The Birch and Swinnerton-Dyer Conjecture

Stefan Moser

Date of the talk

Introduction

In this paper I will first introduce the definition of a congruent number and how it relates to elliptic curves. This will then lead us to the Birch and Swinnerton-Dyer Conjecture with will gives an alternate definition of a congruent in the field of elliptic curves. Finally I will state Tunnells theorem as a variant of the conjecture which will gives us an actual algorith to test if a number is congruent number.

1 The Congruent Number Problem

Let n be a natural number. Then n is said to be congruent if there exits a right triangle with rational sides and area n. More formally:
Definiton 1.1. *n is congurent if there exist positive integers a,b and c st.*

$$a^2 + b^2 = c^2 \text{ and } \frac{ab}{2} = n \tag{1}$$

Now how does this relate to elliptic curves? For this we first note that the equations in (1) can be stated without requiring a, b, c to be positive integers. Instead we look at all real solutions of these equations.
Given a triple (a, b, c) that satisfies (1) we can define x, y by

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

Note that $n \neq 0$ implies $b \neq 0$ by (1) so x and y are well defined. Furthermore $y \neq 0$ since otherwise $a = -c$ and so again by (1) that $a^2 + b^2 = a^2$ but $b \neq 0$.
Now it is an easy calculation to see that these x and y satisfy a cubic equation.
Proposition 1.1. *For x and y as above we have the following equation:*

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

Proof. By plugging 2 into the RHS we get

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

Note that by 1 we have $b^2 = c^2 - a^2 = (c+a)(c-a)$. Thus

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

We can use 1 again to simplify further. From $\frac{ab}{2} = n$ we get $a = \frac{2n}{b}$ and hence

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

□

Remark 1.1. *The discriminant of this cubic equation is $4n^6$. Thus the elliptic curve given by the equation $y^2 = x^3 - n^2x$ is non-singular. We denote the resulting elliptic curve by E_n.*

Conversly, given a point $(x, y), y \neq 0$ on E_n we can define $(a, b, c) = \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right)$. For these a, b, c we have the following:

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

Hence we find a triple (a, b, c) satisfying (1).

It is an easy calculation to show that these maps are inverse to eachother. Moreover since both maps are defined by rational equations they map rational numbers to rational numbers. We conclude:

Proposition 1.2. *n is a congruent number if and only if E_n contains a rational point $(x, y), y \neq 0$.*

We thus translated the definition of a congruent number into the language of elliptic curves. We can now use the tools we gathered so far.

In the next section I will discuss the Birch and Swinnerton-Dyer conjecture and how it could give an answer to the congruent number problem.

2 The Birch and Swinnerton-Dyer conjecture

Before we start let us recall Mordell's theorem that the group of rational points of an elliptic curve is finitely generated. Denote this group by $E(\mathbb{Q})$. By the

fundamental theorem of finitely generated abelian groups we know that this group is isomorphic to $\mathbb{Z}^r \bigoplus E(\mathbb{Q})_{tors}$ where $E(\mathbb{Q})_{tors}$ consists of all the elements of finite order called the torsion group of $E(\mathbb{Q})$. The integer r in this decomposition is well defined. It is called the rank of the elliptic curve E. The main question now is whether it is possilbe to give a critrion for the rank to be positive or if there is even an explicit way to calculate the rank for a given elliptic curve. That is exactly what the conjecture tries to answer.

For this we consider for a given prime p the number of solutions of E modulo p, explicitly if E is given in Weierstrass normal form by $y^2 = x^3 + ax^2 + bx + c$ we consider $N_p := \left| \left\{ x, y \in \{0, 1, ..., p-1\} \left| y^2 \equiv x^3 + ax^2 + bx + c \,(\, mod\, p) \right.\right\} \right| + 1$ where the $+1$ comes from the neutral element.

