On the Arithmetic of $x^3+y^3=nz^3$: Complex Multiplication and Asymptotic Distributions

Xuanlin Huang *

Department of Mathematics, Southern University of Science and Technology, Shenzhen, Guangdong Province, China

* Corresponding Author Email: 12413108@sustech.edu.cn

Abstract. This expository article reviews the arithmetic of the Fermat elliptic curve $x^3+y^3=nz^3$, which admits complex multiplication by the Eisenstein integers $\mathbb{Z}[\omega]$. We outline the computation of Frobenius traces over finite fields via cubic residue characters and Jacobi sums, explicitly linking local Diophantine data to the associated Grössencharakter over $\mathbb{Q}(\omega)$. Following Deuring's theorem, we detail the identification of the Hasse-Weil L-function with a Hecke L-function and review the standard formulation of the Birch and Swinnerton-Dyer conjecture. Finally, we present a linear-time lattice algorithm for computing the sequence of local traces and derive an asymptotic expansion for the mean number of affine solutions.

Keywords: Elliptic Curves, Complex Multiplication, Eisenstein Integers, Hecke Characters, Hasse-Weil L-functions, Birch and Swinnerton-Dyer Conjecture.

1. Introduction

For a cube-free integer n, the equation

$$x^3+y^3=nz^3$$

Defines a smooth projective cubic curve over $\mathbb{Q}$. Since it possesses the rational point $[1:-1:0]$ at infinity, it defines an elliptic curve E_n.

This curve admits complex multiplication by the ring of Eisenstein integers $\mathbb{Z}[\omega]$. In this expository note, we review the computation of local zeta functions, explicitly linking the trace of Frobenius to Jacobi sums. Passing to the global setting via Deuring's theory, we construct the Hasse-Weil L-function. As a natural extension of the Analytic Class Number Formula, we outline how the evaluation of the L-function's leading term at $s=1$ is governed by the Birch and Swinnerton-Dyer conjecture. Finally, we establish an asymptotic expansion for the sum of the number of local affine solutions and present a linear-time lattice algorithm to compute the sequence of Frobenius traces.

2. Algebraic Formulation and Complex Multiplication

Proposition 1. For any cube-free integer n, the Fermat curve C_n defined by [1]

$$x^3+y^3=nz^3$$

is birationally equivalent to the Weierstrass elliptic curve E_n given by

$$Y^2=X^3-432n^2.$$

Proof. The projective closure of C_n defines a smooth plane cubic, hence of genus one. It possesses the trivial $\mathbb{Q}$-rational point $O=[1:-1:0]$ at infinity. By the Riemann-Roch theorem, evaluating the complete linear system $|3O|$ yields an embedding into $\mathbb{P}^2$ corresponding precisely to the Weierstrass cubic form E_n. Explicitly, the birational equivalence over $\mathbb{Q}$ is realized on the affine patch $z=1$ by the rational map $\phi: C_n \longrightarrow E_n$,

$$\phi(x,y)=\left(\frac{12n}{x+y},\frac{36n(y-x)}{x+y}\right),$$

With the inverse rational map $\phi^{-1}:E_n\longrightarrow C_n$ given by

$$\phi^{-1}(X,Y)=\left(\frac{36n-Y}{6X},\frac{36n+Y}{6X}\right).$$

Routine algebraic substitution verifies that these maps are mutually inverse over their domains of definition.

Let $\omega=e^{2\pi i/3}$ be a primitive cubic root of unity. The map $[\omega]:(X,Y)\mapsto(\omega X,Y)$ preserves the Weierstrass equation and defines an automorphism of order 3 on E_n. Because this endomorphism is defined over $\mathbb{Q}(\omega)$ rather than $\mathbb{Q}$, the endomorphism ring $\mathrm{End}(E_n)$ over the algebraic closure strictly contains $\mathbb{Z}$. Consequently, $\mathrm{End}(E_n)$ is canonically isomorphic to the ring of Eisenstein integers $\mathbb{Z}[\omega]$[3]. The curve E_n therefore has complex multiplication by $\mathbb{Z}[\omega]$. This geometric structure dictates the local and global arithmetic of E_n via the class field theory of the imaginary quadratic field $\mathbb{Q}(\omega)$.

