SYLVESTER'S PROBLEM AND MOCK HEEGNER POINTS

SAMIT DASGUPTA AND JOHN VOIGHT

Abstract. We prove that if $p \equiv 4, 7 \pmod 9$ is prime and 3 is not a cube modulo p, then both of the equations $x^3 + y^3 = p$ and $x^3 + y^3 = p^2$ have a solution with $x, y \in \mathbb{Q}$.

1. Introduction

1.1. **Motivation.** We begin with the classical Diophantine question: which integers n can be written as the sum of two cubes of rational numbers? More precisely, let $n \in \mathbb{Z}_{>0}$ be cubefree, and let E_n denote the projective plane curve defined by the equation $x^3 + y^3 = nz^3$. Equipped with the point $\infty = (1 : -1 : 0)$, the curve E_n has the structure of an elliptic curve over $\mathbb{Q}$. (The equation for E_n can be transformed via a change of variables to yield the Weierstrass equation $y^2 = x^3 - 432n^2$.) We have $E_1(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ generated by $(1 : 0 : 1)$ and $E_2(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ generated by $(1 : 1 : 1)$; otherwise, $E_n(\mathbb{Q})_{\mathrm{tors}} = \{\infty\}$ for $n \geq 3$. So our question becomes: for which cubefree integers $n \geq 3$ is $\operatorname{rk} E_n(\mathbb{Q}) > 0$?

A conjecture, attributed to Sylvester, suggests an answer to this question when $n = p$ is prime.

Conjecture 1.1.1 (Sylvester [16], Selmer [13]). *If* $p \equiv 4, 7, 8 \pmod 9$, *then* $\operatorname{rk} E_p(\mathbb{Q}) > 0$.

An explicit 3-descent [11] shows that

$$\operatorname{rk} E_p(\mathbb{Q}) \leq \begin{cases} 0, & \text{if } p \equiv 2, 5 \pmod 9; \\ 1, & \text{if } p \equiv 4, 7, 8 \pmod 9; \\ 2, & \text{if } p \equiv 1 \pmod 9. \end{cases} \tag{1.1.2}$$

In particular, primes $p \equiv 2, 5 \pmod 9$ are *not* the sum of two cubes, a statement that can be traced back to Pépin, Lucas, and Sylvester [16, Section 2, Title 1].

At the same time, the sign of the functional equation for the L-series of E_p is

$$\operatorname{sign}(L(E_p/\mathbb{Q}, s)) = \begin{cases} -1, & \text{if } p \equiv 4, 7, 8 \pmod 9; \\ +1, & \text{otherwise.} \end{cases} \tag{1.1.3}$$

Putting these together, for $p \equiv 1 \pmod 9$, the Birch–Swinnerton-Dyer (BSD) conjecture predicts that $\operatorname{rk} E_p(\mathbb{Q}) = 0$ or 2, depending on p in a nontrivial way. This case was investigated by Rodriguez-Villegas and Zagier [10]: they give three methods to determine for a given prime p whether or not $\operatorname{rk} E_p(\mathbb{Q}) = 0$.

1.2. **Main result.** We are left to consider the cases $p \equiv 4, 7, 8 \pmod 9$. The BSD conjecture together with (1.1.2) and (1.1.3) then predicts that $\operatorname{rk} E_p(\mathbb{Q}) = 1$, and hence that p is the sum of two cubes. In this article, we prove the following (unconditional) result as progress towards Sylvester's conjecture.

Theorem 1.2.1. *Let* $p \equiv 4, 7 \pmod 9$ *be prime and suppose that* 3 *is not a cube modulo* p. *Then* $\operatorname{rk} E_p(\mathbb{Q}) = \operatorname{rk} E_{p^2}(\mathbb{Q}) = 1$.

Date: September 5, 2018.

2010 *Mathematics Subject Classification.* 11D25, 11G05, 11G40, 11G15.

In 1994, Elkies [4] announced a proof of the stronger statement that the conclusion of Theorem 1.2.1 holds for *all* $p \equiv 4, 7 \pmod 9$. The details of the proof have not been published, but his methods differ substantially from ours [5].

Theorem 1.2.1 was announced and the proof sketched in earlier work [3], but several important details were not provided and are finally given here. The construction in this paper has been recently used by Shu–Yin [14] to prove that the power of 3 dividing $\#Ш(E_p)\#Ш(E_{3p^2})$ is as predicted by the BSD conjecture, following a method similar to the work of Cai–Shu–Tian [1]. (See also section 1.4 below.) We are not aware of any results concerning the case $p \equiv 8 \pmod 9$ of Conjecture 1.1.1, which appears to be decidedly more difficult.

1.3. **Sketch of the proof.** We now discuss the proof of Theorem 1.2.1. General philosophy predicts that in the situation where the curve E_p has expected rank 1, one should be able to construct rational nontorsion points on E_p using the theory of complex multiplication (CM). One might first consider the classical method of Heegner points. We start with the modular parameterization $\Phi : X_0(N) \to E_p$, where N is the conductor of E_p, given by

$$N = \begin{cases} 27p^2, & \text{if } p \equiv 4 \pmod 9, \\ 9p^2, & \text{if } p \equiv 7 \pmod 9. \end{cases}$$

Given a quadratic imaginary field K that satisfies the *Heegner hypothesis* that both 3 and p are split, we may define a cyclic N-isogeny that yields a point $P \in X_0(N)(H)$, where H denotes the Hilbert class field of K. The trace $Y = \operatorname{Tr}_{H/K} \Phi(P)$ yields a point on $E_p(K)$. By the Gross-Zagier formula [6], we expect this point to be nontorsion. Indeed, the BSD conjecture (which in particular furnishes an equality of the algebraic and analytic ranks of E_p) implies that this is the case. But in order to apply this method, we must first choose a suitable imaginary quadratic field K, and no natural candidate for K presents itself; after making such a choice, it is unclear how to prove unconditionally that the resulting Heegner points are nontorsion.

Instead, in this article we work with what are known as *mock Heegner points*. This terminology is due to Monsky [8, p. 46], although arguably Heegner's original construction may be described as an example of such "mock" Heegner points. We consider the field $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$, where $\omega = \exp(2\pi i/3)$ is a primitive cube root of unity. Note that the elliptic curve E_n has CM by the ring of integers $\mathbb{Z}_K = \mathbb{Z}[\omega]$, and that the prime 3 is ramified in K, so the Heegner hypothesis is not satisfied. Nevertheless, Heegner-like constructions of points defined by CM theory may still produce nontorsion points in certain situations: for example, one can show that results of Satgé [11] concerning the curve $x^3 + y^3 = 2p$ can be described in the framework of mock Heegner points [3].

We take instead a fixed modular parametrization $X_0(243) \to E_9$. We consider an explicit cyclic 243-isogeny of conductor $9p$ which under this parameterization yields a point $P \in E_9(H_{9p})$, where H_{9p} denotes the ring class field of K associated to the conductor $9p$. We descend the point $P \in E_9(H_{9p})$ with a twist by $\sqrt[3]{3}$ to a point $Q \in E_1(H_{3p})$. This descent argument is particularly appealing and non-standard because it compares the action of the exotic modular automorphism group of $X_0(243)$ as studied by Ogg [9] to the Galois action on CM points provided by the Shimura Reciprocity Law.

We next consider the trace $R = \operatorname{Tr}_{H_{3p}/L} Q \in E_1(L)$, where $L = K(\sqrt[3]{p})$. We show that after translating by an explicit torsion point, R twists to yield a point $Z \in E_p(K)$ or $Z \in E_{p^2}(K)$, depending on the original choice of 243-isogeny. Again this argument employs the group of exotic modular automorphisms of $X_0(243)$.

