Rose-Hulman Undergraduate Mathematics Journal

Volume 23
Issue 1

Article 4

On Isomorphic K-Rational Groups of Isogenous Elliptic Curves Over Finite Fields

Ben Kuehnert
University of Rochester

Geneva Schlafly
University of California, Santa Barbara, gschlafly@gmail.com

Zecheng Yi
Johns Hopkins University

On Isomorphic K-Rational Groups of Isogenous Elliptic Curves Over Finite Fields

Cover Page Footnote

We are grateful to Professor Liljana Babinkostova for her invaluable mentorship and guidance in producing this paper. We additionally give thanks to the National Science Foundation (DMS-1659872) for funding our REU program and to Boise State University for supporting our REU program in Summer 2019.

Rose-Hulman Undergraduate Mathematics Journal
VOLUME 23, ISSUE 1, 2022

On Isomorphic $\mathbb{K}$-Rational Groups of Isogenous Elliptic Curves Over Finite Fields

By *Ben Kuehnert*, *Geneva Schlafly*, and *Zecheng Yi*

Abstract. It is well known that two elliptic curves are isogenous if and only if they have same number of rational points. In fact, isogenous curves can even have isomorphic groups of rational points in certain cases. In this paper, we consolidate all the current literature on this relationship and give an extensive classification of the conditions in which this relationship arises. First we prove two ordinary isogenous elliptic curves have isomorphic groups of rational points when they have the same j-invariant. Then, we extend this result to certain isogenous supersingular elliptic curves, namely those with equal j-invariant of either 0 or 1728, using Vlăduţ's characterization of the group structure of rational points.

1 Introduction

Elliptic curves have long been of great interest in mathematics due to their rich algebraic structure and their unique morphisms known as isogenies. In 1966, Sato and Tate proved that two elliptic curves defined over the same finite field are isogenous if and only if they have the same number of rational points [6]. This theorem offers a helpful tool to relate the study of multiple elliptic curves' algebraic structures to that of the isogenies between them.

The structure of the group of K-rational points of an elliptic curve over a finite field is a central area of study in number theory. In brief, an elliptic curve E is a curve of the form $y^2 = x^3 + Ax + B$. In 1999, Vlăduţ in [7] determined the possible group structures of elliptic curves over $\mathbb{F}_{p^r}$, specifically when they have a cyclic group of rational points based on its trace of Frobenius and the finite field over which the elliptic curve is defined. For prime $p \neq 2,3$ and $r > 0$ integer, the field $\mathbb{F}_{p^r}$ is the field of characteristic p with p^r elements. In 2001, Wittmann determined the possible group structures of $E(\mathbb{F}_{p^r})$ for all elliptic curves defined over $\mathbb{F}_{p^r}$ with isomorphism classes of groups.

Following the technical details we will provide in Section 2, we combine these two results to characterize the differences in the group structure of rational points of an elliptic curve based on the field that the elliptic curve is defined over. Specifically, for an elliptic curve defined over $\mathbb{F}_{p^r}$, we will show the possible structures of $E(\mathbb{F}_{p^r})$ depending

Mathematics Subject Classification. 14H52, 14K22, 11Y01, 11N25, 11G07, 11G20, 11B99
Keywords. Elliptic curves, Mappings, Isogenies, Orders of Elliptic Curves, j-invariants.

on whether r is odd or even. This allows us to link the group structures of $E(\mathbb{F}_{p^r})$ and $E(\mathbb{F}_{p^s})$ when r and s have different parity. In this context, we also condense Vlăduţ's work to analyze the occurrence of both cyclic and non-cyclic groups of rational points.

With this classification of groups of rational points at hand, we then study the situations in which two isogenous curves have isomorphic groups of rational points. In Section 3, we will give a proof that two ordinary elliptic curves with the same j-invariant are isogenous if and only if they have isomorphic groups of rational points. In Section 4 and Section 5, we will then extend this statement to isogenous supersingular elliptic curves when their j-invariants are either 0 or 1728.

2 Preliminaries

2.1 Elliptic Curves

We introduce some elementary features of elliptic curves. Let K be a field and $\overline{K}$ be its algebraic closure (e.g. if K is the real numbers, then $\overline{K}$ would be the complex numbers). In this paper, fields will be assumed to have characteristic not 2 or 3. In this case, an elliptic curve can be defined by Weierstrass normal form given by

$$y^2 = x^3 + Ax + B,$$

with $A, B \in K$ such that the discriminant, $\Delta = 4A^3 + 27B^2$, is nonzero. The discriminant being nonzero guarantees that the curve is non-singular, meaning that the curve does not contain any cusps or self-intersections.

For an elliptic curve E defined over a field K, we will define two important sets. The first is

$$E/K = E(\overline{K}) = \{(x, y) \in \overline{K}^2 : y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

where the element ∞ is called the *point at infinity*. To understand what the point ∞ means, we must consider the equation in its *projective form*, as $Y^2Z = X^3 + AXZ^2 + BZ^3$. This is obtained by the following relationships on coordinates:

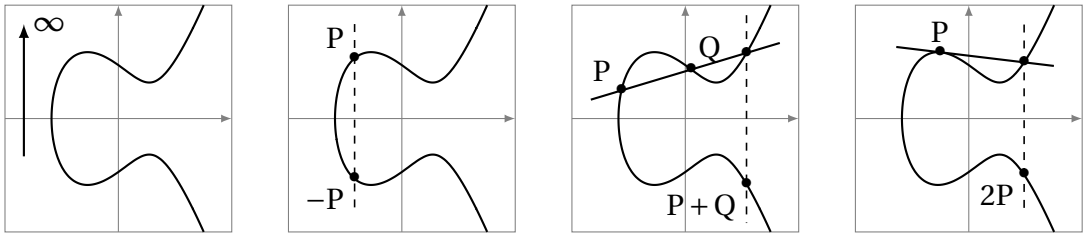
$$x = \frac{X}{Z},\ y = \frac{Y}{Z}$$

In projective coordinates, the point ∞ is defined as the point $(0 : 1 : 0)$ of the curve, and will serve as an identity element under a well-defined operation on E/K described below. Note that this set is infinite in general. The second set is the K-rational points, denoted

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

For two distinct points, P and Q, not equal to ∞ on an elliptic curve, namely $P, Q \in E(K)$, the point $P + Q$ can be uniquely defined by the following process. The point $P + Q$ is

computed by first calculating the line intersecting both P and Q. This line will intersect the elliptic curve at a third point, call it R. Finally, draw a vertical line through R and denote the point at which this line intersects the curve as P + Q. This addition process uniquely defines P + Q. Points that share a vertical line are inverses, and when adding a point to itself, we use the tangent line. Under this operation (E(K), +) is a group. See Figure 1 for some examples of this group operation for an elliptic curve defined over $\mathbb{R}$.



