SELMER GROUPS IN TWIST FAMILIES OF ELLIPTIC CURVES

ILKER INAM

Abstract. The aim of this article is to give some numerical data related to the order of the Selmer groups in twist families of elliptic curves. To do this we assume the Birch and Swinnerton-Dyer conjecture is true and we use a celebrated theorem of Waldspurger to get a fast algorithm to compute $L_E(1)$. Having an extensive amount of data we compare the distribution of the order of the Selmer groups by functions of type $\alpha\frac{(\log\log(X))^{1+\varepsilon}}{\log(X)}$ with ε small. We discuss how the "best choice" of α is depending on the conductor of the chosen elliptic curves and the congruence classes of twist factors.

1. Introduction

The purpose of this article is to give some numerical data related to the order of the Selmer groups in twist families of elliptic curves. This article is of experimental type. It would be most interesting to give theoretical explanations for the statistical observations we make.

Till today there is no algorithm that computes the order of the Selmer group of a random elliptic curve defined over $\mathbb{Q}$ and even assuming the Conjecture of Birch and Swinnerton-Dyer it is a hard computational problem to determine this order.

The situation will become easier if we restrict ourselves to twist families of some specific elliptic curves. Working over $\mathbb{Q}$ we can use the theory of modular forms to get an analytic function for the L-series of the discussed curves.

Assuming the Birch and Swinnerton-Dyer conjecture is true, we are able to exploit a result of Waldspurger, which has a crucial role in this article. It yields an efficient way to compute the order of the Selmer groups in twist families of elliptic curves, if one can find an eigenform of weight 3/2 attached to the elliptic curve via the Shimura-Shintani lift. Examples for this together with an explanation of how to apply Waldspurger's result are discussed in [1] (see Section 4). We use these examples and compute the orders of the Selmer groups of twists of these curves up to $D \leq 10^7$. To do this one begins with a curve E and compares the order of the Selmer groups of two twisted elliptic curves E_{D_0} and E_{D_1} with twist factors D_0 and D_1 in the same quadratic congruence class modulo $4.N_E$ where N_E is the conductor of E. If one chooses the E_{D_0} with D_0 small then its Selmer group can be computed rather easily. So one can compute the order of the Selmer groups for the elliptic curve E_{D_1} by a fast computation described in Subsection 3.3. After these computations and with many data, it is a natural question to study the distribution of members in twist families for which the Selmer groups have the same order, say k times the order of the torsion of E and to find simple functions

2000 *Mathematics Subject Classification.* 14H52, 11G40, 14G10.

Key words and phrases. Elliptic curves, Birch, Swinnerton-Dyer Conjecture, Zeta-functions and related questions.

that approximate this distribution. Through the article, we only interested in k in order to compare the Selmer groups of different elliptic curves. In this article we give numerical evidence that only constants have to be changed for different twist families. We are interested in twisted elliptic curves which have rank zero, but one has to be careful about the cases where twisted elliptic curves have (analytic) positive rank. We define $k = 0$ to mean that the corresponding twisted elliptic curve has positive (analytic) rank. In this case the torsion subgroup doesn't play any role by definition.

1.1. **Overview.**

In Section 2, we present some necessary definitions. The notation used in the article is introduced. Section 3 consists of four subsections. In the first subsection, a statement of Waldspurger's Theorem which plays a pivotal role in the article is given. In Subsection 3.2., we describe how to compute $d(n, n_0)$. Proof is given which can be deduced from some well-known facts. In Subsection 3.3. we describe the algorithm to compute the order of the Selmer groups in twist families of elliptic curves. Furthermore, the approximation function is introduced in this subsection. We take the quotients of the distribution functions and formulate a conjecture. Finally in Section 4, we give examples of our numerical results and in particular tables listing constants α occurring in the approximating functions.

Lastly we plot a graph showing the behavior of the distribution function and the approximating function.

1.2. **Acknowledgements.** This article was partly written during my visit at the Institut für Experimentelle Mathematik in Universität Duisburg-Essen. I wish to express my gratitude for the support and warm hospitality by this institution which made the visit a very pleasant one and especially Prof.Dr.Gerhard Frey who suggested this nice problem and made valuable comments and important improvements on this article. Also I would like to thank Prof.Dr.Gabor Wiese who made comments on an early version. This article has grown out of my PhD thesis. This article is supported by the The Scientific and Technological Research Council of Turkey (TUBITAK) Research Project, Project No: 107T311. I wish to thank the referees for their helpful suggestions.

2. Background Material

Let $E/\mathbb{Q}$ be an elliptic curve and assume that D is a square-free integer. With E_D we denote the *quadratic twist* of E with D. For E given in "short" Weierstrass form

$$y^2 = x^3 - g_2 x - g_3.$$

E_D is given by

$$y^2 = x^3 - g_2 D^2 x - g_3 D^3.$$

E_D is the elliptic curve defined over $\mathbb{Q}$ isomorphic to E over $\mathbb{Q}(\sqrt{D})$ but not over $\mathbb{Q}$.

We recall that E is modular and call the attached eigenform f_E with q-expansion

$$f_E = q + \sum_{n=2}^{\infty} a_n q^n.$$

This is a newform in $S_2(N_E, \chi_1)$ where $S_2(N_E, \chi_1)$ is the space of cusp forms of weight 2, level N_E and χ_1 is the trivial character.

The attached eigenform of E_D is the twist of f_E by the quadratic character χ_D : $f_{E_D} := f_E \otimes \chi_D = \sum\limits_{n=1}^{\infty} \chi_D(n) a_n q^n \in S_2(N_{E_D})$ (and N_{E_D} divides $N_E.D^2$). So the Hasse-Weil $L-$function of E_D is

$$L_{E_D}(s) = \sum_{n=1}^{\infty} \chi_D(n) a_n n^{-s}.$$

In this paper, we shall give numerical data related to the order of the Selmer groups of twist families $\{E_D\}$. In particular we are interested in the number of twists for which there are infinitely many points in $E_D(\mathbb{Q})$. Recall the theorem of Mordell which states that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tor} \times \mathbb{Z}^r,$$

where the torsion subgroup $E(\mathbb{Q})_{tor}$ is finite and the rank r of $E(\mathbb{Q})$ is a non-negative integer.

