# The Ideal Class Group Action on Supersingular Elliptic Curves

Steven Galbraith
University of Auckland
s.galbraith@auckland.ac.nz

From series of lectures at a summer school in Akaroa, New Zealand, January 2022

## Introduction

The aim of these notes is to give a low-brow, elementary, and more-or-less self-contained explanation of the action of the ideal class group of $\mathbb{Z}[\sqrt{-p}]$ on the set of isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_p$. This is the basic mathematical structure underlying the CSIDH isogeny-based cryptosystem.

There is nothing new in these notes. Everything is in Waterhouse's landmark paper [Wat69]. Nowadays Voight's book [Voi21] is an important reference. My hope is that the explicit and computational proofs in the present notes may be of interest to readers who find those references inaccessible.

The notes were adapted from a series of lectures given at the 2022 NZMRI summer workshop in Akaroa, New Zealand in January 2022. I thank Gabriel Pan for help converting the lecture slides into this format.

This is an updated version from September 2024, correcting an error. See Example 3.11 and Lemma 3.12 for details. Thanks to Adolfo Quirós for alerting me to the issue.

## 1 Basic definitions

We give a very brief summary of ideals in imaginary quadratic fields. Good general references for this include Stewart and Tall [ST02].

Throughout this section, we let $R$ denote a commutative ring with multiplicative identity. We denote $R[x]$ the ring of polynomials with coefficients in $R$. If $\alpha$ is a root of a monic quadratic integer polynomial then $\mathbb{Z}[\alpha]$ really means all polynomials in $\alpha$, but it can be identified with $\{a + b\alpha : a, b \in \mathbb{Z}\}$.

When considering imaginary quadratic fields $\mathbb{Q}(\sqrt{-p})$, for ease of proof we generally consider the case where $p \equiv 1 \pmod 4$, since then its ring of integers

is simply $\mathbb{Z}[\sqrt{-p}]$. Many of the results proved will also hold in the case $p \equiv 3 \pmod 4$, but we do not provide those proofs.

## 1.1 Ideals

For completeness, we present some basic definitions regarding ideals of commutative rings.

**Definition 1.1.** An *ideal* is a non-empty subset $I \subseteq R$ such that $I$ is a group under addition and

$$\sum_{i=1}^{m} a_i r_i \quad \in \quad I$$

for any $m \in \mathbb{N}$, $a_i \in I$ and $r_i \in R$ for $1 \leq i \leq m$.

The two simplest examples of ideals are $I = \{0\}$ and $I = R$.

**Definition 1.2.** An ideal $I$ is called *proper* if $I$ is non-zero and $I \neq R$.

**Definition 1.3.** The ideal generated by $a_1, \ldots, a_n \in R$ is the set $(a_1, \ldots, a_n) = \{\sum_{i=1}^{n} a_i r_i : r_i \in R\}$. Such an ideal is called *finitely generated*.

**Definition 1.4.** An ideal $I$ is called *principal* if $I = (a)$ for some $a \in R$.

**Definition 1.5.** A proper ideal $I$ in a ring $R$ is *prime* if, for any $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.

**Definition 1.6.** The *product* of two ideals $I$ and $J$ is

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\}.$$

## 1.2 Ideal classes

We now want to define an equivalence relation on ideals.

**Definition 1.7.** Let $I, J$ be ideals in $R$. We define the equivalence relation $I \sim J$ if there exist $\alpha, \beta \in R$ such that $(\alpha)I = (\beta)J$.

We omit the details that this relation is well defined with respect to ideal multiplication and is an equivalence relation.

**Definition 1.8.** Consider an ideal $I$. Define an inverse ideal $I^{-1}$ (if it exists) to be any ideal such that $II^{-1} = (\alpha)$ for some non-zero $\alpha \in R$.

The ideal (0) is not considered to have an inverse. The ideal $R$ is equal to the principal ideal (1), and is its own inverse.

If an ideal has an inverse then it is called an invertible ideal. In a Dedekind domain every non-zero ideal is invertible. This then allows us to define a useful group structure on the set of ideals.

**Definition 1.9.** The *ideal class group* $\mathrm{Cl}(R)$ is the set of equivalence classes of non-zero invertible ideals with the group operation being the product operation from Definition 1.6.

Again, we omit the details that this satisfies the group axioms. See Stewart and Tall [ST02] for details.

## 1.3 Imaginary quadratic fields

Let $d > 1$ be a square-free integer. An *imaginary quadratic field* is $\mathbb{Q}(\sqrt{-d})$, which is a degree two extension of $\mathbb{Q}$. The *ring of integers* is the set of $\alpha \in \mathbb{Q}(\sqrt{-d})$ that are roots of a monic polynomial with integer coefficients.

**Proposition 1.10.** *If $d \equiv 1 \pmod 4$, then the ring of integers of $\mathbb{Q}(\sqrt{-d})$ is $\mathbb{Z}[\sqrt{-d}]$.*

*Proof.* We note that any number of the form $u + v\sqrt{-d}$ with $u, v \in \mathbb{Z}$ is a root of the polynomial $x^2 - 2ux + v^2 + dv^2$, which clearly has integer coefficients. So $\mathbb{Z}[\sqrt{-d}]$ is a subset of the ring of integers of the quadratic field.

