On the Weierstrass $\wp$-function as an Exponential Map

Dylan Mahoney and Bryan Park

Mentor: Rodrigo Sanches Angelo

September 11, 2022

Abstract

Any elliptic curve over the complex numbers is equivalent to a complex torus. The standard method of showing this is using the Weierstrass $\wp$-function. We first review relevant background and then work out the same equivalence using an exponential map on elliptic curves. Toward this end, we derive some relevant estimates, define the exponential map on elliptic curves, and show that it is a surjective open homomorphism; then a lattice quite naturally emerges as its kernel. We then show that this exponential map is equal to the isomorphism constructed with the Weierstrass $\wp$-function. We include some numerical work (we suspect that our method could be a faster means of numerically computing $wp(z)$) and graphics illustrating the ideas herein presented. Finally, we discuss connections with complex multiplication of elliptic curves.

Acknowledgements

We would like to thank our mentor, Rodrigo Sanches Angelo, for the incredible support, guidance, and instruction we received from him. We would also like to thank the SURIM program at Stanford University for funding this project in the summer of 2022, and Lernik Asserian, who did a wonderful job running SURIM in 2022.

Contents

Chapter 1

Background

1.1 Motivation

Consider the equation $a^4 + b^4 = c^4$. This is a special case of Fermat's last theorem, which implies that the given equation has no non-trivial integer solutions. One way to show this is by the change of variables

$$x = \frac{b^2 + c^2}{a^2},\ y = \frac{4b(b^2 + c^2)}{a^2}$$

where we assume $a \neq 0$. If $a^4 + b^4 = c^4$, then one can check that the relation $y^2 = x^3 - 4x$ must hold. It turns out that the only rational solutions to this relation are $(x, y) = (0, 0)$ or $(\pm 2, 0)$. All cases correspond to $y = 0$ and thus $b = 0$, which indicate that no non-trivial solutions of $a^4 + b^4 = c^4$ exist.

We can prove the cubic case of Fermat's theorem similarly. Consider the equation $a^3 + b^3 = c^3$. Let

$$x = 12\frac{c}{a + b},\ y = 36\frac{a - b}{a + b}$$

where we assume $abc \neq 0$. Assuming the cubic equation is satisfied, we obtain the relation $y^2 = x^3 - 432$. The only rational solutions are $(x, y) = (12, \pm 36)$. This gives either $a = 0$ or $b = 0$, again showing that there are no non-trivial solutions.

Indeed, finding all rational points to such equations is not at all trivial. Rather, we considered the above examples to motivate the concept of *elliptic curves.* Above, we have two equations involving a, b, c and two equations involving x, y. Exactly three of them describe elliptic curves. In the quartic case, only the equation $y^2 = x^3 - 4x$ is an elliptic curve. In the cubic case, both the original Fermat equation and the derived relation are elliptic curves. In fact, the given change of variables gives an isomorphism between the two.

Note the similarity between the equations $y^2 = x^3 - 4x$ and $y^2 = x^3 - 432$. In general, any elliptic curve can be described by its *Weierstrass form*, which is an equation of the form $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{F}$ for some field $\mathbb{F}$. This allows us to give a working definition of elliptic curves.

1.2 Definition

Here, we give a definition of elliptic curves.

Definition 1 (Elliptic Curves)**.** Let $K \subseteq L$ be fields. Take any $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. Then, the corresponding *elliptic curve over K with coordinates in L* is defined as

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + Ax + B\} \cup \{\infty\},$$

where the final point included is the *point at infinity.*

We note that L is usually taken to be the algebraic closure of K. In this paper, we are most interested in the case $K = L = \mathbb{C}$. Moreover, note that the definition above has two technicalities. First, it requires that $4A^3 + 27B^2 \neq 0$, which is equivalent to saying $x^3 + Ax + B$ has no multiple roots. Second, it requires a point at infinity. To understand where these technicalities come from, we need to consider the surprising fact that the set of points $E(L)$ forms a group. This group structure essentially forms the basis of what makes elliptic curves interesting and applicable. In the next section, we describe the actual group operation.

1.3 Group Law

An elliptic curve over any field forms a group. However, the group operation is most intuitive when understood geometrically. Hence, for illustration purposes, we first consider elliptic curves in the real plane. Consider the figure below.

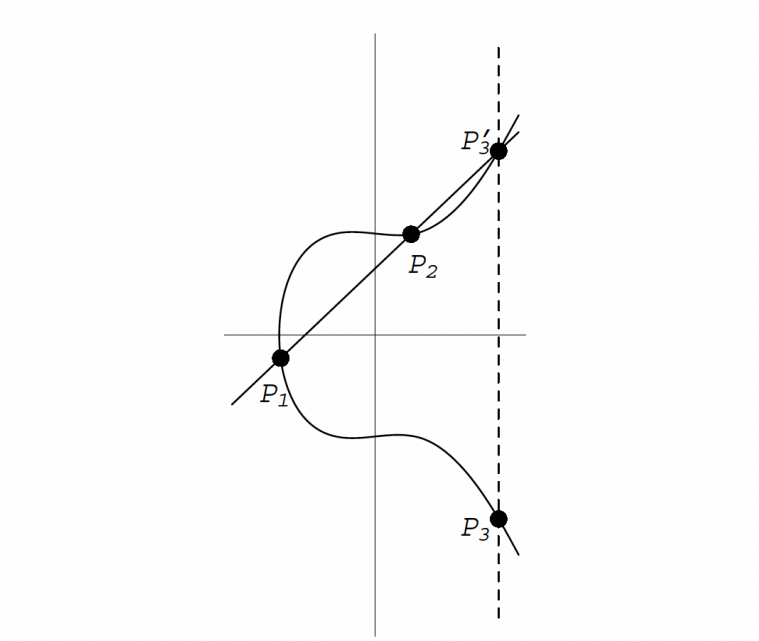

Figure 1.1: The Group Operation

The given graph is an example of an elliptic curve E over $\mathbb{R}$. If we pick any two points P_1 and P_2 on E, then we can produce a third point $P_1 +_E P_2 = P_3$ by the procedure depicted below. The idea is to draw the line passing through points P_1 and P_2 and find the third intersection point with the elliptic curve, then reflect it horizontally. There are a few things, however, to check that this operation actually gives a group structure.

First, we check that the operation is well-defined. By the y^2 term in the Weierstrass form, we see that we can always horizontally reflect points. Moreover, since the Weierstrass form gives a cubic in x, a line passing through two points (including multiplicity) always intersects at a third single point (including the point at infinity). Finally, we make sure that the third point remains in the given field. For instance, assume our elliptic curve is over $\mathbb{Q}$. How do we know the third point produced is also a rational point? To see this, take any equation $y^2 = x^3 + px + q$ where $p, q \in \mathbb{Q}$. If we pick two rational points, the line through them will be given by $y = ax + b$ for some $a, b \in \mathbb{Q}$. Solving for both equations, we will obtain a cubic with rational coefficients. In particular, the coefficient of x^2 is the sum of the x-coordinates of the three intersection points. Since two of them are rational, the third must also be rational. This implies that the y-coordinate of the third point is also rational, and thus our group operation is well-defined. In particular, we remark that the group operation allows one to produce new rational points on an elliptic curve given two already known points.

Next, we show that our group operation has an identity element. In fact, we claim that the point ∞ is the identity, which is exactly why it is included as a technicality in the definition. In figure 1, one can think of ∞ as lying on the top of the y-axis, or the coordinate (c, ∞) for any $c \in \mathbb{R}$. By symmetry, we see that $(c, \infty) \sim (c, -\infty)$ and thus ∞ can also be thought of as lying on the bottom of the y-axis. Indeed, all these coordinates describe the single point ∞. With this in mind, for any point P on the elliptic curve, one can show that $P + \infty = P$ since the line passing through P and ∞ is the vertical line passing through P, thus intersecting the curve at its horizontal reflection. The same observation shows that the inverse of any point P is its horizontal reflection.

Surprisingly, the given operation is also associative, but this isn't as simple to verify as the other two group axioms. One can either show this through direct computation or arguments in projective space. As a final remark, we note that adding a point to itself is given by considering the tangent line of the point. The condition $4A^3 + 27B^2 \neq 0$ is needed so that every point has a tangent line.

To conclude, note that the algebraic formulas describing the geometric procedures above work for any field. Below, we give an algebraic definition of the group operation for elliptic curves.

Definition 2 (Group Law)**.** Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{F}$ for some field $\mathbb{F}$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E such that $P_1, P_2 \neq \infty$. Then, $P_1 + P_2 = P_3 = (x_3, y_3)$ is defined as below:

1. If $x_1 \neq x_2$, then

$$x_3 = m^2 - x_1 - x_2,\ y_3 = m(x_1 - x_3) - y_1,$$

where $m = (y_2 - y_1)/(x_2 - x_1)$.

2. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.
3. If $P_1 = P_2$ and $y_1 \neq 0$, then

$$x_3 = m^2 - 2x_1,\ y_3 = m(x_1 - x_3) - y_1,$$

where $m = (3x_1^2 + A)/(2y_1)$.

4. If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.

Finally, we define $P + \infty = P$ for all points P on E.

With this definition, we are indeed able to work with elliptic curves over any field.

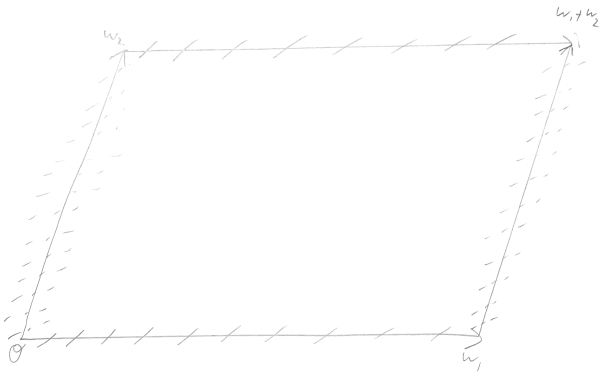

Figure 1.2: The fundamental parallelogram for the complex plane modulo a lattice. The top/bottom and left/right sides are identified modulo the lattice

1.4 Facts about Lattices

Both this section and section 1.5 will closely follow Chapter 9 of Lawrence C. Washington's book on elliptic curves ([Was08]).

1.4.1 The Torus from a Lattice

Given two complex numbers ω_1 and ω_2 which are linearly independent over $\mathbb{R}$, consider the set

$$\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

which we may also write $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, which we call a lattice. Note that a lattice is an additive subgroup of $\mathbb{C}$, so we may consider the quotient $\mathbb{C}/\Lambda$. This quotient may be visualized via the "fundamental parallelogram" of the lattice (Figure 1.2).

If we imagine folding this parallelogram outside of the page, identifying the bottom and top edges, and the left and right edges, we see that this equal as a topological group to the torus.

1.4.2 Reasons Why Lattices are Nice

- The points $z \in \mathbb{C}/\Lambda$ such that $nz \equiv 0$ modulo Λ are very simple to determine geometrically (Figure 1.3), and in particular we may see that that there are n^2 such points on the torus, and hence on any elliptic curve over $\mathbb{C}$.
- While the implementation details are somewhat complicated, the fact that there are n^2 points of order dividing n on an elliptic curve over $\mathbb{C}$ can be used to show that an elliptic curve over a finite field is isomorphic to either a cyclic group or a product of cyclic groups (this is discussed in section 5.1).
- Once we have that elliptic curves over $\mathbb{C}$ are equivalent to tori, endomorphisms (that is, homomorphisms from E to itself given by rational functions) become very simple to visualize, as they are just multiplication of $\mathbb{C}$ by a complex number such that the lattice is preserved (this topic is further discussed in section 5.3).

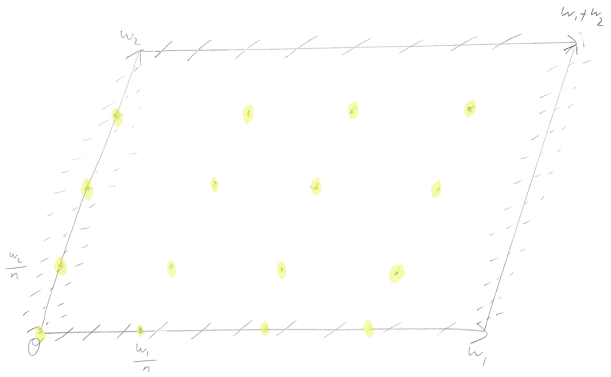

Figure 1.3: Points of order dividing 4 in the fundamental parallelogram.