For any given elliptic curve, it is possible to describe quite precisely the torsion subgroup [11]. The rank is much more difficult to compute, and in general there is no known procedure which is guaranteed to yield an answer. But if the rank of E is positive then a celebrated theorem of Kolyvagin states that $L_E(1) = 0$. So we are sure that if $L_E(1) \neq 0$ then $E(\mathbb{Q})$ is finite. The converse result is not known today but it should be true. One part of the celebrated *Birch and Swinnerton-Dyer Conjecture (BSD)* is that the order of vanishing of $L_E(s)$ at $s = 1$ ("the analytic rank") is equal to the rank of $E(\mathbb{Q})$. BSD states much more. It interprets the value of the first non-vanishing derivative of L_E at $s = 1$ in terms of arithmetical objects attached to E. We shall be interested in this prediction only in the case that the analytic rank of E is 0.

We begin defining the Selmer and the Tate-Shafarevich group of elliptic curves by using the Kummer sequence of elliptic curves: Let E be an elliptic curve over $\mathbb{Q}$. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and $G_{\mathbb{Q}} := Aut_{\mathbb{Q}}(\overline{\mathbb{Q}})$ the absolute Galois group of $\mathbb{Q}$. Consider the abelian group $E(\overline{\mathbb{Q}})$ of all points on E defined over $\overline{\mathbb{Q}}$. One can consider the Galois cohomology groups $H^m(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}}))$ for $m \in \mathbb{N}$.

For all $n \in \mathbb{N}$, we have the exact sequence of $G_{\mathbb{Q}}-$modules

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

As it is well known [9], there is an associated long exact sequence of Galois cohomology groups. We need a consequence of the beginning of this sequence [11]

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n]) \xrightarrow{\alpha} H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}}))[n] \to 0.$$

This sequence is called the *Kummer Sequence* associated to E. For each prime p we choose an extension of the corresponding $p-$adic valuation. Let G_p be the corresponding decomposition group in $G_{\mathbb{Q}}$ which is in a canonical way isomorphic to $G_{\mathbb{Q}_p}$. Let $\gamma_{p,n}$ be the restriction map from $H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n])$ to $H^1(G_p, E(\overline{\mathbb{Q}}_p))[n]$ and P the set of primes. The *Tate-Shafarevich group* of E is denoted by $Sha_{\mathbb{Q}}(E)$ and defined by

$$Sha_{\mathbb{Q}}(E) := \bigcup_{n \in \mathbb{N}} Sha_{\mathbb{Q}}(E)[n],$$

where

$$Sha(E)[n] := \bigcap_{p \in P} \ker(\gamma_{p,n}).$$

The *Selmer group* of E is denoted by $S_{\mathbb{Q}}(E)$ and defined by

$$S_{\mathbb{Q}}(E) := \bigcup_{n \in \mathbb{N}} S_{\mathbb{Q}}(E)[n],$$

where

$$S_{\mathbb{Q}}(E)[n] := \alpha^{-1}(Sha_{\mathbb{Q},S}(E)[n]).$$

So we have the exact sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow S_{\mathbb{Q}}(E)[n] \longrightarrow Sha_{\mathbb{Q}}(E)[n] \longrightarrow 0.$$

We are now ready to state the part of BSD which is of importance for us.

Conjecture 1. [2] *$L_E(1) \neq 0$ iff $E(\mathbb{Q})$ is finite group, and then the Selmer group of E is finite and the following equality holds:*

$$L_E(1) = \left(\int\limits_{E^0(\mathbb{R})} |\omega_E| \right) \left(\prod_{p|N.\infty} c_p \right) \frac{\#S_{\mathbb{Q}}(E)}{\#(E(\mathbb{Q}))^3},$$

where $E^0(\mathbb{R})$ is the connected component of $E(\mathbb{R})$, ω_E is the Néron differential of E, $c_\infty = [E(\mathbb{R}) : E^0(\mathbb{R})]$, and for primes p, $c_p = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$. The numbers c_p are called local Tamagawa numbers.

We remark that all terms different from the order of the Selmer group are computable more or less easily. But in some special cases it is possible to compute the order of the Selmer groups (sometimes one has to assume its finiteness), and then one can verify BSD. So there is numerical evidence for its truth.

Convention: Without further notice we always shall **assume** in this paper that BSD holds and use the analytic theory of modular forms to compute both the order of $S_{\mathbb{Q}}(E)$ and $L_E(1)$ conditionally.

A good test for the exactness of algorithms is a result of Cassels for the order of $S_{\mathbb{Q}}(E)$:

Theorem 1. [3] *Let $E/\mathbb{Q}$ be an elliptic curve. There exists an alternating, bilinear pairing*

$$\Gamma : Sha_{\mathbb{Q}}(E) \times Sha_{\mathbb{Q}}(E) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

whose kernel is precisely the group of divisible elements of Sha.

In particular if $S_{\mathbb{Q}}(E)$ is finite, then $k = \#S_{\mathbb{Q}}(E)/\#(E(\mathbb{Q}))$ is a perfect square.

3. Waldspurger Theorem and Its Consequences

3.1. Statement of Waldspurger's Theorem.

Assume that the rank of E is equal to zero. As said above one can compute the order of the Selmer group and hence of the Tate-Shafarevich group of E by using BSD. Note that the local Tamagawa numbers c_p as well as ω_E can be computed easily (the latter value is transcendental and hence has to be computed up to a desired precision). The most time consuming item is the computation of $L_E(1)$. For this, there is a routine in the computer algebra system MAGMA [7].

It turns out that computing $L_E(1)$ with the necessary precision (again this is a transcendental) for an elliptic curve E with large conductor takes a long time.

For instance, computing $L_E(1)$ for the elliptic curve

$$E : y^2 = x^3 - 87662765543106x + 572205501116432432042932656$$

which has conductor 11520793560025904, one needs at least 1000 hours in a laptop computer[1] with MAGMA which doesn't guarantee to answer. Another hard numerical problem is to decide by computation whether $L_E(1) = 0$.

