

Arithmetic of elliptic curves through the ages

R. Sujatha

August 5, 2009

This expository article is based on a talk that was given at the EWM Symposium held at Cambridge, U.K., in October 2007. The talk was aimed at a broad and general audience and I have tried to retain the flavour of the original lecture while converting it to its present text version. I have also attempted to make the bibliography as comprehensive as possible, but given the vastness of the subject, apologise for any inadvertent omissions. I would like to thank the organisers of the EWM conference for the invitation to speak, and John Coates for helpful discussions and comments. It is a pleasure to thank Chennai Mathematical Institute for hospitality accorded both at the time of preparing the talk, and later, while writing the article.

1 Introduction

The human mind has long contemplated the problem of solving cubic equations. A Babylonian clay tablet from around 1700 B.C., presently exhibited at the Berlin museum is perhaps the oldest piece of evidence in this direction. It lists many problems, some of which can be translated in modern mathematical language, to solving degree three polynomial equations in one variable [19]. Many centuries later, the Greeks, especially Diophantus, were concerned with rational and integral solutions of these equations. While the problem of solving cubic equations in one variable was settled by the 16th century, due to the efforts of del Ferro, Cardano, Tartaglia, Viète and others, mathematicians like Fermat, Euler, Lagrange began to uncover the deep arithmetical mysteries of cubic curves in the 17th and 18th century. In another direction, elliptic integrals arose from the study of the arc lengths of an ellipse, and the theory of elliptic equations grew out of this. We owe to Fermat the discovery of the procedure of infinite descent (see [32]), which he used to prove that $x^4 + y^4 = 1$ has no solution in the field \mathbb{Q} of rational numbers with $xy \neq 0$. He also pondered, leaving no written traces of any success, about the rational solutions of the equation $x^3 + y^3 = 1$. Non-singular cubic curves are the first non-trivial examples of projective curves. For an excellent historical survey of these subjects, see Weil [37]. In more recent times, the study of elliptic curves (see §2) has connections with areas as diverse as complex topology, algebraic geometry and of course, number theory. Some of the most striking unsolved problems of number theory are concerned with the study of rational points (that is, points with coordinates in \mathbb{Q}) on elliptic curves. One of our broad

aims in this article is to give an idea of how they provide a common ground for ancient and modern themes in number theory.

2 Elliptic curves and number theory

Algebraic curves are the simplest objects of study in algebraic geometry. Projective algebraic curves are classified, upto birational transformations, by a basic birational invariant, called the genus (see [17]). If the curve is a non-singular plane curve of degree d , then the genus is given by $(d - 1)(d - 2)/2$. An elliptic curve over a field F is a curve of genus 1 defined over F , together with a given F -rational point on the curve. When F has characteristic different from 2, we can always find an affine equation for E of the form

$$E : y^2 = f(x),$$

where $f(x)$ in $F[X]$ is a cubic equation with distinct roots. Assuming that F has characteristic different from 2 and 3, the Weierstrass equation for E takes the form (see [32])

$$y^2 = x^3 + Ax + B$$

with coefficients in F . The discriminant Δ of E is defined by

$$\Delta = -16(4A^3 + 27B^2)$$

and is a fundamental invariant associated to the elliptic curve. Another important invariant is the conductor of an elliptic curve, which has the same prime divisors as the discriminant. The interested reader is referred to [32] and [33] for details on the basic arithmetic theory of elliptic curves.

We denote by $E(F)$ the set of solutions of E over F together with the “point at infinity” [32]. This set then has an abelian group structure. When F is a number field (i.e. a finite extension of \mathbb{Q}), it is further a celebrated result of Mordell and Weil that $E(F)$ is a finitely generated abelian group. Thus we define an important arithmetic invariant, called the *algebraic rank* of E , as

$$g_{E/F} := \text{rank of } E(F).$$

For example, the curve E_1 over \mathbb{Q} defined by $y^2 = x^3 - x$ has algebraic rank zero while the curve E_2 over \mathbb{Q} given by $y^2 = x^3 - 17x$ has algebraic rank 2. The curve E_1 has discriminant 64, and conductor equal to 32, while for E_2 the discriminant is $2^6 \times 17^3$ and the conductor is $2^5 \times 17^2$. Cremona’s tables [15] gives a list of elliptic curves of small conductor along with their basic arithmetic data.

The primary reason for an abiding interest in this invariant is the important conjecture of Birch and Swinnerton-Dyer, formulated in the 1960’s, based on very strong numerical data. For simplicity, we assume that the curve E is defined over \mathbb{Q} . Then the *Hasse-Weil L-function* of E , denoted $L(E, s)$ is a function of the complex variable s and is a

vast generalisation of the classical Riemann-zeta function. It is defined using the integers $a_p := 1 + p - \#E(\mathbb{F}_p)$ as p varies over the prime numbers; here $\#E(\mathbb{F}_p)$ denotes the number of points on the reduction modulo p of the elliptic curve with coordinates in \mathbb{F}_p , with p a prime of good reduction (see [30], [32] for more details on reduction of elliptic curves). It was classically known that it converges when the real part of s is strictly greater than $3/2$. Let Δ_E denote the minimal discriminant of a generalised Weierstrass equation for the curve E [32, Chap. VII]. The Euler product expression for $L(E, s)$ is given by

$$L(E, s) = \prod_{p \nmid \Delta_E} (1 - a_p p^{-s} + (p^{1-2s}))^{-1} \prod_{p \mid \Delta_E} (1 - a_q q^{-s})^{-1};$$

here for primes q dividing the discriminant of E , $a_q = 0, +1$ or -1 according as the singularity of the reduced elliptic curve over \mathbb{F}_q is a node, or a cusp with rational or irrational tangents over \mathbb{F}_q . Further, it has a Dirichlet series expansion given by

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

where the integers a_n are those defined above when n equals a prime p . The interested reader is referred to [32] and [15] for the explicit computation of the integers a_p .

