\alpha \cdot \frac{x-y}{x+y})$.*

Proof: Let $v = 36\alpha\frac{x-y}{x+y}$ and $u = 12\alpha\frac{1}{x+y}$. Then solving this system in x, y gives $x = \frac{36\alpha+v}{u}$ and $y = \frac{36\alpha-v}{u}$. $(x,y) \in C(\mathbb{Q}) \Rightarrow \left(\frac{36\alpha+v}{6u}\right)^3 + \left(\frac{36\alpha-v}{6u}\right)^3 = \alpha \Rightarrow v^2 = u^3 - 432\alpha^2$. This proves $\varphi(C(\mathbb{Q})) \subset C'(\mathbb{Q})$. It is easy to check that $\psi : C'(\mathbb{Q}) \to C(\mathbb{Q})$ defined by $\psi(u,v) = \left(\frac{36\alpha+v}{6u}, \frac{36\alpha-v}{6u}\right)$ is an inverse for φ. ■

Remark 1.3.13. *In the conditions of the example above, φ can be extended to a group morphism $\bar{\varphi} : \overline{C}(\mathbb{Q}) \to \overline{C'}(\mathbb{Q})$ by setting $\bar{\varphi}(O) = O'$, where $O([1:-1:0])$ and $O'([0:1:0])$ are the only points at infinity of $\overline{C}(\mathbb{Q})$ and $\overline{C'}(\mathbb{Q})$ respectively. The proof that $\bar{\varphi}$ is a group morphism is of geometric nature. $\bar{\varphi}([x:y:z]) = (12\alpha \cdot \frac{z}{x+y}, 36\alpha \cdot \frac{x-y}{x+y})$ is a projective transformation which sends C to C', O to O and lines to lines.*

Example 1.3.14. *Find the rational solutions of $y^2 + 432 = x^3$.*

Proof: The previous example proves that there is bijective correspondence between the rational solutions of $y^2 = x^3 - 432$ and the rational solutions of $u^3 + v^3 = 1$. This is a well known particular case of Fermat's Last Theorem and thus it has no nontrivial solutions. The trivial solutions are $(u,v) \in \{(1,0),(0,1)\}$. The corresponding solutions of $y^2 = x^3 - 432$ are $\varphi(1,0)$ and $\varphi(0,1)$. $\varphi(1,0) = (12,36)$ and $\varphi(0,1) = (12,-36)$. ■

1.3.2 The existence of a Weierstrass Normal Form

This is mostly an Algebraic Geometry section. The main goal is to prove that any rational cubic that admits a flex point with rational coordinates is projectively equivalent through a rational projective transformation to an elliptic curve. We have not yet defined what a flex point is, but the prototype is the point at infinity $O[0:1:0]$ of an elliptic curve which had the nice property $O * O = O$. A projective transformation is basically a linear change of coordinates in $\mathbb{P}^2$, but beware that when restricted to the affine, it may not look linear at all. A rational projective transformation is just as usual a transformation with rational coefficients.

Let $C \subset \mathbb{P}^2_{\mathbb{C}}$ be a cubic given by the equation $F(X,Y,Z) = 0$ with $F \in \mathbb{C}[X,Y,Z]$ a homogeneous polynomial of degree 3.

Definition 1.3.15. *An application $A : \mathbb{P}^2 \to \mathbb{P}^2$ given by $A([x:y:z]) = [a_{11}x+a_{12}y+a_{13}z : a_{21}x+a_{22}y+a_{23}z : a_{31}x+a_{32}y+a_{33}z]$ with $a_{ij} \in \mathbb{C}\ \forall i,j = \overline{1,3}$ is called a projective transformation of $\mathbb{P}^2$ if $(a_{ij})_{i,j=\overline{1,3}} \in GL_3(\mathbb{C})$.*

Let $M = (a_{ij})_{i,j=\overline{1,3}}$. Then M is a linear automorphism of $\mathbb{A}^3$ which fixes the origin. Therefore M induces a well defined application $\mathbb{P}^2 \to \mathbb{P}^2$ which coincides with A. If we identify a point $P = [x:y:z]$ in $\mathbb{P}^2$ with the column vector ${}^\top(x,y,z)$, then we have $A(P) = [M \cdot P]$. Notice that we need M to be invertible, otherwise $[0:0:0]$ would be in the image of A and $[0:0:0]$ is not an element of $\mathbb{P}^2$.

From now on we identify A with M. A is bijective and its inverse is the projective transformation given by the matrix M^{-1}.

Remark 1.3.16. *The composition of two projective transformations is a projective transformation. A projective transformation is bijective and its inverse is again a projective transformation. The identity of $\mathbb{P}^2$ is a projective transformation and is the identity of a group structure on the set of projective transformations.*

Proposition 1.3.17. *Two matrices M, N in $GL_3(\mathbb{C})$ induce the same projective transformation on $\mathbb{P}^2$ if and only if there exists $z \in \mathbb{C}^*$ such that $M = z \cdot N$.*

Proof: For all $P \in \mathbb{P}^2$ we have $[(zN) \cdot P] = [N \cdot (zP)] = [N \cdot P]$ because $[a : b : c] = [za : zb : zc]$ for all $[a : b : c] \in \mathbb{P}^2$ and $z \in \mathbb{C}^*$. Therefore we have proved that proportional elements of $GL_3(\mathbb{C})$ induce the same projective transformation.

If $M = (m_{ij})_{ij}$ and $N = (n_{ij})_{ij}$ induce the same transformation of $\mathbb{P}^2$, then $[M \cdot P] = [N \cdot P]$ for all $P \in \mathbb{P}^2$. This means that MP and NP are collinear for all $P \in \mathbb{A}^3$. This is equivalent to P and $M^{-1}NP$ are collinear for all P which in turn means that $(l_{ij})_{ij} = L = M^{-1}N$ and $I_3 = (\delta_{ij})_{ij}$ induce the same projective transformation. By successively replacing P by $[1 : 0 : 0]$, $[0 : 1 : 0]$ and $[0 : 0 : 1]$, we find that there exist $z_1, z_2, z_3 \in \mathbb{C}^*$ such that $z_j \cdot \delta_{ij} = l_{ij}\ \forall i, j = \overline{1,3}$ i.e. the columns of I_3 and L are proportional. Therefore L is a diagonal matrix with diagonal entries $(z_j)_{j=\overline{1,3}}$. Now replace P by $[0 : 1 : 1]$, $[1 : 0 : 1]$ and $[1 : 1 : 0]$ successively to find $z_{23}, z_{13}, z_{12} \in \mathbb{C}^*$ such that $l_{ij} + l_{ik} = z_{jk}(\delta_{ij} + \delta_{ik})$ for all $i, j, k = \overline{1,3}$, $j < k$. Substituting we have the system:

$$(z_j - z_{jk})\delta_{ij} + (z_k - z_{jk})\delta_{ik} = 0,\ i, j, k = \overline{1,3},\ j < k.$$

Choosing $i = j$ gives $z_j = z_{jk}$ for $j < k$. Choosing $i = k$ gives $z_k = z_{jk}$ for $j < k$. Therefore $z_j = z_k = z_{jk}$ for all $j < k$. This proves $z_1 = z_2 = z_3 = z^{-1}$ for some $z \in \mathbb{C}^*$. So $M^{-1}N = z^{-1}I_3 \Rightarrow M = zN$. ∎

Definition 1.3.18. *The proposition above allows us to identify the set of projective transformations of $\mathbb{P}^2$ with the group $GL_3(\mathbb{C})/\mathbb{C}^*$, that we will denote by $PGL_2(\mathbb{C})$. The identification is actually a group isomorphism. For the factorization above to make sense, notice that $\mathbb{C}^*$ embeds in $GL_3(\mathbb{C})$ as the central subgroup of matrices of the form $\{zI_3 | z \in \mathbb{C}^*\}$. $PGL_2(\mathbb{C})$ is also called the group of linear automorphisms of $\mathbb{P}^2$.*

Remark 1.3.19. *A projective transformation of $\mathbb{P}^2$ sends lines to lines. This is because a linear automorphism of $\mathbb{A}^3$ sends planes to planes.*

Exercise 1.3.20. *The action of $PGL_2(\mathbb{C})$ on the set $\mathcal{P} = \{(P, Q, R) \in (\mathbb{P}^2)^3 | P, Q, R$ are not colinear$\}$ is transitive. This means that for all (P, Q, R),*

(P', Q', R') in $\mathcal{P}$, there exists $A \in PGL_2(\mathbb{C})$ such that $A(P) = P'$, $A(Q) = Q'$ and $A(R) = R'$.

Proposition 1.3.21. *For every two lines l_1, l_2 in $\mathbb{P}^2$ there exists a projective transformation sending l_1 to l_2.*

Proof: This is a consequence of the previous exercise, but it also has a simpler proof. If $l_1 = l_2$ then the identity of $\mathbb{P}^2$ solves the problem. If $l_1 \neq l_2$, take $P = l_1 \cap l_2$. There is a rotation in $\mathbb{A}^3$ around the line which is the pre-image of P through the canonical projection $\pi : \mathbb{A}^3 \setminus \{(0,0,0)\} \to \mathbb{P}^2$ that sends the plane which is the pre-image of l_1 to the plane corresponding to l_2. This rotation is an element of $GL_2(\mathbb{C})$, hence it determines a projective transformation of $\mathbb{P}^2$ which sends l_1 to l_2. ■

Proposition 1.3.22. *Let l_1 and l_2 be lines in the projective plane and let $P_1 \in l_1$ and $P_2 \in l_2$. There exists a projective transformation sending l_1 to l_2 and P_1 to P_2.*

Proof: By the previous problem there exists a projective transformation sending l_1 to l_2. Using the simple fact that composing two projective transformations we find again a projective transformation, we reduce to the case $l_1 = l_2$. We must find a linear automorphism of $\mathbb{P}^2$ which keeps l_1 fixed and sends P_1 to P_2. Through the canonical projection $\mathbb{A}^3 \setminus \{0\} \to \mathbb{P}^2$ we make this an affine problem which translates to finding a linear automorphism of $\mathbb{A}^3$ which fixes the origin, fixes the plane corresponding to the line l_1 and sends the line corresponding to P_1 into the line corresponding to P_2. It is not hard to find a plane rotation with the properties above and this rotation then determines a solution to the problem. ■

So far we have only treated classical topics of projective geometry. The results above are valid in any field. We will introduce some more algebraic geometry from now on.

Definition 1.3.23. *Let C and C' be two projective curves. We say that C is projectively equivalent to C' if there exists $\phi \in PGL_2(\mathbb{C})$ such that $\phi(C) = C'$.*

Remark 1.3.24. *Let C be a complex cubic, $\phi \in PGL_2(\mathbb{C})$ and let $A \in GL_3(\mathbb{C})$ be a representant for ϕ. Then the homogeneous polynomial $F(X, Y, Z)$ gives the equation of C if and only if the homogeneous polynomial $F \circ A^{-1}(X, Y, Z)$ gives the equation of $\phi(C)$. In particular $\phi(C)$ is a complex curve of the same degree as C.*

I said that the definition of the multiplicity of intersection of two projective curves at a common point exceeds the level of this course, but I will introduce the multiplicity of intersection of a line and a curve.

Definition 1.3.25. *Let C be a curve in $\mathbb{P}^2$ given by the equation $F(X,Y,Z) = 0$ with F a homogenous polynomial of degree d. Let l be a line in $\mathbb{P}^2$ and assume P is a common point for C and l.*

Suppose that l is not a component of C i.e. the linear form defining the equation of l does not divide F. Let $Q \in L$, $Q \neq P$. The multiplicity of intersection of l and C at P is by definition the order of the root 0 in the polynomial $f(\lambda) = F(P + \lambda \cdot Q)$. Denote it by $i(C,l,P)$.

If $l \subset C$ then set $i(C,l,P) = \infty$. Throughout, when working with the intersection multiplicity of a curve and a line at a point, we assume this multiplicity to be finite i.e. l is not a component of C.

Remark 1.3.26. *0 is in fact a root of f in the equation above because $f(0) = F(P) = 0$ because $P \in C$ and C is the zero set of F.*

The order of a root of a polynomial is obviously upper bounded by the degree of the polynomial. In our case, $i(C,l,P) \leq deg(f) = deg(F) = d$. Since 0 is a root of f, we also have $1 \leq i(C,l,P)$.

In this particular case, Bezout's Theorem states that $\sum_{P \in C \cap l} i(C,l,P) = d$.

Let $f(\lambda) = F(P + \lambda \cdot Q) = F(P) + \lambda \cdot R(P,Q) + \lambda^2 \cdot H(P,Q)$ for some $R(P,Q), H(P,Q) \in \mathbb{C}$. Then $R(P,Q) = \frac{df}{d\lambda}(0) = \frac{\partial F}{\partial X}(P+0\cdot Q)x(Q) + \frac{\partial F}{\partial Y}(P + 0 \cdot Q)y(Q) + \frac{\partial F}{\partial Z}(P + 0 \cdot Q)z(Q) \Rightarrow$.

$$R(P,Q) = \frac{\partial F}{\partial X}(P)x(Q) + \frac{\partial F}{\partial Y}(P)y(Q) + \frac{\partial F}{\partial Z}(P)z(Q),$$

where $x(Q), y(Q), z(Q)$ are fixed representatives of Q. Based on this we give the following definition:

Definition 1.3.27. *Let C be a projective curve of degree d and let $P \in C$. Define the tangent space at P to C as the linear subspace T_PC of $\mathbb{P}^2$ given by $\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0$.*

A line l passing through P is called tangent at P if $l \subset T_PC$.

If $i(C,l,P) = 1$, we say that l and C meet transversally at P.

Remark 1.3.28. *T_PC is either a line or the the whole $\mathbb{P}^2$. It is $\mathbb{P}^2$ if and only if all the partial derivates of F at P vanish.*

This remark shows that P is a smooth point of C if and only if T_PC is a line, and in this case the definitions of the tangent space and tangent line agree.

A point Q in $\mathbb{P}^2$ different from P is in T_PC if and only if $i(C,PQ,P) \geq 2$.

Exercise 1.3.29. *Let C be a complex curve of degree d, let $l \subset \mathbb{P}^2$ be a line and let $P \in C \cap l$. Prove that $i(C,l,P) = i(\phi(C), \phi(l), \phi(P))$. In particular prove that if $Q \in C$, then $T_{\phi(Q)}(\phi(C)) = \phi(T_QC)$.*

We now introduce the notion of a flex point.

Definition 1.3.30. *Let P be a smooth point on a complex curve C of degree d. P is called a flex point for C if and only if $i(C, T_P C, P) > 2$.*

Remark 1.3.31. *If P is a flex point on a complex cubic C, then it is easy to see that $T_P C$ cuts C in P 3 times (multiplicity 3) and cuts C in no other point. Notice that this implies $P * P = P$.*

Remark 1.3.32. *Let $C(Q)$ be an elliptic curve given in homogeneous coordinates by $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$. By definition, an elliptic curve is smooth. Hence the point $O[0:1:0]$ is smooth. C is given by $F(X,Y,Z) = Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3$. $T_O C$ is given by $Z = 0$. Let $Q = [1:0:0]$. To compute $i(C, T_O C, O)$ we have to compute $f(\lambda) = F((0,1,0) + \lambda \cdot (1,0,0)) = F((\lambda, 1, 0) = -\lambda^3$. The order of the root 0 is 3, hence O is a flex point for C.*

Remark 1.3.33. *It can be proved that a smooth complex curve of degree $d \geq 3$ admits at least a flex point.*

Actually it can be proved that the flex points of the smooth curve C given by $F(X,Y,Z) = 0$ are the intersection points of C and the Hessian of C. By definition, the Hessian $H(C)$ is the complex curve given by $H(F) = \det \begin{pmatrix} \frac{\partial F}{\partial X \partial X} & \frac{\partial F}{\partial X \partial Y} & \frac{\partial F}{\partial X \partial Z} \\ \frac{\partial F}{\partial Y \partial X} & \frac{\partial F}{\partial Y \partial Y} & \frac{\partial F}{\partial Y \partial Z} \\ \frac{\partial F}{\partial Z \partial X} & \frac{\partial F}{\partial Z \partial Y} & \frac{\partial F}{\partial Z \partial Z} \end{pmatrix} = 0$. $H(F)$ is a homogeneous polynomial of degree $3(d-2)$. By Bezout it follows that C and $H(C)$ either have a common component which must be C or meet in $3d(d-2)$ points.

The following theorem is the starting point in proving the existence of a normal Weierstrass form for a special class of cubics:

Theorem 1.3.34. *Let C be a projective curve (not necessarily smooth) and assume that it has a flex point P. Then C is projectively equivalent to a cubic of equation $Y^2Z - F(X,Z) = 0$, where F is a homogeneous polynomial of degree 3.*

Proof: By proposition 1.3.22 there exists a projective transformation sending P to $O[0:1:0]$ and $T_P C$ to the line $Z = 0$. 1.3.24 says that the image of C through this projective transformation is again a cubic. Therefore we can assume $P = O$ and $T_P C = \{Z = 0\}$. Suppose that the equation of C is $a_0X^3 + X^2(a_1Y + a_2Z) + X(a_3Y^2 + a_4YZ + a_5Z^2) + (a_6Y^3 + a_7Y^2Z + a_8YZ^2 + a_9Z^3)$. $[0:1:0] \in C$ implies $a_6 = 0$. Since O is assumed to be a flex point for C, we must have $C \cap \{Z = 0\} = \{[0:1:0]\}$. This says that the equation $a_0X^3 + a_1X^2Y + a_3XY^2 = 0$ gives only the solution $[0:1:0]$ i.e. it has only solutions of the form $(0, y, 0)$ over the complex numbers. This happens only if $a_1 = a_3 = 0$ and $a_0 \neq 0$. Computing the partials at $(0,1,0)$ of the polynomial giving the equation of C we find $(\frac{\partial}{\partial X}, \frac{\partial}{\partial Y}, \frac{\partial}{\partial Z}) = (0, 0, a_7)$. By definition of a flex point, O is smooth therefore

not all the partials at $(0,1,0)$ vanish and $a_7 \neq 0$. Multiplying the coefficients of the homogeneous equation defining C by a nonzero constant does not change its solutions therefore we can assume $a_7 = 1$. The equation of C is now: $Y^2Z + a_4XYZ + a_8YZ^2 + (a_0X^3 + a_2X^2Z + a_5XZ^2 + a_9Z^3)$. It has the form

$$Y^Z + sXYZ + tYZ^2 + A(X,Z) = Z(Y^2 + sXY + tYZ) + A(X,Z),$$

for some homogeneous polynomial A of degree 3 in X, Z. We have $Y^2 + sXY + tYZ = Y(Y + sX + tZ) = (Y + \frac{s}{2}X + \frac{t}{2}Z)^2 - (\frac{s}{2}X + \frac{t}{2}Z)^2$. For $Y' = Y + \frac{s}{2}X + \frac{t}{2}Z$, we get the equation for C: $ZY'^2 - Z(\frac{s}{2}X + \frac{t}{2}Z)^2 + A(X,Z) = 0$ which is of the form $Y'^2Z - F(X,Z)$ with F a homogeneous polynomial of degree 3 in X, Z. Since the application $[X : Y : Z] \to [X : Y' : Z]$ induces a projective transformation, we are done. ∎

Remark 1.3.35. *If C in theorem 1.3.34 is a rational cubic i.e. given by an equation with rational coefficients, and P is a flex point with rational coordinates, then all the projective transformations used in the proof of the theorem are rational.*

Theorem 1.3.36. *If C is a nonsingular complex cubic, then C is projectively equivalent to a curve of equation $Y^Z = X^3 + aXZ^2 + bZ^3$ with $4a^3 + 27b^2 \neq 0$.*

Proof: By 1.3.33, a smooth complex cubic always has a flex point. By theorem 1.3.34, C is projectively equivalent to a curve of equation $Y^2Z = \bar{a}X^3 + \bar{b}X^2Z + \bar{c}XZ^2 + \bar{d}Z^3$. $\bar{a} \neq 0$ or else C contains the line $\{Z = 0\}$ and is no longer smooth. Replacing X, Y by $\bar{a}^{-1} \cdot X$, $\bar{a}^{-1} \cdot Y$ is a projective transformation and the equation of the image C' of C through this transformation is $Y^2Z = X^3 + \bar{b}X^2Z + \bar{a}\bar{c}XZ^2 + \bar{a}^2\bar{d}Z^3 = X^3 + b'X^Z + c'XZ^2 + d'Z^3$. The projective transformation defined by $X \to \frac{X-3Z}{3}$ sends C' to the curve C" of equation $Y^2Z = \frac{(X-b'Z)^3}{27} + b'\frac{(X-b'Z)^2Z}{9} + c'\frac{(X-b'Z)Z^2}{3} + d'Z^3$. The coefficient of X^2Z is $-\frac{b'}{9} + b'\frac{1}{9} = 0$. Therefore the equation of C" is of the form $Y^2Z = X^3 + aXZ^2 + bZ^3$ and C is projectively equivalent to C" through the composure of the projective transformations above. The condition $4a^3 + 27b^2 \neq 0$ is, as we will see in the next course, the condition that the discriminant of $f(X) = X^3 + aX + b$ is nonzero. We will also see that this is equivalent to the condition that f has distinct roots hence to that C is nonsingular. ∎

Definition 1.3.37. *If C is a smooth complex cubic given by the equation $Y^2Z = X^3 + aXZ^2 + bZ^3$, then we say that C is in Weierstrass normal form. Theorem 1.3.36 above states that any smooth complex cubic is projectively equivalent to a curve in Weierstrass normal form.*

Theorem 1.3.38 (Weierstrass Normal Form). *Let C be a smooth rational complex cubic. Suppose that C admits a flex point P with rational coordinates. Then C is projectively equivalent to an elliptic curve. Moreover we can assume that the equation of this elliptic curve is $Y^2Z = X^3+aXZ^2+bZ^3$ with $a, b \in \mathbb{Z}$ and $4a^3 + 27b^2 \neq 0$.*

Proof: If C is rational and P has rational coordinates, then all the projective transformations that appear in the proof of theorem 1.3.36 are rational. Therefore C is projectively equivalent to a complex curve of equation $Y^2Z = X^3 + a'XZ^2 + b'Z^3$ with $a', b' \in \mathbb{Q}$ and $4a'^3 + 27b'^2 \neq 0$. There exist $A, B, C \in \mathbb{Z}$, $C \neq 0$ such that $a' = \frac{A}{C}$ and $b' = \frac{B}{C}$. $[X : Y : Z] \to [C^2X : C^3Y : Z]$ defines a projective transformation that sends the complex curve to the curve of equation $Y^2Z = X^3 + AC^3XZ^2 + BC^5Z^3$. Set $a = AC^3$ and $b = BC^5$. Then $4a^3+27b^2 = C^9(4A^3+27B^2C) = C^{12}(4a'^3+27b'^2) \neq 0$.■

Determining whether a rational cubic has a flex point or not is a completely wild problem. No method effective or not is known, so the condition that C has a rational flex point is quite restrictive.

We will sometimes say that a smooth rational cubic is in Weierstrass normal form if it is determined by an equation of the form $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$ with $a, b, c \in \mathbb{Z}$.

Chapter 2

Nagell-Lutz's Theorem

2.1 Discriminants and Resultants

The main goal of this algebraic digression is to present some properties of the discriminant of a polynomial. We will mainly use it to prove that a polynomial with coefficients in an arbitrary field k has a multiple root in an algebraic closure of k if and only if the discriminant of the polynomial is 0. We will also find some formulas for the discriminant of a polynomial.

Let A be an integral domain, let k be its field of fractions and let Ω be an algebraic closure for k. Let $f \in A[X]$ be a monic polynomial. If k was $\mathbb{R}$ or $\mathbb{C}$ then we had the notion of a derivate for f and in both cases we had the formula $f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$ if $f(X)$ was $a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$.

Definition 2.1.1. *If $f \in A[X]$, $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ then define the formal derivate of f by $f'(X) = na_nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + a_1$.*

The following properties of the formal derivate are easy exercises:

1. $(f+g)' = f' + g'$ for all $f, g \in k[X]$.
2. $(a \cdot f)' = a \cdot f'$ for all $f \in k[X]$ and $a \in k$.
3. $(fg)' = f' \cdot g + f \cdot g'$ for all $f, g \in k[X]$.
4. If k is a field of characteristic 0, then $f' = 0 \Leftrightarrow f$ is a constant polynomial. If k is of characteristic p, then $f' = 0 \Leftrightarrow \exists g \in k[X]$ such that $f(X) = g(X^p)$.

Definition 2.1.2. *Let $f, g \in A[X]$, $f(X) = a_nX^n + \ldots + a_0$ and $g(X) = b_mX^m + \ldots + b_0$. The resultant of f and g, is defined as the determinant of*

the $(n+m)\times(n+m)$ *matrix:*

$$Res(f,g)=\det\begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & \dots \\ 0 & a_n & \dots & a_1 & a_0 & 0 \\ 0 & 0 & a_n & \dots & a_1 & a_0 \\ & & & \ddots & & \\ b_m & b_{m-1} & \dots & b_0 & 0 & \dots \\ 0 & b_m & \dots & b_1 & b_0 & 0 \\ 0 & 0 & b_m & \dots & b_1 & b_0 \\ & & & \ddots & & \end{pmatrix}.$$

The first m *rows are obtained by permuting circularly the* $1\times(n+m)$ *vector* $(a_n,\dots,a_n,0,\dots,0)$ *and the last* n *rows are obtained by permuting circularly the* $1\times(n+m)$ *vector* $(b_m,\dots,b_0,0,\dots,0)$.

Definition 2.1.3. *By definition, the discriminant of a polynomial is*

$$\Delta_f=(-1)^{n(n-1)/2}\cdot\frac{1}{a_n}\cdot Res(f,f').$$

The bare definition of the resultant of two polynomials may look a bit scary, but we will see how it appears naturally in trying to solve the following problem: Given two polynomials with coefficients in A, when can we say that they have a common factor? Simple ring theory proves that it is enough to consider the problem in k, the quotient field of A. The following proposition proves that the resultant of these polynomials plays a decisive role in solving this problem. The proof of the proposition sheds some light on how the definition of the resultant first came to life.

Proposition 2.1.4. *If* $f,g\in A[X]$*, then* f *and* g *have a nonconstant common divisor if and only if* $Res(f,g)=0$.

Proof: It is enough to consider the problem in k, the quotient field of A. Let $deg(f)=n$ and $deg(g)=m$. First notice that f and g have a nonconstant common factor if and only if there exists a nonzero polynomial $h\in k[X]$ such that $f|h$, $g|h$ and $deg(h)\leq m+n-1$. If f,g have a common factor d, then $f=d\cdot f'$ and $g=d\cdot g'$ for some polynomials $f',g'\in k[X]$. For $h=df'g'$, we have $f|h$, $g|h$ and $deg(h)=deg(d)+deg(f')+deg(g')=n+m-deg(d)\leq n+m-1$. Conversely let $h=f\cdot f'$ and $h=g\cdot g'$. If f and g have no common factor then $f|h=gg'\Rightarrow f|g'$ which is impossible because $deg(g')=deg(h)-deg(g)\leq n+m-1-m=n-1$. Therefore f and g have a common factor.

Let V_f be the $k-$vector space of polynomials of degree least of equal to $n+m-1$ divisible by f. It is easy to see that a basis for V_f is given by $\{f,Xf,X^2f,\dots,X^{m-1}f\}$. Similarly define V_g. It has the basis $\{g,Xg,X^2g,\dots,X^{n-1}g\}$. f and g have a nonconstant common factor if

and only if there exists a nonzero polynomial of degree least or equal to $m+n-1$ divisible both by f and g. This is equivalent to $V_f \cap V_g \neq 0$ i.e V_f and V_g are not in direct sum in the vector space V of polynomials of degree least or equal to $n+m-1$. A basis for V is given by $\{1, X, X^2, \ldots, X^{n+m-1}\}$. Now V_f and V_g are not in direct sum if and only if $\{X^{m-1}f, \ldots, Xf, f, X^{n-1}g, X^{n-2}g, \ldots, Xg, g\}$ are linearly dependent over k in V. By writing these elements of V in the basis $\{X^{n+m-1}, \ldots, X, 1\}$, the condition that they are linearly dependent is equivalent to that the determinant of the resulting matrix of coefficients is zero. The matrix of coefficients is the same as the matrix of $Res(f,g)$. ■

Corollary 2.1.5. *If $f \in A[X]$, then f has a multiple root in Ω if and only if $\Delta_f = 0$.*

Proof: f has a multiple root in Ω if and only if f and f' have a non-constant common factor in $k[X]$. ■

We now give some formulas for the resultant and for the discriminant of a polynomial.

Proposition 2.1.6. *If $f, g \in A[X]$, $f(X) = a_n(X-\alpha_1)\ldots(X-\alpha_n)$ and $g(X) = b_m(X-\beta_1)\ldots(X-\beta_m)$ with $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in \Omega$, then $Res(f,g) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (\alpha_i - \beta_j)$.*

Proof: Consider $F, G \in A[X_1, \ldots, X_n, Y_1, \ldots, Y_m][X]$ defined by

$$F(X_1, \ldots, X_n, Y_1, \ldots, Y_m)(X) = a_n(X-X_1)\ldots(X-X_n),$$

$$G(X_1, \ldots, X_n, Y_1, \ldots, Y_m)(X) = b_m(X-Y_1)\ldots(X-Y_m).$$

Clearly $f = F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ and $g = G(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ in $\Omega[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$.

$\tilde{A} = A[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ is an integral domain, so $Res(F,G)$ is a well defined element of $\tilde{A}$ and it is clear from the definitions that

$$Res(F,G)(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = Res(f,g).$$

Hence it suffices to prove $Res(F,G) = a_n^m b_m^n \prod_{i=1}^n \prod_{j=1}^m (X_i - Y_j)$. The formalism of a complete proof is tedious, but the idea is simple. For all $i = \overline{1,n}$, $j = \overline{1,m}$ we prove that $X_i - Y_j | Res(F,G)$. Let $\tilde{A}_j$ be the polynomial ring obtained from $\tilde{A}$ by removing the variable Y_j. Let F_{ij}, G_{ij} and $R(F,G)_{ij}$ be the polynomials in $\tilde{A}_j[X]$ obtained from F, G and $R(F,G)$ respectively by replacing Y_j with X_i. We have $X_i - Y_j | Res(F,G) \Leftrightarrow Res(F,G)_{ij} = 0$. But clearly in $\tilde{A}_j$, $Res(F,G)_{ij} = Res(F_{ij}, G_{ij})$ and the last is 0 because F_{ij} and G_{ij} have an obvious common factor, namely $X - X_i$. These can be formalized rigourously to prove $\prod_{i=1}^n \prod_{j=1}^m (X_i - Y_j) | Res(F,G)$.

Let $V = \prod_{i=1}^{n}\prod_{j=1}^{m}(X_i - Y_j) \in \tilde{A}$. By expanding F and G we see that the variable X_i appears in the matrix of $Res(F,G)$ only on the first n lines and on these lines it appears in degree 1, hence the degree of $Res(F,G)$ in X_i is n for all $i = \overline{1,n}$. Similarly we prove that the degree of $Res(F,G)$ in each Y_j is m. From these we conclude that $Res(F,G) = \tau \cdot V$ with $\tau \in A$.

Notice that $\tau = Res(F,G)(1,\dots,1,0\dots,0) = Res(a_n(X-1)^n, b_m X^m)$. Computing $Res(a_n(X-1)^n, b_m X^m) = a_n^m b_m^n$ is a good exercise. ∎

Corollary 2.1.7. *$Res(f,g) = a_n^m \cdot \prod_{i=1}^{n} g(\alpha_i) = (-1)^{n+m} b_m^n \cdot \prod_{j=1}^{m} f(\beta_j)$.*

Proposition 2.1.8. *If $f \in A[X]$, $f(X) = a_n(X-\alpha_1)\dots(X-\alpha_n)$ and $\alpha_i \in \Omega$ $\forall i = \overline{1,n}$, then*

$$\Delta_f = a_n^{2n-2}\left(\prod_{1\le i<j\le n}(\alpha_i - \alpha_j)\right)^2.$$

Proof: Use $f'(\alpha_i) = \prod_{j\neq i}(\alpha_i - \alpha_j)$. ∎

These formulas are often useful for computations and could have just as well been used to define both the resultant and the discriminant. However they are not quite useful in proving more theoretical results. For example don't make clear why $Res(f,g)$ and Δ_f are not just elements of Ω but also of A.

The following is a very important property of the resultant of two polynomials.

Theorem 2.1.9. *If $f, g \in A[X]$, then $R(f,g) \in (f,g)$ i.e. $R(f,g)$ is in the ideal generated by f and g i.e. there exist polynomials $u, v \in A[X]$ such that $uf + vg = Res(f,g)$.*

Proof: Consider $R(f,g)$ as the determinant of a matrix with entries in $A[X]$. For all $i = \overline{1, n+m-1}$, add the column i in $Res(f,g)$ multiplied by X^{n+m-i} to the last column, $m+n$. The only difference between the matrix of $Res(f,g)$ and the new matrix, M, is the last column, which is ${}^{\top}(fX^{m-1}, \dots, fX, f, gX^{n-1}, \dots, gX, g)$. The determinant of M is $Res(f,g)$. Expanding $\det M$ by the last column gives $Res(f,g) \in (f,g)$. ∎

The following remark will be used intensively throughout the course.

Remark 2.1.10. *Let $f(X) = X^3 + aX^2 + bX + c$ be a polynomial with coefficients in an arbitrary field k. We have:*

$$\Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

2.2 Torsion points on elliptic curves, The Nagell-Lutz Theorem

Let $C(Q)$ be the elliptic curve given by $y^2 = x^3+ax^2+bx+c$. Assume that C is nonsingular. This is equivalent to saying that $f(X) = X^3 + aX^2 + bX + c$ has 3 distinct complex roots. Notice using 2.1.5 that the condition for C to be smooth is equivalent to $\Delta_f \neq 0$, where $\Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

Let's see that up to a rational change of coordinates we can assume that a, b, c are integers. There exist $a', b', c', d \in \mathbb{Z}$, $d \neq 0$ such that $a = \frac{a'}{d}$, $b = \frac{b'}{d}$ and $c = \frac{c'}{d}$. Then $y^2 = x^3 + ax^2 + bx + c \Leftrightarrow (d^3y)^2 = (d^2x)^3 + a'd(d^2x)^2 + b'd^3(d^2x) + c'd^5$. Therefore up to the change of coordinates $(x, y) \to (x/d^2, y/d^3)$ we can assume that a, b, c are integers.

To make writing easier, identify $C(\mathbb{Q})$ with $\overline{C}(\mathbb{Q})$. Recall that $\overline{C}(\mathbb{Q})$ has an abelian group structure with neutral element the only point at infinity of C, $O[0 : 1 : 0]$.

Definition 2.2.1. *A point P on $C(\mathbb{Q})$ is called a torsion point if it is a torsion element of the group $C(\mathbb{Q})$ i.e. there exists an integer $n \neq 0$ such that $nP = O$. The set of torsion points on $C(\mathbb{Q})$ forms an abelian subgroup of $C(\mathbb{Q})$ that we will denote $\mathcal{M}$. For $P \in \mathcal{M}$, denote by $o(P)$ the least positive integer n such that $nP = O$. $o(P)$ is called the order of P.*

The main goal of this section is to prove the Nagell-Lutz Theorem. It will provide us an effective method for determining the torsion points of $C(\mathbb{Q})$ by imposing strong necessary conditions on them.

Theorem 2.2.2 (Nagell-Lutz). *Let $P(x, y)$ be a torsion point on $C(\mathbb{Q})$. We assume $P \neq O$. Then $x, y \in \mathbb{Z}$. Moreover $y = 0$ or $y|\Delta_f$.*

Towards the proof of Nagell-Lutz's Theorem we make the following remark:

Remark 2.2.3. *There exist $g, h \in \mathbb{Z}[X]$ such that $gf + hf' = \Delta_f$. This follows from 2.1.9 but if you have a strong computational disposition you can check that the formulas*

$$\begin{cases} g(X) = (18b - 6a^2)X - (4a^3 - 15ab + 27c) \\ h(X) = (2a^2 - 6b)X^2 + (2a^3 - 7ab + 9c)X + (a^2b + 3ac - 4b^2) \end{cases}$$

provide a solution for the problem.

Proof of 2.2.2: We begin our investigation of $\mathcal{M} \setminus O$ with the points of order 2. We have $2P = O \Leftrightarrow P(x, y) = (-P)(x, -y) \Leftrightarrow y = -y \Leftrightarrow y(P) = 0$. If $y = 0$ then $y^2 = x^3 + ax^2 + bx + c \Rightarrow x^3 + ax^2 + bx + c = 0 \Rightarrow x \in \mathbb{Z}$. An elementary proof for this is to notice that a rational root a/b with $gcd(a, b) =$

1 of a polynomial $a_nX^n + \ldots + a_0$ with integer coefficients satisfies $b|a_n$ and $a|a_0$. A quick algebraic proof is just knowing that $\mathbb{Z}$ is integrally closed. We have proved $o(P) = 2 \Rightarrow y = 0, x \in \mathbb{Z}$.

Assume now that $y(P) \neq 0$ i.e. $P \neq -P$. Consider the following change of coordinates $(t, s) = (\frac{x}{y}, \frac{1}{y}) \Leftrightarrow (x, y) = (\frac{t}{s}, \frac{1}{s})$. $y^2 = x^3 + ax^2 + bx + c \Rightarrow \frac{1}{s^2} = \frac{t^3}{s^3} + a\frac{t^2}{s^2} + b\frac{t}{s} + c \Rightarrow s = t^3 + at^2s + bts^2 + cs^3$.

Let C' be the cubic defined by $s = t^3 + at^2s + bts^2 + cs^3$ and let $O' = (0, 0)$. In the following short escapade to algebraic geometry I prove that $C(\mathbb{Q})$ and $C'(\mathbb{Q})$ are isomorphic as groups and find explicit formulas for an isomorphism φ between them. I prefer the geometric argument to a mechanical verification that would lead to the same result.

Let $\bar{\varphi} : \mathbb{P}^2 \to \mathbb{P}^2$ be defined by $\bar{\varphi}([x : y : z]) = [x : z : y]$. It is obvious that $\bar{\varphi}$ is a linear automorphism of $\mathbb{P}^2$. $\bar{\varphi}$ restricts to a bijection $\varphi : \overline{C} \to \overline{C'}$. This is easily seen by considering the equations of the projective closures $\overline{C} : y^2z = x^3 + ax^2z + bxz^2 + cz^3$ and $\overline{C'} : su^2 = t^3 + at^2s + bts2 + cs^3$. We have $\varphi(O) = \varphi([0 : 1 : 0]) = \bar{\varphi}([0 : 1 : 0]) = [0 : 0 : 1] = (0, 0) = O'$ and $\varphi(P(x, y)) = \varphi([x : y : 1]) = \bar{\varphi}([x : y : 1]) = [x : 1 : y] = (\frac{x}{y}, \frac{1}{y})$ if $y \neq 0$. Similarly $\varphi(P(x, 0)) = [x : 0 : 1]$. Because $\bar{\varphi}$ and $\bar{\varphi}^{-1}$ are linear rational automorphisms, their restrictions to $C(\mathbb{Q})$ and $C'(\mathbb{Q})$ induce bijections that we will also denote $\varphi : C(\mathbb{Q}) \leftrightarrow C'(\mathbb{Q}) : \varphi^{-1}$. The simple fact that φ and φ^{-1} are restrictions of rational linear transformations is enough to give a convincing proof that they are group homomorphisms. Because they are inverse to each other, they are actually group isomorphisms. Notice that C' is symmetric with respect to the point $(0, 0)$. Let $P'(x, y) \in C'(\mathbb{Q})$. Let Q be the point of coordinates $(-x, -y)$. I want to prove that $P' + Q = O'$ in $C'(\mathbb{Q})$. Because Q is the symmetric of P' with respect to O', we have $P * Q = O'$ (recall that for arbitrary points X, Y of a smooth cubic curve, $X * Y$ was defined as the third point of intersection of the line XY with C if $X \neq Y$ and as the third point of intersection of T_XC and C, by imagining that T_XC already cuts C in X twice). To prove $P' + Q = O'$, it is enough to prove $O' * O' = O'$. Let $O' * O' = R$. This implies $R * O' = O'$. On the other hand, $R * O'$ is the symmetric of R with respect to O', hence $R = O'$. We have proved that $-P' = Q$.

Back from the escapade. We had $P(x, y)$ a torsion point on $C(\mathbb{Q})$ with $y \neq 0$ and $o(P) > 2$. We first want to prove that x and y have to be integers. The idea is to write $y = \frac{A}{B}$ with $gcd(A, B) = 1$, $B \geq 1$ and then prove that for all prime numbers p, we have $p \not| B$. This would prove that $B = 1$, hence $y \in \mathbb{Z}$. Because x would be a rational number, root of the polynomial with integer coefficients $X^3 + aX^2 + bX + (c - y^2)$, x would have to be an integer. The hard part is proving that B has no prime divisors.

Definition 2.2.4. *Let p be a prime number and let $x = \frac{m}{n}$ be a rational number. If $m \neq 0$ then there exist $a, b \in \mathbb{N}$ such that $p^a|m$, $p^{a+1} \not| m$ and $p^b|n$, $p^{b+1} \not| n$. Define $v_p(x) = a - b$. Set $v_p(0) = \infty$. If $v_p(x) = 0$, then we*

say that x is prime to p. Some of the most important properties of v_p are:

1. *$v_p : \mathbb{Q}^* \to \mathbb{Z}$ is a well defined group homomorphism, called the p-adic valuation on $\mathbb{Q}$.*

2. *$v_p(n) \geq 0$ for any integer $n \in \mathbb{Z}$. Even more, $v_p(x) \geq 0$ for every prime number p if and only if $x \in \mathbb{Z}$ or $x = \infty$.*

3. *$v_p(x+y) \geq v_p(x)$ if $v_p(x) = v_p(y)$.*

4. *$v_p(x+y) = min\{v_p(x), v_p(y)\}$ if $v_p(x) \neq v_p(y)$.*

Assume there exists a prime number p dividing B. Then there exist $m, n \in \mathbb{Z}$ with $gcd(m,n) = 1$, $p \nmid mn$ and there exists an integer $r \geq 1$ such that $y = \frac{m}{np^r}$. Also there exist integers u, v, t such that $x = p^{-t} \cdot \frac{u}{v}$ with $gcd(u,v) = 1$ and $p \nmid uv$. From the equation we get

$$\frac{m^2}{n^2 p^{2r}} = \frac{u^3}{v^3} \cdot \frac{1}{p^{3t}} + a\frac{u^2}{v^2}\frac{1}{p^{2t}} + b\frac{u}{v}\frac{1}{p^t} + c.$$

If $t \leq 0$, then $\frac{m^2}{n^2p^{2r}} = \frac{u^3}{v^3}p^{-3t} + a\frac{u^2}{v^2}p^{-2t} + b\frac{u}{v}p^{-t} + c$, and it is easy to see that this implies $p|v$ which is a contradiction.

Therefore $t \geq 1$ and then

$$\frac{m^2}{n^2p^{2r}} = \frac{1}{v^3p^{3t}}(u^3 + au^2p^tv + bup^{2t}v^2 + cv^3p^{3t}).$$

Since $p \nmid u \cdot v$, we easily get $p \nmid u^3 + au^2p^tv + bup^{2t}v^2 + cv^3p^{3t}$. From this it follows $v_p(y^2) = v_p(\frac{m^2}{n^2p^{2r}}) = -2r = v_p(\frac{1}{v^3p^{3t}}(u^3 + au^2p^tv + bup^{2t}v^2 + cv^3p^{3t})) = v_p(\frac{1}{v^3p^{3t}}) = -3t$, hence $2r = 3t$ which implies that $r = 3\mu$ and $t = 2\mu$ for some positive integer μ.

Notice that we have not used that P is a torsion point. We only have used $r \geq 1$. We have proved that if $P(x,y) \in C(\mathbb{Q})$, p is a prime number such that $v_p(y) < 0$, then $v_p(y) = -3\sigma$ and $v_p(x) = -2\sigma$ for some $\sigma \in \mathbb{N}$. This proves immediately that there exist $m, n, e, d \in \mathbb{Z}$, $e, d \neq 0$, $gcd(m,e) = gcd(n, ed) = gcd(e,d) = 1$ such that $y = \frac{m}{e^3}$, $x = \frac{n}{e^2d}$. Do not confuse m, n with the ones used earlier. Let $z = \frac{n}{d}$. Multiplying $y^2 = f(x)$ by e^6 yields $z^3 + (ae^2)z^2 + (be^4)z + (ce^6 - m^2) = 0$. Therefore z is an integer being a rational that verifies a polynomial equation with integer coefficients and dominant coefficient 1. Since $gcd(n,d) = 1$, we can assume $d = 1$. Don't forget this argument because it will be used later:

Proposition 2.2.5. *Let $C(\mathbb{Q})$ be the smooth rational elliptic curve given by $y^2 = f(x)$ with f monic in $\mathbb{Z}[X]$. Then for all $(x,y) \in C(\mathbb{Q})$, there exist $m, n, e \in \mathbb{Z}$, $e > 0$, $gcd(m,e) = gcd(n,e) = 1$ such that $y = \frac{m}{e^3}$ and $x = \frac{n}{e^2}$.*

For arbitrary positive integers μ, denote

$$C(p^\mu) = \{P(x,y) \in C(\mathbb{Q}) | v_p(x) \leq -2\mu,\ v_p(y) \leq -3\mu\} \cup \{O\}.$$

We want to prove that $C(p^\mu)$ is a subgroup of $C(\mathbb{Q})$. It happens that it is easier to prove that $C'(p^\mu) = \{P(t,s) \in C'(\mathbb{Q}) | v_p(t) \geq \mu,\ v_p(s) \geq 3\mu\} \cup \{O'\} = \varphi(C(p^\mu))$ is a subgroup of $C'(\mathbb{Q})$.

First I will prove that $C'(p^\mu) = \varphi(C(p^\mu))$. Let $P(x,y) \in C(\mu)$. By what we have seen, we have $v_p(x) = -2(\mu+i)$ and $v_p(y) = -3(\mu+i)$ for some $i \geq 0$ ($C(p^\mu)$ contains no elements with $y = 0$ because $v_p(y) \leq -3\mu < \infty$). Then $\varphi(P) = (\frac{x}{y}, \frac{1}{y}) = (t,s)$ and $v_p(t) = v_p(x) - v_p(y) = \mu + i$, $v_p(t) = -v_p(y) = 3(\mu+i)$. Since $\varphi(O) = O'$ we have proved that $\varphi(C(p^\mu)) \subseteq C'(p^\mu)$. By using the machinery above with C and C' interchanged, we prove $\varphi^{-1}(C'(p^\mu)) \subseteq C(p^\mu)$. So $C'(p^\mu) = \varphi(C(p^\mu))$.

We now prove that $G = C'(p^\mu)$ is a subgroup of $C'(\mathbb{Q})$. Let $P(t,s) \in G$. Then $(-P)(-t,-s) \in G$ so G is stable under taking inverses. Let $P_1(t_1,s_1), P_2(t_2,s_2)$ be two points on $C'(p^\mu)$ and let $s = \alpha \cdot t + \beta$ be the equation of the line P_1P_2. Assume $t_1 \neq t_2$. Then the slope of P_1P_2 is $\alpha = \frac{s_2-s_1}{t_2-t_1}$ and $\beta = s_1 - \alpha \cdot t_1$. We have $s_i = t_i^3 + at_i^2 s_i + bt_i s_i^2 + cs_i^3$ for $i = \overline{1,2}$. By subtracting the two we get $s_2 - s_1 = (t_2^3 - t_1^3) + as_2(t_2^2 - t_1^2) + a(s_2 - s_1)t_1^2 + bt_2(s_2^2 - s_1^2) + bs_1^2(t_2 - t_1) + c(s_2^3 - s_1^3)$. This is the same as $(s_2 - s_1)(1 - at_1^2 - bt_2(s_1 + s_2) - c(s_2^2 + s_1s_2 + s_1^2)) = (t_2 - t_1)(t_2^2 + t_1t_2 + t_1^2 + as_2(t_2 + t_1) + bs_1^2)$.[**1**] Therefore

$$\alpha = \frac{t_2^2 + t_1t_2 + t_1^2 + as_2(t_2 + t_1) + bs_1^2}{1 - at_1^2 - bt_2(s_1 + s_2) - c(s_2^2 + s_1s_2 + s_1^2)}.$$

Since $v_p(t_i) \geq \mu$ and $v_p(s_i) \geq 3\mu$ for $i = \overline{1,2}$ we easily get that the denominator of α is prime to p, hence $v_p(\alpha) = v_p(t_2^2+t_1t_2+t_1^2+as_2(t_2+t_1)+bs_1^2) \geq 2\mu$.

