BOUNDING RANKS OF ELLIPTIC CURVES

by

Jung-Jo Lee

A dissertation submitted to The Johns Hopkins University
in conformity with the requirements for the degree of
Doctor of Philosophy

The Johns Hopkins University
June 7, 2002

ABSTRACT

The purpose of this paper is to provide a new way of approach and get a result on the rank bound problem.

We construct cohomology classes from quadratic twisted elliptic curves very similar to Kolyvagin's cohomology classes. We verify that these cohomology classes satisfy a formula for computation as was obtained by Kolyvagin.

This has an immediate consequence of $E_{(D)}(\mathbb{Q}) \subset E_{(D)}(\mathbb{R})^0$ if E and D satisfy some conditions which will be described.

The formulas from the construction, combined with mod 2 algebra, gives us a bound of $\operatorname{rank} E(\mathbb{Q}) \leqslant 2n$ if $\mathbb{Q}(\sqrt{\Delta})$ is a PID where n is the number of prime divisors of $2N\infty$. Here $\Delta = \Delta(E)$ is the discriminant and N is the conductor of E. This result extends our knowledge on the rank bound.

This dissertation was read by my advisor
Professor Joseph Shalika.

ACKNOWLEDGEMENT

I would like to express my deep gratitude to Professor Kolyvagin, Professor Ram Murty and Professor Shalika for their invaluable ideas, help and guidance.

I also would like to thank Professor Jordan Ellenberg for reading the first draft of my dissertation.

Finally, I wish to thank Professor Myung-Hwan Kim, my friends both at Johns Hopkins and Seoul National University, and my family for their encouragements and patience.

CONTENTS

1. INTRODUCTION

Let E be an elliptic curve defined by a Weierstrass equation

$$y^2 = x^3 + Ax + B \text{ with } A, B \in \mathbb{Q}. \tag{1}$$

The points of $E(\mathbb{Q})$ have a natural, geometrically-defined group structure, with the point at infinity O as its identity element. By the Mordell-Weil theorem,

$$E(\mathbb{Q}) \simeq F \times \mathbb{Z}^r$$

where F is a torsion subgroup of $E(\mathbb{Q})$. Here r is a non-negative integer, called the rank of E over $\mathbb{Q}$.

Let $E_{(D)}$ be an elliptic curve defined by a Weierstrass equation

$$Dy^2 = x^3 + Ax + B \text{ with } A, B \in \mathbb{Q}$$

which we call the D-twisted elliptic curve of E given in (1). So E and $E_{(D)}$ are isomorphic over $K = \mathbb{Q}(\sqrt{D})$.

We are interested in understanding the structure of $E(\mathbb{Q})$ and finding points of $E(\mathbb{Q})$.

For the torsion part, the structure of the group over $\mathbb{Q}$ is fairly well known. On the other hand, to find the rank remains as the one of the most challenging problem of mathematics.

There is a conjecture which says that there can be an "effective" algorithm to compute the rank r.

Conjecture (Birch–Swinnerton-Dyer Conjecture)**.** *Let E be a modular elliptic curve over $\mathbb{Q}$. If r is the rank of E over $\mathbb{Q}$, then the function $L(E, s)$ has a zero of exact order r at $s = 1$.*

Every elliptic curve over $\mathbb{Q}$ is modular. In the above statement "modular" means *Weil parametrization* and important properties of elliptic curves which follow from it.

We call $k = \text{ord}_{s=1} L(E, s)$ the analytic rank of E. So the Birch–Swinnerton-Dyer Conjecture claims that the rank of an elliptic curve is the same as its analytic rank.

The full version of this conjecture relates important arithmetical quantities of E (the order of Shafarevich-Tate group Ш, elliptic regulator, Tamagawa factor, etc.) to the first non-zero coefficient of the L-function of E.

There is a partial result on this conjecture.

Theorem 1.1. *[Kolyvagin, 1988] Let E be a modular curve. Let r be the rank of E over $\mathbb{Q}$. If $\mathrm{ord}_{s=1}L(E,s) = k \leqslant 1$, then $k = r$ and Ш is finite. (And up to some simple factors, the order of Ш divides the order of the conjectural Ш involved in Birch–Swinnerton-Dyer Conjecture.)*

Before Kolyvagin's work, the Birch–Swinnerton-Dyer Conjecture(BSD Conjecture) for $k \leqslant 1$ was known for CM elliptic curves from the results of Coates-Wiles, Gross-Zagier and Rubin. (For the reference, see [IR] Chapter 20.)

Although we expect that there are elliptic curves over $\mathbb{Q}$ with arbitrarily high ranks it is still unknown showing the difference of our situation from the Dirichlet Unit Theorem if we consider the analogy of the Mordell-Weil group with the unit group of an order of any algebraic number field. ([BSh] Chapter 2, §4.3.)

Conjecture (Mai and R. Murty)**.** *Let N be the conductor of E. Then we have*

$$\mathrm{rank}\, E(\mathbb{Q}) = O\Big(\big(\frac{\log N}{\log\log N}\big)^{1/2}\Big).$$

For the idea of this conjecture, see the appendix of [Ra].

Theorem 1.2 (Mestre)**.** *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. The analytic rank of E is bounded by $O\Big(\frac{\log N}{\log\log N}\Big)$ under Generalized Riemann Hypothesis.*

For the proof of this, see [Me], III-2.

In this paper, we will prove that the rank of an elliptic curve is bounded by the estimation of Mestre in the following case:

Theorem 1.3. *Let $E(\mathbb{Q})_2 = O$ and $\mathbb{Q}(\sqrt{\Delta})$ is a PID. Then $\mathrm{rank}\, E(\mathbb{Q}) \leqslant 2n$ where Δ is the discriminant of E and n is the number of prime divisors of $2N\infty$. Here N is the conductor of E.*

In particular, Theorem 1.3 implies that if $\Delta = -16(4A^3 + 27B^2)$ is a square of a rational number, then we have the desired rank bound: $\mathrm{rank}\, E(\mathbb{Q}) \leqslant 2n$.

If $\Delta < 0$, then we know that there are only finitely many fields $\mathbb{Q}(\sqrt{\Delta})$ which is a PID. This is so called Gauss's class number 1 problem, which was solved (with a gap) by Heegner in 1952. On the other hand, Gauss had already noticed that many real quadratic number fields are PID's. Considering such fields which have prime discriminant, computations show that about 80% of them are PID's. ([IR], p.361.)

Let $\nu(x)$ denote the number of prime divisors of x for $x \in \mathbb{Z}$. A theorem of Ramanujan says that $\nu(N) \leqslant O\Big(\dfrac{\log N}{\log\log N}\Big)$. Therefore, our result would imply Mestre's result if we assume BSD conjecture. Moreover, we do *not* assume the Generalized Riemann Hypothesis.

Theorem 1.3 was previously known for the case $E(\mathbb{Q})_2 \cong \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$. A very similar result for $E(\mathbb{Q})_2 \cong \mathbb{Z}/2\mathbb{Z}$ can be found in Coates paper based on Tate's unpublished lecture note. (See the appendix of [Co].) But when $E(\mathbb{Q})_2 = O$, the above theorem was unknown.

There were also previous results on this kind of problem involving the ideal class number. Our improvement here is to remove the factor related to the ideal class number from the following bounds of Brumer-Kramer and Honda. It is significant because to compute the ideal class number of a number field is more old problem and as hard as to compute the rank of an elliptic curve. And we know that the ideal class number can be arbitrarily big.

Theorem 1.4 (Brumer and Kramer)**.** *Suppose that E has no rational point of order two. Then*

$$\operatorname{rank} E(\mathbb{Q}) + [Ш_2] \leqslant g + u + e + \sum_{p \in \Phi_a} (n_p - 1)$$

where

Φ_a	*set of rational primes at which E has additive reduction,*
Φ_m	*set of rational primes at which E has mult. reduction with* $\operatorname{ord}\Delta$ *even,*
e	$[\Phi_m]$,
F	*cubic subfield of two-division field of E,*
g	*dimension of ideal class group of F modulo squares,*
u	*1 or 2 according to the sign of Δ,*
n_p	*number of primes lying over p in F.*

The Theorem 1.4 is the Proposition 7.1 in [BK].

Theorem 1.5 (Honda). $\operatorname{rank} E(\mathbb{Q}) \leqslant 2(s+2[L:\mathbb{Q}]+h_L(2))$, *where* s *is the number of prime divisors of* N *and* $h_L(2)$ *is the 2-rank of the absolute ideal class group of* L, *where* $L = \mathbb{Q}(E_2)$.

The Theorem 1.5 follows from Theorem 5 in [Hon].

The main idea in the proof of Theorem 1.3 is to apply the local-global duality theorem (a reformulation of the reciprocity law) with the explicitly constructed cohomology classes. It is similar to Kolyvagin's idea when he proved Theorem 1.1. In Kolyvagin's case explicit cohomology classes are constructed from Heegner points, whereas in our proof they are constructed from the points of quadratic twisted elliptic curves.

Here "explicit" means that we can describe its construction and control the behavior of such cohomology classes in localizations, and consequently we can obtain an explicit interpretation of the reciprocity law.

In this paper, we apply a variation of Kolyvagin's theory into families of quadratic twists by considering the curve over varying quadratic extensions instead of extending base fields by ring class fields with growing conductor in his case. It is reasonable to expect that if Kolyvagin was able to bound the size of Selmer group using the theory of Euler Systems and study Ш from it, then a similar method can be used to put restrictions on the Mordell-Weil group itself.

The construction of cohomology classes from quadratic twisted elliptic curves will be described in §3.

It will be verified in Proposition 4.2 that Kolyvagin's fundamental formula interpreting the reciprocity law (which is the formula computing the value of Tate pairing) works in our case as well.

The main results of this paper are contained in §5, §6 and §7.

For any elliptic curve A, let $A(\mathbb{R})^0$ denote the connected component of the identity in $A(\mathbb{R})$, in other words, $A(\mathbb{R})^0 = 2A(\mathbb{R})$ under the addition operation of an elliptic curve. Let E denote a given elliptic curve. Assume that the discriminant $\Delta(E) > 0$ and $E(\mathbb{Q})_2 \neq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$. We will obtain a sufficient condition on D so that $E_{(D)}(\mathbb{Q}) \subset E_{(D)}(\mathbb{R})^0$ in §5. And we will find enough numerical data for this in §6.

In §7, we will find the rank bound depending on the number of prime divisors of conductor as stated in Theorem 1.3. The first proof of this (which is slightly

different) uses Gupta and Murty's result on the elliptic curve analogue of Artin's primitive root conjecture[GM]. Later, Prof. Ram Murty pointed out that what is needed here is weaker than their result, and suggested ways of avoiding their result so that we can remove the assumption of Generalized Riemann Hypothesis or other restrictions of their result. Consequently, it worked out as he suggested.

We introduce some common notations. If M is a field, then $\overline{\mathrm{M}}$ is an algebraic closure of M. If L/M is a Galois extension, then Gal(L/M) denotes the Galois group of L over M. We shall use the abbreviations $H^1(\mathrm{M}, A) = H^1(\mathrm{Gal}(\overline{\mathrm{M}}/\mathrm{M}), A)$, where A is a $\mathrm{Gal}(\overline{\mathrm{M}}/\mathrm{M})$-module, and $H^1(\mathrm{M}, E) = H^1(\mathrm{M}, E(\overline{\mathrm{M}}))$ for an elliptic curve E. If O is a commutative ring with identity, then O^* denotes the group of invertible elements of O. For $x \in \mathbb{Z}$, the number $\nu(x)$ denotes the number of prime divisors of x. The field $\overline{\mathbb{Q}}$ is assumed to be embedded in the field of complex numbers $\mathbb{C}$. $a \,|\, b$ denotes that b is divisible by a. For $Q \in E_{(D)}(\mathbb{Q})$, $\mathrm{red}\,(Q)$ at the corresponding place will denote the reduction of the image of Q in $E(K)$ under some inclusion of $E_{(D)}(\mathbb{Q})$ into $E(K)$ where $K = \mathbb{Q}(\sqrt{D})$.

2. GALOIS COHOMOLOGY AND DUALITIES

In this section, how the local and global dualities of class field theory are used to study elliptic curves is explained. In Kolyvagin's papers [Ko1], [Ko2] and [Ko3], this gives a mechanism for bounding the Selmer group and it has the applications to the study of the ideal class group, Iwasawa's main conjecture, Mordell-Weil group of an elliptic curve, Ш (the Safarevich-Tate group), Birch-Swinnerton-Dyer conjecture, and a study of the p-adic main conjecture for elliptic curves. The reader can find the material of this section from [Ru] and [La2].

Let's recall the cohomology theory of elliptic curves over $\mathbb{Q}$.

Let $\mathbf{F}$ be any field and let M be a positive integer such that $(M, \mathit{char}\,\mathbf{F}) = 1$ if $\mathit{char}\,\mathbf{F} > 0$. For a given elliptic curve E, $E_M = E(\overline{\mathbf{F}})_M = \mathbb{Z}/M\mathbb{Z} + \mathbb{Z}/M\mathbb{Z}$ denotes the $G(\overline{\mathbf{F}}/\mathbf{F})$-module of M-torsion points of E over $\overline{\mathbf{F}}$. And μ_M denotes the set of M-th roots of unity of the field.

Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. $E(\overline{\mathbb{Q}})$ has a G-module structure.

A cocycle $\varphi : G \to E(\overline{\mathbb{Q}})$ is given by a continuous homomorphism satisfying

$$\varphi(g_1 g_2) = g_1\varphi(g_2) + \varphi(g_1) \text{ for all } g_1,\, g_2 \in G.$$

Here a cocycle is continuous means that it may be factored through a finite quotient of G, that is, there exists a finite Galois extension F of $\mathbb{Q}$ such that φ is trivial on $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$.

And a coboundary ψ is given by a cocycle satisfying a further condition that

$$\psi(g) = gP - P \text{ with } P \in E(\overline{\mathbb{Q}}) \text{ for all } g \in G.$$

It is easy to check that $\psi(g_1 g_2) = g_1\psi(g_2) + \psi(g_1)$.

A cocycle $\varphi : G(\overline{\mathbb{Q}}/\mathbb{Q}) \to E(\overline{\mathbb{Q}})$ has the property that there exists a cocycle $\varphi' : \mathrm{Gal}(L/\mathbb{Q}) \to E(L)$ where L is a finite Galois extension of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ such that φ is induced by $\varphi(g) = \varphi'(\text{g restricted to L})$ for all $g \in G$. So φ is determined by the following diagram

$$\begin{array}{ccc} G(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\;j\;} & \mathrm{Gal}(L/\mathbb{Q}) \\ & & \big\downarrow{\scriptstyle \varphi'} \\ & & E(L) \end{array}$$

where j is a natural surjection.

