Supersingular Elliptic Curves

MATH470 Report

Nicholas Hayek

Supervised by Prof. Darmon

CONTENTS

Abstract 1

I Genus of a Curve **1**

Algebraic Varieties 1

Differentials 3

Riemann-Roch 4

II Weierstrass Forms **6**

III Isogenies **9**

The Dual Isogeny 11

IV Finite Fields and Supersingularity **16**

Hasse's Bound 16

Supersingular Elliptic Curves 19

V Supersingular Isogeny Graphs **28**

VI Implementation and Results **32**

Arithmetic of Graph Generation 32

Generating Supersingular j-invariants when $p \equiv_{12} 1$ 32

Traversing $\mathcal{G}_2(p)$ 34

Finding Collisions in $\mathcal{G}_2(p)$ 35

Appendix A 37

Appendix B 39

Gallery 40

References 41

ABSTRACT

Elliptic curves are smooth, genus one projective varieties of dimension one. Points on these curves give rise to a group structure, where the analogous discrete logarithm problem is hard. This fact led to the first uses of elliptic curves in cryptography, by adapting schemes which utilize the multiplicative structure of finite fields, such as those based on the Diffie-Hellmann key exchange ([10], [12]).

Since then, promising cryptographic programs have risen from the theory of isogenies—essentially well-structured maps—between elliptic curves. We present the background required to understand isogeny-based elliptic curve cryptography and demonstrate a practical implementation of these ideas with the Charles-Goren-Lauter hash function ([4]).

Cover: supersingular isogeny graph over $\mathbb{F}_{2017}$

I Genus of a Curve

These notes are content from [14], in particular sections I-V; lectures by Prof. Lozano-Robledo ([11]); discussions with Prof. Henri Darmon; and work by Prof. Eyal Goren and others on isogeny-based cryptography ([7], and especially [4]).

Elliptic curves are described in the language of projective varieties—mutual solutions in projective coordinates to a set of n-variable homogeonous polynomials—and the maps between them. Refer to [14], I-II.3, for a self-contained introduction to algebraic varieties (in particular, function fields, morphisms, divisors, and projective space). We assume this knowledge and some basic Galois theory (see Appendix B for symbols not defined).

ALGEBRAIC VARIETIES

Let M/K be an extension over a field K. We call a set $\{a_1, ..., a_k\} \subset M$ *transcendentally independent* if no polynomial $f \in K[\vec{x}]$ exists such that $f(a_1, ..., a_k) = 0$. DEF 1.1

A *transcendence basis* $\beta \subseteq M$ is a maximally transcendentally independent set in M, whose size we call the *transcendence degree of* M.

Eg. 1.1.1

$$K \underbrace{\quad\subset\quad}_{\text{transcendental}} K(t^2) \overbrace{\quad\subset\quad}^{\text{algebraic}} K(t)$$

as t satisfies the polynomial equation $x^2 - t^2$ in $K(t^2)$.

Eg. 1.1.2

$$K \underbrace{\qquad\subset\qquad}_{\text{transcendental}} K(\beta) \overbrace{\qquad\subset\qquad}^{\text{algebraic}} M$$

where β is a transcendence basis for M/K.

DEF 1.2 Let V be an affine variety. Recall the function field of V. The *dimension of V*, denoted $\dim(V)$, is the transcendence degree of $\overline{K}(V)$, viewed as a $\overline{K}$-vector space.

DEF 1.3 Let V be an affine variety defined by polynomials $f_1, ..., f_m \in \overline{K}[\vec{x}]$. Then V is called *smooth at a point $P \in V$* if and only if

$$\operatorname{rank}\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{\substack{i\in[m] \\ j\in[n]}} = n - \dim(V)$$

PROP 1.1 If V be an affine variety defined by one polynomial $f \in \overline{K}[\vec{x}]$, then V is non-smooth at $P \in V \iff \nabla f(P) = 0$.

PROOF. The zeros of f define a hypersurface in $\mathbb{A}^n$, which one may view as $\mathbb{A}^{n-1}$. Then, $\overline{K}(\mathbb{A}^{n-1}) = \overline{K}(x_1, ..., x_{n-1})$, which has transcendence degree $n-1$ over $\overline{K}$. Hence, $\dim(V) = n-1$.

The matrix provided in Def 1.3 is exactly $\nabla f(P)$ when $m = 1$. Any non-zero row matrix has rank 1, so $\operatorname{rank}(\nabla f(P)) = 0 \iff \nabla f(P) = 0$. But $n - \dim(V) = n - (n-1) = 1$, so P is non-smooth $\iff \nabla f(P) = 0$. □

From this point onward we will only consider projective varieties V, with dimensionality and smoothness conditions defined as above on $V \cap \mathbb{A}^n$, where we pick an arbitrary copy $\mathbb{A}^n \subset \mathbb{P}^n$. (In particular, one may choose an inclusion $(x_1, ..., x_n) \hookrightarrow [x_0 : \cdots : x_{n-1} : 1]$).

Frequently, we will present a projective variety in "affine form." By writing $f(x_1, ..., x_n) \mapsto x_0^{\deg(f)} f\left(\frac{x_1}{x_0}, ..., \frac{x_n}{x_0}\right)$, we recover its projective coordinate form. For instance,

$$y^2 = x^3 + x^2 \quad \text{becomes} \quad zy^2 = x^3 + zx^2$$

Applying Prop 1.1, the above variety is smooth everywhere except at $(0,0) = [0:0:1]$.

DEF 1.4 A projective variety of dimension 1 is called a *curve*.

PROP 1.2 Projective varieties in $\mathbb{P}^2$ defined over one polynomial are curves.

PROOF. $\dim(V) = n - 1 = 2 - 1 = 1$, since V is defined over one polynomial. □

DEF 1.5 Let $\phi : C_1 \to C_2$ be a morphism of curves. We call $\deg(\phi) = [K(C_1) : \phi^*(K(C_2))]$ the *degree* of ϕ. The separable and inseparable degrees of this extension are denoted $\deg_s(\phi)$ and $\deg_i(\phi)$, respectively. (For a proof of $K(C_1)/\phi^*(K(C_2))$ being a finite extension, see [8], II.6.2)

Eg. 1.2.1 Let $\phi : \{C : zy^2 = x^3 + z^3\} \to \mathbb{P}^1$ by $[x : y : z] \mapsto [x : z]$. Taking a slice $z = 1$, we have $\mathbb{Q}(\mathbb{P}^1) = \mathbb{Q}(x)$, and $\mathbb{Q}(C) = \mathbb{Q}(x, \sqrt{x^3+1})$. Then $\deg(\phi) = [\mathbb{Q}(C) : \mathbb{Q}(\mathbb{P}^1)] = 2$, since $\sqrt{x^3+1}$ satisfies the polynomial $t^2 - x^3 - 1$ in $\mathbb{Q}(x)$.

DIFFERENTIALS

DEF 1.6 Let C be a curve. The *divisors of* C, denoted $\mathrm{Div}(C)$, is the collection of finite formal sums

$$D = \sum_{P \in C} n_P(P)$$

where n_P is an integer. We add and subtract divisors by collecting coefficients, i.e. $\sum n_P(P) + \sum n'_P(P) = \sum(n_P + n'_P)(P)$, and set $\mathbb{0}_{\mathrm{Div}(C)} = 0$, called the *zero divisor*.

DEF 1.7 Let $\deg(D) = \sum_{P \in C} n_P$. The set of degree 0 divisors, $\mathrm{Div}^0(C)$, forms a subgroup of $\mathrm{Div}(C)$. We similarly define $\mathrm{Div}_K(C)$ and $\mathrm{Div}^0_K(C)$, by choosing divisors fixed by $\sigma \in \mathrm{Gal}(\overline{K}/K)$, with $\sigma D = \sum_{P \in C} n_P(\sigma P)$.

DEF 1.8 For $D \in \mathrm{Div}(C)$, we say $D \geq 0$ if $n_P \geq 0 \ \forall P \in C$.

DEF 1.9 To any function $f \in \overline{K}(C)$, we define the divisor of f, $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P)$. We call these *principle divisors*. We denote by $\mathrm{Pic}(C)$ the quotient of $\mathrm{Div}(C)$ modulo principle divisors, under formal addition. (Similarly for $\mathrm{Pic}^0(C)$).

DEF 1.10 Let C be a curve. Then Ω_C is the collection of differentials $dx : x \in \overline{K}(C)$. It is 1-dimensional $\overline{K}(C)$ vector space, with a generator $\langle dt \rangle$ for any uniformizer $t \in \overline{K}(C)$.

DEF 1.11 Let $\omega \in \Omega_C$ and $P \in C$. Since Ω_C is generated by dt, we may write $\omega = g dt$ for $g \in \overline{K}(C)$. Then we define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(g)$. The divisor associated with ω is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P)$$

DEF 1.12 $\mathcal{L}(D) = \{f \in \overline{K}(C) : \mathrm{div}(f) + D \geq 0\} \cup \{0\}$, and $\ell(D) = \dim_{\overline{K}} \mathcal{L}(D)$.

Eg. 1.3.1 $\mathrm{div}(x) = (0) - (\infty)$, with respect to $\mathbb{P}^1$. Properties of divisors can be found in [14], II.3. Notably, $\deg(\mathrm{div}(f)) = 0$ always.

Eg. 1.3.2 Let $P = [x_0 : y_0] \neq [1 : 0]$. Then $t := x - x_0$ is a uniformizer at P. Note that, in projective coordinates, this is $x - x_0 y$, so, indeed, this doesn't hold for $P = [1 :$

0]. Note that $dt = d(x - x_0) = dx - dx_0 = dx$, so $\text{ord}_P(dx) = \text{ord}_P(1) = 0$.

However, when $P = [1 : 0]$, $t := \frac{1}{x}$ is a uniformizer. This is better observed in projective coordinates, i.e. $\frac{y}{x}$. Then, $dt = d(\frac{1}{x}) = \frac{-dx}{x^2}$, so $\text{ord}_{[1:0]}(dx) = \text{ord}_{[1:0]}(\frac{-1}{x^2}) = -2$. Hence, $\deg(\text{div}(\omega))$ is *not* always 0 for $\omega \in \Omega_C$.

Eg. 1.3.3 If $\deg(D) < 0$, then $\sum_{P \in C} n_P \leq 0$. Hence, if $\text{div}(f) + D \geq 0$, then $\deg(\text{div}(f) + D) \geq 0$. But $\deg(\text{div}(f)) = 0$, so $f = 0$, and hence $\mathcal{L}(D) = \{0\}$.

We now have the tools to state and apply the Riemann-Roch theorem.

RIEMANN-ROCH

1.1 Riemann-Roch

Let C be a smooth curve and let $K_C = \text{div}(\omega)$ for $\omega \neq 0 \in \Omega_C$ (called a *canonical divisor*). Then $\forall D \in \text{Div}(C)$, we have

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1$$

for some unique $g \in \mathbb{Z}^{\geq 0}$.

DEF 1.13 The *genus* of a smooth curve C is $g \in \mathbb{Z}^{\geq 0}$ for which Thm 1.1 holds.

PROP 1.3 We observe the following useful corollaries:

(a) $\ell(K_C) = g$

(b) $\deg(K_C) = 2g - 2$

(c) If $\deg(D) > 2g - 2$, then $\ell(D) = \deg(D) - g + 1$

PROOF.

(a) Fix $D = 0$, the zero divisor. Then $\ell(0) - \ell(K_C - 0) = 1 - \ell(K_C) = \deg(D) - g + 1 = -g + 1 \implies \ell(K_C) = g$. Recall Def 1.12: $\ell(0) = \dim_{\overline{K}}(\mathcal{L}(0))$, where

$$\mathcal{L}(0) = \{f \in \overline{K}(C)^* : \text{div}(f) \geq 0\} \cup \{0\}$$

But such a function f must have no poles, so it is constant. Hence, $\mathcal{L} = \overline{K}^* = \overline{K}$, and the result follows.

(b) Fix $D = K_C$. Then $\ell(K_C) - 1 = \deg(K_C) - g + 1$, so by (a), $g - 1 = \deg(K_C) - g + 1$, so $\deg(K_C) = 2g - 2$.

(c) Suppose $\deg(D) > 2g - 2$. Then $\deg(D) > \deg(K_C)$, so $\deg(K_C - D) < 0$. Hence, $\mathcal{L}(K_C - D) = \{0\}$, and $\ell(K_C - D) = 0$. And we're done.

Recall that, if $\deg(D) < 0 \implies \mathcal{L}(D) = \{0\}$, as shown in Example 1.3 □

From Prop 1.3 (c), if $g = 1$, then $\deg(D) > 0 \implies \ell(D) = \deg(D)$.

Consider the following fleshed-out use cases for Thm 1.1:

Eg. 1.4.1 Let $C = \mathbb{P}^1$, the projective line. Then $\overline{K}(\mathbb{P}^1) = \overline{K}(x)$. Since $\operatorname{ord}_{[0:1]}(x) = 1$, and $x \in \overline{K}(x)$, x is a uniformizer. Hence, $\Omega_C = \langle dx \rangle$.

Since $dx \neq 0$, a canonical divisor may be $K_C = \operatorname{div}(dx)$. Let $P = [x_0 : y_0] \neq [1 : 0]$. We showed in Example 1.3 that $\operatorname{ord}_P(dx) = 0$ and $\operatorname{ord}_{[1:0]} = -2$. Hence, $K_C = -2(\infty)$. We conclude that $\deg(dx) = -2 = 2g - 2 \implies g = 0$ by Prop 1.3.

Eg. 1.4.2 Let $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$ for $e_i \neq e_j \in K$.