The deep modularity results due to Wiles, Breuil *et al.* ([38], [4]) imply that the L -function has an analytic continuation for the entire complex plane. We remark that the L -function of E over a number field F , denoted $L(E/F, s)$ may be defined more generally for elliptic curves E/F , and it too is conjectured to have an analytic continuation over the entire complex plane. An elliptic curve E/\mathbb{Q} is said to have *complex multiplication* if the endomorphism ring of E over an algebraic closure $\bar{\mathbb{Q}}$ of \mathbb{Q} is strictly larger than the ring of integers. Both the curves E_1 and E_2 considered above are elliptic curves with complex multiplication as their endomorphism rings are given by the ring $\mathbb{Z}[i]$ of Gaussian integers. The element i acts as an endomorphism of the elliptic curve by sending a point (x, y) on the curve to $(-x, iy)$. At present the analytic continuation of the L -function is only known for elliptic curves with complex multiplication, thanks to work of Deuring and Weil. The *analytic rank* of E , denoted $r_{E/F}$ is defined to be the order of vanishing of $L(E/F, s)$ at $s = 1$. The Birch and Swinnerton-Dyer conjecture, in its weakest form, asserts that the analytic rank $r_{E/F}$ and the algebraic rank $g_{E/F}$ are equal.

Another important group associated to an elliptic curve defined over a number field F is the *Tate-Shafarevich group*, denoted $\text{III}(E/F)$. For any field K , and a discrete module M over the Galois group $G_K := \text{Gal}(\bar{K}/K)$, the first Galois cohomology group $H^1(G_K, M)$ is denoted by $H^1(K, M)$. For a place v of F , we denote the completion of F at v by F_v . The Tate-Shafarevich group of E/F is defined as the kernel

$$(1) \quad \text{III}(E/F) := \text{Ker} \left(H^1(F, E(\bar{F})) \longrightarrow \prod_v H^1(F_v, E(\bar{F}_v)) \right)$$

of the natural restriction map, where the product on the right is taken over all places v of F . The Tate-Shafarevich group is analogous to the class group occurring in algebraic

number theory (see §3). This group has an interesting geometric description in that it describes the defect of the ‘local-global principle’ for cubic curves. Thus, the non-trivial elements in it are classified by isomorphism classes of curves X defined over F which have the property that X becomes isomorphic to E over an algebraic closure \bar{F} of F and $X(F) = \emptyset$ while $X(F_v) \neq \emptyset$ for all the completions. The Tate-Shafarevich group is one of the most mysterious groups occurring in arithmetic and is always conjectured to be finite. The exact formulae of the Birch and Swinnerton-Dyer conjecture even predicts its order, and surprisingly predicts that this order is usually, but not always, one.

The above discussion places elliptic curves at the heart of one of the deepest conjectures in modern number theory. We now turn to an ancient problem in number theory which has been illuminated by the conjecture of Birch and Swinnerton-Dyer. An integer $N \geq 1$ is said to be a *congruent number* if N is the area of a right angled triangle all of whose sides have *rational* length (see [5] for an excellent survey on this subject). The study of congruent numbers is over a thousand years old and a list of examples of congruent numbers occurs in Arab manuscripts from the 10th century A.D. A later folklore conjecture asserts that

(2) Any positive integer $N \equiv 5, 6, 7 \pmod{8}$ is a congruent number.

This conjecture turns out to be closely related to the study of elliptic curves. Specifically, it is easily seen that an integer N is congruent if and only if the elliptic curve

$$(3) \quad E_N : y^2 = x^3 - N^2x$$

defined over \mathbb{Q} has the property that $E_N(\mathbb{Q})$ is infinite, or equivalently, $g_{E_N/\mathbb{Q}} > 0$. If one accepts the Birch and Swinnerton-Dyer conjecture, then it means that the analytic rank $r_{E/\mathbb{Q}} > 0$, in other words, that the L -function $L(E_N, s)$ vanishes at $s = 1$. The theory of root numbers ([3], see also §6), shows that in fact $L(E_N, s)$ always has a zero of odd multiplicity precisely for the integers N congruent to 5, 6, 7 modulo 8.

3 Iwasawa theory

Iwasawa theory is a relatively new area, owing its origins to the work of Iwasawa on cyclotomic \mathbb{Z}_p -extensions from the 1960’s (see [20]). Henceforth, p will denote an odd prime. For a number field F , recall that the *class group* of F is the group of fractional ideals modulo the principal ideals, and is well-known to be finite. The order of the class group is called the *class number* of F (cf. [26]). For s a complex variable, recall that $\zeta(s)$ is the classical Riemann-zeta function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$. Let μ_p denote the group of p -th roots of unity. The philosophy emerging from Iwasawa’s work initially provided an explanation for the link between special values of the Riemann zeta function and the class numbers of $\mathbb{Q}(\mu_p)$, as stated by Kummer’s criterion (cf. [36]) below:-

Theorem 3.1. (*Kummer's criterion*) Let $K = \mathbb{Q}(\mu_p)$ and let h_K denote the class number of K . Then p divides h_K if and only if p divides the numerator of at least one of the values of $\zeta(-1), \zeta(-2), \dots, \zeta(4-p)$.

Coates and Wiles recognised that techniques from Iwasawa theory could be used to attack the Birch and Swinnerton-Dyer conjecture. Recall that an elliptic curve E/\mathbb{Q} is said to have *complex multiplication* if $\mathbb{Z} \subsetneq \text{End}_{\overline{\mathbb{Q}}}(E)$ [32]. Coates and Wiles proved the first major general result about the Birch and Swinnerton-Dyer conjecture in [14] for elliptic curves with complex multiplication. A special case of their result is the following:

Theorem 3.2. (*Coates-Wiles*) [14] Let E/\mathbb{Q} be an elliptic curve with complex multiplication. Then $L(E, 1) = 0$ whenever $E(\mathbb{Q})$ is infinite. In other words, $g_{E/\mathbb{Q}} > 0$ implies that $r_{E/\mathbb{Q}} > 0$.

