Lectures on the Birch-Swinnerton-Dyer Conjecture

by John Coates

Emmanuel College, University of Cambridge, and POSTECH

Introduction

In 1839, Dirichlet gave his remarkable proof that there are infinitely many primes of the form $an+b$ $(n=1,2,\ldots)$, where a,b are any pair of positive integers with $(a,b)=1$. His proof used L-functions in a fundamental way for the first time in number theory, as well as proving the above result on primes in arithmetic progressions. In particular, his work established the first exact formula in number theory for the class number of an imaginary quadratic field. Let p be a prime >3 with $p\equiv 3 \bmod 4$ and let $h(\mathbb{Q}(\sqrt{-p}))$ be the class number of $\mathbb{Q}(\sqrt{-p})$.

Theorem 1 (Dirichlet). *If $p\equiv 3 \bmod 4$ and $p>3$, then*

$$h(\mathbb{Q}(\sqrt{-p})) = -\frac{1}{p}\sum_{a=1}^{p-1} a\left(\frac{a}{p}\right).$$

No proof of this formula, or even that the right hand side is an integer >0, which does not involve L-functions, has ever been found.

About 120 years after Dirichlet, Birch and Swinnerton-Dyer [1] discovered by numerical calculations that there seems to be a similar deep connection between the arithmetic of elliptic curves defined over $\mathbb{Q}$ and their associated complex L-functions. This is the so-called "Conjecture of Birch and Swinnerton-Dyer", and is the topic of this short and informal course of lectures, given at Tsinghua University and the Chinese Academy of Sciences in Beijing, China, and Tsinghua University in Hsinchu, Taiwan in the summer of 2013. This conjecture is still largely unproven. We will begin by briefly explaining what was known about it until recently. By beautifully generalizing some old work of Heegner [8], Ye Tian [12, 13] has very recently made important progress on this conjecture for one family of elliptic curves (the quadratic twists of the elliptic curve $y^2=x^3-x$), and it is now an important question to generalize his method to the quadratic twists of all elliptic curves defined over $\mathbb{Q}$. In the latter part of the lectures, I will discuss joint ongoing work (see [2]) with Yongxiong Li, Ye Tian and Shuai Zhai, which makes a first step in this direction by establishing analogous results for the elliptic curve $E=X_0(49)$ with equation $y^2+xy=x^3-x^2-2x-1$.

For a beautiful and elegant summary of the background on the arithmetic of elliptic curves which we will need, Tate's old article [11] is still the best introduction to the subject.

I am extremely grateful to Baoshan Wang for his invaluable help in preparing the tex file of these lecture notes, and to Ming-Lun Hsieh and Ye Tian for their very careful proof reading of the final manuscript. I also want to warmly thank Professor Ming-chang Kang, without whose kind assistance, and infinite patience with my corrections, these lecture notes would never have been published.

Finally, we give below a list of some of the basic notation, which will be used later in the lectures, without comment.

- A – an abelian group.
- $n>1$, $A[n]=\mathrm{Ker}(\ A \xrightarrow{\ n\ } A\ )$.
- p – prime, $A(p)=\bigcup_{m\geq 1} A[p^m]$.
- F – a field, F_s – its separable closure; if A is a $\mathrm{Gal}(F_s/F)$-module, we write $H^i(F,A)$ for $H^i(\mathrm{Gal}(F_s/F),A)$.
- E – an elliptic curve, which will nearly always be assumed to be defined over $\mathbb{Q}$.
- $E(F)$ – group of F-rational points for any extension $F/\mathbb{Q}$

Classical Descent Theory

We briefly recall the main facts without proofs. Let E be any elliptic curve over $\mathbb{Q}$. By beautifully generalizing Fermat's proof that 1 is not a congruent number, Mordell proved:

Theorem 2 (Mordell). *$E(\mathbb{Q})$ is a finitely generated abelian group.*

In practice, we can virtually always determine $E(\mathbb{Q})$ for a given numerical example, but theoretically no algorithm for calculating $E(\mathbb{Q})$ in a finite number of steps has ever been proven.

Definition 3. Define $g_E=\dim_{\mathbb{Q}}(E(\mathbb{Q})\otimes_{\mathbb{Z}}\mathbb{Q})$, the rank of $E(\mathbb{Q})$.

Example 4. Let $E: y^2=x^3-82x$. Then $g_E=3$, and generators modulo torsion are given by $(-9,3)$, $(-8,12)$, and $(-1,9)$.

In classical descent theory, we take an integer $m>1$, and take $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-cohomology of the exact sequence

$$0\longrightarrow E[m]\longrightarrow E(\overline{\mathbb{Q}})\xrightarrow{m} E(\overline{\mathbb{Q}})\longrightarrow 0$$

obtaining the exact sequence

$$0\longrightarrow E(\mathbb{Q})/mE(\mathbb{Q})\longrightarrow H^1(\mathbb{Q},E[m])\xrightarrow{j_m} H^1(\mathbb{Q},E)[m]\longrightarrow 0.$$

Definition 5. Define $Ш(E)=\mathrm{Ker}(H^1(\mathbb{Q},E)\to\bigoplus_v H^1(\mathbb{Q}_v, E))$, called the Shafarevich-Tate group of E, where v runs

over all places of $\mathbb{Q}$, and $\mathbb{Q}_v$ denotes the completion of $\mathbb{Q}$ at v.

Definition 6. Define $\mathcal{S}el_m(E) = j_m^{-1}(Ш(E)[m])$, the m-Selmer group of E.

Hence we have the basic exact sequence

$$0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \longrightarrow \mathcal{S}el_m(E) \longrightarrow Ш(E)[m] \longrightarrow 0.$$

Theorem 7. *The group $\mathcal{S}el_m(E)$ is finite for all $m > 1$.*

There are many ingenious classical techniques for calculating $\mathcal{S}el_m(E)$ for small m. But, as we shall see later, it is a subtle question even to calculate $\mathcal{S}el_2(E)$ in many cases. Only one deep theoretical result is known about $Ш(E)$. Let $Ш(E)_{div}$ be the maximal divisible subgroup of $Ш(E)$.

Theorem 8 (Cassels-Tate)**.** *There is a canonical non-degenerate alternating bilinear form on $Ш(E)/Ш(E)_{div}$.*

Corollary 9. *The vector space $(Ш(E)/Ш(E)_{div})[p]$ has even $\mathbb{F}_p$-dimension.*

Corollary 10. *If $Ш(E)_{div}(p) = 0$, then $\sharp(Ш(E)(p))$ is a square.*

Classical Galois cohomology shows that, for some integer $t_{E,p} \geq 0$, we have

$$Ш(E)(p) = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E,p}} \bigoplus \text{(a finite group)},$$

so that $Ш(E)(p)_{div} = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E,p}}$.

Conjecture. *The group $Ш(E)$* is finite.

To settle this conjecture is unquestionably one of the major problems of number theory. However, it has never been proven so far for a single elliptic curve with $g_E \geq 2$. It would of course imply that $t_{E,p} = 0$ for every p. To date, only one deep fact is known about the $t_{E,p}$ as p varies over all primes.

Theorem 11 (T. & V. Dokchitser)**.** *The parity of $t_{E,p}$, i.e. $t_{E,p}$* mod 2*, does not depend on p.*

If we combine this result with the second corollary above of the Cassels-Tate theorem, we obtain the following lemma.

Lemma 12. *Assume that $\mathcal{S}el_2(E)/\mathrm{Im}(E(\mathbb{Q})_{tors})$ has order* 2*. Then either (i) $g_E = 1$ and $Ш(E)(2) = 0$, or (ii) $g_E = 0$, $Ш(E)(2) = \mathbb{Q}_2/\mathbb{Z}_2$, and $Ш(E)(p) \supset \mathbb{Q}_p/\mathbb{Z}_p$ for every odd prime p.*

Of course, we want to prove that the second possibility can never occur. Until recently, this problem seemed largely inaccessible. But Tian [12, 13] has introduced a beautiful new idea which should enable us to eventually prove this for many elliptic curves.

We end this section by recalling another open problem about the Tate-Shafarevich groups of elliptic curves defined over $\mathbb{Q}$. Presumably, there do exist arbitrarily large primes p such that there exists some elliptic curve $E/\mathbb{Q}$ with $Ш(E)(p) \neq 0$, but this has never been proven. At present, the largest prime p for which this is known to occur is $p = 1627$. Indeed, calculations of Z. Liang and D. Wei show that $Ш(E)(1627)$ is finite of order 1627^2 for the elliptic curve

$$E : y^2 = x^3 - (7173305747)^2 x.$$

L-Functions

Although the above questions only involve purely arithmetic phenomena, it seems that there is no way to attack them without the use of L-functions. We briefly recall the definitions and key facts about these, without any proofs. Let E be an elliptic curve over $\mathbb{Q}$, and take any global minimal Weierstrass equation for E:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let Δ be the discriminant of this equation. We recall that the conductor $C(E)$ of E is defined by

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

where $f_p = 1$ if E has multiplicative reduction at p (i.e. the reduction $\widetilde{E}$ at p has a node), and $f_p = 2 + \delta_p$ if E has additive reduction at p (i.e. $\widetilde{E}$ has a cusp). Moreover, $\delta_p = 0$ when $p \geq 5$.

Example 13. Let $E : y^2 + xy = x^3 - x^2 - 2x - 1$, then $\Delta = -7^3$, $j = -3^3 \cdot 5^3$ and $C(E) = 49$. In fact, E has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-7})$.

For each prime p, define A_p by letting $A_p - 1$ denote the number of solutions of the congruence

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

and then define

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

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 has additive reduction at p. The complex L-series of E is then defined by the Euler product

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

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 $\mathrm{Re}(s) > \frac{3}{2}$. To prove the analytic continuation and functional equation for $L(E,s)$, we need the following

deep theorem. Let $\Gamma_0(C(E))$ be the subgroup of $SL_2(\mathbb{Z})$ consisting of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0 \mod C(E)$. Let $\mathscr{H}$ be the upper half complex plane, and put $q = e^{2\pi i\tau}$ with $\tau \in \mathscr{H}$. Define

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

Theorem 14 (Wiles [14] et al)**.** *The holomorphic function $f_E(\tau)$ is a primitive cusp form of weight 2 for $\Gamma_0(C(E))$.*

The key corollary of this theorem for us is the following. Define

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

Corollary 15. *The function $\Lambda(E,s)$ can be analytically continued to an entire function of s, and satisfies the functional equation*

$$\Lambda(E,s) = w_E\Lambda(E,2-s),$$

where $w_E = \pm 1$.

The root number $w_E = \pm 1$, which can be computed as a product of purely local factors, is important for us because we see immediately from the above functional equation that $L(E,s)$ has a zero at $s=1$ of even or odd multiplicity, according as $w_E = +1$ or -1.

A second corollary of the above theorem is of great importance. Define the modular curve $X_0(C(E))$ by

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

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 projective curve defined over $\mathbb{Q}$, which we also denote by $X_0(C(E))$. Let $[\infty]$ be the cusp at ∞ (i.e. corresponding to $\infty \in \mathbb{P}^1(\mathbb{Q})$).

Corollary 16. *There is a non-constant rational map defined over $\mathbb{Q}$*

$$\varphi : X_0(C(E)) \to E$$

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

Example 17. Take $E : y^2 = x^3 - x$, $C(E) = 32$. One can show that there exists

$$\varphi : X_0(32) \longrightarrow E$$

with $\varphi([\infty]) = \mathcal{O}$ and φ of degree 2.

Example 18. Take $E : y^2 + xy = x^3 - x^2 - 2x - 1$, $C(E) = 49$. One can show in this case that we have an isomorphism

$$\varphi : X_0(49) \longrightarrow E$$

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

Finally, we remark that, in the special case when E admits complex multiplication, there is a totally different method for proving the analytic continuation and functional equation for $L(E,s)$, which goes back to Eisenstein and Kronecker in the 19th century (and which probably motivated the later work of Hecke). We will discuss this in detail later, when we come to apply it. Indeed, it turns out to be very useful in studying certain aspects of the conjecture of Birch and Swinnerton-Dyer. There seems to be no analogue of this method for elliptic curves without complex multiplication.

The Conjecture of Birch and Swinnerton-Dyer

The conjecture asserts that there is a remarkably close link between the arithmetic of E (i.e. the groups $E(\mathbb{Q})$ and $Ш(E)$), and the behaviour of $L(E,s)$ at $s=1$, including a beautiful exact formula. All aspects of the conjecture have been tested numerically more extensively than any other conjecture in the history of mathematics, and have always confirmed every aspect of the conjecture. But, as we shall see, our knowledge as far as proofs of theoretical results is much more limited.

Definition 19. $r_E = \operatorname{ord}_{s=1} L(E,s)$.

We recall that $g_E = \operatorname{rank}$ of $E(\mathbb{Q})$.

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

$$r_E = g_E.$$

Before discussing what is known about this statement, let us discuss its parity implications. Indeed this weak Birch-Swinnerton-Dyer Conjecture would immediately imply the

Strong Parity Conjecture. *For all elliptic curves $E/\mathbb{Q}$, we have*

$$r_E \equiv g_E \mod 2.$$

Recall that the parity of r_E is determined by the functional equation

$$\Lambda(E,s) = w_E\Lambda(E,2-s)$$

which gives immediately that $w_E = (-1)^{r_E}$. Thus we see that the strong parity conjecture would imply, in particular, that we must have $E(\mathbb{Q})$ infinite when $w_E = -1$. Very little in general is still known about this assertion, although Ye Tian's method, which we will discuss later, should eventually enable us to prove it in many more cases than before.

Example 20. Let N be a square free positive integer, and let $E^{(N)} : y^2 = x^3 - N^2x$. Then a classical computation shows that $w_{E^{(N)}} = +1$ if $N \equiv 1,2,3 \mod 8$, and $w_{E^{(N)}} = -1$ if $N \equiv 5,6,7 \mod 8$.