The situation is much better in families of twists of a given elliptic curve. The elliptic curve E from above is a member of such family, and we shall see in Section 3.3 how this can be used to accelerate the computation dramatically. The reason is *Waldspurger's Theorem* which is crucial for our work:

Theorem 2. [12] *Let E be an elliptic curve over $\mathbb{Q}$ with attached new form f_E. Assume that $F_E \in S_{3/2}(N', \chi_1)$ is an eigenform and $\boldsymbol{S}(F_E) = f_E$ where $\boldsymbol{S}$ is the Shimura-Shintani lifting.*

Let a_n be the $n-$th Fourier coefficient of F_E. Then for square-free natural numbers n and n_0 with $n \equiv n_0$ mod $\prod_{p|N'} {\mathbb{Q}_p^*}^2$ and $n.n_0$ prime to N' we have

$$a_{n_0}^2 \sqrt{n} L_{E_{-n}}(1) = a_n^2 \sqrt{n_0} L_{E_{-n_0}}(1),$$

Hence we get: If $a_{n_0} \neq 0$ then $L_{E_{-n}}(1)$ is determined by a_n, a_{n_0} and $L_{E-n_0}(1)$.

In particular, $L_{E_{-n}}(1) = 0$ for all $n \equiv n_0$ mod $\prod_{p|N'} {\mathbb{Q}_p^*}^2$ iff $L_{E-n_0}(1) = 0$, and else $L_{E_{-n}}(1) \neq 0$ iff $a_n \neq 0$.

Corollary 1. [1] *Assume that the Birch and Swinnerton-Dyer conjecture holds for E_{-n} and E_{-n_0}, n, n_0 as in the theorem and that $a_{n_0} \cdot L_{E-n_0}(1) \neq 0$. Then $E_{-n}(\mathbb{Q})$ is finite iff $a_n \neq 0$ and*

$$\#S_{\mathbb{Q}}(E_{-n}) = d(n, n_0) \cdot \#S_{\mathbb{Q}}(E_{-n_0}) \frac{a_n^2}{a_{n_0}^2},$$

where $d(n, n_0)$ is easily computed as explained in Subsection 3. 2 and essentially a power of 2 depending on the divisor structure of n, n_0.

3.2. **Computing $d(n, n_0)$.** We continue to assume that E_{-n} and E_{-n_0} are twists of E satisfying the conditions of Corollary 4.

We want to compute the numbers $d(n, n_0)$. By definition $d(n, n_0)$ depends on the Tamagawa numbers and the torsion subgroups of the two elliptic curves E_{-n} and E_{-n_0}.

To be explicit one has to use some easy facts about twists of elliptic curves. $d(n, n_0)$ does not depend on the real period since the twisting factors n_0 and n are odd and congruent modulo 4 and $\omega_{E-n}/\omega_{E-n_0} = \sqrt{n_0}/\sqrt{n}$ and hence cancel in the formula in Corollary 4.

Independence of torsion elements:

It is well known and obvious that for all pairs of elliptic curve E and twists E_{-n} we have $E(\mathbb{Q})[2] = E_{-n}(\mathbb{Q})[2]$.

Moreover for given E there are only finitely many (in fact only very few) twists of E which have torsion points of order > 2 over $\mathbb{Q}$. Avoiding these twists is easy and so one can assume without falsifying the statistic, that all members of the twist families have only $\mathbb{Q}-$rational torsion points of order dividing 2. In fact, in the chosen examples below this holds for all non-trivial twists of the treated curves E. So we can assume that the order of $E_{-n_0}(\mathbb{Q})$ is equal to the order of $E_{-n}(\mathbb{Q})$ and hence $d(n, n_0)$ is independent of torsion elements.

[1] With the properties: Intel Core 2 Duo Mobile, 2GB DDR2, 2.00GHz

The next observation is that the groups of connected components of twists of an elliptic curve E over the reals are equal, and so $d(n, n_0)$ is computed by looking at the non-Archimedean Tamagawa numbers.

Let us denote the Tamagawa numbers for E_{-n} at a prime p by $c_{n,p}$ and the Tamagawa numbers for E_{-n_0} at a prime p by $c_{n_0,p}$.

First observe that for p prime to $n_0 \cdot n \cdot N'$ both twists have good reduction modulo p and so the Tamagawa numbers are equal to 1.

By assumption $-n_0$ and $-n$ lie in the same class of squares in all completions with respect to divisors of N'_E and so the Néron models are equal at all primes dividing N'_E.

Now let p be a divisor of, say, n prime to N'_E. Since E has good reduction modulo p and p is odd we can use the table 15.1 in [11], p. 359 to see that E has Kodaira symbol $\mathcal{I}_0$ and so $c_{n,p} = 4$. The same result holds of course for prime divisors of n_0.

Hence we get

Lemma 1. *Let E be an elliptic curve and E_{-n} and E_{-n_0} be twists of E with $\#E_{-n}(\mathbb{Q}) = \#E_{-n_0}(\mathbb{Q}) < \infty$ and $n.n_0$ prime to N'_E and a square in all completions with respect to divisors of N'_E. Then*

$$d(n, n_0) = \frac{\prod c_{n_0,p}}{\prod c_{n,p}} = \frac{4^{\#div(n_0)}}{4^{\#div(n)}},$$

where $\#div(-)$ denotes the number of prime divisors of $-$.

For using Waldspurger Theorem for members of the twist family $\{E_{-n}\}$ one has to find an eigenform F_E as above. Then one has to implement a fast algorithm for computing the Fourier coefficients of F_E in a large range.