In other words we can consider the direct limit over L

$$\varinjlim H^1(\mathrm{Gal}(L/\mathbb{Q}), E(L))$$

where L runs through finite Galois extensions of $\mathbb{Q}$.

In this way, we get $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}}))$ abbreviated to $H^1(\mathbb{Q}, E)$.

The set of equivalence classes of main homogeneous spaces has a group structure isomorphic to $H^1(\mathbb{Q}, E)$.

Next, we have a natural localization map (via restriction):

$$loc_q \ : \ H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E(\overline{\mathbb{Q}})) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q), E(\overline{\mathbb{Q}}_q)).$$

Consider $G' = \{\, \sigma \mid \sigma : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}} \text{ an automorphism such that } \sigma \text{ is continuous}\}$. Then G' is a subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and we have $G' \tilde{\to} \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, which is obtained from direct limit of finite Galois extensions of $\mathbb{Q}_q$. (It is the same thing as to fix a system of extended valuations of ν_q, which is a valuation of $\mathbb{Q}$ to all finite Galois extensions in a compatible way. So our choice of automorphism is not unique, since extension of ν_q to $\overline{\mathbb{Q}}$ is not unique. In fact, $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of equivalence classes of valuations, thus loc_q doesn't depend on the choice of valuations.)

There is an important short exact sequence involving $H^1(E, \mathbb{Q})$ (recall that it classifies the main homogeneous spaces), which we shall call as our *fundamental exact sequence*

$$O \to E(\mathbb{Q})/ME(\mathbb{Q}) \to H^1(\mathbb{Q}, E_M) \to H^1(\mathbb{Q}, E)_M \to O. \tag{2}$$

There is a *duality pairing* which associates an M-th root of unity $[e_1, e_2]_M$ with two elements e_1 and e_2 of E_M, called the Weil pairing. (See [Shi] pp. 100-101 for definition and details.)

Suppose that M is relatively prime to the characteristic of the field $\mathbf{F}$. Then the Weil pairing $[\ ,\ ]_M \ : \ E_M \times E_M \to \mu_M$ has the following properties :

(a) bilinear : $[e_1 + e_2, e]_M = [e_1, e]_M [e_2, e]_M$
$\qquad\qquad [e, e_1 + e_2]_M = [e, e_1]_M [e, e_2]_M$;

(b) alternating : $[e, e]_M = 1$, so in particular $[e_1, e_2]_M = [e_2, e_1]_M^{-1}$;

(c) nondegenerate : If $[e_1, e_2]_M = 1$ for all $e_1 \in E_M$, then $e_2 = 1$;

(d) Galois invariant : For all $\sigma \in \mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})$, $[e_1, e_2]^\sigma = [e_1^\sigma, e_2^\sigma]$.

Remark. At level 2, the Weil pairing takes a very simple form:

$$[e_1, e_2]_2 = \begin{cases} 1 & \text{if } e_1 = O \text{ or } e_2 = O \text{ or } e_1 = e_2. \\ -1 & \text{otherwise.} \end{cases}$$

It can be checked easily by using properties of Weil pairing (a)–(c).

The Weil pairing induces a bilinear pairing (via cup-product), called the Tate pairing. Let's begin with the local Tate pairing.

Let q be a place of $\mathbb{Q}$. We have a sequence of maps

$$H^1(\mathbb{Q}_q, E_M) \times H^1(\mathbb{Q}_q, E_M) \xrightarrow{(a)} H^2(\mathbb{Q}_q, E_M \otimes E_M) \xrightarrow{(b)} \\ \xrightarrow{(b)} H^2(\mathbb{Q}_q, \mu_M) \xrightarrow{(c)} \mathbb{Z}/M\mathbb{Z} \qquad (3)$$

where (a) is the cup-product map, (b) is the map induced by the Weil pairing, and (c) is the canonical isomorphism obtained by a composition of isomorphisms

$$H^2(\mathbb{Q}_q, \mu_M) \to H^2(\mathbb{Q}_q, \overline{\mathbb{Q}}_q^*)_M \xrightarrow{inv} \frac{1}{M}\mathbb{Z}/\ \mathbb{Z} \xrightarrow{\times M} \mathbb{Z}/M\mathbb{Z}. \qquad (4)$$

Here $H^2(\mathbb{Q}_q, \overline{\mathbb{Q}}_q^*)_M = \mathrm{Br}(\mathbb{Q}_q)_M$ by definition of the Brauer group and inv is the mapping defined in local class field theory. (For the definition and properties of the Brauer group, see [CF] Chapter VI, §1.)

Further, we have the localization of our fundamental exact sequence (2).

$$0 \to E(\mathbb{Q}_q)/ME(\mathbb{Q}_q) \to H^1(\mathbb{Q}_q, E_M) \to H^1(\mathbb{Q}_q, E)_M \to 0. \qquad (2)_q$$

By this exact sequence $(2)_q$ for the first component of the pairing, and by the fact that $E(\mathbb{Q}_q)/ME(\mathbb{Q}_q)$ is an isotropic subgroup of $H^1(\mathbb{Q}_q, E_M)$ relative to the pairing $H^1(\mathbb{Q}_q, E_M) \times H^1(\mathbb{Q}_q, E_M) \to \mathbb{Z}/M\mathbb{Z}$ given by (3) for the second component (Pontryagin duality), we get an induced nondegenerate pairing

$$\langle\ ,\ \rangle_{q,M} : E(\mathbb{Q}_q)/ME(\mathbb{Q}_q) \times H^1(\mathbb{Q}_q, E)_M \to \mathbb{Z}/M\mathbb{Z}$$

which is called the (local) Tate pairing (at q).

The local Tate pairing

$$H^1(\mathbb{Q}_q, E_M) \times H^1(\mathbb{Q}_q, E_M) \to H^2(\mathbb{Q}_q, \mu_M) \subset \mathbb{Q}/\mathbb{Z}$$

is a *perfect* pairing. Hence the cohomology class c_q may be identified with the functional "cupping with c_q", $c_q : H^1(\mathbb{Q}_q, E_M) \to H^2(\mathbb{Q}_q, \mu_M)$.

Next, Global Class Field Theory tells us that if we compose the global (cup-product) pairing

$$H^1(\mathbb{Q}, E_M) \times H^1(\mathbb{Q}, E_M) \to H^2(\mathbb{Q}, \mu_M)$$

with the homomorphism $H^2(\mathbb{Q}, \mu_M) \to \mathbb{Q}/\mathbb{Z}$ which is given by summing local invariants, we get a bilinear pairing

$$H^1(\mathbb{Q}, E_M) \times H^1(\mathbb{Q}, E_M) \to \mathbb{Q}/\mathbb{Z}$$

which has the virtue of vanishing identically. This follows from global class field theory that for an element of the Brauer group the sum of the local invariants at all primes is zero. (For reference see [CF] Chapter VII, Theorem B of §10.)

Finally, we have the global-to-local restriction mappings

$$H^1(\mathbb{Q}, E_M) \longrightarrow \prod_q H^1(\mathbb{Q}_q, E_M),$$

(denoting by $\prod_q c_q$ the image of the global cohomology class c), which connects the local and global class field theories.

Theorem 2.1 (Orthogonality Relation for Elliptic Curves)**.**

For $P \in E(\mathbb{Q})/ME(\mathbb{Q})$ and $C \in H^1(\mathbb{Q}, E)_M$, the sum of the local Tate pairing $\langle P_q, C_q \rangle_{q,M}$ over all prime divisors of $\mathbb{Q}$ (including ∞) equals zero where P_q and C_q are the localizations of P and C respectively.

The relation $\sum_q \langle P_q, C_q \rangle_{q,M} = 0$, which is a reformulation of the reciprocity law, is called the orthogonality relation.

For Theorem 2.1 over general number fields, see [Wa] p.267.

3. CONSTRUCTION OF COHOMOLOGY CLASSES FROM TWISTS

To construct explicit main homogeneous spaces it is essential to find points of trivial norm in our method. The construction idea of this section comes from Kolyvagin. As mentioned in Introduction, we will construct them using rational points on quadratic twists.

Let L/K be a Galois extension with its Galois group G isomorphic to a cyclic group of order M generated by t.

$$G = \mathrm{Gal}(L/K) \tilde{\to} \mathbb{Z}/M\mathbb{Z} = \{\, t^j,\ j = 0, \cdots, M-1\}.$$

G acts on $E(L)$.

When P is a point of trivial norm, then we can construct cocycles of $H^1(G, E(L))$, namely, define $\varphi : G \to E(L)$ by the conditions

$$\varphi(t^0) = 0 \text{ and } \varphi(t^j) = (1 + \cdots + t^{j-1})P,\ \ 1 \leqslant j \leqslant M-1\,.$$

We can show that φ defined in this way are cocycles by checking: $\varphi(g_1 g_2) = g_1\varphi(g_2) + \varphi(g_1)$.

Proposition 3.1. *Every element of $H^1(G(L/K), E(L))$ is obtained in the way described above.*

Proof. A cocycle is a continuous homomorphism satisfying

$$\varphi(g_1 g_2) = g_1\varphi(g_2) + \varphi(g_1).$$

Since the Galois group $G(L/K)$ is a cyclic group of order M generated by t, the cocycle φ is determined by its values at t^i $(0 \leqslant i \leqslant M-1)$, $\varphi(t^i) = t\varphi(t^{i-1}) + \varphi(t)$.

So $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) + \varphi(1) \Rightarrow \varphi(1) = 0$,

$\varphi(t) = \varphi(t \cdot 1) = t\varphi(1) + \varphi(t) \Rightarrow \varphi(1) = 0$,

$\varphi(t^2) = \varphi(t \cdot t) = t\varphi(t) + \varphi(t) = (t+1)\varphi(t)$,

and so on.

Let's use induction on i.

$\varphi(t^i) = t(t^{i-2} + \cdots + 1)\varphi(t) + \varphi(t) = (t^{i-1} + t^{i-2} + \cdots + t + 1)\varphi(t)$.

So every cocycle should be of the given form.

Moreover $\mathrm{Norm}(\varphi(t)) = \varphi(t^M) = \varphi(1) = 0$. So $\varphi(t)$ should be some point of trivial norm. On the other hand, the mapping φ defined as above is a well-defined

cocycle. Thus the cohomology classes are well-defined in this form if and only if $\varphi(t)$ is a point of trivial norm. $\square$

Now we will discuss on the points of trivial norm coming from quadratic twists and construct corresponding cohomology classes.

Let E be an elliptic curve given by a Weierstrass equation $y^2 = x^3 + Ax + B$ and $E_{(D)}$ its quadratic twist given by $Dy^2 = x^3 + Ax + B$ where D is a square-free integer. Let's denote by N the conductor of E. We can construct explicit homogeneous spaces from $E_{(D)}(\mathbb{Q})$ whose rational points will be studied through the orthogonality relation with rational points of E.

Let $K = \mathbb{Q}(\sqrt{D})$. Then $E_{(D)}$ and E are isomorphic over K under an isomorphism $\imath : (x\,,\, y) \mapsto (x\,, \sqrt{D}y)$. The elements Q of $E_{(D)}(\mathbb{Q})$ corresponds to points $Q^\imath$ in $E(K)$ which have the property that $Q^\imath + \sigma\, Q^\imath = O$, where σ is the conjugation automorphism which maps $\sqrt{D}$ to $\overline{\sqrt{D}}$ and $G(K/\mathbb{Q}) = \{1, \sigma\}$.

Considering the quadratic extension $K/\mathbb{Q}$, we have

$$\imath\,(E_{(D)}(\mathbb{Q})) = \{\, Q \in E(K) \,|\, \mathrm{Norm}_{K/\mathbb{Q}}\, Q = 0\},$$

that is, the group of points on $E_{(D)}(\mathbb{Q})$ is isomorphic to a subgroup of points on $E(K)$ with trivial norm from K to $\mathbb{Q}$.

By including $H^1(G(K/\mathbb{Q}), E(K))$ into $H^1(\mathbb{Q}, E)_2$ we get a map

$$\imath\,(E_{(D)}(\mathbb{Q})) \to H^1(\mathbb{Q}, E)_2$$

which maps $Q \in E_{(D)}(\mathbb{Q})$ to $c(Q) \in H^1(\mathbb{Q}, E)_2$, where $c(Q)$ corresponds to a cocycle φ determined by $\varphi\,(1) = 0$ and $\varphi\,(\sigma) = Q^\imath$.

So the cohomology class is defined by :

$$\begin{array}{ccccc} E_{(D)}(\mathbb{Q}) & \to & E(K) & \to & H^1(\mathbb{Q}, E)_2 \\ Q & \mapsto & Q^\imath & \mapsto & \varphi \end{array}$$

From now on we will identify $E_{(D)}(\mathbb{Q})$ with its isomorphic image in $E(K)$ without any notice. In particular, φ is determined by $\varphi\,(1) = 0$ and $\varphi\,(\sigma) = Q$. By $\mathrm{red}_q(Q^\imath)$ or $\mathrm{red}_q(Q)$ we denote the reduction of the image of $Q \in E_{(D)}(\mathbb{Q})$ at $v\,(q = v^2)$ in the corresponding group, otherwise it doesn't make sense.

Proposition 3.2. *Every element of $H^1(G(K/\mathbb{Q}), E(K))$ is obtained in the way described above.*

Proof. Since the Galois group $G(K/\mathbb{Q})$ is a cyclic group of order 2 generated by σ, the cocycle φ is determined by its values at 1 and σ. And then the result follows considering Proposition 3.1 □

Let $\mathcal{K}$ be the completion of K at a prime divisor $v \in K$ which divides q.

Consider those primes $q \nmid 2N\infty$ and $q|D$, therefore q totally ramifies in K. So $G(\mathcal{K}/\mathbb{Q}_q) \simeq G(K/\mathbb{Q}) = \{1, \sigma\}$. And we identify them. In general, the Galois group of corresponding local field extension is a subgroup of the Galois group of global field extension. But if the extension is totally ramified at q, they are isomorphic.

