FINITENESS OF THE TATE-SHAFAREVICH GROUPS FOR ELLIPTIC CURVES OVER THE FIELD OF RATIONAL NUMBERS

LAN NGUYEN

Abstract. Let $E$ be an elliptic curve over $\mathbb{Q}$. Let $\widehat{\text{III}}(E)$ be a certain group of equivalence classes of homogeneous spaces of $E$ called its Tate-Shafarevich group. We show in this paper that this group has finite cardinality and discuss its role in the Birch and Swinnerton-Dyer Conjecture. In particular, our result implies the Parity Conjecture, or the Birch and Swinnerton-Dyer Conjecture modulo 2. It also removes the finiteness condition of $\widehat{\text{III}}(E)$ from previous results in the literature of this subject and makes possible for some computation problems concerning the Strong Birch and Swinnerton-Dyer Conjecture. In addition, we also give an analogue of the Hasse-Minkowski Theorem for cubic plane curves.

1. Introduction

1.1. Elliptic Curves and Tate-Shafarevich Groups. Let $E$ be an elliptic curve over $\mathbb{Q}$. Let $G_\mathbb{Q}$ denote the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. For each rational prime $p$, let $G_{\mathbb{Q}_p}$ denote the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. Let $WC(E/K) := H^1(G_K, E)$ be the associated Weil-Châtelet group where $K$ denotes either $\mathbb{Q}$ or $\mathbb{Q}_p$ for some rational prime $p$, finite or infinite. The Tate-Shafarevich group $\widehat{\text{III}}(E)$ of $E$ is defined by Lang-Tate ([12]) and Shafarevich ([21]) in this case as the collection of elements of $WC(E/\mathbb{Q})$ that becomes trivial in all completions of $\mathbb{Q}$. In other words, $\widehat{\text{III}}(E)$ consists of all homogeneous spaces of $E$, up to equivalence, which have points everywhere locally. In the language of Galois Cohomology, $\widehat{\text{III}}(E)$ can be written as

$$\widehat{\text{III}}(E) := \bigcap_p \ker(H^1(G_{\mathbb{Q}_p}, E) \to H^1(G_{\mathbb{Q}_p}, E)).$$

The group $\widehat{\text{III}}(E)$ has been conjectured by Tate and Shafarevich ([12, 21, 23]), called the Tate Shafarevich Conjecture in the literature, to be finite. Moreover, Cassels ([3]) and Tate show that if the cardinality of $\widehat{\text{III}}(E)$ is finite, then it is a perfect square due to the existence of a certain alternate bilinear pairing on it (see [16] for polarized abelian variety case). The group $\widehat{\text{III}}(E)$ plays a vital role in the Birch and Swinnerton-Dyer Conjecture (BSDC), particularly the strong Birch and Swinnerton Conjecture ([1]). In fact, Artin and Tate ([22]) prove that, in the function field case, the finiteness of $\widehat{\text{III}}(E)$ is equivalent to the entire BSDC. To state this conjecture, we need to define some terminology.

2010 Mathematics Subject Classification. 11C08, 11D09, 11D25, 11G05, 11G07, 11Y16.

Key words and phrases. Tate-Shafarevich Group; Homogeneous Space; Elliptic Curve; Hasse Principle; Hasse-Minkowski Theorem; Birch and Swinnerton-Dyer Conjecture; Parity Conjecture.
Let $E$ be an elliptic curve over $\mathbb{Q}$. Let $E(\mathbb{Q})$ denote the set of points of $E$ defined over $\mathbb{Q}$. By Mordell’s Theorem ([15]), $E(\mathbb{Q})$ is finitely generated and

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tor}}$$

where $E(\mathbb{Q})_{\text{tor}}$ denotes the collection of rational points of finite order, a finite group, and $r$, a nonnegative integer, is called the Weil-Mordell rank of $E$ and denoted by $r_{\text{WM}}(E)$. The group $E(\mathbb{Q})_{\text{tor}}$ is completely understood due to a result of Mazur ([14]). The $L$-function of $E$ in a complex variable $s$ is defined as the Euler product

$$L_E(s) := \prod_{p \nmid N_E} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N_E} (1 - a_p p^{-s})^{-1}$$

where $N_E$ denotes the conductor of $E$. Define

$$r_{\text{anal}}(E) := \text{ord}_{s=1} L_E(s),$$

a nonnegative integer.

**Strong Birch and Swinnerton-Dyer Conjecture**: Let $E$ be an elliptic curve over $\mathbb{Q}$. Then:

1. $r_{\text{anal}}(E) = r_{\text{WM}}(E)$ where $r_{\text{anal}}$ and $r_{\text{WM}}$ are the analytic and the Weil-Mordell ranks of $E$ respectively.
2. $\text{III}(E)$ is finite.
3. $c_E = \lim_{s \to 1} \frac{L_E(s)}{(s-1)^{r_{\text{WM}}}} = \frac{|\text{III}(E)| \Omega(E) \text{Reg}(E) \prod_p c_p}{|E(\mathbb{Q})_{\text{tor}}^2|}$ (1.2)

where:
- $c_E$ is the coefficients of the term $(s - 1)^{r_{\text{anal}}}$ in the Taylor expansion of $L_E(s)$ at $s = 1$.
- $\Omega(E)$ is the real period of $E$ multiplied by the number components of $E(\mathbb{R})$.
- $c_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$ for each prime $p$ is the corresponding Tamagawa number.
- $\text{Reg}(E)$ is the regulator of $E$, which is the determinant of the height pairing.
- $E(\mathbb{Q})_{\text{tor}}$ is the group of rational torsion points of $E$.

One of the first partial result, toward proving the BSDC, was obtained by J. Coates and A. Wiles ([5]). Now the full conjecture is known for all elliptic curves over $\mathbb{Q}$ with rank at most one.