3.3. **Computing Fourier Coefficients and the Selmer Group.** Recall the situation. We have an elliptic curve E with eigenform f_E and the Shimura-Shintani lift F_E given in a concrete way. In particular we shall consider the following examples from [5]:

F_E	E
$(\Theta(X^2 + 11Y^2) - \Theta(3X^2 + 2XY + 4Y^2)).\Theta_{id,11}$	$11a1$
$(\Theta(X^2 + 14Y^2) - \Theta(2X^2 + 7Y^2)).\Theta_{id,14}$	$14a1$
$(\Theta(3X^2 - 2XY + 23Y^2) - \Theta(7X^2 + 6XY + 11Y^2)).\Theta_{id,17}$	$17a1$
$(\Theta(X^2 + 20Y^2) - \Theta(4X^2 + 5Y^2)).\Theta_{id,20}$	$20a1$
$(\Theta(X^2 + 17Y^2) - \Theta(2X^2 + 2XY + 9Y^2)).\Theta_{id,17}$	$34a1$

where $\Theta(.)$ is the theta series of a binary quadratic form and $\Theta_{\psi,t} := \sum_{n=-\infty}^{\infty} \psi(n) q^{tn^2}$ is a Fourier series for the Dirichlet character ψ.

The elliptic curve E is given as in Cremona's Table [4].

Let $F_E \in S_{3/2}(N', \chi_1)$ as above with Fourier expansion $\sum_{n=1}^{\infty} a_n q^n$.

Strategy

1) Calculate the $q-$expansion of F_E up to an upper bound M, construct the list $L := \{(n, a_n) | n \in \{1, \cdots, M\} \text{ squarefree}\}$.

2) Choice of Congruence Classes: To apply Waldspurger's theorem we compare twists with twist factors $-n$, $-n_0$ with n and n_0 odd and prime to N' which are

congruent modulo $\prod_{p|N'} \mathbb{Q}_p^{*^2}$. This is satisfied if $n \equiv n_0 \; mod \; 8 \cdot \prod_{2 \neq p|N_E} p$ and hence we shall investigate twist families with twist factors in such congruence classes. First we determine the twist families (with respect to the above congruences) which consist of *odd* elliptic curves and so have positive analytic rank by looking at the parity of the twist characters. We delete these congruence classes.

We simplify the situation in the cases $N_E = 11$ and $N_E = 17$. To apply Waldspurger's theorem we have to look at congruence classes modulo 88 and respectively 136. We check that for all pairs of these congruence classes which become equal modulo 44 respectively 68 there are $n_0 n_0'$ with the same number of prime divisors, the Fourier coefficients $a_{n_0} = a_{n_0'}$ and the same order of the Selmer groups and hence we can investigate in these cases twist families with families with twist factors running over congruences modulo 44 respectively 68.

We list the resulting congruence classes in Table A.

Elliptic Curve	Modulo	n_0
$11a1$	44	$1, 3, 5, 15, 23, 31, 37$
$14a1$	56	$1, 15, 23, 29, 37, 39, 53$
$17a1$	68	$3, 7, 11, 23, 31, 39$
$20a1$	40	$1, 21, 29$
$34a1$	136	$1, 13, 19, 21, 33, 35, 43, 53, 59, 67, 69, 77,$ $83, 89, 93, 101, 115, 117, 123$

Table A.

3) For the integer M and fixed n_0 calculate

$$x_{n_0}(M) := \#\{n : n \leq M, \; n \text{ is square-free}, \; n \equiv n_0 \; (modN')\},$$

$$s_{n_0,0,E}(M) := \#\{n : n \leq M, \, n \text{ is square-free}, \; n \equiv n_0 \; (mod \; N'), \; a_n = 0\},$$

and plot the function $s_{n_0,0,E}(M)/x_{n_0}(M)$.

4) For n_0, find $\alpha \in \mathbb{R}$ and $\epsilon \in [-0.02, 0.02]$ such that

$$\sigma(x_{n_0}(M)) := \alpha \frac{(\log\log(x_{n_0}(M)))^{1+\epsilon}}{\log(x_{n_0}(M))}.$$

approximates $s_{n_0,0,E}(M)/x_{n_0}(M)$ "well".

5) If $a_{n_0} = 0$ then replace n_0 by the minimal n in the congruence class such that $a_{n_0} \neq 0$. Calculate $L_{E_{-n_0}}(1)$, $\#E_{-n_0}(\mathbb{Q})_{tors}$ and $\#S_{\mathbb{Q}}(E_{-n_0})$ by using the BSD-conjecture and f_E.

6) For n_0 and $n \leq M$, compute $d(n, n_0)$ as described in Subsection 3.2.

7) For n_0 and $n \leq M$, compute

$$s_{E_{-n}} := \frac{\#S_{\mathbb{Q}}(E_{-n_0}) \cdot a_n^2 \cdot d(n, n_0)}{a_{n_0}^2}.$$

which is, according to the BSD-conjecture, the order of $S_{\mathbb{Q}}(E_{-n})$.

8) Compute $t := \#E(\mathbb{Q})$. Recall that twisting E doesn't change the order of the torsion subgroup of E.

9) For M, k, t and n_0 compute

$$s_{n_0,k,E}(M) := \#\{n : n \leq M, \, n \text{ is square-free}, \; n \equiv n_0 \; (mod \; N'), \; \frac{s_{E_{-n}}}{t} = k\}.$$

10) For n_0, plot the function $s_{n_0,k,E}(M)/x_{n_0}(M)$.

11) For n_0, find $\alpha \in \mathbb{R}$ and $\epsilon \in [-0.02, 0.02]$ such that

$$\sigma(x_{n_0}(M)) = \alpha \frac{(\log\log(x_{n_0}(M)))^{1+\epsilon}}{\log(x_{n_0}(M))}$$

approximates $s_{n_0,k,E}(M)/x_{n_0}(M)$ "well".

Remark 1. 1) *All data can be found in* http://homepage.uludag.edu.tr/˜inam/

2) *Having computed $\#S_{\mathbb{Q}}(E_{-n})$, $d(n, n_0)$ and $L_{E_{-n_0}}(1)$, one can use the BSD-conjecture again to compute $L_{E_{-n}}(1)$ as*

$$L_{E_{-n}}(1) = \frac{L_{E_{-n_0}}(1) \cdot \#S_{\mathbb{Q}}(E_{-n})}{\#S_{\mathbb{Q}}(E_{-n_0}) \cdot d(n, n_0)}.$$

This is much faster than to compute $L_{E_{-n}}(1)$ directly. We have included these values in our lists.

