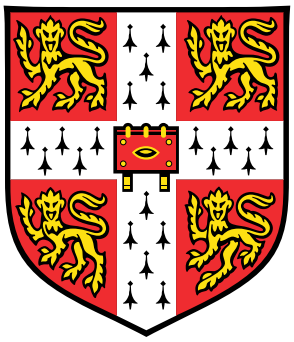
The conjecture of Birch and Swinnerton-Dyer



George Cătălin Ţurcaş

Department of Pure Mathematics and Statistics

University of Cambridge

This essay represents work done as part of the Part III Examination. The content was suggested and supervised by

Professor John H. Coates

St John's College April 2015

I would like to dedicate this essay to my loving grandparents Gheorghe and Florica.

Declaration

I declare that this essay is work done as part of the Part III Examination. I have read and understood the Statement on Plagiarism for Part III and Graduate Courses issued by the Faculty of Mathematics, and have abided by it. This essay is the result of my own work, and except where explicitly stated otherwise, only includes material undertaken since the publication of the list of essay titles, and includes nothing which was performed in collaboration. No part of this essay has been submitted, or is concurrently being submitted, for any degree, diploma or similar qualification at any university or similar institution.

George Cătălin Ţurcaş
April 2015

Acknowledgements

I have my deepest gratitude to Professor John H. Coates for suggesting this interesting essay, providing most of the references and for dedicating his precious time to answer all my questions.

Abstract

This essay starts by first explaining, for elliptic curves defined over $\mathbb{Q}$, the statement of the conjecture of Birch and Swinnerton-Dyer. Alongside, it contains a discussion of some results that have been proved in the direction of the conjecture, such as the theorem of Kolyvagin-Gross-Zagier and the weak parity theorem of Tim and Vladimir Dokchitser.

The second, third and fourth part of the essay represent an account, with detailed proofs, of results about the cases of both week and strong Birch and Swinnerton-Dyer conjecture from the wonderful article by John Coates, Yongxiong Li, Ye Tian and Shuai Zhai [1].

Recently, working on the congruent number curve $E : y^2 = x^3 - x$, Ye Tian introduced a new method of attack for the following general problem.

Problem. Given an elliptic curve E defined over $\mathbb{Q}$, we would like to find a large explicit infinite family of square free integers M, coprime with the conductor $C(E)$, such that $L(E^{(M)}, s)$ has a simple zero at $s = 1$.

Tian [21], [22] succeeded in doing this for his particular choice of curve, and, inspired by his work, the authors carry out this full programme for the elliptic curve $A : y^2 + xy = x^3 - x^2 - 2x - 1$ in [1]. Mysteriously, this required them to prove a weak form of the 2-part of the Birch and Swinnerton-Dyer conjecture for an infinite family of quadratic twists of A, which is described at the end of the third section of this essay.

The last section combines results from all the previous ones to prove the highlight of this essay, an analogue of Tian's result for the elliptic curve $A : y^2 + xy = x^3 - x^2 - 2x - 1$, formulated in Theorem 47.

The autors of [1] belive that there should be analogues of this theorem for every elliptic curve E defined over $\mathbb{Q}$ and it is an important problem to formulate them precisely and then to prove them.

Table of contents

1. What is the Birch and Swinnerton-Dyer conjecture?

In the first part of this essay, I try to introduce the necessary notions for understanding the arithmetic invariants involved in the Birch and Swinnerton-Dyer conjecture. In addition, there will be a discussion, without proofs, about intermediary results and particular cases of this conjecture, which were already proved.

Theorem 1 (Mordell-Weil)**.** *If E is an elliptic curve over $\mathbb{Q}$, the Mordell-Weil group $E(\mathbb{Q})$ is finitely generated, i.e. $E(\mathbb{Q}) \simeq \mathbb{Z}^{g_E} \oplus E(\mathbb{Q})_{tor}$, where $g_E \geq 0$.*

The number of g_E copies of $\mathbb{Z}$ in the Mordell-Weil group $E(\mathbb{Q})$ is called the rank of the elliptic curve E.

This result was proved by Mordell 92 years ago. Soon after, Weil generalized it to abelian varieties over number fields. In practice, we can determine $E(\mathbb{Q})$ most of the times for a given numerical example, but there is no theoretical algorithm for calculating $E(\mathbb{Q})$ in finite time.

Example The curve $E : y^2 + xy = x^3 + x^2 - 696x + 6784$ discussed later as a numerical example to the Birch and Swinnerton-Dyer conjecture, has, according to [6], rank $g_E = 3$ and trivial $E(\mathbb{Q})_{tor}$. Also, the curve $A : y^2 + xy = x^3 - x^2 - 2x - 1$ has $A(\mathbb{Q}) = A(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z}$.

Given an integer $m > 1$, we can consider the multiplication by m isogeny applied to $E(\overline{\mathbb{Q}})$ to get the following exact sequence of modules equipped with the natural continuous action of the profinite group $G := Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

$$0 \longrightarrow E(\overline{\mathbb{Q}})[n] \longrightarrow E(\overline{\mathbb{Q}}) \xrightarrow{\times m} E(\overline{\mathbb{Q}}) \longrightarrow 0 \tag{1.1}$$

Galois cohomology of (1.1) yields the long exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(\mathbb{Q})[n] & \longrightarrow & E(\mathbb{Q}) & \xrightarrow{\times m} & E(\mathbb{Q}) \\ & & & \searrow & & & \\ & & H^1(G,E(\overline{\mathbb{Q}})[n]) & \longrightarrow & H^1(G,E(\overline{\mathbb{Q}})) & \xrightarrow{\times m} & H^1(G,E(\overline{\mathbb{Q}})) \end{array} \tag{1.2}$$

where $H^1(G,E(\overline{\mathbb{Q}}))$ is the first cohomology group of the G module $E(\overline{\mathbb{Q}})$.
From (1.2) we obtain the following short exact sequence

$$0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \longrightarrow H^1(G,E(\overline{\mathbb{Q}})[m]) \longrightarrow H^1(G,E(\overline{\mathbb{Q}}))[m] \longrightarrow 0 \tag{1.3}$$

where $H^1(G,E(\overline{\mathbb{Q}}))[m] = \{c \in H^1(G,E(\overline{\mathbb{Q}}))|m \cdot c = 0\}$.

1.1 The Selmer and Shafarevich-Tate Groups

The exact sequence (1.3) is not very helpful. In particular, we can't even derive from it that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite because the group $H^1(G,E(\overline{\mathbb{Q}})[m])$, in which it embeds, is infinite. The proof for my last assertion can be found, for example, in [7]. In order to get more information, we approach this sequence from a local point of view.

For any place v of $\mathbb{Q}$, the embedding of $\mathbb{Q}$ into the completion $\mathbb{Q}_v$ extends to an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}_v}$ and thus induces an inclusion

$$G_v := Gal(\overline{\mathbb{Q}_v}/\mathbb{Q}_v) \subset G = Gal(\overline{\mathbb{Q}}/\mathbb{Q}),$$

which leads to the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/mE(\mathbb{Q}) & \longrightarrow & H^1(G,E(\overline{\mathbb{Q}})[m]) & \longrightarrow & H^1(G,E(\overline{\mathbb{Q}}))[m] & \longrightarrow & 0 \\ & & \downarrow res_v & & \downarrow res_v & \searrow^{\gamma_v} & \downarrow res_v & & \\ 0 & \longrightarrow & E(\mathbb{Q}_v)/mE(\mathbb{Q}_v) & \longrightarrow & H^1(G_v,E(\overline{\mathbb{Q}})[m]) & \longrightarrow & H^1(G_v,E(\overline{\mathbb{Q}}))[m] & \longrightarrow & 0 \end{array} \tag{1.4}$$

where res_v denotes the restriction homomorphism induced by the inclusion $G_v \subset G$.
This diagram yields the definition of two very important groups.

Definition The Shafarevich-Tate group of E, denoted by $Ш(E)$, is the set of all cohomology classes $c \in H^1(G,E(\overline{\mathbb{Q}}))$ such that $res_v(c) = 0$ for all places v of $\mathbb{Q}$. In other words, $Ш(E) = \ker\left(H^1(G,E(\overline{\mathbb{Q}})) \to \bigoplus_v H^1(G_v,E(\overline{\mathbb{Q}}))\right)$.

Another good way to think about $Ш(E)$ is as the group of homogeneous spaces for E that possesses a $\mathbb{Q}_v$ rational point for every place v of $\mathbb{Q}$.

Definition The m- Selmer group of E, denoted by $S^{(m)}(E)$, is the set of all cohomology classes $c \in H^1(G, E(\overline{\mathbb{Q}})[m])$ such that $\gamma_v(c) = 0 \in H^1(G, E(\overline{\mathbb{Q}}))$ for all places v of $\mathbb{Q}$.

By making use of the snake lemma, we obtain an exact sequence

$$0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \longrightarrow S^{(m)}(E) \longrightarrow Ш(E)[m] \longrightarrow 0 \tag{1.5}$$

Theorem 2. *The group $S^{(m)}(E)$ is finite for all $m > 1$. [19]*

Remark The Selmer group can be defined in greater generality by considering an arbitrary nonzero isogeny $\phi : E \to E'$ instead of the multiplication by m. An analogous of Theorem 2, namely that $S^{(\phi)}(E)$ is finite can be proved. For more details, the reader should consult [19].

Notice that Theorem 2 and the short exact sequence (1.5) imply together that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite, which is the first part of the proof of Mordell-Weil theorem. Although there are many ingenious classical techniques for calculating $S^{(m)}(E)$ for small m, it is a subtle question even to calculate $S^{(2)}(E)$ in many cases.

The Shafarevich-Tate group is a very mysterious object at the moment. Only one general theoretical result is known about it. Let us denote by $Ш(E)_{div}$ the maximal divisible subgroup of $Ш(E)$.

Theorem 3 (Cassels-Tate)**.** *There is a canonical non-degenerate alternating bilinear form on $Ш(E)/Ш(E)_{div}$.*

Corollary 4. *The vector space $(Ш(E)/Ш(E)_{div})[p]$ has even dimension over $\mathbb{F}_p$.*

Corollary 5. *If $Ш(E)_{div}(p) = 0$, then the order of $Ш(E)(p)$ is a square.*

A trivial consequence of the above corollary is that if $Ш(E)$ is finite then its order is a square. This follows easily from the fact that no finite abelian group is divisible.

Making use of classical Galois cohomology, we can deduce another interesting property of $Ш(E)$, namely

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

for some integer $t_{E,p} \geq 0$ and a finite group M_p. Observe that $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible and since no finite group is divisible we can conclude that $Ш(E)(p)_{div} = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E,p}}$.

Conjecture 6. *The Shafarevich-Tate group* $Ш(E)$ *is finite.*

This conjecture is undoubtedly one of the most important unsolved problems in number theory at the moment. It has never been verified so far for any elliptic curve with rank $g_E \geq 2$. Once proved, it would, of course, imply that $Ш(E)(p)$ is finite and hence $t_{E,p} = 0$ for every prime number p.

It has been proved recently by Tim and Vladimir Dokchitser (see Theorem 15) that the parity of $t_{E,p}$ does not depend on the prime p. This result, combined with Corollary 5 gives rise to the following lemma.

Lemma 7. *Assume that* $S^{(2)}(E)/Im(E(\mathbb{Q})_{tor})$ *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.

This lemma will be used to establish the odd cardinality of the Tate-Shafarevich group of a family consisting of quadratic twists of the curve $A = X_0(49)$ in the last theorem, which is the central piece of this essay.

In support of Conjecture 6, we would like to prove that (ii) is impossible. By generalizing old work of Heegner, Ye Tian has recently introduced a new idea in the articles [21] and [22]. The method he suggests should provide new insight and eventually help us to prove this result for large families of elliptic curves.

It is believed that there are infinitely many primes p such that there exists some elliptic curve E over $\mathbb{Q}$ with $Ш(E)(p) \neq 0$, but this is still an open problem. The largest prime P for which this is known to occur is 1627. Calculations of Z. Liang and D. Wei show that for the elliptic curve $E : y^2 = x^3 - (7173305747)^2 x$ the order of $Ш(E)(1627)$ is 1627^2. [3]

1.2 L-Functions

Surprisingly, it seems that there is no way to attack the conjectures above without the use of L-functions. I will briefly recall the definitions and key fact about these. Let E be an elliptic curve over $\mathbb{Q}$ and let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.6}$$

be a global minimal Weierstrass equation for E and denote by $\triangle$ its discriminant. Such a global minimal equation always exists over $\mathbb{Q}$, because the ring $\mathbb{Z}$ is a Principal Ideal domain.

For each prime p, the reduction of (1.6) modulo p defines a curve $\widetilde{E}(p)$ over the finite field $\mathbb{F}_p$.

Definition The conductor $C(E)$ of E is defined by

$$C(E) = \prod_{p|\triangle} p^{f_p}.$$

For each prime p in the product, f_p is called the exponent of the conductor of E at p. It is an isogeny invariant which can be understood as a measurement of the badness of the reduction of E at p and, according to [20]

$$\begin{cases} f_p = 1 \text{ if } E \text{ has multiplicative reduction at } p \text{ (i.e. } \widetilde{E}(p) \text{ has a node)} \\ f_p = 2 + \delta_p \text{ if } E \text{ has additive reduction at } p \text{ (i.e. } \widetilde{E}(p) \text{ has a cusp)} \end{cases}$$

where δ_p is a certain "measure of wild ramification" which is zero unless $p = 2$ or 3 [13].

For each prime p, define A_p to be the number of points of $\widetilde{E}(p)$ over the field $\mathbb{F}_p$ and let $t_p = 1 + p - A_p$. Notice that A_p has to be one more than the number of solutions of the congruence

$$y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

because we have to include the point at infinity which is not visible on the affine piece.

If $p \nmid \triangle$, then E has good reduction at p and t_p represents the trace of the Frobenius, which by Hasse's theorem satisfies $|t_p| \leq 2\sqrt{p}$.

If $p|\triangle$, i.e. E has bad reduction at p, then $t_p = 1, -1, 0$ according as $\widetilde{E}(p)$ has a node with rational tangents, a node with tangents quadratic over $\mathbb{F}_p$ or a cusp.

One associates to E a complex $L-$ series, defined by the following Euler product

$$L(E,s) = \prod_{p|\triangle} \frac{1}{1 - t_p p^{-s}} \cdot \prod_{p\nmid\triangle} \frac{1}{1 - t_p p^{-s} + p^{1-2s}}.$$

Expanded out, this product is a Dirichlet series $L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}$ whose p-th coefficients for p prime are $a_p = t_p$. This series converges in the half plane $Re(s) > \frac{3}{2}$.

Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \middle| c \equiv 0 \pmod{N} \right\}$$

and let $\mathscr{H}$ be the upper half complex plane and let $q = e^{2\pi i\tau}$, where $\tau \in \mathscr{H}$.

Define

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

Theorem 8 (Wiles (...) et al)**.** *The holomorphic function $f_E(\tau)$ is a primitive cusp form of weight 2 for $\Gamma_0(C(E))$.*

This very deep theorem gives us new insight on $L(E,s)$. Note that this is essentially the Mellin transform of the modular form f_E. More precisely, if we set

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

then we have

$$\Lambda(E,s) = C(E)^{\frac{s}{2}}\int_0^\infty f_E(iy)y^s dy/y.$$

This integral representation for $L(E,s)$ gives the analytic continuation of $L(E,s)$ to the entire complex plane. The modular invariance of f_E translates into a functional equation for $L(E,s)$, given in the following corollary.

Corollary 9. *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 $w_E = \pm 1$.

Until Wiles and his collaborators proved the modularity theorem, this corollary was an unsolved special case of a vast conjecture about zeta functions attached to the cohomology of any dimension of any algebraic variety over any global field as formulated by Serre in [18] and by Deligne in an appendix to this article.

The term $w_E = \pm 1$, called the root number, can be computed as $w_E = \prod_p w_{E,p}$, where $w_{E,p}$ is called the local root number. It is well known that $w_{E,p} = 1$ if E has good reduction at p, hence $w_{E,p} = 1$ for all but finitely many primes p. It is also known that $w_{E,\infty} = -1$ and hence we may write

$$w_E = -\prod_{p|\triangle} w_{E,p}.$$

From the above functional equation, we can see immediately 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 theorem is of great importance. Define the modular curve $X_0(N)$ to be the compactification of the quotient of the upper half plane by $\Gamma_0(N)$, i.e.

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

where $\mathbb{P}^1(\mathbb{Q})$ denotes the projective line over $\mathbb{Q}$. As a compact Riemann surface, $X_0(N)$ has a unique structure of the set of complex points of a projective (hence complete) curve defined over $\mathbb{Q}$. We will also denote this curve by $X_0(N)$. An elliptic curve E for which there is a non-constant map $X_0(N) \to E$ for some integer N is called a modular elliptic curve. The following corollary tells us that all elliptic curves are modular.

Corollary 10. *There is a non-constant rational map defined over* $\mathbb{Q}$

$$\varphi : X_0(C(E)) \to E \tag{1.7}$$

with $\varphi([\infty]) = O$*, the origin of the group law on* E*.*

Theorem 11. *(Manin-Drinfeld) If* $\varphi : X_0(C(E)) \to E$ *is a modular parameterization as in* (1.7)*, then* $\varphi([0]) \in E(\mathbb{Q})$ *is a torsion point.*

Example Let us first illustrate this corollary for the elliptic curve $A : y^2 + xy = x^3 - x^2 - 2x - 1$, element of great importance in [1]. This curve has conductor 49 and one can show that there exists an isomorphism $\varphi : X_0(49) \to E$, sending $[\infty]$ to O and $[0]$ to $(2,-1)$. [3]

Another example, illustrate this for the congruent number curve $E : y^2 = x^3 - x$, central character in the work of Tian ([21], [22]). This curve is of conductor 32 and one can show that there exists $\varphi : X_0(32) \to E$, of degree 2, that sends $[\infty]$ to O.

Remark For elliptic curves with complex multiplication, a different proof of the analytic continuation and functional equation for $L(E,s)$ was known since the 19th century, due to Eisenstein and Kronecker. This was subsequently taken up and refined by Weil [23] and Deuring [8] and it relies on showing that $L(E,s)$ is a Hecke L-series with Grossencharacter, but as mentioned in [3], there seems to be no analogue proof using this method for elliptic curves without complex multiplication.