We conclude by showing that the point R (hence Z) is nontorsion when 3 is not a cube modulo p, and this implies the theorem since $\operatorname{rk}_{\mathbb{Z}} E_n(\mathbb{Q}) = \operatorname{rk}_{\mathbb{Z}_K} E_n(K)$. To do this we consider the reduction of R modulo the primes above p. By an explicit computation with η-products, we show that when 3 is not a cube modulo p, this reduction is not the image of any torsion point in $E_1(L)$:

see Proposition 5.2.8. This reduction uses in a crucial way a generalization and refinement of Kronecker's congruence: see Proposition 5.2.1. In the end, we are able to show that when 3 is not a cube modulo p, the point R is nontorsion because it is not congruent to any torsion point modulo p. Without the descent made possible by the exotic modular automorphism group of $X_0(243)$, our point Z (e.g., which could have been defined more simply by taking an appropriate "twisted" trace of P from H_{9p} to K) would have been twice multiplied by 3, and the delicate proof that it is nontorsion would have fallen through.

1.4. **Heuristics and the work of Shu and Yin.** We now explain why it should be expected that the condition "3 is not a cube modulo p" should appear in the statement of Theorem 1.2.1 for our construction. As mentioned above, our setting does not satisfy the Heegner hypothesis and hence the classical Gross–Zagier formula does not apply in this case. Nevertheless, Shu and Yin have proven the following result.

Theorem 1.4.1 ([14, Theorem 4.4]). *Let $p \equiv 4, 7 \pmod{9}$ be prime. Let $\chi_{3p} : \mathrm{Gal}(H_{3p} \,|\, K) \to \mu_3$ be the cubic character associated to the field $K(\sqrt[3]{3p})$, i.e.,*

$$\chi(\sigma) = \sigma\big(\sqrt[3]{3p}\big)/\sqrt[3]{3p} \quad \textit{for } \sigma \in \mathrm{Gal}(H_{3p} \,|\, K).$$

Let $Z \in E_p(K)$ be the mock Heegner point constructed above. Then

$$\frac{L'(E_9/K, \chi_{3p}, 1)}{\Omega} = c \cdot \mathrm{ht}(Z),$$

where the complex period $\Omega \in \mathbb{C}^\times$ and the rational factor $c \in \mathbb{Q}^\times$ are explicitly given.

The Artin formalism for L-functions yields

$$L(E_9/K, \chi_{3p}, s) = L(E_p/\mathbb{Q}, s) L(E_{3p^2}/\mathbb{Q}, s),$$

and hence Theorem 1.4.1 relates $\mathrm{ht}(Z)$ to

$$L'(E_p/\mathbb{Q}, 1) L(E_{3p^2}/\mathbb{Q}, 1). \tag{1.4.2}$$

Therefore we should expect that Z is nontorsion if and only if $L(E_{3p^2}/\mathbb{Q}, 1) \neq 0$. In fact, it is possible to have $L(E_{3p^2}/\mathbb{Q}, 1) = 0$ (e.g., $p = 61, 193$), and in such cases our point $Z \in E_p(K)$ is torsion.

However, whenever 3 is not a cube modulo p, one can show that the Selmer group associated to a certain rational 3-isogeny to E_{3p^2} is trivial (see Satgé [11, Theorem 2.9(3) and p. 313]) and consequently that $E_{3p^2}(\mathbb{Q})$ is finite and hence by BSD that $L(E_{3p^2}/\mathbb{Q}, 1) \neq 0$. This explains why it is reasonable to expect this condition to appear in the statement of Theorem 1.2.1. The appeal of Theorem 1.2.1 is that it is explicit and unconditional—i.e., it does not depend on BSD, even though BSD and the theorem of Shu–Yin explain *why* the condition on 3 modulo p should be expected to appear in the statement.

1.5. **Organization.** In §2 we describe our explicit modular parameterization and the group of modular automorphims of $X_0(243)$. In §3 we define our mock Heegner points, and in §4 we descend and trace them to define points over K. In §5, we prove that our points are nontorsion when 3 is not a cube modulo p.

1.6. **Acknowledgements.** The authors wish to thank Brian Conrad, Henri Darmon, and Noam Elkies for helpful discussions as well as the hospitality of the Centre Recherche de Mathématiques (CRM) in Montréal where part of this work was undertaken in December 2005. The authors would also like to thank Hongbo Yin for comments and the encouragement to publish this work.

2. The modular curve $X_0(243)$

Throughout, let $K := \mathbb{Q}(\omega) \subset \mathbb{C}$ where $\omega := (-1+\sqrt{-3})/2$ is in the upper half-plane and $\mathbb{Z}_K := \mathbb{Z}[\omega]$ its ring of integers. We begin in this section by setting up a few facts about the modular curve $X_0(243)$.

2.1. **Basic facts.** The (smooth, projective, geometrically integral) curve $X_0(243)$ over $\mathbb{Q}$ is the coarse moduli space for cyclic 243-isogenies between (generalized) elliptic curves, and there is an isomorphism of Riemann surfaces

$$X_0(243)(\mathbb{C}) \xrightarrow{\sim} \Gamma_0(243)\backslash\mathfrak{H}^*$$

where $\mathfrak{H}^* := \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ is the completed upper half-plane. Explicitly, to $\tau \in \mathfrak{H}$ we associate the cyclic isogeny

$$\begin{aligned} \phi_\tau \colon \mathbb{C}/\langle 1,\tau\rangle &\to \mathbb{C}/\langle 1, 243\tau\rangle \\ z &\mapsto 243z \end{aligned} \tag{2.1.1}$$

with $\ker\phi_\tau$ generated by $1/243$ in the lattice $\mathbb{Z}+\mathbb{Z}\tau$. The genus of $X_0(243)$ is 19.

For further reading on automorphism groups of modular curves, we refer to Ogg [9]. The group of modular automorphisms of $X_0(243)$ is by definition

$$\mathrm{MAut}(X_0(243)) := N_{\mathrm{PGL}_2^+(\mathbb{Q})}(\Gamma_0(243))/\Gamma_0(243)$$

where N denotes the normalizer. The group $\mathrm{MAut}(X_0(243))$ is generated by an *exotic* automorphism $v := \begin{pmatrix} 1 & 0 \\ 81 & 1 \end{pmatrix} \in \mathrm{MAut}(X_0(243))$ of order 3 and the Atkin–Lehner involution $w := \begin{pmatrix} 0 & -1 \\ 243 & 0 \end{pmatrix} \in \mathrm{MAut}(X_0(243))$ of order 2. We find

$$\mathrm{MAut}(X_0(243)) = \langle w, v^{-1}wv\rangle \rtimes \langle v\rangle \simeq S_3 \rtimes \mathbb{Z}/3\mathbb{Z}.$$

The subgroup of $\mathrm{MAut}(X_0(243))$ isomorphic to S_3 is characteristic, and we let $\Gamma \le \mathrm{PGL}_2^+(\mathbb{Q})$ be the subgroup generated by $\Gamma_0(243)$ and S_3. One can check that v normalizes Γ. Moreover, the matrix $t := \begin{pmatrix} 9 & 1 \\ -243 & -18 \end{pmatrix}$ normalizes the group $\mathrm{MAut}(X_0(243))$ and the group Γ. (But t does not normalize $\Gamma_0(243)$ itself.) One can check that $t^3 = 729$ is scalar, so t has order 3 as a linear fractional transformation.

2.2. **Explicit modular parametrization and modular automorphisms.** We now consider the quotient of $X_0(243)$ by the subgroup $S_3 < \mathrm{MAut}(X_0(243))$

$$X_0(243) \to X_0(243)/S_3 = X(\Gamma) \tag{2.2.1}$$

where $X(\Gamma) := \Gamma\backslash\mathfrak{H}^*$. Riemann–Hurwitz shows that the genus of $X(\Gamma)$ is 1, and the image of the cusp $\infty \in X_0(243)(\mathbb{Q})$ gives it the structure of an elliptic curve over $\mathbb{Q}$. This quotient morphism (2.2.1) is defined over $\mathbb{Q}$ and has a particularly pleasing realization as follows. Let

$$\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n) \tag{2.2.2}$$

with $q := \exp(2\pi i z)$ be the Dedekind η-function.