On the other hand, suppose $u + v\sqrt{-d}$ is in the ring of integers. Then its minimal polynomial, $x^2 - 2ux + u^2 + dv^2$, must be in $\mathbb{Z}[x]$. We proceed by cases.

1. Suppose $u \in \mathbb{Z}$. Then since $u^2 + dv^2$ is an integer, we must have $dv^2$ be an integer. But since $v \in \mathbb{Q}$ and $d$ is squarefree, this implies that $v \in \mathbb{Z}$.

2. Suppose $u \notin \mathbb{Z}$. Then $u' := 2u \in \mathbb{Z}$, and $u'^2 \equiv 1 \pmod 4$. But since $u^2 + dv^2 = \frac{u'^2}{4} + dv^2$ must be an integer, it follows that $dv^2 = z - \frac{1}{4} = \frac{4z-1}{4}$ for some integer $z$. Since $d$ is also an integer, if we write $v = \frac{a}{b}$ in the lowest terms, we must have $b = 2$ and $da^2 \equiv 3 \pmod 4$. But this means that $a^2$ cannot be even, so $a^2 \equiv 1 \pmod 4$ and thus $d \equiv 3 \pmod 4$, a contradiction.

Thus the ring of integers is equal to $\mathbb{Z}[\sqrt{-d}]$ □

**Definition 1.11.** The *norm* of an element $u + v\sqrt{-d}$ is $\mathrm{N}(u + v\sqrt{-d}) = u^2 + dv^2$

## 1.4 Ideals in imaginary quadratic fields

**Example:**

$$I = (2, 1 + \sqrt{-5}) = \{2\alpha + (1 + \sqrt{-5})\beta : \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\}$$

is an ideal in $\mathbb{Z}[\sqrt{-5}]$.

**Exercise 1.12.** Let $I$ be an $R = \mathbb{Z}[\sqrt{-d}]$-ideal. Show that $I \cap \mathbb{Z}$ is an ideal in $\mathbb{Z}$. Let $I \cap \mathbb{Z} = (a)$ for some integer $a \geq 0$. Show that

1. $I = (0)$ if and only if $a = 0$.

2. $I = R$ if and only if $a = 1$.

3. If $a$ is non-zero and $u + v\sqrt{-d} \in I$ then $a \mid \mathrm{N}(u + v\sqrt{-d})$.

4. $I \supseteq (a)$.

5. $I$ a prime ideal implies $a$ is prime.

6. If there is some integer $u > 1$ such that $I \subseteq (u)$, then $I = (u)I'$ for some ideal $I'$ in $R$.

**Exercise 1.13.** If $I$ is a non-zero ideal in $R = \mathbb{Z}[\sqrt{-d}]$ such that $I \not\subseteq (u)$ for any integer $u > 1$ then show there are integers $a, b$ such that $I = (a, b + \sqrt{-d})$. Further, show that $a \mid (b^2 + d)$.

**Exercise 1.14.** Let $I$ be a prime ideal that is non-zero and not $R$. Show there is a prime $\ell$ such that either

- $I = (\ell, \sqrt{-d})$ and $\ell \mid d$,
- $I = (\ell)$ and $(\frac{-d}{\ell}) = -1$,
- $I = (\ell, \pm b + \sqrt{-d})$ for some integer $b$ such that $b^2 \equiv -d \pmod{\ell}$.

In the first case the ideal is its own inverse and $I^2 = (\ell)$. In the second case the ideal is principal and its inverse is $(1) = R$. In the third case an inverse of $I$ is

$$I^{-1} = (\ell, \mp b + \sqrt{-d})$$

(ie., the other choice of sign).

One can define the *norm* $N(I)$ of an ideal $I$ to be the index $[R : I]$. We do not give all the details. However we remark that $N(I)$ is positive integer and if $I = (a, b + \sqrt{-d})$ with $\gcd(a, b) = 1$ and $a \mid (b^2 + d)$ then $N(I) = a$. Also, if $I$ and $J$ are ideals then $N(IJ) = N(I)N(J)$. In the case $I = (\ell, \pm b + \sqrt{-d})$ where $\ell$ is prime and $\ell \mid (b^2 + d)$, we have $N(I) = N(I^{-1}) = \ell$.

There is a reduction theory of ideals that allows to compute efficiently in $\mathrm{Cl}(\mathbb{Z}[\sqrt{-d}])$, but we do not go into the details here. A good basic reference is the book "Binary Quadratic Forms: An Algorithmic Approach" by Johannes Buchmann and Ulrich Vollmer.

# 2 Elliptic curves and isogenies

## 2.1 Elliptic curves

**Definition 2.1.** An *elliptic curve* $E$ over a field $K$ of characteristic $> 3$ is a projective non-singular curve with affine equation $y^2 = x^3 + Ax + B$ where $A, B \in K$ are such that $4A^3 + 27B^2 \neq 0$.