1.3 The conjecture of Birch and Swinnerton-Dyer

One of the seven Millennium Problems of the Clay Mathematics Institute in Cambridge, Massachusetts is the Birch Swinnerton-Dyer conjecture, named after two British mathematicians, Bryan Birch and Peter Swinnerton-Dyer, who first formulated the conjecture in [2]. The conjecture relates the number of infinite order basis elements of the group of rational points on an elliptic curve to the L-function of the curve. As one of the Millennium Problems, the solutions to which carry a prize of one million dollars a piece, the Birch Swinnerton-Dyer conjecture, since its introduction in 1965, has remained both a fundamental

unsolved problem in algebraic number theory and one of the most challenging problems in mathematics. The history of the problem is interesting, as the predecessor to the Birch Swinnerton-Dyer conjecture, the Taniyama Shimura theorem led to one of the most famous recent result in number theory, the solution of Fermat's Last Theorem, while the development of the mathematics instigated by work on the conjecture has led to new error-correcting codes from the algebraic geometry of elliptic curves and an improved method for factoring integers based on elliptic curves over finite fields.

Let us try to take a glimpse at what the conjecture actually is.

Definition $r_E = ord_{s=1}L(E,s)$.

Conjecture 12 (Weak Birch-Swinnerton-Dyer)**.** *For all elliptic curves $E/\mathbb{Q}$, we have $r_E = g_E$.*

This weak Birch-Swinnerton-Dyer Conjecture would immediately imply the

Conjecture 13 (Strong Parity Conjecture)**.** *For all elliptic curves $E/\mathbb{Q}$, we have $r_E = g_E \pmod 2$.*

The functional equation $\Lambda(E,s) = w_E\Lambda(E,2-s)$, discussed in Corollary 9, implies immediately that the parity of the analytic rank r_E is determined by $w_E = (-1)^{r_E}$. The strong parity conjecture, implies that if $w_E = -1$, then r_E and g_E are both odd and in particular strictly greater than 0. Now, by Mordell-Weil theorem one can see that $E(\mathbb{Q})$ is infinite.

Example A very old problem concerning the rational points on elliptic curves is the congruent number problem, which asks which rational integers can occur as the areas of right-angled triangles with rational length sides. Such numbers are called congruent numbers. If N is a congruent number, then s^2N is also a congruent number for any rational integer s, just by multiplying each side of the triangle by s, and vice versa. So, when trying to find congruent numbers, it is sufficient to look at the ones that are square free. Congruent numbers are closely related to the elliptic curve $E^{(N)} : y^2 = x^3 - N^2x$, since

$$N \text{ is congruent } \Leftrightarrow E^{(N)}(\mathbb{Q}) \text{ is infinite.}$$

A classical computation shows that $w_{E^{(N)}} = 1$ if $N \equiv 1,2,3 \pmod 8$, and $w_{E^{(N)}} = -1$ if $N \equiv 5,6,7 \pmod 8$. As we can see, the strong parity conjecture implies:

Conjecture 14. *Every positive integer $N \equiv 5,6,7 \pmod 8$ is a congruent number.*

Numerical evidence supports this conjecture, because we can see in A003273 in OEIS that the sequence of first congruent numbers starts with 5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, ...

The only general result known that supports the strong parity conjecture is a result proved by Tim and Vladimir Dokchitser, which was briefly mentioned after Conjecture 6.

Remember that we defined the integer $t_{E,p} \geq 0$ by $Ш(E)(p)_{div} = (\mathbb{Q}_p/\mathbb{Z}_p)^{t_{E,p}}$

Theorem 15 (Weak Parity Theorem, T Dokchitser & V Dokchitser)**.** *For all elliptic curves $E/\mathbb{Q}$, and all primes p, we have*

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

As we previously mentioned, this implies the fact that $t_{E,p}$ is independent of p. Of course, the conjectured result about the finiteness of $Ш(E)$ would imply that $t_{E,p} = 0$ for every prime p, which supports the Strong Parity Conjecture.

Corollary 16. *For every prime number p, the $\mathbb{F}_p$ dimension of $Sel_p(E)/Im(E(\mathbb{Q})_{tor})$ is even if and only if $w_E = 1$.*

Proof. Consider the multiplication by p map on $Ш(E)(p)/Ш(E)(p)_{div}$. The kernel of this map is a finite $\mathbb{F}_p$ vector space. Denote by m_p its dimension. As pointed out in Corollary 4, m_p is always even.

Denote by $s_p = \dim_{\mathbb{F}_p}(Sel_p(E)/Im(E(\mathbb{Q})_{tor}))$. Then, $s_p = g_E + t_{E,p} + m_p$. Therefore, $s_p = g_E + t_{E,p} \pmod 2$, so $s_p = r_E \pmod 2$, which means that s_p is even if and only if r_E is even, i.e. if and only if $w_E = 1$.

□

Corollary 17. *If $w_E = -1$ and g_E is even, then necessarily $t_{E,p}$ is odd, in particular $t_{E,p} \geq 1$ for any prime number.*

It is conjectured that $Ш(E)$ is finite and hence that $t_{E,p} = 0$ for all the primes p, but proving this still represents one of the major challenges in number theory.

In 1986, Gross and Zagier managed to generalize a previous result by John Coates and Andrew Wiles. They used their formula relating the derivative of $L'(E,s)$ at $s = 1$ and the height of Heegner points of E to deduce that if E is an elliptic curve defined over $\mathbb{Q}$ such that $r_E = 1$, then $E(\mathbb{Q})$ contains points of infinite order.

Inspired by this, Kolyvagin developed theory of Euler systems that lead to the best result to date in the direction of the weak Birch-Swinnerton-Dyer conjecture.

Theorem 18 (Kolyvagin, Gross-Zagier)**.** *Assume that $r_E \leq 1$. Then $r_E = g_E$ and $Ш(E)$ is finite.*

Unfortunately, when the analytic rank of E is greater than or equal to 2, there are no proved results in the support of the weak Birch and Swinnerton Dyer conjecture. Moreover, $Ш(E)$ is not even known to be finite for a single elliptic curve of $r_E \geq 2$.

Definition For $P,Q \in E(\mathbb{Q})$, denote by $\langle P,Q\rangle = \frac{1}{2}\left(\hat{h}(P\oplus Q) - \hat{h}(P) - \hat{h}(Q)\right)$, where $\hat{h} : E(\overline{\mathbb{Q}}) \to \mathbb{R}$ is the Néron-Tate height.

This bilinear form, called the Néron-Tate pairing, is positive definite on $E(\mathbb{Q})\otimes\mathbb{R}$. [19]

Definition The regulator of E over $\mathbb{Q}$ is $R_\infty = \det\langle P_i, P_j\rangle$ where $P_1,\ldots,P_{g_E}$ are a basis of $E(\mathbb{Q})$ modulo torsion.

The next last ingredient that has to be defined before we can present the full statement of the conjecture mentioned in the title of this essay are the so called Tamagawa factors. In what follows, assume that we have fixed a minimal generalized Weierstrass equation for E as in (1.6).

Definition Let $c_\infty(E) = \delta_E\Omega_E$, where δ_E is the number of connected components of $E(\mathbb{R})$ and Ω_E is the least positive real period of the Néron differential $\omega = \frac{dx}{2y+a_1x+a_3} = \frac{d\wp(z)}{\wp'(z)} = dz$.

Next, if p divides the conductor $C(E)$, 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 the generalized Weierstrass equation implies that the index $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ is finite.

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

Remark Tate algorithm, described in detail in [5], can be used to compute $c_p(E)$ on any explicit Weierstrass equation.

Conjecture 19 (Full Birch and Swinnerton-Dyer)**.** *With the notations above, we have $r_E = g_E$, $Ш(E)$ is finite and if we denote by $\mathscr{L}_E = \lim_{s\to 1}\frac{L(E,s)}{(s-1)^{r_E}}$ then*

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

What I find very curious about this conjecture it is the fact that it was not even know that the left hand side of the above equality is defined, except for curves with complex multiplication, at the time the conjecture was formulated.

Remark A proof of this strong form of the conjecture would give an effective way of finding generators for the group $E(\mathbb{Q})$. [12]

Example Let us point a connection to the congruent number problem. Tunnel proved that if n is a congruent number, then

$$\#\{(x,y,z)\in\mathbb{Z}^3 : 2x^2+y^2+8z^2=n, z \text{ is odd}\} = \#\{(x,y,z)\in\mathbb{Z}^3 : 2x^2+y^2+8z^2=n, z \text{ is even}\}.$$

and the converse is also true if the Birch and Swinnerton-Dyer conjecture is true. So the proof of the conjecture will lead to a solution to the congruent number problem in finite computation.

Example By a result of Mazur and Rubin (2010), if the conjecture holds for all elliptic curves over all number fields, then Hilbert's 10th problem has negative answer over $\mathcal{O}_K$ for any number field K.

The exact formula given in Conjecture 19 has been tested numerically in a vast number of cases. Let us first see it at work in the concrete example

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

It is known about this curve that it has conductor $C(A)=49$, $A(\mathbb{Q})=\mathbb{Z}/2\mathbb{Z}$ and the analytic rank is $r_A=0$. In addition, $c_\infty(A)=\Omega_A$, $\frac{\mathscr{L}_A}{c_\infty(A)}=\frac{L(A,1)}{\Omega_A}=1/2$, the regulator $R_\infty(A)=1$ and the Tamagawa factor $c_7(A)=2$.

It has been also proved that the Tate-Shafarevich group $Ш(A)$ is trivial, therefore one can check that the full Birch-Swinnerton-Dyer conjecture is true for this elliptic curve.

There is serious difficulty in verifying the conjecture for specific curves, let alone for infinite families, because as previously noted, the Tate-Shafarevich group is not known to be finite for any specific curve of analytic rank greater or equal to 2. But still, the situation is better than when Tate made his famous comment, characterizing the Birch and Swinnerton-Dyer conjecture as relating the order of a group not known to be finite with the value of a function at a point where it is not known to be defined.

John Cremona [6] summarized how we can verify the weak form of the Birch and Swinnerton-Dyer conjecture if $r_E \leq 3$. He observed that

If $r_E \leq 3$ then one can find the exact value of r_E using

1. The root number w_E to determine the parity;
2. Modular symbols (to establish if $r_E = 0$);

3. The theorem of Kolyvagin and Gross-Zagier to distinguish between $r_E = 1$ and $r_E = 3$;
4. Numerical evaluations of the derivatives of the L-function at the point $s = 1$.

To see how this actually works, let us consider the elliptic curve

$$E : y^2 + xy = x^3 + x^2 - 696x + 6784 \text{ of conductor } C(E) = 234446.$$

This curve has root number $w(E) = -1$, so the analytic rank r_E has to be odd. By estimations on the derivative $L'(E,1)$, it can be observed that this is very small in absolute value, fact that makes one suspect that $r_E \geq 3$.

By the method of 2- descent, described latter in this essay, it can be established that the algebraic rank $g_E = 3$ and we can even find generators. The regulator $R_\infty(E)$ is approximately 2.159011... and the Tate-Shafarevich group has no elements of order 2.

Theorem 18 of Kolyvagin, Gross-Zagier implies that $r_E > 1$. The value of $L^{(3)}(E,1)$ it is estimated to be approximately 59.093..., which implies that the analytic rank $r_E = 3$, so conjecture 12 is holds for this curve. Except the order of $Ш(E)$, all the other terms that appear in the full Birch and Swinnerton-Dyer conjecture can be computed for this elliptic curve and the conjecture predicts in this case that $Ш(E/\mathbb{Q}) = 1$.

Professor Cremona pointed at that time that if $r_E \geq 3$, then he is unaware of a method of determining it rigorously.

In the same presentation [6], professor Cremona stated that there are 614308 isogeny classes of elliptic curves with conductor $C(E) \leq 140000$ and all of them have analytic rank $r_E \leq 3$ and he centralized them in the table below. [6]

range of C(E)	#	$r=0$	$r=1$	$r=2$	$r=3$
0-9999	38042	16450	19622	1969	1
10000-19999	43175	17101	22576	3490	8
20000-29999	44141	17329	22601	4183	28
30000-39999	44324	16980	22789	4517	38
40000-49999	44519	16912	22826	4727	54
50000-59999	44301	16728	22400	5126	47
60000-69999	44361	16568	22558	5147	88
70000-79999	44449	16717	22247	5400	85
80000-89999	44861	17052	22341	5369	99
90000-99999	45053	16923	22749	5568	83
100000-109999	44274	16599	22165	5369	141
110000-119999	44071	16307	22173	5453	138
120000-129999	44655	16288	22621	5648	98
130000-139999	44082	16025	22201	5738	118
0-139999	614308	233979	311599	67704	1026

In every case, it was verified that $r_E = g_E$, supporting the weak Birch and Swinnerton-Dyer conjecture.

2. Generalization of Birch's Lemma

This section starts with a presentation of the classical Lemma 21. Birch proved this lemma by generalizing a result of Heegner, in which, of course, there were no L-functions involved. The section also includes an exposition of a generalization of this lemma, namely Theorem 24, which applies to quite a large class of elliptic curves with $E(\mathbb{Q})[2]$ of order 2.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor $C(E)$ and let $\phi = \sum_{n\geq 1} a_n q^n$ be the corresponding cusp form on $\Gamma_0(C(E))$. Let K be an imaginary quadratic field. For simplicity, we assume that $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. This tells us that the units $\mathscr{O}_K^\times = \{\pm 1\}$.

Suppose that every prime factor of $C(E)$ splits in K. This assumption, called the Heegner Hypothesis, guarantees that there exists a prime ideal $\mathfrak{C} \subseteq \mathscr{O}_K$ such that $\mathscr{O}_K/\mathfrak{C} \simeq \mathbb{Z}/C(E)\mathbb{Z}$.

For each positive integer M that is relatively prime to $C(E)$, let $\mathscr{O}_M = \mathbb{Z} + M \cdot \mathscr{O}_K$ be the order of K of conductor M. Writing $\mathfrak{C}_M = \mathfrak{C} \cap \mathscr{O}_M$, observe that $\mathfrak{C}_M$ is an invertible ideal in $\mathscr{O}_K$ with $\mathfrak{C}_M^{-1}/\mathscr{O}_K \simeq \mathbb{Z}/C(E)\mathbb{Z}$. Now, $(\mathbb{C}/\mathscr{O}_K, \mathfrak{C}_M^{-1})$ is a modular pair, since if $E' = \mathbb{C}/\mathscr{O}_K$ then $\mathfrak{C}_M^{-1}\mathscr{O}_K/\mathscr{O}_K \subset C(E)^{-1}\mathscr{O}_K/\mathscr{O}_K = E'[C(E)]$, so $\mathfrak{C}_M^{-1}\mathscr{O}_K$ is a cyclic subgroup of E which has order $C(E)$.

Definition

$$P_M := (\mathbb{C}/\mathscr{O}_K, \mathfrak{C}_M^{-1}/\mathscr{O}_K)$$

is a Heegner point on $X_0(C(E))$.

This points were first introduced by Heegner in his work on the class-number problem for imaginary quadratic fields. On the curve $X_0(C(E))$, they correspond to the moduli of $C(E)$-isogenous elliptic curves with the same ring of complex multiplication. Using them, Birch was able to construct points of infinite order, as we will soon see.

Remark Equivalently, we can describe Heegner points P_M as isomorphism classes of couples of elliptic curves $(\mathbb{C}/\mathscr{O}_K, \mathbb{C}/\mathfrak{C}_M^{-1})$ with $ker(\mathbb{C}/\mathscr{O}_K \to \mathbb{C}/\mathfrak{C}_M^{-1}) = \mathfrak{C}_M^{-1}/\mathscr{O}_K \simeq \mathbb{Z}/C(E)\mathbb{Z}$. In the article [1], the authors use the notation

$$P_M := (\mathbb{C}/\mathscr{O}_K \to \mathbb{C}/\mathfrak{C}_M^{-1}).$$

The Heegner point P_M, as defined above, lies in $X_0(C(E))(H_M)$, where H_M is the ring class field of K of conductor M. H_M is the abelian extension over K characterized by the property that the Artin map induces an isomorphism $\hat{K}^\times/K^\times\hat{\mathscr{O}}_M^\times \xrightarrow{\sim} Gal(H_M/K)$, where $\hat{K}^\times$ denotes the idéle group of K and $\hat{\mathscr{O}}_M^\times = \mathscr{O}_M^\times \otimes_{\mathbb{Z}} \prod_p \mathbb{Z}_p$.

Gross and Zagier showed that Heegner points satisfy a formula that links their Néron-Tate height to the value at $s=1$ of the first derivative of the L-function of an elliptic curve. The authors present the following generalization of Gross-Zagier formula, proved by Yuan-Zhang-Zhang in [24]. This generalization is useful to extend Theorem 21, known in the literature as Birch's lemma.

If χ denotes an abelian character of K, we write $L(E/K,\chi,s)$ for the complex L-series of E/K twisted by χ.

Theorem 20. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor $C(E)$ and let $f: X_0(C(E)) \to E$ be a modular parameterization as in* (1.7)*. Let $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ be an imaginary quadratic field of discriminant d_K, and assume that every prime dividing $C(E)$ splits in K. Let χ be any ring class character of K with conductor M, where $M \geq 1$ is such that $(M, C(E)\cdot d_K) = 1$. Let P_M denote the Heegner point on $X_0(C(E))$ of conductor M defined above and put*

$$P_\chi(f) := \sum_{\sigma \in Gal(H_M/K)} f(P_M)^\sigma \chi(\sigma),$$

which lies in the tensor product $E(H_M)\otimes\mathbb{C}$. Then

$$L'(E/K,\chi,1) = \frac{8\pi^2(\phi,\phi)_{\Gamma_0(C(E))}}{\sqrt{|d_K M^2|}} \cdot \frac{\hat{h}_K(P_\chi(f))}{\deg f},$$

where $\hat{h}_K$ denotes the Néron-Tate height on E over K, $\phi = \sum_n a_n q^n$ is the primitive eigenform of weight 2 attached to E, and the Petersson norm is defined by

$$(\phi,\phi)_{\Gamma_0(C(E))} = \int\int_{\Gamma_0(C(E))\backslash\mathscr{H}} |\phi(z)|^2 dxdy,\ z = x+iy.$$

Many results about the action of $Gal(H_M/K)$ on the Heegner points on $X_0(C(E))$ are described in the beautiful article by Benedict Gross [9]. An action of particular interests for us is the following. If we denote by $\mathfrak{P}_M$ the set of all conjugates of P_M under the action of $Gal(H_M/K)$, by $w_{C(E)}$ the Fricke involution and by τ the complex conjugation, we have the equality of sets

$$w_{C(E)}\mathfrak{P}_M = \tau\mathfrak{P}_M \tag{2.1}$$

In the remainder of this section, we will take l_0 to be any prime $l_0 > 3$ such that $l_0 \equiv 3 \pmod 4$ and we will define

$$K = \mathbb{Q}\left(\sqrt{-l_0}\right). \tag{2.2}$$

This particular choice of K it is known to have odd class number, feature which will be extremely important in the proof of the next theorem.