Proposition 2.2.3. *We have a modular parametrization*

$$\begin{aligned} \Phi\colon X_0(243) \to X(\Gamma) &\xrightarrow{\sim} E_9\colon y^2+y = x^3-1 \\ z &\mapsto (x,y) \end{aligned}$$

where

$$x(z) = \frac{\eta(9z)\eta(27z)}{\eta(3z)\eta(81z)}, \quad y(z) = -\frac{\eta(9z)^4 + 9\eta(9z)\eta(81z)^3}{\eta(27z)^4 - 3\eta(9z)\eta(81z)^3} - 2. \tag{2.2.4}$$

Proof. The η-product $x(z)$ is a modular function on $X_0(243)$ by Ligozat's criterion [7, Theorem 2]. By the transformation properties of the η-function, it is straightforward to show that $x(z)$ is invariant under the action of the subgroup $S_3 < \mathrm{MAut}(X_0(243))$.

The function $y(z)$ was discovered on a computer experimentally by manipulating η-products via their q-expansions. In a similar way, one can show that y is invariant under $\Gamma_0(243)$ and the subgroup $S_3 < \mathrm{MAut}(X_0(243))$. To prove that the equality $y^2 + y = x^3 - 1$ holds, after clearing denominators we may equivalently show an equality of holomorphic modular forms of weight 7—but then it suffices to verify the equality on enough terms of the q-expansions on a computer to satisfy the Hecke bound. □

Remark 2.2.5. The elliptic curve E_9 of conductor 243 is number `243a1` in the tables of Cremona and has LMFDB label 243.a1.

Remark 2.2.6. One can show that the y-function in (2.2.4) cannot be expressed simply as an η-product, moreover there is no η-product that is invariant under S_3 and has a pole of order 3 at the preimage of the origin in E_9. We do not use the explicit formula for $y(z)$ in this paper.

Because the matrices t, v normalize Γ, they give rise to automorphisms of E_9 as a genus 1 curve. The endomorphism ring of E_9 as an elliptic curve is $\mathbb{Z}_K = \mathbb{Z}[\omega]$, where ω acts via $(x, y) \mapsto (\omega x, y)$. Every endomorphism of E_9 as a genus 1 curve has the form $Z \mapsto aZ + b$ where $a \in \mathbb{Z}_K$ and $b \in E_9$. The following proposition describes the automorphisms t and v of E_9 explicitly in these terms.

Proposition 2.2.7. *The automorphism t acts on the curve E_9 via $t(Z) = \omega^2 Z + (0, \omega)$. The automorphism v acts by $v(Z) = \omega^2(Z)$.*

Proof. Since t^3 is a scalar matrix, $t(Z) = aZ + b$ for $a \in \{1, \omega, \omega^2\}$ and $b \in E_9(\overline{\mathbb{Q}})$. Now $t(\infty) = -1/27$ and under the complex parametrization Φ we compute that $\Phi(-1/27) = (0, \omega) = b$. Unfortunately, we cannot determine a by looking at cusps. Instead, we consider $\tau = (\omega - 1)/27 \in \mathfrak{H}$, which has the property that $t(\tau) = \tau$. Letting $T = \Phi(\tau)$, it follows that $(1 - a)T = b = (0, \omega)$. In particular $T \in E_9[3]$. We compute numerically that $T \approx (\sqrt[3]{3}, -2)$, and since there are only 9 possibilities for T, equality holds. From this, one finds that $a = \omega^2$, and hence $t(Z) = \omega^2 Z + (0, \omega)$.

Next we compute the action of v, which also has order dividing 3, so again $v(Z) = aZ + b$ with $a \in \{1, \omega, \omega^2\}$. We see that $v(\infty) = 1/81$ and $\Phi(1/81) = \infty$ so $b = 0$. As above, we compute that $\tau = (\omega - 1)/27$ has $\Phi(\tau) = T = (\sqrt[3]{3}, -2)$ is a 3-torsion point, hence $\Phi(v(\tau)) = a(\sqrt[3]{3}, -2)$ is also a 3-torsion point and then we verify numerically that $a = \omega^2$. □

3. Mock Heegner points

For the remainder of this paper, let p be a prime congruent to 4 or 7 modulo 9. In this section, we define our mock Heegner point.

3.1. **The isogeny tree.** In Figure 3.1 below, we draw a diagram of 3-isogenies between certain elliptic curves with CM by orders in K. For $\tau \in K \cap \mathfrak{H}$, we denote by $\langle \tau \rangle_f$ the elliptic curve $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ with endomorphism ring the order $\mathbb{Z}_{K,f} := \mathbb{Z}[f\omega]$ of conductor (or index) f in $\mathbb{Z}_K$.

The computation of the conductors in Figure 3.1 relies only on the fact that $p \equiv 1 \pmod 3$. Of particular interest in this diagram is the fact that the curves in the lower right quadrant emanating from the "central vertex" $\langle \omega p \rangle_p$ have endomorphism ring of lower conductor than their counterparts in the other quadrants. We have only listed the 9 curves in the tree of distance 3 from this central vertex in this quadrant for space reasons, since these are the only curves that we will use.

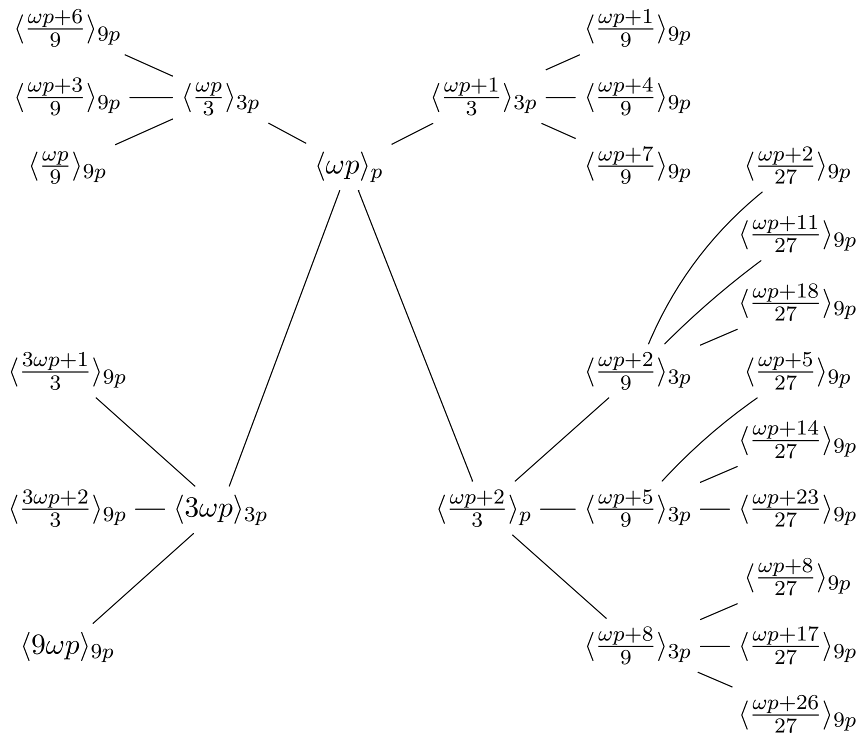

Figure 3.1: Isogeny tree (for $p \equiv 1 \pmod 3$)

Each path of length 5 in this tree (with no backtracking) corresponds to a cyclic 3^5-isogeny and hence yields a corresponding point on $X_0(243)$. Furthermore, the conductor of the order associated to this cyclic 243-isogeny will be the least common multiple of the conductors of the orders of the two curves involved in the isogeny. In particular, for each curve $\langle\tau\rangle_{9p}$ on the left side of this diagram and each $\langle\frac{\omega p+i}{27}\rangle_{9p}$ with $i \equiv -1 \pmod 3$ on the right, there is a point on $X_0(243)(\mathbb{C})$ of conductor $9p$ corresponding to the isogeny between these two curves.

3.2. **Our mock Heegner points.** Recall that our eventual goal is to produce rational points on the curves E_p and E_{p^2}; we refer to these as *case* 1 and *case* 2, and we will eventually show that our points land on the curve E_p or E_{p^2}, accordingly. Our construction starts with the points on $X_0(243)$ of conductor $9p$ corresponding to the following isogenies in each of these cases. We make the following choices:

$$P_0 = \begin{cases} \left\langle\dfrac{\omega p}{9}\right\rangle \to \left\langle\dfrac{\omega p+23}{27}\right\rangle = \left\langle\dfrac{\omega p-4}{27}\right\rangle, & \text{in case 1;} \\ \left\langle\dfrac{\omega p}{9}\right\rangle \to \left\langle\dfrac{\omega p+26}{27}\right\rangle = \left\langle\dfrac{\omega p-1}{27}\right\rangle, & \text{in case 2.} \end{cases} \tag{3.2.1}$$

This gives $P_0 \in X_0(243)(\mathbb{C})$ and we write

$$P = \Phi(P_0) \in E_9(\mathbb{C}). \tag{3.2.2}$$

Remark 3.2.3. In fact, each of the $6 \cdot 9 = 54$ possible choices gives rise to a point on either E_p or E_{p^2} by the procedure we will outline, and we have simply made a choice.