The set of $K$-rational points on an elliptic curve $E$ over $K$ is the set $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{0\}$, where 0 denotes the point at infinity, which is the point $[0 : 1 : 0]$ on the projective curve $y^2z = x^3 + Axz^2 + Bz^3$.

Two elliptic curves are isomorphic over $K$ if there exists a birational map defined over $K$ between them. Concretely, two elliptic curves $y^2 = x^3 + Ax + B$ and $y^2 = x^3 + A'x + B'$ are isomorphic over $K$ under an isomorphism that fixes the point at infinity if and only if $A' = u^4 A$ and $B' = u^6 B$ for some $u \in K$. The $j$-invariant of an elliptic curve is $j(E) = 1728 \cdot 4A^3/(4A^3 + 27B^2)$. Two elliptic curves $E_1, E_2$ over $K$ have $j(E_1) = j(E_2)$ if and only if there is an isomorphism $\phi : E_1 \to E_2$ over $\overline{K}$. We write $E_1 \cong E_2$.

The set of points on an elliptic curve is a group, with the point at infinity as the identity. The details of this can be found in any reference text on elliptic curves, such as [Sil09, Was03]. Since they are not relevant to our discussion, however, we omit these details from these notes.

## 2.2 Isogenies

**Definition 2.2.** Let $E_1, E_2$ be elliptic curves over a field $K$. An *isogeny* is a non-constant map $\phi : E_1 \to E_2$ that is both a morphism in the sense of geometry and a group homomorphism. The isogeny is *defined over* $K$ if the map is described by rational functions with coefficients in $K$.

The *degree* of an isogeny is its degree in the sense of a morphism in algebraic geometry. An important property of degree is that $\deg(\psi \circ \phi) = \deg(\psi)\deg(\phi)$.

We also have a notion of separability of an isogeny. Again, there are many competing definitions, but for our purposes, the following property is sufficient.

**Definition 2.3.** An isogeny is *separable* if the degree of the isogeny is the size of its kernel.

A key example of an isogeny is the multiplication map.

**Example 2.4.** Let $E$ be an elliptic curve. The *multiplication-by-$n$* isogeny, denoted $[n] : E \to E$ maps

$$P \mapsto P + P + \cdots + P \ (n \text{ times})$$

Its kernel is known as the *$n$-torsion group* and is denoted $E[n]$.

An endomorphism is an isogeny from an elliptic curve $E$ to itself. We denote

$$\mathrm{End}(E) = \{\text{isogenies } \phi : E \to E \text{ over } \bar{K}\} \cup \{[0]\}.$$

Then $\mathrm{End}(E)$ is a ring under pointwise addition and composition, with $[0]$ and $[1]$ being the additive and multiplicative identities respectively. In the CSIDH context we are interested in curves $E$ over $\mathbb{F}_p$ and we focus on the ring of endomorphisms that are defined over $\mathbb{F}_p$ (rather than over $\overline{\mathbb{F}}_p$). This ring is sometimes denoted $\mathrm{End}_{\mathbb{F}_p}(E)$.

**Exercise 2.5.** Let $E_1$ and $E_2$ be elliptic curves over $K$ and suppose $\phi : E_1 \to E_2$ is an isogeny over $K$. Show that $\ker(\phi)$ is defined over $K$ (in the sense that $P \in \ker(\phi)$ implies $\sigma(P) \in \ker(\phi)$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$).

A deep theorem (due to Deuring in the elliptic curve case, but in general known as "Tate's isogeny theorem") says that if $E_1$ and $E_2$ are elliptic curves over a finite field $\mathbb{F}_q$ with the same number of points, then there exists an isogeny defined over $\mathbb{F}_q$ from $E_1$ to $E_2$. A proof of this fact is beyond the scope of these notes, but we need this fact to be able to prove that the group action is transitive.

## 2.3 Frobenius map

We now discuss a particularly important endomorphism for elliptic curves over finite fields.

**Definition 2.6.** Let $E$ be an elliptic curve over $\mathbb{F}_p$. Define the *Frobenius map* $\pi : E \to E$ by

$$(x, y) \mapsto (x^p, y^p)$$

The Frobenius map is a group homomorphism, so

$$[n] \circ \pi = \pi \circ [n] \tag{1}$$

for all $n \in \mathbb{Z}$.

The Frobenius map encodes information about the elliptic curve, via its characteristic polynomial.

**Proposition 2.7.** *The Frobenius map $\pi$ satisfies $\pi^2 - t\pi + p = 0$, where $t$ is an integer known as the trace of Frobenius and $t^2 - 4p < 0$. We call $X^2 - tX + p$ the* characteristic polynomial of Frobenius.

What this means is that for all points $P \in E(\overline{\mathbb{F}}_p)$ we have $\pi(\pi(P)) - [t]\pi(P) + [p]P = 0$.

As a result, $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$ is an imaginary quadratic ring, where elements of this ring act as $(a + b\pi)(P) = [a]P + [b]\pi(P)$. Indeed $\mathbb{Z}[\pi]$ is a subring of $\mathrm{End}_{\mathbb{F}_p}(E)$.