B. Birch and P. Swinnerton-Dyer calculated nummerically the numbers $\prod_{\substack{p\, prime \\ p \leq x}} \frac{N_p}{p}$ for big x. This lead them to their famous conjecture:

Conjecture 2.1. *rank(E)* $> 0 \iff \prod_{\substack{p\, prime \\ p \leq x}} \frac{N_p}{p} \to \infty$ *for* $x \to \infty$

This is called the weak form of the BSD conjecture. This gives us a tool to decide whether a given elliptic curve has positive rank or not and equivalently if the elliptic curve has infinitely many rational points or not. Still it does not say something about how the rank can me calculated. But Birch and Swinnerton-Dyer also stated a stronger version of this conjecture where they give an explicit formula of the rank. Unfortunately this will involve some analytical number theory, namely the theory of L-functions so I will only talk about this briefly and leave the details to the reader.

For a given elliptic curve E as above we consider the L-function $L(E, s) = \prod_{\substack{p\, prime \\ p \nmid 2\Delta}} \frac{1}{1-(p+1-N_p)p^{-s}+p^{1-2s}}$. This L-function is definied for all $s \in \mathbb{C}$ with $Re(s) > 3/2$. Now suppose that this function is definied for $s = 1$. Then we would have

$$\begin{aligned} L(E,1) &= \prod_{\substack{p\, prime \\ p \nmid 2\Delta}} \frac{1}{1-(p+1-N_p)p^{-1}+p^{-1}} \\ &= \prod_{\substack{p\, prime \\ p \nmid 2\Delta}} \frac{p}{N_p} = \left(\prod_{\substack{p\, prime \\ p | 2\Delta}} \frac{p}{N_p} \right)^{-1} \prod_{p\, prime} \frac{p}{N_p} \end{aligned}$$

Note that we can do this since $N_p \geq 1$ by definition. So if this L-function of E is definied at $s = 1$ we see that the conjecture can be restated as

$$rank(E) > 0 \iff L(E, 1) = 0$$

Now that we work in the subject of arithemtic number theory we can ask if this L-function can be extended analytically. This leads us to the stronger version of the BSD-conjecture:

Conjecture 2.2. *For an elliptic curve E the corresponding L-function as above can be extended to a holomorphic function on $\mathbb{C}$, in particular its value at $s = 1$ is defined. There the rank can be calculated by*

$$rank(E) = ord_{s=1}L(E, s)$$

Clearly the strong version implies the weak version.

The conjecture has been proven for some special cases, assuming some more explicit properties of the elliptic curve.

Now that we know how this conjectures could give us some answers on how to calculate the rank of an elliptic curve I want to go back to see how the rank of an elliptic curves can give us an answer whether a given number is congruent or not.

3 The rank of an elliptic curve and congruent numbers

In this section we go back to our elliptic curve E_n given by the equation $y^2 = x^3 - n^2x$. We can actually compute the torsion subgroup of this curve, which we will do in this section.
Remember that the curve has discriminant $4n^6$ so we get a good reduction modulo p for every odd prime p that is not a prime divisor of n. Let us denote the set of bad primes by $\mathcal{P}$. That is $\mathcal{P} = \{p \, prime \mid p \mid 2n\}$. It will be important later that this set is finite.

Now we will show the following:

Proposition 3.1. *Let p be a good prime that satisfies $p \equiv 3 \, (mod \, p)$. Then we have $E_n(\mathbb{F}_p) = p + 1$.*

This explicit number of points helps us later calculating the torsion subgroup. Before I proof this we will need two facts about squares in finite fields. The first one is called the "Euler criterion" which shows if a given number is a square or not. The other one will show how squares and non-squares resp. behave under multiplication.

We start with the Euler criterion which I will state without proof.

Theorem 3.1 (Euler criterion)**.** *Let p be an odd prime and $a \not\equiv 0 \, (mod \, p)$. We have the following characterisation:*

$$a^{\frac{p-1}{2}} \equiv 1 \qquad \textit{iff } a \textit{ is a square modulo } p$$
$$a^{\frac{p-1}{2}} \equiv -1 \qquad \textit{iff } a \textit{ is not a square modulo } p$$

Here is where we will need the assumption that $p \equiv 3 \ (mod\ p)$. Because for such p we have the following:

Corollary 3.1. *If $p \equiv 3 \ (mod\ p)$ then -1 is not a square in $\mathbb{F}_p^*$.*

Proof. By assumption $\exists k \in \mathbb{Z} : p = 4k + 3$. We can plug this into the formula in the Euler criterion to see

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1$$

Hence by the Euler criterion -1 is not a square in $\mathbb{F}_p^*$. □

We now need another fact about squares in $\mathbb{F}_p^*$.