Lemma 3.2.4. *The point $P_0 \in X_0(243)$ is represented in the upper half plane by $\tau = M(\omega p/9)$ where $M = \begin{pmatrix} 2 & -1 \\ 9 & -4 \end{pmatrix}$ for case 1 and $M = \begin{pmatrix} 1 & 0 \\ -9 & 1 \end{pmatrix}$ for case 2.*

Proof. We explain case 2, with case 1 being similar. We need to rewrite the isogeny P_0 in normalized terms (2.1.1). The isogeny ϕ is $\langle \omega p/9\rangle \to \langle \omega p\rangle \to \langle(\omega p-1)/27\rangle$ defined by $z \mapsto 9z$; thus, the kernel of ϕ is cyclic generated by $(\omega p-1)/243$ (modulo the lattice $\langle \omega p/9\rangle$). We want a matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that the diagram

$$\begin{tikzcd} \langle \omega p/9\rangle \arrow[r, "z\mapsto 9z"] \arrow[d, "z\mapsto \frac{z}{c(\omega p/9)+d}"'] & \langle(\omega p-1)/27\rangle \arrow[d, "z\mapsto \frac{27z}{c(\omega p/9)+d}"] \\ \langle M(\omega p/9)\rangle \arrow[r, "z\mapsto 243z"] & \langle 243M(\omega p/9)\rangle \end{tikzcd} \tag{3.2.5}$$

commutes. The matrix $M = \begin{pmatrix} 1 & 0 \\ -9 & 1 \end{pmatrix}$ will do: indeed, a generator for the kernel of the isogeny shifts to $\frac{(\omega p-1)/243}{-9(\omega p/9)+1} = -\frac{1}{243}$. $\square$

4. Descent and tracing

With our points in hand, via descent and tracing, we now show how to use the point P defined in (3.2.2) to construct points on $E_p(K)$ and $E_{p^2}(K)$.

4.1. **Field diagram.** Let $H_f \supseteq K$ be the ring class field attached to the conductor $f \in \mathbb{Z}_{\geq 1}$. We have the following diagram of fields.

$$\begin{tikzcd}[column sep=small, row sep=small] &&&& H_{9p} = H_{3p}(\sqrt[3]{3}) \\ &&& H_{3p} \arrow[ur, dash, "3"] & \\ && L = K(\sqrt[3]{p}) \arrow[ur, dash, "(p-1)/3"] && \\ & K \arrow[ur, dash, "3"] &&& \\ \mathbb{Q} \arrow[ur, dash, "2"'] &&&& \end{tikzcd} \tag{4.1.1}$$

By the main theorem of complex multiplication, $P \in E_9(H_{9p})$. Since K has class number 1, the Artin reciprocity map of class field theory yields a canonical isomorphism

$$\mathrm{Gal}(H_f \,|\, K) \simeq (\mathbb{Z}_K/f\mathbb{Z}_K)^\times/(\mathbb{Z}/f\mathbb{Z})^\times \mathbb{Z}_K^\times. \tag{4.1.2}$$

4.2. **Cubic twists.** We pause to recall the behavior of cubic twists in our context, referring to Silverman [15, X.2] for the general theory. Let $K' \supseteq K$ be an algebraic extension and let $a \in (K')^\times \smallsetminus (K')^{\times 3}$, so $L' := K'(\sqrt[3]{a})$ has $[L' : K'] = 3$. Let

$$\rho \in \mathrm{Gal}(L' \,|\, K') \simeq \mathbb{Z}/3\mathbb{Z} \tag{4.2.1}$$

be the generator satisfying $\rho(\sqrt[3]{a}) = \omega\sqrt[3]{a}$. Then for any $b \in (K')^\times$, there is an isomorphism of groups between the subgroup of $E_b(L')$ that transforms under ρ by multiplication by ω and $E_{ab}(K')$:

$$E_b(L')^{\rho=\omega} := \{X \in E_b(L') : \rho(X) = \omega X\} \xrightarrow{\sim} E_{ab}(K'). \tag{4.2.2}$$

4.3. **Descent from H_{9p} to H_{3p}.** We first apply the method of cubic twisting in the previous section to the extension $H_{9p} = H_{3p}(\sqrt[3]{3})$ over H_{3p}. Let $\rho \in \mathrm{Gal}(H_{9p} \,|\, H_{3p})$ be the generator satisfying $\rho(\sqrt[3]{3}) = \omega\sqrt[3]{3}$. The first step of our descent will be to show that the point $P = \Phi(P_0) \in E_9(H_{9p})$ defined in (3.2.1) lies in the left-hand side of (4.2.2) and hence corresponds to a point in $E_1(H_{3p})$. In the models

$$E_9 \colon y^2 + y = x^3 - 1 \quad \text{and} \quad E_1 \colon y^2 + y = 3x^3 - 1, \tag{4.3.1}$$

this twisting isomorphism becomes

$$\begin{aligned} E_9(H_{9p})^{\rho=\omega} &\to E_1(H_{3p}) \\ (x,y) &\mapsto (x/\sqrt[3]{3}, y). \end{aligned} \tag{4.3.2}$$

Proposition 4.3.3. *For the points $P \in E_9(H_{9p})$ defined in (3.2.2), we have $\rho(P) = \omega P$.*

Proof. The idea of the proof is to use the Shimura reciprocity law to calculate the action of ρ on P, and then to identify the image of this Galois action as the image of P under the action of a *geometric* modular automorphism of $X_0(243)$. Using the computations from §2.2 for the action of the group of modular transformations under the parameterization Φ, we deduce the desired result.

The field $K(\sqrt[3]{3})$ has conductor 9 over K. The element $\beta = 1 + 3\omega$ satisfies

$$3^{(\mathrm{Nm}(\beta)-1)/3} \equiv (-1/\omega)^2 \equiv \omega \pmod{\beta}, \tag{4.3.4}$$

and hence under the isomorphism (4.1.2) with $f = 9$, the element β correponds to the automorphism of $K(\sqrt[3]{3})/K$ sending $\sqrt[3]{3} \mapsto \sqrt[3]{3}\omega$. To lift this to the element $\rho \in \mathrm{Gal}(H_{9p} \,|\, H_{3p})$ exhibiting the same action on $\sqrt[3]{3}$, we must therefore find an element α_ρ such that $\alpha_\rho \equiv 1 \pmod{3p}$ and $\alpha_\rho \equiv \beta \pmod{9}$. The element $\alpha_\rho = 1 + 3p\omega$ suffices.

