A Rigorous Treatment of $\mathrm{Aut}(E_{\bar{k}}, O)$ for Elliptic Curves with j-Invariant Zero

February 2026

Abstract

We provide a complete and rigorous proof that for an elliptic curve E with $j(E) = 0$ over an algebraically closed field k of characteristic greater than 3, the automorphism group $\mathrm{Aut}(E_{\bar{k}}, O)$ has exactly 6 elements, and that no elliptic curve in characteristic > 3 can have a larger automorphism group. We give explicit formulas for all six automorphisms, prove that no others exist via direct computation, and establish that the classification is exhaustive through the theory of j-invariants. The treatment includes detailed verification of all computational steps and multiple independent perspectives confirming the result.

Contents

1 Introduction and Setting

1.1 Motivation

The automorphism group of an elliptic curve plays a fundamental role in both the theoretical study of elliptic curves and their applications in cryptography. In the context of the Elliptic Curve Discrete Logarithm Problem (ECDLP), Pollard's rho algorithm can exploit the automorphism group to reduce the expected number of iterations by a factor of $\sqrt{|\operatorname{Aut}(E, O)|}$. This makes curves with larger automorphism groups particularly interesting for cryptanalysis.

The curve secp256k1, widely used in Bitcoin and other cryptocurrencies, has j-invariant equal to 0. A natural question arises: *Is there an elliptic curve with a larger automorphism group that could provide an even greater speedup?* This document provides a rigorous negative answer for characteristic > 3.

1.2 The Field k

Throughout this document, we work over an **algebraically closed field** $k = \bar{k}$ with $\operatorname{char}(k) > 3$.

Definition 1.1. A field k is **algebraically closed** if every non-constant polynomial $f(x) \in k[x]$ has a root in k. Equivalently, every polynomial over k splits completely into linear factors.

Example 1.2. The following are algebraically closed fields:

- The complex numbers $\mathbb{C}$.
- The algebraic closure $\overline{\mathbb{Q}}$ of the rationals.
- The algebraic closure $\overline{\mathbb{F}_p}$ of any finite field $\mathbb{F}_p$.

The following are *not* algebraically closed:

- The real numbers $\mathbb{R}$ (since $x^2 + 1$ has no real root).
- Any finite field $\mathbb{F}_p$ (since $x^p - x - 1$ has no root in $\mathbb{F}_p$).
- The rationals $\mathbb{Q}$.

Remark 1.3 (Why algebraic closure?)**.** When studying elliptic curves over a non-algebraically closed field K (such as $\mathbb{F}_p$ or $\mathbb{Q}$), the automorphism group $\operatorname{Aut}(E_K, O)$ defined over K may be strictly smaller than $\operatorname{Aut}(E_{\bar{K}}, O)$. For instance, an automorphism might require a cube root of unity that doesn't exist in K. Working over $\bar{k}$ ensures we capture all *geometric* automorphisms.

Example: Consider $E : y^2 = x^3 + 1$ over $\mathbb{F}_5$. Since $5 \equiv 2 \pmod 3$, the field $\mathbb{F}_5$ contains no primitive cube root of unity. Over $\mathbb{F}_5$, we have $|\operatorname{Aut}(E_{\mathbb{F}_5}, O)| = 2$. However, over $\overline{\mathbb{F}_5}$, we have $|\operatorname{Aut}(E_{\overline{\mathbb{F}_5}}, O)| = 6$.

Remark 1.4 (Characteristic assumption)**.** The assumption $\mathrm{char}(k) > 3$ is essential. In characteristics 2 and 3, the theory of elliptic curves requires different Weierstrass forms, and supersingular curves can have larger automorphism groups (up to 24 in characteristic 2, up to 12 in characteristic 3). We explicitly exclude these cases.

1.3 Definition of $\mathrm{Aut}(E_{\bar{k}}, O)$

Definition 1.5. Let E be an elliptic curve over k with identity element O. The **automorphism group** $\mathrm{Aut}(E_{\bar{k}}, O)$ consists of all isomorphisms $\phi : E \to E$ (as algebraic varieties over $\bar{k}$) such that $\phi(O) = O$.

Remark 1.6 (Crucial distinction)**.** We explicitly exclude translations. An elliptic curve E has infinitely many automorphisms as an algebraic variety: translating by any point $P \in E$ gives an automorphism $\tau_P : Q \mapsto Q + P$. These form a group isomorphic to E itself (as an abstract group).

However, the group $\mathrm{Aut}(E_{\bar{k}}, O)$ consists only of those automorphisms **fixing the identity element** O. This is a finite group, and its structure depends only on the j-invariant of the curve.

Proposition 1.7. *For an elliptic curve E with identity O, we have:*

$$\mathrm{Aut}(E_{\bar{k}}, O) = \{\phi : E \xrightarrow{\sim} E \mid \phi \text{ is a group homomorphism}\}.$$

That is, automorphisms fixing O are precisely the group automorphisms of $(E, +)$.

Proof. ($\supseteq$) Any group isomorphism necessarily fixes the identity element.

($\subseteq$) Let $\phi \in \mathrm{Aut}(E_{\bar{k}}, O)$. We must show $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E$.

The group law on an elliptic curve is defined geometrically: $P + Q + R = O$ if and only if P, Q, R are collinear (counting multiplicities, with O being the point at infinity).

Since ϕ is an isomorphism of algebraic varieties, it preserves collinearity: three points are collinear if and only if their images are collinear. Moreover, $\phi(O) = O$.

Thus if $P+Q+R = O$, then $\phi(P)$, $\phi(Q)$, $\phi(R)$ are collinear and $\phi(R) = O$ when $R = O$, giving $\phi(P) + \phi(Q) + \phi(R) = O$. This shows ϕ is a group homomorphism. □

Remark 1.8. The proposition shows that our purely geometric definition (isomorphisms fixing O) coincides with the purely algebraic definition (group automorphisms). This justifies using whichever perspective is more convenient.

1.4 Short Weierstrass Form

Since $\text{char}(k) > 3$, every elliptic curve E over k can be written in **short Weierstrass form**:

$$E : y^2 = x^3 + ax + b, \quad \text{where } a, b \in k. \tag{1}$$

This is achieved by completing the square in y and the cube in x, operations that require dividing by 2 and 3 respectively (hence the characteristic assumption).

Definition 1.9. The **discriminant** of the curve $E : y^2 = x^3 + ax + b$ is

$$\Delta = -16(4a^3 + 27b^2).$$

Proposition 1.10. *The curve $E : y^2 = x^3 + ax + b$ is non-singular (i.e., is an elliptic curve) if and only if $\Delta \neq 0$.*

Proof. We prove both directions explicitly.

($\Rightarrow$) Singular implies $\Delta = 0$: The curve is singular if and only if there exists a point (x_0, y_0) where both the curve equation and its partial derivatives vanish:

$$\begin{aligned} y_0^2 &= x_0^3 + ax_0 + b, \\ \frac{\partial}{\partial x}(y^2 - x^3 - ax - b)\big|_{(x_0,y_0)} &= -3x_0^2 - a = 0, \\ \frac{\partial}{\partial y}(y^2 - x^3 - ax - b)\big|_{(x_0,y_0)} &= 2y_0 = 0. \end{aligned}$$

From the second and third equations: $y_0 = 0$ and $x_0^2 = -a/3$. Substituting into the first:

$$0 = x_0^3 + ax_0 + b = x_0(x_0^2 + a) + b = x_0\left(-\frac{a}{3} + a\right) + b = \frac{2a}{3}x_0 + b.$$

Thus $x_0 = -3b/(2a)$ (assuming $a \neq 0$). Substituting back into $x_0^2 = -a/3$:

$$\frac{9b^2}{4a^2} = -\frac{a}{3} \implies 27b^2 = -4a^3 \implies 4a^3 + 27b^2 = 0.$$

The case $a = 0$ gives $x_0^2 = 0$, so $x_0 = 0$, and then $b = 0$, again yielding $4a^3 + 27b^2 = 0$.

($\Leftarrow$) $\Delta = 0$ implies singular: Suppose $4a^3 + 27b^2 = 0$. We construct a singular point.

Case $a \neq 0$: Set $x_0 = -3b/(2a)$ and $y_0 = 0$. Then $x_0^2 = 9b^2/(4a^2) = -a/3$ (using $27b^2 = -4a^3$), so $-3x_0^2 - a = -3(-a/3) - a = 0$. Also $x_0^3 + ax_0 + b = x_0(x_0^2 + a) + b = x_0(2a/3) + b = -b + b = 0$. Thus $(x_0, 0)$ is a singular point.

Case $a = 0$: Then $27b^2 = 0$, so $b = 0$. The curve $y^2 = x^3$ has a cusp at $(0, 0)$. $\square$

1.5 The j-Invariant

Definition 1.11. The **j-invariant** of the elliptic curve $E : y^2 = x^3 + ax + b$ is

$$j(E) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} = 1728 \cdot \frac{4a^3}{-\Delta/16} = -1728 \cdot \frac{64a^3}{\Delta}. \tag{2}$$

Remark 1.12. The factor $1728 = 12^3 = 1728$ is chosen so that $j = 1728$ when $b = 0$ (and $a \neq 0$). The number 1728 also has the property that $1728 = 1728 \cdot 1$ in any field of characteristic > 3.

The fundamental property of the j-invariant is:

Theorem 1.13 (Classification by j-invariant)**.** *Two elliptic curves E_1 and E_2 over an algebraically closed field k are isomorphic (over k) if and only if $j(E_1) = j(E_2)$. Moreover, for every $j_0 \in k$, there exists an elliptic curve E with $j(E) = j_0$.*

Proof sketch. For the "only if" direction: one shows that j is invariant under the admissible coordinate changes. For the "if" direction: one explicitly constructs curves with any given j-invariant. For $j_0 \neq 0, 1728$, one can take $E : y^2 = x^3 - \frac{27j_0}{4(j_0-1728)}x + \frac{27j_0}{4(j_0-1728)}$. For $j_0 = 0$, take $y^2 = x^3 + 1$. For $j_0 = 1728$, take $y^2 = x^3 + x$.

