The Birch and Swinnerton-Dyer Conjecture

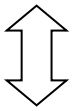
L. Mombelli, C. Tschopp

19.12.2023

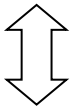
Abstract

This talk aims to discuss the Birch and Swinnerton-Dyer Conjecture and its relation to congruent numbers. More precisely, if this conjecture proves to be true for certain types of elliptic curves, then thanks to Tunnell's Theorem, one can compute in a finite time whether a natural number n is congruent or not. We can assume n to be square-free, then the following holds:

n is a congruent number



$E_n : y^2 = x^3 - n^2x$ contains a rational point (x, y), $y \neq 0$



$rank(E_n(\mathbb{Q})) > 0$

Birch and Swinnerton-Dyer Conjecture

Coates-Wiles (1977)

$L(E_n, 1) = 0$

Theorem of Shimura, Waldsprunger, Tunnell

the n-th q-espansion coefficient in Tunnell's product of theta-functions is zero

1 Congruent Numbers and Elliptic Curves

Problem Let n be a positive natural number. We want to find a right triangle with rational sides $a, b, c \in \mathbb{Q}$ and area n. In other words, we are looking for $a, b, c \in \mathbb{Q}^+$ such that

$$a^2 + b^2 = c^2, \quad \frac{a \cdot b}{2} = n. \tag{1}$$

Definition 1.2 (congruent number) *A natural number $n \in \mathbb{N}$ is called* ***congruent*** *if there is a right triangle with area given by n.*

The problem of whether a given number is a congruent number is called the **congruent number problem**.

Remark 1.3 *Note that if n is a congruent number, $s^2 n$ is a congruent number, too, for $s \in \mathbb{N}$ since we may just multiply the sides of the triangle by s. Therefore, it suffices to reduce the congruent number problem to square-free numbers.*

Example 1.4 *The Pythagorean triple $(3, 4, 5)$ shows that $n = 6$ is a congruent number since $\frac{3 \cdot 4}{2} = 6$.*
It is noteworthy that we may apply Fermat's principle of infinite descent to prove that 1,2 and 3 are not congruent numbers, as will be elaborated in in section 4 . In particular, there is no perfect square amongst congruent numbers since else the corresponding rational triangle would be similar to one with area equal to 1, contradicting that 1 is not a congruent number.

Example 1.5 *The numbers that solve a congruent number problem for a given integer n are much harder to find than one might expect. For example, a solution to the congruent number problem for $n = 7$ is given by*

$$\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right).$$

To answer this question, we may use elliptic curves. Indeed, equation (1) may be rewritten in the following way: Let a, b, c fulfill (1) and define x, y by

$$x := \frac{n(a+c)}{b}, \quad y := \frac{2n^2(a+c)}{b^2}, \tag{2}$$

which are well-defined since $n \neq 0$ implies $b \neq 0$ by (1). Additionally, $y \neq 0$ since else $a = -c$, which would imply that $b = 0$, contradicting (1) for $n \neq 0$.
These numbers fulfil a cubic equation.

Proposition 1.6 *For x, y as above, we have*

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

Proof We have that

$$\begin{aligned} x^3 - n^2 x &= \frac{n^3(a+c)^3}{b^3} - n^2 \frac{n(a+c)}{b} = \frac{n^3(a+c)^3 - n^3 b^2 (a+c)}{b^3} \\ &= \frac{n^3(a+c)}{b^3}((a+c)^2 - b^2). \end{aligned}$$

Since a, b, c fulfill (1), we have that $b^2 = c^2 - a^2 = (c+a)(c-a)$ and hence

$$x^3 - n^2 x = \frac{n^3(a+c)^2}{b^3}\left((a+c) - (c-a)\right) = \frac{2an^3}{b^3}(a+c)^2.$$

using again (1), we use derive $a = \frac{2n}{b}$ from $\frac{ab}{2} = n$ and finally get

$$x^3 - n^2 x = \frac{2n^4}{b^4}(a+c)^2 = y^2. \qquad \square$$

Remark 1.7 *The discriminant of* $y^2 = x^3 - n^2 x =: x^3 + px + q$ *is equal to*

$$\Delta = -4p^3 - 27q^2 = -4 \cdot (-n^6) = 4n^6,$$

so the curve defined by this equation is non-singular.