Since the inverse of α_ρ in the left side of (4.1.2) for $f = 9p$ is $1 + 3p\omega^2$, the Shimura reciprocity Law [2, Theorem 3.7] implies that in case 2, $\rho(P_0)$ is the point on $X_0(243)$ associated to the cyclic 243-isogeny

$$I_\rho \cdot \left\langle \frac{\omega p}{9} \right\rangle \to I_\rho \cdot \left\langle \frac{\omega p - 1}{27} \right\rangle, \tag{4.3.5}$$

where

$$I_\rho := (1 + 3p\omega^2)\mathbb{Z}_K \cap \mathbb{Z}_{K,9p} = (9p^2 - 3p + 1, 3 + 9p\omega^2) \subset \mathbb{Z}_{K,9p} \tag{4.3.6}$$

is an invertible ideal in the order $\mathbb{Z}_{K,9p}$. (Even before carrying out this calculation, the isogeny tree in Figure 3.1 implies that the result must be an isogeny between one of the curves $\langle \frac{\omega p + k}{9} \rangle$ with $k = 0, 3$, or 6 and one of the curves $\langle \frac{\omega p - j}{27} \rangle$ with $j = 1, 10$, or 19, since the adjacent curves in the tree have conductor $3p$ and are hence fixed by ρ.) A simple calculation shows that the result is

$$\rho(P_0) = \left(\left\langle \frac{\omega p + 6}{9} \right\rangle \to \left\langle \frac{\omega p - 10}{27} \right\rangle \right). \tag{4.3.7}$$

We now look for a modular automorphism $A \in \mathrm{MAut}(X_0(243))$ such that $A(P_0) = \rho(P_0)$. A quick computer search over the finite group $\mathrm{MAut}(X_0(243))$ reveals that the matrix $A = \begin{pmatrix} 327 & 2 \\ 53460 & 327 \end{pmatrix}$, corresponding to the element $(v^{-1}wvw)v^2 \in S_3 v^2 \subset \mathrm{MAut}(X_0(243))$, satisfies this condition. Therefore, since the action of S_3 fixes the image on E_9 and v acts by ω^2 on E_9 by Proposition 2.2.7, we conclude $A(P) = \rho(P) = \omega P$. A similar computation holds in case 1. □

From Proposition 4.3.3, it follows that each point $P \in E_9(H_{9p})$ defined in (3.2.2) descends with a cubic twist by 3 to a point $Q \in E_1(H_{3p})$.

4.4. **Trace and descent from H_{3p} to L.** Recall from (4.1.1) that $L = K(\sqrt[3]{p}) \subset H_{3p}$. Define

$$R := \mathrm{Tr}_{H_{3p}/L}\, Q \in E_1(L). \tag{4.4.1}$$

Let σ be the generator of $\mathrm{Gal}(L \,|\, K)$ such that $\sigma(\sqrt[3]{p}) = \omega \sqrt[3]{p}$.

Proposition 4.4.2. *Using the model $y^2 + y = 3x^3 - 1$ for E_1 as in (4.3.1):*

$$\sigma(R) = \begin{cases} \omega R + (0, \omega^2), & \text{in case 1;} \\ \omega^2 R + (0, \omega^2), & \text{in case 2.} \end{cases}$$

Proof. The proof is similar to that of Proposition 4.3.3 so we only sketch the salient points. For $p \equiv 4 \pmod 9$, the element $\alpha_\sigma = 1 - 2p\omega^2 \in \mathbb{Z}_K$ has the property that under the Artin reciprocity isomorphism (4.1.2) for $f = 9p$, the associated element $\sigma \in \mathrm{Gal}(H_{9p} \,|\, K)$ satisfies $\sigma(\sqrt[3]{p}) = \omega\sqrt[3]{p}$ and $\sigma(\sqrt[3]{3}) = \sqrt[3]{3}$. This latter fact will be important to ensure that the $\sqrt[3]{3}$ twisting isomorphism (4.2.2) is equivariant for the action of σ. For $p \equiv 7 \pmod 9$, we instead take $\alpha_\sigma = 1 - 2p\omega$, with the same conclusion.

The Shimura reciprocity law yields the action of σ on P_0, calculated using α_σ as in the proof of Proposition 4.3.3. Here one must further consider the cases $p \equiv 4, 7 \pmod 9$ separately. One obtains:

$$\sigma(P_0) = \begin{cases} \langle \frac{\omega p+4}{9} \rangle \to \langle \frac{\omega p+2}{27} \rangle, & \text{in case 1 with } p \equiv 4 \pmod 9; \\ \langle \frac{\omega p+4}{9} \rangle \to \langle \frac{\omega p-13}{27} \rangle, & \text{in case 2 with } p \equiv 4 \pmod 9; \\ \langle 9\omega p \rangle \to \langle \frac{\omega p-1}{27} \rangle, & \text{in case 1 with } p \equiv 7 \pmod 9; \\ \langle 9\omega p \rangle \to \langle \frac{\omega p+2}{27} \rangle, & \text{in case 2 with } p \equiv 7 \pmod 9. \end{cases} \tag{4.4.3}$$

In each case, we can again identify an automorphism that sends P_0 to $\sigma(P_0)$. For example, in case 2 for $p \equiv 4 \pmod 9$, we find that the matrix $A = \begin{pmatrix} 4473 & 25 \\ 12879 & 72 \end{pmatrix}$, corresponding to the element $(wv^{-1}wv)t^2v^2$, has $A(P_0) = \sigma(P_0)$. Since $wv^{-1}wv \in S_3$, we conclude using Proposition 2.2.7 that

$$\sigma(P) = A(P) = \omega^2 P + (0, \omega^2). \tag{4.4.4}$$

The results in all 4 cases are:

$$\sigma(P) = \begin{cases} \omega P + (0, \omega^2), & \text{in case 1 with } p \equiv 4 \pmod 9; \\ \omega^2 P + (0, \omega^2), & \text{in case 2 with } p \equiv 4 \pmod 9; \\ \omega P + (0, \omega), & \text{in case 1 with } p \equiv 7 \pmod 9; \\ \omega^2 P + (0, \omega), & \text{in case 2 with } p \equiv 7 \pmod 9. \end{cases} \tag{4.4.5}$$

Since the element σ leaves $\sqrt[3]{3}$ invariant, and since the point $(0, \omega)$ is mapped to $(0, \omega)$ under the twisting isomorphism (4.2.2) in the models (4.3.1), we see that the same equations hold for the point Q replacing P.

Finally, in case 1 for $p \equiv 4 \pmod 9$ we calculate

$$\sigma(R) = \sum_{\varsigma \in \mathrm{Gal}(H_{3p} \,|\, L)} \sigma(\varsigma(Q)) = \sum_{\varsigma} \varsigma(\sigma(Q)) = \omega R + \frac{p-1}{3}(0, \omega^2) = \omega R + (0, \omega^2),$$

since $(0, \omega^2)$ is a 3-torsion point fixed by $\mathrm{Gal}(H_{3p} \,|\, L)$ and $[H_{3p} : L] = (p-1)/3$. The other three cases follow similarly. $\square$

4.5. **Descent from L to K.** Unfortunately, Proposition 4.4.2 does not imply that R is nontorsion since there are torsion points in $E_1(L)$ that satisfy these equations. Namely, the torsion point $T = (1, 1)$ satisfies $\sigma(T) = T = \omega^2 T + (0, \omega^2)$, and similarly $T = (1, -2)$ satisfies $\sigma(T) = T = \omega T + (0, \omega^2)$.

But we turn this to our advantage: in case 1 the point $Y := R - T$ for $T = (1, -2)$ satisfies $\sigma(Y) = \omega Y$; and so again by the cubic twist isomorphism (4.2.2), we obtain a point $Z \in E_p(K)$. In case 2, we take $T = (1, 1)$, let $Y = R - T$, and find $\sigma(Y) = \omega^2 Y$ yielding $Z \in E_{p^2}(K)$.

5. Nontorsion

To prove that the point $R \in E_1(K(\sqrt[3]{p}))$ in (4.4.1) is nontorsion, and accordingly its twist $Z \in E_{p^i}(K)$ ($i = 1$ or 2), we now consider its reduction modulo p.

5.1. **Manipulation of η product.** Recall Proposition 2.2.3 giving the modular parametrization $\Phi : X_0(243) \to E_9 : y^2 + y = x^3 - 1$, where

$$x(z) = \frac{\eta(9z)\eta(27z)}{\eta(3z)\eta(81z)}. \tag{5.1.1}$$

In (3.2.1) we considered the points $\tau = M(\omega p/9)$ for $M = \begin{pmatrix} 2 & -1 \\ 9 & -4 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -9 & 1 \end{pmatrix}$ in the two cases (Lemma 3.2.4). We now write the value of $x(\tau)$ in the form $f(p\tau_0)$ where f is a modular function and τ_0 does not depend on p.

The function

$$f(z) := \frac{\eta(27z)}{\eta(3z)} \tag{5.1.2}$$

is a modular unit on $\Gamma_0(81)$ by Ligozat's criterion.

Lemma 5.1.3. *Let $j \in \mathbb{Z}$ satisfy $jp \equiv 4, 1 \pmod{27}$ in case 1 or case 2, respectively. Then*

$$x(\tau) = e^{\pi i/6}\sqrt{3}\, \frac{f(p(\omega - j)/27) f(p\omega/9)}{f(p(\omega - j)/9)} \tag{5.1.4}$$

where f is defined in (5.1.2).