2.1 Birch's lemma

Theorem 21 (Birch)**.** *Let E be any elliptic curve defined over $\mathbb{Q}$ with modular parameterization as in Corollary 10, and assume that $f([0]) \notin 2E(\mathbb{Q})$. Let K be the quadratic imaginary field defined as above, with the additional property that every prime dividing $C(E)$ splits in K. Let $\mathfrak{C}$ be an ideal in $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{C} \simeq \mathbb{Z}/C(E)\mathbb{Z}$, and let $P = P_1$ be the corresponding Heegner point of conductor* 1*. Then $y_K = Tr_{H_1/K}(f(P))$ is of infinite order in $E(K)$.*

Proof. Denote by involution $w_C = w_{C(E)}$ the Fricke involution, which is defined by the matrix $\begin{pmatrix} 0 & -1 \\ C(E) & 0 \end{pmatrix}$. By a result in the theory of modular forms we know that $f \circ w_C - \varepsilon f$ is constant, where $\varepsilon = \pm 1$ is the negative of the sign of the functional equation satisfied by the analytic continuation of the complex L series $L(E,s)$. A proof of this result can be found in the book by Knapp [11].

Thus, for all points $P \in X_0(C(E))$, we have

$$f(P^{w_C}) - \varepsilon f(P) = f([\infty]^{w_C}) - \varepsilon f([\infty]) = f([0]) - \varepsilon \cdot O = f([0]),$$

where O is the zero element of E.

It is known that $X_0(C(E))$ contains fixed points of w_C. Moreover, Ogg showed that this fixed points are non-cusps and he provided a formula for their number in his article [15].

If we now evaluate our constant morphism at a fixed point of P of w_C we get that

$$(1-\varepsilon) f(P) = f([0]).$$

Since $O \in 2E(\mathbb{Q})$, the hypothesis $f([0]) \notin 2E(\mathbb{Q})$, forces $\varepsilon = -1$. Therefore, $f(P^{w_C}) + f(P) = f([0])$ for all $P \in X_0(C(E))$. Now, if we evaluate

$$\overline{y_K} + y_K = Tr_{H_1/K}\left(\overline{f(P)} + f(P)\right) = Tr_{H_1/K}\left(f(\overline{P}) + f(P)\right),$$

so

$$\overline{y_K}+y_K=\sum_{\sigma\in Gal(H_1/K)} f(\overline{P^\sigma})+f(P^\sigma)=\sum_{\sigma\in Gal(H_1/K)} f(P^{\sigma w_C})+f(P^\sigma), \text{ using the equality (2.1).}$$

Therefore, $\overline{y_K}+y_K=\sum_{\rho\in Gal(H_1/K)} f([0])=\#Gal(H_1/K)\cdot f([0])$. It is known that the Galois group of the Hilbert class field H_1 over K is canonically isomorphic to the ideal class group of K. Hence, if we denote by h the class number of K, $\overline{y_K}+y_K=h\cdot f([0])$.

The prime l_0 was chosen such that the class number h is odd, therefore the point $T:=\overline{y_K}+y_K$ does not belong to $2E(\mathbb{Q})$ either.

Because $K/\mathbb{Q}$ is totally ramified at l_0 and the only primes that ramify in $\mathbb{Q}(E[2^\infty])$ are the ones that divide $2\cdot C(E)$, we get that $E(K)[2^\infty]=E(\mathbb{Q})[2^\infty]$.

Suppose y_K is a torsion point. Since the torsion group $E(K)_{tor}$ is finite, we can define the integer $a=lcm\{k\big|k$ is odd and it is the order of a point P $\in E(K)_{tor}\}$. By construction, a annihilates all elements of odd finite order in $E(K)$.

Now, if the order of y_K is $2^t\cdot N$, for some $t,N\in\mathbb{N}$ with N odd, we observe that $a\cdot 2^t\cdot y_K=O=2^t\cdot a\cdot y_K$, so ay_K has order a power of 2, in other words $ay_K\in E(K)[2^\infty]=E(\mathbb{Q})[2^\infty]$. Since the point has rational coordinates, $ay_K=\overline{ay_K}=a\overline{y_K}$, so

$$a\cdot T=a(\overline{y_K}+y_K)=2y_K\in 2E(\mathbb{Q}).$$

But a is odd implies that $T\in 2E(\mathbb{Q})$ which is a contradiction. The proof is now complete. □

We immediately deduce the following corollary.

Corollary 22. *Under the same hypotheses as in Theorem 21, the complex L-function $L(E/K,s)$ of E over K has a simple zero at $s=1$, $L(E,s)$ does not vanish at $s=1$ and $L(E^{(-l_0)},s)$ has a simple zero at $s=1$.*

Proof. The point y_K constructed in the previous theorem has infinite order, therefore non-zero Néron-Tate height. The theorem of Gross-Zagier tells us that that the derivative $L'(E/K,s)\neq 0$. It is known that the complex $L-$ function

$$L(E/K,s)=L(E,s)L(E^{(-l_0)},s) \tag{2.3}$$

and the global root number $w_{E/K}$ of $L(E/K,s)$ satisfies

$$w_{E/K}=w_E\cdot w_{E^{(-l_0)}},$$

where w_E and $w_{E^{(-l_0)}}$ are the root numbers of $L(E,s)$ and $L(E^{(-l_0)},s)$ respectively. In the proof of the previous theorem, it was showed that $\varepsilon = -w_E = -1$, so $w_E = 1$.

Let $\chi_{(-l_0)}$ be the Dirichlet character corresponding to the quadratic extension $K/\mathbb{Q}$. Then, because $C(E)$ is prime to l_0, we will use the formula in [3] to compute $w_{E^{(-l_0)}}$.

$$w_{E^{(-l_0)}} = \chi_{(-l_0)}(-C(E))w_E = \chi_{(-l_0)}(-1)\cdot\chi_{(-l_0)}(C(E))$$

Now, since K is an imaginary quadratic extension, $\chi_{(-l_0)}(-1) = -1$ and because every prime factor p of $C(E)$ splits in K we know that $\chi_{(-l_0)}(p) = 1$, hence $\chi_{(-l_0)}(C(E)) = 1$. All of this proves that $w_{E^{(-l_0)}} = -1$ and in particular that $w_{E/K} = -1$. Combined with the fact that $L'(E/K,1) \neq 0$ this gives us that $L(E/K,s)$ has a simple zero at $s = 1$. Looking at the functional equation for $L(E^{(-l_0)},s)$, the root number -1 tells us that it has a zero at $s = 1$ of odd multiplicity. This implies that $L(E^{(-l_0)},s)$ has a simple zero at $s = 1$ and in the view of (2.3), that $L(E,1) \neq 0$. □

Remark This corollary immediately implies the assertion of the Theorem 26 for $k = 1$.

2.2 Extended Birch's Lemma

In what follows, the authors of [1], extend Birch's result to quadratic twist with arbitrary many prime factors. Before I present their generalization, it is convenient to introduce the following terminology.

Definition A prime q_1 is said to be a *sensitive* supersingular prime for the elliptic curve E if
(i) q_1 is a prime of good supersingular reduction for E,
(ii) $q_1 \equiv 1 \pmod 4$ and
(iii) $C = C_E$ is a square modulo q_1.

Example For the most frequently discussed curve in this essay, namely $A = X_0(49)$, we can take as sensitive supersingular prime any $q_1 \equiv 1 \pmod 4$ that is inert in $\mathbb{Q}(\sqrt{-7})$ as long as l_0 is chosen such that $l_0 \equiv 3 \pmod 4$ and q_1 is inert in $K = \mathbb{Q}(\sqrt{-l_0})$.

Another example of a curve with a supersingular prime pointed in [1] is $E = X_0(14)$ with the prime $q_1 = 5$ and l_0 such that q_1 is inert in $K = \mathbb{Q}(\sqrt{-l_0})$.

The authors of [1] also mention the curves $y^2 + xy + y = x^3 - x - 1$ (conductor 69) and $y^2 = x^3 - x^2 - x - 2$ (conductor 84) for which one can take $q_1 = 5$ and $q_1 = 41$ respectively, as long as we choose $l_0 \equiv 4 \pmod 4$ such that q_1 is inert in $K = \mathbb{Q}(\sqrt{-l_0})$.

Remark If E possesses a sensitive supersingular prime q_1, then necessarily $E(\mathbb{Q})[2^\infty]$ has order at most 2. To see this, notice that by definition $q_1 \geq 5$ and by Exercise 5.10 in [19], the reduction $\widetilde{E}$ modulo q_1 has exactly q_1+1 points on $\mathbb{F}_{q_1}$. Since the reduction modulo q_1 is injective on $E(\mathbb{Q})[2^\infty]$, the order of this torsion subgroup must divide q_1+1, which is congruent to 2 modulo 4. Since $\#E(\mathbb{Q})[2^\infty]$ is a power of 2, the result follows. In particular, this remark implies that

$$E(\mathbb{Q})[2^\infty] = E(\mathbb{Q})[2] \tag{2.4}$$

Recall that we denote by $\phi = \sum_{n\geq 1} a_n q^n$ the primitive cusp form of weight 2 for $\Gamma_0(C(E))$ attached to E. For simplicity, I will denote $C(E)$ by C in what follows.

Lemma 23. *Assume that E possesses a sensitive supersingular prime q_1, which is inert in K. For each integer $r \geq 2$, define $\sum_r$ to be the set of all prime $q \neq q_1$ such that (i) $q \equiv 1 \pmod 4$, (ii) $a_q \equiv 0 \pmod{2^r}$, (iii) $(q,C) = 1$ and C is a square modulo q, and (iv) q is inert in K. Then $\sum_r$ is infinite of positive density in the set of prime numbers.*

Proof. Let $J = \mathbb{Q}(\sqrt{C}, E[2^r])$. Observe that l_0 is totally ramified in $K/\mathbb{Q}$. The primes that ramify in J must divide $2C$ therefore $K \cap J = \mathbb{Q}$. Since the extensions $J/\mathbb{Q}$ and $K/\mathbb{Q}$ are Galois and $K \cap J = \mathbb{Q}$, a very well known result in Galois theory gives that

$$Gal(JK/\mathbb{Q}) \simeq Gal(J/\mathbb{Q}) \times Gal(K/\mathbb{Q}).$$

The prime q_1 is also unramified in J, because $(q_1, 2C) = 1$. If we consider a prime $\mathfrak{q}$ of J that lies above q_1, since the ramification index $e_{\mathfrak{q}/q_1} = 1$, the inertia group $I_{\mathfrak{q}/q_1}$ is trivial.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_{\mathfrak{q}/q_1} & \longrightarrow & D_{\mathfrak{q}/q_1} & \longrightarrow & Gal(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{q_1}) & \longrightarrow & 1 \\ & & \| order & & & & \| order & & \\ & & e_{\mathfrak{q}/q_1} & & & & f_{\mathfrak{q}/q_1} & & \end{array}$$

In this case, the generator $x \mapsto x^{q_1^{f_{\mathfrak{q}/q_1}}}$ of $Gal(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{q_1})$ lifts canonically to the Frobenius element $Frob_{\mathfrak{q}/q_1} \in D_{\mathfrak{q}/q_1} \subset Gal(J/\mathbb{Q})$. Thus, writing $\triangle = Gal(JK/\mathbb{Q})$, there will be a unique element $\sigma \in \triangle$, whose restriction to K is just the complex conjugation and whose restriction to J is the Frobenius automorphism of some prime of J that lies above q_1.

Assuming $r \geq 2$, let $\mathscr{S} = \{p \text{ prime } | p \text{ does not divide } 2l_0q_1C, \text{ whose Frobenius automorphisms in } \triangle \text{ lie in the conjugacy class of } \sigma\}$. Chebotarev density theorem can be applied to deduce that $\mathscr{S}$ is infinite of positive density in the set of all prime numbers. Because $q_1 \geq 5$

is supersingular, $a_{q_1} = 0$, so the characteristic polynomial of the Frobenius automorphism of q_1 acting on the 2- adic Tate module $T_2(E)$ is equal to $X^2 + q_1$. Similarly, the characteristic polynomial of the Frobenius automorphism of a prime q that does not divide $2C$ acting on $T_2(E)$ is $X^2 + a_q X + q$. Because $E[2^r] = T_2(E)/2^r T_2(E)$ then $q \in \mathscr{S}$ must have $a_q \equiv 0 \pmod{2^r}$ and $q \equiv q_1 \pmod{2^r}$. Also, since q_1 is inert in K, q is also inert in K. q_1 splits in $\mathbb{Q}(\sqrt{C})$, therefore q splits as well in this field.

We just proved that $\mathscr{S} \subset \sum_r$, hence $\sum_r$ is infinite and has positive density in the set of all prime numbers. □

Remark It is important to notice that for our example $A = X_0(49)$, the set $\sum_r$ contains all the primes which are $\equiv 1 \pmod 4$ and are inert in $F = \mathbb{Q}(\sqrt{-7})$ and $K = \mathbb{Q}(\sqrt{-l_0})$.

Theorem 24. *Assume that (i) $f([0]) \notin 2E(\mathbb{Q})$ and (ii) there exists a sensitive supersingular prime q_1 for E. Let $K = \mathbb{Q}(\sqrt{-l_0})$, as before, with the property that every prime dividing C splits in K and q_1 is inert in K. For each integer $r \geq 1$, let $R = q_1 q_2 \dots q_r$ where, for $r \geq 2$, $q_2, \dots, q_r$ are any distinct primes in the set $\sum_r$ defined in Lemma 23. Then $K(\sqrt{R})$ is a subfield of the ring class field H_R. Writing χ_R for the character of K attached to this quadratic extension, define the Heegner point y_R by*

$$y_R = \sum_{\sigma \in Gal(H_R/K)} \chi_R(\sigma) f(P_R)^\sigma.$$

Then, for each integer $r \geq 1$, we have $y_R \in 2^{r-1} E\left(\mathbb{Q}(\sqrt{-l_0 R})\right)^- + E\left(\mathbb{Q}(\sqrt{-l_0 R})_{tor}\right)$, but $y_R \notin 2^r E\left(\mathbb{Q}(\sqrt{-l_0 R})\right)^- + E\left(\mathbb{Q}(\sqrt{-l_0 R})_{tor}\right)$. In particular, y_R is of infinite order.

Remark By the theorem of Manin-Drinfeld, $f([0])$ is a torsion point, hence condition (i) implies that $f([0])$ is a point of even order. A multiple of this point will have exact order 2, therefore $E(\mathbb{Q})[2]$ contians a non-trivial element. By a previous remark, the existence of a sensitive supersingular prime ensures the fact that $E(\mathbb{Q})[2]$ has order at most 2, therefore (i) and (ii) together imply that $E(\mathbb{Q})[2]$ has exact order 2.

Remark In general, we will denote by $E(\mathbb{Q}(\sqrt{N}))^-$ the subgroup of $E(\mathbb{Q}(\sqrt{N}))$ consisting of points on which the non-trivial element of $Gal(\mathbb{Q}(\sqrt{N})/\mathbb{Q})$ acts like -1. This is consistent with the notations used in [1] and [3].

Proving this theorem represents a major step in this essay. Indeed, let us see how the assertion of this theorem implies Theorem 26, one of the most general results presented in the

first section of [1]. Since y_R has infinite order, the Néron-Tate height $\hat{h}_K(y_R) = \hat{h}_K(P_{\chi_R}(f)) \neq 0$, which by Theorem 20 implies that

$$L'(E/K, \chi_R, 1) \neq 0. \tag{2.5}$$

We know that

$$L(E/K, \chi_R, s) = L(E^{(-l_0R)}, s)L(E^{(R)}, s).$$

Earlier, in the proof of Theorem 21, it was shown that the root number w_E of $L(E,s)$ is equal to $+1$. Using the formula for computing root numbers of quadratic twists in [1], we see that

$$w_{E^{(R)}} = \chi_{(R)}(-C)w_E = \chi_{(R)}(-1)\chi_{(R)}(C) = 1$$

In the above, $\chi_{(R)}(C) = 1$, since by hypothesis C is a square modulo all the primes dividing R and $\chi_{(R)}(-1) = 1$ because $\mathbb{Q}(\sqrt{R})/\mathbb{Q}$ is a real extension. Similarly, we compute

$$w_{E^{(-l_0R)}} = \chi_{(-l_0R)}(-C) \cdot w_E = \chi_{(-l_0R)}(-1) = -1,$$

the difference being in this case that $\mathbb{Q}(\sqrt{-l_0R})/\mathbb{Q}$ is an imaginary extension. $w_{E^{(-l_0R)}} = -1$, automatically implies that $L(E^{(-l_0R)}, s)$ vanishes at $s = 1$ and (2.5) implies that $L(E^{(-l_0R)}, s)$ has a simple zero at $s = 1$. To summarise, $L(E/K, \chi_R, s)$ and $L(E^{(-l_0R)}, s)$ both have simple zeros at $s = 1$, but $L(E^{(R)}, s)$ does not vanish at 1. The theorem of Kolyvagin-Gross-Zagier applied to $E^{(-l_0R)}$ tells us that $E^{(-l_0R)}(\mathbb{Q})$ has rank 1 and the Tate-Shafarevich group $Ш(E^{(-l_0R)})$ is finite. Similarly, one can deduce analogous results for $E^{(R)}$, but in this case $E^{(R)}(\mathbb{Q})$ has rank 0. All of the above takes the form of a corollary in the first reference as follows.

Corollary 25. *Under the same hypothesis as in Theorem 24, for all $R = q_1 \dots q_r$ with $r \geq 1$ we have (i) the complex L-series of $E^{(R)}$ does not vanish at $s = 1$, and both $E^{(R)}(\mathbb{Q})$ and $Ш(E^{(R)})$ are finite, and (ii) the complex L-series of $E^{(-l_0R)}$ has a simple zero at $s = 1$, $E^{(l_0R)}(\mathbb{Q})$ has rank 1, and $Ш(E^{(-l_0R)})$ is finite.*

As we proved that $\sum_r$ is infinite when $r \geq 2$, the next beautiful result follows easily.