Proposition 3.2. *Let p be an odd prime. Then the set of squares in $\mathbb{F}_p$ form a subgroup of index 2.*

Proof. Clearly the set of squares form a subgroup. Now consider the endomorphism $\phi : \mathbb{F}_p^* \to \mathbb{F}_p^*,\ x \mapsto x^2$. The image of ϕ is exactly the set of squares, let us denote it by S. The kernel of ϕ is $\{1, -1\}$. So by the homomorphism theroem we have $S \cong \mathbb{F}_p^*/\{1, -1\}$. Then by Lagrange's theorem we have

$$\left[\mathbb{F}_p^* : S\right] = \frac{|\mathbb{F}_p^*|}{|S|} = |\mathbb{F}_p^*|\frac{|\{1, -1\}|}{|\mathbb{F}_p^*|} = 2.$$

□

From this we can deduce the behaviour of squares in $\mathbb{F}_p^*$ under multiplication.

Corollary 3.2. *Let a, b be two elements of $\mathbb{F}_p^*$. We then have:*

i) If a and b are squares then so is ab.

ii) If neither a nor b is a square then ab is a square.

iii) If either a or b is a square then ab is not a square.

Proof. i) this is trivial

ii) Since both a and b are not squares we know that $aS = bS$ because the set of squares has index 2 in $\mathbb{F}_p^*$. Hence

$$(ab)S = abS^2 = (aS)(bS) = (aS)^2 = S$$

So we see that $ab \in S$ ie. it is a square.

iii) wlog a is a square but b is not. We then have the following:

$$(ab)S = b(aS) = bS \neq S$$

Hence ab is not a square.

□

Recall that the points of E_n satisfy $y^2 = x^3 - n^2x$. Let $f(x) := x^3 - n^2x$. Now to find points on E_n we look at all the possible values for $f(x)$ and test if they are a square in $\mathbb{F}_p$ or not ie. if there is a y st. $y^2 = f(x)$. This will be our strategy for the proof of the next theorem.

Theorem 3.2. *Let $p \notin \mathcal{P}$ and $p \equiv 3$ (mod 4) be a prime. Then we have:*

$$E_n(\mathbb{F}_p) = p + 1$$

Proof. The first points on E_n we consider are the ones of order 2. Because for these we have $f(x) = 0$. Writing $f(x) = x(x+n)(x-n)$ we find that these points are $(0,0), (n,0)$ and $(-n,0)$. So now we consider the case that $f(x) \neq 0$. Since in this case also $y \neq 0$ we can restrict us to $\mathbb{F}_p^*$.

Since $|\mathbb{F}_p^*| = p - 1$ and p is odd we can group the elements in pairs $\{x, -x\}$. Since we want $f(x) \neq 0$ we exclude the pair $\{n, -n\}$. That leaves us with $\frac{p-3}{2}$ pairs.

Next up we note that $f(-x) = -f(x)$. We therefore see that $f(x)f(-x) = -f(x)^2 = (-1)f(x)^2$. Since we have shown that -1 is not a square in $\mathbb{F}_p^*$ and $f(x)^2$ obviously is a square we deduce from corollary 3.2 that either $f(x)$ or $f(-x)$ is a square. So each pair $\{x, -x\}$ produces exactly 2 squares. This means that for each pair $\{x, -x\}$ we get exactly 2 points on E_n. Namely either the points $(x, \pm\sqrt{f(x)})$ or $(-x, \pm\sqrt{f(-x)})$. So for the $\frac{p-3}{2}$ pairs we get $p-3$ points. Together with the points $(0,0), (n,0), (-n,0)$ and $\mathcal{O}$ we get $p+1$ points on E_n.