The question of the finiteness of $\text{III}(E)$ presents a major obstacle in answering many fundamental questions, both theoretically and computationally, toward understanding the Birch and Swinnerton-Dyer Conjecture. Theoretically, one of such important questions is the Parity Conjecture ([8]). Computationally, important examples of such questions are the verification of $c_E$ in the strong Birch and Swinnerton-Dyer Conjecture and the determination of existence of rational points of an arbitrary genus one curve over $\mathbb{Q}$. Similar situations can be seen throughout the literature on this subject. Even in situations where it is possible to deduce interesting arguments to circumvent this obstacle, it often complicates and lengthens the arguments (see [4] for a discussion of this).
1.2. **Hasse Principle.** One of the fundamental questions in Diophantine Number Theory is whether a rational Diophantine equation or a system of such equations has a solution in \( \mathbb{Q} \). Answering such a question is difficult and not always possible. Such questions are addressed by Hilbert’s 10th problem ([13]).

If a polynomial with rational coefficients has a nontrivial rational solution, then it has nontrivial solutions in all \( p \)-adic fields \( \mathbb{Q}_p \) and in \( \mathbb{R} \). The Hasse principle asks when the reverse direction is true. That is, if a polynomial with rational coefficients has a nontrivial solution in each \( p \)-adic field \( \mathbb{Q}_p \) and in \( \mathbb{R} \), does it have a nontrivial rational solution? If it does, then one says that it satisfies the Hasse principle. More generally, the Hasse principle for a variety is a statement about the existence of global points given the existence of local points. For an elliptic curve \( E \) over \( \mathbb{Q} \), Manin shows that the obstruction for the Hasse principle is completely accounted for by \( \text{III}(E) \). That is, if \( \text{III}(E) \) is nontrivial, then there is at least one homogenous space of \( E \) which has points over all local fields but does not have a global point. For a quadratic form, Minkowski established around 1920 (generalized to arbitrary number fields by Hasse later) the following beautiful theorem ([20]):

**Theorem 1.1.** (Hasse-Minkowski Theorem) Let \( F \) be a quadratic form with rational coefficients. Then \( F \) has a nontrivial rational solution if and only if \( F \) has a nontrivial solution in each completion \( \mathbb{Q}_p \) of \( \mathbb{Q} \) where \( p \) ranges over all finite and infinite primes.

For cubic forms, Selmer shows that the Hasse principle fails with the following well-known counterexample:

\[
3x^3 + 4y^3 + 5z^3 = 0.
\]  

(1.3)

H. Davenport ([7]) shows that the Hasse principle holds trivially for cubic forms with rational coefficients in at least 16 variables. Roger Heath-Brown proves a similar result, using the Hardy-Littlewood circle method, for cubic forms with rational coefficients in at least 14 variables ([9]). For nonsingular cubic forms with rational coefficients, Hooley ([10]) uses a similar method to show that the Hasse principle holds for forms with 9 or more variables.

2. **Main Results**

The problems considered in this paper belong to the general area of local-global principle. Among the results in this area, the Hasse-Minkowski Theorem mentioned above, which treats the case of quadratic forms, is one of the most well-known results. The main results of this paper are our resolutions of the Shafarevich and Tate Conjecture (which has been conjectured by Shafarevich, Tate, Cassels, Birch and Swinnerton-Dyer around 1958-1959 ([12, 21, 23])) which is part of the Strong Birch and Swinnerton-Dyer Conjecture ([1]), and the Parity Conjecture ([8]). These results also make it possible for some important computational problems concerning the strong Birch and Swinnerton-Dyer Conjecture to be carried out.

**Theorem 2.1.** Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Then the associated Tate-Shafarevich group \( \text{III}(E) \) has finite cardinality.

**Remark 2.2.** Theorem 2.1 is proved by Rubin ([18]) for elliptic curves \( E \) having complex multiplication and Weil-Mordell rank at most 1. It is then extended by Kolyvagin ([11]) to modular elliptic curves \( E \) with Weil-Mordell rank at most 1 and then to all elliptic curves \( E \) over \( \mathbb{Q} \) of Weil-Mordell rank at most 1 due to the Modularity Theorem of Breuil, Conrad, Diamond, and Taylor ([2]).
Since there are a number of results in the literature depending on the finiteness of $III(E)$, we select a few important representatives as consequences of our main result.

**Corollary 2.3.** The Parity Conjecture holds. In other words,

$$r_{\text{anal}}(E) \equiv r_{\text{WM}}(E) \pmod{2}$$

where $r_{\text{anal}}(E)$ and $r_{\text{WM}}(E)$ are the analytic and the Weil-Mordell ranks of $E$ respectively.

For computational problems concerning the strong Birch and Swinnerton-Dyer Conjecture, we have the following results ([6, 23]):

**Corollary 2.4.** Let $E$ be an elliptic curve over $\mathbb{Q}$. Then the standard process always produces generators for the group $E(\mathbb{Q})$ and thus the term $c_E$ in the Strong Birch and Swinnerton-Dyer Conjecture is computable.

**Corollary 2.5.** There is an algorithm with a finite number of steps which determines whether a genus one curve $C$ with rational coefficients has a nontrivial rational solution.

3. **Proof of Results**

**Proof.** (Proof of Theorem 2.1) To prove Theorem 2.1, we first prove the following lemma:

**Lemma 3.1.** (Key Lemma) Let $F(x, y, z)$ be a cubic plane curve with rational coefficients, i.e., $F(x, y, z)$ is a cubic form

$$A_1x^3 + A_2y^3 + A_3z^3 + A_4x^2y + A_5x^2z + A_6y^2x + A_7y^2z + A_8z^2x + A_9z^2y + A_{10}xyz$$

where $A_i$ is a rational number for each $i$. Suppose that $F(x, y, z) = 0$ has a nontrivial solution in each $\mathbb{Q}_p$ where $p$ ranges over all primes, finite and infinite. If $F(x, y, z)$ does not have a nontrivial rational solution then $F(x, y, z)$ is of the form

$$F(x, y, z) = A_1x^3 + A_2y^3 + A_3z^3$$

such that $A_1A_2A_3 \neq 0$.