We recall that an integer $N \geq 1$ is said to be *congruent* if it is the area of a right-angled triangle all of whose sides have rational length. It is easy to see that $g_{E^{(N)}} > 0$ if and only if N is congruent. The smallest three congruent numbers are $N = 5,6,7$. In fact, we see that the strong parity conjecture implies:

Conjecture. *Every positive integer $N \equiv 5,6,7 \mod 8$ is a congruent number.*

The only general result known about the strong parity conjecture is the following. Recall that the integer $t_{E,p} \geq 0$ is defined by

$$Ш(E)(p)_{div} = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E,p}}.$$

Weak Parity Theorem (T. Dokchitser & V. Dokchitser [5]). *For all elliptic curves $E/\mathbb{Q}$, and all primes p, we have*

$$r_E \equiv t_{E,p} + g_E \mod 2.$$

Corollary 21. *The parity of $t_{E,p}$ is independent of p.*

For any prime number p, define

$$\mathfrak{S}_p(E) = \mathcal{S}el_p(E)/\operatorname{Im}(E(\mathbb{Q})_{tors}).$$

Corollary 22. *Let p be any prime number. Then the $\mathbb{F}_p$-dimension of $\mathfrak{S}_p(E)$ is even if and only if the root number w_E of E is equal to $+1$.*

Proof. Let $A(p) = Ш(E)(p)/Ш(E)(p)_{div}$. Then, writing s_p for the $\mathbb{F}_p$-dimension of $\mathfrak{S}_p(E)$, we see immediately that

$$s_p = g_E + t_{E,p} + m_p,$$

where m_p denotes the $\mathbb{F}_p$-dimension of the kernel of multiplication by p on $A(p)$. But, as mentioned earlier, the Cassels-Tate pairing shows that m_p is necessarily even, and so the assertion follows immediately from the Dokchitser brothers' theorem. □

Corollary 23. *If $w_E = -1$ and $g_E = 0$, then necessarily $t_{E,p} \geq 1$ for all primes p.*

Of course, we believe that one can never have $t_{E,p} \geq 1$ for even one prime p, and it remains one of the major challenges of number theory to prove it.

The best result to date in the direction of the weak Birch-Swinnerton-Dyer Conjecture is the following deep theorem:

Theorem 24 (Kolyvagin [9], Gross-Zagier [7])**.** *Assume $r_E \leq 1$. Then $r_E = g_E$ and $Ш(E)$ is finite.*

However, while it is usually easy to decide in numerical examples whether or not $r_E \leq 1$, very little is still known about establishing this assertion theoretically for large families of elliptic curves.

The Exact Birch-Swinnerton-Dyer Formula

The full Birch-Swinnerton-Dyer Conjecture is the weak Birch-Swinnerton-Dyer Conjecture that $r_E = g_E$, together with an exact arithmetic formula for the constant $\mathscr{L}_E$ such that

$$L(E,s) = \mathscr{L}_E(s-1)^{r_E} + \text{higher order terms}.$$

The formula for $\mathscr{L}_E$ involves the following arithmetic invariants. Firstly, there is a regulator term coming from the Neron-Tate height. If $\alpha = \frac{m}{n}$, with m and n relatively prime integers, is any rational number, we define its height to be $h(\alpha) = \log(\max(|m|,|n|))$. Then Néron and Tate proved that there is a unique real-valued function $\widehat{h}$ on $E(\mathbb{Q})$ such that, for all P in $E(\mathbb{Q})$, we have (i) $\widehat{h}(2P) = 4\widehat{h}(P)$, and (ii) the difference $\widehat{h}(P) - h(x(P))$ (for any fixed generalized Weierstrass equation for E) is bounded. We then define the bilinear form

Definition 25. $\langle P, Q\rangle = \frac{1}{2}\left(\widehat{h}(P \oplus Q) - \widehat{h}(P) - \widehat{h}(Q)\right)$.

This bilinear form can be shown to be positive definite on $E(\mathbb{Q}) \otimes \mathbb{R}$. Thus, if $P_1, \ldots, P_{g_E}$ are any basis of $E(\mathbb{Q})$ mod torsion, we can define

Definition 26. $R_\infty(E) = \det\langle P_i, P_j\rangle$.

By positive definiteness, $R_\infty(E) \neq 0$. The next, and somewhat unexpected, ingredient in the formula for $\mathscr{L}_E$ are the so called Tamagawa factors $c_v(E)$ for $v = \infty$, and finite primes v dividing $C(E)$. We again suppose that we have fixed a minimal generalized Weierstrass equation for E, and we write Ω_E for the least positive real period of the Néron differential on E, which is given by

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{d\wp(z)}{\wp'(z)} = dz.$$

Definition 27. $c_\infty(E) = \delta_E\Omega_E$, where δ_E is the number of connected components of $E(\mathbb{R})$.

Next assume that p divides $C(E)$. Let $E_0(\mathbb{Q}_p)$ be the subgroup of points of $E(\mathbb{Q}_p)$ with non-singular reduction modulo p. The minimality of our generalized Weierstrass equation guarantees that the index $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is finite.

Definition 28. If p divides $C(E)$, define $c_p(E) = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$.

Tate gave a simple algorithm for computing $c_p(E)$ by working laboriously with an explicit Weierstrass equations. We also have

Lemma 29. *If E has split multiplicative reduction at p, then $c_p(E) = \operatorname{ord}_p(\Delta)$. In all other cases $c_p(E) \leq 4$.*

We shall establish some results about the computation of $c_p(E)$ for primes p additive reduction a little later in these lectures.

Full Birch-Swinnerton-Dyer Conjecture. *We have $r_E = g_E$, $Ш(E)$ is finite, and*

$$\frac{\mathscr{L}_E}{c_\infty(E)} = \frac{\sharp(Ш(E))R_\infty(E)}{\sharp(E(\mathbb{Q})_{tors})^2} \cdot \prod_{p|C(E)} c_p(E).$$

Example 30. Take $E : y^2 + xy = x^3 - x^2 - 2x - 1$, then $E = X_0(49)$, $C(E) = 49$, $E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$, and $r_E = 0$. We have

$$c_\infty(E) = \Omega_E = \frac{\Gamma(\frac{1}{7})\Gamma(\frac{2}{7})\Gamma(\frac{4}{7})}{2\pi\sqrt{7}} \qquad \text{(Chowla-Selberg)},$$

$$\frac{\mathscr{L}_E}{c_\infty(E)} = \frac{L(E,1)}{\Omega_E} = \frac{1}{2}, \;\; R_\infty(E) = 1, \;\; c_7(E) = 2.$$

Hence we get

$$\frac{1}{2} = \frac{\sharp(Ш(E))}{4} \times 2,$$

and so the full Birch-Swinnerton-Dyer conjecture is valid for E provided $\sharp(Ш(E)) = 1$. In fact, this is known to be true in this case.

The above exact formula has been tested numerically in a vast number of cases. We now explain our much more limited theoretical knowledge about this exact formula, discussing first rationality questions. Of course, this conjecture predicts, in particular, that

Conjecture. *For all elliptic curves $E/\mathbb{Q}$, we have*

$$\frac{\mathscr{L}_E}{c_\infty(E)R_\infty(E)} \in \mathbb{Q}.$$

The difficult case of the following theorem, in which $r_E = 1$, is due to Gross and Zagier [7]

Theorem 31. *If $r_E \leq 1$, then $\mathscr{L}_E/(c_\infty(E)R_\infty(E)) \in \mathbb{Q}$.*

Note that Kolyvagin [9] proved the deep result that $r_E \leq 1$ implies that $r_E = g_E$ and $Ш(E)$ is finite. But we stress it is unknown at present how to prove that $g_E \leq 1$ implies that $r_E = g_E$. If we make the stronger hypothesis that $g_E \leq 1$ and $Ш(E)$ is finite, then some results about $r_E = g_E$ can be proven using Iwasawa theory (e.g. it is true when E admits complex multiplication). When $r_E \geq 2$ (in particular, when $g_E \geq 2$), we stress that it has never been proven for a single elliptic curve E that $\mathscr{L}_\infty/c_\infty(E) \in \mathbb{Q}$. Of course, numerically it seems always to be true, but no proof is known for a single E.

We now discuss what is known about the exact Birch-Swinnerton-Dyer formula when we assume $r_E = 0$. Recall that, by Kolyvagin, $r_E = 0$ implies that $E(\mathbb{Q})$ and $Ш(E)$ are both finite. In this case, $\mathscr{L}_E = L(E,1)$ and $R_\infty = 1$. Define

$$L^{(alg)}(E,1) = \frac{L(E,1)}{c_\infty(E)},$$

which has long been known to be a rational number in accord with the Birch-Swinnerton-Dyer conjecture. But, even in this special case, the full exact Birch-Swinnerton-Dyer formula is only known in a few isolated examples, despite much loose talk to the contrary in the literature! In view of this, it is convenient to break the exact formula up into a p-part for all primes p. Put $\mathrm{Tam}(E) = \prod_{q|C(E)} c_q(E)$. Then we have the following p-part of the Birch-Swinnerton-Dyer conjecture:

Conjecture. *Assuming $r_E = 0$, we have, for all primes p,*

$$\mathrm{ord}_p\left(L^{(alg)}(E,1)\right) = \mathrm{ord}_p\left(\mathrm{Tam}(E)\right) - 2\,\mathrm{ord}_p\left(\sharp(E(\mathbb{Q}))\right) + \mathrm{ord}_p\left(\sharp(Ш(E))\right).$$

A considerable amount is known about this p-part of the Birch-Swinnerton-Dyer conjecture using Iwasawa theory (see [10]).

Theorem 32 (Rubin)**.** *Assume that $L(E,1) \neq 0$ and that E has complex multiplication. Then the p-part of the Birch-Swinnerton-Dyer conjecture holds for all primes $p \neq 2$ (in addition, if E has complex multiplication by $\mathbb{Q}(\sqrt{-3})$, we must exclude $p = 3$ as well as $p = 2$).*

When E does not have complex multiplication, we only have the far weaker statement:

Theorem 33 (Kato, Skinner-Urban)**.** *Assume that $L(E,1) \neq 0$. Then the p-part of the Birch-Swinnerton-Dyer conjecture holds for all good ordinary primes p except those in some specified list, which certainly includes $p = 2$.*

Hence we conclude that the 2-part of the Birch-Swinnerton-Dyer conjecture is largely unknown, even though it has been verified numerically in vast numbers of cases. However, the work of M. Razar and C. Zhao (see [15, 16, 17, 18]) has proved the 2-part of the Birch-Swinnerton-Dyer conjecture for certain infinite families of E with complex multiplication and having $r_E = 0$.

There are two very important reasons why are we interested in this 2-part of the Birch-Swinnerton-Dyer conjecture. Firstly, much of the time when one looks at numerical data on L-values (see, for example, the tables in [3]), one sees that the 2-part is "most" of $L^{(alg)}(E,1)$. This is presumably because it seems that usually $Ш$ is either trivial, or has very small order. Secondly, a knowledge of the 2-part of the conjecture is vital to generalize Tian's arguments so as to eventually prove, for many elliptic curves E, that there are large infinite families of quadratic twists of E, with root number -1, whose complex L-series have a simple zero at $s = 1$.

Quadratic Twists of an Elliptic Curve

Given an elliptic curve $E/\mathbb{Q}$, and a non-zero integer N which is not a square, we define $E^{(N)}$ to be the twist of E by the quadratic extension $\mathbb{Q}(\sqrt{N})/\mathbb{Q}$. Thus $E^{(N)}$ is the unique elliptic curve defined $\mathbb{Q}$, which is not isomorphic to E over $\mathbb{Q}$, but which becomes isomorphic to E over $\mathbb{Q}(\sqrt{N})$. Moreover, we then have that $E^{(N)}(\mathbb{Q}) \xrightarrow{\sim} E(\mathbb{Q}(\sqrt{N}))^-$, where this latter group is the subgroup of points in $E(\mathbb{Q}(\sqrt{N}))$ on which the non-trivial element of the Galois group of $\mathbb{Q}(\sqrt{N})/\mathbb{Q}$ acts like -1. As N varies, the $E^{(N)}$ provide the simplest infinite families of elliptic curves. Let $w_{E^{(N)}}$ be the root number of of the complex L-series of $E^{(N)}$. Roughly half the time $w_{E^{(N)}} = +1$, and half the time $w_{E^{(N)}} = -1$, as N varies. More precisely, let χ_N be the Dirichlet character corresponding to the quadratic extension $\mathbb{Q}(\sqrt{N})/\mathbb{Q}$. Then it is well known that $w_{E^{(N)}}$ is given explicitly by

$$w_{E^{(N)}} = \chi_N(-C(E))w_E,$$

provided the conductor of χ_N is prime to $C(E)$.

Example 34. Let $E = X_0(49) : y^2 + xy = x^3 - x^2 - x - 1$. Take $N > 1$, square free, and $(N,7) = 1$. Then $w_{E^{(N)}} = +1$. Liang (see [3] for more extensive Tables) calculated the $L(E^{(N)},1)$ for quite a large range of N using MAGMA. Recall that $L^{(alg)}(E,1) = \frac{1}{2}$.

N	$L^{(alg)}(E^{(N)},1)$
29	2
37	2
113	8
137	2
185	16
233	18
265	36
449	32
969	16

We see most of the time $L^{(alg)}(E^{(N)},1)$ is a power of 2, with only occasionally other small primes occurring (here $p=3$ for $N=233$ and 265).

Behaviour of Tamagawa Factors Under Twisting

If we want to understand the 2-part of the Birch-Swinnerton-Dyer conjecture for the $E^{(N)}$, we have to understand how the 2-part of the $c_p(E^{(N)})$ varies for primes p dividing N. For simplicity, in the discussion which follows, we will always assume that N is square free, odd, and $(N,C(E))=1$. Hence we know that for p dividing such N, the curve $E^{(N)}$ has additive reduction at p, and so $c_p(E^{(N)})\leq 4$, whence

$$\mathrm{ord}_2(c_p(E^{(N)}))=0,1,2.$$

When do these different options occur? For the curve $E: y^2=x^3-x$, we have $C(E)=32$, and $E^{(N)}: y^2=x^3-N^2x$. In this case, it is well known (for example, from Tate's algorithm) that $c_2(E^{(N)})=2$, and it is an immediate consequence of the results proven below that $c_p(E^{(N)})=4$ for all primes p dividing N. However, for other elliptic curves E, the situation is not so simple, as is shown by the following example.

Example 35. Let $E: y^2+y=x^3-x^2-7x+10$, so that $C(E)=11^2$, and $g_E=r_E=1$. We have $E(\mathbb{Q})=\mathbb{Z}$ and a generator is $(4,5)$. We consider $E^{(-M)}$, where M is any positive integer satisfying $M\equiv 3 \mod 4$, and $(M,11)=1$. It then turns out to be true that $c_{11}(E^{(-M)})=2$, $c_p(E^{(-M)})=2$ if p divides M and p is inert in $\mathbb{Q}(\sqrt{-11})$ (thus $p\equiv 2,6,7,8,10 \mod 11$). For most of the primes p which split in K (thus $p\equiv 1,3,4,5,9 \mod 11$), we have $c_p(E^{(-M)})=1$ for p dividing M. However, there is a sequence of split primes, starting with

$$53,257,269,397,401,421,617,757,773,929,\ldots$$

for which $c_p(E^{(-M)})=4$ when p divides M. What is the theoretical significance of these exceptional primes? Recall that $t_p=p+1-A_p$ is the trace of Frobenius of E at p. The key point is that the above exceptional primes p are those with $p\equiv 1 \mod 4$, and for which we have $t_p\equiv 0 \mod 2$.