Theorem 26. *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor $C = C(E)$ and take $f : X_0(C) \to E$ to be a modular parameterization as given in* (1.7)*. Assume that*

(1) $f([0]) \notin 2E(\mathbb{Q})$;

(2) there is a good supersingular prime q_1 for E such that $q_1 \equiv 4 \pmod 4$ and C is a square modulo q_1. (this is what the authors of [1] called a sensitive supersingular prime).

If $k \geq 1$ is an integer, then there are infinitely many square free integers M, having exact k prime factors, such that $L(E^{(M)},s)$ has a zero at $s=1$ of order 1. Similarly, if k is any integer ≥ 2, there are infinitely many square free integers M, having exact k prime factors such that $L(E^{(M)},s)$ does not vanish at $s=1$.

Example Let us see some numerical examples to which this theorem applies. We are going to start with the curve $A: y^2+xy=x^3-x^2-2x-1$, of conductor 49 and $A(\mathbb{Q})=\mathbb{Z}/2\mathbb{Z}$. For this curve, according to [3], there is an isomorphism $f: X_0(49)\to A$ such that $f([\infty])=O$, $f([0])=(-2,1)\notin 2E(\mathbb{Q})$ since $f([0])$ is the only non-trivial torsion point. As we remarked before, we can choose q_1 as any prime $\equiv 1 \pmod 4$ and which is not a square modulo 7.

The theorem also applies to the curve $E=X_0(14)$ with $q_1=5$ and to the curves $y^2+xy+y=x^3-x-1$ (conductor 69) and $y^2=x^3-x^2-x-2$ (conductor 84) for which we already discussed the existence of sensitive supersingular primes.

After we convinced ourselves of the power of Theorem 24, in particular the fact that implies the main theorem of this section, it remains nothing but to prove it. The proof given in [1] relies on three preliminary lemmas.

Let $R=q_1\dots q_r$ be as defined in the statement of Theorem 24. Define also

$$\mathfrak{h}_R = K(\sqrt{q_1},\dots,\sqrt{q_r}). \tag{2.6}$$

Lemma 27. *The field $\mathfrak{h}_R$ is a subfield of the ring class field H_R and the degree $[H_R:\mathfrak{h}_R]$ is odd. Moreover, $E(\mathfrak{h}_R)[2^\infty]=E(\mathbb{Q})[2]$.*

Proof. For $q\in\{q_1,\dots,q_r\}$ denote by H_q the ring class field of conductor q. Because q is inert in K, by class field theory we get that

$$[H_q:K]=(q+1)h,$$

where h is the class number of K. The prime q is congruent to 1 modulo 4 and by the choice of K in (2.2) the class number h is odd, therefore $ord_2([H_q:K])=1$. By Galois theory, H_q contains a unique quadratic extension of K. By basic proprieties of the ring class field, H_q is unramified at all primes outside of q, and since the unique quadratic extension of interest is a subfield of H_q, this will also be unramified outside of q.

Hence, the extension is $K(\sqrt{q^*})$ where $q^*=\left(\frac{-1}{q}\right)\cdot q$ and since $q\equiv 1 \pmod 4$ this is nothing else but $K\left(\sqrt{q}\right)$. By the tower law,

$$[H_R:K(\sqrt{q})]=\frac{[H_R:K]}{2}=\frac{(q+1)h}{2} \text{ which is odd.}$$

H_R is the compositum of $H_{q_1},\dots,H_{q_r}$, so by the above H_R contains $\mathfrak{h}_R$ and the index $[H_R:\mathfrak{h}_R]$ is odd.

Since $\mathfrak{h}_R=\mathbb{Q}\left(\sqrt{-l_0},\sqrt{q_1},\dots,\sqrt{q_r}\right)$, for any intermediary subfield $\mathfrak{h}_r\supseteq L\supsetneq\mathbb{Q}$ at least one of the primes $l_0,q_1,\dots,q_r$ ramifies in L. If $E(\mathfrak{h}_r)[2^\infty]\supsetneq E(\mathbb{Q})[2^\infty]$, we have

$$\mathfrak{h}_r\supseteq\mathbb{Q}(E(\mathfrak{h}_R)[2^\infty])\supsetneq\mathbb{Q}(E(\mathbb{Q})[2^\infty])=\mathbb{Q}$$

and hence there exists a prime $q\in\{l_0,q_1,\dots,q_r\}$ that ramifies in $\mathbb{Q}(E(\mathfrak{h}_R)[2^\infty])$ and in particular, ramifies in $\mathbb{Q}(E[2^\infty])$. But the primes that ramify in the field $\mathbb{Q}(E[2^\infty])$ divide $2C$, so we get a contradiction. This proves that $E(\mathfrak{h}_r)[2^\infty]=E(\mathbb{Q})[2^\infty]$.

Since E possesses a sensitive supersingular prime q_1, the previous remark (2.4) implies that $E(\mathbb{Q})[2^\infty]=E(\mathbb{Q})[2]$, proving the second assertion of the lemma. □

Lemma 28. *Let $\mathfrak{P}(\mathfrak{h}_R)$ be the set of conjugates of the point P_R under the action of the $Gal(H_R/\mathfrak{h}_R)$. Then we have the following equality of sets*

$$w_C\mathfrak{P}(\mathfrak{h}_R)=\tau\mathfrak{P}(\mathfrak{h}_R),\tag{2.7}$$

where w_C denotes the Fricke involution and τ denotes the complex conjugation.

Proof. Recall that $\mathfrak{C}\subset\mathscr{O}$ was defined such that $\mathscr{O}/\mathfrak{C}\simeq\mathbb{Z}/C\mathbb{Z}$. We use the well-known fact that

$$w_C(P_R)=(P_R)^{\sigma_{\mathfrak{C}}},$$

where $\sigma_{\mathfrak{C}}=\left(\frac{H_R/K}{\mathfrak{C}}\right)\in Gal(H_R/K)$ is the Artin symbol of $\mathfrak{C}$ for the extension H_R/K.

If q is a prime that divides R, then the restriction to $\mathbb{Q}\left(\sqrt{q}\right)$ of $\sigma_{\mathfrak{C}}$ is

$$\sigma_{\mathfrak{C}|\mathbb{Q}(\sqrt{q})}=\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{C}\right)$$

and because C is a square modulo q, the Artin symbol $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{C}\right)$ fixes $\sqrt{q}$. Moreover, $\sigma_{\mathfrak{C}}$ fixes $\mathbb{Q}\left(\sqrt{q_i}\right)$ for all $i\in\{1,\dots,r\}$, $\sigma_{\mathfrak{C}}=\sigma'\tau$, where $\sigma'\in Gal(H_R/\mathfrak{h}_R)$. Letting $\rho\in Gal(H_R/\mathfrak{h}_R)$ run through all the elements of the Galois group we get that

$$w_C(P_R^\rho)=(P_R)^{\rho\sigma'\tau},$$

and hence the equality of sets

$$w_C\mathfrak{P}(\mathfrak{h}_R)=\tau\mathfrak{P}(\mathfrak{h}_R).$$

□

Definition For each positive divisor D of R, let χ_D be the character attached to the extension $K(\sqrt{D})/K$, and define the imprimitive Heegner point z_D in $E(K(\sqrt{D}))$ by

$$z_D = \sum_{\sigma \in Gal(H_R/K)} \chi_D(\sigma) f(P_R)^\sigma. \tag{2.8}$$

In the case $D = R$, the formula above gives $z_R = y_R$, but for proper divisors D of R, we have the following lemma.

Lemma 29. *For all positive divisors D of R, define $b_D = \prod_{q|R/D} a_q$, where the product is taken over all primes q dividing R/D. We then have*

$$z_D = b_D y_D. \tag{2.9}$$

In particular, when q_1 does not divide D, since $a_{q_1} = 0$ we get that $b_D = z_D = 0$.

Proof. By Lemma 27, it follows that $K(\sqrt{D})$ is contained into the ring class field H_D. Kolyvagin observed the following general fact: if M is any positive integer prime to C and p a prime number with $(p, MC) = 1$ and p inert in K, then

$$\boxed{Tr_{H_{Mp}/H_M} f(P_{Mp}) = a_p f(P_M).}$$

If $q_i | R/D$ is fixed, then

$$b_D y_D = \prod_{q|R/D} a_q \sum_{\sigma \in Gal(H_D/K)} \chi_D(\sigma) f(P_D)^\sigma =$$

$$= \prod_{q|R/D, q \neq q_i} a_q \sum_{\sigma \in Gal(H_D/K)} \chi_D(\sigma) \sum_{\rho \in Gal(H_{Dq_i}/H_D)} f(P_{Dq_i})^{\rho\sigma} =$$

$$= \prod_{q|R/D, q \neq q_i} a_q \sum_{q \in Gal(H_{Dq_i}/K)} \chi_D(\sigma) f(P_{Dq_i})^\sigma$$

Repeating the same procedure for each prime q_i dividing R/D and changing the index of summation we get that

$$b_D y_D = \sum_{\sigma \in Gal(H_R/K)} \chi_D(\sigma) f(P_R)^\sigma = z_D.$$

□

We now return to the proof of the theorem. We saw in Theorem 11 that $T = f([0])$ is a torsion point. The order of T is in fact even, because if the order would be of the form $2k+1$, for $k \in \mathbb{Z}$ then

$$T = 2(-k \cdot T) \in 2E(\mathbb{Q}),$$

contradicts the hypothesis of our theorem. By composing if necessary f with multiplication by an odd integer on E, we can assume that the order of T is a power of 2. In fact, since E possesses a sensitive supersingular prime our assumption becomes that T has order exactly 2. Define

$$\psi_R = \sum_{\sigma \in Gal(H_R/\mathfrak{h}_R)} f(P_R)^\sigma.$$

Since E satisfies the hypothesis of Theorem 21, as we have seen in the proof of the aforementioned, $L(E,s)$ has root number $+1$. In particular $f \circ w_C + f$ is constant on $X_0(C)$ and hence

$$f(P^{w_C}) + f(P) = f([\infty]^{w_C}) + f([\infty]) = f([0]) + O = T, \text{ for all} P \in X_0(C).$$

Now, we can evaluate

$$\psi_R + \overline{\psi_R} = \sum_{\sigma \in Gal(H_R/\mathfrak{h}_R)} f(P_R)^\sigma + \sum_{\sigma \in Gal(H_R/\mathfrak{h}_R)} f(P_R)^{\sigma\tau},$$

where τ is the complex conjugation. By the result in Lemma 28, this is just

$$\psi_R + \overline{\psi_R} = \sum_{\sigma \in Gal(H_R/\mathfrak{h}_R)} f(P_R)^\sigma + f(P_r)^{\sigma w_C} = \#Gal(H_R/\mathfrak{h}_R) \cdot T.$$

Now, since T has order 2 and $[H_R/\mathfrak{h}_R]$ is odd by Lemma 27 we obtain

$$\psi_R + \overline{\psi_R} = T. \tag{2.10}$$

Let us start by presenting the proof for the particular case $r = 1$, i.e. $R = q_1$. If we denote by σ the non-trivial element in $Gal(K(\sqrt{q_1})/K)$, then

$$\psi_R - \sigma(\psi_R) = \sum_{\rho \in Gal(H_{q_1}/\mathfrak{h}_{q_1})} f(P_{q_1})^\rho - \sum_{\rho \in Gal(H_{q_1}/\mathfrak{h}_{q_1})} f(P_{q_1})^{\rho\sigma} = \sum_{\rho \in Gal(H_{q_1}/K)} \chi_{q_1}(\rho) f(P_{q_1})^\rho = y_R.$$

The prime q_1 is sensitive supersingular, so $a_{q_1} = 0$ and from (2.9) with $D = 1$ we get that

$$0 = z_1 = \sum_{\rho \in Gal(H_{q_1}/K)} f(P_{q_1})^{\rho} = \sum_{\rho \in Gal(H_{q_1}/\mathfrak{h}_{q_1})} f(P_{q_1})^{\rho} + \sum_{\rho \in Gal(H_{q_1}/\mathfrak{h}_{q_1})} f(P_{q_1})^{\rho\sigma} \Leftrightarrow$$

$$0 = z_1 = \psi_R + \sigma(\psi_R).$$

We deduced so far that $y_R = \psi_R - \sigma(\psi_R)$ and $0 = \psi_R + \sigma(\psi_R)$, so $y_R = 2\psi_R$. It follows from (2.10) and the fact that $2T = 0$ that $0 = T + T = y_R + \overline{y_R}$.

Observe that

$$y_R + \sigma(y_R) = \sum_{\rho \in Gal(H_{q_1}/K)} \chi_{q_1}(\rho) f(P_{q_1})^{\rho} + \sum_{\rho \in Gal(H_{q_1}/K)} \chi_{q_1}(\rho) f(P_{q_1})^{\rho\sigma} =$$

$$= \sum_{\rho \in Gal(H_{q_1}/K)} \chi_{q_1}(\rho) f(P_{q_1})^{\rho} - \sum_{\rho \in Gal(H_{q_1}/K)} \chi_{q_1}(\rho) f(P_{q_1})^{\rho} = 0,$$

because $\chi_{q_1}(\sigma) = -1$.

Putting together the fact that $\rho(y_R) = -y_R$ and $\overline{y_R} = -y_R$ we can deduce that the non-trivial element in $Gal\left(\mathbb{Q}\sqrt{-l_0 q_1}/\mathbb{Q}\right)$ maps y_R to $-y_R$, in other words $y_R \in E\left(\mathbb{Q}(\sqrt{-l_0 q_1})\right)^{-}$.

Suppose that $y_R = 2w + t$ for some $w \in E\left(\mathbb{Q}(\sqrt{-l_0 q_1})\right)^{-}$ and a torsion point t. It follows that $\psi_R = w + t'$, where $t' \in E\left(\mathbb{Q}(\sqrt{-l_0 q_1})\right)[2^{\infty}]$. We saw in Lemma 27 that

$$E(\mathbb{Q})[2] = E(\mathfrak{h}_R)[2^{\infty}] = E\left(\mathbb{Q}(\sqrt{-l_0 q_1})\right)[2^{\infty}]$$

and hence $t' \in E(\mathbb{Q})[2]$. This implies that

$$T = \psi_R + \overline{\psi_R} = 2w + t' - 2w + t' = 0$$

which contradicts (2.10) and hence proves the theorem in the case $r = 1$.

To deal with the case $r > 1$, notice at first that

$$y_R + \sum_{D|R, D \neq R} z_D = \sum_{\sigma \in Gal(H_R/K)} \chi_R(\sigma) f(P_R)^{\sigma} + \sum_{D|R, D \neq R} \sum_{\sigma \in Gal(H_R/K)} \chi_D(\sigma) f(P_D)^{\sigma} =$$

$$= \sum_{D|R} \left(\sum_{\sigma \in Gal(H_R/K)} \chi_D(\sigma) f(P_D)^{\sigma} \right) = \sum_{D|R} \left(\sum_{\sigma \in Gal(H_R/\mathfrak{h}_R)} f(P_R)^{\sigma} \right) = 2^r \psi_R$$

and therefore

$$y_R + \sum_{D|R, D\neq R} z_D = 2^r \psi_R. \tag{2.11}$$

When $D \neq R$, the product $b_D = \prod_{q|R/D} a_q$ contains at least one factor, therefore by condition (ii) in Lemma 23 we can write $b_D = 2^r e_D$ for some integer e_D. This implies that $y_R = 2^r u_R$, where $u_R = \psi_R - \sum_{D|R, D\neq R} e_D y_D$. As we previously remarked, if $q_1 \nmid D$, then b_D and in particular e_D is equal to 0.

In the natural map

$$E(K(\sqrt{R}))/2^r E(K(\sqrt{R})) \longrightarrow E(\mathfrak{h}_R)/2^r E(\mathfrak{h}_R)$$

$$y_R \longmapsto 0$$

the class of y_R maps to zero. We have the following inflation-restriction exact sequence

$$0 \longrightarrow H^1\left(Gal(\mathfrak{h}_R/K(\sqrt{R})), E(\mathfrak{h}_R)[2^r]\right) \xrightarrow{inf} H^1\left(K(\sqrt{r}), E[2^r]\right) \xrightarrow{res} H^1\left(\mathfrak{h}_R, E[2^r]\right)$$

where, since by Lemma 27 $E(\mathfrak{h}_R)[2^\infty] = E(\mathbb{Q})[2]$, the kernel on the left is annihilated by 2. It follows that $2y_R \in 2^r E(K(\sqrt{R}))$, so $2y_R = 2^r y$, for some $y \in E(K(\sqrt{R}))$, which implies that $2(y_R - 2^{r-1}y) = 0$ hence $y_R = 2^{r-1}y + t$ where $t \in E(K(\sqrt{R}))[2]) = E(\mathbb{Q})[2]$. Using the fact that $y_R = 2^r u_R$, we get that $y = 2u_R + s$, for some $s \in E(\mathbb{Q})[2]$.

To prove the desired assertion for y_R, we must show that $y \in E\left(\mathbb{Q}(\sqrt{-l_0 R})\right)^-$. Let σ be an element of $Gal(\mathfrak{h}_R/K)$ such that $\sigma(\sqrt{q_1}) = -\sqrt{q_1}$ and $\sigma(\sqrt{q_i}) = \sqrt{q_i}$ for all $2 \leq i \leq r$.

We will prove now that

$$\sigma(\psi_R) + \psi_R = 0 \text{ and } \sigma(y_D) + y_D = 0, \tag{2.12}$$

for all the positive proper divisors D of R that satisfy $e_D \neq 0$.

