# Heegner points and Sylvester's conjecture

Samit Dasgupta and John Voight

Abstract. We consider the classical Diophantine problem of writing positive integers $n$ as the sum of two rational cubes, i.e. $n = x^3 + y^3$ for $x, y \in \mathbb{Q}$. A conjecture attributed to Sylvester asserts that a rational prime $p > 3$ can be so expressed if $p \equiv 4, 7, 8 \pmod 9$. The theory of mock Heegner points gives a method for exhibiting such a pair $(x, y)$ in certain cases. In this article, we give an expository treatment of this theory, focusing on two main examples: a theorem of Satgé, which asserts that $x^3 + y^3 = 2p$ has a solution if $p \equiv 2 \pmod 9$, and a proof sketch that Sylvester's conjecture is true if $p \equiv 4, 7 \pmod 9$ and 3 is not a cube modulo $p$.

## 1. A Diophantine problem

**1.1. Sums of rational cubes.** We begin with the following simple Diophantine question.

Question. Which positive integers $n$ can be written as the sum of two cubes of rational numbers?

For $n \in \mathbb{Z}_{>0}$, let $E_n$ denote the (projective nonsingular) curve defined by the equation $x^3 + y^3 = nz^3$. This curve has the obvious rational point $\infty = (1 : -1 : 0)$, and equipped with this point the curve $E_n$ has the structure of an elliptic curve over $\mathbb{Q}$. The equation for $E_n$ can be transformed via the change of variables

$$X = 12n\frac{z}{x+y}, \quad Y = 36n\frac{x-y}{x+y} \tag{1}$$

to yield the affine Weierstrass equation $Y^2 = X^3 - 432n^2$.

We then have the equivalent question: Which curves $E_n$ have a nontrivial rational point? For $n$ not a cube or twice a cube, $E_n(\mathbb{Q})_{\text{tors}} = \{\infty\}$ (see [**Si**, Exercise 10.19]), so also equivalently, which curves $E_n$ have positive rank $\text{rk}(E_n(\mathbb{Q})) > 0$?

Examples. Famously, $1729 = 1^3 + 12^3 = 9^3 + 10^3$; also,

$$\left(\frac{15642626656646177}{590736058375050}\right)^3 + \left(\frac{-15616184186396177}{590736058375050}\right)^3 = 94.$$

In each case, these solutions yield generators for the group $E_n(\mathbb{Q})$. (Note $n = 94 = 2 \cdot 47$ is a case covered by Satgé's theorem below, cf. §3.1.)

1991 *Mathematics Subject Classification.* Primary 11F11, 11G05; Secondary 11D25.

*Key words and phrases.* Modular forms, elliptic curves, Heegner points, Diophantine equations.

**1.2. Sylvester's conjecture.** We now consider the case $n = p \geq 5$ is prime.

CONJECTURE (Sylvester, Selmer [**Se**]). *If $p \equiv 4, 7, 8 \pmod 9$, then $p$ is the sum of two rational cubes.*

Although this conjecture is traditionally attributed to Sylvester (see [**Sy2**, §2] where he considers "classes of numbers that cannot be resolved into the sum or difference of two rational cubes"), we cannot find a specific reference in his work to the above statement or one of its kind (see also [**Sy1, Sy3, Sy4**]).

An explicit 3-descent (as in [**Se**], see also [**Sa1**]) shows that

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

Hence $\mathrm{rk}(E_p(\mathbb{Q})) = 0$ for $p \equiv 2, 5 \pmod 9$, a statement which can be traced back to Pépin, Lucas, and Sylvester [**Sy2**, Section 2, Title 1].

The sign of the functional equation for the $L$-series of $E_p$ is

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

(See [**K**]; this can be derived from the determination of the local root numbers $w_p(E_p) = (-3/p)$ and $w_3(E_p) = 1$ if and only if $p \equiv \pm 1 \pmod 9$.)

Putting these together, for $p \equiv 4, 7, 8 \pmod 9$, the Birch–Swinnerton-Dyer (BSD) conjecture predicts that $\mathrm{rk}(E_p(\mathbb{Q})) = 1$.

**1.3. A few words on the case $p \equiv 1 \pmod 9$.** For $p \equiv 1 \pmod 9$, the BSD conjecture predicts that $\mathrm{rk}(E_p(\mathbb{Q})) = 0$ or 2, depending on $p$. This case was investigated by Rodriguez-Villegas and Zagier [**R-VZ**].

Define $S_p \in \mathbb{R}$ by

$$L(E_p/\mathbb{Q}, 1) = \frac{\Gamma(\frac{1}{3})^3\sqrt{3}}{2\pi\sqrt[3]{p}} S_p;$$

then in fact $S_p \in \mathbb{Z}$, and conjecturally (BSD) we have $S_p = 0$ if $\#E_p(\mathbb{Q}) = \infty$ and $S_p = \#Ш(E_p)$ otherwise. Rodriguez-Villegas and Zagier give two formulas for $S_p$, one of which proves that $S_p$ is a square. They also give an efficient method to determine whether $S_p = 0$.