We are now in a position to define supersingular elliptic curves. We provide a definition for characteristic $> 3$.

**Definition 2.8.** If $p \neq 2, 3$, an elliptic curve $E$ over $\mathbb{F}_p$ is *supersingular* if and only if the trace of Frobenius is 0.

**Exercise 2.9.** Let $E$ over $\mathbb{F}_p$ be supersingular, so that Frobenius satisfies $\pi^2 = -p$. This exercise is to show that we can identify $\mathbb{Z}[\pi]$ in $\mathrm{End}(E)$ with $\mathbb{Z}[\sqrt{-p}]$. Formally, consider the map from $\mathbb{Z}[\pi]$ to $\mathbb{Z}[\sqrt{-p}]$ by mapping $a + b\pi$ to $a + b\sqrt{-p}$. Show that this map is a ring isomorphism, where the multiplication on the left side is composition of endomorphisms in $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$, and the multiplication on the right side is polynomial multiplication in $\mathbb{Z}[\sqrt{-p}]$.

The above exercise is more subtle than it may appear. It is not true in general that composition of polynomials and multiplication of polynomials give the same result! This works in the case of Frobenius due to equation (1). What this means is that, when $E$ is a supersingular elliptic curve over $\mathbb{F}_p$, then $\mathrm{End}(E)$ contains a subring isomorphic to $\mathbb{Z}[\sqrt{-p}]$.

## 2.4 Isogenies from kernels

We now show that separable isogenies are entirely determined by their kernels.

**Proposition 2.10.** *(Vélu) Given a finite subgroup $G \subseteq E_1(\overline{\mathbb{F}}_p)$ there exists an elliptic curve $E_2$ and a (separable) isogeny $\phi : E_1 \to E_2$ with $\ker(\phi) = G$. The curve $E_2$ and the isogeny $\phi$ are unique up to isomorphism, meaning that if $\phi' : E_1 \to E_3$ is another isogeny with kernel $G$ then there is an isomorphism $\eta : E_2 \to E_3$ and $\phi' = \eta \circ \phi$.*

This result, as well as a concrete algorithm to calculate this isogeny from a kernel, was presented by Vélu [Vél71].

**Theorem 2.11.** *(Silverman [Sil09] Corollary III.4.11, Galbraith [Gal12] Theorem 9.6.18) Let $E_1, E_2, E_3$ be elliptic curves over $K$ and $\phi : E_1 \to E_2$, $\psi : E_1 \to E_3$ isogenies over $K$. Suppose $\ker(\phi) \subseteq \ker(\psi)$ and that $\psi$ is separable. Then there is a unique isogeny $\lambda : E_2 \to E_3$ defined over $K$ such that $\psi = \lambda \circ \phi$.*

A corollary of this result is that if $\phi : E_1 \to E_2$ is an isogeny with non-cyclic kernel then one can factor out a multiplication by $n$ map to get an isogeny $\psi : E_1 \to E_2$ with cyclic kernel.

# 3 The group action of $\mathbf{Cl}(\mathbb{Z}[\sqrt{-p}])$ on supersingular elliptic curves

We are now able to introduce an action of ideals of the imaginary quadratic ring $\mathbb{Z}[\sqrt{-p}]$ on a set of supersingular elliptic curves defined over $\mathbb{F}_p$. To do this, we use the fact that $\mathbb{Z}[\sqrt{-p}]$ is a subset of the endomorphism ring of any supersingular elliptic curve $E$ defined over $\mathbb{F}_p$. As a result, an ideal of $\mathbb{Z}[\sqrt{-p}]$ can be interpreted as a set of endomorphisms of $E$.

In this section, we will show how we can associate with every ideal a (unique separable) isogeny, and vice versa. These ideals can be considered to be acting on supersingular elliptic curves by sending a curve to its image curve under their associated isogeny. We then show that the action is well-defined up to ideal classes, when one works with isomorphism classes of elliptic curves.

## 3.1 Isogenies to ideals and back again

We begin by associating an ideal to an isogeny, and vice versa. We only do this in the special case of a supersingular elliptic curve over $\mathbb{F}_p$, and so $\mathrm{End}(E)$ has a subring $\mathbb{Z}[\sqrt{-p}] \cong \mathbb{Z}[\pi]$. We also avoid discussing some subtleties with the ideal $(\sqrt{-p})$, which need to be handled using the language of group schemes; these issues do not arise in CSIDH.

Let $E$ be an elliptic curve with $\mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}(E)$. Let $G$ be a finite subgroup of $E(\overline{\mathbb{F}}_p)$. Define the ideal

$$I(G) = \{a + b\sqrt{-p} \in \mathbb{Z}[\sqrt{-p}] : (a + b\pi)(P) = 0 \text{ for all } P \in G\}.$$

Similarly, given an isogeny $\phi : E \to E'$, define its kernel ideal to be

$$I_\phi = I(\ker(\phi)) = \{a + b\sqrt{-p} \in \mathbb{Z}[\sqrt{-p}] : (a + b\pi)(P) = 0 \text{ for all } P \in \ker(\phi)\}.$$

**Exercise 3.1.** Show that $I(G)$ is an ideal. Show that $H \subseteq G$ implies $I(G) \subseteq I(H)$.

Similarly, for a given (integral) ideal $I$ of $\mathbb{Z}[\sqrt{-p}]$, we define the set

$$E[I] = \{P \in E : \alpha(P) = 0 \text{ for all } \alpha \in I\}$$

where $I$ is identified as being in $\mathrm{End}(E)$ and $\alpha : E \to E$, as in Exercise 2.9.