Neutral element ∞ Inverse element $-P$ Addition $P+Q$ Doubling $P+P$

Figure 1: Group law of elliptic curves

Note that $E(K) \subseteq E(\overline{K})$, in particular, E(K) is a subgroup of $E(\overline{K})$. This geometric description of the group law can also be expressed by the well-known formulas for computing operations within E(K). Suppose $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with $P \neq Q$, then if $x_1 \neq x_2$, $P + Q = (x_3, -\ell x_3 - m)$, where

$$\ell = \frac{y_1 - y_2}{x_1 - x_2},\ m = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2},\ x_3 = \frac{x_1 x_2^2 + x_1^2 x_2 + A(x_1 + x_2) + 2B - 2y_1 y_2}{(x_1 - x_2)^2},$$

and if $y_1 \neq 0$, $2P = (x_4, -\ell x_4 - m)$, where

$$\ell = \frac{3x_1^2 + A}{2y_1},\ m = \frac{-x_1^3 + Ax_1 + 2B}{2y_1},\ x_4 = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4y_1^2}.$$

These formulas still hold when K is a finite field whose characteristic does not equal 2. So if we let $q = p^r$ where p is prime and $r \in \mathbb{N}$ and let $K = \mathbb{F}_q$, E(K) is a finite abelian group. The following notions and results concerning the size and structure of elliptic curves play an important role.

Theorem 2.1 (Hasse, [3])**.** *Let* E *be an elliptic curve over a finite field* $\mathbb{F}_q$*. Then,*

$$\#E(\mathbb{F}_q) = q + 1 - t$$

where $|t| \leq 2\sqrt{q}$*.*

The following theorem provides characterization of the structure of the elliptic curve group $E(\mathbb{F}_q)$.

Theorem 2.2 (Theorem 4.1 in [8]). *Let* E *be an elliptic curve over a finite field* $\mathbb{F}_q$. *Then* $E(\mathbb{F}_q) \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus (\mathbb{Z}/n_2\mathbb{Z})$ *or* $E(\mathbb{F}_q) \cong (\mathbb{Z}/n\mathbb{Z})$ *for some integer* $n \geq 1$, *or for some integers* $n_1, n_2 \geq 1$ *with* $n_1 | n_2$.

2.2 Isogenies Between Elliptic Curves.

The isogenies between elliptic curves will be crucial in understanding their structure. In this section we provide definitions of an isogeny and state some fundamental properties of this type of a map.

Definition 2.3 ([5], Section 4). . Let E_1 and E_2 be two elliptic curves. An *isogeny* between E_1 and E_2 is a morphism

$$\alpha : E_1 \longrightarrow E_2$$

satisfying $\alpha(\infty_{E_1}) = \infty_{E_2}$. E_1 and E_2 are isogenous if there is an isogeny α between them with $\alpha(E_1) \neq \{\infty_{E_2}\}$.

We do not consider the trivial map $\alpha = \infty_E$. We say that two curves are isogenous over K if there is an isogeny of E_1 to E_2 defined over K. Note that an isogeny is not necessarily an isomorphism because an isogeny may have a non-trivial kernel. Also note that an isomorphism is not necessarily an isogeny, because an isomorphism may not map ∞_{E_1} to ∞_{E_2}.

The notion of isogeny can be defined from a computational viewpoint via rational maps.

Definition 2.4. (Isogeny of Elliptic Curves) [[8], Section 8.6]. Let E_1 and E_2 be elliptic curves defined over a field K. An isogeny is a homomorphism from $E_1(\bar{K})$ to $E_2(\bar{K})$ that is given by rational functions

$$\alpha : E_1(\bar{K}) \longrightarrow E_2(\bar{K})$$
$$\alpha : (x, y) \mapsto \left(\frac{p_x}{q_x}, \frac{p_y}{q_y}\right)$$

where p_x, q_x, p_y, q_y are polynomials in the coordinates of the point (x, y).

Example 2.5. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve. An example of an isogeny is the "multiplication by m" map which sends a point $P \in E$ to $[m]P$ ($m \neq 0$), where the group law on E is written additively using the following formulas for [m]P in terms of the so called division polynomials $\psi_m(x, y)$:

$$[m]P = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{2m}}{2\psi_m^4}\right)$$

The division polynomials $\psi_i(x,y)$ are given by:

$$\begin{aligned}
&\psi_1 = 1\\
&\psi_2 = 2y\\
&\psi_3 = 3x^4 + 6\mathrm{A}x^2 + 12\mathrm{B}x - \mathrm{A}^2\\
&\psi_4 = 4y\left(x^6 + 5\mathrm{A}x^4 + 20\mathrm{B}x^3 - 5\mathrm{A}^2x^2 - 4\mathrm{AB}x - 8\mathrm{B}^2 - \mathrm{A}^3\right), \quad \text{for } m \geq 2,\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad \text{for } m \geq 3.\\
&\psi_{2m} = \left(\tfrac{\psi_m}{2y}\right)\cdot\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right),
\end{aligned}$$

More details about rational maps and division polynomials can be found in Section 3.2 of [8].

Definition 2.6. (Degree of an isogeny). Let $\varphi : \mathrm{E}_1 \to \mathrm{E}_2$ be an isogeny of elliptic curves, with $\alpha : (x,y) \mapsto \left(\frac{p_x}{q_x}, \frac{p_y}{q_y}\right)$. Then the degree of α is the maximum of the degrees of the polynomials p_x and q_x.

The following theorem is a direct consequence of the Sato-Tate's Isogeny Theorem from [6], showing that isogeny classes of curves are in one-to-one correspondence with the orders of the curves' K-rational points.

Theorem 2.7. *Two elliptic curves* $\mathrm{E}(\mathrm{K})$ *and* $\mathrm{E}'(\mathrm{K})$ *are isogeneous if and only if*

$$\#\mathrm{E}(\mathrm{K}) = \#\mathrm{E}'(\mathrm{K}).$$

When K is a finite field, it makes sense to talk about the Galois group, $\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$, since the algebraic closure and separable closure of K coincide. The Galois group is the set of field automorphisms of $\overline{\mathrm{K}}$ that leave K fixed, which forms a group under composition. For E, E' two elliptic curves defined over K and $\phi : \mathrm{E} \to \mathrm{E}'$ an isogeny, $\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$ acts on ϕ by acting on its coefficients. For $\sigma \in \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$, we denote the image of ϕ under the action of σ by ϕ^σ. The following lemma provides a tool to determine whether an isogeny is defined over K.

Lemma 2.8. *Let* E, E' *be two elliptic curves defined over a finite field* K, $\sigma \in \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$, *and* $\phi : \mathrm{E} \to \mathrm{E}'$ *be an isogeny. Then* ϕ *is defined over* K *if and only if* $\phi^\sigma = \phi$ *for all* σ.

Proof. If ϕ is defined over K, then all its coefficients lie in K, thus are preserved by any $\sigma \in \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$. On the other hand, if ϕ has a coefficient lying in $\overline{\mathrm{K}}\backslash\mathrm{K}$, there would exist $\sigma \in \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$ that does not preserve this coefficient since K is the largest subfield of $\overline{\mathrm{K}}$ preserved by $\mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K})$. □

The j-invariant of an elliptic curve is an important invariant of curves. For a curve $\mathrm{E} : y^2 = x^3 + \mathrm{A}x + \mathrm{B}$ in Weierstrass normal form, the j-invariant is given by

$$j(\mathrm{E}) = 1728 \cdot \frac{4\mathrm{A}^3}{4\mathrm{A}^3 + 4\mathrm{B}^2}.$$

For most j-invariants $j \in \mathbb{F}_p$ there are, up to isomorphism, exactly two elliptic curves E over $\mathbb{F}_p$ with $j(E) = j$: a curve E and its quadratic twist. The exceptions are $j = 0$ when $p = 1 \mod 3$ and $j = 1728$ when $p = 1 \mod 4$. In the first case there are six curves and in the second case there are four curves. The following theorems are well known results about j-invariants.