**1.4. The case $p \equiv 4, 7, 8 \pmod 9$: an overview.** Assume from now on that $p \equiv 4, 7, 8 \pmod 9$. We can easily verify Sylvester's conjecture for small primes $p$.

$$\begin{aligned} 7 &= 2^3 + (-1)^3 \\ 13 &= (7/3)^3 + (2/3)^3 \\ 17 &= (18/7)^3 + (-1/7)^3 \\ 31 &= (137/42)^3 + (-65/42)^3 \\ 43 &= (7/2)^3 + (1/2)^3 \\ &\vdots \end{aligned}$$

Again, the BSD conjecture predicts that we should always have that $p$ is the sum of two cubes. General philosophy predicts that in this situation where $E_p$ has

expected rank 1, one should be able to construct rational nontorsion points on $E_p$ using the theory of complex multiplication (CM).

In §2, we introduce the construction of *Heegner points*, which uses the canonical modular parametrization $\Phi : X_0(N) \to E_p$ where $N$ is the conductor of $E_p$; this strategy requires a choice of imaginary quadratic extension $K$ and is therefore not entirely "natural". If instead we try to involve the field $K = \mathbb{Q}(\omega)$, we arrive at a theory of *mock Heegner points*. We then choose a fixed modular parametrization $X_0(N) \to E$ where $E$ is a designated *twist* of $E_p$ for each prime $p$.

In §3, we illustrate one such example, originally due to Satgé. We look at the parametrization $X_0(36) \to E$ where $E : y^2 = x^3 + 1$ is a twist of the curve $E_{2p}$. We show that when $p \equiv 2 \pmod 9$, the equation $x^3 + y^3 = 2p$ has a solution; the proof involves a careful analysis of the relevant Galois action using the Shimura reciprocity law and explicit recognition of modular automorphisms.

In §4, we return to Sylvester's conjecture, and we sketch a proof that the conjecture is true if $p \equiv 4, 7 \pmod 9$ and 3 is not a cube modulo $p$; here, we employ the parametrization $X_0(243) \to E_9$. We close with some open questions.

## 2. Heegner and Mock Heegner points

**2.1. Heegner points.** The curve $E_p$ has conductor $N = 9p^2$ if $p \equiv 7 \pmod 9$ and conductor $N = 27p^2$ if $p \equiv 4, 8 \pmod 9$. We have the modular parametrization

$$\Phi : X_0(N) \to E_p,$$

from which we may define Heegner points as follows.

Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic imaginary field of discriminant $D$ such that 3 and $p$ split in $K$; the pair $(E_p, K)$ then satisfies the *Heegner hypothesis*. Let $\mathcal{O}_K$ denote the ring of integers of $K$, and let $\mathfrak{N} \subset \mathcal{O}_K$ be a cyclic ideal of norm $N$. Then the cyclic $N$-isogeny

$$\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathfrak{N}^{-1}$$

defines a *CM point* $P \in X_0(N)(H)$, where $H$ is the Hilbert class field of $K$.

Let $Y = \mathrm{Tr}_{H/K} \Phi(P) \in E_p(K)$ denote the trace, known as a *Heegner point*. After adding a torsion point if necessary, we may assume $Y \in E_p(\mathbb{Q})$ (see [**D**, §3.4], and note $E_p(K)_{\mathrm{tors}} = E_p[3](K) \cong \mathbb{Z}/3\mathbb{Z}$.)

**2.2. Gross-Zagier formula.** The Gross-Zagier formula indicates when we expect the point $Y \in E_p(\mathbb{Q})$ to be nontorsion, i.e. when its canonical height $\hat{h}(Y)$ is nonzero.

Theorem (Gross-Zagier formula [**D**, Theorem 3.20]). *We have*

$$\hat{h}(Y) \doteq L'(E_p/K, 1) = L'(E_p/\mathbb{Q}, 1)L(E_p/\mathbb{Q}, \chi_K, 1).$$

Here the symbol $\doteq$ denotes equality up to an explicit nonzero "fudge factor." Thus if we choose $K$ such that $L(E_p/\mathbb{Q}, \chi_K, 1) \neq 0$, the BSD conjecture implies that $\hat{h}(Y) \neq 0$ and hence $Y$ will be nontorsion. Working algebraically, without making any reference to $L$-functions, one might hope to prove that $Y$ is nontorsion directly and unconditionally. But this strategy seems tricky—in particular, no natural candidate for $K$ presents itself. In the next section we discuss a more "natural" approach to constructing a nontorsion point on $E_p$.

**2.3. Mock Heegner points.** We consider now a variation of the above method where we construct what are known as *mock Heegner points*; this terminology is due to Monsky [**M**, p. 46], although Heegner's original construction can be described as an example of such "mock" Heegner points.

Consider the field $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$, where $\omega$ is a primitive cube root of unity. Note that the elliptic curve $E_n : x^3 + y^3 = nz^3$ has CM by $\mathcal{O}_K$, given by

$$[\omega](x, y) = (\omega x, \omega y).$$

The prime 3 is ramified in $K$, so the Heegner hypothesis is not satisfied for the pair $(E_p, K)$. Nevertheless, Heegner-like constructions of points defined by CM theory may still produce nontorsion points in certain situations.