When $I \neq (0)$ then $E[I]$ is finite, since it is the intersection of the kernels of all non-zero elements in $I$, and each kernel is a finite subgroup.

**Exercise 3.2.** Show that if $I$ and $J$ are ideals in $\mathbb{Z}[\sqrt{-p}]$ such that $I \subseteq J$, then $E[J] \subseteq E[I]$.

Since $E[I]$ is a finite subgroup of $E$ it defines an isogeny $\phi_I$ from $E$ with kernel $E[I]$. We denote the image curve by $E_I$ (up to isomorphism), so we have associated to an ideal $I$ the isogeny $\phi_I : E \to E_I$.

It is a fact that $\deg(\phi_I) = N(I)$. This can be verified directly for ideals $I = (\ell, \pm b + \sqrt{-d})$ in $\mathbb{Z}[\sqrt{-d}]$ where $\ell$ is prime and $b^2 \equiv -d \pmod{\ell}$, since $\deg(\phi_I) = \ell = N(I)$. Another easy case is $I = (n)$ and $\phi_I = [n]$. The general case follows from decomposition into ideals/isogenies of prime norm/degree.

**Lemma 3.3.** *Let $p \equiv 1 \pmod 4$ and let $E$ be a supersingular elliptic curve over $\mathbb{F}_p$. Let $I$ be an ideal in $\mathbb{Z}[\sqrt{-p}]$ and let $\phi_I : E \to E'$ be the associated isogeny. Denote the $p$-power Frobenius maps on $E$ and $E'$ by $\pi_E$ and $\pi_{E'}$ respectively. Then*

$$\phi_I \circ \pi_E = \pi_{E'} \circ \phi_I.$$

*In other words, the isogeny $\phi_I : E \to E'$ associated with $I$ is defined over $\mathbb{F}_p$, and $E'$ is defined over $\mathbb{F}_p$.*

*Proof.* Note that $\ker(\phi_I) = E[I] = \cap_{a+b\sqrt{-p} \in I} \ker(a + b\pi)$. Suppose $a, b \in \mathbb{Z}$ and $P \in \ker(a + b\pi)$. Then (using equation (1))

$$0 = \pi(0) = \pi(aP + b\pi(P)) = [a]\pi(P) + [b]\pi(\pi(P)) = (a + b\pi)(\pi(P)).$$

Hence $\pi(P) \in \ker(a + b\pi)$. It follows that $\pi(E[I]) = E[I]$. From Vélu's formulae and Galois theory it follows that $\phi_I$ is given by rational functions with coefficients in $\mathbb{F}_p$. This means that $\phi_I$ commutes with Frobenius. □

## 3.2 Action of Ideals

Let $p \equiv 1 \pmod 4$ (as always, the results are true in greater generality, but there are some subtleties that our presentation avoids). Fix a supersingular elliptic curve $E$ over $\mathbb{F}_p$ and consider the ideal class group of $\mathbb{Z}[\sqrt{-p}]$. For an

ideal $I$ in $\mathbb{Z}[\sqrt{-p}]$ we define $I * E$ to be the curve $E_I$, which is the image of $\phi_I$ as defined above.

Note that, by Lemma 3.3, $E_I = I * E$ is defined over $\mathbb{F}_p$. We now show that $E_I$ is supersingular and hence we still have $\mathbb{Z}[\sqrt{-p}] \subseteq \mathrm{End}(E_I)$.

**Lemma 3.4.** *Let $E$ over $\mathbb{F}_p$ be supersingular and let $\phi : E \to E'$ be an isogeny defined over $\mathbb{F}_p$. Then $E'$ is supersingular.*

*Proof.* Let $\pi$ be the Frobenius on $E$ and $\pi'$ the Frobenius on $E'$. Since $E$ is supersingular we have $\pi^2 = [-p]$. By Lemma 3.3 we have

$$\pi'^2 \circ \phi = \phi \circ \pi^2 = \phi \circ [-p] = [-p] \circ \phi.$$

This means $\pi'^2(\phi(P)) = [-p]\phi(P)$ for all points $P \in E$. Since isogenies are surjective, this means $\pi'^2 = [-p]$ on all points of $E'$, and so $\pi'^2 = -p$ and $E'$ is supersingular. □

We will show that there is a well-defined action of ideal *classes* on *isomorphism classes* of elliptic curves. The main result is Theorem 3.9. First we need some lemmas.