Recall that we have a localization map (§2)

$$loc_q \ : \ H^1(\mathrm{Gal}(K/\mathbb{Q}), E(K)) \to H^1(\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_q), E(\mathcal{K})).$$

And we have an embedding $H^1(\mathrm{Gal}(\mathcal{K}/\mathbb{Q}_q), E(\mathcal{K})) \hookrightarrow H^1(\mathbb{Q}_q, E)_2$.

Thus we get a localization of the cohomology class $c : E_{(D)}(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E)_2$ as

$$\mathrm{c}_q : E_{(D)}(\mathbb{Q}) \to H^1(\mathbb{Q}_q, E)_2$$

in the way described above.

For $Q \in E_{(D)}(\mathbb{Q})$, $c_q(Q) \in H^1(G(\mathcal{K}/\mathbb{Q}_q), E(\mathcal{K})) \subset H^1(\mathbb{Q}_q, E)_2$ corresponds to the cocycle $\varphi : \sigma \mapsto Q$. Hence $c_q(Q)$ denotes $loc_q(\varphi)$.

There exists a class b of the cocycle ψ in $H^1(\mathbb{Q}_q, E_2)$, which is mapped into $c_q(Q)$ in $H^1(G(\mathcal{K}/\mathbb{Q}), E(\mathcal{K}))$ corresponding to the cocycle $\psi : \sigma \mapsto Q$ in $H^1(\mathbb{Q}, E)_2$ through our fundamental exact sequence. We will explicitly compute ψ and use it to compute the Tate pairing in the next section.

We can define the Tate pairing of level 2 in exactly the same way as was defined in the previous section for general level M. Then we get a nondegenerate pairing

$$\langle \, , \, \rangle_{q,2} : E(\mathbb{Q}_q)/2E(\mathbb{Q}_q) \times H^1(\mathbb{Q}_q, E)_2 \to \mathbb{Z}/2\mathbb{Z}$$

which is the (local) Tate pairing at q.

Then for $P \in E(\mathbb{Q})/2E(\mathbb{Q})$ and $C \in H^1(\mathbb{Q}, E)_2$, the sum of the local Tate pairing $\langle P_q, C_q \rangle_{q,2}$ over all prime divisors of $\mathbb{Q}$ equals zero where P_q and C_q are the localizations of P and C respectively, that is, $\sum_q \langle P_q, C_q \rangle_{q,2} = 0$, which is the orthogonality relation for quadratic extensions.

The point is that we have a map $\mathrm{c} : E_{(D)}(\mathbb{Q}) \to H^1(\mathbb{Q}, E)_2$ and its localizations $c_q : E_{(D)}(\mathbb{Q}) \to H^1(\mathbb{Q}_q, E)_2$ at each q, so that the orthogonality relation informs us some relations between $E(\mathbb{Q})$ and $E_{(D)}(\mathbb{Q})$.

4. COMPUTATION OF TATE PAIRING

In this section we compute the local Tate pairing at each prime. The computation of it is based on the local class field theory. The explanations and proofs of this section come from those in [Ko1]. The more general proofs can be found there. We will check here that Kolyvagin's formulas with Heegner points also works with points of quadratic twisted elliptic curves. I provide this section for the convenience of the reader.

We assume that $(D, 2N\infty) = 1$.

Let q be a prime of $\mathbb{Q}$ such that $q = v^2$ in $K = \mathbb{Q}(\sqrt{D})$, $q \nmid 2N\infty$. Since $\mathcal{K}/\mathbb{Q}$ is totally ramified, the residue field of $\mathcal{K}$ is the same as that of $\mathbb{Q}_q$, in other words, $\mathbb{Z}/q\mathbb{Z} = O_K/vO_K = \mathbb{Z}_q/q\mathbb{Z}_q = O_{\mathcal{K}}/vO_{\mathcal{K}}$. (The residue class fields doesn't change under completion.) We identify $G(\mathcal{K}/\mathbb{Q}_q)$ with $G(K/\mathbb{Q}) = \{1, \sigma\}$.

Let $\theta : \mathbb{Q}_q^* \to G(K/\mathbb{Q})$ be the *local reciprocity* map. ([CF] Chapter VI.)

Let ξ be a primitive root (i.e. a generator) of $(\mathbb{Z}/q\mathbb{Z})^*$, where $(\mathbb{Z}/q\mathbb{Z})^*$ is a reduced residue system mod q and it is a cyclic group of order $q-1$ under multiplication. Thus $\theta(\xi) = \sigma$ and $\xi^{\frac{q-1}{2}} = -1$(ξ is a quadratic non-residue in particular).

Let η be the uniformizing parameter of $\mathbb{Q}_q$ which is a norm from $\mathcal{K}$. Then $\theta(\eta)$ is trivial on $\mathcal{K}$ and its restriction on $\mathbb{Q}_q^{nr}$ is the Frobenius element Fr_q of $\mathrm{Gal}(\mathbb{Q}_q^{nr}/\mathbb{Q}_q)$ by local class field theory .

Then $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2} = \eta^{\mathbb{Z}/2\mathbb{Z}}\xi^{\mathbb{Z}/2\mathbb{Z}}$ if $q \neq 2$, where $\mathbb{Q}_q^{*2}$ is the subgroup of squares of the multiplicative group $\mathbb{Q}_q^*$ of the field of q-adic numbers. ([BSh] Chapter 1, §6.1.) In fact, $\mathbb{Q}_q^* = \eta^{\mathbb{Z}} \times (\mathbb{Z}/q\mathbb{Z})^* \times (1 + q\mathbb{Z}_q)$. So if $2 \nmid q$, then $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2} = \eta^{\mathbb{Z}/2\mathbb{Z}} \times \xi^{\mathbb{Z}/2\mathbb{Z}}$.

Let $\mathcal{F}$ be a local field with residue field F_1. Let's look at the operation of reduction at non-archimedean places which we denote by a tilde.

Having chosen a minimal Weierstrass equation for E, we can reduce its coefficients to obtain a (possibly singular) curve $\tilde{E}$ over F_1.

This gives a reduction map

$$\mathrm{red} : E(\mathcal{F}) \to \tilde{E}(\bar{F}_1).$$

E is said to have a *good reduction* if $\tilde{E}$ is non-singular. Otherwise it is said to have a *bad reduction.* The prime divisors of the conductor N of an elliptic curve is the set of primes at which the curve has a bad reduction.

Let p be an odd finite prime which doesn't divide the conductor N. Then the elliptic curve has a good reduction at p.

Moreover if $(MN, p) = 1$ then the group $\tilde{E}(\overline{\mathbb{Z}/p\mathbb{Z}})$ is M-divisible, that is, for $\tilde{P} \in \tilde{E}(\overline{\mathbb{Z}/p\mathbb{Z}})$ there exists $\tilde{Q} \in \tilde{E}(\overline{\mathbb{Z}/p\mathbb{Z}})$ such that $M\tilde{Q} = \tilde{P} \in \tilde{E}(\overline{\mathbb{Z}/p\mathbb{Z}})$.

It is a standard property of a good reduction that

$$\mathrm{red} : E(\overline{\mathbb{Q}}_p)_M \xrightarrow{\sim} \tilde{E}(\overline{\mathbb{Z}/p\mathbb{Z}})_M$$

is an isomorphism.

We will often use E instead of $\tilde{E}$ to denote the reduction of E if the situation is clear, especially when we denote $\tilde{E}_M$ because it is isomorphic to E_M(not reduced).

For a finite extension $\mathcal{F}$ of $\mathbb{Q}_p$ (where $(MN, p) = 1$) with residue field F_1, the reduction map is surjective and the multiplication by M is an isomorphism onto its kernel $E_1(\mathcal{F})$. In other words, we have an exact sequence ([Sil] Chapter VII, §2)

$$O \to E_1(\mathcal{F}) \xrightarrow{\times M} E(\mathcal{F}) \xrightarrow{\mathrm{red}} \tilde{E}(F_1) \to O.$$

Suppose $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ is a finite field of characteristic p with $p > 0$, $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$, and let $l = p^r$. If E is an elliptic curve given by a Weierstrass equation, we define Fr_l on $E(\overline{\mathbb{F}})$ to be the morphism given by

$$\mathrm{Fr}_l \ : \ (x\,,\, y) \mapsto (x^l,\, y^l).$$

Then Fr_l is an endomorphism of E, called the *Frobenius endomorphism.* The set of points fixed by Fr_p is exactly the finite group $E(\mathbb{F})$. (See [Sil] p. 74.)

Let P be a point of $E(\mathbb{Q})$ and P_q be its image in $E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)$. Let $R \in E(\overline{\mathbb{Q}})$ such that $2R = P$ and $\tilde{R} \in E(\overline{\mathbb{Z}/q\mathbb{Z}})$ where $2\tilde{R} = \mathrm{red}(P)$. Notice that $\tilde{R}$ is determined only up to 2-torsion points.

Definition 1. Let $q|D$. Then $\mathbb{Q}_q(R)$ is an unramified extension of $\mathbb{Q}_q$. We denote by $e_q(P)$ an element of E_2 obtained by the condition

$$\mathrm{red}(e_q(P)) = \mathrm{Fr}_q(\tilde{R}) - \tilde{R} \pmod{(\mathrm{Fr}_q - 1)E_2}.$$

Since $2\,(\mathrm{Fr}_q(\tilde{R}) - \tilde{R}) = \mathrm{Fr}_q(2\tilde{R}) - 2\tilde{R} = P - P = O$, so $\mathrm{Fr}_q(\tilde{R}) - \tilde{R} \in E(\overline{\mathbb{Z}/q\mathbb{Z}})_2$.

Once we choose R, $e_q(P)$ is well-defined in terms of R, due to the property of good reduction that $\mathrm{red} : E_2 \to E(\overline{F})_2$ is an isomorphism.

But if the 2-torsion points are not defined in the ground field $\mathbb{Q}$ then $e_q(P)$ is not uniquely determined, since $\tilde{R}$ is determined up to 2-torsion points and for any 2-torsion point $t \notin E(\mathbb{Q}_q)_2$, $\mathrm{Fr}_q(t) - t \neq O$. ($\mathrm{Fr}_q(t) - t = O \Leftrightarrow t \in E(\mathbb{Q}_q)_2$.)

Definition 2. Let $Q \in E_{(D)}(\mathbb{Q})$ and $q|D$ (so $q \nmid 2N\infty$). Then $\mathrm{Norm}_{\mathcal{K}/\mathbb{Q}_q}(Q^\iota) = \mathrm{Norm}_{K/\mathbb{Q}}(Q^\iota) = O$, since the Galois groups of the corresponding extensions coincide. We denote by $e'_q(Q)$ an element of $E(\mathbb{Q}_q)_2$ obtained by the condition

$$\mathrm{red}(e'_q(Q)) = \mathrm{red}(Q^\iota).$$

Remark. Since $\mathcal{K}/\mathbb{Q}_q$ is a totally ramified extension and $\mathrm{Norm}_{\mathcal{K}/\mathbb{Q}_q}(Q^\iota) = O$, we have that $2\,\mathrm{red}(Q^\iota) = O$.

Proposition 4.1. *Let $q \nmid 2DN\infty$, then $\langle P_q, c_q(Q) \rangle_{q,2} = 0$.*

Proof. $c_q(Q) \in H^1(\mathbb{Q}_2, E)_{nr}$, and $H^1(\mathbb{Q}_2, E)_{nr} = 0$ due to the property of good reduction.(See [Ko1] p.536.) □

Let's denote the cocycle corresponding to P by ϕ_1, and the cocycle corresponding to Q by ϕ_2.

Then the cocycle $\phi_1 \cup \phi_2$ is defined by a bilinear mapping $\bar{B}$ below:

$$\begin{array}{ccccccc} H^1(\mathbb{Q}_q, E_2) \times H^1(\mathbb{Q}_q, E_2) & \xrightarrow{\cup} & H^2(\mathbb{Q}_q, E_2 \otimes E_2) & \xrightarrow{[,]_2} & H^2(\mathbb{Q}_q, \mu_2) & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \\ (\phi_1 , \phi_2) & \mapsto & \bar{B} & \mapsto & B & & \end{array}$$

Then $\phi_1 \cup \phi_2$ is determined by the conditions $\bar{B}(g_1, g_2) = \phi_1(g_1) \otimes \phi_2(g_2)$ or by $B(g_1, g_2) = [\phi_1(g_1), \phi_2(g_2)]_2$ after Weil pairing for $g_1, g_2 \in \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. B is mapped to an element of $\mathbb{Z}/2\mathbb{Z}$ under the canonical isomorphism given by (c) of exact sequence (3) in §3.

Proposition 4.2. *Let $q|D$, $P \in E(\mathbb{Q})/2E(\mathbb{Q})$, and $Q \in E_{(D)}(\mathbb{Q})$. Then*

$$(-1)^{\langle P_q, c_q(Q) \rangle_{q,2}} = [e_q(P), e'_q(Q)]_2$$

where P_q is the class of P in $E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)$.

Proof. For $Q \in E_{(D)}(\mathbb{Q})$, $c_q(Q) \in H^1(G(\mathcal{K}/\mathbb{Q}_q), E(\mathcal{K})) \subset H^1(\mathbb{Q}_q, E)_2$ corresponds to the cocycle $\varphi : \sigma \mapsto Q$.

If $g \in G(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, then by $\bar{g}$ we denote the image of g in $G(\mathcal{K}/\mathbb{Q}_q)$. Let $\widehat{Q} \in E(\overline{\mathbb{Q}}_q)$ be such that $2\,\widehat{Q} = Q$. The mapping $\psi : g \mapsto \varphi(\bar{g}) + (g-1)\widehat{Q}$ is a cocycle in E_2. In fact, it is obvious that ψ is a cocycle in $E(\overline{\mathbb{Q}}_q)$, and if $\bar{g} = \sigma$, then $2\,\psi(g) = 2\,Q + (\sigma - 1)Q = 2\,Q - 2\,Q = 0$.

The cohomology class b of the cocycle ψ in $H^1(\mathbb{Q}_q, E_2)$ is mapped onto $c_q(Q)$ in $H^1(\mathbb{Q}_q, E)_2$.

Since $E_1(\mathcal{K})$ is 2-divisible, there is a $\widehat{Q}_0 \in E_1(\mathcal{K})$ such that $2\,\widehat{Q}_0 = Q_0$. Therefore $Q = e'_q(Q) + 2\,\widehat{Q}_0$.

We set $\widehat{Q} = \widehat{e'}_q(Q) + \widehat{Q}_0$ where $2\,\widehat{e'}_q(Q) = e'_q(Q)$.