3. Local Point Counting and Trace of Frobenius

Let p be a prime of good reduction ($p\nmid n$). The trace of Frobenius is defined as $a_p=p+1-N_p$, where N_p denotes the total number of $\mathbb{F}_p$-rational points on the projective curve E_n. We define $F(n;p)$ as the number of affine solutions to the congruence

$$x^3+y^3\equiv n\pmod p.$$

Lemma 1. $p\equiv 2\pmod 3$, then E_n is supersingular at p, and $a_p=0$.

Proof. The map $x\mapsto x^3$ is an automorphism of $\mathbb{F}_p^\times$. For any chosen $x\in\mathbb{F}_p$, there exists a unique $y\in\mathbb{F}_p$ such that $y^3\equiv n-x^3\pmod p$. Summing over all x yields $F(n;p)=p$. The projective curve possesses a single rational point at infinity ($z=0$), yielding $N_p=p+1$, from which $a_p=0$ follows immediately.

Lemma 2. Let $p\equiv 1\pmod 3$ and let χ_3 be a non-trivial cubic character on $\mathbb{F}_p^\times$, extended by $\chi_3(0)=0$. The number of affine solutions is

$$F(n;p)=p-2-\overline{\chi_3}(n)\pi-\chi_3(n)\bar{\pi},$$

Where $\pi=-J(\chi_3,\chi_3)\in\mathbb{Z}[\omega]$ is uniquely determined by $\pi\bar{\pi}=p$ and the primary congruence $\pi\equiv 2\pmod 3$.

Proof. The number of solutions to $x^3\equiv u\pmod p$ is $1+\chi_3(u)+\overline{\chi_3}(u)$. The total number of affine solutions is the convolution:

$$F(n;p)=\sum_{u+v=n}(1+\chi_3(u)+\overline{\chi_3}(u))(1+\chi_3(v)+\overline{\chi_3}(v)).$$

Expanding this product, the trivial terms sum to p, and the linear character sums vanish. The mixed Jacobi sums evaluate to:

$$\sum_{u+v=n} \chi_3(u)\overline{\chi_3}(v) = \chi_3(n)\overline{\chi_3}(n)J(\chi_3,\overline{\chi_3}) = -1.$$

The pure character sums evaluate to:

$$\sum_{u+v=n} \chi_3(u)\chi_3(v) = \chi_3(n^2)\sum_{x+y=1} \chi_3(x)\chi_3(y) = \overline{\chi_3}(n)J(\chi_3,\chi_3).$$

Setting $\pi = -J(\chi_3,\chi_3)$ yields the explicit formula for $F(n;p)$, with the algebraic integer satisfying $\pi\overline{\pi} = p$. For $n=1$, the elementary congruence $F(1;p) \equiv 6 \pmod 9$ imposes the condition $\pi \equiv 2 \pmod 3$, which uniquely identifies π among its six associates in $\mathbb{Z}[\omega]$.

Proposition 2. For $p \equiv 1 \pmod 3$, the trace of Frobenius is strictly determined by $F(n;p)$ as

$$a_p = \overline{\chi_3}(n)\pi + \chi_3(n)\overline{\pi}.$$

Proof: The total nuber of projective points N_p is the sum of $F(n;p)$ and the points at infinity. For $p \equiv 1 \pmod 3$, the projective equation $x^3 + y^3 \equiv 0 \pmod p$ admits exactly 3 distinct solutions in $\mathrm{P}^1(\mathrm{F}_p)$ at $z=0$. Thus, $N_p = F(n;p) + 3 = p + 1 - \overline{\chi_3}(n)\pi - \chi_3(n)\overline{\pi}$, yielding the stated trace.

Remark. The prime $p \equiv 1 \pmod 3$ splits completely in $\mathbb{Z}[\omega]$ as $p = \pi\overline{\pi}$. The rigid constraint $\pi \equiv 2 \pmod 3$ coincides precisely with the conductor condition of the Hecke character of $\mathbb{Q}(\omega)$ attached to E_n. Consequently, as $p \to \infty$, the asymptotic distribution of the normalized traces $a_p/(2\sqrt{p})$ is strictly governed by the equidistribution of these Hecke characters, leading to a uniform angular distribution in $[0,\pi]$.

4. Hecke Characters and the Global L-function

Let $K = \mathbb{Q}(\omega)$ be the CM field of E_n, and let $\mathrm{O}_K = \mathbb{Z}[\omega]$ be its ring of integers. The arithmetic of E_n is intrinsically governed by a Hecke character (Grössencharakter) ψ of K.