See [1, Proposition III.1.4] for the complete proof. □

2 The Canonical Model for $j = 0$

2.1 Characterization of $j = 0$

Proposition 2.1. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over k with* $\mathrm{char}(k) > 3$*. Then*

$$j(E) = 0 \iff a = 0.$$

Proof. From the definition (2):

$$j(E) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2}.$$

($\Rightarrow$) Suppose $j(E) = 0$. Then the numerator must vanish: $4a^3 = 0$.

Since $\mathrm{char}(k) > 3$, the factor 4 is a unit in k (it's invertible). Thus $a^3 = 0$.

Since k is a field (hence an integral domain with no nilpotents), $a^3 = 0$ implies $a = 0$.

($\Leftarrow$) Suppose $a = 0$. Then $4a^3 = 0$, so the numerator of $j(E)$ is zero.

We must verify the denominator is non-zero: $4a^3 + 27b^2 = 27b^2$. Since E is an elliptic curve, $\Delta = -16(4a^3 + 27b^2) = -16(27b^2) \neq 0$. This requires $b^2 \neq 0$, hence $b \neq 0$.

Thus the denominator $27b^2 \neq 0$, and $j(E) = 1728 \cdot 0/27b^2 = 0$. □

Corollary 2.2. *Every elliptic curve E with $j(E) = 0$ over k (with $\mathrm{char}(k) > 3$) has the form*

$$E_b : y^2 = x^3 + b$$

for some $b \neq 0$ in k.

2.2 Scaling Argument: Reduction to E_1

Different values of b give different curve equations, but they are all isomorphic over $\bar{k}$.

Lemma 2.3. *All curves $E_b : y^2 = x^3 + b$ with $b \neq 0$ are isomorphic over $\bar{k}$.*

Proof. Consider the change of variables

$$\phi : (x, y) \mapsto (u^2 x, u^3 y)$$

for some $u \in \bar{k}^\times$. We compute how this transformation affects the curve equation.

Step 1: Effect on coordinates. If $(x', y') = (u^2 x, u^3 y)$, then the inverse transformation is $(x, y) = (u^{-2} x', u^{-3} y')$.

Step 2: Transformed curve equation. Substituting into $y^2 = x^3 + b$:

$$\begin{aligned} (u^{-3} y')^2 &= (u^{-2} x')^3 + b \\ u^{-6} y'^2 &= u^{-6} x'^3 + b \\ y'^2 &= x'^3 + u^6 b. \end{aligned}$$

Thus the transformation maps E_b to $E_{u^6 b}$.

Step 3: Choosing u. Given $b \neq 0$, we want to find u such that $u^6 b = 1$, i.e., $u^6 = b^{-1}$.

Since $k = \bar{k}$ is algebraically closed, the polynomial $t^6 - b^{-1}$ has a root in k. Call this root u. Then $u^6 = b^{-1}$, so $u^6 b = 1$.

Step 4: Conclusion. The map $(x, y) \mapsto (u^2 x, u^3 y)$ is an isomorphism from E_b to E_1. □

Corollary 2.4. *For studying $\mathrm{Aut}(E_{\bar{k}}, O)$ for $j = 0$ curves, it suffices to work with the canonical model*

$$E_1 : y^2 = x^3 + 1. \tag{3}$$

Any automorphism of E_b conjugates to an automorphism of E_1 via the scaling isomorphism.

3 Explicit Description of Automorphisms for $j = 0$

3.1 Sixth Roots of Unity

Before constructing the automorphisms, we establish notation for roots of unity.

Definition 3.1. The **n-th roots of unity** in k are elements $\zeta \in k$ satisfying $\zeta^n = 1$. They form a subgroup $\mu_n(k) \subseteq k^\times$.

Lemma 3.2. *In an algebraically closed field k of characteristic $p \geq 0$, if $\gcd(n, p) = 1$ (or $p = 0$), then $|\mu_n(k)| = n$.*

Proof. The n-th roots of unity are roots of $x^n - 1$. When $\gcd(n, p) = 1$ (or $p = 0$), the derivative nx^{n-1} is non-zero for $x \neq 0$, so $x^n - 1$ and its derivative share no common roots. Thus $x^n - 1$ has n distinct roots. □

Remark 3.3. When $p \mid n$, the polynomial $x^n - 1$ becomes inseparable and has fewer than n distinct roots. However, this case does not arise in our setting since $\mathrm{char}(k) > 3$ and we work with $n \in \{2, 3, 4, 6\}$.

Corollary 3.4. *Since $\mathrm{char}(k) > 3$ and $6 = 2 \cdot 3$, we have $\gcd(6, \mathrm{char}(k)) = 1$, so $|\mu_6(k)| = 6$.*

Definition 3.5. A **primitive n-th root of unity** is an element $\zeta \in \mu_n(k)$ of exact order n, i.e., $\zeta^n = 1$ but $\zeta^m \neq 1$ for $0 < m < n$.

Lemma 3.6. *Let $\omega \in k$ be a primitive cube root of unity, i.e., $\omega^3 = 1$ and $\omega \neq 1$. Then:*

(i) $\omega^2 + \omega + 1 = 0$.

(ii) The six 6th roots of unity are: $\mu_6(k) = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$.

(iii) A primitive 6th root of unity is $\zeta_6 = -\omega^2$ (or equivalently $-\omega$).

Proof. **(i)** Since $\omega^3 = 1$ and $\omega \neq 1$, we have $\omega^3 - 1 = 0$, which factors as:

$$(\omega - 1)(\omega^2 + \omega + 1) = 0.$$

Since $\omega \neq 1$, we must have $\omega^2 + \omega + 1 = 0$.

(ii) An element ζ is a 6th root of unity iff $\zeta^6 = 1$. The listed elements all satisfy this:

- $1^6 = 1$, $(-1)^6 = 1$.
- $\omega^6 = (\omega^3)^2 = 1^2 = 1$, and similarly for ω^2.
- $(-\omega)^6 = (-1)^6\omega^6 = 1$, and similarly for $-\omega^2$.

Since there are exactly 6 sixth roots of unity and we have listed 6 distinct elements, the list is complete.

(iii) We verify $\zeta = -\omega^2$ has order exactly 6:

$$\begin{aligned}
\zeta^1 &= -\omega^2 \neq 1, \\
\zeta^2 &= \omega^4 = \omega \neq 1, \\
\zeta^3 &= -\omega^6 = -1 \neq 1, \\
\zeta^4 &= \omega^8 = \omega^2 \neq 1, \\
\zeta^5 &= -\omega^{10} = -\omega \neq 1, \\
\zeta^6 &= \omega^{12} = 1.
\end{aligned}$$

Thus $-\omega^2$ has order exactly 6. □

3.2 Candidates for Automorphisms

Definition 3.7. For each $\zeta \in \mu_6(k)$, define the map

$$\phi_\zeta : E_1 \to E_1, \quad (x, y) \mapsto (\zeta^2 x, \zeta^3 y). \tag{4}$$

Proposition 3.8. *For each 6th root of unity ζ, the map ϕ_ζ is an automorphism of E_1 fixing O.*

Proof. We verify three properties:

(1) ϕ_ζ maps E_1 to itself (preserves the curve equation):

Let $(x, y) \in E_1$, so $y^2 = x^3 + 1$. We must show that $(\zeta^2 x, \zeta^3 y)$ also satisfies $y^2 = x^3 + 1$.

Compute:

$$\begin{aligned}
(\zeta^3 y)^2 &= \zeta^6 y^2 = 1 \cdot y^2 = y^2 \quad (\text{since } \zeta^6 = 1), \\
(\zeta^2 x)^3 + 1 &= \zeta^6 x^3 + 1 = 1 \cdot x^3 + 1 = x^3 + 1 \quad (\text{since } \zeta^6 = 1).
\end{aligned}$$

Since $y^2 = x^3 + 1$, both expressions equal $x^3 + 1$. Thus $(\zeta^2 x, \zeta^3 y)$ satisfies the curve equation. ✓

(2) ϕ_ζ fixes O (the point at infinity):

The curve E_1 in projective coordinates $[X : Y : Z]$ (where $x = X/Z$, $y = Y/Z$) is:

$$Y^2 Z = X^3 + Z^3.$$

The identity element is $O = [0 : 1 : 0]$ (the unique point with $Z = 0$).

The map ϕ_ζ in projective coordinates is:

$$\phi_\zeta : [X : Y : Z] \mapsto [\zeta^2 X : \zeta^3 Y : Z].$$

Evaluating at $O = [0 : 1 : 0]$:

$$\phi_\zeta([0 : 1 : 0]) = [\zeta^2 \cdot 0 : \zeta^3 \cdot 1 : 0] = [0 : \zeta^3 : 0].$$

In projective space, $[0 : \lambda : 0] = [0 : 1 : 0]$ for any $\lambda \neq 0$. Since $\zeta \neq 0$ (it's a root of unity), we have $\zeta^3 \neq 0$, so $[0 : \zeta^3 : 0] = [0 : 1 : 0] = O$. ✓

(3) ϕ_ζ is a bijection (invertible):

The inverse map is $\phi_{\zeta^{-1}}$:

$$\begin{aligned}\phi_\zeta \circ \phi_{\zeta^{-1}}(x, y) &= \phi_\zeta(\zeta^{-2}x, \zeta^{-3}y) \\ &= (\zeta^2 \cdot \zeta^{-2}x, \zeta^3 \cdot \zeta^{-3}y) \\ &= (x, y).\end{aligned}$$

Similarly, $\phi_{\zeta^{-1}} \circ \phi_\zeta = \mathrm{id}$. □

3.3 The Six Automorphisms Explicitly

Theorem 3.9. *The six automorphisms of E_1 fixing O are given by ϕ_ζ for $\zeta \in \mu_6(k)$:*

ζ	ζ^2	ζ^3	$\phi_\zeta(x, y)$
1	1	1	(x, y) *(identity)*
-1	1	-1	$(x, -y)$ *(hyperelliptic involution)*
ω	ω^2	1	$(\omega^2 x, y)$
$-\omega$	ω^2	-1	$(\omega^2 x, -y)$
ω^2	ω	1	$(\omega x, y)$
$-\omega^2$	ω	-1	$(\omega x, -y)$

where ω is a primitive cube root of unity.

