ON GAUSSIAN INTEGER TORSION POINTS OF ELLIPTIC CURVES

by

Tannon N. Warnick

A Senior Honors Thesis Submitted to the Faculty of
The University of Utah
In Partial Fulfillment of the Requirements for the

Honors Degree in Bachelor of Science

In

Mathematics

Approved:

Gordan Savin, PhD Faculty Thesis Mentor	Tommaso de Fernex, PhD Chair, Department of Mathematics
Timothy Tribone, PhD Departmental Honors Liaison	Monisha Pasupathi, PhD Dean, Honors College

April 2026

Abstract

This thesis explores the arithmetic and geometric properties of torsion points on elliptic curves, with a specific focus on curves admitting complex multiplication by the ring of Gaussian integers, $\mathbb{Z}[i]$. We begin by establishing the foundational algebraic geometry of elliptic curves, utilizing the Riemann-Roch theorem to derive the general and short-form Weierstrass equations. After defining the geometric group law and the analytic isomorphism between the complex torus $\mathbb{C}/\Lambda$ and the curve $E(\mathbb{C})$, we provide a rigorous treatment of the torsion subgroup structure. The core of this work focuses on the construction and factorization of division polynomials. For the specific curve $y^2 = x^3 + x$, we derive explicit multiplication-by-π maps for Gaussian integers $\pi = n + im$. We demonstrate that the composite division polynomial satisfies $\Psi_\pi = \psi_\pi \psi_{\bar{\pi}}$ within $\mathbb{Z}[i][x]$. By applying the Eisenstein criterion over the Gaussian integers for, for primes p, $\pi\bar{\pi} = p \equiv 1 \pmod 4$, we show that the Galois group of the field extension of $\mathbb{Q}(i)$ generated by coordinates of π-torsion points in E is cyclic of order $p - 1$. These theoretical results are further supported by computational implementation in Python.

Contents

Abstract ii

List of Figures v

List of Tables v

1 Preliminaries on Elliptic Curves 1

1.1 Derivation of the Weierstrass Equation 1

1.1.1 The Riemann-Roch Theorem 1

1.1.2 Deriving the Weierstrass Equation 2

1.2 Projective Coordinates 3

1.2.1 The Point at Infinity 4

1.3 The Group Law 4

1.3.1 Geometric Addition 5

1.4 Structure of the Torsion Subgroup 7

2 Division Polynomials and Torsion Structure 11

2.1 Division Polynomials 11

2.2 Multiplication-by-n Map 16

3 Complex Multiplication and Special Maps 23

3.1 Derivation of the Gaussian Integer Multiplication Map 23

3.1.1 Derivation of Ψ_π and Φ_π 23

3.2 Arithmetic Properties and the Eisenstein Property 25

4 Abelian Extensions of $\mathbb{Q}(i)$ **30**

4.1 The Division Polynomial and x-Coordinate Extensions 30

4.2 The Full Abelian Extension via the y-Coordinate 33

A Computational Implementation **38**

A.1 Python Script for Division Polynomials 38

A.2 Computational Results 41

A.2.1 Factorization and Eisenstein Verification Table 41

B Properties of the Weierstrass $\wp$-function **43**

References **45**

List of Figures

1.1 Locus of a connected elliptic curve. 5
1.2 Locus of a two component elliptic curve. 6
1.3 Group addition on a curve with three roots. 7
1.4 Torus $\mathbb{C}/\Lambda$ with fundamental parallelogram. 10

List of Tables

A.1 Table of small factorizations of Ψ_π 42

Chapter 1

Preliminaries on Elliptic Curves

Before studying the arithmetic of torsion points of such curves, we must establish their geometric foundations. We begin by deriving the equation of the curve using the Riemann-Roch theorem, then explore the group law of these curves.

1.1 Derivation of the Weierstrass Equation

Since the central topic of this paper discusses Gaussian torsion points of elliptic curves, it may be helpful to define what we mean by an*elliptic curve*. An elliptic curve E has the typical definition as:

Definition 1.1. An *elliptic curve* is a non-singular projective algebraic curve of genus one, with an identity point $\mathcal{O}$.

Often these curves are encountered as cubic equations in the plane. However, their structure comes from a deeper theory of algebraic curves.

1.1.1 The Riemann-Roch Theorem

The Riemann-Roch theorem is the fundamental link between a curve's topological genus and its algebraic properties. It allows us to determine the dimension of the space of rational functions that have poles of a limited order at specific points.

A divisor on C is a sum of points

$$D = \sum_{P \in C} n_P P,$$

where all but finitely many n_P are zero.

Let C be a non-singular projective curve over an algebraically closed field $\bar{F}$. For a divisor D on C, let $\mathcal{L}(D)$ denote the space of rational functions f such that $(f) + D \geq 0$. The dimension of this space is denoted by $\ell(D)$. The Riemann-Roch theorem relates this dimension to the degree of the divisor and the genus of the curve.

Theorem 1.2 (Riemann-Roch)**.** *Let K be a canonical divisor on C. Then for any divisor D:*

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1 \tag{1.1}$$

Proof. A full proof of this theorem is beyond the scope of this thesis; however, a classical proof can be found in [Ful69], and a more modern proof can be found in [Har77]. □

To utilize the Riemann-Roch theorem, we must account for the term $\ell(K - D)$, where K is a *canonical divisor*. Geometrically, a canonical divisor K is the divisor associated with a non-zero meromorphic differential form ω on the curve C. It tracks the zeros and poles of ω, and its degree is a property of the curve it is defined on:

$$\deg(K) = 2g - 2. \tag{1.2}$$

For an elliptic curve, the genus is $g = 1$, which implies $\deg(K) = 2(1) - 2 = 0$. This vanishing degree is a powerful simplification. Because any divisor D with $\deg(D) > 0$ (such as our choice of $D = n\mathcal{O}$) results in a divisor $K - D$ with a negative degree, and since no non-zero rational function can have a divisor of negative degree, we find that $\ell(K - n\mathcal{O}) = 0$. This allows us to reduce the Riemann-Roch formula to the linear relation

$$\ell(n\mathcal{O}) = n,$$

which we use to construct the basis functions for the Weierstrass equation.

1.1.2 Deriving the Weierstrass Equation

We fix the point $\mathcal{O} \in E$ to serve as the identity element. We examine the spaces $\mathcal{L}(n\mathcal{O})$, consisting of functions with a pole at $\mathcal{O}$ of order at most n. We use the simplified Riemann-

Roch result from before, we construct a basis for functions on the curve: We now construct a basis for functions on the curve:

- n=1: $\ell(\mathcal{O}) = 1$. The only functions with no poles (or a pole of order 0) are constants. Basis: $\{1\}$.
- $n = 2$: $\ell(2\mathcal{O}) = 2$. We introduce a function x with a pole of order exactly 2 at $\mathcal{O}$. Basis: $\{1, x\}$.
- $n = 3$: $\ell(3\mathcal{O}) = 3$. We introduce a function y with a pole of order exactly 3 at $\mathcal{O}$. Basis: $\{1, x, y\}$.

The Linear Dependence

Consider the space for $n = 6$. By our formula, $\ell(6\mathcal{O}) = 6$. However, we can form the following seven functions using powers of x and y, all of which have pole orders less than or equal to 6:

$$\{1, x, y, x^2, xy, y^2, x^3\}$$

Since there are 7 vectors in a 6-dimensional space, they must be linearly dependent. Thus, there exist constants a_i such that:

$$y^2 + a_1xy + a_2y = a_3x^3 + a_4x^2 + a_5x + a_6, \quad a_i \in F. \tag{1.3}$$

Where F is some algebraically closed field. This is the general Weierstrass equation. By rescaling variables (assuming char $F \neq 2, 3$), we obtain the short form:

$$y^2 = x^3 + ax + b, \quad a, b \in F. \tag{1.4}$$

1.2 Projective Coordinates

The equation (1.4) describes the curve in the *affine plane* $\mathbb{A}^2$. However, elliptic curves are *projective* varieties [Sil09], meaning they must be closed and compact. The affine model is missing the point $\mathcal{O}$ (the pole of x and y).

To include this point, we embed the curve in the *projective plane* $\mathbb{P}^2$ using homogeneous coordinates $[X : Y : Z]$. The relationship to affine coordinates is:

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}$$

Here, Z acts as the homogenizing variable. Substituting these into (1.4) yields:

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 + a\left(\frac{X}{Z}\right) + b$$

Multiplying through by Z^3 to clear denominators gives the homogeneous Weierstrass equation:

$$Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{1.5}$$

1.2.1 The Point at Infinity

The "missing" point $\mathcal{O}$ corresponds to the location where $Z = 0$. Setting $Z = 0$ in the homogeneous equation:

$$Y^2(0) = X^3 \implies X = 0$$

In projective space, coordinates cannot be simultaneously zero, so $Y \neq 0$. We normalize to get the unique point at infinity:

$$\mathcal{O} = [0 : 1 : 0]$$

This is the geometric realization of the abstract point $\mathcal{O}$ used in our Riemann-Roch derivation. This is what we will use as the identity element for all curves in this thesis. The importance of this point is so that this is the only point we must consider as a three dimensional point, all other points in this paper will be x, y points but we must always remember $\mathcal{O}$ because it is not realized in the short Weierstrass equation.

1.3 The Group Law

A feature of elliptic curves is that their points form an abelian group (equivalently a $\mathbb{Z}$-module and in Chapter 3 we find some curves form $\mathbb{Z}[i]$-modules). To visualize this, consider

the curves $E : y^2 = x^3 - x$ and $C : y^2 = x^3 + x$. Notice that C has one root and E has three, these curves will look different on the plane, but their groups remains unaffected. The real loci in Figure 1.1 and Figure 1.2 on the following page give us a examples of what two elliptic curves look like.

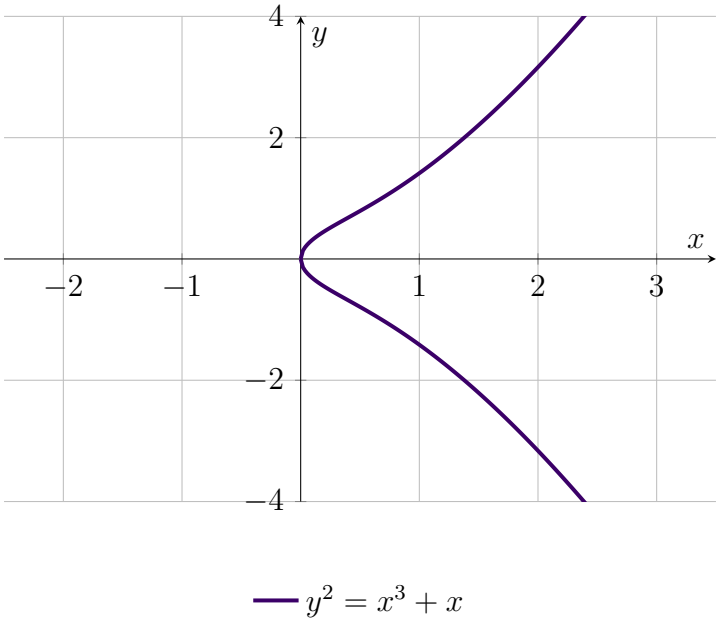

Figure 1.1: Locus of a connected elliptic curve.

1.3.1 Geometric Addition

For two points $P, Q \in E$, the sum $P + Q$ is defined geometrically:

1. Draw the line connecting P and Q (the secant line).

2. Let $P * Q$ be the third point of intersection which counting multiplicity is guaranteed by the fundamental theorem of algebra.