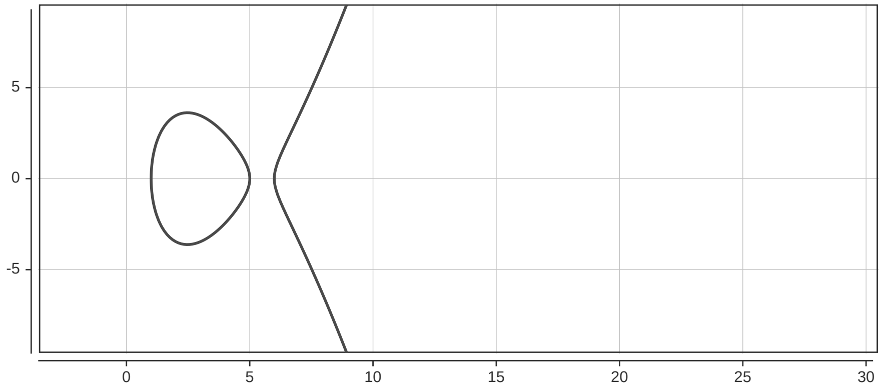


Figure 1: C with $(e_1, e_2, e_3) = (1, 5, 6)$ over $K = \mathbb{Q}$

$\omega = \frac{dx}{y}$ is a non-zero divisor on C, where $\overline{K}(C) \subseteq \overline{K}(\mathbb{P}^2) = \overline{K}(x, y)$. We claim $\operatorname{div}(\omega) = 0$. Consider:

$$\begin{aligned} 2y\,dy &= [(x - e_1)(x - e_2) + (x - e_2)(x - e_3) + (x - e_3)(x - e_1)]dx \\ \implies dx &= \frac{2y\,dy}{\sum_{i\neq}(x - e_i)(x - e_j)} \end{aligned}$$

Notice that y is a uniformizer at $P_k = (e_k, 0)$, and therefore

$$\operatorname{ord}_{P_i}(dx) = \operatorname{ord}_{P_i}\left(\frac{2y}{\sum_{i\neq}(x - e_i)(x - e_j)}\right) = 1$$

since at least one of $(x - e_i)(x - e_j) \neq 0$. Also note that all other $(\alpha, 0) \notin C$. We still need to consider the point at infinity $P = [0 : 1 : 0] = \infty$. For this, $\frac{x}{y}$ is a uniformizer. Thus, we compute

$$d\left(\frac{x}{y}\right) = \frac{y\,dx - x\,dy}{y^2}$$
$$\implies dx = \frac{2y^3}{2y^2 + x\sum_{i \neq j}(x-e_i)(x-e_j)} d\left(\frac{x}{y}\right)$$

Then,

$$\operatorname{ord}_\infty(dx) = \operatorname{ord}_{[0:1:0]} \frac{2y^3}{2y^2 + x\sum_{i \neq j}(x-e_i)(x-e_j)} = -3$$

since the numerator dominates with order 3. All totaled, then

$$\operatorname{div}(dx) = (P_1) + (P_2) + (P_3) - 3(\infty)$$

But also, $\operatorname{div}(y) = (P_1) + (P_2) + (P_3) - 3(\infty)$ by considering the original curve. We have $\operatorname{div}\left(\frac{dx}{y}\right) = \operatorname{div}(dx) - \operatorname{div}(y) = 0$. Hence,

$$\ell(K_C) = \ell(0) = 1 = g$$

We conclude that C has genus 1 by Prop 1.3 (a).

II Weierstrass Forms

We will now shift our focus to genus one curves, as in the last example.

DEF 2.1 The *Weierstrass form* is a curve defined by the following

$$C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in \overline{K}$$

DEF 2.2 With $C : y^2 = x^3 + Ax + B$, we have

$$\Delta := -16(4A^3 + 27B^2) \quad \text{and} \quad j := -1728\frac{(4A)^3}{\Delta}$$

called the *discriminant* and *j-invariant*, respectively. Note that Δ is a scalar multiple of the normal discriminant of a depressed cubic equation, which y^2 satisfies.

Δ and j may be defined over a long Weierstrass form (Def 2.1), but their definitions would be hairier.

Eg. 2.1.1 Weierstrass forms satisfy a few nice properties. For one, coordinate transformations may reduce them into convenient forms: when $\operatorname{char}(K) \neq 2$,

$$\iota_2 : y \mapsto \frac{1}{2}(y - a_1x - a_3) \implies C : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

If char$(K) \neq 3$ as well, we may reduce further:

$$\iota_3 : (x, y) \mapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108} \right) \implies C : y^2 = x^3 - 27c_4 x - 54c_6$$

The coefficients $\{a_i, b_i, c_i\}$ satisfy a set of algebraic relations determined by ι_2 and ι_3, which can be found [14], III.1.

Frequently, in fields with of characteristic not 2 or 3, we simply write a Weierstrass form as $C : y^2 = x^3 + Ax + B$. The quantities outlined in Def 2.2 refer to this form, which we call the *short Weierstrass*.

Eg. 2.1.2 Let C be a short Weierstrass curve. Then we can determine its shape by the quantities Δ and A. In particular, C is smooth $\iff \Delta \neq 0$, and C has a cusp $\iff \Delta = 0, A = 0$.

PROOF.

Let C be in long Weierstrass form, homogeneous, with

$$zy^2 + a_1 zxy + a_3 z^2 y = x^3 + a_2 zx^2 + a_4 z^2 x + a_6 z^3$$

Setting to zero, taking a partial w.r.t. z, and evaluating at $\infty = [0 : 1 : 0]$, we have

$$y^2 + a_1 xy + 2a_3 zy - a_2 x^2 + 2a_4 zx + 3a_6 z^2 \Big|_{[0:1:0]} = 1$$

so C is smooth at infinity always, by invoking Prop 1.1.

For finite points, consider again $y^2 = x^3 + Ax + B = f(x)$. In projective coordinates, this is

$$zy^2 - x^3 - Az^2 x - Bz^3 = 0$$

whose partials are $\left\langle -3x^2 - Az^2, 2zy, y^2 - 2Azx - 3Bz^2 \right\rangle$. In particular, if there is a singular point P, then $f'(P) = 0$ (observing ∂_x) and $f(P) = 0$ (observing ∂_y), so $f(x)$ has a double root. But $\Delta = 0 \iff f(x)$ has a multiple root (as a typical discriminant).

$A = 0$, and if $\Delta = 0$, then $B = 0$ as well. We conclude that $C : y^2 = x^3$, which has a cusp at $(0, 0)$. As it happens, if $A \neq 0$, we observe a node. □

PROP 2.1

Weierstrass forms are easily classifiable by their j-invariants.

(a) Any two short Weierstrass forms in variables (x, y) and $(\hat{x}, \hat{y})$, respectively, may be related by (and only by) a linear change of variables

$$x = u^2 \hat{x} \quad y = u^3 \hat{y} : u \in \overline{K}^*$$

(b) Two smooth Weierstrass curves are isomorphic $\iff$ their j-invariants are equivalent.

PROOF. For (a), see [14], III.1.4. For (b), the ($\implies$) direction follows by plugging in.

For ($\impliedby$), let $j = \hat{j}$, and the two curves have coefficients A, B and $\hat{A}, \hat{B}$, respectively. Then

$$\frac{A^3}{4A^3 + 27B^2} = \frac{\hat{A}^3}{4\hat{A}^3 + 27\hat{B}^2}$$

Rearranging, this yields

$$A^3\hat{B}^2 = \hat{A}^3B^2$$

We consider a few cases:

1. $A = 0$. Then $j = 0$. But $\Delta \neq 0$, so $B \neq 0$, and we conclude $\hat{A} = 0$. We rewrite $y^2 = x^3 + B$ and $y^2 = x^3 + \hat{B}$. These are related by the change of variables
$$(x, y) \xmapsto{\star} (u^2x, u^3y) : u = \left(\frac{B}{\hat{B}}\right)^{\frac{1}{6}}$$
2. $B = 0$. Then $j = 1728$, and $A \neq 0$, since $\Delta \neq 0$. But then $\hat{B} = 0$. With
$$u = \left(\frac{A}{\hat{A}}\right)^{\frac{1}{4}}$$
we perform $\star$ again.
3. Either transformation above will work.

□

The punchline: Weierstrass forms are

- Easy to tell when smooth and easy to visualize (Example 2.1).
- Easy to set into isomorphism classes (Prop 2.1).

Above all, however, Weierstrass forms characterize exactly elliptic curves over K:

DEF 2.3 A curve E is called an *elliptic curve* if it is smooth and genus one, containing a distinguished point $\mathcal{O} \in E$. We say that E is *defined over* K if E/K and $\mathcal{O} \in E(K)$.

2.1 Elliptic Curves over K are Weierstrass Forms

Any elliptic curve $(E, \mathcal{O})$ defined over K is isomorphic to a Weierstrass form with $a_i \in K$, with $\mathcal{O}$ sent to $[0 : 1 : 0]$. Conversely, every smooth Weierstrass form with $a_i \in K$ is an elliptic curve defined over K containing a base point $[0 : 1 : 0]$.

We will prove the latter claim only. For the former, one computes $\mathcal{L}(n(\mathcal{O}))$ explicitly for small values of n, choosing suitable functions from $K(E)$, until $\dim_{\overline{K}} \mathcal{L}(n(\mathcal{O})) < \#\mathcal{L}(n(\mathcal{O}))$, at which point we may claim a linear relation between its elements. This relation satisfies Def 2.1.

PROOF.

Let $C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Consider the differential

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

We claim $\operatorname{div}(\omega) = 0$. The result will follow, since then, setting $K_C = \operatorname{div}(\omega)$, we have $\ell(K_C) = \ell(0) = 1 = g$. One checks by inspection that a standard Weierstrass form contains the point $[0 : 1 : 0]$ when homogenized. It is smooth by assumption.

Writing C as $F(x, y) = 0$, we have

$$\omega = \frac{dx}{F_y} = -\frac{dy}{F_x}$$

Fix $P = (x_0, y_0)$. Since $d(x - x_0) = dx - dx_0 = dx$, we can rewrite, equivalently,

$$\omega = \frac{d(x - x_0)}{F_y} = -\frac{d(y - y_0)}{F_x}$$

P cannot be a pole, or else $F_y = F_x = 0$ at P. But C must be smooth.

P might still be a zero. Consider the map $C \to \mathbb{P}^1$ by $[x : y : 1] \mapsto [x : 1]$, of degree 2. (Since $\#\phi^{-1}(P) = 2$). Then $\operatorname{ord}_P(x - x_0) \leq 2$. In general, $\operatorname{ord}_P(x - x_0) = 2$ if and only if $F(x, y)$ has a double root at P, since $x - x_0$ is order 1 otherwise. So we have two cases, and, in either, we write

Where t is a uniformizer at P, $\operatorname{ord}(dt) = \operatorname{ord}(t) - 1$

$$\operatorname{ord}_P(\omega) = \operatorname{ord}_P\left(\frac{d(x - x_0)}{F_y}\right) = \operatorname{ord}_P(x - x_0) - 1 - \operatorname{ord}_P(F_y)$$

So $\operatorname{ord}_P(\omega) = 2 - 1 - 1 = 0$, or $\operatorname{ord}_P(\omega) = 1 - 1 - 0 = 0$. We conclude that ω cannot have zeros either. It remains to show the same result for the line at infinity $O = [0 : 1 : 0]$. With this base covered, $\operatorname{div}(\omega) = 0$, and we are done. □

III Isogenies

Consider an elliptic curve E. Points $P, Q \in (E, \mathcal{O}) \subseteq \mathbb{P}^2$ satisfy a group law $+ : (P, Q) \to P + Q$, defined by the following procedure:

1. $L \leftarrow$ the line through P and Q

2. $R \leftarrow L \cap E$, not P or Q
3. $L' \leftarrow$ the line through R and $\mathcal{O}$
4. $P + Q \leftarrow L' \cap E$, not P or Q

E becomes an abelian group with $\mathbb{1}_E = \mathcal{O}$. See [14], III.2.2 for a full justification, and II for essential results on morphisms. Using the curve we considered in Example 1.4, with $P = (1, 0)$ and $Q = (3, \sqrt{12})$, we have

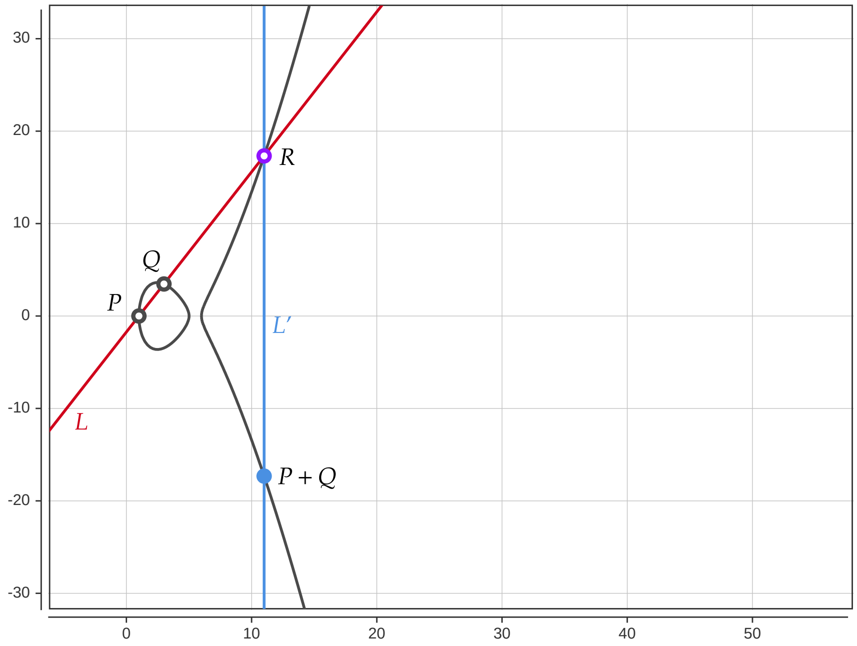


Figure 2: Addition of P and Q on $C : y^2 = (x-1)(x-5)(x-5)$

As groups, we may consider maps between elliptic curves which preserve the group action.