**2.4. Twisting.** Notice that

$$(r/\sqrt[3]{p})^3 + (s/\sqrt[3]{p})^3 = 1 \quad \Longleftrightarrow \quad r^3 + s^3 = p. \tag{2}$$

The obvious equivalence (2) suggests that to find points on $E_p(K)$, we may identify $E_p$ as the *cubic twist* of $E_1$ by $\sqrt[3]{p}$. More precisely, let $L = K(\sqrt[3]{p})$, and let $\sigma$ be the generator of $\mathrm{Gal}(L/K)$ satisfying $\sigma(\sqrt[3]{p}) = \omega\sqrt[3]{p}$. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is generated by complex conjugation, which we denote by $^-$. We have an isomorphism of groups

$$\begin{aligned} E_p(\mathbb{Q}) &\cong \{(r/\sqrt[3]{p}, s/\sqrt[3]{p}) \in E_1(L) : r, s \in \mathbb{Q}\} \\ &= \{Y \in E_1(L) : Y^\sigma = \omega^2 Y,\ \overline{Y} = Y\}. \end{aligned}$$

In other words, we look for points on $E_1(L)$ with specified behavior under $\mathrm{Gal}(L/\mathbb{Q})$.

More generally (see [**Si**, §X.5]), if $E/\mathbb{Q}$ is an elliptic curve, then one defines the set of *twists* of $E$ to be the set of elliptic curves over $\mathbb{Q}$ that become isomorphic to $E$ over $\overline{\mathbb{Q}}$, modulo isomorphism over $\mathbb{Q}$. There is a natural bijection between the set of twists of $E$ and the Galois cohomology group

$$H^1(\mathbb{Q}, \mathrm{Aut}(E)) := H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Aut}(E_{\overline{\mathbb{Q}}})).$$

In our setting,

$$\begin{aligned} E_p(\mathbb{Q}) &\cong \{Y \in E_1(L) : Y^\sigma = \omega^2 Y,\ \overline{Y} = Y\} \\ &= \{Y \in E_1(L) : Y^\tau = c_\tau Y \text{ for all } \tau \in \mathrm{Gal}(L/\mathbb{Q})\} \end{aligned} \tag{3}$$

where $[c_\tau] \in H^1(\mathbb{Q}, \mathrm{Aut}(E_1))$ is the cohomology class represented by the cocycle $c_\tau := \sqrt[3]{p}/\tau(\sqrt[3]{p})$. To find a point $Y$ in the set (3), we may take any $Q \in E_1(L)$ and consider the *twisted trace*

$$Q' = Q + \omega Q^\sigma + \omega^2 Q^{\sigma^2} \in E_1(L).$$

The point $Q'$ has the property that $(Q')^\sigma = \omega^2(Q')$.

Now suppose that $Q'$ is nontorsion. Consider then the point $Y = Q' + \overline{Q'}$ in the set (3); either it will be nontorsion, or else it will be trivial and then instead $\sqrt{-3}Q'$ is a nontorsion point in the set (3). Thus in any case, a nontorsion $Q'$ will yield a nontorsion $Y$.

**2.5. Mock Heegner points on $X_0(27)$.** To summarize, if we can construct a point $Q \in E_1(L)$, then by taking a twisted trace we can construct a (hopefully nontorsion) point $Y \in E_p(\mathbb{Q})$. We look to CM theory to construct the point $Q$.

We have a modular parametrization

$$\begin{aligned}\Phi : X_0(27) &\xrightarrow{\sim} E_1 : Y^2 + 9Y = X^3 - 27 \\ z &\mapsto (X, Y) = \left( \frac{\eta(9z)^4}{\eta(3z)\eta(27z)^3}, \frac{\eta(3z)^3}{\eta(27z)^3} \right),\end{aligned}$$

where $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ is the Dedekind eta-function and $q = \exp(2\pi i z)$. In this case, the map $\Phi$ is an isomorphism of curves.

The field $L = K(\sqrt[3]{p})$ is a cyclic extension of $K$ with conductor

$$\mathfrak{f}(L/K) = f = \begin{cases} 3p, & \text{if } p \equiv 4, 7 \pmod 9; \\ p, & \text{if } p \equiv 8 \pmod 9. \end{cases}$$

As $L$ is of dihedral type over $\mathbb{Q}$, it is contained in the ring class field of $K$ of conductor $f$, denoted $H_f$. Let $\mathcal{O}_{K,f} = \mathbb{Z} + f\mathcal{O}_K$ denote the order of $\mathcal{O}_K$ of conductor $f$, and let $P \in X_0(27)(H_f)$ be defined by a cyclic 27-isogeny between elliptic curves with CM by $\mathcal{O}_{K,f}$. We define the point $Q = \mathrm{Tr}_{H_f/L}\,\Phi(P) \in E_1(L)$ and ask: Is the point $Q$ nontorsion?

Let us compute an example with $p = 7$. For an element $z$ in the complex upper half plane $\mathfrak{H}$, denote by $\langle z \rangle$ the elliptic curve $\mathbb{C}/\langle 1, z\rangle$. We have a cyclic 27-isogeny, obtained as a chain of 3-isogenies, given by

$$\langle \omega p/3\rangle \to \langle \omega p\rangle \to \langle (\omega p + 2)/3\rangle \to \langle (\omega p + 2)/9\rangle; \tag{4}$$

this isogeny has conductor $3p$. Under the identification $\Gamma_0(N)\backslash\mathfrak{H} \cong Y_0(N)$, an element $z \in \mathfrak{H}$ represents the isogeny $\langle z\rangle \to \langle Nz\rangle$. The isogeny in (4) is represented by the point $z = M(\omega p/3)$, where $M = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \in SL_2(\mathbb{Z})$. In this case, we have $H_f = H_{3p} = K(\alpha)$ with $\alpha = \sqrt[6]{-7} = \sqrt[6]{7}\exp(\pi i/6)$. One computes that the point $\Phi(z) = P = (X, Y) \in E_1(H_{3p})$, in Weiestrass coordinates as above, agrees with the point