In computing the value of Tate pairing of the cohomology class $b \in H^1(\mathbb{Q}_q, E_2)$ with $P_q \in E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)$, because $E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)$ is isotropic, we can simply replace $\widehat{Q}$ by $\widehat{Q}_0$. (Since $e'_q(Q) \in E(\mathbb{Q}_q)$, it is killed under Tate pairing by Pontryagin duality.) Thus $\widehat{Q} = \widehat{Q}_0$.

Suppose $\bar{g} = \sigma$. Then $\psi(g) = Q + (\sigma - 1)\widehat{Q}_0 = Q - 2\,\widehat{Q}_0 = e'_q(Q)$.

In other words, the corresponding cohomology class $b \in H^1(\mathbb{Q}_q, E_2)$ is simply the homomorphism of $G(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ into E_2 induced by the homomorphism of $G(\mathcal{K}/\mathbb{Q}_q)$ into E_2 under which $\sigma \mapsto e'_q(Q)$.

Now recall that $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2} = \eta^{\mathbb{Z}/2\mathbb{Z}}\xi^{\mathbb{Z}/2\mathbb{Z}}$ (if $q \neq 2$).

We denote by G_2 the Galois group of the maximal abelian 2-periodic extension of $\mathbb{Q}_q$. Then $\theta : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \to G_2$ is an isomorphism, and we identify G_2 with $\mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$.

The cocycle $\varphi_1 : G_2 \to E_2$ corresponding to $P_q \in E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)$ is determined by the values $\varphi_1(\xi) = 0$ and $\varphi_1(\eta) = e_q(P)$, since $\mathcal{K}(R)$ is an unramified extension of $\mathcal{K}$ where $2R = P$. The cocycle φ_2 corresponding to $e'_q(Q)$ is determined by the values $\varphi_2(\xi) = e'_q(Q)$ and $\varphi_2(\eta) = 0$.

The cohomology class $\varphi_1 \cup \varphi_2 \in H^2(G_2, \mu_2)$ is defined by a bilinear mapping $B_1 : G_2 \times G_2 \to \mu_2$ such that

$$\begin{aligned} B_1(\eta,\eta) &= 1, \qquad & B_1(\eta,\xi) &= [e_q(P), e'_q(Q)]_2, \\ B_1(\xi,\eta) &= 1, \qquad & B_1(\xi,\xi) &= 1. \end{aligned}$$

We have the Hilbert symbol $(,)_2 : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \times \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \to \mu_2$. If $\beta \in \mathbb{Q}_q^*$, then β is associated to a $\varphi_\beta \in H^1(G_2, \mu_2)$ such that $\varphi_\beta(g) = g(\tilde{\beta})/\tilde{\beta}$, where $\tilde{\beta}^2 = \beta$. The Hilbert pairing is defined to be $(\alpha, \beta)_2 = \varphi_\beta(\theta(\alpha))$.

An equivalent definition is the following. We define homomorphisms

$$\bar{\varphi}_\alpha : G_2 \to \mathbb{Z}/2\mathbb{Z} \text{ and } \bar{\varphi}_\beta : G_2 \to \mathbb{Z}/2\mathbb{Z}$$

by the conditions

$$(-1)^{\bar{\varphi}_\alpha(g)} = \varphi_\alpha(g) \text{ and } (-1)^{\bar{\varphi}_\beta(g)} = \varphi_\beta(g).$$

We define an element of $H^2(G_2, \mu_2)$ by the bilinear form

$$B_{\alpha,\beta}(g_1, g_2) = (-1)^{\bar{\varphi}_\alpha(g_1)\bar{\varphi}_\beta(g_2)}.$$

Then $(\alpha, \beta)_2 = (-1)^{(2\,inv B_{\alpha,\beta})}$. ($2\,inv B_{\alpha,\beta}$ is defined as an element of $\mathbb{Z}/2\mathbb{Z}$.) In particular, we have

$$\varphi_\xi(\xi) = (\xi,\xi)_2 = 1, \qquad \varphi_\xi(\eta) = (\eta,\xi)_2 = -1,$$

$$\varphi_{-\eta}(\xi) = (\xi, -\eta)_2 = (-\eta, \xi)_2 = (-1, \xi)_2 \cdot (\eta, \xi)_2 = -1,$$
$$\varphi_{-\eta}(\eta) = (\eta, -\eta)_2 = 1.$$

Therefore

$$B_{\xi,-\eta,}(\eta, \eta) = 1, \qquad B_{\xi,-\eta}(\eta, \xi) = -1,$$
$$B_{\xi,-\eta,}(\xi, \eta) = 1, \qquad B_{\xi,-\eta,}(\xi, \xi) = \quad 1.$$

Let $[e_q(P), e'_q(Q)]_2 = (-1)^x,\ x \in \mathbb{Z}/2\mathbb{Z}$.
Then $B_1 = B^{-x}_{\xi,-\eta}$. Hence, $2\, inv B_1 = (-x) 2\, inv B_{\xi,-\eta}$.
But $(-1)^{2\, inv B_{\xi,-\eta}} = (\xi, -\eta)_2 = -1$.
Hence $2\, inv B_1 = x$, which proves the Proposition. (See [Ko1] pp. 530–532.) $\square$

Caution. In the above proof, Q was used instead of Q^t for simplicity. But the situation would be clear which is meant.

5. NON-EXISTENCE OF RATIONAL POINTS

An immediate consequence of the construction of special cohomology classes from $E(K)$ is the distribution of $\mathbb{Q}$-rational points of $E_{(D)}$ over the real numbers $\mathbb{R}$ where $K = \mathbb{Q}(\sqrt{D})$.

Let E be an elliptic curve over $\mathbb{Q}$, $\Delta(E)$ the discriminant of some Weierstrass equation for E, N the conductor of E, and $J(E)$ be the modular invariant of E.

We begin by considering the following list of conditions on the elliptic curves E. These conditions are assumed throughout this section and the next(§§5–6) if not mentioned otherwise.

Condition 5.1. (a) $\Delta(E) > 0$. (This is equivalent to $E(\mathbb{R})_2 = \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$.)
(b) $E(\mathbb{Q})_2 \neq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$.
(c) For some $P \in E(\mathbb{Q}) \setminus 2E(\mathbb{R})$ and $\forall x \in H^1(\mathbb{Q}_q, E)_2^{nr}$, we have

$$\langle P_q, x \rangle_{q,2} = 0 \ \forall q | N.$$

Of these, only (c) requires clarification. (See Propositions 5.2 and 5.3 as sufficient conditions on (c).)

First, if $2 \nmid [H^1(\mathbb{Q}_q, E)_2^{nr}]$ or $P_q = 0$ then Condition (c) is satisfied. If $P_q = 0$, then (c) is satisfied by the bilinearity of Tate pairing. If $2 \nmid [H^1(\mathbb{Q}_q, E)_2^{nr}]$, then for all $x \in H^1(\mathbb{Q}_q, E)_2^{nr}$, x is killed both by 2 and the order of $H^1(\mathbb{Q}_q, E)_2^{nr}$ which is odd, therefore $x = 0$.

We can say more about this condition.

For any local field $\mathcal{F}$, let $\mathcal{F}^{nr}$ denote the maximal unramified extension (the union of all unramified extensions) of $\mathcal{F}$ in a given separable closure of $\mathcal{F}$.

Let $\mathcal{K}$ be a p-adic field and k be its perfect residue field.

$$H^1(\mathrm{Gal}(\mathcal{K}^{nr}/\mathcal{K}), E(\mathcal{K}^{nr})) = \begin{cases} 0 \text{ if } E \text{ has a good reduction} \\ H^1(\mathrm{Gal}(\mathcal{K}^{nr}/\mathcal{K}), \pi_0(\tilde{E})) \text{ in any case} \end{cases}$$

Here $\tilde{E}$ denotes the special (or closed) fiber of the Néron model of E and π_0 is the (finite algebraic) group of its connected components. For the proof in the

non-degenerate case the problem reduces to showing that the norm mapping for unramified extensions is surjective, which is established by means of Hensel's lemma. (See [Ma], p. 32.)

We abbreviate $H^1(\mathrm{Gal}(\mathcal{K}^{nr}/\mathcal{K}), E(\mathcal{K}^{nr}))$ by $H^1(\mathcal{K}, E)^{nr}$ (or by $H^1(\mathcal{K}, E)_{nr}$). Notice that even if E doesn't have a good reduction at the residue field of $\mathcal{K}$, the group $H^1(\mathcal{K}, E)^{nr}$ is still finite.

Take a minimal Weierstrass equation for E and let $\mathbb{Q}_q$ be a field of q-adic numbers with normalized valuation ν_q.

We have

$$H^1(\mathbb{Q}_q, E)^{nr} = H^1(\mathrm{Gal}({\mathbb{Q}_q}^{nr}/\mathbb{Q}_q), \pi_0(\tilde{E})),$$

where $\tilde{E}$ denotes the special (or closed) fiber of the Néron model of E and π_0 is the (finite algebraic) group of its connected components.

Let $E_0(\mathbb{Q}_q) = \{P \in E(\mathbb{Q}_q) \mid \tilde{P} \in \tilde{E}(k)_{ns}\}$, the set of points of $E(\mathbb{Q}_q)$ with non-singular reduction.

In general, we have an inclusion $E(\mathbb{Q}_q)/E_0(\mathbb{Q}_q) \hookrightarrow \pi_0(\tilde{E})$. In fact, because $\mathbb{Q}_q$ is complete (or even merely Henselian), this inclusion is an isomorphism. See [Si2] Chapter IV, §9, Corollary 9.2(b).

Let $m_q(E)$ denote $[E(\mathbb{Q}_q)/E_0(\mathbb{Q}_q)]$. (In fact, $m_q(E)$ is equal to the number of connected components of the fiber of the Néron model of E that are rational over $\mathbb{Z}/q\mathbb{Z}$.)

Therefore in our case $m_q(E) = [\pi_0(\tilde{E})]$.

Proposition 5.2. *If $m_q(E)$ is odd, then Condition (c) is satisfied.*

Proof. In this case $2 \nmid [H^1(\mathbb{Q}_q, E)_2^{nr}]$. □

Proposition 5.3. *Assume that E has split multiplicative reduction at q, and that $-\nu_q(J(E))$ is odd. Then Condition (c) is satisfied.*

Proof. The group $E(\mathbb{Q}_q)/E_0(\mathbb{Q}_q)$ is finite. More precisely, if E has split multiplicative reduction at q, then $E(\mathbb{Q}_q)/E_0(\mathbb{Q}_q)$ is a cyclic group of order $-\nu_q(J(E))$. ([Si2] Chapter IV, §9, Corollary 9.2(d).)

Thus $[\pi_0(\tilde{E})] = [E(\mathbb{Q}_q)/E_0(\mathbb{Q}_q)] = -\nu_q(J(E))$ is odd. So $2 \nmid [H^1(\mathbb{Q}_q, E)_2^{nr}]$. □

Let D be a negative integer such that $(N, D) = 1$ and $2 \nmid ND$.

Proposition 5.4 (Tate pairing at 2)**.** $\langle P_2, c_2(Q) \rangle_{2,2} = 0$.

Proof. The cocycle representing $Q \in E_{(D)}(\mathbb{Q})$ is given by $\varphi : \sigma \mapsto Q^{\iota}$ (see §3 for the isomorphism ι) where $\sigma : \sqrt{D} \mapsto -\sqrt{D}$. Since $(2, D) = 1$, $\sigma \in \mathrm{Gal}(\mathbb{Q}_2^{nr}/\mathbb{Q}_2)$ and $Q^{\iota} \in E(K) \subset E(\mathbb{Q}_2(\sqrt{D})) \subset E(\mathbb{Q}_2^{nr})$. Thus $loc_2(\varphi) = c_2(Q) \in H^1(\mathbb{Q}_2, E)_{nr}$.

Since 2 is a place of good reduction of E, $H^1(\mathbb{Q}_2, E)_{nr} = 0$.

Hence the corresponding cohomology class is trivial and we get the conclusion. □

Proposition 5.5 (Tate pairing at $q \nmid 2DN\infty$)**.** *Let $Q \in E_{(D)}(\mathbb{Q})$ and $q \nmid 2DN\infty$. Then $\langle P_q, c_q(Q) \rangle_{q,2} = 0$.*

Proof. $c_q(Q) \in H^1(\mathbb{Q}_q, E)_{nr}$ and $H^1(\mathbb{Q}_q, E)_{nr} = 0$ by the property of good redution. □

We considered the value of Tate pairing at prime divisors of D in Proposition 4.2 , assumed its value to be zero at prime divisors of N from Condition (c) of this section, and considered its value at 2. Now it remains to consider its value at infinity. As was seen in Proposition 5.5 the value is zero outside these primes. The idea is that if we can control its value at all localizations, then by local-global duality we get results on the global points.

Proposition 5.6. *There is an isomorphism of real Lie groups*

$$E(\mathbb{R}) \simeq (\mathbb{R}/\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), \text{ if } \Delta(E) > 0.$$

Proof. [Si2] Chapter V, Corollary 2.3.1. In particular, the isomorphism is given by

$$\mathbb{R}^*/q^{\mathbb{Z}} \xrightarrow{\sim} (\mathbb{R}/\mathbb{Z}) \times \{\pm 1\}\ , \quad u \mapsto \left(\frac{\log |u|}{\log q} \pmod{\mathbb{Z}}\ ,\ \mathrm{sign}\,(u) \right)$$

where q is chosen so that $\mathbb{R}^*/q^{\mathbb{Z}}$ is real analytically isomorphic to $E(\mathbb{R})$. □

Corollary 5.7. $E(\mathbb{R})/2E(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$, *if* $\Delta(E) > 0$.

Proof. Clear from the above Proposition. □

Proposition 5.8 (Localization at ∞)**.** *A point $Q \in E_{(D)}(\mathbb{Q})$ is mapped by c_∞ to a trivial class of $H^1(\mathbb{R}, E)_2$ if and only if it is a point from $2E_{(D)}(\mathbb{R})$ for $D < 0$.*

Proof. Let A, B and C denote $A = E(\mathbb{R})/2E(\mathbb{R})$, $B = H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), E(\mathbb{R})_2)$ and $C = H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), E(\mathbb{C}))_2$ respectively.

Then we have an exact sequence

$$O \to A \to B \to C \to O \qquad (*)$$

because $E(\mathbb{R})_2 = E(\mathbb{C})_2 = E_2$, so $B = H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), E(\mathbb{C})_2)$.

