

Some Diophantine applications of Heegner points

John Voight

University of Sydney

University of Minnesota (2006–2007)

University of Vermont (2007–)

Clay Mathematics Institute Summer School

Georg-August-Universität, Göttingen

1 August 2006

Introduction

The following is joint work with Samit Dasgupta at Harvard University and his student Jennifer Balakrishnan.

- A classical Diophantine problem: sums of two cubes.
- Heegner points.
- Mock Heegner points.
- Satgé's construction.
- A theorem of Elkies.
- Mock Heegner points, revisited.

Sums of two cubes

Question: Which positive integers $n \in \mathbb{Z}_{>0}$ can be written as the sum of two cubes of rational numbers?

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

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

For $n \in \mathbb{Z}_{>0}$, define the curve

$$E_n : x^3 + y^3 = nz^3.$$

Equivalent question: Which curves E_n have a (nontrivial) rational point?

Equipped with the rational point $\infty = (1 : -1 : 0)$, the curve E_n has the structure of an elliptic curve. The equation for E_n can be transformed via a change of variables to yield the (affine) Weierstrass equation

$$y^2 = x^3 - 432n^2.$$

For n not a cube or twice a cube, $E_n(\mathbb{Q})_{\text{tors}} = \{\infty\}$, so also equivalently, which curves E_n have rank $\text{rk}(E_n(\mathbb{Q})) > 0$?

Sylvester's conjecture

We consider now the case where $n = p \geq 5$ is prime.

Conjecture (Sylvester 1880?, Selmer 1951). *If $p \equiv 4, 7, 8 \pmod{9}$, then p is the sum of two rational cubes.*

An explicit 3-descent 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 $p \equiv 2, 5 \pmod{9}$ (Sylvester, Lucas, P epin).

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

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

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

The case $p \equiv 4, 7, 8 \pmod{9}$

Assume from now on that $p \equiv 4, 7, 8 \pmod{9}$.

$$7 = 2^3 + (-1)^3$$

$$13 = (7/3)^3 + (2/3)^3$$

$$17 = (18/7)^3 + (-1/7)^3$$

$$31 = (137/42)^3 + (-65/42)^3$$

$$43 = (7/2)^3 + (1/2)^3$$

$$53 = (1872/217)^3 + (-1819/217)^3$$

$$61 = 5^3 + (-4)^3$$

⋮

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).

Heegner points: Definition

The curve E_p has conductor $N = 9p^2$ or $27p^2$ (according as $p \equiv 7 \pmod{9}$ or $p \equiv 4, 8 \pmod{9}$), so we have the modular parametrization

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

from which we may define Heegner points.

Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field of discriminant $D < 0$ such that 3 and p split in K , i.e. the pair (E_p, K) satisfies the Heegner hypothesis. Let \mathcal{O}_K denote the ring of integers of K .

Let $\mathfrak{N} \subset \mathcal{O}_K$ be a cyclic ideal of norm N ; then the cyclic N -isogeny

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

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

Let $Y = \text{Tr}_{H/K} \Phi(P) \in E_p(K)$ denote the trace, known as a *Heegner point*. After adding a torsion point if necessary, we may assume $Y \in E_p(\mathbb{Q})$.

(Note $E_p(K)_{\text{tors}} = E_p[3](K) \cong \mathbb{Z}/3\mathbb{Z}$.)

Heegner points: Gross-Zagier formula

Therefore, associated to the imaginary quadratic field K , we obtain a Heegner point $Y \in E_p(\mathbb{Q})$. The Gross-Zagier formula indicates when we expect this point to be nontorsion.

Proposition (Gross-Zagier formula). *We have*

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

(Here the symbol \doteq denotes equality up to a nonzero “fudge factor”, which in principle can be made explicit.)

Thus, if we choose K such that $L(E_p/\mathbb{Q}, \chi_K, 1) \neq 0$, i.e. the quadratic twist of E_p by χ_K has analytic rank 0, then (assuming the BSD conjecture) we have $\text{ht}(Y) \neq 0$ and hence Y will be nontorsion.

