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

© Sylvain Muise, 2007
NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.
ABSTRACT

Density on Elliptic Curves

Sylvain Muisê

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 v

1 Introduction 1
   1.1 Elliptic Curves ...................................... 1
   1.2 Elliptic Functions .................................. 4
   1.3 The Question ......................................... 7
   1.4 Experimental Data ................................... 8

2 Kronecker’s Theorem 10
   2.1 Definitions .......................................... 10
   2.2 Discrete Submodules ................................ 11
   2.3 Non-discrete Submodules ............................. 13
   2.4 Characters ............................................ 15
   2.5 Character Groups .................................... 16
   2.6 Kronecker’s theorem ................................ 17

3 Density Statements 18
   3.1 General Criterion .................................... 18
   3.2 CM Case ............................................... 19

4 Schneider’s Theorem 20
   4.1 The Main Theorem .................................... 20
   4.2 Dirichlet’s Box Principle ............................ 21
   4.3 The Auxiliary Function .............................. 23
   4.4 Proof of Theorem 4 ................................ 24

5 Elliptic Curves over \( \mathbb{Q} \cap \mathbb{R} \) 26

6 Pari/GP Code 27
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Addition of points on an elliptic curve</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>100 multiples of $z_1$</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>1000 multiples of $z_2$</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>10,000 multiples of $z_3$</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>100,000 multiples of $z_4$</td>
<td>10</td>
</tr>
</tbody>
</table>
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

$$E : y^2 = x^3 + ax + b,$$  \hspace{1cm} (1)

with $a, b \in K$.

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

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

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 structure 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](image)

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 formulas for the sum of two points of \( E \) and the inverse of a point are given in terms of the coefficients 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

\[
\lambda = \frac{3x_1^2 + a}{2y_1} \quad \text{and} \quad \nu = \frac{-x_1^3 + ax_1 + 2b}{2y_1}.
\]
Otherwise, if \( P_1 \neq P_2 \), let
\[
\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.
\]
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:
\[
+ : E \times E \to E \quad \text{and} \quad - : E \to E \quad \begin{array}{ll}
(P_1, P_2) & \mapsto P_1 + P_2 \\
P & \mapsto -P.
\end{array}
\]

An isogeny between two curves \( E_1 \) and \( E_2 \) is a morphism \( \phi : E_1 \to E_2 \) that satisfies \( \phi(O) = O \). For an integer \( m \), we have that the multiplication by \( m \) map given by
\[
[m] : E \to E \\
P & \mapsto P + P + P \cdots + P \quad (m \text{ terms}) \quad \text{if } m > 0 \\
P & \mapsto [-m][-P] \quad \text{if } m < 0 \\
O & \mapsto O
\]
is an isogeny from \( E \) to itself. The ring of all isogenies from \( E \) to itself is denoted by \( \text{End}(E) \) and is called the endomorphism ring of \( E \). The ring structure is given by pointwise addition and composition:
\[
(\phi + \psi)(P) = \phi(P) + \psi(P) \\
(\phi \psi)(P) = \phi(\psi(P))
\]
We have that for any integer \( m \), the map \([m]\) is in \( \text{End}(E) \), so we can say that \( \mathbb{Z} \subset \text{End}(E) \). If there is equality, there are no more maps to study on \( E \). Otherwise, if
\[
\mathbb{Z} \not\supset \text{End}(E),
\]
we say that \( E \) has complex multiplications. It can be shown that for any elliptic curve \( E \), the endomorphism ring \( \text{End}(E) \) 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 over \( \mathbb{C} \), it is either \( \mathbb{Z} \) or an order in a quadratic imaginary field. So in this case, we can form the field of fractions of \( \text{End}(E) \), denoted by \( \text{End}^0(E) \), 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 $\Lambda$ is a meromorphic function $f(z)$ on $\mathbb{C}$ such that

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

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

A fundamental parallelogram for $\Lambda$ is a set of the form

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

where $a \in \mathbb{C}$ and $\omega_1, \omega_2$ are a basis for $\Lambda$.