1.5 The Weierstrass $\wp$-function

One way to show that elliptic curves over $\mathbb{C}$ are tori is to define the Weierstrass $\wp$-function, show that it has certain properties, use it to construct a surjective homomorphism into some elliptic curve over $\mathbb{C}$ whose kernel is a lattice, and then show that for an arbitrary elliptic curve over $\mathbb{C}$ we can construct the right lattice to get such a homomorphism.

1.5.1 Definition and Properties

Given a lattice Λ, we define the Weierstrass $\wp$-function $\wp(z)$ by

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]. \tag{1.1}$$

Then we need to show that this function has the following properties:

- It is meromorphic, with a pole of order 2 at each point in the lattice. That the poles are thus is to be expected from the $\frac{1}{z^2}$ and $\frac{1}{(z-\omega)^2}$ terms in the definition. Since the point at infinity is the identity of the elliptic curve, poles will correspond to the kernel of the homomorphism we will construct.
- It is doubly periodic; that is, $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Lambda$.
- From the lattice, one may compute constants g_2 and g_3 such that

  $$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3, \tag{1.2}$$

  i.e. the image of the map $\mathbb{C} \to \mathbb{C}^2$ given by $z \mapsto (\wp(z), \wp'(z))$ lies on the elliptic curve $y^2 = 4x^3 - g_2x - g_3$.[1]
- The map $z \mapsto (\wp(z), \wp'(z))$ is a homomorphism from $\mathbb{C}$ as an additive group to the elliptic curve $y^2 = 4x^3 - g_2x - g_3$.
- This map is surjective.

[1] One could put this curve into Weierstrass form, but the convention is not to do so.

At this point we have a surjective homomorphism from $\mathbb{C}$ to an elliptic curve whose kernel is a lattice Λ, so by the First Isomorphism Theorem, the elliptic curve is isomorphic to $\mathbb{C}/\Lambda$.

1.5.2 How to Find the Right Lattice Given a Curve

Now we need to show that we can get any elliptic curve through the above procedure. The idea is to define a bijection $j : \mathcal{F} \to \mathbb{C}$ (where $\mathcal{F}$ is a subset of $\mathbb{C}$ called the "fundamental domain") and then show that if an elliptic curve has a j-invariant of ℓ (the j-invariant is a complex number assigned to elliptic curves which characterizes them exactly up to rescaling of axes), then the lattice $\mathbb{Z} + j^{-1}(\ell)\mathbb{Z}$ induces a homomorphism onto the elliptic curve via the $\wp(z)$ this lattice induces. An added bonus of this result is that the space of all possible elliptic curves over $\mathbb{C}$ up to isomorphism is geometrically identified with $\mathcal{F}$, which is rather pretty.

1.6 Inspiration

It is suggested on page 148 of [Wal08] that the map $z \mapsto (\wp(z), \wp'(z))$ is in fact an exponential map, inspiring us to try to work out this exponential map explicitly and show its equivalence to the map constructed with $\wp(z)$. Before we go on, however, let us discuss a toy model which will employ many of our ideas in a simpler setting.

1.7 A Toy Model: the Circle

Before getting to our results on elliptic curves, it is useful to first discuss the circle, since most of the ideas and strategies of the coming results are analogous to much simpler ideas and strategies pertaining to the circle.

1.7.1 The Exponential Map for the Circle

Suppose that we were presented with the circle group as the set

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

with the binary operation

$$(a, b) \times_{\mathbb{S}^1} (x, y) = (ax - by, ay + bx)$$

and identity $(1, 0)$, and wanted to show that this group is isomorphic to $\mathbb{R}/2\pi\mathbb{Z}$. One way to do so is as follows.

Proof. First, note (e.g. by implicit differentiation of $x^2 + y^2 = 1$) that the tangent line to the identity is the line $x = 1$. Then identify this tangent line with $\mathbb{R}$ via the mapping $t \mapsto (1, t)$, and consider the limit

$$\lim_{n\to\infty} \left(1, \frac{t}{2^n}\right)^{2^n}.$$

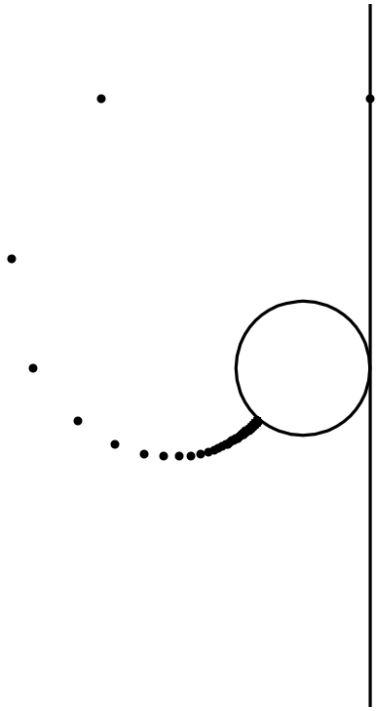

Figure 1.4: Exponential map for the circle

(The reason why we have 2^n's instead of n's in the places where we have 2^n's will become more clear after we define the exponential map for elliptic curves; regardless, passing to a subsequence of a convergent sequence yields the same limit.) If we identify $\mathbb{R}^2$ with $\mathbb{C}$ in the usual way, then $\times_{\mathbb{S}^1}$ becomes regular complex multiplication and $(1, \frac{t}{2^n})$ becomes $1 + i\frac{t}{2^n}$, so this limit becomes

$$\lim_{n\to\infty} (1 + \frac{it}{2^n})^{(2^n)}.$$

By standard results in analysis, this is equal to

$$\lim_{n\to\infty} (1 + \frac{it}{n})^n = e^{it} = \cos t + i \sin t.$$

The identity $\cos^2 t + \sin^2 t = 1$ tells us that the image of this map lies in E. This map is a homomorphism $(\mathbb{R}, +) \to (\mathbb{S}^1, \times_{\mathbb{S}^1})$, since $e^{i(t+s)} = e^{it}e^{is}$, and it is surjective because every point on the circle is equal to $(\cos\theta, \sin\theta)$ for some $\theta \in \mathbb{R}$. Its kernel consists of

$$\{t \in \mathbb{R} : e^{it} = 1\} = \{t \in \mathbb{R} : \cos t = 1 \text{ and } \sin t = 0\} = 2\pi\mathbb{Z}.$$

Hence, by the First Isomorphism Theorem, the image of this homomorphism is isomorphic to its domain modulo its kernel, so $\mathbb{S}^1 \cong \mathbb{R}/2\pi\mathbb{Z}$. □

Chapter 2

Defining the Exponential Map

Let $y^2 = x^3 + Ax + B$ be an elliptic curve E, and let $P = (x_0, y_0)$ be a finite point on E.

Definition 3. We may define an alternative group law on E (which we will denote by $+_{E'}$) via

$$M +_{E'} N \coloneqq M +_E N -_E P, \tag{2.1}$$

and this is the group law we will use to define the exponential map.[1]

We will denote Euclidian operations via a subscript "Eu".

2.1 Defining the Projection Map

Because an elliptic curve is non-singular by definition,[2] the elliptic curve will have a tangent space $T_P E$, which will be a 1-dimensional (over $\mathbb{C}$) subspace of $\mathbb{C}^2$. By implicitly differentiating, we see that the tangent space is given by

$$(3x_0^2 + A)(x - x_0) = 2y_0(y - y_0).$$

We may identify this tangent space with $\mathbb{C}$ via the mapping

$$\iota(z) = (x_0 + 2y_0 z, y_0 + (3x_0^2 + A)z). \tag{2.2}$$

First, let's assume that $y_0 = 0$. In this case we may more simply identify the tangent space with $\mathbb{C}$ via $\iota(z) = (x_0, z)$ (which agrees with the ι above up to re-scaling by a factor of $(3x_0^2 + A)$). Now we want to define a function f that projects from the point (x_0, z) onto the elliptic curve by moving in the x-direction. To construct f, we will use the Implicit Function Theorem. Let

$$\varphi(z, x) = z^2 - x^3 - Ax - B. \tag{2.3}$$

Then φ is a polynomial in z and x and is hence a complex analytic function $\mathbb{C}^2 \to \mathbb{C}$. And $\frac{\partial \varphi}{\partial x} = -3x^2 - A$ is

[1] Really, which point we choose as the identity for the group operation on E is arbitrary in such a way that there's nothing more natural about $+_E$ relative to $+_{E'}$. However, using the point at infinity is the more common convention, and we at times need to mix the two group operations in a single expression, so we adopt the notation $+_E$ and $+_{E'}$ to avoid confusion.

[2] Definition 1 requires that $4A^3 + 27B^2 \neq 0$, which implies that $x^3 + Ax + B$ has no repeated roots, which implies that $3x^2 + A$ is never zero when $x^3 + Ax + B$ is zero, which ensures that the curve is non-singular.

nonzero at $x = x_0, z = 0$ because the elliptic curve is non-singular. Thus by the Implicit Function Theorem for the complex variables setting,[3] there exists a disk $\mathbb{D} \subset \mathbb{C}$ around the origin and a holomorphic map $\tilde{f} : \mathbb{D} \to \mathbb{C}$ such that $\varphi(z, \tilde{f}(z)) = 0$, i.e. $z \mapsto (\tilde{f}(z), z)$ is a map from a disk in the tangent space onto the elliptic curve. Because the zeroes of $x^3 + ax + b$ are separated and $\tilde{f}$ is continuous, and because the implicit function theorem doesn't rely on anything outside of a neighborhood of the point where we took the Jacobian determinant, the image of $\mathbb{D}$ under $z \mapsto (\tilde{f}(z), z)$ contains a neighborhood $V \subset E$ of the point P and $\tilde{f}(0) = x_0$.

When $y_0 \neq 0$, a similar argument applies except that we need to perform a linear change of variables, but this doesn't effect the non-singluarity of the curve and hence doesn't effect the part where the directional derivative of φ in the direction perpendicular to the tangent plane needs to be nonzero.

Thus $f(z) = (z, \tilde{f}(z))$ (or a more complicated expression involving linear changes of variables when $y_0 \neq 0$) is the projection map we want, and is holomorphic $\mathbb{C} \to \mathbb{C}^2$. And the very definition of a tangent space then requires that $\tilde{f}(z) - x_0 = \mathcal{O}(z^2)$, i.e. $\tilde{f}(0) = x_0$ and $\tilde{f}'(0) = 0$. In the case when $y_0 \neq 0$, the algebra is a bit more complicated, but we see from the definition of what a tangent space is that

$$f(z) = \iota(z) +_{Eu} \mathcal{O}(z^2) \tag{2.4}$$

2.2 Some Inequalities

In order to show results about exp, we'll need to derive some estimates showing that near P, the elliptic curve operation is "almost Euclidian". We'll also need to define a function (which will be denoted $\|\cdot\|_R$) that measures distance from P which, near P, satisfies a version of the triangle inequality with respect to the elliptic curve operation.

Because the group law is made up entirely of rational expressions, it is clear that the map

$$g(z, w) \coloneqq f(z) +_{E'} f(w) \tag{2.5}$$

is holomorphic in z and w if the denominators of the relevant rational expressions (once we write each component of $g(z, w)$ as a polynomial in $z, \tilde{f}(z), w, \tilde{f}(w)$ divided by another such polynomial) are nonzero.[4] But $g(0, 0) = f(0) + f(0) - P = P + P - P = P$ is some finite value, so the denominators don't vanish at $(0, 0)$,[5] so they must not vanish on some neighborhood $U_1 \subset \mathbb{C}^2$ of $(0, 0)$, so g is holomorphic $U_1 \to \mathbb{C}^2$.

Thus for $(z, w) \in U_1$, we may apply the following expansion (where all pluses and minuses are Euclidian, with points in $\mathbb{C}^2$):

$$\begin{aligned}
g(z, w) - g(z, 0) - g(0, w) &= [g(z, w) - g(z, 0)] - [g(0, w) - g(0, 0)] - g(0, 0) \\
&= -g(0, 0) + w\tfrac{\partial g}{\partial w}|_{(z,0)} - w\tfrac{\partial g}{\partial w}|_{(0,0)} + \mathcal{O}(z^2, zw, w^2) \\
&= -g(0, 0) + w\left[\tfrac{\partial g}{\partial w}|_{(z,0)} - \tfrac{\partial g}{\partial w}|_{(0,0)}\right] + \mathcal{O}(z^2, zw, w^2) \\
&= -g(0, 0) + w\left(z\tfrac{\partial^2 g}{\partial z \partial w} + \mathcal{O}(z^2)\right) + \mathcal{O}(z^2, zw, w^2) \\
&= -g(0, 0) + \mathcal{O}(z^2, zw, w^2),
\end{aligned}$$

[3] See the statement on the first page of [CP03]. We're using the case of $m = 1$, in which case the Jacobian determinant is of a 1×1 matrix.

