THE CONJECTURE OF BIRCH AND SWINNERTON-DYER

JOHN COATES

Abstract. The conjecture of Birch and Swinnerton-Dyer is one of the principal open problems of number theory today. Since it involves exact formulae rather than asymptotic questions, it has been tested numerically more extensively than any other conjecture in the history of number theory, and the numerical results obtained have always been in perfect accord with every aspect of the conjecture. The present article is aimed at the non-expert, and gives a brief account of the history of the conjecture, its precise formulation, and the partial results obtained so far in support of it.

1. History

The written history of the arithmetic of elliptic curves can be traced back at least to Arab manuscripts of over 1000 years ago, which were concerned with the problem of finding which positive integers are the areas of right-angled triangles, all of whose sides have rational length (traditionally, such positive integers are called *congruent numbers*). For example, 5 is a congruent number because it is the area of a right-angled triangle, whose sides have lengths 9/6, 40/6, 41/6. In fact no smaller congruent number was discovered by the ancients. It is easily seen that a positive integer N is a congruent number if and only if there is a point (x, y), with x and y rational numbers, and $y \neq 0$, on the curve

$$y^2 = x^3 - N^2 x. \tag{1.1}$$

In the 17th century, Fermat gave the first proof that 1 is not a congruent number, by introducing his method of *infinite descent*, and carrying it out on the curve (1.1) with $N = 1$. Fermat also noted that an intermediate step in his proof showed that, when $n = 4$, the curve $x^n + y^n = z^n$ has no solution in integers x, y, z which are all non-zero, and presumably this is what led him to claim that the same assertion holds for all $n \geq 3$. More generally, by an elliptic curve over a field F, we mean an irreducible non-singular projective algebraic curve of genus 1 defined over F, which is endowed with a given F-rational point $\mathcal{O}$. Any such curve has a plane cubic model of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (a_i \in F), \tag{1.2}$$

where $\mathcal{O}$ is now taken as the unique point at infinity (see, for example, [47]). Such an elliptic curve E is an abelian variety of dimension 1, meaning that the set of all points on such a curve with coordinates in some fixed extension field of F has a natural algebraic abelian group structure, with $\mathcal{O}$ as the zero element. In 1922, Mordell beautifully generalised Fermat's infinite descent argument and proved that the group of rational points on every elliptic curve defined over $\mathbb{Q}$ is always finitely generated as an abelian group. However, the big mystery left open by Mordell's proof was whether or not the procedure of infinite descent always terminated in a finite number of steps, thus enabling one to actually determine the group of rational points on the curve. In practice, this always seems to be the case, but, in fact, it has never been proven theoretically. The villain of the piece is a mysterious group, subsequently called the Tate-Shafarevich group of the elliptic curve, which is defined by

$$Ш(E/\mathbb{Q}) = Ker(H^1(\mathbb{Q}, E) \to \prod H^1(\mathbb{Q}_v, E)),$$

where v runs over all places of $\mathbb{Q}$, and $\mathbb{Q}_v$ is the completion of $\mathbb{Q}$ at v. This torsion abelian group is always conjectured to be finite, but today we can still only prove this under a very restrictive hypothesis discussed below.

The discoveries of Birch and Swinnerton-Dyer came as a great surprise to the mathematical world when they first became public around 1962. Starting in the autumn of 1958, they had carried out a series of brilliantly planned numerical experiments on the early EDSAC computers in Cambridge, whose aim was to uncover numerical evidence for the existence of some kind of analogue for elliptic curves of the mysterious exact analytic formulae proven by Dirichlet for the class numbers of binary quadratic forms, and powerfully extended to all quadratic forms by Siegel. Even though Siegel's work had been actively developed further for linear algebraic groups around this time by Kneser, Tamagawa, Weil, and others, it was Birch and Swinnerton-Dyer alone who first sought, and later found evidence for, an analogue for elliptic curves. It surely is one of the great mysteries of number theory, first uncovered by Birch and Swinnerton-Dyer, that purely arithmetic questions about the determination of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for an elliptic curve E over $\mathbb{Q}$ seem to be inextricably involved with the behaviour of the complex L-function of E.

In this survey article, we shall mainly discuss the conjecture of Birch and Swinnerton-Dyer in the most important and down to earth case of elliptic curves defined over $\mathbb{Q}$. However, the conjecture extends without difficulty to abelian varieties of arbitrary dimension defined over either a finite extension of $\mathbb{Q}$, or over a function field in one variable over a finite field (see [51]). To date, very little has been proven about the conjecture for general abelian varieties of dimension > 1 over number fields. However, for abelian varieties defined over a function field in one variable over a finite field, the remarkable work of Artin and Tate [51] makes great progress on the conjecture, apart from the mysterious question of the finiteness of the analogue of the Tate-Shafarevich group.

2. L-functions

Let E be any elliptic curve defined over $\mathbb{Q}$. By a global minimal Weierstrass equation for E, we mean any equation for E of the form (1.2), whose coefficients a_i are all integers, and whose discriminant Δ is as small as possible in absolute value (for the definition of Δ, and other facts about the elementary geometry of elliptic curves see [47]). Such equations are not unique, but we fix any one of them for the discussion which follows. Like all the L-series of arithmetic geometry, the complex L-series of E is defined by an Euler product. For each prime number p, define N_p by letting $N_p - 1$ denote the number of solutions of the congruence

$$y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \bmod p,$$

and then put

$$t_p = p + 1 - N_p.$$

If $(p, \Delta) = 1$, we have $|t_p| \leq 2\sqrt{p}$ by Hasse's theorem. If p divides Δ, then $t_p = 1$ if E has multiplicative reduction at p with tangents at the node defined over $\mathbb{F}_p$, $t_p = -1$ if E has multiplicative reduction at p with tangents at the node not defined over $\mathbb{F}_p$, and $t_p = 0$ when E had additive reduction at p. The complex L-series of E is then defined by the Euler product

$$L(E,s) = \prod_{p|\Delta} \left(1 - t_p p^{-s}\right)^{-1} \prod_{(p,\Delta)=1} \left(1 - t_p p^{-s} + p^{1-2s}\right)^{-1}. \tag{2.1}$$