Proof. We compute ζ^2 and ζ^3 for each ζ, using $\omega^3 = 1$:

$\zeta = 1$**:** $\zeta^2 = 1$, $\zeta^3 = 1$. Map: $(x, y) \mapsto (x, y)$ (identity).

$\zeta = -1$**:** $\zeta^2 = (-1)^2 = 1$, $\zeta^3 = (-1)^3 = -1$. Map: $(x, y) \mapsto (x, -y)$.

$\zeta = \omega$**:** $\zeta^2 = \omega^2$, $\zeta^3 = \omega^3 = 1$. Map: $(x, y) \mapsto (\omega^2 x, y)$.

$\zeta = -\omega$**:** $\zeta^2 = (-\omega)^2 = \omega^2$, $\zeta^3 = (-\omega)^3 = -\omega^3 = -1$. Map: $(x, y) \mapsto (\omega^2 x, -y)$.

$\zeta = \omega^2$**:** $\zeta^2 = \omega^4 = \omega^{3+1} = \omega$, $\zeta^3 = \omega^6 = (\omega^3)^2 = 1$. Map: $(x, y) \mapsto (\omega x, y)$.

$\zeta = -\omega^2$**:** $\zeta^2 = \omega^4 = \omega$, $\zeta^3 = -\omega^6 = -1$. Map: $(x, y) \mapsto (\omega x, -y)$. □

Remark 3.10 (Geometric interpretation)**.** The six automorphisms have natural geometric meanings:

- **Identity:** $(x, y) \mapsto (x, y)$ — do nothing.
- **Hyperelliptic involution:** $(x, y) \mapsto (x, -y)$ — reflection across the x-axis. This is the map $P \mapsto -P$ in the group law.

- **Rotation by $\pm 120°$:** $(x, y) \mapsto (\omega^{\pm 1} x, y)$ — these correspond to multiplying the x-coordinate by a cube root of unity.
- **Combined:** $(x, y) \mapsto (\omega^{\pm 1} x, -y)$ — rotation followed by reflection.

3.4 Group Structure

Proposition 3.11. *The map*

$$\Phi : \mu_6 \to \mathrm{Aut}(E_{\bar{k}}, O), \quad \zeta \mapsto \phi_\zeta$$

is an injective group homomorphism.

Proof. **Homomorphism:** For $\zeta_1, \zeta_2 \in \mu_6$, we compute:

$$\begin{aligned}(\phi_{\zeta_1} \circ \phi_{\zeta_2})(x, y) &= \phi_{\zeta_1}(\zeta_2^2 x, \zeta_2^3 y) \\ &= (\zeta_1^2 \cdot \zeta_2^2 x, \zeta_1^3 \cdot \zeta_2^3 y) \\ &= ((\zeta_1\zeta_2)^2 x, (\zeta_1\zeta_2)^3 y) \\ &= \phi_{\zeta_1\zeta_2}(x, y).\end{aligned}$$

Thus $\phi_{\zeta_1} \circ \phi_{\zeta_2} = \phi_{\zeta_1\zeta_2}$, confirming Φ is a homomorphism.

Injectivity: Suppose $\phi_{\zeta_1} = \phi_{\zeta_2}$. Then for all $(x, y) \in E_1$:

$$(\zeta_1^2 x, \zeta_1^3 y) = (\zeta_2^2 x, \zeta_2^3 y).$$

Choose a point with $x \neq 0$. Then $\zeta_1^2 x = \zeta_2^2 x$ implies $\zeta_1^2 = \zeta_2^2$.

Choose a point with $y \neq 0$. Then $\zeta_1^3 y = \zeta_2^3 y$ implies $\zeta_1^3 = \zeta_2^3$.

(Such points exist: $(0, 1)$ has $y \neq 0$ since $1^2 = 0^3 + 1$. For a point with $x \neq 0$, note that $x^3 + 1 = 0$ has roots $x \in \{-1, -\omega, -\omega^2\}$ (since $x^3 + 1 = (x + 1)(x^2 - x + 1)$ and $x^2 - x + 1$ has roots $-\omega, -\omega^2$). Thus $(-1, 0) \in E_1$ with $x = -1 \neq 0$.)

Now let $\eta = \zeta_1/\zeta_2$. Then $\eta^2 = 1$ and $\eta^3 = 1$.

Claim: $\eta = 1$.

Proof of claim: Since $\gcd(2, 3) = 1$, there exist integers a, b with $2a + 3b = 1$ (e.g., $a = -1$, $b = 1$). Then:

$$\eta = \eta^{2a+3b} = (\eta^2)^a \cdot (\eta^3)^b = 1^a \cdot 1^b = 1.$$

Thus $\zeta_1 = \zeta_2$, proving injectivity. □

Corollary 3.12. *Assuming the surjectivity proved in Section 4, we have:*

$$\mathrm{Aut}(E_{\bar{k}}, O) \cong \mu_6 \cong \mathbb{Z}/6\mathbb{Z}.$$

The group is cyclic of order 6, generated by any primitive 6th root of unity (e.g., $\phi_{-\omega^2}$).

Remark 3.13 (Alternative notation: $\{\pm 1, \pm\lambda, \pm\lambda^2\}$)**.** In the cryptographic literature, particularly in the context of the GLV (Gallant–Lambert–Vanstone) method for scalar multiplication, the six automorphisms are often denoted $\{\pm 1, \pm\lambda, \pm\lambda^2\}$. This notation arises from a different perspective:

Consider the endomorphism $\psi : (x, y) \mapsto (\omega x, y)$ where ω is a primitive cube root of unity. On a point P of prime order n, we have $\psi(P) = [\lambda]P$ for some $\lambda \in \mathbb{Z}/n\mathbb{Z}$. This eigenvalue λ satisfies:

$$\lambda^2 + \lambda + 1 \equiv 0 \pmod{n}$$

since $\psi^2 + \psi + 1 = 0$ (the minimal polynomial of ω).

The correspondence between notations is:

Our notation	GLV notation	Map $(x, y) \mapsto$
ϕ_1	$[1]$	(x, y)
ϕ_{-1}	$[-1]$	$(x, -y)$
ϕ_{ω^2}	$[\lambda]$	$(\omega x, y)$
$\phi_{-\omega^2}$	$[-\lambda]$	$(\omega x, -y)$
ϕ_ω	$[\lambda^2]$	$(\omega^2 x, y)$
$\phi_{-\omega}$	$[-\lambda^2]$	$(\omega^2 x, -y)$

Note that ϕ_{ω^2} corresponds to $[\lambda]$ because $\phi_{\omega^2} : (x, y) \mapsto (\omega x, y) = \psi(x, y)$. The apparent discrepancy (ω vs. ω^2) arises because $(\omega^2)^2 = \omega^4 = \omega$ when $\omega^3 = 1$.

For secp256k1, the eigenvalue is:

$\lambda =$ `0x5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd72`

satisfying $\lambda^2 + \lambda + 1 \equiv 0 \pmod{n}$ where n is the group order.

4 Proof That No Other Automorphisms Exist

We now prove that the six automorphisms ϕ_ζ are the *only* automorphisms of E_1 fixing O. We give two approaches: a direct computational proof (Method A) and a citation of the classification theorem (Method B).

4.1 Method A: Direct Weierstrass Computation

Theorem 4.1. *Every automorphism $\phi \in \mathrm{Aut}(E_1, O)$ has the form $\phi = \phi_\zeta$ for some 6th root of unity ζ.*

Proof. The most general change of coordinates preserving the Weierstrass form over a field of characteristic > 3 is:

$$(x, y) \mapsto (u^2 x + r,\ u^3 y + u^2 s x + t) \tag{5}$$

for some $u \in k^\times$ and $r, s, t \in k$. This is the standard form derived in [1, Chapter III, §1].

We determine which choices give an automorphism of $E_1 : y^2 = x^3 + 1$ that fixes O.

Step 1: Substituting into the curve equation.

Let $(x', y') = (u^2x + r, u^3y + u^2sx + t)$. The inverse transformation is:

$$x = u^{-2}(x' - r),$$
$$y = u^{-3}(y' - u^2s \cdot u^{-2}(x' - r) - t) = u^{-3}(y' - s(x' - r) - t).$$

Substituting into $y^2 = x^3 + 1$:

$$u^{-6}(y' - sx' + sr - t)^2 = u^{-6}(x' - r)^3 + 1.$$

Multiplying both sides by u^6:

$$(y' - sx' + sr - t)^2 = (x' - r)^3 + u^6. \tag{6}$$

Step 2: Expanding both sides.

Left side: Let $A = sr - t$ for brevity.

$$(y' - sx' + A)^2 = y'^2 - 2sx'y' + 2Ay' + s^2x'^2 - 2sAx' + A^2.$$

Right side:

$$(x' - r)^3 + u^6 = x'^3 - 3rx'^2 + 3r^2x' - r^3 + u^6.$$

Step 3: Comparing coefficients.

For the transformed curve to have short Weierstrass form $y'^2 = x'^3 + b'$, we need:

Coefficient of $x'y'$:

$$\text{LHS: } -2s, \quad \text{RHS: } 0.$$

Thus $-2s = 0$, giving $\boxed{s = 0}$.