Notice that

$$\sigma(\psi_R) + \psi_R = \sum_{\rho \in Gal(H_R/\mathfrak{h}_R)} (f(P_R)^{\rho\sigma} + f(P_R)^{\rho}) = \sum_{\rho \in Gal(H_R/K(\sqrt{q_2}, \ldots, \sqrt{q_r}))} (f(P_R)^{\rho})$$

so

$$\sigma(\psi_R)+\psi_R = Tr_{H_R/K(\sqrt{q_2},\ldots,\sqrt{q_r})}\left(f(P_R)\right)=0.$$

The trace in the last term is 0, because by hypothesis $a_{q_1}=0$. To prove the second equality in (2.12), let us observe that if $e_D\neq 0$, then D is a positive divisor of R which is divisible by q_1 and thus the restriction of σ to $K(\sqrt{D})$ must be the non-trivial element of $Gal(K(\sqrt{D})/K)$. Then we have

$$y_D=\sum_{\rho\in Gal(H_D/K)}\chi_D(\rho)f(P_D)^{\rho}=\sum_{\rho\in Gal(H_D/K(\sqrt{D}))}f(P_D)^{\rho}-\sum_{\rho\in Gal(H_D/K(\sqrt{D}))}f(P_D)^{\rho\sigma}.$$

If we denote by $v_D=Tr_{H_D/K(\sqrt{D})}(f(P_D))$, the last equality can be written as $y_D=v_D-\sigma(v_D)$. We are in the case that q_1 divides D and $a_{q_1}=0$, so $v_D+\sigma(v_D)=0$. Now, one can see that $y_D=2v_D$ hence $\sigma(y_D)=2\sigma(v_D)=-2v_D=-y_D$.

Recall that $y=2u_R+s$ for $s\in E(\mathbb{Q})[2]$ and $u_R=\psi_R-\sum\limits_{D|R,D\neq R}e_Dy_D$. Using now the equalities in (2.12) we get

$$\sigma(y)=2\sigma(u_R)+s=\sigma(\psi_R)-\sum_{D|R,D\neq R}e_D\sigma(y_D)+s=-\psi_R+\sum_{D|R,D\neq R}e_Dy_D+s,$$

so

$$\sigma(y)+y=0. \tag{2.13}$$

For all proper divisors D of R such that $e_D\neq 0$, we have that $y_D=2v_D$. But for such D, $\overline{\psi_D}+\psi_D=T\in E(\mathbb{Q})[2]$, hence it follows that $2(\overline{v_D}+v_D)=0$, because $K(\sqrt{D})$ is a subfield of $\mathfrak{h}_D$. It is easy to see that in this case

$$\overline{y_D}+y_D=0, \tag{2.14}$$

so $\overline{u_R}+u_R=\overline{\psi_R}+\psi_R$ thus

$$\overline{y}+y=2(\overline{\psi_R}+\psi_R)=2T=0. \tag{2.15}$$

In view of the equalities (2.13) and , the non-trivial element of $Gal\left(\mathbb{Q}(\sqrt{-l_0R}),\mathbb{Q}\right)$ maps y to $-y$, so $y\in E\left(\mathbb{Q}(\sqrt{-l_0R})\right)^{-}$. Thus we proved that $y_R\in 2^{r-1}E\left(\mathbb{Q}(\sqrt{-l_0R})\right)^{-}+E(\mathbb{Q})[2]$.

Suppose now that $y_R\in 2^rE\left(\mathbb{Q}(\sqrt{-l_0R})\right)^{-}+E\left(\mathbb{Q}(\sqrt{-l_0R})\right)_{tor}$. We can write y_R as $y_R=2^ry'+t$, where $y'\in E\left(\mathbb{Q}(\sqrt{-l_0R})\right)^{-}$ and $t\in E\left(\mathbb{Q}(\sqrt{-l_0R})\right)_{tor}$. Let m be an odd integer number that annihilates the odd part of $E\left(\mathbb{Q}(\sqrt{-l_0R})\right)_{tor}$.

Then

$$m\left(\psi_R - y' - \sum_{D|R, D\neq R} e_D y_D\right) \in E(\mathfrak{h}_R)[2^\infty] = E(\mathbb{Q})[2],$$

but then $m(\overline{\psi_R} + \psi_R) = m \cdot T = 0$, which contradicts the fact that T has order 2. The proof is now complete.

3. The method of 2-Descents

For an elliptic curve E of conductor C, defined over $\mathbb{Q}$ with $L(E,1) \neq 0$, the theorem of Kolyvagin tells us that both $E(\mathbb{Q})$ and the Tate-Shafarevich group $Ш(E)$ are finite. Let Ω_E denote the least positive real period of a Néron differential on E. Since the regulator R_∞ is 1 in this case, we can use Theorem 31 in [3] to deduce that $L(E,1)/\Omega_E$ is a non-zero rational number. Let δ_E denote the number of connected components of $E(\mathbb{R})$, and for each prime q dividing C, let $c_q = [E(\mathbb{Q}_q) : E_0(\mathbb{Q}_q)]$, where $\mathbb{Q}_q$ is the q-adic completion of $\mathbb{Q}$ and $E_0(\mathbb{Q}_q)$ is the subgroup of points with non-singular reduction modulo q. Then, the full Birch-Swinnerton-Dyer conjecture asserts in this case that

$$\frac{L(E,1)}{\Omega_E} = \delta_E \prod_{q|C} c_q(E) \frac{\#(Ш(E))}{\#(E(\mathbb{Q}))^2}.$$

Even in this very special case, the full exact Birch-Swinnerton-Dyer formula is only known in a few isolated examples and in view of this, it is convenient to break the exact formula up into a p-part for all primes p. For a fixed prime number p, the quantity of the powers of p occurring on the two sides of the above is called the exact p-Birch-Swinnerton-Dyer formula.

Conjecture 30 (p-part of Birch-Swinnerton-Dyer)**.** *Assuming $r_E = 0$, we have, for all primes p,*

$$ord_p(L(E,1)) - ord_p(\Omega_E) - ord_p(\delta_E) = ord_p\left(\prod_{q|C} c_q(E)\right) - 2ord_p(\#(E(\mathbb{Q}))) + ord_p(\#(Ш(E))).$$

Considerable progress has been done on this p-part of the Birch-Swinnerton-Dyer conjecture using methods from Iwasawa theory.

Theorem 31 (Rubin [17])**.** *Assume that $L(E,1) \neq 0$ and that E has complex multiplication. Then the p-part of the Birch and 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, only a weaker result is known

Theorem 32 (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 includes $p = 2$.*

However, the methods of Iwasawa theory yield nothing at present for the 2-part of the exact formula, which is largely unknown. This has been verified numerically in a vast number of cases. The 2-part of the exact formula is very important for the following reasons. Firstly, when one looks at numerical data on L- values, one observes that the 2-part is most of what in [3] is denoted by

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

This is maybe because it seems that usually $Ш(E)$ is trivial or of very small order. The values of $L^{(alg)}$ for various twists of the curves $A = X_0(49)$ and $E = X_0(121)$ in the table below illustrate very well this behavior.

$A = X_0(49) : y^2 + xy = x^3 - x^2 - 2x - 1$			$E = X_0(121) : y^2 + y = x^3 - x^2 - 7x + 10$		
N	$L(A^{(N)},1)$	$L^{(alg)}(A^{(N)},1)$	N	$L(E^{(-N)},1)$	$L^{(alg)}(E^{(-N)},1)$
29	0.718...	2	7	1.094...	4
37	0.635...	2	43	0.441...	4
109	0.370...	2	79	0.325...	4
113	1.454...	8	83	0.317...	4
137	0.330...	2	107	0.279...	4
185	2.274...	16	119	0.530...	8
233	2.272...	18	127	1.0279...	16
265	4.275...	36	131	0.253...	4
277	0.929...	8	139	0.245...	4
281	0.230...	2	151	0.253...	4
285	1.813...	16	203	0.406...	8
317	0.868...	8	211	0.797...	16
337	0.210...	2	227	0.192...	4

The curve of conductor 49 in this table has a finite number of rational points and the one of conductor 121 an infinite number of rational points, because it has root number -1. The values used to generate the table were computed by Liang in [4] using MAGMA.

Secondly, in the first reference of this essay, the authors stress that a knowledge of the 2-part of the Birch-Swinnerton Dyer formula is vital for carrying out Tian's induction argument for quadratic twists, 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 $s = 1$.

3.1 Classical 2-Descents on twists of $X_0(49)$

For the rest of this essay, I am going to continue using the notations in the first reference, as A to be the modular curve $X_0(49)$, which has genus 1, and which we view as an elliptic curve by taking the cusp at $[\infty]$ to O, the origin of the group law. It is well known that A has complex multiplication by the ring of integers $\mathfrak{O} = \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ of the field $F = \mathbb{Q}(\sqrt{-7})$ and has a minimal Weierstrass equation given by

$$y^2 + xy = x^3 - x^2 - 2x - 1. \tag{3.1}$$

It is also known that $A(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and consists of cusps $[\infty]$ and $[0] = (2,-1)$. The discriminant of A is -7^3, the j-invariant is $j(A) = -3^3 5^3$ and its Néron differential has fundamental real period $\Omega_A = \frac{\Gamma(1/7)\Gamma(2/7)\Gamma(4/7)}{2\pi\sqrt{7}}$, and $A(\mathbb{R})$ has just one connected component, so $c_\infty(A) = \Omega_A$. [1]

A simple computation shows that $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(A[4]) = \mathbb{Q}(i, \sqrt[4]{-7})$. Writing $L(A,s)$ for the complex L-series of A, it is known that

$$L(A,1)^{(alg)} = \frac{L(A,1)}{c_\infty(A)} = \frac{1}{2}.$$

We have in this case that $R_\infty(A) = 1, c_7(A) = 2$ and $Ш(A)$ is trivial, so the conjecture of Birch and Swinnerton-Dyer is valid for A. However, the 2-part of the conjecture of Birch and Swinerton-Dyer is still unknown for arbitrary quadratic twists of A, even when the complex L-series of the twist does not vanish at $s = 1$. For a discriminant d, which is prime to 7, the curves $A^{(d)}$ and $A^{(-7d)}$ are isogenous over $\mathbb{Q}$. It can be then proved that the root number of $A^{(d)}$ is $+1$ if and only if $d > 0$ and is prime to 7, or $d < 0$ and is divisible by 7.

The easiest way to attack the 2-part of Birch and Swinnerton-Dyer conjecture for the quadratic twists of A should be by using the methods of Iwasawa theory, since every such twists has complex multiplication by F and has the prime 2 as a potentially good ordinary prime. But instead, the authors [1] use a classical 2- descent argument to successfully establish some partial results in this direction.

To carry out the 2-descent as in *Proposition X.4.9* of [19], we must work with a different Weierstrass model. After making the change of variables $x = X/4 + 2$, $y = Y/8 - X/8 - 1$ that moves the non-trivial torsion point to $(0,0)$ we obtain the following equation for A

$$Y^2 = X^3 + 21X^2 + 112X.$$

Let M be any square free integer $\neq 1$. Then, the twist of A by the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$ will have the equation

$$A^{(M)} : Y^2 = X^3 + 21MX^2 + 112M^2X,$$

and if we divide this curve by the subgroup generated by the point $(0,0)$ we obtain a new curve

$$A'^{(M)} : y^2 = X^3 - 42MX^2 - 7M^2X.$$

Notice that $A'^{(M)}$ is just the twist of

$$A' = A'^{(1)} : Y^2 - 42x^2 - 7x$$

by the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. As $-7 = 21^2 - 4 \cdot 112$ and $-42 = -2 \cdot 21$, we can write the isogenies between these two curves explicitly as

$$\phi : A^{(M)} \to A'^{(M)}, (x,y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(112M^2 - x^2)}{x^2} \right)$$

$$\hat{\phi} : A'^{(M)} \to A^{(M)}, (x,y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(-7M^2 - x^2)}{8x^2} \right).$$

Now let us give the following description for the Selmer groups of the dual isogenies ϕ and $\hat{\phi}$. Let V denote the set of all places of $\mathbb{Q}$, and let T_M be the set of primes dividing $14M$. Let $\mathbb{Q}(2,M)$ be the subgroup of $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ consisting of all elements with a representative which has even order at each prime not in T_M. If we write C_d for the homogeneous space of A given by

$$C_d : dw^2 = 64 - 7\left(\frac{M}{d} z^2 + 3 \right)^2,$$

then $S^{(\phi)}(A^{(M)})$ can be naturally identified with the subgroup of all d in $\mathbb{Q}(2,M)$ such that $C_d(\mathbb{Q}_v)$ is non-empty for $v = \infty$ and v dividing $14M$. Similarly, writing

$$C'_d : dw^2 = 1 + 7\left(\frac{2M}{d} z^2 + 3 \right)^2$$

then $S^{(\hat{\phi})}(A'^{(M)})$ can be naturally identified with the subgroup of all d in $\mathbb{Q}(2,M)$ such that $C'_d(\mathbb{Q}_v)$ is non-empty for $v = \infty$ and v dividing $14M$. There is an exact sequence

$$0 \longrightarrow A'^{(M)}/\phi(A^{(M)}(\mathbb{Q})) \xrightarrow{\delta} \mathbb{Q}(2,M) \longrightarrow WC(A^{(M)})[\phi] \ ,$$

where $\delta((0,0)) = -7$, so $-7 \in S^{(\phi)}(A^{(M)})$. Similarly, $7 \in S^{(\hat{\phi})}(A'^{(M)})$. The details of the above can be read in *Proposition X.4.9* of [19].

For convenience, the authors use the following notations. If D is any odd square free integer, define by D_+ to be the product of the primes dividing D which are $\equiv 1 \pmod 4$ and by D_-, the product of the primes dividing D which are $\equiv 3 \pmod 4$. In what follows, M is taken to be prime to 7 and the authors write

$$M = \varepsilon 2^{\delta} RN,$$

where $\varepsilon = \pm 1$, $\delta = 0, 1$, R denotes the product of the prime factors of M which are inert in $F = \mathbb{Q}(\sqrt{-7})$ and N denotes the product of the prime factors of M which are split in F. They also define a divisor d of M to be Confucian if it satisfies the following condition at primes p dividing N_+:

$$\left(\frac{d}{p}\right) = 1 \text{ when } p \text{ divides } \frac{N_+}{(d,N_+)}, \text{ and } \left(\frac{M/d}{p}\right) = \left(\frac{-7}{p}\right)_4 \text{ when } p \text{ divides } (d,N_+). \tag{3.2}$$

Proposition 33. *Let M be a square free integer prime to 7. Then $S^{(\phi)}(A^{(M)})$ consists of classes in $\mathbb{Q}(2,M)$ represented by all integers $d, -7d$ satisfying the following conditions:*

1. *d divides $2^{\delta} R_- N_+$.*
2. *When $M \equiv 1 \pmod 4$, we have $d \equiv 1 \pmod 4$, and when $M \equiv 3 \pmod 4$, we have $d \equiv 1 \pmod 8$.*
3. *When $M \equiv 6 \pmod 8$, we have $d \equiv 1 \pmod 8$, and when $M \equiv 2 \pmod 8$ we have either $d \equiv 1 \pmod 8$ or $d \equiv 5M \pmod{16}$.*
4. *We have $\left(\frac{d}{p}\right) = 1$ for all primes p dividing N_-.*
5. *d is a Confucian divisor of M.*

Proof. Recall that C_d denotes the curve $dw^2 = 64 - 7\left(\frac{M}{d}z^2 + 3\right)^2$. We see that $C_d(\mathbb{R}) \neq \emptyset$ and by Hensel's lemma $C_d(\mathbb{Q}_7) \neq \emptyset$ if and only if $\left(\frac{d}{7}\right) = 1$. The rest of the argument is split into different cases.

Suppose that q is a prime factor of R. In the first case, suppose that q divides d. If C_d contains a point (w,z) with coordinates in $\mathbb{Q}_q$, then $w, z \in \mathbb{Z}_q$ and then $\left(\frac{7}{q}\right) = 1$. Since

q is inert in F by definition, we have that $-1 = \left(\frac{-7}{q}\right) = \left(\frac{7}{q}\right)\left(\frac{-1}{q}\right) = \left(\frac{-1}{q}\right)$, so $q \equiv 3 \pmod 4$ and hence $q|R_-$. Conversely, if $q|R_-$, then using the fact that q is inert in F, we get that $\left(\frac{7}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{-7}{q}\right) = 1$, so we can choose $a \in \mathbb{Z}$ such that $a^2 \equiv 7 \pmod q$ therefore $9(a^2-7)-1 \equiv -1 \pmod q$ which can be written as $(-3a+8)(-3a-b) \equiv -1 \pmod q$. But as $q \equiv 3 \pmod 4$, we know that -1 is not a square modulo q, so one of $-3a+8$ and $-3a-8$ is a square and the other is a non-square modulo q. It follows that one of the two congruences $a\left(\frac{M}{d}z^2+3\right) \equiv \pm 8 \pmod q$ must always be soluble and so $7\left(\frac{M}{d}z^2+3\right)^2 \equiv 64 \pmod q$ is soluble, giving a point on C_d with coordinates in $\mathbb{Z}_q$. In the case $q|d$ we just proved that $C_d(\mathbb{Q}_q) \neq \emptyset$ if and only if q divides R_-. If q does not divide d, then we must consider the following two subcases. If $\left(\frac{d}{q}\right) = 1$, then reducing the equation for C_d modulo q, this becomes $dw^2 - 1 \equiv 0 \pmod q$. Since d is a quadratic residue modulo q, this equation is soluble and this way we obtain a point on C_d with coordinates in $\mathbb{Z}_q$. Otherwise, if $\left(\frac{d}{q}\right) = -1$, then since q is inert in F, $\left(\frac{-7d}{q}\right) = 1$. Now, with the substitution $w = q^{-1}w_1$, $z = q^{-1}z_1$, the equation for C_d becomes $dw_1^2 = 64q^2 - 7\left(\frac{M}{qd}z_1^2 + 3q\right)^2$, which, on taking $z_1 = 1$ is soluble modulo q giving rise to a point in $C_d(\mathbb{Q}_q)$. Therefore, we have just proved that if q is a prime factor of R that does not divide d, then $C_d(\mathbb{Q}_q) \neq \emptyset$.