At present, Iwasawa theory has emerged as a systematic tool to attack the Birch and Swinnerton-Dyer conjecture using p -adic techniques. Let E be an elliptic curve over \mathbb{Q} , and let \mathbb{Z}_p (resp. \mathbb{Q}_p) denote the ring of p -adic integers (resp. the field of p -adic numbers). In the complex world, no general connection between the behaviour of the complex L -function $L(E, s)$ at $s = 1$, and $E(\mathbb{Q})$ or $\text{III}(E/\mathbb{Q})$ has ever been proven (there are some deep results due to Gross-Zagier-Kolyvagin, but they only apply to curves for which $L(E, s)$ has a zero at $s = 1$ of order at most 1). In the p -adic world however, such a link can be derived from the so-called “main conjectures” of Iwasawa theory, provided one replaces the complex L -function $L(E, s)$ by one of its p -adic avatars, at least when E has good ordinary reduction at the prime p . In particular, these main conjectures show that certain p -adic L -functions attached to E do have a zero at the point $s = 1$ in \mathbb{Z}_p of order at least the rank of $E(\mathbb{Q})$ plus the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ occurring in the p -primary subgroup $\text{III}(E/\mathbb{Q})(p)$ of $\text{III}(E/\mathbb{Q})$. We stress again that no result of this kind has ever been proven for the complex L -function. Here is an example of the type of result one can prove using these techniques:-

Theorem 3.3. (*Coates, Liang, Sujatha*) [10] Let E/\mathbb{Q} be an elliptic curve with complex multiplication. For all sufficiently large good ordinary primes p , the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ occurring in $\text{III}(E/\mathbb{Q})(p)$ is at most $2p - g_{E/\mathbb{Q}}$.

The basic idea of Iwasawa theory is to seek a simple connection between special values of L -functions and arithmetic of elliptic curves over certain infinite Galois extensions F_∞ of \mathbb{Q} . Viewed from this perspective, the Birch and Swinnerton-Dyer conjecture seems natural, as it elucidates how points of infinite order on E give rise to zeros of multiplicity at least $g_{E/\mathbb{Q}}$ of a p -adic L -function. Of course, it is beyond the scope of this article to develop the theory of p -adic L -functions in full detail and with greater precision. These are vast generalisations of the p -adic zeta functions that were studied by Kubota, Leopoldt and Iwasawa. We refer the interested reader to [6] for a detailed introduction to p -adic L -functions.

In the remaining sections, we shall outline how Iwasawa theory brings together three different strands viz. the conjecture (2) on congruent numbers, special values of L -functions, and algebraic questions on modules over Iwasawa algebras associated to compact p -adic Lie groups, with elliptic curves occurring as a common motif.

For an introduction to the Iwasawa theory of elliptic curves with complex multiplication, see [7]. The simplest elliptic curves without complex multiplication are the three curves of conductor 11 (see [15]). For a detailed study of their Iwasawa theory over the abelian extension $\mathbb{Q}(\mu_{p^\infty})$, see [11].

4 Iwasawa algebras

Let G be a profinite group, and p be an odd prime. The *Iwasawa algebra* of G , denoted $\Lambda(G)$ or $\mathbb{Z}_p[[G]]$, is the completed group algebra

$$\Lambda(G) := \varprojlim \mathbb{Z}_p[G/U];$$

here U varies over the open normal subgroups of G , $\mathbb{Z}_p[G/U]$ is the ordinary group ring over the finite group G/U and the inverse limit is taken with respect to the natural maps. Of special interest to us is the case when G is a compact p -adic Lie group. These groups were systematically studied by Lazard in his seminal work [24]. The simplest example is when G is isomorphic to \mathbb{Z}_p , in which case $\Lambda(G)$ is (non-canonically) isomorphic to the power series ring $\mathbb{Z}_p[[T]]$ in one variable. In classical cyclotomic theory, as considered by Iwasawa, one works with modules over this algebra (see [20], [12]). More generally, if $G \simeq \mathbb{Z}_p^d$, then $\Lambda(G)$ is isomorphic to the power series ring $\mathbb{Z}_p[[T_1, \dots, T_d]]$ in d variables. If G is commutative, then $\Lambda(G)$ is a commutative \mathbb{Z}_p -algebra.

In classical Iwasawa theory, the infinite Galois extensions F_∞ that were considered were mostly abelian with Galois group G a commutative p -adic Lie group. As a specific example, consider the extension $F_\infty = F(\mu_{p^\infty})$ in which case G is open in \mathbb{Z}_p , and isomorphic to \mathbb{Z}_p^\times if $F = \mathbb{Q}$. The Iwasawa algebra $\Lambda(G)$ is isomorphic to $\mathbb{Z}_p[\Delta][[T]]$, where Δ is cyclic of order dividing $p - 1$. Suppose E/F is an elliptic curve. For an odd prime p , consider the Galois extension

$$(4) \quad F_\infty = F(E_{p^\infty}) = \bigcup_{n \geq 1} F(E_{p^n}(\bar{F})),$$

of F obtained by adjoining the coordinates of all the p -power division points of E . The module E_{p^∞} has a natural action of the Galois group $G(\bar{F}/F)$. If E has complex multiplication defined over F , i.e. $\text{End}_F(E) \not\cong \mathbb{Z}$, then G is abelian and contains an open subgroup isomorphic to \mathbb{Z}_p^2 .