Proof. We show the calculation for case 2; case 1 is similar. With $M = \begin{pmatrix} 1 & 0 \\ -9 & 1 \end{pmatrix}$ and all $z \in \mathfrak{H}$,

$$81M(z) = \frac{9\omega p}{-\omega p + 1} = \frac{9}{-\omega p + 1} - 9 = (T^{-9}S)((\omega p - 1)/9) \tag{5.1.5}$$

where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Similarly

$$\begin{aligned} 27M(z) &= (T^{-3}S)((\omega p - 1)/3), \\ 9M(z) &= (STS)(\omega p), \\ 3M(z) &= (ST^3S)(\omega p/3). \end{aligned} \tag{5.1.6}$$

By the transformation formulas for the Dedekind η-function

$$\eta(T(z)) = \eta(z+1) = e^{\pi i/12}\eta(z), \quad \eta(S(z)) = \eta(-1/z) = \sqrt{-iz}\,\eta(z), \tag{5.1.7}$$

we calculate:

$$\begin{aligned} \eta(81\tau) &= e^{\pi i/4}\sqrt{-i(\omega p - 1)/9}\,\eta((\omega p - 1)/9) \\ \eta(27\tau) &= e^{-\pi i/4}\sqrt{-i(\omega p - 1)/3}\,\eta((\omega p - 1)/3) \\ \eta(9\tau) &= e^{-\pi i/6}\sqrt{-i(\omega p - 1)}\,\eta(\omega p) \\ \eta(3\tau) &= \sqrt{-i(\omega p - 1)}\,\eta(\omega p/3). \end{aligned} \tag{5.1.8}$$

Plugging (5.1.8) into $x(\tau)$ as in (5.1.1) and rewriting slightly gives

$$x(\tau) = x(M(\omega p/9)) = e^{\pi i/3}\sqrt{3} \cdot \frac{\eta(\omega p)}{\eta(\omega p - 1)/9)} \cdot \frac{\eta((\omega p - 1)/3)}{\eta(3\omega p)} \cdot \frac{\eta(3\omega p)}{\eta(\omega p/3)}. \tag{5.1.9}$$

Then with $j = 7, 4$ as $p = 4, 7 \pmod 9$, let $k := (1 - jp)/9 \in 3\mathbb{Z}$.

$$\frac{\omega p - 1}{9} = \frac{p(\omega - j)}{9} - k. \tag{5.1.10}$$

Using the transformation formula and (5.1.10) gives:

$$\frac{\eta(\omega p)}{\eta((\omega p-1)/9)} = \frac{e^{\pi i(jp)/12}\,\eta(p(\omega-j))}{e^{\pi i(-k)/12}\,\eta(p(\omega-j)/9)} = e^{\pi i/12} f(p(\omega-j)/27) \tag{5.1.11}$$

since $k+jp = 1-8k \equiv 1 \pmod{24}$. Similarly,

$$\frac{\eta((\omega p-1)/3)}{\eta(3\omega p)} = e^{-\pi i/4}\frac{1}{f(p(\omega-j)/9)}. \tag{5.1.12}$$

Plugging these into (5.1.9), we obtain (5.1.4). ☐

5.2. **Reduction of R modulo p.** We will use the tidy expression (5.1.4) to reduce our mock Heegner points modulo p. The key result that allows this is the following proposition.

Proposition 5.2.1. *Let $f(z) = \sum_n a_n q^n$ be a nonconstant modular function on $\Gamma_0(N)$ with $a_n \in \mathbb{Z}$ such that f only has poles at cusps. Let K be a quadratic imaginary field and p a prime that splits in K with $p \nmid N$. Let $\tau \in \mathfrak{H}$ have image in $X_0(Np)$ corresponding to a cyclic Np-isogeny $\varphi\colon E_1 \to E_2$ of elliptic curves with CM by orders in K. Suppose that the index $[\mathbb{Z}_K : \mathrm{End}(E_1)]$ is not divisible by p but that $[\mathbb{Z}_K : \mathrm{End}(E_2)]$ is divisible by p.*

Let H be the ring class field of K associated to $\mathrm{End}(\varphi)$ and let $\mathbb{Z}_{H,(p)}$ denote the ring of p-integral elements of H. Then $f(\tau), f(p\tau) \in H^\times$ are integral at each prime of H above p and satisfy the congruence

$$f(\tau) \equiv f(p\tau)^p \pmod{p\mathbb{Z}_{H,(p)}}. \tag{5.2.2}$$

Proposition 5.2.1 is proved in the appendix. Using the proposition, we now finish the proof of our main result (Theorem 1.2.1) by showing that R is not torsion when 3 is not a cube modulo p. We describe the case $j = 7$ (see Lemma 5.1.3), the argument for the other cases only differing by constant factors (specifically, an explicit root of unity only depending on j). We continue to use the model $y^2 + y = 3x^3 - 1$ for the curve E_1. Recall from (4.3.2) and Lemma 5.1.3 that for the point $Q \in E_1(H_{3p})$ we have

$$x(Q) = \frac{x(P)}{\sqrt[3]{3}} = \frac{x(\tau)}{\sqrt[3]{3}} = e^{\pi i/6}\sqrt[6]{3}\,\frac{f(p(\omega-7)/27)f(p\omega/9)}{f(p(\omega-7)/9)}.$$

The assumptions of Proposition 5.2.1 are satisfied by f and the points $\tau = \omega/9, (\omega-7)/27, (\omega-7)/9$. The proposition therefore implies that

$$f((\omega-7)/9)x(Q)^p \equiv (e^{\pi i/6}\sqrt[6]{3})^p f((\omega-7)/27)f(\omega/9) \pmod{p\overline{\mathbb{Z}}}. \tag{5.2.3}$$

We can evaluate the constants in (5.2.3) explicitly.

Lemma 5.2.4. *We have $f((\omega-7)/9) = -\omega^2/\sqrt[3]{9}$ and*

$$\frac{f((\omega-7)/27)f(\omega/9)}{f((\omega-7)/9)} = -e^{\pi i/6}\frac{1}{\sqrt[6]{3}}.$$

Proof. The function $h(z) := f(z/3)^3$ is $\Gamma_0(9)$-invariant by Ligozat's criterion. The point on $X_0(9)$ associated to $\omega/3 \in \mathfrak{H}$ corresponds to the normalized isogeny $\langle\omega/3\rangle \to \langle 3\omega\rangle$ of conductor 3. By the theory of modular units, $h(\omega/3)$ is a 3-unit in the ring class field $H_3 = K$, and hence is equal to a unit in $\mathbb{Z}_K^\times$ times a power of $\sqrt{-3}$. Numerically, we find that $h(\omega/3) = 3\sqrt{-3}$ to several hundred digits of accuracy, so this must be an equality. We then calculate that

$$f(\omega/9) = e^{-\pi i/6}/\sqrt{3}. \tag{5.2.5}$$

In a similar way, we compute

$$f((\omega-7)/9) = -\omega^2/\sqrt[3]{9}, \quad f((\omega-7)/27) = -\omega/\sqrt[3]{3},$$

and putting these together gives the result. ☐

Combining (5.2.3) and Lemma 5.2.4, we obtain

$$x(Q)^p \equiv (e^{\pi i/6}\sqrt[6]{3})^p \left(\frac{-e^{\pi i/6}}{\sqrt[6]{3}}\right) = \omega^2\,(-3)^{(p-1)/6} \pmod{p\overline{\mathbb{Z}}}. \tag{5.2.6}$$

Since $p \equiv 1 \pmod 3$, we have $p\mathbb{Z}_L = (\mathfrak{p}\overline{\mathfrak{p}})^3$ where $\mathbb{Z}_L$ is the ring of integers of $L = K(\sqrt[3]{p})$ and each of $\mathfrak{p}, \overline{\mathfrak{p}}$ have residue field $\mathbb{F}_p$. We consider the pair

$$(R \bmod \mathfrak{p}, R \bmod \overline{\mathfrak{p}}) \in E_1(\mathbb{F}_p)^2. \tag{5.2.7}$$

Proposition 5.2.8. *If 3 is not a cube modulo p, then the image of $R \in E_1(L)$ in $E_1(\mathbb{F}_p)^2$ is not equal to the image of any torsion point in $E_1(L)$, and hence R is nontorsion.*

Before proving this proposition, we need one final lemma.