This Euler product defines a Dirichlet series

$$L(E,s) = \sum_{n=1}^{\infty} c_n n^{-s},$$

where $c_p = t_p$ for every prime p, and which converges in the half plane $Re(s) > \frac{3}{2}$. When Birch and Swinnerton-Dyer first began their calculations, it was only known how to analytically continue this function to the entire complex plane when E has complex multiplication (i.e. the ring of endomorphisms of E, which are defined over $\mathbb{C}$, is strictly bigger than $\mathbb{Z}$), using ideas about Eisenstein series which go back to Eisenstein and Kronecker, and which were subsequently developed systematically by Deuring [17]. To prove the analytic continuation for all E, we need the following fundamental result, the essential idea behind the proof of which we owe to Wiles [57] (see also [5]). The conductor $C(E)$ of E is the positive integer defined by

$$C(E) = \prod_{p|\Delta} p^{f_p},$$

where $f_p = 1$ if E has multiplicative reduction at p, and $f_p = 2 + \delta_p$ for some integer $\delta_p \geq 0$ if E has additive reduction at p. Moreover, in this latter case, $\delta_p = 0$ when $p \geq 5$. Let $\Gamma_0(C(E))$ be the subgroup of $SL_2(\mathbb{Z})$ consisting of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $c \equiv 0 \bmod C(E)$. Let $\mathcal{H}$ be the complex upper half plane, and put $q = e^{2\pi i\tau}$ with $\tau \in \mathcal{H}$. Define

$$f_E(\tau) = \sum_{n=1}^{\infty} c_n q^n.$$

Theorem 2.1. *The holomorphic function $f_E(\tau)$ is a primitive cusp form of weight 2 for $\Gamma_0(C(E))$.*

By a generalization of classical ideas of Hecke, this theorem not only proves that $L(E, s)$ can be extended to an entire holomorphic function of s, but it also establishes the following functional equation. Define

$$\Lambda(E, s) = C(E)^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s).$$

Corollary 2.2. *The function $\Lambda(E, s)$ can be extended to an entire function of s, and satisfies the functional equation*

$$\Lambda(E, s) = w_E\Lambda(E, 2 - s), \tag{2.2}$$

where $w_E = \pm 1$.

The so called root number $w_E = \pm 1$ is important for us because we see immediately from (2.2) that $L(E, s)$ has a zero at $s = 1$ of even or odd multiplicity, according as $w_E = +1$ or $w_E = -1$. Moreover, the theory of L-functions shows that w_E can always be calculated as a product of purely local factors. For example, if E is taken to be the curve (1.1) with N a square free positive integer, then $w_E = +1$ when $N \equiv 1,\ 2,\ 3 \bmod 8$, and $w_E = -1$ when $N \equiv 5,\ 6,\ 7 \bmod 8$, whence, in particular, $L(E, s)$ always has a zero at $s = 1$ whenever $N \equiv 5,\ 6,\ 7 \bmod 8$.

We mention that one can, more generally, consider elliptic curves E which are defined over some finite extension F of $\mathbb{Q}$. Again the group of F-rational points on E is a finitely generated abelian group, and again no algorithm has ever been proven for infallibly determining this group, again thanks to our lack of knowledge of the finiteness of the Tate-Shafarevich group of such a curve. Of course, these elliptic curves also have a complex L-series, which we now denote by $L(E/F, s)$, which is defined in the region $Re(s) > 3/2$ by an entirely analogous Euler product to (2.1), but taken over all finite places of the field F. When E admits complex multiplication, the analytic continuation and functional equation of $L(E/F, s)$ follow immediately from Deuring's theorem [17], which identifies $L(E/F, s)$ with a product of Hecke L-series with Grossencharacters. However, when E does not have complex multiplication, our knowledge of the analytic continuation of $L(E/F, s)$ is still very limited, with the most striking results established so far being proofs of this assertion either when F is a real quadratic field [19], or when F is any finite extension of $\mathbb{Q}$ which is contained in the the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for any prime number p [53].

3. The Birch-Swinnerton-Dyer conjecture

We will now state the conjecture of Birch and Swinnerton-Dyer in both its weak and strong form, and discuss the evidence for it in subsequent sections. The conjecture, which was first published in [3], predicts a remarkable link between the arithmetic of an elliptic curve E defined over $\mathbb{Q}$, and the behaviour of its complex L-series $L(E, s)$ at the point $s = 1$. Let g_E denote the rank of $E(\mathbb{Q})$ (i.e. the $\mathbb{Q}$-dimension of $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$). We define

Definition 3.1. *r_E is the order of the zero of $L(E, s)$ at $s = 1$.*

Weak Birch-Swinnerton-Dyer Conjecture. *For all elliptic curves E over $\mathbb{Q}$, we have*

$$r_E = g_E. \tag{3.1}$$

The full Birch-Swinnerton-Dyer conjecture is the weak Birch-Swinnerton-Dyer conjecture, together with a purely arithmetic exact formula for the constant $\mathfrak{L}_E$ defined by

$$\mathfrak{L}_E = \lim_{s\to 1} L(E, s)/(s - 1)^{r_E}. \tag{3.2}$$

This formula involves the following arithmetic invariants. Firstly, there is a regulator term coming from the Neron-Tate height. If $\alpha = m/n$, with m and n relatively prime integers, is any non-zero rational number, we define its height $h(\alpha)$ by $h(\alpha) = log(max(|m|, |n|))$, and put $h(0) = 0$. Then Neron and Tate proved independently (see [47], Chap. 8) that there is a unique function

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$$

such that $\hat{h}(\mathcal{O}) = 0$, and, as P runs over the non-zero points in $E(\mathbb{Q})$, we have $\hat{h}(2P) = 4\hat{h}(P)$ and $|\hat{h}(P) - h(x(P))|$ is bounded independent of P, where $x(P)$ denotes the x-coordinate of P in any fixed generalised Weierstrass equation (1.2). Then the function on $E(\mathbb{Q}) \times E(\mathbb{Q})$ defined by

