ON THE INDEX OF THE HEEGNER SUBGROUP OF ELLIPTIC CURVES

CARLOS CASTAÑO-BERNARD

Abstract. Let \( E \) be an elliptic curve of conductor \( N \) and rank one over \( \mathbb{Q} \). So there is a non-constant morphism \( X_0^+(N) \to E \) defined over \( \mathbb{Q} \), where \( X_0^+(N) = X_0(N)/w_N \) and \( w_N \) is the Fricke involution. Under this morphism the traces of the Heegner points of \( X_0^+(N) \) map to rational points on \( E \). In this paper we study the index \( I \) of the subgroup generated by all these traces on \( E(\mathbb{Q}) \). We propose and also discuss a conjecture that says that if \( N \) is prime and \( I > 1 \), then either the number of connected components \( \nu_N \) of the real locus \( X_0^+(N)(\mathbb{R}) \) is \( \nu_N > 1 \) or (less likely) the order \( S \) of the Tate-Šafarevič group \( \Sha(E) \) of \( E \) is \( S > 1 \). This conjecture is backed by computations performed on each \( E \) that satisfies the above hypothesis in the range \( N \leq 129999 \).

This paper was prepared for the proceedings of the Conference on Algorithmic Number Theory, Turku, May 8–11, 2007. We tried to make the paper as self contained as possible.

Contents

1. Introduction 2
1.1. Motivation 2
1.2. Acknowledgements 3
2. Background 3
2.1. The Hasse principle and genus one curves 3
2.2. Structure of the Mordell-Weil group 4
2.3. The Birch and Swinnerton-Dyer conjecture 5
3. On the index \( I_\phi \) and the topology of \( X_0^+(N)(\mathbb{R}) \) 7
3.1. Modular parametrisation 7
3.2. Heegner points 8
3.3. Heegner paths 10
3.4. The conjecture 11
References 12
1. Introduction

1.1. Motivation. Let $E$ be an elliptic curve over $\mathbb{Q}$, i.e. a complete curve of genus one with a specified rational point $O_E$, hence $E$ has a natural structure of a commutative algebraic group with zero element $O_E$. The Mordell-Weil theorem asserts that the group $E(\mathbb{Q})$ of rational points on $E$ is finitely generated. So the classical Diophantine problem of determining $E(\mathbb{Q})$ is thus the problem of obtaining a finite set of generators for the group $E(\mathbb{Q})$. The finite subgroup $E(\mathbb{Q})_{\text{tors}}$ of torsion points of $E(\mathbb{Q})$ is easy to compute. However, finding generators $g_1, \ldots, g_{r_E}$ for the free abelian group $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ is in general a hard problem. The Birch and Swinnerton-Dyer conjecture predicts (among other things) that the rank $r_E$ of the Mordell-Weil group $E(\mathbb{Q})$ is the order of vanishing at $s = 1$ of the Hasse-Weil $L$-function $L(E, s)$ attached to $E$. By the work of Kolyvagin on Euler systems of Heegner points on (certain twists of) modular elliptic curves, and the well-known fact due to Wiles [16], and Breuil-Conrad-Diamond-Taylor [2] that every elliptic curve $E$ over $\mathbb{Q}$ admits a (non-constant) morphism $\varphi : X_0(N) \to E$ over $\mathbb{Q}$, we know that this prediction is true for $r_E = 0$ and 1. We are interested in the latter case, and henceforth we assume that $L(E, s)$ has a simple zero at $s = 1$. Then $\varphi$ factors through the quotient $X_0^+(N) = X_0(N)/w_N$ associated to the Fricke involution $w_N$ and the so-called Heegner point construction yields a non-trivial subgroup $H$ of $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$. Gross-Kohnen-Zagier [9, p. 561] proved that the (full) Birch and Swinnerton-Dyer for $r_E = 1$ is equivalent to

\begin{equation}
I_E^2 = c_E \cdot n_E \cdot m_E \cdot |\Sha(E)|,
\end{equation}

where $I_E$ is the index of $H$, $\Sha(E)$ is the Tate-Šafarevič group of $E$, $c_E$ is Manin’s constant, $m_E$ is the product of the Tamagawa numbers, and $n_E$ is the index of a certain subgroup of the $-1$-eigenspace $H_1(E(\mathbb{C}); \mathbb{Z})^-$ of complex conjugation acting on $H_1(E(\mathbb{C}); \mathbb{Z})$ constructed in terms of classes of Heegner geodesic cycles in $H_1(X_0^+(N)(\mathbb{C}); \mathbb{Z})^-$. (The relevant definitions are recalled below.) Let us assume this conjecture. To simplify our discussion let us assume further that the conductor $N_E$ of $E$ is prime so that the index $I_E$ is completely determined by $n_E$ and $|\Sha(E)|$. Numerical evidence strongly suggests that there are 109 curves such that $I_E > 1$ out of the 914 curves $E$ of rank one and prime conductor $N \leq 129999$ in Cremona’s Tables [5]. For each of these curves with $I_E > 1$, then either the number $\nu_N$ of connected components of the real locus $X_0^+(N)(\mathbb{R})$ of the quotient modular curve $X_0^+(N)$ is $\nu_N > 1$ or, less likely (only 8 cases), $\Sha(E)$ is non-trivial. This suggests a non-trivial connection between the topology of $X_0^+(N)(\mathbb{R})$ and the arithmetic of $E$, which is not expected since $\nu_N$ is a certain simple sum of class numbers of real quadratic fields and heuristic considerations suggest that the equality $\nu_N = 1$ is more

\footnote{Heegner points were first studied systematically by Birch [1].}
likely than the inequality $\nu_N > 1$. This paper is about a conjecture motivated by the above discussion. We state it in Subsection 3.4 and then discuss a homological formulation of our conjecture which hopefully will furnish a new approach to Equation 1.1.