It is important to consider elliptic curves over \mathbb{Q} (or more generally over a number field) without complex multiplication. Indeed, elliptic curves with complex multiplication are rather special and those without complex multiplication are more abundant. For such

curves, the elements in the endomorphism ring correspond to multiplication by an integer n , given by the group law and hence the endomorphism ring is isomorphic to the ring of integers. It is a deep result of Serre [31] that the extension (4) is a non-commutative p -adic Lie extension. In fact, Serre also proved that the Galois group $G := G(F_\infty/F)$ for such elliptic curves is an open subgroup of $GL_2(\mathbb{Z}_p)$ and is equal to it for almost all primes p . The Iwasawa algebra $\Lambda(G)$ is thus highly non-commutative. Another natural example of a non-commutative p -adic Lie extension is given by the so-called “False Tate extension”, obtained by adjoining all p -power roots of unity and the p -power roots of an integer m which is p -power free, i.e.

$$(5) \quad F_\infty := F(\mu_{p^\infty}, m^{1/p^\infty}).$$

In this case the Galois group G is an open subgroup of the semi-direct product $\mathbb{Z}_p^\times \ltimes \mathbb{Z}_p$.

Lazard proved that for any compact p -adic Lie group G , the Iwasawa algebra is a left and right noetherian ring. Further, if G is pro- p and has no elements of order p , then $\Lambda(G)$ is a local domain, in the sense that it has no zero divisors, and the set of non-units form a (unique) two-sided maximal ideal. In particular for $G = \text{Gal}(F_\infty/F)$ with F_∞ as in (4), the Iwasawa algebra $\Lambda(G)$ is a left and right noetherian, local domain whenever $p \geq 5$. In the last decade, these algebras have been investigated more thoroughly (see [35]). The analogue in the non-commutative setting, of classical regular local rings in commutative algebra, is that of ‘Auslander-regular’ rings (see [35]) and in all the cases of non-commutative p -adic Lie extensions mentioned above, the corresponding rings are Auslander regular. More precisely, we have

Theorem 4.1. *(Venjakob)[35] Let G be a compact p -adic analytic group without p -torsion, and of dimension d when considered as an analytic manifold. Then $\Lambda(G)$ is an Auslander regular local domain of injective dimension equal to d .*

The main advantage in having this nice extra structure on $\Lambda(G)$ is that it provides a ‘dimension theory’ on the category of finitely generated modules over $\Lambda(G)$. The dimension of $\Lambda(G)$ itself is $d + 1$. This in turn, affords the definition of *pseudonull* modules. Assume that G is as in Theorem 4.1, and let M be a finitely generated module over $\Lambda(G)$. Then M is pseudonull if the dimension of M is less than or equal to $d - 1$. There is an equivalent characterisation of pseudonull modules using homological algebra (see [35]), and it coincides with the classical notion of pseudonull modules in commutative algebra. Note that in the simple case when $\Lambda(G) \simeq \mathbb{Z}_p[[T]]$, pseudonull modules are precisely the finite modules.

In the commutative case, there is also a well-known classical structure theorem for finitely generated modules over $\Lambda(G)$, due to Iwasawa and Serre (see [2], [12, Appendix]). We say that two finitely generated modules M and N over $\Lambda(G)$ are pseudoisomorphic if there is a $\Lambda(G)$ homomorphism between them whose kernel and cokernel are pseudonull.

Theorem 4.2. *Suppose G is a commutative p -adic Lie group with no elements of order p and let $\Lambda(G)$ be its Iwasawa algebra. Let M be a finitely generated torsion module over*

$\Lambda(G)$. Then there is a pseudoisomorphism

$$M \rightarrow \bigoplus_{i=1}^k \Lambda(G)/\mathfrak{p}_i^{n_i}$$

where the \mathfrak{p}_i are prime ideals of height one and n_i are positive integers.

It is well-known [2] that the prime ideals of height one in $\Lambda(G)$, for G as in the theorem above, are principal. Let I denote the ideal defined as the product $I := \prod_i \mathfrak{p}_i^{n_i}$. It is called the *characteristic ideal* of M (this is well-defined, see [2]) and denoted by char_M . A generator of the characteristic ideal is the *characteristic power series* of M and is well-defined up to a unit in the Iwasawa algebra. The characteristic power series plays a central role in the formulation of the main conjecture, and will be discussed in the next section.

In the non-commutative case, the fact that the Iwasawa algebra $\Lambda(G)$ is Auslander regular can be exploited to prove a more rudimentary structure theorem. A module over $\Lambda(G)$ will be assumed to be a left module. A finitely generated $\Lambda(G)$ -module M is said to be *torsion*, if every element of M is annihilated by a non-zero divisor of $\Lambda(G)$. A module M is said to be *reflexive* if the natural map $M \rightarrow M^{++}$ is an isomorphism; here M^+ denotes the dual module $\text{Hom}_{\Lambda(G)}(M, \Lambda(G))$.

Theorem 4.3. (*Coates-Schneider-Sujatha*)[13] *Suppose G is a compact p -adic analytic Lie group of dimension d with no element of order p . Let M be a finitely generated torsion module over $\Lambda(G)$. Then there is a homomorphism*

$$f : M \rightarrow \bigoplus_{i=1}^n \Lambda(G)/J_i$$

where the J_i are reflexive ideals and f has pseudonull kernel and cokernel.

5 Main conjectures

The aim of this section is to outline the philosophy and the formulation of the “main conjectures” in Iwasawa theory for elliptic curves. We do not even pretend to attempt a discussion of the steps involved in the formulation of these conjectures in full detail. Our goal shall be largely confined to giving the reader a flavour of what goes under the rubric of main conjectures. The basic idea is to first attach an algebraic invariant and an analytic invariant to certain canonically defined arithmetic modules over the Iwasawa algebra $\Lambda(G)$ of the Galois group G of an infinite p -adic Lie extension F_∞ . The analytic invariant has the property of interpolating special values of the complex L -function, with the interpolation formula being explicit. The main conjecture asserts the equality of these invariants. We discuss a few concrete examples below.