Definition 3.2. $\langle P, Q\rangle = \frac{1}{2}\left(\widehat{h}(P \oplus Q) - \widehat{h}(P) - \widehat{h}(Q)\right)$

is biadditive. Moreover, we have $\hat{h}(P) = 0$ if and only if P is a torsion point in $E(\mathbb{Q})$. If one uses, in addition, the fact that there are only finitely many points P in $E(\mathbb{Q})$ with $\hat{h}(P) \leq c$ for any constant $c > 0$, it follows, as was first remarked by Cassels, that $\hat{h}$ induces a positive definite quadratic form on $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. Hence, for any choice of g_E independent points $P_1, ..., P_{g_E}$ in $E(\mathbb{Q})$, we always have that the determinant $det\langle P_i, P_j\rangle$ is strictly positive. We then define $R_\infty(E) = 1/\#(E(\mathbb{Q})^2)$ if $g_E = 0$ and

Definition 3.3. $R_\infty(E) = det\langle P_i, P_j\rangle/[E(\mathbb{Q}) : \sum_{i=1}^{g_E} \mathbb{Z}P_i]^2$ *if* $g_E > 0$.

We assume that we have fixed any global minimal Weierstrass equation for E, and we define Ω_E to be the least positive real period of the Neron differential on E, which is given by

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

The next subtle ingredient in the conjectural exact formula for $\mathfrak{L}_E$ are the so called *Tamagawa factors*, which are purely local terms occurring for the prime at infinity, and the finite primes q dividing the conductor $C(E)$ of E.

Definition 3.4. $c_\infty(E)$ *is equal to 1 or 2, according as the group of points* $E(\mathbb{R})$ *on* E *with real coordinates has 1 or 2 connected components.*

Next assume that q is any prime number dividing the conductor $C(E)$. Let $\mathbb{Q}_q$ be the completion of $\mathbb{Q}$ at q. Now, since q is a prime of bad reduction for E, the reduction of E modulo q will be a cubic curve with a singular point, and we define $E_0(\mathbb{Q}_q)$ to be the subgroup of $E(\mathbb{Q}_q)$ consisting of all points whose reduction modulo q is non-singular. Since we are working with a generalised Weierstrass equation which is minimal at q, the index of $E_0(\mathbb{Q}_q)$ in $E(\mathbb{Q}_q)$ will be independent of the choice of the Weierstrass equation.

Definition 3.5. *For a prime* q *of bad reduction,* $c_q(E) = [E(\mathbb{Q}_q) : E_0(\mathbb{Q}_q)]$.

In general, there is no simple formula for $c_q(E)$, but Tate [50] gave an explicit algorithm for computing $c_q(E)$ from any generalised Weierstrass equation for E which is minimal at q, and also proved:-

Lemma 3.6. *If* E *has split multiplicative reduction at* q*, then* $c_q(E) = ord_q(\Delta)$*. For all other primes* q *of bad reduction,* $c_q(E) \leq 4$.

We can now at last state the full Birch-Swinnerton-Dyer conjecture.

Full Birch-Swinnerton-Dyer Conjecture. *We have* $r_E = g_E$*. Moreover,* $\text{Ш}(E/\mathbb{Q})$ *is finite, and the following exact formula is valid*

$$\frac{\mathfrak{L}_E}{\Omega_E} = \#(\text{Ш}(E/\mathbb{Q}))R_\infty(E)c_\infty(E)\prod_{q|C(E)} c_q(E). \tag{3.3}$$

Note that elliptic curves which are $\mathbb{Q}$-isogenous have the same L-functions. However, it is not at all obvious that the exact formula (3.3) being valid for an elliptic curve implies that it is valid for any isogenous curve, but this was proven by Cassels [8] and Tate [51].

We shall spend most of the rest of this article discussing the fragmentary theoretical results proven so far, in the direction of both the weak and full Birch-Swinnerton-Dyer conjecture. However, to illustrate immediately the limits of our present knowledge, let us note three simple consequences of the conjecture which have never been established for a single elliptic curve E over $\mathbb{Q}$. Firstly, it has never been proven that there exists an elliptic curve E defined over $\mathbb{Q}$ with $r_E \geq 4$, even though there are many examples of such E with $g_E \geq 4$. Secondly, it has never been proven that $\text{Ш}(E/\mathbb{Q})$ is finite for a single elliptic curve E with $r_E \geq 2$. Thirdly, it has never been proven that $\mathfrak{L}_E/(\Omega_E R_\infty(E))$ is a rational number for a single E with $r_E \geq 2$.

The earliest numerical work in support of these conjectures is given in the papers [3], [49]. Today, the numerical evidence support of both the weak and full Birch-Swinnerton-Dyer conjecture is overwhelming, and probably more extensive than for any other conjecture in the history of mathematics. Access to the vast amount of numerical data, which, to date, confirms experimentally every aspect of the conjecture, can be made at the website www.lmfdb.org/EllipticCurve/Q (see also the earlier book [15], which is available online on John Cremona's homepage at Warwick University). This website includes tables of all elliptic curves E over $\mathbb{Q}$ with conductor $C(E) < 360,000$. There are 2,247,187 elliptic curves in this table, lying in 1,569,126 $\mathbb{Q}$-isogeny classes. All such curves have $g_E \leq 4$, and in fact there is only one curve in the table with $g_E = 4$ (this curve has conductor 234,446). In addition, Miller, Stoll, and Creutz [35], [14], [36] have verified the full Birch-Swinnerton-Dyer conjecture for all E defined over $\mathbb{Q}$ with $C(E) < 5000$, which have $r_E \leq 1$. The analytic quantity $\mathfrak{L}_E$ can be computed numerically to great accuracy irrespective of the value of r_E, and the same is usually true for all quantities occurring in the exact formula (3.3), except for the order of the Tate-Shafarevich group of E. Even when $Ш(E/\mathbb{Q})$ is known to be finite, it is very difficult to actually compute its true order arithmetically. However, even granted this difficulty, there is one subtle sub-test of the order of $Ш(E/\mathbb{Q})$ as predicted by (3.3) being correct. As we shall explain in the next section, an important theorem of Cassels [9] proves that if $Ш(E/\mathbb{Q})$ is finite, then its order must be the square of an integer. Happily, in all of the vast number of numerical examples computed to date, the formula (3.3) has always produced a conjectural order for the Tate-Shafarevich group which is indeed the square of an integer.

