Wrap up: The BSD conjecture

Holly Green

Today I'm going to present a classical unsolved problem for which the BSD conjecture provides some insight.

Recall, the weak form of the Birch and Swinnerton–Dyer conjecture says

Conjecture 1 (Birch-Swinnerton–Dyer)**.** *For E an elliptic curve over $\mathbb{Q}$,*

$$\mathit{ord}_{s=1} L(E,s) = \mathit{rank}\ E.$$

This is a remarkable statement connecting an analytic property to the primary arithmetic invariant associated to the elliptic curve.

Assuming that this holds true, we can provide a solution to the 'congruent number problem' in certain cases.

Definition 2. $r \in \mathbb{Q}$ is a congruent number if there exists a right-angled triangle of area r whose sides have rational length. This merely says that there exists a ration solution (a, b, c) to the equations

$$a^2 + b^2 = c^2, \qquad \frac{1}{2}ab = r.$$

Example 3. The first three congruent numbers are 5, 6, 7. The triples providing the necessary right-angled triangles are $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$, $(3, 4, 5)$, $(\frac{24}{5}, \frac{35}{12}, \frac{337}{60})$, respectively.

This is an unsolved problem in the sense that no algorithm exists to show definitively whether or not any given r is a congruent number.

We provide an answer upon restricting to $n \in \mathbb{Z}$ positive and square-free. For such an n, define

$$E_n : y^2 = x^3 - n^2 x.$$

Notice that $\Delta = 64n^6 \neq 0$ and so E_n is in fact an elliptic curve.

Proposition 4. *The following defines a one-to-one correspondence*

$$\begin{aligned}
\{(a,b,c) \in \mathbb{Q}^3 \,|\, a^2 + b^2 = c^2, \ \tfrac{1}{2}ab = n\} &\longleftrightarrow \{(x,y) \in E_n(\mathbb{Q}) \,|\, y \neq 0\} \\
(a,b,c) &\longmapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) \\
\left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right) &\longleftarrow\!\shortmid (x,y).
\end{aligned}$$

This allows us to rephrase: n is a congruent number if and only if there's some $(x, y) \in E_n(\mathbb{Q})$ such that $y \neq 0$.

We can make this even more concrete by studying the structure of $E_n(\mathbb{Q})$. The Mordell–Weil theorem tells us that

$$E_n(\mathbb{Q}) \cong E_n(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r,$$

where $E_n(\mathbb{Q})_{\text{tors}}$ is a finite group and $r \geq 0$ is the rank of E_n. We can actually determine $E_n(\mathbb{Q})_{\text{tors}}$ explicitly.

Observe that $E_n(\mathbb{Q})[2] = \{\mathcal{O}, (0,0), (\pm n, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is a subgroup of $E_n(\mathbb{Q})_{\text{tors}}$. I claim that in fact, $E_n(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

This can be determined from the following two lemmas and Dirichlet's Theorem on primes in arithmetic progressions:

Remark. *The latter says that if* $\gcd(a, n) = 1$*, then there are infinitely many primes* p*, such that* $p \equiv a \pmod{n}$.

Lemma 5. *For* $p \equiv 3 \pmod 4$ *such that* $p \nmid \Delta$*,* $\#\tilde{E}_n(\mathbb{F}_p) = p + 1$*, where* $\tilde{E}_n$ *denotes the reduction of* E_n *modulo* p*.*

Proof. Let $0, \pm n \neq x \in \mathbb{F}_p$ so that our point doesn't come from a torsion point. Note that -1 is not a square, so for each x, either $f(x)$ or $f(-x) = -f(x)$ is. So, for each such x we get two points in $\tilde{E}_n(\mathbb{F}_p)$. Counting also our torsion points gives the result. □

Lemma 6. *Given an integer* $m > 4$*, there are infinitely many primes* $p \equiv 3 \pmod 4$ *such that* $m \nmid p + 1$*.*

Proof. If $m = 2^k$ then there are infinitely many primes $p \equiv 3 \pmod m$. If m has an odd prime divisor, q, then the Chinese Remainder Theorem gives the existence of some $x \in \mathbb{Z}$ such that $x \equiv 1 (mod\ q)$ and $x \equiv 3 (mod\ 4)$. Now, there are infinitely many $p \equiv x (mod\ 4q)$ so the result follows, □

Now, Dirichlet tells us that there are infinitely many primes $p \equiv 3 \pmod 4$ such that $\#\tilde{E}_n(\mathbb{F}_p) = p + 1$. A restatement of this says that for only finitely many $p \equiv 3 \pmod 4$, i.e those dividing Δ, does $\#E_n(\mathbb{Q})_{\text{tors}} \nmid p + 1$. So if $\#E_n(\mathbb{Q})_{\text{tors}} > 4$, Lemma 6 would give rise to a contradiction.

We can therefore identify $E_n(\mathbb{Q})_{\text{tors}}$ with $\{\mathcal{O}, (0,0), (\pm n, 0)\}$, and if there exists $P = (x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$, then P must be a point of infinite order.

So n is a congruent number if and only if rank $E_n \geq 1$. Applying BSD, this becomes if and only if $L(E_n, 1) = 0$, and this value is computable (not by hand) using magma, sage, etc.

In particular, Tim Dokchitser has an algorithm implemented in Sage which calculates the L-value at 1 using the following

Theorem 7 (Dokchitser)**.**

$$L(E, 1) = 2(1 + w_E) \sum_{n \geq 1} \frac{a_n}{n} \int_{n\pi\sqrt{(N_E)}^{-1}}^{\infty} \varphi(x)\, dx.$$

We saw that BSD implies the parity conjecture, i.e.

Conjecture 8 (Parity conjecture)**.** $w_E = (-1)^{\text{rank } E}$.

Combining this with the non-trivial fact that $w_{E_n} = -1$ whenever $n \equiv 5, 6, 7 \pmod 8$, we obtain

Theorem 9. *All* $n \equiv 5, 6, 7 \pmod 8$ *are congruent numbers.*

Alternatively, Tim's formulation gives for any n such that $w_{E_n} = -1$, n is congruent.

A more down to earth characterisation of congruent numbers is described in a result of Tunnell, who also assumed that BSD holds.

Theorem 10 (Tunnell)**.** $n \in \mathbb{Z}$ *positive and square-free is a congruent number if and only if*

$$\begin{cases} \#\{(x,y,z) \,|\, n = x^2 + 2y^2 + 8z^2\} = 2\#\{(x,y,z) \,|\, n = x^2 + 2y^2 + 32z^2\}, & n \text{ odd}, \\ \#\{(x,y,z) \,|\, n = 2x^2 + 8y^2 + 16z^2\} = 2\#\{(x,y,z) \,|\, n = 2x^2 + 8y^2 + 64z^2\}, & n \text{ even}. \end{cases}$$

Again this is computable, and much easier to do by hand for small n, i.e. we can immediately see that $n = 1$ is not a congruent number.

The proof of Tunnell's theorem is based on modular forms of weight $\frac{3}{2}$.