**Remark 3.2.** The Key Lemma above can be viewed as an analogue of the Hasse-Minkowski Theorem for cubic plane curves.

**Proof.** (Proof of Key Lemma)

In the rest of the paper, a local or global solution

$$(x_0, y_0, z_0) \quad (3.1)$$

of $F(x, y, z) = 0$ is said to be nontrivial if at least one of the components in nonzero.

Let $F(x, y, z) = 0$ be a cubic plane curve with rational coefficients. Thus it can be written in the form:

$$A_1x^3 + A_2y^3 + A_3z^3 + A_4x^2y + A_5x^2z + A_6y^2x + A_7y^2z + A_8z^2x + A_9z^2y + A_{10}xyz = 0 \quad (3.2)$$

with rational coefficients $A_i$ for each $i$. Suppose that the cubic form $F$ has nontrivial local solutions at all places. We want to study whether $F$ has a nontrivial rational solution. We may assume that

$$A_1A_2A_3 \neq 0 \quad (3.3)$$
since otherwise, say $A_1 = 0$, then $(1, 0, 0)$ is a nontrivial rational solution of $F$. Also, it follows from (3.3) that if $(u, v, t)$ is a nontrivial solution of $F$, then at most one of the components can be zero.

For the rest of the proof of Theorem 2.1, let us suppose that at least one of the coefficients $A_i$ for $i > 3$ is nonzero. By multiply both sides of (3.2) by $x, y,$ and $z$, we obtain respectively:

$$A_1x^4 + A_2xy^3 + A_3xz^3 + A_4x^3y + A_5x^2z + A_6y^2x^2 + A_7y^2zx + A_8z^2x^2 + A_9z^2yx + A_{10}x^2yz = 0,$$

(3.4)

$$A_1x^3y + A_2y^4 + A_3x^3y + A_4x^2y^2 + A_5x^2zy + A_6y^3x + A_7y^3z + A_8z^2xy + A_9z^2y^2 + A_{10}xy^2z = 0,$$

(3.5)

$$A_1x^3z + A_2y^3z + A_3z^4 + A_4x^2yz + A_5x^2z^2 + A_6y^2xz + A_7y^2z^2 + A_8z^3x + A_9z^3y + A_{10}xyz^2 = 0.$$  

(3.6)

Let $X := x^2$, $Y := y^2$, $Z := z^2$, $W := xy$, $M := xz$, and $N := yz$. Then

$$WM - XM = 0,$$

(3.7)

$$MN - ZW = 0,$$

(3.8)

$$WN - YM = 0,$$

(3.9)

$$W^2 - XY = 0,$$

(3.10)

$$M^2 - XZ = 0,$$

(3.11)

$$N^2 - YZ = 0.$$  

(3.12)

Thus (3.4), (3.5), and (3.6) can be rewritten respectively as

$$A_1X^2 + A_2YW + A_3ZM + A_4XM + A_5XM + A_6XY + A_7YM + A_8XZ + A_9ZW + A_{10}XN = 0,$$

(3.13)

$$A_1XW + A_2Y^2 + A_3ZN + A_4XY + A_5XN + A_6YW + A_7YN + A_8ZW + A_9YZ + A_{10}YM = 0,$$

(3.14)

$$A_1XM + A_2YN + A_3Z^2 + A_4XN + A_5XZ + A_6YM + A_7YZ + A_8ZM + A_9ZN + A_{10}ZW = 0.$$  

(3.15)

Note that quadratic forms (3.7)-(3.15) have common nontrivial local solutions at all places since $F(x, y, z) = 0$ is assumed to have nontrivial local solutions at all places. For convenience, we denote (3.13), (3.14), and (3.15) by $F_x(X, Y, Z, W, M, N) = 0$, $F_y(X, Y, Z, W, M, N) = 0$, and $F_z(X, Y, Z, W, M, N) = 0$ respectively where each index indicates which variable is multiplied to both sides of (3.2) to form the corresponding equation.

Since we assume that $A_1A_2A_3 \neq 0$, it can be seen from equations (3.13)-(3.15) that two of the three variables $W$, $M$, and $N$ appear in each of these equations with nonzero coefficients. Since we also assume that $A_i \neq 0$ for at least one $i > 3$, it can be verified that at least one of the equations (3.13)-(3.15) can be rewritten, using equations (3.7)-(3.9), so that all three variables $W$, $M$, and $N$ appear in it with nonzero coefficients. Note that in these rewritten equations, the terms with coefficients $A_1$, $A_2$, and $A_3$ are unchanged.
Proposition 3.3. The system of equations
\[
\begin{align*}
F_x(X, Y, Z, W, M, N) &= 0 \\
F_y(X, Y, Z, W, M, N) &= 0 \\
F_z(X, Y, Z, W, M, N) &= 0 \\
WM - XN &= 0 \\
MN - ZW &= 0 \\
WN - YM &= 0 \\
W^2 - XY &= 0 \\
M^2 - XZ &= 0 \\
N^2 - YZ &= 0 
\end{align*}
\] (3.16)

has a common nontrivial rational solution if and only if equation (3.2) has a nontrivial rational solution.

Proof. If equation (3.2) has a nontrivial rational solution, then it is clear from its construction that the system of equations (3.16) has a common nontrivial rational solution. Suppose that the system of equations (3.16) has a common nontrivial rational solution, say
\[
(X_0, Y_0, Z_0, W_0, M_0, N_0) \neq (0, 0, 0, 0, 0, 0).
\] (3.17)

It follows from (3.3) and (3.13)-(3.15) that at least two of the three components $X_0$, $Y_0$, and $Z_0$ must be nonzero. If all three components are nonzero, then it can be verified that all the rest of the components must also be nonzero. If one of the components $X_0$, $Y_0$, and $Z_0$ is zero, then two of the components $W_0$, $M_0$, and $N_0$ must be zero. For example, if $X_0 = 0$, then it follows that $W_0 = 0$ and $M_0 = 0$. Now let us suppose that $X_0 \neq 0$. Then
\[
\left(1, \frac{Y_0}{X_0}, \frac{Z_0}{X_0}, \frac{W_0}{X_0}, \frac{M_0}{X_0}, \frac{N_0}{X_0}\right)
\] (3.18)
is also a nontrivial common rational solution of system (3.16). Also,
\[
\begin{align*}
W_0^2 - X_0Y_0 &= 0 \\
M_0^2 - X_0Z_0 &= 0 \\
N_0^2 - Y_0Z_0 &= 0 
\end{align*}
\] (3.19)

implies that
\[
\begin{align*}
\left(\frac{W_0}{X_0}\right)^2 &= \frac{Y_0}{X_0} \\
\left(\frac{M_0}{X_0}\right)^2 &= \frac{Z_0}{X_0} \\
\left(\frac{N_0}{X_0}\right)^2 &= \frac{Y_0 \cdot Z_0}{X_0 \cdot X_0}
\end{align*}
\] (3.20)