$$\begin{aligned} X = {} & (-180\omega - 90)\alpha^5 + (-216\omega - 216)\alpha^4 + \tfrac{1}{2}(-345\omega - 690)\alpha^3 \\ & - 414\alpha^2 + (330\omega - 330)\alpha + \tfrac{1}{2}(1581\omega), \\ Y = {} & (-6210\omega + 6210)\alpha^5 - 14877\omega\alpha^4 + (-23760\omega - 11880)\alpha^3 \\ & + (-28458\omega - 28458)\alpha^2 + (-22725\omega - 45450)\alpha - 54441 \end{aligned}$$

to the precision computed. One can then verify computationally that

$$Q = \mathrm{Tr}_{H_f/L}(P) = (3\omega, 0) \in E_1(L)$$

is torsion!

The method we have outlined thus fails in this case; we see similar behavior for the eight other distinguished cyclic 27-isogenies of conductor $3p$, as well as for other values of $p$.

## 3. Satgé's construction

**3.1. Satgé's construction.** Our first attempt at constructing a mock Heegner point using the parametrization $X_0(27) \to E_1$ (in §2.5) yielded only torsion points on $E_p(\mathbb{Q})$. We now exhibit a similar construction which *does* work, but not one which addresses Sylvester's conjecture.

THEOREM (Satgé [**Sa2**]). *If $p \equiv 2 \pmod 9$, then $\#E_{2p}(\mathbb{Q}) = \infty$. If $p \equiv 5 \pmod 9$, then $\#E_{2p^2}(\mathbb{Q}) = \infty$.*

Another result in the same vein is the following.

THEOREM (Coward [**C**]). *If $p \equiv 2 \pmod 9$, then $\#E_{25p}(\mathbb{Q}) = \infty$. If $p \equiv 5 \pmod 9$, then $\#E_{25p^2}(\mathbb{Q}) = \infty$.*

Our expository treatment of Satgé's theorem will treat the first case, where $p \equiv 2 \pmod 9$; see also the undergraduate thesis of Balakrishnan [**Ba**]. The second statement follows similarly. Our proof proceeds different than that of Satgé; his original proof is phrased instead in the language of modular forms.

**3.2. Twisting.** Instead of the parametrization $X_0(27) \to E_1$, we use

$$\Phi : X_0(36) \xrightarrow{\sim} E : y^2 = x^3 + 1$$

and define the action of multiplication by $\omega$ by $\omega(x, y) = (\omega x, y)$ for $(x, y) \in E(K)$.

Over $K$, the cubic twist of $E$ by $\sqrt[3]{p}$ is isomorphic to $E_{2p}$. (Over $\mathbb{Q}$, it is the *sextic twist* of $E$ by $\sqrt[6]{-27p^2}$, given by $y^2 = x^3 - 27p^2$, which is isomorphic to $E_{2p}$; the quadratic twist by $\sqrt{-3}$ yields a curve which is isomorphic over $K$, as well as 3-isogenous over $\mathbb{Q}$.) The twisting is then given by the group isomorphism

$$\begin{aligned} E_{2p}(\mathbb{Q}) &\cong \{P = (r\sqrt[3]{p}, s\sqrt{-3}) \in E(L) : r, s \in \mathbb{Q}\} \\ &= \{P \in E(L) : P^\sigma = c_\tau P \text{ for all } \tau \in \mathrm{Gal}(L/\mathbb{Q})\} \end{aligned}$$

where $[c_\tau] \in H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Aut}(E))$ is the represented by the cocycle

$$c_\tau := \frac{\tau(\beta)}{\beta}, \text{ where } \beta = \sqrt[6]{-27p^2}.$$

**3.3. From $H_{6p}$ to $H_{3p}$.** From the cyclic 36-isogeny $\langle \omega p/6 \rangle \to \langle 6\omega p \rangle$ of conductor $6p$, we obtain a point $P \in E(H_{6p})$, where $E : y^2 = x^3 + 1$.

We have the following diagram of fields.

$$\begin{array}{c} H_{6p} = H_{3p}(\sqrt[3]{2}) \\ \Big| 3 \\ H_{3p} \\ \Big| (p+1)/3 \\ L = K(\sqrt[3]{p}) \\ \Big| 3 \\ K \\ \Big| 2 \\ \mathbb{Q} \end{array}$$

As we now describe, it turns out that the trace from $H_{6p}$ to $H_{3p}$ is unnecessary in the trace from $H_{6p}$ to $L$. Let

$$\rho \in \mathrm{Gal}(H_{6p}/H_{3p}) \subset \mathrm{Gal}(H_{6p}/K)$$

satisfy $\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$.

PROPOSITION. *For $P \in E(H_{6p})$ as defined above, we have*

$$P^\rho = P + (0,1),$$

*where $(0,1)$ is a 3-torsion point.*

This proposition can be proved using the methods we introduce below, and so is left to the reader. It follows from this proposition that $\mathrm{Tr}_{H_{6p}/H_{3p}} P = 3P$. To eliminate this factor of 3, we introduce the point

$$T = (-\sqrt[3]{4}, -\sqrt{-3}) \in E[3](H_6)$$

and note that it also satisfies $T^\rho = T + (0,1)$. Thus letting

$$P_T := P - T, \tag{5}$$

we find $(P_T)^\rho = P_T$, so $P_T \in E(H_{3p})$.