**Lemma 3.5.** *A non-zero principal ideal $I = (\alpha)$ is associated with an endomorphism.*

*Proof.* Since $\alpha \in I$ we have $E[I] \subseteq \ker(\alpha)$. Conversely, every element of $(\alpha)$ is a multiple of $\alpha$ so has kernel containing $\ker(\alpha)$. Hence $E[I] = \ker(\alpha)$. Let $\phi_I : E \to E_I$ be the (uniquely defined) isogeny with kernel $\ker(\alpha)$. Since $\alpha$ is also an isogeny with kernel $\ker(\alpha)$, it follows that $\phi_I = \alpha$ (up to isomorphism), which is an endomorphism. □

**Lemma 3.6.** *Let $I, J \subseteq \mathbb{Z}[\sqrt{-p}]$ be non-zero ideals. Then $\phi_{IJ} = \phi_J \circ \phi_I$.*

*Proof.* Consider some $P \in \ker(\phi_J \circ \phi_I)$. By definition, $\phi_I(P) \in \ker(\phi_J)$; that is, for all $\beta \in J$, $\beta(\phi_I(P)) = 0$, where 0 here denotes the identity element on the elliptic curve. Now $\beta = a + b\pi$ for some integers $a, b$ and so Lemma 3.3 implies $\beta \circ \phi_I = \phi_I \circ \beta$. This means $\phi_I(\beta(P)) = 0$, and by definition this is equivalent to $\alpha(\beta(P)) = 0$ for all $\alpha \in I, \beta \in J$; that is, $P \in \ker(\phi_{IJ})$.

Conversely, let $P \in \ker(\phi_{IJ})$. Then, for all $\alpha \in I, \beta \in J$ we have $\alpha(\beta(P)) = 0$. It follows that $\beta(P) \in E[I]$ and so $\phi_I(\beta(P)) = 0$. We deduce from Lemma 3.3 that $\beta(\phi_I(P)) = 0$ for all $\beta$. Hence $\phi_I(P) \in E[J]$ and so $P \in \ker(\phi_J \circ \phi_I)$.

Since their kernels are equal, it follows that the isogenies are also equal (up to isomorphism) □

The isogeny $\phi_{I^{-1}}$ is the dual isogeny to $\phi_I$. This is immediate from $I^{-1}I = [N(I)]$ and the connection between $\deg(\phi_I)$ and $N(I)$ (neither of which we have rigorously proved).

**Lemma 3.7.** *Suppose $I \sim J$ as ideals. Let $\phi_I : E \to E_I$ and $\phi_J : E \to E_J$. Then $E_I \cong E_J$.*

*Proof.* If $I \sim J$, then there are non-zero $\alpha, \beta \in \mathbb{Z}[\sqrt{-p}]$ with $(\alpha)I = (\beta)J$. We have $\phi_{(\alpha)I} = \phi_{(\beta)J}$. By Lemma 3.6 we can factor this isogeny as

$$E \xrightarrow{\phi_I} E_I \xrightarrow{\alpha} E_I$$

and

$$E \xrightarrow{\phi_J} E_J \xrightarrow{\beta} E_J.$$

Here we are using the fact that $\alpha$ and $\beta$ are principal ideals and so, by Lemma 3.5, they are endomorphisms. Since $\phi_{(\alpha)I} = \phi_{(\beta)J}$ the elliptic curves on the right hand side are isomorphic. This implies that $E_I$ and $E_J$ are isomorphic. □

We now consider the set of supersingular elliptic curves up to isomorphism.

**Lemma 3.8.** *Let $E_1, E_2$ be supersingular elliptic curves over $\mathbb{F}_p$ such that $E_1 \cong E_2$ over $\mathbb{F}_p$ (this implies $j(E_1) = j(E_2)$, but the converse isn't necessarily true). Let $I$ be an ideal in $\mathbb{Z}[\sqrt{-p}]$. Then $I * E_1 \cong I * E_2$.*

*Proof.* Let $\alpha : E_1 \to E_2$ be an isomorphism defined over $\mathbb{F}_p$ and let $\phi_I : E_2 \to E_3 = I * E_2$. It would be nice to argue using $(\alpha)I$ like in Lemma 3.6, but we can't say $\alpha \in \mathbb{Z}[\sqrt{-p}]$ as it is not an endomorphism (it does not map the curve $E_1$ to itself).

Instead, we need to prove that $\ker(\phi_I \circ \alpha) = E_1[I]$. To do this we need to restrict to $\alpha$ being a group homomorphism, which is ok since we can compose with a translation map on $E_1$ if required. So $\alpha$ is a group homomorphism and a bijection.

Since $\alpha$ is defined over $\mathbb{F}_p$ it commutes with Frobenius. Hence, for every $a + b\pi$ in $I$ we have $\alpha \circ (a + b\pi) = (a + b\pi) \circ \alpha$. The result follows. □

The requirement that the isomorphism is defined over $\mathbb{F}_p$ in Lemma 3.8 is important. Two curves with the same $j$-invariant, but not isomorphic over $\mathbb{F}_p$, do not necessarily have the same $\mathbb{F}_p$-endomorphism ring (this is shown in the paper by Delfs and Galbraith).

We can now express the class group action formally.