Since σ acts trivially on $E(\mathbb{R})_2$ (where $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$),

$$B = \mathrm{Hom}(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), E(\mathbb{R})_2) \simeq \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}.$$

Thus $[B] = 4$. ($[\cdot]$ means the order of a set.)

$[A] = 2$, and since C is a quotient of B by A, $[C] = 4/2 = 2$.

Let $B = \{\varphi_e : \sigma \mapsto e, e \in E_2\}$.

Then two elements of B are mapped to the nontrivial cohomology class in C and the other two are mapped to the identity in C through the exact sequence $(*)$. (The images of A will be mapped to the identity in C.)

This means that there is $e \in E_2$ such that $e \neq (\sigma - 1)R$ for all $R \in E(\mathbb{C})$.

Consider a map

$$\begin{aligned} d_\infty : E_{(D)}(\mathbb{R})/2E_{(D)}(\mathbb{R}) &\to H^1(\mathbb{R}, E)_2 \\ Q &\mapsto d_\infty(Q) = (\varphi : \sigma \mapsto Q^\iota) \end{aligned}$$

Since $(1-\sigma)Q^\iota = 2Q^\iota$, the elements of $2E_{(D)}(\mathbb{R})$ are mapped to coboundaries, and this map is well-defined.

Now d_∞ is surjective because there exists $e \in E_{(D)}(\mathbb{R})_2 \subset E_{(D)}(\mathbb{R})$ such that $e \neq (\sigma - 1)R$ for all $R \in E(\mathbb{C})$.

As $2E_{(D)}(\mathbb{R})$ is mapped to the coboundary, so $E_{(D)}(\mathbb{R}) \setminus 2E_{(D)}(\mathbb{R})$ is mapped to the nontrivial cohomology class since both $E_{(D)}(\mathbb{R})/2E_{(D)}(\mathbb{R})$ and $H^1(\mathbb{R}, E)$ have order two. Therefore

$$\begin{aligned} c_\infty : E_{(D)}(\mathbb{Q}) &\to H^1(\mathbb{R}, E)_2 \\ Q &\mapsto c_\infty(Q) = (\varphi : \sigma \mapsto Q^\iota) \end{aligned}$$

is a trivial class if and only if it comes from $2E_{(D)}(\mathbb{R})$. □

Proposition 5.9 (Tate pairing at ∞ for $D < 0$)**.** *Let $Q \in E_{(D)}(\mathbb{Q})$.*

(a) *If $Q \in 2E_{(D)}(\mathbb{R})$, then $\langle P_\infty, c_\infty(Q) \rangle_{\infty,2} = 0$.*

(b) *If $Q \notin 2E_{(D)}(\mathbb{R})$, then $\langle P_\infty, c_\infty(Q) \rangle_{\infty,2} = 1$.*

Proof. We know that the cohomology class corresponding to P at ∞ is nontrivial, which is equivalent to the statement that P is not a square at ∞.

If $Q \in 2E_{(D)}(\mathbb{R})$, then it corresponds to a trivial cohomology class at ∞, so the value of Tate pairing is also trivial.

If Q is a point of $E_{(D)}(\mathbb{Q})$ such that the cohomology class corresponding Q at ∞ is nontrivial, then $\langle P_\infty, c_\infty(Q)\rangle_{\infty,2} = 1$ from the nondegeneracy of the Tate pairing. □

Notation. Let P be a rational point in E. Let $\mathbf{T}_E(P)$ denote the set of all odd primes $q \nmid N$ at which $P \in E(\mathbb{Q})$ is a local square, i.e. there is a point $\tilde{R} \in E(\mathbb{Z}/q\mathbb{Z})$ satisfying $2\,\tilde{R} = \tilde{P}$ where $\tilde{P}$ is the reduction of P at q. Next, set

$$\mathbf{T}_E = \bigcup_{P \in E(\mathbb{Q}) \setminus 2E(\mathbb{R})} \mathbf{T}_E(P),$$

and let $\mathbf{S}_E$ be the set of *negative* square-free D's such that D is a product of primes of $\mathbf{T}_E$.

We have the following result on the non-existence of rational points on the non-trivial connected component of E over $\mathbb{R}$.

Main Theorem 1. *We have* $E_{(D)}(\mathbb{Q}) \subset 2E_{(D)}(\mathbb{R})$ *if* $D \in \mathbf{S}_E$.

Proof. Suppose Q is a point of $E_{(D)}(\mathbb{Q})$ such that the cohomology class representing Q at ∞ is nontrivial.

If $\mathbf{S}_E$ is empty the statement is trivial.

If $\mathbf{S}_E$ is non-empty, then we can choose $P \in E(\mathbb{Q}) \setminus 2E(\mathbb{R})$ so that

$$\langle P_\infty, c_\infty(Q)\rangle_{\infty,2} = 1$$

from Proposition 5.9.

So $\sum_{q|D} \langle P_q, c_q(Q)\rangle_{q,2} = 1$.

If we choose $D \in \mathbf{S}_E$, then $e_q(P) = 0$ for all $q|D$, and so $\sum_{q|D} \langle P_q, c_q(Q)\rangle_{q,2} = 0$, which is a contradiction.

Thus we cannot find a point of $E_{(D)}(\mathbb{Q})$ in $E_{(D)}(\mathbb{Q}) \setminus 2E_{(D)}(\mathbb{R})$. □

We now present another theorem regarding the situation where D is not necessarily in $\mathbf{S}_E$. (See Theorem 5.13.) The following Propositions 5.10 and 5.11 are true for all elliptic curves.

Proposition 5.10. *Assume that* $P \in E(\mathbb{Q})$ *is not a square at a prime* q *and* $R \in E(\overline{\mathbb{Q}})$ *satisfies* $2R = P$, *where* $E(\mathbb{Z}/q\mathbb{Z})_2 = \{O, e\}$, $q \nmid 2N\infty$.

Then $(\mathrm{Fr}_q - 1)\,\mathrm{red}(R) \neq e$.

Proof. Let $t \in E(\overline{\mathbb{Z}/q\mathbb{Z}})_2 \setminus E(\mathbb{Z}/q\mathbb{Z})_2$. Such t exists since $E(\mathbb{Z}/q\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z}$ and $E(\overline{\mathbb{Z}/q\mathbb{Z}})_2 \simeq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$.

Note first that $2\,(\mathrm{Fr}_q - 1)t = (\mathrm{Fr}_q - 1)(2t) = O$, so $(\mathrm{Fr}_q - 1)t$ is a 2-torsion.

Consider the Weil pairing $[\ ,\ ]_2$ of $(\mathrm{Fr}_q - 1)t$ with e:

$$[(\mathrm{Fr}_q - 1)t, e]_2 = [t, (\mathrm{Fr}_q^{-1} - 1)e]_2 = [t, O] = 1,$$

due to the property of Weil pairing that $[ga, gb]_2 = [a, b]_2^g = [a, b]_2$ for any $a, b \in E_2$ and g is in $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$.

This implies that $(\mathrm{Fr}_q - 1)t = O$ or e. But $t \notin E(\mathbb{Z}/q\mathbb{Z})_2$, so $(\mathrm{Fr}_q - 1)t \neq O$. Thus $(\mathrm{Fr}_q - 1)t = e$.

Suppose $(\mathrm{Fr}_q - 1)\,\mathrm{red}(R) = e$.

Then $(\mathrm{Fr}_q - 1)\,\mathrm{red}(R + \bar{t}) = (\mathrm{Fr}_q - 1)\,\mathrm{red}(R) + (\mathrm{Fr}_q - 1)t = e + e = O$, where $\mathrm{red}\bar{t} = t\,,\ \bar{t} \in E(\overline{\mathbb{Q}}_q)_2$.

But then $R + \bar{t} \in E(\mathbb{Q}_q)$ (since it is fixed by Fr_q) and $2\,(R + \bar{t}) = 2R = P$, which means that P is a square at q. □

Proposition 5.11. *Let q be a prime such that $E(\mathbb{Z}/q\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z}$, and suppose that $P \in E(\mathbb{Q})$ is not a local square at q. Let D be an integer with $q|D$. Then for any rational point $Q \in E_{(D)}(\mathbb{Q})$ with $\mathrm{red}_q(Q^\iota) \neq O$, we have*

$$\langle P_q, c_q(Q) \rangle_{q,\,2} = 1.$$

Here Q^ι is the image of Q in $E(K)$, with $K = \mathbb{Q}(\sqrt{D})$ and red *is the reduction in $E(K)$ modulo the prime v in K with $v^2 = q$.*

Proof. By Proposition 5.10, $(\mathrm{Fr}_q - 1)\mathrm{red}(R) \neq \mathrm{red}_q(Q^\iota) = e$. Also $(\mathrm{Fr}_q - 1)\mathrm{red}(R) \neq O$ since P is not a local square at q. So the result follows by Proposition 4.2. □

Proposition 5.12. *Under the same conditions as Proposition 5.11, we have :*

Any rational point of $E_{(-q)}(\mathbb{Q})$ with $\mathrm{red}_q(Q^\iota) \neq O$ has the property that

$$Q \notin 2E_{(-q)}(\mathbb{R}).$$

Proof. Consider the orthogonality relation between $E(\mathbb{Q})$ and $E_{(-q)}(\mathbb{Q})$.

$\langle P_q, c_q(Q) \rangle_{q,\,2} + \langle P_\infty, c_\infty(Q) \rangle_{\infty,\,2} = O$ and $\langle P_q, c_q(Q) \rangle_{q,\,2} = 1$ by Proposition 5.11.

Thus $\langle P_\infty, c_\infty(Q) \rangle_{\infty,\,2} = 1$, which implies that $Q \notin 2E_{(-q)}(\mathbb{R})$. □

We have an extension of Main Theorem 1 regarding on the real connected component the point belongs.

Theorem 5.13. *Let $P \in E(\mathbb{Q}) \setminus 2E(\mathbb{R})$ and $D = D_1 D_2 < 0$ where P is a square at prime divisors of D_1 and P is not a square at prime divisors of D_2. Assume further*

that for any rational point $Q \in E_{(D)}(\mathbb{Q})$ whose image in $E(K)$ has a nontrivial reduction and $E(\mathbb{Z}/q\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z}$ at all prime divisors $q|D_2$. Then

(a) *$Q \in 2E_{(D)}(\mathbb{R})$, if the number of prime divisors of D_2 is even.*

(b) *$Q \notin 2E_{(D)}(\mathbb{R})$, if the number of prime divisors of D_2 is odd.*

Proof. By Proposition 5.11, $\langle P_q, c_q(Q) \rangle_{q,2} = 1$ at all prime divisors q of D_2.

If the number of prime divisors of D_2 is even, then

$$\sum\nolimits_{q|D} \langle P_q, c_q(Q) \rangle_{q,2} = \sum\nolimits_{q|D_2} \langle P_q, c_q(Q) \rangle_{q,2} = 0.$$

So $\langle P_\infty, c_\infty(Q) \rangle_{\infty,2} = 0$ and this case reduces to that of Main Theorem 1.

If it is odd, then $\sum_{q|D_2} \langle P_q, c_q(Q) \rangle_{q,2} = 1$ so $\langle P_\infty, c_\infty(Q) \rangle_{\infty,2} = 1$ and this case reduces to that of Proposition 5.12. □

Lemma 5.14. *If the denominator of x-coordiante of $Q \in E_{(D)}(\mathbb{Q})$ is not divisible by q where $q|D$, then $\mathrm{red}_q(Q^\iota) \neq O$.*

Proof. Let $\mathrm{denom}(\frac{a}{b})$ denote b when $a, b \in \mathbb{Z}$ and $(a, b) = 1$.

Let $Q = (x\,,\, y)$ and $q = v^2$ in $K = \mathbb{Q}(\sqrt{D})$. Let $(q, \Delta(E)) = 1$.

Since x is a rational number, $q \nmid \mathrm{denom}(x) \Leftrightarrow v \nmid \mathrm{denom}(x)$. If this is the case, then $q \nmid \mathrm{denom}(Dy^2) \Leftrightarrow v \nmid \mathrm{denom}(Dy^2)$ because $\mathrm{denom}(x)$ and $\mathrm{denom}(Dy^2)$ have the same factors.

Suppose $q|\mathrm{denom}(y)$, which is equivalent to $q^2|\mathrm{denom}(y^2)$. Then $q|\mathrm{denom}(Dy^2)$ because D is square-free, but we know that this is not the case from our assumption that $q \nmid \mathrm{denom}(x)$. Hence $q \nmid \mathrm{denom}(y)$. Therefore Dy^2 is a q-adic unit and $\sqrt{D}y$ is a v-adic unit in $\mathcal{K}$.

If we consider the reduction of $Q^\iota = (x\,,\, \sqrt{D}y)$ satisfying $(\sqrt{D}y)^2 = x^3 + Ax + B$, then we get $\mathrm{red}_q(Q^\iota)$ (at v) is a finite 2-torsion point, i.e. $\mathrm{red}_q(Q^\iota)$ is not a point at infinity O. □

From the proof of Theorem 5.13 and the above Lemma, the following result about the denominator of the x-coordinate of rational point of $E_{(D)}(\mathbb{Q})$ is obtained.

Corollary 5.15. *Decompose D into D_1D_2 as in Theorem 5.13.*

(a) *If the number of prime divisors of D_2 is even and $Q \in E_{(D)}(\mathbb{Q}) \setminus 2E_{(D)}(\mathbb{R})$, then the denominator of the x-coordinate of Q and D_2 has a common divisor. Moreover the number of "common" prime divisors of D_2 are odd.*

(b) *If the number of prime divisors of D_2 is odd and $Q \in 2E_{(D)}(\mathbb{R})$, then the denominator of the x-coordinate of Q and D_2 has a common divisor.*

In the following we will prove a Proposition which may be useful to determine whether or not a point $P \in E(\mathbb{Q})$ is a square at a given prime. It is valid for any elliptic curve with $E(\mathbb{Q})_2 = O$. Note that this Proposition asserts that if there exists a point in $E(\mathbb{Q})$ and a prime q which satisfies the condition $E(\mathbb{Q}_q)_2 = O$, then we know that P is a local square at q without knowing what the point P is specifically. Thus it may help us to extend the results of this section to other elliptic curves whose generators are not exactly known.

Proposition 5.16. *Let $E(\mathbb{Q}_q)_2 = O$ where $q \nmid 2N\infty$. Then P is a local square at q.*

Proof. Let $R \in E(\overline{\mathbb{Q}})$ satisfy $2R = P$.