3. Reflect $P * Q$ across the x-axis to obtain $P + Q$.

This process is illustrated in Figure 1.3 on page 7. Notice that even though the curve has two separate components (because it has three real roots), the group law functions seamlessly across them.

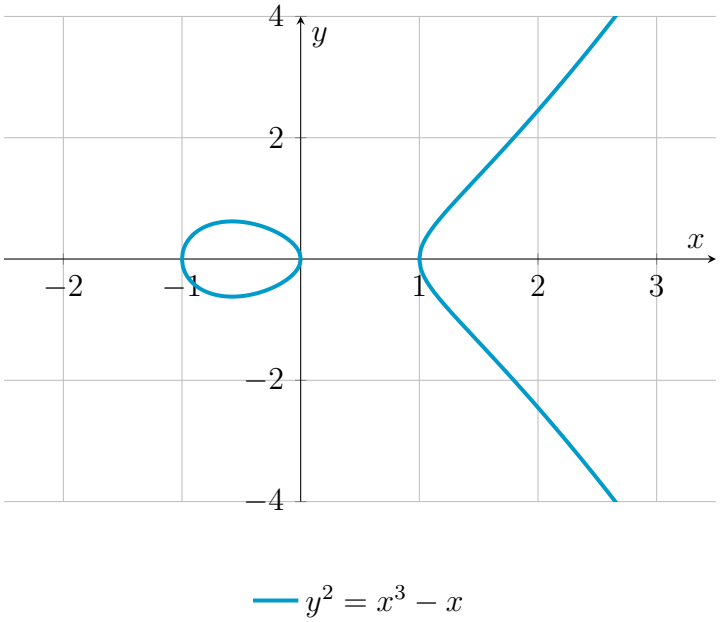

Figure 1.2: Locus of a two component elliptic curve.

Explicitly, on a curve given by the Weierstrass equation $C : y^2 = x^3 + ax + b$, and $P, Q \in C$, if $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, the coordinates of $P + Q$ are given by the algebraic formulas:

$$\begin{aligned} \lambda &= \frac{y_Q - y_P}{x_Q - x_P} \quad (P \neq Q), \\ x_{P+Q} &= \lambda^2 - x_P - x_Q, \\ y_{P+Q} &= \lambda(x_P - x_{P+Q}) - y_P. \end{aligned}$$

If $P = Q$ you follow the same procedure as before although since there is no secant line you must use implicit differentiation to find:

$$\lambda = \frac{3x^2 + a}{2y} \quad (P = Q).$$

From this we can define a map $[2] : C \to C$ which sends $P \mapsto [2]P = P + P$, is called the *point doubling map* and the formula:

$$x([2]P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b} \tag{1.6}$$

is called the point *doubling or duplication formula.*

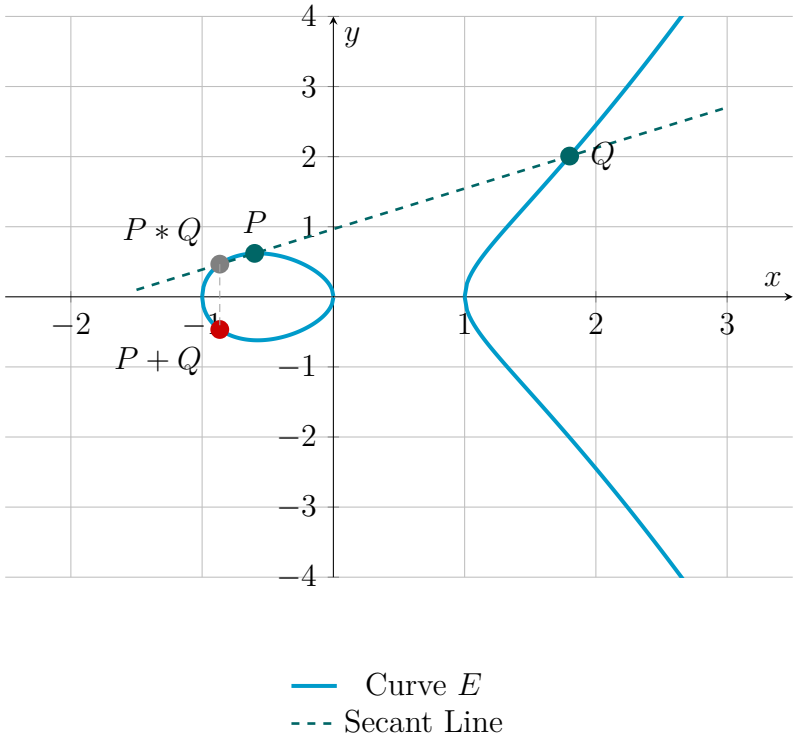

Figure 1.3: Group addition on a curve with three roots.

1.4 Structure of the Torsion Subgroup

Looking at the point doubling formula found in the previous section, we can find points of order two. A point of order two is a point P such that $[2]P = \mathcal{O}$; equivalently the set of two torsion points is the kernel of the map $[2]$. On the curve $y^2 = x^3 - x$ the points of order two are found by finding the roots of $4x^3 - 4x$. Factoring this we find $4x^3 - 4x = 4x(x+1)(x-1)$. Thus the x coordinates are $x = -1, 0, 1$. Plugging into the curve equation we find that $y = 0$ for each x. Additionally, $[2]\mathcal{O} = \mathcal{O}$, Thus we have found all two torsion points of the curve C,

$$C[2] = \{\mathcal{O}, (-1, 0), (0, 0), (1, 0)\}.$$

In this case we have a group of order 4. There are only two unique groups of order 4, $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. each element is of order two (by definition), so it must be isomorphic to

the Klein four-group. So we have shown that

$$C[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

The following theorem is the topic of this section and will give us insight into what all other torsion groups look like.

Theorem 1.3 (Structure of the Torsion Subgroup over $\mathbb{C}$)**.** *Let E be an elliptic curve over $\mathbb{C}$ and let n be a positive integer. The subgroup of n-torsion points $E[n]$ satisfies:*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

To understand the group structure of E, we first examine the analytic properties of the Weierstrass $\wp$-function. Given a lattice $\Lambda \subset \mathbb{C}$ generated by a basis $\{\omega_1, \omega_2\}$, the $\wp$-function is defined as follows:

Definition 1.4 (Weierstrass $\wp$-function)**.**

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

The function $\wp(z)$ is a meromorphic, doubly periodic function with respect to Λ, meaning $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Lambda$. It has a pole of order 2 at each lattice point and is even. This periodicity implies that $\wp$ is essentially a function defined on the quotient space $\mathbb{C}/\Lambda$. These properties are proven in Appendix B on page 43

The connection between this analytic construction and the algebraic geometry of elliptic curves is given by the map Ξ:

Proposition 1.5. *The map $\Xi : \mathbb{C}/\Lambda \to E(\mathbb{C})$ defined by*

$$\Xi(z) = \begin{cases} (\wp(z), \wp'(z)) & \text{if } z \notin \Lambda \\ \mathcal{O} & \text{if } x \in \Lambda \end{cases}$$

is an isomorphism of abelian groups.

Proof. To establish that Ξ is a group isomorphism, we verify three key properties: well-definedness, the homomorphism property, and bijectivity.

1. Well-definedness: The Weierstrass $\wp$-function and its derivative satisfy the algebraic relation:

$$(\wp'(z))^2 = 4\wp(z)^3 - a\wp(z) - b$$

for all $z \in \mathbb{C} \setminus \Lambda$. By definition, the image of any point $z \notin \Lambda$ under Ξ satisfies the affine equation of the elliptic curve E. Since $\Xi(\Lambda) = \mathcal{O}$ (the point at infinity), the map is well-defined from the quotient $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$.

2. Group Homomorphism: We must show that $\Xi(z_1 + z_2) = \Xi(z_1) + \Xi(z_2)$, where the right side follows the group law on E, and the left is the usual addition for complex numbers. Recall that $P_1 + P_2 + P_3 = \mathcal{O}$ on an elliptic curve if and only if the points are collinear.

Consider the elliptic function $f(z) = \wp'(z) - m\wp(z) - c$, where $y = mx + c$ is the line passing through $\Xi(z_1)$ and $\Xi(z_2)$. The function $f(z)$ has a triple pole at $z = 0$ and three zeros at z_1, z_2, and a third point z_3. According to the theory of elliptic functions, the sum of the zeros of a meromorphic function on a torus must be congruent to the sum of its poles modulo the lattice. Thus:

$$z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda}$$

This geometric alignment on the torus corresponds exactly to the collinearity condition on the curve, ensuring that Ξ preserves the group operation.

3. Bijectivity: For any $x \in \mathbb{C}$, the function $g(z) = \wp(z) - x$ is an elliptic function of order 2, meaning it takes the value x exactly twice in the fundamental domain (at some z_0 and $-z_0$). Since $\wp'(z)$ is an odd function, $\wp'(z_0)$ and $\wp'(-z_0)$ provide the two possible y-roots for the cubic $y^2 = 4x^3 - ax - b$. This ensures that every point (x, y) on the curve has a unique preimage $z \in \mathbb{C}/\Lambda$. Combined with $\Xi(0) = \mathcal{O}$, we conclude that Ξ is a bijection. □

Under the isomorphism Ξ, the n-torsion subgroup $E[n]$ corresponds exactly to the n-torsion subgroup of the torus, $(\mathbb{C}/\Lambda)[n]$. These are points on the fundamental parallelogram

shown in Figure 1.4 A point $z + \Lambda$ is an n-torsion point if and only if $nz \in \Lambda$. This requires:

$$nz = a\omega_1 + b\omega_2 \implies z = \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2$$

for some integers a, b. Distinguishing these points modulo Λ, we obtain the set:

$$(\mathbb{C}/\Lambda)[n] = \left\{ \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 + \Lambda : 0 \leq a, b < n \right\}.$$

This set is generated by the two independent elements $\frac{1}{n}\omega_1$ and $\frac{1}{n}\omega_2$, both of order n. Consequently, the group structure is $(\mathbb{C}/\Lambda)[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Since Ξ is a group isomorphism, it follows immediately that $E[n]$ shares this structure. Thus Theorem 1.3 on page 8 is proven.

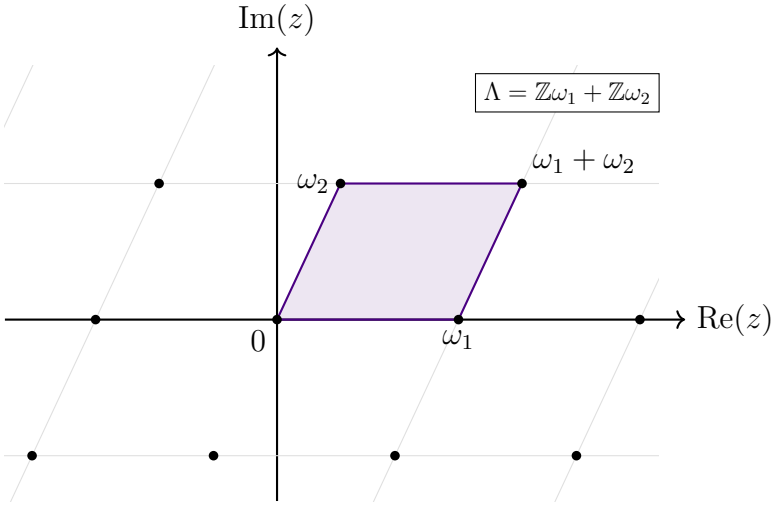

Figure 1.4: Torus $\mathbb{C}/\Lambda$ with fundamental parallelogram.