Definition 3. Let $\mathfrak{f}$ be an integral ideal in O_K dividing $3n\mathrm{O}_K$. We define the Hecke character ψ of infinity type $(1,0)$ and conductor $\mathfrak{f}$ such that for any prime ideal $\mathfrak{p} = (\pi)$ coprime to $\mathfrak{f}$ with the primary generator $\pi \equiv 2 \pmod 3$, its evaluation is given by

$$\psi(\mathfrak{p}) = \overline{\chi_3}(n)\pi.$$

Theorem1(Deuring). The Hasse-Weil L-*functionof* E_n$ over $\mathbb{Q}$ coincides with the Hecke L-function of ψ over K. That is, up to the Euler factors at bad primes dividing $3n$.

$$L(E_n,s) = L(s,\psi).$$

Proof. We establish the identity by matching the local Euler factors of both L-function for all primes $p \not| 3n$. The Hasse-Weil L-function over $\mathbb{Q}$ has the local factor

$$L_p(E_n,s)^{-1} = 1 - a_p p^{-s} + p^{1-2s}.$$

The Hecke L-function over K is defined by the Euler product $L(s,\psi) = \prod_{\mathfrak{p}} (1 - \psi(\mathfrak{p})N(\mathfrak{p})^{-s})^{-1}$.

Case 1: $p \equiv 1 \pmod 3$. The prime p splits completely in O_K as $p\mathrm{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Let $\mathfrak{p} = (\pi)$ where $\pi \equiv 2 \pmod 3$. The norm is $N(\mathfrak{p}) = N(\overline{\mathfrak{p}}) = p$. The corresponding Euler factor in $L(s,\psi)$ is the product of the contributions from $\mathfrak{p}$ and $\overline{\mathfrak{p}}$:

$$\left(1-\psi(\mathfrak{p})p^{-s}\right)\left(1-\psi(\bar{\mathfrak{p}})p^{-s}\right)=1-(\psi(\mathfrak{p})+\psi(\bar{\mathfrak{p}}))p^{-s}+\psi(\mathfrak{p})\psi(\bar{\mathfrak{p}})p^{-2s}.$$

By Definition 3, $\psi(\mathfrak{p})=\overline{\chi_3}(n)\pi$ and $\psi(\bar{\mathfrak{p}})=\chi_3(n)\bar{\pi}$. Applying Proposition 2, we obtain

$$\psi(\mathfrak{p})+\psi(\bar{\mathfrak{p}})=\overline{\chi_3}(n)\pi+\chi_3(n)\bar{\pi}=a_p.$$

Furthermore, $\psi(\mathfrak{p})\psi(\bar{\mathfrak{p}})=\chi_3(n)\overline{\chi_3}(n)\pi\bar{\pi}=p$. Substituting these into the expansion yields exactly $1-a_p p^{-s}+p^{1-2s}$, matching $L_p(E_n,s)^{-1}$.

Case 2: $p\equiv 2 \pmod 3$. The prime p is inert in $\mathcal{O}_K$. Thus, $\mathfrak{p}=p\mathcal{O}_K$ is a prime ideal with norm $N(\mathfrak{p})=p^2$. The correct primary generator is simply p itself, since $p\equiv 2 \pmod 3$. By the theory of Hecke characters for inert primes, $\psi(p\mathcal{O}_K)=-p$. The Hecke Euler factor is:

$$1-\psi(p\mathcal{O}_K)N(p\mathcal{O}_K)^{-s}=1-(-p)p^{-2s}=1+p^{1-2s}.$$

By Lemma 1, E_n is supersingular at p, yielding $a_p=0$. The Hasse-Weil local factor evaluates to $1-0\cdot p^{-s}+p^{1-2s}=1+p^{1-2s}$. The factors match precisely.

Remark. The rigid constraint $\pi\equiv 2 \pmod 3$ utilized in the local point counting is not an ad hoc choice. It is the fundamental primary condition in $\mathbb{Q}[\omega]$ that ensures the map $\mathfrak{p}\mapsto\overline{\chi_3}(n)\pi$ is a well-defined character on the ideal group modulo the conductor $\mathfrak{f}$, seamlessly linking the local Diophantine geometry to the global analytic theory of Hecke L-functions.