DEF 3.1 Let $\phi : (E_1, \mathcal{O}_1) \to (E_2, \mathcal{O}_2)$ be a morphism. If $\phi(\mathcal{O}_1) = \mathcal{O}_2$, then ϕ is called an *isogeny*. A priori, an isogeny ϕ is not a group homomorphism. However, we find shortly (Prop 3.2) that this comes for free.

Eg. 3.1.1 $[0] : E_1 \to E_2$ by $P \mapsto \mathcal{O}$ is called the *constant isogeny*.

Eg. 3.1.2 $[m] : E \to E$ by $P \mapsto [m]P$ is an isogeny, where

$$[m]P = \underbrace{P + \cdots + P}_{m \text{ times}}$$

since $(P, Q) \mapsto P + Q$ is a morphism, and $\underbrace{\mathcal{O} + \cdots + \mathcal{O}}_{m \text{ times}} = \mathcal{O}$.

The goal of the following propositions will be to show the existence of a unique "dual" to ϕ, related closely to the degree of ϕ, which we retain from Def 1.5. By convention, $\deg[0] := 0$.

THE DUAL ISOGENY

Let $(E, \mathcal{O})$ be an elliptic curve. $E \cong \mathrm{Pic}^0(E)$ by the map **PROP 3.1**

$$P \mapsto [(P) - (\mathcal{O})]$$

where, by $[(P) - (\mathcal{O})]$, we mean the representative for $(P) - (\mathcal{O})$ modulo principal divisors (see Def 1.9).

PROOF.

First, we claim that, for any $D \in \mathrm{Div}^0(E)$, $D \sim (P) - (\mathcal{O})$ modulo principle divisors, i.e. $[D] = [(P) - (\mathcal{O})]$, for some $P \in E$.

Thm 1.1 provides $\dim(\mathcal{L}(D + (\mathcal{O}))) = 1$. Pick any non-zero element $f \in \mathcal{L}(D + (\mathcal{O}))$. This must be a basis for it.

By definition of $\mathcal{L}$, we have

$$\mathrm{div}(f) \geq -D - (\mathcal{O})$$

Assuming $[D] \neq [0]$, we find that $\mathrm{div}(f)$ has a $-D - (\mathcal{O})$ term. But, since $\deg(\mathrm{div}(f)) = \deg(D) = 0$, it must be

$$\mathrm{div}(f) = -D - (\mathcal{O}) + K$$

for some degree-1 divisor K. But then $K \geq 0$, so $K = (P)$.

Then, since $-D - (\mathcal{O}) + (P)$ is principle, we have $D \sim (P) - (\mathcal{O})$, as desired.

Under the assignment $P \mapsto [(P) - (\mathcal{O})]$, we have a surjective map $\sigma : E \twoheadrightarrow \mathrm{Pic}^0(E)$. $\ker(\phi) = \mathcal{O}$ by definition, so this is a bijection, and $E \cong \mathrm{Pic}^0(E)$.

In the future, denote $\sigma_i : E_i \to \mathrm{Pic}^0(E_i)$ when E_i is arbitrary. □

Let $\phi : E_1 \to E_2$ be an isogeny. Then $\phi(P + Q) = \phi(P) + \phi(Q)\ \forall P, Q \in E_1$. **PROP 3.2**

PROOF.

If $\phi = [0]$, then this is clear. Otherwise, define

$$\phi_* = \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2) : \sum n_i(P_i) \mapsto \sum n_i\,(\phi(P_i))$$

Combining the previous results, we have the following diagram

$$\begin{tikzcd}
E_1 \arrow[r, leftrightarrow, "\sigma_1"] \arrow[d, "\phi"'] & \mathrm{Pic}^0(E_1) \arrow[d, "\phi_*"] \\
E_2 \arrow[r, leftrightarrow, "\sigma_2"'] & \mathrm{Pic}^0(E_2)
\end{tikzcd}$$

Let $P, Q \in E_1$. Then $P + Q \overset{\sigma_1}{\mapsto} [(P+Q) - (\mathcal{O})]$. One can show that $(P+Q)-(P)-(Q)+(\mathcal{O})$ is principle, so in particular $(P+Q)-(\mathcal{O}) = (P)-(\mathcal{O})+(Q)-(\mathcal{O})$. Proceeding:

$$\begin{aligned}
P + Q &\overset{\sigma_1}{\mapsto} [(P+Q)-(\mathcal{O})] = [(P)-(\mathcal{O})] + [(Q)-(\mathcal{O})] \\
&\overset{\phi_*}{\mapsto} [(\phi(P)) - (\mathcal{O})] + [(\phi(Q)) - (\mathcal{O})] \\
&\overset{\sigma_2^{-1}}{\mapsto} \phi(P) + \phi(Q) \\
P + Q &\overset{\phi}{\mapsto} \phi(P+Q)
\end{aligned}$$

Since $\phi = \sigma_2^{-1} \circ \phi_* \circ \sigma_1$, we conclude that $\phi(P+Q) = \phi(P) + \phi(Q)$. □

Since ϕ is a homomorphism, we have that $\ker(\phi) = \phi^{-1}(\mathcal{O})$ is a subgroup of E.

PROP 3.3 Let $\phi : E_1 \to E_2$ be an isogeny. Then $\# \ker(\phi) \leq \deg(\phi)$.

PROOF.

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi)$$

where $e_\phi(P)$ is the ramification index of ϕ at P. Setting $Q = \mathcal{O}$, and recalling that $e_\phi(P) \geq 1$, yields the result. □

From now on, assume ϕ is separable.

PROP 3.4 Let $\phi : E_1 \to E_2$ be an isogeny. Then $\# \ker(\phi) = \deg(\phi)$.

PROOF. We know that $\#\phi^{-1}(Q) = \deg_s(\phi) = \deg(\phi)$ except at finitely many points in E_2. We'll show this is the case for all points.

Let $Q \in E_2$ be chosen with $\#\phi^{-1}(Q) = \deg(\phi)$ (i.e. it satisfies the property).

Fix $Q' \in E_2$. We wish to show that $\#\phi^{-1}(Q) = \#\phi^{-1}(Q')$. Let $T \in E_2$ satisfy $Q + T = Q'$. Fix $P \in \phi^{-1}(T)$ and let $S \in \phi^{-1}(Q)$ be arbitrary. We compute:

$$\phi(S + P) = \phi(S) + \phi(P) = Q + T = Q'$$

Thus,

$$\deg(\phi) \geq \#\phi^{-1}(Q') \geq \#\{S+P : S \in \phi^{-1}(Q)\} = \phi^{-1}(Q) = \deg(\phi)$$

note that, where $S \neq S'$, $S + P \neq S' + P$ by the group law. □

PROP 3.5 Let $\phi : E_1 \to E_2$ be an isogeny. Then $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ is a Galois extension.

PROOF. Fix $T \in \ker(\phi)$. Let $\tau_T : E_1 \to E_1$ send $P \mapsto P + T$. Then the map

$$\kappa : \ker(\phi) \to \mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))) : T \mapsto \tau_T^*$$

is an isomorphism of groups, where τ_T^* is the induced map on $\overline{K}(E_1)$. We need to show

- κ is well defined as an automorphism.
- κ is a homomorphism
- κ is a bijection

- Let $f \in \overline{K}(E_2)$. Then
  $$\tau_T^*(\phi^* f) = (\phi \circ \tau_T)^* f = \phi^* f$$
  since $\phi \circ \tau_T(P) = \phi(P+T) = \phi(P) + \phi(T) = \phi(P) \implies \phi \circ \tau_T = \phi$.

  Hence, τ_T^* fixes any $\phi^* f$, i.e. is an automorphism of $\overline{K}(E_1)$ over $\phi^*(\overline{K}(E_2))$.
- $\kappa(T + T') = \tau_{T+T'}^* = (\tau_T \circ \tau_{T'})^* = (\tau_{T'} \circ \tau_T)^* = \tau_T^* \circ \tau_{T'}^* = \kappa(T) \circ \kappa(T')$
- Since
  $$\mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))) \leq [\overline{K}(E_1) : \phi^*(\overline{K}(E_2))] = \deg(\phi) = \#\ker(\phi)$$

it suffices to show, then, that κ is injective.

Suppose $T \in \ker(\kappa)$, i.e. τ_T^* fixes all of $\overline{K}(E_1)$. In particular, $f = x$ has a pole at $\mathcal{O}$ and no other poles. But $\tau_T^* x = x \circ (P \mapsto P + T) = x$, so, at T, x must also have a pole. So we conclude $T = \mathcal{O}$, as desired.

Since $\mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))) \cong \ker(\phi)$, we write

$$\#\mathrm{Aut}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))) = \#\ker(\phi) = \deg(\phi) = [\overline{K}(E_1) : \phi^*(\overline{K}(E_2))]$$

□

PROP 3.6 Let $\phi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ be isogenies. If $\ker(\phi) \subseteq \ker(\psi)$, then there exists a unique isogeny $\lambda : E_2 \to E_3$ with $\psi = \lambda \circ \phi$.

PROOF. From above, $\overline{K}(E_1)$ is a Galois extension of $\phi^*(\overline{K}(E_2))$ equivalent to $\ker(\phi)$, and similarly for $\psi^*(\overline{K}(E_3))$ and $\ker(\psi)$. Hence, we have the following diagram:

$$\begin{tikzcd}
\{\mathbb{1}\} \arrow[r, dash, "\subseteq" description] & \mathrm{Gal}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2))) \arrow[r, dash, "\subseteq" description] \arrow[d, leftrightarrow, "\cong" description] & \mathrm{Gal}(\overline{K}(E_1)/\psi^*(\overline{K}(E_3))) \arrow[d, leftrightarrow, "\cong" description] \\
 & \ker(\phi) \arrow[r, dash, "\subseteq" description] & \ker(\psi)
\end{tikzcd}$$

By the Galois correspondence, then, $\psi^*(\overline{K}(E_3)) \subseteq \phi^*(\overline{K}(E_2)) \subseteq \overline{K}(E_1)$. Then $\iota = \phi^{*-1} \circ \psi^*$ is an injection of function fields $\overline{K}(E_3) \hookrightarrow \overline{K}(E_2)$, and by [14], II.2.4, $\exists! \lambda : \lambda^* = \iota$, i.e. $\phi^* \lambda^* = \psi^* \implies \psi = \lambda \circ \phi$, as desired. □

We'll now begin to develop the basis for dual isogenies, using the results we've proven.

DEF 3.2 Let $\phi : E_1 \to E_2$ be an isogeny. Then we define

$$\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1) : (Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P) = \sum_{P \in \phi^{-1}(Q)} (P)$$

Note that $e_\phi(P) = 1$, since $\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi) = \#\phi^{-1}(Q)$. We need to verify that ϕ^* maps degree-0 divisors to degree-0 divisors. Consider the following:

PROP 3.7 $\deg(\phi^* D) = \deg(\phi)\deg(D)$.

PROOF. Let $D = \sum_{P \in E_1} n_P(P)$. Then

$$\phi^* D = \sum_{P \in E_1} n_P \sum_{Q \in \phi^{-1}(P)} e_\phi(Q)(Q) \implies \deg(\phi^* D) = \sum_{P \in E_1} n_P \deg(\phi) = \deg(\phi)\deg(D)$$

□

Hence, Def 3.2 is well-defined. Recalling $\sigma_i : E_i \to \mathrm{Pic}^0(E_i)$ by $P \mapsto [(P) - (O)]$ from the proof of Prop 3.1, we have the diagram

$$\begin{tikzcd}
E_2 \arrow[r, "\sigma_2"] \arrow[rrr, bend right, "\hat{\phi}" description] & \mathrm{Pic}^0(E_2) \arrow[r, "\phi^*"] & \mathrm{Pic}^0(E_1) \arrow[r, "\sigma_1^{-1}"] & E_1
\end{tikzcd}$$

DEF 3.3 Let

$$\hat{\phi} = \sigma_1^{-1} \circ \phi^* \circ \sigma_2$$

be called the *dual isogeny* of ϕ.

PROP 3.8 Let $\phi : E_1 \to E_2$ be an isogeny, and $m = \deg(\phi)$. Then $\hat{\phi} \circ \phi = [m]$.

PROOF.

Fix $Q \in E_2$, where $\phi(P) = Q$. Then $\sigma(Q) = [(Q) - (\mathcal{O})]$. Under ϕ^*, we have

$$\xrightarrow{\phi^*} \sum_{S \in \phi^{-1}(Q)} (S) - \sum_{T \in \phi^{-1}(\mathcal{O})} (T) = \left[\sum_{S \in \phi^{-1}(Q)} (S) - (\mathcal{O}) \right] - \left[\sum_{T \in \phi^{-1}(\mathcal{O})} (T) - (\mathcal{O}) \right]$$

$$\xrightarrow{\sigma_1^{-1}} \sum_{S \in \phi^{-1}(Q)} S - \sum_{T \in \phi^{-1}(\mathcal{O})} T$$

If $\phi(P) = Q$, then $\phi(P + T) = Q$ as well, since

$$\phi(P + T) = \phi(P) + \phi(T) = Q + \mathcal{O} = Q$$

Since $P + T$ provide distinct points for distinct T, and $\#\phi^{-1}(Q) = \#\phi^{-1}(\mathcal{O})$, we can write

$$\sum_{S \in \phi^{-1}(Q)} S - \sum_{T \in \phi^{-1}(\mathcal{O})} T = \sum_{T \in \phi^{-1}(\mathcal{O})} P + T - \sum_{T \in \phi^{-1}(\mathcal{O})} T = \sum_{T \in \phi^{-1}(\mathcal{O})} P = \deg(\phi)P = [m]P$$

□

PROP 3.9

$\hat{\phi}$ is the unique map satisfying $\hat{\phi} \circ \phi = [m]$.