Suppose that p is a prime divisor of N, and assume that p divides d. We are going to prove that

$$C_d(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow p \equiv 1 \pmod 4 \text{ and } \left(\frac{M/d}{p}\right) = \left(\frac{-7}{p}\right)_4. \tag{3.3}$$

To see this, observe that C_d has a point with coordinates in $\mathbb{Q}_p$ if and only if it has a point with coordinates in $\mathbb{Z}_p$ and this, by Hensel's lemma, is true if and only if the defining equation for C_d has a solution modulo p. Modulo p, the equation becomes

$$64 \equiv 7\left(\frac{M}{d}z^2+3\right)^2 \pmod p.$$

If the above is soluble modulo p, then 7 has to be a quadratic residue, i.e. $\left(\frac{7}{p}\right) = 1$ and since p splits in F, we have $1 = \left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{7}{p}\right) = \left(\frac{-1}{p}\right)$ and hence $p \equiv 1 \pmod 4$. Now, pick integers e and b such that $e^2 \equiv -7 \pmod p$ and $b^2 \equiv -1 \pmod p$. We have that $(b+1)^2 \equiv b^2+2b+1 \equiv 2b \pmod p$ and hence $\left(\frac{2b}{p}\right) = 1$ and $2b(3e-8b) \equiv 6be+16 \equiv 9+6eb+e^2b^2 \equiv (3+eb)^2 \pmod p$ which tells us that $\left(\frac{3e-8b}{p}\right) = 1$. Since $(3e-8b)(3e+8b) \equiv 1 \pmod p$, this means that $\left(\frac{3e+8b}{p}\right) = 1$. If we look at the equation of C_d, we observe that it will have a solution modulo p if and only if $-(8b)^2 \equiv -e^2\left(\frac{M}{d}z^2+3\right)^2 \pmod p$ is

soluble, so if one of the equations

$$\frac{M}{d}z^2e+3e\equiv\pm 8b \pmod{p} \text{ is soluble.}$$

The above equations are equivalent to

$$\frac{M}{d}z^2\equiv -e^{-1}(3e\mp 8b) \pmod{p}.$$

Since both $-(3e+8b)$ and $-(3e-8b)$ are quadratic residues modulo p, one of the above equations has solution mod p if and only if $\left(\frac{M}{d}\right)=\left(\frac{e^{-1}}{p}\right)=\left(\frac{e}{p}\right)=\left(\frac{-7}{p}\right)_4$ which completes the proof of the claim in (3.3). Assume now that p does not divide d. We will prove that in this case

$$C_d(\mathbb{Q}_p)\neq\emptyset\Leftrightarrow\left(\frac{d}{p}\right)=1. \tag{3.4}$$

If $\left(\frac{d}{p}\right)=1$ then the equation obtained by putting $z=0$ is $dw^2\equiv 1 \pmod{p}$, which is soluble since d is a quadratic residue modulo p. This gives a point with coordinates in $\mathbb{Z}_p$. To prove the converse, if C_d has a point with coordinates in $\mathbb{Z}_p$, then $dw^2\equiv 64-7\left(\frac{M}{d}z^2+3\right)^2 \pmod{p}$ is in particular soluble. But since $p|\frac{M}{d}$, this means that $dw^2\equiv 1 \pmod{p}$ is soluble and hence $\left(\frac{d}{p}\right)=1$ as desired. If there is a point (w,z) on the homogeneous space C_d with coordinates in $\mathbb{Q}_p\setminus\mathbb{Z}_p$ then we can write $w=p^{-m}w_1$ and $z=p^{-n}z_1$, where $m,n>0$ and $w_1,z_1\in\mathbb{Z}_p^\times$. It then follows that $m=2n-1$ and we can rewrite the defining equation for C_d as $dw_1^2=64p^{2m}-7\left(\frac{M}{pd}z_1^2+3p^m\right)^2$. Now if we consider this new equation modulo p, since p is split in F we see that $\left(\frac{d}{p}\right)=\left(\frac{-7}{p}\right)=1$, completing the proof of claim (3.4).

We have not discussed the prime 2, so let us now focus when $C_d(\mathbb{Q}_2)\neq\emptyset$. We claim that

$$C_d(\mathbb{Q}_2)\neq\emptyset\Leftrightarrow\begin{cases} d/2\equiv 1 \pmod 4 \text{ and } \frac{M}{d}\equiv 5 \pmod 8, \text{ if } d \text{ is even}\\ d\equiv 1 \pmod 8 \text{ or } d\equiv 5 \pmod 8 \text{ and } M/d\equiv 1 \pmod 4, \text{ if } d \text{ is odd.}\end{cases} \tag{3.5}$$

To prove the claim, assume first that d is even. Then if C_d contains a point with (w,z) with coordinates in $\mathbb{Q}_2$, then in fact $w\in\mathbb{Z}_2$ and $z\in\mathbb{Z}_2^\times$ and M is even. Then $\frac{M}{d}z^2+3\equiv 8 \pmod{16}$ and therefore

$$d\left(\frac{w}{8}\right)^2=1-7\left(\frac{\frac{M}{d}z^2+3}{8}\right)^2\equiv 2 \pmod 8. \tag{3.6}$$

If this is soluble, then we must have $d/2\equiv 1 \pmod 4$. To see this, notice that if $d/2\equiv 3 \pmod 4$, then $d\equiv 6 \pmod 8$ and the equation $6\left(\frac{w}{8}\right)^2-2\equiv \pmod 8$ must be soluble. But

this means that $3\left(\frac{w}{8}\right)^2 - 1 \equiv 0 \pmod 4$ is soluble, which is a contradiction since $\left(\frac{3}{4}\right) = -1$. By looking at the possible quadratic residues in $(\mathbb{Z}/16\mathbb{Z})^\times$ we obtain that $\frac{M}{d} \equiv 5 \pmod 8$. Conversely, if $d/2 \equiv 1 \pmod 4$ and $M/d \equiv 5 \pmod 8$ then the congruence (3.6) is soluble since $z^2 \equiv c \pmod{64}$ is soluble for any $c \equiv 1 \pmod 8$. This gives rise to a point on C_d with coordinates in $\mathbb{Q}_2$, i.e. $C_d(\mathbb{Q}_2) \neq 0$.

Suppose that d is odd. In this case $d \equiv 1 \pmod 8$, we will show that $C_d(\mathbb{Q}_2)$ is always non-empty. Indeed, taking the equation for C_d modulo 8, and plugging in $z = 0$ we get $dw^2 \equiv 1 \pmod 8$, which clearly has a solution, because $d \equiv 1 \pmod 8$ is a quadratic residue. This gives a point on C_d with coordinates in $\mathbb{Q}_2$ and therefore proves our claim. If $d \not\equiv 1 \pmod 8$, then suppose C_d contains a point with one of the coordinates in $\mathbb{Q}_p \setminus \mathbb{Z}_p$. Then we can put $w = 2^m w_1$, $z = 2^{-n} z_1$ with $m, n > 0$ and $w_1, z_1 \in \mathbb{Z}_2^\times$. Let $M = 2^\delta M_1$, where M_1 is odd. The defining equation for C_d becomes

$$2^{-2m} d w_1^2 = 2^6 - 7\left(\frac{M_1}{d} 2^{\delta - 2n} z_1^2 + 3\right)^2.$$

Therefore, $m = 2n - \delta$ and we must have that $d \equiv 1 \pmod 8$, which is a contradiction. So if $C_d(\mathbb{Q}_2) \neq \emptyset$, then $C_d(\mathbb{Q}_2) = C_d(\mathbb{Z}_2)$. Now, observe that if we set $w = 0$ then the equation $64 = 7\left(\frac{M}{d} z^2 + 3\right)^2$ does not have a solution in $\mathbb{Z}_2$, because 7 is not a quadratic residue modulo 128 for example. If we set $z = 0$, the equation $dw^2 = 1$ does not have a solution in $\mathbb{Z}_2$, because the congruence $dw^2 \equiv \pmod 8$ does not have a solution when $d \not\equiv 1 \pmod 8$. Hence if (w, z) is a point on C_d with coordinates in $\mathbb{Z}_2$, then $wz \neq 0$ and we can put $w = 2^m w_1$ and $z = 2^n z_1$ for some $w_1, z_1 \in \mathbb{Z}_2^\times$ and $m, n \geq 0$. The defining equation for C_d becomes

$$2^{2m} d w_1^2 = 2^6 - 7\left(\frac{M_1}{d} 2^{\delta + 2n} z_1^2 + 3\right)^2.$$

Observe that if $\delta + 2n > 0$, then the RHS of the above has 2-adic absolute value 1 and hence $2m = 0$ implying that $dw_1^2 = 2^6 - 7\left(\frac{M_1}{d} 2^{\delta+2n} z_1^2 + 3\right)^2$. But if this last equation admits a solution in $\mathbb{Z}_2$, then in articular the congruence $dw^2 = 1 \pmod 8$ has a solution, which gives the contradiction $d \equiv 1 \pmod 8$. So $\delta = n = 0$ and the equation is

$$d w_1^2 = \frac{2^6 - 7\left(\frac{M}{d} z_1^2 + 3\right)^2}{2^{2m}}.$$

Now observe that if $M/d \equiv 3 \pmod 4$, then comparing powers of 2 we must have $m = 1$ and then looking modulo 4 we get the contradiction $d \equiv 1 \pmod 8$. So $M/d \equiv 1 \pmod 4$.

Now, if $M/d \equiv 1 \pmod 8$, comparing powers of 2, we must have $m = 2$ so

$$dw_1^2 = 4 - 7\frac{\left(\frac{M}{d}z^2+3\right)^2}{16} \equiv 5 \pmod 8,$$

which gives a contradiction. If $M/d \equiv 5 \pmod 8$ then choose z such that $ord_2\left(\frac{M}{d}z^2+3\right) = 4$, so $m = 3$ this giving $d \equiv 5 \pmod 8$. Conversely if $d \equiv 5 \pmod 8$ and $m = 3$ we can find a point on C_d with coordinates in $\mathbb{Q}_2$. Taking into account the characterization we previously gave for the Selmer group $S^{(\phi)}(A^{(M)})$, it is clear that the proof of the proposition is complete. □

A trivial corollary of this proposition is the following

Corollary 34. *Assume that M is a square free integer, prime to 7, with $M \equiv 1 \pmod 4$. Then $S^{(\phi)}(A^{(M)})$ consists of the classes in $\mathbb{Q}(2,M)$ represented by integers $d, -7d$, where d runs over all integers such that (i) $d \equiv 1 \pmod 4$, (ii) d divides R_-N_+, (iii) $\left(\frac{d}{p}\right) = 1$ for all primes p dividing N_- and (iv) d is a Confucian divisor of M.*

In a similar fashion, the authors of the first reference manage to describe $S^{(\hat{\phi})}(A'^{(M)})$. Since the proof is similar to the one I presented, I am just going to state the analogous proposition and corollary.

Proposition 35. *Let M be a square free integer prime to 7. Then $S^{(\hat{\phi})}(A'^{(M)})$ consists of all classes in $\mathbb{Q}(2,M)$ represented by integers $d, 7d$ satisfying*

1. *$d > 0$ and d divides $2N$.*
2. *If $M \equiv 1 \pmod 4$, then d is odd, and if $M \equiv 2 \pmod 8$, we have either $d \equiv \pm 1 \pmod 8$ or $d \equiv \pm 3M \pmod{16}$.*
3. *$\left(\frac{d}{1}\right) = 1$ for all primes q dividing R_-.*
4. *d is a Confucian divisor of M.*

The analogous corollary for this proposition is

Corollary 36. *Assume that M is a square free integer prime to 7, with $M \equiv 1 \pmod 4$. Then $S^{(\hat{\phi})}(A'^{(M)})$ consists of all classes in $\mathbb{Q}(2,M)$ represented by integers $d, 7d$ where d runs over all integers satisfying (i) $d > 0$, (ii) d divides N, (iii) $\left(\frac{d}{q}\right) = 1$ for all primes q dividing R_- and (iv) d is a Confucian divisor of M.*

Let us present some consequences of the last two propositions. We assume in what follows that M is a square free integer, prime to 7, with $M \equiv 1 \pmod 4$. As previously, we write $M = \varepsilon RN$, where R (respectively N) denotes the product of prime factors of M which are inert (respectively split) in F. The curve $A^{(M)}$ has good reduction at 2. We also know that its L function has root number $+1$, if $M > 0$ respectively -1 if $M < 0$. If we denote by $S^{(2)}(A^{(M)})$ for the Selmer group of $A^{(M)}$ with respect to the multiplication by 2 endomorphism, we have the following exact sequence

$$0 \longrightarrow A'^{(M)}[\hat{\phi}] \longrightarrow S^{(\phi)}(A^{(M)}) \longrightarrow S^{(2)}(A^{(M)}) \longrightarrow S^{(\hat{\phi})}(A'^{(M)}) \tag{3.7}$$

Now we are going to denote by

$$\mathfrak{S}^{(\phi)}(A^{(M)}) = S^{(\phi)}(A^{(M)})/Im(A'^{(M)}(\mathbb{Q})_{tor})$$

and by

$$\mathfrak{S}^{(2)}(A^{(M)}) = S^{(2)}(A^{(M)})/Im(A^{(M)}(\mathbb{Q})_{tor}).$$

Notice that we mentioned this object before in Lemma 7 and in Corollary 16 without using this new notation for it. Both of the curves $A^{(M)}$ and $A'^{(M)}$ have good reduction at 2 and by the theory of complex multiplication one can prove that the 2- primary subgroups $A^{(M)}(\mathbb{Q})(2)$ and $A'^{(M)}(\mathbb{Q})(2)$ have both order 2. This gives rise to the following exact sequence

$$0 \longrightarrow \mathfrak{S}^{(\phi)}(A^{(M)}) \longrightarrow \mathfrak{S}^{(2)}(A^{(M)}) \longrightarrow S^{(\hat{\phi})}(A'^{(M)}). \tag{3.8}$$

The corollary to the Weak Parity Theorem, stated previously in this essay shows that the $\mathbb{F}_2$ dimension of $\mathfrak{S}^{(2)}(A^{(M)})$ is even if and only if $A^{(M)}$ has root number 1, which holds if and only if $M > 0$.

Corollary 37. *If $M = R_+$, then $\mathfrak{S}^{(2)}(A^{(M)}) = 0$.*

Proof. For this particular choice of M, corollary 34 tells us that $S^{(\phi)}(A^{(M)})$ consists of just two elements, and now considering the observation we have made about the 2-primary part of $A^{(M)}(\mathbb{Q})$, we see that the quotient $\mathfrak{S}^{(\phi)}(A^{(M)})$ is trivial. Similarly, corollary 36 tells us that the Selmer group $\mathfrak{S}^{(\hat{\phi})}(A'^{(M)})$ consists of just two elements. $M > 0$ so the root number of $A^{(M)}$ is 1 and hence $\mathfrak{S}^{(2)}(A^{(M)})$ has even $\mathbb{F}_2$ dimension. Using the above information in the exact sequence (3.8) completes the proof. □

Corollary 38. *Assume that $M = R$ with $M \equiv 1 \pmod 4$ and denote by $r_-(M)$ the number of prime factors of R_-. Then $\mathfrak{S}^{(2)}(A^{(M)})$ has exact order equal to $2^{r_-(M)}$.*

Proof. Again, we are making use of corollaries 34 and 36. The former us that $S^{(\phi)}(A^{(M)})$ can be represented by pairs of classes $d, -7d$ of $\mathbb{Q}(2,M)$ such that $d \equiv 1 \pmod 4$ and $d|R_-$. Therefore, d must contain an even number of prime factors of R_-. But since there is a bijection between the divisors of R_- that contain an odd number of primes and the ones that contain an even number of primes, there are $2^{r_-(M)-1}$ such choices for d. Each d comes in pair with another $-7d$, so $\#\left(S^{(\phi)}(A^{(M)})\right) = 2^{r_-(M)}$ and in the view of the observation about the 2-primary part, $\#\left(Ш^{(\phi)}(A^{(M)})\right) = 2^{r_-(M)-1}$. Looking at the later of the mentioned corollaries, we get that $S^{(\hat{\phi})}(A'^{(M)})$ has order 2. Therefore, using the exact sequence (3.8) we see that $Ш^{(2)}(A^{(M)})$ has order $2^{r_-(M)-1}$ or $2^{r_-(M)}$. Since $A^{(M)}$ has root number 1, $Ш^{(2)}(A^{(M)})$ must have even $\mathbb{F}_2$ dimension and therefore order $2^{r_-(M)}$. □

Corollary 39. *Assume that $M = R_+N_-$ with $M \equiv 1 \pmod 4$, and let $k_-(M)$ denote the number of prime factors of N_-. Then $Ш^{(\hat{\phi})}(A'^{(M)})$ has exact order $2^{k_-(M)}$ and $Ш^{(2)}(A'^{(M)})$ has order at least equal to $2^{k_-(M)}$.*

Proof. There is the following exact sequence, analogue to (3.8) for $A'^{(M)}$:

$$0 \longrightarrow Ш^{(\hat{\phi})}(A'^{(M)}) \longrightarrow Ш^{(2)}(A'^{(M)}) \longrightarrow S^{(\phi)}(A^{(M)}) \ .$$

Using corollary 36 one can deduce that $S^{(\hat{\phi})}(A'^{(M)})$ can be represented as pairs $d, 7d$ of classes of $\mathbb{Q}(2,M)$ such that $d|N_-$. Therefore, $S^{(\hat{\phi})}(A'^{(M)})$ has $2^{k_-(M)+1}$ elements so $\#\left(Ш^{(\hat{\phi})}(A'^{(M)})\right) = 2^{k_-(M)}$ and the second assertion of this corollary follows immediately from the exact sequence above. □

Corollary 40. *Assume that $M = RN_+$, where $M \equiv 1 \pmod 4$ and $N_+ > 1$. Assume further that every prime factor of N_+ splits completely in the field $\mathbb{Q}(i, \sqrt[4]{-7}, \sqrt{R})$. Then $Ш^{(2)}(A^{(M)}) \neq 0$.*

Proof. Under this hypothesis, for every prime factor of N_+, we have that $\left(\frac{R}{p}\right) = \left(\frac{-7}{p}\right)_4$ and hence N_+ is Confucian. Therefore, since N_+ is also congruent to $1 \pmod 4$, we see that $N_+ \in S^{(\phi)}(A^{(M)})$ and since $N_+ > 1$ we have that N_+ can be identified in $Ш^{(2)}(A^{(M)})$ with a non-trivial element. □

Corollary 41. *Assume that $M = -l_0R_+N_+$, where l_0 is a prime such that $l_0 \equiv 3 \pmod 4$ and l_0 is inert in F. Assume further that every prime factor of N_+ splits completely in the field obtained by adjoining to $\mathbb{Q}(i, \sqrt[4]{-7})$ the square roots of all primes dividing R_+. Then $Ш^{(2)}(A^{(M)})$ has order 2 if and only if the ideal class group of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{-l_0N_+}\right)$ has no element of exact order 4.*

Proof. Let $V := -l_0 N_+$. Since $M \equiv 1 \pmod 4$, we are using again corollary 34 to detect elements of the Selmer group $S^{(\phi)}(A^{(M)})$. Observe that the hypothesis that every factor of N_+ splits completely in that specified field tells us that V is Confucian. This, together with the fact that $V \equiv 1 \pmod 4$ gives that $\{V, -7V\} \subset S^{(\phi)}(A^{(M)})$. Using corollary 36, we see that $S^{(\hat{\phi})}(A^{'(M)}) = \{1, 7\}$.