Coefficient of y' (with $s = 0$, so $A = -t$):

$$\text{LHS: } 2A = -2t, \quad \text{RHS: } 0.$$

Thus $-2t = 0$, giving $\boxed{t = 0}$.

Coefficient of x'^2 (with $s = t = 0$):

$$\text{LHS: } s^2 = 0, \quad \text{RHS: } -3r.$$

Thus $-3r = 0$. Since $\mathrm{char}(k) > 3$, we have $3 \neq 0$, so $\boxed{r = 0}$.

Step 4: Simplified transformation.

With $r = s = t = 0$, the transformation becomes:

$$(x, y) \mapsto (u^2 x, u^3 y).$$

Equation (6) simplifies to:

$$y'^2 = x'^3 + u^6.$$

Step 5: Condition for automorphism.

For ϕ to be an automorphism of E_1 (not just a morphism to some other curve), the image curve must be E_1 itself, i.e., we need $y'^2 = x'^3 + 1$.

Comparing with $y'^2 = x'^3 + u^6$, we require:

$$u^6 = 1.$$

Thus u must be a 6th root of unity.

Conclusion: Every automorphism of E_1 fixing O has the form $\phi(x, y) = (u^2 x, u^3 y)$ where $u \in \mu_6$. This is exactly ϕ_ζ with $\zeta = u$. □

4.2 Method B: The Classification Theorem (Black Box)

For completeness, we state the general classification theorem.

Theorem 4.2 (Silverman, Theorem III.10.1)**.** *Let E be an elliptic curve over an algebraically closed field k with* $\mathrm{char}(k) > 3$*. Then:*

(i) If $j(E) \neq 0$ and $j(E) \neq 1728$, then $|\operatorname{Aut}(E_{\bar{k}}, O)| = 2$. The automorphisms are $\pm\mathrm{id}$*.*

(ii) If $j(E) = 1728$, then $|\operatorname{Aut}(E_{\bar{k}}, O)| = 4$. The automorphisms form a group isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

(iii) If $j(E) = 0$, then $|\operatorname{Aut}(E_{\bar{k}}, O)| = 6$. The automorphisms form a group isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

Proof. See [1, Theorem III.10.1]. The proof analyzes the general Weierstrass isomorphism formula exactly as we did in Method A, but systematically for all values of a and b. □

Remark 4.3. Theorem 4.2 encompasses our Method A result as the special case $j = 0$. The theorem provides additional information about the cases $j \neq 0$.

5 Global Classification: No j with $|\operatorname{Aut}| > 6$

Theorem 5.1. *For elliptic curves over an algebraically closed field k with* $\operatorname{char}(k) > 3$*:*

$$\max_{E/k} |\operatorname{Aut}(E_{\bar{k}}, O)| = 6,$$

and this maximum is attained exactly when $j(E) = 0$.

Proof. This is immediate from Theorem 4.2: the only possible values of $|\operatorname{Aut}(E_{\bar{k}}, O)|$ are $\{2, 4, 6\}$, with:

- 6 occurring precisely for $j = 0$,
- 4 occurring precisely for $j = 1728$,
- 2 occurring for all other j.

The maximum is 6, achieved only at $j = 0$. □

Remark 5.2 (Characteristics 2 and 3)**.** In characteristic 2 and 3, the situation is different. Supersingular elliptic curves can have larger automorphism groups:

- In characteristic 2: $|\operatorname{Aut}(E, O)|$ can be 2, 4, 8, or 24.
- In characteristic 3: $|\operatorname{Aut}(E, O)|$ can be 2, 4, 6, or 12.

See [1, Appendix A, Proposition 1.2] for details. These cases are explicitly **excluded** from our setting by the assumption $\operatorname{char}(k) > 3$.

6 Meta-Arguments: Why No "Hidden" Curves Exist

This section addresses potential concerns about whether some "unknown" or "exotic" elliptic curve might have a larger automorphism group. We show that the classification is exhaustive and complete.

6.1 The Moduli Space Perspective

Proposition 6.1. *Isomorphism classes of elliptic curves over $\bar{k}$ are in bijection with elements of $\bar{k}$ via the j-invariant:*

$$\{\textit{Elliptic curves over } \bar{k}\}/\cong \ \longleftrightarrow \ \bar{k}.$$

Proof. This is Theorem 1.13. □

Corollary 6.2. *The classification in Theorem 4.2 covers **every** elliptic curve over $\bar{k}$. There is no room for an elliptic curve whose j-invariant "escapes" the classification.*

Proof. Every elliptic curve E over $\bar{k}$ has a j-invariant $j(E) \in \bar{k}$. This value $j(E)$ falls into one of three cases: $j(E) = 0$, $j(E) = 1728$, or $j(E) \notin \{0, 1728\}$. In each case, Theorem 4.2 determines $|\operatorname{Aut}(E_{\bar{k}}, O)|$. □

The key insight is that the j-invariant provides a **complete** parametrization. The classification isn't a list of examples that might be incomplete; it's a structural result that applies to all curves by virtue of how they're defined.

6.2 The Complex-Analytic Viewpoint

Over $\mathbb{C}$, elliptic curves correspond to complex tori.

Proposition 6.3. *Every elliptic curve E over $\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ with $\Im(\tau) > 0$.*

Proposition 6.4. *Let $E = \mathbb{C}/\Lambda$. Then:*

$$\operatorname{Aut}(E, O) \cong \{\alpha \in \mathbb{C}^\times : \alpha\Lambda = \Lambda\}.$$

That is, automorphisms correspond to complex numbers that scale the lattice to itself.

Proof. An automorphism of $E = \mathbb{C}/\Lambda$ fixing $O = 0+\Lambda$ is a holomorphic map $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ with $\phi(0) = 0$. Such maps lift to multiplication by some $\alpha \in \mathbb{C}^\times$ on $\mathbb{C}$, with the condition that $\alpha\Lambda \subseteq \Lambda$. For ϕ to be an isomorphism, we need $\alpha\Lambda = \Lambda$. □

The lattices fall into exactly three types:

1. **Generic lattice:** $\alpha\Lambda = \Lambda$ only for $\alpha = \pm 1$, giving $|\operatorname{Aut}| = 2$.
2. **Square lattice** $\Lambda = \mathbb{Z} + i\mathbb{Z}$: The units of $\mathbb{Z}[i]$ (Gaussian integers) are $\{\pm 1, \pm i\}$. These all satisfy $\alpha\Lambda = \Lambda$, giving $|\operatorname{Aut}| = 4$. This corresponds to $j = 1728$.
3. **Hexagonal lattice** $\Lambda = \mathbb{Z} + \omega\mathbb{Z}$ where $\omega = e^{2\pi i/3}$: The units of $\mathbb{Z}[\omega]$ (Eisenstein integers) are $\{\pm 1, \pm\omega, \pm\omega^2\}$. These all satisfy $\alpha\Lambda = \Lambda$, giving $|\operatorname{Aut}| = 6$. This corresponds to $j = 0$.

Remark 6.5. This complex-analytic perspective provides an independent confirmation of the classification. The three cases correspond to:

- Generic lattices (most lattices),
- The unique lattice with 4-fold rotational symmetry (square lattice),
- The unique lattice with 6-fold rotational symmetry (hexagonal lattice).

No lattice can have higher rotational symmetry, because the only finite rotation groups of $\mathbb{C}$ compatible with a lattice structure are of order 1, 2, 3, 4, or 6 (the "crystallographic restriction").

Proposition 6.6. *The Eisenstein integers $\mathbb{Z}[\omega]$ and Gaussian integers $\mathbb{Z}[i]$ are the only imaginary quadratic rings with more than two units.*

Proof. For an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$, the ring of integers $\mathcal{O}_K$ has unit group:

- $\mathcal{O}_K^\times = \{\pm 1\}$ if $d \neq -1, -3$,
- $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$ if $d = -1$ (Gaussian integers),
- $\mathcal{O}_K^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ if $d = -3$ (Eisenstein integers).

This follows from the theory of Dirichlet's unit theorem applied to imaginary quadratic fields. □

This explains algebraically why exactly these three automorphism group sizes occur.

6.3 Isogenies Do Not Create Larger Automorphism Groups

Definition 6.7. An **isogeny** $\phi : E \to E'$ is a non-constant morphism of elliptic curves that maps O_E to $O_{E'}$. Two curves are **isogenous** if there exists an isogeny between them.

Proposition 6.8. *If E' is isogenous to E over $\bar{k}$, then E' is still an elliptic curve over $\bar{k}$ with some $j(E') \in \bar{k}$, and $|\operatorname{Aut}(E'_{\bar{k}}, O)|$ is determined by Theorem 4.2.*

Proof. An isogeny $\phi : E \to E'$ has as its target an elliptic curve E' by definition. Every elliptic curve over $\bar{k}$ has a j-invariant, and the classification applies. □

Remark 6.9 (Isogenies do not increase $|\operatorname{Aut}|$)**.** Even if we explore all curves isogenous to a given curve, each such curve is still classified by its j-invariant. The isogeny class of a curve with $j = 0$ contains curves with various j-invariants, but none of them can have $|\operatorname{Aut}| > 6$ in characteristic > 3.

In fact, computational experiments show that for $j = 0$ curves, all other j-invariants in the isogeny class typically give *smaller* automorphism groups ($|\operatorname{Aut}| = 2$), making $j = 0$ uniquely optimal within its isogeny class.

6.4 Complex Multiplication Does Not Increase $|\operatorname{Aut}|$

Definition 6.10. In characteristic 0, an elliptic curve E over $\bar{k}$ has **complex multiplication** (CM) if $\operatorname{End}(E_{\bar{k}})$ is strictly larger than $\mathbb{Z}$. In this case, $\operatorname{End}(E_{\bar{k}})$ is an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ for some $d > 0$.