5. Analytic Continuation and the Birch and Swinnerton-Dyer Conjecture

By Deuring's theorem, the Hasse-Weil L-function $L(E_n,s)$, initially defined by an Euler product for $\mathrm{Re}(s)>\frac{3}{2}$, is identified with the Hecke L-function $L(s,\psi)$ over $K=\mathbb{Q}(\omega)$. Because ψ is a Grössencharakter of infinity type $(1,0)$, Hecke's classical theory guarantees that $L(E_n,s)$ admits an analytic continuation to the entire complex plane $\mathbb{C}$.

Defining the completed L-function as

$$\Lambda(E_n,s)=N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E_n,s),$$

Where N_E is the arithmetic conductor of E_n, it satisfies the functional equation

$$\Lambda(E_n,s)=W(E_n)\Lambda(E_n,2-s),$$

With the root number $W(E_n)\in\{\pm 1\}$. The analytic continuation allows the evaluation of the L-function at the central critical point $s=1$.

Conjecture (Birch and Swinnerton-Dyer). The Taylor expansion of $L(E_n,s)$ at $s=1$ takes the form

$$L(E_n,s)=c(s-1)^r+O\left((s-1)^{r+1}\right),$$

Where $c\neq 0$ and $r=\mathrm{rank}_{\mathbb{Q}}E_n(\mathbb{Q})$. Furthermore, the parity of the algebraic rank is determined by the root number, satisfying $(-1)^r=W(E_n)$.

Remark. The formulation of the leading coefficient c encodes essential arithmetic invariants of E_n, including the order of the Tate-Shafarevich group, the real period, and the regulator. In this

precise sense, the Birch and Swinnerton-Dyer conjecture serves as the systematic, higher-dimensional generalization of the Analytic Class Number Formula, lifting the analytic determination of class numbers from number fields to the realm of elliptic curves [4].

6. Asymptotic Computation of Frobenius Traces

The evaluation of the L-function and the formulation of the Birch and Swinnerton-Dyer conjecture require the sequence of Frobenius traces $\{a_p\}$ for primes $p \le X$.

For $p \equiv 2 \pmod 3$, $a_p = 0$. For $p \equiv 1 \pmod 3$, we established that $a_p = \overline{\chi_3}(n)\pi + \chi_3(n)\overline{\pi}$, where $\pi \in \mathbb{Z}[\omega]$ satisfies $\pi\overline{\pi} = p$ and $\pi \equiv 2 \pmod 3$. Writing $\pi = a + b\omega$ with $a, b \in \mathbb{Z}$, the norm condition implies the quadratic form $a^2 - ab + b^2 = p$. The primary congruence $\pi \equiv 2 \pmod 3$ imposes the strict constraints $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$.

Proposition 3. The sequence of traces $\{a_p\}_{p \le X}$ can be computed in $O(X)$ operations.

Proof. A naive trial division to find the representation $p = a^2 - ab + b^2$ requires $O(\sqrt{p})$ operations per prime. By the Prime Number Theorem, evaluating all primes up to X demands $O(X^{3/2} / \log X)$ operations.

To achieve linear complexity, we iterate over lattice points in the domain of the quadratic form. Consider the set of pairs $(a, b) \in \mathbb{Z}^2$ bounded by the ellipse

$$a^2 - ab + b^2 \le X.$$

The area of the fundamental ellipse $x^2 - xy + y^2 \le X$ in $\mathbb{R}^2$ is $\frac{2\pi}{\sqrt{3}} X$. The congruence conditions restrict (a, b) to a shifted sublattice of index 9 in $\mathbb{Z}^2$. Consequently, the algorithm asymptotically evaluates $\frac{2\pi}{9\sqrt{3}} X$ pairs. For each pair, we compute the norm $N(\pi) = a^2 - ab + b^2$. A linear prime sieve up to X identifies the prime norms in $O(X)$ time. For valid prime norms, the pair uniquely yields π, enabling the direct evaluation of a_p. This geometric approach eliminates redundant trial factorizations, yielding a global linear time complexity.