So although we expect Y to be nontorsion, we have no proof! Working algebraically, perhaps we can prove that Y is nontorsion directly, without making any reference to L -functions. But this strategy seems quite hard, and anyway it is not the most “natural” approach.

Mock Heegner points

We consider now a variation of the above method where we construct what are known as *mock Heegner points* (terminology due to Monsky, arguably Heegner's original construction).

Let $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$, where ω 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 , where

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

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, as predicted by general philosophy.

Twisting

Notice that

$$(r/\sqrt[3]{p})^3 + (s/\sqrt[3]{p})^3 = 1 \iff r^3 + s^3 = p$$

for $r, s \in \mathbb{Q}$. Let $L = K(\sqrt[3]{p})$; then to find points on $E_p(K)$, we identify E_p as the *cubic twist* of E_1 by $\sqrt[3]{p}$. We then may look for points on $E_1(L)$ of this special form.

More precisely, let $\sigma \in \text{Gal}(L/K)$ satisfy $\sigma(\sqrt[3]{p}) = \omega\sqrt[3]{p}$. The Galois group $\text{Gal}(K/\mathbb{Q})$ is generated by complex conjugation, which we denote by $\bar{}$. From the above, we have an isomorphism of groups

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

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

Twisting: Generalities

More generally, if E/\mathbb{Q} is an elliptic curve with j -invariant $j = j(E)$, then there is a bijection between the set of *twists* of E , i.e. the set of elliptic curves with j -invariant j up to isomorphism over \mathbb{Q} , and the set

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

For us,

$$\begin{aligned} E_p(\mathbb{Q}) &\cong \{Y \in E_1(L) : Y^\sigma = \omega^2 Y, \overline{Y} = Y\} \\ &= \{Y \in E_1(L) : Y^\tau = [c_\tau]Y\} \end{aligned}$$

where $[c_\tau] \in H^1(\mathbb{Q}, \mathrm{Aut}(E_1))$ is the cocycle $\tau \mapsto \tau(\sqrt[3]{p})/\sqrt[3]{p}$.

To find such a point Y , 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 either $Y = Q' + \overline{Q'}$ or $Y = \sqrt{-3}Q'$ (if $Q' + \overline{Q'}$ is torsion) yields by the above a point $Y \in E_p(\mathbb{Q})$, which is hopefully nontorsion.

Mock Heegner points on $X_0(27)$

To summarize, if we can construct a point $Q \in E_1(L)$, where $L = K(\sqrt[3]{p})$, 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 $\Phi : X_0(27) \xrightarrow{\sim} E_1$, which in this case is an isomorphism.

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

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

Thus L is contained in the ring class field H_f of K of conductor 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 $Q = \text{Tr}_{H_f/L} \Phi(P) \in E_1(L)$.

Is the point Q nontorsion...?

Mock Heegner points on $X_0(27)$: An example

Let us compute an example. We take $p = 7$. Denoting the elliptic curve $\mathbb{C}/\langle 1, z \rangle$ with $z \in \mathfrak{H}$ by simply $\langle z \rangle$, we have a cyclic 27-isogeny

$$\langle \omega p/3 \rangle \rightarrow \langle \omega p \rangle \rightarrow \langle (\omega p + 2)/3 \rangle \rightarrow \langle (\omega p + 2)/9 \rangle$$

of conductor $3p$. This isogeny is given by a (normalized) point $z \in \mathfrak{H}$.

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 $\Phi(z) = P = (x, y) \in E_1(H_{3p})$ agrees with

$$x = \frac{5}{2}(-\omega + 1)\alpha^3 + \frac{23}{2}\omega^2$$

$$y = -3\alpha^4 + (10\omega + 5)\alpha$$

to the precision computed, and indeed $x^3 + y^3 = 1$.

One can then verify computationally that

$$Q = \text{Tr}_{H_f/L}(P) = (0, \omega^2) \in E_1(L)$$

is torsion!