1.2. Acknowledgements. I would like to heartily thank Professor Birch, whose comments encouraged me to investigate further some “loose ends” related to some odd behaviour for the curve $359A$ mentioned in my Ph.D. thesis [4, p. 75]. I would also like to thank my colleagues at ICTP whose financial support, through the granting of a visiting fellowship, has facilitated the writing of this paper.

Table 1 and Table 2 were computed with the help of PARI [12], installed on GNU/Linux computers.

2. Background

2.1. The Hasse principle and genus one curves. It is a classical Diophantine problem the determination of the set of rational points $C(\mathbb{Q})$ of a given complete non-singular algebraic curve defined over $\mathbb{Q}$. The problem is solved for the case of genus zero. Legendre theorem, as stated by Hasse, says that given any conic $C$ with coefficients in $\mathbb{Q}$ the set $C(\mathbb{Q})$ is non-empty if and only if the set $C(\mathbb{Q}_p)$ is non-empty for every prime $p$ including $p = \infty$, where $\mathbb{Q}_p$ is the field of $p$-adic numbers, if $p \neq \infty$ and $\mathbb{Q}_p = \mathbb{R}$, if $p = \infty$. Moreover, it is known that it suffices to determine whether $C(\mathbb{Q}_p)$ is non-empty for each prime $p$ that divides the discriminant $D$ of an homogeneous equation $f(X, Y, Z) = 0$ for the conic $C$. Then by Hensel’s lemma we know that $f(X, Y, Z) = 0$ will have a non-trivial zero in $\mathbb{Q}_p$ for $p | D$ if and only if it has an “approximate” zero. Once we have a rational point $O$ on $C$, it is easy to see that there are an infinite number of them by fixing any line $L \subset \mathbb{P}^2$ defined over $\mathbb{Q}$ (e.g. the $X$-axis) and parametrise $C(\mathbb{Q})$ with $L$ in the obvious way. This furnishes an algorithm to effectively compute $C(\mathbb{Q})$ in the genus zero case.

Let us consider the genus one case. By the work of Selmer [14] we know that the obvious extension of Legendre’s theorem to curves of genus one is not true. For example the curve $C$ in $\mathbb{P}^2$ given by the Selmer cubic

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

is such that $C(\mathbb{Q}_p) \neq 0$ for every prime $p$, including $p = \infty$. But it turns out that $C(\mathbb{Q}) = \emptyset$. In such cases it is said that $C$ violates the Hasse principle. There is a natural way to measure the extent of failure of this principle. The Jacobian $E = \text{Jac}(C)$ of $C$ is a complete non-singular genus one curve defined over $\mathbb{Q}$ equipped with a commutative algebraic group structure, i.e. $E$ is an elliptic curve, together with an isomorphism $j : C \longrightarrow E$ over $\mathbb{Q}^{alg}$ such that for every element $\sigma$ in the
Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}^{ab}$ over $\mathbb{Q}$ the map

$$(\sigma \circ j) \circ j^{-1} : \text{Jac}(T) \longrightarrow \text{Jac}(T)$$

is of the form $P \mapsto P + a_{\sigma}$, for some $a_{\sigma} \in E(\mathbb{Q}^{ab})$. So we may define the Tate–Šafarevič group $\text{III}(E)$ of $E$ as the set of isomorphism classes of pairs $(T, \iota)$, where $T$ is a smooth curve defined over $\mathbb{Q}$ of genus one such that $T(\mathbb{Q}_p) \neq \emptyset$, for all $p$ prime and $\iota : E \longrightarrow \text{Jac}(T)$ is an isomorphism defined over $\mathbb{Q}$. (Given $T$ such that $E = \text{Jac}(T)$, the map $\sigma \mapsto a_{\sigma}$ is a 1-cocycle whose image in the cohomology group $H^1(G_{\mathbb{Q}}, E)$ is uniquely determined by the isomorphism class of $(T, \iota)$. So we may identify $\text{III}(E)$ with a subgroup of $H^1(G_{\mathbb{Q}}, E)$.) Clearly the Hasse principle holds for $C$ if and only if $\text{III}(E)$ consists of exactly one element, where $E$ is the Jacobian of $C$. It is conjectured to be finite, i.e. that Hasse principle fails by a “finite amount” in the genus one case.

Cassels’ proved that if $\text{III}(E)$ is indeed finite, then its order is a square.

2.2. Structure of the Mordell-Weil group. The algebraic group structure of an elliptic curve $E$ may be made explicit as follows. Let $O_E$ be the zero element of $E$. Using the Riemann-Roch theorem we see that the map Albanese map $P \mapsto P - O_E$ identifies the set $E(K)$ of $K$-rational points of $E$ over any field $K$ containing $\mathbb{Q}$. Using again the Riemann-Roch theorem we may see that $E$ has a Weierstraß model

$$(2.1) \quad Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

where $O_E$ corresponds to $(0 : 1 : 0)$, for $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$ such that the discriminant $\Delta$ of Equation 2.1 is non-zero. It is well-known that the converse holds, so a curve defined by a Weierstraß equation such that $\Delta \neq 0$ is a complete non-singular curve of genus one, and thus an elliptic curve with zero element $O_E = (0 : 1 : 0)$. In particular, the curve obtained by reducing the coefficients of Equation 2.1 modulo a prime number $p$ is an elliptic curve if and only if $p$ does not divide $\Delta$, in which case we say that $E$ has good reduction at $p$. A further consequence of the Riemann-Roch theorem is that the group law is given by the classical chord and tangent construction, which is schematically outlined in Figure 2.1. Using this geometric property we may easily write down explicit rational functions with coefficients in $\mathbb{Q}$ on the coordinate functions $x$ and $y$ for the addition law $E \times E \longrightarrow E$ and for the inverse of an element law $E \longrightarrow E$.