Chapter 2

Division Polynomials and Torsion Structure

Having established the geometric group law, we now turn to an algebraic characterization of the torsion points. To do this, we require a sequence of polynomials that vanish precisely at the points of order n. These are the division polynomials.

2.1 Division Polynomials

Let F be an algebraically closed field of characteristic different from 2 and 3. Let C be an elliptic curve given by the Weierstrass equation

$$C : y^2 = x^3 + ax + b, \quad a, b \in F.$$

In this section, we construct the division polynomials ψ_n, which are defined recursively and correspond to the multiplication-by-n map. We restrict our attention to curves with integer coefficients a and b, viewing them as defined over $\mathbb{Q}$, the field of fractions of $\mathbb{Z}$.

Definition 2.1. The *division polynomials* $\psi_n \in \mathbb{Z}[x, y]$ are defined recursively as follows:

Base Cases:

$$\psi_1 = 1,$$

$$\psi_2 = 2y,$$

$$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3).$$

Where $a, b \in \mathbb{Z}$.

Inductive Steps ($n \geq 2$):

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \tag{2.1}$$

$$2y\psi_{2n} = \psi_n \left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right). \tag{2.2}$$

To ensure the map is well-defined, we must verify that the recursive division by $2y$ yields a polynomial.

Proposition 2.2. *For all $m \geq 1$, $\psi_m \in \mathbb{Z}[x, y]$. Furthermore, considering ψ_m as a polynomial in variables x and y:*

1. *If m is odd, then $\psi_m \in \mathbb{Z}[x]$.*

2. *If m is even, then $\psi_m \in 2y \cdot \mathbb{Z}[x]$.*

Proof. We proceed by induction on m. The base cases $m = 1, 2, 3, 4$ satisfy the proposition by inspection. Assume the proposition holds for all integers $k < m$.

We first examine the recurrence for when m is even, letting $m = 2n$:

$$\psi_{2n} = \frac{\psi_n}{2y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right).$$

- **Case 1.1: m even, n even.** By the inductive assumption, ψ_n is a multiple of $2y$, so $\psi_n/2y \in \mathbb{Z}[x]$. Since n is even, $n \pm 2$ are even and $n \pm 1$ are odd. The expression in parentheses is of the form $2y \cdot f_1(x) - 2y \cdot f_2(x)$, thus $\psi_{2n} \in 2y\mathbb{Z}[x]$.

- **Case 1.2: m even, n odd.** Since n is odd, $\psi_n \in \mathbb{Z}[x]$. However, $n \pm 1$ are even, so they contain $2y$. The term in parentheses becomes $(\dots)(2y\dots)^2 - (\dots)(2y\dots)^2$, which is divisible by $4y^2$. Dividing by the external $2y$ leaves a factor of $2y$.

We now examine the case for when m is odd, letting $m = 2n + 1$:

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3.$$

- **Case 2.1:** m **odd,** n **even.** By the inductive assumption, $\psi_n, \psi_{n+2} \in 2y\mathbb{Z}[x]$. Thus $\psi_{n+2}\psi_n^3 = 16y^4 f$ for some $f \in \mathbb{Z}[x]$. Substituting $y^2 = x^3 + ax + b$ ensures the term is in $\mathbb{Z}[x]$. The same applies to the second term since $n \pm 1$ are odd.

- **Case 2.2:** m **odd,** n **odd.** By symmetry, the parities of the terms swap, but the result remains strictly in $\mathbb{Z}[x]$ after substituting for the y factors.

Thus, in any case, the proposition is fulfilled. □

This proposition is useful; in particular, when looking at (odd) prime torsion points, we need only look at roots of a univariate polynomial. A simple corollary describing the auxiliary polynomials defined by:

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1},$$

$$4y\omega_n = \psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2.$$

Corollary 2.3. *For every natural number* n*:*

i $\phi_n \in \mathbb{Z}[x]$.

ii $\omega_n \in y \cdot \mathbb{Z}[x]$ *for* n *odd, and* $\omega_n \in \mathbb{Z}[x]$ *for* n *even.*

Proof. We prove cases *i* and *ii* separately.

Proof of i. By definition $\phi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1}$. If n is odd, $\psi_n \in \mathbb{Z}[x]$ and $\psi_{n\pm1} \in 2y\mathbb{Z}[x]$, making $\psi_{n-1}\psi_{n+1} \in 4y^2\mathbb{Z}[x]$. If n is even, $\psi_n \in 2y\mathbb{Z}[x]$ and $\psi_{n\pm1} \in \mathbb{Z}[x]$. In both cases, y^2 substitutions leave $\phi_n \in \mathbb{Z}[x]$. □

We next prove the case for ω_n.

Proof of ii. We use the recurrence $\omega_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y}$. Also let f_n be defined by:

$$f_n = \begin{cases} \psi_n & \text{if } i \text{ odd,} \\ \psi_n/2y & \text{if } i \text{ even.} \end{cases}$$

We use this notation to emphasise the fact that $f_n \in \mathbb{Z}[x]$ for every n as proven before.

- **Subcase 2.1:** n **odd.** The numerator is of the form $4y^2(f)$ where

$$f = f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2.$$

We claim f is a function in $\mathbb{Z}[x]$. By Proposition 2.2, since n is even, f is of the form $(f_{n+2})\,(2y \cdot f_{n-1})^2 - (f_{n-2})\,(2y \cdot f_{n+1})^2 = 4y^2\,(f_{n+2})\,(f_{n-1})^2 - 4y^2\,(f_{n-2})\,(f_{n+1})^2 = 4y^2\left(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2\right)$. Dividing by $4y$ leaves $y \cdot \left(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2\right) \in y \cdot \mathbb{Z}[x]$.

- **Subcase 2.2:** n **even.** The numerator is of the form $2y(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2)$ where f_n is defined as above. Dividing by $4y$ yields

$$\frac{1}{2}(f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2). \tag{2.3}$$

To show this is in $\mathbb{Z}[x]$, we must show the $f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2$ is divisible by 2. By Lemma 2.4 which we have yet to prove, the reduction modulo 2 for f_{n+2} and f_{n-2} is given by:

$$\frac{n+2}{2}(x^2+a)^{\frac{((n+2)^2-4)}{4}} \pmod 2 = \left(\frac{n}{2}+1\right)\left(x^2+a\right)^{\frac{((n+2)^2-4)}{4}} \pmod 2$$

and

$$\frac{n-2}{2}(x^2+a)^{\frac{((n-2)^2-4)}{4}} = \left(\frac{n}{2}-1\right)\left(x^2+a\right)^{\frac{((n-2)^2-4)}{4}} \pmod 2$$

respectively. Since $(\frac{n}{2}+1) \equiv (\frac{n}{2}-1) \pmod 2$, we let $c \in \{0,1\}$ denote this common coefficient. Applying the congruences from the Lemma, we have:

$$f_{n\pm2} \equiv c(x^2+a)^{\frac{(n\pm2)^2-4}{4}} \pmod 2$$

$$f_{n\pm1}^2 \equiv \left((x^2+a)^{\frac{(n\pm1)^2-1}{4}}\right)^2 = (x^2+a)^{\frac{(n\pm1)^2-1}{2}} \pmod 2$$

Substituting these into the expression in (2.3) yields:

$$(2.3) \equiv c(x^2+a)^{\frac{n^2+4n}{4}}(x^2+a)^{\frac{n^2-2n}{2}} - c(x^2+a)^{\frac{n^2-4n}{4}}(x^2+a)^{\frac{n^2+2n}{2}} \pmod 2$$

By summing the exponents for the first term:

$$\frac{n^2 + 4n + 2(n^2 - 2n)}{4} = \frac{3n^2}{4}$$

And for the second term:

$$\frac{n^2 - 4n + 2(n^2 + 2n)}{4} = \frac{3n^2}{4}$$

Since the coefficients and the exponents are identical modulo 2, the terms cancel:

$$(2.3) \equiv c(x^2 + a)^{\frac{3n^2}{4}} - c(x^2 + a)^{\frac{3n^2}{4}} \equiv 0 \pmod 2$$

This confirms that 2.3 is divisible by 2, which cancels the remaining factor of 2 in the denominator of the recurrence for ω_n, ensuring $\omega_n \in \mathbb{Z}[x]$.

So we have proven for even and odd n cases for ω_n. □

Thus, assuming that Lemma 2.4 is true, we have proven both statements of the corollary. □

We now must prove for even n, $f_{n+2}f_{n-1}^2 - f_{n-2}f_{n+1}^2$ is congruent to $0 \pmod 2$.

Lemma 2.4. *For the division polynomials ψ_n associated with $y^2 = x^3+ax+b$, the following congruences hold modulo 2:*

1. *If n is odd, $\psi_n \equiv (x^2 + a)^{(n^2-1)/4} \pmod 2$.*
2. *If n is even, $f_n = \frac{\psi_n}{2y} \equiv \frac{n}{2}(x^2 + a)^{(n^2-4)/4} \pmod 2$.*

Proof. We proceed by induction on n. The base cases for small n are easily verified. Assume the lemma holds for all values up to $n - 1$.

Case 1: n **is odd.** Let $n = 2m + 1$. We use the recurrence:

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$$

- **Subcase 1.1:** m **is even.** Then m and $m + 2$ are even. By Proposition 2.2, ψ_m and ψ_{m+2} are both multiples of $2y$. Thus, $\psi_{m+2}\psi_m^3 \equiv 0 \pmod 2$. The expression reduces to:

$$\psi_{2m+1} \equiv \psi_{m-1}\psi_{m+1}^3 \pmod 2$$

Since $m \pm 1$ are odd, we apply the inductive assumption:

$$\psi_{2m+1} \equiv (x^2+a)^{\frac{(m-1)^2-1}{4}} \left((x^2+a)^{\frac{(m+1)^2-1}{4}}\right)^3 = (x^2+a)^{\frac{4m^2+4m}{4}} = (x^2+a)^{\frac{m^2-1}{4}}.$$

- **Subcase 1.2:** m **is odd.** Then $m-1$ and $m+1$ are even, making the second term vanish modulo 2. A symmetric calculation using $\psi_{m+2}\psi_m^3$ yields the same result (since $-1 \equiv 1 \pmod 2$).

Case 2: n **is even.** Let $n = 2m$. Let $f_{2m} = 2y\psi_{2m}$. We use the recurrence:

$$f_{2m} = \psi_m(f_{m-1}^2\psi_{m+2} - f_{m+1}^2\psi_{m-2})$$

- **Subcase 2.1:** m **is even.** By inductive assumption, $\psi_m \equiv 0 \pmod 2$ (since it contains a factor $2y$). Thus $f_{2m} \equiv 0 \pmod 2$, and $\frac{n}{2} = m \equiv 0 \pmod 2$. Matching the coefficient $\frac{n}{2}$.

- **Subcase 2.2:** m **is odd.** Then $\frac{n}{2} = m \equiv 1 \pmod 2$. Here ψ_m is odd, and exactly one of $\frac{m-1}{2}$ or $\frac{m+1}{2}$ is odd. If $\frac{m+1}{2}$ is odd, then $f_{m+1} \equiv (x^2+a)^{\cdots}$ and $f_{m-1} \equiv 0 \pmod 2$. The recurrence then simplifies to:

$$f_{2m} \equiv \psi_m f_{m+1}^2 \psi_{m-2} \pmod 2$$

Summing the exponents from the inductive assumption:

$$\frac{m^2-1}{4} + 2\frac{(m+1)^2-4}{4} + \frac{(m-2)^2-4}{4} = \frac{4m^2-4}{4} = m^2-1.$$

Since $m^2 - 1 = \frac{(2m)^2-4}{4}$, the congruence holds.