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

Satgé's construction

So our first attempt at constructing a mock Heegner point, using the parametrization $X_0(27) \rightarrow E_1$, yielded only a torsion point on $E_p(\mathbb{Q})$.

We now exhibit a similar construction which *does* work, although we cannot apply it towards Sylvester's conjecture.

Theorem (Satgé 1987).

If $p \equiv 2 \pmod{9}$, then $\#E_{2p}(\mathbb{Q}) = \infty$.

If $p \equiv 5 \pmod{9}$, then $\#E_{2p^2}(\mathbb{Q}) = \infty$.

Our expository treatment of Satgé's theorem will treat the first case, where $p \equiv 2 \pmod{9}$; the second statement follows similarly, and is left as an exercise! (His proof is phrased instead in the language of modular forms.)

Satgé's construction: Twisting

Here, instead of the parametrization $X_0(27) \rightarrow E_1$, we instead use

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

and by Φ we identify these two curves.

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 $\sqrt{-3}$ is an isomorphism over K .

The twisting is then given by the group isomorphism

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

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

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

Satgé's construction: From H_{6p} to H_{3p}

From the cyclic 36 -isogeny $\langle \omega p/6 \rangle \rightarrow \langle 6\omega p \rangle$ 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.

$$H_{6p} = H_{3p}(\sqrt[3]{2})$$

In the trace from H_{6p} to L , it turns out that the trace from H_{6p} to H_{3p} is needless. Let

$$\begin{array}{c} | 3 \\ H_{3p} \\ | (p+1)/3 \end{array}$$

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

satisfy $\rho(\sqrt[3]{2}) = \omega\sqrt[3]{2}$. Then one can prove that

$$L = K(\sqrt[3]{p})$$

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

where $(0, 1)$ is a 3-torsion point. (So really, we have $\text{Tr}_{H_{6p}/H_{3p}} P = 3P$.) We find that

$$\begin{array}{c} | 3 \\ K \\ | 2 \\ \mathbb{Q} \end{array}$$

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

also satisfies $T^\rho = T + (0, 1)$, so instead we set

$$P_T = P - T;$$

hence $(P_T)^\rho = P_T$ and $P_T \in E(H_{3p})$.

Satgé's construction: From H_{3p} to \mathbb{Q}

Now, from $P \in E(H_{9p})$, we have a point $P_T \in E(H_{3p})$. $H_{6p} = H_{3p}(\sqrt[3]{2})$

Let

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

We now claim that the following *key equation* holds:

$$Q^\sigma = \omega Q + (0, -1), \quad (\sigma)$$

where $\sigma(\sqrt[3]{p}) = \omega \sqrt[3]{p}$. The point $(0, -1)$ is a 3-torsion point. It follows from (σ) that the twisted trace is just

$$Y = 3Q \in E(L) \longleftrightarrow Y \in E_{2p}(K).$$

(One can also show that $\bar{Q} = -\omega Q + (0, 1)$, where $\bar{}$ denotes complex conjugation, so in fact $Y \in E_{2p}(\mathbb{Q})$.)

To conclude the proof we must prove that Y is nontorsion. It suffices to prove that Q is nontorsion. But $E_{\text{tors}}(L) = \{O, (0, \pm 1)\} = E_{\text{tors}}(\mathbb{Q})$, and no such $S \in E_{\text{tors}}(\mathbb{Q})$ satisfies the equation (σ) : indeed, $S^\sigma = S = \omega S$, so equation (σ) implies $S = S + (0, -1)$, a contradiction!

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

Satgé's construction: the $\text{Gal}(L/\mathbb{Q})$ -action

We now prove the equation

$$Q^\sigma = \omega Q + (0, 1). \quad (\sigma)$$

We will in fact prove the equation for $P \in E(H_{6p})$, namely

$$P^\sigma = \omega P + (-1, 0),$$

from which one can deduce equation (σ) by taking the trace.