Theorem 2.9 (Proposition III.1.4 in [5])**.** *Let* K *be a field and* E_1, E_2 *elliptic curves over* K. *Then there is an isomorphism from* E_1 *to* E_2 *defined over* K *if and only if* $j(E_1) = j(E_2)$. *Moreover given* $j_0 \in K$, *there exists an elliptic curve* E *over* K *with* j*-invariant equal to* j_0.

Theorem 2.10 (Theorem 2.19 in [8])**.** *Let* $E_1 : y_1^2 = x_1^3 + A_1 x_1 + B_1$ *and* $E_2 : y_2^2 = x_2^3 + A_2 x_2 + B_2$ *be elliptic curves defined over* K. *If* $j(E_1) = j(E_2)$ *then there exists a* $\mu \in \overline{K}$ *with*

$$A_2 = \mu^4 A_1, \quad B_2 = \mu^6 B_1$$

such that the transformation

$$x_2 = \mu^2 x_1, \quad y_2 = \mu^3 y_1$$

is an isomorphism over $\overline{K}$.

2.3 Endomorphisms

An endomorphism of an elliptic curve E is an isogeny from E to itself. The set $\mathrm{End}_K(E)$ of endomorphisms over K has a ring structure with the following operations. Let E/K be an elliptic curve and let $\alpha, \beta \in \mathrm{End}_K(E)$. Then, $\alpha + \beta$ will be the pointwise addition of functions. So for $P \in E/K$, $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$. Multiplication will be given by function composition, so $\alpha \cdot \beta = \alpha \circ \beta$. The structure is exactly the same for the ring $\mathrm{End}_{\overline{K}}(E)$ of endomorphisms defined over $\overline{K}$.
An example of an endomorphism is the **multiplication by** n **map**, denoted by $[n]$ where n is a nonzero integer. For an elliptic curve E/K and a point $P \in E/K$, the map is defined via

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

Note that $[0]$ maps everything to zero, so it is constant, and not an isogeny by definition. This map has some noteworthy properties:

- $[n + m] = [n] + [m]$ as $(n + m)P = nP + mP$
- $[nm] = [n] \circ [m]$ as $(nm)P = n(mP)$.

With the multiplication by n map defined, we will also introduce the definition of torsion points here. Given an elliptic curve E/K, $E[n] := \{P \in \overline{K} \mid nP = \infty\}$, that is $E[n]$ is the set of point that goes to infinity under the multiplication by n map. We also have the following theorem concerning the group structure of $E[n]$:

Theorem 2.11 (Theorem 3.2 in [8])**.** *Let* E *be an elliptic curve defined over* K *and* n *be a positive integer. If the characteristic of* K *does not divide* n *or is 0, then*

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

If the char(K) $= p > 0$ *and* $p|n$*, then we can write* $n = p^r n'$ *with* $p \nmid n'$*. Then*

$$\mathrm{E}[n] \cong \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \text{ or } \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}.$$

Definition 2.12. Let E be an elliptic curve defined over a finite field $\mathbb{F}_{p^r}$, then E is **ordinary** if $\mathrm{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$ and E is **supersingular** if $\mathrm{E}[p] \cong 0$.

The proof of the following theorem can be found in [8, Proposition 4.31].

Theorem 2.13. *For* E *an elliptic curve over a finite field* $\mathbb{F}_{p^r}$*,* E *is supersingular if and only if* $\#\mathrm{E}(\mathbb{F}_{p^r}) \equiv 1 \mod p$.

Another important endomorphism is the **Frobenius endomorphism**. Let $\mathrm{E}/\mathbb{F}_q$. Then, the Frobenius endomorphism is defined by

$$\begin{aligned} \pi_q : \mathrm{E}/\mathbb{F}_q &\to \mathrm{E}/\mathbb{F}_q \\ (x, y) &\mapsto (x^q, y^q) \end{aligned}$$

Lemma 2.14 (Lemma 4.5 in [8])**.** *Let* $\mathrm{E}/\mathbb{F}_q$ *be an elliptic curve, and let* $(x, y) \in \mathrm{E}(\overline{\mathbb{F}_q})$*. Then,*

1. $\pi_q(x, y) \in \mathrm{E}(\overline{\mathbb{F}_q})$ *and*
2. $(x, y) \in \mathrm{E}(\mathbb{F}_q)$ *if and only if* $\pi_q(x, y) = (x, y)$.

Corollary 2.15. *If an endomorphism* $\phi \in \mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E})$ *commutes with the Frobenius endomorphism* π_q*, then* $\phi \in \mathrm{End}_{\mathbb{F}_q}(\mathrm{E})$.

Proof. Suppose ϕ commutes with π_q. Let P be a point in $\mathrm{E}(\mathbb{F}_q)$. Then,

$$\pi_q \circ \phi(\mathrm{P}) = \phi \circ \pi_q(\mathrm{P}).$$

Since $\mathrm{P} \in \mathrm{E}(\mathbb{F}_q)$, then $\pi_q(\mathrm{P}) = \mathrm{P}$. Hence,

$$(\phi(\mathrm{P}))^q = \phi(\mathrm{P}^q) = \phi(\mathrm{P}).$$

This means that $\phi(\mathrm{P}) \in \mathrm{E}(\mathbb{F}_q)$. Therefore, ϕ restricted to $\mathrm{E}(\mathbb{F}_q)$ maps into $\mathrm{E}(\mathbb{F}_q)$, and is thus defined over $\mathbb{F}_q$ by Lemma 2.8. □

3 Ordinary Elliptic Curves with Equal j-Invariant

In this section we will discuss the relationship between isogenous elliptic curves' F_q-rational points with equal j-invariant.

Theorem 3.1. *If* $\mathrm{E}/\mathbb{F}_q$ *is an ordinary elliptic curve, then* $\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E})$ *is commutative.*

Proof. The commutativity of $\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E})$ follows from $\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E})$ being an order in an imaginary quadratic field when $\mathrm{E}/\mathbb{F}_q$ is ordinary. See Theorem 10.6 in [8]. □

Corollary 3.2. *If* $\mathrm{E}/\mathbb{F}_q$ *is ordinary, then* $\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E}) = \mathrm{End}_{\mathbb{F}_q}(\mathrm{E})$.