It is then straightforward, using (3.2), (3.7), and (3.13), to verify that
\[
\left(1, \frac{W_0}{X_0}, \frac{M_0}{X_0}\right)
\] (3.21)
is a nontrivial rational solution of (3.2). Similar arguments work for $Y_0 \neq 0$ and for $Z_0 \neq 0$. Note that $A_1 A_2 A_3 \neq 0$ implies that if $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ is a nontrivial solution of system (3.16), then at most one of the numbers $X_0, Y_0, Z_0$ can be zero.

\[ \square \]

**Remark 3.4.** As a result of the proof of Proposition 3.3, it can be verified from construction of (3.13) – (3.15) that (3.2) has a nontrivial rational solution $(x_0, y_0, z_0)$ with

- $x_0 \neq 0$ if and only if system (3.16), without equations $F_x(X, Y, Z, W, M, N)$ and/or $F_y(X, Y, Z, W, M, N)$, has a nontrivial solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $X_0 \neq 0$.
- $y_0 \neq 0$ if and only if system (3.16), without equations $F_x(X, Y, Z, W, M, N)$ and/or $F_z(X, Y, Z, W, M, N)$, has a nontrivial solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $Y_0 \neq 0$.
- $z_0 \neq 0$ if and only if system (3.16), without equations $F_x(X, Y, Z, W, M, N)$ and/or equation $F_y(X, Y, Z, W, M, N)$, has a nontrivial solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $Z_0 \neq 0$.

**Proposition 3.5.** *System of equations (3.16) has a common nontrivial rational solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $X_0 Y_0 Z_0 \neq 0$ if and only if system of equations (3.16) without equation (3.10) has a common nontrivial rational solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $X_0 Y_0 Z_0 \neq 0$. The same statement holds when (3.11) or (3.12) replaces (3.10).*

**Proof.** If system (3.16) has a common nontrivial rational solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $X_0 Y_0 Z_0 \neq 0$ (and thus $W_0 M_0_0$), then it is clear that system (3.16) without equation (3.10) has a common nontrivial rational solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $X_0 Y_0 Z_0 \neq 0$. Now suppose system (3.16) without equation (3.10) has a common nontrivial rational solution $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ with $X_0 Y_0 Z_0 \neq 0$. Since $Y_0 \neq 0$ and

\[
W_0 N_0 - Y_0 M_0 = 0, \tag{3.22}
\]

\[
M_0 = \frac{W_0 N_0}{Y_0}, \tag{3.23}
\]

Since $X_0 Y_0 Z_0 \neq 0$ implies $N_0 \neq 0$,

\[
W_0 M_0 - X_0 N_0 = 0, \tag{3.24}
\]

together with (3.23) give

\[
\frac{N_0 W_0^2}{Y_0} = X_0 N_0 \tag{3.25}
\]

and thus

\[
W_0^2 = X_0 Y_0. \tag{3.26}
\]

Therefore, $(X_0, Y_0, Z_0, W_0, M_0, N_0)$ is also a nontrivial rational solution to equation (3.10) and thus a common nontrivial rational solution to system (3.16). Similar arguments work when (3.11) or (3.12) replaces (3.10).

\[ \square \]
Proposition 3.8. Proof. It follows by a direct computation.

Lemma 3.9. If \((X_0, Y_0, Z_0, W_0, M_0, N_0)\) is a common nontrivial rational solution of system (3.34), then \(X_0Y_0 \neq 0\).
Proof. If \((X_0, Y_0, Z_0, W_0, M_0, N_0)\) is a common nontrivial rational solution of system (3.34), then it is a common nontrivial rational solution of systems
\[
\begin{aligned}
F_x(X, Y, Z, W, M, N) &= 0 \\
M^2 - XZ &= 0
\end{aligned}
\tag{3.35}
\]
and
\[
\begin{aligned}
F_y(X, Y, Z, W, M, N) &= 0 \\
N^2 - YZ &= 0
\end{aligned}
\tag{3.36}
\]
If \(Y_0 = 0\), then it follows from the assumption \(A_1A_2A_3 \neq 0\) that \(X_0Z_0 \neq 0\). It also follows from \(Y_0 = 0\), via equation (3.13) and system (3.35), that
\[
\begin{aligned}
A_1X^2 + A_5ZM + A_8XZ &= 0 \\
M^2 - XZ &= 0
\end{aligned}
\tag{3.37}
\]
has \((X_0, Z_0, M_0)\) as a common nontrivial rational solution. Hence,
\[
\left(1, \frac{Z_0}{X_0}, \frac{M_0}{X_0}\right)
\]
is also a common nontrivial rational solution of (3.37), and thus equation
\[
M^2 - XZ = 0
\]
implies that
\[
\left(\frac{M_0}{X_0}\right)^2 = \frac{Z_0}{X_0}.
\tag{3.38}
\]
Then it can be verified that
\[
\left(1, \frac{M_0}{X_0}\right)
\]
is a nontrivial rational solution of
\[
A_1x^3 + A_3z^3 + A_5x^2z + A_8z^2x = 0,
\]
which contradicts our assumptions in Remark 3.6.
If \(X_0 = 0\), then the assumption \(A_1A_2A_3 \neq 0\) implies that \(Y_0Z_0 \neq 0\). Together with equation (3.14) and system (3.36), it can be verified that
\[
\begin{aligned}
A_2Y^2 + A_3ZN + A_7YN + A_9YZ &= 0 \\
N^2 - YZ &= 0
\end{aligned}
\tag{3.40}
\]
has \((Y_0, Z_0, N_0)\) as a common nontrivial rational solution. Since \(Y_0 \neq 0\),
\[
\left(1, \frac{Z_0}{Y_0}, \frac{N_0}{Y_0}\right)
\]
is also a common nontrivial rational solution of (3.40). Hence, equation
\[
N^2 - YZ
\]
implies that
\[
\left(\frac{N_0}{Y_0}\right)^2 = \frac{Z_0}{Y_0}.
\]
As a result, it can be verified that
\[(1, \frac{N_0}{Y_0})\]

is a nontrivial rational solution of
\[A_2y^3 + A_3z^3 + A_7y^2z + A_9z^2y = 0,\]
which again contradicts the assumption made in Remark 3.6.