We now explain how the $\mathrm{ord}_2(c_p(E^{(N)}))$, for p dividing N, can be calculated theoretically in many cases. Put

$$D_p(E)=E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p).$$

Lemma 36. *Assume E has bad additive reduction at p. Then, for all integers m with $(m,p)=1$, we have*

$$(*) \qquad D_p(E)[m]=E(\mathbb{Q}_p)[m].$$

Proof. We have the exact sequence

$$0\longrightarrow E_1(\mathbb{Q}_p)\longrightarrow E_0(\mathbb{Q}_p)\longrightarrow \mathbb{F}_p\longrightarrow 0\ .$$

Since $(m,p)=1$, it follows that multiplication by m is an automorphism of $E_0(\mathbb{Q}_p)$. It then follows by the snake lemma applied to the sequence

$$0\longrightarrow E_0(\mathbb{Q}_p)\longrightarrow E(\mathbb{Q}_p)\longrightarrow D_p(E)\longrightarrow 0$$

that $(*)$ is valid. □

Lemma 37. *Assume that N is an odd square free integer with $(N,C(E))=1$. Then, for all primes p dividing N, we have*

$$\mathrm{ord}_2(c_p(E^{(N)}))=\mathrm{ord}_2(E(\mathbb{Q}_p)[2]).$$

In particular, the left hand side depends only on p and not on N.

Proof. Since the j-invariant of $E^{(N)}$ is integral at p, it follows from the usual table of reduction types that $D_p(E^{(N)})$ has 2-primary subgroup which is one of 0, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Moreover, $E^{(N)}$ has bad additive reduction at p, and p is odd because N is odd. Hence by the above lemma

$$\mathrm{ord}_2(c_p(E^{(N)}))=\mathrm{ord}_2(\sharp(D_p(E^{(N)})[2]))=\mathrm{ord}_2(\sharp(E^{(N)}(\mathbb{Q}_p)[2])).$$

But clearly $E^{(N)}(\mathbb{Q}_p)[2]=E(\mathbb{Q}_p)[2]$, and the assertion follows. □

We can use this lemma to compute $c_p(E^{(N)})$ in many cases.

Lemma 38. *Let N be an odd square free integer with $(N,C(E))=1$, and let p be any prime dividing N. Assume first that E has supersingular reduction at p. If $p\equiv 1 \mod 4$, then $c_p(E^{(N)})=2$, and if $p>3$ with $p\equiv 3 \mod 4$, then $c_p(E^{(N)})$ is equal to 2 or 4. Assume next that E has ordinary reduction at p, and let $t_p=p+1-A_p$, where A_p denotes the number of points on the reduction of E modulo p. Then $\mathrm{ord}_2(c_p(E^{(N)}))=0$ if t_p is odd, and $c_p(E^{(N)})$ is equal to 2 or 4 if t_p is even.*

Proof. As p is odd, reduction modulo p gives an isomorphism

$$(1) \qquad E(\mathbb{Q}_p)[2]=\widetilde{E}(\mathbb{F}_p)[2].$$

But $\widetilde{E}(\mathbb{F}_p)$ has cardinality $A_p=p+1-t_p$. Recall also that $c_p(E^{(N)})\leq 4$. Assume first that $p>3$, and that p is supersingular for E. Then $t_p=0$ and $A_p=p+1$, and the the assertions of the lemma in this case now follow immediately from (1) and the previous lemma. Suppose next that p is ordinary for E. If t_p is odd, then $\mathrm{ord}_2(A_p)=0$. On the other hand, if t_p is even, then $\mathrm{ord}_2(A_p)>0$, but we cannot

say more about the kernel of multiplication by 2 on $\widetilde{E}(\mathbb{F}_p)$ other than it has order 2 or 4. This gives the remaining assertions of the lemma, and the proof is complete. □

Lemma 39. *Assume E has complex multiplication by the maximal order of an imaginary quadratic field K, and good reduction at 2. Let N be an odd square free integer with $(N, C(E)) = 1$. If p is a prime of good ordinary reduction for E with p dividing N and t_p even, then $c_p(E^{(N)}) = 4$.*

Proof. We have to show that, under the above hypotheses, we have $E(\mathbb{Q}_p)[2] = E[2]$. Since E has good reduction at $p \neq 2$, the extension $\mathbb{Q}_p(E[2])/\mathbb{Q}_p$ is unramified, and we must show it is trivial. Let σ_p denote a Frobenius automorphism at p. Since p splits in K, we can view $\sigma_p \in \mathrm{Gal}(\overline{K}/K)$, and we write ϕ_p for its image in $\mathrm{Aut}_{\mathcal{O}_K}(E[2])$. Now the characteristic polynomial of ϕ_p is

$$X^2 - t_p X + p \mod 2 = X^2 - 1$$

because t_p is even. Hence ϕ_p has order 1 or 2. But, as E has good reduction at 2, it follows that 2 does not ramify in K. Hence $\mathrm{Aut}_{\mathcal{O}_K}(E[2]) = (\mathcal{O}_K/2\mathcal{O}_K)^\times$ has no element of order 2. Thus we must have $\phi_p = 1$. This shows that $E(\mathbb{Q}_p)[2] = E[2]$, as required. □

Example 40. Let $E = X_0(49) : y^2 + xy = x^3 - x^2 - x - 1$. Then E has complex multiplication by the maximal order of $K = \mathbb{Q}(\sqrt{-7})$. Take N to be any odd square free integer with $(N, 7) = 1$, and let p be any prime dividing N. Then, by the theory of complex multiplication, E has supersingular reduction at p when p is inert in K, and E has ordinary reduction at p when p splits in K. Moreover, since $E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z}$ and p is odd, it follows that we always have t_p even. Hence the above lemmas give the following values for the Tamagawa factors. When p splits in K, we have $c_p(E^{(N)}) = 4$. Suppose next that p is inert in K. If $p \equiv 1 \, mod \, 4$, we have $c_p(E^{(N)}) = 2$, and if $p \equiv 3 \, mod \, 4$ with $p \neq 3$, then $c_p(E^{(N)})$ is equal to 2 or 4.

We end this section with the following general remarks. The long term goal of the material discussed in these lectures is to prove, given any $E/\mathbb{Q}$, that there is always an explicit infinite set of quadratic twists of E, say $\{E^{(N)} : N \in \mathscr{P}_E\}$, with $w_{E^{(N)}} = -1$, such that $L(E^{(N)}, s)$ has a zero at $s = 1$ of exact order 1. Tian recently succeeded in doing this for $E : y^2 = x^3 - x$, which, as usual, turns out to be the first elliptic curve for which a deep new arithmetic theorem is proven. We would like to generalize Tian's method to other E. For utterly mysterious reasons which we still do not understand yet, this requires us to prove a weak form of the 2-part of the Birch-Swinnerton-Dyer conjecture for a related infinite family of quadratic twists of E, say $\{E^{(N)} : N \in \mathscr{Z}_E\}$ with $w_{E^{(N)}} = +1$. So far, two methods are known for proving weak forms of the 2-part of the Birch-Swinnerton-Dyer conjecture for these infinite families of quadratic twists. They are:

1. Zhao's method,
2. Waldspurger's method.

Zhao's method (see [15, 16, 17, 18]) really requires E to have complex multiplication. The hope is that one can eventually adapt Waldspurger's method so that it works for all E. In the next lectures, I want to discuss a variant of Zhao's method which leads to an interesting set of results for the 2-part of the Birch-Swinnerton-Dyer conjecture for twists of an $E/\mathbb{Q}$, with good reduction at 2, and having complex multiplication. Later in the lectures, I will explain some joint work with Tian, Shuai Zhai, and Yongxiong Li (see [2]) which will carry out this full programme for the elliptic curve $E = X_0(49)$.

Basic Facts About a Class of Elliptic Curves with Complex Multiplication (Following Deuring)

Let K be an imaginary quadratic field with class number 1, and let $\mathcal{O}_K$ be the ring of integers of K. We now briefly recall the definition and basic properties of the Grossencharacter attached to elliptic curves with complex multiplication by the maximal order of K. Thus we assume that we are given an elliptic curve E/K together with an isomorphism $\mathcal{O}_K \xrightarrow{\sim} \mathrm{End}_K(E)$. Let S_E be the set of primes of K where E has bad reduction. For each $v \notin S_E$, we have the reduced elliptic curve $\widetilde{E}_v/k_v$, where k_v is the residue field of v. We also have a reduction map $\alpha \mapsto \widetilde{\alpha}$ from $\mathrm{End}_K(E)$ to $\mathrm{End}_{k_v}(\widetilde{E}_v)$. Let φ_v be the Frobenius endomorphism of $\widetilde{E}_v/k_v$, i.e.

$$\varphi_v(x, y) = (x^{Nv}, y^{Nv}), \text{ where } \mathrm{Nv} = \sharp(\mathrm{k_v}).$$

A key elementary fact is the following:

Lemma 41. *For each $v \notin S_E$, there exists a unique $\pi_v \in \mathcal{O}_K$ such that $\widetilde{\pi}_v = \varphi_v$.*

This leads us to the definition of the Grossencharacter ψ_E of E/K. We first remark that it is easy to see that $\pi_v \mathcal{O}_K = v$.

Definition 42. Let I_{S_E} be the group of fractional ideals of K prime to S_E. For $v \notin S_E$, define $\psi_E : I_{S_E} \longrightarrow K^\times$ by $\psi_E(v) = \pi_v$, and extend it by multiplicativity to the whole of I_{S_E}.

Theorem 43 (Deuring)**.** *There exists an integral ideal $\mathfrak{f}$ of K such that $\psi_E((\alpha)) = \alpha$ for all α in $K^\times$ with $\mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(\mathfrak{f})$ for all v dividing $\mathfrak{f}$.*

In other words, ψ_E is a Grossencharacter of K in the sense of Hecke. The proof uses the fact that $K(E(\overline{K})_{tors})/K$ is an abelian extension, and applies Artin's reciprocity law to a suitable finite sub-extension. Of course, the smallest integral ideal $\mathfrak{f}$ of K satisfying the property of this theorem is called the *conductor* of ψ_E. It is an important theorem that the prime divisors of the conductor of ψ_E are precisely the bad primes for E/K.

Example 44. Let $E : y^2 = x^3 - x$ so that $K = \mathbb{Q}(i)$, $\mathfrak{p}_2 = (1+i)$, and $\mathfrak{f} = \mathfrak{p}_2^3$. Then $\psi_E(\mathfrak{a}) = \alpha$, where α is the unique generator of $\mathfrak{a}$ which is $\equiv 1 \mod \mathfrak{f}$.

Fix an embedding $K \hookrightarrow \mathbb{C}$. The great importance of the Grossencharacter is that we can recover the complex L-function of E/K from the Hecke L-functions of ψ_E and its complex conjugate Grossencharacter, which we recall are defined by the Euler products

$$L(\psi_E, s) = \prod_v \left(1 - \frac{\psi_E(v)}{(Nv)^s}\right)^{-1}, \; L(\overline{\psi}_E, s) = \prod_v \left(1 - \frac{\overline{\psi}_E(v)}{(Nv)^s}\right)^{-1}.$$

The following theorem then follows easily from the definition of the Grossencharacter.

Theorem 45. *We have $L(E/K,s) = L(\psi_E,s)L(\overline{\psi}_E,s)$. If E is defined over $\mathbb{Q}$, then $\psi_E(\overline{\mathfrak{a}}) = \overline{\psi}_E(\mathfrak{a})$, and $L(\psi_E,s) = L(\overline{\psi}_E,s) = L(E,s)$, where this latter L-series is the complex L-function of $E/\mathbb{Q}$.*

We also need to mention two key facts about the abelian extensions of K generated by points of finite order on E. Let $\mathfrak{g}$ be any integral ideal of K, say $\mathfrak{g} = g\mathcal{O}_K$.

Definition 46. $E_\mathfrak{g} = \mathrm{Ker}(E(\overline{K}) \xrightarrow{g} E(\overline{K}))$.

Plainly $E_\mathfrak{g}$ is isomorphic to $\mathcal{O}_K/\mathfrak{g}\mathcal{O}_K$ as an $\mathcal{O}_K$-module. The action of $\mathrm{Gal}(K(E_\mathfrak{g})/K)$ on $E_\mathfrak{g}$ commutes with the $\mathcal{O}_K$-action, and gives an injection

$$j : \mathrm{Gal}(K(E_\mathfrak{g})/K) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(E_\mathfrak{g}) = (\mathcal{O}_K/\mathfrak{g})^\times.$$

Proposition 47. *If $\mathfrak{g}$ is divisible only by good primes for E/K, then j is an isomorphism.*

Proof. First take $\mathfrak{g} = v^n$, where v is a good prime and $n \geq 1$. Then E_{v^n} lies on the formal group of E at v, and this formal group is a Lubin-Tate group because E has good reduction at v. Thus, by Lubin-Tate theory, the extension $K_v(E_{v^n})/K_v$ is totally ramified and has Galois group isomorphic to $(\mathcal{O}_K/v^n\mathcal{O}_K)^\times$. The general case now follows easily. □

The next result shows that there is always degeneracy in this Galois group when $\mathfrak{g}$ is a multiple of the conductor of ψ_E.

Proposition 48. *Assume that $\mathfrak{g}$ is divisible by the conductor $\mathfrak{f}$ of ψ_E. Then $K(E_\mathfrak{g})$ coincides with the ray class field of K modulo $\mathfrak{g}$. In particular, j is not surjective, and its image always has index equal to $\sharp(\mu_K)$, where μ_K denotes the group of roots of unity of K.*

Proof. By the classical theory of complex multiplication, the ray class field of K modulo $\mathfrak{g}$ is always contained in the field $K(E_\mathfrak{g})$. On the other hand, no prime of K which does not divide $\mathfrak{g}$ is ramified in $K(E_\mathfrak{g})$. Let $\mathfrak{a} = (\alpha)$ be an integral ideal of K, where $\mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(\mathfrak{g})$ for all v dividing $\mathfrak{g}$. Then the Artin symbol of $\mathfrak{a}$ for the extension $K(E_\mathfrak{g})/K$ acts on $E_\mathfrak{g}$ by multiplication by $\psi_E(\mathfrak{a})$. But, since $\mathfrak{g}$ is divisible by $\mathfrak{f}$, we have $\psi_E(\mathfrak{a}) = \alpha$, whence the Artin symbol of $\mathfrak{a}$ acts trivially on $E_\mathfrak{g}$, because $\mathrm{ord}_v(\alpha - 1) \geq \mathrm{ord}_v(\mathfrak{g})$. Thus $K(E_\mathfrak{g})$ is contained in the ray class field of K modulo $\mathfrak{g}$. Note finally that, if ζ is a root of unity in K with $\zeta \equiv 1 \, mod \, \mathfrak{g}$, then necessarily $\psi(\zeta\mathcal{O}_K)$ must be equal to both ζ and 1, and so it follows that $\zeta = 1$. □

Example 49. Let $E : y^2 = x^3 - x$, so that $K = \mathbb{Q}(i)$, $\mathfrak{f} = \mathfrak{p}_2^3$, where $\mathfrak{p}_2 = (1+i)\mathcal{O}_K$, and $\mu_K = \mu_4$. If we take $\mathfrak{g} = \mathfrak{f}$, then we have $K(E_\mathfrak{f}) = K$, because the order of $Gal(K(E_\mathfrak{f})/K)$ is equal to $\sharp((\mathcal{O}_K/\mathfrak{p}_2^3)^\times)/4 = 1$. If we take $\mathfrak{g} = 4\mathcal{O}_K = \mathfrak{p}_2^4$, then $\sharp Gal(K(E_4)/K) = \sharp((\mathcal{O}_K/4\mathcal{O}_K)^\times)/4 = 2$. In fact, it is easily seen that, in this case, we have $K(E_4) = K(\mu_8) = K(\sqrt{2})$.