Iwasawa in his classic study of \mathbb{Z}_p -extensions [20] studied the growth of ideal class groups in the cyclotomic \mathbb{Z}_p -extensions, and was the first to formulate the main conjecture

for the field $\mathbb{Q}(\mu_{p^\infty})$. Here is a brief explanation of one version of his main conjecture. He related the arithmetic of the ‘‘Tate motive’’ over the extension $F_\infty = \mathbb{Q}(\mu_{p^\infty})^+$ (here $+$ denotes the maximal real subfield of $\mathbb{Q}(\mu_{p^\infty})$) to special values of the Riemann-zeta function, via the Kubota-Leopoldt p -adic zeta function. This element ζ_p is viewed as a pseudo-measure on the p -adic Lie group $G = \text{Gal}(F_\infty/\mathbb{Q})$, and also as belonging to an explicit localisation of the Iwasawa algebra $\Lambda(G)$. It has the following interpolation property, where χ is the cyclotomic character giving the action of Galois on μ_{p^∞} :-

$$\int_G \chi(g)^k d\zeta_p = (1 - p^{k-1})\zeta(1 - k)$$

for all even integers $k \geq 2$. The corresponding arithmetic module is as follows. Let X_∞ denote the maximal abelian extension of F_∞ that is unramified outside p . Then X_∞ has a natural structure of a finitely generated $\Lambda(G)$ -module and it is a deep result of Iwasawa that it is a torsion module over $\Lambda(G)$. The main conjecture asserts that the characteristic ideal of X_∞ is equal to the ideal $\zeta_p \cdot I_G$, where I_G is the augmentation ideal of $\Lambda(G)$, i.e. the kernel of the natural quotient map $\Lambda(G) \rightarrow \mathbb{Z}_p$. Iwasawa himself proved a remarkable general theorem about the arithmetic of the field F_∞ , involving a module formed out of cyclotomic units, which is closely related to X_∞ . In particular, this theorem implies his main conjecture when the class number of $\mathbb{Q}(\mu_p)^+$ is prime to p . The first unconditional proof of the main conjecture was given by Mazur-Wiles [25] and Wiles gave a second proof in [39], beautifully extending ideas of Ribet. A simpler proof using Iwasawa’s original approach, along with work of Thaine, Kolyvagin and Rubin on Euler systems [34], [23], [28], is given in [12].

To formulate these main conjectures for elliptic curves, one studies the arithmetic of E over infinite p -adic Lie extensions of a number field F . The p -adic L -functions then seem to mysteriously arise from some natural G -modules describing the arithmetic of E over these p -adic Lie extensions. We shall sketch the formulation of the main conjecture in the important case of elliptic curves with complex multiplication, which was first considered by Coates-Wiles. Of course, the general case of elliptic curves without complex multiplication lies much deeper and is more technical. Let E/\mathbb{Q} be an elliptic curve with complex multiplication by the ring of integers \mathcal{O}_K of an imaginary quadratic field K of class number one. Suppose p is a prime such that p splits as $p = \mathfrak{p}\mathfrak{p}^*$ in \mathcal{O}_K , and assume that E has good ordinary reduction at \mathfrak{p} and \mathfrak{p}^* . By the classical theory of complex multiplication due to Deuring and Weil, it is well-known that the complex L -function $L(E/\mathbb{Q}, s)$ is the Hecke L -function $L(\psi_E, s)$ where ψ_E is a certain Grössencharacter (see [32]).

The p -adic Lie extension that we consider is the extension

$$(6) \quad F_\infty = \bigcup_{n \geq 1} K(E_{\mathfrak{p}}^n)$$

obtained by adjoining all the \mathfrak{p} -division points of the elliptic curve to K . The Galois group of F_∞ over K is isomorphic to \mathbb{Z}_p^\times and we denote by K_∞ the unique \mathbb{Z}_p -extension contained in F_∞ . Let $\Gamma = \text{Gal}(K_\infty/K)$, then the Iwasawa algebra $\Lambda(\Gamma)$ is isomorphic

to $\mathbb{Z}_p[[T]]$ (see §4). The p -adic L -function is then an element $H_{\mathfrak{p}}(T)$ in $\mathcal{I}[[T]]$, where \mathcal{I} denotes the ring of integers in the completion of the maximal unramified extension of \mathbb{Q}_p . It interpolates the values of the complex L -function in that we have

$$\Omega_{\mathfrak{p}}^{-n} H_{\mathfrak{p}}((1+p)^n - 1) = \Omega_{\infty}^{-n} (n-1)! L(\bar{\psi}_E^n, n) \left(1 - \frac{\psi_E^n(\mathfrak{p})}{N\mathfrak{p}} \right),$$

for appropriate complex and p -adic periods Ω_{∞} and $\Omega_{\mathfrak{p}}$ respectively, of the elliptic curve (see [7] for a detailed exposition).

Classical descent theory [32] already points to the arithmetic module that one should consider. This is the *Selmer group* which we define below. Let \mathcal{M} be any Galois extension of a number field F . For each non-archimedean place w of \mathcal{M} , let \mathcal{M}_w be the union of the completions at u of all finite extensions of F contained in \mathcal{M} . The p^{∞} -Selmer group of E over \mathcal{M} is defined by

$$(7) \quad \text{Sel}_p(E/\mathcal{M}) = \text{Ker} \left(H^1(\text{Gal}(\bar{\mathcal{M}}/\mathcal{M}), E_{p^{\infty}}) \rightarrow \prod_w H^1(\text{Gal}(\bar{\mathcal{M}}_w/\mathcal{M}_w), E(\bar{\mathcal{M}}_w)) \right),$$

where w runs over all non-archimedean places of \mathcal{M} , and the map is given by natural restriction. The Galois group of \mathcal{M} over F operates on $\text{Sel}_p(E/\mathcal{M})$ and we have an exact sequence

$$(8) \quad 0 \rightarrow E(\mathcal{M}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \rightarrow \text{Sel}_p(E/\mathcal{M}) \rightarrow \text{III}(E/\mathcal{M})(p) \rightarrow 0.$$