PROOF.

We refer to Prop 3.6, with $E_3 = E_1$ and $\psi = [m]$.

$\# \ker(\phi) = \deg(\phi) = m$. Viewing $\ker(\phi)$ as a subgroup of E_1, then, every element has degree dividing m. Hence, $\ker(\phi) \subseteq \ker[m]$. It follows that there is a unique isogeny $\hat{\phi} : E_2 \to E_1$ with $\hat{\phi} \circ \phi = [m]$. □

PROP 3.10

$\hat{\hat{\phi}} = \phi$ and $\widehat{\phi \circ \psi} = \hat{\psi} \circ \hat{\phi}$

PROOF.

We show, equivalently, that $\phi \circ \hat{\phi} = [m]$ on E_2. We have

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ [m] = [m] \circ \phi$$

since ϕ is a homomorphism under the group law. Then, $[m] = \phi \circ \hat{\phi}$ as desired.

Let $\deg(\phi) = m$ and $\deg(\psi) = n$. Then

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [n] \circ [m] = [nm] \quad \square$$

PROP 3.11

$\langle \phi, \psi \rangle := \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$ is bilinear.

PROOF.

Instead of showing that this quantity is bilinear, we'll show that $[\langle \phi, \psi \rangle]$ is bilinear.

Since $[] : \mathbb{Z} \to \mathrm{End}(E_1)$ is injective, this suffices.

$$\begin{aligned}[\langle \phi, \psi \rangle] &= \widehat{\phi + \psi} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= (\hat{\phi} + \hat{\psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \quad \square\end{aligned}$$

PROP 3.12 $\deg[m] = m^2$

PROOF. $\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$. Hence, by induction, $\widehat{[m]} = [m]$. Let $d = \deg[m]$, and consider $[d]$.

$$[d] = \widehat{[m]} \circ [m] = [m]^2 = [m^2]$$

$\implies d = m^2$. □

In the above two propositions, we used the fact $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$. A proof of this is given in Appendix A.

IV Finite Fields and Supersingularity

In this section, we will focus on the theory of elliptic curves over finite fields, culminating in the definition of supersingularity. Supersingular curves and the isogenies between them form the basis for cryptographic applications.

HASSE'S BOUND

Consider an elliptic curve given by the Weierstrass form

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 : a_i \in \mathbb{F}_q$$

Clearly $\#E(\mathbb{F}_q) \leq |\mathbb{F}_p|^2 + |\{\mathcal{O}\}| = q^2 + 1$. We can do better: fixing $x \in \mathbb{F}_q$, our problem reduces to a normal quadratic in y, which has at most two solutions. Hence, $\#E(\mathbb{F}_q) \leq 2q + 1$. We can do even better. Artin introduced and Hasse proved the following in [9]:

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$$

Before we prove this, we introduce quadratic forms:

DEF 4.1 A map $d : A \to \mathbb{R}$, where A is an abelian group, is called a *quadratic form* if $d(a) = d(-a)$ and $(a, b) \mapsto d(a + b) - d(a) - d(b)$ is bilinear.

PROP 4.1 Let d be a positive-definite quadratic form. Let $L(a, b) = d(a - b) - d(a) - d(b)$. Then $|L(a, b)| \leq 2\sqrt{d(a)d(b)}$

PROOF.

Since d is positive definite, we can write

$$0 \leq d(ma - nb) = m^2 d(a) + mnL(a,b) + n^2 d(b)$$

Now, setting $m = -L(a,b)$ and $n = 2d(a)$, we find

$$0 \leq d(a)[4d(a)d(b) - L(a,b)^2]$$

Hence, when $a \neq 0$, we have that the RHS is positive, and hence $4d(a)d(b) - L(a,b)^2 \geq 0$, so we conclude that $|L(a,b)| \leq 2\sqrt{d(a)d(b)}$. □

Returning to the main result:

PROP 4.2 $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$

PROOF.

Consider $\phi : E \to E$ by $(x, y) \mapsto (x^q, y^q)$. Fundamentally, this is a map from $E \to E^{(q)}$, where $E^{(q)}$ replaces E's coefficients a_i with a_i^q. However, since $a_i \in \mathbb{F}_q$, we have that $\phi(a_i) = a_i$. So, indeed, $\phi : E \to E$.

The elements in $E(\mathbb{F}_q)$ are given by those that are fixed by the Frobenius map ϕ, i.e. $E(\mathbb{F}_q) = \ker(\mathrm{Id} - \phi)$. We write, then

$$\#E(\mathbb{F}_q) = \#\ker(\mathrm{Id} - \phi) = \deg(\mathrm{Id} - \phi)$$

Noting that $\deg(\phi) = q$ and $\deg(\mathrm{Id}) = 1$, this yields

$$|\#E(\mathbb{F}_q) - q - 1| = |\deg(\mathrm{Id} - \phi) - \deg(\phi) - \deg(\mathrm{Id})|$$

But we've shown that $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive-definite quadratic form in Prop 3.11, so we use Prop 4.1 to conclude

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{\deg(\phi)\deg(\mathrm{Id})} = 2\sqrt{q}$$

as desired. □

We proceed now with a series of examples and applications utilizing Hasse's bound, some of which will come in handy later:

Eg. 4.1.1 $\#E(\mathbb{F}_q) \approx q + 1$, by observing

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

Hence, by choosing a large prime power q, we may guarantee a large solution set $E(\mathbb{F}_q)$. This is the basis for the hardness problem posed below in 4.1.4.

Eg. 4.1.2 Let $E : y^2 = f(x) := ax^3 + bx^2 + cx + d$, with $a, b, c, d \in \mathbb{F}_q$, which has distinct roots in $\overline{\mathbb{F}_q}$. Consider the multiplicative group $\mathbb{F}_q^*$, and the order 2 character

$$\chi(a) = \begin{cases} 1 & a \text{ is a square} \\ -1 & \text{o.w.} \end{cases}$$

defined on $\mathbb{F}_q^*$. We can use χ to count $E(\mathbb{F}_q)$: if $f(x)$ is a square, then we see 2 solutions for y in $\mathbb{F}_q$; if it is not, then there are no solutions; if $f(x) = 0$, then we have 1 solution. Hence,

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(f(x))) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

where we extend χ by writing $\chi(0) = 0$.

It follows by Hasse's bound (Prop 4.2) that

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq 2\sqrt{q}$$

This hints at the fact that solutions to $f(x)$ will have squares and non-squares distributed evenly: the expected value of the sum of a random sequence of 1s and -1s is $\sqrt{q}$.

Eg. 4.1.3 Consider $E/\mathbb{F}_7 : y^2 = x^3 + 2$. We list the possible values for $x^3 + 2$:

x	$x^3 + 2 \mod 7$	square?
0	2	$3^2 = 2$
1	3	no
2	3	no
3	1	$1^2 = 1$
4	3	no
5	1	$1^2 = 1$
6	1	$1^2 = 1$

So our solutions are

$$\{\mathcal{O}, (0,3), (0,-3), (3,1), (3,-1), (5,1), (5,-1), (6,1), (6,-1)\}$$

All of these points satisfy $[3]P = \mathcal{O}$ (to see this, $\deg[3] = 9 = \ker([3])$, and we have only 9 solutions above to choose from), so we conclude that $E(\mathbb{F}_7) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, where $\mathcal{O} = (0,0)$.

Eg. 4.1.4 Over finite fields, elliptic curves may be used to encrypt messages. To do so, we consider a some intractable task. Assume $Q = [m]P$, where $P \in E(\mathbb{F}_q)$. Determining m exactly is a hard task, especially for large q (when q is small, just test each m). This is the basis of the following protocol:

1. E and $P \in E(\mathbb{F}_q)$ are public. Alice wants to send a message (say, $M \in E(\mathbb{F}_q)$) to Bob.
2. Bob has d as a private key and publishes $Q = [d]P$.
3. Alice picks a random integer k and computes $R = [k]P$ and $S = M + [k]Q$. She sends this to Bob.
4. Bob recovers M by computing $S + [-d]R$:

$$S + [-d]R = M + [k][d]P + [-d][k]P = M$$

If someone intercepts a message, they would have to find the integer $d : Q = [d]P$ to crack the code. This algorithm (an adaptation of the ElGamal system) is an early application of elliptic curves to cryptography ([10]).

SUPERSINGULAR ELLIPTIC CURVES

Let E/F be an extension. Then let $S = \{\alpha \in E : \alpha \text{ is separable over } F\}$. Then $E/S/F$, with E/S a purely inseparable extension and S/F a purely separable extension. DEF 4.2

Let $\phi : (x, y) \mapsto (x^p, y^p)$ be a morphism from $E \to E^{(p)}$. Let K be a perfect field of characteristic p. ϕ is purely inseparable. DEF 4.3

PROOF.

We first claim that $\phi^*(K(E)) = K(E)^p = \{\alpha^p : \alpha \in K(E)\}$.

We may view $K(E)$ as quotients $\frac{f}{g}$ of homogeneous polynomials f, g of the same degree. Hence, under the map ϕ^*, we have

$$\frac{f(x_0, ..., x_n)}{g(x_0, ..., x_n)} \mapsto \frac{f(x_0^p, ..., x_n^p)}{g(x_0^p, ..., x_n^p)}$$

However, elements in $K(E)^p$ are

$$\frac{f(x_0, ..., x_n)^p}{g(x_0, ..., x_n)^p}$$

But since K is perfect, all its elements are a p^{th} power, so

$$K(x_0, ..., x_n)^p = K(x_0^p, ..., x_n^p)$$

as sets. Its fraction fields, then, are also equivalent.

Consider now the extension $[K(E)/K(E)^p]$. Let $\alpha \in K(E)$. It has a minimal polynomial $t^p - \alpha^p$ in $K(E)^p[t]$. But in the larger field, this is $(t-\alpha)^p$. Hence, α is inseparable, and we are done. □

DEF 4.4 Let E be an elliptic curve and $\text{char}(K) = p$. Then $E[p] = \{\mathcal{O}\}$ or $E[p] \cong \mathbb{Z}/p\mathbb{Z}$.

PROOF. Let ϕ be the p^{th}-power Frobenius morphism. We have

$$\begin{aligned} \#E[p] &= \#\ker[p] = \deg_s[p] \\ &= \deg_s(\hat{\phi} \circ \phi) = [\deg_s(\hat{\phi}) \deg_s(\phi)] \end{aligned}$$

Here, we reintroduce the notion of separability degree, since the Frobenius homomorphism is inseparable. Recall that $\deg(\phi) = \deg(\hat{\phi}) = p$.

Suppose that $\hat{\phi}$ is separable. Then $\deg(\hat{\phi}) = \deg_s(\hat{\phi}) = p$, so $\#E[p] = \deg_s(\hat{\phi}) = p$. However, if $\hat{\phi}$ is inseparable, then $\#E[p] = 1$. In this latter case, its clear that $E[p] = \{O\}$.

If $\hat{\phi}$ is separable, then $E[p] = \mathbb{Z}/p\mathbb{Z}$, by structure theorem. (It's equivalent to a product of cyclic groups, whose orders divide eachother—but p is prime). □

We remark that $\#E[p^r] = 1$ or p^r by identitcal arguments, in which case $E[p^r] = \{\mathcal{O}\}$ or $\mathbb{Z}/p^r\mathbb{Z}$. The separability of $\hat{\phi}$ remains the deciding factor, so if $E[p^r] = \{\mathcal{O}\}$, for some r, $E[p^r] = \{\mathcal{O}\}$ for all r.

PROP 4.3 Let E be an elliptic curve and $\text{char}(K) = p$. Let ϕ_r be the p^r-power Frobenius map. Then the following are equivalent:

1. $E[p^r] = \{O\}$ for $r = 1, 2, \ldots$
2. $\hat{\phi}_r$ is purely inseparable for $r = 1, 2, \ldots$
3. $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$

PROOF. ($1 \iff 2$) Suppose $E[p^r] = \{O\}$. Then $\hat{\phi}_r$ must be inseparable, or else $\#E[p^r] = \deg_s(\hat{\phi}_r \circ \phi_r) = p^r$. We've already proven the converse.

($2 \implies 3$) For free, we get that $\hat{\phi} \circ \phi = [p]$ is purely inseparable. Hence, we just need to show that $j(E) \in \mathbb{F}_{p^2}$. Consider

$$\begin{tikzcd}
E^{(p)} \arrow[rr, "\hat{\phi}"] \arrow[dr, "\phi_1"'] & & E \\
& E^{(p^2)} \arrow[ur, "\psi"'] &
\end{tikzcd}$$

We claim that $\hat{\phi}$ factors as $\psi \circ \phi_1$, where ψ is some separable map.

Consider an arbitrary map $\lambda : E_1 \to E_2$ of smooth curves over characteristic p, with $\deg_i(\lambda) = p$.