Remark 2.2.6. *If $t_1 = t_2 = t$, then $s_1 = s_2 = s$ hence $P_1 = P_2$ and the same formula for α, the slope of the tangent at P_1 to C', holds (just replace t_i and s_i by t and s respectively).*

We first prove $t_1 = t_2 \Rightarrow s_1 = s_2$. From [1] we have $(s_2 - s_1)(1 - at_1^2 - bt_2(s_1+s_2) - c(s_2^2+s_1s_2+s_1^2)) = 0$. We have seen that $v_p(1-at_1^2-bt_2(s_1+s_2)-c(s_2^2+s_1s_2+s_1^2)) = 0$ and this implies $1-at_1^2-bt_2(s_1+s_2)-c(s_2^2+s_1s_2+s_1^2) \neq 0$ because $v_p(0) = \infty$. Therefore $s_1 = s_2$. To find α, "differentiate" $s = t^3 + at^2s + bts^2 + cs^3$ with respect to t. We get

$$\frac{ds}{dt} = 3t^2 + 2ats + at^2\frac{ds}{dt} + bs^2 + 2bts\frac{ds}{dt} + 3cs^2\frac{ds}{dt} \Rightarrow$$

$$\alpha = \frac{ds}{dt} = \frac{3t^2 + 2ats + bs^2}{1 - at^2 - 2bts - 3cs^2}.$$

Just as in the case $t_1 \neq t_2$, $v_p(\alpha) \geq 2\mu$.

$\beta = s_1 - \alpha \cdot t_1 \Rightarrow v_p(\beta) \geq \min\{v_p(s_1), v_p(\alpha \cdot t_1)\} \geq 3\mu$.
The intersection of P_1P_2 and C' is given by

$$\begin{cases} s = t^3 + at^2s + bts^2 + cs^3 \\ s = \alpha \cdot t + \beta \end{cases} \Rightarrow \alpha \cdot t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3.$$

Let $(P_1 * P_2)(t_3, s_3)$ be the third point of intersection of P_1P_2 and C'. Then we must have $t_1 + t_2 + t_3 = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}$. Notice that $v_p(\alpha) \geq 2\mu \Rightarrow v_p(1 + a\alpha + b\alpha^2 + c\alpha^3) = 0 \Rightarrow 1 + a\alpha + b\alpha^2 + c\alpha^3 \neq 0$.

We have $v_p(t_1 + t_2 + t_3) = v_p(\alpha\beta) + v_p(1 + 2b + 3c\alpha) \geq 5\mu + v_p(1 + 2b + 3c\alpha) \geq 5\mu$. Because b, c are integers and $v_p(\alpha) \geq 2\mu$, $v_p(1 + 2b + 3c\alpha) \geq \min\{1, v_p(2b), v_p(3c) + v_p(\alpha)\} \geq \min\{1, 0, 0 + 2\mu\} = 0$. We have $P_1 + P_2 = -P_1 * P_2$, so $v_p(t_1 + t_2 + t_3) \geq 5\mu \Rightarrow v_p(t_1 + t_2 - t(P_1 + P_2)) \geq 5\mu$. Assume $v_p(t(P_1 + P_2)) < \mu$. Then since $v_p(t_1 + t_2) \geq \mu$ we get $v_p(t_1 + t_2 - t(P_1 + P_2)) = v_p(t(P_1 + P_2)) < \mu$ which contradicts $v_p(t_1 + t_2 - t(P_1 + P_2)) = v_p(t(P_1 + P_2)) \geq 5\mu$. Hence $v_p(t(P_1 + P_2)) \geq \mu$. Notice that $p^{5\mu} | t_1 + t_2 - t(P_1 + P_2)$ (we will use this later). $s(P_1 + P_2) = \alpha t(P_1 + P_2) + \beta \Rightarrow v_p(s(P_1 + P_2)) = v_p(\alpha t(P_1 + P_2) + \beta) \geq \min\{v_p(\alpha t(P_1 + P_2)), v_p(\beta)\} \geq 3\mu$. This proves that $C'(p^\mu)$ is a subgroup of $C'(\mathbb{Q})$. From this it follows easily that $C(p^\mu)$ is a subgroup of $C(\mathbb{Q})$. φ maps $C(p^\mu)$ isomorphically onto $C'(p^\mu)$.

I prove that the only torsion point of $C(p)$ is O. It suffices to prove the statement for $C'(P)$ (with O replaced by O'). Assume there exists $P(t, s) \in C'(p)$ such that $o(P) = m > 0$. Let $v_p(t) = \mu \geq 1$. Then $v_p(s) = 3\mu$ (this follows from $C'(p) = \varphi(C(p))$ and from $2v_p(x) = 3v_p(y)$ for every $(x, y) \in C(p)$).

Assume $p \not| m$. We have proved $p^{5\mu} | t_1 + t_2 - t(P_1 + P_2)$. Using this, a simple induction proves that $t(nP) \equiv nt(P) (mod\ p^{5\mu})$ for every every positive integer n. We have $mP = O' = (0, 0) \Rightarrow t(mP) = 0 \Rightarrow p^{5\mu} | mt(P) \Rightarrow p^{5\mu} | t(P)$. This contradicts $\mu = v_p(t(P))$.

Assume $p | m$. The abelian group generated by P is isomorphic to $\mathbb{Z}/m\mathbb{Z}$ hence there exists an element Q of order p in this subgroup, for example $\frac{m}{p}P$. Replacing P by Q we reduce to $m = p$. Just as before we have $p^{5\mu} | t(pQ) - pt(Q)$. Since $v_p(p \cdot t(Q)) = \mu + 1$ we easily get $v_p(t(pQ)) = \mu + 1$. But $pQ = O' \Rightarrow t(pQ) = 0 \Rightarrow v_p(t(pQ)) = \infty$ and we again have a contradiction.

In conclusion $C(p)$ and $C'(p)$ each have exactly one torsion point. Hence if $P(x, y) \in \mathcal{M}$ and $y \neq 0$, then $v_p(y) \geq 0$ for every prime number p. But this implies that y is an integer and then we know how to prove that x is an integer.

Let $P(x, y)$ be a torsion point, $P \neq O$. Then $2P$ is also a torsion point, hence $y(2P)$ and $x(2P)$ are integers. $x(2P) = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x \Rightarrow 4y^2 | f'(x)^2 \Rightarrow 2y | f'(x)$. But also $y^2 = f(x) \Rightarrow y | f(x)$. By remark 2.2.3, there exist polynomials $g, h \in \mathbb{Z}[X]$ such that $\Delta_f = gf + hf' \Rightarrow \Delta_f =$

$g(x)f(x)+h(x)f'(x)\vdots y \Rightarrow y|\Delta_f$.This completes the proof of the Nagell-Lutz Theorem. ■

Theorem 2.2.7 (Nagell-Lutz (strong version)). *In the conditions of the Nagell-Lutz Theorem, $y = 0$ or $y^2|\Delta_f$.*

Proof: Let $P(x, y)$ be a torsion point with $o(P) > 2$. We have proved that $x(P)$, $y(P)$ and $x(2P) = \frac{f'(x)^2}{4y^2} - a - 2x = \frac{f'(x)^2 - 4\cdot f(x)\cdot(a+2x)}{4f(x)}$ are integers. Let $\phi(x) = f'(x)^2 - 4(a - 2x)f(x)$. Now $x(2P) \in \mathbb{Z}$ implies $4f|\phi$. To prove the strong version of Nagell-Lutz's Theorem, we use a stronger version of Remark 2.2.3, but unfortunately we do not prove it.

Remark 2.2.8. *In the context above, there exist $g, h \in \mathbb{Z}[X]$ such that $g\phi + hf = \Delta_f$.*

We have $y^2 = f(x) \Rightarrow y^2|f(x)$. Also $y^2 = f|4f\ |\phi$. Therefore $y^2|g(x)\phi(x)+h(x)f(x) = \Delta_f \Rightarrow y^2|\Delta_f$. ■

In connection to the problem of studying the torsion points of $C(\mathbb{Q})$ we have the following result due to Mazur:

Theorem 2.2.9 (Mazur). *Let $C : y^2 = x^3 + ax^2 + bx + c$ be a nonsingular cubic with $a, b, c \in \mathbb{Q}$. Let m be the number of torsion points of $C(\mathbb{Q})$. Then $m \in \{1, 2, 3 \ldots 10, 12\}$. Notice that 11 is not a possible value for m.*

Example 2.2.10 (Euler). *Let $C(\mathbb{Q}) : y^2 = x^3 + 1$. Find the torsion points $\mathcal{M}$ of $C(\mathbb{Q})$.*

Solution: We obviously have the torsion point $O = [0 : 1 : 0]$. Let $P(x, y)$ be a torsion point different from O. Then, by the Nagell-Lutz Theorem (strong version), we have $x, y \in \mathbb{Z}$ and $y = 0$ of $y^2|\Delta_f$, where $f(x) = x^3 + 1$ and $\Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = -27$ for $(a, b, c) = (0, 0, 1)$. If $y = 0$, we get the solutions $(x, y) = (-1, 0)$. If $y \neq 0$, then $y^2| - 27 \Rightarrow y|3$. This gives the solutions $(x, y) = (0, \pm 1)$ and $(x, y) = (2, \pm 3)$. It is easy to compute $2P = -P$, where $P = (0, 1)$. Also we have a point of order 2, namely $(-1, 0)$. From this we easily get $\mathcal{M} \simeq \mathbb{Z}/6\mathbb{Z}$. ■.

Exercise 2.2.11. *For an arbitrary prime number p, find the torsion points of $C(\mathbb{Q}) : y^2 = x^3 + px$.*

Exercise 2.2.12. *Find the torsion points of $C(\mathbb{Q}) : y^2 + 7xy = x^3 + 16x$.*

Chapter 3

Lecture III

3.1 Torsion points on rational elliptic curves and elliptic curves mod p

Let $C(\mathbb{Q})$ be the elliptic curve given by $y^2 = x^3+ax^2+bx+c$. Let p be a prime number such that $p \not| 2\Delta_f$, where $\Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

It makes sense to consider the curve over $\mathbb{Z}_p$ (the prime field of characteristic p), $C(\mathbb{Z}_p) : y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c} = \bar{f}(x)$, where $\bar{a}, \bar{b}, \bar{c}$ are the residue classes of a, b and c modulo p respectively.

Proposition 3.1.1. *Let Ω_p be an algebraic closure for $\mathbb{Z}_p$. Then $\bar{f}$ has distinct roots in Ω_p if and only if $p \not| 2\Delta_f$.*

Remark 3.1.2. *Just like working over $\mathbb{C}$ we can define what it means for a curve over Ω_p to be nonsingular.*

Proposition 3.1.3. *In view of the remark above, $C(\Omega_p)$ given by $y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$ is nonsingular.*

Proof: Imitating the complex situation we get that $C(\Omega_p)$ is nonsingular if and only if $0 \neq \overline{\Delta_f} = \Delta_{\bar{f}}$, where $\bar{f}$ is the mod p reduced of f. Since $p \not| \Delta_f$, the conclusion follows. ∎

Proposition 3.1.4. *$\overline{C}(\mathbb{Z}_p)$ has a natural group structure with neutral element $\bar{O} = [\bar{0} : \bar{1} : \bar{0}]$ in $\overline{C}(\mathbb{Z}_p) \subset \mathbb{P}^2_{\mathbb{Z}_p}$. This group structure is induced by the group structure of C.*

Proof: This can be done similarly to 1.2.12 and 1.2.13. Another way to prove it is to reduce mod p the algebraic formulas in 1.3.1 and 1.3.2 for $P + Q$ and $2P$ respectively. If p divides the denominators of the fractions in these equations, just set $P + Q$ or $2P$ as $[\bar{0} : \bar{1} : \bar{0}]$. Notice that because $p \not| 2\Delta_f$, $p \neq 2$, $2P$ is not always the point at infinity of $C(\mathbb{Z}_p)$. ∎

Remark 3.1.5. *In order to ease the notations, we will no longer distinguish an elliptic curve from its projective closure. The immediate effect is that the uncomfortable bar will disappear.*

Theorem 3.1.6. *Let p a prime number as above and let $A = \{(x,y) \in C(\mathbb{Q}) | v_p(x) \geq 0, v_p(y) \geq 0\}$. There is a natural application $A \to \mathbb{Z}_p^2 : (x,y) \to (\bar{x},\bar{y})$. Define $\varphi : C(\mathbb{Q}) \to C(\mathbb{Z}_p)$ by:*

$$\varphi(x,y) = \begin{cases} (\bar{x},\bar{y}), & \text{if } (x,y) \in A \\ \bar{O}, & \text{elsewhere} \end{cases}.$$

Then φ is a group homomorphism and $\varphi|_{\mathcal{M}}$ is injective. Recall that $\mathcal{M}$ is the set of torsion points of $\bar{C}(\mathbb{Q})$.

The application $A \to \mathbb{Z}_p^2 : (x,y) \to (\bar{x},\bar{y})$ is componentwise given by $\mathbb{Q} \ni x = \frac{a}{b} \to \bar{a}\bar{b}^{-1} \in \mathbb{Z}_p$, where a, b are coprime integers, $\bar{a}$ and $\bar{b}$ are the mod p residue classes of a and b respectively and $\bar{b}^{-1}$ is the inverse of $\bar{b}$ in $\mathbb{Z}_p$. This inverse exists because $v_p(x) \geq 0 \Rightarrow p \not| b \Rightarrow \bar{b} \neq 0$.

Example 3.1.7. *Let $C(\mathbb{Q})$ be the elliptic curve given by $y^2 = x^3 + 3$. Find $\mathcal{M}$.*

Proof: $\Delta_f = -3^5 = -243$.

$5 \not| -2 \cdot 3^5$ so $\mathcal{M}$ injects in $C(\mathbb{Z}_5)$. By Lagrange's Theorem, $|\mathcal{M}| \mid |C(\mathbb{Z}_5)|$. Because $3 \not| 5-1$, the function $\mathbb{Z}_5 \to \mathbb{Z}_5 : x \to x^3$ is bijective. This means that over $\mathbb{Z}_5^2$, the equation $y^2 = x^3 + 3$ has 5 solutions (for each $y = \overline{0,4}$, x is uniquely defined). The group $C(\mathbb{Z}_5)$ also contains the point at infinity $\bar{O}$, so $|C(\mathbb{Z}_5)| = 6$.

$7 \not| -2 \cdot 3^5$ so $\mathcal{M}$ also injects in $C(\mathbb{Z}_7)$ and $|\mathcal{M}| \mid |C(\mathbb{Z}_7)|$. The solutions over $\mathbb{Z}_7$ of $y^2 = x^3 + 3$ are

$$(1,2),(1,5),(2,2),(2,5),(3,3),(3,4),(4,2),(4,5),(5,3),(5,4),(6,3),(6,4).$$

Adding the point at infinity $\bar{O}$ we get $|C(\mathbb{Z}_7)| = 13$.

Therefore $|\mathcal{M}||gcd(6,13) = 1 \Rightarrow |\mathcal{M}| = 1$. Since $O \in \mathcal{M}$, we have proven that $M = \{O\}$. ■

Exercise 3.1.8. *Let $(t_n)_{n\geq 1}$ be the sequence of rational numbers defined by $t_1 = t_2 = t_3 = t_4 = t_5 = 1$ and*

$$t_{n+5} = \frac{t_{n+4}t_{n+1} + t_{n+3}t_{n+2}}{t_n}$$

for every $n \geq 1$.

Prove that all the terms of $(t_n)_{n\geq 1}$ are in fact integers.

Theorem 3.1.9 (Gauss). *Let p be a prime number different from 2 and 3 and $C(\mathbb{Z}_p)$ be the cubic defined by $x^3 + y^3 = 1$.*

Then

$$|C(\mathbb{Z}_p)| = \begin{cases} p+1, & \text{if } p \equiv 2(mod 3) \\ p+1+A, & \text{if } p \equiv 1(mod 3) \end{cases},$$

where A is uniquely determined by $4p = A^2 + 27 \cdot B^2$, $A, B \in \mathbb{Z}$ and $A \equiv 1(mod 3)$.

Theorem 3.1.10 (Hasse-Weil). *: Let p be a prime number and let C be a nonsingular irreducible curve of genus g defined over $\mathbb{Z}_p$. Then $|C(\mathbb{Z}_p)| = p + 1 + \varepsilon$ with $|\varepsilon| \leq 2g\sqrt{p}$.*

3.2 Test Paper

[1]

Exercise 3.2.1. *Let $C(\mathbb{Q})$ be the elliptic curve defined by $y^2 = x^3 - 4x$. Determine $\mathcal{M}$ (up to isomorphism).*

Exercise 3.2.2. *Let $C(\mathbb{Q}) : y^2 = x^3 + bx$, with $b \in \mathbb{Z}$ and $p^4 \not| b$ for any prime number p. Determine $\mathcal{M}$.*

***Hint**: For suitable prime numbers p such that $p \equiv 3(mod 4)$, prove that $C(\mathbb{Z}_p) = p + 1$. Use this to prove that $|\mathcal{M}||4$.*

Exercise 3.2.3. *Let $C(\mathbb{Q}) : y^2 = x^3 + c$ with $c \in \mathbb{Z}$ and $p^6 \not| c$ for any prime number p. Determine $\mathcal{M}$.*

***Hint**: Prove first that $|\mathcal{M}||6$.*

The next page contains the solutions to these problems. If you want to try to solve them yourself, **do not turn the page**.

[1] Working time 2 hours. This test only counts as extra for the final grade

3.2.1 Solutions

Solution to 3.2.1 For $y = 0$ we get the solutions $(-2, 0), (0, 0), (2, 0)$ which are all elements of order 2 in $\mathcal{M}$. Together with O, $\mathcal{M}$ contains at least 4 elements.

$\Delta_f = 4^4$. $3 \not| 2 \cdot \Delta_f$. The solutions mod 3 of $y^2 = x^3 - 4x = x^3 - x = 0$ are $(0, 0), (1, 0), (2, 0)$. Together with $\bar{O}$ we find that $\bar{C}(\mathbb{Z}_3)$ has 4 elements. Like we did before, we find $|\mathcal{M}||4$. Since $\mathcal{M}$ has at least 4 elements, $|\mathcal{M}| = 4$.

$\mathcal{M}$ is an 2-torsion abelian group with 4 elements (i.e. $2x = O \ \forall x \in \mathcal{M}$), therefore $M \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. ■

Solution to 3.2.2 $\Delta_f = -4b^3$. Let p be a prime number, $p \equiv 3(mod 4)$ and $p \not| b$. Then $p \not| 2\Delta_f$ and we can apply 3.1.6.

Since the equation $x^2 = -1$ has no solutions in $\mathbb{Z}_p$, using the Legendre symbol, $y^2 = n$ has solutions in $\mathbb{Z}_p$ if and only if $y^2 = -n$ has no solutions mod p.

Notice that $x^3 + bx$ is an odd function. If $x^3 + bx \neq 0$, exactly one of $x^3 + bx$ and $-x^3 - bx$ is a square and gives two solutions of the form $(x, \pm y)$ for $y^2 = x^3 + bx$. If $x = 0$ then we get the only solution $(0, 0)$.

If b is a square mod p, then $x^2 = b$ has two distinct solutions $\pm u$ giving the solutions $(\pm u, 0)$ for $y^2 = x^3 + bx$. We have $p - 3$ solutions for $y^2 = x^3 + bx$ corresponding to the pairs $(x, -x)$ with $x \notin \{-u, 0, u\}$, 2 solutions for $x = \pm u$ and 1 solution for $x = 0$. Hence a total of p solutions.

If b is not a square then we have $p - 1$ solutions for pairs $(x, -x)$ with $x \neq 0$ and 1 solution for $x = 0$. Again a total of p solutions.

Adding $\bar{O}$, $|\overline{C}(\mathbb{Z}_p)| = p + 1$ and by Lagrange, $|\mathcal{M}||p + 1$.

The following is meant to prove that if $d = gcd\{p + 1 | p \text{ is prime}, p \equiv 3(mod 4), p \not| b\}$, then $d = 4$. Let $P = \{p + 1 | p \text{ is prime}, p \equiv 3(mod 4), p \not| b\}$. Assume there exists a prime number dividing d, $q \neq 2$. The Chinese Remainder Theorem guarantees the existence of an integer $n > b$ such that $n \equiv 3(mod 4)$ and $n \equiv 1(mod q)$. By Dirichlet's Theorem concerning primes in arithmetic progressions, there exists a prime number p' in the arithmetic progression of initial term n and ratio $4q$. Since $n > b$, it is obvious that $p' \not| n$. It is easy to see that p' is in the set P. But $q|d$ and $q \not| p' + 1$ because $q \neq 2$ and $p' + 1 \equiv n + 1 (mod\ 4q) \Rightarrow p' + 1 \equiv 1 + 1 \not\equiv 0 (mod q)$. This is a contradiction. Therefore d is a power of 2. $4|p + 1 \ \forall p \in P$, so $4|d$. Assume for a contradiction that $8|d$. Again by Dirichlet, there exists a prime number $q' > b$ with $q \equiv 3(mod 8)$. Then $q' \in P$ and $8 \not| q' + 1$. This again is a contradiction. We have proved that $d = 4$, hence $|\mathcal{M}||4$.

In $\mathcal{M}$ we always have the point $(0, 0)$ of order 2 and the neutral element, the point at infinity O. Thus $\mathcal{M}$ has at least 2 elements.

If $\mathcal{M} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ then $\mathcal{M}$ has 3 elements of order 2. The points on $C(\mathbb{Q})$ of order 2 are the points that have the y coordinate 0. If there are at least three such points then the polynomial $X^3 + bX$ has three distinct roots in

$\mathbb{Q}$. These roots must be integers and we easily get that $-b$ must be a square different from 0. From the condition $p^4 \not| b$ for any prime p, $-b$ must be the square of a square free integer.

If $\mathcal{M}$ is cyclic of order 4, let $P(x,y)$ be a generator of this group. Notice that $y \neq 0$ because otherwise P would be of order 2. This implies $x \neq 0$. Because $\mathbb{Z}_4$ has only one element of order 2, namely $\bar{2}$, the only element of $\mathcal{M}$ of order 2 is $(0,0)$. Therefore $2P = (0,0) \Rightarrow P * P = (0,0)$. We get the equations:

$$\left\{ \begin{array}{c} x(P*P) = \left(\frac{3x^2+b}{2y}\right)^2 - 2x = 0 \\ y(P*P) = \frac{3x^2+b}{2y}x(P*P) + (y - \frac{3x^2+b}{2y}x) = 0 \end{array} \right. \Leftrightarrow$$

$$\left\{ \begin{array}{c} \left(\frac{3x^2+b}{2y}\right)^2 - 2x = 0 \\ y - \frac{3x^2+b}{2y}x = 0 \end{array} \right. \Leftrightarrow$$

$$\left\{ \begin{array}{c} \left(\frac{3x^2+b}{2y}\right)^2 - 2x = 0 \\ 2y^2 = 3x^3 + bx \end{array} \right. .$$

Because $P \in C(\mathbb{Q})$, we have $y^2 = x^3 + bx$. Together with $2y^2 = 3x^3 + bx$ this gives $x^3 = bx$. Since $x \neq 0$, $x^2 = b \Rightarrow y^2 = x^3 + bx = 2bx$.

So we have arrived to solving

$$\left\{ \begin{array}{c} x^2 = b \\ y^2 = 2bx \end{array} \right. \Rightarrow y^2 = 2x^3.$$

From the condition $p^4 \not| b$ for any prime p, x must be a square free integer. It is easy to see that $y^2 = 2x^3 \Rightarrow x = 2u^2, y = 4u^3$ for some $u \in \mathbb{Z}$. Since x must be square free, $u = \pm 1 \Rightarrow b = x^2 = 4$. Hence $\mathcal{M}$ is cyclic of order 4 if and only if $b = 4$. A generator for $\mathcal{M}$ is then $P(2,4)$.

A Sherlock Holmes type argument gives that $\mathcal{M} \simeq \mathbb{Z}_2$ if and only if $-b$ is not a square and $b \neq 4$. These in the conditions of the problem of course.■

Solution to 3.2.3 $\Delta_f = -27c^2$. Let p be a prime number, $p \equiv 2(mod 3)$ and $p \not| c$. Then $p \not| 2\Delta_f$ and we can again apply 3.1.6.

Because $3 \not| p-1$, the application $\mathbb{Z}_p \to \mathbb{Z}_p : x \to x^3$ is bijective, therefore for each $y \in \mathbb{Z}_p$, there exists a unique $x \in \mathbb{Z}_p$ such that $x^3 = y^2 - c$. Together with $\bar{O}$, $|\overline{C}(\mathbb{Z}_p)| = p + 1$.

There is a similar argument to the one in the previous problem which proves that $|\mathcal{M}||6$. The choices for $\mathcal{M}$ are: the trivial group, $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_6$.

The choices for $\mathcal{M}$ prove that it has at most one element of order 2. If this element exists, it is a point on the x-axis. $y = 0 \Rightarrow x^3 = -c$, hence c is a cube. The condition $p^6 \not| c$ for any prime p, proves that c is the cube of a square free integer.

Assume $P(x,y)$ is an element of order 3 in $\mathcal{M}$. Then $y \neq 0$ otherwise P would be of order 2. Then $3P = 0 \Leftrightarrow 2P = -P \Leftrightarrow P * P = P$. This gives the system of equations:

$$\begin{cases} \left(\frac{3x^2}{2y}\right)^2 - 2x = x \\ \frac{3x^2}{2y}\left(\left(\frac{3x^2}{2y}\right)^2 - 2x\right) + \left(y - \frac{3x^2}{2y}x\right) = y \end{cases}.$$

Notice that the second equation is a consequence of the first, hence the system is equivalent to $\left(\frac{3x^2}{2y}\right)^2 - 2x = x \Leftrightarrow x \cdot (3x^3 - 4y^2) = 0$.

If $x = 0$, then $y^2 = c$ and so c is a square.

If $3x^3 = 4y^2$, then $x = 12u^2$ and $y = 36u^3$ for some $u \in \mathbb{Z}$. The condition $c = y^2 - x^3$ implies $u^6 | C \Rightarrow u = \pm 1 \Rightarrow c = -432$.

We are now able to characterize $\mathcal{M}$ in the conditions of the problem:

$$\mathcal{M} \simeq \begin{cases} \mathbb{Z}_6, & \text{if } c = 1 \\ \mathbb{Z}_3, & \text{if } (c \text{ is a square and } c \neq 1) \text{ or } c = -432 \\ \mathbb{Z}_2, & \text{if c is a cube and } c \neq 1 \\ trivial = O, & \text{otherwise} \end{cases}$$

■

Chapter 4

A Theorem of Gauss

Theorem 4.0.4 (Gauss). *Let p be a prime number different from 2 and 3 and let $C(\mathbb{Z}_p)$ be the cubic defined by $x^3 + y^3 = 1$.*

Then

$$|C(\mathbb{Z}_p)| = \begin{cases} p+1, & \text{if } p \equiv 2(mod 3) \\ p+1+A, & \text{if } p \equiv 1(mod 3) \end{cases},$$

where A is uniquely determined by $4p = A^2 + 27 \cdot B^2$, $A, B \in \mathbb{Z}$ and $A \equiv 1(mod 3)$.

Proof: We quickly rid the case $p \equiv 2(mod 3)$. In this case, the application $\mathbb{Z}_p \to \mathbb{Z}_p : x \to x^3$ is bijective, hence for each $y \in \mathbb{Z}_p$, there is a unique x such that $x^3 + y^3 = 1$. Together with the unique point at infinity, $|C(\mathbb{Z}_p)| = p + 1$.

Assume $p \equiv 1(mod 3)$. Recall that we have identified $C(\mathbb{Z}_p)$ to its projective closure $\overline{C}(\mathbb{Z}_p)$. If $C(\mathbb{Z}_p)$ is given by $x^3 + y^3 = 1$, then $\overline{C}(\mathbb{Z}_p)$ is given via homogenization by $x^3 + y^3 = z^3$. A substitution $z \to -z$ proves that $|C(\mathbb{Z}_p)|$ is the number of solutions in $\mathbb{P}^2_{\mathbb{Z}_p}$ of $x^3 + y^3 + z^3 = 0$.

$(\mathbb{Z}_p^*, \cdot)$ is a cyclic group generated by an element u. let $R = \{a^3 | a \in \mathbb{Z}_p^*\}$. Notice that $R = \{u^{3i} | i \in \mathbb{Z}\}$ and that it is a subgroup of $\mathbb{Z}_p^*$. Let $S = uR$ and $T = u^2R = uS$. Because $p \equiv 1(mod 3)$, R, S and T are disjoint and actually form a partition of $\mathbb{Z}_p$. To see this, let $m = \frac{p-1}{3}$. In $\mathbb{Z}_p^*$, 1, u^m and u^{2m} are distinct elements of order 3. Over $\mathbb{Z}_p$, the polynomial equation $x^3 = 1$ has at most 3 roots, hence $\{1, u^m, u^{2m}\}$ is the set of elements of order 3 in $\mathbb{Z}_p^*$. This set is a subgroup of $\mathbb{Z}_p^*$ and it is also the kernel of $\mathbb{Z}_p^* \to \mathbb{Z}_p^* : x \to x^3$. The image of this application is R. This proves that R is a subgroup of index 3 in $\mathbb{Z}_p^*$ and that S, T are its cosets. In particular R, S and T partition $\mathbb{Z}_p^*$ and $|R| = |S| = |T| = m$. Moreover, $RS = S$, $ST = R$, $TR = T$, $rR = R$, $rS = S$, $rT = T$ $\forall r \in R$, $sR = S$, $sS = T$, $sT = R$ $\forall s \in S$ and $tR = T$, $tS = R$, $tT = S$ $\forall t \in T$.

For arbitrary nonempty subsets X, Y and Z of $\mathbb{Z}_p$, denote $|XYZ| = |\{(x, y, z) \in X \times Y \times Z | x + y + z = 0\}|$.

We can now start counting the projective solutions of $x^3+y^3+z^3=0$. If $xyz \neq 0$, then the equation has $27|RRR|$ solutions in $(\mathbb{Z}_{\text{ı}}{}^*)^3$. This is because if $a \in R$, then the equation $x^3 = a$ has 3 distinct solutions in $\mathbb{Z}_p^*$. Therefore there are $\frac{27}{p-1}|RRR|$ projective solutions of $x^3+y^3+z^3=0$ with $xyz \neq 0$. If $x=0$, then $y \neq 0$ otherwise $z=0$ and $[0:0:0]$ is not a point in $\mathbb{P}^2_{\mathbb{Z}_p}$. For each $y \in \mathbb{Z}_p^*$, the solutions to $0^3+y^3+z^3=0$ are $z \in \{-y, -u^m y, -u^{2m} y\}$, hence for $x=0$, $x^3+y^3+z^3=0$ has $3(p-1)$ solutions in $(\mathbb{Z}_p)^3$ different from $(0,0,0)$. These give 3 projective solutions if $x=0$. These solutions are actually $\{[0:1:-1],[0:1,-u^m],[0:1:u^{2m}]\}$. The same argument holds for $y=0$ and $z=0$ and the corresponding sets of solutions are easily seen to be disjoint. The conclusion is $|C(\mathbb{Z}_p)| = \frac{27}{p-1}|RRR| + 9 = \frac{9}{m}|RRR| + 9$. So computing $|C(\mathbb{Z}_p)|$ reduces to computing $|RRR|$.

Remark 4.0.5. *It is easily seen that if X, Y, Z_1, Z_2 are nonempty subsets of $\mathbb{Z}_p$ and $Z_1 \cap Z_2 = \emptyset$, then $|XY(Z_1 \cup Z_2)| = |XYZ_1| + |XYZ_2|$.*

We have the partition $\mathbb{Z}_p = \{0\} \sqcup R \sqcup S \sqcup T$. Using the above remark, $|RR\mathbb{Z}_p| = |RR\{0\}|+|RRR|+|RRS|+|RRT|$. For each $a, b \in R$, the equation $a+b+x=0$ has a unique solution in $\mathbb{Z}_p$, so $|RR\mathbb{Z}_p| = |R|^2 = m^2$. For every $a \in R$, $-a \in R$ is the unique solution to $a+x+0=0$, hence $|RR\{0\}| = m$. So $m^2 = m + |RRR| + |RRS| + |RRT|$.

Remark 4.0.6. *If X, Y, Z are nonempty subsets of $\mathbb{Z}_p$ and $a \in \mathbb{Z}_p^*$, then $|(aX)(aY)(aZ)| = |XYZ|$. This is because $x+y+z=0, (x,y,z) \in X \times Y \times Z \Leftrightarrow ax+ay+az=0, (ax, ay, az) \in aX \times aY \times aZ$.*

Using this observation, $|RRR| = |(uR)(uR)(uR)| = |SSS| = |(uS)(uS)(uS)| = |TTT|$. Similarly $|RRS| = |SST| = |TTR|$ and $|RRT| = |SSR| = |TTS|$.

Remark 4.0.7. *If X, Y, Z are nonempty subsets of $\mathbb{Z}_p$, then $|XYZ| = |YXZ| = |XZY|$.*

$m^2 = m + |RRR| + |RRS| + |RRT| = m + |RRR| + |SST| + |TTS| = m + |RRR| + |SST| + TST|$.

$|\{0\}ST| + |RST| + |SST| + |TST| = |\mathbb{Z}_p ST| = m^2$. If there exist $s \in S$ and $t \in T$ such that $0+s+t=0$, then $s=-t$. $(-1) = (-1)^3 \Rightarrow (-1) \in R \Rightarrow T = -T \Rightarrow s \in S \cap T$ which is a contradiction. Hence $|\{0\}ST| = 0$.

$m + |RRR| + |SST| + |TST| = m^2 = |RST| + |SST| + |TST| \Rightarrow m + |RRR| = |RST| \Rightarrow$

$$|C(\mathbb{Z}_p)| = \frac{9}{m}(|RST| - m) + 9 = \frac{9}{m}|RST|.$$

Let ε be a complex primitive p-th root of unity. Because $\varepsilon^p = 1$, ε^k is well defined for every $k \in \mathbb{Z}_p$. Let

$$\alpha_1 = \sum_{r \in R} \varepsilon^r$$

$$\alpha_2 = \sum_{s\in S} \varepsilon^s$$

$$\alpha_3 = \sum_{t\in T} \varepsilon^t.$$

Let $F(X) = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)$. We set to find its coefficients. $\alpha_1+\alpha_2+\alpha_3 = \sum_{i\in\mathbb{Z}_p^*} \varepsilon^i = (\sum_{i=0}^{p-1} \varepsilon^i) - 1 = -1$.

$$\alpha_2\alpha_3 = \sum_{\substack{s\in S\\ t\in T}} \varepsilon^{s+t} = \sum_{x=0}^{p-1} N(x)\varepsilon^x,$$

where $N(x) = |\{(s,t)\in S\times T | s+t = x\}| = |ST\{-x\}|$. We have $N(0) = |ST\{0\}| = 0$. Also $N(x) = |ST\{-x\}| = |(rS)(rT)\{-rx\}| = |ST\{-rx\}| = N(rx)$ for every $r\in R$. We have $|ST(-xR)| = |ST(\bigcup_{r\in R}\{-rx\})| = \sum_{r\in R} N(rx) = |R|\cdot N(x) = mN(x)$. Therefore,

$$mN(x) = \begin{cases} |STR|, & \text{if } x\in R \\ |STS|, & \text{if } x\in S \\ |STT|, & \text{if } x\in T \end{cases}.$$

Let $a,b,c\in\mathbb{N}$ such that $|STR| = ma,\ |STS| = mb,\ |STT| = mc$. Then $|C(\mathbb{Z}_p)| = 9a$ and $\alpha_2\alpha_3 = a\alpha_1 + b\alpha_2 + c\alpha_3$.

Similarly, $\alpha_1\alpha_2 = \sum_{x=1}^{p-1} N_1(x)\varepsilon^x$, where $N_1(x) = |RS\{-x\}|$. Also,

$$mN_1(x) = \begin{cases} |RSR|, & \text{if } x\in R \\ |RSS|, & \text{if } x\in S \\ |RST|, & \text{if } x\in T \end{cases},$$

and $\alpha_1\alpha_2 = \frac{|RSR|}{m}\alpha_1 + \frac{|RSS|}{m}\alpha_2 + \frac{|RST|}{m}\alpha_3 = b\alpha_1 + c\alpha_2 + a\alpha_3$. Analogously we prove $\alpha_1\alpha_3 = c\alpha_1 + a\alpha_2 + b\alpha_3$.

$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = (a+b+c)(\alpha_1+\alpha_2+\alpha_3) = -a-b-c = -\frac{1}{m}(|STR|+|STS|+|STT|) = -\frac{1}{m}(|ST\mathbb{Z}_p|-|ST\{0\}|) = -\frac{1}{m}(m^2-0) = -m$.

$3\alpha_1\alpha_2\alpha_3 = \alpha_1(\alpha_2\alpha_3) + \alpha_2(\alpha_1\alpha_3) + \alpha_3(\alpha_1\alpha_2) = \alpha_1(a\alpha_1+b\alpha_2+c\alpha_3) + \alpha_2(c\alpha_1+a\alpha_2+b\alpha_3) + \alpha_3(b\alpha_1+c\alpha_2+a\alpha_3) = a(\alpha_1^2+\alpha_2^2+\alpha_3^2) + (b+c)(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1) = a((\alpha_1+\alpha_2+\alpha_3)^2 - 2(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)) - m(b+c) = m(2a-b-c) + a = mk + a$, for $k = 2a-b-c$. So $\alpha_1\alpha_2\alpha_3 = \frac{km+a}{3}$.

We now have $F(X) = X^3 + X^2 - mX - \frac{km+a}{3}$.

$k = 2a-b-c = 3a-(a+b+c) = 3a+m \Rightarrow |C(\mathbb{Z}_p)| = 9a = 3(3a) = 3(m+k) = 3m+3k = p-1+3k = p+1+(3k-2)$. Denote $3k-2 = A$. We want to prove that A verifies the conditions of the theorem. Because $A\in\mathbb{Z}$ and $A\equiv 1(mod 3)$, all that is left to prove is that there exists $B\in\mathbb{Z}$ such that $4p = A^2+27B^2$ and that A is unique with this properties.

What follows is an ingenious method to construct B.

Let $\beta_i = 1+3\alpha_i\ \forall i = \overline{1,3}$. Consider the polynomial $G(X) = (X-\beta_1)(X-\beta_2)(X-\beta_3)$ and let's compute its coefficients.

$\beta_1+\beta_2+\beta_3 = 3+3(\alpha_1+\alpha_2+\alpha_3) = 0$.

$\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1 = 3+6(\alpha_1+\alpha_2+\alpha_3)+9(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1) = 3-6-9m = -3(3m+1) = -3p$.

$\beta_1\beta_2\beta_3 = 1+3(\alpha_1+\alpha_2+\alpha_3)+9(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)+27\alpha_1\alpha_2\alpha_3 = 1-3-9m+9(km+a) = -2-9m+9km+3(3a) = -2-9m+9km+3(m+k) = (3k-2)+(9km-6m) = (3k-2)(1+3m) = p\cdot A$.

We have proved $G(X) = X^3-3pX-pA$. Let's compute Δ_G, the discriminant of G. Recall the following formulas for the discriminant of a polynomial:

Proposition 4.0.8. *Let $f(X) = X^3+aX^2+bX+c$ be a polynomial with coefficients in an arbitrary field K and let x_1, x_2, x_3 be the roots of f in an algebraic closure of K. Then $\Delta_f = -4a^3c+a^2b^2+18abc-4b^3-27c^2 = ((x_1-x_2)(x_2-x_3)(x_3-x_1))^2$ and $\Delta_f \in K$.*

$\Delta_G = ((\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3))^2 = 27^2((\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3))^2$.

$(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_2-\alpha_3) = (\alpha_1^2-\alpha_1\alpha_3-\alpha_1\alpha_2+\alpha_2\alpha_3)(\alpha_2-\alpha_3) = \alpha_2\alpha_3(\alpha_2-\alpha_3)+\alpha_1(\alpha_1-\alpha_2-\alpha_3)(\alpha_2-\alpha_3) = \alpha_2\alpha_3(\alpha_2-\alpha_3)+(\alpha_1^2\alpha_2-\alpha_1^2\alpha_3-\alpha_1\alpha_2^2+\alpha_1\alpha_2\alpha_3-\alpha_1\alpha_2\alpha_3+\alpha_1\alpha_3^2) = \alpha_2\alpha_3(\alpha_2-\alpha_3)+\alpha_3\alpha_1(\alpha_3-\alpha_1)+\alpha_1\alpha_2(\alpha_1-\alpha_2) = (a\alpha_1+b\alpha_2+c\alpha_3)(\alpha_2-\alpha_3)+(c\alpha_1+a\alpha_2+b\alpha_3)(\alpha_2-\alpha_1)+(b\alpha_1+c\alpha_2+a\alpha_3)(\alpha_1-\alpha_2) = (\alpha_1^2+\alpha_2^2+\alpha_3^2)(b-c)+(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)(c-b) = (b-c)(\alpha_1^2+\alpha_2^2+\alpha_3^2-\alpha_1\alpha_2-\alpha_2\alpha_3-\alpha_3\alpha_1) = (b-c)(1-3(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1)) = (b-c)(1+3m) = (b-c)p \Rightarrow \Delta_G = 27^2(b-c)^2p^2$.

On the other hand, $\Delta_G = -4(-3p)^3-27(-pA)^2 = 108\cdot p^3-27p^2A^2$. By comparing the two formulas we get $108p^3-27p^2A^2 = 27^2(b-c)^2p^2 \Rightarrow 4p-A^2 = 27(b-c)^2 \Rightarrow 4p = A^2+27B^2$, where $B = b-c$.

We now prove the uniqueness of A.

Assume there exists $A_1 \in \mathbb{Z}$ with $A_1 \equiv 1(mod 3)$ for which there exists $B_1 \in \mathbb{Z}$ such that $4p = A^2+27B^2 = A_1^2+27B_1^2$.

$4p(B_1^2-B^2) = (A^2+27B^2)B_1^2-B^2(A_1^2+27B_1^2) = A^2B_1^2-A_1^2B^2 = (AB_1-BA_1)(AB_1+BA_1) \Rightarrow \begin{cases} p|AB_1+A_1B \\ \quad or \\ p|AB_1-BA_1 \end{cases}$. Assume that $p|AB_1-BA_1$. The other case is treated in perfect analogy.

$(4p)^2 = 16p^2 = (A_1^2+27B_1^2)(A^2+27B^2) = (AA_1+27BB_1)^2+27(AB_1-BA_1)^2 \Rightarrow p|AA_1+27BB_1 \Rightarrow 16 = \left(\frac{AA_1+27BB_1}{p}\right)^2+27\left(\frac{AB_1-BA_1}{p}\right)^2$. If $AB_1 \neq BA_1$, then $27\left(\frac{AB_1-BA_1}{p}\right)^2 \geq 27$. This and $\left(\frac{AA_1+27BB_1}{p}\right)^2 \geq 0$ imply $16 \geq 27$ which is absurd. So $AB_1 = BA_1 \Rightarrow A^2B_1^2 = B^2A_1^2 \Rightarrow (4p-27B^2)B_1^2 = B^2(4p-27B_1^2) \Rightarrow 4pB_1^2-27(BB_1)^2 = 4pB^2-27(BB_1)^2 \Rightarrow 4pB_1^2 = 4pB^2 \Rightarrow B_1^2 = B^2 \Rightarrow 4p-27B_1^2 = 4p-27B^2 \Rightarrow A_1^2 = A^2 \Rightarrow A_1 = \pm A$. Since $A \equiv A_1 \equiv 1(mod 3)$, we finally have the proof for $A = A_1$. ∎

Chapter 5

Mordell-Weil's Theorem

In this lecture we begin the proof of the Mordell-Weil Theorem. The theorem states that the abelian group $C(\mathbb{Q})$ associated to an elliptic curve is finitely generated. Restricted by an elementary proof we will first prove the theorem in the particular case it has points of order 2. Later, in Lecture VIII, we will give a complete proof using some facts of Algebraic Number Theory.

Theorem 5.0.9 (Mordell-Weil). *Let $C(Q)$ be the elliptic curve defined by $y^2 = x^3 + ax^2 + bx + c = f(x)$ with $a, b, c \in \mathbb{Z}$ and $\Delta_f \neq 0$. The abelian group $C(\mathbb{Q})$ is finitely generated.*

We begin by introducing some machinery. We first define the height of a rational point. The general notion of height associated to rational points on projective varieties or to sheaves is fundamental to Arithmetic Geometry one of the leading domains in Arithmetics. The definition of height for rational numbers or points is nevertheless very easy to understand.

Definition 5.0.10. *Let $q \in \mathbb{Q}$. Define $H(q) = \max\{|m|, |n|\}$ if $q = \frac{m}{n}$, $m, n \in \mathbb{Z}$, $n \neq 0$ and $gcd(n, m) = 1$. Define $h(q) = \ln H(q)$. $H(q)$ and $h(q)$ are both called heights of the rational number q.*

Remark 5.0.11. *The condition $gcd(m, n) = 1$ in the definition of $H(q)$ implies that $H(0) = 1$ since the only possible writings for 0 in the form $\frac{m}{n}$ with $gcd(n, m) = 1$ are $\frac{0}{\pm 1}$. Since $|n| = |-n|$ for any integer n, the height H is well defined for any rational number. We have $h(q) = \ln H(q) \geq \ln 1 = 0$, therefore h takes only nonnegative real values.*

Definition 5.0.12. *If $P(x, y)$ is a point in $C(\mathbb{Q})$ different form $O = [0 : 1 : 0]$, the point at infinity of $C(\mathbb{Q})$, then define $H(P) = H(x)$ and $h(P) = h(x)$. Set $H(O) = 1$ and $h(O) = 0$.*

The main steps of the proof of Mordell-Weil's Theorem are given by the following four lemmas. The first three are elementary and will also be used in the proof of the general Mordell-Weil Theorem in Lecture VIII. To prove

the fourth in elementary manner we will need the additional assumption that $C(\mathbb{Q})$ has points of order 2.

Lemma 5.0.13 (Lemma 1). *If $r \in \mathbb{R}$, then $\{P \in C(\mathbb{Q}) | h(P) < r\}$ is a finite set.*

Proof: $h(P(x,y)) = h(x) = \ln H(x) < r \Leftrightarrow H(x) < e^r$. If $x = \frac{m}{n}$ with $m, n \in \mathbb{Z}$, $n \neq 0$ and $gcd(n,m) = 1$ then $H(x) = \max\{|m|, |n|\}$. $H(x) < e^r \Leftrightarrow |m|, |n| < e^r$. Since m, n range in $(-e^r, e^r)$ there are only a finite number of possibilities to choose them, hence a finite number of choices for x. Since y is given by $y^2 = f(x)$, there are only a finite number of choices for P on $C(\mathbb{Q})$. ∎

Remark 5.0.14. *Recall that we have proved in 2.2.5 that for any $P(x,y) \in C(\mathbb{Q})$ there exist $m, n, e \in \mathbb{Z}$ with $e \neq 0$ and $gcd(m,e) = gcd(n,e) = 1$ such that $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$.*

Lemma 5.0.15 (Lemma 2). *For any $P_0 \in C(\mathbb{Q})$ there exists a constant c_1 depending only on P_0 and C such that $h(P + P_0) \leq 2h(P) + c_1$ for any $P \in C(\mathbb{Q})$.*

Proof: If $P_0 = O$ then choose $c_1 = 0$.

Assume $P_0(x_0, y_0) \neq O$ and take $P(x,y) \in C(\mathbb{C})$, $P \neq O, P_0, -P_0$. We have $x(P + P_0) = \lambda^2 - a - x - x_0$ with $\lambda = \frac{y - y_0}{x - x_0}$. Then $x(P + P_0) = \left(\frac{y-y_0}{x-x_0}\right)^2 - a - x - x_0 = \frac{(y-y_0)^2 - a(x-x_0)^2 - (x+x_0)(x-x_0)^2}{(x-x_0)^2} = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$, where $A, B, C, D, E, F, G \in \mathbb{Z}$ depend only on P_0 and C. By the preceding remark, $x(P + P_0) = \frac{A\frac{n}{e^3} + B\frac{m^2}{e^4} + C\frac{m}{e^2} + D}{E\frac{m^2}{e^4} + F\frac{m}{e^2} + G} = \frac{Aen + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$. The denominator and numerator of the last fraction need not be coprime, but we certainly have $H(P + P_0) \leq \max\{|Aen + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}$.