\[\square\]

Define
\[F_1 := \alpha_1(F_x(X,Y,Z,W,M,N)) + \alpha_2(F_y(X,Y,Z,W,M,N)) + \alpha_3(WM - XN) + \alpha_4(MN - ZW) + \alpha_5(WN - YM) + \alpha_6(M^2 - XZ) + \alpha_7(N^2 - YZ)\]
and
\[F_2 := \beta_1(F_x(X,Y,Z,W,M,N)) + \beta_2(F_y(X,Y,Z,W,M,N)) + \beta_3(WM - XN) + \beta_4(MN - ZW) + \beta_5(WN - YM) + \beta_6(M^2 - XZ) + \beta_7(N^2 - YZ)\]
where \(\alpha_i\) and \(\beta_i\) are indeterminates for each \(i\). Let
\[\mathcal{R} := \mathcal{R}(X,Y,Z,M,N,\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7)\]
be the Resultant of \(\mathcal{F}_1\) and \(\mathcal{F}_2\) with respect to the variable \(W\). Then \(\mathcal{R}\) is the determinant of the Sylvester matrix
\[\mathcal{G} := \mathcal{G}(X,Y,Z,M,N,\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7)\]
with \(\mathcal{G}\) being the following matrix
\[
\begin{pmatrix}
A_1 & B_1 & C_1 & 0 \\
0 & A_1 & B_1 & C_1 \\
A_2 & B_2 & C_2 & 0 \\
0 & A_2 & B_2 & C_2 \\
\end{pmatrix}
\]  
(3.41)

where:
- \(A_1\) is the coefficient of \(W^2\) of \(\mathcal{F}_1\).
- \(B_1\) is the coefficient of \(W^1\) of \(\mathcal{F}_1\).
- \(C_1\) is the coefficient of \(W^0\) of \(\mathcal{F}_1\).
- \(A_2\) is the coefficient of \(W^2\) of \(\mathcal{F}_2\).
- \(B_2\) is the coefficient of \(W^1\) of \(\mathcal{F}_2\).
- \(C_2\) is the coefficient of \(W^0\) of \(\mathcal{F}_2\).

Since \(A_1 = A_2 = 0\), it follows from Proposition 3.7 that
\[\mathcal{R} := \mathcal{R}(X,Y,Z,M,N,\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5,\alpha_6,\alpha_7,\beta_1,\beta_2,\beta_3,\beta_4,\beta_5,\beta_6,\beta_7) = 0.\]  
(3.42)
That is \(\mathcal{R}\), viewed as a polynomial in \(X, Y, Z, W, M, \) and \(N\), is identically zero. Therefore, all the equations in system (3.34) have a common factor
\[\mathcal{C}(X,Y,Z,W,M,N),\]
a homogeneous polynomial with rational coefficients. There are two cases:
1. \(\deg(\mathcal{C}(X,Y,Z,W,M,N)) = 1\).
2. \(\deg(\mathcal{C}(X,Y,Z,W,M,N)) = 2\).
If \( \deg(\mathcal{C}(X, Y, Z, W, M, N)) = 1 \), then system (3.34) must have a nontrivial common rational solution. Together with Lemma 3.9, it can be verified that

\[
\mathcal{C}(X, Y, Z, W, M, N) = aX + bY
\]

(3.43)

for some rational numbers \( a \) and \( b \) such that \( ab \neq 0 \). Let \( Z_1 \) be a nonzero rational number. It follows from (3.43) that there exists a nontrivial rational solution \((X_0, Y_0, Z_0, W_0, M_0, N_0)\) such that \( X_0 = -b, Y_0 = a \) and \( Z_0 = LZ_1 \) for some nonzero rational number \( L \). Thus \( X_0Y_0Z_0 \neq 0 \) as required.

If \( \deg(\mathcal{C}(X, Y, Z, W, M, N)) = 2 \), i.e., a quadratic form, then it can be verified that there exist nonzero rational numbers \( E_1, E_2, E_3, E_4, \) and \( E_5 \) such that:

\[
F_x(X, Y, Z, W, M, N) = E_1\mathcal{C}(X, Y, Z, W, M, N),
\]

(3.44)

\[
F_y(X, Y, Z, W, M, N) = E_2\mathcal{C}(X, Y, Z, W, M, N),
\]

(3.45)

\[
WM - XN = E_3\mathcal{C}(X, Y, Z, W, M, N),
\]

(3.46)

\[
MN - ZW = E_4\mathcal{C}(X, Y, Z, W, M, N),
\]

(3.47)

\[
WN - YM = E_5\mathcal{C}(X, Y, Z, W, M, N),
\]

(3.48)

\[
M^2 - XZ = E_6\mathcal{C}(X, Y, Z, W, M, N),
\]

(3.49)

\[
N^2 - YZ = E_7\mathcal{C}(X, Y, Z, W, M, N).
\]

(3.50)

Since system (3.34) has common nontrivial local solutions at all places, \( \mathcal{C}(X, Y, Z, W, M, N) \) also does. Then by the Hasse-Minkowski Theorem for a quadratic form, \( \mathcal{C}(X, Y, Z, W, M, N) \) has a nontrivial rational solution

\[
(X_0, Y_0, Z_0, W_0, M_0, N_0).
\]

(3.51)

Therefore, system (3.34) has \((X_0, Y_0, Z_0, W_0, M_0, N_0)\) as a common nontrivial rational solution.