**3.4. From $H_{3p}$ to $\mathbb{Q}$.** Define

$$Q = \mathrm{Tr}_{H_{3p}/L} P_T \in E(L). \tag{6}$$

We now claim that the following equation holds.

PROPOSITION. *Let $\sigma \in \mathrm{Gal}(L/K)$ satisfy $\sigma(\sqrt[3]{p}) = \omega\sqrt[3]{p}$. Then we have*

$$Q^\sigma = \omega Q + (0,-1). \tag{7}$$

The point $(0,-1)$ is a 3-torsion point. It follows from equation (7) that the twisted trace is just

$$Y := Q + \omega^2 Q^\sigma + \omega Q^{\sigma^2} = 3Q \in E(L),$$

which via twisting corresponds to a point $Y' \in E_{2p}(K)$.

To conclude the proof of Theorem 3.1, assuming that equation (7) holds, we need to prove that $Y$, and hence $Y'$, is nontorsion. It suffices to prove that $Q$ is nontorsion.

We claim that if $S \in E(L)$ is a torsion point satisfying (7), then

$$S \in E_{\mathrm{tors}}(K) = \langle(-\omega, 0), (2,3)\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

This finishes the proof, because then $S^\sigma = S$, so from (7) we find $(1-\omega)S = (0,-1)$, and this is a contradiction: we can check each of the 12 torsion points, or note that $(0,-1)$ is not divisible by $1-\omega$ in $E_{\mathrm{tors}}(K)$—the $(1-\omega)$-division points of $(0,-1)$ in fact belong to the field $K(\sqrt[3]{2})$.

To prove the claim, let $S \in E[m](L)$ satisfy (7) with $m \in \mathbb{Z}_{\geq 1}$. Multiplying by 3 and noting $3(0,-1) = O$ gives $3S^\sigma = (3S)^\sigma = \omega(3S)$, so $3S$ twists to a point in $E_{2p}[m](K)$. The curve $E_{2p}$ has additive reduction at 3, and so the component group $\#\Phi(\mathbb{F}_3) \leq 4$; thus the twist of $12S$ belongs to the identity component of the special fiber (isomorphic to $\mathbb{F}_3$), so $36S = O$. Factoring the 4- and 9-division polynomials on $E_{2p}$ then finishes the claim.

Note that this argument proves not only that the point $Y'$ is nontorsion, but that it is not divisible by 3 in the group $E_{2p}(K)/E_{2p}(K)_{\mathrm{tors}}$.

**3.5. The $\mathrm{Gal}(L/K)$-action.** We now prove the equation (7). We will in fact prove an equation for $P \in E(H_{6p})$. We choose a lift of $\sigma \in \mathrm{Gal}(L/K)$ to $\mathrm{Gal}(H_{6p}/K)$. Namely, we let $\alpha_\sigma = 1 + 2p\omega$ and let $I_\sigma = \alpha\mathcal{O}_K \cap \mathcal{O}_{K,6p}$. One can show directly that under the Artin map

$$\mathrm{Frob} : I_{K,6p}/P_{\mathbb{Z},6p} \xrightarrow{\sim} \mathrm{Gal}(H_{6p}/K), \tag{8}$$

the ideal $I_\sigma$ corresponds to an element $\sigma \in \mathrm{Gal}(H_{3p}/K)$ such that $\sigma(\sqrt[3]{p}) = \omega\sqrt[3]{p}$. In (8), $I_{K,6p}$ denotes the group of fractional ideals of $K$ that are relatively prime to $6p$, and $P_{\mathbb{Z},6p}$ denotes the subgroup generated by principal ideals $(\alpha)$ where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \pmod{6p}$ for some $a \in (\mathbb{Z}/6p\mathbb{Z})^\times$.

The equation we will prove is

$$P^\sigma = \omega P + (-1, 0), \tag{9}$$

from which one can deduce equation (7) using equations (5) and (6). The proof uses two ingredients: an explicit calculation with the *Shimura reciprocity law*, and an explicit identification of this action with a *modular automorphism*.

We begin with the first of these two steps in the following lemma.

LEMMA. *We have* $P^\sigma = \langle 3\omega p/2\rangle \to \langle (2\omega p + 1)/3\rangle$.

PROOF. The point $P$ is given by the isogeny $\langle \omega p/6\rangle \to \langle 6\omega p\rangle$. The Shimura reciprocity law ([**Sh**, §6.8]) implies that $P^\sigma$ is given by the isogeny

$$I_\sigma^{-1} \cdot \langle \omega p/6\rangle \to I_\sigma^{-1} \cdot \langle 6\omega p\rangle.$$

An explicit calculation shows that $I_\sigma^{-1}\cdot\langle \omega p/6\rangle \sim \langle 3\omega p/2\rangle$, where $\sim$ denotes homothety equivalence. Similarly, we find that $I_\sigma^{-1}\langle 6\omega p\rangle \sim \langle (2\omega p+1)/3\rangle$, thus concluding the proof. □

We now proceed with the second step. Any element of the normalizer of $\Gamma_0(36)$ in the group $\mathrm{PSL}_2(\mathbb{R})$ provides by linear fractional transformations an automorphism of $\Gamma_0(36)\backslash\mathfrak{H}^* = X_0(36)$. The group of such *modular automorphisms* is denoted $N(\Gamma_0(36))$. In the second step of the proof of (9), we find a modular automorphism $M$ such that $M(P) = P^\sigma$. Moreover, since $X_0(36)$ is a curve of genus one, it is easy to determine its automorphism group; we may then identify $M$ explicitly as an element of this automorphism group to obtain the relation (9). For more detail concerning the results on modular automorphisms used in this section, see [**O**].