**Theorem 3.9.** *Let $p \equiv 1 \pmod 4$. Then $Cl(\mathbb{Z}[\sqrt{-p}])$ acts on the set of isomorphism classes of supersingular curves defined over $\mathbb{F}_p$ by*

$$(E, I) \mapsto I * E$$

*where $I * E$ is the curve $E_I$ defined by the isogeny $\phi_I : E \to E_I$ with kernel $E[I]$.*

*Proof.* The well-definedness of the group action on classes stems from Lemma 3.7 and Lemma 3.8. The proof that it satisfies the axioms of a group action follows from Lemma 3.5 and Lemma 3.6. □

Let $p \equiv 1 \pmod 4$ and let $X$ be the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ with $\mathbb{F}_p$-endomorphism ring isomorphic to $\mathbb{Z}[\pi] \cong \mathbb{Z}[\sqrt{-p}]$. We have shown that the ideal class group of $\mathbb{Z}[\sqrt{-p}]$ acts on

$X$, by $(E, I) \mapsto I * E$. Indeed, the action is *transitive*, in the sense that for any $E_1, E_2 \in X$ there is some ideal $I$ such that $I * E_1 = E_2$. This more-or-less[1] follows from Tate's isogeny theorem: there exists an isogeny $\phi : E_1 \to E_2$ defined over $\mathbb{F}_p$. Associated to $\phi$ is the ideal $I_\phi$. We will show in Theorem 3.13 below that $I_\phi * E_1 = E_2$.

## 3.3 Further properties

The definitive work by Waterhouse on this topic defines (in much greater generality) a *kernel ideal* to be an ideal $I$ such that $I(E[I]) = I$. The property $I(E[I]) = I$ for ideals in the full supersingular endomorphism ring is established in Proposition 42.2.16 of Voight [Voi21]. We now show a direct proof of this property in our setting of ideals in $\mathbb{Z}[\sqrt{-p}]$.

**Lemma 3.10.** *Let $p \equiv 1 \pmod 4$ and $I = (a, b + \sqrt{-p})$ be an ideal in $\mathbb{Z}[\sqrt{-p}]$ of norm co-prime to $p$ such that $I \cap \mathbb{Z} = (a)$. Let $E$ be an elliptic curve with $End_{\mathbb{F}_p}(E) = \mathbb{Z}[\sqrt{-p}]$. Then*

$$I(E[I]) = I.$$

*Proof.* It is trivial that $I \subseteq I(E[I])$. To prove the opposite inclusion, let $u + v\sqrt{-p} \in I(E[I])$.

Let $P \in E[I]$ be a point of exact order $a$. (This is where we need the norm of the ideal to be co-prime to $p$.) To show such a point exists consider $E[I] = E[a] \cap \ker(b + \sqrt{-p})$. Note that $a \mid \deg(b + \pi)$ (as $I \cap \mathbb{Z} = (a)$), and also note that $b + \pi$ has cyclic kernel (because it is not divisible by any map $[n]$ for $n > 1$).

By definition $(u + v\pi)(P) = 0$. Since $P \in E[I]$ it also follows that $\pi(P) = -bP$. Hence $(u - vb)(P) = 0$. Since $P$ has exact order $a$ it follows that $u - vb = ax$ for some $x \in \mathbb{Z}$. But then

$$u + v\sqrt{-p} = (u - vb) + v(b + \sqrt{-p}) = ax + v(b + \sqrt{-p}) \in I.$$

This completes the proof. □

The next question we consider is the extent to which $I(G)$ determines $G$ in our setting. First we give an example that shows $I(G)$ does not determine $G$ in general. Then in Lemma 3.12 we show that $I(G)$ does determine $G$ in the case when $G$ is the kernel of an $\mathbb{F}_p$-rational isogeny. It is interesting to compare this with Proposition 42.2.15 of Voight [Voi21], where the ideal $I(G)$ is defined with respect to the full quaternion order and not just the Frobenius order.

**Example 3.11.** Let $p \equiv 1 \pmod 4$ and let $E$ be a supersingular curve over $\mathbb{F}_p$. Then $\#E(\mathbb{F}_p) = p + 1 \equiv 2 \pmod 4$ and so there is a point $P \in E(\mathbb{F}_p)$ of order 2. Let $Q \in E(\mathbb{F}_{p^2})$ be another point of order 2, so that $E[2] = \{0, P, Q, P + Q\}$. Note that $\pi(P) = P$ and $\pi(Q) = P + Q$, where $\pi$ is the $p$-power Frobenius.

[1] There are some details about invertibility of ideals and levels of the isogeny volcano I don't want to get into. An alternative approach to proving transitivity of the action is via Deuring lifting and Hilbert class polynomials.

Let $H_1 = \{0, P\}$, $H_2 = \{0, Q\}$ and $G = E[2]$ be subgroups. It is easy to check that $I(H_1) = (2, \pi - 1)$ and $I(G) = (2)$.

To compute $I(H_2)$ note that $(a+b\pi)(Q) = 0$ implies $0 = [a]Q + [b](P+Q) = [b]P + [a+b]Q$. Since $P$ and $Q$ are independent this implies $b \equiv 0 \pmod 2$ and hence $a \equiv 0 \pmod 2$. It follows that $I(H_2) = I(G) = (2)$ and so both subgroups have the same ideal.