We claim it factors as $E_1 \xrightarrow{\phi} E_1^{(p)} \xrightarrow{\psi} E_2$, where ϕ is the p^{th} power Frobenius morphism, and ψ is separable. We have, by our previous result,

$$K(E_1)^p = \phi^*(K(E_1^{(p)})) \quad \text{and} \quad [K(E_1) : \phi^*(K(E_1^{(p)}))] = \deg(\phi) = p$$

where the latter extension is purely inseparable. Let $\mathbb{K}$ be the separable closure of $\lambda^*(K(E_2))$ inside $K(E_1)$. Then $K(E_1)/\mathbb{K}$ is purely inseparable of degree $p = \deg_i(\lambda)$, so it follows that $K(E_1)^p \subseteq \mathbb{K}$. Then, $K(E_1)^{(p)} \subseteq \mathbb{K}$, since all elements in a purely separable extension are necessarily prime powers of the base field. Denoting the degree of an extension as *(separable, inseparable)*, we have

$$\begin{tikzcd}
K(E_1) \arrow[d, dash, "{(1,p)}"'] \arrow[dr, dash, "{(1,p)}"] & \\
\mathbb{K} \arrow[r, dotted, dash, "\supseteq" description] \arrow[d, dash] & K(E_1)^p = \phi^*(K(E_1^{(p)})) \\
\lambda^*(K(E_2)) &
\end{tikzcd}$$

So we get a tower of fields

$$\begin{tikzcd}
K(E_1) \arrow[d, dash] \\
\phi^*(K(E_1^{(p)})) \arrow[d, dash] \\
\lambda^*(K(E_2))
\end{tikzcd}$$

Then, because we have an injection of fields, we know there are associated unique isogenies. Consider each at a time:

1. For the injection $\lambda^* : K(E_2) \hookrightarrow K(E_1)$, $\lambda : E_1 \to E_2$ is our given isogeny.

2. For the injection $\phi^* : K(E_1^{(p)}) \hookrightarrow K(E_1)$, $\phi : E_1 \to E_1^{(p)}$ is the Frobenius morphism, as given.

3. For the injection $\phi^{*-1}\lambda^* : K(E_2) \hookrightarrow K(E_1^{(p)})$, we set $\psi^* = (\lambda \circ \phi^{-1})^*$, implying $\lambda = \psi \circ \phi$, as desired. Since this extension is purely separable, so is the isogeny ψ.

Returning to our setting, we have

$$\begin{tikzcd}
E^{(p)} \arrow[rr, "\hat{\phi}"] \arrow[dr, "\phi_1"'] & & E \\
& E^{(p^2)} \arrow[ur, "\psi"'] &
\end{tikzcd}$$

since $p = \deg_i(\hat{\phi})$ by assumption. ψ is separable by the result above, so its inseparability degree is 1. But since $\deg_s(\hat{\phi}) = 1 = \deg_s(\phi_1)\deg_s(\psi)$, we have that $\deg(\psi) = 1$. All maps of degree 1 must be isomorphisms, since then $\psi^* : K(E) \cong K(E^{(p^2)})$ is an isomorphism of function fields.

Hence, as isomorphic elliptic curves, $j(E) = j(E^{p^2}) = j(E)^{p^2}$, since we raise all coefficients to the p^2-th power. Recall that all fields $\mathbb{F}_q$ are characterized by elements α with $\alpha^q = \alpha$, so we conclude that $j(E) \in \mathbb{F}_{p^2}$.

($3 \implies 2$). For the converse, if $[p]$ is purely inseparable, then $\hat{\phi}$ must be, since ϕ is inseparable. And we are done. □

DEF 4.5 If an elliptic curve E satisfies Prop 4.3, we say it is *supersingular*. Otherwise E is *ordinary*.

PROP 4.4 Given a field K of characteristic p, there are finitely many supersingular curves E.

PROOF. If E is supersingular, then $j(E) \in \mathbb{F}_{p^2}$. Hence, we can have up to p^2 supersingular curves up to isomorphism, by Prop 2.1. □

We turn to a more concrete way of detecting supersingular curves, which will eventually allow us to count, exactly, the number of such curves in a given characteristic (Thm 4.2).

4.1 Algebraic Characterization of Supersingularity

Let $\mathbb{F}_q$ be a field of characteristic $p \geq 3$. Let $E/\mathbb{F}_q$ be an elliptic curve in Weierstrass form given by $y^2 = f(x)$, where f is a cubic polynomial with distinct roots.

E is supersingular $\iff$ the coefficient of x^{q-1} in $f(x)^{\frac{q-1}{2}}$ is zero.

PROOF. We take the following as a black-box theorem, from the study of invariant differentials. Let $E/\mathbb{F}_q$ be an elliptic curve. Let ϕ be the q^{th}-power morphism. Then, for $m, n \in \mathbb{Z}$, $[a] + [b]\phi$ is separable $\iff a \not\equiv_p 0$. ★

Recall the character

$$\chi : \mathbb{F}_q^* \to \{-1, 1\}$$

that sets α to -1 for non-squares, and 1 otherwise. Extend it to the full field $\mathbb{F}_q$ by setting $\chi(0) = 0$. Recall Example 4.1:

$$\#E(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$$

But $\mathbb{F}_q^*$, the multiplicative group, is cyclic of order $q-1$, so $z^{q-1} = 1$ for $z \in \mathbb{F}_q^*$. Therefore, by Euler's Criterion,

$$z^{\frac{q-1}{2}} = \begin{cases} -1 & z \text{ non-square mod } q \\ 1 & z \text{ square mod } q \end{cases}$$

For $z = 0$, we can extend this by observing $0^{\frac{q-1}{2}} = 0$, and hence

$$\#E(\mathbb{F}_q) = 1 + q + \sum_{z \in \mathbb{F}_q} f(z)^{\frac{q-1}{2}} \equiv_p 1 + \sum_{z \in \mathbb{F}_q} f(z)^{\frac{q-1}{2}}$$

Since f is a cubic, $f(x)^{\frac{q-1}{2}}$ may have terms like x^n for $0 \leq n \leq \frac{3}{2}(q-1)$. Hence, $q-1|n$ only when $q-1 = n$. Utilizing the cyclic nature of $\mathbb{F}_q^*$, we have

$$\sum_{x \in \mathbb{F}_q} x^i = \begin{cases} -1 & q-1|i \\ 0 & \text{o.w.} \end{cases}$$

Summing over $x \in \mathbb{F}_q$, then, we see that the only non-zero terms come from x^{q-1}, so

$$\#E(\mathbb{F}_q) \equiv_p 1 + (-1) \cdot A_q = 1 - A_q \quad : \quad A_q = \text{coefficient of } x^{q-1} \text{ in } f(x)^{\frac{q-1}{2}}$$

On the other hand, $\#E(\mathbb{F}_q) = \deg(1-\phi) = 1 - a + q$, where ϕ is the q^{th} power morphism, and $a = 1 - \deg(1-\phi) + \deg(\phi)$. Modulo p, then, $A_q = a$, and we conclude $a \equiv_p 0 \iff A_q = 0$.

Why is it that $\#E(\mathbb{F}_q) = \deg(1-\phi)$? This is $\#\ker(1-\phi) = \#\{(x,y) \in E : (x^q, y^q) = (x,y)\}$, which precisely describes points (x,y) which appear in $\mathbb{F}_q$ (recall that $\mathbb{F}_q$ is the splitting field of $x^q - x$). We write

$$[1 - a + q] = \widehat{1-\phi} \circ (1-\phi) = 1 - \hat{\phi} - \phi + \hat{\phi}\phi$$

Since $[m]P = \overbrace{P + \ldots + P}^{p \text{ times}}$, $[m+n]P = [m]P + [n]P$. Hence,

$$\text{Id} - [a] + [q] = \text{Id} - \hat{\phi} - \phi + [q] \implies [a] = \hat{\phi} + \phi$$

So $a \equiv_p 0 \iff \hat{\phi}$ is inseparable, using ★, and this holds if and only if E is supersingular.

□

As it turns out $A_q = 0 \iff A_p = 0$, so the theorem holds when q is replaced by p.

PROP 4.5 Let $m = \frac{p-1}{2}$. Define

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$$

Then, the elliptic curve

$$E : y^2 = x(x-1)(x-\lambda) \quad : \quad \lambda \neq 0, 1$$

is supersingular $\iff H_p(\lambda) = 0$.

PROOF. We will use Thm 4.1. In particular, E is supersingular $\iff$ the coefficient of x^{p-1} in $[x(x-1)(x-\lambda)]^m$ is 0.

Write $x^m(x-1)^m(x-\lambda)^m = x^m g(x)$. The coefficient of x^m in $g(x)$ will give (when multiplied by x^m), the coefficient of $x^{2m} = x^{p-1}$ in the original equation.

$$g(x) = (x-1)^m(x-\lambda)^m \implies c : cx^m \in g(x) = \sum_{i=0}^{m} \binom{m}{i}(-\lambda)^i \binom{m}{m-i}(-1)^{m-i}$$

For this, recall that

$$(x-\lambda)^m = \sum_{i=0}^{m} \binom{m}{i} x^{m-i}(-\lambda)^i \quad \text{and} \quad (x-1)^m = \sum_{j=0}^{m} \binom{m}{j} x^{m-j}(-1)^j$$

Hence, to find the x^m term in $(x-1)^m(x-\lambda)^m$, we multiply each LHS summand i with the RHS summand for $j = m - i$. Substituting, then, yields the result. We compute:

$$\sum_{i=0}^{m} \binom{m}{i}(-\lambda)^i \binom{m}{m-i}(-1)^{m-i} = \sum_{i=1}^{m} \binom{m}{i}^2 \lambda^i (-1)^m$$

which equals $H_p(\lambda)$ up to a sign. □

Eg. 4.2.1 Consider $E/\mathbb{F}_3$ by $y^2 = x^3 - x$. This factors, mod 3, as $x(x+1)(x+2)$. With distinct roots, we are able to invoke Thm 4.1. The coefficient of $x^{p-1} = x^2$ in $(x^3 - x)^{\frac{3-1}{2}} = x^3 - x$ is 0, so $x^3 - x$ is indeed supersingular. We can calculate its j-invariant directly. Ignoring the x^2 and 1 coefficients:

$$j(E) = \frac{2^8 3^3 \cdot 1}{4} = 1728 \equiv_9 0$$

Hence, $j(E)^2 \equiv_9 j(E)$, and $j(E) \in \mathbb{F}_{p^2}$.

Eg. 4.2.2 However, over $\mathbb{F}_5$, 1728 is 3 mod 5, and $j(E)^2$ is $2,985,984$, which is 4 mod 5. So $j(E) \notin \mathbb{F}_{p^2}$. We conclude that $y^2 = x^3 - x$ cannot not be supersingular. Indeed, $(x^3 - x)^{\frac{5-1}{2}} = (x^3 - x)^2$ has a $p - 1 = 4$th power coefficient.

4.2 Counting Supersingular Elliptic Curves

Let $\overline{K}$ be a characteristic $p \geq 5$ field. The number of supersingular elliptic curves, up to isomorphism, is exactly

$$N = \left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & p \equiv_{12} 1 \\ 1 & p \equiv_{12} 5, 7 \\ 2 & p \equiv_{12} 11 \end{cases}$$

If $\text{char}(K) = 3$, then there is only one supersingular curve.

Before we prove this, we prove the following:

Let $E_\lambda : y^2 = x(x-1)(x-\lambda)$ be an elliptic curve, where $\text{char}(K) \neq 2$. Then every elliptic curve $\hat{E}$ is isomorphic to E_λ for some $\lambda \neq 0, 1 \in \overline{K}$. **PROP 4.6**

PROOF.

Recalling Example 2.1, since $\text{char}(K) \neq 2$, we can write $\hat{E}$ as

$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

Replacing $(x, y) \mapsto (x, 2y)$ yields

$$y^2 = x^3 + \frac{b_2}{4} x^2 + \frac{b_4}{2} x + \frac{b_6}{4}$$

which, as a monic cubic, may be factored as

$$y^2 = (x - e_1)(x - e_2)(x - e_3) : e_i \in \overline{K} \qquad \star$$

The discriminant of this equation, $16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2$, is non-zero by the smoothness assumption, so all roots are distinct. Finally, we perform the transformation

$$(x, y) \mapsto \left((e_2 - e_1)x + e_1, (e_2 - e_1)^{\frac{3}{2}} y\right)$$

This yields, on the RHS of $\star$:

$$\begin{aligned} &(e_2 - e_1)x\left((e_2 - e_1)x + e_1 - e_2\right)\left((e_2 - e_1)x + e_1 - e_3\right) \\ =&(e_2 - e_1)^3 \left[x(x-1)\left(x + \frac{e_1 - e_3}{e_2 - e_1}\right)\right] \end{aligned}$$

and, on the LHS, $(e_2 - e_1)^3 y^2$. Canceling, we have

$$y^2 = x(x-1)\left(x + \frac{e_1 - e_3}{e_2 - e_1}\right)$$

as desired. □

PROP 4.7 The map $\eta : \overline{K} \setminus \{0,1\} \to \overline{K}$ by $\lambda \mapsto j(E_\lambda)$ is surjective and six-to-one. (Except at $j = 0, 1728$, which are two-to-one and three-to-one, respectively).

PROOF. We compute the j-invariant of $x(x-1)(x-\lambda)$ to be

$$j(E_\lambda) = \frac{16^2(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}$$

Since the j-invariant is always written this way, the map is surjective. We also observe that $(1-\lambda)$ and $\frac{1}{\lambda}$ preserve the map:

$$\frac{1}{\lambda} : \frac{\left(\frac{1-\lambda+\lambda^2}{\lambda^2}\right)^3}{\frac{1}{\lambda^2}\frac{(\lambda-1)^2}{\lambda^2}} \qquad 1-\lambda : \frac{(\lambda^2-\lambda+1)^3}{(1-\lambda)^2(-\lambda)^2}$$

so therefore $\frac{1}{1-\lambda}$ and $1 - \frac{1}{\lambda} = \frac{\lambda-1}{\lambda}$ preserve the map, and hence also $\frac{\lambda}{\lambda-1}$. This provides us with all six (by including λ) mappings: $\left\{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}\right\}$.