Lemma 5.2.9. *In the coordinates $y^2 + y = 3x^3 - 1$ for E_1, we have*

$$E_1(L)_{\mathrm{tors}} = E_1(K)_{\mathrm{tors}} = E_1[3] = \{\infty, (0,\omega), (0,\omega^2), (\omega^i, 1), (\omega^i, -2) : i = 0,1,2\} \simeq (\mathbb{Z}/3\mathbb{Z})^2.$$

Proof. The curve E_1 has simplified Weierstrass model $y^2 = x^3 - 432$ with $432 = 2^4 3^3$; since $\sqrt[3]{2} \notin L$, we have $E_1[2](L) = \{\infty\}$. The curve E_1 has good (supersingular) reduction at 2. The prime 2 is unramified in the S_3-extension $L \supseteq \mathbb{Q}$; it is inert in $\mathbb{Z}_K$ and splits into three primes in $\mathbb{Z}_L$ with residue field of size 4, and $\#E(\mathbb{F}_4) = 9$. By the injection of torsion [15, (VII.3.2)], we conclude that $\#E_1(L) \mid 9$. The 3-torsion points of E_1 listed explicitly in the proposition are clearly defined over $K \subset L$, completing the proof. ☐

Proof of Proposition 5.2.8. From (5.2.6) we have that $x(Q)^p \equiv \omega^2\,(-3)^{(p-1)/6} \pmod{p\mathbb{Z}_{H_{3p}}}$. Since $-3 \in \mathbb{F}_p^{\times 2}$, it follows that $(-3)^{(p-1)/6}$ is a cube root of unity in $\mathbb{F}_p^\times$; furthermore, this root of unity is trivial if and only if 3 is a cube modulo p. Meanwhile the image of ω^2 in

$$\mathbb{Z}_K/p\mathbb{Z}_K \simeq \mathbb{Z}_K/\mathfrak{p}_K \times \mathbb{Z}_K/\overline{\mathfrak{p}}_K \simeq \mathbb{F}_p \times \mathbb{F}_p$$

has the form (u, u^2) where $1 \leq u \leq p-1$ is a primitive cube root of unity in $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$. Therefore, (5.2.6) implies that the image of $x(Q)^p$ in $\mathbb{F}_p \times \mathbb{F}_p$ has the form

$$\begin{cases} (u,u^2), & \text{if 3 is a cube mod } p; \\ (u,1) \text{ or } (1,u), & \text{if 3 is not a cube mod } p. \end{cases} \tag{5.2.10}$$

Of course, the same is therefore true for $x(Q)$. In particular, the image of Q in each copy of $E_1(\mathbb{F}_p)$ is a 3-torsion point (namely one of the points $(u^i, 1)$ or $(u^i, -2)$ for $i = 0,1,2$). Now

$$R = \mathrm{Tr}_{H_{3p}/L}\, Q \equiv \frac{p-1}{3} Q \equiv \pm Q \text{ in } E_1(\mathbb{F}_p)^2, \tag{5.2.11}$$

with the sign $\pm$ according to the cases $p \equiv 4, 7 \pmod 9$. The first congruence in (5.2.11) follows since p is totally ramified in the extension H_{3p}/L. To prove the proposition, it therefore suffices to prove that the image of Q in $E_1(\mathbb{F}_p)^2$ is not equal to the image of a torsion point in $E_1(L)$ if 3 is not a cube modulo p. However, this is easily checked directly using Lemma 5.2.9 and (5.2.10). For the nonzero torsion points $T \in E_1[3]$, the images of $x(T)$ in $\mathbb{F}_p \times \mathbb{F}_p$ have the shape $(0,0), (1,1)$, or (u,u^2) with u a primitive cube root of unity in $\mathbb{F}_p^\times$, never $(u,1)$ or $(1,u)$. ☐

Of course, if R is nontorsion, then the points $Y = R - T \in E_1(L)$ and $Z \in E_{p^i}(K)$ will be nontorsion as well. Finally, since E has CM by $\mathbb{Z}_K$ we have $\mathrm{rk}_{\mathbb{Z}}(E(\mathbb{Q})) = \mathrm{rk}_{\mathbb{Z}_K}(E(K))$. Explicitly, if $Z \in E_{p^i}(K)$ is nontorsion then either $Z + \overline{Z}$ or $(\sqrt{-3}Z) + (\overline{\sqrt{-3}Z})$ will be a nontorsion point in $E_{p^i}(\mathbb{Q})$. This concludes the proof of Theorem 1.2.1.

5.3. **Tables.** In the following tables, we show the points constructed with our method, suggesting they are nontorsion whenever the corresponding twisted L-value is nonzero (see §1.4). We define

$$L_{\mathrm{alg}}(E_n,1) := L(E_n,1)\frac{2\pi\sqrt[3]{n}}{\sqrt{3}\Gamma(1/3)^3},$$

the conjectural order of the Shafarevich–Tate group of E_n. We let $m(P)$ denote the index of $\langle P\rangle$ in the Mordell–Weil group $E(\mathbb{Q})$.

p	$L_{\mathrm{alg}}(E_{3p^2},1)$	$(3\,\vert\,p)_3=1?$	$P\in E_p(\mathbb{Q})$	$m(P)$
7	1	no	$(2,-1)$	1
13	4	no	$(\frac{2513}{1005},-\frac{1388}{1005})$	2
31	4	no	$(\frac{277028111}{119531076},\frac{316425265}{119531076})$	2
43	1	no	$(\frac{805}{228},-\frac{229}{228})$	2
61	0	yes	∞	–
67	9	yes	$(\frac{-3481613117857223908773469049678633}{610868942776961094346380627914232},\frac{3859176073959095744240009217935657}{610868942776961094346380627914232})$	3
79	1	no	$(\frac{26897}{6783},\frac{17320}{6783})$	2
97	4	no	$(-\frac{2799894968113535105}{200421477873478047},\frac{2832713504497390136}{200421477873478047})$	4
103	9	yes	$(\frac{8464527409781679166516 51}{26131117682318184495404 64},\frac{1224773973362617976922 4061}{26131117682318184495404 64})$	3
139	4	no	$(\frac{54560}{13317},\frac{54943}{13317})$	2
151	9	yes	$(-\frac{123623\cdots7041}{313952\cdots2740},\frac{1672043\cdots5041}{313952\cdots2740}),\ \mathrm{ht}(P)\approx 140.03$	6
157	4	no	$(-\frac{1495389786913799608288060991 05}{1791111577964806270169796357 6},\frac{1619310709753576028169442105 93}{1791111577964806270169796357 6})$	2
193	0	yes	∞	–

p	$L_{\mathrm{alg}}(E_{3p},1)$	$(3\,\vert\,p)_3=1?$	$P\in E_{p^2}(\mathbb{Q})$	$m(P)$
7	1	no	$(-\frac{2}{3},\frac{11}{3})$	1
13	1	no	$(\frac{1589}{285},-\frac{464}{285})$	2
31	1	no	$(\frac{12376607}{1219092},-\frac{5368415}{1219092})$	2
43	4	no	$(\frac{388481023433394017043486873 5}{316639715249572968055283052},\frac{413561995142793125324177473}{316639715249572968055283052})$	2
61	0	yes	∞	–
67	0	yes	∞	–
79	1	no	$(\frac{416502767358398513}{77680272383924217},\frac{1418322935604634846}{77680272383924217})$	1
97	1	no	$(\frac{76769228526793}{20893884519009},\frac{44032007562523 4}{20893884519009})$	1
103	0	yes	∞	–
139	4	no	$(\frac{273171\cdots7720}{644917\cdots4681},-\frac{247724\cdots7279}{644917\cdots4681}),\ \mathrm{ht}(P)\approx 232.48$	4
151	0	yes	∞	–
157	1	no	$(-\frac{3385020496910041178401474743 35}{1856755205556791736672396152 4},\frac{5814420151676389014601553795 51}{1856755205556791736672396152 4})$	2
193	0	yes	∞	–

Appendix A. Application of mod p geometry

In this appendix we prove Proposition 5.2.1. The proposition will be deduced as a special case of a more general underlying geometric principle. Let X be a proper flat curve over a discrete valuation ring R with mixed characteristic $(0,p)$. Let $F = \operatorname{Frac} R$ denote the fraction field of R and let k be the residue field of R. Suppose that X_F is smooth and geometrically connected. Suppose further that X_k is semistable with two irreducible components, each smooth and geometrically connected. Let D be an R-finite flat closed subscheme of X whose special fiber lies in the smooth locus of the special fiber of X.