The Weierstrass $\wp$-function (relative to $\Lambda$) 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 $0 \leq k \in \mathbb{Z}$, the Eisenstein series of weight $2k$ (relative to $\Lambda$) is defined by

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

When the lattice $\Lambda$ 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 $\Lambda$, we could show that

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z)).$$
i.e. that every elliptic function is a rational combination of \( \varphi \) and \( \varphi' \).

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

\[
\varphi'(z)^2 = 4\varphi(z)^3 - g_2\varphi(z) - g_3.
\]

If \( g_2 \) and \( g_3 \) are the quantities associated to a lattice \( \Lambda \subset \mathbb{C} \), then it can 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** (Uniformization 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 \( \Lambda_1 \) and \( \Lambda_2 \). 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. \( \Lambda_1 \) and \( \Lambda_1 \) 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:

\[
\exp_E : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})
\]

\[
z \mapsto (x, y) = (\varphi(z), \varphi'(z)), \quad \text{if} \ z \notin \Lambda
\]

\[
\omega \mapsto O
\]

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

\[
\mathcal{L}_E : E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda.
\]
It is given by

$$\mathcal{L}_E(P) = \int_0^P \frac{dx}{y} \mod \Lambda.$$  

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 Eisenstein series above. The fact that $E$ is defined over $\mathbb{R}$ means that $g_2(\Lambda), g_3(\Lambda) \in \mathbb{R}$.

We have

$$g_2(\overline{\Lambda}) = 60 \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^4} = 60 \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\overline{\omega}^4} = g_2(\Lambda)$$

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 $\Lambda = \overline{\Lambda}$. \(\square\)

Let $E$ be defined over $\mathbb{R}$ with associated lattice $\Lambda \subset \mathbb{C}$. Lemma 1 tells us that if $\omega$ is in $\Lambda$, its conjugate $\overline{\omega}$ is also in $\Lambda$. Therefore $\omega + \overline{\omega}$, which is real, is in $\Lambda$. So there exists a purely real period in $\Lambda$. Let $\omega_1$ be the smallest such real period, which exists since $\Lambda$ is a lattice (discussed in section 2.2).

Let $\omega_2 \not\in \mathbb{R}$ be such that $\{\omega_1, \omega_2\}$ is a basis for $\Lambda$. We know that $\omega_2 + \overline{\omega_2}$ is in $\Lambda$, 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, $\omega_2$ is purely imaginary, which results in a rectangular lattice. In the second case we see that

$$\omega_2 + \overline{\omega_2} = \omega_1 \quad \Rightarrow \quad 2\Re(\omega_2) = \omega_1$$

$$\Rightarrow \quad \Re(\omega_2) = \frac{1}{2} \omega_1,$$

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 \( \Lambda \) is either a rectangular lattice with \( \Re(\omega_2) = 0 \), or a diamond lattice with \( \Re(\omega_2) = \frac{1}{2} \omega_1 \).

In either case, we can choose a pair of periods \( \omega_1 \) and \( \omega_2 \), such that \( \omega_1 \) is purely real and \( \omega_2 \) is purely imaginary, that generate a sub-lattice of \( \Lambda \) of index at most 2.

1.3 The Question

Let \( E \) be an elliptic curve defined over \( \mathbb{Q} \), and let \( \Lambda \) 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 \( x = \bar{x} \). Let \( z = \mathcal{L}_E(P) \). By the definition of \( \exp_E \), we have

\[
\varphi(z) = \varphi(\bar{x}).
\]

Since \( \varphi \) is a doubly periodic function with respect to \( \Lambda \), this means that

\[
z \equiv \bar{x} \mod \Lambda.
\]

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

If \( \Lambda \) 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 \( \bar{z} \) is not in the same one. Therefore if \( z \notin \mathbb{R} \), then \( z \not\equiv \bar{z} \mod \Lambda \). In this case, \( \exp_E(\mathbb{R}) = E(\mathbb{R}) \). This corresponds to a one component real locus.

