Density on Elliptic Curves

Sylvain Muise

A Thesis

in

The Department

of

Mathematics and Statistics

Presented in Partial Fulfillment of the Requirements
for the Degree of Master of Science (Mathematics) at
Concordia University
Montreal, Quebec, Canada

September 2007

Your file Votre référence
ISBN: 978-0-494-34449-1
Our file Notre référence
ISBN: 978-0-494-34449-1

ABSTRACT

Density on Elliptic Curves

Sylvain Muise

An elliptic curve is an object that has both the analytic structure of a Riemann Surface, and the algebraic structure of a group. Under this group structure, we can consider the cyclic subgroup generated by an algebraic point on the curve, and ask whether this subgroup is dense in the complex points on the curve, under the usual topology on the analytic structure.

We give conditions on the point in question for its multiples to be dense in the complex points on the curve. We discuss transcendence results for the Weierstrass $\wp$ function, analogous to results of the same nature for the regular exponential function.

Table of Contents

List of Figures

1 Introduction

1.1 Elliptic Curves

Let K be a perfect field, and let $\overline{K}$ be a fixed algebraic closure of K. Let $\overline{K}[X, Y, Z]$ denote the ring of polynomials over $\overline{K}$ in X, Y, Z.

Definition 1 *An* ***elliptic curve*** *E is a smooth curve (a 1-dimensional projective variety) of genus 1, having a specified basepoint O.*

The homogeneous ideal $I(V)$ of a projective variety V is given by

$$I(V) = \{\ f \in \overline{K}[X, Y, Z] \ \mid\ f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\ \}.$$

We say that E is **defined** over K if the homogeneous ideal $I(E)$ of E is generated by a homogeneous polynomial in $K[X, Y, Z]$. If char $K \neq 2, 3$, then $I(E)$ is generated by a polynomial of the form

$$f(X, Y, Z) = X^3 + aXZ^2 + bZ^3 - Y^2Z \ \in K[X, Y, Z].$$

When the equation for E is written in this form, the specified basepoint O corresponds to the point $[0, 1, 0] \in \mathbb{P}^2(\overline{K})$.

Switching to non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$, if E is defined over K, then E is given by an equation of the form

$$E : y^2 = x^3 + ax + b, \tag{1}$$

with $a, b \in K$.

Define the **discriminant** and the **j-invariant** by the formulas

$$\Delta = -16(4a^3 + 27b^2), \qquad j = \frac{1728(4a)^3}{\Delta}.$$

It can be shown that an equation of the form (1) is smooth if and only if $\Delta \neq 0$, and that two elliptic curves are isomorphic if and only if they have the same j-invariant.

The set $E(\overline{K})$ is the set of all points $(x, y) \in \mathbb{A}^2(\overline{K})$ that satisfy equation (1). The set of K-rational points of E is the set of points (x, y) in $E(\overline{K})$ such that both x and y are in K.

There is a group stucture on E, with identity element O, given by the following composition law:

Group Law: Let $P, Q \in E$, let L be the line connecting P and Q (tangent line to E if $P = Q$), and R the third point of intersection of L with E. Let L' be the line connecting R and O. Then $P + Q$ is the third point of intersection of L' with E.

Since the point O corresponds to the point at infinity in the purely vertical direction on E, the line L' through R and O is just the vertical line through R. This and the group law are illustrated in Figure 1.

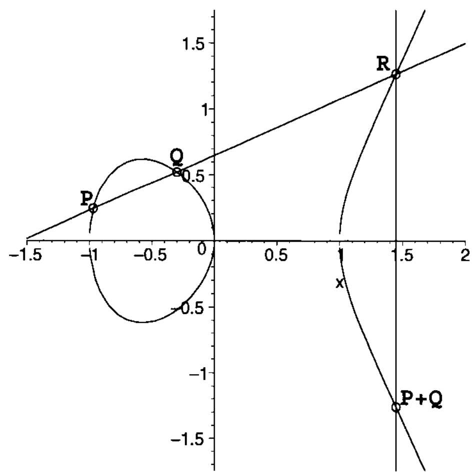

Figure 1: Addition of points on an elliptic curve

The inverse of a point P is given by the third intersection point of the line through P and O with the curve E. This is just the point vertically opposite to P on the curve.

It can be shown that this law does indeed define a group structure on E, and explicit fomulas for the sum of two points of E and the inverse of a point are given in terms of the cooefficients of E below:

Group Law: (Explicit) Let E be an elliptic curve given by the equation

$$E : y^2 = x^3 + ax + b,$$

and let $P_1 + P_2 = P_3$ with $P_i = (x_i, y_i) \in E$ for $i = 1, 2, 3$.

(a) If $P = (x, y) \in E$, then $-P = (x, -y)$.

(b) If $x_1 = x_2$ and $y_1 = -y_2$, then

$$P_1 + P_2 = O$$

(c) If $P_1 = P_2$, let

$$\lambda = \frac{3x_1^2 + a}{2y_1} \qquad \text{and} \qquad \nu = \frac{-x_1^3 + ax_1 + 2b}{2y_1}.$$

Otherwise, if $P_1 \neq P_2$, let

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{and} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

Then

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu).$$

These formulas are rational maps that are regular at each point on E, in other words we obtain two **morphisms**:

$$\begin{array}{rccc} + : & E \times E & \rightarrow & E \\ & (P_1, P_2) & \mapsto & P_1 + P_2 \end{array} \quad \text{and} \quad \begin{array}{rccc} - : & E & \rightarrow & E \\ & P & \mapsto & -P. \end{array}$$

An **isogeny** between two curves E_1 and E_2 is a morphism $\phi : E_1 \rightarrow E_2$ that satisfies $\phi(O) = O$. For an integer m, we have that the **multiplication by** m map given by

$$\begin{array}{rcl} [m] : E & \rightarrow & E \\ P & \mapsto & P + P + P \cdots + P \ (m \text{ terms}) \quad \text{if } m > 0 \\ P & \mapsto & [-m][-P] \qquad \text{if } m < 0 \\ O & \mapsto & O \end{array}$$

is an isogeny from E to itself. The ring of all isogenies from E to itself is denoted by $\mathrm{End}(E)$ and is called the **endomorphism ring** of E. The ring structure is given by pointwise addition and composition:

$$\begin{array}{rcl} (\phi + \psi)(P) & = & \phi(P) + \psi(P) \\ (\phi\psi)(P) & = & \phi(\psi(P)) \end{array}$$

We have that for any integer m, the map $[m]$ is in $\mathrm{End}(E)$, so we can say that $\mathbb{Z} \subset \mathrm{End}(E)$. If there is equality, there are no more maps to study on E. Otherwise, if

$$\mathbb{Z} \subsetneqq \mathrm{End}(E),$$

we say that E has **complex multiplications**. It can be shown that for any elliptic curve E, the endomorphism ring $\mathrm{End}(E)$ is either $\mathbb{Z}$, an order in a quadratic imaginary field, or an order in a quaternion algebra. In the case where E is defined of $\mathbb{C}$, it is either Z or an order in a quadratic imaginary field. So in this case, we can form the field of fractions of $\mathrm{End}(E)$, denoted by $\mathrm{End}^0(E)$, and it is called the field of endomorphisms of E.

If E is defined over $\mathbb{C}$, we also know that since the group law $+ : E \times E \to E$ is given by everywhere locally defined rational functions, the set $E(\mathbb{C})$ is a **complex Lie group**, i.e. a complex manifold with a group law given locally by complex analytic functions. This complex manifold has a natural topology given by the usual topology on $\mathbb{C}$. So by a **dense** subset of $E(\mathbb{C})$ we mean dense in this usual topology.

1.2 Elliptic Functions

Let $\Lambda \subset \mathbb{C}$ be a lattice, i.e. a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$. The **torus** $\mathbb{C}/\Lambda$ with its natural addition is also a complex Lie group. An **elliptic function** relative to the lattice Λ is a meromorphic function $f(z)$ on $\mathbb{C}$ such that

$$f(z+\omega) = f(z) \qquad \text{for all } \omega \in \Lambda, z \in \mathbb{C}.$$

The field of all such functions is denoted $\mathbb{C}(\Lambda)$.

A **fundamental parallelogram** for Λ is a set of the form

$$D = \{\ a + t_1\omega_1 + t_2\omega_2 \ \mid \ 0 \le t_1, t_2 < 1\ \},$$

where $a \in \mathbb{C}$ and ω_1, ω_2 are a basis for Λ.

The **Weierstrass $\wp$-function** (relative to Λ) is defined by

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

and for $0 \le k \in \mathbb{Z}$, the **Eisenstein series of weight** $2k$ (relative to Λ) is defined by

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^{2k}}.$$

When the lattice Λ is understood, we just write $\wp(z)$ and G_{2k}.

It can be shown that the series G_{2k} is absolutely convergent for all $k > 1$, that the series defining $\wp(z)$ is absolutely and uniformly convergent on every compact subset of $\mathbb{C} - \Lambda$, that $\wp(z)$ defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point, and no other poles, and that $\wp(z)$ is an even elliptic function. Moreover, for any lattice Λ, we could show that

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z)),$$

i.e. that every elliptic function is a rational combination of $\wp$ and $\wp'$.