Finally, we state without proof the following well known relationship between conductors. Assume that E is defined over $\mathbb{Q}$, but has complex multiplication by the ring of integers of K. Let $C(E)$ be its conductor as an elliptic curve defined over $\mathbb{Q}$, and let $\mathfrak{f}$ be the conductor of its Grossencharacter ψ_E, when E is viewed as a curve defined over K.

Proposition 50. *We have $C(E) = |d_K| N_{K/\mathbb{Q}}\mathfrak{f}$, where d_K denotes the discriminant of K.*

Example 51. Let $E := X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1$. It has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-7})$. Let $\mathfrak{f}$ be the conductor of its Grossencharacter. Then $49 = 7 \cdot N_{K/\mathbb{Q}}\mathfrak{f}$. This immediately tells us that $\mathfrak{f} = \sqrt{-7}\mathcal{O}_K$. The above proposition then shows that the field $K(E_\mathfrak{f})$ has degree 3 over K, because the group of roots of unity of K has order 2.

Expression for the L-Series in Terms of Eisenstein Series

We shall now use the 19-th century expression, going back to Eisenstein and Kronecker, for the L-function of an elliptic curve with complex multiplication in terms of Eisenstein series, to study the 2-part of the conjecture of Birch and Swinnerton-Dyer for the quadratic twists, with root number $+1$, of our fixed elliptic curve with complex multiplication. This method was pioneered by Zhao [15, 16, 17, 18] for the quadratic twists of the curve $y^2 = x^3 - x$, and we shall use a variant of it. However, later we will use the quite different modular parametrization of our curve to study the conjecture of Birch and Swinnerton-Dyer for the quadratic twists of E with root number -1, following Tian's [12, 13] method.

Let K be an imaginary quadratic field, and $\mathcal{O}_K$ the ring of integers of K. We assume for the whole of this section that we are given an elliptic curve E/K with $\mathrm{End}_K(E) = \mathcal{O}_K$. Thus, by the theory of complex multiplication, K necessarily has class number 1. Fix a generalized global minimal equation for E

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \; (a_i \in \mathcal{O}_K).$$

We assume $K \hookrightarrow \mathbb{C}$, and let $\mathscr{L}$ be the period lattice of the Néron differential $dx/(2y + a_1x + a_3)$ on E. Then $\mathscr{L}$ is a free $\mathcal{O}_K$-module of rank 1, and so we can find $\Omega_\infty \in \mathbb{C}^\times$ such that $\mathscr{L} = \Omega_\infty\mathcal{O}_K$. Let $\mathfrak{f}$ be the conductor of ψ_E, and let $\mathfrak{g}$ be some integral multiple of $\mathfrak{f}$. Let S be the set of primes of K dividing $\mathfrak{g}$. We consider the (usually) imprimitive Hecke L-function

$$L_S(\overline{\psi}_E, s) = \sum_{(\mathfrak{a},\mathfrak{g})=1} \frac{\overline{\psi}_E(\mathfrak{a})}{(N\mathfrak{a})^s}.$$

We want to express this L-function in terms of Kronecker-Eisenstein series. We now recall the definition of these Kronecker-Eisenstein series (see [6]). Let L be any lattice in the complex plane.

Definition 52. Let

$$H(z,s,L)=\sum_{w\in L}\frac{\overline{z}+\overline{w}}{|z+w|^{2s}};$$

here, of course, we exclude $-z$ from the sum if $z\in L$. This series converges for $\mathrm{Re}(s)>\frac{3}{2}$. It is well-known that $H(z,s,L)$ has an analytic continuation to the whole complex plane (see, for example, [6]).

Let $\mathfrak{R}=K(E_{\mathfrak{g}})$, so that $\mathfrak{R}$ is the ray class field of K modulo $\mathfrak{g}$, because of our hypothesis that $\mathfrak{g}$ is divisible by the conductor $\mathfrak{f}$ of ψ_E. Let $\mathcal{B}$ be any set of integral ideals of K, prime to $\mathfrak{g}$, whose Artin symbols give rise precisely to $\mathrm{Gal}(\mathfrak{R}/K)$. Fix any generator g of $\mathfrak{g}$, so that $\mathfrak{g}=g\mathcal{O}_K$.

Theorem 53. *We have*

$$L_S(\overline{\psi}_E,s)=\frac{|\Omega_\infty/g|^{2s}}{\overline{\Omega_\infty/g}}\sum_{\mathfrak{b}\in\mathcal{B}}H\left(\psi_E(\mathfrak{b})\frac{\Omega_\infty}{g},s,\mathscr{L}\right).$$

Proof. By a remark made earlier, we have $\mathfrak{b}=\psi_E(\mathfrak{b})\mathcal{O}_K$ for $(\mathfrak{b},\mathfrak{g})=1$. Thus, as $\mathfrak{R}$ is the ray class field mod $\mathfrak{g}$, the Artin map shows that $\mathrm{Gal}(\mathfrak{R}/K)\xrightarrow{\sim}(\mathcal{O}_K/\mathfrak{g})^\times/\widetilde{\mu}_K$. As the $\psi_E(\mathfrak{b})(\mathfrak{b}\in\mathcal{B})$ are representatives of generators of ideals in $\mathcal{B}$, we see that the ideals $(\psi_E(\mathfrak{b})+c)$, with $\mathfrak{b}$ running over $\mathcal{B}$, and c running over $\mathfrak{g}$, give all integral ideals of K prime to $\mathfrak{g}$. Hence

$$L_S(\overline{\psi}_E,s)=\sum_{\mathfrak{b}\in\mathcal{B}}\sum_{c\in\mathfrak{g}}\frac{\overline{\psi}_E((\psi_E(\mathfrak{b})+c))}{|\psi_E(\mathfrak{b})+c|^{2s}}.$$

But

$$(\psi_E(\mathfrak{b})+c)=(\psi_E(\mathfrak{b}))\left(1+\frac{c}{\psi_E(\mathfrak{b})}\right)=\mathfrak{b}\left(1+\frac{c}{\psi_E(\mathfrak{b})}\right).$$

Hence, as $\mathfrak{f}$ divides $\mathfrak{g}$, we obtain

$$\psi_E((\psi_E(\mathfrak{b})+c))=\psi_E(\mathfrak{b})\left(1+\frac{c}{\psi_E(\mathfrak{b})}\right)=\psi_E(\mathfrak{b})+c.$$

Hence

$$L_S(\overline{\psi}_E,s)=\sum_{\mathfrak{b}\in\mathcal{B}}\sum_{c\in\mathfrak{g}}\frac{\overline{\psi_E(\mathfrak{b})+c}}{|\psi_E(\mathfrak{b})+c|^{2s}}=\sum_{\mathfrak{b}\in\mathcal{B}}H(\psi_E(\mathfrak{b}),s,\mathfrak{g}).$$

We now renormalize the right hand side in the obvious fashion to get the desired result. □

Before going further, we digress to discuss the Eisenstein series of weight 1 for an arbitrary lattice L in the complex plane. If we naively put $s=1$ in the series for $H(z,s,L)$ we get the non-convergent series

$$\sum_{w\in L}\frac{1}{z+w}.$$

In order to avoid the difficulties with convergence, we therefore define:

Definition 54. $\mathscr{E}_1^*(z,L)=H(z,1,L)$, where we have now taken the value of analytic continuation of $H(z,s,L)$ at $s=1$.

Write $L=\mathbb{Z}u+\mathbb{Z}v$ with $\mathrm{Im}(v/u)>0$. We then define the positive real number $A(L)$ by $A(L)=\frac{\bar{u}v-u\bar{v}}{2\pi i}$. Also let

$$s_2(L)=\lim_{s\to0,s>0}\sum_{w\in L\setminus\{0\}}w^{-2}|w|^{-2s}.$$

Let $\sigma(z,L)$, $\zeta(z,L)$, $\wp(z,L)$ be the respective Weierstrass σ-function, zeta function, and $\wp$-function attached to L. Hence

$$\zeta(z,L)=\frac{d}{dz}\log\sigma(z,L),\quad \wp(z,L)=-\zeta'(z,L).$$

The following theorem goes back to Eisenstein (for a modern treatment, see [6]).

Theorem 55. *We have* $\mathscr{E}_1^*(z,L)=\zeta(z,L)-zs_2(L)-\bar{z}A(L)^{-1}$.

In particular, we see that $\mathscr{E}_1^*(z,L)$ is <u>not</u> holomorphic as a function of z. However, it is obviously periodic, that is $\mathscr{E}_1^*(z+w,L)=\mathscr{E}_1^*(z,L)$ for $w\in L$. But naturally it cannot be written as a rational function of $\wp(z,L),\wp'(z,L)$.

For each integer $m\geq2$, we define

$$2B_m(z,L)=\frac{\wp'(z,L)}{\wp'(z,L)}+\sum_{k=2}^{m-1}\frac{\wp'(kz,L)-\wp'(z,L)}{\wp(kz,L)-\wp(z,L)}.$$

Lemma 56. *For all integers $m\geq2$, we have*

$$B_m(z,L)=\mathscr{E}_1^*(mz,L)-m\mathscr{E}_1^*(z,L).$$

Proof. Using $\mathscr{E}_1^*(z,L)=\zeta(z,L)-zs_2(L)-\bar{z}A(L)^{-1}$, we immediately obtain

$$\mathscr{E}_1^*(mz,L)-m\mathscr{E}_1^*(z,L)=\zeta(mz,L)-m\zeta(z,L).$$

Now we have the addition formula

$$\zeta(z_1+z_2,L)=\zeta(z_1,L)+\zeta(z_2,L)+\frac{1}{2}\frac{\wp'(z_1,L)-\wp'(z_2,L)}{\wp(z_1,L)-\wp(z_2,L)}.$$

Letting $z_1\to z_2$, we get the above formula for $m=2$. For any $m\geq2$, the addition formula shows that

$$\begin{aligned}&\zeta((m+1)z,L)-(m+1)\zeta(z,L)\\&\quad=\zeta(mz,L)-m\zeta(z,L)+\frac{1}{2}\frac{\wp'(mz,L)-\wp'(z,L)}{\wp(mz,L)-\wp(z,L)},\end{aligned}$$

and so the lemma clearly follows by induction on m. □

The next lemma is attributed to Swinnerton-Dyer in [4].

Lemma 57. *Let u be a complex number such that $u+L$ has exact finite order $m\geq3$ in $\mathbb{C}/L$. Then*

$$\mathscr{E}_1^*(u,L)=-B_{m-1}(u,L)/m.$$

Proof. By the previous lemma, we have, since $m \geq 3$,

$$B_{m-1}(u,L) = \mathscr{E}_1^*((m-1)u,L) - (m-1)\mathscr{E}_1^*(u,L).$$

But $\mathscr{E}_1^*(-u,L) = -\mathscr{E}_1^*(u,L)$, and $\mathscr{E}_1^*(z,L)$ is periodic with respect to L. Hence, as $mu \in L$, we have

$$\mathscr{E}_1^*((m-1)u,L) = \mathscr{E}_1^*(-u,L) = -\mathscr{E}_1^*(u,L),$$

and the assertion now follows from the previous lemma. □

Corollary 58. *Let $E_L = \mathbb{C}/L$, and let F be any field of definition of E_L. Assume $u \in \mathbb{C}$ is such that $u+L$ has exact order $m \geq 3$ in $\mathbb{C}/L$. Then*

$$\mathscr{E}_1^*(u,L) \in F(E_L[m]).$$

We now return to our elliptic curve E/K with complex multiplication. Putting $s = 1$ in the earlier Theorem 53, we get:

Theorem 59. *We have*

$$\frac{L_S(\overline{\psi}_E, 1)}{\Omega_\infty} = g^{-1} \sum_{\mathfrak{b} \in \mathcal{B}} \mathscr{E}_1^*\left(\psi_E(\mathfrak{b})\frac{\Omega_\infty}{g}, \mathscr{L}\right).$$

It is more convenient to write this result in a slightly different form

Theorem 60. *We have that $\mathscr{E}_1^*(\frac{\Omega_\infty}{g}, \mathscr{L})$ lies in the field $\mathcal{R}$, and*

$$\frac{L_S(\overline{\psi}_E, 1)}{\Omega_\infty} = g^{-1}\,\mathrm{Tr}_{\mathcal{R}/K}\left(\mathscr{E}_1^*\left(\frac{\Omega_\infty}{g}, \mathscr{L}\right)\right).$$

Proof. The first assertion follows immediately from the above corollary applied to E/K, since $\mathcal{R} = K(E_\mathfrak{g})$. For $\mathfrak{b} \in \mathcal{B}$, let $\sigma_\mathfrak{b}$ be the Artin symbol of $\mathfrak{b}$ in $\mathrm{Gal}(\mathcal{R}/K)$. Then, essentially from the definition of the Grossencharacter, we have

$$\sigma_\mathfrak{b}\left(\wp\left(\frac{\Omega_\infty}{g}, \mathscr{L}\right),\ \wp'\left(\frac{\Omega_\infty}{g}, \mathscr{L}\right)\right) = \left(\wp\left(\frac{\psi_E(\mathfrak{b})\Omega_\infty}{g}, \mathscr{L}\right),\ \wp'\left(\frac{\psi_E(\mathfrak{b})\Omega_\infty}{g}, \mathscr{L}\right)\right).$$

It then follows form the lemma 57 that

$$\sigma_\mathfrak{b}\left(\mathscr{E}_1^*\left(\frac{\Omega_\infty}{g}, \mathscr{L}\right)\right) = \mathscr{E}_1^*\left(\frac{\psi_E(\mathfrak{b})\Omega_\infty}{g}, \mathscr{L}\right),$$

whence the result follows immediately. □

We now consider the twisting of E by certain quadratic extensions of K.