4. Parity Questions

The only deep general results known about the conjecture of Birch and Swinnerton-Dyer, which do not involve in some fashion the hypothesis that the L-series of the curve has a zero at $s = 1$ of order at most 1, are parity theorems of two kinds. As always, E will be an elliptic curve defined over $\mathbb{Q}$, and $Ш(E/\mathbb{Q})$ will denote its Tate-Shafarevich group. If A is any abelian group and p a prime number, we write $A(p)$ for the p-primary subgroup of A, and $A[p]$ for the kernel of multiplication by p on A. Also, A_{div} will denote the maximal divisible subgroup of A. The following theorem is due to Cassels [9] and Tate [52].

Theorem 4.1. *There is a canonical non-degenerate, alternating, bilinear form on* $Ш(E/\mathbb{Q})/Ш(E/\mathbb{Q})_{div}$.

Corollary 4.2. *For every prime p, the $\mathbb{F}_p$-vector space given by the kernel of multiplication by p on* $Ш(E/\mathbb{Q})/Ш(E/\mathbb{Q})_{div}$ *has even dimension.*

Corollary 4.3. *If p is a prime such that $Ш(E/\mathbb{Q})(p)_{div} = 0$, then the order of $Ш(E/\mathbb{Q})(p)$ is a square.*

In particular, if $Ш(E/\mathbb{Q})$ is finite, its order must be a perfect square. We note that, for every prime p, classical Galois cohomology shows that, for some integer $t_{E,p} \geq 0$, one has

$$Ш(E/\mathbb{Q})(p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E,p}} \oplus J_{E,p},$$

where $J_{E,p}$ is a finite group. Plainly $Ш(E/\mathbb{Q})(p)_{div} = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E,p}}$. Of course, conjecturally $t_{E,p} = 0$ for every prime p, but the only far weaker general known result in this direction is the following parity theorem of the Dokchitser brothers [16]. Recall that g_E denotes the rank of $E(\mathbb{Q})$, and r_E denotes the order of zero of $L(E, s)$ at the point $s = 1$.

Theorem 4.4. *For every prime number p, we have $r_E \equiv g_E + t_{E,p} \bmod 2$. In particular, the parity of $t_{E,p}$ is independent of p.*

As a simple application of this theorem, we see that if there did exist a square free positive integer N with $N \equiv 5, 6, 7 \bmod 8$, which is not a congruent number, then the p-primary subgroup of the Tate-Shafarevich of the elliptic curve (1.1) would have to contain a copy of the divisible group $\mathbb{Q}_p/\mathbb{Z}_p$ for every prime p, and so a copy of $\mathbb{Q}/\mathbb{Z}$. We also note that the strong parity conjecture is the assertion that $r_E \equiv g_E \bmod 2$, but this has only been proven at present under the assumption that $r_E \leq 1$, when, as we shall see in the next section, we even have $r_E = g_E$, in accord with the weak Birch-Swinnerton-Dyer conjecture.

5. Main results

As before, let E denote any elliptic curve defined over $\mathbb{Q}$. Define the modular curve $X_0(C(E))$ by

$$X_0(C(E)) = \Gamma_0(C(E)) \setminus (\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})),$$

where $\mathbb{P}^1(\mathbb{Q})$ denotes the projective line over $\mathbb{Q}$. Then $X_0(C(E))$ is the set of complex points of a curve defined over $\mathbb{Q}$, which we also denote by $X_0(C(E))$. Let $[\infty\ ]$ denote the cusp ∞ of this curve. The modularity Theorem 2.1 of Wiles [57] , [5], when combined with work of Shimura [46], shows that there exists an elliptic curve $E(f_E)$ defined over $\mathbb{Q}$, which is a factor up to isogeny of the Jacobian variety of $X_0(C(E))$, and has the same L-series as the elliptic curve E. Hence, by Faltings theorem [18], E and $E(f_E)$ must be isogenous over $\mathbb{Q}$, whence we obtain the following result.

Theorem 5.1. *There is a non-constant rational map defined over* $\mathbb{Q}$

$$\phi : X_0(C(E)) \to E \tag{5.1}$$

with $\phi(\ [\infty\ ]) = \mathcal{O}$.

The most important result to date in the direction of the conjecture of Birch and Swinnerton-Dyer is the following theorem of Kolyvagin and Gross-Zagier (see [23]). We again write r_E and g_E for the order of the zero of the complex L-series of E at $s = 1$, and for the rank of $E(\mathbb{Q})$.

Theorem 5.2. *If* $r_E \leq 1$*, then* $r_E = g_E$*, and* $Ш(E/\mathbb{Q})$ *is finite.*

The proof relies heavily on the earlier work of Gross-Zagier [24], relating the canonical height of Heegner points to derivatives of L-functions, as well as on Kolyvagin's highly original notion of an Euler system [27]. Heegner points were first discovered, in a special case, by Heegner in his celebrated paper [25], and it was Birch and Stephens who first conjectured that they should be related to the derivatives of L-series. We also note that the proof of the above theorem establishes the following rationality result.

Theorem 5.3. *If* $r_E \leq 1$*, then* $\mathfrak{L}_E/(\Omega_E R_\infty(E))$ *lies in* $\mathbb{Q}$*.*

When $r_E = 0$, we know by Theorem 5.2 that $g_E = 0$, whence $R_\infty(E) = 1/\#(E(\mathbb{Q}))^2$, and Theorem 5.3 in this case is just a consequence of the classical theory of modular symbols going back to the work of Hecke and others (see [15]). However, when $r_E = 1$, so that $g_E = 1$ by Theorem 5.2, the assertion of Theorem 5.3 can only be proven by using the Gross-Zagier theorem [24]. Moreover, we stress that, contrary to what is often stated in the literature, we still cannot prove the Birch-Swinnerton-Dyer conjectural exact formula for the order of $Ш(E/\mathbb{Q})$ under the hypothesis that $r_E \leq 1$. Finally, we note that some special cases of Theorem 5.2 were proven earlier for elliptic curves with complex multiplication by rather different methods, which make use of elliptic units rather than Heegner points (see [12], [42], [43], [44]). In another direction, S. Zhang [59] has generalised the above results to the Jacobian varieties of Shimura curves defined over totally real number fields.