If we set $g_2 = g_2(\Lambda) = 60G_4$ and $g_3 = g_3(\Lambda) = 140G_6$, then it can be shown that $\wp$ and $\wp'$ satisfy the following algebraic relation:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

If g_2 and g_3 are the quantities associated to a lattice $\Lambda \subset \mathbb{C}$, then it can be also be shown that the polynomial

$$y^2 = 4x^3 - g_2x - g_3$$

has distinct roots and non-zero discriminant, and that it defines an elliptic curve. For an elliptic curve E written in this form, we say that x, y are **Weierstrass coordinate functions of E.**

Conversely, let $E/\mathbb{C}$ be an elliptic curve. We quote the two following theorems from [5] on page 161:

Proposition 1 (Unifomization Theorem) *Let $A, B \in \mathbb{C}$ satisfy $A^3 - 27B^2 \neq 0$. Then there exists a unique lattice $\Lambda \subset \mathbb{C}$ such that $g_2(\Lambda) = A$ and $g_3(\Lambda) = B$.*

Proposition 2 *Let $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ be elliptic curves corresponding to lattices Λ_1 and Λ_2. Then E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if there is $\alpha \in \mathbb{C}^*$ such that $\Lambda_1 = \alpha\Lambda_2$ (i.e. Λ_1 and Λ_1 are homothetic).*

Then we can say that if $E/\mathbb{C}$ is given by $y^2 = 4x^3 - Ax - B$ with $A^3 - 27B^2 \neq 0$, then there exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, such that the following map is a complex analytic isomorphism of complex Lie groups:

$$\begin{array}{rcll} \exp_E : \mathbb{C}/\Lambda & \to & E(\mathbb{C}) & \\ z & \mapsto & (x, y) = (\wp(z), \wp'(z)), & \quad \text{if } z \notin \Lambda \\ \omega & \mapsto & O & \end{array}$$

where O is the "point at infinity". We call x, y the Weierstrass coordinate functions of E.

This means that the map $\exp_E$ is an isomorphism of Riemann surfaces, and a group homomorphism. Denote the inverse of this isomorphism by

$$\mathscr{L}_E : E(\mathbb{C}) \to \mathbb{C}/\Lambda.$$

It is given by

$$\mathscr{L}_E(P) = \int_O^P \frac{dx}{y} (\bmod \Lambda).$$

So for any elliptic curve E there is an associated lattice $\Lambda \subset \mathbb{C}$ such that $E(\mathbb{C})$ is isomorphic to the torus $\mathbb{C}/\Lambda$. In the case that E is defined over $\mathbb{R}$, we can show that the lattice is stable under complex conjugation:

Lemma 1 *If E is an elliptic curve defined over $\mathbb{R}$, and $\Lambda \subset \mathbb{C}$ is its associated lattice, then $\overline{\Lambda} = \Lambda$.*

Proof: Write E in the form

$$E(\Lambda) : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

where $g_2(\Lambda), g_3(\Lambda)$ are given by the Eisentein series above. The fact that E is defined over $\mathbb{R}$ means that $g_2(\Lambda), g_3(\Lambda) \in \mathbb{R}$.

We have

$$\begin{aligned} g_2(\overline{\Lambda}) &= 60 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\overline{\omega}^4} = \overline{60 \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^4}} \\ &= \overline{g_2(\Lambda)} = g_2(\Lambda) \end{aligned}$$

since $g_2(\Lambda) \in \mathbb{R}$. Similarly, $g_3(\overline{\Lambda}) = g_3(\Lambda)$. So by proposition 1, the lattices associated to $E(\Lambda)$ and $E(\overline{\Lambda})$ are exactly the same lattice. In other words $\Lambda = \overline{\Lambda}$. □

Let E be defined over $\mathbb{R}$ with associated lattice $\Lambda \subset \mathbb{C}$. Lemma 1 tells us that if ω is in Λ, its conjugate $\overline{w}$ is also in Λ. Therefore $\omega + \overline{\omega}$, which is real, is in Λ. So there exists a purely real period in Λ. Let ω_1 be the smallest such real period, which exists since Λ is a lattice (discussed in section 2.2).

Let $\omega_2 \notin \mathbb{R}$ be such that $\{\omega_1, \omega_2\}$ is a basis for Λ. We know that $\omega_2 + \overline{\omega}_2$ is in Λ, and since it is real, either

$$\omega_2 + \overline{\omega}_2 = 0 \quad \text{or} \quad \omega_2 + \overline{\omega}_2 = \omega_1.$$

In the first case, ω_2 is purely imaginary, which results in a rectangular lattice. In the second case we see that

$$\begin{aligned} \omega_2 + \overline{\omega_2} = \omega_1 &\Rightarrow 2\Re(\omega_2) = \omega_1 \\ &\Rightarrow \Re(\omega_2) = \frac{1}{2}\omega_1, \end{aligned}$$

which gives a diamond lattice. We have shown the following lemma:

Lemma 2 *With notation as above, if E is defined over $\mathbb{R}$, then Λ is either a rectangular lattice with $\Re(\omega_2) = 0$, or a diamond lattice with $\Re(w_2) = \frac{1}{2}\omega_1$.*

In either case, we can choose a pair of periods ω_1 and ω_2, such that ω_1 is purely real and ω_2 is purely imaginary, that generate a sub-lattice of Λ of index at most 2.

1.3 The Question

Let E be an elliptic curve defined over $\mathbb{Q}$, and let Λ be the associated lattice in the complex plane with basis $\{\omega_1, \omega_2\}$. A point $(x, y) \in E(\mathbb{C})$ is an algebraic point if $x, y \in \overline{\mathbb{Q}}$.

The set $E(\mathbb{R})$ is given by

$$E(\mathbb{R}) = \{(x, y) \in E(\mathbb{C}) \mid x, y \in \mathbb{R}\}.$$

If $P = (x, y) \in E(\mathbb{R})$, then $x = \overline{x}$. Let $z = \mathscr{L}_E(P)$. By the definition of $\exp_E$, we have

$$\wp(z) = \wp(\overline{z}).$$

Since $\wp$ is a doubly periodic function with respect to Λ, this means that

$$z \equiv \overline{z} \mod \Lambda.$$

Since $z - \overline{z}$ is purely imaginary, it either equals 0 or some imaginary period. If $z - \overline{z} = 0$, then $z \in \mathbb{R}$, and $\exp_E(\mathbb{R}) \subset E(\mathbb{R})$.

If Λ is a diamond lattice, then $\Re(\omega_2) = \frac{1}{2}\omega_1$. A fundamental parallelogram D for this lattice can be divided into four equal right triangles. It is easy to see that if z is in one triangle, then $\overline{z}$ is not in the same one. Therefore if $z \notin \mathbb{R}$, then $z \not\equiv \overline{z} \mod \Lambda$. In this case, $\exp_E(\mathbb{R}) = E(\mathbb{R})$. This corresponds to a one component real locus.

Otherwise if Λ is a rectangular lattice, then we may have $z - \overline{z} = \omega_2$, which means that $\Im(z) = \frac{1}{2}\Im(\omega_2)$. So the horizontal line bisecting the square also corresponds to real points on the curve. This is the case where the real locus of E has two connected components, as in Figure 1, where the polynomial defining E has three real roots.

Let $E^+(\mathbb{C}) = E(\mathbb{R})$ and let $E^-(\mathbb{C}) = \{P \in E(\mathbb{C}) \mid P = -\overline{P}\}$. We would like to study the following question, given in [3]:

Conjecture 1 *Let P be an algebraic point on $E/\mathbb{Q}$, such that there is no $\lambda \in \mathrm{End}(E)$ such that $\lambda(P) \in E^+(\mathbb{C}) \cup E^-(\mathbb{C})$. Then $\mathbb{Z}P$, the cyclic subgroup generated by P in $E(\mathbb{C})$, is dense in $E(\mathbb{C})$.*

Given the isomorphism between $E(\mathbb{C})$ and $\mathbb{C}/\Lambda$, we can consider the point $z = \mathscr{L}_E(P)$ in $\mathbb{C}/\Lambda$, and we can rephrase the conjecture to say, if there is no $\lambda \in \mathrm{End}(E)$ such that λz is purely real, then cyclic subgroup of $\mathbb{C}/\Lambda$ generated by z is dense in $\mathbb{C}/\Lambda$. By dense we mean in the usual topology on $\mathbb{C}$. First let's consider some specific examples and compute the multiples of certain points on those curves. The program used to produce this data is given in section 6.

1.4 Experimental Data

Let E be the curve given by $y^2 = x^3 - x$. This curve has complex multiplication by i given by $[i] : (x, y) \longmapsto (-x, iy)$, and we know that $\mathrm{End}^0(E) = \mathbb{Q}(i)$. The lattice Λ associated to this curve is a square lattice: let ω_1, ω_2 be a basis for Λ with ω_1 purely real and ω_2 purely imaginary and $|\omega_1| = |\omega_2|$. A non-zero element $\lambda = (a + bi) \in \mathrm{End}^0(E)$ corresponds to multiplication by $a + bi$ on the torus $\mathbb{C}/\Lambda$.

First let's take the point $z_1 = \frac{3}{7}\omega_1 + \frac{5}{9}\omega_2$, and $P_1 = \exp_E(z_1)$. The subgroup $\mathbb{Z}P_1$ should not be dense since $[9]P_1 \in E(\mathbb{R})$. Indeed, Figure 2 shows the first 100 multiples of z_1 in $\mathbb{C}/\Lambda$, and we see that $\mathbb{Z}P_1$ is not dense in E.