We come back to the example in Section 3.1. Recall that we wanted to compute the value of $L_E(1)$ of the curve

$$E : y^2 = x^3 - 87662765543106x + 5722055011164324320429322656.$$

It is the twist of the elliptic curve $11a1$ with the twist factor $n = 8090677$, and by the method described above, we get very fast

$$L_E(1) = 2.1007202306109041811092762 6775$$

approximately in 360 seconds.

We now fix an elliptic curve E as well as n_0 and k.

We sketch how to determine an approximation function for $q_{n_0,k,E}$. We choose α and ε in the following way: In this work, using the data obtained up to the bound $M = 10^7$, we construct a family $\{I_i\}$ of subintervals of $I := [0, M]$ defined by $I_i = [0, 50000i]$ for $i = 1, 2, \cdots, 200$ such that

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_{200} = I.$$

First we calculate the value $\frac{s_{n_0,k,E}(M_i)}{x_{n_0}(M_i)}$ and afterwards $\frac{\log(\log(x_{n_0}(M_i))}{x_{n_0}(M_i)}$. Comparing these two values, the constant α_i can be obtained for each I_i. Using the weighted average for the constants α_i we determine α (depending on M). By means of these constants α, we compare the values

$$\frac{s_{n_0,k,E}(M_i)}{x_{n_0}(M_i)} \text{ and } \alpha \frac{\log(\log(x_{n_0}(M_i))}{x_{n_0}(M_i)}.$$

After this step we choose for fine-tuning $\varepsilon \in [-0.02, 0.02]$ such that the approximation is getting better.

4. Numerical Results

We use the considerations of Subsection 3.3 for extensive computations and observe that in all our examples the functions

$$q_{n_0,k,E} := \frac{s_{n_0,k,E}}{x_{n_0}}(M)$$

are fairly well approximated by

$$\alpha \frac{\log(\log(x_{n_0}(M))^{1+\varepsilon}}{\log(x_{n_0}(M))}$$

where $\alpha > 0$ and $\varepsilon \in [-0.02, 0.02]$.

This observation confirms predictions stated by Birch and lead to

Conjecture 2. *For all elliptic curves E, E' over $\mathbb{Q}$, all n_0, n_0' satisfying the conditions of Theorem* 3 *and all k, k' the asymptotic behavior of $\frac{q_{n_0,k,E}}{q_{n_0',k',E'}}$ is well approximated by a constant times a factor* $\log(\log(x(M))^\delta$ *where $x(M)$ is the number of square-free numbers $\leq M$ and δ is a real number with small absolute value.*

Of course one should be much more precise and predict how the factor depends on the parameters. In our context we shall restrict ourselves to a discussion of the reals α we get out of our data by the approximation process in the algorithm described above.

4.1. **Observations.** Conjecture 7 predicts that the type of the approximation function is independent of k. But the constants α vary and so a finer analysis seems necessary in order to find reasons or patterns for the size of α.

But let us begin with a word of caution. In our examples we computed α for $k \leq 961$. For large k we do not have enough material for any statistical statement. (The record, $k = 68121$ occurs just one time).

We now discuss examples of the weighted average values which are given in Section 4.3.

4.1.1. *Some Examples.* Considering the values of α in our examples we see that it depends significantly on the congruence classes modulo 4 respectively 8.

Case 1. For the elliptic curve $11a1$, we have the class $K := \{1, 5, 37\}$ which have members congruent to 1 modulo 4 and the class $L := \{3, 15, 23, 31\}$ with members congruent to 3 modulo 4. As example, we take $k = 1$ and see that the values of α for n_0 in class K are respectively 0.296, 0.299, 0.300, where as for n_0 in class L they are respectively 0.458, 0.459, 0.469, and 0.464 (See Section 4.3).

Case 2. For the elliptic curve $14a1$, we have one class modulo 8 in which all twists are odd curves, namely n congruent to 3 modulo 8. The other classes modulo 8 separate our congruence classes modulo 56 into $K := \{1\}$, $L := \{29, 37, 53\}$, $M := \{15, 23, 39\}$. As example we take $k = 9$ and get the values of α for n_0 in class K are 0.485, for n_0 in class L are respectively 0.195, 0.185 and 0.192 whereas for n_0 in class M they are respectively 0.559, 0.568 and 0.536.

Case 3. For the elliptic curve $17a1$. In this case all congruence classes modulo 68 which are congruent to 1 modulo 4 are odd, and for all classes congruent 3 modulo 4 the values α are around 0.33 and hence of the same size for $k = 0$ as an example.

Case 4. For the elliptic curve $20a1$, all congruence classes modulo 40 which are congruent to 3 modulo 4 are odd, and for all classes congruent 1 modulo 4 the values α are around 0.1 and hence of the same size for $k = 225$ as an example.

Case 5. For the elliptic curve $34a1$, we looked at congruence classes modulo 8. If n is congruent 7 modulo 8 we get odd curves. The other classes modulo 8 consist of $K := \{1, 33, 89\}$, $L := \{19, 35, 43, 59, 67, 83, 115, 123\}$, $M := \{21, 53, 69, 77, 93, 101, 117\}$. Again take $k = 1$, then the values of α are around 0.38 and for every $n_0 \in L$, the values of α are around 0.47 and for every $n_0 \in M$, the values of α are around 0.41.

4.2. **Some Actual Values.** We give some examples of actual values. Here, all the notation given before is valid and $\sigma(x_{n_0}(M))$ is defined by $\sigma(x_{n_0}(M)) := \alpha\frac{(\log\log(x_{n_0}(M)))^{1+\epsilon}}{\log(x_{n_0}(M))}$. The values of α are given in Subsection 4.3.