Lemma 61. *Let M be a non-zero and non-unit element of $\mathcal{O}_K$, such that (i) M is square free, (ii) M is prime to the discriminant of K, and (iii) $M \equiv 1 \mod 4$. Then the extension $K(\sqrt{M})/K$ has conductor equal to $M\mathcal{O}_K$.*

Proof. Since M is square free and not divisible by a prime above 2, the extension $K(\sqrt{M})/K$ is totally and tamely ramified at all primes dividing of K dividing M. Thus we need only show that the primes of K above 2 are not ramified in this extension. Let v be a place of K above 2. Let w be such that $w^2 = M$, and put $z = \frac{w-1}{2}$. Then z is a root of the polynomial $f(X) = X^2 - X - \frac{(M-1)}{4}$, so that z is an algebraic integer. But $f'(z) = 2z - 1$, whence $f'(z)$ is a unit at v, and thus $K(\sqrt{M})/K$ is unramified. □

Let M be as in the lemma above, and assume, in addition, from now on that $(M, \mathfrak{f}) = 1$. Let $E^{(M)}$ be the twist of E by the quadratic extension $K(\sqrt{M})/K$, and let $\mathcal{X}_M$ denote the abelian character of K defining this extension. The following lemma is then immediate, the second part being valid because $(M, \mathfrak{f}) = 1$. To simplify notation, we shall from now on denote the Grossencharacter of E by ψ.

Lemma 62. *Let ψ_M denote the Grossencharacter of $E^{(M)}/K$. Then $\psi_M = \psi\mathcal{X}_M$. Moreover, ψ_M has conductor $M\mathfrak{f}$.*

What is the period lattice of $E^{(M)}$? Recall that we have fixed a global minimal Weierstrass equation for E/K with coordinates x, y. Then

$$\wp(z, \mathscr{L}) = x + (a_1^2 + 4a_2)/12, \quad \wp'(z, \mathscr{L}) = 2y + a_1 x + a_3,$$

where $\mathscr{L} = \Omega_\infty \mathcal{O}_K$.

Lemma 63. *A period lattice for $E^{(M)}$ over $\mathbb{C}$ is given by*

$$\mathscr{L}_M = \frac{\Omega_\infty}{\sqrt{M}}\mathcal{O}_K.$$

Proof. Suppose E has classical Weierstrass equation

$$Y^2 = 4X^3 - g_2(\mathscr{L})X - g_3(\mathscr{L})$$

where $X = \wp(z, \mathscr{L})$, $Y = \wp'(z, \mathscr{L})$. Then $E^{(M)}$ has classical Weierstrass equation

$$Y^2 = 4X^3 - M^2 g_2(\mathscr{L})X - M^3 g_3(\mathscr{L}),$$

and so

$$\mathscr{L}_M = \frac{\Omega_\infty}{\sqrt{M}}\mathcal{O}_K.$$ □

We now establish the key averaging lemma, from which all of our later induction arguments to study the 2-part of the Birch-Swinnerton-Dyer conjecture will follow. Let n be any integer ≥ 0, and suppose that we are given n elements $\pi_1, \ldots, \pi_n$ of $\mathcal{O}_K$ (we take the empty set of elements if $n = 0$), which generate distinct prime ideals in $\mathcal{O}_K$, and which satisfy

(i) $(\pi_j, d_K) = 1$,
(ii) $(\pi_j, \mathfrak{f}) = 1$, and
(iii) $\pi_j \equiv 1 \mod 4$ $(1 \leq j \leq n)$.

Recalling that $\mathfrak{f} = f\mathcal{O}_K$, we then define

$$\mathfrak{M}_n = \pi_1 \cdots \pi_n, \quad g_n = \mathfrak{M}_n f, \quad \mathfrak{g}_n = g_n \mathcal{O}_K.$$

Definition 64. Let $\mathcal{R}_n$ be the ray class field of K modulo $\mathfrak{g}_n$.

Since $\pi_j \equiv 1 \mod 4$, and $(\pi_j, d_K) = 1$, the quadratic extension $K(\sqrt{\pi_j})/K$ has conductor $\pi_j \mathcal{O}_K$ by our earlier lemma. Hence, as its conductor divides $\mathfrak{g}_n$, we see that $K(\sqrt{\pi_j}) \subset \mathcal{R}_n$.

Definition 65. $\mathscr{D}_n$ = set of all divisors of $\mathfrak{g}_n$ which are given by any product of the elements in a subset of $\{\pi_1, \dots, \pi_n\}$.

Finally, define

Definition 66. $\mathscr{J}_n = K(\sqrt{\pi_1}, \dots, \sqrt{\pi_n})$.

Hence, by the above remark, $\mathscr{J}_n$ is a subfield of $\mathcal{R}_n$. Let S_n be the set of prime ideals $\{(\pi_1), \dots, (\pi_n)\}$. For $M \in \mathscr{D}_n$, we write $L_{S_n}(\overline{\psi}_M, s)$ for the Hecke L-function of $\overline{\psi}_M$, with the Euler factors for the places of K in S_n removed from its Euler product. The following averaging lemma is fundamental for our subsequent arguments.

Theorem 67. *For all sequences $\pi_1, \dots, \pi_n$ as above, we have*

$$\sum_{M \in \mathscr{D}_n} L_{S_n}(\overline{\psi}_M, 1)/\Omega_\infty = 2^n \operatorname{Tr}_{\mathcal{R}_n/\mathscr{J}_n}\left(g_n^{-1} \mathscr{E}_1^*\left(\frac{\Omega_\infty}{g_n}, \mathscr{L}\right)\right).$$

Proof. We have

$$\frac{L_{S_n}(\overline{\psi}_M, 1)}{\frac{\Omega_\infty}{\sqrt{M}}} = \operatorname{Tr}_{\mathcal{R}_n/K}\left(g_n^{-1} \mathscr{E}_1^*\left(\frac{\Omega_\infty}{\sqrt{M} g_n}, \mathscr{L}_M\right)\right).$$

But we have $\mathscr{E}_1^*(z, L) = \lambda \mathscr{E}_1^*(\lambda z, \lambda L)$ for any $\lambda \in \mathbb{C}^\times$. Taking $\lambda = (\sqrt{M})^{-1}$, and writing $G_n = \operatorname{Gal}(\mathcal{R}_n/K)$, we obtain

$$\frac{L_{S_n}(\overline{\psi}_M, 1)}{\Omega_\infty} = \sum_{\sigma \in G_n} (\sqrt{M})^{\sigma - 1} g_n^{-1}\left(\mathscr{E}_1^*\left(\frac{\Omega_\infty}{g_n}, \mathscr{L}\right)\right)^\sigma.$$

All is now clear from the following lemma:

Lemma 68. *Let $H_n = \operatorname{Gal}(\mathcal{R}_n/\mathscr{J}_n)$. If $\sigma \in G_n$, then*

$$\sum_{M \in \mathscr{D}_n} (\sqrt{M})^{\sigma - 1} = \begin{cases} 2^n, & \text{if } \sigma \in H_n; \\ 0, & \text{if } \sigma \notin H_n. \end{cases}$$

The first assertion of this lemma is clear. Take $\sigma \notin H_n$, and suppose that σ maps $k \geq 1$ elements of $\{\sqrt{\pi_1}, \dots, \sqrt{\pi_n}\}$ to minus themselves. Let $V(\sigma)$ be the subset of $\{\sqrt{\pi_1}, \dots, \sqrt{\pi_n}\}$ which are mapped to minus themselves. If $M \in \mathscr{D}_n$, then σ will fix $\sqrt{M}$ if and only if it is a product of an even number of elements of $V(\sigma)$. Hence the total number of M in $\mathscr{D}_n$ with $\sqrt{M}$ fixed by σ is

$$2^{n-k}\left(\binom{k}{0} + \binom{k}{2} + \binom{k}{4} + \cdots\right) = 2^{n-1}.$$

Similarly, the total number of M in $\mathscr{D}_n$ such that $\sigma\sqrt{M} = -\sqrt{M}$ is

$$2^{n-k}\left(\binom{k}{1} + \binom{k}{3} + \cdots\right) = 2^{n-1}.$$

Since these last two expressions are equal, the second assertion of the lemma follows. □

CM Elliptic Curves Defined over K Having Good Reduction at Primes above 2

From now on, we shall only be concerned with elliptic curves E/K with $\operatorname{End}_K(E) = \mathcal{O}_K$, and having the additional property that E has good reduction at all places v of K dividing 2. We denote the Grossencharacter of E/K simply by ψ, and $\mathfrak{f}$ will always denote its conductor. Much of the material we discuss in this section, in particular the proof of Theorem 72, is taken from [3].

Example 69. Let $E = X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1$, so $K = \mathbb{Q}(\sqrt{-7})$, $C(E) = 49$. The prime 2 splits in $\mathbb{Q}(\sqrt{-7})$, which implies that E has good ordinary reduction at 2

Example 70. Let $E : y^2 + y = x^3 - x^2 - 7x + 10$, so $K = \mathbb{Q}(\sqrt{-11})$, $C(E) = 121$. The prime 2 is inert in $\mathbb{Q}(\sqrt{-11})$, which implies that E has good supersingular reduction at 2.

As earlier, $\{\pi_1, \dots, \pi_n\}$ will always be $n \geq 0$ distinct prime elements of K satisfying

$$(2) \qquad (\pi_j, d_K) = 1, \ \ (\pi_j, \mathfrak{f}) = 1, \ \ \pi_j \equiv 1 \ mod\ 4\, (1 \leq j \leq n),$$

and we put $g_n = \pi_1 \cdots \pi_n f$, where $\mathfrak{f} = f\mathcal{O}_K$. Again $\mathcal{R}_n$ will be the ray class field of K modulo $\mathfrak{g}_n$, which we recall coincides with the field $K(E_{g_n})$. Again put $\mathscr{J}_n = K(\sqrt{\pi_1}, \dots, \sqrt{\pi_n})$, which we showed earlier is a subfield of $\mathcal{R}_n$. For simplicity, we assume in what follows that $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$, so that 2 is not ramified in K. If v is any prime of $\overline{\mathbb{Q}}$ above 2, we always normalize ord_v so that $\operatorname{ord}_v(2) = 1$. We write a_1 for the coefficient of xy in our fixed global minimal Weierstrass equation for E/K.

Definition 71. $\Lambda_n(E) = \operatorname{Tr}_{\mathcal{R}_n/\mathscr{J}_n}(g_n^{-1} \mathscr{E}_1^*(\frac{\Omega_\infty}{g_n}, \mathscr{L}))$.

Theorem 72. *Assume E has good reduction at the primes of K above 2. Then, for all $n \geq 0$*

$$\operatorname{ord}_v(\Lambda_n(E)) \geq -1$$

for all primes v of $\mathscr{J}_n$ above 2. Moreover, $\operatorname{ord}_v(\Lambda_n(E)) \geq 0$ *if 2 divides a_1 in $\mathcal{O}$.*

Note that, when $n = 0$, we have $L(\overline{\psi}, 1)/\Omega_\infty = \Lambda_0(E)$. Hence we immediately obtain the following special case of this theorem.

Corollary 73. *For all places v of K above 2, we have* $\operatorname{ord}_v(\frac{L(\overline{\psi},1)}{\Omega_\infty}) \geq -1$. *Moreover, if 2 divides a_1, then* $\operatorname{ord}_v(\frac{L(\overline{\psi},1)}{\Omega_\infty}) \geq 0$.

This result is best possible. For example, if we take $E = X_0(49)$, we have $a_1 = 1$, and $L(\overline{\psi}, 1)/\Omega_\infty = \frac{1}{2}$.

For the proof of the above theorem, it is simplest to find an alternative expression for $B_m(z, L)$, where $(m \geq 2)$ for any lattice L in $\mathbb{C}$. Recall that $B_m(z, L)$ is defined by

$$B_m(z, L) = \frac{1}{2}\frac{\wp''(z, L)}{\wp'(z, L)} + \frac{1}{2}\sum_{k=2}^{m-1} \frac{\wp'(kz, L) - \wp'(z, L)}{\wp(kz, L) - \wp(z, L)}.$$

Lemma 74. *For all $m \geq 2$, we have*

$$B_m(z,L) = \sum_{k=1}^{m-1} (\wp((k+1)z,L) + \wp(kz,L) + \wp(z,L))^{\frac{1}{2}},$$

with an appropriate choice of the square root in each case.

Proof. We have the addition formula

$$\wp(z_1+z_2,L)+\wp(z_1,L)+\wp(z_2,L) = \frac{1}{4}\left(\frac{\wp'(z_1,L)-\wp'(z_2,L)}{\wp(z_1,L)-\wp(z_2,L)}\right)^2.$$

Letting $z_1 \to z_2$, and taking square roots, we get the formula for $m = 2$. If $k \geq 2$, we also obtain

$$\wp((k+1)z,L)+\wp(kz,L)+\wp(z,L) = \frac{1}{4}\left(\frac{\wp'(kz,L)-\wp'(z,L)}{\wp(kz,L)-\wp(z,L)}\right)^2,$$

and so the assertion of the lemma follows by induction on m. □

We recall that if u is a complex number such that u has finite exact order $m \geq 3$ in $\mathbb{C}/L$, then $\mathscr{E}_1^*(u,L) = -\frac{1}{m}B_{m-1}(u,L)$.

Corollary 75. *Assume u has exact order $m \geq 3$ in $\mathbb{C}/L$. Then*

$$\mathscr{E}_1^*(u,L) = -\frac{1}{m}\sum_{k=1}^{m-2} (\wp((k+1)u,L) + \wp(ku,L) + \wp(u,L))^{\frac{1}{2}}.$$

Proof of Theorem 72. Take $L = \mathscr{L}$, and $u = \Omega_\infty/g_n$. Let m be the least positive rational integer in $\mathfrak{g}_n = g_n\mathcal{O}_K$. Since $\mathfrak{f}$ must be divisible by at least one prime of K, and no prime divisor of $\mathfrak{f}$ lies above 2, we must have $m \geq 3$. Let P be the point on E corresponding to $u = \Omega_\infty/g_n$ on $\mathbb{C}/\mathscr{L}$. Recalling that

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is our global minimal generalized Weierstrass equation for E, we make the following key observation. For all places v of $\overline{\mathbb{Q}}$ above 2, we have $\mathrm{ord}_v(x(P)) \geq 0$ and $\mathrm{ord}_v(y(P)) \geq 0$.

Indeed, if $\mathrm{ord}_v(x(P)) < 0$, then P would necessarily lie on the formal group of E at v since there is good reduction at v. But this is impossible because P has finite order m, which is odd. Recalling that

$$\wp(ru,\mathscr{L}) = x(rP) + \frac{a_1^2+4a_2}{12} \quad (r = 1,\ldots,m-1).$$

The assertion of Theorem 72 is now clear from the above corollary. □

Our next goal is to establish the following stronger result.