The proof uses two ingredients: An explicit calculation with the *Shimura reciprocity law*, and an explicit identification of this action with a *modular automorphism*.

In the second step, we find a matrix $M \in N(\Gamma_0(36))$ such that $M(P) = P^\sigma$. We may then identify M explicitly as an element of $\text{Aut}(X_0(36))$ to obtain the relation.

Satgé's construction: Shimura reciprocity law

We choose a lift of $\sigma \in \text{Gal}(L/K)$ to $\text{Gal}(H_{3p}/K)$, 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 indeed by the Artin map the ideal I_σ corresponds to an element $\sigma \in \text{Gal}(H_{3p}/K)$ such that $\sigma(\sqrt[3]{p}) = \omega\sqrt[3]{p}$.

The point P is given by the isogeny $\langle \omega p/6 \rangle \rightarrow \langle 6\omega p \rangle$. The Shimura reciprocity law implies that P^σ is given by the isogeny

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

Now

$$I_{\sigma^{-1}} = \bar{\alpha}\mathcal{O}_K \cap \mathcal{O}_{K,6p}.$$

Multiplying out (exercise!), we find that

$$I_{\sigma^{-1}} \cdot \langle \omega p/6 \rangle \sim \langle 3\omega p/2 \rangle,$$

where \sim denotes up to homothety.

Similarly, we find that $I_{\sigma^{-1}} \langle 6\omega p \rangle = \langle (2\omega p + 1)/3 \rangle$. Thus,

$$P^\sigma = \langle 3\omega p/2 \rangle \rightarrow \langle (2\omega p + 1)/3 \rangle.$$

Satgé's construction: A modular automorphism

We are proving $P^\sigma = \omega P + (-1, 0)$; we have computed P^σ explicitly.

We now look for a matrix $M \in N(\Gamma_0(36))$ such that $M(P) = P^\sigma$. We let H be the group 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. The group H is a solvable group of order $\#H = 72$. One then computes directly that $M = \begin{pmatrix} 9 & -4 \\ 36 & -15 \end{pmatrix} \in H$ satisfies $M(P) = P^\sigma$.

Now M corresponds to an element of $\text{Aut}(X_0(36))$ (as an abstract curve), and therefore $M(Z) = aZ + b$, where $a \in \mu_6$ and $b \in X_0(36)(K)_{\text{tors}}$ for all $Z \in X_0(36)$.

To determine a, b , we evaluate M on the cusps. The point $\infty \in X_0(36)$ corresponds under Φ to the origin of the elliptic curve. We find that $M(\infty) = 1/4$, which corresponds to the point $(-1, 0)$, so $b = (-1, 0)$. Similarly, evaluating at the cusp 0, we find that $a = \omega$.

Satgé's construction: An example with $p = 11$

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

$$\begin{aligned}
& x^{36} + 462331656\omega x^{35} + (-11767817160\omega - 11767817160)x^{34} + 179182057872x^{33} + 543458657808\omega x^{32} \\
& + (312201400896\omega + 312201400896)x^{31} - 13619042432160x^{30} - 21212636962176\omega x^{29} \\
& + (-57693983073408\omega - 57693983073408)x^{28} + 231529596162304x^{27} + 117311400340992\omega x^{26} \\
& + (616102775838720\omega + 616102775838720)x^{25} - 1899296312438016x^{24} + 938491202727936\omega x^{23} \\
& + (618203645005824\omega + 618203645005824)x^{22} + 9370183184474112x^{21} - 4632810589642752\omega x^{20} \\
& + (-14234295245930496\omega - 14234295245930496)x^{19} - 14909037763952640x^{18} - 18227317846966272\omega x^{17} \\
& + (-11498964860731392\omega - 11498964860731392)x^{16} - 61657505431289856x^{15} + 23215009300217856\omega x^{14} \\
& + (-688757250981888\omega - 688757250981888)x^{13} + 23480810781474816x^{12} + 73565264486596608\omega x^{11} \\
& + (-21877440536641536\omega - 21877440536641536)x^{10} + 105685878131654656x^9 + 40948795261845504\omega x^8 \\
& + (-30848626615910400\omega - 30848626615910400)x^7 + 46971501435420672x^6 + 5332688663740416\omega x^5 \\
& + (-12339450646364160\omega - 12339450646364160)x^4 + 50331648x^3 + 1939159514087424\omega x^2 + 16777216.
\end{aligned}$$

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

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

Satgé's construction: An example with $p = 11$

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

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

We indeed find the key equation $Q^\sigma = \omega Q + (0, 1)$.