Let $(\mathrm{Fr}_q - 1)R = t \in E_2$.

Since $\mathrm{Fr}_q - 1$ is an automorphism on E_2 if $E(\mathbb{Q}_q)_2 = O$, choose $t' \in E_2$ such that $(\mathrm{Fr}_q - 1)t' = t$. (Let $t_1, t_2 \in E_2$ and $t_1 \neq t_2$. Since $t_1 - t_2 \in E_2 \setminus O$, so $(\mathrm{Fr}_q - 1)(t_1 - t_2) \neq O$, i.e. $(\mathrm{Fr}_q - 1)t_1 \neq (\mathrm{Fr}_q - 1)t_2$. Thus $\mathrm{Fr}_q - 1$ is an injective endomorphism on a finite group E_2, therefore an automorphism.)

Considering $(\mathrm{Fr}_q - 1)(R + t') = (\mathrm{Fr}_q - 1)R + (\mathrm{Fr}_q - 1)t' = t + t = O$, we have that $R + t' \in E(\mathbb{Q}_q)$. Thus $2(R + t') = P$ implies that P is a square at q. □

General Case

Previously, we considered the case when $E(\mathbb{Z}/q\mathbb{Z})_2 = \mathbb{Z}/2\mathbb{Z}$ in Proposition 5.11. Also we considered the case when $E(\mathbb{Z}/q\mathbb{Z})_2 = O$ in Proposition 5.16. Now consider the case when D includes a factor q at which $E(\mathbb{Z}/q\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$.

Let's decompose D into relatively prime factors D_1, D_2, and D_3 where

$$\begin{cases} q \,|\, D_1 & \Leftrightarrow \ P \text{ is a square at } q \\ q \,|\, D_2 & \Leftrightarrow \ q \nmid D_1 \text{ and } E(\mathbb{Z}/q\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z} \\ q \,|\, D_3 & \Leftrightarrow \ q \nmid D_1 \text{ and } E(\mathbb{Z}/q\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}. \end{cases}$$

Suppose $\mathrm{red}_q(Q^i) \neq O$ at all $q \,|\, D_2$. Then

$$\begin{aligned} \sum_{q \,|\, D_3} \langle P_q, c_q(Q) \rangle_{q,2} &= \sum_{q \,|\, D_1 D_2 \infty} \langle P_q, c_q(Q) \rangle_{q,2} \\ &= \sum_{q \,|\, D_2} \langle P_q, c_q(Q) \rangle_{q,2} + \langle P_\infty(Q), c_\infty(Q) \rangle_{\infty,2} \\ &= \text{number of prime divisors of } D_2 + \epsilon \pmod 2 \end{aligned}$$

where $\epsilon = \begin{cases} 0 & \text{if } Q \in 2E_{(D)}(\mathbb{R}) \\ 1 & \text{if } Q \notin 2E_{(D)}(\mathbb{R}) \end{cases}$

Moreover by Proposition 4.2, we have

$$(-1)^{\langle P_q, c_q(Q)\rangle_{q,2}} = [e_q(P), e'_q(Q)]_2 = \begin{cases} 1 & \text{if } e'_q(Q) = O \text{ or } e'_q(Q) = e_q(P) \\ -1 & \text{otherwise.} \end{cases}$$

This can be considered as a general restriction which the orthogonality relation imposes on the rational points of the Mordell-Weil group.

6. QUADRATIC TWISTS OF $y^2 = 4x^3 - 4x + 1$

In this section we will consider the curve $y^2 = 4x^3 - 4x + 1$ and its quadratic twists to see the usefulness of the theorems established in the previous section. It will be proved that this curve satisfies all the requirements to apply the theorems.

We start by proving a lemma which describes the behaviour of x-coordinates of twisted elliptic curves. This is useful in finding rational points actually.

Most of calculations in this section are done by algorithms written in MATLAB.

Let $y^2 = x^3 + Ax + B$ and $E_{(D)} : Dy^2 = x^3 + Ax + B$ where $(D\,,\,2N\infty) = 1$.

Proposition 6.1. *Every rational point $Q \in E_{(p)}(\mathbb{Q})$ with p-integral coordinates has its x-coordinates of the form*

$$x(Q) = \frac{a + pm}{1 + pn} \quad \textit{for some} \;\; m, n \in \mathbb{Z}$$

where $a \in \mathbb{Z}$, $(\bar{a}, 0) \in E(\mathbb{Z}/p\mathbb{Z})_2 \setminus O$ and $a \equiv \bar{a} \pmod{p}$.

Proof. Consider the p-twisted elliptic curve $py^2 = x^3 + Ax + B$ and its rational point $Q = (x, y) \in E_{(p)}(\mathbb{Q})$.

Since Q is p-integral, we have $x^3 + Ax + B \equiv O \pmod{p}$, that is, $x(Q) \equiv \bar{a} \pmod{p}$ for some $(\bar{a}, 0) \in E(\mathbb{Z}/p\mathbb{Z})_2 \setminus O$. So

$$x(Q) = \frac{\alpha + pk}{\beta + pl} \text{ where } \frac{\alpha}{\beta} \equiv \bar{a} \pmod{p} \text{ and } k, l \in \mathbb{Z}.$$

We exclude the case when $\beta \equiv O \pmod{p}$, in which case Q is not p-integral. So $\beta \not\equiv O \pmod{p}$. Let β^* be the arithmetic inverse of β in $\mathbb{Z}/p\mathbb{Z}$. Then

$$x(Q) = \frac{\alpha + pk}{\beta + pl} = \frac{\beta^*(\alpha + pk)}{\beta^*(\beta + pl)} = \frac{\alpha\beta^* + p(\beta^* k)}{\beta\beta^* + p(\beta^* l)}.$$

Let $\alpha\beta^* = a + pi,\ \beta\beta^* = 1 + pj \quad i, j \in \mathbb{Z}$. Thus

$$x(Q) = \frac{a + p(\beta^* k + i)}{1 + p(\beta^* l + j)} = \frac{a + pm}{1 + pn} \quad \exists m, n \in \mathbb{Z}. \qquad \square$$

Example. $-139y^2 = 4x^3 - 4x + 1$. $E(\mathbb{Z}/139\mathbb{Z})_2 = \{O, (74, 0), (94, 0), (110, 0)\}$.

$x = \dfrac{94 + 139 \times 17}{1 + 137 \times (-7)}$ gives a point $Q = (-\dfrac{91}{36}\,,\, \dfrac{67}{2^2 \cdot 3^2}) \in E_{(-139)}(\mathbb{Q})$.

Corollary 6.2. *Every rational point $Q \in E_{(D)}(\mathbb{Q})$, $(D, 2N\infty) = 1$, D is square-free, with p-integral coordinates at each prime divisors p of D has its x-coordinates of the form*

$$x(Q) = \frac{a_p + pm_p}{1 + pn_p} \quad \textit{for some} \;\; m_p, n_p \in \mathbb{Z}$$

where $a_p \in \mathbb{Z}$, $(\bar{a}_p, 0) \in E(\mathbb{Z}/p\mathbb{Z})_2 \setminus O$ and $a_p \equiv \bar{a}_p \pmod{p}$.

Proof. The proof at $p|D$ is exactly the same as that of Lemma 6.1. □

Proposition 6.3. *Every rational point $Q \in E_{(D)}(\mathbb{Q})$, $(D, 2N\infty) = 1$, D is square-free, with p-integral coordinates at prime divisor p of D has its x-coordinates of the form*

$$x(Q) = a_p + p \cdot \frac{m}{n^2} \quad \textit{for some} \;\; m, n \in \mathbb{Z}$$

where $a_p \in \mathbb{Z}$, $(\bar{a}_p, 0) \in E(\mathbb{Z}/p\mathbb{Z})_2 \setminus O$ and $a_p \equiv \bar{a}_p \pmod{p}$.

Proof. Let $f(x) = x^3 + Ax + B$ and $1 + pn = s\alpha^2$ and s is square-free. Then $x(Q)$ is given by $(a_p + pm)/(1 + pn)$ for some $m, n \in \mathbb{Z}$ by Corollary 6.2. So

$$\begin{aligned} f(\frac{a_p + pm}{1 + pn}) &= (\frac{a_p + pm}{1 + pn})^3 + A \cdot (\frac{a_p + pm}{1 + pn}) + B \\ &= \frac{(a_p + pm)^3 + A(a_p + pm)(1 + pn)^2 + B(1 + pn)^3}{(1 + pn)^3} \\ &= \frac{(a_p + pm)^3 + A(a_p + pm)s^2\alpha^4 + Bs^3\alpha^6}{s^3\alpha^6}. \end{aligned}$$

For $(a_p + pm)/(1 + pn)$ to be an x-coordinate of a rational point of $E_{(D)}(\mathbb{Q})$, this number should be $D\cdot$(a square). So it is necessary that $s|a_p + pm$, otherwise the denominator cannot be a square.

Thus $\begin{cases} 1 + pn = s\alpha^2 \\ a_p + pm = s\beta \end{cases} \Rightarrow \; p(na_p - m) = s(a_p\alpha^2 - \beta) \; \Rightarrow \; s|p(na_p - m) \; \Rightarrow$ $s|na_p - m$.

Hence $na_p - m = sk' \;\; \exists k' \in \mathbb{Z} \Leftrightarrow m = na_p - sk' = na_p + sk \;\; \exists k \in \mathbb{Z}$.

$$\begin{aligned} \text{Therefore } x(Q) = \frac{a_p + p(na_p + sk)}{1 + pn} &= \frac{a_p(1 + pn) + spk}{1 + pn} \\ &= a_p + \frac{spk}{1 + pn} = a_p + \frac{spk}{s\alpha^2} = a_p + p \cdot \frac{k}{\alpha^2} \end{aligned}$$

So we have the desired result by adjusting variables from k and α to m and n. □

Remark. A point $Q \in E_{(D)}(\mathbb{Q})$, $(D, 2N\infty) = 1$, D is square-free, with p-integral x-coordinate at all prime divisors p of D has its x-coordinate of the form

$$x(Q) = \frac{a + Dm}{1 + Dn} \quad \text{for some } \ m, n \in \mathbb{Z} \text{ or}$$

$$x(Q) = a + D \cdot \frac{m}{n^2} \quad \text{for some } \ m, n \in \mathbb{Z}$$

where $a \in \mathbb{Z}$ is obtained from Chinese Remainder Theorem satisfying $a \equiv \bar{a}_p \pmod{p}$ at all prime divisors p of D.($\bar{a}_p$ comes from the previous Propositions.)

In the following we will find some numerical data for the elliptic curve

$$E : y^2 = 4x^3 - 4x + 1 \ .$$

There exists a point $P = (0, 1) \in E(\mathbb{Q}) \setminus E(\mathbb{R})$ and $\Delta(E) > 0$.

We can prove that the value of Tate pairing at the conductor is 0. In our specific case $N = 37$. The modular invariant $J(E) = 2^{12} \cdot 3^3/37$.

Proposition 6.4. $\forall x \in H^1(\mathbb{Q}_{37}, E)_2^{nr}$, $\langle P_{37}, x \rangle_{37,2} = 0$.

Proof. $[\pi_0(\tilde{E})] = m_{37}(E) = 1$.(See [Ko2], §3).

So $H^1(\mathbb{Q}_{37}, E)_{nr} = H^1(\mathrm{Gal}(\mathbb{Q}_{37}^{nr}/\mathbb{Q}_{37}), \pi_0(\tilde{E})) = 0$. □

Therefore all the results of §5 applies to this elliptic curve and its quadratic twists.

Data 1.

(**A**) Odd primes $p < 500$ at which P is a local square ($p \neq 37$). (59)

3, 7, 11, 23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 83, 97, 101, 113, 127, 139, 149, 157, 173, 179, 181, 191, 197, 199, 211, 223, 227, 229, 239, 241, 257, 263, 271, 277, 281, 283, 293, 307, 331, 337, 347, 359, 373, 379, 383, 389, 397, 409, 419, 433, 439, 443, 463, 467, 479, 499.

(**B**) D's satisfying $-D \equiv$ a square (mod $4 \cdot 37$), $-D \neq -3, -4$, $0 < D < 500$, D is square-free, $(D\,,\, 2 \cdot 37) = 1$. (47)

7, 11, 47, 67, 71, 83, 95, 107, 115, 123, 127, 139, 151, 155, 159, 195, 211, 215, 219, 223, 231, 247, 255, 263, 271, 287, 295, 299, 303, 307, 323, 359, 367, 371, 379, 391, 395, 403, 411, 419, 435, 443, 447, 451, 455, 471, 491.

(**C**) D's of (**B**) such that $E_{(-D)}(\mathbb{Q})$ has a positive rank

$$D = 95, 107, 139, 215, 255, 391.$$

(According to [Ko2] Theorem H, for all other cases it is proved that $E_{(D)}(\mathbb{Q}) = O$. For these 6 cases we can actually find a point not at infinity on each of them. This is enough to conclude that they have positive rank, since they have trivial torsion part.)

(**D**) D's of (**B**) such that all prime divisors of D are from (**A**). (26)

7, 11, 47, 71, 83, 123, 127, 139, 159, 211, 219, 223, 231, 263, 271, 287, 303, 307, 359, 371, 379, 419, 443, 447, 451, 471.

Let $\mathbf{V}_{500}$ be the set of D's obtained in (**D**).

$\#\mathbf{V}_{500} = 26$ and for one of them the corresponding $(-D)$-twisted elliptic curve has a positive rank. $(D = 139)$

$\#(\{D\text{'s in (B)}\} \setminus \mathbf{V}_{500}) = 21$ and for 5 of them the corresponding $(-D)$-twisted elliptic curves have positive ranks.

$$D = 95, 107, 215, 255, 391.$$

Data 2.

(a) There are 30 primes $p < 500$ at which $E(\mathbb{Z}/p\mathbb{Z})_2 = O$ ($p \neq 2, 37$):
3, 7, 11, 41, 47, 53, 71, 73, 83, 101, 127, 149, 157, 173, 181, 197, 211, 223, 229, 263, 271, 307, 337, 359, 373, 379, 397, 419, 433, 443.

According to Proposition 5.16, P is a square at these primes. So these primes form a subset of those primes in Data 1(A).

(b) There are 51 primes $p < 500$ at which $E(\mathbb{Z}/p\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z}$ $(p \neq 2, 37)$:
5, 13, 17, 19, 23, 29, 31, 43, 59, 61, 79, 89, 97, 103, 109, 113, 131, 163, 167, 179, 191, 193, 199, 227, 239, 241, 251, 257, 277, 281, 283, 311, 313, 331, 347, 353, 383, 389, 401, 409, 421, 431, 439, 449, 457, 461, 463, 467, 479, 487, 499.