Next let $z_2 = \dfrac{\omega_1/3}{2+5i}$, and $P_2 = \exp_E(z_2)$. This point should not be dense either, since $[2 + 5i]P_2 \in E(\mathbb{R})$. Indeed, the first 1000 multiples of z_2 in $\mathbb{C}/\Lambda$ are shown in Figure 3. Again $\mathbb{Z}P_2$ is not dense.

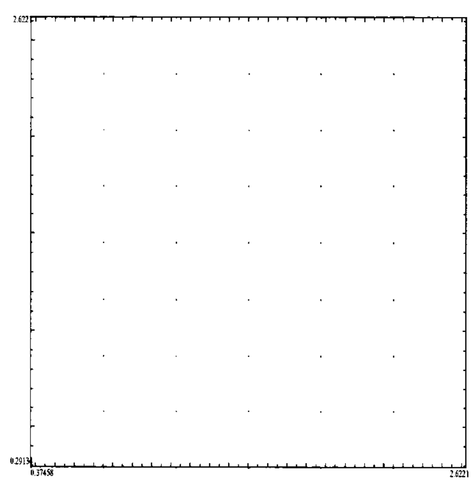

Figure 2: 100 multiples of $z_1 = \frac{3}{7}\omega_1 + \frac{5}{9}\omega_2$

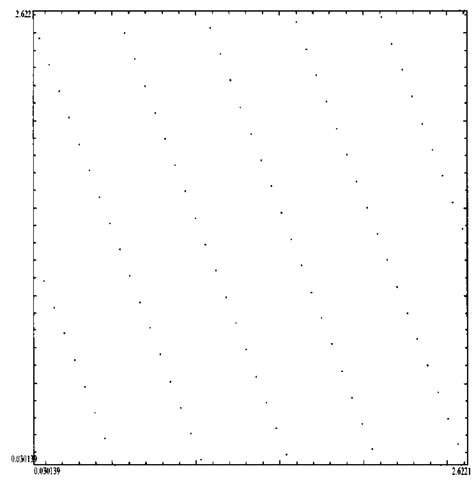

Figure 3: 1000 multiples of $z_2 = \dfrac{\omega_1/3}{2+5i}$

Now let $z_3 = \dfrac{\sqrt{2}\omega_1}{2+5i}$, and $P_3 = \exp_E(z_3)$. As with the last example, $[2+5i]P_3 \in E(\mathbb{R})$, so we do not expect $\mathbb{Z}P_3$ to be dense in $E(\mathbb{C})$. The first 10,000 multiples of z_3 in $\mathbb{C}/\Lambda$ are shown in Figure 4. True enough, $\mathbb{Z}P_3$ is not dense everywhere in $E(\mathbb{C})$, but it does seem to

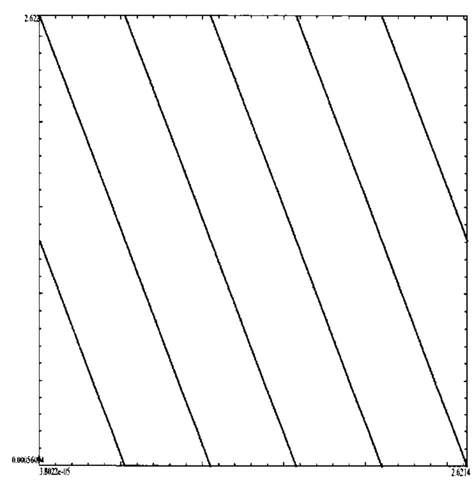

Figure 4: 10,000 multiples of $z_3 = \dfrac{\sqrt{2}\omega_1}{2+5i}$

be dense on a set of lines in $\mathbb{C}/\Lambda$. It isn't dense everywhere in $\mathbb{C}/\Lambda$ because it is a division point of a real point, but it is dense in a set on lines because that real point is irrational.

Finally let $z_4 = \sqrt{2}\omega_1 + \sqrt{3}\omega_2$, and $P_4 = \exp_E(z_4)$. The first 100,000 multiples of z_4 in $\mathbb{C}/\Lambda$ are shown in Figure 5. This time the multiples are dense, and we notice that the coordinates of z_4, with respect to the basis ω_1, ω_2, are linearly independent over $\mathbb{Q}$. Is this

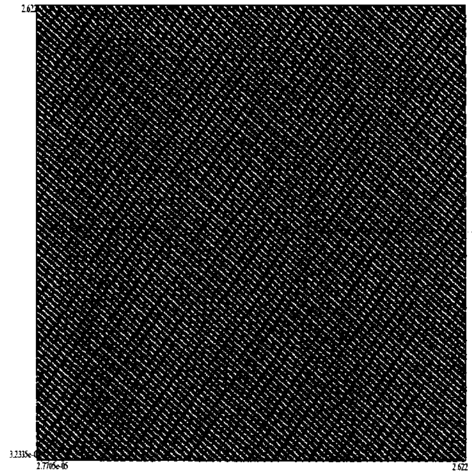

Figure 5: 100,000 multiples of $z_4 = \sqrt{2}\omega_1 + \sqrt{3}\omega_2$

always true, and is this condition enough to prove conjecture 1? We will need Kronecker's theorem to prove this, and it is proved in the following section.

2 Kronecker's Theorem

2.1 Definitions

Let G be a $\mathbb{Z}$-submodule of $\mathbb{R}^n$. If $G = \{a_1 y_1 + \ldots + a_k y_k \mid a_i \in \mathbb{Z}\}$ we say that G is generated by the set $\{y_1, \ldots, y_k\} \subset \mathbb{R}^n$, and write $G = \langle y_1, \ldots, y_k \rangle$.

Definition 2 *If $G = \langle y_1, \ldots, y_k \rangle$, the* rank r *of G is equal to the dimension of the $\mathbb{R}$-vector space spanned by $\{y_1, \ldots, y_k\}$.*

The rank of a $\mathbb{Z}$-submodule $G \subset \mathbb{R}^n$ represents the maximum number of $\mathbb{R}$-linearly independent elements we can find in G. Since the vector space spanned by $\{y_1, \ldots, y_k\}$ is a subspace of $\mathbb{R}^n$, we know that $0 \leq r \leq n$.

For $x = (x_1, \ldots, x_n) \in G$, define the norm of x to be $N(x) = \sqrt{x_1^2 + \ldots + x_n^2}$. For any $\epsilon > 0$, let

$$B(\epsilon) = \{x \in G \mid N(x) < \epsilon\}$$

and let $r(\epsilon)$ be the maximum number of $\mathbb{R}$-linearly independent elements of $B(\epsilon)$. Since $B(\epsilon) \subset G$, we know that $0 \leq r(\epsilon) \leq r$. As ϵ goes to zero, the function $r(\epsilon)$ is non-increasing, therefore it attains a limit since it is bounded below by 0.

Definition 3 *The* local rank *s of G is given by*

$$s = \lim_{\epsilon \longrightarrow 0} r(\epsilon).$$

In words, the local rank s of a $\mathbb{Z}$-submodule $G \subset \mathbb{R}^n$ is the maximum number of $\mathbb{R}$-linearly independent elements of G of arbitrarily small norm. Like $r(\epsilon)$, the local rank is bounded by 0 and r, and there is a small enough ϵ such that $r(\epsilon) = s$.

2.2 Discrete Submodules

If $s = 0$, this means that there do not exist non-zero elements of G of arbitrarily small norm. We call G a *discrete* $\mathbb{Z}$-submodule of $\mathbb{R}^n$. If G is discrete then there exists an $\epsilon > 0$ such that $x \in G$ and $N(x) < \epsilon$ together imply $x = 0$. Using this we can see that a discrete $\mathbb{Z}$-submodule G is a closed subset of $\mathbb{R}^n$:

Let $\{y_n\}_{n=1}^{\infty}$ be a sequence of elements of a discrete G that converges to $y \in \mathbb{R}^n$. This says that for any $\epsilon > 0$, there is an $n_0 \in \mathbb{Z}^+$ such that $N(y - y_n) < \epsilon$ for all $n > n_0$. But by above, for some ϵ small enough this means that $y = y_n$ for all $n > n_0$, and therefore $y \in G$, and G is closed.

We can always choose $\mathbb{R}$-linearly independent elements $y_1, \ldots, y_r \in G$ where r is the rank of G. We can construct an $\mathbb{Z}$-basis for G from these elements to show that G is a free $\mathbb{Z}$-module:

Proposition 3 *Let G be a discrete $\mathbb{Z}$-submodule of $\mathbb{R}^n$ and suppose the rank of G is r. Then $G \backsimeq \mathbb{Z}^r$.*

Proof: Let $\{y_1, \ldots, y_r\}$ be any set of $\mathbb{R}$-linearly independent elements of G. We must produce a basis $\{x_1, \ldots, x_r\}$ for G such that $G = \mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_r \backsimeq \mathbb{Z}^r$.

