The Oldest Problem

by John Coates*†

Introduction

One of the great mysteries of mathematics is the fact that the most primitive of all mathematical objects, namely the integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ and the rational numbers $\mathbb{Q} = \{m/n : m, n \in \mathbb{Z}, \text{with } n \neq 0\}$, have certain deep and very beautiful properties, which often cannot be at all explained by elementary arithmetic. It is the role of number theory to uncover these properties, usually by numerical experiment, and to try and prove them. In my lecture today, I want to discuss one example, which remains the oldest major unsolved problem in number theory, and explain some important recent progress on it. This problem also exhibits one of the most striking examples of a purely elementary arithmetic phenomena, which can only be explained in terms of L-functions (see Conjecture 1.2 below). An integer $D \geq 1$ is defined to be a *congruent number* if it is the area of a right-angled triangle, all of whose sides have lengths in $\mathbb{Q}$. For example, 5, 6, and 7 are all congruent numbers, because of the existence of the right-angled triangles with side lengths given respectively by (40/6, 9/6, 41/6), (3, 4, 5), and (288/60, 175/60, 337/60). Note that, because of similarity considerations, we need only consider square free positive integers in determining whether a number is congruent or not, and we shall always assume in this lecture that D is square free. The origins of the search for congruent numbers lies shrouded in mystery in the ancient Eastern world. The written history can be traced back at least to the tenth century Arab manuscript of al-Kazin in the Bibliotheque Nationale de Paris, which gives quite extensive tables of congruent numbers. The first known European manuscript related to congruent numbers is Fibonacci's book *Liber Quadratorum* published in 1225, in which he points out that 5 and 7 are congruent numbers, and claims without proper justification that 1 is not. We owe to Fermat, probably a little before 1640 (see [24], Chapter 2, §10), the first proof that 1 is not a congruent number, and the method of *infinite descent* which Fermat introduced in his proof underlies all subsequent work to the present day. Fermat also pointed out that his method proves that, for $n = 4$, the equation

$$x^n + y^n = z^n$$

has no solution in integers x, y, z with $xyz \neq 0$, and conjectured that the same assertion holds for all integer exponents $n \geq 3$. This celebrated conjecture was at last finally proven by Wiles [26] in 1995.

Today, vast tables of square free congruent numbers exist, created always by the naive procedure of explicitly writing down a corresponding rational right-angled triangle of the given area. These tables begin with

(1.1)
$$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 46, 47,$$

and it is known that this is the complete list of square free congruent integers D with $1 \leq D \leq 50$. The two fundamental open problems about congruent numbers are the following conjectures:-

Conjecture 1.1. *There exists an algorithm which will decide in a finite number of steps whether or not a given integer $D \geq 1$ is a congruent number or not.*

Conjecture 1.2. *Every integer D of the form $8n+5, 8n+6, 8n+7$, for some integer $n \geq 0$, is a congruent number.*

In the case of the first conjecture, what is curious is that in practice it is usually possible to decide fairly rapidly whether or not a given numerical $D \geq 1$ is

* Emmanuel College, Cambridge, United Kingdom
E-mail: jhc13@dpmms.cam.ac.uk
† This is the written version of the first ICCM Sze Lim Lecture, which was given at Tsinghua University on April 24, 2017.

congruent or not. Nevertheless, noone has ever succeeded in proving theoretically that, for any D, the process will always terminate after a finite number of steps. The second conjecture seems totally inexplicable in terms of elementary arithmetic, and it was only after the discovery of the conjecture of Birch and Swinnerton-Dyer in the early 1960's that a probable explanation for it in terms of L-functions was uncovered.

It has long been known that the problem of deciding whether a given integer is a congruent number or not is equivalent to the following statement about the existence of a non-trivial rational point on a curve.