For the elliptic curve $11a1$, $n_0 = 3, k = 4$ and $\varepsilon = 0.005$ we have

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
50000	0.106452	0.099558
1500000	0.074267	0.066593
3000000	0.066195	0.062381
4000000	0.062997	0.060786
5000000	0.060743	0.059604
10000000	0.053981	0.056209

For the elliptic curve $14a1$, $n_0 = 1, k = 16$ and $\varepsilon = 0.005$ we have

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
100000	0.082313	0.09115
1400000	0.066638	0.066978
2000000	0.06462	0.064665
5000000	0.060241	0.059394
8000000	0.056955	0.057011
10000000	0.055412	0.055946

For the elliptic curve $17a1$, $n_0 = 7, k = 324$ and $\varepsilon = 0.005$ we have

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
100000	0	0.016898
5000000	0.009965	0.010903
6000000	0.010771	0.010726
7000000	0.011213	0.01058
8000000	0.011651	0.010458
10000000	0.012272	0.010259

For the elliptic curve $20a1$, $n_0 = 1, k = 100$ and $\varepsilon = 0.005$ we have

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
500000	0.026748	0.038045
3000000	0.029427	0.031896
5000000	0.029764	0.030491
6000000	0.029958	0.030019
7000000	0.030039	0.029632
10000000	0.030132	0.028772

For the elliptic curve $34a1$, $n_0 = 1, k = 36$ and $\varepsilon = 0.005$ we have

M	$s_{n_0,k}(x_{n_0}(M))/x_{n_0}(M)$	$\sigma(x_{n_0}(M))$
3000000	0.066667	0.071691
5000000	0.069827	0.069099
6000000	0.068564	0.067903
7000000	0.0682	0.066922
8000000	0.067812	0.066096
10000000	0.067339	0.064759

4.3. **Weighted average values of α's.**

E	n_0	0	1	4	9	16
$11a1$	1	0.140221	0.295669	0.204751	0.309679	0.184184
$11a1$	3	0.214424	0.458141	0.296646	0.445157	0.244439
$11a1$	5	0.139959	0.299438	0.199569	0.308824	0.186938
$11a1$	15	0.211029	0.458734	0.299005	0.442075	0.244968
$11a1$	23	0.208441	0.468673	0.304083	0.440648	0.23676
$11a1$	31	0.208064	0.46357	0.205327	0.441027	0.23975
$11a1$	37	0.14234	0.300449	0.205431	0.314227	0.18237

E	n_0	25	36	49	64	81
$11a1$	1	0.312985	0.179629	0.239533	0.144443	0.235818
$11a1$	3	0.423453	0.208141	0.27803	0.141689	0.258489
$11a1$	5	0.320314	0.180445	0.238248	0.140963	0.234221
$11a1$	15	0.415875	0.207029	0.278424	0.146673	0.249818
$11a1$	23	0.411152	0.20807	0.283056	0.149102	0.250205
$11a1$	31	0.412866	0.205186	0.277763	0.150807	0.254808
$11a1$	37	0.314151	0.171081	0.235285	0.143295	0.230991

E	n_0	100	121	144	169	196
$11a1$	1	0.149895	0.188637	0.115865	0.171031	0.091912
$11a1$	3	0.144478	0.144478	0.099708	0.158332	0.068375
$11a1$	5	0.151277	0.183852	0.117823	0.165406	0.089266
$11a1$	15	0.1391	0.1391	0.096762	0.156685	0.069026
$11a1$	23	0.140066	0.190515	0.09152	0.159746	0.070316
$11a1$	31	0.141375	0.185663	0.098614	0.162711	0.071718
$11a1$	37	0.152059	0.184835	0.112431	0.172438	0.08812

E	n_0	225	256	289	324	361
$11a1$	1	0.203897	0.076341	0.135676	0.07271	0.117004
$11a1$	3	0.178166	0.054526	0.113502	0.047742	0.097803
$11a1$	5	0.201578	0.076127	0.132841	0.070794	0.116838
$11a1$	15	0.185691	0.055885	0.117211	0.0487	0.094476
$11a1$	23	0.179255	0.058757	0.112958	0.048998	0.0973
$11a1$	31	0.18378	0.054368	0.116274	0.049585	0.0968
$11a1$	37	0.208334	0.079288	0.132626	0.06951	0.117505

E	n_0	0	1	4	9	16
$14a1$	1	0.283019	0.386791	0.349053	0.485425	0.289702
$14a1$	15	0.319039	0.483879	0.409463	0.559197	0.319645
$14a1$	23	0.336754	0.461198	0.402525	0.567646	0.312323
$14a1$	29	0.442312	0.172938	0.560877	0.194746	0.485192
$14a1$	37	0.42059	0.175757	0.589686	0.185407	0.492192
$14a1$	39	0.312339	0.493768	0.407928	0.536247	0.328624
$14a1$	53	0.447676	0.171374	0.571985	0.191641	0.472537

E	n_0	25	36	49	64	81
$14a1$	1	0.28595	0.326485	0.190388	0.148085	0.292196
$14a1$	15	0.314341	0.322687	0.235968	0.181454	0.290788
$14a1$	23	0.314975	0.331965	0.236908	0.173742	0.299374
$14a1$	29	0.099951	0.567019	0.071551	0.310347	0.086056
$14a1$	37	0.108121	0.544933	0.076132	0.32644	0.081628
$14a1$	39	0.327089	0.316292	0.251003	0.186261	0.27054
$14a1$	53	0.104698	0.561543	0.073051	0.321251	0.086696

E	n_0	100	121	144	169	196
$14a1$	1	0.142119	0.149737	0.159668	0.119627	0.087451
$14a1$	15	0.139186	0.150902	0.143504	0.116318	0.076208
$14a1$	23	0.134807	0.144059	0.150461	0.112789	0.072932
$14a1$	29	0.265114	0.039297	0.303978	0.03107	0.174705
$14a1$	37	0.276584	0.042321	0.285788	0.029985	0.18166
$14a1$	39	0.140236	0.14836	0.135962	0.11914	0.079435
$14a1$	53	0.264155	0.036761	0.306407	0.029676	0.174854

E	n_0	225	256	289	324	361
$14a1$	1	0.147626	0.073324	0.081276	0.090333	0.069123
$14a1$	15	0.13048	0.060237	0.071448	0.066382	0.058287
$14a1$	23	0.138795	0.059647	0.070181	0.074594	0.054617
$14a1$	29	0.033083	0.144352	0.017318	0.190917	0.011085
$14a1$	37	0.031929	0.141464	0.01651	0.180291	0.011341
$14a1$	39	0.129477	0.062409	0.074189	0.06682	0.059717
$14a1$	53	0.03286	0.137962	0.01691	0.194275	0.012076