Definition 1.8 (elliptic curve E_n) *The elliptic curve defined by*

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

is called E_n*.*

On the other hand, we may define for $(x, y), y \neq 0$ on E_n the triple

$$(a, b, c) := \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right), \tag{3}$$

which fulfills (1). Through this construction, we have shown (up to showing that the above maps are inverse to each other) that we may rewrite the congruent number problem to a problem about elliptic curves.

Proposition 1.9 $n \in \mathbb{N}$ *is a congruent number if and only if the elliptic curve* E_n *contains a rational point* $(x, y), y \neq 0$*.*

Before introducing the Birch and Swinnterton-Dyer conjecture, which, together with Tunnel's theorem, would answer the congruent number problem, let us recall some important definitions and theorems for this talk.
Let E be the elliptic curve with a rational point at infinity, then it is given by the equation

$$y^2 = x^3 + ax^2 + bx + c \tag{4}$$

for $a, b, c \in \mathbb{Z}$.
We denote by $E(\mathbb{Q})$ the set of rational points on E, which is an abelian group. We want to study this group further to answer the congruent number theorem. Here, Mordell's theorem comes in handy:

Theorem 1.10 (Mordell) *If the elliptic curve* E *has a rational point, then the group of rational points is finitely generated.*

Since we chose E to have a rational point, we thus conclude that the group $E(\mathbb{Q})$ is finitely generated, and by the fundamental theorem of finitely generated abelian groups, we may write

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{free}} \oplus E(\mathbb{Q})_{\text{finite}}$$

where $E(\mathbb{Q})_{\text{free}}$ is the free and $E(\mathbb{Q})_{\text{finite}}$ is the torsion part of the abelian group $E(\mathbb{Q})$.

Since $E(\mathbb{Q})_{\text{finite}}$ is a finite abelian group, its elements are of finite order. Hence, $E(\mathbb{Q})_{\text{finite}}$ consists of the rational points of finite order on E. Mazur's theorem (see talk 2) classifies $E(\mathbb{Q})_{\text{finite}}$ up to isomorphism, so we restrict our attention to the free part of $E(\mathbb{Q})$.
We know that

$$E(\mathbb{Q})_{\text{free}} \cong \mathbb{Z}^{r_E}$$

where r_E is called the **rank** of E. This allows us to give a criterion for when there are finitely many and when there are infinitely many rational points on an elliptic curve E. More precisely:

$$r_E = 0 \iff |E(\mathbb{Q})| < \infty$$
$$r_E > 0 \iff |E(\mathbb{Q})| = +\infty.$$

Thus, we see that describing the set $E(\mathbb{Q})$ works through finding the rank of the elliptic curve r_E. This is where the Birch and Swinnerton-Dyer conjecture comes into play.

2 The Birch and Swinnerton-Dyer Conjecture

Let E be an elliptic curve defined by equation (4). The BSD conjecture yields an analytic tool to determine whether $r_E = 0$ or $r_E > 0$.
For this, let p be a prime and define

$$N_p := |\{x, y \in \{0, \dots, p-1\} \mid y^2 \equiv x^3 + ax^2 + bx + c \mod p\}| + 1,$$

where the $+1$ arises from the neutral element. Birch and Swinnerton-Dyer found the following equivalence through experiments.

Conjecture (weak Birch Swinnerton-Dyer) For an elliptic curve E given by (4), it holds that

$$r_E > 0 \iff \prod_{p \text{ prime}, p \leq x} \frac{N_p}{p} \xrightarrow[x \to \infty]{} \infty. \tag{5}$$

□

While this conjecture helps us know whether there are infinitely many rational points on an elliptic curve E, it still does not explicitly answer how to calculate the rank r_E. For this, we need the stronger version of the BSD conjecture. For this, let $L(E, s)$ be the L-function associated to E for $Re(s) > \frac{3}{2}$ given by

$$L(E, s) := \prod_{p \text{ prim}, p \not| 2\Delta} \frac{1}{1 - (p + 1 - N_p)p^{-s} + p^{1-2s}}.$$