The Mordell-Weil theorem asserts that the group $E(\mathbb{Q})$ is a finitely generated abelian group, thus $E(\mathbb{Q}) = E(\mathbb{Q})^{\text{tors}} + E(\mathbb{Q})^{\text{free}}$, where the torsion subgroup $E(\mathbb{Q})^{\text{tors}} \subset E(\mathbb{Q})$ is finite and $E(\mathbb{Q})^{\text{free}} \subset E(\mathbb{Q})$ is a free subgroup of (finite) rank $r_E$. It is well-known that the subgroup $E(\mathbb{Q})^{\text{tors}}$ is not difficult to compute. However, obtaining generators for a subgroup $E(\mathbb{Q})^{\text{free}}$ is in general a hard problem. A measure of the
arithmetic complexity of a given non-torsion rational point $P$ on $E$ is given by its 
Néron-Tate height

$$\hat{h}(P) = \lim_{n \to \infty} 4^{-n} h(2^n P),$$

where the naive height $h(P)$ of a point $P = (x : y : z)$ in $\mathbb{P}^2(\mathbb{Q})$ is given by $h(P) = \log \max(|x|, |y|, |z|)$, where $x$, $y$, and $z$ are integers such that $\gcd(x, y, z) = 1$. It is well-known that $\hat{h}(P)$ does not depend on the choice of Weierstraß model for $E$ and, moreover, it defines a non-degenerate positive definite quadratic form on the $r_E$-dimensional real vector space $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. The height paring is the bilinear form $\langle \cdot, \cdot \rangle$ on $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ such that $\langle P, P \rangle = \hat{h}(P)$, for all $P \in E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. The determinant $R_E$ of the $r_E$ by $r_E$ matrix whose entries are given by the height paring $\langle \cdot, \cdot \rangle$ applied to a set of generators of $E(\mathbb{Q})^{free}$ is known as the regulator of $E(\mathbb{Q})$.

2.3. The Birch and Swinnerton-Dyer conjecture. As above let $E$ be an elliptic curve defined over $\mathbb{Q}$, and suppose we have used Tate's algorithm [15] to obtain the conductor $N_E$ and a minimal Weierstraß model of $E$, i.e. an integral Weierstraß model of $E$ with $|\Delta|$ minimal. Such discriminant is known as the minimal
discriminant$^2$ of $E$ and denote we it $\Delta_E$. The Hasse-Weil $L$-function of $E$ over $\mathbb{Q}$ is
\[ L(E, s) = \sum_{n=1}^{\infty} a_E(n)n^{-s} = \prod_{\text{prime } p \mid N} (1 - a_E(p)p^{-s})^{-1} \prod_{\text{prime } p \not\mid N} (1 - a_E(p)p^{-s} + p^{1-2s})^{-1}, \]
where
\[ a_E(p) = \begin{cases} p + 1 - \#(E(\mathbb{F}_p)), & \text{good reduction,} \\ 1, & \text{split reduction,} \\ -1, & \text{non-split reduction,} \\ 0, & \text{cuspidal reduction.} \end{cases} \]

Since $E$ is defined over $\mathbb{Q}$ the work of Wiles [16] and Breuil-Conrad-Diamond-Taylor [2] implies that $E$ is modular, and in particular $L(E, s)$ may be analytically continued to the whole complex plane $\mathbb{C}$. (See below.) The Birch and Swinnerton-Dyer conjecture predicts that $L(E, s)$ has a Taylor expansion around $s = 1$ of the form
\[ L(E, s) = \kappa_{r_E}(s - 1)^{r_E} + \kappa_{r_E+1}(s - 1)^{r_E+1} + \ldots, \]
where
\[ \kappa_{r_E} = \frac{|\Sha(E)|m_E}{|E(\mathbb{Q})_{\text{tors}}|} \Omega_E \]
where $m_E$ is the product of all the local Tamagawa numbers $c_p$, and $\Omega_E$ is the least positive real period of the Néron differential
\[ \omega_E = \frac{dX}{2Y + a_1X + a_3}, \]
where $a_1$ and $a_3$ are as in Equation 2.1 (assuming the Weierstraß equation is minimal).

**Example 2.1.** The Selmer cubic $C$ defined by $3X^3 + 4Y^3 + 5Z^3 = 0$ has Jacobian $E$ with Weierstraß model $Y^2 = 4X^3 - 97200$. (Cf. Perlis [13, p. 58].) Using Tate’s algorithm we may see that $E$ has conductor $N_E = 24300$ and minimal Weierstraß model $Y^2 = 4X^3 - 24300$. Using this information we may identify $E$ in entry 24300 Y 2 of Cremona’s Tables [5]. According to that entry the rank of $E$ is zero and the order of Tate–Shaferetvič group predicted by the Birch and Swinnerton-Dyer conjecture is $|\Sha(E)| = 3^2$. This is consistent with the fact that the Hasse principle fails for $C$, as remarked above.