Proof. Let $\phi \in \mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E})$. Since $\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E})$ is commutative, then ϕ commutes with π_q, hence $\phi \in \mathrm{End}_{\mathbb{F}_q}(\mathrm{E})$. Thus, $\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E}) \subseteq \mathrm{End}_{\mathbb{F}_q}(\mathrm{E})$. Trivially, $\mathrm{End}_{\mathbb{F}_q}(\mathrm{E}) \subseteq \mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E})$ since all isogenies defined over $\mathbb{F}_q$ are also defined over $\overline{\mathbb{F}_q}$. Thus,

$$\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E}) = \mathrm{End}_{\mathbb{F}_q}(\mathrm{E})$$

□

Theorem 3.3. *Suppose* E_1 *and* E_2 *are ordinary elliptic curves defined over* $\mathbb{F}_q$ *with* $j(\mathrm{E}_1) = j(\mathrm{E}_2)$. *Then,*

$$\#\mathrm{E}_1(\mathbb{F}_q) = \#\mathrm{E}_2(\mathbb{F}_q) \iff \mathrm{E}_1(\mathbb{F}_q) \cong \mathrm{E}_2(\mathbb{F}_q)$$

Proof. We proceed as Proposition 14.19 in [2]. Suppose $\mathrm{E}_1(\mathbb{F}_q) \cong \mathrm{E}_2(\mathbb{F}_q)$, then $\#\mathrm{E}_1(\mathbb{F}_q) = \#\mathrm{E}_2(\mathbb{F}_q)$, as isomorphisms of finite groups preserve order. Conversely, suppose $\#\mathrm{E}_1(\mathbb{F}_q) = \#\mathrm{E}_2(\mathbb{F}_q)$. By Theorem 2.7, these curves are isogenous over $\mathbb{F}_q$, so there exists some isogeny $\lambda : \mathrm{E}_1 \to \mathrm{E}_2$ defined over $\mathbb{F}_q$. Next, since $j(\mathrm{E}_1) = j(\mathrm{E}_2)$, there exists an isomorphism $\phi : \mathrm{E}_2 \to \mathrm{E}_1$ defined over $\overline{\mathbb{F}_q}$ by Theorem 2.10. Consider $\phi \circ \lambda$ which is in $\mathrm{End}_{\overline{\mathbb{F}_q}}(\mathrm{E}_1)$. Since E_1 is ordinary, this endomorphism can be defined over $\mathbb{F}_q$ by Corollary 3.2, so $\phi \circ \lambda \in \mathrm{End}_{\mathbb{F}_q}(\mathrm{E}_1)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Then,

$$\phi^\sigma \circ \lambda = \phi^\sigma \circ \lambda^\sigma = (\phi \circ \lambda)^\sigma = \phi \circ \lambda$$

Since isogenies are surjective, we have that $\phi^\sigma = \phi$. This holds for all such σ, so by Lemma 2.8 ϕ is defined over $\mathbb{F}_q$. Finally, as both E_1 and E_2 are isomorphic over $\mathbb{F}_q$, we conclude that $\mathrm{E}_1(\mathbb{F}_q) \cong \mathrm{E}_2(\mathbb{F}_q)$ via Theorem 2.7. □

4 The case when the j-invariant $j = 0$

In this section we consider the elliptic curves with j-invariant $j = 0$, i.e. elliptic curves of the form $\mathrm{E}(\mathbb{F}_q) : y^2 = x^3 + \mathrm{B}$. We prove that when the j-invariant is 0, two curves are in

the same isogeny class if and only if they have isomorphic groups of $\mathbb{F}_q$-rational points. Recall that two curves are in the same isogeny class if an only if they have the same number of $\mathbb{F}_q$ rational points. We will show that two curves with $j = 0$ have the same number of $\mathbb{F}_q$-rational points if and only if the group of $\mathbb{F}_q$-rational points are isomorphic. We will prove this statement in two cases: the case when $j = 0$ and the elliptic curve is supersingular and the case when $j = 0$ and the elliptic curve is ordinary. The following two theorems classify the number or $\mathbb{F}_q$-rational points of elliptic curves with j-invariant $j = 0$. The proof of Theorem 4.1 can be found in [1] (Theorem 2.4 and Theorem 2.5).

Theorem 4.1. *For $p \equiv 2 \mod 3$, if E is an elliptic curve with j-invariant $j = 0$ defined over $\mathbb{F}_q$, then*

1. *if q is an odd power of p, then $\#\mathrm{E}(\mathbb{F}_q) = q + 1$; and*
2. *if q is an even power of p, then*

$$\#\mathrm{E}(\mathbb{F}_q) \in \{q + 1 + 2\sqrt{q}, q + 1 - \sqrt{q}, q + 1 + 2\sqrt{q}, q + 1 - 2\sqrt{q}\}.$$

Theorem 4.2 (Gauss)**.** *Let $\mathrm{E}(\mathbb{F}_p) : y^2 = x^3 + r$ be an elliptic curve and $p \equiv 1 \mod 3$. Then*

$$\#\mathrm{E}(\mathbb{F}_p) = \begin{cases} p + 1 + 2a & \text{if } r \text{ is sextic residue modulo } p \\ p + 1 - 2a & \text{if } r \text{ is cubic residue but not quadratic residue modulo } p \\ p + 1 - a \pm 3b & \text{if } r \text{ is quadratic residue but not cubic residue modulo } p \\ p + 1 + a \pm 3b & \text{if } r \text{ is neither quadratic nor cubic residue modulo } p, \end{cases}$$

where a, b satisfy the conditions $a^2 + 3b^2 = p$, $b > 0$, and $a \equiv 2 \mod 3$. If If $p \equiv 2 \mod 3$, then $\#\mathrm{E}(\mathbb{F}_p) = p + 1$.

We now introduce an important invariant of elliptic curves, the trace of Frobenius.

Definition 4.3. The **trace of Frobenius** of an elliptic curve $\mathrm{E}/\mathbb{F}_q$, denoted by m, is defined as $m = q + 1 - \#\mathrm{E}(\mathbb{F}_q)$.

With the notion of the trace of Frobenius, we are able to prove the following lemma which describes a sufficient condition for an elliptic curve with $j = 0$ defined over $\mathbb{F}_p$ to be ordinary.

Lemma 4.4. *An elliptic curve $\mathrm{E} : y^2 = x^3 + r$ defined over $\mathbb{F}_p$ is ordinary if $p \equiv 1 \mod 3$.*

Proof. Here we consider the relationship between p and the trace of Frobenius, $m = p + 1 - \#\mathrm{E}(\mathbb{F}_p)$. By Theorem 4.2, when $p \equiv 1 \mod 3$, we have

$m \in \{\pm 2a, -a \pm 3b, a \pm 3b\}$ where $a \equiv 2 \mod 3$ and $b > 0$. These conditions give us the following inequalities:

$$\begin{aligned} |2a| &\leq a^2 = p - 3b^2 < p, \\ |-a \pm 3b| &\leq |a| + |3b| < a^2 + 3b^2 = p, \\ |a \pm 3b| &\leq |a| + |3b| < a^2 + 3b^2 = p. \end{aligned}$$

Thus, p does not divide any of the elements in $\{\pm 2a, -a \pm 3b, a \pm 3b\}$. Hence, p does not divide the trace of Frobenius. Therefore, when $p \equiv 1 \mod 3$, E is ordinary.

Remark 4.5. Observe that $|2a| \leq a^2 = p - 3b^2 < p$. So $p \nmid 2a$ and $p \nmid -2a$. Additionally, we have that

$$|-a \pm 3b| \leq |a| + |3b| < a^2 + 3b^2 = p$$

and

$$|a \pm 3b| \leq |a| + |3b| < a^2 + 3b^2 = p,$$

which implies p does not divide any of the elements in $\{2a, -2a, -a \pm 3b, a \pm 3b\}$. Since p does not divide the trace of Frobenius when $p \equiv 1 \mod 3$, every elliptic curve defined over F_p is ordinary.

□

The following lemma characterizes the group structure of $\mathrm{E}(\mathbb{F}_q)$ knowing the structure of $\mathrm{E}(\mathbb{F}_p)$.