Lemma 1.3. *Let D be an integer ≥ 1. Then D is a congruent number if and only if there exists a point (x,y), with both coordinates x,y in $\mathbb{Q}$ and $y \neq 0$, on the curve*

$$E^{(D)} : y^2 = x^3 - D^2 x. \tag{1.2}$$

Proof. Suppose first that (x,y) is a point on $E^{(D)}$ with x and y in $\mathbb{Q}$, and $y \neq 0$. Then

$$a = \left|\frac{(D^2-x^2)}{y}\right|,\ b = \left|\frac{2Dx}{y}\right|,\ c = \left|\frac{D^2+x^2}{y}\right|$$

are the sides of a right-angled triangle, whose area is D. Conversely, suppose we are given positive rational numbers a,b,c such that $a^2+b^2=c^2$ and $ab/2 = D$. One verifies easily that

$$x = \frac{D(a+c)}{b},\ y = \frac{2D^2(a+c)}{b^2}$$

is a rational point on $E^{(D)}$, with $y \neq 0$. This completes the proof. □

The curve $E^{(D)}$ is non-singular and has genus 1, and the projective version of it, given by the equation $y^2z = x^3 - D^2xz^2$, has a unique rational point at infinity $\mathcal{O}$ with projective coordinates $x=0, y=1, z=0$, making it into what is called an *elliptic curve*. What is important for us is that its set of rational points $E^{(D)}(\mathbb{Q})$ consisting of the point $\mathcal{O}$ and all points (x,y) on $E^{(D)}$ with coordinates x,y in $\mathbb{Q}$ has a natural structure as an abelian group. This abelian group law, which we will denote by $\oplus$, is characterized by the property that $\mathcal{O}$ is the zero element, and points P,Q,R in $E^{(D)}(\mathbb{Q})$ satisfy $P \oplus Q \oplus R = \mathcal{O}$ whenever P,Q,R are the points of intersection, taken with multiplicity, of some straight line with $E^{(D)}$. Moreover, it is not difficult to prove, by a classical argument, that the only points of finite order in $E^{(D)}(\mathbb{Q})$ are the 4 points $\mathcal{O}, (0,0), (D,0), (-D,0)$, and that the latter three points are of order 2. Thus the above lemma can be rephrased as follows:-

Corollary 1.4. *$D \geq 1$ is congruent if and only if $E^{(D)}(\mathbb{Q})$ is infinite.*

An immediate consequence of this corollary is that if there exists one right-angled triangle with rational side lengths of area D, then there are infinitely many such triangles.

Fermat's highly original proof that 1 is not a congruent number introduced the notion of *infinite descent*, and used it to show that the only rational points on the curve $E^{(1)}$ are the four obvious points $\mathcal{O}, (0,0), (1,0), (-1,0)$. About three hundred years later, Mordell [15] beautifully generalized Fermat's argument to prove that the abelian group $E^{(D)}(\mathbb{Q})$ is finitely generated for all non-zero positive integers D, and in fact showed more generally that this statement holds for every elliptic curve defined over $\mathbb{Q}$. Thus, by the structure theory of finitely generated abelian groups, it follows from Mordell's theorem that we must have

$$E^{(D)}(\mathbb{Q}) = \mathbb{Z}^{g_D} \oplus T, \tag{1.3}$$

where T is isomorphic to a product of two cyclic groups of order 2, and g_D is some integer ≥ 0. In particular, D will be a congruent number if and only if $g_D > 0$. One of the great unresolved mysteries of number theory is to somehow discover a stronger form Mordell's descent argument to show that it will always infallibly decide, in a finite number of steps, whether or not $g_D > 0$. Our inability to do this to date is why Conjecture 1.1 still remains open. We shall return to this question later.

In the early 1960's, Birch and Swinnerton-Dyer [2, 3] made the revolutionary discovery, as a special case of a general conjecture for all elliptic curves defined over $\mathbb{Q}$, that the question of whether or not D is congruent is related to L-functions. The first person to define and use L-functions to prove deep arithmetic results was Dirichlet [5], who in 1837 proved the existence infinitely primes in an arithmetic progression with prime modulus, and also established a remarkable exact formula, which had been conjectured earlier by Jacobi, for the order of the group of ideal classes of an imaginary quadratic field of prime discriminant. Later in the 19th century, German mathematicians realized that many other L-functions play an important role in number theory, and today these L-series are ubiquitous in the subject. As is the case for all L-functions of number theory, the L-series attached to $E^{(D)}$, which we shall denote by $L(E^{(D)},s)$, is defined by an Euler product. Let $\mathcal{O}$ denote the set of all complex numbers of the form $a+bi$, where a,b lie in $\mathbb{Z}$ and, as usual, $i^2 = -1$. Note that $\mathcal{O}$ is closed under addition and multiplication, and so is a subring of the field of complex numbers $\mathbb{C}$. If z is an element of $\mathcal{O}$, we write as usual $\bar{z}$ for its complex conjugate. Now $\mathcal{O}$ obviously contains the group of all 4-th roots of unity, and it is easily verified that no two distinct 4-th roots of unity are congruent modulo $2+2i$ in the