$^2$The minimal discriminant $\Delta_E$ and the conductor $N_E$ share the same prime divisors, and under certain circumstances they coincide (up to multiplication by $\pm 1$), e.g. when $\Delta_E$ is prime.
3. On the index \( I_\phi \) and the topology of \( X^+_0(N)(\mathbb{R}) \)

3.1. Modular parametrisation. Let \( X_0(N) \) be the normalisation of the moduli space that classifies pairs \((A, A')\) of elliptic curves together an isogeny \( \phi : A \to A' \) with cyclic kernel of order \( N \). The curve \( X_0(N) \) may be described as follows. Let \( \Gamma \) be the group \( SL_2(\mathbb{R}) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - cb = 1 \} \) modulo multiplication by \( \pm 1 \), and let \( \Gamma \) act on the upper half plane \( \mathfrak{h} = \{ z \in \mathbb{C} : \Im(\tau) > 0 \} \) in the usual way by letting

\[
\tau \mapsto \frac{a\tau + b}{c\tau + d}.
\]

First we may identify the complex points of the moduli space \( Y(1) \) that classifies elliptic curves \( E \) over \( \mathbb{C} \) with the complex points of the affine line \( \mathbb{A}^1 \) by mapping the isomorphism class of \( E \sim C/ (\mathbb{Z}\tau + \mathbb{Z}) \) to the image of \( \tau \) in \( \Gamma \backslash \mathfrak{h} \) followed by the classical \( j \)-invariant map

\[
j(\tau) = \frac{E_4^3}{\Delta}(\tau) = \frac{1}{q} + 744 + 196884q + \ldots,
\]

where \( \Delta \) is the cusp form of weight 12 defined by the infinite product \( \Delta(\tau) = q \prod_{n>0}(1 - q^n)^{24} \), and \( E_4 \) is the modular form of weight 4 defined by the series \( E_4(\tau) = 1 + 240 \sum_{n>0} \sigma_3(n) q^n \), where as usual \( \sigma_k(n) = \sum_{d|n} d^k \) and \( q = e^{2\pi i \tau} \). The obvious action of \( \Gamma \) on the cusps \( \mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{ i\infty \} \) is transitive, so the (one-point) compactification \( X(1)(\mathbb{C}) \) of the complex line \( Y(1)(\mathbb{C}) \) is the Riemann sphere \( X(1) = \Gamma \backslash \mathfrak{h}^* \), where \( \mathfrak{h}^* = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q}) \). We also have a bijection

\[
\Gamma_0(N) \backslash \mathfrak{h}^* \to X_0(N)(\mathbb{C})
\]

where

\[
\Gamma_0(N) = \left\{ \mu = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.
\]

The quotient set \( \Gamma_0(N) \backslash \mathfrak{h}^* \) has a unique complex-analytic structure such that the natural map \( \psi : \Gamma_0(N) \backslash \mathfrak{h}^* \to X(1)(\mathbb{C}) \) is a proper. Moreover, the above bijection is in fact an isomorphism between \( \Gamma_0(N) \backslash \mathfrak{h}^* \) and \( X_0(N)(\mathbb{C}) \) as Riemann surfaces in such a way that \( \psi \) is induced by the projection map \( (A, A') \mapsto A \). The degree of \( \psi \) is the degree of the minimum polynomial \( \Phi_N(j, Y) \in \mathbb{C}(j)[Y] \) of \( j(N\tau) \) over \( \mathbb{C}(j) \), and it turns out that \( \Phi_N(X, Y) \) has integral coefficients. The field of fractions of \( \mathbb{Q}[X, Y]/(\Phi_N(X, Y)) \) gives the canonical \( \mathbb{Q} \)-structure of \( X_0(N) \).
The Fricke involution $w_N$ may be defined as the morphism of $X_0(N)$ to itself induced by mapping an isogeny $\phi: A \to A'$ to its dual $\phi: A' \to A$. In the complex-analytic setting $w_N$ is induced by the involution $\tau \mapsto -\frac{1}{N^2} \tau$ of $\mathfrak{h}$. Let $X_0^+(N)$ be the quotient of $X_0(N)$ by the group $\{1, w_N\}$. The classical result $\Phi_N(X, Y) = \Phi_N(Y, X)$ implies that the canonical map $X_0(N) \to X_0^+(N)$ is defined over $\mathbb{Q}$.

Again let $E$ be an elliptic curve defined over $\mathbb{Q}$. As mentioned above, by the work of Wiles [16] and Breuil-Conrad-Diamond-Taylor [2] we know that if $E$ has rank one over $\mathbb{Q}$. By the work of Kolyvagin [10], Gross-Kohnen-Zagier [9] and results due to Waldspurger, we know that if $s = 0$ or $1$, then the order of vanishing of $L(E, s)$ is as predicted by the Birch and Swinnerton-Dyer conjecture (and also that $\text{ord}_E$ is finite). In particular $L(E, s)$ has a simple zero at $s = 1$ and thus $w_N \omega_f = \omega_f$. So the modular parametrisation factors through the quotient map $X_0^+(N) \to X_0(N)$.

3.2. Heegner points. Now suppose we fix a pair of integers $(D, r)$ that satisfy the so-called Heegner condition\(^3\) i.e. $D$ is the discriminant of an imaginary quadratic order $\mathcal{O}_D$ of conductor $f$ such that $\gcd(N, f) = 1$ and $r \in \mathbb{Z}$ is such that

$$D \equiv r^2 \pmod{4N}.$$ 

So we have a proper $\mathcal{O}_D$-ideal $n_r = \mathbb{Z}N + \mathbb{Z}\frac{r+\sqrt{D}}{2} \subset K = \mathbb{Q}(\sqrt{D})$ and $\mathcal{O}_D/\mathfrak{n}_r \cong \mathbb{Z}/N\mathbb{Z}$. So for each proper $\mathcal{O}_D$-ideal $\mathfrak{a} \subset K$ we have a point $x = (\mathbb{C}/\mathfrak{a}, \mathbb{C}/(\mathfrak{n}_r^{-1}\mathfrak{a}))$ on $X_0(N)$. This point $x$ is known as a Heegner point, and following Gross [6] we denote it by $x = (\mathcal{O}_D, \mathfrak{n}_r, [\mathfrak{a}])$, where $[\mathfrak{a}]$ is the class of $\mathfrak{a}$ in $\text{Pic}(\mathcal{O}_D)$. The latter set may be identified with the $\Gamma$-orbits $\Gamma\backslash \mathcal{Q}_D^0$ of the set $\mathcal{Q}_D^0$ of primitive binary quadratic forms $[A, B, C]$ of discriminant $D = B^2 - 4AC$ and $A > 0$ by writing each $\mathcal{O}_D$-ideal $\mathfrak{a}$ as $\mathfrak{a} = \mathbb{A}Z + \frac{-B+\sqrt{D}}{2}Z$, for some $[A, B, C] \in \mathcal{Q}_D^0$. Moreover, the $\Gamma_0(N)$-orbits $\Gamma_0(N)\backslash \mathcal{Q}_{N,D,r}^0$ of the set $\mathcal{Q}_{N,D,r}^0$ of $\mathcal{O}_D$ such that $N|A$ and

