0.1 Introduction

In this talk I shall attempt to introduce some of the main features of the Birch and Swinnerton-Dyer conjecture, (BSD).

The congruent number problem, deciding whether an integer $D$ is the area of a right angle triangle with rational sides, is not easy. It turns out that the problem is equivalent to finding out if a certain elliptic curve has an infinite number of rational points. In 1983 Tunnell found a simple condition for this to be true-dependent upon the truth of the 'weak' BSD. The Birch and Swinnerton-Dyer conjecture was formulated in the 1960s based on computational evidence and is a set of interlinked conjectures about the $L$-function of an abelian variety defined over a global field. A lot of work has been done and some special cases have been established, but the conjecture is still unproved in general.

0.2 Congruent Numbers

Let $D$ be a positive integer without square factors. We say that $D$ is congruent if there exist $a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $D = \frac{ab}{2}$.

Let $u = \frac{a}{c}$ and $v = \frac{b}{c}$. Then finding congruent numbers becomes equivalent to finding rational points on the first quadrant of the unit circle $u^2 + v^2 = 1$.

Let $t = \frac{v}{u+1}$. Then $t^2 + 1 = \frac{2}{u+1}$, so $v = \frac{2t}{t^2+1}$ and since $u^2 + v^2 = 1$, $u = \frac{1-t^2}{t^2+1}$.

Now let $y = \frac{t^2+1}{c}$. Then

$$D = \frac{uv^2}{2} = \frac{c^2t(1-t^2)}{(t^2+1)^2},$$

so

$$Dy^2 = \frac{c^2t(1-t^2)(t^2+1)^2}{c^2} = t - t^3,$$

so our problem has become one of finding rational points on an elliptic curve.

As Mordell proved in 1922, if $E(\mathbb{Q})$ is nonempty it is a finitely generated abelian group and

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})^{\text{tors}},$$

where $r$ is the rank of $E$.

In 1983 Faltings proved Mordell’s conjecture that if the genus of a curve $C$ is at least 2 then $C(\mathbb{Q})$, the group of rational points of $C$, is finite. If the genus of $C$ is 0 then either $C(\mathbb{Q})$ is empty or it is infinite, and this can be determined
by solving a finite number of congruences. If $C$ is an elliptic curve $E$, on the other hand, $E(\mathbb{Q})$ may be either empty, finite or infinite.

**Proposition 1** $D$ is congruent if and only if the rank of $E_D : Dy^2 = t - t^3$ is at least 1.

**Lemma 1** $E_D(\mathbb{Q})_{tors} = \{\infty, (0,0), (\pm1,0)\}$

It is easy to see that none of these points lead to a congruent number, so if $D$ is congruent there must be another rational point and by the lemma it has infinite order so $r \geq 1$.

Suppose that $E$ has an affine model

$$E : y^2 = x^3 + ax + b$$

and discriminant $\Delta$. Let $p$ be a prime and

$$N_p = |\{(x,y) : y^2 \equiv x^3 + ax + b \pmod{p}\}|,$$

$$a_p = p - N_p,$$

$$L(E,s) = \prod_p (1 - a_pp^{-s} + p^{1-2s})^{-1},$$

where the product is taken over primes $p$ not dividing $\Delta$. $L(E,s)$ converges for $Re(s) > 3/2$ and has holomorphic continuation to the whole complex plane. This brings us to the first statement of the Birch and Swinnerton-Dyer conjecture:

**Conjecture 1** The Taylor expansion of $L(E,s)$ at $s = 1$ has the form

$$L(E,s) = c(s - 1)^r + \text{higher order terms, } c \neq 0. \quad (BSD1)$$

If BSD1 holds then clearly $L(E,s) = 0 \iff E(\mathbb{Q})$ is infinite. Coates and Wiles (1977) showed that if $E$ has complex multiplication then $r \geq 1 \Rightarrow L(E,1) = 0$. Kolyvagin (1990) proved that if $L(E,s) = c(s - 1)^m + \text{higher order terms, and } m = 0$ or 1 then the $m = r$. (This result was proved under the assumption that $E$ was modular, before it was discovered that this is true of all elliptic curves.)

In 1983, Tunnell connected this form of BSD with the congruent number problem in a very nice way using the theory of modular forms:

**Theorem 1** Let $D$ be an odd squarefree integer. If $D$ is congruent then

$$|\{(x,y,z \in \mathbb{Z} : 2x^2 + y^2 + 8z^2 = D\}| = 2|\{(x,y,z \in \mathbb{Z} : 2x^2 + y^2 + 32z^2 = D\}| \quad (*)$$

If $2D$ is congruent then

$$|\{(x,y,z \in \mathbb{Z} : 4x^2 + y^2 + 8z^2 = 2D\}| = 2|\{(x,y,z \in \mathbb{Z} : 4x^2 + y^2 + 32z^2 = 2D\}| \quad (**)$$

If $D$ satisfies $(*)$ (resp. $2D$ satisfies $(**)$) and BSD1 is true, then $D$ (resp. $2D$) is congruent.
Let \( q = e^{2\pi i z} \) where \( z \) is a complex variable. A major theorem of Waldspurger says (among other things) that there are functions \( f = \sum a_n q^n, f' = \sum a'_n q^n \) and constants \( c, c' \) such that if \( D \) is an odd squarefree integer,

\[
L(E_D,1) = c a_D^2 \quad \text{and} \quad L(E_{2D},1) = c' a_D'^2,
\]

where \( f, f' \) are modular forms of weight 3/2 and level 128, which satisfy certain other conditions.