ring $\mathcal{O}$. Let p be any prime number which does not divide $2D$, where we recall that D is always assumed to be square free. If $p \equiv 3 \bmod 4$, we define $a_p = 0$. Suppose now that $p \equiv 1 \bmod 4$. Since the multiplicative group of the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a cyclic group of order $p-1$, we follow Legendre and define the symbol (D/p) to be $+1$ or -1, according as the image of D in $\mathbb{F}_p$ is a square or a non-square. It is then not difficult to see that there exists an element α_p in $\mathcal{O}$ such that $\alpha_p \equiv (D/p) \bmod 2+2i$ and $\alpha_p \bar{\alpha}_p = p$. Note that the complex conjugate $\bar{\alpha}_p$ of α_p has the same properties, and the rational integer $a_p = \alpha_p + \bar{\alpha}_p$ is then unique. For every prime number p, which does not divide $2D$, it can be shown that the number of solutions in $\mathbb{F}_p$ of the congruence

$$y^2 \equiv x^3 - D^2 x \bmod p$$

is precisely equal to $p - a_p$. We now define the L-function $L(E^{(D)}, s)$ by the Euler product

$$L(E^{(D)}, s) = \prod_{(p,2D)=1} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \tag{1.4}$$

which converges to a holomorphic function of the complex variable s in the half plane given by the real part of s is greater than $3/2$, because $|a_p| \leq 2\sqrt{p}$ for all primes p with $(p, 2D) = 1$. Of course, the Euler product (1.4) does not converge at the point $s = 1$, and so to make sense of the conjecture of Birch and Swinnerton-Dyer, we must find an analytic continuation of the function $L(E^{(D)}, s)$ to a region of the complex plane which includes $s = 1$. In fact, such an analytic continuation was already discovered by German mathematicians in the 19th century (Eisenstein and Kronecker [25], and Hecke [9]), and we merely state the final result which emerges from their work (see Koblitz [14] for a good self contained account).

Theorem 1.5. *Let $C(D) = 32D^2$ or $16D^2$, according as the square free positive integer D is odd or even, and put $\Phi(E^{(D)}, s) = C(D)^{s/2}(2\pi)^{-s}\Gamma(s)L(E^{(D)}, s)$, where $\Gamma(s)$ is the classical Gamma function. Then $\Phi(E^{(D)}, s)$ has an analytic continuation to the whole complex s-plane, and satisfies the functional equation*

$$\Phi(E^{(D)}, s) = w(D)\Phi(E^{(D)}, 2-s), \tag{1.5}$$

where $w(D) = +1$ if $D \equiv 1, 2, 3 \bmod 8$ and $w(D) = -1$ if $D \equiv 5, 6, 7 \bmod 8$.

Note that $s = 1$ is the only fixed point of the map $s \mapsto 2 - s$. Since $\Gamma(1) = 1$, we conclude immediately from the theorem that $L(E^{(D)}, s)$ is holomorphic at $s = 1$. Moreover, from the functional equation (1.5), we see that $L(E^{(D)}, s)$ has a zero of even or odd multiplicity at $s = 1$, according as $w(D) = +1$ or $w(D) = -1$. The mystery discovered by Birch and Swinnerton-Dyer is that the purely arithmetic question of whether or not $g_D > 0$ seems to be precisely related to the question of whether or not $L(E^{(D)}, 1) = 0$.

Conjecture 1.6. *We have $g_D > 0$ if and only if $L(E^{(D)}, 1) = 0$.*

Note that a poof of this conjecture would immediately solve the ancient Conjectures 1.1 and 1.2. Indeed, it is well known (see, for example, Tunnell [23]) that there are simple algorithms which will always decide in a finite number of steps whether or not $L(E^{(D)}, 1) = 0$, and so Conjecture 1.6 implies Conjecture 1.1. Moreover, it is clear from Theorem (1.5) that $L(E^{(D)}, 1) = 0$ whenever D is a positive square free integer with $D \equiv 5, 6, 7 \bmod 8$, whence Conjecture 1.6 also implies Conjecture 1.2. One direction of Conjecture 1.6 was proven 40 years ago by Wiles and myself [4], using p-adic ideas from Iwasawa theory inspired by Iwasawa's great paper [12].