For any integer k with $1 \leq k \leq r$, let M be the k-dimensional vector space spanned by the vectors $\{y_1, \ldots, y_k\}$ and let $L = M \cap G$:

$$\begin{aligned} M &= \{\lambda_1 y_1 + \ldots + \lambda_k y_k,\ \lambda_i \in \mathbb{R}\} \\ L &= M \cap G. \end{aligned}$$

We can always write elements in M with respect to its basis $\mathcal{B} = \{y_1, \ldots, y_k\}$. So if we have $x = (\lambda_1, \ldots, \lambda_k)_{\mathcal{B}} \in M$ such that $\lambda_i \in \mathbb{Z}$ for all i, then $x \in G$ by the module property since $y_1, \ldots, y_k \in G$. Therefore L is non-empty.

However the converse is not true. Take for example the lattice $G = \langle e_1, e_2, P\rangle \subset \mathbb{R}^2$, where e_1, e_2 are the standard basis vectors and $P = (1/2, 1/2)$. The rank of G is 2, and the set $\{y_1, y_2\} = \{(5/2, 5/2), (-3, 9)\}$ is $\mathbb{R}$-linearly independent. Then the point P is in G, but $P = y_1/5$.

Consider the subset $L' \subset L$ containing elements whose first $k-1$ coordinates are bounded by 0 and 1, and whose last coordinate is bounded below by 0:

$$L' = \{x = (\lambda_1, \ldots, \lambda_k)_{\mathcal{B}} \in L \mid 0 \leq \lambda_i < 1, \text{ for } 1 \leq i \leq k-1, \text{ and } \lambda_k > 0\}$$

This set is non-empty since $x = (0, \ldots, 0, \lambda_k)_{\mathcal{B}} \in L'$ for any positive integer λ_k. The idea is to find $x \in L'$ such that λ_k is minimum.

Let $\pi_i : L' \longrightarrow \mathbb{R}$ be the natural projection map onto the i-th component. The image of this map, $\pi_k(L')$, is a subset of the interval $(0, \infty)$, since $\lambda_k > 0$ for all $x \in L'$. Therefore an infimum of the set $\pi_k(L')$ exists. Let

$$c_k = \inf \pi_k(L').$$

Then c_k must belong to $\pi_k(L')$, for if it doesn't, there would exist a sequence of elements of L' whose k-th coordinate tends to c_k. Since all other coordinates of elements of L' are bounded, there is a subsequence that converges to a limiting vector of $\mathbb{R}^n$. But since G is closed in $\mathbb{R}^n$, there must be some element of L' with $\lambda_k = c_k$. Call this element x_k:

$$x_k = c_{k1}y_1 + \ldots + c_{k,k-1}y_{k-1} + c_k y_k \tag{2}$$

with $c_{ki} \in [0, 1)$ for $1 \leq i \leq k-1$ and $c_k > 0$.

For each $1 \leq k \leq r$, we can find a corresponding x_k. The set $\{x_1, \ldots, x_r\}$ then forms a basis for G:

Suppose we have $\lambda_1 x_1 + \ldots + \lambda_r x_r = 0$ for some λ_i. Using (2) we can rewrite this in terms of y_i:

$$\sum_{i=1}^{r-1} \mu_i y_i + \lambda_r c_r y_r = 0$$

where the μ_i's are some linear combination of $\lambda_1, \ldots, \lambda_{r-1}$. Now y_r is $\mathbb{R}$-linearly independent of $y_1, \ldots, y_{r-1}$, and $c_r \neq 0$, so $\lambda_r = 0$. Repeating this starting with $\lambda_1 x_1 + \ldots + \lambda_{r-1} x_{r-1} = 0$, and again, etc, we get that $\lambda_1 = \ldots = \lambda_{r-1} = 0$, so we get that $x_1, \ldots, x_r$ is $\mathbb{R}$-linearly independent.

We can now say that any element $x \in G$ can be written as $x = \sum_{i=1}^{r} \nu_i x_i$, where the ν_i's are in $\mathbb{R}$. We want to show that $\nu_i \in \mathbb{Z}$ for all i.

Suppose $x \in G$ is such that not all the ν_i's are integers. Let ν_k be the last one that isn't, i.e. $\nu_{k+1}, \ldots, \nu_r \in \mathbb{Z}$. Then $\sum_{i=k+1}^{r} \nu_i x_i$ is an element of G, and

$$x - \sum_{i=k+1}^{r} \nu_i x_i = \sum_{i=1}^{k} \nu_i x_i$$

is also in G. Now let $\nu_k = h_k + r_k$ with $h_k \in \mathbb{Z}$ and $0 < r_k < 1$. So

$$\sum_{i=1}^{k} \nu_i x_i - h_k x_k = \sum_{i=1}^{k-1} \nu_i x_i + r_k x_k$$

is in G with $0 < r_k < 1$, since $h_k x_k \in G$. Using (2) again we can rewrite this in terms of the y_i's:

$$\sum_{i=1}^{k-1} \nu_i' y_i + r_k c_k y_k$$

where $\nu_1', \ldots, \nu_{k-1}'$ are real numbers. For all i, let $\nu_i' = h_i + r_i$ with $h_i \in \mathbb{Z}$ and $0 \leq r_i < 1$. Since $\sum_{i=1}^{k-1} h_i y_i$ is in G, we get that

$$\sum_{i=1}^{k-1} \nu_i' y_i + r_k c_k y_k - \sum_{i=1}^{k-1} h_i y_i = \sum_{i=1}^{k-1} r_i y_i + r_k c_k y_k$$

is also in G, with $0 \leq r_i < 1$ for $i \in [1, k-1]$ and $0 < r_k < 1$. So we now have an element of G, which is in L', whose k-th component is less than c_k, which contradicts the definition of c_k, therefore all the ν_i's are integers, and $G \simeq \mathbb{Z}^r$ is a lattice. □

2.3 Non-discrete Submodules

If $s > 0$, then we can always choose s linearly independent elements of G of arbitrarily small length.

For ϵ small enough so that $r(\epsilon) = s$, let $\{y_1, \ldots, y_s\}$ be linearly independent elements such that $N(y_i) < \epsilon$ for all i. Let E be the $\mathbb{R}$-vector space spanned by $\{y_1, \ldots, y_s\}$, and let D be the set of elements of G that are also in E;

$$\begin{aligned} E &= \{x \in \mathbb{R}^n \mid x = \lambda_1 y_1 + \ldots + \lambda_s y_s,\ \lambda_i \in \mathbb{R}\} \\ D &= E \cap G. \end{aligned}$$

The set D is non-empty since $y_i \in D$ for all i. If $x, y \in D$, and $a \in \mathbb{Z}$, then $x + ay \in G$ since $x, y \in G$, and $x + ay \in E$ since $x, y \in E$. Therefore $x + ay \in E \cap G = D$, and D is a $\mathbb{Z}$-submodule of G.

Lemma 3 *D is dense in E. In other words, the closure $\overline{D}$ of D is E.*

Proof: Let $\overline{y} \in E$. We must find an element $y \in D$ that is arbitrarily close to $\overline{y}$. For any $\delta > 0$, choose as a basis for E vectors $y_1, \ldots, y_s$ of length less than δ/s. We can always choose δ small enough so that $r(\delta/s) = s$. We can express $\overline{y}$ in terms of this basis of E:

$$\overline{y} = \sum_{i=1}^{s} \lambda_i y_i \qquad \lambda_i \in \mathbb{R} \tag{3}$$

We can write $\lambda_i = g_i + r_i$ with $g_i \in \mathbb{Z}$, and $0 \leq r_i < 1$, so (3) becomes

$$\begin{aligned} \overline{y} &= \sum_{i=1}^{s} g_i y_i + \sum_{i=1}^{s} r_i y_i \\ &= y + \sum_{i=1}^{s} r_i y_i \end{aligned}$$

where y is some element of $E \cap G = D$. The distance between $\overline{y} \in E$ and $y \in D$ is then

$$|\overline{y} - y| = \left| \sum_{i=1}^{s} r_i y_i \right| \leq \sum_{i=1}^{s} |r_i y_i| < \sum_{i=1}^{s} |y_i| < s\frac{\delta}{s} = \delta$$

since $0 \leq r_i < 1$ and $|y_i| < \delta/s$. So $\overline{y} \in \overline{D}$ and $\overline{D} = E$. □

If $s = r$, the rank of G, then we can always choose r linearly independent elements of G of arbitrary length, so $D = G$. If not, let $q = r - s$. We can choose q $\mathbb{R}$-linearly independent elements $z_1, \ldots, z_q$ of G that are linearly independent of $y_1, \ldots, y_s$. Let M be the subspace of $\mathbb{R}^n$ generated by $z_1, \ldots, z_q$, and let $L = M \cap G$. Then

Proposition 4 *L is a lattice of rank $q = r - s$.*

Proof: First, L is a $\mathbb{Z}$-submodule of G since if $x, y \in L$, and $a \in \mathbb{Z}$, then $x + ay \in M$ since $x, y \in M$, and $x + ay \in G$ since $x, y \in G$, so $x + ay \in M \cap G = L$.

Now suppose L is not discrete. Then there is at least one x in L of arbitrarily small length, which by construction is $\mathbb{R}$-linearly independent of $y_1, \ldots, y_s$. So we have $s + 1$ $\mathbb{R}$-linearly independent arbitrarily small elements of G, which contradicts the definition of s. Therefore L is discrete, and $L \backsimeq \mathbb{Z}^{r-s}$ by Proposition 3. □

We can then conclude that $G = D \oplus L$. In other words, if $x \in G$, then

$$x = \sum_{i=1}^{s} \lambda_i y_i + \sum_{j=1}^{q} a_j z_j$$

where the y_i's are a basis for E, the z_i's are a basis for L, the λ_i's are some real numbers, and the a_i's are integers.