Now, we are turning back to our exact sequence (3.8)

$$0 \longrightarrow \text{Ш}^{(\phi)}(A^{(M)}) \longrightarrow \text{Ш}^{(2)}(A^{(M)}) \longrightarrow S^{(\hat{\phi})}(A^{'(M)}) \ .$$

We know that $S^{(\phi)}(A^{(M)})$ has at least four elements, namely $1, -7, V, -7V$ and therefore $\#\left(\text{Ш}^{(\phi)}(A^{(M)})\right)$ is at least 2. We claim that $\text{Ш}^{(2)}(A^{(M)})$ has order 2 if and only if $\text{Ш}^{(\phi)}(A^{(M)})$ has order 2. Indeed, if $\text{Ш}^{(\phi)}(A^{(M)})$ has order 2, then by the exact sequence above $\text{Ш}^{(2)}(A^{(M)})$ must have order 2 or 4. But since $M < 0$ in this case, the corollary of the Dokchitser brothers theorem implies that $\text{Ш}^{(2)}(A^{(M)})$ has odd $\mathbb{F}_2$ dimension, therefore $\text{Ш}^{(2)}(A^{(M)})$ must have order 2. Conversely, if $\#\left(\text{Ш}^{(2)}(A^{(M)})\right) = 2$, then since $\text{Ш}^{(\phi)}(A^{(M)})$ injects into $\text{Ш}^{(2)}(A^{(M)})$, we must have $\#\left(\text{Ш}^{(\phi)}(A^{(M)})\right) \leq 2$ but since we saw that $\text{Ш}^{(\phi)}(A^{(M)})$ has at least 2 elements, the claim is now completely proved.

We established that $\text{Ш}^{(2)}(A^{(M)})$ has order 2 if and only if $\text{Ш}^{(\phi)}(A^{(M)})$ has order 2 and the later is equivalent to $S^{(\phi)}(A^{(M)}) = \{1, -7, V, -7V\}$. In other words, using corollary 34 again we are left to show that there is no divisor d of V, except 1 and V, such that $d \equiv 1 \pmod 4$ and d is Confucian. The authors of the first reference finish this argument by observing that this last assertion by the theory of genra, interpreted via the Rédei matrix, is equivalent to the fact that $\mathbb{Q}\left(\sqrt{V}\right)$ has no element of order 4 in its ideal class group.

□

If we want to understand the 2-part of the Birch and Swinnerton-Dyer conjecture, in particular to compare the 2-descent arguments presented above with the predictions from the conjecture, we need to have a knowledge about the Tamagawa factors of the curves $A^{(M)}$ and $A^{'(M)}$. We quickly recall that for an elliptic curve E over the rationals and a prime p, the Tamagawa factor $c_p(E)$ is defined as follows $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$, where where $\mathbb{Q}_p$ is the p-adic completion of $\mathbb{Q}$ and $E_0(\mathbb{Q}_p)$ is the subgroup of points with non-singular reduction modulo p. We assume in what follows that M is an arbitrary square free integer prime to 7 and we write D_M for the discriminant of the quadratic field $\mathbb{Q}(\sqrt{M})$. Both of the curves $A^{(M)}$ and $A^{'(M)}$ have bad additive reduction at all primes dividing $7D_M$. If we write $c_p(A^{(M)})$ for the Tamagawa factor of $A^{(M)}$ and similarly for $A^{'(M)}$ we have that for every odd prime p of

bad additive reduction,

$$c_p(A^{(M)}) = \#\left(A\left(\mathbb{Q}_p\right)[2]\right) \text{ and } c_p(A'^{(M)}) = \#\left(A'(\mathbb{Q}_p)[2]\right).$$

It can be checked via an easy computation that $F = \mathbb{Q}(A[2])$ and if we denote by $F' = \mathbb{Q}(\sqrt{7})$ we have that $F' = \mathbb{Q}(A'[2])$. In what follows, we are going to give the Tamagawa factors for the curves in discussion with a brief indication of the proofs, as in the first reference.

Proposition 42. *For all square free integers M, we have (i) $A^{(M)}(\mathbb{R})$ has one connected component, (ii) $c_2(A^{(M)})$ is equal to 1 or 4, according as D_M is odd or even, (iii) $c_7(A^{(M)}) = 2$, (iv) $c_p(A^{(M)}) = 2$ for every odd prime dividing M, which is inert in F, and (v) $c_p(A^{(M)}) = 4$ if p is an odd prime dividing M which is split in F.*

Proof. We have seen that $F = \mathbb{Q}(A[2])$. As a Galois module, the 2-torsion does not change under quadratic twists, therefore the 2-torsion points of $A^{(M)}(\mathbb{R})$ are not all real. This implies that $A^{(M)}(\mathbb{R})$ has one connected component. The second assertion can be proved using Tate's algorithm when the discriminant D_M is even. Now, for odd primes p of bad reduction we have

$$c_p(A^{(M)}) = \#(A(\mathbb{Q}_p)[2]) = \begin{cases} 2, \text{ if } p \text{ is inert in } F \\ 4, \text{ if } p \text{ is split in } F \end{cases}.$$

□

With a completely analogous proof, the authors establish the following analogue for $A'^{(M)}$. Notice that in this case, since the 2-torsion points of A', and hence of $A'^{(M)}$ are real, $A'^{(M)}(\mathbb{R})$ has two connected components.

Proposition 43. *For all square free integers M, we have (i) $A'^{(M)}(\mathbb{R})$ has two connected components, (ii) $c_2(A'^{(M)})$ is equal to 1 if D_M is odd, to 2 if $ord_2(D_M) = 2$, to 2 if $8|D_M$ and $M/2 \equiv 3 \pmod 4$ and to 4 if $8|D_M$ and $M/2 \equiv 1 \pmod 4$, (iii) $c_7(A'^{(M)}) = 2$, (iv) if p is an odd prime dividing M, which is inert in F, then $c_p(A'^{(M)})$ is equal to 2 or 4 according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$, and (v) if p is an odd prime dividing M, which splits in F, then $c_p(A'^{(M)})$ is equal to 2 or 4 according as $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 4$.*

It is an easy exercise to show that isogenous elliptic curves have the same number of points modulo p for all primes p (see Exercise 5.4 in [19]) and, since the factors for primes of bad reduction also agree, they have the same L-series. Consequently, if the full Birch and Swinnerton-Dyer conjecture is true, then, using the same notations as in the statement of

Conjecture 19, the quantity

$$c_\infty \frac{|Ш(E)| \cdot R_\infty(E)}{|E(\mathbb{Q})_{tor}|^2} \cdot \prod_{p|C(E)} c_p(E)$$

remains invariant under isogeny. This is what the authors mean when they write that the Birch and Swinnerton-Dyer conjecture is known to be compatible with isogenies. This was first proved by Cassels and extended to abelian varieties by Tate, in both cases using the assumption that Ш is finite. It is interesting to point out that none of the individual terms in the product above need to be the same for isogenous curves.

It is possible now to determine the explicit relationship between the orders of the Tate-Shafarevich groups of $A^{(M)}$ and $A'^{(M)}$, which follows from the above compatibility. Assume that M is a square free integer, written $M = \varepsilon 2^\delta RN$, exactly as before. We write $r_-(M)$ for the number of prime factors of R_- as in corollary 38 and $k_-(M)$ for the number of prime factors of N_- as in corollary 39. We define by $g(M) = rank_{\mathbb{Z}} A^{(M)}(\mathbb{Q}) = rank_{\mathbb{Z}} A'^{(M)}(\mathbb{Q})$.

Let $\rho(M)$ be defined by

$$\rho(M) = ord_2 \left([A'^{(M)}(\mathbb{Q}) : \phi(A^{(M)}(\mathbb{Q})) + A'^{(M)}(\mathbb{Q})_{tor}] \right).$$

Remark that $\rho(M) \leq g(M)$.

Define $a(M)$ to be 1 if $N_-R_- \equiv -sign(M) \pmod 4$, respectively 0 if $N_-R_- \equiv sign(M) \pmod 4$. We write $Ш(A^{(M)})$ and $Ш(A'^{(M)})$ for the Tate-Shafarevich groups of $A^{(M)}$ and $A'^{(M)}$ respectively, viewed as elliptic curves over $\mathbb{Q}$.

Proposition 44. *Let M be a square free integer prime to 7. Then $Ш(A^{(M)})$ and $Ш(A'^{(M)})$ are either both infinite or both finite, and in the latter case we have*

$$\frac{\#\left(Ш(A'^{(M)})\right)}{\#\left(Ш(A^{(M)})\right)} = 2^{a(M)+k_-(M)-r_-(M)+2\rho(M)-g(M)}.$$

Proof. Denote by $\Omega_\infty(A^{(M)})$ the integral of a Néron differential over $A^{(M)}(\mathbb{R})$ and by $\Omega_\infty(A'^{(M)})$ the analogous quantity over $A'^{(M)}(\mathbb{R})$. The behavior of the Tate-Shafarevich group under isogenies is well known, as it is part of Tate's proof of the fact that the Birch and Swinnerton-Dyer conjecture is invariant under isogeny. In particular, this implies the first assertion of the proposition, i.e. if one of the Tate-Shafarevich groups is finite, then the other is finite as well.

If we assume the finiteness of this groups, and for brevity denote by $Tam(A^{(M)}) = \prod_p c_p(A^{(M)})$ and by $Tam(A'^{(M)}) = \prod_p c_p(A'^{(M)})$ where in both cases the product is taken over the primes dividing the conductor of the curve, then we have the equality

$$\frac{Tam(A^{(M)})\Omega_\infty(A^{(M)})R(A^{(M)})\#\left(Ш(A^{(M)})\right)}{\#\left(A^{(M)}(\mathbb{Q})_{tor}\right)^2}=\frac{Tam(A^{'(M)})\Omega_\infty(A^{'(M)})R(A^{'(M)})\#\left(Ш(A^{'(M)})\right)}{\#\left(A^{'(M)}(\mathbb{Q})_{tor}\right)^2}.$$

The regulator terms represent just volumes with respect to the canonical height (or Néron-Tate) bilinear pairing and we can compute

$$R(A^{'(M)})=Vol\left(A^{'(M)}(\mathbb{Q})\right)^2=Vol\left(\phi\left(A^{(M)}(\mathbb{Q})\right)\right)^2\cdot 2^{-2\rho(M)}.$$

But $Vol\left(\phi\left(A^{(M)}(\mathbb{Q})\right)\right)=2^{g(M)}Vol\left(A^{(M)}(\mathbb{Q})\right)^2=2^{g(M)}R(A^{(M)})$ and plugging this in the above equality, we can derive the ratio of the two regulators as being

$$\frac{R(A^{(M)})}{R(A^{'(M)})}=2^{2\rho(M)-g(M)}.$$

Now we are going to make use of propositions 42 and 43 to compute the ratio between $Tam(A^{(M)})$ and $Tam(A^{'(M)})$. The Tamagawa factors corresponding to 7 are the same for both curves, so they will cancel in the ratio. For each prime factor of R (inert in F) we have that $c_p(A^{'(M)})=c_p(A^{(M)})=2$ if p divides R_+, and respectively $c_p(A^{'(M)})=2c_p(A^{(M)})=4$ if p divides R_-. Similarly, for each prime factor of N (split in F), we have $c_p(A^{'(M)})=2^{-1}c_p(A^{(M)})=2$ if p divides N_- and $c_p(A^{'(M)})=c_p(A^{'(M)})=4$ if p divides N_+. By definition of $a(M)$, the factor $2^{a(M)}$ represents the ratio $c_2(A^{(M)})/c_2(A^{'(M)})$.

The above can be summarized in

$$\frac{Tam(A^{(M)})}{Tam(A^{'(M)})}=2^{a(M)+k_-(M)-r_-(M)}.$$

We know that the torsion groups $A^{(M)}(\mathbb{Q})_{tor}$ and $A^{'(M)}(\mathbb{Q})_{tor}$ are both isomorphic to $\mathbb{Z}/2\mathbb{Z}$, so the only ratio that we need in order to complete the proof of this proposition is the one between $\Omega_\infty(A^{(M)})$ and $\Omega_\infty(A^{'(M)})$.

Following the notation used by the authors, let $\omega(A)$ be the least positive real period and $\omega^-(A)$ be the least purely imaginary period in the upper half plane of the Néron differential on A. Denote also by $\omega(A')$ and $\omega^-(A')$ the analogue quantities for A'. In the paper [16], Vivek Pal provides formulas for the relation between the period of an elliptic curve and the period of its real and imaginary quadratic twists. The authors of [1] derived from the main

result of Pal's paper that

$$\Omega_\infty(A^{(M)}) = \begin{cases} \frac{u}{\sqrt{M}}\omega(A), \text{ if } M>0, \\ \frac{u}{\sqrt{M}}\omega^-(A), \text{ if } M<0, \end{cases} \quad \text{and } \Omega_\infty(A'^{(M)}) = \begin{cases} \frac{u}{M}2\omega(A'), \text{ if } M>0, \\ \frac{u}{\sqrt{M}}2\omega^-(A), \text{ if } M<0, \end{cases}$$

where $u=1$ if $d \equiv 1 \pmod 4$ and $u=1/2$ otherwise. Hence $\frac{\Omega_\infty(A^{(M)})}{\Omega_\infty(A'^{(M)})}=1$ since $\omega(A)=2\omega(A')$ and respectively $\omega^-(A)=2\omega^-(A')$. Now we can start plugging in the quantities we know, to get

$$\frac{\#\left(Ш(A'^{(M)})\right)}{\#\left(Ш(A^{(M)})\right)} = \frac{\#\left(A'^{(M)}(\mathbb{Q})_{tor}\right)^2}{\#\left(A^{(M)}(\mathbb{Q})_{tor}\right)^2} \cdot \frac{Tam(A^{(M)})}{Tam(A'^{(M)})} \cdot \frac{R(A^{(M)})}{R(A'^{(M)})} \cdot \frac{\Omega_\infty(A^{(M)})}{\Omega_\infty(A'^{(M)})} =$$

$$= 1 \cdot 2^{a(M)+k_-(M)-r_-(M)} \cdot 2^{2\rho(M)-g(M)} \cdot 1 = 2^{a(M)+k_-(M)-r_-(M)+2\rho(M)-g(M)}$$

which completes the proof. □

3.2 Consequences of the 2-part of the conjecture

The following two theorems, stated here without proof, can be derived from the work presented in this section if we knew the unproven 2-part of the Birch and Swinnerton-Dyer conjecture. In the absence of this last result, the authors of the first reference dedicate a new section to prove them using, what they call, the method of Zhao [4].

Theorem 45. *Let $q_1, q_2, \ldots, q_r$ be $r \geq 1$ distinct primes, all of them $\equiv 1 \pmod 4$ and inert in F. Denote by $R = q_1 \cdot \cdots \cdot q_r$ their product. Then*

$$ord_2\left(L^{(alg)}(A^{(R)},1)\right) = r-1,$$

where $L^{(alg)}$ was defined at the beginning of this section. In particular, we have $L(A^{(R)},1) \neq 0$.

Let us remark some implications of this theorem. Since $L(A^{(R)},1) \neq 0$ we know that the Tate Shafarevich group is finite and we know from Theorem 31 that the p-part of the Birch and Swinnerton-Dyer conjecture holds for every $p>2$. The aforementioned theorem is presented as an application to the "main conjectures" of Iwasawa theory for imaginary quadratic fields proved by Rubin in [17]. Hence to prove that the full conjecture holds in this case, it is sufficient to prove that the 2-part is true. But we are in the situation of corollary

37, so we know that $\text{Ш}^{(2)}(A^{(R)}) = 0$ which implies further that the Tate Shafarevich group $\text{Ш}(A^{(M)})$ does not have elements of order 2 and therefore 2 does not divide the order of this group. Proposition 42 tells us that the Tamagawa factors of $A^{(R)}$ at bad primes are $c_7 = 2$ and $c_{q_i} = 2$ for all $1 \leq i \leq r$. Now if we look back at conjecture 30, since $ord_2\left(\#(A^{(R)}(\mathbb{Q}))\right) = 1$, we observe that the 2-part of the Birch and Swinnerton Dyer conjecture is equivalent to $ord_2 L^{(alg)}(A^{(R)}, 1) = r - 1$. So theorem 45 shows that the full conjecture holds for such curves $A^{(R)}$.

In the next theorem, M is a square free integer $\equiv 1 \pmod 4$.

Theorem 46. *Let $R = q_1 \dots q_r$ be a product of $r \geq 0$ distinct primes $\equiv 1 \pmod 4$, which are inert in F and let $N = p_1 \dots p_k$ be a product of $k \geq 1$ distinct primes, all of which split completely in the field $\mathfrak{h} = \mathbb{Q}(A[4], \sqrt{q_1}, \dots, \sqrt{q_r}) = \mathbb{Q}(i, \sqrt[4]{-7}, \sqrt{q_1}, \dots, \sqrt{q_r})$. Let $M = RN$. Then*

$$ord_2\left(L^{(alg)}(A^{(M)}, 1)\right) \geq r + 2k.$$

As I previously mentioned, the authors prove this result by Zhao's method. In the hypothesis of the last theorem, if one also assumes that $L(A^{(M)}, 1) \neq 0$ then, by Kolyvagin's theorem $A^{(M)}(\mathbb{Q})$ is finite. M satisfies the hypothesis of corollary 40, from which we get that $\text{Ш}^{(2)}(A^{(M)}) \neq 0$, therefore there is an element of order 2 in the Tate Shafarevich group $\text{Ш}(A^{(M)})$, in particular this group is non-zero.

Remark If we knew the 2-part of the Birch and Swinnerton-Dyer conjecture, one can even derive a sharper lower bound than the one in Theorem 46 for $ord_2\left(L^{(alg)}(A^{(M)}, 1)\right)$. We pointed above that Corollary 40 gives $\text{Ш}(A^{(M)})(2) \neq 0$ for this twists. This, combined with the values of the Tamagawa factors provided by Proposition 42 and the 2-part of the Birch and Swinnerton Dyer conjecture gives that

$$ord_2\left(L^{(alg)}(A^{(M)}, 1)\right) = 2k + r - 1 + ord_2\left(\#(\text{Ш}(A^{(M)})(2))\right).$$

From the Corollary 5 derived from the Cassels-Tate pairing, we know that $\#(\text{Ш}(A^{(M)})(2)$ is a square, so $ord_2\left(\#(\text{Ш}(A^{(M)})(2))\right) \geq 2$. Therefore, assuming the unproved 2-part of the Birch and Swinnerton-Dyer conjecture we get the sharper lower bound $ord_2\left(L^{(alg)}(A^{(M)}, 1)\right) \geq r + 2k + 1$. In [1], the authors point out that it does not seem easy to achieve this sharper lower bound using Zhao's method, but they are able to achieve it, independent on the 2-part of Birch and Swinnerton-Dyer conjecture, via a method that uses Waldspurger's formula (Section 4 of [1]).