□

2.2 Multiplication-by-n Map

The results of the previous section give us insight on how nicely the division polynomials work. In this section we will discuss why these are important and are being studied. The following lemma shows us the degree of the leading term; again, this will be useful in the study of torsion points.

Lemma 2.5 (Degrees and Leading Terms, cf. [Was08, Lemma 3.5])**.** *For the division polynomials ψ_m and ϕ_m:*

1. *If m is odd, ψ_m is a polynomial in x with leading term $mx^{(m^2-1)/2}$.*
2. *If m is even, ψ_m is a polynomial in x multiplied by y, with leading term $myx^{(m^2-4)/2}$.*
3. *$\phi_m(x)$ is a polynomial in x of degree m^2 with leading coefficient 1.*

Proof. We proceed by induction on m. The base cases $m = 1, 2, 3, 4$ satisfy the lemma by inspection. Assume the lemma holds for all integers $k < m$.

We first examine the leading term of ψ_m. Consider the case where $m = 2n + 1$. The recurrence relation is:

$$\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$$

Assume n is even (the case for odd n is structurally identical). By the inductive assumption, the leading terms (lt) are:

$$\text{lt}(\psi_{n+2}) = (n+2)yx^{\frac{(n+2)^2-4}{2}}, \qquad \text{lt}(\psi_n) = nyx^{\frac{n^2-4}{2}}$$
$$\text{lt}(\psi_{n+1}) = (n+1)x^{\frac{(n+1)^2-1}{2}}, \qquad \text{lt}(\psi_{n-1}) = (n-1)x^{\frac{(n-1)^2-1}{2}}$$

Substituting these into the recurrence and substituting $y^2 = x^3$:

- The first term $\psi_{n+2}\psi_n^3$ has leading coefficient $(n+2)n^3$ and an x-exponent of $\frac{(n+2)^2-4}{2} + 3\left(\frac{n^2-4}{2}\right) + 6 = \frac{4n^2+4n}{2}$.
- The second term $\psi_{n-1}\psi_{n+1}^3$ has leading coefficient $(n-1)(n+1)^3$ and an x-exponent of $\frac{(n-1)^2-1}{2} + 3\left(\frac{(n+1)^2-1}{2}\right) = \frac{4n^2+4n}{2}$.

Subtracting the coefficients:

$$(n+2)n^3 - (n-1)(n+1)^3 = n^4 + 2n^3 - (n^4 + 2n^3 - 2n - 1) = 2n + 1$$

Thus, $\text{lt}(\psi_{2n+1}) = (2n+1)x^{\frac{(2n+1)^2-1}{2}} = mx^{\frac{m^2-1}{2}}$.

Next, we examine the case where $m = 2n$. The recurrence relation is:

$$\psi_{2n} = \frac{\psi_n}{2y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right)$$

Assume n is odd. By the inductive assumption:

$$\text{lt}(\psi_n) = nx^{\frac{n^2-1}{2}}$$

$$\text{lt}(\psi_{n+2}) = (n+2)x^{\frac{(n+2)^2-1}{2}}, \qquad \text{lt}(\psi_{n-1}) = (n-1)yx^{\frac{(n-1)^2-4}{2}},$$
$$\text{lt}(\psi_{n-2}) = (n-2)x^{\frac{(n-2)^2-1}{2}}, \qquad \text{lt}(\psi_{n+1}) = (n+1)yx^{\frac{(n+1)^2-4}{2}}.$$

Substituting these into the parentheses and using $y^2 = x^3$:

- **First term:** $\text{lt}(\psi_{n+2}\psi_{n-1}^2) = (n+2)(n-1)^2x^{\frac{(n+2)^2-1}{2}+(n-1)^2-4+3} = (n^3 - 3n + 2)x^{\frac{3n^2+3}{2}}$.
- **Second term:** $\text{lt}(\psi_{n-2}\psi_{n+1}^2) = (n-2)(n+1)^2x^{\frac{(n-2)^2-1}{2}+(n+1)^2-4+3} = (n^3 - 3n - 2)x^{\frac{3n^2+3}{2}}$.

The difference inside the parentheses is:

$$(n^3 - 3n + 2) - (n^3 - 3n - 2) = 4$$

So the bracketed term is $4x^{\frac{3n^2+3}{2}}$. Multiplying by the external factor:

$$\text{lt}(\psi_{2n}) = \left(\frac{nx^{\frac{n^2-1}{2}}}{2y}\right)\left(4x^{\frac{3n^2+3}{2}}\right) = \frac{2n}{y}x^{\frac{4n^2+2}{2}}$$

Multiplying the numerator and denominator by y gives $\frac{2ny}{y^2}x^{2n^2+1}$. Since $y^2 = x^3$, this simplifies exactly to:

$$\text{lt}(\psi_{2n}) = 2nyx^{2n^2-2} = myx^{\frac{m^2-4}{2}}$$

Next, we examine the case where $m = 2n$, and n is even: Here, ψ_n, ψ_{n+2}, and ψ_{n-2} are even-indexed (contain a y factor), while ψ_{n+1} and ψ_{n-1} are odd.

- $\text{lt}(\psi_{n+2}\psi_{n-1}^2) = (n+2)(n-1)^2yx^{\frac{(n+2)^2-4}{2}}x^{(n-1)^2-1} = (n^3 - 3n + 2)yx^{\frac{3n^2}{2}}$.

- $\text{lt}(\psi_{n-2}\psi_{n+1}^2) = (n-2)(n+1)^2 y x^{\frac{(n-2)^2-4}{2}} x^{(n+1)^2-1} = (n^3-3n-2)yx^{\frac{3n^2}{2}}$.

The difference inside the parentheses is $4yx^{\frac{3n^2}{2}}$. The external factor is $\frac{\text{lt}(\psi_n)}{2y} = \frac{nyx^{(n^2-4)/2}}{2y} = \frac{n}{2}x^{\frac{n^2-4}{2}}$ (the y factors cancel). Multiplying these together yields $2nyx^{\frac{4n^2-4}{2}} = myx^{\frac{m^2-4}{2}}$.

Both sub-cases yield the exact same leading term, confirming the inductive step for even m. This confirms the inductive step for all m.

Finally, we prove the case of ϕ_m. By definition, $\phi_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}$. If m is odd, ψ_{m-1} and ψ_{m+1} are even, so their product contains $y^2 = x^3$. If m is even, ψ_m^2 contains $y^2 = x^3$. In either case, calculating the leading terms using the previously established results gives:

- $\text{lt}(x\psi_m^2) = x \cdot \left(m^2 x^{m^2-1}\right) = m^2 x^{m^2}$.
- $\text{lt}(\psi_{m-1}\psi_{m+1}) = (m-1)(m+1)x^{\frac{(m-1)^2+(m+1)^2-2}{2}} = (m^2-1)x^{m^2}$.

Combining these results:

$$\text{lt}(\phi_m) = m^2 x^{m^2} - (m^2-1)x^{m^2} = x^{m^2}$$

Thus, ϕ_m is monic with degree m^2. □

A corollary to this lemma shows a stronger structure of the polynomials

Corollary 2.6. *On the curve $y^2 = x^3 - x$, and for odd m, $\psi_m = mx^{(m^2-1)/2} \ldots \pm 1$. In fact we claim that:*

- $\psi_m = mx^{(m^2-1)/2} \cdots + 1$ *for* $m \equiv 1 \pmod 4$
- $\psi_m = mx^{(m^2-1)/2} \cdots - 1$ *for* $m \equiv 3 \pmod 4$

Proof. We have proven in Lemma 2.5 that the leading coefficient is as shown. We now must prove the claim regarding the trailing coefficient. We prove this by induction on odd m. Note that it suffices to show that the constant term of ψ_m is $(-1)^{(m-1)/2}$.

For the base cases, from the definition of the curve $y^2 = x^3 - x$, we have $\psi_1 = 1$ and $\psi_3 = 3x^4 - 6x^2 - 1$. Their constant terms are 1 and -1, which perfectly match the formula for $m = 1$ and $m = 3$.

Let $m = 2n + 1$. Assume this condition holds for all odd division polynomials up to ψ_{2n-1}. We evaluate ψ_{2n+1} using the standard recurrence relation: $\psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$. This breaks into two cases based on the parity of n:

1. **Case 1:** n **is even.** Let $n = 2k$. Then our index is $m = 4k + 1 \equiv 1 \pmod 4$, and we must show the constant term is 1. As proven in Proposition 2.2, ψ_n has a factor of y because n is even. Consequently, the term $\psi_{n+2}\psi_n^3$ has no constant term. The constant term of ψ_{2n+1} is therefore entirely determined by $-\psi_{n-1}\psi_{n+1}^3$. Their constant terms are $(-1)^{(2k-2)/2} = (-1)^{k-1}$ and $(-1)^{(2k)/2} = (-1)^k$, respectively. Multiplying these gives $-(-1)^{k-1} \cdot ((-1)^k)^3 = -(-1)^{4k-1} = 1$.

2. **Case 2:** n **is odd.** Let $n = 2k + 1$. Then our index is $m = 4k + 3 \equiv 3 \pmod 4$, and we must show the constant term is -1. Here, $n + 1$ is even, so ψ_{n+1} has a factor of y. By the exact same logic as Case 1, the term $-\psi_{n-1}\psi_{n+1}^3$ has no constant term. The constant term of ψ_{2n+1} is therefore determined by $\psi_{n+2}\psi_n^3$. Their constant terms are $(-1)^{(2k+2)/2} = (-1)^{k+1}$ and $(-1)^{(2k)/2} = (-1)^k$, respectively. Multiplying these gives $(-1)^{k+1} \cdot ((-1)^k)^3 = (-1)^{4k+1} = -1$.

In both cases, the constant term matches our formula, completing the induction. □

We now have the tools to discuss the main objective of this chapter and motivation behind the study of division polynomials, that is we can define a general multiplication-by-n map for points on a curve.

Theorem 2.7. *Let $P = (x, y) \in C$ such that $nP \neq \mathcal{O}$. Then*

$$[n]P = \left(\frac{\phi_n(P)}{\psi_n(P)^2}, \frac{\omega_n(P)}{\psi_n(P)^3} \right).$$

Proof. We again use the powerful tool of induction on n. For $n = 1$, the statement is trivial since $\psi_1 = 1, \phi_1 = x, \omega_1 = y$. For $n = 2$, the formula follows immediately from the standard duplication formula on the Weierstrass curve. Recall from Section 1.3.1:

$$x([2]P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

Calculating ϕ_2/ψ_2^2 using the definitions $\phi_2 = x\psi_2^2 - \psi_3\psi_1$ and $\psi_2 = 2y$ yields:

$$x([2]P) = \frac{x^4 - 2ax^2 - 8bx + b^2}{4y^2}.$$

Notice the denominators are different but by substituting $y^2 = x^3+ax+b$ in the denominator, we find they are equivalent.