$H(P) = \max\{|m|, |e^2|\} \Rightarrow e^2 \leq H(P)$ and $|m| \leq H(P)$. Don't confuse the integer e that appears here with Euler's constant $e = 2.7\ldots$.

We prove $|n| \leq kH(P)^{\frac{3}{2}}$ where k depends only on $C(\mathbb{Q})$. We have $y^2 = x^3 + ax^2 + bx + c \Rightarrow \frac{n^2}{e^6} = \frac{m^3}{e^6} + a\frac{m^2}{e^4} + b\frac{m}{e^2} + c \Rightarrow n^2 = m^3 + am^2e^2 + bme^4 + ce^6 \Rightarrow |n|^2 \leq H(P)^3(1 + |a| + |b| + |c|)$. Denote $k = 1 + |a| + |b| + |c|$. Therefore $|n| \leq kH(P)^{\frac{3}{2}}$ and k depends only on C.

Now $H(P + P_0) \leq \max\{H(P)^2(|A|k + |B| + |C| + |D|), H(P)^2(|E| + |F| + |G|)\} = H(P)^2 k_1$ for some k_1 depending only on $C(\mathbb{Q})$ and P_0. From this it easily follows that $h(P + P_0) \leq 2h(P) + \ln k_1$. Choosing $c_1 = \max\{h(P_0), h(2P_0), h(O), \ln k_1\}$ finishes the proof. ∎

Lemma 5.0.16 (Lemma 3). *There exists a constant c_2 depending only on $C(\mathbb{Q})$ such that $h(2P) \geq 4h(P) - c_2$ for all $P \in C(\mathbb{Q})$.*

Proof: Assume $P(x,y)$ is a point on $C(\mathbb{Q})$ of order different from 1 or 2. We have $x(2P) = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x = \frac{f'(x)^2}{4f(x)} - a - 2x = \frac{(3x^2 + 2ax + b)^2 - 4(a + 2x)(x^3 + ax^2 + bx + c)}{4(x^3 + ax^2 + bx + c)} =$

$\frac{\varphi(x)}{\psi(x)}$, where φ and ψ are polynomials in x of degrees 4 and 3 respectively. If φ and ψ had common roots, then f and f' would have had common roots contradicting the smoothness of C. The coefficients of φ and ψ are integers and only depend on $C(\mathbb{Q})$.

To finish the proof of 5.0.16 we need the following lemma:

Lemma 5.0.17. *Let $\varphi, \psi \in \mathbb{Z}[X]$ be two polynomials with no common complex roots. Let $d = \max\{deg(\varphi), deg(\psi)\}$. Then:*

1. *There exists a nonzero integer R such that $gcd(n^d\varphi(\frac{m}{n}), n^d\psi(\frac{m}{n}))|R$ for all $m, n \in \mathbb{Z}$, $n \neq 0$ and $gcd(m, n) = 1$.*

2. *There exist $c_2, c_3 \in \mathbb{R}_+$ such that $d \cdot h(\frac{m}{n}) - c_2 \leq h(\frac{\varphi(\frac{m}{n})}{\psi(\frac{m}{n})}) \leq d \cdot h(\frac{m}{n}) + c_3$ for rational numbers $\frac{m}{n}$ such that $\psi(\frac{m}{n}) \neq 0$.*

Assume the above lemma proved. Applied to our setting, it gives the existence of a constant c_2' such that $4h(P) - c_2' \leq h(2P)$ for every $P(x, y) \in C(\mathbb{Q})$ of order different from 1 or 2. Let $c_2" = \max\{4h(P) - h(2P) | P \in C(\mathbb{Q})$ is of order 1 or 2$\}$. Choosing $c_2 = \max\{c_2', c_2"\}$ we have proved 5.0.16.

Proof of 5.0.17: (1) Using that $h(q) = h(\frac{1}{q})$ for any nonzero rational number q, we can assume $d = deg(\varphi) \geq deg(\psi) = e$. Because φ and ψ have no common complex roots, there exist φ_1 and ψ_1 in $\mathbb{Q}[X]$ such that $\varphi\varphi_1 + \psi\psi_1 = 1$. There exists a positive integer A such that $A\varphi_1, A\psi \in \mathbb{Z}[X]$ and A depends only on φ and ψ. Let $D = \max\{deg(\varphi_1), deg(\psi_1)\}$. Then

$$n^d\varphi(\frac{m}{n}) \cdot n^D A\varphi_1(\frac{m}{n}) + n^d\psi(\frac{m}{n}) \cdot n^D A\psi_1(\frac{m}{n}) = n^{d+D}A.$$

Let $k = gcd(n^d\varphi(\frac{m}{n}), n^d\psi(\frac{m}{n}))$. It is easy to see that the previous equality implies $k|An^{d+D}$. Let $\varphi(x) = a_0x^d + a_1x^{d-1} + \ldots + a_d$.

$k|n^d\varphi(\frac{m}{n}) \Rightarrow k|An^{d+D-1} \cdot (n^d\varphi(\frac{m}{n})) = An^{d+D-1}(a_0m^d + a_1m^{d-1}n + \ldots + a_dn^d)$. For $i > 0$, $k|An^{d+D} \Rightarrow k|An^{d+D-1+i}m^{d-i}a_i$. From this we conclude $k|Aa_0n^{d+D-1}m^d$. Therefore $k|gcd(Aa_0n^{d+D-1}m^d, An^{n+D}) = An^{d+D-1} \cdot gcd(a_0m^d, n) = An^{d+D-1} \cdot gcd(a_0, n)|Aa_0n^{d+D-1}$. Repeating this argument we prove $k|Aa_0^{d+D}$. A solution to the problem is $R = Aa_0^{d+D}$.

(2) We are only interested in the first inequality i.e. in the existence of c_2. Proving the existence of c_3 is done in analogy to Lemma 2.

The previous point proves that $H(\frac{n^d\varphi(\frac{m}{n})}{n^d\psi(\frac{m}{n})}) \geq \frac{1}{R}\max\{|n^d\varphi(\frac{m}{n})|, |n^d\psi(\frac{m}{n})|\}$. This is because what is cancelled to make the the denominator and numerator of $\frac{n^d\varphi(\frac{m}{n})}{n^d\psi(\frac{m}{n})}$ coprime divides R and therefore is less or equal to R.

By the well known inequality $\max\{|a|, |b|\} \geq \frac{1}{2}(a + b)$ for positive reals a, b, we have $H(\frac{n^d\varphi(\frac{m}{n})}{n^d\psi(\frac{m}{n})}) \geq \frac{1}{2R}(|n^d\varphi(\frac{m}{n})| + |n^d\psi(\frac{m}{n})|)$.

$$\frac{H(\frac{varphi(\frac{m}{n})}{\psi(\frac{m}{n})})}{H(\frac{m}{n})^d} \geq \frac{|n^d\varphi(\frac{m}{n})| + |n^d\psi(\frac{m}{n})|}{2R\max\{|m|^d, |n|^d\}} = \frac{|\varphi(\frac{m}{n})| + |\psi(\frac{m}{n})|}{2R\max\{|\frac{m}{n}|^d, 1\}} \geq k_1 > 0$$

for some $k_1 > 0$, for all integers m, n, $n \neq 0$, $gcd(m,n) = 1$ and $\psi(\frac{m}{n}) \neq 0$. To prove the existence of k_1, consider the function $f(x) = \frac{|\varphi(x)|+|\psi(x)|}{2R\max\{|x|^d,1\}}$. f is a continuous function on $\mathbb{R}$ and $f(x) \geq 0$ for all $x \in \mathbb{R}$. We have $f(x) = 0 \Rightarrow |\varphi(x)| + |\psi(x)| = 0 \Rightarrow \varphi(x) = \psi(x) = 0$ contradicting the hypothesis that φ and ψ have no common complex roots. We have proved $f(x) > 0$ for all reals x. For $|x| > 1$ we have $\lim_{|x|\to\infty} f(x) = \lim_{|x|\to\infty} \frac{|\varphi(x)|+|\psi(x)|}{2R|x|^d}$. This limit exists and is equal to the sum of the absolute values of the coefficients of the terms of degree d in φ and ψ. By the assumption $deg(\varphi) = d$, at least the one in φ is nonzero, hence the limit is nonzero and greater than some real $l > 0$. There exists $N \in \mathbb{N}$ such that $f(x) > \frac{l}{2}$ for $|x| > N$. Since $f(x) > 0$ for $x \in \mathbb{R}$, $f(x) > l'$ on $[-N, N]$ for some $l' > 0$. Just take $k_1 = \min\{\frac{l}{2}, l'\}$.

We have proved $\frac{H(\frac{\varphi(\frac{m}{n})}{\psi(\frac{m}{n})})}{H(\frac{m}{n})^d} \geq k_1 > 0$. Taking logarithms and setting $c_2 = -\ln k_1$ we find the required inequality: $dh(\frac{m}{n}) - c_2 \leq h(\frac{\varphi(\frac{m}{n})}{\psi(\frac{m}{n})})$. ■

Lemma 5.0.18 (Lemma 4 Weak Mordell-Weil Theorem).

$$|C(\mathbb{Q}) : 2C(\mathbb{Q})| < \infty.$$

For the beginning, assume we have proved Lemma 4 and let's see how the proof of Mordell-Weil's Theorem follows. We will use the following descent argument:

Theorem 5.0.19 (Descent Argument Theorem). *Let $(G, +)$ be an abelian group and let $h : G \to \mathbb{R}_+$ be a function such that:*

1. *$\forall\ r \in \mathbb{R}$ the set $\{g \in G | h(g) < r\}$ is finite.*
2. *$\forall\ g_0 \in G$ there exists $c_1 > 0$ such that $h(g + g_0) \leq 2h(g) + c_1$ for all $g \in G$.*
3. *There exists $c_2 > 0$ such that $h(2g) \geq 4h(g) - c_2$ for all $g \in G$.*
4. *$|G : 2G| < \infty$.*

Then G is finitely generated.

Proof of Mordell-Weil's Theorem: Plunge $G = C(\mathbb{Q})$, h the height function on $C(\mathbb{Q})$, c_1 and c_2 the constants given by Lemmas 2 and 3 in the Descent Argument Theorem. Notice that conditions (1) and (4) in the theorem are guaranteed by Lemmas 1 and 4 and conclude that $C(\mathbb{Q})$ is finitely generated. ■

Proof of 5.0.19: Let $q_1, \ldots, q_m$ be a complete system of representants in G for $G/2G$. By condition (4), $m < \infty$.

Let $p \in G$. By induction, there exists a sequence of elements $p_k \in G$ such that $p_0 = p$ and there exists $i_k \in \overline{1,m}$ such that $p_{k-1} - q_{i_k} = 2p_k$ for all $k > 0$. Just take q_{i_k} to be the reprezentant of p_{k-1} in $G/2G$.

A simple induction proves $p = q_{i_1} + 2q_{i_2} + \ldots + 2^s q_{i_{s+1}} + 2^{s+1}P_{s+1}$ for all $s > 0$.

By (2) there exist positive real constants $c_{1,1}, \ldots, c_{1,m}$ such that $h(g - q_i) \leq 2h(g) + c_{1,i}$ for all $g \in G$ and all $i = \overline{1,m}$. Take $c_1 = \max\{c_{1,i} | i = \overline{1,m}\}$. $c_1 > 0$. Then $h(g - q_i) \leq 2h(g) + c_1$ for all $g \in G$ (5).

Combining (3) and (5) gives $2h(p_{s-1}) + c_1 \geq h(p_{s-1} - q_{i_s}) = h(2p_s) \geq 4h(p_s) - c_2 \Rightarrow 2h(p_s) \leq h(p_{s-1}) + \frac{c_1+c_2}{2} \Rightarrow h(p_s) \leq \frac{3}{4}h(p_{s-1}) + \frac{1}{4}(c_1 + c_2 - h(p_{s-1}))$. (6)

If $h(p_{s-1}) \geq c_1 + c_2$ for some s, then by (6), $h(p_s) \leq \frac{3}{4}h(p_{s-1}) < h(p_{s-1})$. The inequality is strict otherwise $0 = h(p_{s-1}) \geq c_1 + c_2 > 0$ is a contradiction. If $h(p_t) \geq c_1 + c_2$ for all $t \geq s$, then by induction $(p_t)_{t \geq s}$ is an infinite sequence of elements of G with the property $h(p_s) > h(p_{s+1}) > \ldots$. This contradicts the hypothesis (1). Therefore there exists $t \geq s$ such that $h(p_t) < c_1 + c_2$. For this t, $p = q_{i_1} + 2q_{i_2} + \ldots + 2^{t-1}q_{i_t} + 2^t p_t$. So p is a combination of $q_1, q_2, \ldots, q_m$ and $\{r \in G | h(r) < c_1 + c_2\}$.

We have proved that $q_1, \ldots, q_m$ and the finite set $\{r \in G | h(r) < c_1 + c_2\}$ (this set is finite by (1)) generate G. ∎

Proof of 5.0.18: As I have said, we will first prove the Weak Mordell-Weil Theorem only in the case $C(\mathbb{Q})$ has a point of order 2. The equation of $C(\mathbb{Q})$ was given by $y^2 = x^3 + ax^2 + bx + c = f(x)$ with $a, b, c \in \mathbb{Z}$ and $\Delta_f \neq 0$. We have seen that the points $P(x, y)$ of order 2 of $C(\mathbb{Q})$ are given by $y = 0 \Leftrightarrow f(x) = 0$. $x \in \mathbb{Q}$ and $f(x) = 0$ imply that x is a rational number, integral over $\mathbb{Z}$, therefore x is an integer. Assume x_0 is an integer root of f. Up to the substitution $x \to x - x_0$ we can assume that $x_0 = 0 \Rightarrow c = 0$. The condition for non-singularity of C is $0 \neq \Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = a^2b^2 - 4b^3 = b^2(a^2 - 4b)$.

Define the curve $\bar{C}$ given by the equation $\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x = \bar{f}(x)$, where $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. We have $\Delta_{\bar{f}} = \bar{b}^2(\bar{a}^2 - 4\bar{b}) = (a^2 - 4b)^2(4a^2 - 4a^2 + 16b) = 16b(a^2 - 4b)^2 \neq 0$, hence $\bar{C}(\mathbb{Q})$ is a smooth elliptic curve.

Remark 5.0.20. *Repeating the construction above for $\bar{C}$, we have $\overline{\overline{C}}(\mathbb{Q}) : y^2 = x^3 + \overline{\bar{a}}x^2 + \overline{\bar{b}}x$, where $\overline{\bar{a}} = -2\bar{a} = 4a$ and $\overline{\bar{b}} = \bar{a}^2 - 4\bar{b} = 4a^2 - 4(a^2 - 4b) = 16b$.*

The substitutions $x \to \frac{x}{4}$ and $y \to \frac{y}{8}$ induce a rational transformation between C and $\overline{\overline{C}}$. In other words, the projective closures of C and $\overline{\overline{C}}$ are projectively equivalent through a rational transformation. This is because $(x, y) \in C(\mathbb{Q}) \Leftrightarrow y^2 = x^3 + ax^2 + bx \Leftrightarrow 64y^2 = 64x^3 + 64ax^2 + 64bx \Leftrightarrow (8y)^2 = (4x)^2 + 4a(4x)^2 + 16b(4x) \Leftrightarrow (8y)^2 = (4x)^3 + \overline{\bar{a}}(4x)^2 + \overline{\bar{b}}(4x) \Leftrightarrow$

$(4x, 8y) \in \overline{\overline{C}}(\mathbb{Q})$.

Proposition 5.0.21. *Let $\varphi : C \to \bar{C}$ be defined by*

$$\varphi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}), & \text{if } P(x,y) \neq O[0:1:0], T(0,0) \\ O[0:1:0], & \text{if } P \in \{O, T\} \end{cases}.$$

Then φ is a group homomorphism from $C(\mathbb{Q})$ to $\bar{C}(\mathbb{Q})$ and $\ker\varphi = \{O, T\}$.

Let $\psi : \bar{C} \to C$ be defined by

$$\psi(\bar{P}) = \begin{cases} (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}), & \text{if } \bar{P}(\bar{x},\bar{y}) \neq \bar{O}[0:1:0], \bar{T}(0,0) \\ O[0:1:0], & \text{if } \bar{P} \in \{\bar{O}, \bar{T}\} \end{cases}.$$

Then ψ is a group morphism from $\bar{C}(\mathbb{Q})$ to $C(\mathbb{Q})$ whose kernel is $\{\bar{O}, \bar{T}\}$. Also $\psi\varphi(P) = 2P\ \forall P \in C(\mathbb{Q})$ and $\varphi\psi(\bar{P}) = 2\bar{P}\ \forall \bar{P} \in \bar{C}(\mathbb{Q})$.

Proof: It suffices to verify the assertions made for φ in the proposition above.

We first prove that φ is well defined i.e. $\varphi(P) \in \bar{C}\ \forall\ P \in C$. If $P \in \{O, T\}$, then $\varphi(P) = \bar{O} \in \bar{C}$. If $P(x,y) \in C$, $P \neq O, T$ implies $x \neq 0$. We have $\varphi(P) \in \bar{C}$ if and only if

$$\left(\frac{y(x^2-b)}{x^2}\right)^2 = \left(\frac{y^2}{x^2}\right)^3 + \bar{a}\left(\frac{y^2}{x^2}\right)^2 + \bar{b}\frac{y^2}{x^2} \Leftrightarrow$$

$$\frac{y^2(x^2-b)^2}{x^4} = \frac{y^6}{x^6} - 2a\frac{y^4}{x^4} + (a^2-4b)\frac{y^2}{x^2} \Leftrightarrow$$

If $y = 0$, the equality is obviously true. If $y \neq 0$, then the equality is equivalent to:

$$(x^2-b)^2x^2 = y^4 - 2ay^2x^2 + (a^2-4b)x^4 \Leftrightarrow$$

$$(x^2-b)^2x^2 = (y^2-ax^2)^2 - 4bx^4 \Leftrightarrow (x^3-bx)^2 = (x^3+bx)^2 - 4bx^4$$

which holds by the identity $(A-B)^2 = (A+B)^2 - 4AB$. We have proved that φ is well defined. It is easy to see that $\varphi(C(\mathbb{Q})) \subset \bar{C}(\mathbb{Q})$.

We prove that φ is a group homomorphism. First, some particular cases must be excluded. We have $\varphi(O) = \bar{O}$. $\varphi(P+O) = \varphi(P) = \varphi(P) + \bar{O} = \varphi(P) + \varphi(O)$.

We wish to prove $\varphi(P+T) = \varphi(P) + \varphi(T) = \varphi(P) + \bar{O} = \varphi(P)$ for all $P \in C$. For $P = O$, $\varphi(O+T) = \varphi(T) = \bar{O} = \varphi(O)$. For $P = T$, $\varphi(T+T) = \varphi(O) = \bar{O} = \varphi(T)$. I have used that T is a point of order 2 because its y coordinate is 0. Assume $P(x,y) \neq O, T$. Then $x \neq 0$ and $x(P+T) =$

$\lambda^2 - a - x - 0 = \left(\frac{y-0}{x-0}\right)^2 - a - x = \frac{b}{x}$. $y(P+T) = -\lambda \cdot x(P+T) - \nu = -\frac{by}{x^2}$. In conclusion $\varphi(P+T) = (\left(\frac{\frac{-by}{x^2}}{\frac{b}{x}}\right)^2, \frac{\frac{-by}{x^2}(\frac{b^2}{x^2}-b)}{\frac{b^2}{x^2}}) = (\frac{y^2}{x^2}, \frac{-y(b-x^2)}{x^2}) = \varphi(P)$. We have used $b \neq 0$ as implied by $b^2(a^2 - 4b) = \Delta_f \neq 0$.

It is clear from the definition that $\varphi(P) = -\varphi(-P)$. We now wish to prove $\varphi(P_1) + \varphi(P_2) = \varphi(P_1 + P_2)$ for all $P_1, P_2 \in C(\mathbb{Q})$. This is equivalent to $\varphi(P_1)+\varphi(P_2)-\varphi(P_1+P_2) = O \Leftrightarrow \varphi(P_1)+\varphi(P_2)+\varphi(P_1 * P_2) = O$. Thus it suffices to prove the following problem: Given P_1, P_2, P_3 three collinear points on $C(\mathbb{Q})$, prove that $\varphi(P_1) + \varphi(P_2) + \varphi(P_3) = 0$. The collinearity of P_1, P_2, P_3 is equivalent to $P_1 + P_2 + P_3 = O$. By the preceding remarks it is enough to consider $P_j \neq O, T \ \forall \ j = \overline{1,3}$. Assume P_1, P_2, P_3 are 3 distinct. Let $y = \lambda \cdot x + \nu$ be the equation of the line l passing through the three collinear points P_1, P_2 and P_3. We prove that $y = \bar{\lambda} \cdot x + \bar{\nu}$ with

$$\bar{\lambda} = \frac{\nu\lambda - b}{\nu}$$

and

$$\bar{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}$$

is the equation of a line passing through $\varphi(P_1)$, $\varphi(P_2)$ and $\varphi(P_3)$. Notice that $\nu \neq 0$ otherwise the line l contains T and by Bezout P_1, P_2 or P_3 is T which contradicts our choice for the three collinear points. Let $\bar{P}(\bar{x}, \bar{y}) = \varphi(P_1)$. It is enough to prove $\bar{y} = \bar{\lambda}\bar{x} + \bar{\nu}$.

$$\bar{\lambda}\bar{x} + \bar{\nu} = \frac{\nu\lambda - b}{\nu}\frac{y_1^2}{x_1^2} + \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu} =$$

$$\frac{(\nu\lambda - b)y_1^2 + x_1^2(\nu^2 - a\nu\lambda + b\lambda^2)}{\nu x_1^2} = \frac{\nu\lambda(y_1^2 - ax_1^2) + b(\lambda^2 x_1^2 - y_1^2) + \nu^2 x_1^2}{\nu x_1^2} =$$

$$\frac{\nu\lambda(x_1^3 + bx_1) - b\nu(\lambda x_1 + y_1) + \nu^2 x_1^2}{\nu x_1^2} = \frac{\lambda x_1^3 - by_1 + x_1^3\nu}{x_1^2} = \frac{x_1^2 y_1 - by_1}{x_1^2} = \bar{y}_1.$$

Therefore φ is a group morphism.

Checking that $\ker\varphi = \{O, T\}$ is a very easy exercise.

Proving that ψ is a well defined group morphism with kernel $\{\bar{O}, \bar{T}\}$ is done just like for φ.

We are left with proving $\psi\varphi(P) = 2P$ for all $P \in C(\mathbb{Q})$ and $\varphi\psi(\bar{P}) = 2\bar{P}$ for all $\bar{P} \in \bar{C}(\mathbb{Q})$. Since their proofs are basically the same, it is enough to prove $\psi\varphi(P) = 2P$.

If $P \in \{O, T\}$, $\psi\varphi(P) = \psi(\bar{O}) = O = 2P$. Don't forget that T has order 2 in $C(\mathbb{Q})$.

Let $P(x,y) \in C(\mathbb{Q})$, $P \neq O, T$ i.e. $x, y \in \mathbb{Q}$ and $x \neq 0$.

$$\psi\varphi(P) = \psi(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}) = \left(\frac{\frac{y^2(x^2-b)^2}{x^4}}{4\frac{y^4}{x^4}}, \frac{\frac{y(x^2-b)^2}{x^2} \cdot (\frac{y^4}{x^4} - a^2 + 4b)}{8\frac{y^4}{x^4}}\right) =$$

$$\left(\frac{(x^2-b)^2}{4y^2}, \frac{x^2(x^2-b)}{8y^3} \cdot (\frac{y^4}{x^4} - a^2 + 4b)\right) =$$

$$\left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(y^4 + (4b-a^2)x^4)}{8y^3x^2}\right). \tag{5.0.1}$$

We have that $\varphi(P) = \bar{T}$ if and only if $y = 0$ if and only if $2P = O$. If $2P = 0$, then $\psi(\varphi(P)) = \psi(\bar{T}) = O = 2P$. Assume now $y \neq 0$. Then the equality 5.0.1 is equivalent to

$$\psi\varphi(P) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^2(x^2+ax+b)^2 + (4b-a^2)x^4)}{8y^3x^2}\right) =$$

$$\left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)((x^2+ax+b)^2 + (4b-a^2)x^2)}{8y^3}\right) =$$

$$\left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3}\right) \tag{5.0.2}$$

We now compute $x(2P)$ and $y(2P)$.

$$x(2P) = \lambda^2 - a - 2x = \frac{f'(x)^2}{4y^2} - a - 2x = \frac{(3x^2+2ax+b)^2}{4(x^3+ax^2+bx)} - a - 2x =$$

$$\frac{(3x^2+2ax+b)^2 - 4(x^3+ax^2+bx)(2x+a)}{4y^2} =$$

$$\frac{9x^4 + 12ax^3 + (4a^2+6b)x^2 + 4abx + b^2 - 8x^4 - 12ax^3 - (4a^2+8b)x^2 - 4abx}{4y^2}$$

$$= \frac{x^4 - 2bx^2 + b^2}{4y^2} = \frac{(x^2-b)^2}{4y^2}.$$

$$y(2P) = -\lambda \cdot x(2P) - \nu = -\lambda \cdot x(2P) - (y - \lambda \cdot x) = -(\frac{f'(x)}{2y}\left(\frac{(x^2-b)^2}{4y^2} - x\right) + y) =$$

$$-\frac{3x^2+2ax+b}{2y} \cdot \frac{x^4 - 2bx^2 + b^2 - 4x(x^3+ax^2+bx)}{4y^2} - y =$$

$$-\frac{(3x^2+2ax+b)(x^4 - 2bx^2 + b^2 - 4x(x^3+ax^2+bx)) + 8(x^3+ax^2+bx)^2}{8y^3} =$$

$$-\frac{f'(x)((x^2-b)^2 - 4xf(x)) + 8f^2(x)}{8y^3} = -\frac{f'(x)(x^2-b)^2 - 4f(x)(xf'(x) - 2f(x))}{8y^3} =$$

$$-\frac{(x^2-b)^2 f'(x) - 4f(x)(3x^3+2ax^2+bx-2x^3-2ax^2-2bx)}{8y^3} =$$

$$-(x^2-b)\frac{(x^2-b)f'(x)-4xf(x)}{8y^3}.$$

To prove 5.0.2 It is enough to prove:

$$x^4+2ax^3+6bx^2+2abx+b^2 = -(x^2-b)f'(x)+4xf(x).$$

$(x^2-b)f'(x) - 4xf(x) = (x^2-b)(3x^2+2ax+b) - 4x(x^3+ax^2+bx) = 3x^4+2ax^3-2bx^2-2abx-b^2-4x^4-4ax^3-4bx^2 = -x^4-2ax^3-6bx^2-2abx-b^2$.
■

Chapter 6

Lecture VI

6.1 The "Weak" Mordell-Weil Theorem

Let $C(\mathbb{Q})$ be the elliptic curve given by the equation $y^2 = f(x) = x^3+ax^2+bx$ with $a, b \in \mathbb{Z}$ and $b^2(a^2 - 4b) \neq 0$. In the condition above we prove:

Theorem 6.1.1 (Weak Mordell-Weil Theorem).

$$|C(\mathbb{Q}) : 2C(\mathbb{Q})| < \infty.$$

Proof: In the previous lecture we have defined $\bar{C}(\mathbb{Q}) : y^2 = \bar{f}(x) = x^3 + \bar{a}x^2 + \bar{b}x$, with $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$, and we have proved:

Proposition 6.1.2. *Let $\varphi : C \to \bar{C}$ be defined by*

$$\varphi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}), & \text{if } P(x,y) \neq O[0:1:0], T(0,0) \\ \bar{O}[0:1:0], & \text{if } P \in \{O, T\} \end{cases}.$$

Then φ is a group homomorphism from $C(\mathbb{Q})$ to $\bar{C}(\mathbb{Q})$ and $\ker\varphi = \{O, T\}$.

Let $\psi : \bar{C} \to C$ be defined by

$$\psi(\bar{P}) = \begin{cases} (\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-\bar{b})}{8\bar{x}^2}), & \text{if } \bar{P}(\bar{x},\bar{y}) \neq \bar{O}[0:1:0], \bar{T}(0,0) \\ O[0:1:0], & \text{if } \bar{P} \in \{\bar{O}, \bar{T}\} \end{cases}.$$

Then ψ is a group morphism from $\bar{C}(\mathbb{Q})$ to $C(\mathbb{Q})$ whose kernel is $\{\bar{O}, \bar{T}\}$.
Also $\psi\varphi(P) = 2P \ \forall P \in C(\mathbb{Q})$ and $\varphi\psi(\bar{P}) = 2\bar{P} \ \forall \bar{P} \in \bar{C}(\mathbb{Q})$.

The following group theory theorem will provide the finishing argument in our proof. However matching the conditions in the hypothesis of the theorem to 6.1.1 will take some time.

Theorem 6.1.3. *Let A and B be two abelian groups. Let $\varphi : A \to B$ and $\psi : B \to A$ be two group homomorphisms such that*

1. $\psi\varphi = 2 \cdot 1_A$ *and* $\varphi\psi = 2 \cdot 1_B$.

2. $|B : Im\varphi| < \infty$ *and* $|A : Im\psi| < \infty$.

Then $|A : 2A| < \infty$.

Proof: We prove $|A : 2A| \leq |A : Im\psi| \cdot |B : Im\varphi|$.

We have $|A : 2A| = |A : \psi\varphi(A)| = |A : \psi(B)||\psi(B) : \psi\varphi(A)|$. The image of $\varphi(A)$ through the canonical projection given by

$$B \to \psi(B) \to \frac{\psi(B)}{\psi\varphi(A)}$$

is trivial, therefore there exists a surjective group homomorphism $B/\varphi(A) \to \psi(B)/\psi\varphi(A) \Rightarrow |B : Im\varphi| = |B/\varphi(A)| \geq |\psi(B)/\psi\varphi(A)| = |Im\psi : \psi\varphi(A)|$. Therefore $|A : 2A| = |A : \psi(B)||\psi(B) : \psi\varphi(A)| \leq |A : \psi(B)||B : \varphi(A)|$. ■

In 6.1.3 put $A = C(\mathbb{Q})$, $B = \bar{C}(\mathbb{Q})$ and φ, ψ the group homomorphisms given in 6.1.2, to conclude that $|C(\mathbb{Q}) : 2C(\mathbb{Q})| < \infty$ if $|A : Im\psi| < \infty$ and $|B : Im\varphi| < \infty$. To finish the proof of the Weak Mordell-Weil Theorem, it is enough to prove $|A : Im\psi| < \infty$. In doing so, we will need the following lemma:

Lemma 6.1.4. *Define*

$$\alpha : C(\mathbb{Q}) \to \frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2},$$

where $\mathcal{Q} = \mathbb{Q}^*/(\mathbb{Q}^*)^2$ *is the factor group of the multiplicative group of nonzero rational numbers by the subgroup of squares, by*

$$\alpha(P) = \begin{cases} \hat{1}, & \text{if } P = O \\ \hat{b}, & \text{if } P = T(0,0) \\ \hat{x}, & \text{for } P(x,y) \neq O, T \end{cases}.$$

Then:

1. α *is a group homomorphism.*

2. $\ker \alpha = Im\psi$.

3. $|Im\alpha| \leq 2^{t+1}$, *where* t *is the number of distinct prime factors of* b.

Proof: α is well defined. This is because $b \neq 0$ ($\Delta_f = b^2(a^2 - 4b) \neq 0$) and $x \neq 0$ if $P(x,y) \neq O, P$.

(1). It is clear from the definition and from $x(P) = x(-P)\ \forall\ P \in C(\mathbb{Q})$ that $\alpha(P) = \alpha(-P)$. Also $\alpha(P)^2 = \hat{1}\ \forall P \in C(\mathbb{Q})$. Let $P, Q \in C(\mathbb{Q})$. Then $\alpha(P)\alpha(Q) = \alpha(P+Q) \Leftrightarrow \hat{1} = \hat{1} \cdot \hat{1} = \alpha(P)\alpha(-P)\alpha(Q)\alpha(-Q) = \alpha(-P)\alpha(-Q)\alpha(P+Q)$.

For α to be a homomorphism is enough to prove that if P, Q, R are collinear points on $C(\mathbb{Q})$, then $\alpha(P)\alpha(Q)\alpha(R) = \hat{1}$. If all P, Q, R are different from O and T, then let $y = \lambda x + \nu$ be the equation of the line passing through them. The condition $P, Q, R \neq O, T$ implies $\nu \neq 0$. $x(P)$, $x(Q)$ and $x(R)$ are the solutions of the system

$$\begin{cases} y^2 = x^3 + ax^2 + bx \\ y = \lambda x + \nu \end{cases} \Rightarrow x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x - \nu^2 = 0 \Rightarrow$$

$$x(P)x(Q)x(R) = \nu^2 \Rightarrow \alpha(P)\alpha(Q)\alpha(R) = \widehat{x(P)}\widehat{x(Q)}\widehat{x(R)} = \hat{\nu}^2 = \hat{1}.$$

If one of P, Q or R is O, then without loss of generality we can assume $R = O$ and the $Q = -P$. $\alpha(P)\alpha(Q)\alpha(R) = \alpha(P)\alpha(-P)\alpha(O) = \alpha(P)\alpha(P)\hat{1} = \alpha(P)^2 = \hat{1}$. For $R = T$ (and similarly for P and Q), the equation of the line passing through P, Q and T is $y = \lambda x$. Then $x(P), x(Q)$ and $0 = x(T)$ are the solutions of the system

$$\begin{cases} y^2 = x^3 + ax^2 + bx \\ y = \lambda x \end{cases} \Rightarrow x^3 + (a - \lambda^2)x^2 + bx = 0 \Rightarrow x(P)x(Q) = b \Rightarrow$$

$$\alpha(P)\alpha(Q)\alpha(R) = \widehat{x(P)}\widehat{x(Q)}\hat{b} = \widehat{x(P)x(Q)}\hat{b} = \hat{b} \cdot \hat{b} = \hat{1}.$$

We have proved that α is a group homomorphism.

(2). $\alpha(\psi(\bar{O})) = \alpha(O) = \hat{1} = \alpha(O) = \alpha(\psi(\bar{T}))$. Let $\bar{P}(\bar{x}, \bar{y}) \in \bar{C}(\mathbb{Q})$, $\bar{P} \neq \bar{O}, \bar{T}$. If $\bar{y} \neq 0 \Rightarrow \bar{x} \neq 0$, then

$$x(\psi(\bar{P})) = \frac{\bar{y}^2}{4\bar{x}^2} \Rightarrow \alpha(\psi(P)) = \hat{1}.$$

If $\bar{y} = 0$, then $\bar{P} \neq \bar{T} \Rightarrow \bar{x} \neq 0$. Then $0 = \bar{y}^2 = \bar{x}^3 + \bar{a}\bar{x}^2 + \bar{b}\bar{x} \Rightarrow \bar{x}^2 + \bar{a}\bar{x} + \bar{b} = 0 \Rightarrow (\bar{x} - \frac{\bar{a}}{2})^2 = \frac{\bar{a}^2 - 4\bar{b}}{4} = \frac{(-2a)^2 - 4(a^2 - 4b)}{4} = 4b \Rightarrow \widehat{\bar{b}} = \widehat{4b} = \hat{1}$. We have used that $\bar{x} \in \mathbb{Q}$ and $\bar{a}^2 - 4\bar{b}, \bar{b} \neq 0$ ($\bar{C}$ is nonsingular) to make sure we get elements of $\mathcal{Q}$.

$$\bar{y} = 0 \Rightarrow \psi(\bar{P}) = \bar{T} \Rightarrow \alpha\psi(\bar{P}) = \hat{\bar{b}} = \hat{1}.$$

We have proved $Im\psi \subset \ker\alpha$.

We now prove the reverse inclusion. It is clear that $O \in Im\psi$. If $T \in \ker\alpha$, then $\hat{b} = \alpha(T) = \hat{1} \Rightarrow b = d^2$ for some rational (hence integer) d. The equation $\bar{x}^2 + \bar{a}x + \bar{b} = 0$ has discriminant $\bar{a}^2 - 4\bar{b} = 16b = 16d^2$, hence it has an integer solution $\bar{x}$. $\bar{P}(\bar{x}, 0)$ is then a point on $\bar{C}(\mathbb{Q})$ such that $\psi(\bar{P}) = T$. Therefore

$$T \in \ker\alpha \Rightarrow T \in Im\psi.$$

Let $P(x, y) \in \ker\alpha$, $P \neq O, T$. Then $x \neq 0$ and $\hat{1} = \alpha(P) = \hat{x} \Rightarrow x = u^2$ for some rational, hence integer, $u \neq 0$. We want to prove that $P \in Im\psi$ i.e. $(x, y) = \psi(\bar{P}) = \left(\frac{\bar{y}^2}{4\bar{x}^2}, (\bar{x}^2 - \bar{b})\frac{\bar{y}}{8\bar{x}^2}\right)$ for some $\bar{P} \in \bar{C}(\mathbb{Q})$. Let

$$\bar{x}_1 = 2(u^2 - \frac{\bar{a}}{4} + \frac{y}{u}), \quad \bar{y}_1 = 2u\bar{x}_1,$$

$$\bar{x}_2 = 2(u^2 - \frac{\bar{a}}{4} - \frac{y}{u}), \quad \bar{y}_2 = -2u\bar{x}_2.$$

We prove that $\bar{P}_1(\bar{x}_1, \bar{y}_1)$, $\bar{P}_2(\bar{x}_2, \bar{y}_2) \in \bar{C}(\mathbb{Q})$ and $\psi(\bar{P}_1) = \psi(\bar{P}_2) = P \in Im\psi$.

We have $\bar{x}_1\bar{x}_2 = 4((x - \frac{\bar{a}}{4})^2 - \frac{y^2}{x}) = 4((x + \frac{a}{2})^2 - \frac{y^2}{x}) = 4\frac{x^3 + ax^2 + \frac{a^2x}{4} - y^2}{4x} = a^2 - 4b = \bar{b} \neq 0 \Rightarrow \bar{x}_1, \bar{x}_2 \neq 0$.

We want to prove $\bar{y}_i = \bar{x}_i^3 + \bar{a}\bar{x}_i^2 + \bar{b}\bar{x}_i \ \forall i = \overline{1,2}$. Since $\bar{x}_i \neq 0$, this is equivalent to $\left(\frac{\bar{y}_i}{\bar{x}_i}\right)^2 = \bar{x}_i + \bar{a} + \frac{\bar{b}}{\bar{x}_i} = \bar{a} + (\bar{x}_i + \frac{\bar{x}_1 \cdot \bar{x}_2}{\bar{x}_i}) = \bar{a} + (\bar{x}_1 + \bar{x}_2) = 4u^2$ which holds by the definition of $\bar{y}_i$. Therefore $\bar{P}_1, \bar{P}_2 \in \bar{C}(\mathbb{Q})$.

$\psi(\bar{P}_i) = \left(\frac{\bar{y}_i^2}{4\bar{x}_i^2}, (\bar{x}_i^2 - \bar{b})\frac{\bar{y}_i}{8\bar{x}_i^2}\right)$.

$$\frac{\bar{y}_i^2}{4\bar{x}_i^2} = \frac{(\pm 2u\bar{x}_i)^2}{4\bar{x}_i^2} = u^2 = x.$$

$$\frac{\bar{y}_i(\bar{x}_i^2 - \bar{b})}{8\bar{x}_i^2} = \frac{\bar{y}_i(\bar{x}_i^2 - \bar{x}_1 \cdot \bar{x}_2)}{8\bar{x}_i^2} = \frac{2u\bar{x}_1(\bar{x}_1^2 - \bar{x}_1 \cdot \bar{x}_2)}{8\bar{x}_1^2} = \frac{u(\bar{x}_1 - \bar{x}_2)}{4} = y.$$

We have also proved $\psi(P_i) = P(x, y)$. This proves the reverse inclusion $\ker\alpha \subset Im\psi$ and we have $\ker\alpha = Im\psi$.

(3) By 2.2.5, if $P(x, y) \in C(\mathbb{Q})$ and $P \neq O$, then there exist $m, n, e \in \mathbb{Z}$, $e \neq 0$, $gcd(m, e) = gcd(n, e) = 1$ such that $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$.

Assume first $P \neq O, T$. Then $m \neq 0$, otherwise $P = T$, and

$$\alpha(P) = \widehat{\frac{m}{e^2}} = \hat{m}.$$

$y^2 = x^3 + ax^2 + bx \Rightarrow \frac{n^2}{e^6} = \frac{m^3}{e^6} + a\frac{m^2}{e^4} + b\frac{m}{e^2} \Rightarrow n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4)$. Let $d = gcd(m, m^2 + ame^2 + be^4) = gcd(m, be^4) = gcd(m, b)$. Since $m(m^2 + ame^2 + be^4)$ is a square, there exists $m_1 \in \mathbb{Z}$ such that $m = d \cdot m_1^2 \Rightarrow \hat{m} = \hat{d}$. Let $b = \pm p_1^{a_1} \cdot \ldots \cdot p_t^{a_t}$ be the prime factor decomposition of b with $p_1, \ldots, p_t$ distinct prime numbers and $a_i \geq 1 \ \forall i = \overline{1,t}$. Then $d|b \Rightarrow \hat{d} = \pm\widehat{p_1^{\varepsilon_1} \cdot \ldots \cdot p_t^{\varepsilon_t}}$ with $\varepsilon_i \in \{0, 1\} \ \forall i = \overline{1,t}$. It is easy to see that these give at most 2^{t+1} possibilities for $\hat{d}$, hence also for $\alpha(P)$. These possibilities include $\hat{d} \in \{\hat{1}, \hat{b}\}$, therefore we need not consider the cases $P \in \{O, T\}$.

Now $Im\alpha \simeq C(\mathbb{Q})/\ker\alpha = C(\mathbb{Q})/Im\psi \Rightarrow |C(\mathbb{Q}) : Im\psi| \leq 2^{t+1}$. ∎

Remark 6.1.5. *Similarly to the lemma above we can prove $|\bar{C}(\mathbb{Q}) : Im\varphi| \leq 2^{s+1}$, where s is the number of distinct prime factors of $\bar{b} = a^2 - 4b$.*

We have proved $|A : Im\psi| < \infty$ and $|B : Im\varphi| < \infty$ and by 6.1.3 we have the Weak Mordell-Weil Theorem. ∎

The proof of 6.1.3 actually gives the estimation:

$$|C(\mathbb{Q}) : 2C(\mathbb{Q})| \leq 2^{s+t+2}.$$

By what we have seen in the previous lecture, we have finished the proof for the Mordell-Weil Theorem in the case $C(\mathbb{Q})$ has points of order 2.

6.2 Computing the rank of elliptic curves

Mordell-Weil's Theorem tells that $C(\mathbb{Q})$ is a finitely generated abelian group. We have proved it just for curves that have points of order 2. The Structure Theorem for finitely generated abelian groups tells us that $C(\mathbb{Q})$ is isomorphic to the direct sum of a free abelian group $\mathbb{Z}^r$ and a finite group $\mathcal{M}$. By definition, the rank of $C(\mathbb{Q})$ is r. $\mathcal{M}$ is the torsion subgroup of $C(\mathbb{Q})$ and is characterized sufficiently well by Nagell-Lutz's Theorem. The purpose of this section is to present a strategy for determining the rank of an elliptic curve. We will see that the effectiveness of this strategy is given by our ability to solve some Diophantine equations. We will work in the same hypothesis: $C(\mathbb{Q})$ has points of order 2 i.e. $C(\mathbb{Q}) : y^2 = f(x) = x^3 + ax^2 + bx$, $a, b \in \mathbb{Z}$ and $b^2(a^2 - 4b) \neq 0$. Let $\bar{C}(\mathbb{Q}) : y^2 = \bar{f}(x) = x^3 + \bar{a}x^2 + \bar{b}x$ for $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$. Let $G = C(\mathbb{Q})$ and $G' = \bar{C}(\mathbb{Q})$.

By the Structure Theorem for finitely generated abelian groups, $\mathcal{M} \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \ldots \times \mathbb{Z}_{p_k^{\alpha_k}}$ for some $k \in \mathbb{N}$, not necessarily distinct prime numbers p_i and integers $\alpha_i \in \mathbb{N}^*$, $i = \overline{1,k}$.

$$G/2G \simeq (\mathbb{Z}_2)^r \times (\mathbb{Z}_{p_1^{\alpha_1}}/2\mathbb{Z}_{p_1^{\alpha_1}}) \times \ldots \times (\mathbb{Z}_{p_k^{\alpha_k}}/2\mathbb{Z}_{p_k^{\alpha_k}}).$$

If p is a prime number, $p \neq 2$ and $\alpha \geq 1$, then $\mathbb{Z}_{p^\alpha} = 2\mathbb{Z}_{p^\alpha}$. This is because 2 is a unit in $\mathbb{Z}_{p^\alpha}$, hence multiplication by it defines an automorphism of $\mathbb{Z}_{p^\alpha}$. If $p = 2$, then $2\mathbb{Z}_{2^\alpha}$ is a subgroup of $\mathbb{Z}_{2^\alpha}$ of index 2. Let

$$\delta = |\{i \in \overline{1,k} | p_i = 2\}|.$$

It is easy to see that

$$|G/2G| = 2^{r+\delta}.$$

Let $G(2) = \{P \in G | 2P = O\}$. It is easy to see that $G(2)$ is a subgroup of G. Moreover:

$$G(2) \simeq (0 \cdot \mathbb{Z})^r \times \prod_{i=\overline{1,k}, p_i=2} (2^{\alpha_i - 1} \cdot \mathbb{Z}_{2^{\alpha_i}}),$$

and $|G(2)| = 2^\delta$. We have seen that $G(2) = \{O[0:1:0]\} \cup \{P(x,y) \in G | y = 0\}$. Since the equation $f(x) = 0$ has at most 3 integer roots, we find that $|G(2)| \leq 4$. $G(2)$ contains at least the elements O and $T(0,0)$ of G and its order is a power of 2 least or equal to 4, hence $|G(2)| \in \{2, 4\}$. $|G(2)| = 4$ if and only if there are 3 points of order 2 i.e. the equation $f(x) = 0$ has 3 integer solutions i.e. the equation $x^2 + ax + b = 0$ has 2 integer roots. The equation $x^2 + ax + b = 0$ has 2 integer roots if and only if $a^2 - 4b = c^2$ for some integer c. Note that $b^2(a^2 - 4b) \neq 0$ implies that $c \neq 0$ and that the roots of f are all distinct.

For $\varphi : G \to G'$ and $\psi : G' \to G$ defined as in 6.1.2, and for $\alpha : G \to \mathcal{Q}$ as defined in 6.1.4, we have:

$$|G/2G| = |G/\psi\varphi(G)| = |G/\psi(G')| \cdot |\psi(G')/\psi\varphi(G)| = |Im\alpha| \cdot |\psi(G')/\psi\varphi(G)|.$$

The kernel of the canonical map

$$G' \to \psi(G') \to \psi(G')/\psi\varphi(G)$$

is the set of elements $g' \in G'$ such that $\psi(g') \in \psi\varphi(G) \Leftrightarrow \psi(g') = \psi\varphi(g)$ for some $g \in G$. $\psi(g') = \psi\varphi(g) \Leftrightarrow g' - \varphi(g) \in \ker\psi \Rightarrow g' \in \varphi(G) + \ker\psi$. We have proved $\ker(G' \to \psi(G')/\psi\varphi(G)) \subset \varphi(G) + \ker\psi$. The reverse inclusion is obvious, hence $\ker(G' \to \psi(G')/\psi\varphi(G)) = \varphi(G) + \ker\psi$, and by the Fundamental Theorem of Isomorphism applied several times in many of its forms:

$$\frac{\psi(G')}{\psi\varphi(G)} \simeq \frac{G'}{\varphi(G) + \ker\psi} \simeq \frac{\frac{G'}{\varphi(G)}}{\frac{\varphi(G)+\ker\psi}{\varphi(G)}} \simeq \frac{\frac{G'}{\varphi(G)}}{\frac{\ker\psi}{\ker\psi \cap \varphi(G)}} \Rightarrow$$

$$|\frac{\psi(G')}{\psi\varphi(G)}| = |\frac{G'}{\varphi(G)}| : |\frac{\ker\psi}{\ker\psi \cap \varphi(G)}| = \frac{|Im\alpha'|}{s}$$

for $s = |\frac{\ker\psi}{\ker\psi \cap \varphi(G)}|$ and for $\alpha' : G' \to \mathcal{Q}$ a morphism defined similarly to α. We have proved in 6.1.2 that $\ker\psi = \{\bar{O}, \bar{T}\}$, hence $s \in \{1, 2\}$.