Theorem 1.7. *If $g_D > 0$, then $L(E^{(D)}, 1) = 0$.*

Unfortunately, a general proof of the implication in the opposite direction, i.e. the assertion that $L(E^{(D)}, 1) = 0$ implies that $g_D > 0$, still seems to be a long way off. However, as we shall briefly explain later, a better understanding of the Iwasawa theory of the elliptic curve $E^{(D)}$ at the prime $p = 2$ could hopefully lead some day to a proof of a weaker but very useful partial result in this direction. The one deep partial converse result established so far is due to Gross and Zagier [8], who found a remarkable proof of a conjecture of Birch and Stephens, which, in turn, had grown out of the earlier work of Heegner [11].

Theorem 1.8. *If $L(E^{(D)}, s)$ has a simple zero at $s = 1$, then $g_D > 0$.*

Chinese mathematicians, notably C. Zhao and Y. Tian, have been the leaders in showing how to exploit Theorems 1.7 and 1.8 to study congruent numbers, and we shall briefly discuss their work later.

Goldfeld's Conjecture

While every square free integer in the residue classes of $5, 6, \text{or} 7$ modulo 8 is conjecturally a congruent number, the situation is very different for the square free integers which lie in the residue classes of $1, 2, \text{or} 3$ modulo 8. Indeed, the list (1.1) of all square free congruent numbers ≤ 50 shows that 34 and 41 are the only two congruent numbers in this range in these latter three residue classes modulo 8. In fact, this paucity of congruent numbers in these three residue classes continues if one considers much more extensive tables. A conjectural explanation for this phenomenon was first proposed by Goldfeld [7]. We write $\mathcal{D}(e)$ for the set of all square free positive integers which lie in the residue classes of $1, 2, \text{or} 3$ modulo 8, and $\mathcal{D}(o)$ for the set of all square free positive integers which lie in the residue classes of $5, 6, \text{or} 7$ modulo 8.

Writing $\mathcal{W}$ for the set of all square free positive integers, we say that any subset $\mathcal{U}$ of $\mathcal{W}$ has density δ, where $0 \leq \delta \leq 1$, if

$$\lim_{M\to\infty} \#(\mathcal{U}_M)/\#(\mathcal{W}_M) = \delta\,;$$

here $\mathcal{W}_M$ (resp. $\mathcal{U}_M$) denotes the set of D in $\mathcal{W}$ (resp. D in $\mathcal{U}$) with $D \leq M$. Then Goldfeld's conjecture is the following assertion.

Conjecture 2.1. *The subset of all $D \in \mathcal{D}(e)$ where $L(E^{(D)},s)$ vanishes at $s=1$ has density 0, and similarly the subset of all D in $D \in \mathcal{D}(o)$ where $L(E^{(D)},s)$ has a zero at $s=1$ of order strictly greater than 1 has density 0.*

Of course, in view of Theorem 1.7, we see that, in particular, Goldfeld's conjecture would imply that the set of all square free congruent numbers lying in the residue classes of $1,2,\text{or}\,3$ modulo 8, has density zero, an assertion which no longer explicitly involves L-functions. The first important progress on this question was made by Heath-Brown [10], who showed that at least 41.9% of all integers in $\mathcal{D}(e)$ were not congruent numbers. Very recently, a remarkable preprint of Smith [18] gives a full proof of the general assertion.

Theorem 2.2 (Smith)**.** *The set of all square free congruent numbers in $\mathcal{D}(e)$ has density 0.*

The arguments of Heath-Brown and Smith rely crucially on techniques from classical analytic number theory. However, beyond implicitly making use of the value of the root number $w(D)$ given by Theorem 1.5, it should be stressed that their methods at present make no explicit use of the analytic properties of the complex L-function $L(E^{(D)},s)$. As far as congruent numbers lying in the set $\mathcal{D}(o)$ is concerned, the best result at present is due to the work of Tian-Yuan-Zhang [22], and Smith [19], combined with Theorem 1.8 of Gross-Zagier.