From (3.44)-(3.50), it can be verified that there exist nonzero rational numbers \( L_1, L_2, L_3, L_4, L_5, \) and \( L_6 \) such that:

\[
F_x(X, Y, Z, W, M, N) = L_1(M^2 - XZ),
\]

(3.52)

\[
F_y(X, Y, Z, W, M, N) = L_2(M^2 - XZ),
\]

(3.53)

\[
WM - XN = L_3(M^2 - XZ),
\]

(3.54)

\[
MN - ZW = L_4(M^2 - XZ),
\]

(3.55)

\[
WN - YM = L_5(M^2 - XZ),
\]

(3.56)

\[
N^2 - YZ = L_6(M^2 - XZ).
\]

(3.57)

From (3.51) and (3.57), it follows that

\[
N_0^2 - Y_0Z_0 = (\sqrt[3]{L_6}M_0)^2 - (L_6X_0)Z_0
\]

(3.58)

and thus

\[
(N_0 - \sqrt[3]{L_6}M_0)(N_0 + \sqrt[3]{L_6}M_0) = (Y_0 - L_6X_0)Z_0.
\]

(3.59)

Hence,

\[
N_0 = \begin{cases} 
-\sqrt[3]{L_6}M_0, & \text{or} \\
+\sqrt[3]{L_6}M_0
\end{cases}
\]

(3.60)

and

\[
Y_0 = L_6X_0.
\]

(3.61)
It follows from (3.51) and (3.60) that
\[
\frac{N_0}{M_0} = \left\{ \begin{array}{c}
-\frac{2\sqrt{L_6}M_0}{M_0} \\
+\frac{2\sqrt{L_6}M_0}{M_0}
\end{array} \right. \text{ or }
\]
implies that \( \sqrt{L_6} \) is a rational number, i.e., \( L_6 \) is a square of a rational number.

Let us choose \( X_1 \) and \( Z_1 \) to be any two nonzero rational numbers such that \( X_1Z_1 \) is a square of a rational number. Then it follows from (3.52)-(3.57) that there exists a nontrivial rational solution \((X_0, Y_0, Z_0, W_0, M_0, N_0)\) such that \( X_0 = X_1, Y_0 = L_6X_1, \) and \( Z_0 = Z_1. \) Thus \( X_0Y_0Z_0 \neq 0 \) as required.

Therefore, in either case, cubic form (3.2) has a nontrivial rational solution by Proposition 3.3, Proposition 3.5, Key Proposition, and Remark 3.4.

\[
\text{□}
\]

Remark 3.10. From the proof of the Key Proposition above, the Key Proposition also holds if system (3.34) is replaced by
\[
\begin{cases}
F_y(X, Y, Z, W, M, N) = 0 \\
F_z(X, Y, Z, W, M, N) = 0 \\
WM - XN = 0 \\
MN - ZW = 0 \\
WN - YM = 0 \\
W^2 - XY = 0 \\
M^2 - XZ = 0
\end{cases}
\]

or
\[
\begin{cases}
F_y(X, Y, Z, W, M, N) = 0 \\
F_z(X, Y, Z, W, M, N) = 0 \\
WM - XN = 0 \\
MN - ZW = 0 \\
WN - YM = 0 \\
W^2 - XY = 0 \\
N^2 - YZ = 0.
\end{cases}
\]

\[
\text{□}
\]

To continue with the proof of Theorem 2.1, let \( E \) be an elliptic curve over \( \mathbb{Q}. \) Let
\[
\mathcal{L} := \{ C \}
\]
be the collection of all equivalent classes of homogeneous spaces of \( E. \) Thus \( E \) is the Jacobian of each of these curves \( C. \) It is known that each \( C \) in \( \mathcal{L} \) can be represented as a smooth cubic plane curve \( F(x, y, z) = 0 \) with rational coefficients.

If none of these cubic forms \( F(x, y, z) = 0 \) can be written in the form
\[
F(x, y, z) = A_1x^3 + A_2y^3 + A_3z^3
\]
with \( A_1, A_2, A_3 \) rational numbers and \( A_1A_2A_3 \neq 0, \) then \( \text{III}(E) \) must be trivial by the Key Lemma above.
Thus let us suppose that at least one $C$ in $\mathcal{L}$ can be represented by a smooth cubic form $F(x, y, z) = 0$ of the form

$$F(x, y, z) = A_1 x^3 + A_2 y^3 + A_3 z^3$$  \hfill (3.64)

where $A_1, A_2,$ and $A_3$ are rational numbers with $A_1 A_2 A_3 \neq 0$. By multiplying both sides of (3.64) by an appropriate integer, we may assume that $A_1, A_2, A_3$ are cube free integers and $\gcd(A_1, A_2, A_3) = 1$.

**Proposition 3.11.** Let $C$ be an element of $\mathcal{L}$ such that $C$ can be written in the form (3.64). Then $E$ is birationally equivalent over $\mathbb{Q}$ to the following curve:

$$Y^2 = X^3 - 432(A_1 A_2 A_3)^2,$$  \hfill (3.65)

Proof. To establish this, we use a construction of Selmer ([19]). We consider the matrices

$$A = \begin{pmatrix} 0 & 0 & -9A_3 \\ 27A_3^3 \sqrt[3]{A_1} & -27A_3^3 \sqrt[3]{A_2} & 0 \\ \frac{3 \sqrt[3]{A_1}}{4} & \frac{3 \sqrt[3]{A_2}}{4} & 0 \end{pmatrix}$$  \hfill (3.66)

and

$$A^{-1} = \begin{pmatrix} 0 & \frac{1}{54A_3^2 \sqrt[3]{A_1}} & \frac{2}{3 \sqrt[3]{A_2}} \\ \frac{1}{54A_3 \sqrt[3]{A_1}} & 0 & \frac{3 \sqrt[3]{A_2}}{3 \sqrt[3]{A_2}} \\ \frac{9A_3}{54} & 0 & 0 \end{pmatrix}$$  \hfill (3.67)

which represent the maps

$$x = \frac{36A_3 Z + Y}{54 \sqrt[3]{A_1 A_2}}, \quad y = \frac{36A_3 Z - Y}{54 \sqrt[3]{A_1 A_2}}, \quad z = -\frac{X}{9A_3}$$  \hfill (3.68)

and

$$X = -9A_3 z, \quad Y = 27A_3 (\sqrt[3]{A_1} x - \sqrt[3]{A_2} y), \quad Z = \frac{2}{3} (\sqrt[3]{A_1} x + \sqrt[3]{A_2} y).$$  \hfill (3.69)