For the inductive step, we utilize the addition formulas. Specifically, we assume the formula holds for n and $n - 1$. From the group law, we have the relation:

$$x_{n+1} - x_{n-1} = -\frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}(x_n - x)^{-2},$$

where x_k denotes the x-coordinate of $[k]P$. By the definition of ϕ_n, we have $x_n = \phi_n/\psi_n^2$. Substituting this into the left-hand side and manipulating the recurrence relations (from (2.1) and (2.2)) allows us to verify that x_{n+1} satisfies the required form ϕ_{n+1}/ψ_{n+1}^2. The y-coordinate follows similarly from the fact that we are working from a curve $y^2 = x^3 + ax + b$ □

Corollary 2.8. *Let $n \in \mathbb{Z}^+$. A point $P = (x, y) \in C$ is an n-torsion point if and only if $\psi_n(P) = 0$. That is, the roots of the division polynomial ψ_n are exactly the x-coordinates of the points in $E[n] \setminus \{\mathcal{O}\}$.*

Proof. By definition, a point P is an n-torsion point if and only if $[n]P = \mathcal{O}$. In the context of the rational functions defined in Theorem 2.7, the point at infinity $\mathcal{O}$ corresponds to the pole of the coordinate functions. The x-coordinate of the multiplied point is given by the rational function:

$$x([n]P) = \frac{\phi_n(P)}{\psi_n(P)^2}.$$

If ϕ_n and ψ_n^2 shared a root P, then the map $[n]$ would be defined and finite at P, implying P is not an n-torsion point. However, in Section 1.4, we proved that $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which implies that $|E[n] \setminus \{\mathcal{O}\}| = n^2 - 1$.

Since ψ_n^2 is a polynomial in x of degree $n^2 - 1$, it has at most $n^2 - 1$ roots. Because each of the $n^2 - 1$ non-trivial torsion points must be a pole of the x-coordinate function, they must all be roots of the denominator. There is, therefore, no room for ϕ_n and ψ_n^2 to share a root. Consequently, the x-coordinate becomes infinite if and only if the denominator vanishes. Specifically:

$$[n]P = \mathcal{O} \iff \psi_n(P)^2 = 0 \iff \psi_n(P) = 0.$$

Thus, the non-trivial n-torsion points are precisely those points whose x-coordinates are roots of the n-th division polynomial ψ_n. □

With Corollary 2.8, the construction of the division polynomials is complete. We have shown that these recursively defined sequences provide a closed-form expression for the multiplication-by-n map. These torsion points and roots of division polynomials will be studied in more general in Chapter 4 on page 30.

Chapter 3

Complex Multiplication and Special Maps

In the previous chapter, we derived the multiplication maps for integers $[n]$. However, the specific curve $y^2 = x^3+x$ admits a larger ring of endomorphisms isomorphic to the Gaussian integers $\mathbb{Z}[i]$. In this chapter, we derive the explicit maps for these complex endomorphisms.

3.1 Derivation of the Gaussian Integer Multiplication Map

The curve $C : y^2 = x^3 + x$ possesses an automorphism defined by the imaginary unit i:

$$[i] : (x, y) \mapsto (-x, iy).$$

Consequently, there exist Gaussian torsion points such that for $\pi \in \mathbb{Z}[i]$, $[\pi]P = \mathcal{O}$.

Example 3.1. Consider $\pi = 1 + i$. A point P is in the kernel if $(1 + i)P = P + [i]P = \mathcal{O}$. The norm is $N(1 + i) = 2$, so these points lie inside $E[2]$.

3.1.1 Derivation of Ψ_π and Φ_π

Let $\pi = n + im$ be a Gaussian integer. The point $[\pi]P$ is given by $[\pi]P = nP + [i](mP)$. Let $P_1 = nP$ and $P_2 = [i](mP)$. Substituting the standard division polynomials:

$$P_1 = \left(\frac{\phi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right) \tag{3.1}$$

$$P_2 = [i]\left(\frac{\phi_m}{\psi_m^2}, \frac{\omega_m}{\psi_m^3}\right) = \left(-\frac{\phi_m}{\psi_m^2}, \frac{i\omega_m}{\psi_m^3}\right) \tag{3.2}$$

Using the addition law for $y^2 = x^3 + x$, the x-coordinate of the sum $P_3 = P_1 + P_2$ is:

$$x_3 = \frac{(x_1 + x_2)(1 + x_1x_2) - 2y_1y_2}{(x_2 - x_1)^2}.$$

The Denominator and Numerator

We now must substitute our x, y points from the n, mi derivations, to find $(n+mi)P = [\pi]P$. For simplicity sake, we will split this into numerator N and denominator D.

D: for this case we will look specifically at $(x_2 - x_1)^2$. Substituting from (3.1) and (3.2), we see:

$$D = (x_2 - x_1)^2 = \left(-\frac{\phi_m}{\psi_m^2} - \frac{\phi_n}{\psi_n^2}\right)^2 = \left(-\frac{\phi_m\psi_n^2 + \phi_n\psi_m^2}{\psi_m^2\psi_n^2}\right)^2 = \frac{(\phi_m\psi_n^2 + \phi_n\psi_m^2)^2}{\psi_m^4\psi_n^4}$$

N: for this case we will look at $(x_1 + x_2)(1 + x_1x_2) - 2y_1y_2$. Substituting, we see:

$$(x_1 + x_2)(1 + x_1x_2) - 2y_1y_2 = \left(\frac{\phi_n}{\psi_n^2} - \frac{\phi_m}{\psi_m^2}\right)\left(1 + \frac{\phi_n}{\psi_n^2} \cdot -\frac{\phi_m}{\psi_m^2}\right) - 2i\frac{\omega_n}{\psi_n^3} \cdot \frac{\omega_m}{\psi_m^3}.$$

Breaking this down even more we will look at the $(x_1 + x_2)$ term which simplifies as such:

$$\left(\frac{\phi_n}{\psi_n^2} - \frac{\phi_m}{\psi_m^2}\right) = \left(\frac{\phi_n\psi_m^2 - \phi_m\psi_n^2}{\psi_m^2\psi_n^2}\right) \tag{3.3}$$

Looking at $(1 + x_1x_2)$:

$$\left(1 + \frac{\phi_n}{\psi_n^2} \cdot -\frac{\phi_m}{\psi_m^2}\right) = \left(\frac{\psi_n^2\psi_m^2 - \phi_m\phi_n}{\psi_m^2\psi_n^2}\right) \tag{3.4}$$

We multiply (3.3) and (3.4):

$$\left(\frac{\phi_n\psi_m^2 - \phi_m\psi_n^2}{\psi_m^2\psi_n^2}\right) \cdot \left(\frac{\psi_n^2\psi_m^2 - \phi_m\phi_n}{\psi_m^2\psi_n^2}\right) = \\ = \frac{\phi_n\psi_n^2\psi_m^4 - \phi_m\psi_n^4\psi_m^2 - \phi_n^2\phi_m\psi_m^2 + \phi_m^2\phi_n\psi_n^2}{\psi_m^4\psi_n^4}$$

Finally we look at $2y_1y_2$:

$$2\left(\frac{\omega_n}{\psi_n^3}\right)\left(\frac{i\omega_m}{\psi_m^3}\right) = \frac{2i\omega_n\omega_m\psi_m\psi_n}{\psi_n^4\psi_m^4}$$

Adding this together we get

$$N = \frac{\phi_n\psi_n^2\psi_m^4 - \phi_m\psi_n^4\psi_m^2 - \phi_n^2\phi_m\psi_m^2 + \phi_n\phi_m^2\psi_n^2 - 2i\omega_n\omega_m\psi_n\psi_m}{\psi_m^4\psi_n^4}.$$

Notice that N and D have common denominators, put it all together to find $\frac{N}{D}$ yields:

$$x([\pi]P) = \frac{\phi_n\psi_n^2\psi_m^4 - \phi_m\psi_n^4\psi_m^2 - \phi_n^2\phi_m\psi_m^2 + \phi_n\phi_m^2\psi_n^2 - 2i\omega_n\omega_m\psi_n\psi_m}{(\phi_m\psi_n^2 + \phi_n\psi_m^2)^2}$$

While in the denominator $\sqrt{D} =: \Psi_\pi$ derived from the addition law correctly vanishes on the π-torsion points, its degree $N(\pi) - 1$ indicates that it is the product of the π-division polynomial and its conjugate, $\psi_\pi \cdot \psi_{\bar{\pi}}$. This is expected, as the x-coordinate addition law is symmetric with respect to π and $\bar{\pi}$. To apply the Eisenstein criterion, we must isolate the irreducible factor $\psi_\pi \in \mathbb{Z}[i][x]$ whose leading coefficient is π. As seen in the following examples, this factor possesses a constant term that is a unit in $\mathbb{Z}[i]$, while all intermediate coefficients are divisible by π. For completeness, we define:

$$\Psi_\pi := \phi_m\psi_n^2 + \phi_n\psi_m^2 \tag{3.5}$$

$$\Phi_\pi := \phi_n\psi_n^2\psi_m^4 - \phi_m\psi_n^4\psi_m^2 - \phi_n^2\phi_m\psi_m^2 + \phi_n\phi_m^2\psi_n^2 - 2i\omega_n\omega_m\psi_n\psi_m. \tag{3.6}$$

We derive Ω_π from our x value, substituting into our curve equation.

$$\begin{aligned}\Omega_\pi = {} & \omega_n\psi_m\left[\psi_m^2(\phi_n\psi_m^2 + \phi_m\psi_n^2)^2 - (\phi_n\psi_m^2 - \phi_m\psi_n^2)^2\right] \\ & - i\omega_m\psi_n\left[\psi_n^2(\phi_n\psi_m^2 + \phi_m\psi_n^2)^2 - (\phi_n\psi_m^2 - \phi_m\psi_n^2)^2\right] \\ & + 4i\omega_n\omega_m(\phi_n\psi_m^2 + \phi_m\psi_n^2).\end{aligned} \tag{3.7}$$

So we have derived a map:

$$[\pi]P = \left(\frac{\Phi_\pi}{\Psi_\pi^2}, \frac{\Omega_\pi}{\Psi_\pi^3}\right).$$

3.2 Arithmetic Properties and the Eisenstein Property

We now examine the reduction of Ψ_π. This serves as the foundation for proving that the torsion fields generate totally ramified extensions. Using a computer for prime π, we

compute[1] Ψ_{1+2i} and Ψ_{2+3i}. This script simply uses induction to find all ψ_n needed and does the multiplication as defined for Ψ_π

$$\begin{aligned}\Psi_{1+2i} &= 5x^4 + 2x^2 + 1,\\ \Psi_{2+3i} &= 13x^{12} - 26x^{10} + 39x^8 + 228x^6 + 235x^4 + 22x^2 + 1.\end{aligned}$$

Ψ_{1+2i} can be factored into $((1+2i)x^2+1)((1-2i)x^2+1)$. These factors clearly are irreducible by Eisenstein criterion with prime $\pi = 1+2i$ and $\bar{\pi}$ respectively. Ψ_{2+3i} can be factored as such:

$$\begin{aligned}\Psi_{2+3i} = ((2+3i)x^6 + (4-7i)x^4 + (10-11i)x^2 - i)\cdot\\ \cdot ((2-3i)x^6 + (4+7i)x^4 + (10+11i)x^2 + i).\end{aligned}$$

We will show that this satisfies Eisenstein criterion. We check individually that $(4-7i) \mid (2+3i)$, and $(10-11i) \mid (2+3i)$. Calculating $(2+3i)(-1-2i) = (4-7i)$ this implies that $(4-7i) \mid (2+3i)$, calculate $(2+3i)(-1-4i) = (10+11i)$. Thus $(2+3i)$ (which is a Gaussian prime) divides all but the constant coefficient and $\pi^2 \nmid \pi$, so it satisfies Eisenstein. The same calculation can be done on the second factor, we claim that all coefficients are complex conjugates of the first factor.