Since a lattice is a closed subset of $\mathbb{R}^n$ and we know that $\overline{D} = E$, we have that $\overline{G} = E \oplus L$.

2.4 Characters

A continuous function $\chi : \mathbb{R}^n \longrightarrow \mathbb{R}$ satisfying

$$\chi(x+y) = \chi(x) + \chi(y), \quad x, y \in \mathbb{R}^n \tag{4}$$

is called a *character* on G if $\chi(x)$ is an integer for all $x \in G$. From this we can see that $\chi(0) = 0$, since $\chi(x) = \chi(x+0) = \chi(x) + \chi(0)$ and subtracting by $\chi(x)$ we get $0 = \chi(0)$.

Characters exist since $\chi(x) := 0$ for all $x \in G$ is a character, and it is called the trivial character. We have for $a \in \mathbb{Z}$ and $x \in G$, $\chi(ax) = \chi(x+\ldots+x) = \chi(x)+\ldots+\chi(x) = a\chi(x)$. So χ is a linear function on G, and for $x = (x_1, \ldots, x_n)$,

$$\chi(x) = \xi_1 x_1 + \ldots + \xi_n x_n, \quad \xi_i \in \mathbb{R}, \ \forall i.$$

We can then think of χ as follows:

$$\begin{aligned} \chi : \mathbb{R}^n &\longrightarrow \mathbb{R} \\ x &\longmapsto x \cdot \xi \end{aligned}$$

where $\xi = (\xi_1, \ldots, \xi_n)$, and $x \cdot \xi$ is the dot product. The vector ξ determines χ, and vice versa, and we mean by χ_ξ the character determined by ξ.

Let $\mathcal{B} = \{y_1, \ldots, y_s, z_1, \ldots, z_q, t_1, \ldots, t_{n-r}\}$ be a basis for $\mathbb{R}^n$, where the y_i's are a basis of E, the z_j's are a basis for L, and the t_k's are $n-r$ linearly independent vectors in the orthogonal complement with respect to the usual inner product to the vector space spanned by G in $\mathbb{R}^n$. Then any x in $\mathbb{R}^n$ written with coordinates with respect to $\mathcal{B}$ looks like

$$x = (\lambda_1, \ldots, \lambda_s, \mu_1, \ldots, \mu_q, \nu_1, \ldots, \nu_{n-r})_{\mathcal{B}}, \quad \lambda_i, \mu_j, \nu_k \in \mathbb{R} \tag{5}$$

with $x \in G$ only if $\mu_j \in \mathbb{Z}$ and $\nu_k = 0$ for all j and k.

Let χ be determined by

$$\xi = (a_1, \ldots, a_s, b_1, \ldots, b_q, c_1, \ldots, c_{n-r})_{\mathcal{B}}. \tag{6}$$

Then for $x \in \mathbb{R}^n$ as above, we have

$$\chi(x) = \sum_{i=1}^{s} \lambda_i a_i + \sum_{j=1}^{q} \mu_j b_j + \sum_{k=1}^{n-r} \nu_k c_k \ .$$

Proposition 5 *χ is a character of G if and only if $a_i = 0$ for all $1 \leq i \leq s$ and $b_j \in \mathbb{Z}$ for all $1 \leq j \leq q$.*

Note that this says nothing about the c_k's; they can be arbitrary real numbers.

Proof: For the '*if*' part, if $x \in G$, then

$$\chi(x) = \sum_{i=1}^{s} \lambda_i \cdot 0 + \sum_{j=1}^{q} \mu_j b_j + \sum_{k=1}^{n-r} 0 \cdot c_k = \sum_{j=1}^{q} \mu_j b_j.$$

But both the μ_j's and the b_j's are integers, so χ is a character of G.

Now suppose χ is a character, i.e. $\chi(x) \in \mathbb{Z}$ for all $x \in G$. Let x be any element of D. Then x is of the form $x = (\lambda_1, \ldots, \lambda_s, 0, \ldots, 0, 0, \ldots, 0)_{\mathcal{B}}$. When restricted to D, χ is a continuous *integer*-valued function on a dense subset of a vector space. So χ must be constant, and since $\chi(0) = 0$, we have for all $x \in D$:

$$\chi(x) = \sum_{i=1}^{s} \lambda_i a_i = 0$$

which implies that $a_i = 0$ for all i.

Now suppose one of b_j's is not an integer, say $b_1 \notin \mathbb{Z}$. Then for $z_1 = (0, \ldots, 0, 1, \ldots, 0, 0, \ldots, 0)_{\mathcal{B}}$ we have

$$\chi(z_1) = 1 \cdot b_1 \notin \mathbb{Z}$$

but $z_1 \in G$. So χ is not a character of G. $\square$

2.5 Character Groups

Let $G^\star$ be the set of vectors in $\mathbb{R}^n$ that determine a character on G. Then $G^\star$ is a $\mathbb{Z}$-submodule of $\mathbb{R}^n$ since for $\xi_1, \xi_2 \in G^\star$, $a \in \mathbb{Z}$, and $x \in G$, we have

$$x \cdot (\xi_1 + a\xi_2) = x \cdot \xi_1 + a(x \cdot \xi_2) \in \mathbb{Z}$$

since ξ_1 and ξ_2 determine characters on G. So $\xi_1 + a\xi_2 \in G^\star$. We call $G^\star$ the character group of G.

Lemma 4 *Any character group $G^\star$ is a closed subset of $\mathbb{R}^n$.*

Proof: Suppose $\{\xi_n\}_{n=1}^{\infty}$ is a sequence of elements of $G^\star$ that converge to a vector $\xi \in \mathbb{R}^n$. For any $x \in G$, it follows that $x \cdot \xi_n \to x \cdot \xi$ since the scalar product is a continuous function. But $x \cdot \xi_n$ is an integer for all n, therefore $x \cdot \xi \in \mathbb{Z}$, since $\mathbb{Z}$ is closed, so $\xi \in G^\star$. $\square$

We can now prove a duality theorem for these characters:

Proposition 6 $(G^\star)^\star = \overline{G}$. *In words, the character group of the character group of G is the closure of G.*

Proof: Let $x \in G$. Since for any $\xi \in G^\star$, we have that $x \cdot \xi \in \mathbb{Z}$, we see that x determines a character of $G^\star$. i.e. $x \in (G^\star)^\star$. Therefore $G \subset (G^\star)^\star$. But since any character group is closed, we have that $\overline{G} \subset (G^\star)^\star$.

Recall that $\overline{G} = E \oplus L$, so that any $x \in \overline{G}$ written as in (5) has $\lambda_i \in \mathbb{R}$, $\mu_i \in \mathbb{Z}$, and $\nu_i = 0$. Suppose $x \notin \overline{G}$. Then either $\mu_i \notin \mathbb{Z}$ for some i, or $\nu_i \neq 0$ for some i. In either case, x cannot be in $(G^\star)^\star$.

Suppose $\mu_1 \notin \mathbb{Z}$, and let $\xi \in G^\star$ with $b_1 = 1$ and every other coordinate equal 0 in the representation for ξ given in (6). Then

$$x \cdot \xi = \mu_1 \cdot 1 \notin \mathbb{Z}$$

so $x \notin (G^\star)^\star$.

Now suppose $\nu_1 \neq 0$, and let $\xi \in G^\star$ with $c_1 = 1/2\nu_1$ and every other coordinate 0. Then

$$x \cdot \xi = \nu_1 \cdot \frac{1}{2\nu_1} = \frac{1}{2} \notin \mathbb{Z}$$

so $x \notin (G^\star)^\star$, and we have that $(G^\star)^\star \subset \overline{G}$. Therefore $(G^\star)^\star = \overline{G}$. □

2.6 Kronecker's theorem

Let $G \in \mathbb{R}^n$ be generated by $e_1, \ldots, e_n, P$ where $P = (x_1, \ldots, x_n)$ and the e_i's are the standard basis vectors. Given $b \in \mathbb{R}^n$, when is $b \in \overline{G}$? First a little lemma:

Lemma 5 *The vector $\xi = (\xi_1, \ldots, \xi_n)$ is a character of G if and only if $\xi_i \in \mathbb{Z}$ for all i, and $\xi_1 x_1 + \ldots + \xi_n x_n \in \mathbb{Z}$.*

Proof: If ξ is a character of G, then in particular $e_i \cdot \xi = \xi_i \in \mathbb{Z}$ for all i, and also we have $\xi \cdot P = \xi_1 x_1 + \ldots + \xi_n x_n \in \mathbb{Z}$. This proves the only if part.