Theorem 5.2 has a surprising application to Gauss' class number problem for imaginary quadratic fields, as was discovered by Goldfeld [20] (see also [38]). If E is an elliptic curve with $g_E \geq 3$, Theorem 5.2 guarantees that necessarily $r_E > 1$, and so we must have that $r_E \geq 3$ when $w_E = -1$. It is usually easy to check numerically that $r_E \leq 3$ when $g_E = 3$, and thus one can prove that there exist elliptic curves E over $\mathbb{Q}$ with $r_E = 3$. For example, $r_E = 3$ for the curve

$$E : y^2 + y = x^3 - 7x + 3,$$

which has conductor $C(E) = 5077$, and $g_E = 3$. Goldfeld's work then enables one to give, for the first time, an explicit upper bound for the absolute value of the discriminants of all imaginary quadratic fields having any prescribed class number. The earlier work on this problem by Heilbronn and Siegel, while proving that the class number of an imaginary quadratic field tends to infinity with the absolute value of the discriminant of the field, was ineffective.

In view of Theorem 5.2, it is plainly an important problem to decide when the hypothesis $r_E \leq 1$ holds. In any particular numerical example, it is usually easy to settle this question, but our knowledge of theoretical results is still very limited. The most natural example of infinite families of elliptic curves defined over $\mathbb{Q}$ is given by the family of quadratic twists of a fixed elliptic curve E. If M is the discriminant of a quadratic field, $E^{(M)}$ will denote the quadratic twist of E by the extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$ (in other words, $E^{(M)}$ is the unique elliptic curve defined over $\mathbb{Q}$, which is not isomorphic to E over $\mathbb{Q}$, but becomes isomorphic to E over $\mathbb{Q}(\sqrt{M})$). It is not difficult to see that, in the family of all quadratic twists $E^{(M)}$ of a given E defined over $\mathbb{Q}$, the root numbers $w_{E^{(M)}} = +1$ and $w_{E^{(M)}} = -1$ will each occur half the time. A folklore conjecture (see [21]) asserts that amongst those quadratic twists $E^{(M)}$ with $w_{E^{(M)}} = +1$ (respectively, with $w_{E^{(M)}} = -1$), we should have $r_{E^{(M)}} = 0$ (respectively, $r_{E^{(M)}} = 1$) outside a set of discriminants M of density zero, but this has never been proven for a single elliptic curve E. However, the papers [6] and [37] prove, by rather different methods, the important result that there always exist infinitely many discriminants M such that $r_{E^{(M)}} = 0$, and infinitely many discriminants M such that $r_{E^{(M)}} = 1$. From the point of view of diophantine equations, there is great interest in establishing conditions on the prime factors of M which guarantee that $r_{E^{(M)}} = 1$, since $E^{(M)}(\mathbb{Q})$ is infinite for such M by Theorem 5.2. The first result in this direction is due to Heegner [25], and subsequently Birch [4] generalised and reformulated it. We write $[0\ ]$ for the zero cusp on the modular curve $X_0(C(E))$.

Theorem 5.4. *Let $E/\mathbb{Q}$ be any elliptic such that $\phi(\ [0\ ])$ is not contained in $2E(\mathbb{Q})$, and let p be any prime number such that $p \equiv 3 \bmod 4$,and every prime dividing $C(E)$ splits in the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Then $r_{E^{(-p)}} = 1$, and so, in particular, $E^{(-p)}(\mathbb{Q})$ is infinite.*

Recently, Tian discovered a method for generalising this result to quadratic twists by discriminants having an arbitrary prescribed number of prime factors, which he first applied to the classical congruent number problem [55]. More generally, his method yields the following theorem [13].

Theorem 5.5. *Let $E/\mathbb{Q}$ be any elliptic curve such that (i) $\phi(\ [0\ ])$ is not contained in $2E(\mathbb{Q})$, and (ii) there exists a good supersingular prime q with $q \equiv 1 \bmod 4$, and with $C(E)$ a square modulo q. Then, for each integer $k \geq 1$, there exist infinitely many square free discriminants M having exactly k prime factors, and with $(M, C(E)) = 1$, such that $r_{E^{(M)}} = 1$, whence, in particular, $E^{(M)}(\mathbb{Q})$ is infinite.*

Finally, we mention a recent result proven by Bertolini, Darmon, and Rotger [1], which is a key first step towards generalizing Theorem 5.2 to certain finite Galois extensions of $\mathbb{Q}$. Let ρ denote an odd, irreducible, 2-dimensional Artin representation of the absolute Galois group of $\mathbb{Q}$. As usual, we define $L(E, \rho, s)$ to be the Euler product attached to the tensor product of the Artin representation ρ with the the l-adic Tate module of E. Since both E and ρ are known to be modular, it follows from the theory of modular forms that $L(E, \rho, s)$ is also entire.

Theorem 5.6. *If $L(E, \rho, 1) \neq 0$, then ρ does not occur in $E(F) \otimes_{\mathbb{Z}} \mathbb{C}$, where F is the fixed field of the kernel of ρ.*

Moreover, very recent work of Kings, Lei, Loeffler and Zerbes [30], [29], [31] constructs a new Euler system, and they use it both to give another proof of Theorem 5.6, and, in addition, to show that, when $L(E, \rho, 1) \neq 0$, the ρ-component of the p-primary subgroup of the Tate-Shafarevich group of E over F is finite for most primes p.