Then, supposing that $L(E, s)$ can be extended to $s = 1$, we could write

$$\begin{aligned} L(E, 1) &= \prod_{p \text{ prime}, p \not| 2\Delta} \frac{1}{1 - (p + 1 - N_p)p^{-1} + p^{-1}} \\ &= \prod_{p \text{ prime}, p \not| 2\Delta} \frac{p}{N_p} = \left(\prod_{p \text{ prime}, p | 2\Delta} \frac{p}{N_p} \right)^{-1} \prod_{p \text{ prime}} \frac{p}{N_p}. \end{aligned}$$

Therefore, assuming that $L(E,s)$ can be extended to $s=1$, (5) can be formally rewritten to

$$r_E > 0 \Longleftrightarrow L(E,1) = 0. \tag{6}$$

This leads us to the strong Birch Swinnerton-Dyer conjecture.

Conjecture (strong Birch Swinnerton-Dyer) For an elliptic curve E given by (4), we have

- The L-function $L(E,s)$ can be extended holomorphically to the whole $\mathbb{C}$. In particular, $L(E,1)$ is defined.
- The order of vanishing $\mathrm{ord}_{s=1}L(E,s)$ of $L(E,s)$ at $s=1$ fulfills the equation

$$r_E = \mathrm{ord}_{s=1}L(E,s) \tag{7}$$

and there is an explicit formula, which relates the first non-vanishing coefficient of the Taylor series of $L(E,s)$ around $s=1$ with the arithmetic of E. □

Current state of the proof

- Coates and Wiles: proved that for elliptic curves $E \mid \mathbb{Q}$ with complex multiplication and $L_E(1) \neq 0$, it follows that $r_E = 0$.
- Gross and Zagier: proved that for modular curves $E \mid \mathbb{Q}$ with $L_E(1) = 0$ but $L'_E(1) \neq 0$ there are infinitely many rational points, i.e. $r_E > 0$.
- Kolyvagin: proved that if $L_E(1) \neq 0$, then $r_E = 0$. Additionally, if $L_E(1)$ and $L'_E(1) \neq 0$, then $r_E = 1$.

3 Points of Finite Order of E_n

In this section, we will prove that the only points of finite order in E_n are $\mathcal{O}$, $(\pm n, 0)$ and $(0,0)$, i.e. $E_n(\mathbb{Q})_{finite}$ contains only 4 elements. Thus if for $n \in \mathbb{N}$ there are $a,b,c \in \mathbb{Q}^+$ such that $a^2+b^2=c^2$ and $ab/2 = n$, i.e. n is congruent, then from the map defined in section 1 we get a rational point on E_n with $y \neq 0$, hence a point in $E_n(\mathbb{Q})_{free}$. Viceversa, if there is a point of infinite order in $E_n(\mathbb{Q})$, then n is a congruent number.

For the proof, first recall the following theorem from the fifth talk of this seminar:

Theorem 3.1 (Reduction Modulo p Theorem) *Let $E: y^2 = x^3 + ax^2 + bx + c$ be a non-singular cubic curve with $a,b,c \in \mathbb{Z}$ and let D be the discriminant. Let p be a prime and consider the reduction modulo p map of the torsion group:*

$$\varphi : E(\mathbb{Q})_{finite} \to \tilde{E}(\mathbb{F}_p)$$
$$Q \mapsto \tilde{Q} = \begin{cases} (\overline{x}, \overline{y}) & if\ Q = (x,y) \\ \overline{\mathcal{O}} & if\ Q = \mathcal{O} \end{cases}$$

If $p \nmid 2D$, then $\varphi : E(\mathbb{Q})_{finite} \to \tilde{E}(\mathbb{F}_p)$ is an isomorphism of $E(\mathbb{Q})_{finite}$ onto a subgroup of $\tilde{E}(\mathbb{F}_p)$. In this case, $\tilde{E}$ is an elliptic curve, and we call this a good reduction. Moreover $\#E(\mathbb{Q})_{finite} \mid \#\tilde{E}(\mathbb{F}_p)$ since it is isomorph to one of its subgroups.

We consider the elliptic curve $E_n : y^2 = f(x) = x^3 - n^2x$ with determinant $D = 4n^6$. For any prime p not dividing $4n^6$, which is equivalent to $p \nmid 2n$, we get a good reduction modulo p of E_n. We call primes of this kind *good primes*.