\(^3\)This condition was introduced by Birch [1].
\( B \equiv r \pmod{2N} \) may be identified with the set of Heegner points \((\mathbb{C}/a, \mathbb{C}/(n^{-1}a))\), and also with the set of \( \Gamma \) \( \equiv B \).

The field of definition \( H \) of each Heegner point \( x = (A, A') \) may be described as follows. Note that a point \( (A, A') \) on \( X_0(N)(\mathbb{C}) \) is a Heegner point associated to \( D \) if and only if \( \text{End}(A) = \text{End}(A') = \mathcal{O}_D \). So \( H = K(\tau) \) where \( \tau = \frac{B + \sqrt{D}}{2A} \) is as above, and by the theory of Complex Multiplication the action of the Galois group \( \text{Gal}(K^{\text{alg}}/K) \) on \( x \) is determined by a homomorphism

\[
\delta: \text{Gal}(K^{\text{alg}}/K) \rightarrow \text{Pic}(\mathcal{O}_D)
\]

such that \( \delta(\sigma) \ast x = x^\sigma \), where \( \ast \) is defined by \( b \ast x = (\mathcal{O}_D, n_r, [b^{-1}a]) \). In other words \( H \) is the fixed field of the Galois group \( \ker(\delta) \) and \( \text{Gal}(H/K) \cong \text{Pic}(\mathcal{O}_D) \). The field \( H \) is known as the ring class field attached to \( \mathcal{O}_D \), i.e. the maximal abelian extension of \( K \) unramified at all primes \( p \) of \( K \) which do not divide \( f \). More precisely, the homomorphism \( \delta \) is the inverse of the Artin reciprocity map, so in fact \( \delta(\text{Frob}_p) = [p] \) for each prime \( p \) of \( K \) which does not divide \( f \), where \( \text{Frob}_p \in \text{Gal}(H/K) \) is the Frobenius element at \( p \), which is characterised by the properties \( \text{Frob}_p \mathfrak{p} = \mathfrak{p} \) and \( \text{Frob}_p \alpha \equiv \alpha^q \pmod{\mathfrak{p}} \), for each \( \alpha \) in the ring of integers \( \mathcal{O}_H \) of \( H \), where \( \mathfrak{p} \) is a prime ideal of \( H \) above \( p \) and \( q = \#(\mathcal{O}_K/p) \).

To simplify the exposition we assume from now on that the discriminant \( D \) is fundamental, and also that \( E(\mathbb{Q}) \cong \mathbb{Z} \). The weighted trace \( y_{D,r,\varphi} \) on \( E \) associated to the pair \((D, r)\) may be defined by the equation

\[
y_{D,r,\varphi} = \sum_{a \in \text{Pic}(\mathcal{O}_D)} \varphi(\mathcal{O}_D, n_r, [a]),
\]

where

\[
u_D = \begin{cases} 
\frac{1}{2} \#(\mathcal{O}_D^\times), & \text{if } \#(\mathcal{O}_D^\times) > 2, \\
2, & \text{if } \#(\mathcal{O}_D^\times) = 2 \text{ and } N|D, \\
1, & \text{otherwise}.
\end{cases}
\]

We claim that \( y_{D,r,\varphi} \) is a rational point on \( E \). Since \( K \) is an imaginary quadratic field, the non-trivial element of \( \text{Gal}(K/\mathbb{Q}) \) is complex conjugation, which acts on Heegner points as \((\mathcal{O}_D, n_r, [a]) \mapsto (\mathcal{O}_D, n_{-r}, [a^{-1}])\). Also, note that the action of the Fricke involution \( w_N \) is given by \( w_N(\mathcal{O}_D, n_r, [a]) = (\mathcal{O}_D, n_{-r}, [n^{-1}a]) \). Therefore the action of \( w_N \) on the right-hand side of Equation 3.1 is the same as that of complex conjugation. But we assumed \( \varphi \) factors through the canonical quotient map \( X_0(N) \rightarrow X_0^+(N) \) associated to \( w_N \). Thus the right-hand side of Equation 3.1 is defined over \( \mathbb{Q} \). Finally, each Heegner point \( \tau \in \mathfrak{h} \) of discriminant \( D \) is the fixed point of an element of order \( u_D \) of the group generated by \( \Gamma_0(N) \) and the Fricke involution \( w_N \) (cf. Zagier [17]), and our claim follows.
Recall we assumed \( E(\mathbb{Q}) \cong \mathbb{Z} \). So we may fix a generator \( g_E \) of the Mordell-Weil group \( E(\mathbb{Q}) \) of \( E \) over \( \mathbb{Q} \). The index \( I_{D,r,\varphi} \) of \( y_{D,r,\varphi} \) in \( E(\mathbb{Q}) \) may be expressed as
\[
y_{D,r,\varphi} = I_{D,r,\varphi} g_E;
\]
We are interested in the index \( I_{\varphi} \) of the group generated by the Heegner points, i.e. the greatest common divisor of the indexes \( I_{D,r,\varphi} \) for all pairs \((D, r)\) that satisfy the Heegner condition.