We now look for a matrix $M$ in $N(\Gamma_0(36))$ such that $M(P) = P^\sigma$. Let $H$ be the subgroup of $N(\Gamma_0(36))$ generated by the Atkin-Lehner involutions $w_4 = \begin{pmatrix} 4 & -1 \\ 36 & -8 \end{pmatrix}$ and $w_9 = \begin{pmatrix} 9 & 2 \\ 36 & 9 \end{pmatrix}$, together with the *exotic automorphism* $e = \begin{pmatrix} 1 & 0 \\ 6 & 1 \end{pmatrix}$ of order 6—there exists such an exotic automorphism $\begin{pmatrix} 1 & 0 \\ N/t & 1 \end{pmatrix}$ normalizing $\Gamma_0(N)$ whenever $t \in \mathbb{Z}_{>0}$ satisfies $t \mid 24$ and $t^2 \mid N$ (see [**O**]). The group $H$ is a solvable group of order $\#H = 72$. One computes directly that $M = \begin{pmatrix} 9 & -4 \\ 36 & -15 \end{pmatrix} \in H$ satisfies $M(P) = P^\sigma$, using the previous lemma.

Now the matrix $M$ corresponds to an element of $\mathrm{Aut}(X_0(36))$, the automorphism group of $X_0(36)$ as an abstract curve. Via the isomorphism $\Phi$, we may view $X_0(36)$ as the elliptic curve $E$ and hence write $M(Z) = aZ + b$ for some $a \in \mathrm{Aut}(E) \cong \mu_6$ and some $b \in E(K)$. To determine $a$ and $b$, we evaluate $M$ on

the cusps. The point $\infty \in X_0(36)$ corresponds under $\Phi$ to the origin of the elliptic curve. We find that $M(\infty) = 1/4$, which corresponds to the point $\Phi(1/4) = (-1, 0)$. Thus $b = (-1, 0)$. Similarly, evaluating at the cusp 0, we find that $a = \omega$. Putting these pieces together, we have $P^\sigma = M(P) = \omega P + (-1, 0)$ as claimed.

**3.6. An example with $p = 11$.** We illustrate the method of the preceding section with $p = 11$. Beginning with $z = \omega p/6$, we compute $P \in E(H_{6p})$ with $x$-coordinate which satisfies

$$x^{36} + 462331656\omega x^{35} + 11767817160\omega^2 x^{34} + 179182057872x^{33} + 543458657808\omega x^{32} + \ldots + 50331648x^3 + 1939159514087424\omega x^2 + 16777216 = 0$$

to the precision computed.

We next compute $P_T = P - T \in E(H_{3p})$, where $T = (-\sqrt[3]{4}, -\sqrt{-3})$ as above. The point $P_T$ has $x$-coordinate which satisfies

$$\begin{aligned} &25x^{12} + (354\omega - 270)x^{11} + (-5313\omega - 3432)x^{10} + (2376\omega + 17578)x^9 \\ &\quad + (21879\omega - 297)x^8 + (-6732\omega - 24552)x^7 + (-16632\omega + 61116)x^6 \\ &\quad + (3168\omega - 9504)x^5 + (-12672\omega - 45936)x^4 + (-19008\omega - 2816)x^3 \\ &\quad + (10560\omega)x^2 + (17664\omega - 5376)x + 10240 = 0. \end{aligned}$$

The trace $Q = \mathrm{Tr}_{H_{3p}/L} P_T \in E(L)$, again to the precision calculated, is the point

$$\begin{aligned} Q = \Bigg( &-\frac{1849}{5776}\sqrt[3]{11}^2 + \frac{645}{5776}\omega\sqrt[3]{11} + \frac{225\omega + 225}{5776}, \\ &\frac{27735\omega + 55470}{438976}\sqrt[3]{11}^2 + \frac{-9675\omega + 9675}{438976}\sqrt[3]{11} + \frac{871202\omega + 435601}{438976}\Bigg). \end{aligned}$$

We indeed find that the equation $Q^\sigma = \omega Q + (0, 1)$ holds as in (7). Finally, the twisted trace is

$$Y = 3Q = \left( -\frac{767848016929}{79297693200}\omega\sqrt[3]{11}, \frac{672808015029320783}{11661518761992000}\sqrt{-3} \right).$$

The point $Y$ gives rise to the solution (as in (1))

$$\left(\frac{684469533791312783}{112919729369578740}\right)^3 + \left(-\frac{661146496267328783}{112919729369578740}\right)^3 = 22,$$

which is twice a Mordell-Weil generator $(17299/9954, 25469/9954)$.

## 4. Sylvester's conjecture, revisited

**4.1. A theorem of Elkies: A breakthrough.** We now return to the original question of Sylvester's conjecture. In 1994, Elkies announced the following result [**E**], which remains unpublished.