(c) There are 12 primes $p < 500$ at which $E(\mathbb{Z}/p\mathbb{Z})_2 \simeq \mathbb{Z}/2\mathbb{Z}+\mathbb{Z}/2\mathbb{Z}$ $(p \neq 2, 37)$:
67, 107, 137, 139, 151, 233, 269, 293, 317, 349, 367, 491.

Interpretation of the Main Theorem 1.

It is known that there are 6 twisted elliptic curves $E_{(-D)}(\mathbb{Q})$ among $(-D)$'s computed in Data 1(B) with rank $E_{(-D)}(\mathbb{Q}) \neq 0$. (See Data 1(C))

The Main Theorem 1 says that for those $D \in \mathbf{V}_{500}$, $E_{(-D)}(\mathbb{Q}) \subset 2E_{(-D)}(\mathbb{R})$.

On the other hand, for all of those 5 of $D \notin \mathbf{V}_{500}$, I could find rational points on $E_{(-D)}(\mathbb{Q}) \setminus 2E_{(-D)}(\mathbb{R})$.

For example,

$$(\frac{8}{19}, \frac{23}{19^2}), \quad (\frac{13}{16}, \frac{1}{2^6}), \quad (\frac{2}{5}, \frac{1}{5^2}), \quad (\frac{163}{204}, \frac{257}{(2\cdot 3\cdot 17)^2}), \quad (\frac{5}{9}, \frac{1}{3^3})$$

are the points on $E_{(-D)}(\mathbb{Q})\setminus 2E_{(-D)}(\mathbb{R})$ for $D = 95,\ 107,\ 215,\ 255,\ 391$ respectively in this order. These points were found using Corollary 6.2 and Proposition 6.3.

Interpretation of Theorem 5.13.

Based on Data 1 (A) and Data 2, we can divide D into types described by Main Theorem 1, Theorem 5.13 (a) or (b), or the general case.

There are 196 elliptic curves which correspond to $(-D)$'s such that $-D \neq -3, -4$, $0 < D < 500$, D is square-free, $(D\,, 2\cdot 37) = 1$. And there are 180 elliptic curves whose x-coordinates are under the restriction by the Main Theorems 1 or Theorem 5.13.

Let's see how we can use these results to analyze the behavior of rational points on quadratic twists $E_{(-D)}(\mathbb{Q})$ corresponding to $-D$ in Data 1(C).

(a) $D = 95 = 5\times 19$. This is the case of Theorem 5.13(a). So if a rational point exists on $E_{(-95)}(\mathbb{Q})\setminus 2E_{(-95)}(\mathbb{R})$, then its denominator must be divisible either by 5 or 19 :

$$(\frac{4}{5}, \frac{1}{5^2}), \quad (\frac{8}{19}, \frac{23}{19^2}).$$

(b) $D = 215 = 5\times 43$. This is the case of Theorem 5.13(a). So if a rational point exists on $E_{(-215)}(\mathbb{Q}) \setminus 2E_{(-215)}(\mathbb{R})$, then its denominator must be divisible either by 5 or 43 :

$$(\frac{2}{5}, \frac{1}{5^2}), \quad (\frac{16}{43}, \frac{67}{43^2}).$$

(c) $D = 255 = 3\times 5\times 17$. This is the case of Theorem 5.13(a). So if a rational point exists on $E_{(-255)}(\mathbb{Q}) \setminus 2E_{(-255)}(\mathbb{R})$, its denominator must be divisible

either by 5 or 17 :

$$(\frac{163}{2^2 \cdot 3 \cdot 17}, \frac{257}{(2 \cdot 3 \cdot 17)^2}).$$

(d) $D = 391 = 17 \times 23$. This is the case of Theorem 5.13(b) since P is a local square at 23. Therefore, it is possible to find a point like $(\frac{5}{9}, \frac{1}{3^3})$. But on $2E_{(-391)}(\mathbb{R})$, every point has its x-coordinate whose denominator is divisible either by 17 or 23.

(e) For $E_{(-107)}(\mathbb{Q})$ the restriction is by the general case. For $E_{(-139)}(\mathbb{Q})$, P is a square at 139, so there's no rational point at all on $E_{(-139)}(\mathbb{Q}) \setminus 2E_{(-139)}(\mathbb{R})$ as considered earlier. (Main Theorem 1.)

These exhaust all known positive rank cases.

From the theorems and examples so far, it can be said that the orthogonality relation imposes direct restriction on the existence or type of rational points on quadratic twists over $\mathbb{Q}$. The restrictions can be simply described in some cases if we can compute the value of Tate pairing at prime divisors of conductor of E.

7. A NEW RESULT ON THE RANK BOUND

Let E be an elliptic curve with $E(\mathbb{Q})_2 = O$ and $\mathbb{Q}(\sqrt{\Delta})$ is a PID where $\Delta = \Delta(E)$ is the discriminant of E.

The aim of this section is to prove that $\operatorname{rank} E(\mathbb{Q}) \leqslant 2n$ where $n = \nu(2N\infty)$.

I would like to say thank you to Prof. Ram Murty for his suggestions and helps to clarify the proof and extend the result.

We may assume that $\operatorname{rank} E(\mathbb{Q}) \geqslant 1$. Otherwise $\operatorname{rank} E(\mathbb{Q}) = 0$ and the result on the rank bound holds trivially.

The point is that most of our previous results remain true over general number fields. In fact, Kolyvagin's papers are already based on the general setting.

Let F be a finite algebraic extension of $\mathbb{Q}$.

Mordell-Weil theorem over F

$$E(F) \simeq T \times \mathbb{Z}^{r(E,F)}$$

where T is the torsion part. Here $r(E, F)$ is a nonnegative integer.

Tate pairing is defined over $\mathcal{F}$, where $\mathcal{F}$ is the localization of F:

$$H^1(\mathcal{F}, E_M) \times H^1(\mathcal{F}, E_M) \to \mathbb{Z}/M\mathbb{Z}.$$

For this see [Ba]. We again consider the case when $M = 2$.

Local-global duality theorem (Orthogonality relation)

For $P \in E(F)/ME(F)$ and $C \in H^1(F, E)_M$, the sum of the local Tate pairing $\langle P_\ell, C_\ell \rangle_{\ell,M}$ over all prime divisors of F (including ∞) equals zero where P_ℓ and C_ℓ are the localizations of P and C at ℓ respectively. In other words,

$$\sum_{\ell} \langle P_\ell, C_\ell \rangle_{\ell,M} = 0.$$

Construction of explicit cohomology classes

For $D \in F$ with D square-free and $(2N, D) = 1$, we have $E_{(D)}$ and E are isomorphic over $K_F = F(\sqrt{D})$ under an isomorphism $\imath : (x\,,\, y) \mapsto (x\,, \sqrt{D}y)$ and we have

$$\imath\,(E_{(D)}(F)) = \{\, Q \in E(K_F) \,|\, \operatorname{Norm}_{K_F/F}\, Q = 0\} \hookrightarrow H^1(F, E)_2.$$

Proposition 4.2 can be formulated without change if we replace $\mathbb{Q}$ by F as following Proposition 7.1 shows. The more general formula can be found in [Ko1] where it was done for cyclic extensions not just for quadratic extensions. We assume that D is square-free and $(2N, D) = 1$ in the following Proposition:

Proposition 7.1. *Let $\ell | D$, ℓ a prime of F, $P \in E(F)/2E(F)$, and $Q \in E_{(D)}(F)$. Then*

$$(-1)^{\langle P_\ell, c_\ell(Q)\rangle_{\ell,2}} = [e_\ell(P), e'_\ell(Q)]_2$$

where P_ℓ is the class of P in $E(\mathcal{F})/2E(\mathcal{F})$. Here $e_\ell(P)$ and $e'_\ell(Q)$ are defined in exactly the same way as in Definitions 1 and 2 of §4 if we replace $\mathbb{Q}$ by F and K by K_F, and $\mathcal{F}$ is the localization of F at ℓ.

Remark. For a prime ℓ of F which divides p of $\mathbb{Q}$, we denote by Fr_ℓ the Frobenius endomorphism of $E(\overline{\mathbb{Q}}_p)$ over $E(\mathcal{F})$ given by $\mathrm{Fr}_\ell(x, y) = (x^{\mathrm{Norm}(\ell)}, y^{\mathrm{Norm}(\ell)})$. Here $\mathrm{Norm}(\ell) = p^f$ if f is the corresponding inertial degree.

Corollary 7.2. *Assume the conditions of Proposition 7.1. If $e \in E_{(D)}(F)_2$, then*

$$(-1)^{\langle P_\ell, c_\ell(e)\rangle_{\ell,2}} = [e_\ell(P), e]_2,$$

and $e_\ell(P) = O$ if and only if P is a square at ℓ.

Proof. Clear from the Definitions 1 and 2 of §4. □

Let Γ be a free subgroup of $E(\mathbb{Q})$ defined by $\Gamma = \{P \in E(\mathbb{Q}) |\ P$ is a point of infinite order, a square at $2N\infty$ but not a global square over $\mathbb{Q}\ \}$.

Lemma 7.3. *There is an injective homomorphism*

$$\alpha : E(\mathbb{Q}_q)/2E(\mathbb{Q}_q) \to (\mathbb{Z}/2\mathbb{Z})^a$$

where $a = 2$ if q is an odd prime, $a = 3$ if $q = 2$, and $a = 1$ if $q = \infty$.

Proof. Consider

$$\mathrm{Hom}(\mathbb{Q}_q, E_2) \cong \mathrm{Hom}(\mathbb{Q}_q, \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}) \cong \mathrm{Hom}(\mathbb{Q}_q, \mu_2) + \mathrm{Hom}(\mathbb{Q}_q, \mu_2).$$

Then using Kummer theory, as $\{\pm 1\} \subset \mathbb{Q}_q$, we have $\mathrm{Hom}(\mathbb{Q}_q, \mu_2) \cong \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \cong (\mathbb{Z}/2\mathbb{Z})^a$ where $a = 2$ if q is an odd prime, $a = 3$ if $q = 2$, and $a = 1$ if $q = \infty$.

On the other hand, we have $[E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)] \cdot [H^1(\mathbb{Q}_q, E)_2] = [H^1(\mathbb{Q}_q, E_2)]$ and $[E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)] = [H^1(\mathbb{Q}_q, E)_2]$. (For these equalities, see [Ba], p.37.)

As $E(\mathbb{Q}_q)/2E(\mathbb{Q}_q)$ is a subgroup of $H^1(\mathbb{Q}_q, E_2)$ from the descent exact sequence, we get our conclusion. □

Proposition 7.4. *Let* $\operatorname{rank} E(\mathbb{Q}) = r$. *Then* $\operatorname{rank}(\Gamma) \geqslant r - 2n$, *where* n *is the number of prime divisors of* $2N\infty$ *in* $\mathbb{Q}$. *Here* $\operatorname{rank}(\Gamma)$ *denotes the maximum number of linearly independent points in the set* Γ *up to torsion part.*

Proof. Let $P \in E(\mathbb{Q})$ be a point of infinite order. (The existence of such a point is guaranteed by the assumption that $\operatorname{rank} E(\mathbb{Q}) \geq 1$.)

Then we define maps for $q|N$ and $q \neq 2$

$$f_q : E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{loc} E(\mathbb{Q}_q)/2E(\mathbb{Q}_q) \xhookrightarrow{\alpha} \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} =< a_q, b_q > .$$

For $q = 2$, let $f_2 : E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{loc} E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) \xhookrightarrow{\alpha} (\mathbb{Z}/2\mathbb{Z})^3 =< a_2, b_2, a_\infty >$.

Here we write a_∞ instead of c_2 for notational convenience.

For $q = \infty$, let $f_\infty : E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{loc} E(\mathbb{R})/2E(\mathbb{R}) \xhookrightarrow{\alpha} \mathbb{Z}/2\mathbb{Z} =< b_\infty >$.

For $q|N$ and $q \neq 2$, define $f_q^1(P)$ and $f_q^2(P)$ in $\mathbb{Z}/2\mathbb{Z}$ by

$$f_q(P) = f_q^1(P)a_q + f_q^2(P)b_q.$$

For $q = 2$ and ∞, define analogously by $f_2(P) = f_2^1(P)a_2 + f_2^2(P)b_2 + f_\infty^1(P)a_\infty$ and $f_\infty(P) = f_\infty^1(P)b_\infty$.

If P is a square at q if and only if $f_q^k(P) = 0$ for $k = 1, 2$ when $q \neq 2, \infty$. (We can say a similar fact for the other cases also.)

Let $\{P_i\}_{1 \leq i \leq r}$ be a set of generators of $E(\mathbb{Q})$ of infinite order. Consider all points P which can be expressed as $P = \sum_{i=1}^r m_i P_i$. (Some points of $E(\mathbb{Q})$ may not be expressed in this way. We exclude those points.)

Suppose that P is a square at prime divisors of $q_j (1 \leq j \leq n)$ of $2N\infty$.

Then we have a set of relations:

$$f_{q_j}^k(P) = \sum_{i=1}^r n_i f_{q_j}^k(P_i) = O$$

where $n_i \in \mathbb{Z}/2\mathbb{Z}$ such that $n_i \equiv m_i \pmod 2$. (We have one linear equation over $\mathbb{Z}/2\mathbb{Z}$ for each generator upon localizations at bad primes.)

Let $a_{ji} = f_{q_j}^1(P_i)$, and $b_{ji} = f_{q_j}^2(P_i)$. And let $A = (a_{ij}), B = (b_{ij})$ and $X(P) = \begin{bmatrix} n_1 \\ \vdots \\ n_r \end{bmatrix}$. We will write $X = X(P) \in (\mathbb{Z}/2\mathbb{Z})^r$ within context. Note that the matrices A and B depend on the generators $\{P_i\}_{1 \leq i \leq r}$, but not on particular points P. So the coefficients a_{ij}'s are constants, but X is determined by P.

Let $C = \left[\begin{array}{c} A \\ \hline B \end{array}\right]$. That is, C is the matrix composed of first n-rows of its entries coming from those of matrix A and the second n-rows of entries coming from those of matrix B, so C is a $2n \times r$ matrix.

Hence we have the following:

$P = \sum_{i=1}^{r} m_i P_i$ is a square at prime divisors of $2N\infty$ if and only if $CX(P) = O$.