Theorem 76. *Assume that E has good reduction at all places of K above 2. If $n \geq 1$, we have*

$$\mathrm{ord}_v(\Lambda_n(E)) \geq 0$$

for all places v of $\mathscr{J}_n$ above 2.

Before embarking on the proof, we need a preliminary lemma.

Lemma 77. *Let v be any place of K where E has good reduction, and let $\pi_v = \psi(v)$. Then the formal group of E at v is a Lubin-Tate formal group over K_v, with local parameter π_v.*

Proof. The parameter on the curve of the formal group is $t = -x/y$, and the assertion of the lemma then follows easily from the fact that $\widetilde{\pi}_v(x,y) = (x^{N_v}, y^{N_v})$ on the reduction of E modulo v. □

The next corollary is an immediate consequence of Lubin-Tate theory.

Corollary 78. *Let v be any place of K where E has good reduction. Then the action of $\mathrm{Gal}(K(E_{\pi_v^n})/K)$ on $E_{\pi_v^n}$ gives an isomorphism from this Galois group onto $(\mathcal{O}_K/v^n\mathcal{O}_K)^\times$. Moreover, v is totally ramified in the extension $K(E_{\pi_v^n})/K$.*

We now use a consequence of these results the field $\mathcal{R}_n = K(E_{g_n})$. Put $F = K(E_f)$.

Lemma 79. *The action of the Galois group of $\mathcal{R}_n/F$ on $E_{\mathfrak{M}_n}$ defines an isomorphism,*

$$j_n : \mathrm{Gal}(\mathcal{R}_n/F) \xrightarrow{\sim} (\mathcal{O}_K/\mathfrak{M}_n\mathcal{O}_K)^\times.$$

Proof. By the above lemma, since each (π_i) is totally ramified in $K(E_{\pi_i})/K$, we see that $K(E_{\mathfrak{M}_n}) \cap F = K$, and that $\mathrm{Gal}(K(E_{\mathfrak{M}_n})/K) \xrightarrow{\sim} (\mathcal{O}/\mathfrak{M}_n\mathcal{O})^\times$. The assertion of the lemma is then clear. □

We now define τ to be the element of order 2 in $\mathrm{Gal}(\mathcal{R}_n/F)$ defined by

$$\tau = j_n^{-1}(-1 \mod \mathfrak{M}_n).$$

Write $\mathscr{P}_n$ for the fixed field of this element τ in $\mathrm{Gal}(\mathcal{R}_n/F)$. Hence we have $[\mathcal{R}_n : \mathscr{P}_n] = 2$.

Lemma 80. *The element τ fixes the field $F(\sqrt{\pi_1},\ldots,\sqrt{\pi_n})$.*

Proof. It suffices to show that τ fixes $K(\sqrt{\pi_i})$ for $i = 1,\ldots,n$. Since $\pi_i \equiv 1 \mod 4$, $(\mathcal{O}_K/\pi_i\mathcal{O}_K)^\times$ is a cyclic group whose order is divisible by 4. Thus -1 is a square in $(\mathcal{O}_K/\pi_i\mathcal{O}_K)^\times$, and so it must fix the unique quadratic subfield $K(\sqrt{\pi_j})$ when viewed as an element of $\mathrm{Gal}(K(E_{\pi_j})/K)$. □

In order to establish Theorem 76, it clearly suffices to establish the following result.

Proposition 81. *When $n \geq 1$, the element $\mathrm{Tr}_{\mathcal{R}_n/\mathscr{P}_n}(g_n^{-1}\mathscr{E}_1^* \times (\frac{\Omega_\infty}{g_n}, \mathscr{L}))$ is integral at all places of $\mathscr{P}_n$ above 2.*

Note first that, since $(f, \mathfrak{M}_n) = 1$, we can find α, β in $\mathcal{O}_K$ such that $1 = \alpha\mathfrak{M}_n + \beta f$. It follows immediately that, for all $n \geq 1$,

$$\mathrm{Tr}_{\mathcal{R}_n/\mathscr{P}_n}\left(g_n^{-1}\mathscr{E}_1^*\left(\frac{\Omega_\infty}{g_n}, \mathscr{L}\right)\right) = g_n^{-1}\left(\mathscr{E}_1^*(u_1+u_2,\mathscr{L}) + \mathscr{E}_1^*(u_1-u_2,\mathscr{L})\right),$$

where $u_1 = \alpha\Omega_\infty/f$, $u_2 = \beta\Omega_\infty/\mathfrak{M}_n$. We now simplify the right hand side by using the following general identity. Let L be any lattice in $\mathbb{C}$, and let z_1, z_2 be arbitrary complex variables.

Lemma 82. $\mathscr{E}_1^*(z_1+z_2,L)+\mathscr{E}_1^*(z_1-z_2,L) = 2\mathscr{E}_1^*(z_1,L) + \frac{\wp'(z_1,L)}{\wp(z_1,L)-\wp(z_2,L)}$.

Proof. Using $\mathscr{E}_1^*(z,L) = \zeta(z,L) - zs_2(L) - \bar{z}/A(L)$, we deduce that

$$\mathscr{E}_1^*(z_1+z_2,L)+\mathscr{E}_1^*(z_1-z_2,L) = \zeta(z_1+z_2,L)+\zeta(z_1-z_2,L) - 2z_1 s_2(L) - 2\bar{z_1}/A(L).$$

We then use that identity

$$\zeta(u+v,L) = \zeta(u,L)+\zeta(v,L)+\frac{1}{2}\frac{\wp'(u,L)-\wp'(v,L)}{\wp(u,L)-\wp(v,L)}$$

for $u = z_1$, $v = z_2$, and for $u = z_1$, $v = -z_2$. Noting that $\zeta(-z_2,L) = -\zeta(z_2,L)$, the assertion of the lemma follows. □

We now return to our curve $E = \mathbb{C}/\mathscr{L}$. Let P_1 be the point on E given by $u_1 = \alpha\Omega_\infty/f$, and P_2 the point on E corresponding to $u_2 = \beta\Omega_\infty/\mathfrak{M}_n$. Recall that the classical Weierstrass functions can be written in terms of the x and y coordinates of the generalized Weierstrass equation for E by

$$\wp(z,\mathscr{L}) = x + \frac{a_1^2+4a_2}{12}, \quad \wp'(z,\mathscr{L}) = 2y + a_1x + a_3.$$

Hence we conclude from the above lemma that $\mathrm{Tr}_{\mathcal{R}_n/\mathscr{P}_n}(\mathscr{E}_1^*(\frac{\Omega_\infty}{g_n},\mathscr{L}))$ is given by

$$(**) \qquad 2\mathscr{E}_1^*(u_1,\mathscr{L}) + \frac{2y(P_1)+a_1x(P_1)+a_3}{x(P_1)-x(P_2)}.$$

Let v be any place of $\mathscr{P}_n$ above 2. Since g_n is odd, it suffices, in order to prove Theorem 76, to show that ord_v of the expression $(**)$ is ≥ 0. Now exactly the same argument as used to prove Theorem 72 shows that we always have

$$\mathrm{ord}_v\,(2\mathscr{E}_1^*(u_1,\mathscr{L})) \geq 0.$$

Moreover, the fact that E has good reduction at v, and that $(f,2) = (\mathfrak{M}_n,2) = 1$ shows again that we have

$$\mathrm{ord}_v(x(P_1)) \geq 0,\ \mathrm{ord}_v(y(P_1)) \geq 0,\ \mathrm{ord}_v(x(P_2)) \geq 0.$$

Hence, to complete the proof of Theorem 76, it suffices to prove

Lemma 83. $\mathrm{ord}_v\,(x(P_1)-x(P_2)) = 0$.

Proof. Suppose, on the contrary, that $\mathrm{ord}_v\,(x(P_1)-x(P_2)) > 0$. Let $\widetilde{E}$ denote the reduction of E modulo v. Then, under reduction modulo v, we would have $\widetilde{x(P_1)} = \widetilde{x(P_2)}$. But, by the explicit group law on $\widetilde{E}$, this last equation implies that $\widetilde{P_1} = \pm\widetilde{P_2}$. Hence either $P_1 - P_2$ or $P_1 + P_2$ must lie on the formal group of E at v, and so they would have to be 2-power torsion. But this is clearly impossible since $(f,\mathfrak{M}_n) = 1$ and $(f,2) = (\mathfrak{M}_n,2) = 1$. □

On the 2-part of the Conjecture of Birch and Swinnerton-Dyer

We assume in this section that our elliptic curve E is defined over $\mathbb{Q}$, has good reduction at 2, and complex multiplication by the ring of integers $\mathcal{O}_K$ of K. As $C(E) = |d_K|N\mathfrak{f}$, we automatically have $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$. For reasons which will become clear below, we shall also assume that $K \neq \mathbb{Q}(\sqrt{-3})$. Thus K must be one of the fields $K = \mathbb{Q}(\sqrt{-q})$, with $q = 7, 11, 19, 43, 67, 163$. Our goal now is to use our theorem asserting that, for all $n \geq 1$, we have

$$\sum_{M \in \mathscr{D}_n} \frac{L_{S_n}(\overline{\psi}_M, 1)}{\Omega_\infty} = 2^n\Lambda_n,$$

with $ord_v(\Lambda_n) \geq 0$ for all primes v above 2, to prove various weak forms of the 2-part of Birch-Swinnerton-Dyer conjecture for twists of E.

We will work with a subset of the set of quadratic twists, which we will call admissible twists of E, and which we will denote by $Ad(E)$. By definition, $N \in Ad(E)$ if N is a square free element of $\mathbb{Z}$ satisfying the following conditions:

(i) $(N, C(E)) = 1$;
(ii) $w_{E^{(N)}} = +1$;
(iii) N can be written in $\mathcal{O}_K$ as $N = \pi_1 \cdots \pi_n$, where $n \geq 1$ and the π_i are distinct prime elements of $\mathcal{O}_K$ satisfying $\pi_i \equiv 1 \mod 4$ $(1 \leq i \leq n)$.

We make the following remarks. Under our assumptions, it is easily seen that the conductor $C(E)$ is always the square of an integer in $\mathbb{Z}$. Hence to achieve (ii) we take $N > 0$ and $N \equiv 1 \mod 4$ if $w_E = +1$, and $N < 0$ with $|N| \equiv 3 \mod 4$ if $w_E = -1$. It turns out that (iii) is far more restrictive. Of course if $\pi_i\mathcal{O}_K = p_i\mathcal{O}_K$ for a rational p_i, we can choose $\pi_i = \pm p_i$ so that $\pi_i \equiv 1 \mod 4$. But if $\pi_i\bar{\pi}_i = p_i$, then we must necessarily have $p_i \equiv 1 \mod 4$. But this is not in general sufficient, and so we are led to the following definition.

Definition 84. A prime p with $p \equiv 1 \mod 4$ and p split in K is said to be a special split prime if we can write $p = \pi\bar{\pi}$ with $\pi \in \mathcal{O}_K$ satisfying $\pi \equiv 1 \mod 4$.

We leave the following lemmas as an easy exercise.

Lemma 85. *Let p be a prime $\equiv 1 \mod 4$ which splits in K, say $p = \pi\bar{\pi}$ in $\mathcal{O}_K$. Then (i) if $K = \mathbb{Q}(\sqrt{-7})$, all such p are special, and (ii) if $K = \mathbb{Q}(\sqrt{-q})$, with $q = 11, 19, 43, 67, 163$, then p is special if and only if $\pi + \bar{\pi} \equiv 2 \mod 4$.*

We note that, by Lemma 39, if p is a special spit prime of K with p dividing N and $(N, C(E)) = 1$, then the Tamagawa factor $c_p(E^{(N)}) = 4$, because t_p is equal to $\pm(\pi + \bar{\pi})$. This is the reason why special split primes play an important role in Tian's induction argument for Heegner points, which is discussed in the last part of these notes.

Example 86. Take $K = \mathbb{Q}(\sqrt{-11})$, $p \equiv 1 \mod 4$ and $p \equiv 1, 3, 4, 5, 9 \mod 11$. Then the special split primes < 1000 for K are

$$53, 257, 269, 397, 401, 421, 617, 757, 773, 929.$$

Here is another way of constructing special split primes.

Lemma 87. *Assume that $(p,C(E))=1$ and that p splits completely in $K(E[4])$. Then p is a special split prime for K. In particular, there is always a positive density of special split primes for K.*

Proof. Assume $(p,C(E))=1$ and that p splits completely in $K(E[4])$. Then $p\equiv 1 \mod 4$ because $\mu_4\subset K(E[4])$. Also $p\mathcal{O}=v\bar{v}$. Take $\pi=\psi(v)$, so that $\bar{\pi}=\psi(\bar{v})$ because E is defined over $\mathbb{Q}$. Now v is unramified in $K(E[4])$ because E has good reduction at v, and the Frobenius automorphism of v, which we denote by Frob_v, acts on $E[4]$ by multiplication by $\psi(v)$. But $\mathrm{Frob}_v=\mathrm{Frob}_{\bar{v}}=1$ because p splits completely in $K(E[4])$, and we conclude that $\pi\equiv\bar{\pi}\equiv 1 \mod 4$, as required. □

The following remark on Euler factors is crucial for the induction arguments which follow. Suppose, as earlier, that we have $n\geq 1$ elements $\pi_1\cdots\pi_n$ satisfying the conditions 2, and put $\mathfrak{M}_n=\pi_1\cdots\pi_n$. If π denotes one of these elements, put $v_\pi=\pi\mathcal{O}_K$. Then, if $M\in\mathscr{D}_n$, and v_π divides $\mathfrak{M}_n/M$, then

$$1-\frac{\overline{\psi}_M(v_\pi)}{Nv_\pi}=\frac{\psi_M(v_\pi)-1}{\psi_M(v_\pi)}$$

because $Nv_\pi=\psi_M(v_\pi)\overline{\psi_M(v_\pi)}$. Also $\psi_M(v_\pi)=\pm\pi$ because $K\neq\mathbb{Q}(\sqrt{-3}),\mathbb{Q}(\sqrt{-1})$. Hence

$$\mathrm{ord}_2\left(1-\frac{\overline{\psi}_M(v_\pi)}{Nv_\pi}\right)\geq 1,$$

and

$$\mathrm{ord}_2\left(1-\frac{\overline{\psi}_M(v_\pi)}{Nv_\pi}\right)\geq 2 \quad \text{if } \psi_M(v_\pi)=\pi.$$

Note also that

$$\frac{L_{S_n}(\overline{\psi}_M,1)}{\Omega_\infty}=\frac{L(\overline{\psi}_M,1)}{\Omega_\infty}\times\prod_{\pi|\frac{\mathfrak{M}_n}{M}}\left(1-\frac{\overline{\psi}_M(v_\pi)}{N_{v_\pi}}\right).$$

We shall also make use of the following notation. If $N\in Ad(E)$, let $n(N)$ denote the number of prime factors of N in $\mathcal{O}_K$, and $k(N)$ number of prime factors of N in $\mathbb{Z}$. We also put $\Omega_N=\Omega_\infty/\sqrt{|N|}$.