Thus we claim that $\Psi_\pi = \psi_\pi \psi_{\bar{\pi}}$ where ψ_π is irreducible for Gaussian prime π. In order to prove this, we must first show that Ψ can be split into these polynomials and that these two factors are irreducible.

A point P is a torsion point of Ψ_π if and only if $x([m]P + [ni]P)$ vanishes. Thus occurs if and only if $[m]P + [ni]P = \mathcal{O}$

We would like to study how this torsion group looks and how we can interact with it. The following theorem builds from Theorem 1.3 on page 8.

Theorem 3.2 (Structure of the Gaussian Torsion Subgroup)**.** *For p-torsion points on the curve $y^2 = x^3 + x$:*

[1]The python script used for calculating can be found in Appendix A on page 38

(1) If $p \equiv 1 \pmod 4$, the p-torsion subgroup is

$$E[p] \cong E[\pi] \oplus E[\bar{\pi}]$$

for Gaussian integer π such that $p = \pi\bar{\pi}$.

(2) If $p \equiv 3 \pmod 4$, the p-torsion subgroup is indecomposable.

Proof. We first consider the case (1). Let $V = E[p]$. Consider the multiplication by i map we have been studying in this section. $[i]P = (-x, iy)$, taking this map twice $[i]^2P = (x, -y) = -P$, thus $[i]^2 = [-1]$. Think of the multiplication by i map as a matrix:

$$[i]^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

Thus $[i]^2 + I = 0$, finding eigenvalues and eigenvectors of this matrix leads to the characteristic polynomial $\varphi^2 + 1 = 0$ for some φ. Since $p \equiv 1 \pmod 2$, there exists some λ such that $\lambda^2 \equiv -1 \pmod p$ (i.e. $\varphi^2 + 1 = (\varphi - \lambda)(\varphi + \lambda)$.) Thus the eigenvalues are $\lambda, -\lambda$ and since they are distinct (since $\lambda \neq 0$), they are linearly independent, and:

$$V_\lambda = \{P \in E[p] \mid [i]P = \lambda P\}$$
$$V_{-\lambda} = \{P \in E[p] \mid [i]P = -\lambda P\}.$$

Thus for V_λ, $[i]P = [\lambda]P$ this implies $[i]P - [\lambda]P = 0$. So $V_\lambda = \ker([i] - [\lambda])$. Similarly for $V_{-\lambda} = \ker([i] + [\lambda])$. The map $[i] + [\lambda]$ corresponds to π, and the map $[i] - [\lambda]$ to $\bar{\pi}$. Thus $V_\lambda = E[\pi]$ and $V_{-\lambda} = E[\bar{\pi}]$. Since $E[\pi]$ and $E[\bar{\pi}]$ are linearly independent eigenspaces:

$$E[p] \cong E[\pi] \oplus E[\bar{\pi}].$$

We now consider the case (2). Let $V = E[p]$. Since p is a prime not dividing the discriminant of the curve, V is a 2-dimensional vector space over the finite field $\mathbb{F}_p$. The endomorphism $[i]$ acts as a linear transformation $\phi : V \to V$ satisfying the relation $\phi^2 + I = 0$.

The minimal polynomial of ϕ is $P(\varphi) = \varphi^2 + 1$. For V to be decomposable as a $\mathbb{Z}[i]$-module, it must possess a 1-dimensional invariant subspace (a line) $W \subset V$ such that

$\phi(W) \subseteq W$. The existence of such a subspace is equivalent to ϕ having an eigenvalue $\lambda \in \mathbb{F}_p$.

However, the eigenvalues of ϕ are the roots of $\varphi^2 \equiv -1 \pmod{p}$. However, -1 is a quadratic non-residue for all primes $p \equiv 3 \pmod{4}$. Consequently, $\varphi^2 + 1$ is irreducible over $\mathbb{F}_p$, and ϕ has no eigenvectors in V. Since there are no proper non-trivial invariant subspaces, V is indecomposable. In fact, V is a simple $\mathbb{Z}[i]$-module in this case. □

This will be required in order to show that Ψ is reducible. We finally will prove the main theorem of this chapter.

Theorem 3.3. *For a Gaussian prime $\pi \in \mathbb{Z}[i]$, the polynomial Ψ_π factors as $\Psi_\pi = \psi_\pi \psi_{\bar{\pi}}$ in $\mathbb{Z}[i][x]$. Furthermore, the factor ψ_π is irreducible over $\mathbb{Z}[i]$.*

Proof. By Theorem 3.2, the p-torsion subgroup for $p = \pi\bar{\pi}$ decomposes into the direct sum of the kernels of the maps $[\pi]$ and $[\bar{\pi}]$:

$$E[p] \cong E[\pi] \oplus E[\bar{\pi}].$$

The roots of the division polynomial Ψ_π are precisely the x-coordinates of the non-trivial points in $E[p]$. Since the x-coordinate map is symmetric with respect to the eigenspaces of $[i]$ and $[-i]$, the polynomial must partition into factors corresponding to these subspaces. We define $\psi_\pi \in \mathbb{Z}[i][x]$ to be the polynomial whose roots are the x-coordinates of the points in $E[\pi] \setminus \{\mathcal{O}\}$. Because the map $[\pi]$ is defined over $\mathbb{Z}[i]$, the coefficients of ψ_π lie in the Gaussian integers. Thus $\Psi_\pi = \psi_\pi \psi_{\bar{\pi}}$.

We show that ψ_π satisfies the Eisenstein Criterion over the $\mathbb{Z}[i]$ with respect to the prime element π:

1. **Leading Coefficient:** The leading coefficient of the π-division polynomial is π (up to a unit). Since π is prime in $\mathbb{Z}[i]$, it follows that $\pi \mid \pi$ but $\pi^2 \nmid \pi$.

2. **Intermediate Coefficients:** Let $\tilde{E}$ be the reduction of the curve E modulo the prime ideal (π) over the finite field $\mathbb{F}_p$, where $p = N(\pi)$. The reduction of the

endomorphism $[\pi]$, denoted $\widetilde{[\pi]}$, is the p-th power Frobenius endomorphism [Sil94, Chapter II, Proposition 5.3]:

$$\widetilde{[\pi]} : (x, y) \mapsto (x^p, y^p).$$

The Frobenius map $\widetilde{[\pi]}$ is a purely inseparable morphism of degree p. A fundamental property of purely inseparable maps is that their kernel consists only of the identity element $\mathcal{O}$ with multiplicity. Consequently, $\widetilde{[\pi]}(P) = \mathcal{O}$ for all points $P \in \tilde{E}(\overline{\mathbb{F}}_p)$.

3. **Constant Term:** By Corollary 2.6, the trailing coefficient of the division polynomials for this curve is a unit in $\mathbb{Z}[i]$ (specifically ± 1 or $\pm i$). Since units are not divisible by any prime in $\mathbb{Z}[i]$, we have $\pi \nmid \psi_\pi(0)$.

Having satisfied these conditions, ψ_π is irreducible over $\mathbb{Z}[i]$. By symmetry of the complex conjugation map, $\psi_{\bar{\pi}}$ is likewise irreducible. □

Thus we have constructed a polynomial ψ_π such that it is irreducible and whose roots correspond to Gaussian prime torsion points on the curve $y^2 = x^3 + x$

Chapter 4

Abelian Extensions of $\mathbb{Q}(i)$

In this chapter, we explore the utility of the division polynomials ψ_π derived in Chapter 3. We demonstrate that the coordinates of the π-torsion points generate specific field extensions over $\mathbb{Q}(i)$ and that we can precisely control the degree of these extensions.

4.1 The Division Polynomial and x-Coordinate Extensions

We first establish a structural property of the division polynomial ψ_π, which connects to the geometric symmetries of the curve E. In particular, the complex multiplication map $[i]$ induces the transformation $x \mapsto -x$ on the x-coordinates.

Proposition 4.1. *The roots of the π-division polynomial $\psi_\pi(x)$ for $E : y^2 = x^3 + x$ are closed under the map $x \mapsto -x$. Consequently, $\psi_\pi(x)$ is an even polynomial and can be factored into terms of the form $(x^2 - x_j^2)$.*

Proof. Let x_j be the x-coordinate of a point $P \in E[\pi] \setminus \{\mathcal{O}\}$. Since $E[\pi]$ is a $\mathbb{Z}[i]$-module, if $P \in E[\pi]$, then $[i]P \in E[\pi]$. For the curve $E : y^2 = x^3 + x$, the complex multiplication map $[i]$ acts on the coordinates by $[i](x, y) = (-x, iy)$. Thus, the x-coordinate of $[i]P$ is $-x_j$. Since $[i]P$ is also a π-torsion point, its x-coordinate $-x_j$ must also be a root of $\psi_\pi(x)$. This shows that roots occur in pairs $\pm x_j$. Therefore, $\psi_\pi(x)$ is an even polynomial, leading to the factored form $\prod(x^2 - x_j^2)$. □

With the structure of the roots established, we now demonstrate that the field extension constructed from these x-coordinates is independent of the specific root chosen.

Theorem 4.2. *Let x_j and x_k be any two roots of the irreducible π-division polynomial $\psi_\pi(x)$. Then $K(x_j) = K(x_k)$.*

Proof. Let $P_j = (x_j, y_j)$ and $P_k = (x_k, y_k)$ be the corresponding π-torsion points on E. Because π is a Gaussian prime, the quotient ring $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$ is a finite field. Furthermore, the π-torsion subgroup $E[\pi]$ acts as a 1-dimensional vector space over this field.

Since x_j and x_k are roots of the irreducible division polynomial, P_j and P_k are non-trivial torsion points ($P \neq \mathcal{O}$). In a 1-dimensional vector space, any non-zero element serves as a basis. Therefore, P_k must be a scalar multiple of P_j by some non-zero scalar. Thus, there exists a unit $\alpha \in (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$ such that $P_k = [\alpha]P_j$.

As established in Section 3.1.1 on page 23, the x-coordinate of $[\alpha]P_j$ is a K-rational function of x_j:

$$x_k = \frac{\phi_\alpha(x_j)}{\psi_\alpha^2(x_j)}$$

This implies $x_k \in K(x_j)$ for all roots x_k. Since $K(x_j)$ contains all roots of the irreducible polynomial $\psi_\pi(x)$, it is the splitting field over K. Therefore, the extension $K(x_j)/K$ is a Galois extension. Because any root generates the splitting field, $K(x_j) = K(x_k)$. □

Before determining the Galois group, we must formally establish the degree of the field extension generated by the x-coordinate by analyzing the degree of the division polynomial.

Lemma 4.3. *Let $K = \mathbb{Q}(i)$ and let x_1 be a root of the irreducible π-division polynomial $\psi_\pi(x)$. Then the degree of the extension is*

$$[K(x_1) : K] = \frac{N(\pi) - 1}{2}.$$

Proof. Because we established in Chapter 3 that $\psi_\pi(x)$ is irreducible over K, it serves as the minimal polynomial for x_1. A fundamental property of field extensions dictates that $[K(x_1) : K] = \deg(\psi_\pi)$. We will determine this degree algebraically using the leading terms established in Lemma 2.5.

Recall from Section 3.1.1 that for $\pi = n + im$, the composite polynomial is defined as:

$$\Psi_\pi = \phi_m\psi_n^2 + \phi_n\psi_m^2$$

By Lemma 2.5, for any integer k, the polynomial $\phi_k(x)$ has degree k^2.