[4] See Proposition 2.1 of [Kni96].

[5] It could also be that the numerator and denominator both vanish and we have a removable discontinuity, but in this case the same conclusion still holds.

or, rearranging, $g(z,w)-g(0,0)=g(z,0)-g(0,0)+g(0,w)-g(0,0)+\mathcal{O}(z^2,zw,w^2)$. Hence, since $f(0)=P$, we get the following result:

Lemma 1. For z,w in some neighborhood U_1 of the origin, we have that

$$f(z)+_{E'}f(w)-_{Eu}P=f(z)-_{Eu}P+_{Eu}f(w)-_{Eu}P+\mathcal{O}(z^2,zw,w^2). \tag{2.6}$$

Note that if $z=0$ or $w=0$, we have that $f(z)+_{E'}f(w)-_{Eu}P=f(z)-_{Eu}P+_{Eu}f(w)-_{Eu}P$ exactly, so each term in the $\mathcal{O}(z^2,zw,w^2)$ must have at least one factor of z and at least one factor of w. Hence, we get that for some $a\in\mathbb{C}^2$,

$$f(z)+_{E'}f(w)-_{Eu}P=f(z)-_{Eu}P+_{Eu}f(w)-_{Eu}P+azw+z\mathcal{O}(w^2,z)+w\mathcal{O}(z^2,w).$$

Then, taking the Euclidian norm of both sides and applying the triangle inequality, we get that

$$\|f(z)+_{E'}f(w)-_{Eu}P\|_{Eu}\leq\|f(z)-_{Eu}P\|_{Eu}+\|f(w)-_{Eu}P\|_{Eu}+\|a\|_{Eu}|z||w|+\mathcal{O}(|w|^2,|z|)+\mathcal{O}(|z|^2,|w|).$$

Thus there exists a constant $C_0>0$ such that for z and w in a neighborhood $U_2\subset\mathbb{C}$ of the origin,

$$\|f(z)+_{E'}f(w)-_{Eu}P\|_{Eu}\leq\|f(z)-_{Eu}P\|_{Eu}+\|f(w)-_{Eu}P\|_{Eu}+C|z||w|.$$

To make the notation simpler we have the following definition:

Definition 4. Define $|\cdot|_R:E\to\mathbb{R}_{\geq 0}$ by $|M|_R=\|M-_{Eu}P\|_{Eu}$ ('R' for Rodrigo).

Then we can write this more compactly as

$$|f(z)+_{E'}f(w)|_R\leq|f(z)|_R+|f(w)|_R+C|z||w|. \tag{2.7}$$

Note that because $f(z)$ consists of first moving a distance $|z|\sqrt{|2y_0|^2+|3x_0^2+A|^2}$ from P in one direction and then moving a distance which is $\mathcal{O}(z^2)$ in a perpendicular direction, there exists a constant $C_{\frac{1}{2}}$ such that $|f(z)|_R\geq C_{\frac{1}{2}}|z|$, so there exists a constant C_1 such that

$$|f(z)+_{E'}f(w)|_R\leq|f(z)|_R+|f(w)|_R+C_1|f(z)|_R|f(w)|_R. \tag{2.8}$$

Thus we may write that for $M,N\in f(U_2)$ (note that $f(U_2)$ is a neighborhood of P in the elliptic curve),

$$|M+_{E'}N|_R\leq|M|_R+|N|_R+C_1|M|_R|N|_R. \tag{2.9}$$

We now make the following definition, which will later be used to show that the sequence defining the exponential map for elliptic curves converges:

Definition 5. Let $\|\cdot\|_R:E\to\mathbb{R}_{\geq 0}$ be given by

$$\|M\|_R=\log(1+C_1|M|_R).$$

Near P, this satisfies a version of the triangle inequality:

Lemma 2. For $M,N\in f(U_2)$ (which is a neighborhood of P on E), $\|M+_{E'}N\|_R\leq\|M\|_R+\|N\|_R$.

Proof. We simply use Inequality 2.9 and the properties of the logarithm to write

$$\begin{aligned}\|M +_{E'} N\|_R &= \log(1 + C_1|M+_{E'}|_R) \\ &\leq \log(1 + C_1|M|_R + C_1|N|_R + C_1^2|M|_R|N|_R) \\ &= \log((1 + C_1|M|_R)(1 + C_1|N|_R)) \\ &= \log(1 + C_1|M|_R) + \log(1 + C_1|N|_R) \\ &= \|M\|_R + \|N\|_R\end{aligned}$$

□

Note that from the definition of f, the definition of ι (Equation 2.2) and Equation 2.4,

$$f(z + w) = \iota(z + w) +_{Eu} \mathcal{O}((z + w)^2) = \iota(z) +_{Eu} \iota(w) -_{Eu} P +_{Eu} \mathcal{O}((z + w)^2)$$

while

$$f(z) -_{Eu} P +_{Eu} f(w) -_{Eu} P = \iota(z) -_{Eu} P + \mathcal{O}(z^2) +_{Eu} \iota(w) -_{Eu} P + \mathcal{O}(w^2),$$

which together show that

$$f(z + w) -_{Eu} P = f(z) -_{Eu} P +_{Eu} f(w) -_{Eu} P +_{Eu} \mathcal{O}(z^2, zw, w^2) \tag{2.10}$$

If we combine this with Lemma 1, we get the following:

Lemma 3. For z and w near the origin,

$$f(z + w) = f(z) +_{E'} f(w) + \mathcal{O}(z, w)^2. \tag{2.11}$$

This will provide the connection between addition in $\mathbb{C}$ on the left and addition in the elliptic curve on the right which we'll use to show that exp is a homomorphism.

Before defining the exponential map, we need to show one last inequality. Define $h(z, w) = f(z) -_{E'} f(w) -_{Eu} P$. Since $h(0, 0) = (0, 0)$, h is holomorphic on a neighborhood of the origin by the same reasoning that applied to g earlier. Changing variables to $h(u, v)$ where $u = z + w$ and $v = z - w$, the observation that $h(u, 0)$ is identically $(0, 0)$ shows that every term in the Taylor series for $h(u, v)$ has at least one power of v. Hence we may write, for some $a, b \in \mathbb{C}^2$,

$$h(u, v) = av + buv + \mathcal{O}(v^2, u) = (a + bu)v + \mathcal{O}(v^2, u).$$

Hence there exists a neighborhood $\tilde{U}_3 \subset \mathbb{C}$ of the origin and a constant $C_{\frac{3}{2}} > 0$ such that for u, v in $\tilde{U}_3$, $\|h(u, v)\|_{Eu} \leq C_{\frac{3}{2}}|v|$. Returning to the variables z and w, there exists a neighborhood $U_3 \subset \mathbb{C}$ of the origin such that for $z, w \in U_3$, $\|h(z, w)\|_{Eu} \leq C_{\frac{3}{2}}|z - w|$. And it's clear from the construction of f and ι that there exists a constant $C_{\frac{5}{6}} > 0$ such that

$$\|f(z) -_{Eu} f(w)\|_{Eu} \geq C_{\frac{5}{6}}|z - w|,$$

this implies that for some constant C_2,

$$\|f(z) -_{E'} f(w)\|_{Eu} \leq C_2 \|f(z) -_{Eu} f(w)\|_{Eu}.$$

This implies the following:

Lemma 4. For M, N in $f(U_3)$,

$$|M -_{E'} N|_R \leq C_2 \|M -_{Eu} N\|_{Eu}. \tag{2.12}$$

2.3 Topological Considerations

Thus far we have thought of E as a subset of $\mathbb{C}^2$ along with a point at infinity. Here it will be more convenient to think of E as being the the subset of $\mathbb{CP}^2$ given by

$$\{[x : y : z] \in \mathbb{CP}^2 : y^2 z = x^3 + Axz^2 + Bz^3\}.$$

Then $\mathbb{C}^2$ can be identified with the points with non-zero z by representing them as $[x : y : 1]$ and the point at infinity on the elliptic curve is $[0 : 1 : 0]$.

First, note that E is path-connected. To show this, it suffices to choose a point $(x_0, 0)$ on E (we are guaranteed to have three such points) and show that any other point on E can be connected to it by a continuous path $\Gamma : [0, 1] \to E$. Let $(x, y) \in E$. Modulo 2π, $\arg(y)$ must be equivalent to $\frac{x^3+ax+b}{2} + \alpha$ where α is either 0 or π. Because $\mathbb{C}$ is path-connected, there exists a path $\Gamma_1 : [0, 1] \to \mathbb{C}$ such that $\Gamma_1(0) = x_0$ and $\Gamma_1(1) = x$. We can choose continuous $r : [0, 1] \to \mathbb{R}_{\geq 0}$ and $\theta : [0, 1] \to \mathbb{R}$ such that $\Gamma_1(t)^3 + a\Gamma_1(t) + b = r(t)e^{i\theta(t)}$. Then $(\Gamma_1(t), r(t)^{\frac{1}{2}} e^{i\left[\frac{\theta(t)}{2}+\alpha\right]})$ is the continuous path we need. The same argument works for the point at infinity; we just need Γ_1 to have a pole at 1.[6] Since path-connectedness is a stronger condition than connectedness, E is also connected.

Let us define the open and closed subsets of E to be given by the subspace topology of E as a subset of the projective plane $\mathbb{CP}^2$.

With this topology we may see that E is sequentially compact. Let (x_n, y_n) be a sequence of points on E. If this sequence has a bounded subsequence, then that subsequence is contained in a ball in $\mathbb{C}^2$ (which is compact) and hence has a subsequence (x_{n_k}, y_{n_k}) converging to a point in that ball. But because polynomials are continuous, $(\lim_{k\to\infty} y_{n_k})^2 = (\lim_{k\to\infty} x_{n_k})^3 + a(\lim_{k\to\infty} x_{n_k}) + b$, so this limit is on E. If the sequence has no bounded subsequence. Because $|y| \sim |x|^{\frac{3}{2}}$ when x and y are large, $\lim_{n\to\infty} \frac{|x_n|}{|y_n|} = 0$ and $\lim_{n\to\infty} \frac{1}{|y_n|} = 0$, so in $\mathbb{CP}^2$ the sequence converges to the point $[0 : 1 : 0]$, which is the point at infinity on the elliptic curve.

2.4 The Definition as a Limit

Let us now define the map $\exp : \mathbb{C} \to E$ via

$$\exp(z) = \lim_{n\to\infty} 2^n f(\frac{z}{2^n}) \tag{2.13}$$

[6] In this case because $|y| \sim |x|^{\frac{3}{2}}$ when x and y are large, $\Gamma(1)$ will be the point $[0 : 1 : 0]$ in $\mathbb{CP}^2$.

(where the multiplication by 2^n means to add $f(\frac{z}{2^n})$ to itself 2^n times with respect to $+_{E'}$). Our first task is to show that this limit always converges to a point on E (which could be the point at infinity).

First, let's write the nth term in the sequence as

$$\begin{aligned}2^n f(\frac{z}{2^n}) &= f(z) + \left[2f(\frac{z}{2}) - f(z)\right] + \left[4f(\frac{z}{4}) - 2f(\frac{z}{2})\right] + \cdots + \left[2^n f(\frac{z}{2^n}) - 2^{n-1} f(\frac{z}{2^{n-1}})\right] \\ &= f(z) + \sum_{k=1}^{n} 2^k f(\frac{z}{2^k}) - 2^{k-1} f(\frac{z}{2^{k-1}}).\end{aligned}$$

Thus the convergence of sequence 2.13 is equivalent to the convergence of the series

$$f(z) + \sum_{k=1}^{\infty} 2^k f(\frac{z}{2^k}) - 2^{k-1} f(\frac{z}{2^{k-1}}). \tag{2.14}$$

Remark 1. If z is outside of the domain of definition of f, then let $\tilde{n}$ be sufficiently large such that $z/2^{\tilde{n}}$ is in the domain of f, and for $n > \tilde{n}$, write

$$2^n f(\frac{z}{2^n}) = 2^{\tilde{n}} f(\frac{z}{2^{\tilde{n}}}) + \sum_{k=\tilde{n}+1}^{n} 2^k f(\frac{z}{2^k}) - 2^{k-1} f(\frac{z}{2^{k-1}}).$$

To avoid notational clutter we will generally ignore this subtlety and write as if z is in the domain of f.