Theorem 2.3. *There is an explicit subset of $\mathcal{D}(o)$ with density at least $1/2$ such that every D lying in this subset is a congruent number.*

Unlike Theorem 2.2, the proof of this result does make crucial use of the L-series $L(E^{(D)},s)$, and proceeds by showing that there is an explicit subset of $\mathcal{D}(o)$ with density at least $1/2$ such that $L(E^{(D)},s)$ has a simple zero at $s=1$, whence the assertion follows from Theorem 1.8.

Infinite Descent

Ultimately, all important results we know about the congruent number problem, follow from some form of analysis of the procedure of infinite descent, which was first introduced by Fermat. For simplicity, write $E = E^{(D)}$. Let $p = 2,3,5,\ldots$ be any prime number, and $n \geq 1$ a positive integer. If P is any point in $E(\mathbb{Q})$, the naive idea underlying infinite descent theory is to try and find a simpler or smaller point, in a sense which has to be made precise, by dividing P by p^n. Of course, this is not always possible in the abelian group $E(\mathbb{Q})$ itself, and this is what leads us into Galois cohomology. Indeed, writing $\bar{\mathbb{Q}}$ for a fixed algebraic closure of $\mathbb{Q}$, the abelian group $E(\bar{\mathbb{Q}})$ of points on E with coordinates in $\bar{\mathbb{Q}}$ is divisible, and so we can always find a point R in $E(\bar{\mathbb{Q}})$ such that $p^nR = P$. Of course, R is then only determined up to the addition of any element of $E(\bar{\mathbb{Q}})$ which is annihilated by p^n. Let $G_{\mathbb{Q}}$ denote the Galois group of $\bar{\mathbb{Q}}$ over $\mathbb{Q}$, which operates on the left on $E(\bar{\mathbb{Q}})$ via its action on the coordinates of a point. Defining $f_P(\sigma) = \sigma R \ominus R$ for $\sigma \in G_{\mathbb{Q}}$, we see immediately that f_P defines a 1-cocycle on $G_{\mathbb{Q}}$ with values in the Galois module $E[p^n]$ of all points in $E(\bar{\mathbb{Q}})$ of order dividing p^n. If A is any discrete $G_{\mathbb{Q}}$-module, we write, as usual, $H^1(\mathbb{Q},A)$ for the usual cohomology group $H^1(G_{\mathbb{Q}},A)$ of continuous 1-cocycles for this action. In particular, by mapping P to the cohomology class of f_P, we obtain a canonical homomorphism

$$\kappa(p^n) : E(\mathbb{Q})/p^nE(\mathbb{Q}) \to H^1(\mathbb{Q},E[p^n]), \tag{3.1}$$

which is easily seen to be injective, and to have cokernel equal to $H^1(\mathbb{Q},E(\bar{\mathbb{Q}}))[p^n]$; in general if B is any abelian group we write $B[p^n]$ for the subgroup of all points of order dividing p^n. Similarly, if v is any place of $\mathbb{Q}$, we write $\mathbb{Q}_v$ for the completion of $\mathbb{Q}$ at v, $\bar{\mathbb{Q}}_v$ for its algebraic closure, and G_v for the Galois of $\bar{\mathbb{Q}}_v$ over $\mathbb{Q}_v$. Exactly, as above we obtain a canonical injective homomorphism

$$\kappa_v(p^n) : E(\mathbb{Q}_v)/p^nE(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v,E[p^n]), \tag{3.2}$$

with cokernel equal to $H^1(\mathbb{Q}_v,E(\bar{\mathbb{Q}}_v))[p^n]$. Moreover, for each such v, we can identify the local Galois group G_v with a subgroup of $G_{\mathbb{Q}}$, and then the restriction map on cocycles gives a canonical homomorphism

$$r_v(p^n) : H^1(\mathbb{Q},E[p^n]) \to H^1(\mathbb{Q}_v,E[p^n]). \tag{3.3}$$

The all important Selmer group $Sel_{p^n}(E)$ is then defined to be the subgroup of $H^1(\mathbb{Q},E[p^n])$ consisting all elements z such that $r_v(p^n)(z)$ lies in the image of $\kappa_v(p^n)$ for all places v of $\mathbb{Q}$. It is not too difficult to prove that $Sel_{p^n}(E)$ is always a finite group, which, at least in theory, can always be computed in a finite number of steps. Moreover, simple diagram chasing shows that we always have the exact sequence