We now determine the x-degree of $\psi_k^2(x)$. If k is odd, $\psi_k(x)$ has degree $\frac{k^2-1}{2}$, making the degree of its square exactly k^2-1. If k is even, $\psi_k(x,y)$ has a leading term of the form $yx^{(k^2-4)/2}$. Squaring this yields $y^2x^{k^2-4}$. Substituting the curve equation $y^2 = x^3 + x$, the highest power of x becomes $x^3 \cdot x^{k^2-4} = x^{k^2-1}$. Thus, for any k, $\deg_x(\psi_k^2) = k^2 - 1$.

We can now find the degree of the terms in Ψ_π:

$$\deg_x(\phi_m\psi_n^2) = m^2 + (n^2-1) = m^2 + n^2 - 1$$
$$\deg_x(\phi_n\psi_m^2) = n^2 + (m^2-1) = m^2 + n^2 - 1$$

Because the norm of the Gaussian integer is $N(\pi) = n^2 + m^2$, the degree of the composite polynomial Ψ_π is exactly $N(\pi) - 1$.

In Theorem 3.3, we established the factorization $\Psi_\pi = \psi_\pi\psi_{\overline{\pi}}$ over $\mathbb{Z}[i][x]$. Because complex conjugation is a field automorphism, it preserves the degree of polynomials, meaning $\deg(\psi_\pi) = \deg(\psi_{\overline{\pi}})$. Therefore:

$$2\deg(\psi_\pi) = \deg(\Psi_\pi) = N(\pi) - 1$$
$$\deg(\psi_\pi) = \frac{N(\pi)-1}{2}$$

Since ψ_π is the minimal polynomial of x_1, the degree of the field extension is $\frac{N(\pi)-1}{2}$. □

Because $K(x_1)/K$ is a Galois extension, we can precisely determine the structure of its Galois group by utilizing the torsion maps.

Theorem 4.4. *Let $K = \mathbb{Q}(i)$ and $M = K(x_1)$, where x_1 is a root of the irreducible π-division polynomial ψ_π. Then M/K is a Galois extension with a cyclic Galois group of order $\frac{N(\pi)-1}{2}$.*

Proof. As previously discussed in Lemma 4.3, $[M : K] = \frac{N(\pi)-1}{2}$.

For any root x_k of $\psi_\pi(x)$, there exists a π-torsion point $P_k = (x_k, y_k)$. Since the π-torsion $E[\pi]$ is a cyclic $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$-module, we have $P_k = [\alpha]P_1$ for some $\alpha \in (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$. The

x-coordinate map is a rational function $x_k = f(x_1) \in K(x_1)$. Thus, all roots of the minimal polynomial lie in M, making M/K Galois.

Let $G = \mathrm{Gal}(M/K)$. Each $\sigma \in G$ is determined by its action on x_1. Specifically, $\sigma(x(P_1)) = x([\alpha]P_1)$ for some α. Because $x(P) = x(-P)$, the elements α and $-\alpha$ induce the same transformation on the x-coordinate.

The map $\sigma_\alpha \mapsto \alpha$ defines a surjective homomorphism from $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times \to G$ with kernel $\{\pm 1\}$. Since $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$ is a cyclic group of order $N(\pi) - 1$, the quotient G is a cyclic group of order $\frac{N(\pi)-1}{2}$. □

4.2 The Full Abelian Extension via the y-Coordinate

While the field $K(x_1)$ provides a systematic mechanism for generating cyclic extensions, it is limited to degrees dividing $\frac{N(\pi)-1}{2}$ due to the $x(P) = x(-P)$ symmetry. To recover the full multiplicative structure of the residue field, we must consider the extension generated by the y-coordinate.

Our first observation is that the field generated by the x-coordinate is sufficient to describe the arithmetic of the curve's equation squared. The following proposition bridges the extensions generated by x_1 and y_1.

Proposition 4.5. *Let $P = (x_1, y_1)$ be an odd π-torsion point on E. Then*

$$\mathbb{Q}(i)(x_1) = \mathbb{Q}(i)(y_1^2).$$

Proof. First note that an odd Gaussian integer is one such that $N(\pi)$ is odd. Let $K = \mathbb{Q}(i)$. In order to prove this we will show inclusion, then that they have the same degree over K. Note since we are working on the curve E, $y^2 = x^3 + x$, so we will prove that

$$K(x_1) = K(x_1^3 + x_1).$$

We first show $K(x_1^3 + x_1) \subseteq K(x_1)$. This inclusion is straightforward. Since K is a field and $x_1 \in K$ then so must be x_1^3 and so must be $x_1^3 + x_1$. Thus any field containing x_1 must also contain $x_1^3 + x_1$.

Since both of these are field extensions over K, we have that $K(x_1) \supseteq K(x_1^3 + x_1) \supseteq K$. It suffices to show that $[K(x_1) : K] = [K(x_1^3 + x_1) : K]$. We have shown in Theorem 3.3, that the torsion points are generated by roots of ψ_π, Since ψ_π is irreducible over Gaussian integers, it is also in the field $\mathbb{Q}(i)[x]$, thus the degree, $[K(x_1) : K] = \deg \psi_\pi = \frac{N(\pi)-1}{2}$. Let $p = N(\pi)$, and $\alpha = x_1^3 + x_1$. Since we have a sequence of subfields, we know that $[K(x_1) : K] = [K(x_1) : K(\alpha)] \cdot [K(\alpha) : K]$. It suffices to show that $[K(x_1) : K(\alpha)] = 1$

Consider the polynomial $f(t) = t^3 + t - \alpha \in K(\alpha)[t]$. By definition, x_1 is a root of $f(t)$. Let x_k be any Galois conjugate of x_1 over the field $K(\alpha)$. Because x_k must also be a root of $f(t)$, it satisfies $x_k^3 + x_k = \alpha = x_1^3 + x_1$.

Since x_k is a conjugate of x_1 over $K(\alpha)$, it is also a conjugate of x_1 over K, meaning x_k is another root of the π-division polynomial $\psi_\pi(x)$. Let $P_1 = (x_1, y_1)$ and $P_k = (x_k, y_k)$ be their corresponding π-torsion points on the curve E.

From the curve equation $y^2 = x^3 + x$, the relation $x_k^3 + x_k = x_1^3 + x_1$ immediately implies $y_k^2 = y_1^2$. Thus, $y_k = \pm y_1$. Geometrically, this means $P_k = P_1$ or $P_k = -P_1$.

In either case, the symmetry of the curve dictates that their x-coordinates must be identical, yielding $x_k = x_1$. Because the only conjugate of x_1 over $K(\alpha)$ is x_1 itself, the minimal polynomial of x_1 over $K(\alpha)$ has degree 1. Therefore, $[K(x_1) : K(\alpha)] = 1$, implying $K(x_1) = K(x_1^3 + x_1)$. □

A significant result of the previous section is the ability to generate extensions of degree $\frac{p-1}{2}$ for any prime $p \equiv 1 \pmod 4$. By adjoining y_1, we eliminate the symmetry collapse and double this degree.

Proposition 4.6. *The field extension $K(y_1)$ has degree $N(\pi) - 1$ over $K = \mathbb{Q}(i)$.*

Proof. Again, let $K = \mathbb{Q}(i)$ and let π be an odd Gaussian prime. We have established in Lemma 4.3 that the degree $[K(x_1) : K] = \frac{N(\pi)-1}{2}$ and in Theorem 3.3 that the π-division polynomial $\psi_\pi(x)$ satisfies Eisenstein criterion and is irreducible.

By Proposition 4.5, which we have just proven, we have the field equality $K(x_1) = K(y_1^2)$. To determine the degree $[K(y_1) : K]$, we observe that y_1 is the square root of

$x_1^3 + x_1 \in K(x_1)$. The relation $y_1^2 = x_1(x_1^2 + 1)$ ensures that y_1^2 has an odd multiplicity with respect to x_1.

In any extension where the minimal polynomial is Eisenstein, taking the square root of an element with odd multiplicity necessarily doubles the degree of the extension. Since the multiplicity of y_1^2 is not divisible by 2, the coordinate y_1 cannot reside in $K(x_1)$; if it did, that would contradict irreducility and separability of ψ_π. Therefore, the degree must double:

$$[K(y_1) : K] = [K(y_1) : K(x_1)] \cdot [K(x_1) : K] = 2 \cdot \frac{N(\pi) - 1}{2} = N(\pi) - 1.$$

Thus, the coordinates of a single π-torsion point generates a field extension of degree $N(\pi) - 1$. □

We now prove that the Galois group is cyclic and thus the extension is abelian.

Theorem 4.7. *Let $K = \mathbb{Q}(i)$ and $M = K(y_1)$, where $y_1^2 = x_1^3 + x_1$ is a root of the irreducible π-division polynomial ψ_π. Then M/K is a Galois extension with a cyclic Galois group of order $N(\pi) - 1$.*

Proof. As established in Theorem 4.2, the field $M = K(y_1)$ is independent of the choice of root y_1, implying that M contains all conjugates of y_1 and is thus a Galois extension of K. From Proposition 4.6, we have already determined that the degree of this extension is $[M : K] = N(\pi) - 1$.

To determine the Galois group $G = \text{Gal}(M/K)$, we utilize the coordinate maps derived in Section 3.1.1. Any $\sigma \in G$ acts on the torsion point $P_1 = (x_1, y_1)$ by $\sigma(P_1) = [\alpha]P_1$ for some $\alpha \in (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$. This induces an injective homomorphism:

$$\rho : G \hookrightarrow (\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$$

In the case of the x-coordinate field (Theorem 4.4), the map $x(P) = x(-P)$ created a non-trivial kernel $\{\pm 1\}$. However, for the y-coordinate, $\sigma(y_1) = y([\alpha]P_1) = y_1$ implies $[\alpha]P_1 = P_1$, which only occurs when $\alpha \equiv 1 \pmod{\pi}$.

Thus, the map ρ is an isomorphism. Since $(\mathbb{Z}[i]/\pi\mathbb{Z}[i])^\times$ is the multiplicative group of a finite field, it is cyclic of order $N(\pi) - 1$. It follows that $\text{Gal}(M/K)$ is a cyclic group of order $N(\pi) - 1$. □

The extension $K(y_1)$ is abelian because its Galois group is cyclic; this implies that all subextensions are also Galois and abelian.

The fact that the Galois group is cyclic of order $N(\pi)-1$ allows us to explicitly construct any cyclic extension of $\mathbb{Q}(i)$ with degree dividing $N(\pi) - 1$ by taking the appropriate fixed fields of $K(y_1)$.

Example 4.8. We now demonstrate the explicit construction of these extensions using the Gaussian prime $\pi = 1 + 2i$. Note that $N(\pi) = 5$, meaning the π-torsion points are a subspace of the full 5-torsion group $E[5]$.

From our computational results in Appendix A, the irreducible π-division polynomial is:

$$\psi_{1+2i}(x) = (1 + 2i)x^2 + 1$$

To find the x-coordinates of the π-torsion points, we find the roots of this polynomial:

$$x_1^2 = \frac{-1}{1+2i} = \frac{-1(1-2i)}{5} = \frac{-1+2i}{5}$$

Let $K = \mathbb{Q}(i)$. We define our first field extension by adjoining a root x_1:

$$M_x = K\left(\sqrt{\frac{-1+2i}{5}}\right)$$

By Theorem 4.4, we expect this to be a cyclic Galois extension of degree $\frac{N(\pi)-1}{2} = \frac{5-1}{2} = 2$. Because x_1 is the square root of an element in K that is not a perfect square, M_x is clearly a quadratic extension over $\mathbb{Q}(i)$, perfectly matching our theoretical result.