To show convergence, we will show that after a finite number of terms, the tail of the series can be shown to remain within an arbitrarily small neighborhood of P. First, note from Equation 2.11 that

$$f(z) = 2f(z/2) +_{Eu} \mathcal{O}(z^2). \tag{2.15}$$

If we combine this with Inequality 2.12, we see that there exists a neighborhood $U_4 \subset \mathbb{C}$ of the origin and a constant $C_3 > 0$ such that for $z \in U_4$,

$$|2f(z/2) -_{E'} f(z)|_R \leq C\|2f(z/2) +_{Eu} \mathcal{O}(z^2) -_{Eu} 2f(z/2)\|_{Eu} \leq C_3|z|^2.$$

Then, because $\log(1+ct) = t + \mathcal{O}(t^2)$, we get that for z in a neighborhood U_5 of the origin and some constant $C_4 > 0$,

$$\|2f(z/2) -_{E'} f(z)\|_R \leq C_4|z|^2.$$

Hence, using the "triangle inequality" of $\|\cdot\|_R$, for any $N_2 \geq N_1$ such that $z/2^{N_1}$ is in U_5 and $\|M\|_R \leq 4C_4|z|^2/2^{N_1}$ implies M is in the neighborhood where our 'triangle inequality" holds, we get that

$$\begin{aligned}\|2^k f(\frac{z}{2^k}) - 2^{k-1} f(\frac{z}{2^{k-1}})\|_R &= \|2^{k-1}\left[2f(\frac{z}{2^k}) - f(\frac{z}{2^{k-1}})\right]\|_R \\ &\leq 2^{k-1} C_4 |\frac{z}{2^{k-1}}|^2 \\ &= \frac{2C_4|z|^2}{2^k}\end{aligned}$$

and hence that

$$\begin{aligned}\|\sum_{k=N_1}^{N_2} 2^k f(\frac{z}{2^k}) - 2^{k-1} f(\frac{z}{2^{k-1}})\|_R &\leq \sum_{k=N_1}^{N_2} \|2^k f(\frac{z}{2^k}) - 2^{k-1} f(\frac{z}{2^{k-1}})\|_R \\ &\leq \sum_{k=N_1}^{N_2} \frac{2C_4|z|^2}{2^k} \\ &\leq \frac{2C_4|z|^2}{2^{N_1}}(1 + \frac{1}{2} + \frac{1}{4} + \dots) \\ &\leq \frac{4C_4|z|^2}{2^{N_1}}\end{aligned}$$

which goes to zero as N_1 goes to infinity.

Thus we have shown that for any z and any $\varepsilon > 0$ there exists an N such that for all $n, m \geq N$, $|2^m f(\frac{z}{2^m}) -_{E'} 2^n f(\frac{z}{2^n})|_R < \varepsilon$.

Note that given a point M on E, if we extend the formula for $M +_{E'} (x, y)$ (which consists of rational expressions) to points (x, y) not on the elliptic curve, we get components which are meromorphic in x and y, and[7] since M is finite, holomorphic on some neighborhood of P.[8] Hence, since holomorphic functions are *a fortiori* continuous, by requiring the Euclidian distance from (x, y) to P to be sufficiently small, we can ensure that the Euclidian distance from M to $M +_{E'} (x, y)$ is as small as we like.

Hence showing that "for any z and any $\varepsilon > 0$ there exists an N such that for all $n, m \geq N$, $|2^m f(\frac{z}{2^m}) -_{E'} 2^n f(\frac{z}{2^n})|_R < \varepsilon$" suffices to show that the series is Cauchy and hence converges. And it must converge to a point on the elliptic curve because the elliptic curve is topologically closed.

[7]The argument is slightly different if M is the point at infinity.
[8]There could be a removable hole, but this is fine.

Chapter 3

Properties of the Exponential Map

3.1 The Exponential Map is a Homomorphism

We now wish to show that $\exp(z+w) = \exp(z) +_{E'} \exp(w)$, i.e. that $\exp(z+w) -_{E'} \exp(z) -_{E'} \exp(w) = P$, i.e. that $\lim_{n\to\infty} 2^n f(\frac{z+w}{2^n}) - \lim_{n\to\infty} 2^n f(\frac{z}{2^n}) - \lim_{n\to\infty} 2^n f(\frac{w}{2^n}) = P$. Since the three limits all converge and the elliptic curve operation is commutative, this is equivalent to the statement that

$$\lim_{n\to\infty} 2^n f(\frac{z+w}{2^n}) - 2^n f(\frac{z}{2^n}) - 2^n f(\frac{w}{2^n}) = P,$$

which is equivalent to the statement that

$$\lim_{n\to\infty} \left\| 2^n \left[f(\frac{z+w}{2^n}) - f(\frac{z}{2^n}) - f(\frac{w}{2^n}) \right] \right\|_R = 0.$$

But from inequalities 2.11 and 2.12 and that $\log(1+ct) = ct+\mathcal{O}(t^2)$, we know that there is a neighborhood U_6 of the origin and a constant C_5 such that for z and w in U_6, $\|f(z+w) -_{E'} f(z) -_{E'} f(w)\|_R \leq C_5(|z|^2+|w|^2)$. Hence for n sufficiently large such that $z/2^n$ and $w/2^n$ are in U_6 and such that

$$\|M\|_R \leq 2^n C_5(|z/2^n|^2 + |w/2^n|^2) = \frac{C_5(|z|^2+|w|^2)}{2^n}$$

implies M is in the neighborhood of P where our "triangle inequality" holds, we get that

$$\left\| 2^n \left[f(\frac{z+w}{2^n}) - f(\frac{z}{2^n}) - f(\frac{w}{2^n}) \right] \right\|_R \leq \frac{C_5(|z|^2+|w|^2)}{2^n}$$

which goes to zero as n goes to infinity.

3.2 The Exponential Map is an Open Map

Let Ω be a bounded subset of $\mathbb{C}$, and let K be a compact subset of Ω. Let $B > 0$ be such that $|z| < B$ for all $z \in \Omega$. As in the argument that $\exp(z)$ converges, let N be sufficiently large such that $z/2^N$ is in U_5 and the intersection of E with the ball of radius $4C_4|z|^2/2^N$ centered at P in $\mathbb{C}^2$ is in the neighborhood where our

"triangle inequality" holds, for all $z \in \Omega$ (this is possible because Ω is bounded). On Ω, let us write $\exp(z)$ as

$$\exp(z) = 2^N f(\frac{z}{2^N}) +_{E'} \sum_{k=N+1}^{\infty} 2^k f(\frac{z}{2^k}) -_{E'} 2^{k-1} f(\frac{z}{2^{k-1}}). \tag{3.1}$$

Because of how large we chose N to be, we know from our proof that $\exp(z)$ converges that $\sum_{k=N+1}^{\infty} 2^k f(\frac{z}{2^k}) -_{E'} 2^{k-1} f(\frac{z}{2^{k-1}})$ can never have a pole. And if we cut off this sum after finitely many terms, then because the elliptic curve operation is rational, we get a meromorphic function of z (which will in fact be holomorphic on Ω because we know there are no poles). And our proof of the convergence of the sequence also bounds the error from cutting off this sum after N_1 terms by $\frac{4C_4B^2}{2^{N_1}}$, which is a uniform bound on K. Thus each component of $\sum_{k=N+1}^{\infty} 2^k f(\frac{z}{2^k}) -_{E'} 2^{k-1} f(\frac{z}{2^{k-1}})$ is, on compact subsets of Ω, the limit of a uniformly convergent sequence of holomorphic functions on Ω and is hence holomorphic. Then because $+_{E'}$ consists of rational expressions and $2^N f(\frac{z}{2^N})$ is at least meromorphic, both components of $\exp(z) =$ "meromorphic" $+_{E'}$ "holomorphic" are meromorphic. Since Ω was arbitrary, this shows that each component of $\exp(z)$ is meromorphic on $\mathbb{C}$.

Because meromorphic functions are open maps when we include the point at infinity properly in $\mathbb{C}$, this implies that $\exp(z)$ is an open map $\mathbb{C} \to E$.

3.3 The Image of the Exponential Map is Closed

Suppose we have a sequence of points $x_n \in \mathbb{C}$ such that $\exp(x_n) \to W \in E$. Because the elliptic curve operation is continuous away from where it returns the point at infinity, $\lim_{n\to\infty} \exp(x_n) = w$ implies that $\lim_{n\to\infty} \exp(x_n) -_{E'} w = P$.

Because exp is open, its image includes a neighborhood U of P. For sufficiently large N, then, $\exp(x_N) -_{E'} W$ lies in U. So there exists $y \in \mathbb{C}$ such that $\exp(x_N) -_{E'} W = \exp(y)$, which implies that $W = \exp(x_N) -_{E'} \exp(y) = \exp(x_N - y)$, showing that w is in the image of exp.

3.4 Putting It Together

Since $\mathbb{C}$ is open and closed, the image of exp is open and closed. The image is non-empty and E is connected, so the image must be all of E.

Because exp is a surjective homomorphism $\mathbb{C} \to E$, its kernel H must be an additive subgroup of $\mathbb{C}$, and exp will induce a bijection $\varphi : \mathbb{C}/H \to E$. Since exp is an open map, φ is both an open map and a closed map (i.e. a homeomorphism), so since E is compact, $\mathbb{C}/H$ must also be compact.

Because each component of exp is meromorphic, and the pre-image of any point by a meromorphic map must be a discrete set, H must be discrete. Hence H is a discrete additive subgroup of $\mathbb{C}$ such that $\mathbb{C}/H$ is compact. Then H must be a lattice.[1] Thus as a group and as a topological space, E is isomorphic to $\mathbb{C}$ modulo a lattice, which is a torus. And because our isomorphism consists of meromorphic functions, which locally preserve angles, elliptic curves over $\mathbb{C}$ are also equivalent to tori in a geometric sense.

Remark 2. It is not difficult to see that with a few superficial modifications, our argument can also show that each connected component of an elliptic curve over $\mathbb{R}$ is isomorphic to S^1 (see Chapter 2 of [Was08]).

[1] See the sentence immediately following Definition 5.4 in [Gor11].

3.5 The Exponential Map is Equal to $z \mapsto \left(\wp(z), \frac{1}{2}\wp'(z)\right)$

Definition 6. To move the identity point back to the point at infinity, let us define $\widetilde{\exp} : \mathbb{C} \to E$ by

$$\widetilde{\exp}(z) \coloneqq \exp(z) -_E P. \tag{3.2}$$

Since $+_E$ consists of rational operations, it is clear that $\widetilde{\exp}_1(z)$ and $\widetilde{\exp}_2(z)$ are still both meromorphic, and the computation

$$\begin{aligned}
\widetilde{\exp}(z+w) &= \exp(z+w) -_E P \\
&= \exp(z) +_{E'} \exp(w) -_E P \\
&= \exp(z) +_E \exp(w) -_E P -_E P \\
&= (\exp(z) -_E P) +_E (\exp(w) -_E P) \\
&= \widetilde{\exp}(z) +_E \widetilde{\exp}(z)
\end{aligned}$$

shows that $\widetilde{\exp}$ is a homomorphism $(\mathbb{C}, +) \to (E, +_E)$.

If we consider the reasoning we used to show that $\exp(z)$ converges, but instead of setting K large we consider z small, we see that

$$\exp(z) = f(z) +_{Eu} \mathcal{O}(z^2). \tag{3.3}$$

And we discussed earlier (Equation 2.4) that $f(z) = \iota(z) + \mathcal{O}(z^2)$, so we see that $\exp(z) = (x_0 + 2y_0 z, y_0 + (3x_0^2 + A)z) +_{Eu} \mathcal{O}(z^2)$, from which it follows that $\exp_1'(0) = 2y_0$ and $\exp_2'(0) = (3x_0^2 + A)$. By plugging the expression

$$(x_0 + 2y_0 z + \mathcal{O}(z^2), y_0 + (3x_0^2 + A)z + \mathcal{O}(z^2)) -_E P = (x_0 + 2y_0 z + \mathcal{O}(z^2), y_0 + (3x_0^2 + A)z + \mathcal{O}(z^2)) +_E (x_0, -y_0)$$

into Mathematica (details in Appendix A) we may see that $\widetilde{exp}_1(z)$ has a pole of order 2 and residue 1 at the origin, while $\widetilde{exp}_2(z)$ has a pole of order 3 and residue -1 at the origin. Before continuing on, let's have a digression relating to our toy model, the circle.