THEOREM (Elkies). *If $p \equiv 4, 7 \pmod 9$, then $\#E_p(\mathbb{Q}) = \#E_{p^2}(\mathbb{Q}) = \infty$.*

The method of Elkies can be sketched as follows. Write $p = \pi\overline{\pi} \in \mathbb{Z}[\omega]$, where $\pi, \overline{\pi} \equiv 1 \pmod 3$. Elkies defines a modular curve $X$ defined over $K$, and constructs an explicit modular parametrization

$$\Phi : X \to E_\pi : x^3 + y^3 = \pi$$

defined over $K$. He uses the map $\Phi$ to define a point on $E_\pi$ over $K(\sqrt[3]{\overline{\pi}})$, and twists to get a point in $E_p(K)$.

**4.2. Mock Heegner points, revisited.** Using the strategy of mock Heegner points, we have re-proved the theorem under a further hypothesis on $p$.

THEOREM. *If $p \equiv 4, 7 \pmod 9$ and 3 is not a cube modulo $p$, then $\#E_p(\mathbb{Q}) = \#E_{p^2}(\mathbb{Q}) = \infty$.*

We remark that two-thirds of primes $p \equiv 4, 7 \pmod 9$ have that 3 is not a cube modulo $p$.

We only provide a sketch of the proof. Consider the modular parametrization $\Phi : X_0(243) \to E_9 : x^3 + y^3 = 9$; the curve $X_0(243) = X_0(3^5)$ has genus 19. The modular automorphism group of $X_0(243)$ is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times S_3$, where the $S_3$ factor is generated by $\begin{pmatrix} 28 & 1/3 \\ -81 & 1 \end{pmatrix}$ and the Atkin-Lehner involution $w_{243} = \begin{pmatrix} 0 & -1 \\ 243 & 0 \end{pmatrix}$. The modular parametrization $\Phi$ is exactly the quotient of $X_0(243)$ by this $S_3$.

We start with a cyclic 243-isogeny of conductor $9p$, which yields a point $P \in E_9(H_{9p})$. One can descend the point $P \in E_9(H_{9p})$ with a twist by $\sqrt[3]{3}$ to a point $Q \in E_1(H_{3p})$. We next consider the trace $R = \mathrm{Tr}_{H_{3p}/L} Q \in E_1(L)$. We show that $R^\sigma = \omega R + T$ where $\sigma(\sqrt[3]{p}) = \sqrt[3]{p}$ and $T$ is a 3-torsion point. Thus $R$ yields a point $Y \in E_{p^2}(K)$ by twisting. (This depends on the choice of $P$; another choice yields a point on $E_p(K)$.)

Unfortunately, there exist points $S \in E_1(K)_{\mathrm{tors}}$ that satisfy the equation $S^\sigma = S = \omega S + T$! Indeed, in certain cases the point $R$ (equivalently, $Y$) is torsion; see section 4.4 below for a discussion of when we expect $R$ to be torsion. To prove that the point $R$ is nontorsion when 3 is not a cube modulo $p$, we instead consider the reduction of $R$ modulo $p$. The prime $p$ factors as $(\mathfrak{p}\overline{\mathfrak{p}})^3$ in $L$, so we consider the pair

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

By an explicit computation with $\eta$-products, we are able to show that when 3 is not a cube modulo $p$, this reduction is not the image of any torsion point $S \in E_1(L)_{\mathrm{tors}}$.

**4.3. Example.** We illustrate our method with $p = 7$.

The isogeny $\langle 7\omega/9 \rangle \to \langle (7\omega - 1)/27 \rangle$ is a cyclic 243-isogeny with conductor 63, which yields a point $P = (x, y) \in E_9(H_{63})$ with

$$x^6 - 81x^3 + 5184 = 0, \quad y^6 + 63y^3 + 4536 = 0.$$

The twist $Q = (x, y) \in E_1(H_{21})$ has

$$x^2 + 3\omega^2 x + 4\omega = 0, \quad y^6 + 7y^3 + 56 = 0.$$

We again have $H_{21} = K(\alpha)$ where $\alpha^6 + 7 = 0$; we then recognize

$$Q = (\tfrac{1}{2}\omega^2\alpha^3 - \tfrac{3}{2}\omega^2, -\tfrac{1}{2}\alpha^4 + \tfrac{1}{2}\alpha)$$

to the precision computed. The trace $R = \mathrm{Tr}_{H_{21}/L} Q \in E_1(L)$ is then simply

$$R = (-\tfrac{3}{2}\sqrt[3]{7^2}, \tfrac{11}{2}\omega^2),$$

which yields the solution $Y = (11/3, -2/3)$, i.e.

$$\left(\frac{11}{3}\right)^3 + \left(\frac{-2}{3}\right)^3 = 7^2.$$

**4.4. A Gross-Zagier formula.** A direct naïve analogue of the Gross-Zagier formula in this case would state that

$$\hat{h}(Y) \doteq L'(E_9/K, \chi_{3p}, 1),$$

where $\chi_{3p} : \mathrm{Gal}(H_{3p}/K) \to \mu_3$ is the cubic character associated to the field $K(\sqrt[3]{3p})$. Since formally

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

this formula becomes

$$\hat{h}(Y) \doteq L'(E_p/\mathbb{Q}, 1)L(E_{3p^2}/\mathbb{Q}, 1).$$

When 3 is not a cube modulo $p$, one can prove that $\mathrm{rk}(E_{3p^2}(\mathbb{Q})) = 0$ (see [**Sa1**]), which motivates the fact that the point $Y$ in our construction is nontorsion in this case. Furthermore, one can show that 3 is a cube modulo $p$ if and only if either 3 divides $\#Ш(E_{3p^2}/\mathbb{Q})$ or $\mathrm{rk}(E_{3p^2}/\mathbb{Q}) > 0$; the order of this Tate-Shafarevich group is conjecturally the "algebraic part" of $L(E_{3p^2}/\mathbb{Q}, 1)$ when this value is non-zero. Thus the "naïve analogue of Gross-Zagier" combined with the BSD conjecture suggest the equivalence

$$Y \text{ is divisible by 3 in } E_p(K)/E_p(K)_{\mathrm{tors}} \iff 3 \text{ is a cube modulo } p.$$

The proof sketched in §4.2 yields the forward direction of this implication unconditionally. It should be possible to prove the converse as well, though we have not yet attempted to do so.