Lemma 4.6. *Let* $\mathrm{E}(\mathbb{F}_q) : y^2 = x^3 + r$ *be an elliptic curve with* $q = p^r$ *and* $r \in \mathbb{F}_p^\times$. *If* E *is ordinary over* $\mathbb{F}_p$, *then* E *is ordinary over* $\mathbb{F}_q$.

Proof. Since E be an ordinary elliptic curve over $\mathbb{F}_p$. By Definition 2.12 for ordinary elliptic curves we have that $\mathrm{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{F}_q$ is of characteristic p, the fact that $\mathrm{E}[p] \cong \mathbb{Z}/p\mathbb{Z}$ implies that $\mathrm{E}(\mathbb{F}_q)$ is ordinary by the same definition. □

Now we give an integrated classification of ordinary (and resp. supersingular) elliptic curves when $j = 0$. To do so, we first need the following proposition. The proof of this proposition can be found in [1].

Theorem 4.7. *Let* $a, r \in \mathbb{F}_q^\times$, *then for elliptic curves* E *and* E′ *given by*

$$\begin{aligned} \mathrm{E} &: y^2 = x^3 + r \\ \mathrm{E}' &: y^2 = x^3 + a^6 r, \end{aligned}$$

we have $\mathrm{E}(\mathbb{F}_q) = \mathrm{E}'(\mathbb{F}_q)$.

Remark 4.8. Let R denote the image of the map from $\mathbb{F}_q^\times$ to $\mathbb{F}_q^\times$ given by $r \mapsto r^6$. Then it gives at most 6 cosets of R in $\mathbb{F}_q$, which are referred as **sextic residue classes** of $\mathbb{F}_q$. From the proposition above we have that the order of an elliptic curve $E : y^2 = x^3 + r$ only depends on the sextic residue class of r.

Theorem 4.9. *Let* $E(\mathbb{F}_q)$ *be a non-singular elliptic curve with* $j(E) = 0$ *and* $q = p^r$. *Then* E *is supersingular if and only if* $p \equiv 2 \mod 3$.

Proof. As mentioned earlier in the paper, the elliptic curves considered in this paper are defined over a field of characteristic $p \neq 2, 3$. Thus, we need to consider the following two cases: $p \equiv 1 \mod 3$ and $p \equiv 2 \mod 3$.
Suppose $p \equiv 2 \mod 3$, then by Theorem 4.1 the trace of Frobenius is

$$m = q + 1 - \#E(\mathbb{F}_q) = \begin{cases} 0 & \text{if } q \text{ is an odd power of } p \\ \pm 2\sqrt{q} \text{ or } \pm\sqrt{q} & \text{if } q \text{ is an even power of } p. \end{cases}$$

Thus if $q = p^r$ and $p \mid m = 0$, then E is supersingular.
Now suppose $p \not\equiv 2 \mod 3$, i.e. $p \equiv 1 \mod 3$. For any non-elliptic curve $E : y^2 = x^3 + r$ and $r \in \mathbb{F}_q^\times$, there is an $r' \in \mathbb{F}_q^\times$ distinct from r such that r and r' are in the same sextic residue class over $\mathbb{F}_q^\times$. Indeed, when $q > 7$, it is clear that each sextic residue class of $\mathbb{F}_q^\times$ contains at least two elements. When $q = 7$, we have only one sextic class which contains all elements of $\mathbb{F}_q^\times$. Let m_r be the trace of the elliptic curve $y^2 = x^3 + r$ and $m_{r'}$ be the trace of the elliptic curve $y^2 = x^3 + r'$. By Proposition 4.7, we have that the elliptic curves have the same number of rational points, and thus $m_r = m_{r'}$.
By Lemma 4.4 and Lemma 4.6, along with the fact that $p \nmid m_{r'}$ and $r' \in \mathbb{F}_q^\times$, we have that $p \nmid m_r$ and $E(\mathbb{F}_q)$ is ordinary. □

In the next two subsections we will discuss the relationship between group order and group structure of $\mathbb{F}_q$-rational points of elliptic curves when the curves are ordinary and when the curves are supersingular separately in the following two subsections. According to Theorem 4.9, these two cases correspond to $p \equiv 1 \mod 3$ and $p \equiv 2 \mod 3$ respectively.

4.1 Group Structure of Ordinary Elliptic Curves

According to Theorem 4.9, we know that E is ordinary if $p \equiv 1 \mod 3$. Therefore, the results for ordinary elliptic curves will hold here. We conclude that for elliptic curves E_1, E_2 defined over $\mathbb{F}_q$, if their $\mathbb{F}_q$-rational points have the same cardinality, then $E_1(\mathbb{F}_q) \cong E_2(\mathbb{F}_q)$.

4.2 Group Structure of Supersingular Curves

We first discuss the case when the elliptic curves are supersingular, i.e. when $p \equiv 2 \mod 3$. The following theorem of Vlăduţ describes the group structure of the group of $\mathbb{F}_q$-rational points of elliptic curves defined over $\mathbb{F}_q$.

Theorem 4.10 (Theorem 2.1 in [7])**.** *A finite abelian group* G *of order* $N = q+1-m$*, with* $m^2 \leq 4q$*, is isomorphic to* $E(\mathbb{F}_q)$ *for* E *over* $\mathbb{F}_q$ *if and only if one of the following conditions holds:*

1. *p does not divide m, and* $G \cong \mathbb{Z}/A \times \mathbb{Z}/B$*, where* $B|A$ *and* $B|(m-2)$.
2. *q is an odd power of p and one of the following holds:*
   (a) $m = 0$, $p \equiv 1,2 \mod 4$, *and* G *is cyclic.*
   (b) $m = 0$, $p \equiv 3 \mod 4$, *and* G *is either cyclic or* $G \cong \mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   (c) $p = 2$ *or* 3, $m = \pm\sqrt{pq}$, *and* G *is cyclic.*
3. *q is an even power of p and one of the following holds:*
   (a) $m = \pm 2\sqrt{q}$ *and* $G \cong (\mathbb{Z}/(\sqrt{q} \mp 1)\mathbb{Z})^2$.
   (b) $m = \pm\sqrt{q}$, *and* $p = 3$ *or* $p \equiv 2 \mod 3$, *and* G *is cyclic.*
   (c) $m = 0$, *and* $p \equiv 2,3 \mod 4$, *and* G *is cyclic.*

Using Theorem 4.10 and Lemma 4.11 below, we will show that two supersingular elliptic curves with j-invariant $j = 0$ have the same number of $\mathbb{F}_q$-rational points if and only if their groups of $\mathbb{F}_q$-rational points are isomorphic.

Lemma 4.11. *When* $p \equiv 11 \mod 12$ *and q is an odd power of p,* $E(\mathbb{F}_q) \cong \mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if and only if* $E[2] \subseteq E(\mathbb{F}_q)$.

Proof. By Theorem 2.11, we know that $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $E[2] \subseteq E(\mathbb{F}_q)$, $E(\mathbb{F}_q)$ is not cyclic. Moreover, for q satisfying the conditions in the lemma, we know $m = 0$ as is shown in the proof of Theorem 4.9. Thus $E(\mathbb{F}_q)$ must be isomorphic to $\mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ by Theorem 4.10 (2b).
For the other direction, if $E(\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then since q is an odd power of p and $p \equiv 11 \mod 12$, we know that 2 divides $(q+1)/2$. So $E(\mathbb{F}_q)$ contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; that subgroup must be contained in $E[2]$. By Theorem 2.11, this implies that $E[2] \subseteq E(\mathbb{F}_q)$. □

Theorem 4.12. *If* $E_1(\mathbb{F}_q)$ *and* $E_2(\mathbb{F}_q)$ *are two elliptic curves with* $j(E_1) = j(E_2) = 0$ *and* $p \equiv 2 \mod 3$, *then* $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ *if and only if* $E_1(\mathbb{F}_q) \cong E_2(\mathbb{F}_q)$.