□

The knowledge of the solutions modulo p together with the "Reduction modulo p theorem" will allow us to proof the following fact:

Proposition 3.3. $E_n(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$

Recall that the "Reduction modulo p theorem tells us that if p is a good prime of E i.e. $p \nmid 2\Delta$ then $E(\mathbb{Q})_{tors} \mid E(\mathbb{F}_p)$.

For the proof we will need one last theorem. It is the famous Dirichlet theorem about primes in arithmetic progressions. I will state thes theorem without proof.

Theorem 3.3 (Dirichlet)**.** *Let a and d be coprime. Consider the arithmetic progression $a, a+d, a+2d, \ldots$. This sequence contains infinitely many primes.*

The idea of the proof of theorem 3.3 is to find such sequences where every prime in this sequence must belong to $\mathcal{P}$. Since $\mathcal{P}$ is finite we will get a contradiction to heorem 3.3.

Proof of proposition 3.3. Suppose by contradiction that there exits a point in $E_n(\mathbb{Q})_{tors}$ of order higher than 2. Suppose first that it has order m for m odd. Then we can consider the subgroup generated by this point, hence we have that $m \mid E_n(\mathbb{Q})_{tors}$. Suppose otherwise that $E_n(\mathbb{Q})_{tors}$ has no points of odd order. Denote the point of order > 2 by Q. Since Q by assumption has even order we can denote the order by $2k$ for some k. But k must be even as well since otherwise the point $2Q$ had odd order k. So we can write $k = 2l$ for some l and hence Q has order $4l$. We get that the point lQ has order 4. So without loss of generality we can assume that the point Q has order 4.

Now we can consider the subgroup H generated by Q and our points of order 2. Since Q has order 4 we know that $2Q$ has order 2. Since we know all points of order 2 we have that $2Q \in \{(0,0), (\pm n, 0)\}$. We get that $H = \{\mathcal{O}, (0,0), (\pm n, 0), Q, Q + (0,0), Q + (\pm n, 0)\}$. We therefore find $m := |H| = 8$ with $m \mid E_n(\mathbb{Q})_{tors}$.

We conclude that we can find either an m odd or $m = 8$ such that $m \mid E_n(\mathbb{Q})_{tors}$. Let us go through all possible cases:

i) m odd, $3 \nmid m$: Consider the primes of the form $p = 4km + 3$ for $p \notin \mathcal{P}$. Since p is a good prime we know that $E_n(\mathbb{Q})_{tors} \mid E_n(\mathbb{F}_p)$ and consecuently that $m \mid E_n(\mathbb{F}_p)$. Since $p \equiv 3$ $(mod\ 4)$ we know that $E_n(\mathbb{F}_p) = p + 1$ by Theorem 3.2. Hence $m|p + 1$ or equivalently $p \equiv -1 \pmod{m}$. But we also have that $p \equiv 3 \pmod{m}$. But $3 \equiv -1 \pmod{m}$ is only possible for $m = 2, 4$, a contradiction. Thus all primes of the form $p = 4km + 3$ have to be in the finite set P. But by assumption $(4m, 3) = 1$ so by Theorem 3.3 there are infinitely many primes of this form. This leads to our desired contradiction.

ii) m odd, $3 \mid m$: Consider the primes of the form $p = 12k + 7$ for $p \notin \mathcal{P}$. Note that $p \equiv 3 \pmod 4$. By the same argument as above we have that $p \equiv -1 \pmod{m}$. Since $3 \mid m$ this implies that $p \equiv -1 \pmod 3$. We therefore get that $p \equiv 1 \equiv -1 \pmod 3$, a contradiction. Hence all primes of this form must be contained in the set $\mathcal{P}$. But (12,7)=1 so this contradicts Theorem 3.3.

iii) $m = 8$: Consider the primes of the form $p = 8k + 3$ for $p \notin \mathcal{P}$. Again $p \equiv 3 \pmod 4$ so $p \equiv -1 \pmod{m}$. Since $m = 8$ we have that $p \equiv 3 \equiv -1 \pmod 8$, a contradiction. Since (8,3)=1 we get a contradiction as above.

This contradiction shows us that there are no points of order > 2 and we can conclude the proposition.