$s = 1 \Leftrightarrow \ker\psi = \ker\psi \cap \varphi(G) \Leftrightarrow \ker\psi \subset \varphi(G)$. $\bar{O} = \varphi(O)$ is automatically in $\varphi(G)$, therefore $\ker\psi \subset \varphi(G) \Leftrightarrow \bar{T} \in \varphi(G) \leftrightarrow \bar{T} \in \ker\alpha' \Leftrightarrow \widehat{\bar{b}} = \alpha'(\bar{T}) = \hat{1} \Leftrightarrow \bar{b} = a^2 - 4b$ is a perfect square.

$$|G/2G| = |Im\alpha| \cdot \frac{|Im\alpha'|}{s} \Rightarrow$$

$$2^r|G(2)| = 2^{r+\delta} = |G/2G| = \frac{|Im\alpha||Im\alpha'|}{s} \Rightarrow 2^r = \frac{|Im\alpha||Im\alpha'|}{s \cdot |G(2)|}.$$

$$\text{We have } s \cdot |G(2)| = \begin{cases} 1 \cdot 4, & \text{if } a^2 - 4b \text{ is a perfect square} \\ 2 \cdot 2, & \text{if } a^2 - 4b \text{ is not a perfect square} \end{cases} = 4 \Rightarrow$$

$$2^r = \frac{|Im\alpha| \cdot |Im\alpha'|}{4}.$$

We wish to find $Im\alpha$. Let $P(x, y) \in G$. By 2.2.5 there exist $m, n, e \in \mathbb{Z}$ such that $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, $e \neq 0$ and $gcd(m, e) = gcd(n, e) = 1$. The case $e = 0$ corresponds to $P = O$.

$$P \in G = C(\mathbb{Q}) \Rightarrow n^2 = m(m^2 + ame^2 + be^4).$$

Let $b_1 = \pm gcd(b, m) = \pm gcd(m, m^2 + ame^2 + be^4)$, where the sign is taken such that $\frac{m}{b_1}$ is a nonnegative integer. Then there exist $m_1 \in \mathbb{N}$ and $b_2 \in \mathbb{Z}$ such that $m = b_1 \cdot m_1$, $b = b_1 \cdot b_2$ and $gcd(m_1, b_2) = 1$.

$n^2 = b_1m_1(b_1^2m_1^2 + ab_1m_1e^2 + b_1b_2e^4) = b_1^2m_1(b_1m_1^2 + am_1e^2 + b_2e^4) \Rightarrow t^2 = m_1(b_1m_1^2 + am_1e^2 + b_2e^4)$ for an integer t such that $n = b_1t$. Since $gcd(m_1, b_1m_1^2+am_1e^2+b_2e^4) = gcd(m_1, b_2e^4) = gcd(m_1, e^4) = 1$ and $m_1 \geq 0$, we find that there exist $M, N \in \mathbb{Z}$ such that $m_1 = M^2$ and $b_1m_1^2 + am_1e^2 + b_2e^4 = N^2$.

$$gcd(m, e) = 1 \Rightarrow gcd(b_1, e) = gcd(M, e) = 1.$$

$$gcd(n, e) = 1 \Rightarrow gcd(t, e) = 1 \Rightarrow gcd(N^2, e) =$$

$$gcd(b_1m_1^2 + am_1e^2 + b_2e^4, e) = 1 \Rightarrow gcd(N, e) = 1.$$

$$1 = gcd(m_1, b_1m_1^2 + am_1e^2 + b_2e^4) = gcd(M^2, N^2) \Rightarrow gcd(N, M) = 1.$$

$$gcd(m_1, b_2) = 1 \Rightarrow gcd(M^2, b_2) = 1 \Rightarrow gcd(b_2, M) = 1.$$

If $P(x, y) \neq O, T$, we have $e \neq 0$ and $m \neq 0 \Rightarrow M \neq 0$, and:

$$\alpha(P) = \widehat{\frac{m}{e^2}} = \hat{m} = \widehat{b_1 \cdot M^2} = \hat{b}_1.$$

If $M = 0$, then $P = T \Rightarrow \alpha(P) = \hat{b}$. $\alpha(O) = \hat{1}$.

Conversely, if there exist $M, N, e, b_1, b_2 \in \mathbb{Z}$ such that:

$$\begin{cases} b_1M^4 + aM^2e^2 + b_2e^4 = N^2 \\ b_1b_2 = b \\ gcd(M, e) = gcd(M, N) = gcd(e, N) = gcd(b_2, M) = gcd(b_1, e) = 1 \end{cases}, \tag{6.2.1}$$

then $x = \frac{b_1M^2}{e^2}$ and $y = \pm\frac{b_1MN}{e^3}$ give a point $P \in G$ and $\alpha(P) = \hat{b}_1$.

Remark 6.2.1. *The conclusion is $q \in Im\alpha$ if and only if there exist $b_1, b_2 \in \mathbb{Z}$ such that $\hat{b}_1 = q$, $b_1 \cdot b_2 = b$ and there exists a solution M, N, e to the system 6.2.1.*

We have a similar result for $Im\bar{\alpha}$.

Notice that $\hat{1}$ and $\hat{b}$ are always in $Im\alpha$ as the images of O and T respectively. T corresponds to $b_1 = b$, $b_2 = 1$, $M = 0$, $N = \pm 1$ and $e = \pm 1$. O corresponds to $e = 0$, $b_1 = 1$, $N = \pm 1$ and $M = \pm 1$.

The remark 6.2.1 reduces determining $Im\alpha$ to finding solutions to systems of type 6.2.1. These are basically Diophantine equations, but we don't have to solve them, but find one solution subjected to the conditions in 6.2.1, or prove that the finite number of systems with the same $\hat{b}_1$ don't have solutions. We will see that this is not always an easy task as many problems on the subject are still left open.

Example 6.2.2. *Let's begin our examples by characterizing $C(\mathbb{Q}) : y^2 = x^3 - x$.*

Solution: We have seen, for example in 3.2.2, that the torsion group of $C(\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and as a set is $\{O, T, (1,0), (-1,0)\}$.

We now compute the rank r of $C(\mathbb{Q})$. We know $2^r = \frac{|Im\alpha| \cdot |Im\alpha'|}{4}$. We use 6.2.1 to determine $|Im\alpha|$ and $|Im\alpha'|$.

To find $|Im\alpha|$, we must solve the systems 6.2.1 for all $b_1 \cdot b_2 = b = -1$ i.e. $(b_1, b_2) \in \{(1,-1), (-1,1)\}$. The least we can say is $|Im\alpha| \leq 2$. But $\{\hat{1}, \widehat{-1}\} \subset Im\alpha$ and we get $|Im\alpha| = 2$.

$\bar{C}(\mathbb{Q}) : y^2 = x^3 + 4x$. We apply again 6.2.1 to find $|Im\alpha'|$. We must solve systems of type 6.2.1, but the equation is $b_1 M^4 + b_2 e^4 = N^2$ and $b_1 \cdot b_2 = \bar{b} = 4$. For the cases $(b_1, b_2) \in \{(-1,-4), (-2,-2), (-4,-1)\}$, the equation $b_1 M^4 + b_2 e^4 = N^2$ only has the trivial solution $(M, N, e) = (0, 0, 0)$ which fails the restriction $gcd(M, N) = 1$ in 6.2.1. The remaining cases $b_1 = b_2 = 2$ and $(b_1, b_2) \in \{(1,4), (4,1)\}$ are bound to give solutions as they correspond to $\hat{2}$ or $\hat{1}$ being in $Im\alpha'$, and $2^r = \frac{|Im\alpha'|}{2} \Rightarrow |Im\alpha'| \geq 2$. In conclusion $r = 0$ and $C(\mathbb{Q})$ is a torsion group isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

We have proved that the only rational solutions of the equation $y^2 = x^3 - x$ are $(0,0), (\pm 1, 0)$. ■

Example 6.2.3. *Our second example is a famous one, Euler's equation. Find the rational solutions of the equation $y^2 = x^3 + 1$.*

In the next lecture we will provide an elementary solution for it. Comparing the lengths and depths of the two proofs will show the strength of Nagell-Lutz's and Mordell-Weil's Theorems.

Proof: We will do more than finding the rational solutions. We will also characterize the abelian group $C(\mathbb{Q}) : y^2 = x^3 + 1$. The torsion points of $C(\mathbb{Q})$ are, as seen for example in 3.2.3, O, $(0, \pm 1)$, $(-1, 0)$ and $(2, \pm 3)$.

Because our proof for the Mordell-Weil Theorem and our algorithm for finding the rank of an elliptic curve are restricted to the assumption $T \in C(\mathbb{Q})$, we will first make the substitution $x \to x - 1$ to find the elliptic curve that we also denote $C(\mathbb{Q}) : y^2 = x^3 - 3x^2 + 3x$. We will prove that the rank r of $C(\mathbb{Q})$ is 0.

We first find $|Im\alpha|$. We have $a = -3$ and $b = 3$. The equations to solve in the systems 6.2.1, are $b_1 M^4 - 3M^2 e^2 + b_2 e^4 = N^2$ for $b_1 \cdot b_2 = 3$. We have seen that $\hat{1}, \hat{3}$ are in $Im\alpha$ as the images of O and T respectively. $\widehat{-1}$ and $\widehat{-3}$ are not as the associated equations only give the trivial solution $(M, N, e) = (0, 0, 0)$ which contradicts $gcd(N, M) = 1$. Therefore $|Im\alpha| = 2$.

For $|Im\alpha'|$ we have $\bar{a} = 6$ and $\bar{b} = -3$. Again $\hat{1}, \widehat{-3} \in Im\alpha'$. For $\hat{3}$ to be in $Im\alpha'$, the equation $3M^4 + 6M^2 e^2 - e^4 = N^2$ must have a solution satisfying the conditions in 6.2.1. Reducing mod 3 we find $-e^4 = N^2 (mod 3)$ which implies $3|e$ and $3|N$, thus contradicting $gcd(N, e) = 1$. Therefore $\hat{3} \notin Im\alpha'$ and similarly $\widehat{-1} \notin Im\alpha$. We have $|Im\alpha'| = 2$ and $r = 0$. It is not hard to prove that the rank of the elliptic curve associated to Euler's equation is also 0 and conclude that the only rational solutions of the equation are $(0, \pm 1)$, $(-1, 0)$ and $(2, \pm 3)$. ■

Corollary 6.2.4. *The only rational solutions of the equation* $1 + 2x^3 = y^3$ *are* $(0, 1)$ *and* $(-1, -1)$.

Proof: Let $\begin{cases} \frac{t-1}{2} = 2x^3 \\ \frac{t+1}{2} = y^3 \end{cases} \Rightarrow t^2 = (2xy)^3 + 1$. From Euler's equation we get $(2xy, t) \in \{(0, 1),\ (0, -1),\ (-1, 0),\ (2, 3),\ (2, -3)\}$.

$$t = 1 \Rightarrow x = 0, y = 1.$$

$t = -1 \Rightarrow 2x^3 = -1$ which has no rational solution. $t = 0$ and $2xy = -1$ is impossible. $t = 3 \Rightarrow y^3 = 2$ which has no rational solution.

$$t = -3 \Rightarrow x = -1, y = -1.$$

Therefore the only rational solutions to $1+2x^3 = y^3$ are $(0, 1)$ and $(-1, -1)$. ■

Corollary 6.2.5. *The only rational solution of the equation* $1 + 4x^3 = y^3$ *is* $(0, 1)$.

Proof: With the same notations and substitutions as in the previous corollary, we get $t^2 = (4xy)^3 + 1$, so

$$(4xy, t) \in \{(0, 1),\ (0, -1),\ (-1, 0),\ (2, 3),\ (2, -3)\}.$$

Modulo 4 we see that these possibilities restrict to $(4xy, t) \in \{(0, 1),\ (0, -1)\}$. This means $4xy = 0$. $y \neq 0$, otherwise we get a contradiction modulo 2 in $1 + 4x^3 = 0$, hence $x = 0$ and $y = 1$. ■

Chapter 7

Lecture VII

7.1 Euler's Equation

As an application to Mordell-Weil's Theorem and to Nagell-Lutz's Theorem, we have proved that the only rational solutions of the equation $y^2 = x^3 + 1$ are $(x, y) \in \{(0, \pm 1), (-1, 0), (2, \pm 3)\}$. It turns out that this diophantine equation is quite a famous one. It caries Euler's name as back to 1738, he was the first to find a proof, even though it turned out he made some mistakes. Based on Euler's ideas, we will give an elementary proof, free of the machinery that we have developed earlier.

The disadvantage of the elementary proof is that it is quite difficult and the ideas are not at all transparent. We will need the following statement which is apparently not connected to Euler's equation:

Proposition 7.1.1. *There are no integers $b, c \in \mathbb{N}^*$, $gcd(b, c) = 1$, $b \neq c$, $3 \not| c$ such that $bc(c^2 - 3bc + 3b^2)$ is a perfect square.*

Before proving the proposition, let's see how it applies to:

Theorem 7.1.2 (Euler(1738)). *The only rational solutions to $y^2 = x^3 + 1$ are $(x, y) \in \{(0, \pm 1), (-1, 0), (2, \pm 3)\}$.*

Proof: Assume for a contradiction that there exist $x, y \in \mathbb{Q}$ such that $y^2 = x^3 + 1$ and $x \notin \{-1, 0, 2\}$.

By 2.2.5 there exist $m, n, e \in \mathbb{Z}$, $e > 0$, $gcd(m, e) = gcd(n, e) = 1$ such that $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$. Then we have $\frac{n^2}{e^6} = \frac{m^3}{e^6} + 1 \Rightarrow n^2 = m^3 + e^6 = (m + e^2)(m^2 - me^2 + e^4)$. We now seek to apply 7.1.1. For this, we must first define b, c. Let $c = m + e^2$ and $b = e^2$. Then $m = c - b$ and $n^2 = c((c-b)^2 - (c-b)b + b^2) = c(c^2 - 2bc + b^2 - bc + b^2 + b^2) = c(c^2 - 3bc + 3b^2)$. Since b is a perfect square we get that $bc(c^2 - 3bc + 3b^2)$ is a square. Obviously $b > 0$. We have $c^2 - 3bc + 3b^2 = (c - \frac{3}{2}b)^2 + \frac{3}{4}b^2 > 0$. Since $c(c^2 - 3bc + 3b^2)$ is a perfect square we get $c \geq 0$. If $c = 0$, then $n^2 = c(c^2 - 3bc + 3b^2) = 0 \Rightarrow y = 0 \Rightarrow x = -1$ which contradicts our choice for x. Therefore $c > 0$.

$gcd(b,c) = gcd(m+e^2, e^2) = gcd(m, e^2) = 1$. If $b = c$, then $m = 0 \Rightarrow x = 0$ and we again contradict the choice for x. On applying 7.1.1 we find that the only possibility is $3|c$.

Let $c = 3d$, Then $(ne)^2 = 9bd(3d^2 - 3bd + b^2)$ implies that $bd(b^2 - 3bd + 3d^2)$ is a square. It is clear that $b, d \in \mathbb{N}^*$. Also $1 = gcd(b,c) = gcd(3d, b) \Rightarrow gcd(d,b) = 1$ and $3 \not| b$. Again by 7.1.1 the only possibility left is $b = d$. But $gcd(b,d) = 1$ implies $b = d = 1 \Rightarrow c = 3 \Rightarrow 1 = e^2 = b$ and $3 = c = m + e^2 \Rightarrow m = 2, e = 1 \Rightarrow x = 2$ which of course contradicts the choice of x.

Since obviously $\{(0, \pm 1), (-1, 0), (2, \pm 3)\}$ are all the solutions to $y^2 = x^3 + 1$ with $x \in \{-1, 0, 2\}$, we have finished solving Euler's equation. ■

Proof of 7.1.1: The main idea of the proof is Fermat's descent argument. Assume that there exists a solution with the required properties. Chose one for which b is minimal. We have $gcd(b, c^2 - 3bc + 3b^2) = gcd(b, c^2) = 1$ and $gcd(c, c^2 - 3bc + 3b^2) = gcd(c, 3b^2) = 1$. Since $bc(c^2 - 3bc + 3b^2)$ is a square and $b, c, c^2 - 3bc + 3b^2$ are pairwise coprime positive integers, they must all be squares. Hence there exists $k \in \mathbb{N}^*$ such that $c^2 - 3bc + 3b^2 = k^2$. Let $\frac{k+c}{b} = \frac{m}{n}$ with $gcd(m,n) = 1$, $m, n \in \mathbb{N}^*$. Then $k = \frac{m}{n}b - c$.

$c^2 - 3bc + 3b^2 = (\frac{m}{n}b - c)^2 \Leftrightarrow c^2 - 3bc + 3b^2 = \frac{m^2}{n^2}b^2 - 2\frac{m}{n}bc + c^2 \Leftrightarrow 3(b-c)n^2 = m^2 b - 2cmn \Leftrightarrow b(m^2 - 3n^2) = c(2mn - 3n^2) \Leftrightarrow \frac{b}{c} = \frac{2mn - 3n^2}{m^2 - 3n^2}$.

Let's prove that $m^2 - 3n^2 > 0 \Leftrightarrow \frac{m}{n} > \sqrt{3}$. This is equivalent to $\frac{k+c}{b} > \sqrt{3} \Leftrightarrow k > b\sqrt{3} - c$. If $b\sqrt{3} - c \leq 0$ then the inequality is obviously true. If $b\sqrt{3} - c > 0$ then the inequality is equivalent to $k^2 > (b\sqrt{3} - c)^2 = 3b^2 - 2\sqrt{3}bc + c^2 \Leftrightarrow c^2 - 3bc + 3b^2 > c^2 - 2\sqrt{3}bc + 3b^2 \Leftrightarrow 3 < 2\sqrt{3} \Leftrightarrow 9 < 12$ which holds.

$\frac{b}{c} = \frac{2mn - 3n^2}{m^2 - 3n^2}$ and $m^2 > 3n^2$ imply $2mn - 3n^2, m^2 - 3n^2 \in \mathbb{N}^*$.

Assume $3|m$. Then $m = 3l \Rightarrow \frac{b}{c} = \frac{2nl - n^2}{3l^2 - n^2}$ and $gcd(3l, n) = 1$. Assume there exists a prime number p such that $p|2ln - n^2$ and $p|3l^2 - n^2$. Then $p|n(2l - n)$ and $p|(3l^2 - n^2) - (2ln - n^2) = l(3l - 2n)$. These give four possibilities:

1. $p|gcd(n, l) = 1$;
2. $p|gcd(n, 3l - 2n) = gcd(n, 3l) = 1$;
3. $p|gcd(2l - n, l) = gcd(n, l) = 1$;
4. $p|gcd(2l - n, 3l - 2n) \Rightarrow p|2(2l - n) - (3l - 2n) = l \Rightarrow p|2l - (2l - n) = n \Rightarrow p|gcd(n, l) = 1$.

Since all cases lead to the contradiction $p|1$, $gcd(2ln - n^2, 3l^2 - n^2) = 1$. This, $gcd(b,c) = 1$, $(b, c, 2nl - n^2, 3l^2 - n^2 > 0)$ and $\frac{b}{c} = \frac{2nl - n^2}{3l^2 - n^2}$ imply

$\begin{cases} b = 2nl - n^2 = b_1^2 \\ c = 3l^2 - n^2 = c_1^2 \end{cases}$. Recall that b, c are squares. So we have $c_1^2 + n^2 = 3l^2$. It is well known that:

Remark 7.1.3. *If p is a prime number $p \equiv 3(mod 4)$ then $p|a^2+b^2 \Rightarrow p|a, p|b$ for all $a, b \in \mathbb{Z}$.*

Using this remark, we have $3|c_1$ and $3|n$ which contradicts $gcd(3l, n) = 1$. Actually, a descent argument proves that the only integer solutions of $c_1^2 + n^2 = 3l^2$ are $c_1 = n = l = 0$. The conclusion is $3 \not| m$. As in the case $3|m$, we prove $gcd(2mn - 3n^2, m^2 - 3n^2) = 1$. This implies $\begin{cases} b_1^2 = b = 2mn - 3n^2 \\ c_1^2 = c = m^2 - 3n^2 \end{cases}$.

Let $\frac{p}{q} = \frac{\pm c_1 + m}{n}$ such that $p, q \in \mathbb{N}^*$, $gcd(p, q) = 1$ and the sign is taken such that $3 \not| \pm c_1 + m$. Let's see that this choices are possible. We have $(m - c_1)(m + c_1) = m^2 - c_1^2 = m^2 - c = 3n^2 > 0 \Rightarrow m \pm c_1 > 0$, so we can chose positive p, q. Since $3 \not| m$, we cannot simultaneously have $3|m + c_1$ and $3|m - c_1$.

Let's see that (q, p) is a solution to the problem with $q < b$. If we prove this, then we contradict the minimality of b in the choice of (b, c) and we solve the problem.

We have $(n\frac{p}{q} - m)^2 = (\pm c_1)^2 = c = m^2 - 3n^2 \Rightarrow n(\frac{p}{q})^2 - 2m\frac{p}{q} = -3n \Rightarrow np^2 - 2mpq + 3nq^2 = 0 \Rightarrow \frac{m}{n} = \frac{p^2+3q^2}{2pq}$. $\frac{b}{n^2} = \frac{2mn-3n^2}{n^2} = 2\frac{m}{n} - 3 = \frac{p^2+3q^2}{pq} - 3 = \frac{p^2-3pq+3q^2}{pq} \Rightarrow pq(p^2 - 3pq + 3q^2) = (pq\frac{b_1}{n})^2 \Rightarrow pq(p^2 - 3pq + 3q^2)$ is a perfect square and $n|pqb_1$.

$p = q \Rightarrow \frac{m}{n} = \frac{p^2+3q^2}{2pq} = 2 \Rightarrow m = 2n$. Since $gcd(m, n) = 1$, we get $n = 1$, $m = 2$. But then $c = 1$ and $b = 1$ contradicting $b \neq c$. Therefore $p \neq q$.

We now prove $q < b$. Assume for a contradiction $q \geq b$. We have $2mpq = n(p^2 + 3q^2) \Rightarrow q|n(p^2 + 3q^2)$. $gcd(p, q) = 1 \Rightarrow gcd(q, p^2 + 3q^2) = 1 \Rightarrow q|n$. $b = 2mn - 3n^2 \Rightarrow n|b$. So $q|n|b$. This and $q \geq b$ imply $q = n = b$. Then $\frac{m}{n} = \frac{p^2+3q^2}{2pq} \Rightarrow m = \frac{p^2+3q^2}{2p} \Rightarrow 2pm = p^2 + 3q^2 \Rightarrow p|3q^2$. But our choices for p, q prove $gcd(p, 3q) = 1$, hence $p = 1 \Rightarrow m = \frac{3q^2+1}{2}$. $n = b = 2mn - 3n^2 \Rightarrow 1 = 2m - 3n \Rightarrow m = \frac{3n+1}{2}$. $\frac{3n+1}{2} = m = \frac{3n^2+1}{2} \Rightarrow n = n^2 \Rightarrow n = 1 \Rightarrow b = 1 \Rightarrow m = 2 \Rightarrow c = 1$. We again contradict $b \neq c$. So (q, p) is also a solution of the problem with $q < b$ contradicting the minimality of b among the solutions of the problem. ■

7.2 Computing the rank of nonsingular elliptic curves

We give more examples of how to compute the rank of an elliptic curve. The setting is:

$C(\mathbb{Q})$ is the smooth rational elliptic curve given by $y^2 = x^3 + ax^2 + bx$ with $a, b \in \mathbb{Z}$. This amounts to $b(a^2 - 4b) \neq 0$. Let $O = [0 : 1 : 0]$ be the

point at infinity of $C(\mathbb{Q})$ and let $T = (0,0)$. Let $\tilde{C}(\mathbb{Q})$ be the smooth rational elliptic curve given by $y^2 = x^3 + \bar{a}x^2 + \bar{b}x$ with $\bar{a} = -2a$ and $\bar{b} = a^2 - 4b$.

Let $\alpha : C(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ be defined by

$$\alpha(P) = \begin{cases} \hat{x}, & \text{if } P = (x,y) \neq (0,0), O \\ \hat{b}, & \text{if } P = T(0,0) \\ \hat{1}, & \text{if } P = O \end{cases} .$$

We have proved that α is a group morphism. Similarly we define α' for $\tilde{C}(\mathbb{Q})$. We have proved that $2^r = \frac{|Im\alpha||Im\alpha'|}{4}$, where r is the rank of $C(\mathbb{Q})$.

We have seen that finding $Im\alpha$ (or $Im\alpha'$) amounts to finding solutions for equations of the form:

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4$$

with the numerous but important conditions: $b_1b_2 = b$, $1 = gcd(M,e) = gcd(M,N) = gcd(e,N) = gcd(b_2,M) = gcd(b_1,e)$. We say that the equation above is associated to b_1 and we call one of its solutions "good" if it verifies "the numerous conditions". We have seen that a "good" solution to the equation above corresponds to the point $P(x,y) = (\frac{b_1M^2}{e^2}, \frac{b_1MN}{e^3})$ ($P = O$ if $e = 0$) on $C(\mathbb{Q})$ such that $\alpha(P) = \hat{b}_1$. Conversely, $\hat{l} \in Im\alpha$ if and only if there exists b_1 like above with $\hat{b}_1 = \hat{l}$ such that the associated equation has a "good" solution. The equations for α' change accordingly.

Example 7.2.1. *Let $C(\mathbb{Q})$ be the smooth rational elliptic curve given by $y^2 = x^3 + x$. Compute the rank of $C(\mathbb{Q})$.*

Solution: $\tilde{C}$ is given by $\tilde{C} : y^2 = x^3 - 4x$, $\bar{a} = 0$, $\bar{b} = -4$.
We first compute $|Im\alpha|$. Since $b = 1$, there are only two cases to consider:

1. $b_1 = b_2 = 1$. $\hat{1}$ is always in the image of α as $\alpha(O)$.
2. $b_1 = b_2 = -1$. The associated equation $N^2 = -M^2 - e^4$ obviously has only the solution $(N,M,e) = (0,0,0)$, which does not verify "the numerous" conditions. So $\widehat{-1} \notin Im\alpha$.

We have proved that $|Im\alpha| = 1$.

We now compute $|Im\alpha'|$. $\bar{b} = -4$ and it seems like there is a bit more work to be done. The cases to consider are $b_1 \in \{\pm 4, \pm 2, \pm 1\}$. Since $\hat{4} = \hat{1}$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ we have only to consider the possibilities $b_1 \in \{\pm 2, \pm 1\}$. This means that $|Im\alpha'| \leq 4$. On the other hand, $4||Im\alpha||Im\alpha'| = |Im\alpha'|$. These imply $|Im\alpha'| = 4 \Rightarrow r = 0$.

The rank of $C(\mathbb{Q})$ being 0, $C(\mathbb{Q})$ must be a torsion group. We have seen in 3.2.2 that the torsion points of $C(\mathbb{Q})$ are T and O. Combining our results we have proved:

Theorem 7.2.2. *The only rational solutions to the equation $y^2 = x^3 + x$ are $(x,y) = (0,0)$.*

Corollary 7.2.3. *If N, M, e are rational numbers such that $N^2 = M^4 + e^4$, then $e = 0$ or $M = 0$.*

Proof: If $e \neq 0$, then $x = \frac{M^2}{e^2}$ and $y = \frac{MN}{e^3}$ define a point on $C(\mathbb{Q})$: $y^2 = x^3 + x$. By the previous theorem, we get $(x, y) = (0, 0) \Rightarrow M = 0$. ■

As a consequence of this corollary we have Fermat's Theorem for exponent 4:

Theorem 7.2.4. *All the integer solutions to the equation $X^4 + Y^4 = Z^4$ satisfy $XYZ = 0$.*

7.2.1 The curves C_p

This subsection is entirely devoted to the special class of elliptic curves $\{C_p(\mathbb{Q})|p \text{ is a prime number}\}$.

Definition 7.2.5. *Let p be a prime number. $C_p(\mathbb{Q})$ is the elliptic curve given by $y^2 = x^3 + px$.*

Remark 7.2.6. *If p is a prime number, then C_p is smooth. This is because $C_p : y^2 = f(x) = x^3 + ax^2 + bx = x^3 + px$ and $\Delta_f = b(a^2 - 4b) = -4p^2 \neq 0$. The curve $\tilde{C}_p$ is given by $\tilde{C}_p : y^2 = x^3 - 4px$, $\bar{a} = 0$ and $\bar{b} = -4p$.*

Theorem 7.2.7. *If p is a prime number, then $rank(C_p(\mathbb{Q})) \leq 2$.*

Proof: We have $b = p$, so the elements of $Im\alpha$ are given by the solvability of the equations we have seen before for $b_1 \in \{\pm 1, \pm p\}$. $b_1 \in \{-1, -p\}$ don't give points in the image of α because the associated equations $N^2 = -M^2 - pe^4$ and $N^2 = -pM^2 - e^4$ only have the trivial solution $(0, 0, 0)$. On the other hand, $\hat{1} = \alpha(O)$ and $\hat{p} = \alpha(T(0, 0))$. These prove that $|Im\alpha| = 2$.

$\bar{b} = -4p$. To find $Im\alpha'$ we must solve equations for

$$b_1 \in \{\pm 1, \pm 2, \pm 4, \pm p, \pm 2p, \pm 4p\}.$$

Since $\hat{4} = \hat{1}$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, we need only consider the 8 cases $\{\widehat{\pm 1}, \widehat{\pm 2}, \widehat{\pm p}, \widehat{\pm 2p}\}$. Therefore $|Im\alpha'| \leq 8 \Rightarrow 2^r = \frac{|Im\alpha||Im\alpha'|}{4} \leq \frac{2 \cdot 8}{4} = 4 \Rightarrow r \leq 2$. ■

Proposition 7.2.8. *If p is a prime number, $p \equiv 7, 11 (mod 16)$, then $rank(C_p(\mathbb{Q})) = 0$.*

Proof: We have seen that $|Im\alpha| = 2$ and we know that $\hat{1}$ and $\widehat{-4p} = \widehat{-p}$ are in $Im\alpha'$ as the images of $\tilde{O} = O$ and $\tilde{T} = T$. Since $2^r = \frac{|Im\alpha||Im\alpha'|}{4}$, we only have to prove that the associated equations for $b_1 \in \{-1, \pm 2, p, \pm 2p\}$ don't provide elements in $Im\alpha'$.

Let's assume we have proved that none of the elements $\widehat{-1}, \widehat{\pm 2}$ is in $Im\alpha'$. Since α' is a group homomorphism, $Im\alpha'$ is a group. If $\hat{p} \in Im\alpha'$, then $\widehat{-1} = \widehat{-p^2} = \widehat{-p} \cdot \hat{p} \in Im\alpha'$ which is a contradiction. If $\widehat{\pm 2p} \in Im\alpha'$, then $\widehat{\mp 2} = \widehat{\mp 2p^2} = \widehat{-p} \cdot \widehat{\pm 2p} \in Im\alpha'$ which again would be a contradiction.

If $b_1 = -1$ the associated equation is $N^2 = -M^4 + 4pe^4$. We have $p|N^2 + M^4$ and $p \equiv 3(mod4)$ implying that $p|gcd(M,N) = 1$ which is a contradiction. Similarly we treat the case $b_1 = -4$. Therefore $\widehat{-1} \notin Im\alpha'$.

If $b_1 = 2$, the associated equation is $N^2 = 2M^4 - 2pe^4$.

If $p \equiv 11(mod16)$, then we have $N^2 \equiv 2M^4(modp)$. If $p \not| MN$, then 2 must be a quadratic residue mod p. But the Legendre symbol, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$ if $p \equiv 3, 5(mod8)$ which happens since $p \equiv 11(mod16) \Rightarrow p \equiv 3(mod8)$. But $\left(\frac{2}{p}\right) = -1 \Rightarrow 2$ is not a quadratic residue. The other possibility $p|MN$ is easily seen to contradict $gcd(M,N) = 1$.

If $p \equiv 7(mod16)$, then $N^2 = 2M^4 - 2pe^4 \Rightarrow N = 2n$ for some integer n. Substituting in the equation and reducing by 2 we get $2n^2 = M^4 - pe^4$. It is easy to see that being coprime, both M and N must be odd. If x is an odd number, then $x-1, x+1, x^2+1$ are all even numbers and exactly one of the numbers $x \pm 1$ is divisible by 4. The conclusion is $16|x^4 - 1 = (x-1)(x+1)(x^2+1) \Rightarrow x^4 \equiv 1(mod16)$. $2n^2 = M^4 - pe^4 \Rightarrow 2n^2 \equiv 1 - 7 = -6(mod16) \Rightarrow n^2 \equiv -3(mod16) \Rightarrow n^2 \equiv -3(mod8)$ which is a contradiction because $x^2 \equiv 0, 1, 4(mod8)$ for all integers x. We have proved $\hat{2} \notin Im\alpha'$.

If $b_1 = -2$, then the associated equation is $N^2 = -2M^4 + 2pe^4$.

If $p \equiv 7(mod16)$, then -2 is not a square mod p and we treat this case similarly to the previous one.

If $p \equiv 11(mod16)$, then like for $b_1 = 2$ we reach to the contradiction $n^2 \equiv 5(mod16)$.

We have proved that $\widehat{b_1} \in \{\widehat{-1}, \widehat{\pm 2}\}$ are not in $Im\alpha'$, therefore $|Im\alpha'| = 2 \Rightarrow r = 0$. ■

Proposition 7.2.9. *If p is a prime number, $p \equiv 3, 5, 13, 15(mod16)$, then $rank(C_p(\mathbb{Q})) \leq 1$.*

It is conjectured that in these cases, $rank(C_p(\mathbb{Q})) = 1$.

Proof: We have $\tilde{C} : y^2 = x^3 - 4px$, $\bar{b} = -4p$. We have seen that $|Im\alpha| = 2$ and $|Im\alpha'| \leq 8$. All we have to prove is $|Im\alpha'| \leq 4$. Because $Im\alpha'$ is a subgroup, all that we actually have to prove is that not all of the equations associated to $b_1 \in \{\pm 1, \pm 4, \pm 2, \pm p, \pm 4p \pm 2p\}$ give elements in $Im\alpha'$. This is because the set above gives 8 elements in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

If $p \equiv 3, 15(mod16)$, then $p \equiv 3(mod4)$ and then $N^2 = -M^4 + 4pe^4 \Rightarrow -1$ is a quadratic residue mod p or $p|gcd(M,N)$. These contradict $p \equiv 3(mod4)$ or $gcd(M,N) = 1$. So $\widehat{-1} \notin Im\alpha'$ (the case $b_1 = -4$ is dealt with similarly).

If $p \equiv 5, 13(mod16)$, then $p \equiv 5(mod8)$ and $\left(\frac{-2}{p}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2}} = -1$ if $p \equiv 5, 7(mod8)$. The equation for $b_1 = -2$ is $N^2 = -2M^4 + 2pe^4$. Just as before this implies that -2 is a quadratic residue mod p, or $p|gcd(M,N)$. These contradict $p \equiv 5(mod8)$ or $gcd(M,N) = 1$. Therefore $\widehat{-2} \notin Im\alpha'$. ■

Example 7.2.10. *As an example to the conjecture stated before, let's consider the case $p = 13$.*

Solution: If $b_1 = -4$ then we have the solution $(N, M, e) = (3, 1, 1)$, so $\widehat{-4} = \widehat{-1} \in Im\alpha'$. Since $\{\hat{1}, \widehat{-4}, \widehat{-13}\} \in Im\alpha'$ and $Im\alpha'$ is a group, $|Im\alpha'| \geq 4$. This proves $r \geq 1$. Combining with the previous proposition we get $r = 1$. ■

Example 7.2.11. *$rank(C_{73}(\mathbb{Q})) = 2$.*

Solution: $(N, M, e) = (3, 4, 1)$ provides a solution for $b_1 = -4$. Therefore $\widehat{-4} = \widehat{-1} \in Im\alpha'$. $(N, M, e) = (12, 1, 1)$ provides a solution for $b_1 = -2$, so $\widehat{-2} \in Im\alpha'$. We know $\hat{1}, \widehat{-292} = \widehat{-73} \in Im\alpha'$. It is easy to see that these four elements generate a group with 8 elements, hence $|Im\alpha'| = 8$ and then $r = 2$. ■

Remark 7.2.12. *It can be proved that $rank(C_p(\mathbb{Q})) = 0$ for $p = 17$ or $p = 41$. An interesting example that dampens our hopes in finding an algorithm for determining the rank of $C(\mathbb{Q})$, that would be based on solving equations like we did this section, is given by the equation associated to $b_1 = 17$ if $p = 17$. This equation, $N^2 = 17M^4 - 4e^4$, has a solution modulo any prime number q, but has no solution in integers.*

7.3 Stories and conjectures about the rank of an elliptic curve

The stories that follow can be found in A. Wiles's description of the Birch and Swinnerton-Dyer conjecture on Claymath's Web site.

7.3.1 Congruent numbers

A positive integer d is called a *congruent number* if there exist positive rational numbers a, b, c that are the side lengths of a right triangle with area d. A connection of congruent numbers with elliptic curves is given by the following result:

Proposition 7.3.1. *$d \in \mathbb{N}^*$ is a congruent number if and only if the equation $y^2 = x^3 - d^2x$ has integer solutions with $y \neq 0$.*

Proof: Obviously we can reduce to the case when d is square-free. Since $d \neq 0$, $C(\mathbb{Q}) : y^2 = x^3 - d^2x$ is a smooth elliptic curve. As an easy consequence of Nagell-Lutz's Theorem it can be proved that the only torsion points of $C(\mathbb{Q})$ are $\{O[0:1:0],\ (0,0),\ (\pm d, 0)\}$ if d is square-free. Therefore proving the proposition is equivalent to proving that $rank(C(\mathbb{Q})) \geq 1$. This reveals the connection of this problem with the theory of elliptic curves. However we give an elementary proof for it.

Let x, y be rational number with $y \neq 0$ and $y^2 = x^3 - d^2x$. Let $a = \left|\frac{x^2-d^2}{y}\right|$, $b = \left|\frac{2xd}{y}\right|$ and $c = \left|\frac{x^2+d^2}{y}\right|$. Then $a^2 + b^2 = c^2$, so a, b, c are the sides of a right triangle whose area is $\left|\frac{2xd(x^2-d^2)}{2y^2}\right| = d \cdot \left|\frac{x^3-d^2x}{y^2}\right| = d$.

Conversely, assume d is a congruent number and let $a, b, c \in \mathbb{Q}_+^*$ such that $a^2 + b^2 = c^2$ and $ab = 2d$. Set $x = \frac{1}{2} \cdot a(a-c)$ and $y = \frac{1}{2} \cdot a^2(a-c)$. It is easy to prove that $y \neq 0$.

$$y^2 = \frac{a^4(a-c)^2}{4}$$

$$x^3 - d^2x = \frac{a^3(a-c)^3}{8} - \frac{a(a-c)d^2}{2} =$$

$$= \frac{a^3(a-c)^3 - a(a-c)a^2b^2}{8} = a^3(a-c) \cdot \frac{(a-c)^2 - b^2}{8} =$$

$$= a^3(a-c)\frac{a^2 - 2ac + c^2 - b^2}{8} = a^3(a-c)\frac{a^2 - 2ac + a^2}{8} = \frac{a^4(a-c)^2}{4}$$

So $y^2 = x^3 - d^2x$ and $y \neq 0$. ■

Example 7.3.2. *6 and 5 are congruent numbers.*

Solution: For $d = 6$ we can take $a = 3$, $b = 4$ and $c = 5$.

For $d = 5$ we can take $a = \frac{3}{2}$, $b = \frac{20}{3}$ and $c = \frac{41}{6}$. History assigns the proof of 5 being a congruent number to Fibonacci. ■

The weak form of Birch and Swinnerton-Dyer conjecture you can read about in the next subsection implies that every positive integer congruent modulo 8 to 5,6 or 7 is a congruent number.

Theorem 7.3.3 (Tunnel). *Let d be an odd, square-free positive integer. Then d is a congruent number if and only if*

$$|\{(x,y,z) \in \mathbb{Z}^3 |\ 2x^2+y^2+8z^2 = d\}| = 2 \cdot |\{(x,y,z) \in \mathbb{Z}^3 |\ 2x^2+y^2+32z^2 = d\}|.$$

7.3.2 The Birch and Swinnerton-Dyer Conjecture

It is an important problem to determine if there are infinitely many rational solutions (x, y) to the equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$.

If $C(\mathbb{Q}) : y^2 = x^3 + ax + b$ is not smooth i.e. $f(x) = x^3 + ax + b$ has multiple complex roots, then it can be proved that $C(\mathbb{Q})$ has infinitely many rational points. For this, consider a line l in $\mathbb{A}^3$ that has an equation with rational coefficients. Then let α be a multiple root of f. It follows that $\alpha \in \mathbb{Q}$. Consider the point with rational coordinates $P(\alpha, 0) \in C(\mathbb{Q})$. For every point Q with rational coordinates on l, prove that the line PQ intersects C again in a point of rational coordinates i.e. in a point of $C(\mathbb{Q})$. Since there are infinitely many rational points on l, we conclude that $C(\mathbb{Q})$ is infinite.

Therefore we can consider the following problem: When is $C(\mathbb{Q})$ infinite?

In 1901 *Poincare* gave the abelian group structure on $C(\mathbb{Q})$. In 1922 *Mordell* completed a version of the Mordell-Weil Theorem that proved $C(\mathbb{Q})$

is a finitely generated abelian group. Mordell's result and *Nagell-Lutz's Theorem* proves that $C(\mathbb{Q})$ is infinite if and only if $rank(C(\mathbb{Q})) \geq 1$.

But how to decide whether the rank of an elliptic curve is greater or equal to one? No one knows for sure, but an idea is to find a connection between the rank of the elliptic curve and the number of "mod p points" of $C(\mathbb{Q})$ for every prime number p for which this makes sense. Let's make the terms more clear.

In the beginning of the third Lecture we have proved that if p is a prime number such that $p \nmid 2\Delta_f$, where $C(\mathbb{Q}) : y^2 = f(x)$, $f = x^3+ax^2+bx+c$ and $a, b, c \in \mathbb{Z}$, then it makes sense to define $C(\mathbb{Z}_p)$ which is also a group. In our case, $f = x^3 + ax + b$. These mean that except for a finite number of prime numbers, we can define $C(\mathbb{Z}_p)$ and give it an abelian group structure. For these primes p, define $N(p) = |C(\mathbb{Z}_p)|$. A result concerning these numbers, $N(p)$, is:

Theorem 7.3.4 (Hasse-Weil). *If p is a prime number such that $p \nmid 2\Delta_f$, then:*

$$|p + 1 - N(p)| \leq 2\sqrt{p}.$$

Similarly to the definition of Riemann's function

$$\zeta(s) = \sum_{i=1}^{\infty} \frac{1}{n^s} = \prod_p \left(\frac{1}{1 - \frac{1}{p^s}} \right),$$

for $\Re e(s) > 1$, where the product is taken over all the prime numbers, the following function was introduced:

$$L(C, s) = \prod_{p \nmid 2\Delta_f,\ p \textbf{ is prime}} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}} \right)^{-1},$$

where $a_p = p+1-N_p$. It can be proved that $L(C, s)$ converges for $\Re e(s) > \frac{3}{2}$. *Hasse* conjectured that $L(C, s)$ has a holomorphic extension to $\mathbb{C}$. In 1999, *Taylor, Breuil, Conrad and Diamond* proved Hasse's Conjecture.

A weak form of The Birch and Swinnerton-Dyer Conjecture states:

Conjecture 7.3.5. *$C(\mathbb{Q})$ is infinite if and only if $L(C, 1) = 0$.*

This means that to find out if $C(\mathbb{Q})$ is infinite, it is enough to compute $L(C, 1)$ and see if it is 0. Roughly speaking, $L(C, 1) = \left(\prod_p \frac{N(p)}{p} \right)^{-1} = \prod_p \frac{p}{N(p)}$. The strong version of the conjecture would give even more information on $C(\mathbb{Q})$.

Conjecture 7.3.6 (Birch and Swinnerton-Dyer). *The order of 1 as a zero of $L(C, s)$ is $r = rank(C(\mathbb{Q}))$.*

Using results of *Wiles, Coates (1977)* and *Zagier, Gross (1983)*, *Kolyvagin* proved in 1990 that for *modular* elliptic curves the following hold:

$$L(C,1) \neq 0 \Rightarrow rank(C(\mathbb{Q})) = 0$$

$$L(C,1) = 0 \text{ and } L'(C,1) \neq 0 \text{ imply that } rank(C(\mathbb{Q})) = 1.$$

You may not know what a modular elliptic curve is, but in 1994, while solving Fermat's Last Theorem, *A. Wiles* proved that every elliptic curve is modular.

Chapter 8

Lecture VIII

In this lecture we give a complete proof to the Mordell-Weil Theorem. This proof is not elementary and some knowledge in Algebraic Number Theory is required.

8.1 Algebraic Number Theory Prerequisites

Definition 8.1.1. *A number field is an algebraic extension $\mathbb{Q} \subset K$ of finite degree.*

Let K be a number filed with $[K : \mathbb{Q}] = n$. K is an algebraic extension of $\mathbb{Q}$, hence every element of K is a root of a polynomial with rational coefficients. By multiplying the coefficients of the polynomial by a convenient nonzero integer, we can assume that all of them are integers. An element of K is called integral if it is root to a monic polynomial with integer coefficients.

Proposition 8.1.2. *Let A be the set of integral elements of K. Then:*

1. *A is a ring with quotient field K. A is called the ring of integers of K. Any element of K can be written as $\frac{a}{m}$ with $a \in A$ and $m \in \mathbb{Z}^*$.*
2. *A is a free abelian group of rank n. Any basis for A as a free abelian group is also a basis for K as a vector space over $\mathbb{Q}$.*
3. *Any nonzero prime ideal of A is maximal.*
4. *Any nonzero ideal in A decomposes uniquely, up to the order of factors, as a product of prime ideals.*
5. *If I is a nonzero ideal of A, then $N(I) \stackrel{def}{=} |A/I|$ is a finite positive integer. It is called the norm of the ideal I.*

   We have $N(I \cdot J) = N(I) \cdot N(J)$ for all nonzero ideals I, J of A.

If $x \in K$, then we can define the norm $N(x)$ of x over $\mathbb{Q}$ as the product of all the conjugates of x i.e. the product of all the distinct complex roots of the irreducible polynomial of x over $\mathbb{Q}$. It can be proved that $N(xA) = |N(x)|^{[K:\mathbb{Q}(x)]}$.

6. *If $I, J \leq A$ are nonzero ideals of A, then $I \subset J \Leftrightarrow J|I$ i.e. there exists an ideal L of A such that $J \cdot L = I$.*

7. *It can be proved that $N(I) \in I$ which implies $I|\ N(I) \cdot A$.*

8. *If P is a nonzero prime ideal of A, then it is maximal, so A/P is a field. This means $N(P) = p^k$ for some prime number p and some $k \in \mathbb{N}$. Since $N(P) \in P$, $p^k \in P$ and since P is a prime ideal, $p \in P$, so $P|\ pA$.*

   This can be used to prove that every ideal whose norm is a power of a prime number p is a product of prime ideals dividing pA and every ideal whose norm is not a prime power is not prime.