3.3. **Heegner paths.** Suppose that the pair \((\Delta, \rho)\) satisfies the Heegner condition. Suppose further that \( \Delta > 0 \) and that \( \Delta \) is not the square of an integer. Assume the above notation and let \( Q = [A, B, C] \in Q_0^0 \). The condition \( N | A \) implies that all the automorphs of \( Q \) lie in \( \Gamma_0(N) \). More explicitly, if \((x, y) \in \mathbb{Z} \times \mathbb{Z} \) is a fundamental solution of Pell’s equation \( X^2 - DY^2 = 1 \) then the fundamental automorph of \( Q \) given by
\[
M_Q = \begin{pmatrix} x - By & -2Cy \\ 2Ay & x + By \end{pmatrix}
\]
lies in \( \Gamma_0(N) \). Note that \( M_Q \) fixes \( \tau^+(Q) = \frac{-B \pm \sqrt{\Delta}}{2A} \in \mathbb{P}^1(\mathbb{R}) \). We normalise our choice of \( M_Q \) by assuming that the eigenvalue \( \lambda_Q = x + y\sqrt{\Delta} \in \mathcal{O}_D^x \) is \( \lambda_Q > 1 \), so that \( \tau^-(Q) \) is repelling and \( \tau^+(Q) \) is attracting. The axis of \( M_Q \) is the geodesic \( \{\tau^-(Q), \tau^+(Q)\} \subset \mathfrak{h} \) from \( \tau^-(Q) \) to \( \tau^+(Q) \). Clearly it is stable under the action of \( M_Q \) and has the same orientation as the geodesic segment \( \{\tau_0, M_Q\tau_0\} \), given any point \( \tau_0 \) on it. Now let \( \gamma_{Q,\tau_0} \) be the closed path on \( X_0(N)(\mathbb{C}) \) defined by \( \{\tau_0, M_Q\tau_0\} \). It is a smooth path on \( X_0(N)(\mathbb{C}) \) except when it contains an elliptic point of order 2, in which case \( \gamma_{Q,\tau_0} = -\gamma_{Q,\tau_0} \) as 1-cycles. Note \( \gamma_{Q,\tau_0} \) depends only on the \( \Gamma_0(N) \)-equivalence class of \( Q \) so given \((D_0, r_0)\) and \((D_1, r_1)\) that satisfy the Heegner condition we may define the (twisted) Heegner cycle
\[
\gamma_{D_0,D_1,\rho} = \sum_{[Q] \in \Gamma_0(N) \setminus Q_0^0} \chi_{D_0}(Q) \gamma_{Q}
\]
where \( \chi_{D_0} \) is the generalised genus character, following Gross-Kohnen-Zagier [9, p. 508]:
\[
\chi_{D_0}(Q) = \begin{cases} \left( \frac{D_0}{n} \right), & \text{if } \gcd(A/N, B/C, D_0) = 1 \\ 0, & \text{otherwise.} \end{cases}
\]
where \( \Delta = D_0D_1 \) and \( \rho = r_0r_1 \). Here in the first case \( n \) is an integer represented by \([A/N', B/CN']\), where \( N' \) is a positive divisor of \( N \), and \( Q = [A, B, C] \). Note \( \gamma_{D_0,D_1,\rho} \) is invariant with respect the action of the Fricke involution \( w_N \), so it defines a 1-cycle on the quotient Riemann surface \( X_0^+(N)(\mathbb{C}) \). If we assume further that \( D_0 < 0 \) and \( D_1 < 0 \), then the Heegner cycle \( \gamma_{D_0,D_1,\rho} \) is anti-invariant under the action of complex
conjugation on $X_0^+(N)(\mathbb{C})$. In particular the homology class $[\gamma_{D_0,D_1,\rho}]$ represented by the cycle $\gamma_{D_0,D_1,\rho}$ in fact lies in the $-1$-eigenspace $H_1(X_0^+(N)(\mathbb{C}),\mathbb{Z})^-$. Following Gross-Kohnen-Zagier [9, p. 559] we may define an element $e \in H_1(E(\mathbb{C}),\mathbb{Z})^-$ such that

$$\text{det} \begin{pmatrix} 
\gamma(D_0, D_1, r_0 r_1) 
\end{pmatrix} E = I_{D_0, r_0, E} I_{D_1, r_1, E} e_E,
$$

where $[\gamma(D_0, D_1, r_0 r_1)]_E$ is the canonical image in $H_1(E(\mathbb{C}),\mathbb{Z})^-$ of the homology class $[\gamma(D_0, D_1, r_0 r_1)]$, and as above $I_{D_i, r_i, E}$ denotes the index of the trace $y_{D_i, r_i, E}$ in $E(\mathbb{Q})$, for all pairs $(D_i, r_i)$ with $D < 0$ that satisfy the Heegner condition. It is well-known that the index $n_E$ of the subgroup generated by $e_E$ in $H_1(E(\mathbb{C}),\mathbb{Z})^-$ is uniquely defined by the above condition.

Ogg [11] describes the real locus $(S/w_m)(\mathbb{R})$ of quotients $S/w_m$ of Shimura curves $S$, attached to Eichler orders $\mathcal{O}$ of indefinite quaternion algebras over $\mathbb{Q}$, in terms of embeddings of $\mathbb{Q}(\sqrt{m})$ into $\mathcal{O}$. In particular, from his work it is known that the number $\nu_N$ of connected components of $X_0^+(N)(\mathbb{R})$ is given by the formula

$$\nu_N = \begin{cases} 
\frac{h(4N)+h(N)}{2}, & \text{if } N \equiv 1 \pmod{4} \\
\frac{h(4N)+1}{2}, & \text{otherwise.}
\end{cases}$$

Moreover, as shown in [4] it is possible to describe explicitly the connected components of $X_0^+(N)(\mathbb{R})$ as a sum of “weighted” Heegner cycles over discriminants $\Delta > 0$ such that $N|\Delta$ and $\Delta|4N$, in analogy with the fixed points of the Fricke involution (cf. Gross [7]).