**Lemma 3.12.** *Let $E$ be a supersingular elliptic curve over $\mathbb{F}_p$. Let $H \subseteq G$ be subgroups of $E$ that are both kernels of separable $\mathbb{F}_p$-rational isogenies. If $I(G) = I(H)$ then $G = H$.*

*Proof.* This is Proposition 42.2.15 of Voight [Voi21] in the case of the full endomorphism ring. We sketch an elementary argument.

Suppose $G \neq H$. Due to the structure of elliptic curve groups, there are only two possibilities:

1. There is a prime $\ell$ and integer $k$ such that $\ell^k$ divides the order of a point $P \in G$ but $\ell^k$ does not divide the order of any element in $H$.

2. There is a prime $\ell$ and integer $k$ such that $G$ contains $E[\ell^k]$ but $H$ does not contain $E[\ell^k]$.

In both cases we explain how one can write down maps $a + b\pi$ which are zero on $H$ but non-zero on $G$. Note that $\ell \neq p$ since the isogenies are separable.

For example, in the first case let $m$ be the exponent of $H$. Then $a+b\pi \in I(H)$ implies $(a + m) + b\pi \in I(H)$. But $\ell^k \nmid m$ so $[m]P \neq 0$. This means it can't be true that both $a + b\pi$ and $(a + m) + b\pi$ are in $I(G)$.

In the second case, let $P \in H$ have order $\ell^k$. Let $Q \in E[\ell^k]$ be such that $E[\ell^k] = \langle P, Q\rangle$. It follows that $Q \notin H$. Since $H$ is $\mathbb{F}_p$-rational it follows that $\pi(P) \in H$. We also know that $\pi(P)$ has order $\ell^k$, and so $\pi(P) = [\lambda]P + R$ for some non-zero integer $\lambda$ and some $R \in E[\ell^{k-1}]$. Then $\ell^{k-1}(\pi - \lambda) \in I(H)$. Suppose for contradiction that $\ell^{k-1}(\pi - \lambda) \in I(G)$. Then $\pi(Q) = [\lambda]Q + R'$ for some $R' \in E[\ell^{k-1}]$. Define $P' = [\ell^{k-1}]P$ and $Q' = [\ell^{k-1}]Q$. Then $\langle P', Q'\rangle = E[\ell]$ and $\pi(R) = [\lambda]R$ for all $R \in E[\ell]$. When $\ell = 2$ this is impossible, as we are assuming that $p \equiv 1 \pmod 4$ and so $\#E(\mathbb{F}_p) = p + 1 \equiv 2 \pmod 4$ (in other words, $E[2]$ contains an $\mathbb{F}_p$-rational point and a non-$\mathbb{F}_p$-rational point). When $\ell > 2$ this is also impossible since Frobenius has characteristic polynomial $X^2+p$, which does not have a repeated root (so $\pi$ cannot have a repeated eigenvalue). Hence we have a contradiction as required. □

**Theorem 3.13.** *Let $p \equiv 1 \pmod 4$. Let $E$ be a supersingular elliptic curve over $\mathbb{F}_p$.*

1. *Let $I$ be an ideal in $\mathbb{Z}[\sqrt{-p}]$ of norm co-prime to $p$ and let $\phi_I : E \to E'$ be the associated isogeny. Then*

$$I_{\phi_I} = I.$$

2. *Let $\phi : E \to E'$ be a separable isogeny over $\mathbb{F}_p$. Let $I_\phi$ be the associated ideal. Then*

$$\phi_{I_\phi} = \phi.$$

*Proof.* Let $I$ be an ideal. Then $\ker(\phi_I) = E[I]$. Then $I_{\phi_I} = I(\ker \phi_I) = I(E[I])$ and the result follows from Lemma 3.10.

For the second claim note that $G = E[I_\phi]$ contains $H = \ker(\phi)$. By definition, $H$ is the kernel of an $\mathbb{F}_p$-rational isogeny, and Lemma 3.3 shows that $G$ is also the kernel of an $\mathbb{F}_p$-rational isogeny. By Lemma 3.12, if $G \neq H$ then $I(G) \neq I(H)$. But $I(G) = I[E[I_\phi]] = I_\phi$ by Lemma 3.10. Hence $G = H$ and so $\phi_{I_\phi} = \phi$. (As always we are working up to isomorphism, meaning that two isogenies with the same kernel, like $\phi$ and $-\phi$, are considered equal.) □

# References


[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography.* Cambridge University Press, 2012.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Text in Mathematics. Springer, 2009.

[ST02] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem.* AK Peters, 3rd edition, 2002.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C.R. Acad. Sc. Paris, Série A.*, page 238–241, 1971.

[Voi21] John Voight. *Quaternion Algebras*, volume 288. Springer Graduate Text Math., 2021.

[Was03] Lawrence C. Washington. *Elliptic curves : number theory and cryptography.* CRC Press, 2003.

[Wat69] E. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2:521–560, 1969.