Remark 6.11 (Positive characteristic)**.** In characteristic $p > 0$, curves with $\operatorname{End}(E_{\bar{k}}) \supsetneq \mathbb{Z}$ fall into two categories:

- **Ordinary curves:** $\operatorname{End}(E_{\bar{k}})$ is an order in an imaginary quadratic field (analogous to CM in char 0).
- **Supersingular curves:** $\operatorname{End}(E_{\bar{k}})$ is a maximal order in a quaternion algebra over $\mathbb{Q}$.

The term "CM" is sometimes reserved for the ordinary case. However, for our purposes (counting automorphisms), the distinction does not matter—see Section 9.4 for details.

Proposition 6.12. *Having complex multiplication does not increase* $|\operatorname{Aut}(E_{\bar{k}}, O)|$ *beyond the classification.*

Proof. The automorphism group $\operatorname{Aut}(E, O)$ equals the **unit group** of $\operatorname{End}(E)$:

$$\operatorname{Aut}(E, O) = \operatorname{End}(E)^{\times}.$$

Here $\operatorname{End}(E)^{\times}$ denotes endomorphisms that are invertible as morphisms, i.e., those of degree 1. An endomorphism $\phi \in \operatorname{End}(E)$ is a unit if and only if there exists $\psi \in \operatorname{End}(E)$ with $\phi \circ \psi = \psi \circ \phi = \mathrm{id}$, which happens precisely when ϕ is an automorphism fixing O.

Even when $\operatorname{End}(E)$ is a larger ring (CM case), its unit group is still finite and bounded:

- For orders in $\mathbb{Q}(i)$: units are $\{\pm 1, \pm i\}$ at most, giving $|\operatorname{Aut}| \leq 4$.
- For orders in $\mathbb{Q}(\omega)$: units are $\{\pm 1, \pm\omega, \pm\omega^2\}$ at most, giving $|\operatorname{Aut}| \leq 6$.
- For orders in other imaginary quadratic fields: units are $\{\pm 1\}$, giving $|\operatorname{Aut}| = 2$.

The curves with $j = 0$ have $\operatorname{End}(E) \supseteq \mathbb{Z}[\omega]$, achieving the maximum of 6 units. Having CM with a larger endomorphism ring doesn't add units beyond those already in the base ring. □

6.5 Mathematical Classification vs. Lists of Examples

Remark 6.13 (The nature of mathematical classification)**.** The classification of automorphism groups is a **structural theorem**, not a catalog of known examples. The theorem states:

> For *every* elliptic curve E over $\bar{k}$ with $\mathrm{char}(\bar{k}) > 3$, the value of $|\operatorname{Aut}(E_{\bar{k}}, O)|$ is uniquely determined by $j(E)$.

This is fundamentally different from empirical statements like "all known curves satisfy $|\operatorname{Aut}| \leq 6$." The classification covers *all* curves, including those never explicitly written down.

The proof proceeds by exhaustive analysis of coordinate transformations. Since:

1. Every elliptic curve has a Weierstrass equation (after possibly extending the field),
2. Every automorphism corresponds to an admissible coordinate change,
3. The admissible coordinate changes have a known parametric form,
4. Analyzing this form yields exactly which transformations are automorphisms,

the classification is complete by construction.

6.6 Computational Verification (Sanity Check)

Remark 6.14. While not a substitute for proof, one can verify consistency with databases:

- The LMFDB (L-functions and Modular Forms Database) contains extensive data on elliptic curves over $\mathbb{Q}$ and finite fields.
- The Cremona tables catalog elliptic curves over $\mathbb{Q}$ up to large conductor bounds.
- In all cases examined, $|\operatorname{Aut}(E_{\bar{k}}, O)| \in \{2, 4, 6\}$ for curves in characteristic > 3.

This consistency is expected since these databases contain examples of curves, and the classification applies to all examples. The databases cannot contain counterexamples because none exist—not because we haven't found them, but because the mathematical structure forbids them.

7 Twists and the Role of the Automorphism Group

The classification $|\operatorname{Aut}(E_{\bar{k}}, O)| \in \{2, 4, 6\}$ has an immediate and beautiful consequence: it governs the structure of **twists** of elliptic curves. The existence of sextic twists is *equivalent* to $|\operatorname{Aut}| = 6$, i.e., to $j = 0$.

7.1 Definition of Twists and Galois Cohomology

Definition 7.1 (Twist)**.** Let K be a field with separable closure $\bar{K}$, and let E/K be an elliptic curve. A **twist** of E over K is an elliptic curve E^{tw}/K such that

$$E^{\mathrm{tw}}_{\bar{K}} \cong E_{\bar{K}}.$$

Two twists are considered equivalent if they are isomorphic over K. We write $\operatorname{Twist}(E/K)$ for the set of equivalence classes of twists of E over K.

The key theorem connecting twists to automorphisms uses Galois cohomology:

Theorem 7.2 (Twists and cohomology)**.** *Let E/K be an elliptic curve over a field K with $\operatorname{char}(K) > 3$, and let $G_K = \operatorname{Gal}(\bar{K}/K)$. There is a natural bijection:*

$$\operatorname{Twist}(E/K) \;\cong\; H^1(G_K, \operatorname{Aut}(E_{\bar{K}}, O)).$$

Proof. This is a standard result in the theory of algebraic groups and descent. See [1, Chapter X, Proposition 2.2] for the complete proof. The key idea is that a twist corresponds to a "way of descending" the isomorphism $E^{\mathrm{tw}}_{\bar{K}} \cong E_{\bar{K}}$ to K, and such descents are classified by H^1. □

Recall from our earlier work that in characteristic > 3:

$$\operatorname{Aut}(E_{\bar{K}}, O) \cong \mu_n \quad \text{where } n \in \{2, 4, 6\},$$

with $n = 2$ for generic j, $n = 4$ for $j = 1728$, and $n = 6$ for $j = 0$.

7.2 Structure of Twists When $\operatorname{Aut} \cong \mu_n$

Proposition 7.3 (Structure of $H^1(G_K, \mu_n)$)**.** *Let K be a field of characteristic > 3, and $n \in \{2, 4, 6\}$.*

(i) Every twist of E corresponds to an element in $H^1(G_K, \mu_n)$.

(ii) If $\mu_n \subseteq K$ (i.e., all n-th roots of unity are in K), there is a natural isomorphism:

$$H^1(G_K, \mu_n) \;\cong\; K^\times/(K^\times)^n.$$

(iii) The group $H^1(G_K, \mu_n)$ has a filtration by subgroups corresponding to divisors of n:

$$H^1(G_K, \mu_d) \hookrightarrow H^1(G_K, \mu_n) \quad \text{for } d \mid n.$$

Proof. **(i)** follows from Theorem 7.2 and $\mathrm{Aut}(E_{\bar{K}}, O) \cong \mu_n$.

(ii) When $\mu_n \subseteq K$, the Galois action on μ_n is trivial, and the Kummer sequence

$$1 \to \mu_n \to \bar{K}^\times \xrightarrow{x \mapsto x^n} \bar{K}^\times \to 1$$

gives rise to the connecting homomorphism in cohomology:

$$K^\times/(K^\times)^n \xrightarrow{\sim} H^1(G_K, \mu_n).$$

(iii) The inclusion $\mu_d \hookrightarrow \mu_n$ for $d \mid n$ induces the map on cohomology. See [1, Chapter X, Section 3] for details. □

Theorem 7.4 (Classification of twist types)**.** *Let K be a field of characteristic > 3, and let E/K be an elliptic curve.*

(a) ***Generic case*** *($j \neq 0, 1728$)**:*** $\mathrm{Aut}(E_{\bar{K}}, O) \cong \mu_2$, *so*

$$\mathrm{Twist}(E/K) \cong H^1(G_K, \mu_2).$$

All twists are ***quadratic twists****, classified by $K^\times/(K^\times)^2$ when $-1 \in K$.*

(b) ***Case*** *$j = 1728$**:*** $\mathrm{Aut}(E_{\bar{K}}, O) \cong \mu_4$, *so*

$$\mathrm{Twist}(E/K) \cong H^1(G_K, \mu_4).$$

Besides quadratic twists (from $\mu_2 \subset \mu_4$), there exist ***quartic twists****.*

(c) ***Case*** *$j = 0$**:*** $\mathrm{Aut}(E_{\bar{K}}, O) \cong \mu_6$, *so*

$$\mathrm{Twist}(E/K) \cong H^1(G_K, \mu_6).$$

Besides quadratic twists (from $\mu_2 \subset \mu_6$), there exist:

- ***Cubic twists*** *(from $\mu_3 \subset \mu_6$),*
- ***Sextic twists*** *(from elements of exact order 6 in μ_6).*

Proof. This follows directly from Theorem 7.2 and the classification of $\mathrm{Aut}(E_{\bar{K}}, O)$ from Section 5. The subgroup structure of μ_n determines which "lower-degree" twists exist:

- μ_2 has no proper subgroups containing elements of order > 1 besides itself.
- μ_4 has μ_2 as a subgroup.
- μ_6 has μ_2 and μ_3 as subgroups.

Elements of $H^1(G_K, \mu_n)$ coming from a proper subgroup $\mu_d \subsetneq \mu_n$ correspond to twists of "lower degree" d. □

Remark 7.5 (Key insight)**.** The existence of sextic twists is **equivalent** to the condition $|\mathrm{Aut}(E_{\bar{K}}, O)| = 6$, which is equivalent to $j(E) = 0$. This is not a coincidence—the automorphisms *are* what make the different twist structures possible.

7.3 Explicit Formulas for Twists of $j = 0$ Curves

We now give explicit formulas for the model $E_b : y^2 = x^3 + b$ with $j = 0$.

Proposition 7.6 (Twists of $E_b : y^2 = x^3 + b$)**.** *Let K be a field of characteristic > 3, $b \in K^\times$, and*

$$E_b/K : y^2 = x^3 + b, \quad j(E_b) = 0.$$

For each $D \in K^\times$, consider the curve

$$E_{b,D} : y^2 = x^3 + D \cdot b.$$

Then:

(i) $E_{b,D}$ is a twist of E_b over K.