3.5.1 A Digression on our Toy Model: Showing That $\frac{\mathrm{d}}{\mathrm{d}x} \sin x = \cos x$

Suppose that we just learned about sine and cosine and we wanted to find their derivatives. One way to do this is to expand $(\cos(x+h), \sin(x+h))$ to first order in h. Because we know that $x \mapsto (\cos x, \sin x)$ is a homomorphism $(\mathbb{R}, +) \to (\mathbb{S}^1, \times_{\mathbb{S}^1})$, we may write that

$$\begin{aligned}
(\cos(x+h), \sin(x+h)) &= (\cos x, \sin x) \times_{\mathbb{S}^1} (\cos h, \sin h) \\
&= (\cos h \cos x - \sin h \sin x, \sin h \cos x + \cos h \sin x).
\end{aligned}$$

Suppose that we are also given that $\cos(0) = 1$ and $\sin(0) = 0$ and $\cos'(0) = 0$ and $\sin'(0) = 1$. Then

$$(\cos(x+h), \sin(x+h)) = ((1)\cos x - (h)\sin x, h\cos x + (1)\sin x) + \mathcal{O}(h^2) \tag{3.4}$$

so $\cos(x+h) = \cos x + (-\sin x)h + \mathcal{O}(h^2)$ and $\sin(x+h) = \sin x + (\cos x)h + \mathcal{O}(h^2)$, which shows that $\frac{\mathrm{d}}{\mathrm{d}x} \cos x = -\sin x$ and $\frac{\mathrm{d}}{\mathrm{d}x} \sin x = \cos x$.

3.5.2 Extending this Method to the Exponential Map for Elliptic Curves

Consider also that

$$\widetilde{\exp}(z+h) = \widetilde{\exp}(z) +_E \widetilde{\exp}(h) = \widetilde{\exp}(z) +_E \exp(h) -_E P. \tag{3.5}$$

If we plug the expression $\widetilde{\exp}(z) +_E \exp(h) -_E P$ into Mathematica (details in Appendix A) and compute a power series (analagous to Equation 3.4) for $\widetilde{\exp}_1(z+h)$ around $h = 0$ given that $\exp_1'(0) = 2y_0$ and $\exp_2'(0) = (3x_0^2 + A)$ and that $\exp_1(0) = x_0$ and $\exp_2(0) = y_0$, we get that

$$\widetilde{\exp}_1(z+h) = \widetilde{\exp}_1(z) + 2\widetilde{\exp}_2(z)h + \mathcal{O}(h^2), \tag{3.6}$$

so $\widetilde{\exp}_1'(z) = \widetilde{\exp}_2(z)$.

3.5.3 The Desired Equality

We now have the machinery in place to prove the following proposition:

Proposition 1. Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the lattice which is the kernel of exp, and let $\wp(z)$ be the Weierstrass $\wp$-function associated to this lattice. Then $\widetilde{\exp}(z) = (\wp(z), \frac{1}{2}\wp'(z))$.

Proof. Because the points of order 2 on E (with respect to $+_E$) are precisely those points with $y = 0$, $\widetilde{\exp}(z)$ is of order 2 if and only if $\widetilde{\exp}_2(z) = 0$. And since L is the kernel of $\widetilde{\exp}$, $\widetilde{\exp}(z)$ is of order 2 if and only if z is congruent modulo L to $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, or $\frac{\omega_1+\omega_2}{2}$. Hence $\widetilde{\exp}_2(z) = 0$ if and only if z is congruent modulo L to $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, or $\frac{\omega_1+\omega_2}{2}$.

Since L is the kernel of $\widetilde{\exp}$ and the point at infinity is the identity of E, $\widetilde{\exp}_2(z)$ has poles only at each point in L. And since $\widetilde{\exp}_2(z+\alpha) = \widetilde{\exp}_2(z)$ for $\alpha \in L$, the degrees and residues of each pole are the same as at zero, which we already know to be order 3 and residue -1.

But it is known[2] that $\wp'(z)$ only has zeros (all of which are of order 1) at points z such that z is congruent modulo L to $\frac{1}{2}\omega_1$, $\frac{1}{2}\omega_2$, or $\frac{\omega_1+\omega_2}{2}$ and that the only poles of $\wp'(z)$ are at the points of L and are of order 3 with residue -2. Hence $\widetilde{\exp}_2(z)/\wp'(z)$ has no poles[3] and so can be made holomorphic by filling in the removable discontinuities. And $\widetilde{\exp}_2(z)/\wp'(z)$ is doubly periodic with respect to L (since both $\wp'(z)$ and $\widetilde{\exp}_2(z)$ are). Thus $\widetilde{\exp}_2(z)/\wp'(z)$ attains its whole image over a compact subset of $\mathbb{C}$ and hence is bounded. Since it's entire, Liouville's Theorem requires that $\widetilde{\exp}_2(z)/\wp'(z)$ is constant. By comparing residues at the poles at L we see that the constant is $\frac{1}{2}$, i.e. $\widetilde{\exp}_2(z) = \frac{1}{2}\wp'(z)$.

Thus we have that $\frac{1}{2}\widetilde{\exp}_1'(z) = \frac{1}{2}\wp'(z)$, so $\widetilde{\exp}_1(z) = \wp(z) + c$ for some constant c. But $\widetilde{\exp}(z)$ lies on E, so we know that

$$\widetilde{\exp}_2(z)^2 = \widetilde{\exp}_1(z)^3 + A\widetilde{\exp}(z) + B$$

for all $z \in \mathbb{C}$. But we just found that $\widetilde{\exp}_2(z) = \frac{1}{2}\wp'(z)$, and we also know (Equation 1.2) that

$$\frac{1}{4}\wp'(z)^2 = \wp(z)^3 - \frac{g_2}{4}\wp(z) - \frac{g_3}{4}$$

for constants g_2 and g_3 determined by the lattice. Hence for all $z \in \mathbb{C}$,

$$\widetilde{\exp}_1(z)^3 + A\widetilde{\exp}(z) + B = (\wp(z)+c)^3 + A(\wp(z)+c) + B = \wp(z)^3 - \frac{g_2}{4}\wp(z) - \frac{g_3}{4}$$

[2] See Chapter 9 of [Was08], especially Part 3 of Theorem 9.1 for the orders of the zeros being 1.

[3] Dividing a pole of order 3 by a pole of order 3 yields a removable discontinuity, while dividing a zero of order greater than or equal to one by a zero of order one also yields a removable discontinuity.

from which it follows that for all $z \in \mathbb{C}$,

$$\begin{aligned}
&(\wp(z)+c)^3 + A(\wp(z)+c) + B - \wp(z)^3 + \frac{g_2}{4}\wp(z) + \frac{g_3}{4} \\
&= \wp(z)^3 + 3c\wp(z)^2 + 3c^2\wp(z) + A\wp(z) + Ac + B - \wp(z)^3 + \frac{g_2}{4}\wp(z) + \frac{g_3}{4} \\
&= 3c\wp(z)^2 + (3c^2 + \frac{g_2}{4} + A)\wp(z) + Ac + B + \frac{g_3}{4} = 0
\end{aligned}$$

for all $z \in \mathbb{C}$. But a nontrivial degree 2 polynomial over $\mathbb{C}$ has at most two solutions, and $\wp(z)$ clearly takes on more than two values, so we must have that

$$3c = (3c^2 + \frac{g_2}{4} + A) = Ac + B + \frac{g_3}{4} = 0$$

which implies that $c = 0$ (so $\widetilde{\exp}_1(z) = \wp(z)$) and $A = -\frac{g_2}{4}$ and $B = -\frac{g_3}{4}$. □

Chapter 4

Numerical Simulations and Graphics

Prior to attempting a formal proof of the above results, we decided to carry out some numerical simulations to see whether the results we expected to be true were reasonable, and we include here some aesthetically pleasing graphics produced by the program we wrote.

Using Python, we first implemented the elliptic curve group operation. We then implemented the exponential map $\widetilde{\exp}$ as follows:

- Choose a point $P = (x_0, y_0)$ on the curve.
- Choose some sufficiently large N (through trial and error we settled on $N = 8$) such that our function will return the Nth element of sequence 2.13 and do a good job of approximating the limit of the sequence.
- Given a complex number z, identify $\frac{z}{2^N}$ with a point on the tangent space of E at P via ι (Equation 2.2).
- Plug the point we get into the elliptic curve operation to double it N times.
- Subtract P (with respect to the elliptic curve operation) from what we get.

Remark 3. Here we plug points into the elliptic curve operation which aren't actually on the elliptic curve, since we neglected to implement the projection map f. But by making N sufficiently large, the points not on the elliptic curve are only off by a little bit, hence why we see to still get good results with the program.

In addition to producing the following graphics, we also numerically checked for some randomly chosen values of z and w that the exponential map is a homomorphism and that the derivative of the first component is twice the second component.

Remark 4. We suspect that this method of numerically computing the Weierstass $\wp$-function could be more efficient than summing the terms in Equation 1.1. Heuristically, if we include only those terms ω in Equation 1.1 with $|\omega| < R$ then we get accuracy $\sim \frac{1}{R}$, so we need to include a number of terms on the order of $\frac{1}{\varepsilon^2}$ to get an error below ε. Based on our error estimates in Section 2.4, we expect that the number of terms required to get a certain level of accuracy with our method will grow more slowly than this.

The results (with $N = 8$) for various values of A, B, and P are shown below. We graph a color map where the RGB corresponds to the argument (red corresponds to an argument of 0, green corresponds to an

argument of $\frac{2\pi}{3}$, and blue corresponds to an argument of $\frac{4\pi}{3}$) and opacity corresponds to the absolute value (zeros in white, poles have maximum opacity),[1] of both the first and second components of the exponential map, as well as the Euclidian norm in $\mathbb{C}^2$ of the exponential map,[2] with z in a specified range. Some key takeaways:

- By counting how many times a small loop around each pole hits each color, we can see that the first component of the exponential map has poles of order 2 and the second component has poles of order 3, agreeing with the Weierstrass $\wp$-function and its derivative.
- From our proof that the sequence which defines the exponential map converges, we would expect that when z is larger, we need to go further along in the sequence to get a good approximation to its limit. Indeed, we see that for $(\Re(z), \Im(z)) \in [-40, 40]^2$, we get some errors for large z when $N = 8$ which disappear if we increase N to 12.

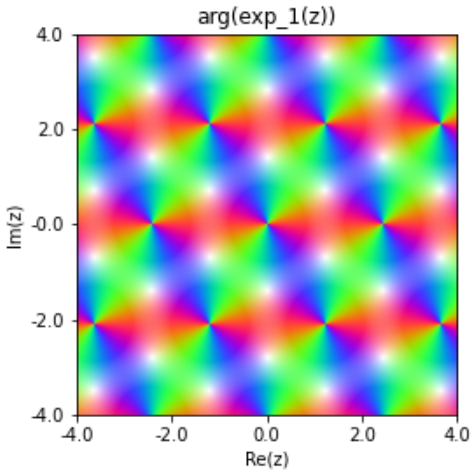

Figure 4.1: The first component of the exponential map for $A = 0$, $B = -1$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-4, 4]^2$

[1] More precisely, a complex number z is sent to the RGBA value with $R = (\cos(\arg(z)) + 1)/2$, $B = (\cos(\arg(z) + \frac{2\pi}{3}) + 1)/2$, $G = (\cos(\arg(z) + \frac{4\pi}{3}) + 1)/2$, and $A = \arctan(|z|)$. Because arctan can output values outside of $[0, 1]$, matplotlib clipped its output into that range. This was unintentional but aesthetically fortuitous.

[2] We cap the norm at a finite value so that the resulting heat map is easier to read.

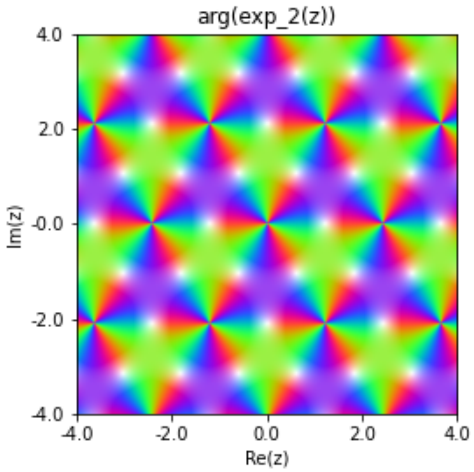

Figure 4.2: The second component of the exponential map for $A = 0$, $B = -1$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-4, 4]^2$

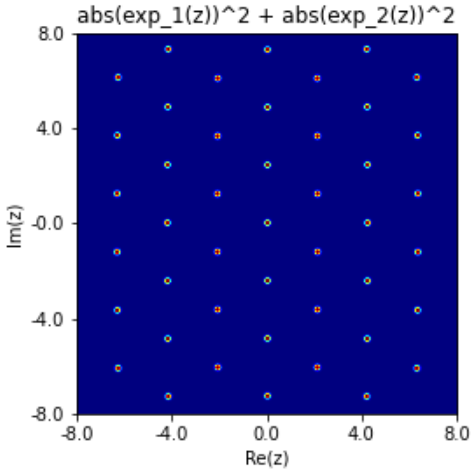

Figure 4.3: The kernel of the exponential map for $A = 0$, $B = -1$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-4, 4]^2$. The lattice being composed of equilateral triangles is to be expected, since it can be shown that the endomorphism ring of $y^2 = x^3 - 1$ is $\mathbb{Z}[\omega]$ for ω a cube root of unity (endomorphism rings and complex multiplication are explained in Chapter 5).