$$0 \to E(\mathbb{Q})/p^nE(\mathbb{Q}) \to Sel_{p^n}(E) \to Ш(E)[p^n] \to 0, \tag{3.4}$$

where $Ш(E)$ is the Tate-Shafarevich group of E defined by

$$Ш(E) = Ker(H^1(\mathbb{Q},E(\bar{\mathbb{Q}})) \to \prod_v H^1(\mathbb{Q}_v,E(\bar{\mathbb{Q}}_v))).$$

This group $Ш(E)$ is unquestionably one of the most mysterious, and so far largely inaccessible, objects in number theory. It is always conjectured to be finite, but at present this is only known to be true when the complex L-series $L(E,s)$ has a zero at $s=1$ of order at most 1. Some indication of its importance for the congruent number problem is given by the following theorem due to the Dokchitser brothers [6]. If B is any abelian group, $B(p)$ will denote the subgroup of elements of B of p-power order.

Theorem 3.1. *Let D be any square free positive integer lying in the residue classes of $5, 6,$ or 7 modulo 8. If there exists a prime number p such that $Ш(E^{(D)})(p)$ is finite, then D is a congruent number.*

Unfortunately, at present we have no idea of how to prove that, for any given D, there does always exist at least one prime p with $Ш(E^{(D)})(p)$ finite.

Smith's Work

We now briefly discuss the ideas which have led to the proof of Theorem 2.2 in [18], building on the earlier work in [10], [13], [20]. Unlike the Iwasawa theory to be discussed in the next section, the arguments from analytic number theory used in this work seem to only work for studying the p-power Selmer groups $Sel_{p^n}(E^{(D)})$ for the special prime $p=2$. For each $n \geq 1$, the abelian group $2^{n-1}Sel_{2^n}(E^{(D)})$ is a finite dimensional vector space over the field $\mathbb{F}_2$ with 2 elements. For $n \geq 2$, we define

$$r_D(n) = dim_{\mathbb{F}_2}(2^{n-1}Sel_{2^n}(E^{(D)})), \tag{4.1}$$

and for $n=1$, we take $r_D(1) = dim_{\mathbb{F}_2}(Sel_2(E^{(D)})) - 2$. It is clear from (3.4) that $r_D(n) \geq g_D$, for all $n \geq 1$, where g_D is the rank of $E^{(D)}(\mathbb{Q})$. Moreover, we have

$$\lim_{n\to\infty} r_D(n) = g_D \tag{4.2}$$

if, and also only if by a classical result from Galois cohomology, the group $Ш(E^{(D)})(2)$ is finite. Recall that an $m \times m$ matrix A with entries in $\mathbb{F}_2$ is defined to be *alternating* if $A^t = -A$, and the diagonal elements of A are zero. Take m, j to be any pair of integers satisfying $m \geq j \geq 0$. Define $\delta(m,j)$ to be the probability that an arbitrary $m \times m$-alternating matrix with entries in $\mathbb{F}_2$ has a kernel of dimension j. Recall that $\mathcal{W}$ denotes the set of all square free positive integers. For any $n > 1$, we define

$$\Re_n(m,j) = \{D \in \mathcal{W} : r_D(n-1) = m \text{ and } r_D(n) = j\},$$

and

$$\Im_n(m) = \{D \in \mathcal{W} : r_D(n-1) = m\}.$$

As before, if M is any positive integer, and $\mathcal{U}$ is a subset of $\mathcal{W}$, then $\mathcal{U}_M$ will denote the set of all U in $\mathcal{U}$ with $U \leq M$. Then the main result of [18] is as follows.

Theorem 4.1. *. Let m, j be arbitrary integers with $m \geq j \geq 0$. Then, for all integers $n > 1$, the limit*

$$\lim_{M\to\infty} \#(\Re_n(m,j)_M)/\#(\Im_n(m)_M) \tag{4.3}$$

exists, and is equal to $\delta(m,j)$.