Otherwise if \( \Lambda \) is a rectangular lattice, then we may have \( z - \bar{z} = \omega_2 \), 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 \( E^-(\mathbb{C}) = \{P \in E(\mathbb{C}) \mid P = -\bar{P}\} \). 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 \( \lambda \in \text{End}(E) \) 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 $z = L_{E}(P)$ in $\mathbb{C}/\Lambda$, and we can rephrase the conjecture to say, if there is no $\lambda \in \text{End}(E)$ such that $\lambda z$ 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 $[i]: (x, y) \mapsto (-x, iy)$, and we know that $\text{End}^0(E) = \mathbb{Q}(i)$. The lattice $\Lambda$ associated to this curve is a square lattice: let $\omega_1, \omega_2$ be a basis for $\Lambda$ with $\omega_1$ purely real and $\omega_2$ purely imaginary and $|\omega_1| = |\omega_2|$. A non-zero element $\lambda = (a + bi) \in \text{End}^0(E)$ 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 $z_2 = \frac{\omega_1/3}{2 + 5i}$, 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 $z_1 = \frac{3}{7} \omega_1 + \frac{5}{9} \omega_2$
Now let \( z_3 = \frac{\sqrt{2}\omega_1}{2 + 5i} \), 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 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 \( \omega_1, \omega_2 \), are linearly independent over \( \mathbb{Q} \). Is this
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 \( \epsilon \) 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

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

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 $\epsilon$ 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 $\epsilon$ 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 $G \cong \mathbb{Z}^r$.

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 $G = \mathbb{Z}x_1 \oplus \ldots \oplus \mathbb{Z}x_r \cong \mathbb{Z}^r$.

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 $L = M \cap G$:

$$M = \{\lambda_1 y_1 + \ldots + \lambda_k y_k, \lambda_i \in \mathbb{R}\}$$

$$L = M \cap G.$$

We can always write elements in $M$ with respect to its basis $B = \{y_1, \ldots, y_k\}$. So if we have $x = (\lambda_1, \ldots, \lambda_k)_B \in M$ 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:

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

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

Let $\pi_i : L' \rightarrow \mathbb{R}$ 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 $\lambda_i$. 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 $\mu_i$'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 \( \nu_i \)'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 \( \nu_i \)'s are integers. Let \( \nu_k \) 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 \( \nu_i \)'s are integers, and \( G \vartriangleleft \mathbb{Z}^r \) is a lattice. \( \Box \)

### 2.3 Non-discrete Submodules

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

For \( \epsilon \) 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 \( E \):

\[
E = \{ x \in \mathbb{R}^n \mid x = \lambda_1 y_1 + \ldots + \lambda_s y_s, \ \lambda_i \in \mathbb{R} \}
\]

\[
D = E \cap G.
\]

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 \(\delta/s\). We can always choose \(\delta\) small enough so that \(r(\delta/s) = s\). We can express \(\overline{y}\) in terms of this basis of \(E\):

\[
\overline{y} = \sum_{i=1}^{s} \lambda_i y_i, \quad \lambda_i \in \mathbb{R}
\]

(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

\[
\overline{y} = \sum_{i=1}^{s} g_i y_i + \sum_{i=1}^{s} r_i y_i
\]

\[
= y + \sum_{i=1}^{s} r_i y_i
\]

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 \(\overline{D} = E\). \(\square\)

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 \(L \cong \mathbb{Z}^{r-s}\) by Proposition 3. \(\square\)

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 \(\lambda_i\)'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 $\chi : \mathbb{R}^n \rightarrow \mathbb{R}$ satisfying

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

(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 $\chi$ is a linear function on $G$, and for $x = (x_1, \ldots, x_n)$,