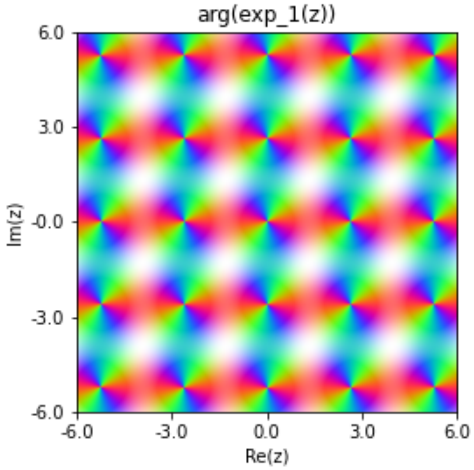

Figure 4.4: The first component of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-2, 2]^2$

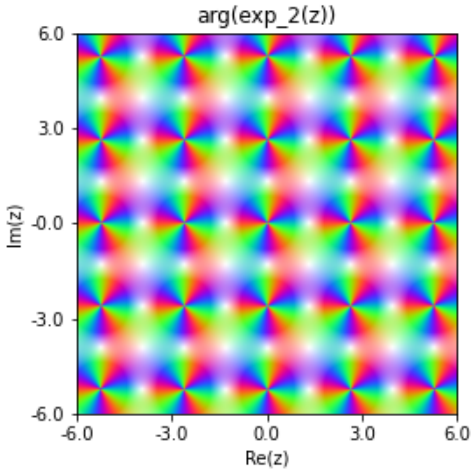

Figure 4.5: The second component of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-2, 2]^2$

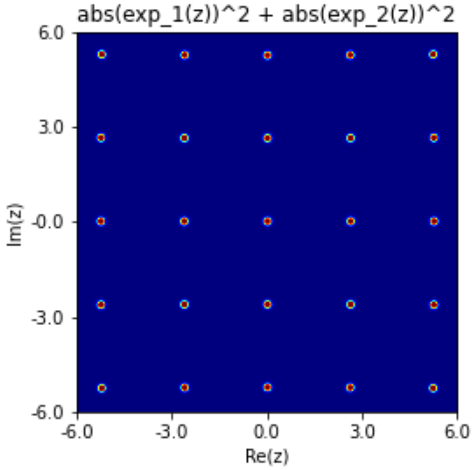

Figure 4.6: The kernel of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-2, 2]^2$

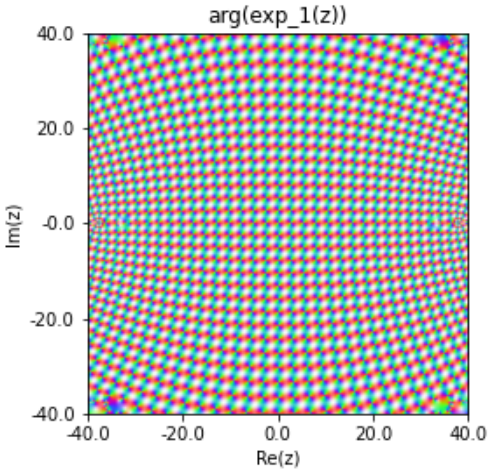

Figure 4.7: The first component of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-20, 20]^2$. Note the errors for large z.

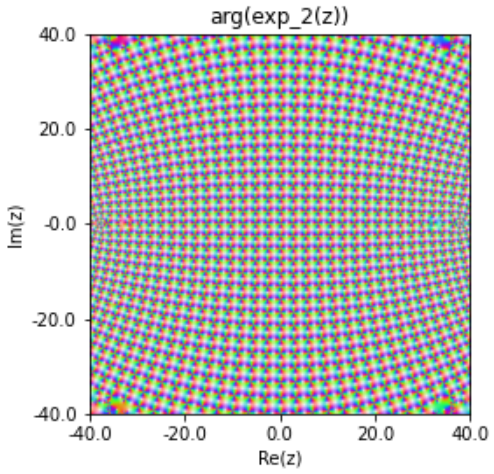

Figure 4.8: The second component of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-20, 20]^2$. Note the errors for large z.

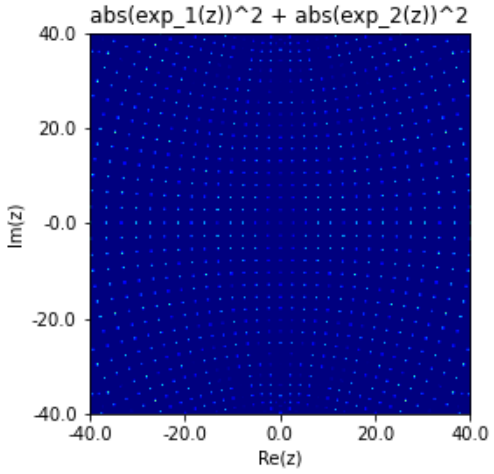

Figure 4.9: The kernel of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 8$, $(\Re(z), \Im(z)) \in [-20, 20]^2$. Note the errors for large z.

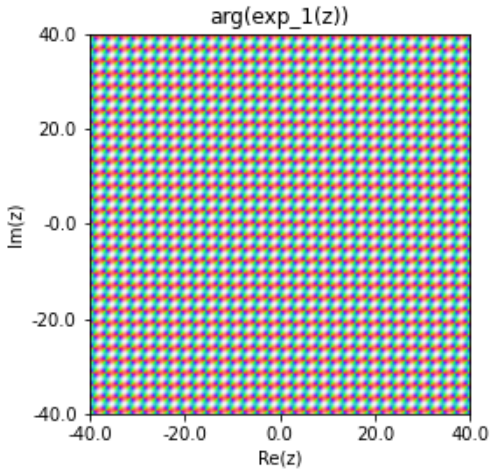

Figure 4.10: The first component of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 12$, $(\Re(z), \Im(z)) \in [-20, 20]^2$. Note the errors for large z have gone away.

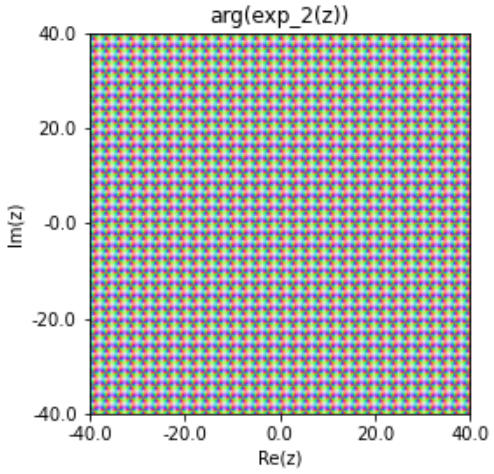

Figure 4.11: The second component of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 12$, $(\Re(z), \Im(z)) \in [-20, 20]^2$. Note the errors for large z have gone away.

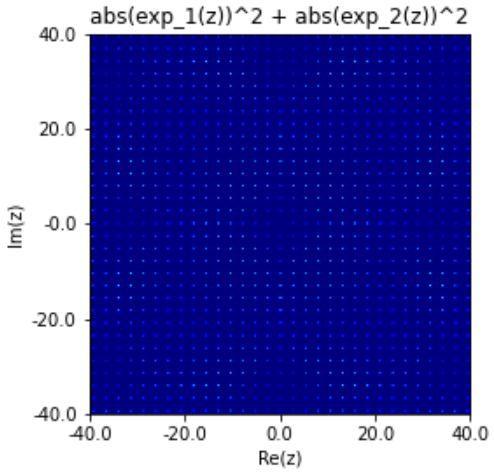

Figure 4.12: The poles of the exponential map for $A = -1$, $B = 0$, $P = (1, 0)$, $N = 12$, $(\Re(z), \Im(z)) \in [-20, 20]^2$. Note the errors for large z have gone away.

Chapter 5

Application of Lattices

Previously, we studied the exponential map on elliptic curves over $\mathbb{C}$ to show they are equivalent to complex tori. One nice aspect of this approach is how lattices naturally emerge as the kernel. In fact, we stress that lattices are very closely related to elliptic curves over $\mathbb{C}$. Here, we discuss some applications that illustrate this connection.

5.1 Elliptic Curves over Finite Fields

Let $\mathbb{F}_q$ denote a finite field of q elements. Consider the elliptic curve $\mathbb{E}(\mathbb{F}_q)$. Then, we see that $E(\mathbb{F}_q)$ is a finite abelian group. Here, we use the close connection between lattices and elliptic curves over $\mathbb{C}$ to describe elliptic curves over $\mathbb{F}_q$.

Proposition 2. *Let $E(\mathbb{F}_q)$ be any elliptic curve over $\mathbb{F}_q$. Also, let C_n denote the cyclic group with n elements. Then, we have*

$$E(\mathbb{F}_q) \cong C_n \text{ or } E(\mathbb{F}_q) \cong C_n \times C_m$$

for some integer $n \geq 1$ or integers $n, m \geq 1$ such that $n \mid m$.

Proof. By the classification theorem for finite abelian groups, we have

$$E(\mathbb{F}_q) \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}$$

for some integers $k \geq 1$ and $d_1, \ldots, d_k \geq 1$ such that $d_i \mid d_{i+1}$ for all $i \in \{1, 2, \ldots, k-1\}$. Let the function $[m] : E(\mathbb{F}_q) \to E(\mathbb{F}_q)$ given by

$$[m](x) = \underbrace{x + x + \cdots + x}_{m \text{ times}}$$

denote the multiplication by m map. First, consider the set

$$A = \{x \in E(\mathbb{F}_q) \mid [d_1](x) = \mathcal{O}\}.$$

Since C_{d_1} is cyclic, all d_1 points equal the identity when added to themselves d_1 times. Moreover, since $C_{d_1} \leq C_{d_i}$ for all $i \in \{1, 2, \ldots, k\}$, we see that each C_{d_i} contains d_1 such points. Hence, we conclude $|A| = d_1^k$. Moreover, A exactly gives roots of the map $[d_1]$.

Finally, we will show that $[d_1]$ over any field has at most d_1^2 distinct roots. The solutions of $[d_1](x) = \mathcal{O}$ come from the same rational polynomial regardless of the ambient field. Hence, the number of distinct solutions of $[d_1]$ over $\mathbb{F}_p$ is at most the number of distinct solutions over $\mathbb{C}$. In the complex case, we claim that $[d_1]$ has exactly d_1^2 roots. To see this, let $E = \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Also, let Λ be generated by $\omega_1, \omega_2 \in \mathbb{C}$. Then, the points in $\mathbb{C}/\Lambda$ that result in the identity when added to themselves d_1 times are exactly given by the points $(a\omega_1 + b\omega_2)/d_1$ where $a, b \in \{0, 1, \ldots, d_1 - 1\}$. One can see these give exactly d_1^2 points. Therefore, we have $d_1^k \leq d_1^2$ and thus $k \leq 2$. This concludes our proof. □

5.2 Endomorphisms of Elliptic Curves over $\mathbb{C}$

Let E denote an elliptic curve over $\mathbb{C}$. Since E is an abelian group, its endomorphisms form a ring, which we denote as $\mathrm{End}(E)$. It turns out that the geometry of the lattice corresponding to E exactly determines $\mathrm{End}(E)$. In this section, we will prove a precise statement of this phenomenon by closely following Chapter 10 of [Was08].

Recall that an endomorphism of E is a group homomorphism from E to itself given by rational functions. The most basic examples include the multiplication-by-m maps we discussed in the previous section. Again, they are given by

$$[m](x) = \underbrace{x +_E \cdots +_E x}_{m \text{ times}}.$$

Indeed, since E is an abelian group, one can easily check that $[m](x +_E y) = [m](x) +_E [m](y)$ for any $x, y \in E$. Moreover, we can extend the map to negative integers by defining $[-m](x) := [m](-x)$. Hence, we always have $\mathbb{Z} \subseteq \mathrm{End}(E)$, where each $m \in \mathbb{Z}$ corresponds to the map $[m]$.