What is remarkable about this result is that, while it does not tell us the precise structure of any particular 2^n-Selmer group, it does give the asymptotic distribution of these groups, and shows that this asymptotic distribution is exactly as predicted by the probabilistic model given in [1]. Moreover, it is shown in [1] that Theorem 2.2 then follows from Theorem 4.1.

Iwasawa Theory and Other Methods

The idea underlying Iwasawa theory is to precisely relate the Selmer groups $Sel_{p^n}(E^{(D)})$, for all primes p and all sufficiently large integers $n \geq 1$, to the behaviour at the point $s=1$ in the p-adic plane of a p-adic analogue of the complex L-series $L(E^{(D)},s)$. This connexion is achieved by first proving a so called *main conjecture* of Iwasawa theory for the Selmer group of $E^{(D)}$ over an appropriate infinite Galois extension, with Galois group isomorphic to the additive group of p-adic integers $\mathbb{Z}_p$ of the field $\mathbb{Q}(i)$. Here is a typical example of the type of result, which can be proven at present by these methods (see [17] and [16]).

Theorem 5.1. *Let p be any prime which does not divide $2D$. Then $L(E^{(D)},1) \neq 0$ if and only if both $g_D = 0$ and $Ш(E(D))(p)$ is finite.*

Unfortunately, this result as it stands is of no real use in proving the non-vanishing of $L(E^{(D)},s)$ at the point $s=1$ because we have no alternative method at present for proving that $Ш(E(D))(p)$ is indeed finite for some prime p which does not divide $2D$. For this and other reasons, there would be great interest in establishing this theorem also for the primes p which divide $2D$, especially in the most interesting case of the prime $p=2$, since, as Alexander Smith has pointed out to me, his methods in [18] do indeed show that we have both $g_D = 0$ and $Ш(E^{(D)})(2)$ finite for a set of square free D of density 1 lying in the residue classes of 1, 2, and 3 modulo 8. We remark that $E^{(D)}$ has potential supersingular reduction at the prime $p=2$, and this seems to be one of the main reasons for the technical difficulties which arise when one attempts to prove a suitable main conjecture of Iwasawa theory for our curve at $p=2$.

We also mention two other results proving the non-vanishing of $L(E^{(D)},1)$ when $g_D = 0$ and $Ш(E^{(D)})(2)$ is finite. Firstly, Zhao [27], [28], [29] has shown that $L(E^{(D)},1) \neq 0$ for certain explicit infinite families of square free $D \equiv 1 \bmod 8$ with many prime factors, which have $Ш(E^{(D)})(2)$ either trivial or of order 4. Secondly. the results of [22], when combined with [19], prove, in general, that $L(E^{(D)},1) \neq 0$ for all positive square free D lying in the residue classes of 1, 2, or 3 modulo 8 such that both $g_D = 0$ and $Ш(E^{(D)})(2) = 0$. The arguments used to establish these results depend on the ingenious use of explicit expressions for $L(E^{(D)},1)$, and make no appeal to ideas from Iwasawa theory.

Heegner [11] was the first person to prove that, in each of the residue classes of 5, 6, or 7 modulo 8, every square free positive integer D with exactly one odd prime factor is a congruent number. The next major progress was made by Tian [21], who introduced a powerful new induction argument to prove the following result.

Theorem 5.2. *Let D be a square free positive integer lying in the residue classes of 5, 6, or 7 modulo 8 such that its odd part N has a prime factorization of the form $N = p_0 p_1 \dots p_k$ where $k \geq 0$, and $p_i \equiv 1 \bmod 8$ for $1 \leq i \leq k$. Assume that the ideal class group of the field $K = \mathbb{Q}(\sqrt{-N})$ has no element of exact order 4. Then D is a congruent number, and $L(E^{(D)},s)$ has a simple zero at $s = 1$.*

In order to strengthen this result to the statement of Theorem 2.3, one first needs the following result due to Heath-Brown [10] and Kane [13]. For $k = 5,6,7$, let $\mathcal{W}_k$ be the set of all square free positive integers D with $D \equiv k \bmod 8$. Recall that

$$r_D(1) = dim_{\mathbb{F}_2}(Sel_2(E^{(D)})) - 2 = g_D + dim_{\mathbb{F}_2}(Ш(E^{(D)})[2].$$

We define $\mathcal{M}_k$ to be the subset of all $D \in \mathcal{W}_k$ with $r_D(1) = 1$.