Let $r = 2n + c$.

Then the solutions of the homogeneous system $CX = O$ has at least c independent vectors $X \in (\mathbb{Z}/2\mathbb{Z})^r$ (exactly c independent vectors X if C is nondegenerate). So the solutions of the system $CX = O$ has rank at least $c = r - 2n$. Now any nontrivial point P satisfying $CX(P) = O$ is a point in Γ. $\square$

The following Theorem 7.5 and Proposition 7.6 were provided by Kolyvagin in reply to my question.

Theorem 7.5. *Let a point P on an elliptic curve $E(K)$ be a square over $K' = K(E_2)$, then it is a square over K.*

Proof. K'/K is a finite Galois extension. Let $H = Gal(K'/K) \hookrightarrow GL_2(\mathbb{Z}/2\mathbb{Z}) \xrightarrow{\sim} S_3$,

where S_3 is the permutation group of e_1, e_2 and $e_3 = e_1 + e_2$ which denote the nontrivial elements of E_2. So H is a subgroup of S_3.

Since P is a square in $E(K')$, there exists $Q \in E(K')$ such that $2Q = P$.

Then for all $h \in H$, $2(h(Q)) = h(2Q) = hP = P$.

So $h(Q) - Q \in E_2$ and $h \mapsto h(Q) - Q$ is a cocycle of H in E_2 because

$$\mathrm{Norm}_{K'/K}\, h(Q) = \sum_{\sigma \in H} \sigma h Q = \sum_{\sigma \in H} \sigma Q = \mathrm{Norm}_{K'/K}\, Q,$$

i.e. $h(Q) - Q$ is a point of trivial norm.

We will show that $H^1(H, E_2) = O$. Then $h(Q) - Q = he - e$ for some $e \in E_2$. This implies that $h(Q - e) = Q - e$. So $Q - e \in E(K)$ and $P = 2(Q - e) \in 2E(K)$.

Now the only remaining thing is to prove that $H^1(H, E_2) = O$. There are three cases(we consider the case $H \neq O$);

Case 1) H has order 2.

$H = \{1, \sigma\}$ where σ is a transposition, say $\sigma(e_1) = e_2, \sigma(e_2) = e_1$, and $\sigma(e_3) = e_3$. Then

$\sigma(e) + e = O \Leftrightarrow e = O$ or $e = e_3 = \sigma(e_1) - e_1 = \sigma(e_2) - e_2 \Rightarrow H^1(H, E_2) = O$.

Case 2) H has order 3.

$H^1(H, E_2) = O$ because it is killed both by $|H| = 3$ and 2.

Case 3) $H = S_3$.

We have a Restriction-Inflation exact sequence (A_3 is a normal subgroup of S_3 because it is a subgroup of index 2)

$$O \to H^1(S_3/A_3, E_2^{A_3}) \xrightarrow{Inf} H^1(S_3, E_2) \xrightarrow{Res} H^1(A_3, E_2)$$

Here $E_2^{A_3} = O$, so $H^1(S_3/A_3, E_2^{A_3}) = O$ and $H^1(A_3, E_2) = O$ by the second case. Therefore we conclude that $H^1(S_3, E_2) = O$. □

The above theorem implies that a point $P \in \Gamma$ is not a global square over $L = \mathbb{Q}(E_2)$ either.

Proposition 7.6. *If $P \in E(K)$ is a square almost everywhere, then it is a global square, i.e. $P \in 2E(K)$.*

Proof. Let $K' = K(E_2)$. We will prove that if P is a square almost everywhere, it is a square in $E(K')$. Then the result would follow from Theorem 7.5.

Let $Q \in E(\bar{K})$ be such that $2Q = P$.

Let v be a prime of K such that P is a local square at v. Then there is a $Q_v \in E(K_v)$ such that $P = 2Q_v$.

Let $F = K(Q)$, the field generated by the coordinates of Q over K. Then F is a finite subextension of $\bar{K}$. Let w be a prime of F with $w|v$.

Then $F \subset F_w$ and $Q \in E(F_w)$ where $2Q = P$. And $Q_v \in E(F_w)$ under a canonical embedding $K_v \hookrightarrow F_w$.

So $2(Q - Q_v) = O$, that is $Q - Q_v \in E_2$. Thus $Q = Q_v + e \in E(K_v(E_2))$, which implies that $F \subset K_v(E_2)$.

Thus $F(E_2) \subset K_v(E_2) \subset K'_{v'}$ for almost all prime v of K, where v' is a prime of K' dividing v. Moreover $K' \subset F(E_2)$, so $F(E_2) = K'$. And hence $Q \in E(K')$. □

Recall that Γ is defined by $\Gamma = \{P \in E(\mathbb{Q}) |\ P$ is a point of infinite order, a square at $2N\infty$ but not a global square over $\mathbb{Q}\ \}$.

Let $S(\Gamma) = \{p$ prime in $\mathbb{Q} \mid p \nmid 2\Delta\infty$ where there exists $P \in \Gamma$ with P is not a local square at $p\}$.

Then Proposition 7.6 says that $S(\Gamma)$ is an infinite set if $\Gamma \neq \emptyset$.

Main Theorem 2. *Let $E(\mathbb{Q})_2 = O$ and $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}$, where $\Delta = \Delta(E)$ is the discriminant of E. Then* $\operatorname{rank} E(\mathbb{Q}) \leqslant 2n$ *where $n = \nu(2N\infty)$.*

Proof. Suppose

$$\operatorname{rank} E(\mathbb{Q}) > 2 \cdot \nu(2N\infty). \qquad (*)$$

Then as $\Gamma \neq \emptyset$ by Proposition 7.4, so $S(\Gamma)$ is an infinite set by Proposition 7.6. Therefore we can choose $P \in \Gamma$ and $p \in S(\Gamma)$ such that P is not a square at p, in other words, P represents a nontrivial element of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$.

Let $L = \mathbb{Q}(E_2)$ and let L_ℓ be a completion of L at ℓ where $\ell | p$. Then from Theorem 7.5, we have that $P \in E(\mathbb{Q}_p)$ is a square over $\mathbb{Q}_p$ if and only if P is a square over L_ℓ. Thus if P represents a nontrivial element of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$, then it represents a nontrivial element of $E(L_\ell)/2E(L_\ell)$ also.

We now consider the orthogonality relation between $E(L)$ and $E_{(p)}(L)$. (Notice that a prime p is square-free over L, since $p \nmid 2\Delta\infty$.)

If we choose $P \in \Gamma$, then the orthogonality relation becomes

$$\sum_{\ell | p} \langle P_\ell, c_\ell(Q) \rangle_{\ell,2} = 0 \text{ for all } Q \in E_{(p)}(L).$$

In particular,

$$\sum_{\ell | p} \langle P_\ell, c_\ell(e) \rangle_{\ell,2} = 0 \text{ for all } e \in E_{(p)}(L)_2.$$

Let $R \in E(\overline{\mathbb{Q}}_p)$ such that $2\tilde{R} = \tilde{P}$.

If p is inert in L, then the above relation becomes

$$\langle P_\ell, c_\ell(e) \rangle_{\ell,2} = 0 \text{ for all } e \in E_{(p)}(L)_2$$

which implies that $[(\mathrm{Fr}_\ell - 1)(R), e]_2 = 1$ for all $e \in E_{(p)}(L)_2$. Then the nondegeneracy of Weil pairing implies that $(\mathrm{Fr}_\ell - 1)(R) = O$, that is, $R \in E(L_\ell)$. Therefore, P is a square over L_ℓ. This should be true for all $P \in \Gamma$, but we know that there is a point $P \in \Gamma$ which represents a nontrivial element of $E(L_\ell)/2E(L_\ell)$. So we get a contradiction.

Now suppose that p splits into three different primes. Then $L_\ell = \mathbb{Q}_p$, so $\mathrm{Fr}_\ell = \mathrm{Fr}_p$, which is given by $\mathrm{Fr}_p(x, y) = (x^p, y^p)$ for all $\ell | p$.

Thus the orthogonality relation, in terms of Weil pairing, is

$$\prod_{\ell | p} [(\mathrm{Fr}_\ell - 1)(R), e]_2 = [(\mathrm{Fr}_p - 1)(R), e]_2^3 = [(\mathrm{Fr}_p - 1)(R), e]_2 = 1.$$

The above relation should be true for all $e \in E_{(p)}(L)_2$, which again implies that P is a square at p (or equivalently at ℓ) and we get a contradiction.

This contradiction comes from the assumption that $\operatorname{rank} E(\mathbb{Q}) > 2n$, which assures that $\Gamma \neq \emptyset$. Therefore we get the conclusion that $\operatorname{rank} E(\mathbb{Q}) \leqslant 2n$. $\square$

Theorem 7.7. *Let $E(\mathbb{Q})_2 = O$ and $\mathbb{Q}(\sqrt{\Delta})$ is a PID. Then* $\operatorname{rank} E(\mathbb{Q}) \leqslant 2n$ *where Δ and n are as defined in the above theorem.*

Proof. Let $\wp$ be a prime of $\mathbb{Q}(\sqrt{\Delta})$ with $\wp | p$ where $p \in S(\Gamma)$.

As $\mathbb{Q}(\sqrt{\Delta})$ is a PID, we can consider the orthogonality relation between $E(L)$ and $E_{(\wp)}(L)$ where $L = \mathbb{Q}(E_2)$.

The rest of the arguments are exactly the same as those of the Main Theorem 2 with p replaced by $\wp$. Note that $\mathrm{Fr}_\wp$ is now given by $\mathrm{Fr}_\wp(x, y) = (x^{p^f}, y^{p^f})$ where $f = 1$ if p splits and $f = 2$ if p is inert in $\mathbb{Q}(\sqrt{\Delta})$. □

Example (The curve $E : y^2 = x^3 - 3x + 1$ and its quadratic twists)**.**
Let Δ and Δ_D denote the discriminant of E and $E_{(D)}$ respectively. Then $\mathbb{Q}(\Delta) = \mathbb{Q}(\Delta_D) = \mathbb{Q}$. Therefore, we can have that $\operatorname{rank} E_{(D)}(\mathbb{Q}) \leqslant 2n$ where $n = \nu(D) + 3$. Here 3 is the number of prime divisors of $2N\infty$.

Example (The curve $E : y^2 = 4x^3 - 4x + 1$ and its quadratic twists)**.**
In this case, $\mathbb{Q}(\Delta) = \mathbb{Q}(\Delta_D) = \mathbb{Q}(\sqrt{37})$ and $\mathbb{Q}(\sqrt{37})$ has class number 1. Therefore, we can have that $\operatorname{rank} E_{(D)}(\mathbb{Q}) \leqslant 2n$ where $n = \nu(D) + 3$. Here 3 is the number of prime divisors of $2N\infty$.

References

[Ba] M. Bashmakov *The cohomology of Abelian varieties over a number field*, Russian Math. Surveys Vol.**27**, No.**6** (1972), 25–70.

[BK] A. Brumer and K. Kramer *The rank of elliptic curves*, Duke Mathematical journal Vol.**44**, No.**4** (1977), 715–743.

[BSh] Z. Borevich and I. Shafarevich, *Number theory*, Academic Press, 1966

[CF] J. Cassels and A. Fröhlich, editors, *Algebraic Number Theory*, Academic Press, 1967

[Co] J. Coates, *Elliptic curves and Iwasawa theory*, editor Rankin, Ellis Horwood Series in Mathematics and its applications, 1984, 51–73.

[GMa] F. Gouvëa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, Journal of American Mathematical Society **8**, No.**1** (1991), 1–23.

[GM] R. Gupta and R. Murty, *Primitive points on elliptic curves*, Compositio Mathematica Vol.**58**, (1986), 13-44.

[GM2] ———, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. Vol.**101**, (1990), 225–235.

[Hon] T. Honda, *Isogenies, rational points and section points of group varieties*, Jap. Journal of Math. **30**, (1960), 84–101.

[IR] K. Ireland and M. Rosen, *A classical introduction to modern number theory, GTM 84*, Springer-Verlag, New York, 1990

[Ko1] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR. Ser. Mat. **52** (1988), 522–540 [English transl. in Math. USSR Izv. **32** (1989), 523–542].

[Ko2] ———, *Mordell-Weil and Shafarevich-Tate groups*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), 1154–1180 [English transl. in Math. USSR Izv. **33** (1989), 474–499].

[Ko3] ———, *Euler Systems*, Prog. Math. **87**, Birkhäuser, Boston (1990), 435–483.

[Kr] K. Kramer, *Arithmetic of elliptic curves upon quadratic extensions*, Trans. of American Math. Soc. **264**, No.**1**, (1981), 121–135.

[La1] S. Lang, *Elliptic Functions*, Addison Wesley, 1973

[La2] ———, *Cyclotomic Fields I and II*, Springer-Verlag, New York, 1990

[M] R. Murty, *Artin's conjecture and elliptic analogues*, London Mathematical Society Lecture Note Series **237**, (1995), 325-344.

[Ma] Y. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys Vol.**26**, No.**6** (1971), 7–78.

[Me] J. Mestre, *Courbes elliptique et formula explicite*, Prog. Math. **38**, Birkhäuser, Boston (1983), 179–187.

[Ra] C. Rajan, *On the size of the Shafarevich-Tate group of elliptic curves over function fields*, Compositio Mathematica Vol.**105**, (1997), 24-41.

[RS] K. Rubin and A. Silverberg, *Ranks of elliptic curves in families of quadratic twists*, Experimental Mathematics Vol.**9**, No.**4** (2000), 583–590.

[Ru] K. Rubin, *Euler Systems*, Annals of Mathematics Studies **147**, Princeton University Press, 2000.

[ST] J. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. Math. **68**, (1968), 492–517.

[Se] J. Serre, *Local Fields, GTM 67*, Springer-Verlag, New York, 1979

[Shi] G. Shimura, *Introduction to the Arithmetic Theorey of Automorphic Functions*, Princeton University Press, 1971.

[Sil] J. Silverman, *The arithmetic of elliptic curves, GTM 106*, Springer-Verlag, New York, 1986

[Si2] ———, *Advanced Topics in the Arithmetic of Elliptic Curves, GTM 151*, Springer-Verlag, New York, 1994

[Ta] J. Tate, *The Arithmetic of Elliptic Curves*, Inv. Math. **23**, (1974), 179–206.

[Wa] L. Washington, *Number theory and elliptic curves*, editor R.A.Mollin, Number theory and applications, 1989, 245–278.