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

We can then think of $\chi$ as follows:

$$\chi : \mathbb{R}^n \rightarrow \mathbb{R}$$

$$x \mapsto x \cdot \xi$$

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

Let $B = \{y_1, \ldots, y_s, z_1, \ldots, z_q, t_1, \ldots, t_{n-r}\}$ 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 $B$ looks like

$$x = (\lambda_1, \ldots, \lambda_s, \mu_1, \ldots, \mu_q, \nu_1, \ldots, \nu_{n-r})_B, \; \lambda_i, \mu_j, \nu_k \in \mathbb{R}$$

(5)

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

Let $\chi$ be determined by

$$\xi = (a_1, \ldots, a_s, b_1, \ldots, b_q, c_1, \ldots, c_{n-r})_B.$$  

(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 $\chi$ 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 $1 \leq j \leq q$. 

15
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 $\mu_j$’s and the $b_j$’s are integers, so $\chi$ is a character of $G$.

Now suppose $\chi$ 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 $x = (\lambda_1, \ldots, \lambda_s, 0, \ldots, 0, 0, \ldots, 0)_B$. When restricted to $D$, $\chi$ is a continuous integer-valued function on a dense subset of a vector space. So $\chi$ 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 $z_1 = (0, \ldots, 0, 1, \ldots, 0, 0, \ldots, 0)_B$ we have

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

but $z_1 \in G$. So $\chi$ is not a character of $G$. □

### 2.5 Character Groups

Let $G^*$ be the set of vectors in $\mathbb{R}^n$ that determine a character on $G$. Then $G^*$ is a $\mathbb{Z}$-submodule of $\mathbb{R}^n$ since for $\xi_1, \xi_2 \in G^*$, $a \in \mathbb{Z}$, 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 $\xi_1$ and $\xi_2$ determine characters on $G$. So $\xi_1 + a\xi_2 \in G^*$. We call $G^*$ the character group of $G$.

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

**Proof:** Suppose $\{\xi_n\}_{n=1}^{\infty}$ is a sequence of elements of $G^*$ 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 $\xi \in G^*$. □

We can now prove a duality theorem for these characters:
Proposition 6 \((G^*)^* = \overline{G}\). In words, the character group of the character group of \(G\) is the closure of \(G\).

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

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 \(x \not\in \overline{G}\). Then either \(\mu_i \not\in \mathbb{Z}\) for some \(i\), or \(\nu_i \neq 0\) for some \(i\). In either case, \(x\) cannot be in \((G^*)^*\).

Suppose \(\mu_1 \not\in \mathbb{Z}\), and let \(\xi \in G^*\) with \(b_1 = 1\) and every other coordinate equal 0 in the representation for \(\xi\) given in (6). Then

\[x \cdot \xi = \mu_1 \cdot 1 \not\in \mathbb{Z}\]

so \(x \not\in (G^*)^*\).

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

\[x \cdot \xi = \nu_1 \cdot \frac{1}{2
\nu_1} = \frac{1}{2} \not\in \mathbb{Z}\]

so \(x \not\in (G^*)^*\), and we have that \((G^*)^* \subset \overline{G}\). Therefore \((G^*)^* = \overline{G}\). \(\square\)

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 \(\xi\) 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 \(x = a_1 e_1 + \ldots + a_n e_n + a_{n+1} P = (a_1 + a_{n+1} x_1) \ldots (a_n + a_{n+1} x_n)\) 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

\[
  x \cdot \xi = (a_1 + a_{n+1} x_1) \xi_1 + \ldots + (a_n + a_{n+1} x_n) \xi_n \\
  = a_1 \xi_1 + \ldots + a_n \xi_n + a_{n+1} (x_1 \xi_1 + \ldots + x_n \xi_n) \in \mathbb{Z}
\]

by assumption on the \( \xi_i \)'s, and therefore \( \xi \) is a character of \( G \). \( \square \)

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, \( \chi \) is identically zero on all of \( \mathbb{R}^n \), for each \( \chi \in G^* \).