The converse is true since for $x \in G$, we can write $x = a_1 e_1 + \ldots + a_n e_n + a_{n+1} P = \begin{pmatrix} a_1 + a_{n+1} x_1 \\ \vdots \\ a_n + a_{n+1} x_n \end{pmatrix}$ with $a_i \in \mathbb{Z}$, so for some vector $\xi = (\xi_1, \ldots, \xi_n)$ satisfying $\xi_i \in \mathbb{Z}$ and

$\xi_1 x_1 + \ldots + \xi_n x_n \in \mathbb{Z}$ we have

$$\begin{aligned} x \cdot \xi &= (a_1 + a_{n+1}x_1)\xi_1 + \ldots + (a_n + a_{n+1}x_n)\xi_n \\ &= a_1\xi_1 + \ldots + a_n\xi_n + a_{n+1}(x_1\xi_1 + \ldots + x_n\xi_n) \in \mathbb{Z} \end{aligned}$$

by assumption on the ξ_i's, and therefore ξ is a character of G. □

We can now use Proposition 6 to prove:

Theorem 1 (Kronecker) $\overline{G} = \mathbb{R}^n$ *if and only if* $\{1, x_1, \ldots, x_n\}$ *are* $\mathbb{Q}$*-linearly independent.*

Proof: Let $b \in \overline{G}$. This means that G is dense in all of $\mathbb{R}^n$, and therefore $G = D$. So as in the proof of proposition 5, χ is identically zero on all of $\mathbb{R}^n$, for each $\chi \in G^\star$.

Suppose we have $a_1x_1 + \ldots + a_nx_n = a$ with $a_1, \ldots, a_n, a \in \mathbb{Z}$. This means that the vector defined by $\xi = (a_1, \ldots, a_n)$ is a character on G by lemma 5. Therefore $a_i = 0$ for all i, and $a = 0$, so rewriting the equation as $a_1x_1 + \ldots + a_nx_n - a = 0$ we see that $\{1, x_1, \ldots, x_n\}$ are $\mathbb{Q}$-linearly independent. This proves one direction.

Now suppose we have the converse: given that $\{1, x_1, \ldots, x_n\}$ are $\mathbb{Q}$-linearly independent, is any arbitrary $b \in \mathbb{R}^n$ actually in $\overline{G}$? Equivalently, by proposition 6 we can ask is $b \in (G^\star)^\star$. This is true if $b \cdot \xi \in \mathbb{Z}$ for all $\xi \in G^\star$.

Well if $\xi \in G^\star$ we know that $\xi_i \in \mathbb{Z}$ for all i and that $\xi_1x_1 + \ldots + \xi_nx_n \in \mathbb{Z}$ by lemma 5. The last equation says that

$$\xi_1x_1 + \ldots + \xi_nx_n = g \quad \text{for some } g \in \mathbb{Z}.$$

But $\{1, x_1, \ldots, x_n\}$ are linearly independent over $\mathbb{Q}$, so $\xi_1 = \ldots = \xi_n = g = 0$, so any character of G is again identically zero.

So for any arbitrary $b \in \mathbb{R}^n$, b is a character of the character group of G since for any $\xi \in G^\star$,

$$\xi \cdot b = 0 \cdot b_1 + \ldots 0 \cdot b_n = 0 \in \mathbb{Z}$$

so $b \in \overline{G}$. □

3 Density Statements

3.1 General Criterion

Back to an elliptic curve E defined over $\mathbb{Q}$, with associated lattice Λ, and let ω_1 and ω_2 be purely real and purely imaginary periods, respectively, such that they span a rectangular sub-lattice of finite index at most 2 in Λ. We can reword theorem 1 to get the following density criterion:

Theorem 2 *Let $u = s + it \in \mathbb{C}$, and let $P = \exp_E(u) \in E(\mathbb{C})$. Then the subgroup $\mathbb{Z}P$ generated by P in $E(\mathbb{C})$ is dense in $E(\mathbb{C})$ if and only if the numbers $1, \frac{s}{\omega_1}, \frac{it}{\omega_2}$ are linearly independent over $\mathbb{Q}$.*

Proof: Assume $\mathbb{Z}P$ is dense in $E(\mathbb{C})$. This means that the set $\mathbb{Z}u$ is dense in $\mathbb{C}/\Lambda$. If we scale the rectangle formed by ω_1 and ω_2 back to the unit square, u gets mapped to $u' = \frac{s}{\omega_1} + i\frac{it}{\omega_2}$, and this is the same as saying that the $\mathbb{Z}$-submodule generated by e_1, e_2, u' is everywhere dense in $\mathbb{R}^2$. Theorem 1 then gives the desired result. □

3.2 CM Case

Now assume our elliptic curve E has complex multiplication. I.e. if ω_1 and ω_2 are purely real and purely imaginary periods respectively, then $\tau = \frac{\omega_2}{\omega_1}$ is such that $\tau^2 \in \mathbb{Q}$ and the field of endomorphisms of E is $\operatorname{End}^0 E = \mathbb{Q}(\tau)$. Of course theorem 2 still applies, but we can say even more. Motivated by figures 3 and 4, and using theorem 2 we can show

Theorem 3 *Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication, and let $P \in E(\mathbb{C})$. Then $\mathbb{Z}P$ is not dense in $E(\mathbb{C})$ if and only if there is a non-zero $\lambda \in \operatorname{End}^0 E$ such that $\lambda P \in E(\mathbb{R})$.*

Proof: Let $0 \neq \lambda \in \operatorname{End}^0 E$ be such that $\lambda P \in E(\mathbb{R})$. Since $\operatorname{End}^0 E = \mathbb{Q}(\tau)$, we can write $\lambda = a + b\tau$ for non-zero $a, b \in \mathbb{Q}$. Let $u = s + it = \mathscr{L}_E(P)$. We have that λu is real or it lies on the horizontal line bisecting the fundamental parallelogram. If the latter, then $2\lambda u \in \mathbb{R}$, so we can assume that $\lambda u \in \mathbb{R}$. Writing this out we see that

$$\lambda u = (a + b\tau)(s + it) = as + bt\tau i + bs\tau + iat \in \mathbb{R}.$$

Therefore the imaginary part is 0, and dividing by ω_2 we get

$$b\frac{s}{\omega_1} + a\frac{it}{\omega_2} = 0$$

for non-zero $a, b \in \mathbb{Q}$, so by theorem 2, $\mathbb{Z}P$ is not dense.

Conversely suppose $\mathbb{Z}P$ is not dense. Then we know again by theorem 2 that we have a linear relation

$$a\omega_1\omega_2 + bs\omega_2 + ict\omega_1 = 0 \tag{7}$$

with $a, b, c \in \mathbb{Q}$ not all zero. Let $\lambda_0 = c + b\tau \in \mathrm{End}^0 E$. Then we have

$$\begin{aligned} \lambda_0 u = (c + b\tau)(s + it) &= cs + ibt\tau + bs\tau + ict \\ &= q - a\omega_2 \qquad \in \mathbb{R} + \mathbb{Q}L \end{aligned}$$

using (7), and for $q = cs + ibt\tau \in \mathbb{R}$. Hence if $a = \dfrac{a_1}{a_2}$, we have that $a_2\lambda_0 u \in \mathbb{R} + L$, which means that $a_2\lambda_0 P \in E(\mathbb{R})$. $\square$

The second part of this proof still holds if $\lambda_0 = c \in \mathbb{Z}$, so it includes the non-CM case in one direction.

4 Schneider's Theorem

4.1 The Main Theorem

A meromorphic function $f(z)$ is said to have finite order if there exists $\rho > 0$ and we can write $f = \dfrac{g}{h}$, where g and h are entire functions such that, for any $R \geq 2$, and for all z with $|z| \leq R$, we have

$$\max(|g(z)|, |h(z)|) < \exp(R^\rho) \tag{8}$$

The ring $K[f_1, \ldots, f_n]$ is the ring of polynomials in $f_1, \ldots, f_n$ with coefficients in K, and the transcendence degree is the maximum number of elements in an algebraically independent subset. By a number field K we mean an algebraic extension of finite degree over $\mathbb{Q}$.

Theorem 4 *Let K be a number field and let $f_1, \ldots, f_n$ be meromorphic functions of finite order. Suppose that the ring $K[f_1, \ldots, f_n]$ is mapped into itself by differentiation and has transcendence degree at least 2 over K. Then there are only finitely many numbers z at which $f_1, \ldots, f_n$ simultaneously assume values in K.*

Corollary 1 (Schneider) *If g_2 and g_3 are algebraic, then for any algebraic $\alpha \neq 0$, $\wp(\alpha)$ is transcendental.*

Proof: The functions

$$f_1(z) = \wp(\alpha z), \quad f_2(z) = \wp'(\alpha z), \quad f_3(z) = z$$

satisfy the requirements of theorem 4. Suppose that $\wp(\alpha)$ is algebraic. Then for infinitely many integral values of z, the three functions above would simultaneously assume values in the number field generated by $g_2, g_3, \alpha, \wp(\alpha)$, and $\wp'(\alpha)$ over $\mathbb{Q}$, contrary to theorem 4. $\square$

This statement is an analogue to the Gelfond-Schneider Theorem which states that for $\alpha, \beta \in \overline{\mathbb{Q}}$ with $\alpha \neq 0, 1$, and $\beta \notin \mathbb{Q}$, we have that α^β is transcendental.

The proof of theorem 4 is outlined in the following sections. It can be found in complete detail in [1] chapter 6.