When $j = 0$, $\lambda^2 - \lambda + 1 = 0 \implies \lambda^2 = \lambda - 1$. But then $\lambda^2 = (\lambda-1)^2 = \lambda^2 - 2\lambda + 1 = -\lambda$, and hence

$$1 - \lambda = -\lambda^2 = \lambda \qquad \frac{1}{1-\lambda} = \frac{-1}{\lambda^2} = \frac{1}{\lambda}$$

$$\frac{\lambda-1}{\lambda} = \frac{\lambda^2}{\lambda} = \lambda \qquad \frac{\lambda}{\lambda-1} = \frac{1}{\lambda}$$

which makes η two-to-one. When $j = 1728$, we have $\lambda = -1$. But then our mappings are

$$\left\{-1, -1, 2, \frac{1}{2}, 2, \frac{1}{2}\right\}$$

which makes η three-to-one. □

PROP 4.8 Fix a field of characteristic $p \geq 5$. Let

$$\varepsilon(j) = \begin{cases} 1 & E_\lambda : j(E_\lambda) = j \text{ is supersingular} \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\varepsilon(0) = \begin{cases} 0 & p \equiv_3 1 \\ 1 & p \equiv_3 2 \end{cases} \qquad \varepsilon(1728) = \begin{cases} 0 & p \equiv_4 1 \\ 1 & p \equiv_4 3 \end{cases}$$

PROOF.

The curve $y^2 = x^3 + 1$ has j-invariant 0:

$$j(y^2 = x^3 + Ax + B) = \frac{2^8 3^3 A^3}{4A^3 + 27B^2}$$

For which values of p is $y^2 = x^3 + 1$ supersingular? We know, by a previous criterion, that we should look for coefficient of x^{p-1} in $(x^3 + 1)^{\frac{p-1}{2}}$. If $p \equiv_3 2$, then we find terms of powers x^{3k} by the binomial theorem. But $p - 1 \equiv 1$, so no such powers exist in the expansion. Hence, $y^2 = x^3 + 1$ is supersingular.

Now suppose $p \equiv_3 1$. Then $\frac{p-1}{2} \equiv 0$. By the binomial theorem, again, the $p - 1^{th}$ power has coefficient

$$\binom{\frac{p-1}{2}}{\frac{p-1}{3}}$$

by setting $3k = p - 1$. So $y^2 = x^3 + 1$ is ordinary.

The curve $y^2 = x^3 + x$ has j-invariant 1728:

$$\frac{2^8 3^3 \cdot 1}{4} = 1728$$

We rewrite $x(x^2 + 1)$. The coefficient of x^{p-1} in $[x(x^2 + 1)]^{\frac{p-1}{2}}$ is equivalent to the coefficient of $x^{\frac{p-1}{2}}$ in $x^2 + 1$. By the binomial theorem, terms in $(x^2 + 1)^{\frac{p-1}{2}}$ have powers x^{2k}. When $p \equiv_4 3$, then $\frac{p-1}{2} \equiv_4 1$. But $2k \equiv_4 2$ or 4. Hence, no $\frac{p-1}{2}^{th}$ power exists, and the curve is supersingular.

By the binomial theorem, the $\frac{p-1}{2}^{th}$ term has coefficient

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$$

by setting $2k = \frac{p-1}{2}$. So $y^2 = x^3 + x$ is ordinary.

□

We now return to the proof of Thm 4.2:

PROOF. Recall the definition of $H_p(t)$:

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i \qquad m := \frac{p-1}{2}$$

In $\overline{\mathbb{F}_q}$, this has distinct roots. Each root λ will give a supersingular polynomial

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

$H_p(t)$ has $m = \frac{p-1}{2}$ distinct roots. For almost all choices of λ, the map $\eta : \lambda \mapsto j(E_\lambda)$ is six-to-one, so our discussions above yield $\frac{1}{6} \cdot \frac{p-1}{2} = \frac{p-1}{12}$ supersingular curves up to isomorphism. However, we need to account for j-invariants 0 or 1728.

Suppose that the elliptic curve associated to j-invariant 0 is supersingular, but that of 1728 is ordinary. $H_p(\lambda)$ has $\frac{p-1}{2}$ roots. How many of those roots are dedicated to E_0?

If E_0 is supersingular, then $\eta^{-1}(0)$ is a root of $H_p(t)$. But $\eta^{-1}(0)$ has size two by our discussion, so we identify two roots $\{\lambda', \lambda\}$ of $H_p(t)$ whose elliptic curves $E_\lambda \cong E_{\lambda'}$ have j-invariant 0. All $(p-1)/2 - 2$ other roots belong to j-invariants *not* 0 or 1728, so we have

$$\frac{1}{6}\left(\frac{p-1}{2} - 2\right) + 1$$

total supersingular curves, where the "+1" accounts for E_λ itself. Following this logic, and adapting notation, our number of curves is exactly

$$\begin{aligned} N &= \frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon(0) - 3\varepsilon(1728)\right) + \varepsilon(0) + \varepsilon(1728) \\ &= \frac{p-1}{12} + \frac{2}{3}\varepsilon(0) + \frac{1}{2}\varepsilon(1728) \end{aligned}$$

Note that ε relies on the characteristic p. Reworking the result of Prop 4.8, we have

$$(\varepsilon(0), \varepsilon(1728)) = \begin{cases} (0,0) & p \equiv_{12} 1 \\ (1,0) & p \equiv_{12} 5 \\ (0,1) & p \equiv_{12} 7 \\ (1,1) & p \equiv_{12} 11 \end{cases} \implies N = \frac{p-1}{12} + \begin{cases} 0 & p \equiv_{12} 1 \\ \frac{2}{3} & p \equiv_{12} 5 \\ \frac{1}{2} & p \equiv_{12} 7 \\ \frac{7}{6} & p \equiv_{12} 11 \end{cases}$$

To yield the final result, we do case analysis. When $p = 3$, $H_3(t) = 1 + t$, so only $y^2 = x(x-1)(x+1) = x^3 + x$ is supersingular. □

V Supersingular Isogeny Graphs

Isogenies, as homomorphisms, preserve supersingularity: if $P \in E_1[p]$, then $p(P) = \mathcal{O}_1$. However, then, $[p]P = \phi([p]P) = \mathcal{O}_2$, where $\phi : (E_1, \mathcal{O}_1) \to (E_2, \mathcal{O}_2)$. (See Prop 4.3). This allows us to consider the graph of isogenous supersingular curves of a specified degree:

DEF 5.1 Fix a field $\mathbb{F}_p$. Let $\mathcal{G}_\ell(p) = (V, E)$ be the graph such that $V = \{\text{supersingular curves over } \mathbb{F}_p\}$ and $uv \in E$ if and only if there exists a degree-ℓ isogeny $\phi : E_u \to E_v$, where ℓ is prime. We typically let $u \in V$ be represented by a j-invariant. $\mathcal{G}_\ell(p)$ is called an *ℓ-isogeny graph*.

DEF 5.2 Let $E[n] : \{P \in E : [n]P = \mathcal{O}\}$, and call a point $Q \in E[n]$ an *n-torsion point*.

PROP 5.1 $\mathcal{G}_\ell(p)$ is an undirected graph which is $(\ell + 1)$-regular, up to automorphism.

PROOF. Prop 3.8 guarantees that $uv \in E \iff vu \in E$ by taking the dual. By Prop 3.2, an isogeny $\phi : E \to E_i$ is a homomorphism. As a morphism, it is also surjective, and so $E/\ker(\phi) = E_i$. Since ℓ is prime, ϕ must be separable.

By Prop 3.4, $\#\ker(\phi) = \ell$, so $[\ell]P = \mathcal{O}$ for $P \in \ker(\phi)$. Hence, $\ker(\phi) < E[\ell]$, and we therefore associate subgroups of $E[\ell]$ with separable isogenies. How many subgroups exist?

$E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. We know by Prop 3.12 that $\deg[\ell] = \#\ker([\ell]) = \#E[\ell] = \ell^2$. Since $E[\ell]$ is abelian, this leaves $(\mathbb{Z}/\ell\mathbb{Z})^2$ or $\mathbb{Z}/\ell^2\mathbb{Z}$. The former would suggest an element of order ℓ^2, which cannot exist in $E[\ell]$, so the result follows.

There are $\ell + 1$ subgroups of $(\mathbb{Z}/\ell\mathbb{Z})^2$, and the result follows. If E has an extra automorphism ι (which is true when $j = 0$ or $j = 1728$), then it may be that unequal kernels quotient to the same elliptic curve by post-composing ι^i with this automorphism. □

PROP 5.2 $\mathcal{G}_\ell(p))$ has $\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & p \equiv_{12} 1 \\ 1 & p \equiv_{12} 5, 7 \\ 2 & p \equiv_{12} 11 \end{cases}$ vertices, all in $\mathbb{F}_{p^2}$.

PROOF. Direct from Thm 4.2 and Prop 4.3. □

From this point onward, we will focus on $\mathcal{G}_2(p)$, detailing some special properties essential to their computation and a foundational cryptographic application.

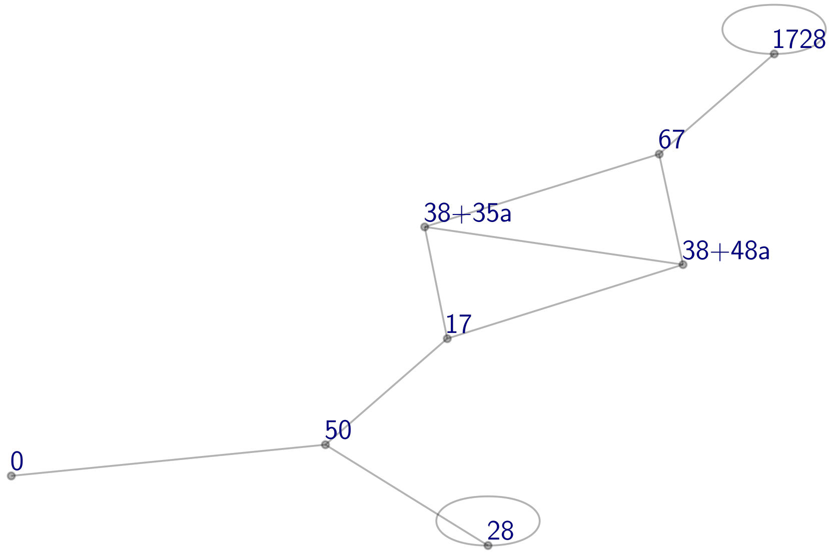


Figure 3: $\mathcal{G}_2(83)$. Notice the extra automorphisms of $j = 0$ and $j = 1728$.

PROP 5.3 Let $\phi : E_1 \to E_2$ be such that $E_1/\langle P \rangle = E_2$ for $P \in E_1[2]$. Then $\phi(Q_1) = \phi(Q_2) \in E_2[2]$ for the other two non-trivial torsion points $Q_i \in E_1[2]$. Furthermore, $\ker(\hat{\phi}) = \langle \phi(Q_i) \rangle$.

PROOF. Since ϕ is a homomorphism in E_1, we have $[2]\phi(Q_1) = \phi([2]Q_1) = \phi(\mathcal{O}_1) = \mathcal{O}_2 \implies \phi(Q_i) \in E_2[2]$. Furthermore, since $E_1[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, $P + Q_1 = Q_2$. Hence, under the quotient map, $Q_1 \sim Q_2$.

The dual $\hat{\phi}$ satisfies $\hat{\phi} \circ \phi(Q_i) = [2]Q_i = \mathcal{O}_1$, so indeed $\ker(\hat{\phi}) = \langle \phi(Q_i) \rangle$, and we can reverse the isogeny by quotienting $E_2/\langle \phi(Q_i) \rangle$. □

PROP 5.4 Let $\langle P \rangle < E$ be an order 2 subgroup of $E : y^2 = x^3 + Ax + B$, with $\mathrm{char}(K) \neq 2, 3$ and $P = (x_0, 0) \in E$. Then $E/\langle P \rangle$ is given by

$$y^2 = x^3 + (A - 5t)x + (B - 7x_0 t)$$

where $t = 3x_0^2 + A$, under the mapping

$$(x, y) \mapsto \left(\frac{x^2 - x_0 x + t}{x - x_0}, \frac{(x - x_0)^2 - t}{(x - x_0^2)} y \right)$$

PROOF. These formulas are proven in generality for finite subgroups of E in [15]. □

DEF 5.3 Let $\alpha \in \mathbb{F}_{p^2}$. We define a magnitude $S(\alpha) := a + br$, where $a, b \in \mathbb{F}_p$, and α is written uniquely as $a + b\sqrt{r}$, where we view $\mathbb{F}_{p^2} \cong \mathbb{F}_p/\langle x^2 - r \rangle$ for some non-quadratic residue r.

5.1 Random Walks on a 2-Isogeny Graph

We outline a procedure for traversing a 2-isogeny graph, while minding not to backtrack. Let $p \geq 5$ be a prime, and let r be a fixed non-quadratic residue in $\mathbb{F}_p$. Let $\mathcal{N}_{0,1} \in \{0,1\}$ be a random distribution. Denote by E_j the supersingular curve with j-invariant j.