(ii) $E_{b,D_1} \cong_K E_{b,D_2}$ if and only if $D_1/D_2 \in (K^\times)^6$.

(iii) Therefore, isomorphism classes of twists of E_b over K are parametrized by

$$K^\times/(K^\times)^6,$$

in accordance with $|\operatorname{Aut}(E_{\bar{K}}, O)| = 6$.

Proof. **(i)** Over $\bar{K}$, choose $u \in \bar{K}$ with $u^6 = D$. Then the map

$$(x, y) \mapsto (u^2 x, u^3 y)$$

is an isomorphism from E_b to $E_{b,D}$:

$$y^2 = x^3 + b \implies (u^3 y)^2 = (u^2 x)^3 + u^6 b = (u^2 x)^3 + Db.$$

So $E_{b,D} \cong_{\bar{K}} E_b$.

(ii) $E_{b,D_1} \cong_K E_{b,D_2}$ iff there exists $u \in K^\times$ with:

$$D_2 b = u^6 \cdot D_1 b \implies D_2/D_1 = u^6 \in (K^\times)^6.$$

(iii) Follows from (ii). □

Corollary 7.7 (Substructure of twists for $j = 0$)**.** *For $E_b : y^2 = x^3 + b$ with $j = 0$:*

Twist type	*Subgroup of μ_6*	*Parametrized by*
Quadratic	$\mu_2 = \{1, -1\}$	$K^\times/(K^\times)^2$
Cubic	$\mu_3 = \{1, \omega, \omega^2\}$	$K^\times/(K^\times)^3$
Sextic	*full* μ_6	$K^\times/(K^\times)^6$

Explicitly:

- ***Quadratic twist*** *by D: corresponds to $D \bmod (K^\times)^2$, giving $E_{b,D^3} : y^2 = x^3 + D^3 b$.*
- ***Cubic twist*** *by D: corresponds to $D \bmod (K^\times)^3$, giving $E_{b,D^2} : y^2 = x^3 + D^2 b$.*
- ***Sextic twist*** *by D: corresponds to $D \bmod (K^\times)^6$, giving $E_{b,D} : y^2 = x^3 + Db$.*

A sextic twist is "genuinely new" (not quadratic or cubic) when D is not a square or cube in K.

Remark 7.8 (Twists over $\mathbb{Q}$)**.** All elliptic curves over $\mathbb{Q}$ with j-invariant 0 are sextic twists of one another. The set of such curves is parametrized by $\mathbb{Q}^\times/(\mathbb{Q}^\times)^6$, which is infinite (since $\mathbb{Q}^\times/(\mathbb{Q}^\times)^6 \cong \mathbb{Z}/6\mathbb{Z} \times \bigoplus_p \mathbb{Z}/6\mathbb{Z}$).

Example 7.9 (secp256k1 and its twists)**.** The curve secp256k1: $y^2 = x^3 + 7$ over $\mathbb{F}_p$ has $j = 0$.

Quadratic twist: For a non-square $D \in \mathbb{F}_p^\times$:

$$E^{(D)} : y^2 = x^3 + D^3 \cdot 7.$$

The point counts satisfy $|E(\mathbb{F}_p)| + |E^{(D)}(\mathbb{F}_p)| = 2p + 2$, so the quadratic twist has trace of Frobenius with opposite sign.

Cubic twist: If $\omega \in \mathbb{F}_p$ is a primitive cube root of unity (which exists since $p \equiv 1 \pmod 3$), then for D not a cube:

$$E^{(D)} : y^2 = x^3 + D^2 \cdot 7.$$

Sextic twist: For D neither a square nor a cube in $\mathbb{F}_p^\times$:

$$E^{(D)} : y^2 = x^3 + D \cdot 7.$$

This is isomorphic to secp256k1 only over a degree-6 extension of $\mathbb{F}_p$.

Remark 7.10 (Cryptographic relevance of twists)**.**

1. **Twist attacks:** In ECDH and ECDSA, if a malicious party sends a point on a twist rather than the original curve, the discrete log may be computable in a smaller group. For $j = 0$ curves, there are more twist classes to consider.
2. **Pairing-based cryptography:** Curves with $j = 0$ (like BLS12-381) use sextic twists to define the "twist" subgroup G_2 for pairings. The sextic twist structure allows embedding degree optimization.
3. **Hash-to-curve:** The isogeny structure between a curve and its twists can be exploited for efficient deterministic hashing to the curve.

7.4 The Fundamental Connection

We conclude this section by emphasizing the tight relationship:

Theorem 7.11 (Automorphisms determine twist structure)**.** *For an elliptic curve E over a field K of characteristic > 3:*

$$\boxed{\textit{Sextic twists of } E \textit{ exist} \iff |\operatorname{Aut}(E_{\bar{K}}, O)| = 6 \iff j(E) = 0.}$$

Similarly:

$$\begin{aligned} \textit{Quartic twists exist} &\iff |\operatorname{Aut}| \geq 4 \iff j \in \{0, 1728\}, \\ \textit{Only quadratic twists exist} &\iff |\operatorname{Aut}| = 2 \iff j \neq 0, 1728. \end{aligned}$$

Proof. This is a direct consequence of Theorems 7.2 and 7.4, combined with the classification of $\operatorname{Aut}(E_{\bar{K}}, O)$ by j-invariant. □

This theorem elegantly explains *why* the classification $|\operatorname{Aut}| \in \{2, 4, 6\}$ matters beyond just counting symmetries: it directly governs the arithmetic structure of how curves can be "twisted" over non-algebraically-closed fields.

8 Examples and Sanity Checks

8.1 Detailed Example over $\mathbb{C}$

Consider $E : y^2 = x^3 + 1$ over $\mathbb{C}$. This curve corresponds to the hexagonal lattice $\Lambda = \mathbb{Z} + \omega\mathbb{Z}$ where $\omega = e^{2\pi i/3}$.

Proposition 8.1. *The automorphism $\phi_{\omega^2} : (x, y) \mapsto (\omega x, y)$ corresponds to multiplication by ω^2 on the torus $\mathbb{C}/\Lambda$.*

Proof. If $z \in \mathbb{C}$ corresponds to a point $(x, y) \in E(\mathbb{C})$ via the Weierstrass parametrization, then:

$$x = \wp(z; \Lambda), \quad y = \wp'(z; \Lambda),$$

where $\wp$ is the Weierstrass $\wp$-function.

For the hexagonal lattice with $\omega^3 = 1$, the $\wp$-function satisfies:

$$\wp(\omega z; \Lambda) = \omega^{-2}\wp(z; \Lambda).$$

This can be verified by noting that $\omega\Lambda = \Lambda$ (the lattice is preserved under multiplication by ω), and tracking how the double periodicity transforms.

Since $\omega^{-2} = \omega^{3-2} = \omega$, we have:

$$\wp(\omega z) = \omega\wp(z).$$

For the derivative:

$$\wp'(\omega z) = \frac{d}{d(\omega z)}\wp(\omega z) = \omega^{-1}\frac{d}{dz}(\omega\wp(z)) = \omega^{-1}\cdot\omega\cdot\wp'(z) = \wp'(z).$$

Thus multiplication by ω on $\mathbb{C}/\Lambda$ induces:

$$(x,y) = (\wp(z),\wp'(z)) \mapsto (\wp(\omega z),\wp'(\omega z)) = (\omega\wp(z),\wp'(z)) = (\omega x, y).$$

This is ϕ_{ω^2}. □

Remark 8.2. The apparent mismatch (ω^2 in the subscript vs. multiplication by ω) arises because our convention defines $\phi_\zeta(x,y) = (\zeta^2 x, \zeta^3 y)$. For $\zeta = \omega^2$: $\zeta^2 = \omega^4 = \omega$ and $\zeta^3 = \omega^6 = 1$.

8.2 Detailed Example over $\mathbb{F}_p$ with $p \equiv 1 \pmod 3$

Let p be a prime with $p \equiv 1 \pmod 3$. Then $\mathbb{F}_p^\times$ has order $p-1$, which is divisible by 3. Thus $\mathbb{F}_p$ contains a primitive cube root of unity ω.

Example 8.3 (Explicit computation for $p = 7$)**.** We have $7 \equiv 1 \pmod 3$. The primitive cube roots of unity in $\mathbb{F}_7$ satisfy $\omega^3 = 1, \omega \neq 1$, i.e., $\omega^2+\omega+1 = 0$.

Checking: $2^3 = 8 \equiv 1 \pmod 7$ and $2 \neq 1$. Also $2^2 + 2 + 1 = 7 \equiv 0 \pmod 7$. So $\omega = 2$ works.

The 6th roots of unity in $\mathbb{F}_7$ are:

$$\mu_6(\mathbb{F}_7) = \{1,6,2,5,4,3\} = \{1,-1,\omega,-\omega,\omega^2,-\omega^2\}.$$

(Here $-1 = 6$, $\omega = 2$, $-\omega = 5$, $\omega^2 = 4$, $-\omega^2 = 3$.)

The six automorphisms of $E : y^2 = x^3 + 1$ over $\mathbb{F}_7$ are:

ζ	$\phi_\zeta(x,y)$
1	(x,y)
6	$(x,6y) = (x,-y)$
2	$(4x,y)$
5	$(4x,6y) = (4x,-y)$
4	$(2x,y)$
3	$(2x,6y) = (2x,-y)$

All six automorphisms are defined over $\mathbb{F}_7$ (not just over $\overline{\mathbb{F}_7}$) because $\omega \in \mathbb{F}_7$.