4.2 Dirichlet's Box Principle

Lemma 6 *Let $N > M > 0$ be integers, and let u_{ij} be integers such that $|u_{ij}| \leq U$, for $1 \leq i \leq M$, $1 \leq j \leq N$, and some $U \geq 1$. Then there are integers $x_1, \ldots, x_N$ not all zero, with $|x_j| \leq (NU)^{M/(N-M)}$, such that*

$$\sum_{j=1}^{N} u_{ij} x_j = 0 \qquad \text{for } 1 \leq i \leq M. \tag{9}$$

Proof: Let $B = \left[(NU)^{M/(N-M)}\right]$, where $[x]$ denotes the integral part of x. There are $(B+1)^N$ different sets $\{x_1, \ldots, x_N\}$ with

$$0 \leq x_j \leq B \qquad \text{for } 1 \leq j \leq N,$$

and for each such set let

$$y_i = \sum_{j=1}^{N} u_{ij} x_j \in \mathbb{Z}, \qquad \text{for } 1 \leq i \leq M.$$

For any i, let $-V_i$ and W_i denote the sum of the negative and positive parts of u_{ij} for all j, respectively. Since

$$-V_i B \leq y_i \leq W_i B,$$

and $V_i + W_i \leq NU$, which means that $V_i B + W_i B \leq NUB$, we see that there are at most $(NUB+1)^M$ different sets $\{y_1, \ldots, y_M\}$ in $\mathbb{Z}$.

Now we have

$$\begin{aligned} (B+1)^{N-M} &= \left(\left[(NU)^{M/(N-M)}\right] + 1\right)^{N-M} \\ &= (NU)^M + \text{positive terms} \end{aligned}$$

which implies that $(B+1)^{N-M} > (NU)^M$, therefore

$$\begin{aligned} (B+1)^N &= (B+1)^{N-M}(B+1)^M \\ &> (NU)^M (B+1)^M \\ &= (NUB + NU)^M \\ &> (NUB+1)^M \end{aligned}$$

since $NU > 0$.

So two distinct sets $x_1, \ldots, x_N$ and $x'_1, \ldots, x'_N$ correspond to the same set $y_1, \ldots, y_M$, and so the set $x_1 - x'_1, \ldots, x_N - x'_N$ is a solution of (9), since

$$\sum_{j=1}^{N} u_{ij}(x_j - x'_j) = \sum_{j=1}^{N} u_{ij}x_j - \sum_{j=1}^{N} u_{ij}x'_j = y_i - y_i = 0 \qquad \forall i.$$

□

Now let K be an algebraic number field, and let c_1, c_2, c_3 denote positive numbers that will depend only on K. For any α in K, let $\|\alpha\|$ denote the size of α, that is, the maximum of the absolute values of the conjugates of α.

Lemma 7 *Let $N > M > 0$ be rational integers, and let u_{ij} be algebraic integers in K such that $\|u_{ij}\| \leq U$, for $1 \leq i \leq M$, $1 \leq j \leq N$, and some $U \geq 1$. Then there are algebraic integers $x_1, \ldots, x_N$ in K not all zero, with $\|x_j\| < c_1(c_1NU)^{M/(N-M)}$, such that*

$$\sum_{j=1}^{N} u_{ij}x_j = 0 \qquad \text{for } 1 \leq i \leq M. \tag{10}$$

Proof: Let $\omega_1, \ldots, \omega_n$ be an integral basis of K. For any i, j, and k, the number $u_{ij}\omega_k$ can be expressed as

$$u_{ij}\omega_k = \sum_{h=1}^{n} u_{hijk}\omega h$$

for some u_{hijk} in $\mathbb{Z}$. From these equations, we can write the u_{hijk} in terms of the u_{ij}, with coefficients only depending of K, so $|u_{hijk}| < c_2U$. Lemma 6 says that the system of equations

$$\sum_{j=1}^{N} \sum_{k=1}^{n} u_{hijk}x_{jk} = 0 \qquad \text{for } 1 \leq k \leq n, 1 \leq i \leq M$$

has a non-trivial solution with $|x_{jk}| < (c_3NU)^{M/(N-M)}$. A solution to (10) is now given by

$$x_j = \sum_{k=1}^{n} x_{jk}\omega_k \qquad \text{for } 1 \leq j \leq N$$

since

$$\begin{aligned}
\sum_{j=1}^{N} u_{ij} x_j &= \sum_{j=1}^{N} u_{ij} \left(\sum_{k=1}^{n} x_{jk} w_k \right) \\
&= \sum_{j=1}^{N} \sum_{k=1}^{n} (u_{ij} \omega_k)\, x_{jk} \\
&= \sum_{j=1}^{N} \sum_{k=1}^{n} \left(\sum_{h=1}^{n} u_{hijk} \omega_h \right) x_{jk} \\
&= \sum_{h=1}^{n} \left(\sum_{j=1}^{N} \sum_{k=1}^{n} u_{hijk} x_{jk} \right) \omega_h \\
&= \sum_{h=1}^{n} 0 \cdot \omega_h = 0
\end{aligned}$$

□

4.3 The Auxiliary Function

Now assume that all the hypotheses of Theorem 4 are satisfied, and write $f_i = \frac{g_i}{h_i}$, where g_i and h_i are entire functions such that (8) holds. Suppose that the conclusion of the theorem is false, so that there is an infinite sequence of distinct complex numbers $y_1, y_2, \ldots$ such that $f_i(y_j)$ is in K for all i and j.

Let $c_4, c_5, \ldots$ denote positive numbers which will depend only on the quantities defined so far, let m be an integer that exceeds a sufficiently large c_4, and let k be an integer that is sufficiently large compared to m. For convenience, let $L = [k^{3/4}]$, and let $f^{(j)}$ denote the j-th derivative of f.

We build a nice auxiliary function Φ from any two of the functions in question, say f_1 and f_2, in hopes to show that it and all its derivatives vanish at the points $y_1, y_2, \ldots$.

Lemma 8 *There are algebraic integers $p(\lambda_1, \lambda_2)$ in K, not all zero, with sizes at most $k^{c_5 k}$, such that the function*

$$\Phi(z) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2) f_1(z)^{\lambda_1} f_2(z)^{\lambda_2}$$

satisfies

$$\Phi^{(j)}(y_l) = 0 \qquad \text{for} \quad 0 \le j \le k,\ 1 \le l \le m.$$

Proof: The number $\Phi^{(j)}(y_l)$ can be written as

$$\Phi^{(j)}(y_l) = \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p(\lambda_1, \lambda_2)\Big[f_1(y_l)^{\lambda_1} f_2(y_l)^{\lambda_2}\Big]^{(j)}, \tag{11}$$

which is a linear form in the $p(\lambda_1, \lambda_2)$. Since the derivatives of $f_1, \dots, f_n$ are again elements of $K[f_1, \dots, f_n]$ by hypothesis, the coefficients of the $p(\lambda_1, \lambda_2)$ in (11) are given by polynomials in $f_1(y_l), \dots, f_n(y_l)$, and thus belong to K. Multiplying by some positive integer, these coefficients become algebraic integers, and suppose their size is at most U.

So considering $\Phi^{(j)}(y_l) = 0$ for $0 \le j \le k$ and $1 \le l \le m$, we have $M = m(k+1)$ equations in $N = (L+1)^2$ variables. But since

$$N = (L+1)^2 = \left([k^{3/4}]+1\right)^2 > \left(k^{3/4}\right)^2 = k^{3/2},$$

and for k sufficitently large, $k^{3/2} > 2m(k+1)$, we have that $N > 2M$. So by Lemma 7, there is a non-trivial solution. And since

$$\frac{M}{N-M} < \frac{M}{2M-M} = 1,$$

we have that $(NU)^{M/(N-M)} < NU$, so the sizes of the $p(\lambda_1, \lambda_2)$ are at most $c_1^2 NU$. It can be shown that we can take $U \le k^{c_6 k}$

□

Lemma 9 *For and $R \ge 2$ and for all z with $|z| \le R$, the function $\phi = (h_1 \cdots h_n)^L \cdot \Phi$ satisfies*

$$|\phi(z)| < \exp\{c_{11}(k \log k + LR^\rho)\}.$$

Further, for any j, l with $j \ge k, l \le m$ such that $\Phi^{(i)}(y_l) = 0$ for all $i < j$, the number $\phi^{(j)}(y_l)$ either vanishes or has absolute value at least $j^{-c_{12} j}$.

4.4 Proof of Theorem 4

First we show that Φ and all its derivatives vanish at the points $y_1, \dots, y_m$. Using induction on j, assume that

$$\Phi^{(i)}(y_l) = 0 \qquad \text{for } \ 0 \le i < j, \ 1 \le l \le m$$

and show that the same is true for $i = j$. We can assume that $j > k$, as seen in Lemma 8.

Now let C be the contour of circle in the positive orientation in the complex plane, with center the origin, and radius $R = j^{1/(4\rho)}$, let

$$F(z) = (z - y_1)\cdots(z - y_m),$$

and let l be any integer with $1 \leq l \leq m$. We integrate the function

$$f(z) = \frac{\phi(z)}{(z - y_l)(F(z))^j}$$

over C using the Cauchy residue theorem.