In general, we have the following theorem.

Theorem 1. *Let E be an elliptic curve over $\mathbb{C}$ corresponding to the lattice Λ. Then,*

$$\mathrm{End}(E) \cong \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}.$$

Note that $\beta\Lambda$ is simply multiplying all elements of Λ by β. Moreover, say that β *preserves* Λ if and only if $\beta\Lambda \subseteq \Lambda$. Then, an alternate way of viewing the statement $\mathbb{Z} \subseteq \mathrm{End}(E)$ is noticing that stretching a lattice by an integer (and possibly flipping it) always preserves the original lattice. When the lattice has extra symmetry, we can preserve the lattice through actions other than stretching. For instance, rotating a square lattice by 90 degrees, which corresponds to multiplication by i, gives the same lattice as the original one. In the case that $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, we say that E has *complex multiplication*. We will consider elliptic curves with complex multiplication in the final part of this chapter.

We make one remark before proving theorem 1. Take any $\alpha : E \to E$ given by $(x, y) \mapsto (R_1(x, y), R_2(x, y))$. If α is an endomorphism, one can assume $(x, y) \mapsto (r_1(x), r_2(x)y)$ instead where $r_1(x), r_2(x)$ are rational functions. Hence, being an endomorphism requires a big restriction on functions from E to itself.

To check the above remark, assume E has Weierstrass form $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{C}$. Since $R_1(x, y)$ and $R_2(x, y)$ need to be rational functions and we can replace even powers of y by polynomials in x, we see that

$$R_1(x, y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}$$

where $p_1(x), \ldots, p_4(x)$ are polynomials in x. If we multiply both sides of the fraction by $p_3(x) - p_4(x)y$ and

again simplify, we get

$$R_1(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)},$$

where again $q_1(x), \ldots, q_3(x)$ are polynomials in x. One can conclude the same for $R_2(x,y)$.

For $(x,y) \in E$, recall that $-(x,y) = (x,-y)$. Since α is a homomorphism, we must have the relation $\alpha(x,-y) = -\alpha(x,y)$, which implies $R_1(x,-y) = R_1(x,y)$ and $R_2(x,-y) = -R_2(x,y)$. This shows that $q_2(x)$ above must equal the zero function, which gives $R_1(x,y) = r_1(x)$ for some rational function r_1. Similarly, we may conclude that $R_2(x,y) = r_2(x)y$ for some rational function r_2.

We now prove our main theorem of the section.

Proof of Theorem 1. First, we show that $\mathrm{End}(E) \subseteq \{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\}$. Take any $\alpha \in \mathrm{End}(E)$. Recall that $\varphi : \mathbb{C}/\Lambda \to E$ given by $z \mapsto (\wp(z), \wp'(z))$ is an isomorphism where $\wp$ is the Weierstrass $\wp$-function (or equivalently the exponential function we previously defined). Define $\tilde{\alpha} : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ by $z \mapsto \varphi^{-1}(\alpha(\varphi(z)))$. One can easily check that $\tilde{\alpha}$ is a homomorphism.

Restrict $\tilde{\alpha}$ to a small neighborhood U of $z = 0$ such that $\tilde{\alpha}$ is an analytic map from U to $\mathbb{C}$ where $\tilde{\alpha}(x+y) \equiv \tilde{\alpha}(x) + \tilde{\alpha}(y) \mod \Lambda$ for all $x, y \in U$. Shift the map so that $\tilde{\alpha}(0) = 0$. Then, for sufficiently small U, we can assume that

$$\tilde{\alpha}(x+y) = \tilde{\alpha}(x) + \tilde{\alpha}(y)$$

since both sides are close to zero and can differ only by $0 \in \Lambda$. Hence, for any $z \in U$, we have

$$\tilde{\alpha}'(z) = \lim_{h \to 0} \frac{\tilde{\alpha}(z+h) - \tilde{\alpha}(z)}{h} = \lim_{h \to 0} \frac{\tilde{\alpha}(h)}{h} = \tilde{\alpha}'(0).$$

Let $\beta = \tilde{\alpha}'(0)$. Then, we conclude that $\tilde{\alpha}(z) = \beta z$ for all $z \in U$.

Now pick an arbitrary $z \in \mathbb{C}$. Then, there exists an integer n such that $z/n \in U$. Hence, we have

$$\tilde{\alpha}(z) \equiv n\tilde{\alpha}(z/n) = \beta z \mod \Lambda.$$

Recall the definition of $\tilde{\alpha}$. If $z \in \Lambda$, we know that $\wp(z)$ maps to the identity and thus $\tilde{\alpha} \in \Lambda$. In other words, $\tilde{\alpha}(\Lambda) \subseteq \Lambda$. This gives $\beta\Lambda \subseteq \Lambda$ as desired.

Next, we show that $\{\beta \in \mathbb{C} \mid \beta\Lambda \subseteq \Lambda\} \subseteq \mathrm{End}(E)$. Take any $\beta \in \mathbb{C}$ such that $\beta\Lambda \subseteq \Lambda$. Then, multiplication by β gives a homomorphism $\beta : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$. Since $E \cong \mathbb{C}/\Lambda$, we wish to check the corresponding map on E is given by rational functions. Since $\beta\Lambda \subseteq \Lambda$, note that $\wp(\beta z)$ and $\wp'(\beta z)$ are doubly periodic with respect to Λ. A nice property of the Weierstrass $\wp$-function states that every doubly periodic function for Λ is a rational function of $\wp$ and $\wp'$. Hence, there exists rational functions R, S such that $\wp(\beta(z)) = R(\wp(z))$ and $\wp'(\beta(z)) = \wp'(z)S(\wp(z))$. In other words, β induces a map $[\beta] : E \to E$ given by $(\wp(z), \wp'(z)) \mapsto (\wp(\beta z), \wp'(\beta z))$, which is given by rational functions. To see it is a homomorphism, note that $[\beta](x) = \wp(\beta(\wp^{-1}(x)))$. This concludes our proof. □

5.3 Complex Multiplication

In this section, we give an example of complex multiplication. We further show how the previous theorem can be used to determine the endomorphism ring.

Consider the elliptic curve $y^2 = x^3 - x$ over $\mathbb{C}$. Then, $E \cong \mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z}\omega + \mathbb{Z}i\omega$ for some $\omega \in \mathbb{R}$. In particular, Λ is a square lattice. By the theorem above, we will show that $\mathrm{End}(E) \cong \mathbb{Z}[i]$, which implies

E has complex multiplication. Note that Λ is generated by ω and ωi. Take any $z \in \mathbb{C}$.

If $z \in \mathbb{Z}[i]$, then $z = a + bi$ for some $a, b \in \mathbb{Z}$. Hence, $\omega z = \omega(a + bi) \in \Lambda$. and $(\omega i)z = \omega(-b + ai) \in \Lambda$. Note that the generators are mapped to two new points in Λ. Since a lattice is closed under addition and multiplication by z is a linear transformation, we see that $z\Lambda \subseteq \Lambda$ as desired. This gives $\mathbb{Z}[i] \subseteq \mathrm{End}(E)$.

If $z \notin \mathbb{Z}[i]$, then without loss of generality we may assume $z = a + bi$ where $a \notin \mathbb{Z}$. Hence, we have $\omega z = \omega(a + bi) \notin \Lambda$. This shows that if $z \notin \mathbb{Z}[i]$, then $z\Lambda \nsubseteq \Lambda$. This gives $\mathrm{End}(E) \subseteq \mathbb{Z}[i]$.

Together, we have $\mathrm{End}(E) \cong \mathbb{Z}[i]$ as desired. The fact that E has complex multiplication corresponds to the fact that the square lattice Λ has extra symmetries than merely stretching the lattice by an integer. For instance, $i \in \mathrm{End}(E)$ corresponds to a 90-degree rotation. As a more interesting example, consider $i + 2 \in \mathrm{End}(E)$. Through the figure below, we provide a detailed picture of this endomorphism.

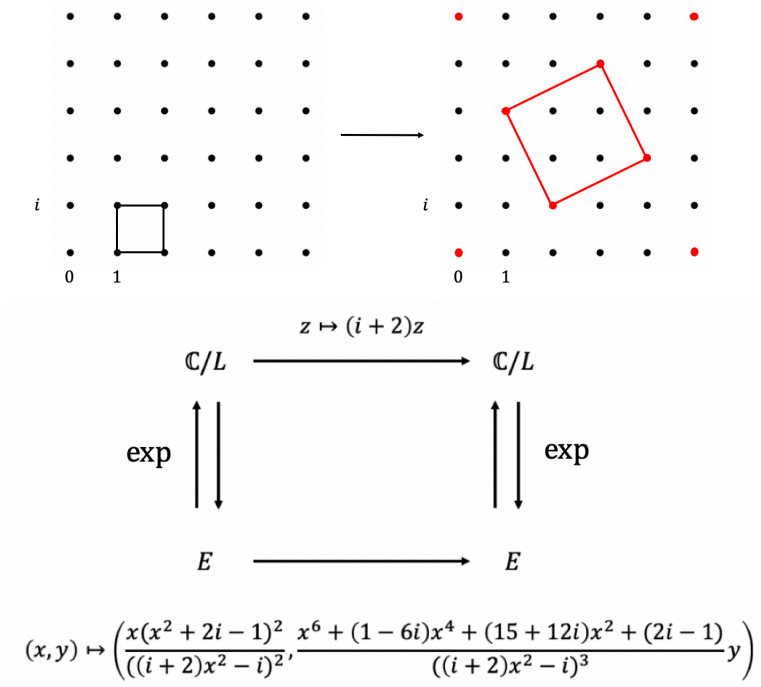

Figure 5.1: The endomorphism $i + 2$.

First, the picture above describes the endomorphism in $\mathbb{C}/\Lambda$. Here, the map is simply multiplication by $i+2$, and the points of Λ are mapped to the red points on the right, which form a subset of Λ. Geometrically, the map describes a certain "stretch-and-rotate" procedure. The map below describes the explicit endomorphism on the elliptic curve E. Note that the formula is given by rational functions. One can obtain the formula using $[i + 2](x) = [i](x) +_E [2](x)$.

Moreover, by definition, the degree of this endomorphism is the larger degree of the numerator and denominator of the first component of the image. In this case, we see that the degree is five. We can also understand this in the picture above. First, note that $\|i+2\| = 5$ and the unit square on the left is stretched to a square of area five. Alternatively, recall that all points of the lattice correspond to the kernel of the endomorphism. Hence, we see that the preimage of the red square on the right, which we can regard as the unit square on the left, contains five distinct points (with respect to Λ) that map to the kernel. Either way,

we check that the degree of the map is indeed five.

To conclude, the lattice picture of elliptic curves is especially nice since the rather complicated algebraic map on E can be interpreted as a simple geometric map on $\mathbb{C}/\Lambda$. The bridge that allows us to jump back and forth E and $\mathbb{C}/\Lambda$ is exactly the isomorphism between them given by the exponential map (or the Weierstrass $\wp$-function).

Appendix A

Mathematica Computations

The following pages contain the Mathematica code that was referenced in Section 3.5

In[24]:=
```
Normalx[x1, x2, y1, y2] := ((y2 - y1) / (x2 - x1))^2 - x1 - x2
```

In[25]:=
```
Normaly[x1, x2, y1, y2] := ((y2 - y1) / (x2 - x1)) * (x1 - Normalx[x1, x2, y1, y2]) - y1
```

The above functions give the x and y components of the group operation on the elliptic curve.

In[40]:=
```
(((y2 - y1) / (x2 - x1))^2 - x1 - x2) /. {x1 → (x0 + 2 * y0 * h + O[h]^2),
  x2 → x0, y1 → (y0 + (3 * x0^2 + A) h + O[h]^2), y2 → (-y0)}
```

Out[40]=

$$\frac{1}{h^2} + \frac{1}{O[h]}$$

In[27]:=
```
Normaly[x1, x2, y1, y2]
```

Out[27]=

$$-y1 + \frac{(-y1 + y2)\left(2\,x1 + x2 - \frac{(-y1+y2)^2}{(-x1+x2)^2}\right)}{-x1 + x2}$$

In[28]:=
```
(-y1 + ((-y1 + y2) (2 x1 + x2 - (-y1+y2)^2/(-x1+x2)^2)) / (-x1 + x2)) /.
  {x1 → x0 + 2 * y0 * h + O[h]^2, x2 → x0, y1 → y0 + (3 * x0^2 + A) h + O[h]^2, y2 → -y0}
```

Out[28]=

$$-\frac{1}{h^3} + \frac{1}{O[h]^2}$$

Here we use that $\exp(h) = \iota(h) + \mathcal{O}(h^2)$ to determine the orders and residues of the poles of $\tilde{\exp}_1(z)$ and $\tilde{\exp}_2(z)$.