Here $\text{III}(E/\mathcal{M})$ denotes the Tate-Shafarevich group of E over \mathcal{M} , which is the inductive limit of $\text{III}(E/L)$ as L varies over all finite extensions of F in \mathcal{M} , and for any abelian group A , $A(p)$ is the submodule consisting of all elements annihilated by a power of p . We shall consider the Pontryagin dual

$$(9) \quad X_p(E/\mathcal{M}) = \text{Hom}(\text{Sel}_p(E/\mathcal{M}), \mathbb{Q}_p/\mathbb{Z}_p).$$

which is a compact module over the Galois group $\text{Gal}(\mathcal{M}/K)$. The dual Selmer group considered as a module over the Iwasawa algebra, simultaneously reflects both the arithmetic of the elliptic curve and the special values of the complex L -function. Further, by virtue of the additional Galois module structure, it encodes information about $E(L)$ and $\text{III}(E/L)$ for all finite extensions L of F in \mathcal{M} .

Suppose now that E/\mathbb{Q} is an elliptic curve with complex multiplication such that $\text{End}_K(E) \simeq \mathcal{O}_K$, and let K_{∞} be the \mathbb{Z}_p -extension of K contained in F_{∞} (cf. (6)). The Selmer group $\text{Sel}_p(E/K_{\infty})$ is similarly defined as the kernel of the restriction map

$$\text{Ker} \left(H^1(\text{Gal}(\bar{\mathbb{Q}}/K_{\infty}), E_{p^{\infty}}) \rightarrow \prod_w H^1(\text{Gal}(\bar{K}_{\infty,w}/K_{\infty,w}), E(\bar{K}_{\infty,w})) \right)$$

where w runs over all the non-archimedean places of K_{∞} . Clearly the Galois group of K_{∞} over K operates on $\text{Sel}_p(E/K_{\infty})$ and we have an exact sequence

$$0 \rightarrow E(K_{\infty}) \otimes_{\mathcal{O}_K} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \rightarrow \text{Sel}_p(E/K_{\infty}) \rightarrow \text{III}(E/K_{\infty})(\mathfrak{p}) \rightarrow 0.$$

Here $\text{III}(E/K_\infty)$ denotes the Tate-Shafarevich group of E over K_∞ and for any \mathcal{O}_K -module A , $A(\mathfrak{p})$ denotes the submodule consisting of elements annihilated by some power of a generator of \mathfrak{p} . As before (cf. (9)), we consider the compact dual, which we denote by $X_{\mathfrak{p}}(E/K_\infty)$. This is a finitely generated module over $\Lambda(\Gamma)$, which is torsion, thanks to a result of Coates-Wiles [14]. By the structure theorem described in §4, we can define the characteristic power series of the dual Selmer group, which we denote by $B_{\mathfrak{p}}(T) \in \mathbb{Z}_p[[T]]$. The one variable main conjecture, proved by Rubin [29], is the following deep result:-

Theorem 5.1. *(One variable main conjecture)[29] We have*

$$H_{\mathfrak{p}}((1+p)(1+T)-1)\mathcal{I}[[T]] = B_{\mathfrak{p}}(T)\mathcal{I}[[T]].$$

Let E/\mathbb{Q} be an elliptic curve without complex multiplication, and let p be a prime of good ordinary reduction. In this case, the formulation of the main conjecture over the cyclotomic \mathbb{Z}_p -extension can be found in [18]. For the algebraic invariant, a deep result of Kato [22] proves that the dual Selmer group is a finitely generated torsion module over the corresponding Iwasawa algebra, and hence the characteristic ideal can be defined as before. Moreover, Kato proves that the p -adic L -function is divisible by this characteristic ideal. Completing the proof of the main conjecture is however considerably harder, and to date, a full proof has not been published, (Skinner and Urban have announced results in this direction).

For nonabelian p -adic Lie extensions as in the division field extension (4) or the false Tate extension (5), even the precise formulation of the main conjecture is far from obvious. Let G be the corresponding Galois group and $\Lambda(G)$ the associated Iwasawa algebra. Though the dual Selmer group is known to be finitely generated as a (left) module over the corresponding Iwasawa algebra $\Lambda(G)$, and is even conjectured to be torsion (in fact, there is even a stronger conjecture, see [9]), there is no well-defined analogue of the characteristic ideal. A main conjecture in this set-up is formulated in [9], and the principal novelty in these non-commutative examples is the use of algebraic K -theory [1]. The algebraic and analytic invariants are elements of the group $K_1(R)$, where R is an explicit localisation of the Iwasawa algebra $\Lambda(G)$. The existence of a canonical Ore set in $\Lambda(G)$ makes this explicit localisation possible. Furthermore, this formulation can be intrinsically linked to Iwasawa theory of the elliptic curve over the cyclotomic extension, which is a quotient of F_∞ in the examples considered above. For a commutative ring R , $K_1(R)$ may be identified with the units in R and therefore, the occurrence of K_1 in the non-commutative set-up may be viewed as a natural extension of the commutative context. The main conjecture then predicts the equality of the analytic and algebraic invariants, as elements in the K -group. We do not go into any further details but state that the non-commutative phenomenon is vastly different in one other aspect. Namely, it has infinite families of self-dual Artin representations of G (these are representations that factor through a finite quotient of G) and thus gives rise to twists of complex L -functions. The interpolation property of the p -adic L -function then has to take into account these twisted L -values, in the formulation of the main conjecture. This in turn leads to interesting connections

with root numbers, which we shall touch upon in the next section. When E has supersingular reduction at p [32], we still have no idea how to formulate a non-commutative main conjecture.