6. The exact formula prime by prime

In this section, we will discuss the partial results which are known about the conjectural exact Birch-Swinnerton-Dyer formula for the order of the Tate-Shafarevich group of an elliptic curve $E/\mathbb{Q}$ when we assume that $r_E \leq 1$. Theorem 5.2 assures us that, in this case, $E(\mathbb{Q})$ has rank r_E, and $\text{Ш}(E/\mathbb{Q})$ is finite. We note that the order of the torsion subgroup $E(\mathbb{Q})$ is easily determined, and has only one of 12 possibilities, thanks to the beautiful work of Mazur [32]. However, the classical theory of descent does not give a practical way to compute the order of the p-primary part of $\text{Ш}(E/\mathbb{Q})$ once $p > 5$, and the only techniques which work at present are p-adic methods related to Iwasawa theory. In view of this, it is convenient to break the conjecture up into a p-part for every prime number p. To simplify the notation, we define

$$Tam(E) = c_\infty(E) \prod_{q|C(E)} c_q(E).$$

It is also convenient to put

$$L^{(alg)}(E, 1) = L(E, 1)/\Omega_E,$$

which we know lies in $\mathbb{Q}$ by Theorem 5.3. Then, for every prime number p, the strong Birch-Swinnerton-Dyer conjecture predicts the following exact formula for the order of the p-primary subgroup $\text{Ш}(E/\mathbb{Q})(p)$ of $\text{Ш}(E/\mathbb{Q})$ when $r_E = 0$.

p-part of the Birch-Swinnerton-Dyer conjecture for analytic rank 0. *Assume* that $r_E = 0$. *Then, for each prime p,* we have

$$ord_p(\#(\text{Ш}(E/\mathbb{Q})(p))) = ord_p(L^{(alg)}(E, 1)) + 2ord_p(\#(E(\mathbb{Q}))) - ord_p(Tam(E)). \tag{6.1}$$

The strongest general result known about this p-part of the Birch and Swinnerton-Dyer conjecture is for E with complex multiplication, and is proven using the Euler system of elliptic units, combined with arguments from Iwasawa theory. The result is due to Rubin [42], but also uses earlier work of Yager [58].

Theorem 6.1. *Assume that $r_E = 0$, and that E admits complex multiplication by an order in an imaginary quadratic field K. If p is any prime which does not divide the order of the group of roots of unity of K, then the p-part of the Birch-Swinnerton-Dyer conjecture is valid for E.*

As an example of this theorem, consider the modular curve $A = X_0(49)$, which is an elliptic curve with equation

$$A : y^2 + xy = x^3 - x^2 - 2x - 1.$$

Take $E = A^{(M)}$, with $M = q_1...q_r$, where the q_i are distinct primes, with $q_i \equiv 1 \bmod 4$ and $q_i \equiv 3, 5, 6 \bmod 7$, for $i = 1, \ldots, r$. It is shown in [13] that $ord_2(L^{(alg)}(E, 1)) = r - 1$ for all $r \geq 0$. This proves that $L(E, 1) \neq 0$, and it is easy to see that it establishes the 2-part of the Birch-Swinnerton-Dyer conjecture for E. Hence, applying Theorem 6.1, we conclude that $g_E = 0$, $Ш(E/\mathbb{Q})$ is finite, and the exact Birch-Swinnerton-Dyer formula is valid for the order of $Ш(E/\mathbb{Q})$.

For elliptic curves without complex multiplication, the only way of attacking the p-part of the conjecture of Birch and Swinnerton-Dyer when $r_E = 0$ is by considering the Iwasawa theory of E over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We recall that, for p any prime, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, which we denote by Φ_∞, is the unique subfield of the field generated over $\mathbb{Q}$ by all p-power roots of unity, whose Galois group Γ over $\mathbb{Q}$ is isomorphic to the additive group of $\mathbb{Z}_p$. Mazur and Swinnerton-Dyer [36] were the first to prove the existence of a p-adic L-function attached to E over Φ_∞ when p is a prime of good ordinary reduction for E, and to formulate a "main conjecture" relating this p-adic L-function to the Γ-module given by the p^∞-Selmer group of E over Φ_∞. As a special case of a more general result, Schneider [45] showed that, for p any odd prime number where E has good ordinary reduction, this "main conjecture" would indeed imply the p-part of the Birch-Swinnerton-Dyer conjecture for the order of $Ш(E/\mathbb{Q})$ when $r_E = 0$. The first major breakthrough in the direction of proving this main conjecture for odd good ordinary primes p was made by Kato [26]. He proved the existence of a remarkable new Euler system attached to E, and used it to prove a partial result in the direction of the "main conjecture" for sufficiently large good ordinary primes p. Subsequently, Skinner and Urban [48] have completed the proof of this "main conjecture" in many cases, by combining Kato's result with deep arguments from the theory of modular forms. This leads to the following specific theorem [48] about the p-part of the conjecture of Birch and Swinnerton-Dyer. Let E_p denote the Galois module of p-division points on E, and let

$$\nu_{E,p} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut(E_p) = GL_2(\mathbb{F}_p)$$

be the associated Galois representation.

Theorem 6.2. *Assume that E does not admit complex multiplication, and that $r_E = 0$. Let p be any prime number such that (i) $p \neq 2$, (ii) E has good ordinary reduction at p, (iii) $\nu_{E,p}$ is surjective, and (iv) there exists a prime q, where E has bad multiplicative reduction, such that the Galois module E_p is ramified at q. Then the p-part of the Birch-Swinnerton-Dyer conjecture is valid for E.*

In particular, if E is semistable (i.e. E has multiplicative reduction at all primes of bad reduction), and $r_E = 0$, then this theorem establishes the p-part of the Birch-Swinnerton-Dyer conjecture for all primes $p \geq 11$ of good ordinary reduction. For primes $p > 2$ where E has good supersingular reduction and $t_p = 0$, Wan [56] uses quite different methods in Iwasawa theory to give a proof of the p-part of the conjecture of Birch and Swinnerton-Dyer, assuming that $r_E = 0$ and E is semistable.

One can also formulate the p-part of the conjecture of Birch and Swinnerton-Dyer for every prime p when $r_E = 1$.

p-part of the Birch-Swinnerton-Dyer conjecture for analytic rank 1. *Assume that $r_E = 1$. Then, for each prime p, we have*

$$ord_p(\#(Ш(E/\mathbb{Q})(p))) = ord_p(\mathfrak{L}_E/(\Omega_E R_\infty(E))) - ord_p(Tam(E)). \tag{6.2}$$

When E admits complex multiplication and $r_E = 1$, the work of Kobayashi [28], Perrin-Riou [40], Pollak-Rubin [41], Rubin [42] establishes the following analogue of Theorem 6.1.