Proof. If $E_1(\mathbb{F}_q) \cong E_2(\mathbb{F}_q)$, then clearly $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$. It remains to prove that the converse also holds. First, assume that q is an odd power of p. By Theorem 4.1, all elliptic curves $E(\mathbb{F}_q)$ with $j(E) = 0$ and $p \equiv 2 \mod 3$ have order

$$\#E(\mathbb{F}_q) = q + 1.$$

So the trace of Frobenius, denoted by m, is equal to zero, i.e.

$$m = q + 1 - \#E(\mathbb{F}_q) = 0.$$

Since $p \equiv 2 \mod 3$ and the field the characteristic of the field $\mathbb{F}_q$ is not equal to 2, we can either have $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$. From Theorem 4.10 (2a), if $p \equiv 1 \mod 4$, then $E(\mathbb{F}_q)$ is cyclic. From Theorem 4.10 (2b), if $p \equiv 3 \mod 4$, then $E(\mathbb{F}_q)$ is either cyclic or isomorphic to $\mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
We will now show that when $j(E) = 0$ and $p \equiv 3 \mod 4$, the case $\mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is eliminated and $E(\mathbb{F}_q)$ is always cyclic. First notice that the conditions of $p \equiv 2 \mod 3$ and $p \equiv 3 \mod 4$ is equivalent to $p \equiv 11 \mod 12$.
Since $j(E) = 0$, the equation of E is of the form $y^2 = x^3 + c$ where $c \in \mathbb{F}_q$ and $c \neq 0$. So the 2-torsion points of E are given by

$$\{(x_1, 0), (x_2, 0), (x_3, 0), \infty\} \tag{1}$$

for some $x_1, x_2, x_3 \in \overline{\mathbb{F}_q}$ satisfying the equation $x^3 + c = 0$. Notice that when $p \equiv 11 \mod 12$, we have $3 \nmid p - 1$ and thus the map $x \mapsto x^3$ on $\mathbb{F}_q^\times$ is an automorphism. So $x^3 + c = 0$ has only one solution in $\mathbb{F}_q$, thus only two points (counting ∞) in (1) are in $E(\mathbb{F}_q)$. Therefore, $E[2] \not\subseteq E(\mathbb{F}_q)$ and the case $E(\mathbb{F}_q) \cong \mathbb{Z}/((q+1)/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is excluded by Lemma 4.11. Thus $E(\mathbb{F}_q)$ is always cyclic when $p \equiv 2 \mod 3$ and q is an odd power of p. So if E_1 and E_2 have the same order, we know that

$$E_1(\mathbb{F}_q) \cong \mathbb{Z}/(q+1)\mathbb{Z} \cong E_2(\mathbb{F}_q).$$

Next, assume that q is an even power of p. Then by Theorem 4.1, the trace of Frobenius is

$$m = q + 1 - \#E(\mathbb{F}_q) = \pm 2\sqrt{q} \text{ or } \pm\sqrt{q}.$$

If $m = \pm\sqrt{q}$, then by Theorem 4.10 (3b) we have that $E(\mathbb{F}_q)$ is cyclic, i.e.
$E_1(\mathbb{F}_q) \cong A \cong E_2(\mathbb{F}_q)$ where

$$A \in \{\mathbb{Z}/(q + 1 + \sqrt{q})\mathbb{Z}, \mathbb{Z}/(q + 1 - \sqrt{q})\mathbb{Z}\}.$$

If $m = \pm 2\sqrt{q}$, then by Theorem 4.10 (3c) we have that

$$E_1(\mathbb{F}_q) \cong B \cong E_2(\mathbb{F}_q),$$

where

$$B \in \{\mathbb{Z}/(\sqrt{q} - 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} - 1)\mathbb{Z}, \mathbb{Z}/(\sqrt{q} + 1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q} + 1)\mathbb{Z}\}.$$

Therefore, in the case when $p \equiv 2 \mod 3$, if two curves defined over $\mathbb{F}_q$ with $j = 0$ have the same number of $\mathbb{F}_q$-rational points, their groups of $\mathbb{F}_q$-rational points are isomorphic. □

5 The case when the j-invariant is $j = 1728$

In this section, we consider elliptic curves E over a finite field $\mathbb{F}_q$ with j-invariant $j = 1728$, which means E is of the form

$$y^2 = x^3 + \mathrm{A}x, \tag{2}$$

where $\mathrm{A} \in \mathbb{F}_q$. We will discuss whether two elliptic curves defined over $\mathbb{F}_q$ with $j = 1728$ have same number of $\mathbb{F}_q$-rational points if and only if their group of $\mathbb{F}_q$-rational points are isomorphic. Similar to what we did in the last section, we will discuss this question in two cases: when E is ordinary and when E is supersingular.

Remark 5.1. Its automorphism group $\mathrm{A}ut(\mathrm{E})$ has order 4, with one automorphism mapping (x, y) to $(-x, iy)$.

Theorem 5.2. *Let* E *be an elliptic curve defined over* $\mathbb{F}_q$ *and* $p \equiv 3 \mod 4$.

1. *If q is an odd power of p, then* $\#\mathrm{E}(\mathbb{F}_q) = q + 1$.
2. *If q is an even power of p, then* $\#\mathrm{E}(\mathbb{F}_q) \in \{q + 1\,,\ q + 1 \pm 2\sqrt{q}\}$

Proof. The proof follows directly from Theorem 3.6 and 3.7 in [1]. □

The following theorem allows us to study supersingular and ordinary elliptic curves with j-invariant $j = 1728$ separately based on the characteristic of the underlying field $\mathbb{F}_q$.

Theorem 5.3. *Let* E *be an elliptic curve over the field* $\mathbb{F}_q$ *of characteristic* $p \neq 2$ *and with* j*-invariant* $j = 1728$. *Then* E *is supersingular if and only if* $p \equiv 3 \mod 4$.

Proof. Suppose $p \equiv 3 \mod 4$. By Theorem 5.2 the trace of Frobenius is

$$m = \begin{cases} 0 & \text{if } q \text{ is an odd power of } p \\ 0 \text{ or } \pm 2\sqrt{q} & \text{if } q \text{ is an even power of } p. \end{cases}$$

Since p divides m when $m = 0$, and p divides $2\sqrt{q}$ when q is an even power of p, E is supersingular by 2.13.
Now suppose $p \equiv 1 \mod 4$. Use a similar technique to the proof of Theorem 4.9, by applying Theorem 4.2 for $\mathrm{E} : y^2 = x^3 + ax$ and extend the result from $\mathbb{F}_p$ to $\mathbb{F}_q$. This shows E is ordinary. Alternatively, see the proof of Theorem V.4.1 in [5]. □

5.1 Group Structure of Ordinary Curves

By Theorem 5.3, $\mathrm{E}(\mathbb{F}_q)$ with j-invariant 1728 is ordinary if and only if $p \equiv 1 \mod 4$. Then by Theorem 3.3, we have $\#\mathrm{E}_1(\mathrm{K}) = \#\mathrm{E}_2(\mathrm{K})$ if and only if $\mathrm{E}_1(\mathrm{K}) \cong \mathrm{E}_2(\mathrm{K})$ and this concludes the case of ordinary elliptic curves with j-invariant 1728.