Finally, the twisted trace is

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

which gives rise to the solution

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

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

A theorem of Elkies: A breakthrough

We now return to the original question of Sylvester's conjecture. In 1994, Elkies announced the following result.

Theorem (Elkies). *If $p \equiv 4, 7 \pmod{9}$, then $\#E_p(\mathbb{Q}) = \#E_{p^2}(\mathbb{Q}) = \infty$. His method proceeds as follows. Write $p = \pi\bar{\pi}$, where $\pi, \bar{\pi} \equiv 1 \pmod{3}$. He then defines a modular curve X defined over K using π -level structure, and constructs a modular parametrization*

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

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

Using the strategy of mock Heegner points, we have reproved the theorem in the following weaker form.

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

Mock Heegner points, revisited

We now sketch the proof. We begin with the modular parametrization $\Phi : X_0(243) \rightarrow E_9$; the curve $X_0(243) = X_0(3^5)$ now has genus 19 (!).

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 $R = \text{Tr}_{H_{3p}/L} Q \in E_1(L)$. One can show that $R^\sigma = \omega R + T$ where 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 torsion points $S \in (E_1)_{\text{tors}}(K)$ that satisfy the equation $S^\sigma = S = \omega S + T$!

To prove that the point R is nontorsion, we instead consider the reduction $(R \bmod p) \in E_9(\mathcal{O}_L/p\mathcal{O}_L)$. By an explicit computation with η -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 $S \in (E_9)_{\text{tors}}(L)$.

Mock Heegner points, revisited: An example

We illustrate our method with $p = 7$.

The isogeny $\langle 7\omega/9 \rangle \rightarrow \langle (7\omega - 1)/27 \rangle$ 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

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

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

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

The trace $R = \text{Tr}_{H_{21}/L} Q \in E_1(L)$ is then simply

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

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

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

A Gross-Zagier formula

The analog of the Gross-Zagier formula in this case would state that

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

where $\chi_{3p} : \text{Gal}(H_{3p}/K) \rightarrow \mu_3$ 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

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

When 3 is not a cube modulo p , one can prove that $\text{rk}(E_{3p^2}(\mathbb{Q})) = 0$, which is why we expect the point Y in our construction to be nontorsion.

In Satgé's construction, we constructed a point on the cubic twist of E_2 by $\sqrt[3]{p}$, so we would instead obtain

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

In this case one can prove that $\text{rk}(E_{2p^2}(\mathbb{Q})) = 0$.

Question. What is the 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.

The case $p \equiv 8 \pmod{9}$

What remains open is the case $p \equiv 8 \pmod{9}$ in Sylvester's conjecture.

In this case, we may use the parametrization $\Phi : X_0(243) \rightarrow E_3$ 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

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

There seems to be no simple criterion for $L(E_{9p^2}/\mathbb{Q}, 1) \neq 0$.

Question. When $p \equiv 8 \pmod{9}$, can one prove that 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 $L(E_{9p^2}/\mathbb{Q}, 1)$?

Conclusion

Heegner points, useful in abstract theory, can also be made very explicit. They are amenable to explicit and efficient computation.

One can also consider fruitfully their cousins, known as mock Heegner points; these points arise when the Heegner hypothesis is not satisfied because the discriminant D of the CM order and the conductor N of the elliptic curve are not coprime. Mock Heegner points can be used in various ways to solve some very concrete Diophantine problems.

Several open questions remain to be answered in this area of research.