Suppose first that $ord_2(L(E,1)/\Omega_\infty)=-1$. Using the calculation of $c_p(E^{(N)})$, for p dividing N, given earlier, it is not difficult to see that the 2-part of the conjecture of Birch and Swinnerton-Dyer then predicts that, provided $L(E^{(N)},1)\neq 0$, we have

$$\mathrm{ord}_2\left(\frac{L(E^{(N)},1)}{\Omega_N}\right)=n(N)-1+\mathrm{ord}_2\left(\sharp(Ш(E))\right). \tag{3}$$

Theorem 88. *Assume that E has good reduction at 2, and that $ord_2(L(E,1)/\Omega_\infty)=-1$. Then, for all $N\in Ad(E)$, we have*

$$\mathrm{ord}_2\left(\frac{L(E^{(N)},1)}{\Omega_N}\right)\geq n(N)-1.$$

Proof. Put $R=\pi_1\cdots\pi_r$, with $1\leq r\leq n(N)$. We prove by induction on r that

$$\mathrm{ord}_2\left(\frac{L(\overline{\psi}_R,1)}{\Omega_\infty}\right)\geq r-1. \tag{$*$}$$

This will give the theorem when $r=n(N)$. Let $\mathscr{D}(R)$ be the set of all divisors of R given by products of subsets of $\{\pi_1,\ldots,\pi_r\}$. Then

$$\sum_{M\in\mathscr{D}(R)}\frac{L_{S_R}(\overline{\psi}_M,1)}{\Omega_\infty}=2^r\Lambda_r, \tag{$**$}$$

where $\mathrm{ord}_v(\Lambda_r)\geq 0$ for all places v above 2. Now $(*)$ is valid for $r=0$, and, by induction, we assume it is true for all $r'<r$, where now $r\geq 1$. Hence, for $M\neq R$, we have

$$\mathrm{ord}_2\left(\frac{L(\overline{\psi}_M,1)}{\Omega_\infty}\right)\geq r(M)-1.$$

But, as remarked earlier, we have

$$\mathrm{ord}_2\left(\prod_{v|\frac{R}{M}}\left(1-\frac{\psi_M(v)}{N_v}\right)\right)\geq r\left(\frac{R}{M}\right).$$

Hence all terms in $(**)$ on the left hand side have 2-order at least $r(R)-1$, except when $M=R$. The right hand side has 2-order at least $r(R)$, and so we get $(*)$ for R. This completes the proof. □

We remark that Liang's computations show that this theorem is in general best possible, e.g. when $E=X_0(49)$, $N=29=\pi_1\pi_2$ in $\mathcal{O}_K$. Then

$$\frac{L(E^{(N)},1)}{\Omega_N}=2.$$

However, we show next that the following stronger result holds when one imposes additional conditions on the prime factors of N.

Theorem 89. *Assume that E has good reduction at 2, and that $\mathrm{ord}_2(L(E,1)/\Omega_\infty)=-1$. Let $N=p_1\cdots p_k$ be a product of $k\geq 1$ distinct primes which split completely in $\mathbb{Q}(E[4])$. Then*

$$\mathrm{ord}_2\left(\frac{L(E^{(N)},1)}{\Omega_N}\right)\geq 2k.$$

Proof. Note first that it is easy to see that $K=\mathbb{Q}(E[2])=\mathbb{Q}(\sqrt{-7})$. Hence all of $p_1,\ldots,p_k$ split in K. Moreover, for every v of K dividing N, we have $\psi(v)\equiv 1 \mod 4$ because every p_i split completely in $\mathbb{Q}(E[4])$. Hence, if $R=\pi_1\cdots\pi_r$ with $r\geq 1$, we have

$$\mathrm{ord}_2\left(\frac{L_{S_R}(\overline{\psi},1)}{\Omega_\infty}\right)\geq 2r-1\geq r.$$

The induction argument then proceeds as before. □

Remark. A comparison of the above result with the prediction of the 2-part of the conjecture of Birch and Swinnerton-Dyer given by (3) shows that, provided $L(E^{(N)},1)\neq 0$, we must have $Ш(E^{(N)})(2)\neq 0$, under the hypotheses of this last theorem. Then, in fact (3), would even predict the stronger assertion that

$$\mathrm{ord}_2\left(\frac{L(E^{(N)},1)}{\Omega_N}\right)\geq 2k+1.$$

We note also that it seems that $E=X_0(49)$ and its isogenous curves (there are 4 curves in the isogeny class over $\mathbb{Q}$ of $X_0(49)$) are the only elliptic curves over $\mathbb{Q}$, with good reduction at 2, having complex multiplication by the maximal order $\mathcal{O}_K$ of K, and with $\mathrm{ord}_2(\frac{L(E,1)}{\Omega_\infty})=-1$. For $E=X_0(49)$, the primes $p<1000$ which split completely in $\mathbb{Q}(E[4])$ are given by

$$53,113,149,193,197,277,317,373,421,449,457,541,557,$$
$$809,821,953.$$

Suppose finally that $\mathrm{ord}_2(\frac{L(E,1)}{\Omega_\infty})\geq 0$. The induction method then leads to the following result by entirely similar arguments to those discussed above. We omit the details of the proof.

Theorem 90. *Assume that E has good reduction at 2, and that $\mathrm{ord}_2(\frac{L(E,1)}{\Omega_\infty})\geq 0$. Then, for all $N\in Ad(E)$, we have*

$$\mathrm{ord}_2\left(\frac{L(E^{(N)},1)}{\Omega_N}\right)\geq n(N),$$

where $n(N)$ is the number of prime factors of N in $\mathcal{O}_K$.

Tian's Argument for $E=X_0(49)$

The general question posed by Ye Tian's work on the congruent number elliptic $y^2=x^3-x$ is the following. Let E be any elliptic curve over $\mathbb{Q}$. If N is a square free integer, we write as usual $E^{(N)}$ for the twist of E by $\mathbb{Q}(\sqrt{N})/\mathbb{Q}$.

General Problem. Find a large (in a sense to be made precise) explicit infinite family $\mathcal{J}(E)$ of square free integers N with $(N,C(E))=1$ such that $L(E^{(N)},s)$ has a simple zero at $s=1$ for all $N\in\mathcal{J}(E)$.

Needless to say, the natural largest choice of $\mathcal{J}(E)$ would be the set of all N such that $\mathcal{S}el_2(E^{(N)})/\mathrm{Im}(E^{(N)}(\mathbb{Q})_{tors})$ has order 2.

In the rest of these lectures I want to describe ongoing joint work with Yongxiong Li, Ye Tian, and Shuai Zhai which provides an answer to this problem for the curve $E=X_0(49)$, whose equation, we recall, is given by

$$y^2+xy=x^3-x^2-2x-1, \tag{4}$$

and which has complex multiplication by the ring of integers of $K=\mathbb{Q}(\sqrt{-7})$. For this curve, we have

$$\mathbb{Q}(E[2])=\mathbb{Q}(\sqrt{-7}),\quad \mathbb{Q}(E[4])=\mathbb{Q}(\mu_4,\sqrt[4]{-7}).$$

We shall sketch the proof of the following theorem. The full details of the proof, as well as some generalizations, will be appearing in [2].

Theorem 91. *Let $E=X_0(49)$, and let $N=p_0p_1\cdots p_k$ be a product of distinct primes satisfying (i) $p_0\equiv 3 \mod 4$, $p_0\neq 7$, and p_0 is a quadratic non-residue modulo 7, (ii) $p_1,\ldots,p_k$ split completely in $\mathbb{Q}(E[4])$, and (iii) the ideal class group C_N of the field $F_N=\mathbb{Q}(\sqrt{-N})$ has no element of order 4. Then $L(E^{(-N)},s)$ has a simple zero at $s=1$, $E^{(-N)}(\mathbb{Q})$ has rank 1, and $Ш(E^{(-N)})$ is finite of odd order.*

We remark that, for N satisfying the hypotheses of the above theorem, we have $w_{E^{(-N)}}=-1$ because $N\equiv 3 \mod 4$. Note also that once we have shown that $L(E^{(-N)},s)$ has a simple zero at $s=1$, Kolyvagin's theorem implies immediately that $E^{(-N)}(\mathbb{Q})$ has rank 1 and $Ш(E^{(-N)})$ is finite. However, one needs an additional argument by classical 2-descent theory, to show that the 2-primary subgroup of $Ш(E^{(-N)})$ is zero for such N (see [2]).

The curve $X_0(49)$ has genus 1 and is defined over $\mathbb{Q}$. It has precisely two rational cusps, namely $[\infty]$ and $[0]$. We make the cusp $[\infty]$ the zero element for the group law on $X_0(49)$. It is then well known that there is an isomorphism of elliptic curves $f:X_0(49)\to E$, where E is defined by (4), which maps $[0]$ to the point $(2,-1)$. We now recall the definition of Heegner points on $X_0(49)$. From the moduli point of view, the non-cuspidal points of $X_0(49)$ correspond to isogenies $\{E_1\xrightarrow{\varphi}E_2\}$, where E_1 and E_2 are elliptic curves, and the degree of φ is 49. As Heegner [8] was the first to observe and exploit (for other modular curves), the classical theory of complex multiplication provides us with the following supply of points on $X_0(49)$. Let D be any positive square free integer with $D\equiv 3 \mod 4$. Define

$$K_D=\mathbb{Q}(\sqrt{-D}),$$

and let A_D be the ring of integers of K_D. Assume now that the following condition is valid for K_D:

Birch's Heegner condition The prime 7 splits in K_D.

Let $\mathfrak{a}=\wp_7^2$, where $\wp_7$ is one of the two primes of K_D above 7. Then we have a natural isogeny $\mathbb{C}/A_D\to\mathbb{C}/A_D\mathfrak{a}^{-1}$ of degree 49. We define $w_D=[\{\mathbb{C}/A_D\to\mathbb{C}/A_D\mathfrak{a}^{-1}\}]$ to be the corresponding point on $X_0(49)$. It is defined over the Hilbert class field of K_D, which we denote by $\mathcal{H}_D$ in what follows. We then define the Heegner point u_D on $X_0(49)$ by

Definition 92. $u_D=\mathrm{Tr}_{\mathcal{H}_D/K_D}(w_D)$.

Of course, the crucial question now is to decide what arithmetic conditions on D will guarantee that u_D is of infinite order, and this is where Tian's beautiful new idea enters.

From now on, we write $\mathfrak{M}(E)$ for the set of all square free positive integers N of the form $N=p_0p_1\cdots p_k$, where (i) $p_0\neq 7$ is a prime which is inert in $\mathbb{Q}(\sqrt{-7})$, and $p_0\equiv 3 \mod 4$, and (ii) $p_1,\ldots,p_k$ are primes which all split completely in $\mathbb{Q}(E[4])=\mathbb{Q}(\mu_4,\sqrt[4]{-7})$. When it is demanded by clarity, we will write $k(N)$ instead of simply k. Our goal now

is to use Tian's induction method to prove the following unconditional result. We recall that $E(K_N)^-$ denotes the subgroup of $E(K_N)$ consisting of the points on which the non-trivial element of $\mathrm{Gal}(K_N/\mathbb{Q})$ acts like -1, and that it can be identified naturally with $E^{(N)}(\mathbb{Q})$.

Theorem 93. *Assume that $N \in \mathfrak{N}(E)$. If $k(N) = 0$, we have $2u_N$ is in $E(K_N)^-$. If $k(N) \geq 1$, we have*

$$u_N \in 2^{k(N)-1}E(K_N)^- + E(K_N)_{tors}.$$

We now begin the proof of this theorem. Let $\mathcal{H}_N$ as before denote the Hilbert class field of K_N, so that class field theory provides an isomorphism

$$j : \mathrm{Gal}(\mathcal{H}_N/K_N) \xrightarrow{\sim} C_N.$$

The fixed field of $j^{-1}(2C_N)$ is called the genus class field of K_N, and we denote it by $\mathscr{J}_N$. Explicitly, we have

$$\mathscr{J}_N = K_N(\sqrt{-p_0}, \sqrt{p_1}, \ldots, \sqrt{p_k}).$$

Define $\mathscr{D}(N)$ to be the set of all positive divisors M of N which are divisible by p_0. Thus, for each $M \in \mathscr{D}(N)$, we have

$$K_N(\sqrt{-M}) \subset \mathcal{H}_N.$$

For $M \in \mathscr{D}(N)$ with $M \neq N$, let $\mathcal{X}_M$ denote the quadratic character of K_N defining the abelian extension $K_N(\sqrt{-M})/K_N$; if $M = N$, $\mathcal{X}_M$ will denote the trivial character. We then define the "non-primitive" Heegner point $u_{N,M}$ by

Definition 94. $u_{N,M} = \sum_{\sigma \in G} \mathcal{X}_M(\sigma)\sigma(w_N)$.

Here $G = \mathrm{Gal}(\mathcal{H}_N/K_N)$. Note that $u_{N,N} = u_N$. Clearly, $u_{N,M} \in E(K_N(\sqrt{-M}))$. However, it is not difficult to see that it is fixed by the Galois group of $K_M(\sqrt{-N})/K_M$, and hence we have $u_{N,M} \in E(K_M)$. We now use the following deep and beautiful theorem of Gross and Zagier [7]. Let $\widehat{h} : E(\overline{\mathbb{Q}}) \to \mathbb{R}$ be the absolute canonical Neron-Tate height on E. Let $L(E/K_N, \mathcal{X}_M, s)$ be the complex L-series of E/K_N, twisted by the abelian character $\mathcal{X}_M$ of K_N.

Theorem 95. *For each $M \in \mathscr{D}(N)$, we have*

$$L'(E/K_N, \mathcal{X}_M, 1) = 16\lambda(E)N^{-1/2}\widehat{h}(u_{N,M}),$$

where $\lambda(E)$ denotes the Petersson inner product with itself of the cusp form of weight 2 for $\Gamma_0(49)$ corresponding to E.

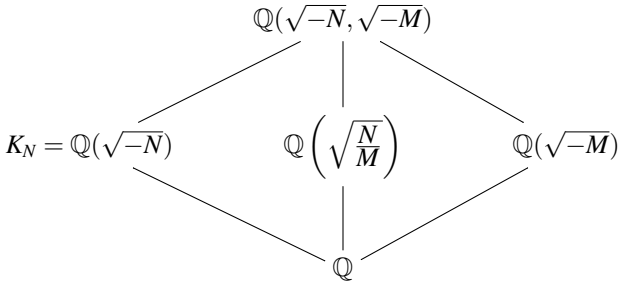
For any integer $R \neq 0$, recall that $L(E^{(R)}, s)$ denotes the complex L-series of $E^{(R)}$ over $\mathbb{Q}$.