5.2 Group Structure of Supersingular Curves

By Theorem 5.3, $E(\mathbb{F}_q)$ with j-invariant 1728 is supersingular if and only if $p \equiv 3 \mod 4$. As before, we will discuss the group structure of $\mathbb{F}_q$-rational points separately according to the two cases: when q is an odd power of p and when q is an even power of p.

5.2.1 When q is an odd power of p. The group structure of $\mathbb{F}_q$-rational points in this case corresponds to Theorem 4.10 (2b), from which we can see that there are two possible group structures for $E(\mathbb{F}_q)$. However, when q is an odd power of p, the order of $E(\mathbb{F}_q)$ is uniquely given by $\#E(\mathbb{F}_q) = q+1$. So two elliptic curves having the same number of $\mathbb{F}_q$-rational points do not necessarily have isomorphic group of $\mathbb{F}_q$-rational points. The following example verifies our assertion.

Example 5.4. As shown in the fourth table ($j = 1728, r = 1$) in the Appendix, over $\mathbb{F}_7$ there are six elliptic curves all of order 8. So, all the curves are isogeneous by Sato-Tate Theorem, forming one isogeny class. But, there are two isomorphism classes with distinct group structures. In this case these are $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Therefore, when q is an odd power of p and $j = 1728$, two elliptic curves having same number of $\mathbb{F}_q$-rational points does not imply that their groups of $\mathbb{F}_q$-rational points are isomorphic.

5.2.2 When q is an even power of p. On the other hand, in the following example where q is an even power of p, two elliptic curves having the same number of $\mathbb{F}_q$-rational points does imply that the curves have isomorphic group structures.

Example 5.5. As shown in the fifth table ($j = 1728, r = 2$) in the Appendix, over $\mathbb{F}_{7^2}$ there are 48 elliptic curves of three distinct orders, forming three isogeny classes, by Sato-Tate Theorem. All the curves within the same isogeny class have the same group structure.

In fact, this is true whenever q is an even power of p, and we will now prove this statement.

Theorem 5.6. *Let $q = p^r$ where $p \neq 2$ and r is even. If E_1, E_2 are supersingular elliptic curves over $\mathbb{F}_q$ and the j-invariant is 1728, then*

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) \iff E_1(\mathbb{F}_q) \cong E_2(\mathbb{F}_q).$$

Proof. $E_1(\mathbb{F}_q) \cong E_2(\mathbb{F}_q)$ implies $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$ by properties of isomorphic groups. So we only need to show that if E_1 and E_2 have the same number of $\mathbb{F}_q$ rational points, then they have isomorphic group structures.

In proof of Theorem 5.3, we showed that when $p \equiv 3 \mod 4$ and q is an even power of p, $m \in \{0, 2\sqrt{q}, -2\sqrt{q}\}$. When $m = 0$, $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) = q+1$. By Theorem 4.10 (3c), we know both $E_1(\mathbb{F}_q)$ and $E_2(\mathbb{F}_q)$ are cyclic, that is

$$E_1(\mathbb{F}_q) \cong \mathbb{Z}/(q+1)\mathbb{Z} \cong E_2(\mathbb{F}_q).$$

When $m = 2\sqrt{q}$, $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) = p^r + 1 - 2\sqrt{q}$. By Theorem 4.10 (3a), we have

$$E_1(\mathbb{F}_q) \cong A \cong E_2(\mathbb{F}_q),$$

where A is given by

$$A = \mathbb{Z}/(\sqrt{q}-1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q}-1)\mathbb{Z}.$$

When $m = -2\sqrt{q}$, $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) = p^r + 1 + 2\sqrt{q}$. Again, by Theorem 4.10 (3a), we have

$$E_1(\mathbb{F}_q) \cong B \cong E_2(\mathbb{F}_q),$$

where B is given by

$$B = \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z} \times \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z}.$$

Therefore, we may conclude that when q is an even power of p and $p \equiv 3 \mod 4$, two elliptic with j-invariant 1728 have the same number of $\mathbb{F}_q$ rational points if and only if their group of $\mathbb{F}_q$ rational points are isomorphic. □

6 Conclusion

In this paper, we discussed the relationship between elliptic curves being isogenous and elliptic curves having isomorphic group of rational points. Specifically, we focused on the case of elliptic curves over finite fields with j-invariant 0 or 1728. By considering ordinary elliptic curves and supersingular elliptic curves separately, we proved that two elliptic curves with j-invariant 0 over a finite field $\mathbb{F}_{p^r}$ are isogenous if and only if their group of $\mathbb{F}_{p^r}$-rational points are isomorphic. We also proved that two elliptic curves with j-invariant 1728 over a finite field $\mathbb{F}_{p^r}$ with r even are isogenous if and only if their group of $\mathbb{F}_{p^r}$-rational points are isomorphic. Specifically, we gave examples of isogenous elliptic curves over $\mathbb{F}_{p^r}$ with j-invariant 1728 not having isomorphic group of $\mathbb{F}_{p^r}$-rational points when r is odd.

Appendix: Data of group structures of $E(\mathbb{F}_{p^r})$

The following are some data we collected on the group structure of $E(\mathbb{F}_{p^r})$ for elliptic curves with j-invariant 0 and 1728. For each j-invariant, we give three tables varying the power of p, which we denote by r.

For each prime, each sub-row represents an isogeny class. In the first column, an example curve from that class is given, next is the number of curves in that isogeny class, then the group structure(s) found among elliptic curves in that isogeny class. The final row "Success" indicates whether the data agrees with statement "two elliptic curves over $\mathbb{F}_{p^r}$ are isogenous if and only if their group of rational points of $\mathbb{F}_{p^r}$ are isomorphic". Note that elements of fields $\mathbb{F}_{p^r}$ where $r > 1$ are represented as polynomials in $\mathbb{Z}$.

$j = 0$, $r = 1$					
p	Example	Order	No. of EC	Group Structure(s)	Success
5	$y^2 = x^3 + 1$	6	4	$\mathbb{Z}/6\mathbb{Z}$	Yes
7	$y^2 = x^3 + 1$	24	1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	Yes
	$y^2 = x^3 + 2$	9	1	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	
	$y^2 = x^3 + 3$	13	1	$\mathbb{Z}/13\mathbb{Z}$	
	$y^2 = x^3 + 4$	3	1	$\mathbb{Z}/3\mathbb{Z}$	
	$y^2 = x^3 + 5$	7	1	$\mathbb{Z}/7\mathbb{Z}$	
	$y^2 = x^3 + 6$	4	1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	
11	$y^2 = x^3 + 1$	12	10	$\mathbb{Z}/12\mathbb{Z}$	Yes
13	$y^2 = x^3 + 1$	12	2	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	Yes
	$y^2 = x^3 + 2$	19	2	$\mathbb{Z}/19\mathbb{Z}$	
	$y^2 = x^3 + 3$	9	2	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	
	$y^2 = x^3 + 4$	21	2	$\mathbb{Z}/21\mathbb{Z}$	
	$y^2 = x^3 + 5$	16	2	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	
	$y^2 = x^3 + 6$	7	2	$\mathbb{Z}/7\mathbb{Z}$	
17	$y^2 = x^3 + 1$	18	16	$\mathbb{Z}/18\mathbb{Z}$	Yes