By an additional change of variable

$$x = \frac{X}{\sqrt[3]{A_1 A_2}}$$  \hfill (3.70)

together with a scaling of $x$ and $Y$, we have

$$Y^2 = X^3 - 432(A_1 A_2 A_3)^2.$$  \hfill (3.71)

Therefore the curve in (3.71) is the Jacobian of all the curves $C$ in $\mathcal{L}$ and thus is birationally equivalent to $E$ over $\mathbb{Q}$. \hfill \Box

It can be verified from (3.71) that there are finitely many distinct inequivalent cubic forms of the form (3.64) having the curve (3.71) as its Jacobian. Therefore, $E$ only has at most finitely many inequivalent homogenous spaces of the form (3.64). As a result, it follows that $\Sha(E)$ must have finite order. \hfill \Box

**Remark 3.12.** It can be seen from the proof of Theorem 2.1 that, for a given elliptic curve $E$ over $\mathbb{Q}$, the order of $\Sha(E)$ is in principle computable.
Proof. (Proof of Corollary 2.3)

In [8], T. Dokchitzer and V. Dokchitzer prove that the Parity Conjecture for an elliptic curve $E$ over $\mathbb{Q}$, namely
\[ r_{\text{anal}}(E) \equiv r_{W_M}(E) \pmod{2}, \]
follows from the finiteness of the Tate-Shafarevich group $\Sha(E)$. As a result, Theorem 2.1 implies the Parity Conjecture. Thus the first statement in the strong Birch and Swinnerton Conjecture,
\[ r_{\text{anal}}(E) = r_{W_M}(E), \]
is known modulo 2 for any elliptic curve $E$ over $\mathbb{Q}$. □

Proof. (Proof of Corollary 2.4)

Up to this point, all the quantities appearing in (1.2) are known to be computable completely except $|\Sha(E)|$ and $\text{Reg}(E)$.

- $\Omega(E)$ can be computed to any precision using the doubly exponential AGM algorithm.
- For each $p$, $c_p$ can be computed using Tate’s algorithm.
- The order of the group of torsion points $|E(\mathbb{Q})_{tor}|$ is computable.
- The regulator $\text{Reg}(E)$ can be computed to any desired precision if one knows generators for the Mordell group $E(\mathbb{Q})$.

With regard to the term $|\Sha(E)|$, Theorem 2.1 shows that $\Sha(E)$ is finite and the proof of Theorem 2.1 shows that $|\Sha(E)|$ is computable in principle. Now let us show that Theorem 2.1 guarantees that the standard process for producing generators of $E(\mathbb{Q})$ reaches its goal in a finite number of steps.

Let $h$ be the canonical height function on the Mordell group $E(\mathbb{Q})$. Let $n > 1$ be an integer and $\mathcal{E} = \{e_j\}$ be the set of representatives for the cosets of $nE(\mathbb{Q})$ in $E(\mathbb{Q})$. It is known that if there exists a positive integer $H$ such that $h(e_j) < H$ for all $j$, then $E(\mathbb{Q})$ is generated by the collection $\mathcal{E}$ of all points $\overline{e}$ of $E(\mathbb{Q})$ with $h(\overline{e}) < H$.

It is known that (3.72) implies $\mathcal{E}$ has finite order. Thus one needs $\mathcal{E}$ to be of finite order. Consider the exact sequence
\[ E(\mathbb{Q}) \xrightarrow{[n]} E(\mathbb{Q}) \xrightarrow{\delta} \text{Sel}^{[n]}(E) \xrightarrow{} \Sha_n(E) \]
where
- $\text{Sel}^{[n]}(E)$ is the $n$-Selmer group of $E$, which is a computable finite group.
- $\Sha_n(E)$ is the subgroup of $\Sha(E)$ of elements of order dividing $n$ for which there is not yet an effective method for computing.
- $[n]$ is the multiplication by $n$ map.

For each positive integer $l \geq 1$, there is a commutative diagram
\[ E(\mathbb{Q}) \xrightarrow{\delta} \text{Sel}^{[n]}(E) \xrightarrow{} \Sha_{n^l}(E) \xrightarrow{} 0 \]
\[ \downarrow [1] \quad \downarrow \gamma_n \quad \downarrow [n^{l-1}] \]
\[ E(\mathbb{Q}) \xrightarrow{\delta} \text{Sel}^{[n]}(E) \xrightarrow{} \Sha_{n^l}(E) \xrightarrow{} 0 \]
which leads to the following exact sequence

\[ E(\mathbb{Q})^{[n]} \to E(\mathbb{Q}) \xrightarrow{\delta} \text{Sel}_t^{[n]}(E) \to n^{l-1} \text{III}(E) \]  

(3.75)

where:

- \( \gamma_n \) denotes the \( n \)th-descent which is computable.
- \( \gamma_n(\text{Sel}^{[n]}(E)) = \text{Sel}_t^{[n]}(E) \).