E	n_0	0	1	4	9	16
$17a1$	3	0.337432	0.477285	0.501361	0.41195	0.402614
$17a1$	7	0.333173	0.480345	0.512958	0.411449	0.397752
$17a1$	11	0.331548	0.470597	0.506991	0.41595	0.398308
$17a1$	23	0.324727	0.469987	0.510093	0.413703	0.409981
$17a1$	31	0.332091	0.482396	0.496191	0.410295	0.405293
$17a1$	39	0.335686	0.481485	0.50061	0.403566	0.403538

E	n_0	25	36	49	64	81
$17a1$	3	0.291697	0.298922	0.227993	0.217491	0.190683
$17a1$	7	0.294852	0.305199	0.224537	0.209766	0.191861
$17a1$	11	0.29197	0.307093	0.224453	0.212266	0.194131
$17a1$	23	0.302838	0.296815	0.223042	0.212759	0.197424
$17a1$	31	0.299154	0.303459	0.219757	0.213895	0.19307
$17a1$	39	0.29654	0.302868	0.21993	0.218869	0.19364

E	n_0	100	121	144	169	196
$17a1$	3	0.155873	0.138493	0.129301	0.109835	0.086544
$17a1$	7	0.153253	0.134025	0.127087	0.109443	0.08902
$17a1$	11	0.152146	0.142299	0.1244	0.115795	0.090622
$17a1$	23	0.149471	0.136131	0.125797	0.115204	0.088695
$17a1$	31	0.153817	0.141537	0.128656	0.10723	0.086032
$17a1$	39	0.155061	0.139321	0.12622	0.110953	0.084326

E	n_0	225	256	289	324	361
$17a1$	3	0.10133	0.066479	0.070144	0.054392	0.063161
$17a1$	7	0.102284	0.066453	0.07182	0.052183	0.061862
$17a1$	11	0.101815	0.06621	0.073766	0.053459	0.060803
$17a1$	23	0.104502	0.066214	0.069106	0.055098	0.060021
$17a1$	31	0.106572	0.068254	0.071002	0.057448	0.058929
$17a1$	39	0.108346	0.065278	0.073044	0.055616	0.058537

E	n_0	0	1	4	9	16
$20a1$	1	0.268253	0.3465	0.315475	0.427111	0.27129
$20a1$	21	0.266462	0.337876	0.32056	0.431508	0.272359
$20a1$	29	0.267792	0.343135	0.317666	0.425236	0.271235

E	n_0	25	36	49	64	81
$20a1$	1	0.254326	0.307296	0.210761	0.179752	0.245513
$20a1$	21	0.253463	0.304903	0.209301	0.178783	0.246748
$20a1$	29	0.258567	0.308143	0.20873	0.178674	0.252364

E	n_0	100	121	144	169	196
$20a1$	1	0.144222	0.141449	0.171656	0.115768	0.095252
$20a1$	21	0.146098	0.144796	0.165373	0.115249	0.09443
$20a1$	29	0.142937	0.14178	0.1634	0.115021	0.09569

E	n_0	225	256	289	324	361
$20a1$	1	0.141739	0.076533	0.082182	0.091834	0.066588
$20a1$	21	0.147373	0.078015	0.082924	0.091549	0.067251
$20a1$	29	0.14228	0.081021	0.081558	0.091311	0.067867

E	n_0	0	1	4	9	16
$34a1$	1	0.300968	0.385865	0.387258	0.462396	0.28402
$34a1$	13	0.290206	0.415303	0.352209	0.474225	0.272241
$34a1$	19	0.353435	0.475157	0.436218	0.505167	0.317592
$34a1$	21	0.29167	0.415613	0.359182	0.472539	0.274045
$34a1$	33	0.30458	0.388798	0.381037	0.440285	0.291886
$34a1$	35	0.357437	0.47347	0.42035	0.504132	0.326558
$34a1$	43	0.355486	0.466179	0.44077	0.503479	0.323861
$34a1$	53	0.281215	0.413834	0.357105	0.470171	0.283536
$34a1$	59	0.345971	0.471297	0.436144	0.50406	0.327326
$34a1$	67	0.351665	0.467335	0.427308	0.512714	0.326024
$34a1$	69	0.290429	0.408492	0.366839	0.478386	0.275193
$34a1$	77	0.293768	0.41554	0.350608	0.478178	0.272873
$34a1$	83	0.352644	0.475251	0.440215	0.500611	0.328119
$34a1$	89	0.305732	0.396955	0.372179	0.443078	0.296228
$34a1$	93	0.283804	0.42395	0.358696	0.479956	0.279951
$34a1$	101	0.29705	0.412981	0.359811	0.476887	0.286045
$34a1$	115	0.34747	0.476572	0.438912	0.505538	0.321909
$34a1$	117	0.291683	0.420945	0.355004	0.476725	0.278145
$34a1$	123	0.354215	0.475638	0.437478	0.495364	0.32921

E	n_0	25	36	49	64	81
$34a1$	1	0.247423	0.309932	0.194351	0.177262	0.225383
$34a1$	13	0.271392	0.294956	0.199301	0.166857	0.230411
$34a1$	19	0.271006	0.324198	0.191454	0.171407	0.214279
$34a1$	21	0.265973	0.301452	0.19956	0.159942	0.230879
$34a1$	33	0.267835	0.311831	0.193117	0.172183	0.229097
$34a1$	35	0.275831	0.327544	0.189914	0.17779	0.220039
$34a1$	43	0.272699	0.317971	0.202658	0.174474	0.211269
$34a1$	53	0.277814	0.310885	0.201981	0.161572	0.229304
$34a1$	59	0.267928	0.327115	0.193429	0.175461	0.215779
$34a1$	67	0.273065	0.324959	0.192272	0.172805	0.212269
$34a1$	69	0.267456	0.29777	0.207129	0.162831	0.232521
$34a1$	77	0.272458	0.297814	0.201069	0.167444	0.227964
$34a1$	83	0.275118	0.314132	0.199511	0.174251	0.210163
$34a1$	89	0.255453	0.318219	0.207944	0.165966	0.226874
$34a1$	93	0.259963	0.297419	0.204218	0.165222	0.234308
$34a1$	101	0.254251	0.303388	0.197465	0.15854	0.23436
$34a1$	115	0.270414	0.323107	0.196365	0.177784	0.19878
$34a1$	117	0.260653	0.2887	0.202377	0.157916	0.244395
$34a1$	123	0.270226	0.335145	0.200594	0.170866	0.208101