Theorem 6.3. *Assume that E admits complex multiplication and that $r_E = 1$. Let p be any odd prime where E has good reduction. Then the p-part of the Birch-Swinnerton-Dyer conjecture is valid for E.*

When E does not admit complex multiplication, we have the following recent theorem of W. Zhang [60].

Theorem 6.4. *Assume that E does not admit complex multiplication, and that $r_E = 1$. Let p be any prime number such that (i) $p \geq 5$, (ii) E has good ordinary reduction at p, (iii) $\nu_{E,p}$ is surjective, (iv) there exist two primes $q_i (i = 1, 2)$ of bad multiplicative reduction for E such that the Galois module E_p is ramified at both q_1 and q_2, and (v) If q is any prime of bad multiplicative reduction for E with*

$q \equiv \pm 1 \bmod p$, then E_p is ramified at q. Then the p-part of the Birch-Swinnerton-Dyer conjecture is valid for E.

Finally, it is also interesting to note that Kato's work [27], combined with a theorem of Rohrlich [39], proves the following result, which was originally conjectured by Mazur [33]. Let μ_{p^∞} denote the group of all p-power roots of unity.

Theorem 6.5. *For all primes p, the abelian group $E(\mathbb{Q}(\mu_{p^\infty}))$ is finitely generated.*

7. A numerical example

Although this article is not directly concerned with the conjecture of Birch and Swinnerton-Dyer for elliptic curves over number fields, I want to end by briefly explaining a remarkable and naturally occurring numerical example, related to the elliptic curves of conductor 11. We recall that 11 is the smallest conductor for an elliptic curve defined over $\mathbb{Q}$, and there are three isogenous curves of conductor 11 defined over $\mathbb{Q}$. Two of these curves are given by

$$A_1 : y^2 + y = x^3 - x^2, \quad A_2 : y^2 + y = x^3 - x^2 - 7820x - 263580,$$

and they are linked by a $\mathbb{Q}$-isogeny $\psi : A_2 \to A_1$ of degree 25. It is well known that $A_1(\mathbb{Q}) = \mathbb{Z}/5\mathbb{Z}$, and $A_2(\mathbb{Q}) = 0$. As was pointed out to me by Fisher and Matsuno, the splitting field of the Galois representation given by the kernel of ψ, which we denote by J, is the field $\mathbb{Q}(\mu_5, r)$, where μ_5 is the group of 5-th roots of unity, and r denotes any root of the abelian polynomial

$$x^5 - 65x^4 + 205x^3 + 140x^2 + 25x + 1.$$

Around the year 2000, Matsuno discovered that the complex L-series of either of these two curves, when viewed as curves over J, has a zero of order 4 at $s = 1$. It therefore became an interesting numerical challenge to show that the group of points of either of these two curves with coordinates in J also has rank 4, as predicted by the natural generalization of the weak Birch-Swinnerton-Dyer conjecture. Recently, S. Donnelly (private communication) finally found four linearly independent points, using the MAGMA system in Sydney University. I am very grateful to him for providing the following data. Define $E = A_1^{(5)}$ to be the quadratic twist of A_1 by $\mathbb{Q}(\sqrt{5})$, so that $C(E) = 275$. An equation for the curve E is given by

$$y^2 = x^3 - 10800x + 1026000.$$

Then Donnelly discovered that there is a point in $E(J)$ with x-coordinate

$$(1632096r^4 - 106533648r^3 + 363696696r^2 + 134074044r + 8312592)/41323, \tag{7.1}$$

and the conjugates of this point under the Galois group of $\mathbb{Q}(r)/\mathbb{Q}$ span a subgroup of rank 4 in $E(\mathbb{Q}(r))$. Moreover, the torsion subgroup of $E(\mathbb{Q}(r))$ is trivial, and it is very probable that $E(\mathbb{Q}(r))$ is generated by any four of the conjugates of the point (7.1). Also, the Birch-Swinnerton-Dyer conjecture predicts that the Tate-Shafarevich group of E over $\mathbb{Q}(r)$ should be trivial. Note that $E(J) = A_1(J)$ because $\sqrt{5} \in J$. It also seems very likely that $A_1(J)$ is generated by any four of the conjugates of the point (7.1), together with the point $(0,0)$ of order 5. Obviously, J is a subfield of the field F_∞ which is obtained by adjoining to $\mathbb{Q}$ the coordinates of all 5-power division points on any of the three curves of conductor 11. At present, these points found by Donnelly are the only known points of infinite order on the curves of conductor 11 with coordinates in F_∞ (see [11]).

References

[1] M. Bertolini, H. Darmon, V. Rotger, *Beilinson-Flach elements and Euler systems II: The Birch-Swinnerton-Dyer conjecture for Hasse-Weil-Artin L-series*, J. Algebraic Geometry 24 (2015), 569-604.

[2] B. Birch, P. Swinnerton-Dyer, *Notes on elliptic curves I*, Crelle 212 (1963), 7-25.

[3] B. Birch, P. Swinnerton-Dyer, *Notes on elliptic curves II*, Crelle 218 (1965), 79-108.

[4] B. Birch, *Elliptic curves and modular functions* in *Symposia Mathematica, Indam Rome 1968/1969*, Academic Press, 4 (1970), 27-32

[5] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843-939.

[6] D. Bump, S. Friedberg and J. Hoffstein, *Non-vanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. 102 (1990), 543-618.

[7] L. Cai, J. Shu, Y. Tian, *Explicit Gross-Zagier and Waldpsurger formulae*, Algebra and Number Theory, 8 (2014), 2523-2572.

[8] J. Cassels, *Arithmetic on curves of genus 1, VIII*, Crelle 217 (1965), 180-199.