9. *If $I, J \leq A$ and $I, J \neq (0)$, we say $I \equiv J$ if and only if there exist $a, b \in A^*$ such that $aI = bJ$. " $\equiv$ " is an equivalence relation on the set of nonzero ideals of A and the factor set $\mathcal{C} = \{I \leq A | I \neq (0)\}/\equiv$ inherits a group structure from the multiplication of ideals. This means that if we set $\hat{I} \cdot \hat{J} \stackrel{def}{=} \widehat{I \cdot J}$, this is a well defined operation on $\mathcal{C}$ such that $(\mathcal{C}, \cdot)$ is a group. The neutral element is the class $\hat{1}$ of all principal ideals of A. We sometimes use the notation $I \equiv J (mod\ PrA)$ to say that I and J have equal classes in $\mathcal{C}$.*

Probably the most famous examples of rings of integers are the rings of integers associated to quadratic extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{d}) = K$ with d a square free integer, $d \neq 1$. The integral elements of K are:

$$A = \begin{cases} \mathbb{Z}[\sqrt{d}], & \text{if } d \equiv 2, 3 (mod 4) \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}], & \text{if } d \equiv 1 (mod 4) \end{cases}.$$

For any two ideals I and J of A, not both 0, there exists the greatest common divisor $gcd(I, J)$ of I and J defined just like for integers by $gcd(I, J) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot \ldots \cdot p_k^{\min\{\alpha_k, \beta_k\}}$ if $I = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ and $J = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$ with $p_1, \ldots, p_k$ distinct prime ideals of A and $\alpha_i, \beta_i \in \mathbb{N}$ for all $i = \overline{1, k}$. Since $I \subset I+J$ and $J \subset I+J$, $I+J|I$ and $I+J|J$, hence $I+J|gcd(I, J)$. Conversely $gcd(I, J)|I$ and $gcd(I, J)|J$ imply $gcd(I, J)|I + J$, so $gcd(I, J) = I + J$. In particular, I and J are coprime if and only if $I + J = A$. We see that the ideals of the ring of integers of a number field have similar properties to the integers in $\mathbb{Z}$.

Theorem 8.1.3 (Dirichlet). *$\mathcal{C}$ is a finite abelian group.*

Proposition 8.1.4. *A is factorial if and only if $|\mathcal{C}| = 1$ if and only if A is a principal ideal domain.*

Theorem 8.1.5 (Dirichlet). *Denote by $U(A)$ the group of invertible elements of A. Then $U(A)$ is a finitely generated abelian group.*

By the Structure Theorem for Finitely Generated Abelian Groups, $U(A) \simeq \mathbb{Z}^r \times W$, where W is the torsion part of $U(A)$. W is the set of roots of unity of K and it can be shown that it is cyclic. We can also determine r. There exist exactly n distinct field embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$, $i = \overline{1,n}$. Of these field morphisms, some are real (the image is a subfield of $\mathbb{R}$), and the rest can be coupled in pairwise complex conjugate homomorphisms. Let s be the number of real embeddings, and 2t the number of remaining complex homomorphisms. Then

$$\begin{cases} s + 2t = n \\ s + t - 1 = r \end{cases}.$$

Let's evaluate the strength of this result by applying it to Pell's equation. Let $K = \mathbb{Q}(\sqrt{d})$ with d a square free integer, $d \neq 1$. Then $[K : \mathbb{Q}] = 2$ and the two field embeddings of K in $\mathbb{C}$ are completely characterized by

$$\begin{cases} \sigma_1(\sqrt{d}) = \sqrt{d} \\ \sigma_2(\sqrt{d}) = -\sqrt{d}. \end{cases}.$$

If $d < 0$, then there are no real embeddings, hence $s = 0 \Rightarrow t = 1 \Rightarrow r = 0 \Rightarrow U(A) = W$. It can be proven:

$$W = \begin{cases} \{\pm 1, \pm i\}, & \text{if } d = -1 \\ \{\pm 1, \frac{\pm 1 \pm \sqrt{3}}{2}, & \text{if } d = -3 \\ \pm 1, & \text{elsewhere} \end{cases}.$$

If $d > 0$, then both σ_1 and σ_2 are real, therefore $s = 2 \Rightarrow t = 0 \Rightarrow r = 1$ implying that $U(A)$ is of rank 1. Since the only roots of unity in K are ± 1, we find

$$U(A) = \{\pm \varepsilon^n | \varepsilon \in U(A), \varepsilon \neq \pm 1\},$$

for some $\varepsilon \in A$.

8.2 Completing the proof of Mordell-Weil's Theorem

We are now ready to tackle the complete proof of Mordell-Weil's Theorem. We have seen, for example in the proof of the existence of a Weierstrass normal form, that any elliptic curve is projectively equivalent to a an elliptic curve $C(\mathbb{Q})$ given by an equation of the form $y^2 = x^3 + ax + b = f(x)$ with $a, b \in \mathbb{Z}$ and $\Delta_f = -4a^3 - 27b^2 \neq 0$.

Theorem 8.2.1 (Mordell-Weil). *Let $C(\mathbb{Q})$ be the elliptic curve given by $y^2 = f(x) = x^3 + ax + b$ with $a, b \in \mathbb{Z}$ and $\Delta_f = -4a^3 - 27b^2 \neq 0$.*

Then the abelian group $C(\mathbb{Q})$ is finitely generated.

We have seen that Mordell-Weil's Theorem is equivalent to the weak Mordell-Weil Theorem:

Theorem 8.2.2. $|C(\mathbb{Q}) : 2C(\mathbb{Q})| < \infty$.

We have proved this theorem elementarily, but only in the particular case $C(\mathbb{Q})$ had at least a point of order 2.

Let θ_1, θ_2 and θ_3 be the complex roots of f. Because $\Delta_f \neq 0$, all θ's are distinct. Let

$$U = U(\mathbb{Q}(\theta_1) \times \mathbb{Q}(\theta_2) \times \mathbb{Q}(\theta_3)),$$

where $U(A)$ denotes the multiplicative group of units of a ring A.

Define $\varphi : C(\mathbb{Q}) \to U/U^2$ by

$$\varphi(P) = \begin{cases} \hat{1}, & \text{if } P = O \\ (f'(\theta_1), \widehat{\theta_1 - \theta_2}, \theta_1 - \theta_3), & \text{if } P = (\theta_1, 0) \\ (\theta_2 - \theta_1, \widehat{f'(\theta_2)}, \theta_2 - \theta_3), & \text{if } P = (\theta_2, 0) \\ (\theta_3 - \theta_1, \widehat{\theta_3 - \theta_2}, f'(\theta_3)), & \text{if } P = (\theta_3, 0) \\ (\alpha - \theta_1, \widehat{\alpha - \theta_2}, \alpha - \theta_3), & \text{if } P = (\alpha, \beta),\ \beta \neq 0 \end{cases}.$$

If $P = (\alpha, \beta) \in C(\mathbb{Q})$ and $\beta \neq 0$, then $(\alpha-\theta_1)(\alpha-\theta_2)(\alpha-\theta_3) = f(\alpha) = \beta^2 \neq 0$ implies that $\alpha - \theta_i$ are nonzero elements of $\mathbb{Q}(\theta_i)$ for all $i = \overline{1,3}$ and $\varphi(P)$ is a well defined element of U/U^2. If $P = (\theta_1, 0) \in C(\mathbb{Q})$, then $\theta_1 \in \mathbb{Q}$ and $\theta_1 - \theta_2$ and $\theta_1 - \theta_3$ are well defined elements of $\mathbb{Q}(\theta_2)$ and $\mathbb{Q}(\theta_3)$ respectively. They are nonzero because the θ's are all distinct. $\mathbb{Q}(\theta_1) \ni f'(\theta_1) \neq 0$ for otherwise θ_1 would be a multiple root of f contradicting $\Delta_f \neq 0$. We have proved that $\varphi(\theta_1, 0)$ is a well defined element of U/U^2. The same holds for θ_1 and θ_2. These prove that φ is well defined.

Lemma 8.2.3. *$\varphi : C(\mathbb{Q}) \to U/U^2$ is a group homomorphism.*

Proof: $\varphi(P) = \varphi(-P)$ for all $P \in C(\mathbb{Q})$ because $x(P) = x(-P)$ for all $P \neq O$ and $O = -O$. $\varphi(P + Q) = \varphi(P)\varphi(Q) \Leftrightarrow \varphi(P)\varphi(Q)\varphi(P * Q) =$

$\varphi(P+Q)\varphi(P*Q) = \varphi(P+Q)^2 = \hat{1}$. So, to prove that φ is a group homomorphism, it is enough to prove that if A, B and C are collinear points of $C(\mathbb{Q})$, then

$$\varphi(A)\varphi(B)\varphi(C) = \hat{1}.$$

If $C = O$, then $\varphi(A)\varphi(B)\varphi(C) = \varphi(A)\varphi(-A)\varphi(O) = \varphi(A)^2 = \hat{1}$. Assume now that all of A, B and C are different from O. Let $x(A) = x_1$, $x(B) = x_2$ and $x(C) = x_3$. Let $y = \lambda x + \nu$ be the equation of the line passing through A, B and C. The following identity holds:

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3).$$

If none of A, B and C is a point of order 2, then $(x_1 - \theta_1)(x_2 - \theta_1)(x_3 - \theta_1) = -f(\theta_1) + (\lambda\theta_1 + \nu)^2 = (\lambda\theta_1 + \nu)^2$. The line $y = \lambda x + \nu$ cuts $C(\mathbb{Q})$ in A, B and C only, so the assumption that A, B and C are not of order 2 guarantees $\lambda\theta_1 + \nu \neq 0$. Similarly we prove $(x_1 - \theta_2)(x_2 - \theta_2)(x_3 - \theta_2) = (\lambda\theta_2 + \nu)^2 \neq 0$ and $(x_1 - \theta_3)(x_2 - \theta_3)(x_3 - \theta_3) = (\lambda\theta_3 + \nu)^2 \neq 0$. Now we can say

$$\varphi(A)\varphi(B)\varphi(C) = ((\lambda\theta_1 + \nu)^2, \widehat{(\lambda\theta_2 + \nu)^2}, (\lambda\theta_3 + \nu)^2) = \hat{1}.$$

If $A = (\theta_1, 0)$, then $y = \lambda x + \nu \Leftrightarrow y = \lambda(x - \theta_1)$ and $f(x) - \lambda^2(x - \theta_1)^2 = (x - \theta_1)(x - x_2)(x - x_3)$. From the last, $f'(x) - 2\lambda^2(x - \theta_1) = (x - x_2)(x - x_3) + (x - \theta_1)(x - x_3) + (x - \theta_1)(x - x_2) \Rightarrow f'(\theta_1) = (\theta_1 - x_2)(\theta_1 - x_3)$. Therefore

$$\varphi(A)\varphi(B)\varphi(C) = (f'(\theta_1)(x_2 - \theta_1)\widehat{(x_3 - \theta_1), (\lambda\theta_2 + \nu)^2}, (\lambda\theta_3 + \nu)^2) =$$

$$(f'(\theta_1)^2, \widehat{(\lambda\theta_2 + \nu)^2}, (\lambda\theta_3 + \nu)^2) = \hat{1}.$$

Similarly we treat the cases $A = (\theta_2, 0)$ and $A = (\theta_3, 0)$. These prove that φ is a group homomorphism. ■

Lemma 8.2.4. $\ker\varphi = 2C(\mathbb{Q})$ *and as a simple consequence* $\frac{C(\mathbb{Q})}{2C(\mathbb{Q})} \simeq Im\varphi$ *and* $\left|\frac{C(\mathbb{Q})}{2C(\mathbb{Q})}\right| = |Im\varphi|$.

Proof: Since $\varphi(2P) = \varphi(P)^2 = \hat{1}$ for all $P \in C(\mathbb{Q})$ we have $2C(\mathbb{Q}) \subset \ker\varphi$. We prove the reverse inclusion.

We first treat the case f is irreducible over $\mathbb{Q}$. Then we have the isomorphisms

$$\rho_i : \frac{\mathbb{Q}[X]}{f \cdot \mathbb{Q}[X]} \to \mathbb{Q}(\theta_i)\ \forall i = \overline{1,3}$$

uniquely determined by $\rho_i(\tilde{x}) = \theta_i$, where $\tilde{x}$ denotes the class of X in $\mathbb{Q}[X]/f\mathbb{Q}[X]$. Let $\rho_i^j : \mathbb{Q}(\theta_j) \to \mathbb{Q}(\theta_i)$ be the isomorphism defined by $\rho_i^j = \rho_i \circ \rho_j^{-1}$ for all $i, j = \overline{1,3}$. Note that $\rho_i^j(\theta_j) = \theta_i$ and $\rho_i^j|_{\mathbb{Q}} = 1_{\mathbb{Q}}$ for all $i, j = \overline{1,3}$.

It is obvious that $\ker\varphi \subset \ker \pi_i\varphi$, where $\pi_i : \frac{U}{U^2} \to \frac{\mathbb{Q}(\theta_i)^*}{(\mathbb{Q}(\theta_i)^*)^2}$ denotes the canonical projection via the isomorphism $\frac{U}{U^2} \simeq \prod_{i=1}^3 \frac{\mathbb{Q}(\theta_i)^*}{(\mathbb{Q}(\theta_i)^*)^2}$. The reverse inclusion now follows from $\pi_i = \rho_i^j \pi_j$.

So it suffices to prove that $\ker \pi_1\varphi = \ker \tilde{\rho}_1^{-1}\pi_1\varphi \subset 2C(\mathbb{Q})$, where $\tilde{\rho}_i : \frac{U(\mathbb{Q}[X]/f\cdot\mathbb{Q}[X])}{U(\mathbb{Q}[X]/f\cdot\mathbb{Q}[X])^2} \to \frac{\mathbb{Q}(\theta_i)^*}{(\mathbb{Q}(\theta_i)^*)^2}$ is the isomorphism obtained canonically from ρ_i. Denote $\phi = \tilde{\rho}_1^{-1}\pi_1\varphi$. Let $P \in \ker\phi$. If $P = O$, then $P = 2O \in 2C(\mathbb{Q})$. Let $P = (\alpha, \beta)$ with $\alpha, \beta \in \mathbb{Q}$. By the assumption that f is irreducible over $\mathbb{Q}$, $\theta_j \notin \mathbb{Q}\ \forall j = \overline{1,3}$, hence $C(\mathbb{Q})$ does not have points of order 2. We want to find $Q \in C(\mathbb{Q})$ such that $2Q = P$.

We have $\hat{1} = \phi(P) = \tilde{\rho}_1^{-1}\circ\pi_1\circ\varphi(P) = \tilde{\rho}_1^{-1}\circ\pi_1((\alpha-\theta_1, \widehat{\alpha-\theta_2}, \alpha-\theta_3)) = \tilde{\rho}_1^{-1}(\widehat{\alpha-\theta_1}) = \widehat{\alpha - X} \Rightarrow \widetilde{\alpha - X} = (\alpha_1 X^2 + \widetilde{\alpha_2 X} + \alpha_3)^2$ for some α_1, α_2 and α_3 in $\mathbb{Q}$.

$(\alpha_1 \cdot X^2 + \widetilde{\alpha_2 \cdot X} + \alpha_3)\cdot(\alpha_1\widetilde{X - \alpha_2}) = (\alpha_1^2 X^3 - \alpha_2^2\widetilde{X + \alpha_1\alpha_3 X} - \alpha_2\alpha_3) = ((-\alpha_1^2 - \alpha_2^2 + \widetilde{\alpha_1\alpha_3)X} - (\alpha_1^2 + \alpha_1\alpha_3)) = \widetilde{e_1 X + f_1}$ for appropriate e_1 and f_1 in $\mathbb{Q}$. Then $(\widetilde{e_1 X + f_1})^2 = (\widetilde{\alpha - X})\cdot(\widetilde{\alpha_1 X - \alpha_2})^2$.

If $\alpha_1 = 0$, then $\widetilde{\alpha - X} = (\widetilde{\alpha_2 X + \alpha_3})^2 \Rightarrow \alpha_2 = 0 \Rightarrow \widetilde{\alpha - X} = \tilde{\alpha}_3^2$, which is a contradiction. So $\alpha_1 \neq 0$ and for suitable e_2, f_2 and h in $\mathbb{Q}$, we have $(\widetilde{e_2 X + f_2})^2 = (\widetilde{\alpha - X})\cdot(\widetilde{X - h})^2 \Rightarrow f|(e_2X + f_2)^2 - (\alpha - X)(X - h)^2$. Since $(e_2X + f_2)^2 - (\alpha - X)(X - h)^2$ is a monic third degree polynomial, $f(x) = (e_2X+f_2)^2-(\alpha-X)(X-h)^2 \Rightarrow f(x)-(e_2X+f_2)^2 = (X-\alpha)(X-h)^2$. The last equality shows that the line $y = e_2x + f_2$ cuts $C(\mathbb{Q})$ one point with the x coordinate α and in two points with the x coordinate h. Let $\mathbb{Q} \ni k = e_2h+f_2$. Then $f(h) = k^2$, so $Q(h,k) \in C(\mathbb{Q})$. If $\{Q, -Q\} \subset \{y^2 = e_2x+f_2\}$, then the line $y^2 = e_2x + f_2$ cuts $C(\mathbb{Q})$ in Q, $-Q$ and in $Q*(-Q) = O$, hence $O = P$ which contradicts the assumption $P \neq O$. So $y^2 = e_2x + f_2$ cuts $C(\mathbb{Q})$ in P or $-P$ and twice in Q or $-Q$. So $(\pm Q)*(\pm Q) = \pm P \Rightarrow 2\cdot(\pm Q) = P \Rightarrow P \in 2C(\mathbb{Q})$.

Lemma 8.2.5. *Let $\theta \in \{\theta_1, \theta_2, \theta_3\}$. Let A be the ring of integers of $\mathbb{Q}(\theta)$. Let $f(x) = (x-\theta)g(x)$, $g \in A[X]$ and $deg(g) = 2$. For $C(\mathbb{Q}) \ni P(\alpha,\beta) \neq O$ such that $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b > 0$ and $gcd(a,b) = 1$, let*

$$I(P) = (a - b\theta)A + b^2 g(\frac{a}{b})A.$$

Then $I(P)$ ranges through a finite number of ideals of A as P varies in $C(\mathbb{Q}) \setminus \{O\}$.

Proof: Notice that since g is a degree 2 polynomial with coefficients in A, $b^2 g(\frac{a}{b}) \in A$, hence $I(P)$ is a well defined ideal of A. $g(\theta) \neq 0$ because f has no multiple roots.

Let $g(x) - g(\theta) = (x-\theta)\cdot h(x)$, $deg(h) = 1$, $h \in A[X]$. Then

$$g(\frac{a}{b}) - g(\theta) = (\frac{a}{b} - \theta)h(\frac{a}{b}) \Rightarrow b^2 g(\frac{a}{b}) - b^2 g(\theta) = (a - b\theta)\cdot(bh(\frac{a}{b})) \Rightarrow$$

$b^2g(\theta) \in I(P)$. We have used that since h is a degree 1 polynomial in $A[X]$, $b \cdot h(\frac{a}{b}) \in A$.

Let $\theta^2 \cdot g(x) - x^2 g(\theta) = (x-\theta)h_1(x)$ with $deg(h_1) = 1$ and $h_1 \in A[X]$. Then

$$\theta^2 \cdot g(\frac{a}{b}) - \frac{a^2}{b^2}g(\theta) = (\frac{a}{b} - \theta)h_1(\frac{a}{b}) \Rightarrow b^2\theta^2 g(\frac{a}{b}) - a^2 g(\theta) = (a - b\theta)\cdot(b \cdot h_1(\frac{a}{b})) \Rightarrow$$

$a^2g(\theta) \in I(P)$.

$a^2g(\theta) \in I(P)$ and $b^2g(\theta) \in I(P)$ imply $g(\theta) \in I(P)$. So $I(P)|g(\theta)A$ implying that $I(P)$ is one of the divisors of $g(\theta)A$. Since $g(\theta)A$ is a nonzero ideal, it has only a finite number of divisors, leaving only a finite number of possibilities for $I(P)$. ■

Lemma 8.2.6. *If $P \in C(\mathbb{Q})$ is such that $2P \neq O$, then there exists an ideal D of A such that*

$$(a - b\theta)A = I(P) \cdot D^2,$$

where $a, b, I(P)$ are defined as in 8.2.5.

Proof: $I(P) = (a - b\theta)A + b^2g(\frac{a}{b})A = gcd((a - b\theta)A, b^2g(\frac{a}{b})A)$. There exist ideals B and C of A such that $(a - b\theta)A = B \cdot I(P)$, $b^2g(\frac{a}{b})A = C \cdot I(P)$ and $gcd(B, C) = A \Leftrightarrow B + C = A$.

$f(x) = (x - \theta)g(x) \Rightarrow f(\frac{a}{b}) = (\frac{a}{b} - \theta)g(\frac{a}{b}) \Rightarrow f(\frac{a}{b}) \cdot b^3A = ((a - b\theta)A) \cdot (b^2g(\frac{a}{b})A) = (B \cdot I(P)) \cdot (C \cdot I(P))$. $f(\alpha) = \beta^2 \Rightarrow \beta^2b^3A = BC \cdot I(P)^2$. We have seen in 2.2.5 that $b = e^2$ for some $e \in \mathbb{Z}$. So $(\beta \cdot e^3)^2A = BC \cdot I(P)^2$. Since B and C are coprime, they must be squares, hence there exists an ideal D of A such that $(a - b\theta)A = I(P) \cdot D^2$. ■

Lemma 8.2.7. *There exists a finite number of algebraic integers γ for which there exist u and τ such that $a - b\theta = \gamma \cdot u \cdot \tau^2$ with $u \in U(A)$ and $\tau \in K = \mathbb{Q}(\theta)$, as $P(\alpha, \beta)$ varies in $C(\mathbb{Q}) \setminus \{O\}$ with $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b > 0$ and $gcd(a, b) = 1$.*

Proof: Let $C_1, \ldots, C_s$ be a complete system of representatives for the ideal class group of A. Note that by 8.1.3 this group is finite. This and 8.2.5 imply that the set of ideals $\{C_i^2 \cdot I(P) | i = \overline{1, s}, P \in C(\mathbb{Q}) \setminus \{O\}\}$ is finite. For each principal ideal in this set, choose γ a generator. We obtain a finite set of these γ's. From 8.2.6, there exists an ideal D such that $(a - b\theta)A = I(P) \cdot D^2 \Rightarrow \hat{1} = \widehat{I(P)} \cdot \hat{D}^2$ in the ideal class group of A, $\mathcal{C}(A)$. Then $\widehat{I(P)} = \hat{C}_i^{-2}$ for some $i = \overline{1, s}$ such that $\hat{D} = \hat{C}_i$, so $I(P) \cdot C_i^2 = \gamma \cdot A$. Since $\hat{D} = \hat{C}_i$, there exists $\tau \in K^*$ such that $C_i = D \cdot \tau^{-1}$. Clearly $I(P) \cdot D^2 \cdot \tau^{-2} = \gamma \cdot A \Rightarrow (a - b\theta)A = \gamma \cdot \tau^2 \cdot A \Rightarrow (a - b\theta) = \gamma \cdot u \cdot \tau^2$ for some $u \in U(A)$. ■

Proof of 8.2.1: By 8.2.4, $\left|\frac{C(\mathbb{Q})}{2C(\mathbb{Q})}\right| \simeq Im\varphi$, hence it suffices to prove that $Im\varphi$ is a finite set. Since there are at most 4 points $P \in C(\mathbb{Q})$ such that

$2P = O$, we can only investigate $\varphi(P)$ for $2P \neq O$ and $P = (\alpha, \beta)$ with $\alpha = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b > 1$ and $gcd(a, b) = 1$.

$$\varphi(P) = (\alpha - \theta_1, \widehat{\alpha - \theta_2}, \alpha - \theta_3).$$

From 2.2.5, there exists $e \in \mathbb{N}^*$ such that $b = e^2$.

$$\widehat{\frac{a}{b} - \theta_1} = \frac{\widehat{a - b\theta_1}}{e^2} = \widehat{a - b\theta_1} = \gamma \widehat{\cdot u \cdot \tau^2} = \widehat{\gamma \cdot u},$$

for some $u \in U(A)$, $0 \neq \tau \in K = \mathbb{Q}(\theta_1)$ and for some γ belonging to the finite set in 8.2.7.

By 8.1.5, $U(A)$ is a finitely generated abelian group, hence there exists $r \in \mathbb{N}$ such that $U(A)$ is generated by $u_1, \ldots, u_r$. It is easy to see that every element of $U(A)/U(A)^2$ is of the form $u_1^{\varepsilon_1} \widehat{\cdot \ldots \cdot} u_r^{\varepsilon_r}$ with $\varepsilon_i \in \{0, 1\}$ for $i = \overline{1, r}$. So $|U(A)/U(A)^2| \leq 2^r$. Manifestly, there is only a finite number of possibilities for $\widehat{\frac{a}{b} - \theta_1}$. We treat the second and third coordinates similarly and keeping in mind that

$$\frac{U(\mathbb{Q}(\theta_1) \times \mathbb{Q}(\theta_2) \times \mathbb{Q}(\theta_3))}{U(\mathbb{Q}(\theta_1) \times \mathbb{Q}(\theta_2) \times \mathbb{Q}(\theta_3))^2} \simeq \frac{\mathbb{Q}(\theta_1)^*}{(\mathbb{Q}(\theta_1)^*)^2} \times \frac{\mathbb{Q}(\theta_2)^*}{(\mathbb{Q}(\theta_2)^*)^2} \times \frac{\mathbb{Q}(\theta_3)^*}{(\mathbb{Q}(\theta_3)^*)^2},$$

we conclude that $Im\varphi$ is finite. ■

8.3 C_{17}

We return to 7.2.12 and prove that even though the rank of $C_{17}(\mathbb{Q}) : y^2 = x^3 + 17x$ is 0, one of the equations that we will stumble upon, namely $x^2 + 4y^4 = 17e^4$, has nontrivial solutions modulo any positive integer $m > 1$, but has no nontrivial solution in integers. To simplify the notation, we will use $C(\mathbb{Q})$ instead of $C_{17}(\mathbb{Q})$. The procedure is standard. We consider the associated curve $\bar{C}(\mathbb{Q}) : y^2 = x^3 - 68x$ and the group homomorphisms $\alpha : C(\mathbb{Q}) \to \mathcal{Q}$, $\alpha' : \bar{C}(\mathbb{Q}) \to \mathcal{Q}$, defined by

$$\alpha(P) = \begin{cases} \hat{x}, & \text{if } P(x, y) \neq O[0:1:0], T(0,0) \\ \hat{17}, & \text{if } P = T \\ \hat{1}, & \text{if } P = O \end{cases},$$

$$\alpha'(\bar{P}) = \begin{cases} \widehat{\bar{x}}, & \text{if } \bar{P}(\bar{x}, \bar{y}) \neq \bar{O}[0:1:0], \bar{T}(0,0) \\ \widehat{-17}, & \text{if } \bar{P} = \bar{T} \\ \hat{1}, & \text{if } \bar{P} = \bar{O} \end{cases},$$

where $\mathcal{Q} = \frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$. It was proved that $2^r = \frac{|Im\alpha| \cdot |Im\alpha'|}{4}$, where r is the rank of $C(\mathbb{Q})$. We have proved that for curves of type $C_p(\mathbb{Q})$ with p a prime integer, $|Im\alpha| = 2$, so all that is left to prove is that $|Im\alpha'| = 2$.

We have proved that $x \in Im\alpha'$ if and only if there exist $b_1, b_2, M, N, e \in \mathbb{Z}$ such that

$$N^2 = b_1M^4 + b_2e^4,$$

$\hat{b}_1 = x$, $b_1b_2 = -68$ and $1 = gcd(M, e) = gcd(M, N) = gcd(e, N) = gcd(b_2, M) = gcd(b_1, e)$. We have seen that a solution to the equation above corresponds to the point $\bar{P} = (\frac{b_1M^2}{e^2}, \frac{b_1MN}{e^3})$ ($\bar{P} = \bar{O}$ if $e = 0$) on $\bar{C}(\mathbb{Q})$ such that $\alpha'(\bar{P}) = \hat{b}_1 = x$.

It is known that $\hat{1}, \widehat{-17} \in Im\alpha'$. So we have to prove that for $b_1 \in \{-1, \pm2, -4, 17, \pm34, 68\}$, the equation above has no solutions.

If $b_1 = -1$, we have the equation $N^2 = -M^4 + 68e^4$ with some additional conditions. Let's assume that the equation has a nontrivial solution $(N, M, e) \neq (0, 0, 0)$. We can assume that $gcd(M, N, e) = 1$. Reducing modulo 4 we have $N^2 = -M^4(mod4)$ and since the quadratic residues modulo 4 are 0 and 1, N and M are even numbers. $gcd(N, M, e) = 1$ implies that e is odd.

Let $N = 2x$ and $M = 2y$. The equation is $x^2 = -4y^4+17e^4 \Leftrightarrow x^2+4y^4 = 17e^4$. If p is a prime number such that $p|gcd(x, y)$, then $p|17e^4$, hence $p|e$ or $p|17$. $p|e$ contradicts $gcd(2x, 2y, e) = 1$, therefore $p|17 \Rightarrow p = 17$. Then $17\left(\frac{x}{17}\right)^2+4\cdot17^3\left(\frac{e}{17}\right)^4 = e^4 \Rightarrow 17|e$ which also contradicts $gcd(2x, 2y, e) = 1$. These prove that $gcd(x, y) = 1$. Similarly $gcd(e, y) = 1$. Since e is odd, x is also odd.

We solve the equation

$$x^2 + 4y^4 = 17e^4,\ gcd(x, y) = gcd(e, y) = 1,\ \text{with } x \text{ and } e \text{ odd integers},$$

at the help of $\mathbb{Z}[\imath]$ which is an euclidian domain.

$(x + 2\imath y^2)(x - 2\imath y^2) = 17e^4$.

Let $d = gcd(x+2\imath y^2, x-2\imath y^2)$. Then $d|2x$ and $d|4y^2$, hence $d|gcd(4x, 4y^2)$. Since x and y are coprime in $\mathbb{Z}$, they are also coprime in $\mathbb{Z}[\imath]$, so $gcd(x, y^2) = 1$. It follows that $d|4$. The prime factor decomposition of 4 in $\mathbb{Z}[\imath]$ is $4 = -(1 + i)^4$. If $1 + \imath|d$, then $1 + \imath|x^2 + 4y^4 = 17e^4$ which is impossible since e is odd. Therefore $d = 1$.

$17|x + 2\imath y^2$ if and only if $x + 2\imath y^2 = 17 \cdot z$ for some $z \in \mathbb{Z}[\imath]$ if and only if $x - 2\imath y^2 = 17 \cdot \bar{z}$, where $\bar{z}$ is the complex conjugate of z, if and only if $17|x-2\imath y^2$. Hence $17|x+2\imath y^2 \Leftrightarrow 17|x-2\imath y^2$. In this case, $17|2x$ and $17|4\imath y^2$ which imply $17|x$ and $17|y$. This is a contradiction. Therefore $17 \not| x \pm 2\imath y^2$.

The prime factor decomposition of 17 in $\mathbb{Z}[\imath]$ is $17 = (4+\imath)(4-\imath)$ and the two primes appearing in the decomposition are not associated in divisibility i.e. they do not generate the same ideal of $\mathbb{Z}[\imath]$. It is easy to obtain $x+2\imath y^2 = (\pm4 \pm \imath)\alpha^4$ or $x + 2\imath y^2 = (\pm4 \pm \imath)\imath\alpha^4$ for some $\alpha = a + \imath b \in \mathbb{Z}[\imath]$. $(\alpha \cdot \bar{\alpha})^4 = e^4 \Rightarrow (a^2 + b^2)^4 = e^4$. a and b must have different parities otherwise e would be even. A simple computation yields $\alpha^4 = (a^4 - 6a^2b^2 + b^4) + 4ab(a^2 - b^2)\imath$.

$$x + 2\imath y^2 = (\pm4 \pm \imath)\alpha^4 \Rightarrow x = \pm4(a^4 - 6a^2b^2 + b^4) \mp 4ab(a^2 - b^2) \Rightarrow 2|x$$

which is impossible since x is odd.

$$x + 2\imath y^2 = (\pm 4 \pm \imath)\imath\alpha^4 \Rightarrow 2y^2 = \pm 4(a^4 - 6a^2b^2 + b^4) \pm 4ab(a^2 - b^2) \Rightarrow$$

$$2|y \Rightarrow 2| \pm (a^4 + b^4 - 6a^2b^2) \pm ab(a^2 - b^2).$$

Since a and b have different parities, $a^4 + b^4 - 6a^2b^2$ is odd and $ab(a^2 - b^2)$ is even thus contradicting the previous divisibility.

Remark 8.3.1. *We have proved that the only solution in $\mathbb{Z}$ of the equation $x^2 + 4y^4 = 17z^4$ is $(x, y, z) = (0, 0, 0)$.*

We postpone the proof of $r = 0$ to prove:

Proposition 8.3.2. *For all $m \in \mathbb{Z}$, $m > 1$, there exist $x, y, z \in \mathbb{Z}$ such that $x^2 + 4y^4 \equiv 17e^4 (mod\ m)$ and $(\hat{x}, \hat{y}, \hat{e}) \neq (\hat{0}, \hat{0}, \hat{0})$ in $\mathbb{Z}_m$.*

Proof: The Chinese Remainder Theorem allows us to reduce to the case $m = p^\alpha$ for some prime number p and integer $\alpha > 0$. The main tool is the following lemma:

Lemma 8.3.3. *Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ be a polynomial with integer coefficients and let p be a prime number. A modulo p zero $(x_1, \ldots, x_n)$ of f is called simple if $f(x_1, \ldots, x_n) \equiv 0 (mod\ p)$ and one of the partial derivates $\frac{\partial f}{\partial X_i}(x_1, \ldots, x_n)$ is nonzero mod p.*

Then for any simple mod p zero $(x_1, \ldots, x_n)$ of f and any $\alpha > 0$ there exists $(x_1^{(\alpha)}, \ldots, x_n^{(\alpha)}) \in (\mathbb{Z})^n$ such that $f(x_1^{(\alpha)}, \ldots, x_n^{(\alpha)}) \equiv 0 (mod\ p^\alpha)$.

Assume first that $\alpha = 1$. Then $m = p$. If $p = 2$, then take $(x, y, e) = (1, 0, 1)$. If $p = 17$, take $(x, y, e) = (8, 1, 1)$. If $p \equiv 1 (mod 4)$, then there exists $z \in \mathbb{Z}$ such that $p|z^2 + 1$. Take $(x, y, e) = (2z, 1, 0)$. If $p \equiv 3 (mod 4)$, then we prove that any square in $\mathbb{Z}_p$ is also a fourth power in $\mathbb{Z}_p$. We know that if z is not divisible by p then it is a square mod p if and only if $-z$ is not a square mod p. Let t be a square mod p not divisible by p. Then there exists $z \in \mathbb{Z}$ such that $t \equiv z^2 (mod\ p)$. Then $p \not| z$, so z or $-z$ is a square modulo p leading to t is a fourth power in $\mathbb{Z}_p$. Take $(x, y, e) = (8, 1, z)$ such that $z^4 \equiv 2^2 (mod\ p)$.

It is easy to see that if $p \neq 2$, then the solutions given above are simple mod p zeros of $f(x, y, e) = x^2 + 4y^4 - 17e^4$ and the proposition follows from 8.3.3.

There is no simple mod 2 zero of f since all the partials are obviously divisible by 2, so we cannot apply 8.3.3 in this case, but we prove by induction that we can construct $x_n \in \mathbb{Z}$ such that $x_n^2 + 4 \cdot 0^4 - 17 \cdot 1^4 \equiv 0 (mod\ 2^n)$ for any $n > 0$. Taking $(x, y, e) = (x_n, 0, 1)$ would then complete the proof.

Notice that we can take $x_1 = x_2 = x_3 = x_4 = 1$. Assume we have constructed $x_n^2 - 17 = 2^n \cdot y_n$ for some $y_n \in \mathbb{Z}$ and $n \geq 4$. We try to find $t \in \mathbb{Z}$ such that $2^{n+1} | (x_n + 2^{n-1}t)^2 - 17$.

$$(x_n + 2^{n-1}t)^2 - 17 = x_n^2 + 2^n x_n t + 2^{2n-2}t^2 - 17 = 2^n(y_n + x_n t) + 2^{2n-2}t^2.$$

Since $n \geq 3$, $2n-2 \geq n+1$, so $2^{n+1}|(x_n+2^{n-1}t)^2-17$ if and only if $2|y_n+x_nt$. Such t exists because $2^n|x_n^2-17 \Rightarrow x_n$ is odd. Take $x_{n+1}=x_n+2^{n-1}t$.

Alternatively we could have used the following lemma for $f(x)=x^2-17$, $n=3$ and $k=1$:

Lemma 8.3.4. *Let $f \in \mathbb{Z}[X]$ with f' its derivate and let p be a prime number. Let $x \in \mathbb{Z}$, $n,k \in \mathbb{Z}$ such that $0 \leq 2k < n$, $p^n|f(x)$ and $v_p(f'(x)) = k$ i.e. $p^k|f'(x)$ and $p^{k+1} \not| f'(x)$.*

Then there exists $y \in \mathbb{Z}$ of the form $x+p^{n-k}z$ such that $p^{n+1}|f(y)$ and $v_p(f'(y))=k$.

■

Let's see what we have worked so hard for. We have proved that the equation $x^2+4y^4-17z^4=0$ has no nontrivial solution in $\mathbb{Z}$ even though it has nontrivial solutions in $\mathbb{Z}_m$ for any $m>1$. This means that generally we cannot hope to have an algorithm, based on reductions by various integers, that would help us prove that an equation of the form $N^2=b_1M^4+aM^2e^2+b_2e^4$ has no nontrivial integer solutions. The reason why such an algorithm was expected until the discovery of a counterexample like the one above was that such an algorithm exists for quadratic forms:

Theorem 8.3.5 (Minkowski-Hasse). *The equation with nonzero integer coefficients $a_1x_1^2+\ldots+a_nx_n^2=0$ has nontrivial solutions ($(x_1,\ldots,x_n) \neq (0,\ldots,0)$) in $\mathbb{Z}$ if and only if it has nontrivial solutions in $\mathbb{R}$ and in $\mathbb{Z}_m$ for any $m>1$.*

We should now return to $C_{17}(\mathbb{Q})$. We have proved that the equations $N^2=-M^4+68e^4$ and $N^2=-4M^4+17e^4$ have no nontrivial integer solutions. This means that $\widehat{-1} \notin Im\alpha'$.

If $b_1=-2$, the equation is $N^2=-2M^4+34e^4$ with $1=gcd(M,e)=gcd(M,N)=gcd(e,N)=gcd(34,M)=gcd(-2,e)$. N must be even, so there exists $n \in \mathbb{Z}$ such that $N=2n$ and $M^4+2n^2=17e^4$. M and e have the same parity hence they are both odd since $gcd(M,e)=1$. Reducing mod 16 we obtain $M^4+2n^2 \equiv e^4 (mod\ 16)$. But $\hat{\alpha}^4 \in \{\hat{0},\hat{1},\hat{4}\}$ mod 16 for all $\alpha \in \mathbb{Z}$, and since M and e are odd, we obtain $16|2n^2 \Rightarrow 4|n$.

In $\mathbb{Z}[\imath\sqrt{2}]$, which is an euclidian domain, we have $(M^2+\imath\sqrt{2}\cdot n)(M^2-\imath\sqrt{2}\cdot n)=17e^4$.

Let $d=gcd(M^2+\imath\sqrt{2}\cdot n, M^2-\imath\sqrt{2}\cdot n)$. Then $d|2M^2$ and $d|2\imath\sqrt{2}\cdot n$ imply $d|gcd(2\imath\sqrt{2}\cdot M^2, 2\imath\sqrt{2}\cdot n)=2\imath\sqrt{2}$. The prime factor decomposition of $2\imath\sqrt{2}$ is $-(\imath\sqrt{2})^3$. If $\imath\sqrt{2}|d$, then $d^2|(M^2+\imath\sqrt{2}\cdot n)(M^2-\imath\sqrt{2}\cdot n)=17e^4 \Rightarrow 2|17e^4$ contradicting that e is odd. Therefore $d=1$.

$17|M^2+\imath\sqrt{2}\cdot n$ if and only if there exists $z \in \mathbb{Z}[\imath\sqrt{2}]$ such that $M^2+\imath\sqrt{2}\cdot n=17z \Leftrightarrow M^2-\imath\sqrt{2}\cdot n=17\bar{z}$, where $\bar{z}$ is the complex conjugate of z, if and only if $17|M^2-\imath\sqrt{2}\cdot n$. So $17|M^2+\imath\sqrt{2}\cdot n \Leftrightarrow 17|M^2-\imath\sqrt{2}\cdot n$. In this case we easily find that $17|M$ and $17|n$ which contradict $gcd(M,N)=1$.

The prime factor decomposition of 17 is $(3+2\imath\sqrt{2})(3-2\imath\sqrt{2})$ and it is easy to see that $M^2+\imath\sqrt{2}\cdot n=(\pm 3\pm 2\imath\sqrt{2})(a+b\imath\sqrt{2})^4$ for some $a,b\in\mathbb{Z}$ such that $(a+\imath\sqrt{2}\cdot b)^4(a-\imath\sqrt{2}\cdot b)^4=e^4$. Since e is odd, it follows that a is also odd. It is an easy computation to verify $(a+b\imath\sqrt{2})^4=(a^4-12a^2b^2+4b^2)+4ab(a^2-2b^2)\imath\sqrt{2}$. It follows that $n=\pm 2(a^4-12a^2b^2+4b^4)\pm 12ab(a^2-2b^2)$. Modulo 4 we have $n\equiv 2a^4(mod 4)$ which is impossible because a is odd and $4|n$. We have proved that $\widehat{-2}\notin Im\alpha'$.

If $b_1=2$, then the equation is $N^2=2M^4-34e^4$ and we have the additional conditions: $1=gcd(M,e)=gcd(M,N)=gcd(e,N)=gcd(-34,M)=gcd(2,e)$. $gcd(2,e)=gcd(-34,M)=1$ implies that M and e are odd. $N^2=2M^4-34e^4\Rightarrow N=2n$ for some $n\in\mathbb{Z}$ and $2n^2=M^4-17e^4$. Reducing modulo 16 we get $2n^2\equiv 1-17(mod\ 16)\Rightarrow 16|2n^2\Rightarrow 4|n\Rightarrow n=4m$ for some $m\in\mathbb{Z}$. The equation is $32m^2=M^4-17e^4$ and the restrictions are that M and e be odd and $gcd(M,e)=1$. It is not hard to prove that $gcd(M,8m)=gcd(e,8m)=gcd(-34,M)=gcd(2,e)=gcd(m,17)=1$.

We consider $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ which as we will prove is a principal ideal domain. Its elements are of the form $\frac{a+\sqrt{17}\cdot b}{2}$ with a,b integers of the same parity.

$32m^2=M^4-17e^4\Leftrightarrow\frac{M^2+\sqrt{17}e^2}{2}\cdot\frac{M^2-\sqrt{17}e^2}{2}=8m^2$.

Let $d=gcd(\frac{M^2+\sqrt{17}e^2}{2},\frac{M^2-\sqrt{17}e^2}{2})$ in $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$. Then $d|M^2$ and $d|\sqrt{17}\cdot e^2$, hence $d|gcd(\sqrt{17}\cdot M^2,\sqrt{17}\cdot e^2)=\sqrt{17}$. $\sqrt{17}$ is a prime element of $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$. If $d=\sqrt{17}$, then $17=d^2|\frac{M^2+\sqrt{17}e^2}{2}\cdot\frac{M^2-\sqrt{17}e^2}{2}=8m^2$ which is easily seen to be false. Therefore $d=1$.

There is the prime factor decomposition $2=\frac{3+\sqrt{17}}{2}\cdot\frac{-3+\sqrt{17}}{2}$ and the two primes that appear in the decomposition are not associated in divisibility i.e. they do not generate the same ideal of $\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$.

$2\not|\frac{M^2\pm\sqrt{17}\cdot e^2}{2}$ because M and e are odd integers.

The elements of the group of units $U(\mathbb{Z}[\frac{1+\sqrt{17}}{2}])$ are $\{\pm(4+\sqrt{17})^n|n\in\mathbb{Z}\}$.

We must have

$$\frac{M^2+\sqrt{17}\cdot e^4}{2}=\pm(4+\sqrt{17})^n\cdot\frac{\pm 3+\sqrt{17}}{2}\cdot\left(\frac{a+\sqrt{17}\cdot b}{2}\right)^2$$

for some $a,b,n\in\mathbb{Z}$ such that a and b have the same parity and $(a^2-17b^2)^2=64m^2$. Since $M^2+\sqrt{17}\cdot e^2>0$, we have

$$M^2+\sqrt{17}\cdot e^2=(4+\sqrt{17})^n\cdot(\pm 3+\sqrt{17})\cdot\left(\frac{a+\sqrt{17}\cdot b}{2}\right)^2.$$

Let $(4+\sqrt{17})^r=A_r+\sqrt{17}\cdot B_r$ with $A_r,B_r\in\mathbb{Z}$ uniquely defined by the recurrence:

$$\begin{cases} A_{r+1}=4A_r+17B_r \\ B_{r+1}=A_r+4B_r \end{cases},\ \forall r\in\mathbb{Z}$$

with "initial terms" $A_0 = 1$ and $B_0 = 0$. Note the recurrence goes both ways. A_{r+1} and B_{r+1} are obviously uniquely defined by A_r and B_r. Conversely, A_r and B_r are uniquely defined by A_{r+1} and B_{r+1} as a consequence of $\det \begin{pmatrix} 4 & 17 \\ 1 & 4 \end{pmatrix} = -1$.

The equation can be rewritten as:

$$4 \cdot (M^2 + \sqrt{17} \cdot e^2) = (A_n + \sqrt{17} \cdot B_n) \cdot (\pm 3 + \sqrt{17}) \cdot (\alpha + \sqrt{17} \cdot \beta)$$

for $\alpha = a^2 + 17b^2$ and $\beta = 2ab$. So $4(M^2 + \sqrt{17}e^2) = ((\pm 3A_n + 17B_n) + (A_n \pm 3B_n)\sqrt{17}) \cdot (\alpha + \sqrt{17} \cdot \beta)$. We have the same $\pm$ everywhere it appears in the preceding equality. Since $\sqrt{17}$ is not a rational number, we find the system:

$$\begin{cases} 4M^2 = (\pm 3A_n + 17B_n) \cdot \alpha + 17(A_n \pm 3B_n) \cdot \beta \\ 4e^2 = (\pm 3A_n + 17B_n) \cdot \beta + (A_n \pm 3B_n) \cdot \alpha \end{cases}$$

with the same convention on the sign $\pm$. By adding the two equations reduced modulo 16 we have

$$4(M^2 + e^2) \equiv (\alpha + \beta)(\pm 3A_n + B_n + A_n \pm 3B_n) (mod\ 16).$$

If the sign is " + ", then the equation mod 16 above is equivalent to $M^2 + e^2 \equiv (\alpha + \beta)(A_n + B_n) (mod\ 4)$. It is easy to prove by induction that $A_r + B_r \equiv A_{r+1} + B_{r+1} \equiv A_0 + B_0 \equiv 1 (mod\ 4)$ for all $r \in \mathbb{Z}$. $\alpha + \beta = a^2 + 17b^2 + 2ab \equiv a^2 + b^2 + 2ab = (a + b)^2 (mod\ 4)$. Since a and b have the same parity, $\alpha + \beta \equiv 0 (mod\ 4)$, so $4 | M^2 + e^2$. But this is not possible because M and e are both odd, hence $M^2 + e^2 \equiv 2 (mod\ 4)$.

If the sign is " − ", then $0 < M^2 + \sqrt{17} \cdot e^2 = (4 + \sqrt{17})^n \cdot (-3 + \sqrt{17}) \cdot \left(\frac{a + \sqrt{17} \cdot b}{2}\right)^2 \Rightarrow$

$$M^2 - \sqrt{17} \cdot e^2 = (4 - \sqrt{17})^n \cdot (-3 - \sqrt{17}) \cdot \left(\frac{a - \sqrt{17} \cdot b}{2}\right)^2.$$

Since $(M^2 + \sqrt{17} \cdot e^2) \cdot (M^2 - \sqrt{17} \cdot e^2) = 32m^2 > 0$, it follows that $M^2 - \sqrt{17} \cdot e^2 > 0$. Then $M^2 - \sqrt{17} \cdot e^2 = (4 - \sqrt{17})^n \cdot (-3 - \sqrt{17}) \cdot \left(\frac{a - \sqrt{17} \cdot b}{2}\right)^2 > 0 \Rightarrow$ n is odd.

$4M^2 = (-3A_n + 17B_n) \cdot \alpha + 17(A_n - 3B_n) \cdot \beta \Rightarrow 4M^2 \equiv (-3A_n + B_n)(a^2 + b^2) + (A_n - 3B_n)(2ab) \equiv (-3A_n + B_n)(a + b)^2 + 2ab(4A_n - 4B_n) (mod\ 16) \Rightarrow 1 \equiv M^2 \equiv (-3A_n + B_n) \left(\frac{a+b}{2}\right)^2 + 2ab(A_n - B_n) (mod\ 4)$. Note that $\frac{a+b}{2}$ is an integer because a and b have the same parity.