The standard process for producing generators for \( E(\mathbb{Q}) \) is as follows: Let \( L_i(E) \) denote the subgroup of \( \text{Sel}^{[n]}(E) \) generated by all the elements \( \delta(e) \) where \( e \)'s are points on \( E(\mathbb{Q}) \) such that their \( x \) coordinates satisfy \( h(x) \leq i \). Next, compute:

1. \( \text{Sel}_t^{[1]}(E) \supset \text{Sel}_t^{[2]}(E) \supset \ldots \)
2. \( L_1(E) \subset L_2(E) \subset \ldots \)

If \( L_i(E) = \text{Sel}_t^{[n]} \) for some \( i \) and \( l \), then it follows that

\[ n^{l-1} \text{III}_{nl}(E) = 0 \]

and the points \( e \) with \( x \) coordinates satisfying \( h(x) \leq i \) generate \( E(\mathbb{Q})/nE(\mathbb{Q}) \). The corresponding generators for \( E(\mathbb{Q}) \) can thus be found. This process will not stop if \( \text{III}_{nl}(E) \) contains an infinitely divisible element. Theorem 2.1 guarantees that such an element does not exist and thus the above process must stop in a finite number of steps, producing generators for \( E(\mathbb{Q}) \).

Therefore, the term \( \epsilon_E \) in the strong Birch and Swinnerton-Dyer Conjecture can be computed, in principle, for any elliptic curve \( E \) over \( \mathbb{Q} \).

\[ \square \]

**Proof.** (Proof of Corollary 2.5)

This is outlined in [17]. The procedure can be stated briefly as follows: Let \( C \) be a genus 1 curve with rational coefficients and let \( \text{Jac}(C) \) be its Jacobian. Let

\[ \Phi : \text{III}(\text{Jac}(C)) \times \text{III}(\text{Jac}(C)) \to \mathbb{Q}/\mathbb{Z} \]

be the Cassels-Tate pairing. Then:

- If \( C(\mathbb{Q}_p) = \emptyset \) for some finite or infinite prime \( p \), then the Mordell-Weil group \( C(\mathbb{Q}) = \emptyset \).
- If the Mordell Weil group \( C(\mathbb{Q}) \neq \emptyset \), then a rational point can be found by searching.
- If \( C(\mathbb{Q}_p) \neq \emptyset \) for all finite and infinite primes \( p \) and the Mordell Weil group \( C(\mathbb{Q}) = \emptyset \), then \( C \) is a nontrivial element of \( \text{III}(\text{Jac}(C)) \). This can be proven, given that \( \text{III}(\text{Jac}(C)) \) is finite by Theorem 2.1, by finding another element \( C' \) of \( \text{III}(\text{Jac}(C)) \) such that

\[ \Phi(C, C') \]

is nontrivial in \( \mathbb{Q}/\mathbb{Z} \).

\[ \square \]

**References**

[1] B. Birch, P. Swinnerton-Dyer, *Notes on Elliptic Curves II*, J. Für Die Reine Und Angewandte Mathematik 218 (165), 79-108.

[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the Modularity of Elliptic Curves over \( \mathbb{Q} \): Wild 3-adic Exercices*, J. Amer. Math. Soc. 14 (201), 843-939.
[3] J. W. S. Cassels, *Arithmetic of Curves of Genus 1, IV. Proof of the Hauptvermutung*, J. Reine Angew Math. 211 (1962), 95-112.

[4] A. Ciperiani, A. Wiles, *Solvable Points on Genus One Curves*, Duke Math. J. 142 (2008), 381-464.

[5] J. Coates, A. Wiles, *On the Conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223-251.

[6] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, Cambridge 1992.

[7] H. Davenport, *Cubic Forms in 16 Variables*, Proceedings of the Royal Society A 272 (1350), 285-303.

[8] T. Dokchitser, V. Dokchitser, *Regulator Constants and the Parity Conjecture*, Invent. Math. 178, no. 1 (2009), 23-71.

[9] D.R. Heath Brown, *Cubic Forms in 14 Variables*, Invent. Math. 170, no.1 (2007), 199-230.

[10] C. Hooley, *On Nonary Cubic Forms*, J. Für Die Reine Und Angewandte Mathematik 386 (1988), 32-98.

[11] V. Kolyvagin, *Finiteness of E(Q) and SH(E, Q) for a Subclass of Weil Curves*, Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya, Vol. 53, no. 3 (1988), 522-540.

[12] S. Lang, J. Tate, *Principal Homogeneous Spaces over Abelian Varieties*, American Journal of Mathematics, Vol. 80, no. 3 (1958), 659-684.

[13] Y. Matiyasevich, *Hilbert’s Tenth Problem*, MIT Press, Massachusetts, 1993.

[14] B. Mazur, *Rational Isogenies of Prime Degree*, Invent. Math., Vol 4, no. 2 (1978), 129-162.

[15] L. Mordell, *On the Rational Solutions of the Indeterminate Equations of the Third and Fourth Degrees*, Proc. Cambridge Phil. Soc., Vol. 21 (1922-1923), 179-192.

[16] B. Poonen, *Cassels-Tate Pairing on Polarized Abelian Varieties*, Ann. of Math. (2) 150, no. 3, 1109-1149.

[17] B. Poonen, *Computing Rational Points on Curves*, Proceedings of the Millenial Conference on Number Theory, 21-26 May, University of Illinois at Urbana-Champaign.

[18] K. Rubin, *Tate-Shafarevich Groups and L-Functions of Elliptic Curves with Complex Multiplication*, Inventiones Mathematicae, Vol. 89, no. 3 (1989), 527-559.

[19] E. Selmer, *The Diophantine Equation ax^3 + by^3 + cz^3*, Acta Mathematica, Vol. 85, no. 1 (1951), 203-362.

[20] J. P. Serre, *A First Course in Arithmetic*, Graduate Texts in Mathematics 7 (1973), Berlin, New York: Springer Verlag.

[21] I. R. Shafarevich, *The Group of Principal Homogeneous Algebraic Manifolds*, Doklady Akademii Nauk SSSR., Vol. 124 (1959), 42-43.

[22] J. Tate, *On the Conjectures of Birch and Swinnerton-Dyer and a Geometric Analog*, Séminair Bourbaki, 18e année, 1965/66, no. 306.

[23] J. Tate, *The Arithmetic of Elliptic Curves*, Invent. Math. 23 (1974), 179-206.

Department of Mathematics
E-mail address: nguyenl@uwp.edu