In[44]:=
```
((y2 - y1) / (x2 - x1))^2 - x1 - x2) /. {x1 → E1[z], x2 → E1[h], y1 → E2[z], y2 → E2[h]}
```

Out[44]=

$$-E1[h] - E1[z] + \frac{(E2[h] - E2[z])^2}{(E1[h] - E1[z])^2}$$

In[45]:=
```
(-y1 + ((-y1 + y2) (2 x1 + x2 - (-y1+y2)^2/(-x1+x2)^2)) / (-x1 + x2)) /. {x1 → E1[z], x2 → E1[h], y1 → E2[z], y2 → E2[h]}
```

Out[45]=

$$\frac{\left(E1[h] + 2\,E1[z] - \frac{(E2[h]-E2[z])^2}{(E1[h]-E1[z])^2}\right)(E2[h] - E2[z])}{E1[h] - E1[z]} - E2[z]$$

The above cells compute that x and y components of $\tilde{\exp}(z) +_E \exp(h)$ (where E1[h] and E2[h] are the components of exp while E1[z] and E2[z] are the components of $\tilde{\exp}$.

In[46]:=
```
(((y2 - y1) / (x2 - x1))^2 - x1 - x2) /. {x1 → -E1[h] - E1[z] + (E2[h] - E2[z])^2 / (E1[h] - E1[z])^2,
  y1 → ((E1[h] + 2 E1[z] - (E2[h] - E2[z])^2 / (E1[h] - E1[z])^2) (E2[h] - E2[z])) / (E1[h] - E1[z]) - E2[z], x2 → x0, y2 → -y0}
```

Out[46]=

$$-x0 + E1[h] + E1[z] - \frac{(E2[h] - E2[z])^2}{(E1[h] - E1[z])^2} + \frac{\left(-y0 - \frac{\left(E1[h] + 2\,E1[z] - \frac{(E2[h] - E2[z])^2}{(E1[h] - E1[z])^2}\right)(E2[h] - E2[z])}{E1[h] - E1[z]} + E2[z]\right)^2}{\left(x0 + E1[h] + E1[z] - \frac{(E2[h] - E2[z])^2}{(E1[h] - E1[z])^2}\right)^2}$$

The above is the x component of $e\tilde{x}p(z) +_E \exp(h) -_E P$. We then take its series expansion with respect to h around $h = 0$, plug in what we know, and simplify in order to show that the derivative of the first component of $e\tilde{x}p$ is twice the second component.

In[47]:=
$$\text{Series}\left[-x0+E1[h]+E1[z]-\frac{(E2[h]-E2[z])^2}{(E1[h]-E1[z])^2}+\frac{\left(-y0-\frac{\left(E1[h]+2\,E1[z]-\frac{(E2[h]-E2[z])^2}{(E1[h]-E1[z])^2}\right)(E2[h]-E2[z])}{E1[h]-E1[z]}+E2[z]\right)^2}{\left(x0+E1[h]+E1[z]-\frac{(E2[h]-E2[z])^2}{(E1[h]-E1[z])^2}\right)^2},\{h,0,1\}\right]$$

Out[47]=
$$\left(-x0+E1[0]+E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}+\frac{\left(-y0-\frac{\left(E1[0]+2\,E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)(E2[0]-E2[z])}{E1[0]-E1[z]}+E2[z]\right)^2}{\left(x0+E1[0]+E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)^2}\right)+$$

$$\left(E1'[0]+\frac{2\,(E2[0]-E2[z])^2\,E1'[0]}{(E1[0]-E1[z])^3}-\frac{2\,(E2[0]-E2[z])\,E2'[0]}{(E1[0]-E1[z])^2}-\right.$$

$$\left(2\left(-y0-\frac{\left(E1[0]+2\,E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)(E2[0]-E2[z])}{E1[0]-E1[z]}+E2[z]\right)\right.$$

$$\left.\left.\left(E1'[0]+\frac{2\,(E2[0]-E2[z])^2\,E1'[0]}{(E1[0]-E1[z])^3}-\frac{2\,(E2[0]-E2[z])\,E2'[0]}{(E1[0]-E1[z])^2}\right)\right)\Big/$$

$$\left(x0+E1[0]+E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)^3+\frac{1}{\left(x0+E1[0]+E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)^2}$$

$$2\left(-y0-\frac{\left(E1[0]+2\,E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)(E2[0]-E2[z])}{E1[0]-E1[z]}+E2[z]\right)$$

$$\left(-\frac{\left(E1[0]+2\,E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)E2'[0]}{E1[0]-E1[z]}-\right.$$

$$(E2[0]-E2[z])\left(-\frac{\left(E1[0]+2\,E1[z]-\frac{(E2[0]-E2[z])^2}{(E1[0]-E1[z])^2}\right)E1'[0]}{(E1[0]-E1[z])^2}+\right.$$

$$\left.\left.\left.\frac{E1'[0]+\frac{2\,(E2[0]-E2[z])^2\,E1'[0]}{(E1[0]-E1[z])^3}-\frac{2\,(E2[0]-E2[z])\,E2'[0]}{(E1[0]-E1[z])^2}}{E1[0]-E1[z]}\right)\right)\right)h+O[h]^2$$

In[49]:=

$$\left(\mathrm{E1}'[0] + \frac{2\,(\mathrm{E2}[0]-\mathrm{E2}[z])^2\,\mathrm{E1}'[0]}{(\mathrm{E1}[0]-\mathrm{E1}[z])^3} - \frac{2\,(\mathrm{E2}[0]-\mathrm{E2}[z])\,\mathrm{E2}'[0]}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2} - \left(2\left(-y0 - \frac{\left(\mathrm{E1}[0]+2\,\mathrm{E1}[z]-\frac{(\mathrm{E2}[0]-\mathrm{E2}[z])^2}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}\right)(\mathrm{E2}[0]-\mathrm{E2}[z])}{\mathrm{E1}[0]-\mathrm{E1}[z]} + \mathrm{E2}[z]\right)\right)^2 \left(\mathrm{E1}'[0] + \frac{2\,(\mathrm{E2}[0]-\mathrm{E2}[z])^2\,\mathrm{E1}'[0]}{(\mathrm{E1}[0]-\mathrm{E1}[z])^3} - \frac{2\,(\mathrm{E2}[0]-\mathrm{E2}[z])\,\mathrm{E2}'[0]}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}\right)\right) \Big/$$

$$\left(\left(x0+\mathrm{E1}[0]+\mathrm{E1}[z]-\frac{(\mathrm{E2}[0]-\mathrm{E2}[z])^2}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}\right)^3 + \frac{1}{\left(x0+\mathrm{E1}[0]+\mathrm{E1}[z]-\frac{(\mathrm{E2}[0]-\mathrm{E2}[z])^2}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}\right)^2}\right.$$

$$2\left(-y0 - \frac{\left(\mathrm{E1}[0]+2\,\mathrm{E1}[z]-\frac{(\mathrm{E2}[0]-\mathrm{E2}[z])^2}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}\right)(\mathrm{E2}[0]-\mathrm{E2}[z])}{\mathrm{E1}[0]-\mathrm{E1}[z]} + \mathrm{E2}[z]\right)$$

$$\left(-\frac{\left(\mathrm{E1}[0]+2\,\mathrm{E1}[z]-\frac{(\mathrm{E2}[0]-\mathrm{E2}[z])^2}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}\right)\mathrm{E2}'[0]}{\mathrm{E1}[0]-\mathrm{E1}[z]} - (\mathrm{E2}[0]-\mathrm{E2}[z])\left(-\frac{\left(\mathrm{E1}[0]+2\,\mathrm{E1}[z]-\frac{(\mathrm{E2}[0]-\mathrm{E2}[z])^2}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}\right)\mathrm{E1}'[0]}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2} + \right.\right.$$

$$\left.\left.\left.\frac{\mathrm{E1}'[0]+\frac{2\,(\mathrm{E2}[0]-\mathrm{E2}[z])^2\,\mathrm{E1}'[0]}{(\mathrm{E1}[0]-\mathrm{E1}[z])^3}-\frac{2\,(\mathrm{E2}[0]-\mathrm{E2}[z])\,\mathrm{E2}'[0]}{(\mathrm{E1}[0]-\mathrm{E1}[z])^2}}{\mathrm{E1}[0]-\mathrm{E1}[z]}\right)\right)\right)\ /.$$

```
{E1'[0] → 2 y0, E2'[0] → 3 x0^2 + A, E1[0] → x0, E2[0] → y0}
```

In[52]:=
```
FullSimplify[2 y0 - 2 (A + 3 x0^2) (y0 - E2[z]) / (x0 - E1[z])^2 + 4 y0 (y0 - E2[z])^2 / (x0 - E1[z])^3 +
 1 / (2 x0 + E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2)^2 2 (
  - ((A + 3 x0^2) (x0 + 2 E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2)) / (x0 - E1[z]) -
   ((2 y0 - 2 (A + 3 x0^2) (y0 - E2[z]) / (x0 - E1[z])^2 + 4 y0 (y0 - E2[z])^2 / (x0 - E1[z])^3) / (x0 - E1[z])
    - 2 y0 (x0 + 2 E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2) / (x0 - E1[z])^2) (y0 - E2[z])) (
  - y0 - ((x0 + 2 E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2) (y0 - E2[z])) / (x0 - E1[z]) + E2[z]) -
 2 (2 y0 - 2 (A + 3 x0^2) (y0 - E2[z]) / (x0 - E1[z])^2 + 4 y0 (y0 - E2[z])^2 / (x0 - E1[z])^3) (
  - y0 - ((x0 + 2 E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2) (y0 - E2[z])) / (x0 - E1[z]) + E2[z])^2 /
  (2 x0 + E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2)^3,
 {y0^2 == x0^3 + A * x0 + B && E2[z]^2 == E1[z]^3 + A * E1[z] + B}]
```

Out[52]=
```
2 E2[z]
```

In[54]:=
```
(-x0 + E1[0] + E1[z] - (E2[0] - E2[z])^2 / (E1[0] - E1[z])^2 +
  (- y0 - ((E1[0] + 2 E1[z] - (E2[0] - E2[z])^2 / (E1[0] - E1[z])^2) (E2[0] - E2[z])) / (E1[0] - E1[z]) + E2[z])^2 /
   (x0 + E1[0] + E1[z] - (E2[0] - E2[z])^2 / (E1[0] - E1[z])^2)^2) /.
 {E1'[0] → 2 y0, E2'[0] → 3 x0^2 + A, E1[0] → x0, E2[0] → y0}
```

Out[54]=
```
E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2 +
 (- y0 - ((x0 + 2 E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2) (y0 - E2[z])) / (x0 - E1[z]) + E2[z])^2 /
  (2 x0 + E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2)^2
```

In[55]:=
```
FullSimplify[E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2 +
  (- y0 - ((x0 + 2 E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2) (y0 - E2[z])) / (x0 - E1[z]) + E2[z])^2 /
   (2 x0 + E1[z] - (y0 - E2[z])^2 / (x0 - E1[z])^2)^2,
 {y0^2 == x0^3 + A * x0 + B && E2[z]^2 == E1[z]^3 + A * E1[z] + B}]
```

Out[55]=
```
E1[z]
```

Bibliography

[Kni96] Oliver Knill. *A short introduction to several complex variables*. 1996. URL: https://people.math.harvard.edu/~knill/teaching/severalcomplex_1996/severalcomplex.pdf.

[CP03] H. CHANG and Nagabhushana Prabhu. "THE ANALYTIC DOMAIN IN THE IMPLICIT FUNCTION THEOREM". In: *JIPAM. Journal of Inequalities in Pure & Applied Mathematics [electronic only]* 4 (Jan. 2003).

[Wal08] Michel Waldschmidt. "Elliptic Functions and Transcendence". In: *Surveys in Number Theory*. Developments in Mathematics 17. Springer Verlag, 2008, pp. 143–188. URL: https://hal.archives-ouvertes.fr/hal-00407231.

[Was08] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition*. 2nd ed. Chapman & Hall/CRC, 2008. ISBN: 9781420071467.

[Gor11] Alexander Gorodnik. *Lie groups, algebraic groups and lattices*. 2011. URL: https://www.math.uzh.ch/gorodnik/papers/bedlewo.pdf.