However, M_x does not capture the full torsion structure. We must find the corresponding y-coordinate for the point $P_1 = (x_1, y_1)$ on the curve $E : y^2 = x^3 + x$.

$$y_1^2 = x_1^3 + x_1 = x_1(x_1^2 + 1)$$

Substituting our known value for x_1^2:

$$y_1^2 = x_1\left(\frac{-1+2i}{5} + \frac{5}{5}\right) = x_1\left(\frac{4+2i}{5}\right)$$

We now define the full extension $M_y = M_x(y_1) = K(y_1)$. By the preceding theorem, we expect this to be a cyclic Galois extension of degree $N(\pi) - 1 = 4$.

Since $\frac{4+2i}{5}$ is not a perfect square in M_x, adjoining the square root of this value strictly doubles the degree of the extension. Thus, the degree of M_y over K is exactly $2 \cdot 2 = 4$.

Through the geometry of the curve $y^2 = x^3 + x$, we have explicitly constructed a cyclic abelian extension of degree 4 over $\mathbb{Q}(i)$ by simply adjoining the coordinates of a single torsion point.

This realization of complex multiplication theory provides an answer to a piece of Hilbert's 12th problem, historically rooted in Kronecker's *Jugendtraum*. Just as the roots of cyclotomic polynomials generate the abelian extensions of the rational numbers $\mathbb{Q}$, we have demonstrated that the geometric torsion structure of elliptic curves serves the exact same purpose for the imaginary quadratic field $\mathbb{Q}(i)$.

Appendix A

Computational Implementation

A.1 Python Script for Division Polynomials

The following script calculates the division polynomial Ψ_π, then factors by the given π into $\psi_\pi \psi_{\bar{\pi}}$.

```
import sympy as sp
import re

def format_poly_latex(poly):
    return sp.latex(poly).replace(r'\mathbf{I}', 'i').
       replace('I', 'i')

def is_Z_i_poly(expr):
    x = sp.symbols('x')
    try:
        coeffs = sp.Poly(expr, x).coeffs()
    except (sp.GeneratorsNeeded, sp.PolynomialError):
        coeffs = [expr]

    for c in coeffs:
        try:
            re_part = sp.re(c)
            im_part = sp.im(c)
            if not (re_part.is_integer and im_part.
               is_integer):
                return False
        except AttributeError:
            return False
    return True

def format_grouped_latex(factors_list):
    res = ""
```

```
    for f, p in factors_list:
        f_latex = format_poly_latex(f)
        if p == 1:
            res += rf"({f_latex})"
        else:
            res += rf"({f_latex})^{{{p}}}"
    return res

def format_factor_pair_latex(poly, n_map, m_map):
    x = sp.symbols('x')
    pi = n_map + m_map * sp.I
    pi_bar = n_map - m_map * sp.I
    coeff, factors_list = sp.factor_list(poly, extension=[sp
       .I])

    psi_pi_factors = []
    psi_bar_factors = []

    for f, p in factors_list:
        if is_Z_i_poly(f):
            psi_pi_factors.append((f, p // 2 if p > 1 else
               1))
            psi_bar_factors.append((f, p // 2 if p > 1 else
               1))
        else:
            test_pi = sp.expand(f * pi)
            test_bar = sp.expand(f * pi_bar)
            if is_Z_i_poly(test_pi):
                psi_pi_factors.append((test_pi, p))
            elif is_Z_i_poly(test_bar):
                psi_bar_factors.append((test_bar, p))
            else:
                psi_pi_factors.append((f, p))

    return f"{format_grouped_latex(psi_pi_factors)}{
       format_grouped_latex(psi_bar_factors)}"

def get_psi_basic(n, x, y):
    psi_cache = {}
    def psi(k):
        if k in psi_cache: return psi_cache[k]
        if k <= 0: return 0
        if k == 1: return 1
        if k == 2: return 2*y
        if k == 3: return 3*x**4 + 6*x**2 - 1
```

```
67          if k == 4: return 4*y*(x**6 + 5*x**4 - 5*x**2 - 1)
68          m = k // 2
69          if k % 2 == 0:
70              res = (psi(m) * (psi(m+2)*psi(m-1)**2 - psi(m-2)
                   *psi(m+1)**2)) / (2*y)
71          else:
72              res = psi(m+2)*psi(m)**3 - psi(m-1)*psi(m+1)**3
73          psi_cache[k] = sp.expand(res)
74          return psi_cache[k]
75      return psi(n)
76
77  def main():
78      try:
79          n_map = int(input())
80          m_map = int(input())
81      except ValueError:
82          return
83
84      x, y = sp.symbols('x y')
85      curve_eq = x**3 + x
86
87      def clean_poly(expr):
88          return sp.expand(expr).subs(y**2, curve_eq).expand()
89
90      p_n = get_psi_basic(abs(n_map), x, y)
91      p_m = get_psi_basic(abs(m_map), x, y)
92
93      phi_n = clean_poly(x * p_n**2 - get_psi_basic(abs(n_map)
           +1, x, y) * get_psi_basic(abs(n_map)-1, x, y))
94      phi_m = clean_poly(x * p_m**2 - get_psi_basic(abs(m_map)
           +1, x, y) * get_psi_basic(abs(m_map)-1, x, y))
95
96      Psi_pi_final = clean_poly(phi_m * p_n**2 + phi_n * p_m
           **2)
97
98      print(format_poly_latex(Psi_pi_final))
99      print(format_factor_pair_latex(Psi_pi_final, n_map,
           m_map))
100
101 if __name__ == "__main__":
102     main()
```

A.2 Computational Results

This section provides numerical verification for the algebraic properties of the Gaussian endomorphisms derived in Chapter 3. By utilizing the symbolic algebra implementation in Section A.1, we have calculated the division polynomials for several Gaussian primes π where $N(\pi) = p \equiv 1 \pmod 4$.

The primary goal of these computations is to demonstrate the factorization $\Psi_\pi = \psi_\pi \psi_{\bar{\pi}}$, verifying that the p-torsion subgroup indeed decomposes into two distinct eigenspaces of the endomorphism ring $\mathbb{Z}[i]$.

A.2.1 Factorization and Eisenstein Verification Table

Table A.2.1 on the following page lists the irreducible Gaussian factors $\psi_\pi(x)$ for the curve $y^2 = x^3 + x$. All intermediate coefficients are checked for divisibility by π in $\mathbb{Z}[i]$.

Table A.1: Table of small factorizations of Ψ_π

Prime π	$N(\pi)$	**Irreducible Factor** $\psi_\pi(x) \in \mathbb{Z}[i][x]$
$1+2i$	5	$(1+2i)x^2+1$
$1-2i$	5	$(1-2i)x^2+1$
$2+3i$	13	$(2+3i)x^6+(4-7i)x^4+(10-11i)x^2-i$
$2-3i$	13	$(2-3i)x^6+(4+7i)x^4+(10+11i)x^2+i$
$3+2i$	13	$(3+2i)x^6-(7+4i)x^4-(11+10i)x^2-1$
$3-2i$	13	$(3-2i)x^6-(7-4i)x^4-(11-10i)x^2-1$
$1+4i$	17	$(1+4i)x^8+(20+12i)x^6-(10+28i)x^4-(12+20i)x^2+1$
$4+i$	17	$(4+i)x^8+(12+20i)x^6+(28-10i)x^4+(20-12i)x^2+i$
$2+5i$	29	$(2+5i)x^{14}+(76-13i)x^{12}+(246+325i)x^{10}+(520+459i)x^8+(398+183i)x^6-(148+65i)x^4-(70-i)x^2+i$
$5+2i$	29	$(5+2i)x^{14}-(13+76i)x^{12}+(325+246i)x^{10}+(459+520i)x^8+(183+398i)x^6+(65-148i)x^4-(1-70i)x^2+1$
$6+i$	37	$(6+i)x^{18}+(112+105i)x^{16}+(168-860i)x^{14}+(784-3372i)x^{12}+(996-3682i)x^{10}+(3088-546i)x^8+(2600+532i)x^6+(368-284i)x^4+(70-87i)x^2+i$
$5+4i$	41	$(5+4i)x^{20}-(158-28i)x^{18}-(2243+272i)x^{16}-(2824-816i)x^{14}+(586-3336i)x^{12}+(2412-11912i)x^{10}+(930-13360i)x^8+(952-3568i)x^6+(209+36i)x^4+(130-60i)x^2+1$

Appendix B

Properties of the Weierstrass $\wp$-function

In this appendix, we provide the proofs for the fundamental properties of the Weierstrass $\wp$-function relative to a lattice $\Lambda \subset \mathbb{C}$.

We first show that the function converges in $\mathbb{C}$. The definition of the $\wp$-function is given by:

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

Proof. To show $\wp(z)$ is meromorphic, we examine the general term of the series for $|z|<\frac{1}{2}|\omega|$:

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2-(z-\omega)^2}{\omega^2(z-\omega)^2} \right| = \left| \frac{2z\omega - z^2}{\omega^2(z-\omega)^2} \right|$$

As $|\omega|\to\infty$, the term is $O(|\omega|^{-3})$. A series of the form $\sum_{\omega\in\Lambda\setminus\{0\}}|\omega|^{-k}$ converges if and only if $k > 2$. Since $k = 3$, the series converges absolutely and uniformly on compact subsets of $\mathbb{C}\setminus\Lambda$. Thus, $\wp(z)$ is holomorphic on $\mathbb{C}\setminus\Lambda$. The term $1/z^2$ creates a pole of order 2 at $z = 0$, and by periodicity, at every $\omega \in \Lambda$. □

Now we will prove that $\wp$ is an even function (i.e. $\wp(-z) = \wp(z)$)

Proof. Consider $\wp(-z)$. By the definition:

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

Since Λ is a lattice (a group under addition), the map $\omega \mapsto -\omega$ is a bijection of the set

$\Lambda \setminus \{0\}$. We can therefore re-index the sum:

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

Thus, the function is even. □

We next prove it's characteristic of *double periodicity*

Proof. It is easier to first consider the derivative $\wp'(z)$. Differentiating the series term-by-term (justified by uniform convergence):

$$\wp'(z) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

This sum is clearly periodic for any $\omega_i \in \Lambda$, as $\wp'(z+\omega_i)$ simply shifts the indices of the summation. Thus, $\wp'(z+\omega_i) = \wp'(z)$. Integrating this equality, we find that for each generator ω_i:

$$\wp(z+\omega_i) = \wp(z) + C_i$$

for some constant C_i. To determine C_i, we substitute $z = -\omega_i/2$:

$$\wp(\omega_i/2) = \wp(-\omega_i/2) + C_i$$

Since $\wp$ is even, $\wp(\omega_i/2) = \wp(-\omega_i/2)$, which implies $C_i = 0$. Therefore, $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Lambda$. □

References

[Ful69] William Fulton. *Algebraic curves: an introduction to algebraic geometry*. Mathematics lecture note series. Addison-Wesley, 1969.

[Har77] Robin Hartshorne. *Algebraic geometry*. Graduate texts in mathematics; 52. Springer, 1977.

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer, 1994.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2 edition, 2009.

[Was08] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Discrete mathematics and its applications. Chapman & Hall/CRC, Boca Raton, FL, 2nd ed.. edition, 2008.

Name of Candidate: Tannon N. Warnick

Date of Submission: April 14, 2026