In our description of Satgé's construction with $p \equiv 2 \pmod 9$, we constructed a point on the cubic twist of $E_2$ by $\sqrt[3]{p}$, so a direct analogue of Gross-Zagier would yield

$$\hat{h}(Y) \doteq L'(E_{2p}/\mathbb{Q}, 1)L(E_{2p^2}/\mathbb{Q}, 1).$$

In this case one can prove that $\mathrm{rk}(E_{2p^2}(\mathbb{Q})) = 0$ and $3 \nmid \#Ш(E_{2p^2}/\mathbb{Q})$ without extra condition. This provides intuition for why Satgé's construction produces points that are provably not divisible by 3 (in particular nontorsion) without any extra condition, whereas our result for $p \equiv 4, 7 \pmod 9$ requires an extra condition.

Question. What is the precise statement of the Gross-Zagier formula in the cases when the Heegner hypothesis does not hold?

This is the subject of current research by Ben Howard at Boston College. Some aspect of this new formula (perhaps some extra Euler factors which sometimes trivially vanish) would have to account for various cases when the mock Heegner point is torsion even when the derivative of the $L$-function is not zero. Also, this formula would have to exhibit a dependence on the choice of CM point—the formula will in general not depend only on the conductor as in the classical Heegner case.

**4.5. The case $p \equiv 8 \pmod 9$.** What remains untouched by our discussion so far is the case $p \equiv 8 \pmod 9$ in Sylvester's conjecture. In this case, we may use the parametrization $\Phi : X_0(243) \to E_3$ and a cyclic isogeny of conductor $9p$, corresponding to a point $P \in E_3(H_{9p})$.

Adding a torsion point, the point $P$ descends with a twist to a point $Q \in E_1(H_{3p})$, and a twisted trace $Y \in E_p(\mathbb{Q})$. Here, Gross-Zagier would imply that

$$\hat{h}(Y) \doteq L'(E_3/K, \chi_{9p}, 1) = L'(E_p/\mathbb{Q}, 1)L(E_{9p^2}/\mathbb{Q}, 1).$$

There seems to be no simple criterion for $L(E_{9p^2}/\mathbb{Q}, 1) \neq 0$, though one could hope to prove an analogue of the formulas of Rodriguez-Villegas and Zagier [**R-VZ**].

QUESTION. When $p \equiv 8 \pmod 9$, can one prove that the point $Y$ is nontorsion when $L(E_{9p^2}/\mathbb{Q}, 1) \neq 0$, or perhaps at least when 3 does not divide the algebraic part of $L(E_{9p^2}/\mathbb{Q}, 1)$?

## References


[Ba] Jennifer Balakrishnan, CM constructions for elliptic curves, Senior thesis, Harvard University, 2006.

[Bi] B.J. Birch and N.M. Stephens, Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$, *Seminar on number theory, Paris 1981–82 (Paris, 1981/1982)*, Progr. Math., vol. 38, Birkhäuser Boston, Boston, MA, 1983, 1–19.

[C] Daniel R. Coward, Some sums of two rational cubes, *Quart. J. Math.* **51** (2000), 451–464.

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

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

[K] Shin-ichi Kobayashi, The local root number of elliptic curves, *Currents trends in number theory (Allahabad, 2000)*, Hindustan Book Agency, New Delhi, 2002, 73–83.

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

[O] 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.

[R-VZ] 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.

[Sa1] Philippe Satgé, Groupes de Selmer et corps cubiques, *J. Number Theory* **23** (1986), 294–317.

[Sa2] Philippe Satgé, Un analogue du calcul de Heegner, *Inv. Math.* **87** (1987), 425–439.

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

[Sh] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, 1971.

[Si] Joseph Silverman, *The arithmetic of elliptic curves*, Graduate texts in math., vol. 106, Springer-Verlag, New York, 1986.

[Sy1] J.J. Sylvester, On certain ternary cubic-form equations, *Amer. J. Math.* **2** (1879), no. 3, 280–285.

[Sy2] J.J. Sylvester, On certain ternary cubic-form equations, *Amer. J. Math.* **2** (1879), no. 4, 357–393.

[Sy3] J.J. Sylvester, On certain ternary cubic-form equations, *Amer. J. Math.* **3** (1880), no. 1, 58–88.

[Sy4] J.J. Sylvester, On certain ternary cubic-form equations, *Amer. J. Math.* **3** (1880), no. 2, 179–189.



DEPARTMENT OF MATHEMATICS, 1 OXFORD ST, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138

*E-mail address*: dasgupta@math.harvard.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF VERMONT, BURLINGTON, VT 05401

*E-mail address*: jvoight@gmail.com