Proposition 3.2 *Let p be a good prime with $p \equiv 3$ mod 4, then $\#\tilde{E_n}(\mathbb{F}_p) = p + 1$.*

Proof First of all $\tilde{E_n}(\mathbb{F}_p)$ contains the neutral element $\overline{\mathcal{O}}$ and three points of order 2, i.e. $(\overline{0}, \overline{0})$ and $(\pm\overline{n}, \overline{0})$. Since p is a good prime, these are four different elements of the curve $\tilde{E_n}$. We now consider all $\overline{x} \in \mathbb{F}_p$ with $\overline{x} \neq \overline{0}, \pm\overline{n}$ and we arrange these $p-3$ $\overline{x}$'s in $\frac{p-3}{2}$ pairs $\{\overline{x}, -\overline{x}\}$. Since $f(x)$ is an odd function, i.e. $f(-x) = -f(x)$, we get $f(x)f(-x) = (-1) \cdot f(x)^2$. Recall the following properties of squares in $\mathbb{F}_p$:

- For p prime, $p \equiv 3$ mod 4, -1 is not a square modulo p
- The set of squares in F_p is is a subgroup of index 2

It follows that $(-1) \cdot f(x)^2$ is not a square modulo p, hence exactly one between $f(x)$ and $f(-x)$ is a square modulo p, i.e. there is an element $\overline{y} \in \mathbb{F}_p$ with $\overline{y}^2 = \overline{f(x)}$ or $\overline{y}^2 = \overline{f(-x)}$. Thus for any pair $\{\overline{x}, -\overline{x}\}$ we get exactly two distinct points of $\tilde{E_n}(\mathbb{F}_p)$, either $(\overline{x}, \pm\overline{y})$ or $(-\overline{x}, \pm\overline{y})$. From the $\frac{p-3}{2}$ pairs, we get in total $p-3$ points, and together with the four points at the beginning, we get $\#\tilde{E_n}(\mathbb{F}_p) = p + 1$. □

We will now prove that the only points of finite orders in E_n are $\mathcal{O}$, $(\pm n, 0)$ and $(0, 0)$ by contradiction using the following theorem:

Theorem 3.3 (Dirichlet prime number theorem) *Let $a, b \in \mathbb{N}$ coprime and consider the arithmetic progression $\{a, a+b, a+2b, \dots\}$. This sequence contains infinitely many primes.*

Proposition 3.4 $E_n(\mathbb{Q})_{finite} = \{\mathcal{O}, (0, 0), (\pm n, 0)\}$

Proof (by contradiction) First of all the only elements of $E_n(\mathbb{Q})$ of order 2 are $(0, 0)$, $(\pm n, 0)$, since the y-coordinate must be zero. Hence, if $E_n(\mathbb{Q})_{finite}$ contains some other element, it must have order greater than 2. Suppose this is true, then there exists a point Q in $E_n(\mathbb{Q})_{finite}$ either of odd order m or of order 4. In the first case Q generates a subgroup of size m, while in the second case $\{\mathcal{O}, (0, 0), (\pm n, 0), Q, Q + (0, 0), Q + (\pm n, 0)\}$ is a subgroup of size 8. Thus either $m \mid \#E_n(\mathbb{Q})_{finite}$ for m odd or $8 \mid \#E_n(\mathbb{Q})_{finite}$.

Recall from the **Reduction Modulo p Theorem** together with **proposition 3.2** that for any good prime p, i.e. $p \nmid 2n$, congruent to 3 modulo 4 it holds $\#E_n(\mathbb{Q})_{finite}$ divides $\#\tilde{E_n}(\mathbb{F}_p) = p + 1$. Hence either $m \mid p + 1$ or $8 \mid p + 1$. Let's now go through all possible cases:

1. m odd, $3 \nmid m$: consider all good primes of the form $p = 3 + k \cdot 4m$. Since $p \equiv 3$ mod 4, we know from above that $m \mid p + 1$, i.e. $p \equiv -1$ mod m. But from construction it holds $p \equiv 3$ mod m, hence $-1 \equiv 3$ mod m, which means $m = 2$ or $m = 4$, a contradiction. It follows that all primes of the form $p = 3 + k \cdot 4m$ are not good primes, i.e. $p \mid 2n$. But this would mean that there are finitely many primes of this form, which is a contradiction to **Dirichlet prime number theorem** since $4m$ and 3 are coprime.