Example 8.4 (secp256k1)**.** The curve secp256k1 is defined over $\mathbb{F}_p$ where:

$$p = 2^{256} - 2^{32} - 977.$$

One can verify that $p \equiv 1 \pmod 3$:

$$2^{256} \equiv 2^{256 \mod \phi(3)} = 2^{256 \mod 2} = 2^0 = 1 \pmod 3.$$

$$2^{32} \equiv 2^{32 \mod 2} = 2^0 = 1 \pmod 3.$$

$$977 = 975 + 2 = 325 \cdot 3 + 2 \equiv 2 \pmod 3.$$

$$p \equiv 1 - 1 - 2 \equiv -2 \equiv 1 \pmod 3.$$

Thus all six automorphisms exist over $\mathbb{F}_p$. The cube root of unity is:

$\omega =$ `0x7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ee`.

The automorphism $(x, y) \mapsto (\omega x, y)$ can be computed with a single field multiplication, making automorphism detection in Pollard's rho algorithm very efficient.

8.3 Example over $\mathbb{F}_p$ with $p \equiv 2 \pmod 3$

Example 8.5 ($p = 5$)**.** We have $5 \equiv 2 \pmod 3$. The multiplicative group $\mathbb{F}_5^\times$ has order 4, not divisible by 3. Thus $\mathbb{F}_5$ contains no primitive cube root of unity.

For $E : y^2 = x^3 + 1$ over $\mathbb{F}_5$:

- Over $\mathbb{F}_5$: $\mathrm{Aut}(E_{\mathbb{F}_5}, O) = \{(x, y) \mapsto (x, y),\ (x, y) \mapsto (x, -y)\} \cong \mathbb{Z}/2\mathbb{Z}$.
- Over $\overline{\mathbb{F}_5}$: $\mathrm{Aut}(E_{\overline{\mathbb{F}_5}}, O) \cong \mathbb{Z}/6\mathbb{Z}$ (all six automorphisms).

The "missing" automorphisms require a cube root of unity ω, which exists in $\mathbb{F}_{5^2} = \mathbb{F}_{25}$ but not in $\mathbb{F}_5$.

8.4 Contrast: $j = 1728$

Example 8.6. Consider $E : y^2 = x^3 + x$ with $j(E) = 1728$.

Claim: $|\mathrm{Aut}(E_{\bar{k}}, O)| = 4$, with automorphisms:

$$\phi_u : (x, y) \mapsto (u^2 x, u^3 y) \quad \text{for } u \in \mu_4 = \{1, -1, i, -i\} \text{ where } u^4 = 1.$$

Proof: Using Method A, a transformation $(x, y) \mapsto (u^2 x, u^3 y)$ preserves $y^2 = x^3 + x$ iff:

$$(u^3 y)^2 = (u^2 x)^3 + (u^2 x)$$
$$u^6 y^2 = u^6 x^3 + u^2 x.$$

Substituting $y^2 = x^3 + x$:

$$u^6(x^3 + x) = u^6 x^3 + u^2 x \implies u^6 x = u^2 x.$$

For this to hold for all x, we need $u^6 = u^2$, i.e., $u^4 = 1$.

Thus $u \in \mu_4$, giving 4 automorphisms:

- $u = 1$: $(x, y) \mapsto (x, y)$
- $u = -1$: $(x, y) \mapsto (x, -y)$
- $u = i$: $(x, y) \mapsto (i^2 x, i^3 y) = (-x, -iy)$
- $u = -i$: $(x, y) \mapsto ((-i)^2 x, (-i)^3 y) = (-x, iy)$

This curve corresponds to the square lattice $\Lambda = \mathbb{Z} + i\mathbb{Z}$ with unit group μ_4.

8.5 Contrast: Generic Curve ($j \neq 0, 1728$)

Example 8.7. Consider $E : y^2 = x^3 + 2x + 3$. We verify that $|\operatorname{Aut}(E_{\bar{k}}, O)| = 2$.

First, check non-singularity: $\Delta = -16(4 \cdot 8 + 27 \cdot 9) = -16(32 + 243) = -16 \cdot 275 = -4400 \neq 0$. ✓

Next, compute j: $j = 1728 \cdot 32/275 = 55296/275 \approx 201$. Since $j \neq 0, 1728$, this is a generic curve.

A transformation $(x, y) \mapsto (u^2 x, u^3 y)$ preserves $y^2 = x^3 + 2x + 3$ iff:

$$u^6 y^2 = u^6 x^3 + 2u^2 x + 3.$$

Substituting $y^2 = x^3 + 2x + 3$:

$$u^6(x^3 + 2x + 3) = u^6 x^3 + 2u^2 x + 3.$$

Comparing coefficients:

- x^3: $u^6 = u^6$ ✓
- x: $2u^6 = 2u^2 \implies u^4 = 1$
- constant: $3u^6 = 3 \implies u^6 = 1$

So $u^4 = 1$ and $u^6 = 1$. Since $\gcd(4, 6) = 2$, we have $u^2 = 1$, giving $u = \pm 1$.

Thus $\operatorname{Aut}(E_{\bar{k}}, O) = \{(x, y) \mapsto (x, y),\ (x, y) \mapsto (x, -y)\} \cong \mathbb{Z}/2\mathbb{Z}$.

9 Advanced Topics

9.1 Automorphisms over the Base Field vs. the Algebraic Closure

So far we have worked over an algebraically closed field $k = \bar{k}$. For applications, one often needs to understand which automorphisms are defined over a smaller base field K.

Definition 9.1. Let E be an elliptic curve over a field K with $\mathrm{char}(K) > 3$. Define:

- $\mathrm{Aut}(E_K, O)$: automorphisms of E defined over K,
- $\mathrm{Aut}(E_{\bar{K}}, O)$: geometric automorphisms over $\bar{K}$.

There is a natural inclusion $\mathrm{Aut}(E_K, O) \hookrightarrow \mathrm{Aut}(E_{\bar{K}}, O)$.

Proposition 9.2. *For a curve $E : y^2 = x^3 + b$ with $j(E) = 0$ over a field K of characteristic > 3:*

$$\mathrm{Aut}(E_K, O) \cong \mu_6(K),$$

where $\mu_6(K) = \{\zeta \in K : \zeta^6 = 1\}$ is the group of 6th roots of unity in K.

Proof. An automorphism $\phi_\zeta : (x, y) \mapsto (\zeta^2 x, \zeta^3 y)$ is defined over K if and only if $\zeta^2, \zeta^3 \in K$. Since $\gcd(2, 3) = 1$, this is equivalent to $\zeta \in K$. Combined with $\zeta^6 = 1$, this gives $\zeta \in \mu_6(K)$. □

Corollary 9.3 (Automorphisms over finite fields)**.** *For $E : y^2 = x^3 + b$ over $\mathbb{F}_q$ with $q = p^n$, $p > 3$:*

$$|\mathrm{Aut}(E_{\mathbb{F}_q}, O)| = \gcd(6, q - 1).$$

Explicitly:

$q \bmod 6$	$\gcd(6, q-1)$	$\lvert\mathrm{Aut}(E_{\mathbb{F}_q}, O)\rvert$
1	6	6
5	2	2

(For $p > 3$, we have $q \equiv 1$ or $5 \pmod 6$.)

Example 9.4 (secp256k1 revisited)**.** For secp256k1, $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 2$, so $p \equiv 1 \pmod 6$. Thus all six geometric automorphisms are defined over $\mathbb{F}_p$:

$$|\mathrm{Aut}(E_{\mathbb{F}_p}, O)| = 6.$$

Example 9.5 (Automorphisms over $\mathbb{Q}$ and $\mathbb{R}$)**.** For $E : y^2 = x^3 + 1$ over $\mathbb{Q}$:

- $\mu_6(\mathbb{Q}) = \{1, -1\}$ (the only rational roots of unity),
- Thus $|\mathrm{Aut}(E_{\mathbb{Q}}, O)| = 2$.

Over $\mathbb{R}$: same result, $|\mathrm{Aut}(E_{\mathbb{R}}, O)| = 2$.

Over $\mathbb{C}$: $\mu_6(\mathbb{C}) = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}$, so $|\mathrm{Aut}(E_{\mathbb{C}}, O)| = 6$.

9.2 Characteristics 2 and 3: The Excluded Cases

Our main results require $\mathrm{char}(k) > 3$. Here we explain precisely what happens in characteristics 2 and 3.

Theorem 9.6 (Automorphisms in characteristic 2 and 3)**.** *Over an algebraically closed field k:*

(i) In characteristic 2: $|\operatorname{Aut}(E_k, O)| \in \{2, 4, 8, 24\}$.

(ii) In characteristic 3: $|\operatorname{Aut}(E_k, O)| \in \{2, 4, 6, 12\}$.

Proof. See [1, Appendix A, Proposition 1.2]. □

Remark 9.7 (Why larger groups exist in small characteristic)**.** In characteristics 2 and 3, the Weierstrass equation takes different forms that allow additional symmetries:

Characteristic 2: The short Weierstrass form $y^2 = x^3 + ax + b$ is not available (we cannot complete the square). Instead, curves have forms like $y^2 + xy = x^3 + a_2x^2 + a_6$ or $y^2 + a_3y = x^3 + a_4x + a_6$. Supersingular curves in characteristic 2 can have automorphism groups of order up to 24.

Characteristic 3: Similarly, $y^2 = x^3+ax+b$ is available but the polynomial x^3 has different behavior. Supersingular curves can have automorphism groups of order up to 12.

Example 9.8 (Order 24 in characteristic 2)**.** Over $\overline{\mathbb{F}_2}$, the curve $y^2+y = x^3$ is supersingular with $j = 0$ and $|\operatorname{Aut}(E, O)| = 24$. This group is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$.

Example 9.9 (Order 12 in characteristic 3)**.** Over $\overline{\mathbb{F}_3}$, the curve $y^2 = x^3-x$ is supersingular with $j = 0$ and $|\operatorname{Aut}(E, O)| = 12$.