Suppose we have \( a_1 x_1 + \ldots + a_n x_n = a \) 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 \( a_1 x_1 + \ldots + a_n x_n - a = 0 \) 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 \( b \in (G^*)^* \). This is true if \( b \cdot \xi \in \mathbb{Z} \) for all \( \xi \in G^* \).

Well if \( \xi \in G^* \) we know that \( \xi_i \in \mathbb{Z} \) for all \( i \) and that \( \xi_1 x_1 + \ldots + \xi_n x_n \in \mathbb{Z} \) by lemma 5. The last equation says that

\[
  \xi_1 x_1 + \ldots + \xi_n x_n = g \quad \text{for some } g \in \mathbb{Z}.
\]

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 \( \xi \in G^* \),

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

so \( b \in \overline{G} \). \( \square \)

### 3 Density Statements

#### 3.1 General Criterion

Back to an elliptic curve \( E \) defined over \( \mathbb{Q} \), with associated lattice \( \Lambda \), and let \( \omega_1 \) and \( \omega_2 \) be purely real and purely imaginary periods, respectively, such that they span a rectangular
sub-lattice of finite index at most 2 in $\Lambda$. 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 $zu$ is dense in $\mathbb{C}/\Lambda$. If we scale the rectangle formed by $\omega_1$ and $\omega_2$ back to the unit square, $u$ gets mapped to $u' = \frac{s}{\omega_1} + i \frac{t}{\omega_2}$, 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 $\omega_1$ and $\omega_2$ 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 $\text{End}^0 E = \mathbb{Q}(\tau)$. 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 $\lambda \in \text{End}^0 E$ such that $\lambda P \in E(\mathbb{R})$.

**Proof:** Let $0 \neq \lambda \in \text{End}^0 E$ be such that $\lambda P \in E(\mathbb{R})$. Since $\text{End}^0 E = \mathbb{Q}(\tau)$, we can write $\lambda = a + \tau b$ for non-zero $a, b \in \mathbb{Q}$. Let $u = s + it = \mathcal{L}_E(P)$. We have that $\lambda u$ 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

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

Therefore the imaginary part is 0, and dividing by $\omega_2$ 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

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

19
with $a, b, c \in \mathbb{Q}$ not all zero. Let $\lambda_0 = c + br \in \text{End}^0 E$. Then we have
\[
\lambda_0 u = (c + br)(s + it) = cs + ibt + bsr + ict = q - a\omega_2 \in \mathbb{R} + \mathbb{Q}L
\]
using (7), and for $q = cs + ibt \in \mathbb{R}$. Hence if $a = \frac{a_1}{a_2}$ we have that $a_2\lambda_0 u \in \mathbb{R} + L$, which means that $a_2\lambda_0 P \in E(\mathbb{R})$. □

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 $f = \frac{g}{h}$, where $g$ and $h$ are entire functions such that, for any $R \geq 2$, and for all $z$ with $|z| \leq R$, we have
\[
\max(|g(z)|, |h(z)|) < \exp(R^\rho)
\]
(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 $\alpha \neq 0$, $\varphi(\alpha)$ is transcendental.

Proof: The functions
\[
f_1(z) = \varphi(\alpha z), \quad f_2(z) = \varphi'(\alpha z), \quad f_3(z) = z
\]
satisfy the requirements of theorem 4. Suppose that $\varphi(\alpha)$ is algebraic. Then for infinitely many integral values of $z$, the three functions above would simultaneously assume values in the number field generated by $g_2, g_3, \alpha, \varphi(\alpha)$, and $\varphi'(\alpha)$ over $\mathbb{Q}$, contrary to theorem 4. □
This statement is an analogue to the Gelfond-Schneider Theorem which states that for \( \alpha, \beta \in \bar{\mathbb{Q}} \) with \( \alpha \neq 0,1 \), and \( \beta \notin \mathbb{Q} \), we have that \( \alpha^\beta \) 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