3.4. The conjecture. As above, let $E$ be an elliptic curve of rank one over $\mathbb{Q}$, and let $I_\psi$ be the index of the group generated by the Heegner points, i.e. the greatest common divisor of the indexes $I_{D, r, \psi}$ for all pairs $(D, r)$ that satisfy the Heegner condition with fundamental $D < 0$. From now on assume that $N_E$ is prime. In particular $E$ is alone in its isogeny class, so we may write $I_E$ instead of $I_\psi$.

**Conjecture 3.1.** If $I_E > 1$ then either the number $\nu_{N_E}$ of connected components of the real locus $X_0^+(N_E)(\mathbb{R})$ is $\nu_{N_E} > 1$ or the Tate-Safarevič group $\text{III}(E)$ of $E$ is non-trivial.

There are some curves $E$ in the range of our computations that have $\nu_{N_E} > 1$ but have index $I_E = 1$. So knowing $\nu_N$ is not enough in order to predict when $I_E > 1$. We sketch, in a rather impressionistic style, some ideas that hopefully will lead to a more aesthetically pleasing version of the conjecture as follows. As shown by Gross-Harris [8, pp. 164–165], given any complete, non-singular, geometrically connected curve defined over $\mathbb{R}$ the number $\nu$ of connected components of $X(\mathbb{R})$ may be recovered from the homology group $H_1(X(\mathbb{C}),\mathbb{F}_2)$, regarded as a symplectic
\( \mathbb{F}_2 \)-vector space with involution \( \tau \) induced by complex conjugation acting on \( X(\mathbb{C}) \).

In fact they prove that

\[ \nu = g + 1 - \text{rank}(H) \]

where \( g \) is the genus of \( X \), and \( H \) is the \( g \times g \) symmetric matrix defined by

\[ [\tau]_\beta = \begin{pmatrix} I_g & H \\ 0 & I_g \end{pmatrix}, \]

where \( \beta \) is a suitable symplectic basis for \( H_1(X(\mathbb{C}), \mathbb{F}_2) \). So our conjecture may be expressed in homological terms. It is hoped that a more refined version of our conjecture may be meaningfully stated in terms of a finer homological invariant, perhaps associated to the modular parametrisation \( X_0^+(N) \to E \) over \( \mathbb{Q}_p \) for each prime \( p \), with special attention to the primes \( p = N, \infty \); maybe there is some kind of “product formula” for \( n_E \) in which \( \nu_N \) is just a very crude approximation to the contribution from \( p = \infty \). Such formula might lead to a more natural form of Equation 1.1, if we consider that the Tate-Šafarevič group \( \text{III}(E) \) is a subgroup of the cohomology group \( H^1(G_{\mathbb{Q}}, E) \) determined by local conditions.

Table 1 and Table 2 (below) were computed as follows. For each elliptic curve \( E \) of rank one over \( \mathbb{Q} \) and prime conductor \( N_E < 129999 \), we computed the greatest common divisor \( d \) of the indexes \( I_{D,E} \), for each pair \((D, r)\) that satisfies the Heegner condition with \( D < 0 \) fundamental and \( |D| \leq 163 \). Such \( d \) is likely to be the index \( I_E \) of the group generated by all the traces \( y_{D,E} \) in \( E(\mathbb{Q}) \) in the range \( N_E < 129999 \). All our elliptic curve data comes from Cremona’s Tables [5], and we stick to the notation used there.