We have

$$\begin{cases} A_{r+1} \equiv B_r (mod\ 4) \\ B_{r+1} \equiv A_r (mod\ 4) \end{cases}, \ \forall r \in \mathbb{Z}.$$

It is easy to see that since n is odd, $A_n \equiv 0 (mod\ 4)$ and $B_n \equiv 1 (mod\ 4)$. Then $1 \equiv \left(\frac{a+b}{2}\right)^2 - 2ab (mod\ 4)$. If a and b are both odd, then $2ab \equiv 2 (mod\ 4)$,

so $\left(\frac{a+b}{2}\right)^2 \equiv 3(mod\ 4)$ which is impossible. Therefore a and b are both even. Then there exist $u, v \in \mathbb{Z}$ such that $a = 2u$, $b = 2v$ and $(u^2 - 17v^2)^2 = 4m^2$. This means that u and v have the same parity. Just like before, we get the system:

$$\begin{cases} M^2 = (-3A_n + 17B_n) \cdot (u^2 + 17v^2) + 17(A_n - 3B_n) \cdot (2uv) \\ e^2 = (-3A_n + 17B_n) \cdot (2uv) + (A_n - 3B_n) \cdot (u^2 + 17v^2) \end{cases}.$$

By adding the equations modulo 8 we have

$$M^2 + e^2 \equiv -2(A_n + B_n)(u + v)^2 \equiv 0(mod\ 8).$$

We have used that $u+v$ is even because u and v have the same parity, hence $4|(u + v)^2$. But $8|M^2 + e^2$ implies that M and e are even which is false.

We have finished proving that $\hat{2} \notin Im\alpha'$.

We know that $Im\alpha'$ is an abelian group containing $\hat{1}$ and $\widehat{-17}$. Also $\widehat{-1}, \widehat{\pm 2} \notin Im\alpha'$. Using these and the group structure of $Im\alpha'$, it is easy to prove that $\widehat{17}, \widehat{\pm 34} \notin Im\alpha'$. Hence $|Im\alpha'| = 2$ and the rank r of $C_{17}(\mathbb{Q})$ is 0.■

Lemma 8.3.6. *$\mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ is a principal ideal domain.*

Towards the proof of the lemma we need the following:

Theorem 8.3.7 (Hasse-Dedekind). *Let $(A, +, \cdot)$ be a subring of $\mathbb{C}$. Let $\varphi : A \to \mathbb{N}$ be a function such that:*

1. *$\varphi(\alpha) = 0 \Leftrightarrow \alpha = 0$;*
2. *$\forall x, y \in A$ such that $y \neq 0$ and $y \not| x$ there exist $u, v \in A$ such that $0 < \varphi(xu + yv) < \varphi(y)$.*

Then A is a principal ideal domain.

Proof: Let I be a nonzero ideal of A. There exists $a \in I$ such that $0 < \varphi(a) \leq \varphi(x)$ for all nonzero elements $x \in I$. We will prove that $I = a \cdot A$.

Let $x \in I$, $x \neq 0$. Suppose $a \not| x$. Then there exist $u, v \in A$ such that $0 < \varphi(au + xv) < \varphi(a)$. Since $a, x \in I$, $au + xv$ is also an element of I. The condition $0 < \varphi(au + xv)$ implies that $au + xv \neq 0$. The inequality $\varphi(au + xv) < \varphi(a)$ contradicts the choice of a. Therefore $a|x$ for all nonzero $x \in I$. This implies $I \subset a \cdot A$. The reverse inclusion is obvious. ■

Proof of 8.3.6: To prove this lemma we use the Hasse-Dedekind Theorem for $A = \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ and $\varphi(\frac{a+b\cdot\sqrt{17}}{2}) = \left|\frac{a^2-17\cdot b^2}{4}\right|$ for all $a, b \in \mathbb{Z}$ of the same parity.

We prove that φ satisfies the conditions in Hasse-Dedekind's Theorem. If a and b have the same parity, then $a^2 \equiv b^2 \equiv 17b^2(mod 4) \Rightarrow 4|a^2 - 17b^2$.

Since obviously $\varphi(x) \geq 0$ for all $x \in A$, we have proved that $\varphi(x) \in \mathbb{N}$ for all $x \in A$. φ can be extended on $\mathbb{Q}(\sqrt{17})$ by $\varphi(a+b\sqrt{17}) = |a^2 - 17b^2|$. φ is multiplicative on $\mathbb{Q}(\sqrt{17})$ and on A.

$\varphi(a+b\sqrt{17}) = 0 \Leftrightarrow |a^2 - 17b^2| = 0 \Leftrightarrow a^2 = 17b^2$. It is easy to prove using $\sqrt{17} \notin \mathbb{Q}$ that $a^2 = 17b^2 \Leftrightarrow a = b = 0$. Therefore $\varphi(x) = 0 \Leftrightarrow x = 0$.

Let $x, y \in A$ such that $y \neq 0$ and $y \not| x$. It is clear that $0 < \varphi(xu+yv) < \varphi(y) \Leftrightarrow 0 < \varphi(\frac{x}{y} \cdot u + v) < 1$. $\frac{x}{y} \in \mathbb{Q}(\sqrt{17}) \Rightarrow \exists\ a, b, c \in \mathbb{Z},\ c \in \mathbb{N}^*$ such that $gcd(a,b,c) = 1$ and $\frac{x}{y} = \frac{a+b\sqrt{17}}{c}$. Because $gcd(a,b,c) = 1$, there exist $d, e, f \in \mathbb{Z}$ such that $ad + be + cf = 1$. Let

$$u = e + d\sqrt{17} \in A.$$

Then $\frac{x}{y} \cdot u = \frac{(a+b\sqrt{17})(e+d\sqrt{17})}{c} = \frac{ae+17db+(ad+be)\sqrt{17}}{c}$. Let $q, r \in \mathbb{Z}$ be defined by $ae + 17bd = cq + r$ with $-\frac{c}{2} \leq r \leq \frac{c}{2}$, and let

$$v = -q + f\sqrt{17} \in A.$$

Then $\frac{x}{y} \cdot u + v = \frac{ae+17db-cq+(ad+be+cf)\sqrt{17}}{c} = \frac{r+\sqrt{17}}{c}$.

For $c \geq 5$, we have $0 < \varphi(\frac{x}{y} \cdot u + v) = \left|\frac{r^2-17}{c^2}\right| \leq \left(\frac{r}{c}\right)^2 + \frac{17}{c^2} \leq \frac{1}{4} + \frac{17}{25} < 1$.

If $c = 1$, then we contradict $y \not| x$.

If $c = 2$, then a and b must have different parities otherwise $\frac{x}{y} \in A$ which contradicts $y \not| x$. Let $u = a - b\sqrt{17}$ and $v = -q$ such that $a^2 - 17b^2 = 2q+1$. Then $\frac{x}{y} \cdot u + v = \frac{(a+b\sqrt{17})(a-b\sqrt{17})-2q}{2} = \frac{1}{2} \Rightarrow 0 < \varphi(\frac{x}{y} \cdot u + v) = \frac{1}{4} < 1$.

If $c = 3$, then let $u = a - b\sqrt{17}$ and $v = -q$ such that $a^2 - 17b^2 = 3q + r$ and $r \in \{0, 1, 2\}$. If $r = 0$, then $3|a^2 - 17b^2 \Rightarrow 3|a^2 + b^2 \Rightarrow 3|gcd(a,b)$ which contradicts $gcd(a,b,3) = 1$. Hence $r \neq 0$. Then $\frac{x}{y} \cdot u + v = \frac{a^2-17b^2-3q}{3} = \frac{r}{3} \Rightarrow 0 < \varphi(\frac{x}{y} \cdot u + v) < 1$.

Assume $c = 4$. If a and b have different parities, let $u = a - b\sqrt{17}$. $a^2 - 17b^2$ is an odd number, so there exist $q, r \in \mathbb{Z}$ such that $a^2 - 17b^2 = 4q + r$ and $r \in \{1, 3\}$. Let $v = -q$. Then $\frac{x}{y} \cdot u + v = \frac{r}{4} \Rightarrow 0 < \varphi(\frac{x}{y} \cdot u + v) < 1$.

If a and b have the same parity, then they must both be odd because $gcd(a,b,4) = 1$. We have the two cases two consider:

1. If $a \equiv 3(mod 4)$, then let $u = 1$ and $a = 4k+3$. Let $v = -k - l\sqrt{17}$ with l defined by $b = 4l \pm 1$. Then $\frac{x}{y} \cdot u + v = \frac{3 \pm \sqrt{17}}{4} \Rightarrow 0 < \frac{x}{y} \cdot u + v = \frac{1}{2} < 1$.
2. If $a \equiv 1(mod 4)$, let $u = -1$, $-a = 4k + 3$, $-b = 4l \pm 1$ and $v = -k - l\sqrt{17}$. Then $\frac{x}{y} \cdot u + v = \frac{3 \pm \sqrt{17}}{4} \Rightarrow 0 < \varphi(\frac{x}{y} \cdot u + v) = \frac{1}{2} < 1$.

■

Lemma 8.3.8. *The group of units of* $A = \mathbb{Z}[\frac{1+\sqrt{17}}{2}]$ *is*

$$U(A) = \{\pm(4 + \sqrt{17})^n | n \in \mathbb{Z}\}.$$

Proof: It is very easy to see that $\pm(4+\sqrt{17})^n$ is a unit for every integer n.

Let now $u = \frac{a+\sqrt{17}b}{2}$ be a unit in A. $a, b \in \mathbb{Z}$ and have the same parity. Since u is invertible, there exists $v \in A$ such that $uv = 1$. Since φ is multiplicative, we find $\varphi(u) \cdot \varphi(v) = 1 \Rightarrow \varphi(u) = \varphi(v) = 1 \Rightarrow \left|\frac{a^2-17b^2}{4}\right| = 1$. Assume first $1 < u < 4 + \sqrt{17}$. $1 = \left|\frac{a^2-17b^2}{4}\right| = \left|\frac{a+b\sqrt{17}}{2}\right| \cdot \left|\frac{a-b\sqrt{17}}{2}\right| \Rightarrow \left|\frac{a-b\sqrt{17}}{2}\right| = \left|\frac{2}{a+b\sqrt{17}}\right| = \frac{1}{u} < 1 \Rightarrow -1 < \frac{b\sqrt{17}-a}{2} < 1$. Since $1 < \frac{a+b\sqrt{17}}{2} < 4 + \sqrt{17}$, we get $0 < b\sqrt{17} < 5 + \sqrt{17} \Rightarrow 0 < b < 1 + \frac{5\sqrt{17}}{17} < 3$. We have the two cases:

1. If $b = 1$, then $|a^2 - 17| = 4 \Rightarrow a^2 \in \{13, 21\}$ which is not possible if a is an integer.

2. If $b = 2$, then $|a^2 - 17b^2| = 4 \Rightarrow |a^2 - 68| = 4 \Rightarrow a^2 \in \{64, 72\} \Rightarrow a^2 = 68 \Rightarrow a = \pm 8 \Rightarrow u = \pm 4 + \sqrt{17}$. The condition $1 < u$ implies $u = 4 + \sqrt{17}$ which contradicts the choice $u < 4 + \sqrt{17}$.

Assume now that $u \in A$ is a unit such that $1 < u$. $0 < \sqrt{17} - 4 < 1$ is a unit. Since

$$\lim_{n\to\infty} u \cdot (\sqrt{17} - 4)^n = 0,$$

there exists $n \in \mathbb{N}$ such that $u \cdot (\sqrt{17} - 4)^{n+1} < 1 \leq u \cdot (\sqrt{17} - 4)^n$. Let $v = u \cdot (\sqrt{17} - 4)^2$. Then v is a unit and $v \cdot (\sqrt{17} - 4) < 1 \leq v \Rightarrow 1 \leq v < 4 + \sqrt{17}$. Since we have seen that there are no units of A in $(1, 4 + \sqrt{17})$, $v = 1$, hence $u = (4 + \sqrt{17})^n$.

Let now u be an arbitrary unit in A, $u \neq \pm 1$. Then exactly one of the units $\pm u^{\pm 1}$ of A is greater than 1. Using the previous case, we conclude that $u = \pm(4 + \sqrt{17})^n$ for some $n \in \mathbb{Z}$. ■

Chapter 9

Lecture IX

9.1 Test Paper

[1]

Exercise 9.1.1. *Compute the rank of the elliptic curve*

$$C(\mathbb{Q}) : y^2 = x^3 - 82x.$$

Exercise 9.1.2. *Prove that if x, y and z are integers such that $x^4 + 2y^2 = 17z^4$, then $x = y = z = 0$.*

Exercise 9.1.3. *Consider the rational cubic curve*

$$C(\mathbb{Q}) : y(y + x) = x(x - 1)(x + 2).$$

Prove that $(2, 2)$ and $(0, 0)$ belong to $C(\mathbb{Q})$.

Prove that C is smooth and that its unique point at infinity is $O[0 : 1 : 0]$. In 1.2.12 and 1.2.13, we gave $C(\mathbb{Q})$ an abelian group structure with neutral element O. For $n \in \mathbb{N}^*$, let x_n, y_n be the rational numbers defined by $(x_n, y_n) = n \cdot (2, 2) + (0, 0)$, where the operation " + " is the one in $C(\mathbb{Q})$.

Compute x_n for $n \in \overline{1, 5}$. It is known that there exists integers a_n, b_n and t_n such that $gcd(a_n, t_n) = gcd(b_n, t_n) = 1$, $t_n > 0$ and $x_n = \frac{a_n}{t_n^2}$, $y_n = \frac{b_n}{t_n^3}$.

Prove that

$$t_n \cdot t_{n+5} = t_{n+4} \cdot t_{n+1} + t_{n+3} \cdot t_{n+2} \ \forall n \geq 1.$$

The next page contains the solutions to these problems.

[1] Working time 150 minutes. This test paper only counts as extra for the final exam.

9.1.1 Solutions

Solution to 9.1.1: Let $\bar{C}(\mathbb{Q}) : y^2 = x^3 + 328x$. Let r denote the rank of the elliptic curve $C(\mathbb{Q})$. We have proved that

$$2^r = \frac{|Im\alpha| \cdot |Im\alpha'|}{4},$$

where $\alpha : C(\mathbb{Q}) \to \mathcal{Q} = \frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2}$ and $\alpha' : \bar{C}(\mathbb{Q}) \to \mathcal{Q}$ are group homomorphisms. We have seen that $x \in Im\alpha$ if and only if there exists $b_1|82$ such that $\hat{b}_1 = x$ and the equation

$$N^2 = b_1 M^4 - \frac{82}{b_1} e^4$$

has nontrivial solutions i.e. $(N, M, e) \neq (0, 0, 0)$. Similarly, for α' we have the equations

$$N^2 = b_1 M^4 + \frac{328}{b_1} e^4.$$

We first compute $Im\alpha$. The divisors of 82 are $\{\pm 1, \pm 2, \pm 41, \pm 82\}$. Therefore $Im\alpha \subseteq \{\widehat{\pm 1}, \widehat{\pm 2}, \widehat{\pm 41}, \widehat{\pm 82}\}$. We prove that the previous inclusion is in fact equality. To do so, we give nontrivial solutions to each of the equations for $b_1 \in \{\pm 1, \pm 2, \pm 41, \pm 82\}$. To make computations easier, notice that if (N, M, e) is a nontrivial solution to the equation $N^2 = b_1 M^4 - \frac{82}{b_1} e^4$, then (N, e, M) is a nontrivial solution to $N^2 = -\frac{82}{b_1} M^4 - \frac{82}{-\frac{82}{b_1}} e^4 = b_1 e^4 - \frac{82}{b_1} M^4$. This means that $\hat{b}_1 \in Im\alpha \Rightarrow \widehat{-\frac{82}{b_1}} \in Im\alpha$. We have the solutions:

b_1	N	M	e
1	1	0	1
2	11	1	3
41	3	2	1
82	1	1	3

.

Hence $|Im\alpha| = 8$.

We now compute $Im\alpha'$. We have $b_1 < 0 \Leftrightarrow \frac{328}{b_1} < 0$. In this case, $N^2 = b_1 M^4 + \frac{328}{b_1} e^4$ implies $N = M = e = 0$. Therefore the equations $N^2 = b_1 M^4 + \frac{328}{b_1} e^4$ give only trivial solutions for $b_1 < 0$.

The positive divisors of 328 are $\{1, 2, 4, 8, 41, 82, 164, 328\}$, so $Im\alpha' \subseteq \{\hat{1}, \hat{2}, \hat{41}, \hat{82}\}$. We prove that this last inclusion is in fact an equality. Just like for α, we need consider only half the cases, because of the pairing $\left(b_1, \frac{328}{b_1}\right)$.

$\hat{b}_1$	b_1	N	M	e
$\hat{1}$	1	1	0	1
$\hat{2}$	8	7	1	1

.

We have proved $|Im\alpha'| = 4$.
$2^r = \frac{8 \cdot 4}{4} = 8 \Rightarrow r = 3$. ■

Proof of 9.1.2: The problem was solved while proving that

$$rank C_{17}(\mathbb{Q}) = 0,$$

back in Lecture VIII. ■

Proof of 9.1.3: This problem is the subject of the next lecture. ■

Chapter 10

An unexpectedly hard problem

In Lecture III, the following problem appeared as exercise 3.1.8:

Exercise 10.0.4. *Let $(t_n)_{n\geq 1}$ be the sequence of rational numbers defined by $t_1 = t_2 = t_3 = t_4 = t_5 = 1$ and*

$$t_{n+5} = \frac{t_{n+4}t_{n+1} + t_{n+3}t_{n+2}}{t_n}$$

for every $n \geq 1$.

Prove that all the terms of $(t_n)_{n\geq 1}$ are in fact integers.

This problem, presented by Don Zagier on the fifth day of the St. Andrews Colloquium in 1996, has a deceivingly elementary text, but it knows no elementary proof so far. The first hints towards a proof are given by the third problem, 9.1.3 of the Test Paper in the previous lecture:

Exercise 10.0.5. *Consider the rational cubic curve*

$$C(\mathbb{Q}) : y(y + x) = x(x - 1)(x + 2).$$

Prove that $P(2, 2)$ and $T(0, 0)$ belong to $C(\mathbb{Q})$.

Prove that C is smooth and that its unique point at infinity is $O[0 : 1 : 0]$. In 1.2.12 and 1.2.13, we gave $C(\mathbb{Q})$ an abelian group structure with neutral element O. For $n \in \mathbb{N}^*$, let x_n, y_n be the rational numbers defined by $(x_n, y_n) = n \cdot (2, 2) + (0, 0)$, where the operation " + " is the one in $C(\mathbb{Q})$ and $n \cdot \bar{P} = \underbrace{\bar{P} + \bar{P} + \ldots + \bar{P}}_{n \text{ times}}$ for all $\bar{P} \in C(\mathbb{Q})$.

Compute x_n for $n \in \overline{1, 5}$. Prove that there exists integers a_n, b_n and t_n such that $gcd(a_n, t_n) = gcd(b_n, t_n) = 1$, $t_n > 0$ and $x_n = \frac{a_n}{t_n^2}$, $y_n = \frac{b_n}{t_n^3}$.

Prove that

$$t_n \cdot t_{n+5} = t_{n+4} \cdot t_{n+1} + t_{n+3} \cdot t_{n+2}, \ \forall n \geq 1.$$

Proof: $P(2,2)$ and $T(0,0)$ belong to the cubic C. Let $P_n(x_n, y_n) = n \cdot P + T$.

The homogenized equation of $C(\mathbb{Q})$ is $F(x,y,z) = y(y+x)z - x(x-z)(x+2z) = 0$. To prove that C is smooth we have the standard method of computing the partial derivates of F and proving that at each point of $\mathbb{P}^2$ at least one of them does not vanish. This method is quite tedious but fortunately we have a more elegant proof. The rational projective transformation:

$$[x : y : z] \xrightarrow{\rho} [4x : 8y + 4x : z]$$

sends O to itself, T to itself, $P(2,2) = [2 : 2 : 1]$ to $[8 : 24 : 1]$ and C to:

$$C' : y^2 z = x^3 + 5x^2 z - 32xz^2.$$

Clearly C is smooth if and only if C' is smooth. The affine equation of C' has the familiar form $y^2 = f(x) = x^3 + 5x^2 - 32x$. Therefore C' is smooth if and only if $C'(\mathbb{Q})$ is a smooth elliptic curve i.e. if and only if $\Delta_f \neq 0$. $\Delta_f = -32(5^2 + 4 \cdot 32) \neq 0$.

The points at infinity of C are given by $F(x,y,0) = 0 \Leftrightarrow -x^3 = 0 \Leftrightarrow x = 0$. The only projective solution is $O[0 : 1 : 0]$. The rational projective transformation ρ induces an isomorphism between $C(\mathbb{Q})$ and $C'(\mathbb{Q})$.

To compute x_n and y_n for $n = \overline{1,5}$, several methods can be used. We can use the recurrence $P_{n+1} = P_n + P$, or we can compute $\rho(P_n)$ and then apply ρ^{-1}. The results will be:

n	x_n	y_n
1	-1	2
2	-2	0
3	$-\frac{1}{4}$	$-\frac{5}{8}$
4	$-\frac{2}{9}$	$\frac{22}{27}$
5	$-\frac{49}{25}$	$\frac{259}{125}$

The inverse transformation of ρ is given by:

$$[x : y : z] \xrightarrow{\rho^{-1}} [\frac{x}{4} : \frac{y-x}{8} : z].$$

Since $\rho(P_n) \in C'(\mathbb{Q})$, there exist $a'_n, b'_n, t'_n \in \mathbb{Z}$ such that:

$$\rho(P_n) = [a'_n \cdot t'_n : b'_n : (t'_n)^3],\ t'_n > 0 \text{ and } gcd(a'_n, t'_n) = gcd(b'_n, t'_n) = 1.$$

This corresponds to the affine situation $\rho(P_n) = (\frac{a'_n}{(t'_n)^2}, \frac{b'_n}{(t'_n)^3})$ which follows from 2.2.5 if we prove that $\rho(P_n) \neq O$ for all $n \geq 1$. Assume $\rho(P_n) = O$ for some $n \geq 1$. Then $\rho(n \cdot P + T) = O \Rightarrow n \cdot (8,24) + (0,0) = O \Rightarrow 2n \cdot (8,24) + 2 \cdot (0,0) = O$ in $C'(\mathbb{Q})$. In $C'(\mathbb{Q})$, we have $2T = 0$, so $2n \cdot \rho(P) = O$. If that was so, then $\rho(P)$ would be a torsion point of $C'(\mathbb{Q})$. Since T is also

a torsion point and the torsion of an abelian group is a subgroup, we would have that $\rho(P_m)$ is a torsion element of $C'(\mathbb{Q})$ for all $m \geq 1$. By Nagell-Lutz, a torsion point on an elliptic curve has integer coordinates, so $\rho(P_m)$ would have integer coordinates for all $m \geq 1$. But $\rho(P_4) = \rho\left(-\frac{2}{9}, \frac{22}{27}\right) = \rho([-6 : 22 : 27]) = [-24 : 152 : 27] = \left(-\frac{8}{9}, \frac{152}{27}\right)$ which clearly does not have integer coordinates. Here we also have proved that P is not a torsion point of $C(\mathbb{Q})$.

$P_n = \rho^{-1}([a'_n \cdot t'_n : b'_n : (t'_n)^3]) = [\frac{a'_n t'_n}{4} : \frac{b'_n - a'_n t'_n}{8} : (t'_n)^3] = [2a'_n t'_n : b'_n - a'_n t'_n : (2t'_n)^3]$. For all $n \geq 1$, define the triplet (a_n, b_n, t_n) by:

$$(a_n, b_n, t_n) = \begin{cases} (a'_n, b'_n - a'_n t'_n, 2t'_n), & \text{if } a'_n \text{ is odd} \\ \left(\frac{a'_n}{4}, \frac{b'_n - a'_n t'_n}{8}, t'_n\right), & \text{if } a'_n \text{ is even} \end{cases}.$$

We will prove that a_n, b_n, t_n are integers $t_n > 0$ and $gcd(a_n, t_n) = gcd(b_n, t_n) = 1$. Since $t'_n > 0$ for all $n \geq 1$, we get that $t_n > 1$ for all $n \geq 1$.

If a'_n is odd, then clearly a_n, b_n, t_n are integers and $gcd(a'_n, 2t'_n) = 1$. Assume p is a prime number such that $p|gcd(b_n, t_n) \Leftrightarrow p|b'_n - a'_n t'_n$ and $p|2t'_n$. Since $\rho(P_n) \in C'(\mathbb{Q})$, we have $(b'_n)^2(t'_n)^3 = (a'_n)^3(t'_n)^3 + 5(a'_n)^2(t'_n)^5 - 32a'_n(t'_n)^7 \Rightarrow (b'_n)^2 = (a'_n)^3 + 5(a'_n)^2(t'_n)^2 - 32a'_n(t'_n)^4$. $p|b'_n - a'_n t'_n \Rightarrow p|(a'_n)^3 + 4(a'_n)^2(t'_n) - 32a'_n(t'_n)^4$. Together with $p|2t'_n$ this yields $p|(a'_n)^3$ which contradicts $gcd(a'_n, 2t'_n) = 1$. Therefore $gcd(b'_n - a'_n t'_n, 2t'_n) = 1$.

If a'_n is even then from $(b'_n)^2 = (a'_n)^3 + 5(a'_n)^2(t'_n)^2 - 32a'_n(t'_n)^4$ we get that b'_n is also even. We want to prove that a_n, b_n, t_n are integers and $gcd(a_n, t_n) = gcd(b_n, t_n) = 1$. Let $a'_n = 2a$, $b'_n = 2b$ and $t'_n = t$. The condition $gcd(a'_n, t'_n) = 1$ proves that $t = t'_n$ is odd. Then $b^2 = 2a^3 + 5a^2t^2 - 16at^4$. To prove that a_n is an integer, we must prove that $4|a'_n \Leftrightarrow 2|a$. Assume a is odd. Modulo 8, we have $b^2 \equiv 2a^3 + 5a^2t^2$. Since a and t are odd, we get that b is odd, so $1 \equiv 2a + 5(mod 8) \Rightarrow 2a \equiv 4(mod 8) \Rightarrow a \equiv 2(mod 4)$ which is impossible if a is odd. Therefore a is even and $4|a'_n$, so a_n is an integer. To prove that b_n is an integer, we must prove that $8|b'_n - a'_n t'_n \Leftrightarrow 4|b - at$. $b^2 = 2a^3 + 5a^2t^2 - 16at^4 \Rightarrow 2|b$. Let $b = 2\bar{b}$ and $a = 2\bar{a}$. Then $\bar{b}^2 = 4\bar{a}^3 + 5\bar{a}^2t^2 - 8\bar{a}t^4 \Rightarrow 4|\bar{b}^2 - \bar{a}^2t^2 \Rightarrow \bar{b}$ and $\bar{a}t$ have the same parity. So $2|\bar{b} - \bar{a}t \Rightarrow 8|b'_n - a'_n t'_n \Rightarrow b_n \in \mathbb{Z}$. Similarly to the previous case we prove $gcd(a_n, t_n) = gcd(b_n, t_n) = 1$.

We have proved that for all $n \geq 1$ there exist integers a_n, b_n and t_n such that $t_n > 0$, $gcd(a_n, t_n) = gcd(b_n, t_n) = 1$ and $P_n(x_n, y_n) = [a_n t_n : b_n : t_n^3]$ from which it follows that $x_n = \frac{a_n}{t_n^2}$ and $y_n = \frac{b_n}{t_n^3}$.

The "only" thing left to prove is the recurrence $t_{n+5}t_n = t_{n+4}t_{n+1} + t_{n+3}t_{n+2}$. Let's see that this is the same as proving 10.0.4. The recurrence is the same, but the initial terms slightly differ. If we look at P_n for $n = \overline{1, n}$, we get $t_1 = t_2 = 1$, $t_3 = 2$, $t_4 = 3$ and $t_5 = 5$. The first five terms in 10.0.4 are $t_1 = t_2 = t_3 = t_4 = t_5 = 1$. However $t_6 = 2$, $t_7 = 3$ and $t_8 = 3$. So if we manage to solve 10.0.5 we also obtain the other sequence, but shifted 3

places to the right which changes nothing on the recurrence or on the terms of the sequence being integers.

Consider the projective rational transformation given by

$$[x : y : z] \overset{\varphi}{\to} [2z - y - 3x : 2z + y - 2x : 2z - x].$$

The corresponding affine map is $\varphi(x, y) = \left(\frac{2-y-3x}{2-x}, \frac{2+y-2x}{2-x}\right)$.

Let $C_1 : (xy + z^2)(5z - x - y) = 6z^3$. We will prove that $\varphi(C(\mathbb{Q})) = C_1(\mathbb{Q})$. For this, let $[x : y : z] \in C(\mathbb{Q})$, $u = 2z - y - 3x$, $v = 2z + y - 2x$ and $t = 2z - x$. We must prove that $(uv + t^2)(5t - u - v) = 6t^3$. $uv = 4z^2 - 10xz - (y + 3x)(y - 2x)$. $u + v = 4z - 5x$. $(uv + t^2)(5t - u - v) = (4z^2 - 10xz - y^2 - xy + 6x^2 + 4z^2 - 4xz + x^2)(10z - 5x - 4z + 5x) = (-y^2 - xy + 7x^2 - 14xz + 8z^2) \cdot 6z = 6(-y(y+x)z + 7x^2z - 14xz^2 + 8z^3)$. Now we use $[x : y : z] \in C(\mathbb{Q})$. $y(y+x)z = x(x-z)(x+2z) \Rightarrow (uv+t^2)(5t-u-v) = 6(-x^3 - x^2z + 2xz^2 + 7x^2z - 14xz^2 + 8z^3) = 6(-x^3 + 6x^2z - 12xz^2 + 8z^3) = 6(2z - x)^3 = 6t^3$.

The inverse of φ is given by $[x : y : z] \overset{\varphi^{-1}}{\to} [2x + 2y - 4z : 2x - 4y + 2z : x + y - 5z]$ and the affine map is $\varphi^{-1}(x, y) = \left(2 \cdot \frac{x+y-2}{x+y-5}, 2 \cdot \frac{x-2y+1}{x+y-5}\right)$.

φ induces an isomorphism from $C(\mathbb{Q})$ to $C_1(\mathbb{Q})$. The neutral element of $C_1(\mathbb{Q})$ is $\varphi(O) = [-1 : 1 : 0]$ and not O like for C and C'.

Lemma 10.0.6. *Let* $v_n = \frac{t_n t_{n+3}}{t_{n+1} t_{n+2}}$. *Then* $\varphi(P_{n+2}) = (v_n, v_{n+1})$ *for every* $n \geq 1$.

Assume we have proved it. Then notice that $(u, v) \in C_1(\mathbb{Q}) \Rightarrow (v, u) \in C_1(\mathbb{Q})$ because the affine equation of C_1, $(xy+1)(5-x-y) = 6$, is symmetric in x and y. Actually we can prove that if $(u, v) \in C_1(\mathbb{Q})$, then $-(u, v)$, the inverse of (u, v) in $C_1(\mathbb{Q})$ is (v, u). If $uv \neq 0$, then $(uv+1)(5-u-v) = 6 \Leftrightarrow v^2 + (\frac{1}{u} + u - 5)v + \frac{u+1}{u} = 0$. By Viete's relations, the last equation has the solution v for fixed u if and only if it has also the solution $\frac{u+1}{uv}$. The same argument holds for proving that if $u \neq 0$, then the affine line $x = u$ cuts $C_1(\mathbb{Q})$ in at most two points. So, for $uv \neq 0$, we have $\left(v, \frac{v+1}{uv}\right) \in C_1(\mathbb{Q}) \Leftrightarrow (v, u) \in C_1(\mathbb{Q}) \Leftrightarrow (u, v) \in C_1(\mathbb{Q}) \Leftrightarrow \left(u, \frac{u+1}{uv}\right) \in C_1(\mathbb{Q})$.

Since $t_n > 0$ for all $n \geq 1$, it is easy to see that $v_n > 0$ for all $n \geq 1$.

Assuming the lemma, we have $\varphi(P_{n+2}) = (v_n, v_{n+1}) \in C_1(\mathbb{Q}) \Rightarrow (v_{n+1}, v_n) \in C_1(\mathbb{Q})$. Also $(v_{n+1}, v_{n+2}) = \varphi(P_{n+3}) \in C_1(\mathbb{Q})$ and $\left(v_{n+1}, \frac{v_{n+1}+1}{v_n v_{n+1}}\right) \in C_1(\mathbb{Q})$. Since the affine line $x = v_{n+1}$ cuts $C_1(\mathbb{Q})$ in at most the two points (v_{n+1}, v_n) and $\left(v_{n+1}, \frac{v_{n+1}+1}{v_n v_{n+1}}\right)$, we have $v_{n+2} = v_n$ or $v_{n+2} = \frac{v_{n+1}+1}{v_n v_{n+1}}$.

If $v_{n+2} = \frac{v_{n+1}+1}{v_n v_{n+1}}$, then $1 + \frac{1}{v_{n+1}} = v_n \cdot v_{n+2} \Rightarrow 1 + \frac{t_{n+2}t_{n+3}}{t_{n+1}t_{n+4}} = \frac{t_n t_{n+3}}{t_{n+1}t_{n+2}} \cdot \frac{t_{n+2}t_{n+5}}{t_{n+3}t_{n+4}} \Rightarrow t_{n+1}t_{n+4} + t_{n+2}t_{n+3} = t_n t_{n+5}$.

Assume for a contradiction that there exists an n such that $v_n = v_{n+2}$. Then $(v_n, v_{n+1}) = -(v_{n+1}, v_{n+2}) \Rightarrow \varphi(P_{n+2}) = -\varphi(P_{n+3}) \Rightarrow \varphi(P_{n+2} + P_{n+3}) = O \Rightarrow P_{n+2} + P_{n+3} = O \Rightarrow (n+2)P + T + (n+3) + T = O \Rightarrow$

$(2n+5)P = O$ which contradicts that P is not a torsion point of $C(\mathbb{Q})$. We have used that φ is a group isomorphism. Therefore we have the recurrence $t_{n+5}t_n = t_{n+4}t_{n+1} + t_{n+3}t_{n+2}$ for all $n \geq 1$. What is left to prove is 10.0.6.

Lemma 10.0.7. *If $n \geq 1$, then $x_n < 0$.*

Proof: We prove this by induction on n. We already have checked it for $n = \overline{1,5}$. $P_{n+1} = P_n + (2,2)$. $P_n \neq P(2,2)$ since $x_n < 0 < 2$. The equation of the line P_nP is $\frac{y-2}{x-2} = \frac{y_n-2}{x_n-2}$. When we intersect it again with C we find

$$x_{n+1} = \frac{-4 - 6y_n + 2x_n^2 + 4x_n}{(x_n-2)^2}.$$

$x_{n+1} < 0 \Leftrightarrow -4 - 6y_n + 2x_n^2 + 2x_n < 0 \Leftrightarrow x_n^2 + 2x_n - 2 < 3y_n \Leftrightarrow y_n(y_n + x_n) + x_n^2 = x_n^3 + 2x_n^2 - 2x_n > 3x_ny_n$ which holds if $x_n \neq y_n$. If not, then $x_{n+1} = 0$ which implies $y_{n+1} = 0$, so $P_{n+1} = T$. This is impossible since P and P_m are not torsion points of $C(\mathbb{Q})$ for any m. ∎

Lemma 10.0.8. *For every $n \geq 1$, we have $a_{n+2} - t_{n+2}^2 = -t_nt_{n+4}$.*

Proof: Denote $a_{n+2} = a$, $b_{n+2} = b$ and $t_{n+2} = t$. $P_{n+2} \in C(\mathbb{Q}) \Rightarrow \frac{b}{t^3}(\frac{b}{t^3} + \frac{a}{t^2}) = \frac{a}{t^2}\left(\frac{a}{t^2} - 1\right)\left(\frac{a}{t^2} + 2\right) \Rightarrow b(b+at) = a(a-t^2)(a+2t^2)$. We have $P_{n+4} = P_{n+2} + 2 \cdot (2,2)$.

Notice that if $Q(x,y) \in C(\mathbb{Q})$, then $-Q = Q * O$ is the second point of intersection of C and $\{X = x\}$. It is not hard to see that this point is $-Q(x, -y-x)$.

The tangent to C at $P(2,2)$ is $2x - y - 2 = 0$. It cuts C again at $(1,0)$, so $2P = O * (1,0) = (1,-1)$.

The equation of the line $P_{n+2}(1,-1)$ is $\frac{y+1}{x-1} = \frac{y_{n+2}+1}{x_{n+2}-1} = \frac{\frac{b}{t^3}+1}{\frac{a}{t^2}-1} = \frac{b+t^3}{at-t^3} = \alpha$. The x-coordinates of the intersection of $P_{n+2}(1,-1)$ and $C(\mathbb{Q})$ are given by $(\alpha(x-1)-1)(\alpha(x-1)+(x-1)) = x(x-1)(x+2)$. Since we already know that this equation has the solutions 1 and x_{n+2}, we find $x_{n+4} = \frac{(\alpha+1)^2}{x_{n+2}} = \frac{\left(\frac{b+at}{at-t^3}\right)^2 \cdot t^2}{a} = \frac{(b+at)^2}{a(a-t^2)^2} = \frac{b^2+2abt+a^2t^2}{a(a-t^2)^2} = \frac{a(a-t^2)(a+2t^2)+abt+a^2t^2}{a(a-t^2)^2} = \frac{a^2+at^2-2t^4+bt+at^2}{(a-t^2)^2} = 1 + \frac{4t^2(a-t^2)+t(b+t^3)}{(a-t^2)^2}$.

Similarly, $P_n = P_{n+2} - 2(2,2) = P_{n+2} + (1,0)$ and $x_n = 1 + \frac{3t^2(a-t^2)-tb}{(a-t^2)^2}$.

Since $x_n = \frac{a_n}{t_n^2}$, $x_{n+4} = \frac{a_{n+4}}{t_{n+4}^2}$ and $gcd(a_n, t_n) = gcd(a_{n+4}, t_{n+4}) = 1$, the certain thing to say is $t_{n+4}|a - t^2$ and $t_n|a - t^2$.

Let p be a prime number such that $p|a - t^2$. Then $p|b(b+at) = a(a - t^2)(a + 2t^2)$. If p was to divide both b and $b + at$, then $p|at$ which together with $p|a - t^2$ yields $p|gcd(a,t)$ which contradicts $gcd(a,t) = 1$. By Lemma 10.0.7, $x_{n+2} < 0 \Rightarrow \frac{a}{t^2} < 0$. In particular, this implies $a \neq t^2$. If $p|b + at$, then since $p|a - t^2$, also $p|b + t^3$. Let $v_p(a - t^2) = k$ i.e. $p^k|a - t^2$ and $p^{k+1} \not| a - t^2$. Then it is easy to prove that $p^k|b$ or $p^k|b + t^3$.

If $p^k|b$, then we will prove that $p^{2k}|3t^2(a-t^2)-tb$. If $p^k|b+t^3$, then we prove that $p^{2k}|4t^2(a-t^2)+t(b+t^3)$. Let's see how these solve this lemma. t_n^2 is obtained from $(a-t^2)^2$ by clearing the factors it has in common with $3t^2(a-t^2)-tb$. If p is a prime dividing both $a-t^2$ and $3t^2(a-t^2)-tb$, then $p|tb$. If $p|t$, then also $p|a$ which contradicts $gcd(a,t)=1$. Therefore $p|b$ and in this case $v_p(a-t^2)=k \Rightarrow p^{2k}|3t^2(a-t^2)-tb$ which means nothing else than $p \not| t_n$. A similar argument proves that if p divides both $a-t^2$ and $4t^2(a-t^2)+t(b+t^3)$, then it does not divide t_{n+4}. But any prime number dividing $a-t^2$ divides exactly one of the numbers $4t^2(a-t^2)+t(b+t^3)$ and $3t^2(a-t^2)-tb$. So the prime factors of $a-t^2$ are split at their greatest powers between t_n and t_{n+4} who both divide $a-t^2$. Hence $t_nt_{n+4}=\pm(a-t^2)$. How do we decide on the sign then? By the previous lemma, $x_{n+2}<0 \Leftrightarrow \frac{a_{n+2}}{t_{n+2}^2}<0 \Leftrightarrow a=a_{n+2}<0$. Since $t_m>0 \ \forall \ m\geq 1$, we have $\pm(a-t^2)=t_nt_{n+4}\geq 1$. If the sign was " $+$ ", then we would have $0>a-t^2\geq 1$ which is impossible. Therefore the sign is " $-$ " and $t_nt_{n+4}=a-t^2=a_{n+2}-t_{n+2}^2$.

Assume then that $p^k|b$, so there exist $\alpha,\beta\in\mathbb{Z}$ such that $a-t^2=p^k\alpha$ and $b=p^k\beta$. We know that $b(b+at)=a(a-t^2)(a+2t^2)$, hence $\beta(b+at)=a\alpha(a+2t^2)\Rightarrow \beta t^3\equiv t^2\alpha(3t^2)(mod\ p^k)\Rightarrow p^k|3t^2\alpha-t\beta\Rightarrow p^{2k}|3t^2(a-t^2)-tb$. We have used that $gcd(b,t)=1$ and $p|b$ imply $p \not| t$. The case $p^k|b+t^3$ is treated similarly. ■

Lemma 10.0.9. *For all n we have:*

$$\frac{t_{n+3}t_n}{t_{n+1}}=\frac{-3at-b+2t^3}{2t^2-a} \ \textit{and}$$

$$\frac{t_{n+4}t_{n+1}}{t_{n+3}}=\frac{-2at+b+2t^3}{2t^2-a},$$

where $(a,b,t)=(a_{n+2},b_{n+2},t_{n+2})$.

Proof: We first prove that these equalities imply each other, so it suffices to prove just one of them. By multiplying the two, and keeping in mind the equation $(xy+1)(5-x-y)=6$ of $C'(\mathbb{Q})=\varphi(C(\mathbb{Q}))$, we get

$$t_nt_{n+4}=\frac{(-3at-b+2t^3)(-2at+b+2t^3)}{(2t^2-a)^2}=t^2\alpha\beta=t^2\cdot\left(\frac{1+\alpha+\beta}{5-\alpha-\beta}\right),$$

with $(\alpha,\beta)=\varphi(x,y)=\left(\frac{2-y-3x}{2-x},\frac{2+y-2x}{2-x}\right)$. Since $\alpha+\beta=\frac{4-5x}{2-x}$, we get $t_nt_{n+4}=t^2(1-x)=-a+t^2=-a_{n+2}+t_{n+2}^2$ which is Lemma 10.0.8. Hence it is enough to prove just one of the assertions of Lemma 10.0.9.

Let's say we want to prove

$$\frac{t_{n+3}t_n}{t_{n+1}}=\frac{-3at-b+2t^3}{2t^2-a}$$

for all $n \geq 1$. Following the ideas in Lemma 10.0.8 it can be proved that:

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} x_{n+3} = 2 + \frac{12t^2(a-2t^2)-6t(b-2t^3)}{(a-2t^2)^2} \\ x_{n+1} = 2 + \frac{18t^2(a-2t^2)+6t(b+4t^3)}{(a-2t^2)^2} \end{array} \right. \Rightarrow t_{n+3}t_{n+1} = \frac{2t^2-a}{gcd(2t^2-a,6)} \\ \left\{ \begin{array}{l} x_{n+3} = 2 + \frac{12t^2(a-2t^2)-6t(b-2t^3)}{(a-2t^2)^2} \\ x_n = 1 + \frac{3t^2(a-t^2)-tb}{(a-t^2)^2} \end{array} \right. \Rightarrow t_{n+3}^2 t_n = \frac{-3at-b+2t^3}{gcd(2t^2-a,6)} \end{array} \right. .$$

The result follows obviously by dividing the two new relations. ■

From Lemma 10.0.9, it follows $v_n = \frac{t_{n+3}t_n}{t_{n+2}t_{n+1}} = \frac{1}{t} \cdot \frac{-3at-b+2t^3}{2t^2-a} = \frac{-3\frac{a}{t^2} - \frac{b}{t^3} + 2}{2-\frac{a}{t^3}} = \frac{2-y-3x}{2-x}$. Similarly $v_{n+1} = \frac{2+y-2x}{2-x}$. It follows that $\varphi(x_{n+2}, y_{n+2}) = (v_n, v_{n+1})$ and so Lemma 10.0.6 is proved. We have seen how this completes the proof of the problem. ■

Chapter 11

Integer points on elliptic curves

So far we have only been interested in the structure of the rational points $C(\mathbb{Q})$ of an elliptic curve given by $C : y^2 = x^3 + ax^2 + bx + c$. But for ages number theorists have been interested in Diophantine Equations. To honor their work, we begin the study of integer points on elliptic curves. The Diophantine Equation to consider is $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$. In the spirit of the course, we denote the set of integer solutions of this equation by $C(\mathbb{Z})$.

One of the strongest results in connection to this problem is:

Theorem 11.0.10 (Siegel). *If C is nonsingular, then the equation $y^2 = x^3 + ax^2 + bx + c$ has a finite number of integer solutions i.e. $C(\mathbb{Z})$ is finite.*

Notice that Siegel's Theorem does not hold if we drop the assumption on the non-singularity of C. For example, the equation $y^2 = x^3$ has an infinite number of integer solutions. They can actually pe parameterized as $(x, y) \in \{(t^2, t^3) |\ t \in \mathbb{Z}\}$.

For the time being we leave aside the proof of Siegel's Theorem and shall content ourselves to prove another result concerning equations of a more particular form. This is Thue's Theorem proved by Thue around 1909. We dedicate to it the next section.

11.1 Thue's Theorem

Theorem 11.1.1 (Thue). *If $a, b, c \in \mathbb{Z}^*$, then the equation $C(\mathbb{Z}) : ax^3 + by^3 = c$ has a finite number of integer solutions.*

In connection to Thue's Theorem we have the next two famous equations:

Proposition 11.1.2. *If d is a positive integer which is not the cubic power of another integer then the equation $x^3 - dy^3 = 1$ has at most two integer solutions.*

We will return to this problem in the final lecture.

Another particular case of the equation in Thue's Theorem, is Mordell's Equation:

$$y^2 = x^3 - k, \text{ given that } k \neq 0.$$

We have already treated some particular cases of Mordell's Equation in 3.2.3.

11.1.1 Proof of Thue's Theorem and Diophantine Approximation

We want to prove that given $a, b, c, \in \mathbb{Z}^*$, the equation $ax^3 + by^3 = c$ has a finite number of integer solutions. By multiplying the equation with a^2 we obtain the equivalent equation $(ax)^3 + (a^2b)y^3 = (a^2c)$. Its integer solutions are in one-to-one correspondence to the integer solutions of the equation $x^3 - (-a^2b)y^2 = (a^2c)$ for which $a|x$. We see that if we prove that for $b, c \in \mathbb{Z}^*$, the equation $x^3 - by^3 = c$ has a finite number of solutions, then Thue's Theorem follows.

If $b = k^3$ for some $k \in \mathbb{Z}$, then the equation is $(x-ky)(x^2+kxy+k^2y^2) = c$. Since $c \neq 0$, solving the equation reduces to solving the simple system of equations in integers:

$$\begin{cases} x - ky = c_1 \\ x^2 + kxy + k^2y^2 = c_2 \\ c_1 \cdot c_2 = c \end{cases}.$$

Let's take an example for this case:

Example 11.1.3. *Solve in integers the equation:* $x^3 + y^3 = 1729$.

Solution: We have to solve the system:

$$\begin{cases} x + y = c_1 \\ x^2 - xy + y^2 = c_2 \\ c_1 \cdot c_2 = 1729 \end{cases}.$$

We have the prime factor decomposition $1729 = 7 \cdot 13 \cdot 19$. It is easy to see that $x^2 - xy + y^2 > 0$, so we need only consider the positive candidates for c_1 and c_2. The solutions given by solving the equations are $(9, 10), (10, 9), (1, 12), (12, 1)$. ■

This example was not given at random. 1729 is the first positive integer that can be written in two distinct ways as a sum of two cubes. It also has an anecdote attached. It is said that one day Hardy, the famous mathematician, was visiting his not less famous, hospitalized friend, Ramanujan. To cheer him up, he told Ramanujan that he was extremely bored by his ride to the hospital. He was displeased because 1729, the number of the carriage he used, was completely uninteresting to him. Believe it or not, after a moment of thought, Ramanujan pointed his friend on the nice property of 1729 we have described above.