Theorem 5.3. *For $k = 5,6,7$, the subset $\mathcal{M}_k$ of $\mathcal{W}_k$ has density equal to $2\prod_{n=1}^{n=\infty}(1+2^{-n}) = 0.8388\dots$.*

On the other hand, Smith [19] has shown that, for each of $k = 5,6,7$, a remarkable explicit formula for the value at $s = 1$ of the first derivative of $L(E^{(D)},s)$ proven in [22] enables one to establish the existence of an explicit subset $\mathcal{U}_k$ of $\mathcal{M}_k$ such that (i) $L(E^{(D)},s)$ has a simple zero at $s = 1$ for all $D \in \mathcal{U}_k$, and (ii) the density of $\mathcal{U}_k$ in $\mathcal{M}_k$ is equal to $3/4, 1/2, 3/4$, according as $k = 5,6,7$. Theorem 2.3 now follows from Theorems 1.8 and 5.3.

References

[1] M. Bhargava, D. Kane, H. Lenstra, B. Poonen, E. Rains *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Cambridge J. Math. 3 (2015), 275–321.

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

[5] P. Dirichlet *Mathematische Werke I*, Teubner, 313–342.

[6] T. Dokchitser, V. Dokcitser *On the Birch-Swinnerton-Dyer conjecture modulo squares*, Annals Math. 172 (2010), 567–596.

[7] D. Goldfeld *Conjectures on elliptic curves over quadratic fields*, in *Number Theory, Carbondale 1979*, Springer Lecture Notes 751 (1979), 235–256.

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

[9] E. Hecke *Mathematische Werke*, Vandenhoek and Ruprecht, 1959.

[10] R. Heath-Brown *The size of Selmer groups for the congruent number problem II*, Invent. Math. 118 (1994), 331–370.

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

[12] K. Iwasawa *On some modules in the theory of cyclotomic fields*, J. Math. Soc. Japan 20 (1964), 42–82.

[13] D. Kane *On the ranks of 2-Selmer groups of twists of a given elliptic curve*, Algebra Number Theory 7 (2013), 1253–1279.

[14] N. Koblitz *Introduction to elliptic curves and modular forms*, Springer, 1984.

[15] L. Mordell *On the rational solutions of indeterminate equations of the third and fourth degrees*, Proc. Cambridge Phil. Soc. 21 (1922), 179–192.

[16] R. Pollack, K. Rubin *The main conjecture for CM elliptic curves at supersingular primes*, Annals Math. 159 (2004), 447–464.

[17] K. Rubin *The one variable main conjecture for elliptic curves with complex multiplication*, London Math. Soc. Lecture Notes 153 (1991), 353–371.

[18] A. Smith 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, arXiv preprint arXiv:1702.02325v1.

[19] A. Smith *The congruent numbers have positive natural density*, preprint (2016).

[20] P. Swinnerton-Dyer *The effect of twisting on the 2-Selmer group*, Proc. Cambridge Phil. Soc. 145 (2008), 513–526.

[21] Y. Tian *Congruent numbers and Heegner points*, Cambridge J. Math. 2 (2014), 117–161.

[22] Y. Tian, X. Yuan, S. Zhang *Genus periods, genus points, and the congruent number problem*, to appear in Asian Journal of Mathematics.

[23] G. Tunnell *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. 72 (1983), 323–334.

[24] A. Weil *Number Theory. An approach through history*, Birkhauser, 1983.

[25] A. Weil *Elliptic functions according to Eisenstein and Kronecker*, Springer, 1976.

[26] A. Wiles *Modular elliptic curves and Fermat's Last Theorem*, Annals Math. 141 (1995), 443–541.

[27] C. Zhao *A criterion for elliptic curves with lowest 2-power in* $L(1)$, Proc. Cambridge Phil. Soc. 121 (1997), 385–400.

[28] C. Zhao *A criterion for elliptic curves with second lowest 2-power in* $L(1)$, Proc. Cambridge Phil. Soc. 131 (2001), 385–404.

[29] C. Zhao *A criterion for elliptic curves with second lowest 2-power in* $L(1)$ *(II)*, Acta Math. Sinica 21 (2005), 961–976.