6 Applications and examples

In this final section, we mention a few theorems that are proved using Iwasawa theory. We remark that even though the main conjecture has only been established in a few cases, it provides great insights into the Birch and Swinnerton-Dyer conjecture. Kakde [K] has recently proven the existence of the p -adic L -function and made important progress towards the main conjecture in the non-commutative case for the Tate motive over p -adic Lie extensions of totally real number fields. Another interesting phenomenon is the connection between root numbers and non-commutative Iwasawa theory which is studied in [8]. In particular, these results give information on the growth of the Mordell-Weil ranks along finite layers of the false Tate extension and the division field extension. We first recall the definition of the root number.

Let E/\mathbb{Q} be an elliptic curve. The modified L -function denoted $\Lambda(E, s)$, s a complex variable, is defined by

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

By the modularity result of Wiles *et al.*, this function is entire and satisfies the functional equation

$$\Lambda(E, s) = \omega_E N_E^{1-s}\Lambda(E, 2-s),$$

where $\omega_E = \pm 1$ is the *root number* and N_E is the conductor of E [32]. We have

$$(10) \quad \omega_E = (-1)^{r_{E/\mathbb{Q}}}$$

where $r_{E/\mathbb{Q}}$ is the analytic rank of E . Root numbers can also be defined over finite extensions of \mathbb{Q} . The study of root numbers by Rohrlich [27] along the cyclotomic extension, combined with the deep result of Kato that the dual Selmer group of E is torsion over the Iwasawa algebra [22] yields the following result:-

Theorem 6.1. (*Kato, Rohrlich*) *For every prime p , $E(\mathbb{Q}(\mu_{p^\infty}))$ is a finitely generated abelian group.*

We next consider a false Tate extension tower. Fix an integer $m > 1$, which is assumed to be p -power free. Define

$$L_n = \mathbb{Q}(m^{1/p^n}), \quad K_n = \mathbb{Q}(\mu_{p^n}), \quad F_n = \mathbb{Q}(\mu_{p^n}, m^{1/p^n}),$$

and consider the false Tate extension

$$F_\infty = \bigcup_{n \geq 0} F_n$$

with Galois group G . Let H be the normal subgroup

$$H := \text{Gal}(F_\infty/\mathbb{Q}(\mu_{p^\infty})) \simeq \mathbb{Z}_p.$$

Then G is isomorphic to the semi-direct product of \mathbb{Z}_p^\times and \mathbb{Z}_p . The extensions L_n are not Galois, while F_n are nonabelian Galois extensions, and the Artin representations of G can be fully described. Put

$$Y(E/F_\infty) = X_p(E/F_\infty)/X_p(E/F_\infty)(p),$$

where $X_p(E/F_\infty)(p)$ is the p -primary submodule of the dual Selmer group (9). For any finite extension M of \mathbb{Q} , we define

$$(11) \quad s_{E/M,p} = \mathbb{Z}_p - \text{corank of the Selmer group of } E \text{ over } M.$$

The study of root numbers, combined with results from Iwasawa theory, yields the following theorem:-

Theorem 6.2. [8, Theorem 4.8] *Assume that E has good ordinary reduction at p and that $Y(E/F_\infty)$ is finitely generated as a $\Lambda(H)$ -module, with $\Lambda(H)$ -rank 1. Then for all $n \geq 1$, we have*

$$s_{E/L_n,p} = n + s_{E/\mathbb{Q},p}, \quad s_{E/F_n,p} = p^n - 1 + s_{E/K_1,p}.$$

As a specific numerical example where the above theory can be applied, we consider the elliptic curve E/\mathbb{Q} of conductor 11 defined by

$$(12) \quad E : y^2 + y = x^3 - x^2,$$

and the prime $p = 7$.

Theorem 6.3. *Let F_∞ be a false Tate extension. For the elliptic curve E as in (12), and $p = 7$, we have the algebraic rank*

$$g_{E/L_n} \geq n, \quad (n = 1, 2, 3, \dots)$$

provided $\text{III}(E/L_n)(7)$ is finite,

We remark that even for $n = 1$, it is numerically very difficult to find points of infinite order in $E(L_1)$. Surprisingly, Iwasawa theory also provides lower bounds in some cases.

Theorem 6.4. *Assume that m is any 7-power free integer with prime factors in the set $\{2, 3, 7\}$. Then for E as in (12), and all integers $n = 2, 3, \dots$, we have*

$$g_{E/L_n} \leq n$$

with equality if and only if $\text{III}(E/L_n)(7)$ is finite.

A natural question that arises in light of (10) and the Birch and Swinnerton-Dyer conjecture is whether the root number and the algebraic rank have the same parity. Assuming that the Tate-Shafarevich group is finite, this is equivalent to the question whether $s_{E/\mathbb{Q},p}$ (cf. (8), (11)) and the root number have the same parity. An important general result in this direction has been proved by T. Dokchitser and V. Dokchitser [16]:-

Theorem 6.5. *(T. Dokchitser and V. Dokchitser) Let E/\mathbb{Q} be an elliptic curve. Then for any prime p , the root number ω_E and $s_{E/\mathbb{Q},p}$ have the same parity.*

We end this article by showing how these results enable us to go considerably closer to proving the folklore conjecture (2) on congruent numbers.