Lemma 96. *For each $M \in \mathscr{D}(N)$, we have*

$$L(E/K_N, \mathcal{X}_M, s) = L(E^{(-M)}, s)L(E^{(\frac{N}{M})}, s).$$

Remark. Note that $w_{E^{(N/M)}} = +1$, and we studied the 2-part of the Birch-Swinnerton-Dyer conjecture for its value at $s = 1$ earlier in our lectures!

Proof. For $M = N, \mathcal{X}_M$ is the trivial character, and this is just the usual factorization of L-series. Hence we can assume that $M \neq N$. Then we have



Let Δ be the Galois group of this quartic extension of $\mathbb{Q}$. Let ϕ_M denote the Artin character of dimension 2 obtained by inducing $\mathcal{X}_M$ to Δ. By the functorial properties of L-functions under induction, we have

$$L(E/K_N, \mathcal{X}_M, s) = L(E/\mathbb{Q}, \phi_M, s).$$

But $\phi_M = \phi_1 + \phi_2$, where ϕ_1 is the non-trivial character of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-M})/\mathbb{Q})$, and ϕ_2 is the non-trivial character of $\mathrm{Gal}(\mathbb{Q}(\sqrt{N/M})/\mathbb{Q})$. Hence

$$L(E/\mathbb{Q}, \phi_M, s) = L(E, \phi_1, s)L(E, \phi_2, s).$$

But $L(E, \phi_1, s) = L(E^{(-M)}, s)$ and $L(E, \phi_2, s) = L(E^{(\frac{N}{M})}, s)$, and the lemma is proven. □

Combining the above lemma with the theorems of Gross-Zagier and Kolyvagin, we obtain the following key corollary needed in Tian's induction argument.

Corollary 97. *Let M be any element of $\mathscr{D}(N)$. If $u_{N,M}$ has infinite order, then u_M has infinite order, $E(K_M)$ has rank 1, and $L(E^{(N/M)}, 1) \neq 0$.*

Proof. Since $u_{N,M}$ has infinite order, $L(E/F_N, \mathcal{X}_M, s)$ has a simple zero at $s = 1$ by Theorem 95. Hence, by the above lemma, $L(E^{(-M)}, s)$ has a simple zero at $s = 1$, and $L(E^{(N/M)}, 1) \neq 0$. But applying Theorem 95 again, we conclude that u_M must then be of infinite order, and so, by Kolyvagin's theorem, $E(K_M)$ has rank 1. □

For any square free integer R, let us define

$$\Omega_R = \Omega_\infty/\sqrt{|R|},\ L^{(alg)}(E^{(R)}, 1) = L(E^{(R)}, 1)/\Omega_R,$$

where Ω_∞ is the usual least positive real period of the Néron differential on E. In particular, we know that

$$L^{(alg)}(E, 1) = \frac{1}{2}.$$

Of course, it may well happen that the Heegner point $u_{N,M}$ is torsion for some $M \in \mathscr{D}(N)$. However, if it is not, we immediately obtain from the above deep results the following theorem, which lies at the heart of Tian's method.

Theorem 98. *Assume $M \in \mathscr{D}(N)$, and that $u_{N,M}$ is of infinite order. Then $E(K_M)$ has rank 1, and*

$$\frac{\widehat{h}(u_{N,M})}{\widehat{h}(u_M)} = \frac{L^{(alg)}(E^{(\frac{N}{M})},1)}{L^{(alg)}(E^{(1)},1)}.$$

On the other hand, noting that N/M is a product of distinct primes which split completely in $\mathbb{Q}(E[4])$, and applying the weak form of the 2-Birch-Swinnerton-Dyer conjecture given by Theorem 89, we also have

Theorem 99. *If $L(E^{(N/M)},1) \neq 0$, then*

$$\mathrm{ord}_2(L^{(alg)}(E^{(N/M)},1)) \geq k(N) - k(M).$$

Combining the two previous theorems, we now establish the following result.

Corollary 100. *Assume $M \in \mathscr{D}(N)$. If $u_{N,M}$ is of infinite order, and $u_M \in 2^{k(M)-1}E(K_M)^- + E(K_M)_{tors}$ (when $k(M) = 0$ this means that $2u_M \in E(K_M)^-$), then $u_{N,M} \in 2^{k(N)}E(K_M)^- + E(K_M)_{tors}$.*

Proof. Since $u_{N,M}$ is of infinite order, $E(K_M) \otimes \mathbb{Q}$ has dimension 1, and so, using the same symbols to denote the classes of both Heegner points in this vector space, we have

$$u_{N,M} = \alpha u_M$$

for some $\alpha \in \mathbb{Q}^\times$. Hence

$$\frac{\widehat{h}(u_{N,M})}{\widehat{h}(u_M)} = \alpha^2$$

by the quadraticity of the Néron-Tate height. Thus, by Theorem 98,

$$2\,\mathrm{ord}_2(\alpha) = \mathrm{ord}_2\left(\frac{L^{(alg)}(E^{(N/M)},1)}{L^{(alg)}(E,1)}\right).$$

Moreover, by Theorem 99, we have $\mathrm{ord}_2(L^{(alg)}(E^{(N/M)},1)) \geq 2k(N/M)$ and $L^{(alg)}(E,1) = \frac{1}{2}$. Hence $2\,\mathrm{ord}_2(\alpha) \geq 2k(N/M)+1$, and so $\mathrm{ord}_2(\alpha) \geq k(N/M)+1$. Thus we see that $u_{N,M} \in 2^{k(N)}E(K_M)^- + E(K_M)_{tors}$, as required. □

The reader is referred to [2] for the proof of the following averaging result by the theory of complex multiplication.

Proposition 101. *Assume $k(N) \geq 1$. For each $M \in \mathscr{D}(N)$, $u_{N,M} \in E(K_M)^-$, and*

$$\sum_{M \in \mathscr{D}(N)} u_{N,M} = 2^{k(N)} v_N,$$

where $v_N = \mathrm{Tr}_{\mathcal{H}_N/\mathscr{J}_N}(w_N)$. Moreover, we have

$$\bar{v}_N + v_N = \sharp(2C_N)[0]. \tag{5}$$

Assuming this result, we will now complete the proof of Theorem 93. We use induction on $k(N)$. We first claim that the result is true when $k(N) = 1$. Indeed, when $k(N) = 1$, we have $\mathscr{J}_N = K_N(\sqrt{-p_0})$. In this case, we clearly have

$$u_N = v_N + v_N^\tau, \;\; u_{N,p_0} = v_N - v_N^\tau,$$

where τ denotes the non-trivial element of $Gal(\mathscr{J}_N/K_N)$. In particular, it follows that

$$u_N + \bar{u}_N = v_N + \bar{v}_N + (v_N + \bar{v}_N)^\tau,$$

and the expression on the right is then zero because of (5). This establishes Theorem 93 for $k(N) = 1$. Now assume that $k(N) > 1$. Our inductive hypothesis is then that, for all $M \neq N$ with $k(M) \geq 1$, we have

$$u_M \in 2^{k(M)-1}E(K_M)^- + E(K_N)_{tors}.$$

It follows from the corollary above that either $u_{N,M}$ is a torsion or

$$u_{N,M} \in 2^{k(N)}E(K_M)^- + E(K_M)_{tors}$$

for all $M \in \mathscr{D}(N)$ with $M \neq N$. Hence we conclude from the averaging lemma that

$$u_N \in 2^{k(N)}E(\mathscr{J}_N) + E(\mathscr{J}_N)_{tors}.$$

We must deduce from this that

$$u_N \in 2^{k(N)-1}E(K_N)^- + E(K_N)_{tors}.$$

Lemma 102. $E(\mathscr{J}_N)[2^\infty] \subset E[2](\mathbb{Q})$.

Proof. Since E has good reduction at 2, we have seen earlier that ramification must occur at 2 in the extension $\mathbb{Q}(P)$, where P is any point of order 4 on E, since the formal groups of E at the primes of K above 2 are Lubin-Tate groups. But the extension $\mathscr{J}_N/\mathbb{Q}$ is unramified at 2 because 2 is not ramified in K_N and $\mathscr{J}_N/K_N$ is unramified. Thus the lemma is clear, on noting that $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{-7}) \not\subset \mathscr{J}_N$. □

Since the prime to 2 part of $E(\mathscr{J}_N)_{tors}$ is 2-divisible, we conclude from the above and this lemma that

$$u_N \in 2^{k(N)}E(\mathscr{J}_N) + E[2](\mathbb{Q}).$$

Hence $2u_N \in 2^{k(N)+1}E(\mathscr{J}_N)$. Now we have the commutative diagram

$$\begin{array}{ccccc}
0 & \to & E(\mathscr{J}_N)/2^{k(N)+1}E(\mathscr{J}_N) & \longrightarrow & H^1(\mathscr{J}_N, E[2^{k(N)+1}]) \\
 & & \uparrow{\scriptstyle \alpha} & & \uparrow \\
0 & \to & E(K_N)/2^{k(N)+1}E(K_N) & \longrightarrow & H^1(K_N, E[2^{k(N)+1}]) \\
 & & \uparrow & & \uparrow \\
0 & \longrightarrow & \mathrm{Ker}\,\alpha & \longrightarrow & H^1(Gal(\mathscr{J}_N/K_N), E(\mathscr{J}_N)[2]) \\
 & & & & \uparrow \\
 & & & & 0
\end{array}$$

The kernel of the right vertical map is killed by 2, whence $\mathrm{Ker}\,\alpha$ is also killed by 2. But $2u_N \in \mathrm{Ker}\,\alpha$. Hence $4u_N \in 2^{k(N)+1}E(K_N)$. It follows easily that $u_N = 2^{k(N)-1}r_N$ modulo $E[2](\mathbb{Q})$, where $r_N \in E(K_N)$ is given explicitly by

$$r_N = 2v_N - \sum_{M\in\mathscr{D}(N),M\neq N} 2z_M + t_1,$$

with $t_1 \in E[2](\mathbb{Q})$ and $z_M \in E(K_M)^-$. We conclude that

$$\bar{r}_N + r_N = 2(\bar{v}_N + v_N).$$

Hence $\bar{r}_N + r_N = 0$ by (5), and the proof of Theorem 93 is now complete.

We can now prove Theorem 91. We have shown that if $N = p_0p_1\cdots p_{k(N)}$ belongs to the set $\mathfrak{M}(E)$ and has $k(N) \geq 1$, then the Heegner point u_N satisfies

$$u_N \in 2^{k(N)-1}E(K_N)^- + E(K_N)_{tors}.$$

We want to show that u_N is of infinite order if we assume, in addition, that the ideal class group C_N of K_N has no element of order 4, or equivalently that the group $2C_N$ has odd order. We now give the detailed proof of this assertion when $k(N) \geq 1$. We omit the details of a very similar argument for the case $k(N) = 0$.

We know from the proof of Theorem 93 given above that, for all $M \in \mathscr{D}(N)$, excluding $M = N$, we have

$$(*) \qquad u_{N,M} \in 2^{k(N)}E(K_M)^- + E(K_M)_{tors} \ (M \neq N).$$

Let us assume now that we also have

$$(**) \qquad u_N \in 2^{k(N)}E(K_N)^- + E(K_N)_{tors},$$

and we will show this leads to a contradiction when $2C_N$ has odd order. This will certainly prove that u_N has infinite order. Recall that we have the identity given by the averaging lemma, namely

$$\sum_{M\in\mathscr{D}(N)} u_{N,M} = 2^{k(N)}v_N$$

where $v_N = \mathrm{Tr}_{\mathcal{H}_n/\mathscr{J}_n}(w_N)$, and $\mathscr{J}_N = K_N(\sqrt{-p_0}, \sqrt{p_1}, \ldots, \sqrt{p_{k(N)}})$. In view of $(*)$ and $(**)$, for each $M \in \mathscr{D}(N)$, we can write

$$u_{N,M} = 2^{k(N)}z_M + t_M,$$

for some $z_M \in E(K_M)^-$ and some torsion element t_M in $E(K_M)$. Since the only torsion in $E(\mathbb{Q})$ is 2-torsion, it follows that all torsion elements in $E(K_M)$ of order prime to 2 must have trace zero to $E(\mathbb{Q})$, and thus lie in $E(K_M)^-$. Such torsion in $E(K_M)$ of order prime to 2 is also clearly 2-divisible. Hence we can suppose in the above equation that t_M belongs to $E(K_M)[2^\infty]$. It follows from the averaging lemma that

$$2^{k(N)}\left(v_N - \sum_{M\in\mathscr{D}(N)} z_M\right) \in E(\mathscr{J}_M)[2^\infty].$$

But then

$$v_N - \sum_{M\in\mathscr{D}(N)} z_M \in E(\mathscr{J}_M)[2^\infty].$$

But we have already remarked that, by a ramification argument, we have $E(\mathscr{J}_M)[2^\infty] = E[2](\mathbb{Q})$. Hence

$$v_N - \sum_{M\in\mathscr{D}(N)} z_M \in E[2](\mathbb{Q}),$$

whence $\bar{v}_N + v_N = 0$ because all $z_M \in E(K_M)^-$. But, as we already used earlier (see (5)), the theory of complex multiplication shows that

$$v_N + \bar{v}_N = \sharp(2C_N)[0].$$

Since the cusp $[0]$ is a rational point of order 2, we get our desired contradiction when $\sharp(2C_N)$ is odd. This completes the proof of Theorem 91.

References

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

[2] J. Coates, Y. Li, Y. Tian, S. Zhai, *Quadratic twists of elliptic curves*, to appear.

[3] J. Coates, M. Kim, Z. Liang, C. Zhao, *On the 2-part of the Birch-Swinnerton-Dyer conjecture for elliptic curves with complex multiplication*, Munster J. of Math., to appear.

[4] R. Damerell, *L-functions of elliptic curves with complex multiplication II*, Acta Arithmetica **19** (1971), 311–317.

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

[6] C. Goldstein, N. Schappacher, *Series d'Eisenstein et fonctions L de courbes elliptiques a multiplication complexe*, Crelle **327** (1981), 184–218.

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

[8] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Zeitschrift **56** (1952), 227–253.

[9] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a class of Weil curves*, Izv. Akad. Nauk. SSSR **52** (1988), 522–540, 670–671, translation Math. USSR-Izv. **32** (1989), 523–541.

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

[11] J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

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

[13] Y. Tian, *Congruent numbers and Heegner points*, to appear.

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

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

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

[17] C. Zhao, *A criterion for elliptic curves with lowest 2-power in $L(1)$ (II)*, Proc. Cambridge Phil. Soc. **134** (2003), 407–420.

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