The only pole of $f(z)$ inside C is y_l, and it is a simple pole. Its residue there is equal to

$$\operatorname{Res}(f, y_l) = \lim_{z \to y_l} f(z)(z - y_l).$$

By the induction hypothesis, we know that $\phi(z)$ has a zero of order at least j at y_l, so we can write

$$\phi(z) = (z - y_l)^j a(z)$$

for some $a(z)$. Differentiating and evaluating at y_l we obtain

$$\phi^{(j)}(y_l) = j!\, a(y_l).$$

Therefore,

$$\lim_{z \to y_l} f(z)(z - y_l) = \lim_{z \to y_l} \frac{(z - y_l)^{j+1} a(z)}{(z - y_l)(F(z))^j} = \frac{\phi^{(j)}(y_l)}{j!(F'(y_l))^j}.$$

In other words,

$$\frac{\phi^{(j)}(y_l)}{(F'(y_l))^j} = \frac{j!}{2\pi i} \int_C \frac{\phi(z)\, dz}{(z - y_l)(F(z))^j}$$

To finish the proof, we show that

$$|\phi^{(j)}(y_l)| \leq j^{c_{15} j - jm/(8\rho)}.$$

But if we take m big enough, say $m > 8\rho(c_{12} + c_{15})$, then by lemma 9, $\phi^{(j)}(y_l) = 0$, and therefore $\Phi^{(j)}(y_l) = 0$ assuming that $h_1 \cdots h_n$ does not vanish at y_l, which we can. Therefore by induction, Φ and all its derivatives vanish at $y_1, \ldots, y_m$.

This implies that the functions f_1 and f_2 are algebraically dependent, and since we can construct the auxiliary function from any two functions from $f_1, \ldots, f_n$, this shows that $K[f_1, \ldots, f_n]$ has transcendence degree at most 1. This contradicts the hypothesis of theorem 4, therefore there are only finitely many complex numbers $y_1, \ldots, y_m$ such that $f_i(y_j) \in K$ for all i, j.

5 Elliptic Curves over $\overline{\mathbb{Q}} \cap \mathbb{R}$

Let E be an elliptic curve defined over $\overline{\mathbb{Q}} \cap \mathbb{R}$, the field of real algebraic numbers. We state below an alternate form of Kronecker's theorem. In this statement, the $\mathbb{Z}$-submodule G is generated by $l+1$ arbitrary elements in $\mathbb{R}^n$, not the standard basis plus another point.

Theorem 5 (Kronecker) *Let G be a $\mathbb{Z}$-submodule of $\mathbb{R}^n$ generated by $g_1, g_2, \ldots, g_l$. For $1 \leq j \leq l$, write g_j in terms of the standard basis of $\mathbb{R}^n$:*

$$g_j = (g_{1j}, \ldots, g_{nj}).$$

Then G is dense in $\mathbb{R}^n$ if and only if for all non-zero $(s_1, \ldots, s_l) \in \mathbb{Z}^l$, the matrix

$$\begin{pmatrix} g_{11} & \cdots & g_{1l} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{nl} \\ s_1 & \cdots & s_l \end{pmatrix}$$

has rank $n+1$.

Let $E^+(\mathbb{C}) = E(\mathbb{R})$, and by $E^-(\mathbb{C})$ we mean the set of points on $P = (x, y) \in E(\mathbb{C})$ such that x is real and y is purely imaginary. In other words, $E^+(\mathbb{C})$ is the set of points $P \in E(\mathbb{C})$ such that $P = \overline{P}$, and $E^-(\mathbb{C})$ is the set of points $P \in E(\mathbb{C})$ such that $P = -\overline{P}$.

Now suppose we have three algebraic points on the curve E. If no integral linear combination of these points is purely real or purely imaginary, then theorem 5 implies that the subgroup generated by these points is dense in $E(\mathbb{C})$:

Theorem 6 *Let E be an elliptic curve defined over $\overline{\mathbb{Q}} \cap \mathbb{R}$ without complex multiplication. Let P_1, P_2, P_3 be three algebraic points on E. Assume that for any non-zero $(m_1, m_2, m_3) \in \mathbb{Z}^3$ we have $m_1P_1 + m_2P_2 + m_3P_3 \notin E^+(\mathbb{C}) \cup E^-(\mathbb{C})$. Then the subgroup generated by P_1, P_2, P_3 is dense in $E(\mathbb{C})$.*

As an immediate corollary we obtain:

Corollary 2 *Let E be an elliptic curve defined over $\overline{\mathbb{Q}} \cap \mathbb{R}$ without complex multiplication. Let P_1, P_2, P_3 be three points on E such that for any non-zero $(m_1, m_2, m_3) \in \mathbb{Z}^3$ we have $m_1P_1 + m_2P_2 + m_3P_3 \notin E^+(\mathbb{C}) \cup E^-(\mathbb{C})$. Assume that the subgroup generated by P_1, P_2, P_3 in $E(\mathbb{C})$ is not dense in $E(\mathbb{C})$. Then at least one of P_1, P_2, P_3 is a transcendental point on E.*

This statement would be an analogue to the six exponentials theorem, which can be stated as follows:

Theorem 7 *Let $\{x_1, x_2\}$ and $\{y_1, y_2, y_3\}$ be two sets of complex numbers, each of which is $\mathbb{Q}$-linearly independent. Then at least one of the six numbers*

$$e^{x_i y_j} \qquad i = 1, 2, \;\; j = 1, 2, 3$$

is transcendental.

6 Pari/GP Code

The file `gp/plotmultiples.gp` contains the function definitions used by the script below.

```
--------------------------------------------------------------------------------
/*
File: gp/plotmultiples.gp
*/

/*
Returns a plot of the n first multiples of P on the curve E.
If ps=1, outputs the plot to the default psfile.
*/
ellplotmultiples(E,P,n,{view=[0,1,0,1]},{ps=0}) =
{
  local(dots);
  dots = ellgetmultiples(E,P,n,view);
  if(ps, \
    psplothraw(dots[1],dots[2]) \
  , \
    plothraw(dots[1],dots[2]) \
  );
}

ellgetmultiples(E,P,n,view) =
{
  local(area,N,x,y,a,b,z);
  area = (view[2]-view[1])*(view[4]-view[3]);
  N = floor((1.05)*n*area);
  x = listcreate(N);
  y = listcreate(N);
  a = kEtoCL(E,P);
  for(i=1,n, \
    b = modZ2(i*a); \
    if(inView(b,view), \
      z = b[1]*E.omega[1] + b[2]*E.omega[2]; \
      listput(x,real(z)); \
      listput(y,imag(z)); \
    ); \
  );
```

```
  return([Vec(x),Vec(y)]);
}

/*
Takes a point P on E, and returns the point z in C mod Z^2
corresponding to P.
*/
kEtoCL(E,P) =
{
  local(z_0,x_0,y_0,z,x,y);
  z_0 = ellpointtoz(E,P);
  x_0 = real(z_0);
  y_0 = imag(z_0);
  x = (x_0-y_0*real(E.omega[2])/imag(E.omega[2]))/E.omega[1];
  y = y_0/imag(E.omega[2]);
  z = x+I*y;
}

modZ2(z) = [frac(real(z)),frac(imag(z))];

inView(z,view) = \
  ( z[1]>=view[1] && z[1]<=view[2] && z[2]>=view[3] && z[2]<=view[4] );
--------------------------------------------------------------------------------
```

The script used to generate the images in section 1.4 is the following:

```
--------------------------------------------------------------------------------
\p 150;
read("gp/plotmultiples.gp");

e1 = ellinit([0,0,0,-1,0]);

w = e1.omega;

z1 = 3*w[1]/7 + 5*w[2]/9;
p1 = ellztopoint(e1,z1);
default(psfile,"ps/z1.ps");
ellplotmultiples(e1,p1,100,1);

z2 = (w[1]/3)/(2+5*I);
p2 = ellztopoint(e1,z2);
default(psfile,"ps/z2.ps");
ellplotmultiples(e1,p2,1000,1);

z3 = (sqrt(2)*w[1])/(2+5*I);
p3 = ellztopoint(e1,z3);
default(psfile,"ps/z3.ps");
ellplotmultiples(e1,p3,10000,1);

z4 = sqrt(2)*w[1] + sqrt(3)*w[2];
p4 = ellztopoint(e1,z4);
default(psfile,"ps/z4.ps");
ellplotmultiples(e1,p4,100000,1);
--------------------------------------------------------------------------------
```

References

[1] A. BAKER – "Transcendental Number Theory", Cambridge University Press, 1975.

[2] M. BERTOLA – "Topics in Complex Analysis", `http://www.mathstat.concordia.ca/faculty/bertola/ComplexAnalysis/ComplexAnalysis.pdf`, 2005.

[3] H. KISILEVSKY – "Ranks of elliptic curves in cubic extensions", submitted as a contributed article to a special volume in honour of Serge Lang.

[4] C. SIEGEL – "Lectures on the Geometry of Numbers", Springer-Verlag, 1989.

[5] J. SILVERMAN – "The Arithmetic of Elliptic Curves", Springer-Verlag, 1986.

[6] J. SILVERMAN, J. TATE – "Rational Points on Elliptic Curves", Springer-Verlag, 1992.

[7] M. WALDSCHMIDT – "Densité des points rationnels sur un groupe algébrique", Experimental Mathematics. Volume 3, Issue 4, 1994, pp 329-352.

[8] M. WALDSCHMIDT – "On a question of Hershy Kisilevsky", manuscript.

[9] M. WALDSCHMIDT – "Topologie des Points Rationnels," `http://www.institut.math.jussieu.fr/~miw/articles/pdf/TPR.pdf`, 1998.