2. m odd, $3 \mid m$, hence w.l.o.g. $m = 3$: consider all good primes of the form $p = 7 + k \cdot 12$. Since $p \equiv 3 \bmod 4$, similarly to above, we get $-1 \equiv p \equiv 1 \bmod 3$, which is a contradiction. Since 7 and 12 are coprime, we arrive at the same conclusion as above.

3. $8 \mid \#E_n(\mathbb{Q})_{finite}$: consider all good primes of the form $p = 3 + k \cdot 8$. Since $p \equiv 3 \bmod 4$, we obtain $3 \equiv p \equiv -1 \bmod 8$, which is a contradiction. Since 3 and 8 are coprime, we arrive at the same conclusion as above.

From these contradictions, it follows that there is no point in $E_n(\mathbb{Q})_{finite}$ of order greater than 2, and we conclude that $E_n(\mathbb{Q})_{finite} = \{\mathcal{O}, (0,0), (\pm n, 0)\}$. □

Hence, a natural number n is congruent if and only if there is a rational point (x, y) of the curve E_n with $y \neq 0$, which is equivalent to $rank(E_n(\mathbb{Q}) > 0$. Moreover, if the Birch and Swinnerton-Dyer Conjecture proves to be true for elliptic curves of this kind, this is equivalent to $L(E_n, 1) = 0$.

4 Tunnel's Theorem

Before stating Tunnel's theorem, we look at a couple of methods one can currently use to help determine whether a natural number is congruent or not.

First of all, there is a simple algorithm that will eventually list all congruent numbers: recall that for any primitive Pythagorean triple (a, b, c) (w.l.o.g. b is even), there exist $x > y > 0$ coprime integers, not both odd, such that $a = x^2 - y^2$, $b = 2xy$, $c = x^2 + y^2$, and vice versa for any $x > y > 0$ coprime integers, not both odd, (a, b, c) is a primitive Pythagorean triple. Hence, by listing all pair $(x, y) \in \mathbb{N}$ with $x > y > 0$ coprime, not both odd and the corresponding Pythagorean triple (a, b, c), we can compute the area of the triangle $\frac{ab}{2} = xy(x + y)(x - y)$. By removing the square from the factorization, we get a congruent square-free natural number. Unfortunately, with this method, we cannot tell if a natural number n is not congruent or if we have not waited long enough.

Another possibility is using Fermat's method of infinite descent: for example, to prove whether 1 is congruent or not is the same as proving the existence of an integer right triangle with square area. Suppose (a, b, c) is a primitive Pythagorean triple with square area, then one can check that it is always possible to derive a smaller Pythagorean triple with square area. Thus, we would get an infinite strictly decreasing sequence of integer squares, which is not possible; hence, we conclude that 1 is not congruent. Using the same idea, one can show that neither 2 nor 3 are congruent.

We now look at the last equivalence shown in the abstract, namely the relation between the L-function of an elliptic form E_n, for n, a square-free natural number, and Tunnell's product of theta-functions. We are not going to discuss the proof since it goes beyond the topics of this seminar (you can find more about this in [3, Chapter 4]). We are more interested in what this implies for congruent square-free natural numbers, that is the following theorem:

Theorem 4.1 (Tunnel 1983) *Let n be a square-free natural number and consider the following values:*

$$A_n := \#\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\}$$
$$B_n := \#\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\}$$
$$C_n := \#\{(x,y,z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 64z^2\}$$
$$D_n := \#\{(x,y,z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 16z^2\}$$

Then the following statements are true:

1. *If n is an odd congruent number, then $2A_n = B_n$*
2. *If n is an even congruent number, then $2C_n = D_n$*

Moreover, if the Birch and Swinnerton-Dyer Conjecture proves to be true for the curves $E_n : y^2 = x^3 - n^2x$, these equalities are sufficient to determine whether n is congruent.

Note that for any of the values defined in the theorem above, the entries of an integer solution of the respective quadratic equation are bounded in absolute value by $\sqrt{n}$. Hence, should the BSD Conjecture be proven true, we would be able to determine in a finite time whether any natural number is congruent or not.

References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (1992).

[2] J. Kramer, *Die Vermutung von Birch und Swinnerton-Dyer*, Birkhäuser Verlag (2002).

[3] N.I. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer (1993)