Proposition 4. Let $F(1; p)$ denote the number of affine solutions to $x^3 + y^3 \equiv 1 \pmod p$. As $N \to \infty$, the sum of $F(1; p)$ over primes $p \le N$ admits the asymptotic expansion

$$\sum_{p \le N} F(1; p) = \frac{N^2}{2 \log N} + \frac{N^2}{4 \log^2 N} + O\left(\frac{N^2}{\log^3 N} \right).$$

Proof. We decompose the sum according to the residue classes modulo 3. For $p = 3$, $F(1; 3) = 3$. For $p > 3$,

$$\sum_{p \le N} F(1; p) = 3 + \sum_{\substack{p \le N \\ p \equiv 2 \pmod 3}} p + \sum_{\substack{p \le N \\ p \equiv 1 \pmod 3}} (p - 2 - a_p) = \sum_{p \le N} p - \sum_{\substack{p \le N \\ p \equiv 1 \pmod 3}} 2 - \sum_{\substack{p \le N \\ p \equiv 1 \pmod 3}} a_p.$$

We evaluate the main term strictly via Abel's summation formula[2]. Let $\pi(x)$ denote the prime counting function. Then

$$\sum_{p \le N} p = N\pi(N) - \int_2^N \pi(t) \mathrm{d}t.$$

Inserting the Prime Number Theorem expansion $\pi(x)=\frac{x}{\log x}+\frac{x}{\log^2 x}+O\left(\frac{x}{\log^3 x}\right)$, the boundary term evaluates to $N\pi(N)=\frac{N^2}{\log N}+\frac{N^2}{\log^2 N}+O\left(\frac{N^2}{\log^3 N}\right)$. The integral evaluates to

$$\int_2^N \pi(t)\mathrm{d}t=\int_2^N\left(\frac{t}{\log t}+\frac{t}{\log^2 t}\right)\mathrm{d}t+O\left(\frac{N^2}{\log^3 N}\right)=\frac{N^2}{2\log N}+\frac{3N^2}{4\log^2 N}+O\left(\frac{N^2}{\log^3 N}\right).\$$

Subtracting the integral from $N\pi(N)$ yields the main term expansion $\frac{N^2}{2\log N}+\frac{N^2}{4\log^2 N}+O\left(\frac{N^2}{\log^3 N}\right)$.

By the Prime Number Theorem for arithmetic progressions, the constant summation term is $O(N/\log N)$. For the trace summation, the Hasse bound $|a_p|\le 2\sqrt{p}$ furnishes the trivial upper bound [5]

$$\left|\sum_{\substack{p\le N\\ p\equiv 1 \pmod 3}} a_p\right|\le \sum_{p\le N} 2\sqrt{p}=O\left(\frac{N^{3/2}}{\log N}\right).$$

Because both $O(N/\log N)$ and $O(N^{3/2}/\log N)$ are strictly absorbed by $O(N^2/\log^3 N)$, the lower-order terms do not affect the main asymptotic expansion.

7. Conclusion

The arithmetic of the Fermat elliptic curve

$$x^3+y^3=nz^3$$

is fundamentally governed by its complex multiplication by the Eisenstein integers $\mathbb{Z}[\omega]$. Local point counting over finite fields is completely determined by the evaluation of Hecke characters, demonstrating that elementary Diophantine congruence conditions arise as direct consequences of class field theory over $\mathbb{Q}(\omega)$.

Passing to the global setting, this local data assembles into the Hasse-Weil L-function. The geometric symmetry of the curve guarantees the analytic continuation of the L-function via Deuring's theorem. This provides the exact analytic framework required to formulate the Birch and Swinnerton-Dyer conjecture, connecting the central L-value to the rank of the Mordell-Weil group.

Finally, the asymptotic distribution of the Frobenius traces reflects the equidistribution of Grössencharakters, yielding a limiting measure with both discrete and continuous components. The synthesis of these local, global, and asymptotic behaviors illustrates how the algebraic structure of complex multiplication rigidly dictates the analytic properties of the curve.

References

[1] Joseph H Silverman. The arithmetic of elliptic curves. Vol. 106. 2. Springer, 2009.

[2] Tom M Apostol. Introduction to analytic number theory. Springer Science & Business Media,2013.

[3] Joseph H Silverman. Advanced topics in the arithmetic of elliptic curves. Springer Science &BusinessMedia,2013.

[4] Chebolu K S, Merzel L J, Mináč J, et al. On the arithmetic of join rings over finite fields[J].Journal of Algebra,2026,700185-212.

[5] Hasson R E. Adding It Up: Arithmetic shortcuts predict future STEM performance. [J]. Scientific American,2026,334(4):20.