$j=0$, $r=2$					
p	Example	Order	No. of EC	Group Structure(s)	Success
5	$y^2=x^3+z$	31	8	$\mathbb{Z}/31\mathbb{Z}$	Yes
	$y^2=x^3+z+3$	21	8	$\mathbb{Z}/21\mathbb{Z}$	
	$y^2=x^3+3$	16	4	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$	
	$y^2=x^3+2$	36	4	$\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$	
7	$y^2=x^3+z$	37	8	$\mathbb{Z}/37\mathbb{Z}$	Yes
	$y^2=x^3+z+4$	39	8	$\mathbb{Z}/39\mathbb{Z}$	
	$y^2=x^3+5z+4$	52	8	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/26\mathbb{Z}$	
	$y^2=x^3+2z+6$	63	8	$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/21\mathbb{Z}$	
	$y^2=x^3+z+1$	61	8	$\mathbb{Z}/61\mathbb{Z}$	
	$y^2=x^3+2z+4$	48	8	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$	
11	$y^2=x^3+z$	133	40	$\mathbb{Z}/133\mathbb{Z}$	Yes
	$y^2=x^3+4z+9$	111	40	$\mathbb{Z}/111\mathbb{Z}$	
	$y^2=x^3+3z+3$	100	20	$\mathbb{Z}/10\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$	
	$y^2=x^3+2$	144	20	$\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$	

$j=0$, $r=3$					
p	Example	Order	No. of EC	Group Structure(s)	Success
5	$y^2=x^3+z$	126	124	$\mathbb{Z}/126\mathbb{Z}$	Yes
7	$y^2=x^3+z$	361	57	$\mathbb{Z}/19\mathbb{Z}\times\mathbb{Z}/19\mathbb{Z}$	Yes
	$y^2=x^3+z^2$	381	57	$\mathbb{Z}/381\mathbb{Z}$	
	$y^2=x^3+z^2+3$	364	57	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/182\mathbb{Z}$	
	$y^2=x^3+z^2+4z$	327	57	$\mathbb{Z}/327\mathbb{Z}$	
	$y^2=x^3+z^2+1$	307	57	$\mathbb{Z}/307\mathbb{Z}$	
	$y^2=x^3+3z+5$	324	57	$\mathbb{Z}/18\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$	
11	$y^2=x^3+z$	1332	1330	$\mathbb{Z}/1332\mathbb{Z}$	Yes

$j = 1728$, $r = 1$					
p	Example	Order	No. of EC	Group Structure(s)	Success
5	$y^2 = x^3 + x$	4	1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	Yes
	$y^2 = x^3 + 2x$	2	1	$\mathbb{Z}/2\mathbb{Z}$	
	$y^2 = x^3 + 3x$	10	1	$\mathbb{Z}/10\mathbb{Z}$	
	$y^2 = x^3 + 4x$	8	1	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	
7	$y^2 = x^3 + x$	8	6	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	No
11	$y^2 = x^3 + x$	12	10	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$	No
13	$y^2 = x^3 + x$	20	3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	Yes
	$y^2 = x^3 + 2x$	10	3	$\mathbb{Z}/10\mathbb{Z}$	
	$y^2 = x^3 + 4x$	8	3	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	
	$y^2 = x^3 + 7x$	18	3	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	
17	$y^2 = x^3 + x$	16	4	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	Yes
	$y^2 = x^3 + 2x$	20	4	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	
	$y^2 = x^3 + 3x$	26	4	$\mathbb{Z}/26\mathbb{Z}$	
	$y^2 = x^3 + 6x$	10	4	$\mathbb{Z}/10\mathbb{Z}$	

$j = 1728$, $r = 2$					
p	Example	Order	No. of EC	Group Structure(s)	Success
5	$y^2 = x^3 + zx$	18	6	$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	Yes
	$y^2 = x^3 + 2x$	20	6	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	
	$y^2 = x^3 + (4z+3)x$	34	6	$\mathbb{Z}/34\mathbb{Z}$	
	$y^2 = x^3 + x$	32	6	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	
7	$y^2 = x^3 + zx$	50	24	$\mathbb{Z}/50\mathbb{Z}$	Yes
	$y^2 = x^3 + (2z+5)x$	36	12	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	
	$y^2 = x^3 + x$	64	12	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	
11	$y^2 = x^3 + zx$	122	60	$\mathbb{Z}/122\mathbb{Z}$	Yes
	$y^2 = x^3 + (4z+9)x$	100	30	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$	
	$y^2 = x^3 + x$	144	30	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$	

$j = 1728$, $r = 3$					
p	Example	Order	No. of EC	Group Structure(s)	Success
5	$y^2 = x^3 + zx$	130	31	$\mathbb{Z}/130\mathbb{Z}$	Yes
	$y^2 = x^3 + z^2x$	104	31	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/52\mathbb{Z}$	
	$y^2 = x^3 + (2z+2)x$	122	31	$\mathbb{Z}/122\mathbb{Z}$	
	$y^2 = x^3 + x$	148	31	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/74\mathbb{Z}$	
7	$y^2 = x^3 + x$	344	342	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/172\mathbb{Z}$, $\mathbb{Z}/344\mathbb{Z}$	No
11	$y^2 = x^3 + x$	1332	1330	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/666\mathbb{Z}$, $\mathbb{Z}/1332\mathbb{Z}$	No

Appendix: Code

The code that generated the above data can be found at
`https://github.com/bkuehnert/isogeny-data-collection`

References

[1] J. Bahr, Y. H. Kim, E. Neyman and G. Taylor, *On Orders of Elliptic Curves over Finite Fields*, **Rose-Hulman Undergraduate Mathematics Journal**, Vol. 19:1 (2018), Article 2.

[2] D. A. Cox, *Primes of the form $x^2 + ny^2$*, **A Wiley-Interscience Publication**, John Wiley & Sons Inc., (1989).

[3] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkorper I, II III*, **Crelle's Journal** (175), 1936.

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Vol. 84 ofGraduate Texts in Mathematics, **Springer-Verlag**, 2nd edition (1998).

[5] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Vol. 106 of **Graduate Texts in Mathematics**, **Springer-Verlag**, 1st ed., (1986).

[6] J. Tate, *Endomoprhisms of abelian varieties over finite fields*, **Inventiones Mathematica**, Vol.2 (1966), 134–144.

[7] S.G. Vlăduţ, *On the Cyclicity of Elliptic Curves over Finite Field Extensions*, **Finite Fields and Their Applications**, Vol. 5:4 (1999), 354–363.

[8] L.C. Washington, *Number Theory: Elliptic Curves and Cryptography*, **Discrete Mathematics and Its Applications**, Chapman & Hall/CRC, 2nd ed., (2008).

[9] C. Wittmann, *Group Structure of Elliptic Curves over Finite Fields*, **Journal of Number Theory** Vol.88 (2001), 335–344.

Ben Kuehnert
University of Rochester
`bkuehnert@gmail.com`

Geneva Schlafly
University of California, Santa Barbara
`gschlafly@gmail.com`

Zecheng Yi

Johns Hopkins University
zechengyi97@gmail.com