Theorem 6.6. *Assume $N \equiv 5, 6, 7 \pmod{8}$, and let E_N be the elliptic curve defined by (3). If the p -primary torsion part $\text{III}(E_N/\mathbb{Q})(p)$ is finite for some prime p , then N is congruent.*

Proof. As remarked earlier, it is known from the theory of L -functions that $L(E_N, s)$ vanishes to odd order at $s = 1$ for N as in the theorem. By the parity theorem 6.5, we therefore see that $s_{E_N/\mathbb{Q},p}$ is odd for all primes p . Suppose there exists a prime p such that $\text{III}(E_N/\mathbb{Q})(p)$ is finite. Then by the exact sequence (8), we have $g_{E_N/\mathbb{Q}} \geq 1$ and hence E_N has a point of infinite order. By our remarks at the end of §2, this implies that N is a congruent number. \square

References

- [1] H. BASS, Algebraic K-theory, W. A. Benjamin, Inc., New York-Amsterdam (1968).
- [2] N. BOURBAKI, Elements of Mathematics, Commutative Algebra, Chapters 1-7, Springer (1989).
- [3] B. BIRCH, G. STEVENS, *The parity of the rank of the Mordell-Weil group*, *Topology* **5** (1966), 295–299.
- [4] 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.
- [5] J. COATES, *Congruent number problem*, *Q. J. Pure Appl. Math.* **1** (2005), 14–27.
- [6] J. COATES, *p -adic L -functions and Iwasawa’s theory*, in *Algebraic Number fields (Durham Symposium)*; ed. A. Frohlich, Academic Press (1977), 269–353.
- [7] J. COATES, *Elliptic curves with complex multiplication and Iwasawa theory*, *Bull. LMS.* **23** (1991), 321–350.
- [8] J. COATES, T. FUKAYA, K. KATO, R. SUJATHA, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, *Jour. Alg. Geom.* (To appear).

- [9] J. COATES, T. FUKAYA, K. KATO, R. SUJATHA, O. VENJAKOB, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163–208.
- [10] J. COATES, Z. LIANG, R. SUJATHA, Tate Shafarevich groups of elliptic curves with complex multiplication, arXiv:0901.3832v1 [math.NT], To appear in Journal of Algebra.
- [11] J. COATES, R. SUJATHA, Galois cohomology of elliptic curves, Tata Institute of Fundamental Research Lectures on Mathematics **88**, Narosa Publishing House, New Delhi, (2000).
- [12] J. COATES, R. SUJATHA, Cyclotomic fields and zeta values, Springer Monographs in Mathematics, Springer (2006).
- [13] J. COATES, P. SCHNEIDER, R. SUJATHA, *Modules over Iwasawa algebras*, J. Inst. Math. Jussieu **2** (2003), 73–108.
- [14] J. COATES, A. WILES, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.
- [15] J. CREMONA, Algorithms for modular elliptic curves, Second edition, Cambridge University Press, Cambridge, (1997).
- [16] T. DOKCHITSER, V. DOKCHITSER, *On the Birch-Swinnerton Dyer quotients modulo squares*, Ann. of Math. (To appear).
- [17] W. FULTON, Algebraic curves. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original, Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.
- [18] R. GREENBERG, *Iwasawa theory for elliptic curves*, in Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., 1716, Springer, Berlin, (1999), 51–144.
- [19] J. HOYRUP, *The Babylonian Cellar Text BM85200 + VAT 6599 Retranslation and Analysis*, in Amphora Festschrift for Hans Wussing on the occasion of his 65th birthday, ed. Hans Wussing, Sergei Sergeewich Demidov, Birkhäuser, 315–338.
- [20] K. IWASAWA, *On Z_l -extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.
- [21] M. KAKDE, *The Main Conjecture of non-commutative Iwasawa theory for totally real fields*, Jour. Alg. Geom. (To appear).

- [22] K. KATO, *p-adic Hodge theory and values of zeta functions of modular forms*, in Cohomologies p -adiques et applications arithmétiques. III. Astérisque **295** (2004), ix, 117–290.
- [23] V. KOLYVAGIN, *Euler systems*, in The Grothendieck Festschrift, Vol. II, Progr. Math. **87**, Birkhäuser Boston, Boston, MA (1990), 435–483.
- [24] M. LAZARD, *Groupes analytiques p -adiques*, Publ. Math. IHES **26** (1965) 389–603.
- [25] B. MAZUR, A. WILES, *Class fields of abelian extensions of \mathbb{Q}* , Invent. Math. **76** (1984), 179–330.
- [26] J. NEUKIRCH, Algebraic number theory, Grundlehren der Mathematischen Wissenschaften **322** Springer-Verlag, Berlin (1999).
- [27] D. ROHRLICH, *On L -functions of elliptic curves and cyclotomic towers*, Invent. Math. **18** (1972), 183–266.
- [28] K. RUBIN, *The “main conjectures” of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25–68.
- [29] K. RUBIN, *The one-variable main conjecture for elliptic curves with complex multiplication*, in L -functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., **153**, Cambridge Univ. Press, Cambridge, 1991, 353–371.
- [30] J.-P. SERRE, J. TATE, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.
- [31] J.-P. SERRE, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
- [32] J. SILVERMAN, The arithmetic of elliptic curves, Corrected reprint of the 1986 original. Graduate Texts in Mathematics **106** Springer-Verlag, New York, (1992).
- [33] J. SILVERMAN, J. TATE, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, (1992).
- [34] F. THAINE, *On the ideal class groups of real abelian number fields*, Ann. of Math. **128**, (1988), 1–18.
- [35] O. VENJAKOB, *On the structure theory of Iwasawa algebra of a p -adic Lie group*, J. Eur. Math. Soc. **4** (2002), 271–311.
- [36] L. WASHINGTON, Introduction to Cyclotomic fields, Graduate Texts in Mathematics **83**, Springer (1982).
- [37] A. WEIL, Number theory. An approach through history. From Hammurapi to Legendre, Birkhuser Boston, Inc., Boston, MA, (1984).

- [38] A. WILES, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443–551.
- [39] A. WILES, *The Iwasawa conjecture for totally real fields*, Ann. of Math. **131** (1990), 493–540.

R. Sujatha
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road, Colaba
Mumbai, INDIA 400005
email: sujatha@math.tifr.res.in