Let $f \in \mathscr{O}_{X_F}(U_F)$ for $U := X \smallsetminus D$. Let $\infty \in D(R)$ be such that the image of f in the ∞_F-adic completion $\mathrm{Frac}(\widehat{O}_{X_F,\infty_F})$ of $F(X)$ belongs to the polar localization along ∞ of the ∞-adic completion of $\mathscr{O}_X$. More concretely, if q is a local generator along ∞ of its ideal sheaf in $\mathscr{O}_X$ then we are supposing that the natural map

$$F(X) \to F(\!(q)\!) = F[\![q]\!][1/q]$$

carries f into $R[\![q]\!][1/q]$. We claim that the following general congruence holds.

Proposition A.1. *Suppose that $g \in \mathscr{O}_{X_F}(U_F)$ is such that its image in $\mathrm{Frac}(\widehat{O}_{X_F,\infty_F}) = F(\!(q)\!)$ belongs to $R[\![q]\!][1/q]$ and has reduction modulo pR coinciding with the image of f^p. Then for any $u \in U(R)$ such that u and ∞ reduce into the same connected component of the smooth locus of X_k, we have $f(u), g(u) \in R$ and $g(u) \equiv f(u)^p \pmod{pR}$.*

We first show how this proposition implies Proposition 5.2.1.

Proof of Proposition 5.2.1. We apply Proposition A.1 with $X = X_0(Np)$ over the localization $R = \mathbb{Z}_{H,(\mathfrak{p})}$ with $F = H$ and $\mathfrak{p}$ a prime above p; we take D to be the closed subscheme of cusps including the cusp ∞; and the modular function f as in Proposition 5.2.1.

We let $g(z) := f(pz)$ and $u := W_p(\tau)$ for τ as in Proposition 5.2.1 with W_p the Atkin–Lehner involution of $X_0(Np)$. Since the q-expansion of f has coefficients in $\mathbb{Z}$, the q-expansions of f^p and g are congruent modulo p.

The point on $X_0(Np)$ associated to τ corresponds to a cyclic Np-isogeny $\varphi\colon E_1 \to E_2$, and we are assuming that $m = [\mathbb{Z}_K : \mathrm{End}(E_1)]$ is relatively prime to p, but that $p \mid m_2$ where $m_2 := [\mathbb{Z}_K : \mathrm{End}(E_2)]$. As we explain below, these conditions ensure that τ has reduction in the connected component of the smooth locus of X_k corresponding to étale p-level structure (i.e., the component distinct from the one into which ∞ reduces). Therefore u and ∞ have reduction into the same component of the smooth locus of X_k. Granting that, since $g(u) = f(\tau)$ and $f(u) = f(p\tau)$ by the $\Gamma_0(N)$-invariance of f, we then get from Proposition A.1 that that $f(\tau)$ and $f(p\tau)$ belong to R and satisfy $f(\tau) \equiv f(p\tau)^p \pmod{pR}$.

To see that τ has reduction with étale p-level structure, it is equivalent to show that its reduction does not have multiplicative p-level structure. Suppose for the sake of contradiction that this is the case (i.e., that the reduction of τ does have multiplicative p-level structure). Extending F a finite amount if necessary, the F-point τ of the coarse space $Y_0(Np)$ comes from a CM elliptic curve E over R, and $E[p]$ then has connected-étale sequence over R which (by canonicity) is stable by the order $\mathbb{Z}_{K,m}$. Hence, passing to generic fibers, the subgroup J of order p in $\ker\varphi$ must be stable by $\mathbb{Z}_{K,m}$. But then E_1/J would have endomorphisms by $\mathbb{Z}_{K,m}$, and hence p would not divide m_2 (since E_2 is a quotient of E_1/J by a subgroup of size N, which is prime to p). This contradiction to our assumptions implies that τ has reduction with étale p-level structure and concludes the proof. ☐

We conclude with a proof of Proposition A.1.

Proof of Proposition A.1. Pick an affine open $V \subset U$ around the reduction u_k of u such that V_k is contained in the common irreducible component that contains the reductions of ∞ and u, so V is R-smooth with geometrically connected (hence geometrically integral) fibers and $u \in V(R)$. Since an integrally closed noetherian domain (such as $R[V]$) is the intersection in its fraction field of its localizations at all height-1 primes, the only obstacle to $f|_{V_K} \in K[V_K]$ coming from $R[V]$ is that the order of f at the generic point of V_k may be negative.

Assuming this order is negative, say $-m$, if π is a uniformizer of R then $\pi^m f$ comes from $R[V]$ and has nonzero reduction modulo π. To rule this out, we observe (by some elementary unraveling of definitions) that the image in $k[\![q]\!][1/q]$ of the reduction of $\pi^m f$ is the reduction of π^m times the element of $R[\![q]\!][1/q]$ that is assumed to be the image of f in $K(\!(q)\!) = K[\![q]\!][1/q]$, and the latter reduction is clearly 0. This is a contradiction. The same reasoning applies to g, as well as to $(f^p - g)/p$, so it follows that

$$f, g, \frac{f^p - g}{p} \in R[V].$$

Now evaluating at $u \in V(R)$ gives the desired conclusions concerning $f(u)$ and $g(u)$. $\square$

References

[1] Li Cai, Jie Shu, and Ye Tian, *Cube sum problem and an explicit Gross-Zagier formula*, Amer. J. Math. **139** (2017), no. 3, 785–816.

[2] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Reg. Conf. Ser. in Math., vol. 101, Amer. Math. Soc., Providence, 2004.

[3] Samit Dasgupta and John Voight, *Heegner points and Sylvester's conjecture*, Arithmetic geometry, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, 2009, 91–102.

[4] Noam Elkies, *Heegner point computations*, Algorithmic number theory (ANTS-I, Ithaca, NY, 1994), Lecture Notes in Comp. Sci., vol. 877, 1994, 122–133.

[5] Noam Elkies, Tables of fundamental integer solutions (x, y, z) of $x^3 + y^3 = pz^3$ with p a prime congruent to 4 mod 9 and less than 5000 or congruent to 7 mod 9 and less than 1000, available at `http://www.math.harvard.edu/~elkies/sel_p.html`.

[6] Benedict H. Gross and Don Zagier, *Heegner points and derivatives of L-series*, Inv. Math. **84** (1986), no. 2, 225–320.

[7] Lloyd Kilford, *Generating spaces of modular forms with η-quotients*, JP J. Algebra Number Theory Appl. **8** (2007), no. 2, 213–226.

[8] Paul Monsky, *Mock Heegner points and congruent numbers*, Math. Z. **204** (1990), 45–68.

[9] A.P. Ogg, *Modular functions*, Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, 1980, 521–532.

[10] Fernando Rodriguez-Villegas and Don Zagier, *Which primes are sums of two cubes?*, Number theory (Halifax, NS, 1994), CMS Conf. Proc., vol. 15, Amer. Math. Soc., Providence, 1995, 295–306.

[11] Philippe Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory **23** (1986), 294–317.

[12] Philippe Satgé, *Un analogue du calcul de Heegner*, Inv. Math. **87** (1987), 425–439.

[13] E.S. Selmer, *The diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. **85** (1951), 203–362.

[14] Jie Shu and Hongbo Yin, *An explicit Gross-Zagier formula related to the Sylvester conjecture*, preprint, 2017.

[15] Joseph Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, **106**. Springer, Dordrecht, 2009. 513 pp.

[16] J.J. Sylvester, *On certain ternary cubic-form equations*, Amer. J. Math. **2** (1879), no. 4, 357–393.