[9] J. Cassels, *Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung*, Crelle 211 (1962), 95-112

[10] J. Coates, *Elliptic curves with complex multiplication and Iwasawa theory*, Bull. London Math. Soc. 23 (1991), 321-350.

[11] J. Coates, *Elliptic curves - The crossroads of theory and computation* in ANTS 2002, Springer LNCS 2369 (2002), 9-19.

[12] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 233-251

[13] J. Coates, Y. Li, Y. Tian, S. Zhai, Quadratic twists of elliptic curves, Proc. London Math. Soc. 110 (2015), 357-394.

[14] B.Creutz, R. Miller, Second isogeny descents and the Birch-Swinnerton-Dyer conjectural formula, J. of Algebra 372 (2012), 673-701.

[15] J. Cremona, *Algorithms for Modular Elliptic Curves*, second Edition, Cambridge University Press, 1997.

[16] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. 172 (2010), 567-596.

[17] M. Deuring, *Die Zetafunktionen einer algebraischen Kurve von Geschlechts Eins*, Nach. Akad. Wiss. Gttingen, (1953) 85-94, (1955) 13-42, (1956) 37-76, (1957) 55-80.

[18] G. Faltings, *Endlichkeitssatze fur abelsche Varietten ber zahlkorpern*, Invent. Math. 73 (1983), 349-366.

[19] N. Freitas, B. Le Hung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*, Invent. Math., 201 (2015), 159-206.

[20] D. Goldfeld *The conjectures of Birch and Swinnerton-Dyer and the class numbers of imaginary quadratic fields*, in *Journees arithmetiques de Caen*, Asterisque 41-42 (1977), 219-227.

[21] D. Goldfeld *Conjectures on elliptic curves over quadratic fields*, in *Number Theory, Carbondale 1979*, Springer Lecture Notes 751 (1979), 108-118.

[22] B. Gross, *Heegner Points on $X_0(N)$*, in *Modular Forms* (ed. R. A. Rankin). Ellis Horwood (1984).

[23] B. Gross, *Kolyvagin's work on modular elliptic curves* in *L-functions and arithmetic (Durham 1989)*, London Math. Soc. Lecture Notes 153 (1991), 235-256.

[24] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225-320.

[25] K. Heegner, *Diophantische analysis und modulfunktionen*, Math. Z. 56 (1952), 227-253.

[26] K. Kato, *p-adic Hodge theory and values of zeta functions and modular forms* in *Cohomologies p-adiques et applications arithmetiques III*, Asterisque 295 (2004), 117-290.

[27] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a class of Weil curves*, Izv. Akad. Nauk SSSR 52 (1988), translation Math. USSR-Izv. 32 (1989), 523-541.

[28] S. Kobayashi, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. 191 (2013), 527-629.

[29] G. Kings, D. Loeffler, S. Zerbes, *Rankin-Eisenstein classes and explicit reciprocity laws* arXiv.org/abs/1503.02888.

[30] A. Lei, D. Loeffler, S. Zerbes *Euler systems for Rankin-Selberg convolutions of modular forms*, Ann. of Math., 180 (2014), 653-771.

[31] D. Loeffler, S. Zerbes, *Rankin-Eisenstein classes in Coleman families*, arXiv.org/abs/1506.06703.

[32] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES 47 (1977), 33-186.

[33] B. Mazur, *Rational points of abelian varieties in towers of number fields*, Invent. Math. 18 (1972), 183-266.

[34] B. Mazur, P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. 25 (1974), 1-61.

[35] R. Miller, *Proving the Birch-Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, London Math. Soc. J. Comput. Math. 14(2011), 327-350.

[36] R. Miller, M. Stoll, *Explicit isogeny descent on elliptic curves*, Math. Comp. 82 (2013), 513-529.

[37] K. Murty and R. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math., 133 (1991), 447-475.

[38] J. Oesterle, *Nombres de classes de corps quadratiques imaginaires*, Seminaire N. Bourbaki, 1983-1984, 631, 309-323.

[39] D. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. 75 (1984), 404-423

[40] B. Perrin-Riou, *Fonctions L p-adiques, thorie d'Iwasawa, et points de Heegner*, Bull. Soc. Math. France, 115(1987), 399-456.

[41] R. Pollack, K. Rubin *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. 159 (2004), 447-464.

[42] K. Rubin, *The main conjectures of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25-68.

[43] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), 527-560.

[44] K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 93 (1988), 701-713.

[45] P. Schneider, *p-adic height pairings II*, Invent. Math. 79 (1985), 329-374.

[46] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan 11 (1971).

[47] J. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math. 106, 1986, Springer.

[48] C. Skinner, E. Urban, *The Iwasawa main conjecture for GL_2*, Invent. Math. 195 (2014), 1-277.

[49] N. Stephens, *The Diophantine equation $x^3 + y^3 = Dz^3$ and the conjectures of Birch and Swinnerton-Dyer*, Crelle 231 (1968), 121-162.

[50] J. Tate, *Algorithm for determining the type of singular fiber in an elliptic pencil*, Modular Functions of One Variable IV, Springer Lecture Notes 476 (1975), 33-52.

[51] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Seminaire N. Bourbaki, 1964-1966, 306, 415-440.

[52] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Int. Cong. Math., Stockholm (1962), 288-295.

[53] J. Thorne, *Elliptic curves over $\mathbb{Q}_\infty$ are modular*, to appear

[54] Y. Tian, *Congruent numbers with many prime factors*, Proc. Natl. Acad. Sci. USA 109 (2012), 21256-21258.

[55] Y. Tian, *Congruent Numbers and Heegner Points*, Cambridge Journal of Mathematics, 2 (2014), 117-161.

[56] X. Wan, *Iwasawa main conjectures for supersingular elliptic curves*, arXiv.org/abs/1411.6352

[57] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. 172 (2010), 567-596.

[58] R. Yager, *On two variable p-adic L-functions*, Ann. of Math. 115 (1982), 411-449.

[59] S. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. 153 (2001), 27-147.

[60] W. Zhang, *Selmer group and the indivisibility of Heegner points*, Cambridge Journal of Mathematics 2 (2014), 191-253.

John Coates
Emmanuel College
Cambridge CB2 3AP, England.