Let \( \beta = \int_1^\infty \frac{1}{\sqrt{x^3 - x}} \, dx \),

\[
f_1(z) = \sum_{m,n \in \mathbb{Z}} (-1)^n q^{(4m+1)^2 + 8n^2},
\]

\[
\Theta(z) = \sum_{n=\infty} q^{n^2}.
\]

Tunnells calculated that

\[
f(z) = f_1(z)\Theta(2z), \quad c = \beta \frac{2}{\sqrt{D}},
\]

\[
f'(z) = f_1(z)\Theta(4z), \quad c' = \beta \frac{2}{\sqrt{2D}}.
\]

Equating coefficients of \( q^D \) gives the theorem.

Although it is ‘incredibly difficult to say anything precise about \( L(E,s) \)’ (William Stein), it is not too hard to check (with a computer) if \( L(E,1) = 0 \).

At \( s = 1 \) we have the rapidly converging sum

\[
L(E,1) = (1 + \epsilon) \sum_{n=1}^{\infty} \frac{b_n}{n} e^{-2\pi n/\sqrt{N}},
\]

where \( \epsilon = \pm 1, N \) is the conductor of the curve. For example, when \( E = E_D \) and \( D \equiv 1, 2, 3 \pmod{8} \) we have \( \epsilon = 1 \) and \( N = 4D^2 \) for \( D \) even, \( N = 8D^2 \) for \( D \) odd.

**Proposition 2** Let \( \gamma \) be the largest real root of \( x^3 + ax + b \) and

\[
\Omega(E) = 2^n \int_{\gamma}^{\infty} \frac{1}{\sqrt{x^3 + ax + b}} \, dx,
\]

where \( n = 0 \) if \( \Delta < 0 \) and \( n = 1 \) otherwise. Then

\[
\frac{L(E,1)}{\Omega(E)} \in \mathbb{Q}
\]

with denominator \( \leq 24 \).
The rank can be estimated in the obvious way: find a rapidly converging sum for $L(E, 1)$ and then try to find which derivatives look nonzero. There is a useful bound on $|b_n|$ for this. If $n = p_1^{e_1} \cdots p_l^{e_l}$ then

$$|b_n| \leq \prod_{j=1}^{l} (e_j + 1)p_j^{e_j/2}.$$ 

Using this method we can prove, for example, that 1 is not a congruent number. For more details, see Koblitz, Stein.

### 0.3 Tate-Shafarevich Group III

While BSD1 is easily the most famous part of the conjecture it is not the whole story. Birch and Swinnerton-Dyer were also interested in the value of the constant $c$, which they conjectured to be closely connected to a group called III.

The Tate-Shafarevich group of $E$ over $\mathbb{Q}$, $\Sha(E)$ is defined by the exact (group cohomological) sequence

$$0 \to \Sha(E) \to H^1(\mathbb{Q}, E) \to \bigoplus_{all \, p} H^1(\mathbb{Q}_p, E).$$

**Conjecture 2** $\Sha(E)$ is finite.

(I don’t know if this has shown for any particular curve $E$, at least over $\mathbb{Q}$.) We do know that if $\Sha(E)$ is finite, then its order is a square, and that the $p$-primary component of $\Sha(E)$ is finite for some small $p$ for many curves. If results mentioned below for elliptic curves over function fields can be generalised, this may be enough to ‘almost’ prove the conjecture.

The third and final conjecture is more complicated. It gives the expected value of $c$ in conjecture 1 and involves $|\Sha(E)|$, the height pairing $h : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ and Haar measures defined on the local fields $\mathbb{Q}_p$.

**Conjecture 3**

$$\lim_{s \to 1} (s - 1)^r L(E, s) = \frac{|\Sha(E)|\text{Disc}(h)}{|E(\mathbb{Q})^{\text{tors}}|^2} \text{vol}(\prod_{p \notin U} E(\mathbb{Q}_p)).$$

Clearly, conjecture 3 only makes sense if the first two conjectures hold, but a priori 1 and 2 do not imply each other and both could be correct without implying 3. However, there are interesting indications that this is not true.

### 0.4 BSD for abelian varieties

Now we broaden our sphere of interest. Instead of considering an elliptic curve $E$ defined over $\mathbb{Q}$ let $A$ be an abelian variety defined over a global field $K$. This means that $K$ is either a number field or an algebraic function field over a finite field. (A finite algebraic extension of the field of rational functions over some finite field.)
By the Mordell-Weil theorem $A(K)$ is a finitely generated abelian group of rank $r$. One can extend the Birch and Swinnerton-Dyer conjecture to this case under the assumption that a suitably modified $L$-function has a holomorphic extension to the complex plane. This is known to be true for elliptic curves over function fields, but has not been proved in general.

Under this assumption, it has been proved (Kato and Trîhan, 2003):

**Theorem 2** Conjectures 1, 2, 3 are true if and only if there is some prime $p$ such that the $p$-primary part of $\text{III}(A)$ is a finite group.

In the case that $A = E$ and char $K \neq 2$ Milne showed in 1975 that conjectures 1, 2, 3 were equivalent to this condition and to each other.

In both cases the method of proof relies on comparing different forms of cohomology; the $L$-function is defined using $\ell$-adic etale and crystalline cohomology but $A(K)$ and $\text{III}(A)$ are defined using flat cohomology.

Unfortunately these methods cannot really be translated to number fields.

### 0.5 References

Colmez essentially gives a heavily shortened version of Koblitz, who is very strong on modular forms. Wiles gives a more geometric introduction. If you had rather think about class fields than modular forms Coates and Wiles is a nice paper. Kato and Trîhan discuss more forms of cohomology than I knew existed. Tate introduces $\text{III}$.