Conjecture 11.1.4. *It is an open problem whether for all $n \geq 1$ there exists an $m \in \mathbb{Z}$ such that the equation $x^3 + y^3 = m$ has exactly n distinct integer solutions with $x \geq y$.*

We return to the proof of Thue's Theorem by studying the equations of the form $x^3 - by^3 = c$ with $b, c \in \mathbb{Z}^*$ and b and integer which is not the cubic power of another integer. Eventually by multiplying the equation by -1 and replacing x or y by $-x$ or $-y$ respectively, we can assume that b and c are positive integers. We can consider only the case when b is not a cube because we have already seen how to treat the other case.

Let $\beta = \sqrt[3]{b}$. The equation can be rewritten as $(x-y\beta)(x^2+xy\beta+y^2\beta^2) = c$. It is easy to prove $x^2+xy\beta+y^2\beta^2 \geq \frac{3}{4}\beta^2y^2$. We have at most one solution for $x^3 + 0^3 = c$, so at most one solution with $y = 0$.

With $y \neq 0$, we have $x - y\beta = \frac{c}{x^2+xy\beta+y^2\beta^2} \leq \frac{c}{\frac{3}{4}\beta^2y^2} = \frac{4c}{3\beta^2y^2}$. Since by the assumption $b, c \in \mathbb{N}^*$, $c > 0$, the right hand side of the previous inequality is positive, hence so is the left hand side. Therefore

$$\left|\frac{x}{y} - \beta\right| \leq \frac{4c}{3\beta^2}\left|\frac{1}{y^3}\right|.$$

If we manage to prove that this inequality has a finite number of integer solutions (x, y), then we are done. This is achieved by *Diophantine Approximation*, which will justify in full the second part of the title of this subsection.

In 1909 Thue actually proved a much stronger version of the theorem we prove here:

Theorem 11.1.5 (Thue). *Let $f \in \mathbb{Z}[X, Y]$ be a homogeneous polynomial of degree greater of equal to 3. We assume that $f(X, 1)$ is irreducible in $\mathbb{Q}[X]$. Then for every $k \in \mathbb{Z}$, the equation $f(x, y) = k$ has only a finite number of integer solutions.*

To prove this, Thue first proved the following approximation theorem:

Theorem 11.1.6 (Thue). *Let $f \in \mathbb{Z}[X]$ be a polynomial, irreducible over $\mathbb{Q}[X]$, of degree $d \geq 3$ and let β be one of its complex roots. Then for all real $\varepsilon > 0$ and $C > 0$ there exists only a finite number of pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ such that $\left|\frac{p}{q} - \beta\right| \leq \frac{C}{q^{\frac{d}{2}+1+\varepsilon}}$.*

This theorem is part of the following approximation problem: In the conditions of the theorem above, what is the smallest function $\tau : \mathbb{N} \to \mathbb{R}_+$ for which there are only a finite number of pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ such that

$\left|\frac{p}{q}-\beta\right| \leq \frac{C}{q^{\tau(d)+\varepsilon}}$. The history of the advances made in this problem is:

$$\begin{array}{cc} Liouville(1850) & \tau(d)=d \\ Thue(1909) & \tau(d)=\frac{d}{2}+1 \\ Siegel(1921) & \tau(d)=2\sqrt{d} \\ Gelfon,\ Dyson(1947) & \tau(d)=\sqrt{2d} \\ Roth(1955) & \tau(d)=2 \end{array}$$

Roth also proved that the bound $\tau(d)=2$ cannot be improved. He was awarded the Fields Prize for his contribution to this problem.

To solve our problem, we will prove the following particularization of the previous approximation theorem:

Theorem 11.1.7 (Thue). *If $b \in \mathbb{N}^*$ such that $\beta = \sqrt[3]{b} \notin \mathbb{Q}$ and C is a positive real number, then there is a finite number of pairs $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ such that $\left|\frac{p}{q}-\beta\right| < \frac{C}{q^3}$.*

The proof of this theorem is made up of a series of technical lemmas.

Lemma 11.1.8 (Siegel's Lemma). *Let $N > M$ be two positive integers and let $(a_{ij})_{i=\overline{1,M},j=\overline{1,N}} \in \mathbb{Z}$, not all 0. Then the system:*

$$\begin{cases} a_{11}T_1 + a_{12}T_2 + \ldots + a_{1N}T_N = 0 \\ a_{21}T_1 + a_{22}T_2 + \ldots + a_{2N}T_N = 0 \\ \vdots \\ a_{M1}T_1 + a_{M2}T_2 + \ldots + a_{MN}T_N = 0 \end{cases}$$

has a nontrivial solution such that

$$\max\{|T_i| \mid i=\overline{1,N}\} < 2(4N \cdot \max\{|a_{ij}| \mid i=\overline{1,M}, j=\overline{1,N}\})^{\frac{M}{N-M}}.$$

Proof: Let $A \in M_{M,N}(\mathbb{Z})$ be the matrix whose entries are $(a_{ij})_{i=\overline{1,N},j=\overline{1,M}}$. Let $t \in M_{N,1}(\mathbb{Z})$ be the vertical vector whose entries are $(T_i)_{i=\overline{1,N}}$. Denote $\| t \| = \max\{|T_i| \mid i=\overline{1,N}\}$ and $\| A \| = \max\{|a_{ij}| \mid i=\overline{1,M}, j=\overline{1,N}\}$.

We are looking for t such that $At=0$ and $\| t \| < 2(4N \cdot \| A \|)^{\frac{M}{N-M}}$.

For arbitrary $H>1$, let

$$T_H = \{t \in \mathbb{Z}^N \mid \| t \| \leq H\}.$$

By the triangle inequality we see that $t \in T_H \Rightarrow \| At \| \leq N \cdot \| A \| \cdot H$. If we set

$$U_H = \{u \in \mathbb{Z}^M \mid \| u \| \leq N \cdot H \cdot \| A \|\},$$

we have proved that

$$t \in T_H \Rightarrow At \in U_H.$$

A simple count yields $|T_H| = (2[H]+1)^N$ and $|U_H| = (2[NH\cdot \parallel A \parallel]+1)^M$, where $[H]$ denotes the integer part of H, i.e. the greatest integer least or equal to H.

Since $N > M$, there exists $H > 0$ such that $(2[H]+1)^N > (2[NH\cdot \parallel A \parallel]+1)^M$. For such H we have $|T_H| > |U_H|$. Since A sends T_H into U_H, there exist $t_1 \neq t_2$ in T_H such that $At_1 = At_2$. Then for $t = t_1 - t_2$ we have $t \neq 0$, $At = 0$ and $\parallel t \parallel \leq 2H$.

To finish the proof of the lemma we must prove that we can choose such H with the additional restriction $H < (4N\cdot \parallel A \parallel)^{\frac{M}{N-M}}$. So we need $H > 0$ with $(2[H]+1)^N > (2[NH\cdot \parallel A \parallel]+1)^M$ and $H < (4N\cdot \parallel A \parallel)^{\frac{M}{N-M}}$.

We have $(2[H]+1)^N > (2H-1)^N \geq H^N$ and $(2[NH\cdot \parallel A \parallel]+1)^M \leq (2NH\cdot \parallel A \parallel +1)^M \leq (3NH \parallel A \parallel)^M$. Thus for having $(2[H]+1)^N > (2[NH\cdot \parallel A \parallel]+1)^M$, it suffices $H^N \geq (3HN\cdot \parallel A \parallel)^M \Leftrightarrow H \geq (3N \parallel A \parallel)^{\frac{M}{N-M}}$. We take $H = (3N \parallel A \parallel)^{\frac{M}{N-M}}$ to finish the proof of the lemma. ■

Theorem 11.1.9 (Auxiliary Polynomial). *Let $b \in \mathbb{N}^*$ such that $\beta = \sqrt[3]{b} \notin \mathbb{Q}$. Let $m, n \in \mathbb{N}$ such that $m+1 > \frac{2n}{3} \geq m \geq 3$ i.e. $3 \leq m = \left[\frac{2n}{3}\right]$. Then there exist $P, Q \in \mathbb{Z}[X]$, not both 0, both of degree at most $m+n$, $P(X) = \sum_{i=0}^{m+n} u_i X^i$, $Q(X) = \sum_{i=0}^{m+n} v_i X^i$, such that $F^{(k)}(\beta,\beta) = 0$ for all $k = \overline{0, n-1}$ and*

$$\max\{|u_i|,\ |v_j| \mid i,j = \overline{0, m+n}\} \leq 2(16b)^{9(m+n)},$$

where $F(X,Y) = P(X) + Y\cdot Q(X)$ and $F^{(k)}(x,y) \overset{not}{=} \frac{1}{k!}\cdot \frac{\partial^k F}{\partial X^k}(x,y)$.

Proof: First of all we will be looking for a polynomial $F(x,y) = \sum_{i=0}^{m+n}(u_i x^i + v_i x^i y)$ such that $F^{(k)}(\beta,\beta) = 0$ for all $k = \overline{0, n-1}$. It is easy to see that

$$F^{(k)}(x,y) = \sum_{i=k}^{m+n}\left(u_i x^{i-k}\cdot \binom{i}{k} + v_i x^{i-k} y\cdot \binom{i}{k}\right) =$$

$$= \sum_{j=0}^{m+n-k}\left(u_{k+j}x^j\cdot \binom{j+k}{k} + v_{k+j}x^j y\cdot \binom{j+k}{k}\right).$$

$\binom{n}{k}$ denotes the binomial coefficient equal to $\frac{n!}{(n-k)!\cdot k!}$, also denoted by C_n^k. When we substitute $x = y = \beta$ in the previous polynomial equality, we get

$$F^{(k)}(\beta,\beta) = \sum_{j=0}^{m+n-k}\left(\binom{j+k}{k}\cdot u_{k+j}\beta^j + \binom{j+k}{k}\cdot v_{k+j}\beta^{j+1}\right) =$$

$$= \sum_{i=0}^{m+n-k+1}\left(\binom{i+k}{k}\cdot u_{k+i} + \binom{i+k-1}{k}\cdot v_{k+i-1}\right)\cdot \beta^i.$$

We use the convention $\binom{n}{k} = 0$ if $k > n$. Keeping in mind that $\beta^3 = b$, we can write

$$F^{(k)}(\beta,\beta) = \sum_{l=0}^{2} \left(\sum_{0=i=3j+l}^{m+n-k+1} \left(\binom{i+k}{k} \cdot u_{i+l} + \binom{i+k-1}{k} \cdot v_{i+l-1} \right) \cdot b^j \right) \cdot \beta^l.$$

The index i in the previous expression is an auxiliary index (no connection with the name of the theorem we prove) used to shorten the writing of the formula. The second sum actually runs with j from 0 to $\left[\frac{m+n-k-l+1}{3}\right]$.

To have $F^{(k)}(\beta,\beta) = 0$ for all $k = \overline{0, n-1}$, it is enough to have

$$\sum_{j=0}^{\left[\frac{m+n-k-l+1}{3}\right]} \left(\binom{3j+l+k}{k} \cdot u_{k+3j+l} + \binom{3j+l+k-1}{k} \cdot v_{k+3j+l-1} \right) = 0$$

for all $k = \overline{0, n-1}$ and $l = \overline{0, 2}$. The conditions are also necessary since $\{1, \beta, \beta^2\}$ are linearly independent over $\mathbb{Q}$. We can see this as a linear system of $3n$ equations with $2(m+n+1)$ numbers to determinate i.e. u_r and v_r with $r = \overline{0, m+n}$. Denote $M = 3n$ and $N = 2(m+n+1)$.

If we prove that $N > M$, then by Siegel's Lemma 11.1.8, it follows that there exist u_i and v_j for all $i, j = \overline{0, m+n}$, not all 0, such that

$$\max\{|u_i|,\ |v_j| \mid i, j = \overline{0, m+n}\} < 2(4N \cdot \max\{|a_{rs}| \mid r = \overline{1, M}, s = \overline{1, N}\})^{\frac{M}{N-M}},$$

where a_{rs} are the coefficients in the system, all of them having the form $b^j \cdot \binom{3j+l+k}{k}$ or $b^j \cdot \binom{3j+l+k-1}{k}$ with $0 \le l \le 2$ and $3j+l+k \le m+n$. It is easy to see that $b^{\frac{m+n}{3}} \cdot 2^{m+n}$ is greater than any of them. Therefore there exist u_i and v_j such that $F^{(k)}(\beta,\beta) = 0$ for all $k = \overline{0, n-1}$ and

$$\max\{|u_i|,\ |v_j| \mid i, j = \overline{0, m+n}\} < 2(4 \cdot 2(m+n+1) \cdot b^{\frac{m+n}{3}} \cdot 2^{m+n})^{\frac{3n}{2m-n+2}}.$$

To finish the proof, it suffices to show

$$2(4 \cdot 2(m+n+1) \cdot b^{\frac{m+n}{3}} \cdot 2^{m+n})^{\frac{3n}{2m-n+2}} \le 2(16 \cdot b)^{9(m+n)}.$$

And don't forget we still had to prove $N > M$.

$N > M \Leftrightarrow 2(m+n+1) > 3n \Leftrightarrow 2m+2 > n \Leftrightarrow 2\left[\frac{2n}{3}\right] + 2 > n$. The last follows from $2\left[\frac{2n}{3}\right] + 2 > \frac{4n}{3} > n$.

From the inequality $x + 1 \le 2^x$ for all $x > 0$, it follows that $2(4 \cdot 2(m+n+1) \cdot b^{\frac{m+n}{3}} \cdot 2^{m+n})^{\frac{3n}{2m-n+2}} \le 2(2^{2m+2n+3} b^{\frac{m+n}{2}})^{\frac{3n}{2m-n+2}}$. We have $2(2^{2m+2n+3} b^{\frac{m+n}{2}})^{\frac{3n}{2m-n+2}} \le 2(16 \cdot b)^{9(m+n)} \Leftrightarrow 2^{\frac{3n(2m+2n+3)}{2m-n+2}} \cdot b^{\frac{(m+n)n}{2m-n+2}} \le (16 \cdot b)^{9(m+n)}$. We just have to prove

$$\frac{n \cdot (2m+2n+3)}{2m-n+2} < 12(m+n)$$

and

$$\frac{(m+n)\cdot n}{2m-n+2} < 9(m+n)$$

to be done.

$\frac{(m+n)\cdot n}{2m-n+2} < 9(m+n) \Leftrightarrow n < 18m - 9n + 18 \Leftrightarrow n < \frac{9m+9}{4}$, which follows from $n < \frac{3(m+1)}{2} < \frac{9(m+1)}{5}$.

$\frac{2m+2n+3}{2m-n+2} < \frac{\frac{4n}{3}+2n+3}{\frac{4n}{3}-n} = \frac{10n+9}{n}$. For $\frac{n\cdot(2m+2n+3)}{2m-n+2} < 12(m+n)$ it suffices to prove $10n+9 < 12(m+n) \Leftrightarrow 9 < 12m+2n$. By hypothesis, $m \geq 3$ and the conclusion follows. ■

Theorem 11.1.10 (Smallness Theorem). *In the conditions of the Auxiliary Polynomial Theorem, there exists a real number c_1 depending just on b such that for all $x, y \in \mathbb{R}$ with $|x-\beta| \leq 1$ and for all $t = \overline{0, n-1}$, we have*

$$|F^{(t)}(x,y)| \leq c_1^n(|x-\beta|^{n-t} + |y-\beta|).$$

Proof: The backbone of this proof is Taylor's Expansion Formula for F around (β, β). According to this formula, we have

$$F(x,y) = \sum_{j,k\geq 0} \frac{1}{k!j!} \cdot \frac{\partial^{k+j}F}{\partial x^k \partial y^j}(\beta,\beta)\cdot(x-\beta)^k(y-\beta)^j.$$

Since $F(x,y) = P(x) + y\cdot Q(x)$, $F^{(k)}(\beta,\beta) = 0$ for all $k = \overline{0, n-1}$, the degrees of F and Q in X are both least or equal to $m+n$, and $F^{(k)}(x,y) \overset{not}{=} \frac{1}{k!}\cdot\frac{\partial^k F}{\partial X^k}(x,y)$, it is easy to see that

$$F(x,y) = \sum_{k=n}^{m+n} F^{(k)}(\beta,\beta)\cdot(x-\beta)^k + (y-\beta)\cdot\sum_{k=0}^{m+n} Q^{(k)}(\beta)\cdot(x-\beta)^k.$$

By induction,

$$F^{(t)}(x,y) = \sum_{k=n}^{m+n} F^{(k)}(\beta,\beta)\cdot(x-\beta)^{k-t}\cdot\binom{k}{t} + (y-\beta)\cdot\sum_{k=t}^{m+n} Q^{(t)}(\beta)\cdot(x-\beta)^{k-t}\cdot\binom{k}{t}$$

for all $t = \overline{0, n-1}$. By the triangle inequality, for $|x-\beta| \leq 1$, we have:

$$|F^{(t)}(x,y)| \leq \underbrace{\left(\sum_{k=n}^{m+n} |F^{(k)}(\beta,\beta)|\cdot\binom{k}{t}\right)}_{A(t)}\cdot|x-\beta|^{n-t} + |y-\beta|\cdot\underbrace{\left(\sum_{k=t}^{m+n}|Q^{(t)}(\beta)|\cdot\binom{k}{t}\right)}_{B(t)}$$

for all $t = \overline{0, n-1}$. To complete the proof of the problem it is enough to prove that we can find $c_1 > 0$ depending only on $b = \beta^3$ such that $A(t) < c_1^n$ and $B(t) < c_1^n$ for all $t = \overline{0, n-1}$.

Recall that $F(x,y) = \sum_{i=0}^{m+n}(u_i x^i + v_i x^i y)$. From this it follows

$$F^{(k)}(\beta,\beta) = \sum_{i=0}^{m+n}\left(\binom{i}{k}\cdot u_i \cdot \beta^{i-k} + \binom{i}{k}\cdot v_i \cdot \beta^{i-k+1}\right)$$

for all $k = \overline{n, m+n}$. From the Auxiliary Polynomial Theorem 11.1.9, $\max\{|u_i|,\ |v_j| \mid i,j = \overline{0, m+n}\} \leq 2(16b)^{9(m+n)}$. Using this, the triangle inequality and the obvious inequalities $\beta^{i-k+1} < \beta^{m+n}$ and $\binom{i}{k} < 2^{m+n}$ for $i = \overline{0, m+n}$ and $k = \overline{n, m+n}$, we get

$$|F^{(k)}(\beta,\beta)| \leq 2^{m+n}\cdot(2(16b)^{9(m+n)})\cdot\beta^{m+n}\cdot(2(m+n+1)).$$

From this and again from the triangle inequality, it follows

$$A(t) \leq \sum_{k=n}^{m+n}|F^{(k)}(\beta,\beta)|\cdot\binom{k}{t} \leq$$

$$\leq (m+1)\cdot 2^{m+n}\cdot(2^{m+n}\cdot(2(16b)^{9(m+n)})\cdot\beta^{m+n}\cdot(2(m+n+1)))) \leq$$

$$< 2^{42(m+n)}\cdot b^{\frac{28}{3}(m+n)} \leq (2^{42\cdot\frac{5}{3}}\cdot b^{\frac{28}{3}\cdot\frac{5}{3}})^n.$$

Let $c_1 = 2^{70}\cdot b^{\frac{140}{9}}$. c_1 indeed depends only on b. Analogously we prove that $B(t) < c_1^n$. ∎

Theorem 11.1.11 (Non-Vanishing Theorem). *In the conditions of The Auxiliary Polynomial Theorem 11.1.9, there exists a constant c_2 depending only on b such that for all irreducible fractions with positive denominators, $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$, there exists $0 \leq t \leq 1 + \frac{c_2\cdot n}{\ln q_1}$ such that $F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \neq 0$.*

Proof: The main ingredient of this proof is what is called the Wronskian of P and Q, defined as

$$W(x) = \begin{vmatrix} P(x) & Q(x) \\ P'(x) & Q'(x) \end{vmatrix} = P(x)Q'(x) - P'(x)Q(x).$$

We prove that $W \neq 0$. If $Q = 0$, then $F = P$ and since $F^{(k)}(\beta,\beta) = 0$ for all $k = \overline{0, n-1}$, it follows that $(x-\beta)^n | P(x)$. Since the minimal polynomial of β is $x^3 - b$, we have that $(x^3-b)^n | P(x)$. By comparing the degrees of the two, $m+n \geq 3n \Rightarrow m \geq 2n$. But $2n \geq 3m$ and we have a contradiction. Therefore $Q \neq 0$. Assume $W = 0$. Then since $\left(\frac{P(x)}{Q(x)}\right)' = \frac{P'(x)Q(x) - P(x)Q'(x)}{Q^2(x)} = 0$, the rational function $\frac{P}{Q}$ must be a constant. So there exists $u \in \mathbb{Q}$ such that $P(x) = u\cdot Q(x)$. We then have $F(x,y) = (u+y)\cdot Q(x)$. Just like before, since $F^{(k)}(x,y) = (u+y)\cdot Q^{(k)}(x)$, we prove that $(x^3-b)^n | Q(x)$ and we find the same contradiction $m \geq 2n \geq 3m$. We have proved $W \neq 0$.

Let T be an integer such that $F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = 0$ for all $t = \overline{0, T-1}$ and $F^{(T)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) \neq 0$. We use the convention $F^{(0)} = F$. Such an integer T exists because $F \neq 0$. For all $t, t' \leq T-1$, we have

$$\begin{cases} P^{(t)}\left(\frac{p_1}{q_1}\right) + \frac{p_2}{q_2} \cdot Q^{(t)}\left(\frac{p_1}{q_1}\right) = 0 \\ P^{(t')}\left(\frac{p_1}{q_1}\right) + \frac{p_2}{q_2} \cdot Q^{(t')}\left(\frac{p_1}{q_1}\right) = 0 \end{cases} \Rightarrow$$

$$\Rightarrow P^{(t)}\left(\frac{p_1}{q_1}\right) \cdot Q^{(t')}\left(\frac{p_1}{q_1}\right) - P^{(t')}\left(\frac{p_1}{q_1}\right) \cdot Q^{(t)}\left(\frac{p_1}{q_1}\right) = 0.$$

By induction, $W^{(r)}\left(\frac{p_1}{q_1}\right)$ is a linear combination of such terms, hence is 0 for all $r = \overline{0, T-2}$. It follows that $\left(x - \frac{p_1}{q_1}\right)^{T-1} | W(x)$. Since p_1 and q_1 are coprime and since W has integer coefficients, it is not hard to prove that there exists $V \in \mathbb{Z}[X]$ such that $(q_1 \cdot x - p_1)^{T-1} \cdot V(x) = W(x)$. $W \neq 0 \Rightarrow V \neq 0$. If s and a_s are the degree and the leading term respectively of W, then from the previous divisibility relation, $q_1^{T-1} | a_s$. Since $V \neq 0$, $|a_s| \geq q_1^{T-1}$. By passing to logarithms,

$$T - 1 \leq \frac{\ln |a_s|}{\ln q_1}.$$

$W(x) = PQ' - P'Q = \left(\sum_{i=0}^{m+n} u_i \cdot x^i\right) \cdot \left(\sum_{j=0}^{m+n} j \cdot v_j \cdot x^{j-1}\right) - \left(\sum_{j=0}^{m+n} j \cdot u_j \cdot x^{j-1}\right) \cdot \left(\sum_{i=0}^{m+n} v_i \cdot x^i\right)$. The leading term of this polynomial expression is, by notation, the coefficient of the degree s part. This means

$$a_s = \sum_{i+j=s+1} j \cdot (u_i v_j - u_j v_i).$$

By the Auxiliary Polynomial Theorem 11.1.9, $\max\{|u_i|, |v_j| \mid i, j = \overline{0, m+n}\} \leq 2(16b)^{9(m+n)} = \gamma$. By the triangle inequality, since in the previous sum the terms with i or j greater than $m+n$ are 0, $|a_s| \leq 2\gamma^2 \cdot \sum_{j=0}^{m+n} j = \gamma^2 \cdot (m+n)(m+n+1) \leq 4^{m+n} \cdot [2 \cdot (16b)^{9(m+n)}]^2 \Rightarrow$

$$\ln |a_s| \leq (m+n) \ln 4 + \ln 4 + 18(m+n) \ln(16b) \leq \frac{5n}{3} \ln 4 + \ln 4 + 45n \ln(16b) \leq$$

$$\leq \underbrace{\left(\frac{5}{3} \ln 4 + 45 \ln(16b) + 1\right)}_{c_2} \cdot n.$$

c_2 indeed only depends on b. Also, $T - 1 \leq \frac{c_2 \cdot n}{\ln q_1}$. ∎

Proof of Thue's Diophantine Approximation Theorem 11.1.7: For clarity, we recall what we want to prove. We want to prove that given

$b \in \mathbb{N}^*$ such that $\beta = \sqrt[3]{b} \notin \mathbb{Q}$ and given any real number $C > 0$, there exist only a finite number of pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ such that $\left|\frac{p}{q} - \beta\right| < \frac{C}{q^3}$. It is easy to see that we can assume that $gcd(p, q) = 1$ and $C > 1$.

Assume for a contradiction that there exist infinitely many such pairs. Then we can find such pairs with arbitrary large q. In particular, there exists $(p_1, q_1) \in \mathbb{Z} \times \mathbb{N}^*$ such that

$$gcd(p_1, q_1) = 1,\ \left|\frac{p_1}{q_1} - \beta\right| < \frac{C}{q_1^3},\ q_1 > e^{9c_2} \text{ and } q_1 > (2c_1 \cdot C)^{18},$$

with c_1 given by *The Smallness Theorem 11.1.10* and c_2 given by the *Non-Vanishing Theorem 11.1.11*. It is easy to see that we can assume $c_1 > 1$ and $c_2 > 1$. Take another pair $(p_2, q_2) \in \mathbb{Z} \times \mathbb{N}^*$ with

$$gcd(p_2, q_2) = 1,\ \left|\frac{p_2}{q_2} - \beta\right| < \frac{C}{q_2^3} \text{ and } q_2 > q_1^{65}.$$

The importance of the dependence of c_1 and c_2 only on b in 11.1.10 and 11.1.11 is now visible as it intervenes in the choice of q_1. Take

$$n = \left[\frac{9}{8} \cdot \frac{\ln q_2}{\ln q_1}\right] \text{ and } m = \left[\frac{2n}{3}\right].$$

We check that with these choices of n and m we are in the conditions of the Auxiliary Polynomial Theorem. All that we have to prove is that $m \geq 3$. We have $n > \frac{9}{8} \cdot \frac{\ln q_2}{\ln q_1} - 1 > \frac{9}{8} \cdot 65 - 1 > 72 \Rightarrow m \geq \frac{2n}{3} - 1 > 47 \geq 3$.

$$n = \left[\frac{9}{8} \cdot \frac{\ln q_2}{\ln q_1}\right] \Rightarrow \frac{8}{9} \ln q_1 \cdot n \leq \ln q_2 < \frac{8}{9} \ln q_1 \cdot (n+1) \Rightarrow q_1^{\frac{8n}{9}} \leq q_2 < q_1^{\frac{8(n+1)}{9}}.$$

$$q_1 > e^{9c_2} \Rightarrow c_2 < \frac{\ln q_1}{9} \Rightarrow t \leq 1 + \frac{c_2 \cdot n}{\ln q_1} \leq 1 + \frac{n}{9} \leq n - 1,$$

where t is the one given by *The Non-Vanishing Theorem 11.1.11*. Since F has integer coefficients, after bringing fractions to a common denominator, $0 \neq F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right) = \frac{z}{q_1^{m+n} q_2}$ for some $z \in \mathbb{Z}^*$, it follows

$$|F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)| \geq \frac{1}{q_1^{m+n} q_2} > \frac{1}{q_1^{\frac{2n}{3} + \frac{8}{9}(n+1)+n}} = \frac{1}{q_1^{\frac{23n}{9} + \frac{8}{9}}}.$$

We now check that with $x = \frac{p_1}{q_1}$, $y = \frac{p_2}{q_2}$ and t we are in the condition of *The Smallness Theorem 11.1.10*. We have seen that $t \neq n - 1$. By assumption $|x - \beta| < \frac{C}{q_1^3}$. $q_1 > (2c_1 C)^{18} > C^{18} > \sqrt[3]{C}$. We have used that c_1 and C are greater than 1. Therefore $|x - \beta| < \frac{C}{q_1^3} < 1$ and we can apply *The Smallness Theorem 11.1.10* to obtain

$$|F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)| \leq c_1^n \left(\left(\frac{C}{q_1^3}\right)^{n-t} + \frac{C}{q_2^3}\right) \leq c_1^n \left(\left(\frac{C}{q_1^3}\right)^{n-1-\frac{n}{9}} + \frac{C}{q_1^{\frac{8n}{3}}}\right) \leq$$

$$\leq c_1^n \cdot \left(2 \cdot \frac{C^{\frac{8}{9}n-1}}{q_1^{\frac{8}{3}n-3}} \right) \leq \frac{(2c_1C)^n}{q_1^{\frac{8}{3}n-3}} < \frac{q_1^{\frac{n}{18}}}{q_1^{\frac{8}{3}-3}} = \frac{1}{q_1^{\frac{47}{18}n-3}}.$$

We have used $q_2^3 \geq q_1^{\frac{8}{3}n}$. Which follows from $n \leq \frac{9}{8}\frac{\ln q_2}{\ln q_1}$. Therefore

$$\frac{1}{q_1^{\frac{47}{18}n-3}} \geq |F^{(t)}\left(\frac{p_1}{q_1}, \frac{p_2}{q_2}\right)| \geq \frac{1}{q_1^{\frac{23n}{9}+\frac{8}{9}}} \Rightarrow \frac{8}{9} + \frac{23}{9}n \geq \frac{47}{18}n - 3 \Rightarrow$$

$$\Rightarrow 16 + 46n \geq 47n - 54 \Rightarrow 70 \geq n$$

which contradicts $n > 72$. ■

11.2 Ljunggren's Equation - a particular case

Theorem 11.2.1 (Ljunggren). *The integer solutions of the equation*

$$x^2 - x + 1 = y^3$$

are $(x, y) \in \{(0, 1),\ (1, 1),\ (19, 7),\ (-18, 7)\}$.

It is easy to prove that every element of the set given above is a solution to the equation. However, proving that these are the only solutions is a very difficult problem and for now we will content ourselves to solving a particular case of the problem.

Example 11.2.2 (Balkan Mathematics Olympiad 2005). *Find the integer solutions of the equation* $p^2 - p + 1 = k^3$ *with* p *being a positive prime number.*

Solution: First of all, notice that we can assume $p > 3$. This is because the equations $k^3 = 3 = 2^2 - 2 + 1$ and $k^3 = 7 = 3^2 - 3 + 1$ have no solutions in integers.

By multiplying by 4, the equation can be rewritten as $(2p-1)^2+3 = 4k^3$. Assume $p \equiv -1(mod\ 3)$. Then $3|\ 2p-1 \Rightarrow 3|\ 4k^3 \Rightarrow 3|\ k$. Reducing modulo 9 in the equation we obtain $3 \equiv 0(mod\ 9)$ which is impossible.

Therefore $p \equiv 1(mod\ 9)$. Then $p^2 - p + 1 = k^3 \Rightarrow 1 \equiv k(mod\ 3)$. Let $k = 3s+1$. Then $k^3 = 9 \cdot (3s^3 + 3s^2 + s) + 1 \Rightarrow 9|\ k^3 - 1 = p^2 - p \Rightarrow 9|\ p - 1$. We have

$$p \cdot \frac{p-1}{9} = \frac{k^3-1}{9} = \frac{k-1}{3} \cdot \frac{k^2+k+1}{3}.$$

Since $p > 1$ and $k^2+k+1 > 0$, it is easy to prove that $k > 1$. Since $p|\ p \cdot \frac{p-1}{9}$, it follows that $p|\ \frac{k-1}{3}$ or $p|\ \frac{k^2+k+1}{3}$.

If $p|\ \frac{k-1}{3}$, then $p \leq \frac{k-1}{3}$. Also $\frac{p-1}{9} = \underbrace{\frac{\frac{k-1}{3}}{p}}_{\in\mathbb{N}^*} \cdot \frac{k^2+k+1}{3} \geq \frac{k^2+k+1}{3} \Rightarrow p-1 \geq 3k^2+3k+3$. By combining the two inequalities, we have $\frac{k-1}{3} \geq 3k^2+3k+4 \Rightarrow 0 \geq 9k^2+8k+13$ which is impossible in integers. Therefore $p|\ \frac{k^2+k+1}{3}$.

Set $\frac{k^2+k+1}{3} = p \cdot t$ with $t \in \mathbb{N}^*$. Then $p \cdot \frac{p-1}{9} = \frac{k-1}{3} \cdot \frac{k^2+k+1}{3} \Rightarrow \frac{p-1}{9} = \frac{k-1}{3} \cdot t$. We have $\frac{k^2+k+1}{3} = 3 \cdot \left(\frac{k-1}{3}\right)^2 + 3 \cdot \frac{k-1}{3} + 1$, hence $\frac{k^2+k+1}{3} \equiv 1 (mod\ \frac{k-1}{3})$. $\frac{k-1}{3}|\ \frac{p-1}{9} \Rightarrow p \equiv 1 (mod\ \frac{k-1}{3})$. $1 \equiv \frac{k^2+k+1}{3} = pt (mod\ \frac{k-1}{3}) \Rightarrow t \equiv 1 (mod\ \frac{k-1}{3})$.

Assume $t > 1$. Since $t \equiv 1 (mod\ \frac{k-1}{3})$, $t \geq \frac{k+2}{3} \Rightarrow \frac{k^2+k+1}{3} = p \cdot t \geq p \cdot \frac{k+2}{3}$. Since $t \cdot \frac{k-1}{3} = \frac{p-1}{9}$, $p \geq 3k-2$. Then $\frac{k^2+k+1}{3} \geq \frac{(3k-2)(k+2)}{3} = \frac{3k^2+4k-4}{3} \Rightarrow 0 \geq 2k^2+3k-5 = (k-1)(2k+5) \Rightarrow -\frac{5}{2} \leq k \leq 1$ which contradicts $k > 1$.

Therefore $t = 1$ which implies $\frac{k^2+k+1}{3} = p$ and $p-1 = 3(k-1) \Rightarrow p = 3k-2$. Substituting yields $k^2+k+1 = 9k-6 \Rightarrow k^2-8k+7 = 0 \Rightarrow k \in \{1, 7\}$. Since $k > 1$, $k = 7$ which implies $p = 19$.

So the only solution of the equation $p^2+p+1 = k^3$ with p prime is $(p, k) = (19, 7)$. ■

Chapter 12

Generators for Elliptic Curves

The thematic of this lecture is obvious from the title. We have seen some methods for computing the rank of elliptic curves in a few particular cases. We will illustrate some examples to prove that computing explicit generators for the abelian group of an elliptic curve is a much harder problem.

We recommend (re)reading the Algebraic Number Theory Prerequisites section in the beginning of Lecture VIII.

Example 12.0.3. *Find a set of generators for the abelian group $C(\mathbb{Q})$ associated to the elliptic curve $y^2 = x^3 - 13$.*

Proof: The working plan is:

1. There are no torsion points on $C(\mathbb{Q})$ different from O.
2. $rank(C(\mathbb{Q})) = 1$.
3. $(17, 70)$ or $(17, -70)$ generate $C(\mathbb{Q})$.

We will first prove:

Proposition 12.0.4. *The only integer solutions of $y^2 = x^3 - 13$ are $(17, \pm 70)$.*

Proof: $(\pm 70)^2 + 13 = 4913 = 17^3$, so $(17, \pm 70)$ are indeed solutions to the given equation. To see that these are all the solutions of the equation, we will use the ring $A = \mathbb{Z}[i\sqrt{13}]$. Unfortunately, A is not factorial. For this we prove that 2 is irreducible, but not prime. In A we have a multiplicative norm function $N : A \to \mathbb{N}^*$ which extends to a group homomorphism $N : \mathbb{Q}(i\sqrt{13})^* \to \mathbb{Q}_+^*$ such that $N(a + b \cdot i\sqrt{13}) = a^2 + 13b^2$ for all $a, b \in \mathbb{Q}$, not both 0. It is easy to prove that $x \in A$ is a unit if and only if $N(x) = 1$. Assume 2 is not irreducible. Then there exist non-units $x, y \in A$ such that $2 = xy$. Then $N(2) = N(x)N(y)$. Since $N(2) = 4$ and x and y are not

units, $N(x) = N(y) = 2$. Let $x = a + b \cdot i\sqrt{13}$ with $a, b \in \mathbb{Z}$. Then $N(x) = 2 \Leftrightarrow a^2 + 13b^2 = 2$. But the last equation obviously has no integer solutions, so we get a contradiction, therefore 2 is irreducible. We have $2|14 = (1 + i\sqrt{13})(1 - i\sqrt{13})$ and $2 \not| 1 \pm i\sqrt{13}$ in A, hence 2 is not prime. That A is not factorial is also a consequence of the ideal class group $\mathcal{C}$ of A (see 8.1.2) not being trivial. We will prove that $|\mathcal{C}| = 2$ and that a complete set of representatives is A (the class of principal ideals of A) and the class of the maximal ideal $P = 2A + (1 + i\sqrt{13})A$.

Assume we have proved these assertions on $\mathcal{C}$. Then the equation $y^2 + 13 = x^3$ is equivalent to $(y + i\sqrt{13})(y - i\sqrt{13}) = x^3 \Rightarrow (xA)^3 = x^3A = (y + i\sqrt{13})A \cdot (y - i\sqrt{13})A$. By 8.1.2, every nonzero ideal of A decomposes uniquely as a product of prime ideals, and, as a consequence, we have proved the existence of an ideal theoretic greatest common divisor for two nonzero ideals. With this in mind, let $I = gcd((y + i\sqrt{13})A, (y - i\sqrt{13})A)$. Then

$$I|(y \pm i\sqrt{13})A \Rightarrow (y \pm i\sqrt{13})A \subseteq I \Rightarrow 2i\sqrt{13} \in I \Rightarrow I|2i\sqrt{13}A.$$

$P = (2,\ 1 + i\sqrt{13}) \Rightarrow P^2 = (4,\ 2 + 2i\sqrt{13},\ -12 + 2i\sqrt{13}) = (4,\ 2 + 2i\sqrt{13},\ 2i\sqrt{13}) = (4,\ 2,\ 2i\sqrt{13}) = 2A$. It is not hard to prove that $i\sqrt{13}$ is irreducible and prime, hence $Q = i\sqrt{13}A$ is a maximal ideal of A. Therefore $I|P^2Q$. If $Q|I$, then $I \subseteq Q$ and since $y \pm i\sqrt{13} \in I$, it follows $2y \in Q$. Since $i\sqrt{13} \not| 2$ in A, $i\sqrt{13}|\ 2y \Rightarrow i\sqrt{13}|\ y \Rightarrow y = i\sqrt{13} \cdot (a + b \cdot i\sqrt{13})$ for some $a, b \in \mathbb{Z}$. We obtain $y = -13b$. But $(-13b)^2 - 13 = x^3 \Rightarrow 13|\ x \Rightarrow 13^2|\ (-13b)^2 - 13$ which is impossible. So $Q \not| I$ and $I|\ P^2$. If $P|\ I$, then $P^2|\ (y+i\sqrt{13})A \cdot (y-i\sqrt{13})A \Rightarrow P^2|\ (xA)^3 \Rightarrow 2A|\ (xA)^3 \Rightarrow (xA)^3 \subseteq 2A \Rightarrow x$ is even. We have $y^2 + 13 = x^3$ and modulo 8 we get $y^2 \equiv 3(mod\ 8)$ which is impossible. Therefore $P \not| I$ and finally $I = A$.

The unique decomposition of the nonzero ideals of A as products of prime ideals, $(y + i\sqrt{13})A \cdot (y - i\sqrt{13})A = (xA)^3$ and $gcd((y + i\sqrt{13})A, (y - i\sqrt{13})A) = A$ prove that $(y + i\sqrt{13})A = J^3$ for some ideal J of A. By going to classes in $\mathcal{C}$, we get $\hat{A} = \hat{J}^3 = \hat{J}$ since we assume $|\mathcal{C}| = 2$, thus J is a principal ideal of A. It follows that $y + i\sqrt{13}$ is associated to a cube z^3 of A. $u = a + b \cdot i\sqrt{13}$ is a unit of A if and only if $N(u) = 1 \Leftrightarrow a^2 + 13b^2 = 1$. It is easy to see that the only solutions are $u = \pm 1$. Since -1 is also a cube in A, we get that $y + i\sqrt{13} = z^3$ for some $z \in A$. If $z = a + b \cdot i\sqrt{13}$ for some $a, b \in \mathbb{Z}$, then

$$\begin{cases} y = a^3 - 3ab^2 \cdot 13 \\ 1 = 3a^2b - b^3 \cdot 13 \end{cases}.$$

The last equation can be rewritten as $b(3a^2 - 13b^2) = 1 \Rightarrow b = \pm 1$. $b = 1$ leads to $3a^2 - 13 = 1$ which is impossible. Therefore $b = -1$ and $3a^2 - 13 = -1 \Rightarrow a = \pm 2$. These lead to the solution $(x, y) = (17, \pm 70)$.

We are left to prove the assertions made on $\mathcal{C}$. To prove them we will need some more results from Algebraic Number Theory.

Theorem 12.0.5 (Minkowski). *Let K be an algebraic extension of $\mathbb{Q}$ of degree n and let A be the ring of integers of K. Assume $A = \mathbb{Z}[u]$ for some $u \in A$. If J is a nonzero ideal of A, then there exists a nonzero ideal I of A such that $I \equiv J(mod\ PrA)$ and*

$$|A/I| = N(I) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\delta_K|},$$

where $\delta_K = \det(Tr_K(e_ie_j))_{i,j=\overline{1,n}}$, $(e_i)_i$ is a basis for K over $\mathbb{Q}$ such that $A = \oplus_{i=1}^n \mathbb{Z}e_i$, $s + 2t = n$ and s is the number of real embeddings of K i.e. field homomorphism $K \hookrightarrow \mathbb{R}$. $Tr_K(x)$ is by definition $[K : \mathbb{Q}(x)] \cdot Tr(x)$, where $Tr(x)$ is the sum of conjugates of x i.e. the sum of all the distinct complex roots of the irreducible polynomial of x over $\mathbb{Q}$.

δ_K is called the discriminant of K over $\mathbb{Q}$. $\left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\delta_K|}$ is called the Minkowski constant of K.

In our case, we have $K = \mathbb{Q}(i\sqrt{13})$, $A = \mathbb{Z}[i\sqrt{13}]$, $u = i\sqrt{13}$, $n = 2$, $s = 0$, $t = 1$, $e_1 = 1$, $e_2 = i\sqrt{13}$. With these,

$$\delta_K = \det\begin{vmatrix} Tr_K(1) & Tr_K(i\sqrt{13}) \\ Tr_K(i\sqrt{13}) & Tr_K(-13) \end{vmatrix} = \det\begin{vmatrix} 2 & 0 \\ 0 & -26 \end{vmatrix} = -52.$$

By 12.0.5, for every nonzero ideal J of A, there exists a nonzero ideal I such that $I \equiv J(mod\ PrA)$ and $N(I) \leq \frac{4}{\pi} \cdot \frac{2}{4} \cdot \sqrt{52} = \frac{\sqrt{208}}{\pi} \leq 4 \Rightarrow N(I) \in \{1, 2, 3, 4\}$. So, to determine a complete set of representatives for $\mathcal{C}$ it is enough to look through the non-equivalent ideals of norm least or equal to 4. To determine these ideals we need one more result of Algebraic Number Theory. This result describes the behavior of prime integers in the rings of integers of number fields:

Theorem 12.0.6. *Let K be a number field such that $[K : \mathbb{Q}] = n$ and let A be its ring of integers. Assume $A = \mathbb{Z}[u]$ for some $u \in K$. Let $f = Irr_{\mathbb{Q}}(u)$ be the irreducible polynomial of u in $\mathbb{Q}[X]$. Let p be a prime integer. Assume $\bar{f} = \bar{\varphi}_1^{e_1} \cdot \ldots \cdot \bar{\varphi}_r^{e_r}$, where $\bar{f}$ is the reduced of f modulo p and $\varphi_1, \ldots, \varphi_r$ are monic polynomials such that when reduced mod p they become irreducible and pairwise distinct.*

Then for all $i = \overline{1, r}$, $P_i = pA + \varphi_i(u)A$ is a maximal ideal of A of norm p^{f_i}, where $f_i = deg\varphi_i$. Moreover $P_i \neq P_j$ for all $i \neq j$, $pA = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r}$ and $\sum_{i=1}^r e_i f_i = n$.

We are now able to find the ideals of A of norm least or equal to 4.

If $N(I) = 1$, then $|A/I| = 1 \Rightarrow I = A$.

If $N(I) = 4$, then $|A/I| = 4$. So A/I is a ring with 4 elements. It follows by Lagrange, that $4 \cdot \hat{1} = \hat{0}$ in A/I, so $\hat{4} = \hat{0} \Rightarrow 4 \in I \Rightarrow I|4A = (2A + (1 + i\sqrt{13})A)^4$. $2A = (2A + (1 + i\sqrt{13})A)^2 \Rightarrow 4 = N(2A) = N(2A + (1 + i\sqrt{13})A)^2 \Rightarrow N(2A + (1 + i\sqrt{13})A) = 2$. It is not hard to prove that

$I = (2A + (1 + i\sqrt{13})A)^2 = 2A$. Notice that $I \equiv A(mod\ PrA)$ because I is principal.

If $N(I) = 2$, then A/I has 2 elements, hence it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, so I is a maximal ideal of A. Just like before we prove $2 \in I$, which implies $I|2A$. To find the maximal ideals of A dividing $2A$ we can use 12.0.6. We have $A = \mathbb{Z}[i\sqrt{13}]$. Let $u = i\sqrt{13}$. Then $f(X) = Irr_{\mathbb{Q}}(u) = X^2 + 13$. Modulo 2 we have $\bar{f} = (X + \bar{1})^2$. From 12.0.6 we obtain $2A = P_1^2$ with $P_1 = 2A + (u + 1)A = 2A + (1 + i\sqrt{13})A$. Therefore P_1 is the only ideal of A of norm 2. Assume that P_1 is principal. Then there exists $x \in P_1$ such that $P_1 = xA$. Then by 8.1.2, $2 = N(P_1) = N(xA) = N(x)^{[\mathbb{Q}(i\sqrt{13}):\mathbb{Q}(x)]}$, where $N(x)$ is the norm of x defined in 8.1.2 which is easily seen to coincide to the norm N we defined on A in the beginning of the proof. It is easy to prove that $x \notin \mathbb{Q}$, otherwise $x \in \mathbb{Z}$ and it would follow that $x^2|2$ in A which is impossible. Therefore $[\mathbb{Q}(i\sqrt{13}) : \mathbb{Q}(x)] = 1$. It follows that $2 = N(x)$. Assume $x = a + b \cdot i\sqrt{13}$. Then $2 = N(x) \Rightarrow 2 = a^2 + 13b^2$ which is easily seen to have no integer solutions. We have proved that P_1 is not principal. But $P_1^2 = 2A$ is a principal ideal, so $\hat{P_1}$ has order 2 in $\mathcal{C}$.

If $N(I) = 3$, then just like before I is a maximal ideal of A dividing $3A$. Modulo 3 we have $\bar{f}(X) = X^2 + \bar{1}$ which is irreducible. By 12.0.6, $3A = P_2$ and $N(P_2) = 9$. This proves that A has no ideals of norm 3.

We have proved that the only ideals of A of norm least or equal to 4 are A, P_1 and $2A$. Also a complete set of non-equivalent representatives for $\mathcal{C}$ is A and P_1. We conclude $\mathcal{C} \simeq \mathbb{Z}/2\mathbb{Z}$ as groups. We have also finished proving that the only integer solutions of $y^2 = x^3 - 13$ are $(17, \pm 70)$. ■

We return to the proof of 12.0.3: We prove the first item on the working plan i.e. that $C(\mathbb{Q})$ has no non-trivial elements of finite order. This is a simple application of Nagell-Lutz's Theorem. The discriminant of $X^3 - 13$ is $\Delta = -3^3 \cdot 13^2$. If (x, y) is a non-trivial element of $C(\mathbb{Q})$ of finite order, then by Nagell-Lutz's $x, y \in \mathbb{Z}$ and $y|\Delta$. But we have seen that the only integer solutions of $y^2 = x^3 - 13$ are $(17, \pm 70)$. It is enough to prove that they are not torsion points. This follows from $\pm 70 \not| \ \Delta = -3^3 \cdot 13^2$. We have proved that $C(\mathbb{Q})$ is torsion-free, hence it is a free abelian group.