E	n_0	100	121	144	169	196
$34a1$	1	0.128304	0.122231	0.147564	0.102664	0.082786
$34a1$	13	0.129592	0.130917	0.143784	0.100675	0.07895
$34a1$	19	0.130772	0.109944	0.140669	0.086182	0.077919
$34a1$	21	0.132753	0.126583	0.143338	0.106306	0.080138
$34a1$	33	0.131932	0.123085	0.140728	0.099784	0.082223
$34a1$	35	0.130884	0.111755	0.141213	0.08385	0.079269
$34a1$	43	0.128261	0.109375	0.13594	0.083931	0.071109
$34a1$	53	0.12997	0.126922	0.142644	0.100092	0.07645
$34a1$	59	0.137624	0.106901	0.140647	0.08392	0.074337
$34a1$	67	0.138161	0.108241	0.136687	0.090009	0.081168
$34a1$	69	0.127983	0.12296	0.146421	0.100218	0.072738
$34a1$	77	0.130561	0.122929	0.148044	0.098305	0.080768
$34a1$	83	0.130011	0.103015	0.141567	0.085853	0.077536
$34a1$	89	0.132737	0.115162	0.150665	0.0967	0.08984
$34a1$	93	0.127371	0.120887	0.147903	0.100794	0.071056
$34a1$	101	0.124347	0.118514	0.136806	0.10392	0.079833
$34a1$	115	0.13509	0.116645	0.140947	0.089575	0.075199
$34a1$	117	0.130015	0.124739	0.140575	0.104611	0.078912
$34a1$	123	0.135871	0.107328	0.133703	0.093233	0.07586

E	n_0	225	256	289	324	361
$34a1$	1	0.120486	0.06472	0.062951	0.070443	0.055249
$34a1$	13	0.120107	0.0621	0.0692	0.077468	0.055683
$34a1$	19	0.077919	0.059063	0.053673	0.070172	0.038649
$34a1$	21	0.118898	0.062197	0.06578	0.071127	0.056771
$34a1$	33	0.118185	0.059254	0.065998	0.072214	0.053245
$34a1$	35	0.092942	0.058685	0.050621	0.063069	0.039964
$34a1$	43	0.097305	0.057743	0.053748	0.069417	0.0381
$34a1$	53	0.120493	0.060345	0.065208	0.071921	0.049442
$34a1$	59	0.097042	0.061403	0.047947	0.065448	0.040482
$34a1$	67	0.09381	0.057656	0.066198	0.064485	0.038135
$34a1$	69	0.121028	0.065232	0.066193	0.066645	0.052697
$34a1$	77	0.120666	0.065448	0.067139	0.072256	0.052677
$34a1$	83	0.098931	0.058119	0.049453	0.067301	0.040662
$34a1$	89	0.117926	0.059319	0.062727	0.072717	0.055294
$34a1$	93	0.115051	0.060207	0.061973	0.076746	0.058861
$34a1$	101	0.123836	0.063449	0.070854	0.072985	0.058416
$34a1$	115	0.099212	0.057176	0.049053	0.065697	0.037937
$34a1$	117	0.120381	0.061819	0.067332	0.07149	0.054083
$34a1$	123	0.097763	0.057011	0.049838	0.06636	0.038657

4.4. **A Graphical Example.** We plot some graph of the data for $E = 11a1$, $n_0 = 1$, $k = 1$. In this graph on the $x-$axis we plot $x_{n_0}(M)$ up to $M = 10^7$. Dots above at the beginning belong to the graph of the function $s_{1,1}(x_1(M))/x_1(M)$, dots below at the beginning belong to the graph of the function $0.295669\frac{(\log\log(x_1(M)))^{1.005}}{\log(x_1(M))}$.

References

[1] J. A. Antoniadis, M. Bungert and G. Frey, Properties of Twist of Elliptic Curves, *J. Reine Angew. Math.*, **405** (1990), 1-28,

[2] B. Birch and H. P. F. Swinnerton-Dyer, Notes on Elliptic Curves II, *J. Reine Angew. Math.*, **218** (1965), 79-108,

[3] J. W. S. Cassels, Arithmetic on Curves Genus 1, VIII On Conjectures of Birch and Swinnerton-Dyer, *J. Reine Angew. Math.*, **217** (1965), 180-199,

[4] J. E. Cremona, Algorithms for Modular Elliptic Curves, 2nd Edition, Cambridge Univ. Press, Cambridge, 1997,

[5] G. Frey, Construction and Arithmetical Applications of Modular Forms of Low Weight, *CRM Proceedings & Lecture Notes Amer. Math. Soc*, **4**, (1994), 1-21,

[6] V. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $Sha_E(\mathbb{Q})$ for a class of Weil curves, *Math. USSR, Izv.,* **32** (1989), 523-541,

[7] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.,* **24** (1997), (3-4):235-265,

[8] A. P. Ogg, Rational Points of Finite Order on Elliptic Curves, *Invent. Math.*, **9** (1971), 105-111,

[9] J. P. Serre, Local Fields, Volume 67 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1979,

[10] G. Shimura, On Modular Forms of half-integral weight, *Annals of Math.*, **97** (1973), 440-481,

[11] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986, ISBN 0-387-96203-4,

[12] J. L. Waldspurger, Sur les Coefficients de Fourier des Formes Modulaires de Poids Demi-Entier, *J. Math. Pures et Appl.,* **60** (1981), 375-484.

Received: 27 September, 2010 and in revised form 24 January 2011.

Uludag University, Faculty of Art and Science, Department of Mathematics, Gorukle, Bursa-Turkey

E-mail address: inam@uludag.edu.tr, ilker.inam@gmail.com