

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

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

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 [Sil86, 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,

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

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F11, 11D25.

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

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.)

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

CONJECTURE (Sylvester, Selmer [Sel51]). *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 [Syl179b, §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 [Syl179a, Syl180a, Syl180b]).

An explicit 3-descent (as in [Sel51], see also [Sat86]) 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 [Syl179b, 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 [Kob02]; 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 [RVZ95].

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 $S_p = \#\mathrm{III}(E_p)$ 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 .

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

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

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

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

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

⋮

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 $\Phi : X_0(N) \rightarrow E_p$ 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 $X_0(N) \rightarrow E$ 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 $X_0(36) \rightarrow E$ 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 $X_0(243) \rightarrow E_9$. 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

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

from which we may define Heegner points as follows.

Let $K = \mathbb{Q}(\sqrt{D})$ be a imaginary quadratic 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

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

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 $Y \in E_p(\mathbb{Q})$ (see [Dar04, §3.4], and note $E_p(K)_{\text{tors}} = E_p[3](K) \cong \mathbb{Z}/3\mathbb{Z}$.)

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 [Dar04, 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 .