Having the previous results at hand, we are now able to start the new section.

4. Heegner Points for Infinite Family of Quadratic Twist of $A = X_0(49)$

The last part of this essay is dedicated to the result in *Section 6 of* [1]. As professor John Coates described it in [3], a very general problem that motivates this section is the following.

General problem. Given an elliptic curve E defined over $\mathbb{Q}$, we would like to find a large explicit infinite family of square free integers M, coprime with the conductor $C(E)$, such that $L(E^{(M)}, s)$ has a simple zero at $s = 1$.

In his works [21] and [22], Ye Tian managed to establish such a result for the congruent number curve $y^2 = x^3 - x$ and the authors of [1] ingeniously combined the induction method used by Tian with the method described in the previously presented generalization of Birch's lemma to find such a family for the elliptic curve $A = X_0(49)$.

We have to remember that the hypothesis of the generalization of Birch's lemma required the existence of a such called sensitive supersingular prime. This was just a prime q_1 of good supersingular reduction such that $q_1 \equiv 1 \pmod 4$ and the conductor is a square modulo q_1. For $A = X_0(49)$ we have quite a few choices, since every prime q_1 such that $q_1 \equiv 1 \pmod 4$ and q_1 inert in $F = \mathbb{Q}\left(\sqrt{-7}\right)$ is sensitive supersingular.

$X_0(49)$ has precisely two rational cusps, namely $[\infty]$ and $[0]$. We choose a modular parameterization $f : X_0(49) \to A$, that sends $[\infty]$ to the origin of the group law and $[0]$ to $(-2, 1)$ if A is written in the form

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

Notice that $f(0) \notin 2A(\mathbb{Q})$, which is in accordance with the hypothesis required to apply the generalization of Birch's lemma.

The main result of this section is the following.

Theorem 47. *Let $M = -l_0RN$ be a negative square free integer, prime to 7, such that*

(1) $l_0 > 3$ is a prime which is $\equiv 3 \pmod 4$ and which is inert in F,

(2) R is a product of primes which are $\equiv 1 \pmod 4$*, and which are inert both in F and in $\mathbb{Q}(\sqrt{-l_0})$,*

(3) N is a product of primes which split completely in $\mathbb{Q}(A[4])$ and in the fields $\mathbb{Q}(\sqrt{q})$ for every prime q dividing R

(4) the ideal class group of $K_N = \mathbb{Q}(\sqrt{-l_0 N})$ has no element of order 4*.*

Then $L(A^{(M)}, s)$ has a simple zero at $s = 1$, $A^{(M)}(\mathbb{Q})$ has rank 1 *and the Tate Shafarevich group $Ш(A^{(M)}(\mathbb{Q}))$ is finite of odd cardinality.*

The proof is done by constructing a non-trivial Heeger point. Assume that $M = -l_0 RN$ is taken such that it satisfies the first three conditions in the hypothesis of the theorem above. Remember that in order to construct Heegner points, we had to consider an imaginary quadratic field that satisfied the so-called Heegner hypothesis. The later means that every prime factor of the conductor has to split in the selected imaginary quadratic. In the given situation, we are going to work with the field $K_N = \mathbb{Q}(\sqrt{-l_0 N})$ and since the conductor is 49 we just have to check that 7 splits in this field.

Observe that $\mathbb{Q}(A[4]) = \mathbb{Q}(i, \sqrt[4]{-7})$, so the condition (3) in theorem 47 tells us that the prime factors of N split completely in this field, from where we can deduce that $\left(\frac{N}{7}\right) = 1$. We know that l_0 is inert in F, therefore $\left(\frac{-7}{l_0}\right) = -1$, so $\left(\frac{7}{l_0}\right) = 1$ and hence by the law of quadratic reciprocity $\left(\frac{l_0}{7}\right) = -1$. From all of this, we can deduce that

$$\left(\frac{-4l_0N}{7}\right) = \left(\frac{-l_0N}{7}\right) = -1 \cdot (-1) \cdot 1 = 1,$$

hence 7 is split in $K_N = \mathbb{Q}(\sqrt{-l_0 N})$, regardless $N \equiv 1$ or $N \equiv 3 \bmod 4$, so the classical Heegner hypothesis holds for A and the imaginary quadratic field K_N.

Denote by $H_{R,N}$ the ring class field of conductor R and define by

$$\mathfrak{I}_{R,N} = K_N(\sqrt{-l_0}, \sqrt{q_1}, \ldots, \sqrt{q_r}, \sqrt{p_1}, \ldots, \sqrt{p_k}),$$

where $q_1, \ldots, q_r$ and $p_1, \ldots, p_k$ are the distinct prime factors of R and N respectively.

Using techniques similar to the ones in the proof of Lemma 27 together with the theory of genra (to exploit hypothesis (4) in Theorem 47 given for K_N), the authors are able to prove that $\mathfrak{I}_{R,N} \subseteq H_{R,N}$. This implies in particular that $K_N\left(\sqrt{RN}\right) \subset H_{R,N}$.

Let $P_{R,N}$ be the Heegner point of conductor R attached to $A = X_0(49)$ and the field K_N. Let us recall that $P_{R,N} \in A(H_{R,N})$. Denote by χ_R the quadratic character defining the extension $K_N(\sqrt{R})/K_N$ and define the following Heegner point

$$Y_{R,N} = \sum_{\sigma \in Gal(H_{R,N}/K_N)} \chi_R(\sigma)\sigma(P_{R,N}) \in A(K_N(\sqrt{R})).$$

The authors begin by proving the following stronger result.

Theorem 48. *Let $M = -l_0RN$ be a negative square free integer, prime to 7, satisfying conditions (1), (2) and (3) of Theorem 47. Then, the Heegner point $Y_{R,N} \in A(K_N(\sqrt{R}))$ defined above satisfies*

$$Y_{R,N} \in 2^{k+r-1}A\left(\mathbb{Q}(\sqrt{M})\right)^{-} + A\left(\mathbb{Q}(\sqrt{M})\right)_{tor},$$

where r,k denote the number of prime factors of R and N, respectively, and when $r = k = 0$, this should be interpreted as meaning that $2Y_{R,N} \in A\left(\mathbb{Q}(\sqrt{M})\right)^{-}$. If, in addition, the ideal class group of K_N has no element of order 4, then

$$Y_{R,N} \notin 2^{k+r}A\left(\mathbb{Q}(\sqrt{M})\right)^{-} + A\left(\mathbb{Q}(\sqrt{M})\right)_{tor},$$

whence $Y_{R,N}$ is of infinite order.

Remark We quickly recall that here $A\left(\mathbb{Q}(\sqrt{M})\right)^{-}$ denotes, as in the section dedicated to Birch's lemma, the subgroup of points in $A\left(\mathbb{Q}(\sqrt{M})\right)$ on which the non-trivial element of $Gal(\mathbb{Q}(\sqrt{M})/\mathbb{Q})$ acts like -1.

Proof. Since the case $k = r = 0$ was already proved in Theorem 21 (Birch's lemma) and the case $k = 0, r \geq 1$ was proved in Theorem 24 (the generalization to Birch's lemma), we see that the authors have set the ground for a proof by induction on k.

Assume now that $k \geq 1$. For each positive divisor D of NR, let χ_D be the character defining the extension $K_N(\sqrt{D})/K_N$ and, similarly to what we did in the proof of theorem 24, define the associated imprimitive Heegner point

$$Z_{D,N} = \sum_{\sigma \in Gal(H_{R,N}/K_N)} \chi_D(\sigma)\sigma(P_{R,N}) \in A\left(K_N(\sqrt{D})\right).$$

In particular, $Y_{R,N} = Z_{R,N}$. Define also

$$\Psi_{R,N} = Tr_{H_{R,N}/\mathfrak{I}_{R,N}}(P_{R,N}).$$

In the spirit of lemma 29, we prove the following analogue

Lemma 49. *Let D be any positive divisor of RN. Then $Z_{D,N} = 0$ unless R divides D. Moreover, we have*

$$\sum_{R|D|RN} Z_{D,N} = 2^{k+r}\Psi_{R,N} \tag{4.1}$$

where the sum is taken over all positive divisors D of RN that are divisible by D.

Proof. Let D be any positive divisor of RN, not divisible by R. There exists a prime factor q of R that does not divide D as discussed before in lemma 29, $a_q = 0$. Now, using the boxed formula, due to Kolyvagin, discussed in the proof of the aforementioned lemma, we get that

$$Tr_{H_{R,N}/H_{R',N}}(P_{R,N}) = a_q P_{R',N} = 0,$$

where $R' = R/q$.

But now, observe that z_D can be written as

$$Z_{D,N} = \sum_{\sigma \in Gal(H_{R,N}/K_N)} \chi_D(\sigma)\sigma(P_{R,N}) = \sum_{\sigma \in Gal(H_{R',N}/K_N)} \chi_D(\sigma)\sigma(Tr_{H_{R,N}/H_{R',N}}(P_{R,N})) = 0.$$

,

Now, since we established that $Z_{D,N}$ vanishes if R does not divide D, we can write

$$\sum_{R|D|RN} Z_{D,N} = \sum_{D|RN} Z_{D,N} = \sum_{\sigma \in Gal(\mathfrak{I}_{R,N}/K_N)} \left(\sum_{D|N} \chi_D(\sigma) \right) \sigma(\Psi_{R,N}) = 2^{k+r}\Psi_{R,N},$$

since the number of divisors of DN is 2^{k+r}.

□

Using this last lemma and the fact that $Y_{R,N} = Z_{R,N}$, we can express

$$Y_{R,N} = -\sum_{1<d|N} Z_{dR,N} + 2^{k+r}\Psi_{R,N},$$

where the sum runs over all divisors d of N that are > 1. For every such d, if we denotes by $N_d = N/d$, it can be proved that $Z_{dR,N} \in A\left(\mathbb{Q}(\sqrt{-l_0 RN_d})\right)^-$.

The authors use an induction argument now to prove that

$$Z_{dR,N} \in 2^{k+r} A\left(\mathbb{Q}(\sqrt{-l_0 RN_d})\right)^- + A\left(\mathbb{Q}(\sqrt{-l_0 RN_d})\right)_{tor} \tag{4.2}$$

for every divisor $d > 1$ of N. For this, define $K_{N_d} = \mathbb{Q}(\sqrt{-l_0 N_d})$ and construct, analogously, the Heegner point $Y_{R,N_d} \in A(K_{N_d}(\sqrt{R}))$.

Since $Z_{dR,N}$ and Y_{R,N_d} both belong to $A\left(\mathbb{Q}(\sqrt{-l_0 RN_d})\right)^-$, we can compare their heights by using the generalization of Gross-Zagier formula presented in Theorem 20.

We know that

$$\frac{L(A/K_N,\chi_{dR},s)}{L(A/K_{N_d},\chi_R,s)}=\frac{L(A^{(dR)},s)}{L(A^{(R)},s)}.$$

We have seen in Theorem 45 that $L(A^{(R)},s)$ does not vanish at $s=1$.

If Y_{R,N_d} has finite order then $Z_{dR,N}$ is a torsion point, which means that (4.2) is true. If Y_{R,N_d} is of infinite order, we can derive from Kolyvagin theorem and Theorem 20 that $A\left(\mathbb{Q}(\sqrt{-l_0RN_d})\right)^-$ has rank 1 and that the ratio of Néron-Tate heights

$$\frac{\widehat{h}_{K_N}(Z_{dR,N})}{\widehat{h}_{K_{N_d}}(Y_{R,N_d})}=\frac{L^{(alg)}(A^{(dR)},1)}{L^{(alg)}(A^{(R)},1)},$$

where $L(A^{(dR)},1)\neq 0$.

Now, using theorems 45 and 46 one gets that

$$ord_2\left(\frac{L^{(alg)}(A^{(dR)},1)}{L^{(alg)}(A^{(R)},1)}\right)\geq 2k(d)+1,$$

where $k(d)$ is the number of primes that divide d.

Assume in the induction hypothesis that

$$Y_{R,N_d}\in 2^{k-k(d)-1}\cdot A\left(\mathbb{Q}(\sqrt{-l_0RN_d})\right)^-+A\left(\mathbb{Q}(\sqrt{-l_0RN_d})\right)_{tor}$$

and then (4.2) follows easily from the last two relations. Induction is complete, so 4.2 holds for all divisors $d>1$ of N.

Now, from $Y_{R,N}=-\sum_{1<d|N} Z_{dR,N}+2^{k+r}\Psi_{R,N}$, we derive that

$$Y_{R,N}\in 2^{k+r}A(\mathfrak{I}_{R,N})+A(\mathfrak{I}_{R,N})_{tor}.$$

From this point, the first assertion can be proved by Galois cohomology methods, very similar to the ones used in the proof of Theorem 24.

The condition saying the ideal class group of K_N has no elements of order 4 implies the fact that the degree $[H_{R,N}:\mathfrak{I}_{R,N}]$ is odd. It can then be proved that $\Psi_{R,N}+\overline{\Psi_{R,N}}$ is the non-trivial element of order 2 in $\mathbb{A}(\mathbb{Q})$ and, by the same argument as in the proof of Theorem 24, it can be proved that

$$Y_{R,N}\notin 2^{k+r}A\left(\mathbb{Q}(\sqrt{M})\right)^-+A\left(\mathbb{Q}(\sqrt{M})\right)_{tor},$$

and hence $Y_{R,N}$ has infinite order. □

Now, to prove the Theorem 47, the central result of this essay, just use the Heegner point $Y_{R,N}$ in the generalized Gross-Zagier formula presented in Theorem 20. Since this point has infinite order, we see that the complex L-series of A/K_N twisted by an abelian character χ of K_N has a simple zero at $s = 1$. Now, because the root number of $A^{(M)}$ is -1, we know that $L(A^{(M)}, s)$ has a simple root at $s = 1$. This implies, by the Kolyvagin theorem that $A^{(M)}(\mathbb{Q})$ has rank 1 and the Tate-Shafarevich group $Ш(A^{(M)})$ is finite.

To establish the odd cardinality of this group, we are going to use Corollary 41. Notice that we are in the hypothesis of this corollary, since every prime factor of N splits completely in $\mathbb{Q}(\sqrt{7})$ and in $\mathbb{Q}(\sqrt{-7})$ and hence it is $\equiv 1 \pmod 4$. We can therefore derive that $\mathfrak{S}^{(2)}(A^{(M)}) = S^{(2)}(A^{(M)})/Im(A^{(M)}(\mathbb{Q})_{tor})$ has exact order 2. Since the rank of $A^{(M)}(\mathbb{Q})$ is 1, Lemma 7 gives that $Ш(A^{(M)})(2) = 0$, so order of the Tate-Shafarevich group is odd which completes the proof of Theorem 47.

References

[1] J. Coates, Y. Li, Y. Tian and S. Zhai. *Quadratic Twists of Elliptic Curves.* Proceedings of the London Mathematical Society, 2014.

[2] B. Birch, P. Swinnerton-Dyer. *Notes on elliptic curves (II)* J. Rene Ange. Math. 218, 1965

[3] J. Coates. *Lectures on the Birch-Swinnerton-Dyer Conjecture*. Notices of the ICCM Vol 1, 2013.

[4] J. Coates, M. Kim, Z. Liang and C. Zhao. *On the 2-part of the Birch-Swinnerton-Dyer conjecture for elliptic curves with complex multiplication.* Munster J. of Math. Vol. 7, 2014.

[5] J. Cremona. *Algorithms for modular elliptic curves, 2nd edition.* CUP, 1997.

[6] J. Cremona *Numerical evidence for the BSD Conjecture.* Slides from Conference on the BSD conjecture, Cambridge, 2011.

[7] H. Darmon. *Rational Points on Modular Elliptic Curves.* No. 101 in Regional Conference Series in Mathematics. American Mathematical Society, 2004.

[8] M. Deuring. *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins, I, II, III, IV* Gott. Nach., 1953, 1955, 1956, 1957.

[9] B.H. Gross. *Heegner Points on $X_0(N)$.*, Modular Forms, R.A. Rankin, 1984.

[10] K. Heegner. *Diphantische Analysis und Modulfunktionen.* Math. Zeitschrift 56, 1972.

[11] A. W. Knapp. *Elliptic curves.*, Princeton University Press, 1992.

[12] J.I. Manin. *Cyclotomic fields and Modular Curves.* Russian Mathematical Surveys, Vol. 26, 1971.

[13] A.P. Ogg. *Abelian curves of small conductor.* J. Reine Angew. Math. 226, 1967.

[14] A.P. Ogg. *Elliptic curves and wild ramification.* Amer. J., 1967.

[15] A.P. Ogg. *Hyperelliptic modular curves.* Bull. Soc. Math. France 102, 1974.

[16] V. Pal. *Periods of quadratic twists of elliptic curves.* Proceedings AMS 140, 2012.

[17] K. Rubin. *The "main conjectures" of Iwasawa theory for imaginary quadratic fields.* Invent. math. Vol. 103, 1991.

[18] J-P. Serre. *Facteurs locaux des fonctions zêta des variétés algébriqués (définitions et conjectures).* Séminare Delange-Pisot-Poitou, 1970.

[19] J.H. Silverman. *The arithmetic of elliptic curves, volume 106.* Springer Verlag, 2009.

[20] J. Tate. *The Arithmetic of Elliptic Curves.* Inventiones math. 23, 1974.

[21] Y. Tian. *Congruent numbers with many prime factors.* Proceedings of the National Academy of Sciences USA 109, 2012.

[22] Y. Tian. *Congruent number and Heegner points.* Cambridge Journal of Mathematics Vol 2, 2014.

[23] A. Weil. *Jacobi sums as "Grossencharaktere".* Trans. Amer. Math. Soc. 75, 1952.

[24] X. Yuan, S. Zhang and W. Zhang. *The Gross-Zagier Formula on Shimura Curves*. Annals of Mathematics Studies Number 184, 2012.