Require: Prime $p \geq 5$, non-quadratic residue r, N bits sampled from $\mathcal{N}_{0,1}$.
Ensure: A walk of length N along the 2-isogeny graph, with nodes in $\mathbb{F}_{p^2}$.

```
1:  if $p \equiv_{12} 1$ then
2:      see Prop 6.1
3:  else if $p \equiv_{12} 5$ then
4:      $j_{\text{prev}} \leftarrow 0$
5:      $P_{\text{prev}} \leftarrow (1, 0)$
6:  else                                                          ▷ $p \equiv_{12} 7, 11$
7:      $j_{\text{prev}} \leftarrow 1728$
8:      $P_{\text{prev}} \leftarrow (0, 0)$
9:  for $i \in [N]$ do
10:     $b \leftarrow \mathcal{N}_{0,1}$
11:     $T \leftarrow$ 2-torsion points on $E_{j_{\text{prev}}}$
12:     $Q \leftarrow \textbf{argmin}_{Q \in T \setminus \{P_{\text{prev}}\}} S(Q_x) \cdot (-1)^b$, where $Q = (Q_x, Q_y)$
13:     $\phi \leftarrow$ quotient map $E_{j_{\text{prev}}} \twoheadrightarrow E_{j_{\text{prev}}} / \langle Q \rangle$      ▷ by Vélu
14:     $j_{\text{prev}} \leftarrow \phi(E_{j_{\text{prev}}})$
15:     $P_{\text{prev}} \leftarrow \phi(Q)$
16:     output $j_{\text{prev}}$
```

PROOF.

We begin the algorithm by finding an explicit supersingular curve in characteristic p. Prop 4.8 outlines suitable choices except when $p \equiv_{12} 1$, which we will investigate in the next section. (Lines 1-8).

Def 5.2 provides an ordering on elements in $\mathbb{F}_{p^2}$, allowing us to choose between two isogenous curves (not including the one previously visited), corresponding to two 2-torsion points. (Lines 10-13).

Prop 5.3 tells us that, if we quotient by $\phi(P_{\text{prev}})$, we will return to $E_{j_{\text{prev}}}$ (Line 15). □

When we feed this algorithm a string of bits to replace $\mathcal{N}_{0,1}$, we produce an interesting hashing function.

DEF 5.4

Let B be a string of $N = \lfloor \log_2(p) \rfloor$ bits. Traverse along $\mathcal{G}_2(p)$ according to Thm 5.1, replacing Line 10 with $b \leftarrow B[i]$. Let j be the final output of the algorithm. Then let $H_p : B \mapsto j$ be called the *CGL hash function*, as formulated in [4].

One should choose some embedding of the final j-invariant into $\mathbb{F}_p$. For our purposes, we will simple refer to the j-invariant itself (e.g. $H_{277}(\texttt{01000111}) = 261 + 198a$).

VI Implementation and Results

The algorithm provided is useful for two reasons: it generates all supersingular j-invariants via the Monte Carlo method (e.g. traverse $\mathcal{G}_2(p)$ until we find the number of nodes detailed in Thm 4.2); and it can hash binary strings, as in Def 5.3. We will discuss $\mathcal{G}_2(p)$ in light of these uses, and provide details on our implementation.

ARITHMETIC OF GRAPH GENERATION

The algorithm in Thm 5.1 was implemented in Python without the use of any symbolic algebraic tools (Sage, Magma, etc.). We outline the process here, and demonstrate some computational results:

1. $\mathbb{F}_{p^2}$ is implemented as the splitting field $\mathbb{F}_p/\langle x^2 - r\rangle$ for some non-quadratic residue r mod p. We perform operations on $(a + b\sqrt{r})$ in the typical way, e.g.

$$(a+b\sqrt{r})^{-1} = a(a^2 - rb^2)^{-1} - b(a^2 - rb^2)^{-1}\sqrt{r}$$

2. In (1), we require inverses in $\mathbb{F}_p$. Computing α^{-1} mod p is equivalent to finding x such that

$$\alpha x + py = 1$$

which is Bézout's identity. Hence, we perform the Euclidean algorithm on $\gcd(\alpha, p)$ and recover (x, y). This runs in $O(\log(\alpha))$, an improvement of the naive solution, i.e. trying combinations in $O(p)$.

3. Supposing $j_{\text{prev}} = (x_0, 0)$ and P_{prev} are known, we need to identify the two other torsion points on $E_{j_{\text{prev}}} : y^2 = x^3 + Ax + B$. Roots of the form $(x, 0)$ have order 2, since the tangent line there passes through $\mathcal{O}$. Hence, factoring out x_0 yields

$$x^2 + x_0 x + (A + x_0^2)$$

which has discriminant $-3x_0^2 - 4A \implies x = \frac{-x_0 \pm \sqrt{-3x_0^2 - 4A}}{2}$.

4. In (3), we require a square root function over $\mathbb{F}_p$. A generalized version of the Tonelli-Shanks algorithm for even extensions of $\mathbb{F}_p$, detailed in [1], is employed here. Note that this requires a square root function in $\mathbb{F}_p$, for which we use the typical Tonelli-Shanks. Exponentiation is essential to both algorithms—for this, we adapt a square-and-multiply technique.

GENERATING SUPERSINGULAR j-INVARIANTS WHEN $p \equiv_{12} 1$

We discuss Line 2 of Thm 5.1: given $p \equiv_{12} 1$, how can we generate a supersingular elliptic curve in $\mathbb{F}_p$ and one of its 2-torsion points?

PROP 6.1 Consider a quadratic imaginary field K. Let E be an elliptic curve in $\overline{K}$ with complex multiplication. Then E has a good reduction in $\mathbb{F}_p$, where $j(E) \in \mathbb{Z}$ if K has class number one. In particular, if p is inert in K, then the reduction is supersingular.

PROOF. Reductions of curves are covered in II.6 of [13], and the full "complex multiplication method" to generating supersingular curves in [2] and [5]. □

Eg. 6.1.1 $j(\frac{1+\sqrt{-d}}{2})$ is a good example of a complex j-invariant in $K = \mathbb{Q}(\sqrt{-d})$, where j is the j function. The class one fields of this form are exactly $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ (the "Heegner numbers", see [6]).

Eg. 6.1.2 When $d = 1$, i.e. in $\mathbb{Q}(i)$, we consider $j(\frac{1+\sqrt{-1}}{2}) = 1728$. We know this curve has complex multiplication (an automorphism of order 2). p is inert when -1 is a non-square residue in $\mathbb{F}_p$, which occurs when $p \equiv 3 \mod 4$. This is consistent with Prop 4.8.

Eg. 6.1.3 Examples of complex j-invariants for $\mathbb{Q}(\sqrt{-d})$, written $(-d, j)$, are

$$(-1, 1728) \quad (-3, 0) \quad (-2, 8000) \quad (-7, -3375) \quad (-11, -32768)$$

Once a suitable j-invariant is found, we can reconstruct the elliptic curve, where $j \neq 1728$:

$$y^2 = x^3 - \frac{3j}{j-1728}x + \frac{2j}{j-1728}$$

The first root of this equation can be solved naively via brute force, with the general cubic formula, etc., to find the first torsion point. This slow down is negligible in a traversal of $\mathcal{G}_2(p)$, as it only is required for the initial j-invariant.

PROP 6.2 The primes for which, in light of Prop 4.8 and Prop 6.1, we cannot yet identity a supersingular elliptic curve have density $2^{-9} \approx 0.001953$.

PROOF. We find a supersingular reduction in $\mathbb{F}_p$ from a class one quadratic field $\mathbb{Q}(\sqrt{-d})$ if an only if

$$\left(\frac{-d}{p}\right) = -1$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. When $d \geq 3$ is a prime, we have, by quadratic reciprocity,

$$\left(\frac{-d}{p}\right)\left(\frac{-p}{d}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{d-1}{2}}\left(\frac{d}{p}\right)\left(\frac{p}{d}\right) = (-1)^{p-1}(-1)^{q-1} = 1$$

Hence, asking whether $-d = x^2$ in $\mathbb{F}_p$ is equivalent to asking whether $-p = x^2$ in $\mathbb{F}_q$. For fixed p, then, the probability that $-p$ it is a quadratic residue in any given field $\mathbb{F}_d$

is $\frac{1}{2}$. Considering over all class one fields gives the result. □

The first 10 primes p for which neither 1728 nor 0 are supersingular j-invariants in $\mathbb{F}_p$, nor do any integer ones exist via a reduction in a quadratic imaginary field, are:

$i : p = i^{\text{th}}$ prime	p	i	p
1760	15073	9603	100153
2100	18313	10131	106297
4091	38833	10216	107209
6883	69337	10322	108529
7090	71593	10581	111577

Notice that these are all $p \equiv_{12} 1$. The empirical density of these primes is `0.001694` over the first 500,000 primes, which is consistent with Prop 6.2.

TRAVERSING $\mathcal{G}_2(p)$

A typical hash appears as a path $P \in \mathcal{G}_p(2)$, since our prime p (and therefore $|V(\mathcal{G}_2(p))|$) is exponential in traversal length. For instance:

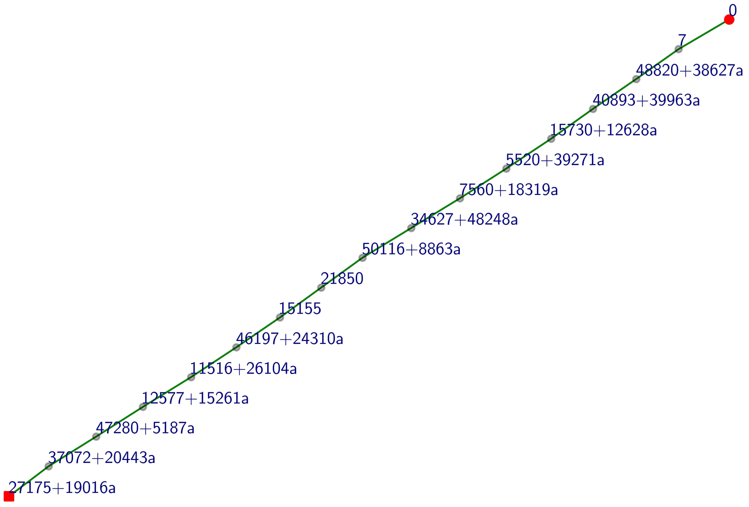


Figure 4: $H_{53993}(\texttt{0000110101001011}) = 27175 + 19016a$

Occasionally, we find loops, i.e. 2-isogenies $\phi : E_j \to E_j$. When $j = 1728$, we observe an extra automorphism via complex multiplication, and so all $\mathcal{G}_2(p) : p \equiv_4 3$ contain this loop. We find more examples by considering the modular polynomial $\Phi_2(x, y)$, as detailed in Exercise 2.18 of [13]. All cyclic 2-isogenies $\phi : E_x \to E_y$, are represented by the roots of this polynomial, which factors as

$$\Phi_2(x, x) = -(x + 3375)^2(x - 1728)(x - 8000)$$

Notice that these correspond to curves in $\mathbb{Q}(\sqrt{-d})$ with complex multiplication for $d = -1, -2,$ and -7 (Example 6.1). In **Figure 3**, $\left(\frac{-7}{83}\right) = -1$, and hence $-3375 \equiv_{83} 28$ has a loop.

FINDING COLLISIONS IN $\mathcal{G}_2(p)$

When hashing, we care that finding the preimage of our output (the traversal taken to reach our final j-invariant) is hard, and that finding a collision (e.g. two 2^k-isogenies between curves for $k < N$) is hard.

The former problem is equivalent to computing the endomorphism ring of a given output curve E, a problem which is exponential in p ([7], [3]). The latter problem is made hard by ensuring no cycles of bounded length $2N$ exist containing our initial j-invariant.

Let E_p be the initial supersingular elliptic curve generated by Thm 5.1. Let $N = \lfloor \log_2(p) \rfloor$. DEF 6.1
Let $\phi, \tilde{\phi}$ be two 2^N-degree isogenies from E_p corresponding to a cycle of length $2N$ in $\mathcal{G}_2(p)$. Then $\mathcal{G}_2(p)$ has a *hard collision*.

Eg. 6.2.1 The first prime for which $\mathcal{G}_2(p)$ contains a hard collision is 277, which has 71 offending isogenies of degree $\ell^{2N} = 2^{16}$. In other words, there exist 71 collisions of 8 bit binary input hashes. Since $277 \equiv_{12} = 1$, this curve was generated with an initial j-invariant 244, corresponding to a complex multiplication reduction from $\mathbb{Q}(\sqrt{-7})$.

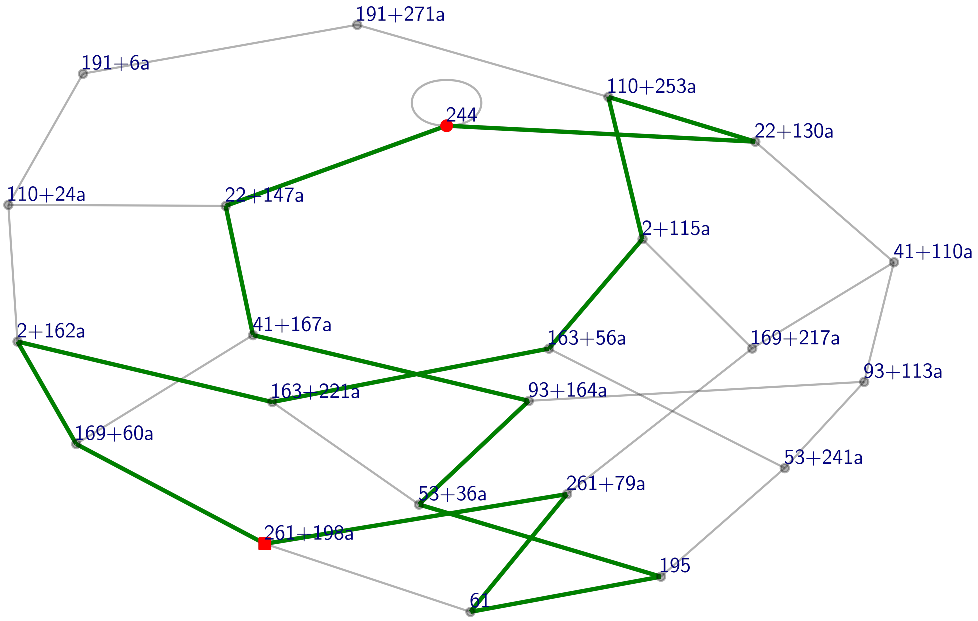


Figure 5: One of 71 hard collisions in $\mathcal{G}_2(277)$

Here, both `01000111` (going "right" from 244) and `11100001` (going "left") hash to the j-invariant $261 + 198a$.