Remark 9.10 (Design decision)**.** The restriction to characteristic > 3 is standard in elliptic curve cryptography for several reasons:

1. Short Weierstrass form is available, simplifying formulas.
2. The classification $|\operatorname{Aut}| \in \{2, 4, 6\}$ is clean.
3. Supersingular curves (which have larger automorphism groups in char 2, 3) are avoided for security reasons.

Our statement "$|\operatorname{Aut}(E_{\bar{k}}, O)| \leq 6$ in characteristic > 3" is precisely valid, and the exclusion of characteristics 2 and 3 is essential.

9.3 The Moduli Perspective: $j = 0$ as an Orbifold Point

The classification of automorphisms has a beautiful interpretation in terms of the moduli stack of elliptic curves.

Definition 9.11. The **moduli stack** $\mathcal{M}_{1,1}$ parametrizes elliptic curves. Over an algebraically closed field k of characteristic > 3, the coarse moduli space is the affine line $\mathbb{A}^1_k$ with coordinate j.

Proposition 9.12. *The stabilizer of a geometric point of $\mathcal{M}_{1,1}$ corresponding to an elliptic curve E is canonically isomorphic to $\mathrm{Aut}(E_k, O)$.*

This explains why $j = 0$ and $j = 1728$ are special:

- **Generic points** ($j \neq 0, 1728$): stabilizer of order 2, the minimum possible for an elliptic curve (since $-\mathrm{id}$ is always an automorphism).
- $j = 1728$: stabilizer of order 4, corresponding to the Gaussian symmetry (square lattice over $\mathbb{C}$).
- $j = 0$: stabilizer of order 6, the maximum in characteristic > 3, corresponding to hexagonal symmetry (Eisenstein lattice over $\mathbb{C}$).

Remark 9.13 (Orbifold points)**.** In the language of stacks, $j = 0$ and $j = 1728$ are **orbifold points** where the moduli stack has non-trivial automorphisms. The point $j = 0$ is the "most symmetric" point in characteristic > 3, having the largest stabilizer group.

Proposition 9.14 (Uniqueness of the maximum)**.** *In characteristic > 3, the point $j = 0$ is the unique point of $\mathcal{M}_{1,1}$ with stabilizer of order 6. No other point has a larger stabilizer.*

Proof. This follows from Theorem 4.2: the only possible stabilizer orders are $\{2, 4, 6\}$, and 6 is achieved exactly at $j = 0$. □

9.4 The Identity $\mathrm{Aut}(E, O) = \mathrm{End}(E)^\times$ in Detail

We now give a more detailed treatment of the relationship between automorphisms and the endomorphism ring.

Proposition 9.15. *For an elliptic curve E over an algebraically closed field k:*

$$\mathrm{Aut}(E_k, O) = \mathrm{End}(E_k)^\times,$$

where $\mathrm{End}(E_k)^\times$ denotes the group of units (invertible elements) in the endomorphism ring.

Proof. An endomorphism $\phi : E \to E$ is in $\mathrm{End}(E_k)^\times$ if and only if there exists $\psi : E \to E$ with $\phi \circ \psi = \psi \circ \phi = [1]$ (the identity map). This happens if and only if ϕ is an isomorphism, which (since ϕ is a group homomorphism fixing O) means $\phi \in \mathrm{Aut}(E_k, O)$.

Alternatively, $\phi \in \mathrm{End}(E_k)^\times$ iff $\deg(\phi) = 1$ (since the degree is multiplicative and $\deg([1]) = 1$). Endomorphisms of degree 1 are exactly the automorphisms. □

Corollary 9.16 (Classification of units in endomorphism rings)**.** *The group* $\mathrm{End}(E_k)^\times$ *(units = automorphisms) is determined by* $j(E)$*:*

j-invariant	$\mathrm{End}(E_k)^\times$	$\lvert \mathrm{Aut}(E_k, O) \rvert$
$j \neq 0, 1728$	$\{\pm 1\}$	2
$j = 1728$	$\{\pm 1, \pm i\}$	4
$j = 0$	$\{\pm 1, \pm\omega, \pm\omega^2\}$	6

where $\omega = e^{2\pi i/3}$ *is a primitive cube root of unity.*

Proof. The key observation is that $\mathrm{End}(E_k)^\times$ consists of endomorphisms of degree 1, and these are precisely determined by the j-invariant regardless of whether the full endomorphism ring is commutative or not.

In characteristic 0 (e.g., over $\mathbb{C}$):

- For $j \neq 0, 1728$: $\mathrm{End}(E_k) = \mathbb{Z}$ or an order in an imaginary quadratic field $K \neq \mathbb{Q}(i), \mathbb{Q}(\omega)$. Units are $\{\pm 1\}$.
- For $j = 1728$: $\mathrm{End}(E_k)$ is an order in $\mathbb{Q}(i)$. Units are $\{\pm 1, \pm i\}$.
- For $j = 0$: $\mathrm{End}(E_k)$ is an order in $\mathbb{Q}(\omega)$. Units are $\{\pm 1, \pm\omega, \pm\omega^2\}$.

In characteristic $p > 3$: For *supersingular* curves, $\mathrm{End}(E_k)$ is a maximal order in a quaternion algebra, which is non-commutative. However, the degree-1 endomorphisms (units) still form the same finite groups as above, because:

- The center of $\mathrm{End}(E_k)$ contains an imaginary quadratic order, and
- Units of degree 1 must lie in this center and satisfy the same constraints.

Thus $\lvert \mathrm{Aut}(E_k, O) \rvert \in \{2, 4, 6\}$ holds in all characteristics > 3, with the value determined by $j(E)$. □

Remark 9.17. The cases $j = 0$ and $j = 1728$ are exactly those where the endomorphism ring contains an imaginary quadratic order with more than 2 units. This is no coincidence: the extra automorphisms *are* the extra units. In characteristic 0, these are precisely the CM curves with $\mathrm{End}(E_k)$ an order in $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$.

10 Conclusion

We have established the following facts for elliptic curves over an algebraically closed field k with $\mathrm{char}(k) > 3$:

1. **Explicit structure for $j = 0$:** For E with $j(E) = 0$, we have $|\operatorname{Aut}(E_{\bar{k}}, O)| = 6$, with automorphisms explicitly given by:
$$\phi_\zeta : (x, y) \mapsto (\zeta^2 x, \zeta^3 y) \quad \text{for } \zeta \in \mu_6.$$
2. **Group structure:** The automorphism group $\operatorname{Aut}(E_{\bar{k}}, O) \cong \mathbb{Z}/6\mathbb{Z}$ is cyclic of order 6.
3. **Completeness:** No other automorphisms exist, as proven by direct computation of all possible Weierstrass coordinate changes.
4. **Global optimality:** The maximum $|\operatorname{Aut}(E_{\bar{k}}, O)| = 6$ is achieved **only** for $j = 0$. For $j = 1728$, we get $|\operatorname{Aut}| = 4$; for all other j, we get $|\operatorname{Aut}| = 2$.
5. **Exhaustive classification:** Every elliptic curve over $\bar{k}$ has some j-invariant, and the classification theorem determines $|\operatorname{Aut}|$ for all possible j. No "hidden" curves with larger automorphism groups can exist in characteristic > 3.
6. **Cryptographic relevance:** For Pollard's rho algorithm on ECDLP, the speedup factor $\sqrt{|\operatorname{Aut}|}$ is maximized at $\sqrt{6} \approx 2.45$ for curves with $j = 0$, such as secp256k1.

References

[1] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 2nd edition, 2009.

[2] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[3] Dale Husemöller, *Elliptic Curves*, Graduate Texts in Mathematics, vol. 111, Springer-Verlag, New York, 2nd edition, 2004.

[4] Lawrence C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2nd edition, 2008.

[5] Max Kronberg, Muhammad Afzal Soomro, and Jaap Top, *Twists of Elliptic Curves*, Symmetry, Integrability and Geometry: Methods and Applications (SIGMA), vol. 13, 083, 2017.

A Summary of Key Results

j-invariant	$\lvert \mathrm{Aut}(E_{\bar{k}}, O) \rvert$	Structure	Representative curve
$j \neq 0, 1728$	2	$\mathbb{Z}/2\mathbb{Z}$	$y^2 = x^3 + ax + b$ (generic)
$j = 1728$	4	$\mathbb{Z}/4\mathbb{Z}$	$y^2 = x^3 + x$
$j = 0$	6	$\mathbb{Z}/6\mathbb{Z}$	$y^2 = x^3 + 1$

Valid for: Algebraically closed field k with $\mathrm{char}(k) > 3$.

Twist Structure (Section 7):

j-invariant	$\lvert \mathrm{Aut} \rvert$	Types of twists
$j \neq 0, 1728$	2	Quadratic only
$j = 1728$	4	Quadratic, quartic
$j = 0$	6	Quadratic, cubic, sextic

Key insight: Sextic twists exist $\Leftrightarrow \lvert \mathrm{Aut} \rvert = 6 \Leftrightarrow j = 0$.

B Verification of Key Formulas

The following formulas have been verified computationally:

1. **Discriminant:** $\Delta = -16(4a^3 + 27b^2)$
2. **j-invariant:** $j = 1728 \cdot \frac{4a^3}{4a^3+27b^2}$
3. $j = 0 \Leftrightarrow a = 0$ (for non-singular curves)
4. **Automorphism formula:** $(x, y) \mapsto (\zeta^2 x, \zeta^3 y)$ preserves $y^2 = x^3 + 1$ iff $\zeta^6 = 1$
5. **Powers of ω:** For $\omega^3 = 1$, $\omega \neq 1$: $\omega^4 = \omega$, $\omega^6 = 1$, $\omega^2 + \omega + 1 = 0$
6. **secp256k1:** $p = 2^{256} - 2^{32} - 977 \equiv 1 \pmod 3$, and the given ω satisfies $\omega^3 \equiv 1 \pmod p$

All verifications pass with numerical tests over multiple primes.