Assume we have proved that $C(\mathbb{Q})$ is of rank 1. It follows that there exists $(x, y) \in \mathbb{C}(Q)$ such that $C(\mathbb{Q}) = \mathbb{Z} \cdot (x, y)$. To prove that $(17, 70)$ or its opposite $(17, -70) = -(17, 70)$ generate $C(\mathbb{Q})$, we use the following lemma:

Lemma 12.0.7. *Let $C(Q) : y^2 = x^3 + ax^2 + bx + c$ be a nonsingular elliptic curve with $a, b, c \in \mathbb{Z}$. Let $P \in C(\mathbb{Q})$, $P \neq O[0 : 1 : 0]$ and assume that $n \cdot P \in C(\mathbb{Z}) \setminus \{O\}$ for some $n \in \mathbb{N}^*$. Then $P \in C(\mathbb{Z})$.*

Proof: For a prime number p, denote

$$C_p = \left\{ \left(\frac{a}{t^2}, \frac{b}{t^3} \right) \in C(\mathbb{Q}) |\ a, b, t \in \mathbb{Z},\ t > 0, gcd(a, t) = gcd(b, t) = 1, p \mid t \right\} \cup \{O\}.$$

During the proof of Nagell-Lutz's Theorem, we have proved $(C_p, +) \leq (C(\mathbb{Q}), +)$.

Assume P does not have integer coordinates. Then by 2.2.5, $P = \left(\frac{a}{t^2}, \frac{b}{t^3}\right)$ for some $a, b, t \in \mathbb{Z}$, $t > 1$ and $gcd(a, t) = gcd(b, t) = 1$. Let p be a prime number such that $p \mid t$. Then $P \in C_p$ and $n \cdot P \in C_p \setminus \{O\}$ which contradicts $n \cdot P$ being a nontrivial point with integer coordinates. ■

Assume $P = (x, y)$ is a generator for $C(\mathbb{Q})$. Since $(17, \pm 70) \in C(\mathbb{Q})$ and $C(\mathbb{Q}) = \mathbb{Z} \cdot P$, there exists $n \in \mathbb{Z}$ such that $n \cdot P = (17, 70)$. From the previous lemma we get that $P \in C(\mathbb{Z})$. Since $C(\mathbb{Z}) = \{(17, \pm 70)\} \cup \{O\}$, $P \in \{(17, \pm 70)\}$.

To complete the proof of the problem we have to prove $rank(C(\mathbb{Q})) = 1$. An algorithm for computing the rank of $C(\mathbb{Q})$ can be deduced from the proof of the General Mordell-Weil Theorem in Lecture VIII. We have already seen that $C(\mathbb{Q})$ is a free abelian group. Then $C(\mathbb{Q}) \simeq \mathbb{Z}^r$, where $r = rank(C(\mathbb{Q}))$ and $C(\mathbb{Q})/2C(\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^r$. It is enough to prove that $|C(\mathbb{Q})/2C(\mathbb{Q})| = 2$.

The equation of $C(\mathbb{Q})$ is $y^2 = x^3 - 13 = f(x)$. $f(x) = (x - \sqrt[3]{13})(x - \omega\sqrt[3]{13})(x - \omega^2\sqrt[3]{13})$ with $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$. Let $\theta = \sqrt[3]{13}$, $A = \mathbb{Z}[\theta]$ and let $K = \mathbb{Q}(\theta)$. If we define $\varphi : C(\mathbb{Q}) \to \mathcal{Q}(\theta) \stackrel{def}{=} \frac{K^*}{(K^*)^2}$ by

$$\varphi(P) = \begin{cases} \hat{1}, & \text{if } P = O \\ \widehat{\alpha - \beta \cdot \theta}, & \text{if } P = \left(\frac{\alpha}{\beta}, w\right), \alpha \in \mathbb{Z}, \beta \in \mathbb{N}^*, gcd(\alpha, \beta) = 1, \beta = t^2, t \in \mathbb{N}^* \end{cases},$$

then the proofs of 8.2.4 and 8.2.5 show that φ is a well defined group homomorphism whose kernel is $2C(\mathbb{Q})$. By the fundamental theorem of isomorphism it is enough to determine $Im\varphi$. From 8.2.7 we know that there exist a finite number of algebraic integers $\gamma \in A$ for which there exist $u \in U(A)$ and $\tau \in K$ such that $\alpha - \beta \cdot \theta = u \cdot \gamma \cdot \tau^2$ as $P = \left(\frac{\alpha}{\beta}, w\right)$ varies in $C(\mathbb{Q}) \setminus \{O\}$ with $\alpha, \beta \in \mathbb{Z}$, $\beta > 0$ and $gcd(\alpha, \beta) = 1$. Then $\varphi(P) = \widehat{u \cdot \gamma}$. Define

$$I(P) = (\alpha - \beta \cdot \theta)A + \beta^2 \cdot g\left(\frac{\alpha}{\beta}\right) A,$$

where $f(x) = (x - \theta)g(x) \Rightarrow g(x) = x^2 + \theta x + \theta^2$. The γ's where chosen as generators for the principal ideals appearing in the set $\{I(P) \cdot C_i^2\}$ as P ranges in $C(\mathbb{Q}) \setminus \{O\}$, $i \in \{1, \ldots, s\}$ and $\{C_1, \ldots, C_s\}$ is a complete set of representatives for the ideal class group $\mathcal{C}$ of A. It was proved in 8.2.5 that there is a finite number of ideals of A of type $I(P)$ and all these ideals divide $g(\theta)A = 3\sqrt[3]{169}A = 3\theta^2 A$.

It is clear that we need more information on $\mathcal{C}$ and $U(A)$. For this we have two lemmas.

Lemma 12.0.8. *$U(\mathbb{Z}[\sqrt[3]{13}]) = \{\pm\varepsilon_0^n | \ n \in \mathbb{Z}\}$ with $\varepsilon_0 = 94 + 40\sqrt[3]{13} + 17\sqrt[3]{169}$.*

Proof: Define $N : K \to \mathbb{C}$ by $N(x) = \sigma_1(x)\sigma_2(x)\sigma_3(x)$, where $\sigma_i : K \to \mathbb{C}$ are the field homomorphisms uniquely defined by $\sigma_i(\theta) = \omega^{i-1}\theta$. Notice that $\sigma_1 = 1_K$ and $\sigma_2 = \bar{\sigma}_3$, where for a complex number z, $\bar{z}$ represents its complex conjugate. It can be proved that N is a multiplicative function on K with rational values and $N(A) \subseteq \mathbb{Z}$. Moreover $N(x) = 0 \Leftrightarrow x = 0$. It is easy to prove that $u \in U(A) \Leftrightarrow N(u) = \pm 1$. Again a simple computation proves that if $x = a + b\theta + c\theta^2$, then $N(x) = a^3 + 13 \cdot b^3 + 169 \cdot c^3 - 3 \cdot 13 \cdot abc$.

$N(\varepsilon_0) = 94^3 + 13 \cdot 40^3 + 169 \cdot 17^3 - 3 \cdot 13 \cdot 94 \cdot 40 \cdot 17 = 830584 + 832000 + 830297 - 2492880 = -1$, hence ε_0 is a unit. It follows that every number of the form $\pm\varepsilon_0^n$ is a unit in A.

Conversely, given u a unit in A we want to prove that $u = \pm\varepsilon_0^n$ for a suitable choice of the sign and for some $n \in \mathbb{Z}$. For this we first prove that there is no unit of A such that $1 < u < \varepsilon_0$. Assume there is such a unit of the form $u = a + b\theta + c\theta^2$ with $a, b, c \in \mathbb{Z}$. We then have

$$\begin{cases} \sigma_1(u) = a + b\theta + c\theta^2 \\ \sigma_2(u) = a + b\omega\theta + c\omega^2\theta^2 \\ \sigma_3(u) = a + b\omega^2\theta + c\omega\theta^2 \end{cases}.$$

$1 = |N(u)| = |\sigma_1(u)\sigma_2(u)\sigma_3(u)| = u|\sigma_2(u)|^2 \Rightarrow |\sigma_2(u)|^2 = \frac{1}{u} < 1$. Keeping in mind that $\sigma_2 = \bar{\sigma}_3$ and $1 + \omega + \omega^2 = 0$, we have $|3a| = |\sigma_1(u) + \sigma_2(u) + \sigma_3(u)| \leq u + 2|\sigma_2(u)| < \varepsilon_0 + 2$. Therefore

$$|a| < \frac{\varepsilon_0 + 2}{3}.$$

$|3b\theta| = |\sigma_1(u) + \omega^2\sigma_2(u) + \omega\sigma_3(u)| \leq u + 2|\sigma_2(u)| < \varepsilon_0 + 2 \Rightarrow$

$$|b| < \frac{\varepsilon_0 + 2}{3\theta}.$$

Similarly, from $3c\theta^2 = \sigma_1(u) + \omega\sigma_2(u) + \omega^2\sigma_3(u)$, we prove

$$|c| < \frac{\varepsilon_0 + 2}{3\theta^2}.$$

A simple enough computer program can show that no element of the form $a + b\theta + c\theta^2$ in between 1 and ε_0 and with a, b and c subjected to the upper restrictions is invertible in A.

Assume u is a unit of A. Exactly one of the units of A $\{\pm u, \pm u^{-1}\}$ is greater or equal to 1. Without loss of generality, assume $1 \leq u$. Since $1 < \varepsilon_0$, $\lim_{n\to\infty} \varepsilon_0^{-n} = 0$. Choose n such that $0 < u \cdot \varepsilon_0^{-n-1} \leq 1 < u \cdot \varepsilon_0^{-n}$. It is easy to see that such n exists. We have proved that there is no unit of A in $(1, \varepsilon_0)$. Since $1 < u \cdot \varepsilon_0^{-n} \leq \varepsilon_0$, we conclude that $u = \varepsilon_0^{n+1}$. The other cases are treated similarly. ■

Lemma 12.0.9. *The ideal class group $\mathcal{C}$ of $A = \mathbb{Z}[\sqrt[3]{13}]$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}, +)$.*

Proof: By Minkowski's Theorem 12.0.5, for every nonzero ideal M of $A = \mathbb{Z}[\sqrt[3]{13}]$, there exists an ideal I of A such that $M \equiv I(mod\ PrA)$ and $N(I) \leq \left(\frac{4}{\pi}\right)^t \cdot \frac{n!}{n^n} \cdot \sqrt{|\delta_K|}$, where $n = [K : \mathbb{Q}] = [\mathbb{Q}(\theta) : \mathbb{Q}] = 3$, $t = 1$ is half the number of non-real embeddings of K in $\mathbb{C}$ and

$$\delta_K = \det \begin{vmatrix} Tr_K(1) & Tr_K(\theta) & Tr_K(\theta^2) \\ Tr_K(\theta) & Tr_K(\theta^2) & Tr_K(\theta^3) \\ Tr_K(\theta^2) & Tr_K(\theta^3) & Tr_K(\theta^4) \end{vmatrix} = \det \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 39 \\ 0 & 39 & 0 \end{vmatrix} = -27 \cdot 169.$$

Therefore $N(I) \leq \frac{4}{\pi} \cdot \frac{3!}{3^3} \cdot \sqrt{27 \cdot 169} < 20$. This means that every class of $\mathcal{C}$ has a representative whose norm is at most 19.

We are now looking for ideals of A of norm least or equal to 19. By using Theorem 12.0.6, we can find the prime ideals of A of norm at most 19. We have $A = \mathbb{Z}[\theta]$ who is the ring of integers of an algebraic extension of $\mathbb{Q}$ of degree 3, $K = \mathbb{Q}(\sqrt[3]{13})$, and $f = Irr_Q(\theta) = X^3 - 13$ so Theorem 12.0.6 applies merrily. Remember the notation $\theta = \sqrt[3]{13}$.

There is only one ideal of norm 1, and this is A.

Since for every ideal I of A, we have $N(I) \in I \Rightarrow N(I) \cdot A \subset I \Rightarrow I|\ N(I) \cdot A$, the ideals of norm 2 can be found among the divisors of $2A$. To decompose $2A$ as a product of prime ideals, we apply Theorem 12.0.6. Modulo 2 we have the decomposition in irreducible factors $\bar{f} = X^3 - \bar{1}\bar{3} = (X - \bar{1})(X^2 + X + \bar{1})$. Therefore $2A = P_1 \cdot P_2$ with $P_1 = 2A + (\theta - 1)A$, $N(P_1) = 2$ and $P_2 = 2A + (\theta^2 + \theta + 1)A$, $N(P_2) = 4$. P_1 and P_2 are both maximal ideals of A. Our main goal is to prove that A, P_1 and P_1^2 is a complete set of representatives of $\mathcal{C}$. So far we have $P_2 \equiv P_1^{-1}(mod\ PrA)$.

Modulo 3, $\bar{f} = (X - \bar{1})^3$, so $3A = P_3^3$ with $P_3 = 3A + (\theta - 1)A$ and $N(P_3) = 3$. We have $N((\theta - 1)A) = |N_K(\theta - 1)| = |-1 + 13| = 12$. Also $P_3|\ (\theta - 1)A$ and $P_1|\ (\theta - 1)A$. We conclude $(\theta - 1)A = P_1P_3Q$ for some prime ideal Q of norm 2. Since P_1 is the only such ideal, $P_1^2P_3 = (\theta - 1)A \Rightarrow P_3 \equiv P_1^{-2}(mod\ PrA)$.

As a consequence of 8.1.2, the only ideals of norm 4 are P_1^2 and P_2. For the same purpose, at first, we will only be looking for the prime ideal of norm at most 19.

The ideals of norm 5 are divisors of $5A$. Modulo 5, $\bar{f} = X^3 - \bar{1}\bar{3} = (X - \bar{2})(X^2 + \bar{2}X + \bar{4})$ and $X^2 + \bar{2}X + \bar{4}$ is irreducible modulo 5 because it has no roots modulo 5, or because its discriminant, $\Delta = \bar{5}$, is not a square modulo 5. By 12.0.6, $5A = P_4P_5$ with $P_4 = 5A + (\theta - 2)A$, $N(P_4) = 5$ and $P_5 = 5A + (\theta^2 + 2\theta + 4\theta)A$, $N(P_5) = 25$. P_4 and P_5 are both maximal. Since $N(P_5) = 25 > 19$, P_5 is not of great interest for us. We have $N(\theta - 2) = -8 + 13 = 5$, so $(\theta - 2)|\ 5$ in A, hence $P_4 = (\theta - 2)A$ and $P_4 \equiv A(mod\ PrA)$. Since $N((\theta + 3)A) = |N(\theta + 3)| = |27 + 13| = 40 = 2^3 \cdot 5$, $(\theta + 3)A = P_4 \cdot Q$, where Q is an ideal of norm 8. But the only ideals of norm 8 are P_1^3 and P_1P_2. If $Q = P_1P_2 = 2A$, then $2A|\ (\theta + 3)A \Rightarrow 2|\ \theta + 3$ which is impossible. Therefore $(\theta + 3)A = P_4P_1^3 \Rightarrow A \equiv P_4 \cdot P_1^3(mod\ PrA) \Rightarrow A \equiv P_1^3(mod\ PrA)$.

Modulo 7, $\bar{f} = X^3 + \bar{1} = (X + \bar{1})(X + \bar{2})(X - \bar{3})$, so $7A = P_6P_7P_8$ with $P_6 = 7A + (\theta + 1)A$, $P_7 = 7A + (\theta + 2)A$ and $P_8 = 7A + (\theta - 3)A$ are all maximal ideals of norm 7 in A. $N((\theta + 1)A) = N(\theta + 1) = 14$ and $P_6|\ (\theta + 1)A$ imply $(\theta + 1)A = P_6P_1 \Rightarrow P_6 \equiv P_1^{-1}(mod\ PrA)$. Similarly $(\theta + 2)A = P_7P_3 \Rightarrow P_7 \equiv P_3^{-1} \equiv P_1^2(mod\ PrA)$ and $(\theta - 3)A = P_8P_1 \Rightarrow P_8 \equiv P_1^{-1}(mod\ PrA)$.

Modulo 11, $\bar{f} = X^3 - \bar{2} = (X + \bar{4})(X^2 - \bar{4}X + \bar{5})$ and $X^2 - 4X + 5$ is irreducible modulo 11 because its discriminant modulo 11 is $\bar{7}$ which is not a square modulo 11. So $11A = P_9P_{10}$ with $P_9 = 11A + (\theta + 4)A$ a maximal ideal of norm 11 and P_10 a non-interesting maximal ideal of norm 121. We have $P_9|\ (\theta + 4)A$ and $P_8|\ (\theta + 4)A$ because $P_8 = 7A + (\theta - 3)A \Rightarrow \theta + 4 = 7 + (\theta - 3) \in P_8$. Since $N((\theta + 4)A) = |N(\theta + 4)| = 64 + 13 = 77$, the only possibility is $(\theta + 4)A = P_8P_9 \Rightarrow P_9 \equiv P_8^{-1} \equiv P_1(mod\ PrA)$.

Modulo 13, $\bar{f} = X^3 \Rightarrow 13A = P_{11}^3$ with $P_{11} = \theta \cdot A$ of norm 11 and $P_{11} \equiv A(mod\ PrA)$.

Modulo 17, $\bar{f} = X^3 + \bar{4} = (X - \bar{4})(X^2 + \bar{4}X + \bar{16})$ with $X^2 + 4X + 16$ irreducible modulo 17. Then $17A = P_{12}P_{13}$ with $P_{12} = 17A + (\theta - 4)A$, $N(P_{12}) = 17$ and P_{13} is a non-interesting maximal ideal of norm $17^2 > 19$. As before, we can prove $(\theta - 4)A = P_3P_{12} \Rightarrow P_{12} \equiv P_3^{-1} \equiv P_1^2(mod\ PrA)$.

Modulo 19, $\bar{f} = X^3 - \bar{13}$ is irreducible because $\bar{13}$ is not a cube mod 19, so $19A = P_{14}$ is a maximal ideal of norm $19^3 > 19$.

We have proved that all the prime ideals of norm at most 19 are equivalent modulo PrA to a power of P_1 and we can easily prove the same result for every ideal, not necessarily prime, whose norm is least or equal to 19. With a little help from Minkowski's 12.0.5 we can remove the restriction on the bound of the ideal from the previous sentence and conclude that PrA is generated by the class of the ideal P_1. We have proved that $P_1^3 \equiv A(mod\ PrA)$, so P_1 has either order 3 or 1. If $P_1 \equiv A(mod\ PrA)$ then P_1 is principal, so there exists $x \in A$ such that $xA = P_1$. Let $x = a + b\theta + c\theta^2$ with $a, b, c \in \mathbb{Z}$. Then $2 = N(P_1) = N(xA) = |N(x)| = |a^3 + 13b^3 + 169c^3 - 39abc|$. Modulo 13 we get $\pm 2 \equiv a^3(mod\ 13)$. But the cubes modulo 13 are $\{\bar{0}, \pm\bar{1}, \pm\bar{8}\}$ and $\pm\bar{2}$ is not among them. Therefore the equality $2 = |N(x)|$ is impossible and P_1 is not principal. We conclude that $PrA \simeq (\mathbb{Z}/3\mathbb{Z}, +)$. ∎

Back to our problem, we wanted to describe $Im\varphi$ and for this we saw that we must describe the set of γ's. With the notations in the proof of Lemma 12.0.9, all the ideals $I(P)$ appear among divisors of $g(\theta)A = 3\sqrt[3]{169}A = P_3^3P_{11}^2$. Assume $P_{11}|\ I(P) = (\alpha - \beta \cdot \theta)A + \beta^2 \cdot g\left(\frac{\alpha}{\beta}\right)$ for some $P \in C(\mathbb{Q})$ with $P = \left(\frac{\alpha}{\beta}, w\right)$, $\alpha, \beta \in \mathbb{Z}$, $\beta > 0$ and $gcd(\alpha, \beta) = 1$. Then $13 = N(P_{11})|\ N(I(P))|\ N((\alpha - \beta \cdot \theta)A) = |N(\alpha - \beta \cdot \theta)| = |\alpha^3 - 13 \cdot \beta^3|$. From 2.2.5, there exist $\rho, t \in \mathbb{Z}$ with $t > 0$, $gcd(\rho, t) = 1$ such that $w = \frac{\rho}{t^3}$ and $\beta = t^2$. Using that $P \in C(\mathbb{Q})$, we get $\frac{\alpha^3}{\beta^3} - 13 = \frac{\rho^2}{t^6} \Rightarrow \alpha^3 - 13\beta^3 = \rho^2$.

Since $13|\ |\alpha^3 - 13\beta^3|,\ 13|\ \rho^2 \Rightarrow 13|\ \rho \Rightarrow 13|\ \alpha \Rightarrow 13|\ \beta$ which contradicts $gcd(\alpha, \beta) = 1$.

Assume $P_3|\ I(P)$. Just as before we get $3|\ |\alpha^3 - 13\beta^3| = \rho^2 \Rightarrow 3|\ \rho$. It is easy to see that $3|\ \alpha \Leftrightarrow 3|\ \beta$. Using that $gcd(\alpha, \beta) = 1$, we get that $3 \not| \alpha$ and $3 \not| \beta$. Since $\alpha \equiv \alpha^3 \equiv 13\beta^3 \equiv \beta^3 \equiv \beta (mod\ 3)$, $\alpha \equiv \beta \equiv 1 (mod\ 3)$ or $\alpha \equiv \beta \equiv -1 (mod\ 3)$. If $\alpha \equiv 1 (mod\ 3)$, then $\alpha^3 \equiv 1 (mod\ 9)$ and then $0 \equiv \rho^2 = \alpha^3 - 13\beta^3 \equiv 1 - 13 = 12 (mod\ 9)$ which is impossible. Similarly if $\alpha \equiv -1 (mod\ 3)$ we reach a contradiction.

We have proved that P_{11} and P_3 do not divide $I(P)$ for any $P \in C(\mathbb{Q}) \setminus \{O\}$. Since $I(P)|\ P_3^3 P_{11}^2$, we obtain $I(P) = A$ for every P as above. The γ's are now selected as generators for the principal ideals in the set $\{A,\ P_1^2,\ P_1^4\}$. Only A is principal in this set, so there is only one γ to choose and we choose it to be 1. It follows that for every choice of P as above, $\alpha - \beta \cdot \theta = u \cdot \tau^2$ for some $u \in U(A)$ and $\tau \in K^*$. Then $\varphi(P) = \widehat{\alpha - \beta \cdot \theta} = \widehat{u \cdot \tau^2} = \hat{u} \in \{\pm\hat{1},\ \pm\hat{\varepsilon}_0\}$. Assume $\varphi(P) = \widehat{-1}$. Then $\alpha - \beta \cdot \theta = -\tau^2$ for some $\tau \in K^*$. Then $N(\alpha - \beta \cdot \theta) = N(-\tau^2) = -N(\tau)^2$. But $N(\alpha - \beta \cdot \theta) = \alpha^3 - 13\beta^3 = \rho^2 \geq 0$. We have reached a contradiction. Similarly $\varphi(P) \neq \widehat{-\varepsilon_0}$. We have proved $Im\varphi \subset \{\hat{1},\ \hat{\varepsilon}_0\}$. Therefore $|Im\varphi| \leq 2$ and $r \leq 1$. If $r = rank(C(\mathbb{Q})) = 0$, then $C(\mathbb{Q}) = \{O\}$ which contradicts $(17, 70) \in C(\mathbb{Q})$.

We have completed the proof for $rank(C(\mathbb{Q})) = 1$. ■

Chapter 13

Lecture XIII

We have reserved this lecture for the proof of the problem 11.1.2, related to Thue's Theorem 11.1.1. We will present it in an enriched form that will provide us a rare example of an effective method of determining the solutions of a diophantine equation.

Theorem 13.0.10. *The equation $x^3 - dy^3 = 1$, where d is a positive integer that is not the cubic power of another integer, has at most two integer solutions. The equation always has the obvious solution $(1, 0)$.*

Let $A = \mathbb{Z}[\sqrt[3]{d}]$. Then the units of A are $U(A) = \{\pm\varepsilon_0^n |\ n \in \mathbb{Z}\}$ for some $0 < \varepsilon_0 < 1$, $\varepsilon_0 \in A$.

The equation $X^3 - dY^3 = 1$ has a non-trivial solution if and only if $\varepsilon_0 = a + b\sqrt[3]{d}$ for some $a, b \in \mathbb{Z}^*$.

Remark 13.0.11. *The condition $d \in \mathbb{N}$ is not important because we can reduce to this case anyway by replacing y with $-y$ if necessary. The same substitution proves a strong connections between the equations $x^3 - dy^3 = 1$ and $x^3 + dy^3 = 1$.*

Before proving this theorem, we give an example to illustrate its strength.

Example 13.0.12. *The equation $x^3 - 9y^3 = 1$ has an obvious solution i.e. $(1, 0)$ and a visible second solution i.e. $(-2, -1)$. By applying 13.0.10, we obtain that these are the only integer solutions of the equation.*

We make some notations and easy remarks first. Let $\theta = \sqrt[3]{d}$. On $K = \mathbb{Q}(\theta)$ we define a function $N : K \to \mathbb{C}$ by

$$N(a + b\theta + c\theta^2) = a^3 + b^3d + c^3d^3 - 3abcd$$

for all $a, b, c \in \mathbb{Q}$. It is obvious that $N(K) \subseteq \mathbb{Q}$ and $N(A) \subseteq \mathbb{Z}$. It is easy to prove that

$$N(x) = \sigma_1(x)\sigma_2(x)\sigma_3(x),$$

where $\sigma : K \to \mathbb{C}$ are the field homomorphisms uniquely determined by $\sigma_i(\theta) = \omega^{i-1}\theta$ for all $i = \overline{1,3}$, where $\omega = e^{\frac{2\pi i}{3}}$. With this remark it follows immediately that N is a multiplicative function on K and on A. Also, it is easy to prove that $u \in A$ is invertible in A if and only if $N(u) = \pm 1$. Notice that $\sigma_1 = 1_K$ and $\sigma_2 = \bar{\sigma}_3$, where $\bar{z}$ is the complex conjugate of the complex number z.

Lemma 13.0.13. *Let $\eta = P + Q\theta + R\theta^2$ such that $\eta \in U(A)$ and $|\eta| > 1$. Then $QR \neq 0$.*

Proof: Assume $QR = 0$. Then $Q = 0$ or $R = 0$. Eventually by changing η by $-\eta$, we can assume $N(\eta) = 1$.

We treat the case $R = 0$, the case $Q = 0$ being treated similarly. We have $1 = N(\eta) = P^3 + dQ^3$. It is easy to see that P and Q are nonzero and cannot have the same sign, hence $PQ < 0$. From this, we have

$$\eta = P + Q\theta = \frac{1}{P^2 - PQ\theta + Q^2\theta^2} \leq \frac{1}{1 + \theta + \theta^2} < \frac{1}{3} < 1.$$

Since $|\eta| > 1$, we obtain $\eta < -1$. But $N(\eta) = 1 \Rightarrow \sigma_1(\eta)\sigma_2(\eta)\sigma_3(\eta) = 1 \Rightarrow \eta \cdot |\sigma_2(\eta)|^2 = 1$. It follows that η is positive which is a contradiction. ■

Lemma 13.0.14. *1. If there exist $x, y \in \mathbb{Z}^*$ and $n \in \mathbb{Z}$ such that*

$$(x + y\theta)^n = a + b\theta \in U(A)$$

for some $a, b \in \mathbb{Z}$, then $|n| \leq 1$.

2. If there exist $x, y \in \mathbb{Z}^*$ and $n \in \mathbb{Z}$ such that

$$(x + y\theta^2)^n = a + b\theta \in U(A)$$

for some $a, b \in \mathbb{Z}$, then $n = 0$.

Proof: Because the proofs of the two statements are similar, we will only prove the first. We assume that $d \geq 3$ and solve the case $d = 2$ separately in the last part of the proof.

Assume there exist $x, y \in \mathbb{Z}^*$ and $n \in \mathbb{Z}$ with $|n| \geq 2$ and $(x + y\theta)^n = a + b\theta \in U(A)$. Then obviously $x + y\theta \in U(A)$. We can eventually replace x, y by $-x, -y$ to assume $x^3 + dy^3 = N(x + y\theta) = 1$. From Lemma 13.0.13, $|a + b\theta| \leq 1$ and $|x + y\theta| \leq 1$. Their absolute value cannot be 1 because of the assumption $x, y \in \mathbb{Z}^*$. $(x + y\theta)^n = a + b\theta$, $|x + y\theta| < 1$ and $|a + b\theta| < 1$ imply $n > 0$, so $n \geq 2$.

We have $1 = N(x + y\theta) = (x + y\theta) \cdot |\sigma_2(x + y\theta)|^2$, so $x + y\theta > 0$. Since $a + b\theta = (x + y\theta)^n$, we get $a + b\theta > 0$. If $|x| \leq 1$, then $dy^3 = 1 - x^3 \Rightarrow |dy^3| \leq 2$. From the assumption $d \geq 3$, we obtain $y = 0$. Since $x = x + y\theta \in U(A)$, $x = \pm 1$ and we contradict $|x + y\theta| < 1$. Therefore $|x| \geq 2$.

We have $(x+y\theta)^n = A_n + B_n\theta + C_n\theta^2$ for some $A_n,\ B_n,\ C_n \in \mathbb{Z}$. Since $\{1,\ \theta,\ \theta^2\}$ is a basis for $K = \mathbb{Q}(\theta)$ seen as a vector space over $\mathbb{Q}$, $A_n,\ B_n$ and C_n are uniquely defined. By identifying coefficients in $(x+y\theta)^n = a + b\theta$, using Newton's binomial expansion formula and $n \geq 2$, we get $C_n = 0 \Leftrightarrow$

$$\sum_{0\leq 3k+2\leq n} \binom{n}{3k+2} x^{n-3k-2} y^{3k+2} d^k.$$

Since we have proved that $|x| \geq 2$, there exists a prime number p dividing x.

According to the mod 3 residue of n, we have three cases.

If $n \equiv 2(mod\ 3)$, then

$$\binom{n}{2} x^{n-2}y^2 + \binom{n}{5} x^{n-5}y^5 d + \ldots + \binom{n}{n} y^n d^{\frac{n-2}{3}} = 0.$$

Reducing modulo x we see that $x | y^n d^{\frac{n-2}{3}}$. But $x^3 + dy^3 = 1$ implies that x and dy are coprime, so we obtain $|x| = 1$ which contradicts $|x| \geq 2$.

If $n \equiv 1(mod\ 3)$, then we can write the condition $C_n = 0$ as

$$\binom{n}{n-2} x^{n-2}y + \binom{n}{n-5} x^{n-5}y^5 d + \ldots + \binom{n}{2} x^2 y^{n-2} d^{\frac{n-4}{3}} = 0.$$

We can divide by x^2 which is nonzero for

$$\binom{n}{n-2} x^{n-4}y + \binom{n}{n-5} x^{n-7}y^5 d + \ldots + \binom{n}{5} x^3 y^{n-5} + \binom{n}{2} y^{n-2} d^{\frac{n-4}{3}} = 0.$$

Reducing modulo p and keeping in mind that x and dy are coprime (from $x^3 + dy^3 = 1$), we obtain $p | \binom{n}{2}$. Let $a \in \mathbb{N}^*$ such that $p^a | \binom{n}{2}$ and $p^{a+1} \not| \binom{n}{2}$ i.e. $0 < a = v_p\left(\binom{n}{2}\right)$. We prove that $p^{a+1} | \binom{n}{3k+2} x^{3k} y^{n-3k-2} d^k$ for all $k \geq 1$ i.e. p^{a+1} divides all the terms different form the last in the above sum. The last term is $\binom{n}{2} y^{n-2} d^{\frac{n-4}{3}}$ and it is divisible by p^a, but not by p^{a+1} because $gcd(x, dy) = 1$ and $p | x$. So if we manage to prove what we planned, then we obtain a contradiction modulo p^{a+1} in the second combinatorial sum above. It is enough to prove that $p^{a+1} | \binom{n}{3k+2} x^{3k}$ for all $k \geq 1$. $\binom{n}{3k+2} = \frac{n!}{(3k+2)!(n-3k-2)!} = \frac{n(n-1)}{2} \cdot \frac{(n-2)!}{(3k)!(n-2-3k)!} \cdot \frac{2}{(3k+1)(3k+2)}$, so

$$\binom{n}{3k+2} x^{3k} = \binom{n}{2} \cdot \binom{n-2}{3k} \cdot \frac{2}{(3k+1)(3k+2)} x^{3k}.$$

It is enough to prove $p | \binom{n-2}{3k} \cdot \frac{2}{(3k+1)(3k+2)} \cdot x^{3k}$. For this, since $p^{3k} | x^{3k}$, we prove $p^{3k} \not| (3k+1)(3k+2)$. Assume $p^{3k} | (3k+1)(3k+2)$. Then $p^{3k} | 3k+1$ or $p^{3k} | 3k+2$ because $gcd(3k+1, 3k+2) = 1$. But an easy induction proves $p^{3k} > 3k+2 > 3k+1$ for every prime $p \geq 2$ and $k \geq 1$, so we get our long sought contradiction and we are done with this case.

If $3|\ n$, then like before,

$$\binom{n}{n-2}x^{n-3}y^2+\ldots+\binom{n}{1}y^{n-1}d^{\frac{n-2}{3}}=0.$$

Reducing modulo p, we obtain $p|\ n$. Just like before, for $a=v_p(n)$ we prove that $p^{a+1}|\ \binom{n}{3k+1}x^{3k}$ for all $k\geq 1$ and we obtain a contradiction modulo p^{a+1} in the combinatorial sum above.

The proof of the lemma is complete if we solve the case $d=2$. By 6.2.4, the only integer solutions to $x^3+2y^3=1$ are $(1,0)$ and $(-1,1)$. This time we prove both parts of the lemma.

If $(x+y\theta)^n=a+b\theta\in U(A)=U(\mathbb{Z}[\sqrt[3]{2}])$ with $x,y\in\mathbb{Z}^*$ and $n\in\mathbb{Z}$, $|n|\geq 2$, then $x+y\theta\in U(A)$, so $x^3+2y^3=\pm 1$. We have seen far too many times how we can assume $x^3+2y^3=1$. But x and y are nonzero integers, so $x+y\theta=-1+\sqrt[3]{2}$. Similarly $a+b\theta\in\{1,\ -1+\sqrt[3]{2}\}$. $(-1+\sqrt[3]{2})^n\in\{1,\ -1+\sqrt[3]{2}\}$ contradicts $|n|\geq 2$.

If $(x+y\theta^2)^n=a+b\theta\in U(A)$ with $x,y\in\mathbb{Z}^*$ and $|n|\geq 1$, then $x+y\theta^2\in U(A)$, so $N(x+y\theta^2)=\pm 1\Leftrightarrow x^3+4y^3=\pm 1$. From 6.2.5 we get $x=\pm 1$ and $y=0$ which contradicts $x,y\in\mathbb{Z}^*$. ■

The following two lemmas will help us prove Theorem 13.0.10, but before dealing with them, we will see how they apply.

Lemma 13.0.15. *If there exists $\eta\in U(A)$ such that $\eta^2=a+b\theta$ for some $a,b\in\mathbb{Z}$, then $\eta=\pm 1$.*

Lemma 13.0.16. *If there exists $\eta\in U(A)$ such that $\eta^3=a+b\theta$ for some $a,b\in\mathbb{Z}$, then $\eta=\pm 1$.*

We prove the following form of 13.0.10:

Theorem 13.0.17. *Let d be a positive integer which is not a cube. Let $x,y\in\mathbb{Z}^*$ such that $x^3+dy^3=1$. Then there is no other integer solution of $X^3+dY^3=1$ with $XY\neq 0$. Moreover $U(A)=\{\pm(x+y\theta)^n|\ n\in\mathbb{Z}\}$.*

Proof: Since $N(x+y\theta)=x^3+dy^3=1$, $(x+y\theta)|\sigma_2(x+y\theta)|^2=1$, so $x+y\theta>0$. By 13.0.13, $0<x+y\theta<1$. With similar methods to the ones used in 12.0.8, it can be proved that there exists

$$\varepsilon_0=\max\{\varepsilon\in U(A)|\ x+y\theta\leq\varepsilon<1\}$$

and that

$$U(A)=\{\pm\varepsilon_0^n|\ n\in\mathbb{Z}\}.$$

Since $x+y\theta\in U(A)$, there exists $n\in\mathbb{Z}$ such that $x+y\theta=\pm\varepsilon_0^n$. Since $x+y\theta$ and ε_0 are positive, the sign " $\pm$ " is actually " $+$ ". Since $x+y\theta$ and ε_0 are strictly smaller than 1, $n>0$. From 13.0.15 and 13.0.16, n is odd and not a multiple of 3.

Let $\varepsilon_0 = P + Q\theta + R\theta^2$. We have $\pm 1 = N(\varepsilon_0) = \sigma_1(\varepsilon_0)\sigma_2(\varepsilon_0)\sigma_3(\varepsilon_0) = \varepsilon_0|\sigma_2(\varepsilon_0)|^2 > 0 \Rightarrow N(\varepsilon_0) = 1 \Rightarrow$

$$P^3 + dQ^3 + d^2R^3 - 3dPQR = 1 \tag{13.0.1}$$

Let $\eta = \sigma_2(\varepsilon_0)$ and $\gamma = \sigma_3(\varepsilon_0)$. Then $\eta^n = x + y\omega\theta$ and $\gamma^n = x + y\omega^2\theta$ because σ_i is a field homomorphism for all $i = \overline{1,3}$. $\varepsilon_0^n + \omega\eta^n + \omega^2\gamma^n = (1 + \omega + \omega^2)(x + y\theta) = 0 \Rightarrow \omega\eta^n + \omega^2\gamma^n = -\varepsilon_0^n \in U(A)$.

If $n \equiv 2(mod\ 3)$, then $\omega^n = \omega^2$ and $\omega^{2n} = \omega$. $U(A) \ni -\varepsilon_0^n = \omega\eta^n + \omega^2\gamma^n = (\omega^2\eta)^n + (\omega\gamma)^n \Rightarrow$

$$(\omega^2\eta + \omega\gamma)((\omega^2\eta)^{n-1} - (\omega^2\eta)^{n-2}(\omega\gamma) + \ldots + (\omega\gamma)^{n-1}) = -\varepsilon_0^n. \tag{13.0.2}$$

$\omega^2\eta + \omega\gamma = \omega^2\sigma_2(\varepsilon_0) + \omega\sigma_3(\varepsilon_0) = \omega^2(P + Q\omega\theta + R\omega^2\theta^2) + \omega(P + Q\omega^2\theta + R\omega\theta^2) = -P + 2Q\theta - R\theta^2 \in A$. It is clear that

$$(\omega^2\eta)^{n-1} - (\omega^2\eta)^{n-2}(\omega\gamma) + \ldots + (\omega\gamma)^{n-1} \in \mathbb{Z}[\theta, \omega].$$

We want to prove that it actually belongs to A. For this it is enough to prove that it is a real number since $A = \mathbb{Z}[\theta] = \mathbb{Z}[\theta, \omega] \cap \mathbb{R}$. But

$$(\omega^2\eta)^{n-1} - (\omega^2\eta)^{n-2}(\omega\gamma) + \ldots + (\omega\gamma)^{n-1} = \sum_{k=0}^{n-1}(-1)^k(\omega^2\sigma_2(\varepsilon_0))^k(\omega\sigma_3(\varepsilon_0))^{n-1-k} =$$

$$= \sum_{k=0}^{n-1}(-1)^k(\bar{\omega}\sigma_2(\varepsilon_0))^k(\omega\bar{\sigma}_2(\varepsilon_0))^{n-1-k}.$$

$$\overline{\sum_{k=0}^{n-1}(-1)^k(\bar{\omega}\sigma_2(\varepsilon_0))^k(\omega\bar{\sigma}_2(\varepsilon_0))^{n-1-k}} = \sum_{k=0}^{n-1}(-1)^k(\omega\bar{\sigma}_2(\varepsilon_0))^k(\bar{\omega}\sigma_2(\varepsilon_0))^{n-1-k} =$$

$$= \sum_{k=0}^{n-1}(-1)^{n-1-k}(\bar{\omega}\sigma_2(\varepsilon_0))^k(\omega\bar{\sigma}_2(\varepsilon_0))^{n-1-k} = \sum_{k=0}^{n-1}(-1)^k(\bar{\omega}\sigma_2(\varepsilon_0))^k(\omega\bar{\sigma}_2(\varepsilon_0))^{n-1-k},$$

hence $(\omega^2\eta)^{n-1} - (\omega^2\eta)^{n-2}(\omega\gamma) + \ldots + (\omega\gamma)^{n-1} \in A$. We have used here that n is odd, so $n-1$ is even. From the equation 13.0.2 it now follows that

$$\omega^2\eta + \omega\gamma = -P + 2Q\theta - R\theta^2 \in U(A),$$

so $\pm 1 = N(-P+2Q\theta-R\theta^2) = -P^3+8dQ^3-d^2R^3-6dPQR$. If we add this to the equation 13.0.1 for $N(\varepsilon_0) = 1$, we get $9dQ^3 - 9dPQR \in \{0,\ 2\}$. Since the left hand side is a multiple of 9, we get $9dQ^3 - 9dPQR = 0 \Rightarrow Q^3 = PQR \Rightarrow \begin{cases} Q = 0 \\ \text{or} \\ Q^2 = PR \end{cases}$. If $Q = 0$, then $PQ \neq 0$ because ε_0 is invertible and contained in $[x + y\theta, 1)$. $(P + R\theta^2)^n = x + y\theta$ and $n > 0$ now contradict the second part of Lemma 13.0.14. Therefore $Q \neq 0$ and $Q^2 = PR$.

We have $1 < \varepsilon_0^{-1} = \eta\gamma = (P + Q\omega\theta + R\omega^2\theta^2)(P + Q\omega^2\theta + R\omega\theta^2) = P^2 + Q^2\theta^2 + dR^2\theta - PQ\theta - PR\theta^2 - dRQ = (P^2 - dRQ) + (dR^2 - PQ)\theta + (Q^2 - PR)\theta^2 = (P^2 - dRQ) + (dR^2 - PQ)\theta$, which contradicts Lemma 13.0.13.

If $n \equiv 1(mod\ 3)$, then $\omega^n = \omega$ and $\omega^{2n} = \omega^2$. Just like before we obtain $\omega\eta + \omega^2\gamma = -P - Q\theta + 2R\theta^2 \in U(A)$, so

$$-P^3 - dQ^3 + 8d^2R^3 - 6dPQR = \pm 1.$$

By adding to the equation 13.0.2, we get $9d^2R^3 - 9dPQR \in \{0,\ 2\} \Rightarrow dR^3 = PQR$. If $dR^2 = PQ$, then $1 < \varepsilon_0^{-1} = (P^2 - dRQ) + (dR^2 - PQ)\theta + (Q^2 - PR)\theta^2 = (P^2 - dRQ) + (Q^2 - PR)\theta^2$ which contradicts Lemma 13.0.13.

Therefore $R = 0$. Since $\varepsilon_0^n = (P + Q\theta)^n = x + y\theta$, by the first part of Lemma 13.0.14 and by $n > 0$, we get $n = 1$ which means $x + y\theta = \varepsilon_0$. We have proved that $U(A) = \{\pm(x + y\theta)^n |\ n \in \mathbb{Z}\}$.

If $u + v\theta$ is another solution of $X^3 + dY^3 = 1$ with $uv \neq 0$, then just like before we prove that $u + v\theta = \varepsilon_0$. Therefore $u + v\theta = x + y\theta$, so (x, y) is the only solution of the equation $X^3 + dY^3 = 1$ with $x, y \in \mathbb{Z}^*$. ■

Proof of Theorem 13.0.10: The theorem above proves the hardest part of Theorem 13.0.10. It proves that if the equation $X^3 - dY^3 = 1$ has a non-trivial solution (x, y), then $\varepsilon_0 = x - y\theta$ and that the non-trivial solution is unique.

Conversely, if $\varepsilon_0 = a + b\theta$ for some $a, b \in \mathbb{Z}^*$, then $a^3 + db^3 = N(\varepsilon_0) = 1$, so $(a, -b)$ is a non-trivial solution to the equation and by applying Theorem 13.0.17 we prove that it is unique. ■

Proof of Lemma 13.0.15: Assume there exists $\eta \in U(A) \setminus \{\pm 1\}$ such that $\eta^2 = u + v\theta$ for some $u, v \in \mathbb{Z}$. Let $\eta = P + Q\theta + R\theta^2$. We can assume $N(\eta) = 1$ which means

$$P^3 + dQ^2 + d^2R^3 - 3dPQR = 1 \tag{13.0.3}$$

$\eta^2 = u + v\theta \Rightarrow$

$$2PR + Q^2 = 0 \tag{13.0.4}$$

i.e. the coefficient of θ^2 in η^2 is zero. If $gcd(P, R) \neq 1$, then there exists a prime number p dividing both of them. From the equation 13.0.4 it follows that $p|\ Q$ (even if $p = 2$). But then $p|\ \eta$ in A which is impossible since η is invertible, but $N(p) = p^3 > 1$ implies that p is not invertible. Therefore $gcd(P, R) = 1$.

If $PR = 0$, then 13.0.4 implies $Q = 0$ and we have the possibilities $(P, Q, R) = (0, \pm 1, 0)$ or $(P, Q, R) = (\pm 1, 0, 0)$. We use here $gcd(P, R) = 1$. $(P, Q, R) = (0, \pm 1, 0) \overset{13.0.3}{\Longrightarrow} \pm d^2 = 1$ which is impossible because d is not a cube. $(P, Q, R) = (\pm 1, 0, 0) \overset{13.0.3}{\Longrightarrow} \eta = \pm 1$ which contradicts the assumption $\eta \in U(A) \setminus \{\pm 1\}$. Therefore $PR \neq 0$.

From the equation 13.0.4 we have that there exist $a, b \in \mathbb{Z}^*$ such that $Q = 2ab$ and one of the following occurs:

If $P = -a^2$ and $R = 2b^2$, then from 13.0.3, $-a^6 + 8da^3b^3 + 8d^2b^6 + 12da^3b^3 = 1$ which yields a contradiction modulo 4. Similarly we prove that the case $P = 2a^2$ and $R = -b^2$ is contradictory.

If $P = a^2$ and $R = -2b^2$, then $a^6 + 8da^3b^3 - 8d^2b^6 + 12da^3b^3 = 1$. Set $x = db^3$. Then $1 = a^6 + 20a^3x - 8x^2 \Leftrightarrow (3a^2)^3 - (4x - 5a^3)^2 = 2$. It is known that the integer solutions of *Fermat's equation*, $2 + x^2 = y^3$, are $(x, y) \in (\pm 5, 3)$. It follows that $a^2 = 1$ and $4x - 5a^3 = \pm 5 \Rightarrow 4x \in \{0, \ \pm 10\} \Rightarrow x = 0 \Rightarrow db^3 = 0 \Rightarrow b = 0 \Rightarrow Q = R = 0$ and $P = 1$ which contradicts $\eta \neq \pm 1$.

If $P = -2a^2$ and $Q = b^2$, then $1 = -8a^6 + 20da^3b^3 + d^2b^6$. For $x = db^3$, we have $x^2 + 20a^3x - 8a^6 \Rightarrow (x + 10a^3)^2 - 108a^6 = 1$. Let $t = x + 10a^4$ and $s = 3a^2$. Then $t^2 - 1 = 4s^3 \Rightarrow \frac{t-1}{2} \cdot \frac{t+1}{2} = s^3$. Since $gcd(\frac{t-1}{2}, \frac{t+1}{2}) = 1$ we have $\frac{t-1}{2} = A^3$ and $\frac{t+1}{2} = B^3$ for some $A, B \in \mathbb{Z}$. Then $A^3 + 1 = B^3$ which implies $(A, B) \in \{(0, 1), \ (-1, 0)\} \Rightarrow t = \pm 1$ and $3a^2 = s = 0 \Rightarrow a = 0$ which implies $P = Q = 0$. But we have proved $PR \neq 0$, so we have found again a contradiction. ■

Similar methods can be used for a proof of Lemma 13.0.16. With the same notations as in the later proof, the equation 13.0.4 is replaced by

$$P^2R + PQ^2 + dQR^2 = 0.$$

It must be proved that $\eta = 1$ is the only solution of this equation such that $P^3 + dQ^3 + d^2R^3 - 3dPQR = 1$ i.e. $N(\eta) = 1$. The proof uses that the only integer solutions of the equation $x^3 - 9y^3 = 1$ are $(x, y) \in \{(1, 0), \ (-2, -1)\}$.