□

This proposition is what relates the problem of finding a congruent number with the rank of the curve E_n. Namely we have the following corollary:

Corollary 3.3. *A rational point $P = (x, y)$ on E_n has finite order if and only if $y = 0$.*

Proof. Proposition 3.3 tells us that the only points of finite order are those of order 2. And by Nagell-Lutz this is equivalent to having $y = 0$. □

Thus we see that finding a rational point $P = (x, y)$ with $y \neq 0$ is the same as finding a point of infinite order. Hence Proposition 1.2 can be restated as follows:

Proposition 3.4. *n is a congruent number if and only if E_n has positive rank.*

This proposition is exactly what connects the problem of finding a congrent number with the BS-D conjecture. Since we only need to know if the rank is positive or not even the weak form of the BS-D conjecture is enough to give an explicit criteria for a number to be congruent. For that suppose that the weak for of the BS-D conjecture was true, then we had the following proposition:

Proposition 3.5. *n is a congruent number if and only if $\prod_{\substack{p \text{ prime} \\ p \leq x}} \frac{N_p}{p} \to \infty$ for $x \to \infty$.*

If the strong version was true, we could give another criteria for a number to be congruent. Namely

Proposition 3.6. *n is a congruent number if and only if $L(E_n, 1) = 0$.*

These criterias are still not easy to show, especially in a finite amount of time. So in the next section we take a look at "Tunnell's theorem" which will give us an actual algorith to show that a number is congruent or not.

4 Tunnell's theorem

For this theorem we have to make the assumption that n is a square free integer. Luckily this assumption does not restrict us at all. This follows from the following lemma:

Lemma 4.1. *Let n be an integer and $s \in \mathbb{Q}$. Then n is congruent iff $s^2 n$ is congruent.*

Proof. Suppose n is congruent. Hence we find $a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $\frac{ab}{2} = n$. But then also $sa, sb, sc \in \mathbb{Q}$ with:

$$(sa)^2 + (sb)^2 = s^2(a^2 + b^2) = s^2c^2 = (sc)^2$$
$$\frac{(sa)(sb)}{2} = s^2\frac{ab}{2} = s^2 n$$

Hence $s^2 n$ is a congruent number by definition. For the opposite direction we note that $n = (s^{-1})^2(s^2 n)$ so the same argument applies. □

Now suppose we are given an integer n. We can write $n = s^2 n'$ such that $s \in \mathbb{Z}$ and n' is square free. Then by the lemma above n is congruent if and only if n' is congruent. So to find congruent numbers it suffices to consider all square free integers.

For Tunnell's theorem we consider the following sets:
$A_n = |\{(x, y, z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 32z^2\}|$,
$B_n = |\{(x, y, z) \in \mathbb{Z}^3 \mid n = 2x^2 + y^2 + 8z^2\}|$,
$C_n = |\{(x, y, z) \in \mathbb{Z}^3 \mid n = 8x^2 + 2y^2 + 64z^2\}|$,
$D_n = |\{(x, y, z) \in \mathbb{Z}^3 \mid n = 8x^2 + 2y^2 + 16z^2\}|$.

Remark 4.1. *Even though the set $\mathbb{Z}^3$ is infinite we actually only have a finite amount of possibilites for (x, y, z). To see this consider any of these sets above and note that the right hand sides only consist of squares. We therefore get that the only possibilites for x, y and z are in the range $[-\sqrt{n}, \sqrt{n}]$.*

Now we can state Tunnell's theorem:

Theorem 4.1 (Tunnell)**.** *For n square free let A_n, B_n, C_n, D_n as above and suppose n is a congruent number. If n is odd then $2A_n = B_n$ and if n is even then $2C_n = D_n$.*
Conversly suppose that the weak BS-D conjecture is true for the elliptic curves E_n. Then this condition is not only neccessairy but also sufficient.

This theorem together with remark 4.1 gives us an explicit algorithm to deduce if a given number is congruent that can be solved in a finite amount of time. This is why this theorem is so important, because this theorem can give us a satisfying answer to the question if a given number is congruent or not.
That the theorem requires the weak BS-D conjecture to be true is not surprising by the last two proposition of the last section.

References

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

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