Eg. 6.2.2 Finding hard collisions is computationally equivalent to reversing the hash.

However, one may instead find a small cycle containing two points along a given traversal to yield, by stitching, two (non-disjoint) 2^N isogenies. This attack is more concerning.

The absence of cycles of short length can be guaranteed by choosing p optimally relative to ℓ. In [4], $\mathcal{G}_2(p) : p \equiv_{420} 1$ is shown to have no distinct 2-isogenies between two curves, corresponding to cycles of length 2. ($\mathcal{G}_2(421)$ still contains 2,159 cycles of length $< 2\lfloor p \rfloor$.)

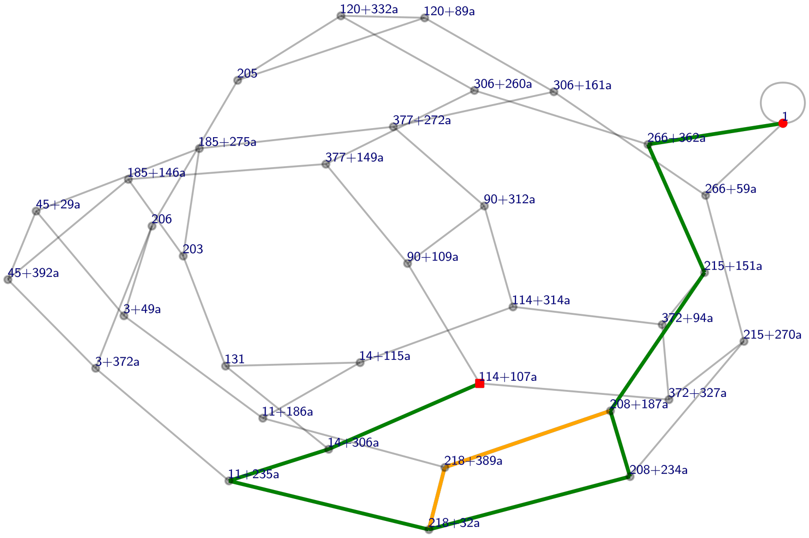


Figure 6: a short cycle collision in $\mathcal{G}_2(421)$

APPENDIX A

Let $\phi, \psi : E_1 \to E_2$ be isogenies of elliptic curves E_1, E_2. Then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$. Before we prove this, we consider another proposition, which will be useful.

Recall $\mathrm{Div}^0(E)$, the class of divisors of degree-0 on E. Denote

$$D = \sum_{P \in E} n_P(P)$$

Then, if $\sum_{P \in E}[n_P]P = O$, as in the group law, then $D = 0$ modulo principle divisors.

PROOF.

Recall that every degree-0 divisor is equivalent to $(P) - (O)$ mod principle divisors (we proved this earlier). Hence, $[D] = 0 \iff \sigma^{-1}(D) = O$, where σ^{-1} maps $D \to P$, as above.

This holds, then, $\iff \sigma^{-1}\left(\sum_{P \in E} n_P(P)\right) = O$. We proved earlier that addition under $\mathrm{Pic}^0(E)$ is compatible with addition under the group law, i.e.

$$\sigma^{-1}\left(\sum_{P \in E} n_P(P)\right) = \sum_{P \in E}[n_P]\sigma^{-1}((P) - (O)) = \sum_{P \in E}[n_P]P = O$$

and we're done. □

Now for $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$. In particular, we will show that $(\phi + \psi)^* = \phi^* + \psi^*$.

PROOF.

Recall that ϕ, ψ, as isogenies, are especially morphisms of $E_1 \to E_2$. In particular, they are rational maps.

Recall also the mapping

$$\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1) : (Q) \mapsto \sum_{P \in \phi^{-1}(Q)} (P) \quad \text{mod principle divisors}$$

Consider x_1, y_1, the Weierstrass coordinates of E_1 that provide the isomorphism

$$E_1 \to \mathbb{P}^2 : P \mapsto [x_1(P), y_1(P), 1]$$

As an extension of K, we consider the $K(E_1) = K(x_1, y_1)$-rational points on E_1 and E_2. Note that (x_1, y_1) itself is a $K(x_1, y_1)$-rational point on E_1.

$$(\phi + \psi)(x_1, y_1) \quad \phi(x_1, y_1) \quad \psi(x_1, y_1)$$

are all mapped to $K(x_1, y_1)$-rational points on E_2, i.e. in $E_2(K(x_1, x_2))$. Then, we consider the divisor

$$D = ((\phi + \psi)(x_1, y_1)) - (\phi(x_1, x_2)) - (\psi(x_1, y_1)) + (O) \in \mathrm{Div}^0_{K(x_1,y_1)}(E_2)$$

Observe that this divisor is degree-0. By linearity of $\phi + \psi$ (recall: $(\phi + \psi)(f) = \phi(f) + \psi(f)$), we invoke the previous proposition, i.e. conclude that D is principle. Hence, $D = \mathrm{Div}(f)$ for some $f \in K(x_1, y_1)(E_2)$. But $E_2 = K(x_2, y_2)$ for *its* Weierstrass coordinates, i.e. $f \in K(x_1, y_1, x_2, y_2)$.

We may now switch our view of f as a function on $K(x_2, y_2)(E_1)$, i.e. functions on E_1 in variables x_2, y_2.

f must be a function in (x_2, y_2) that, when having $(x_2, y_2) = \phi(x_1, y_1)$, yields a pole (observe this in D). Similarly for $\psi(x_1, y_1)$. When $(\phi + \psi)(x_1, y_1) = (x_2, y_2)$, we observe a zero. Hence

$$\begin{aligned} D &= \sum_{P\in(\phi+\psi)^{-1}(x_2,y_2)} (P) - \sum_{P\in\phi^{-1}(x_2,y_2)} (Q) - \sum_{P\in\psi^{-1}(x_2,y_2)} (R) + (O) \\ &= (\phi + \psi)^*(x_2, y_2) - \phi^*(x_2, y_2) - \psi^*(x_2, y_2) + (O) \end{aligned}$$

This divisor is still the same as before: in particular, it is equivalent to 0, and so

$$(\phi + \psi)^* = \phi^* + \psi^*$$

Finally, then

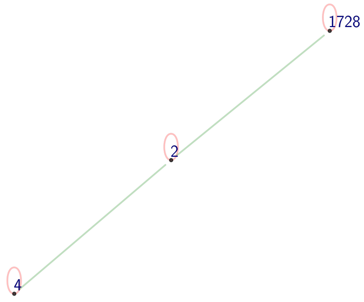
$$\begin{aligned} \widehat{\phi + \psi} &= \sigma_1^{-1} \circ (\psi + \psi)^* \circ \sigma_2 = \sigma_1^{-1} \circ (\phi^* + \psi^*) \circ \sigma_2 \\ &= \sigma_1^{-1} \circ \phi^* \circ \sigma_2 + \sigma_1^{-1} \circ \psi^* \circ \sigma_2 = \hat{\phi} + \hat{\psi} \end{aligned}$$

APPENDIX B

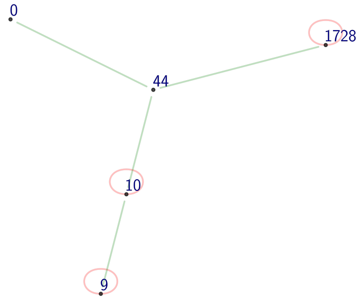
$\mathbb{F}_q$	finite field of size $q = p^r$, for a prime p
$\mathbb{A}^n$	affine space of dimension n
$\mathbb{P}^n$	projective space of dimension n
K	arbitrary field
$\overline{K}$	algebraic closure of K
$\overline{K}[\vec{x}]$	polynomial ring over $x_1, \ldots, x_k$
V	affine variety
V/K	variety defined over K
$I(V)$	ideal of polynomials vanishing on V
$\overline{K}[V]$	the ring of polynomials $\overline{K}[\vec{x}]$ mod $I(V)$
$\overline{K}(V)$	the function field of $\overline{K}[V]$

GALLERY

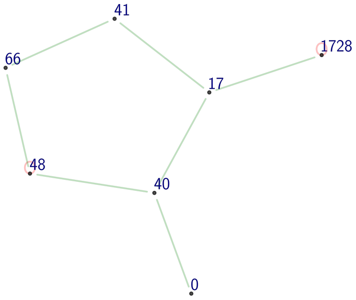
Parallel edges are removed (e.g. 3-edge from $j = 0$)



$\mathbb{F}_{31}$



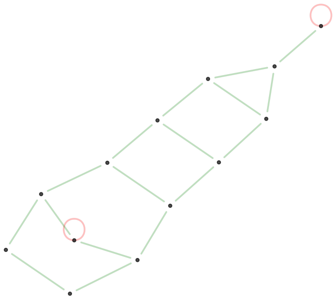
$\mathbb{F}_{47}$



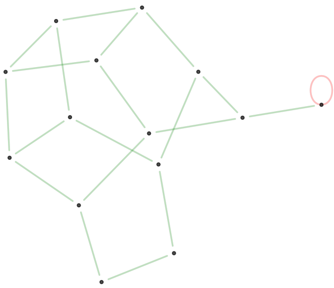
$\mathbb{F}_{71}$

also, the last prime for which all supersingular curves are defined over $\mathbb{F}_p$

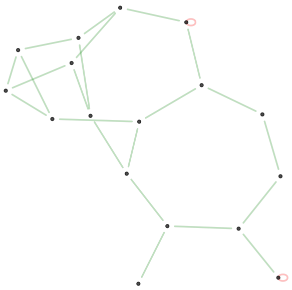
dimethylcyclopentane



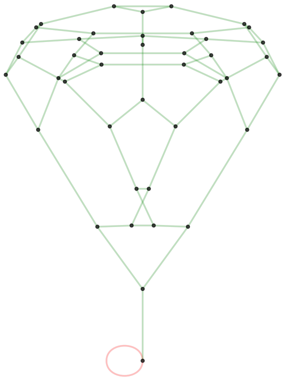
$\mathbb{F}_{157}$
odd hopscotch



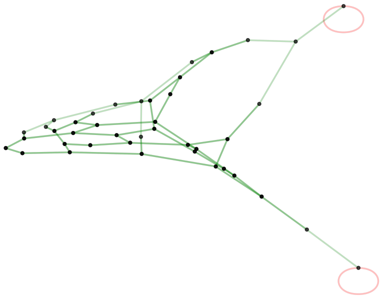
$\mathbb{F}_{163}$
exploding box



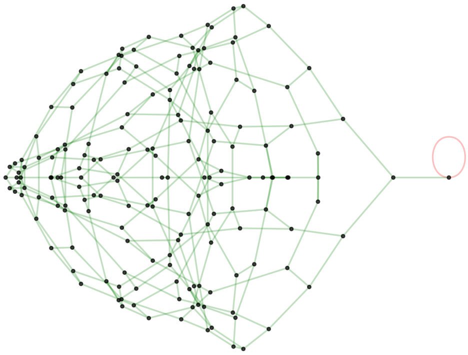
$\mathbb{F}_{191}$
peppa the pig



$\mathbb{F}_{499}$
diamond



$\mathbb{F}_{811}$
crow's beak



$\mathbb{F}_{2027}$
horseshoe crab

REFERENCES

[1] Gora Adj and Francisco Rodriguez-Henriquez. Square root computation over even extension fields. *IEEE Trans. Comput.*, 63(11):2829–2841, November 2014.

[2] Reinier Bröker. Constructing supersingular elliptic curves. 2007.

[3] Juan Marcos Cerviño. On the correspondence between supersingular elliptic curves and maximal quaternionic orders. 2004.

[4] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, January 2009.

[5] Ilya Chevyrev and Steven D Galbraith. Constructing supersingular elliptic curves with a given endomorphism ring. *LMS J. Comput. Math.*, 17(A):71–91, 2014.

[6] Noam D. Elkies. The Klein quartic in number theory. In *The eightfold way*, volume 35 of *Math. Sci. Res. Inst. Publ.*, pages 51–101. Cambridge Univ. Press, Cambridge, 1999.

[7] Eyal Z Goren and Jonathan R Love. Supersingular elliptic curves, quaternion algebras and applications to cryptography. 2024.

[8] Robin Hartshorne. *Algebraic Geometry*. Graduate texts in mathematics. Springer, New York, NY, December 2010.

[9] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper iii. die struktur des meromorphismenrings. die riemannsche vermutung. *Journal für die reine und angewandte Mathematik*, 175:193–208, 1936.

[10] Neal Koblitz. Elliptic curve cryptosystems. *Math. Comput.*, 48(177):203–209, 1987.

[11] Alvaro Lozano-Robledo. MATH5020 - The Arithmetic of Elliptic Curves. *Class page*, December 2015.

[12] Victor S Miller. Use of elliptic curves in cryptography. In *Lecture Notes in Computer Science*, pages 417–426. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[13] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*. Graduate texts in mathematics. Springer, New York, NY, September 1999.

[14] Joseph H Silverman. *The arithmetic of elliptic curves*. Graduate texts in mathematics. Springer, New York, NY, 2 edition, December 2009.

[15] J. Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Série I*, 273:238–241, juillet 1971.

`https://q.uiver.app/` and `https://www.mathcha.io/` aided in the creation of commutative diagrams and figures, and `https://networkx.org/` in graph visualization. Many thanks to Prof. Henri Darmon for guiding our MATH470 cohort and this project.