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

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

\[
0 \leq x_j \leq B \quad \text{for} \quad 1 \leq j \leq N,
\]

and for each such set let

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

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

\[
-V_iB \leq y_i \leq W_iB,
\]

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

Now we have

\[
(B + 1)^{N-M} = \left\lfloor (NU)^{M/(N-M)} \right\rfloor + 1 \right)^{N-M} = (NU)^M + \text{positive terms}
\]

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

\[
(B + 1)^N = (B + 1)^{N-M}(B + 1)^M > (NU)^M(B + 1)^M = (NUB + NU)^M > (NUB + 1)^M
\]
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

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

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 $\alpha$ in $K$, let $\|\alpha\|$ denote the size of $\alpha$, that is, the maximum of the absolute values of the conjugates of $\alpha$.

**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

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

**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 $|u_{hijk}| < c_2 U$. Lemma 6 says that the system of equations

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

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

$$x_j = \sum_{k=1}^{n} x_{jk}\omega_k \quad \text{for } 1 \leq j \leq N$$
since
\[
\sum_{j=1}^{N} u_{ij} x_j = \sum_{j=1}^{N} u_{ij} \left( \sum_{k=1}^{n} x_{jk} w_k \right)
\]
\[
= \sum_{j=1}^{N} \sum_{k=1}^{n} (u_{ij} w_k) x_{jk}
\]
\[
= \sum_{j=1}^{N} \sum_{k=1}^{n} \left( \sum_{h=1}^{n} u_{hijk} w_h \right) x_{jk}
\]
\[
= \sum_{h=1}^{n} \left( \sum_{j=1}^{N} \sum_{k=1}^{n} u_{hijk} x_{jk} \right) w_h
\]
\[
= \sum_{h=1}^{n} 0 \cdot w_h = 0
\]
\[
\square
\]

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 \( \Phi \) 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 \( k^{c_4 k} \), 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
\[
\Phi^{(j)}(y_l) = 0 \quad \text{for} \quad 0 \leq j \leq k, \ 1 \leq l \leq m.
\]
Proof: The number $\Phi^{(j)}(y_l)$ can be written as

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

which is a linear form in the $p(\lambda_1, \lambda_2)$. Since the derivatives of $f_1, \ldots, f_n$ are again elements of $K[f_1, \ldots, f_n]$ by hypothesis, the coefficients of the $p(\lambda_1, \lambda_2)$ in (11) are given by polynomials in $f_1(y_l), \ldots, f_n(y_l)$, 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 $0 \leq j \leq k$ and $1 \leq l \leq m$, we have $M = m(k+1)$ equations in $N = (L+1)^2$ variables. But since

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

and for $k$ sufficiently 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 $c_2^2 NU$. It can be shown that we can take $U \leq k^{c_0 k}$

\[\square\]

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

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

Further, for any $j, l$ with $j \geq k, l \leq m$ 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 $\Phi$ and all its derivatives vanish at the points $y_1, \ldots, y_m$. Using induction on $j$, assume that

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

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

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

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

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

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,

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

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

$$|\phi^{(j)}(y_l)| \leq j^{c_1 j - j m/(8\rho)}.$$

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 $h_1 \cdots h_m$ does not vanish at $y_l$, which we can. Therefore by induction, $\Phi$ 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 $i, j$. 

25
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 $E$.  

26
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

\[
e^{x_i y_j} \quad i = 1, 2, \quad j = 1, 2, 3
\]

is transcendental.

### 6 Pari/GP Code

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

```gp
/*
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]) \
    , \
    plotraw(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)); \
    ); \
  );
}
```

27
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) = \ 
--------------------------------------------------------------------------------------------------------------------------------- 

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