**References**

1. B.J. Birch, *Heegner points of elliptic curves*, Symp. Mat., Ist. di Alta Mat., vol. 15, Academic Press, London, 1975, pp. 411–445.
2. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over \( \mathbb{Q} \): wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843–939 (electronic).
3. J.W.S. Cassels, *Lectures on elliptic curves*, Cambridge University Press, Cambridge, 1991.
4. C. Castaño-Bernard, *On certain sets of Heegner points Heegner paths*, University of Cambridge, 2005, Ph. D. thesis.
5. J.E. Cremona, *Elliptic curves of conductor \( \leq 20,000 \)*,
   http://www.maths.nott.ac.uk/personal/jec/ftp/data/.
6. B.H. Gross, *Heegner points on \( X_0(N) \)*, Modular forms (Durham, 1983), Horwood, Chichester, 1984, pp. 87–105.
7. _____, *Heegner points and the modular curve of prime level*, J. Math. Soc. Japan 39 (1987), no. 2, 345–362.
8. B.H. Gross and J. Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) 14 (1981), no. 2, 157–182.
9. B.H. Gross, W. Kohnen, and D.B. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. 278 (1987), no. 1–4, 497–562.
| $E$    | $I_E$ | $\nu_{N_E}$ | $\text{III}(E)$ | $E$          | $I_E$ | $\nu_{N_E}$ | $\text{III}(E)$ |
|--------|-------|--------------|-----------------|--------------|-------|--------------|-----------------|
| 359A   | 2  2  | 1            |                 | 39133A      | 2  2  | 1            |                 |
| 359B   | 2  2  | 1            |                 | 39133B      | 2  2  | 1            |                 |
| 997A   | 2  2  | 1            |                 | 39301A      | 2  14 | 1            |                 |
| 3797A  | 2  2  | 1            |                 | 40237A      | 2  2  | 1            |                 |
| 4159A  | 2  2  | 1            |                 | 45979A      | 4  2  | 4            |                 |
| 4159B  | 2  2  | 1            |                 | 47143A      | 2  2  | 1            |                 |
| 6373A  | 2  2  | 1            |                 | 47309A      | 2  2  | 1            |                 |
| 8069A  | 2  3  | 1            |                 | 48731A      | 4  1  | 4            |                 |
| 8597A  | 2  6  | 1            |                 | 50329A      | 2  3  | 1            |                 |
| 9829A  | 2  10 | 1            |                 | 51437A      | 2  6  | 1            |                 |
| 13723A | 2  2  | 1            |                 | 52237A      | 2  2  | 1            |                 |
| 17299A | 2  2  | 1            |                 | 55837A      | 2  14 | 1            |                 |
| 17573A | 2  2  | 1            |                 | 59243A      | 2  2  | 1            |                 |
| 18097A | 2  3  | 1            |                 | 61909A      | 2  6  | 1            |                 |
| 18397A | 2  2  | 1            |                 | 62191A      | 2  5  | 1            |                 |
| 20323A | 2  2  | 1            |                 | 63149A      | 2  2  | 1            |                 |
| 21283A | 2  2  | 1            |                 | 65789A      | 2  2  | 1            |                 |
| 23957A | 2  6  | 1            |                 | 66109A      | 2  2  | 1            |                 |
| 24251A | 2  5  | 1            |                 | 66109B      | 2  2  | 1            |                 |
| 26083A | 2  2  | 1            |                 | 67427A      | 2  5  | 1            |                 |
| 28621A | 2  2  | 1            |                 | 68489B      | 2  3  | 1            |                 |
| 28927A | 2  2  | 1            |                 | 69677A      | 2  2  | 1            |                 |
| 29101A | 2  2  | 1            |                 | 72053A      | 2  2  | 1            |                 |
| 29501A | 2  2  | 1            |                 | 73709A      | 2  2  | 1            |                 |
| 31039A | 2  2  | 1            |                 | 74411A      | 2  2  | 1            |                 |
| 31319A | 2  2  | 1            |                 | 74713A      | 4  3  | 4            |                 |
| 33629A | 2  2  | 1            |                 | 74797A      | 2  2  | 1            |                 |
| 34613A | 2  2  | 1            |                 | 77849A      | 2  3  | 1            |                 |
| 34721A | 2  3  | 1            |                 | 78277A      | 2  2  | 1            |                 |
| 35083B | 4  1  | 4            |                 | 78919A      | 2  2  | 1            |                 |
| 35401A | 2  3  | 1            |                 | 81163B      | 2  2  | 1            |                 |
| 35533A | 2  2  | 1            |                 | 81349A      | 2  2  | 1            |                 |
| 36479A | 2  11 | 1            |                 | 82301A      | 2  2  | 1            |                 |
| 36781A | 2  2  | 1            |                 | 84653A      | 2  2  | 1            |                 |
| 36781B | 2  2  | 1            |                 | 84701A      | 2  3  | 1            |                 |
Table 2. Nontrivial indexes $I_E$ for prime $85837 \leq N < 129999$.

| $E$       | $I_E$ | $\nu_{N_E}$ | $\text{III}(E)$ | $E$       | $I_E$ | $\nu_{N_E}$ | $\text{III}(E)$ |
|-----------|-------|-------------|-----------------|-----------|-------|-------------|-----------------|
| 85837A    | 2     | 2           | 1               | 108971A   | 2     | 2           | 1               |
| 87013A    | 2     | 3           | 1               | 113933A   | 2     | 2           | 1               |
| 90001B    | 2     | 87          | 1               | 118673A   | 2     | 3           | 1               |
| 90001C    | 2     | 87          | 1               | 119689A   | 2     | 3           | 1               |
| 90001D    | 2     | 87          | 1               | 119701A   | 2     | 3           | 1               |
| 91381A    | 2     | 2           | 1               | 119773A   | 2     | 2           | 1               |
| 92419A    | 4     | 1           | 4               | 123791A   | 2     | 2           | 1               |
| 101771A   | 2     | 2           | 1               | 124213A   | 2     | 2           | 1               |
| 101879A   | 2     | 2           | 1               | 126683A   | 2     | 2           | 1               |
| 102061B   | 2     | 6           | 1               | 127669A   | 2     | 2           | 1               |
| 103811A   | 2     | 2           | 1               | 129277A   | 2     | 2           | 1               |
| 104239A   | 4     | 14          | 4               | 129853A   | 2     | 2           | 1               |
| 104239B   | 4     | 14          | 4               |           |       |             |                 |
| 105143A   | 2     | 2           | 1               |           |       |             |                 |
| 105401A   | 2     | 3           | 1               |           |       |             |                 |
| 105541A   | 2     | 2           | 1               |           |       |             |                 |
| 106277A   | 2     | 14          | 1               |           |       |             |                 |
| 106949A   | 2     | 2           | 1               |           |       |             |                 |
| 106979A   | 4     | 1           | 4               |           |       |             |                 |
| 107981A   | 2     | 2           | 1               |           |       |             |                 |

10. V. A. Kolyvagin, Euler systems, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.
11. A. P. Ogg, Real points on Shimura curves, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 277–307.
12. The PARI Group, Bordeaux, PARI/GP, Version 2.1.5, http://www.parigp-home.de/.
13. A. R. Perlis, On the projective geometry of curves of genus one, and an algorithm for the jacobian of such a curve, University of Arizona, 2004, Ph. D. thesis.
14. E. S. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math. 85 (1951), 203–362 (1 plate).
15. J. T. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.
16. A. Wiles, Modular elliptic curves and fermat’s last theorem, Ann. of Math. 141 (1995), no. 3, 443–551.
17. D. Zagier, Modular points, modular curves, modular surfaces and modular forms, Workshop Bonn 1984, Lecture Notes in Math., vol. 1111, Springer, Berlin, 1985, pp. 225–248.
URL: http://users.ictp.it/~ccastano/
E-mail address: ccastano@ictp.it

Mathematics Section, ICTP, Strada Costiera 11, I-34014 Trieste (Italy)