Elliptic curves with large analytic order of $Ш(E)$

Andrzej Dąbrowski[1] and Mariusz Wodzicki[2]

[1] Instytut Matematyki, Uniwersytet Szczeciński, ul. Wielkopolska 15, 70-451 Szczecin, Poland
[2] Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA

To Yuri Ivanovich Manin on His Seventieth Birthday

Introduction

The L-series $L(E,s)=\sum_{n=1}^{\infty} a_n n^{-s}$ of an elliptic curve E over $\mathbb{Q}$ converges for $\operatorname{Re} s > 3/2$. The Modularity Conjecture, settled by Wiles-Taylor-Diamond-Breuil-Conrad [BCDT], implies that $L(E,s)$ analytically continues to an entire function and its leading term at $s=1$ is described by the following long standing conjecture.

Conjecture 1 (Birch and Swinnerton-Dyer). *L-function $L(E,s)$ has a zero of order $r = \mathit{rank}\, E(\mathbb{Q})$ at $s=1$, and*

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{c_\infty(E) c_{fin}(E) R(E) |Ш(E)|}{|E(\mathbb{Q})_{tors}|^2}.$$

Here $E(\mathbb{Q})_{\mathrm{tors}}$ denotes the torsion subgroup of the group $E(\mathbb{Q})$ of rational points of E, the fudge factor c_{fin} is the Tamagawa number of E, and $R(E)$ is the regulator calculated with respect to the Néron-Tate height pairing. If ω is the *real* period of E, then $c_\infty = \omega$ or 2ω, according to whether the group of real points $E(\mathbb{R})$ is connected or not.

Finally, $Ш(E)$ denotes the Tate-Shafarevich group of E. The latter is formed by isomorphism classes of pairs (T,ϕ), where T is a smooth projective curve over $\mathbb{Q}$ of genus one which possesses a $\mathbb{Q}_p$-rational point for every prime p (including $p=\infty$), and $\phi : E \to Jac(T)$ is an isomorphism defined over $\mathbb{Q}$. The Tate-Shafarevich group is very difficult to determine. It is known that the subgroup

$$Ш(E)[n] := \{a \in Ш(E) \mid na = 0\}$$

is finite for any $n > 1$ and it is conjectured that $Ш(E)$ is always finite. In theory, the standard 2-descent method calculates the dimension of the $\mathbb{F}_2$-vector space $Ш(E)[2]$ (see [Cr$_1$], [S]). It is not clear in general how to exhibit the curves of genus 1 which represent elements of $Ш(E)$ of order > 2 (see, however, [CFNS^2]).

It has been known for a long time that the order of $Ш(E)$, provided the latter is always finite, can take arbitrarily large values. Cassels [C] was the first one to show this by proving that $|Ш(E)[3]|$ can be arbitrarily large for a special family of elliptic curves with j-invariant zero. Only in 1987 it was finally established that there are any elliptic curves over $\mathbb{Q}$ for which the Tate-Shafarevich group is finite (Rubin [Ru], Kolyvagin [K], Kato). Ten years later Rohrlich [Ro] by combining results of [HL] and [K], proved that given a modular elliptic curve E over $\mathbb{Q}$ (hence any curve—according to [BCDT]), and a positive integer n, there exists a quadratic twist E_d of E such that $Ш(E_d)$ *is* finite and $|Ш(E_d)[2]| \geqslant n$. This finally proved that $Ш(E)$ can indeed be a group of arbitrarily large finite order.

Assuming the Birch and Swinnerton-Dyer Conjecture, Mai and Murty [M$_2$] showed that for the family of quadratic twists of any elliptic curve E, one has

$$\varliminf_{d} \frac{N(E_d)^{\frac{1}{4}-\epsilon}}{|Ш(E_d)|} = 0.$$

Goldfeld and Szpiro [GS], and Mai and Murty [MM$_2$] (as reported by Rajan [R]), in the early 1990s proposed the following general conjecture:

Conjecture 2 (Goldfeld-Szpiro-Mai-Murty). *For any $\epsilon > 0$ we have*[3]

$$|Ш(E)| \ll N(E)^{1/2+\epsilon}.$$

Estimate (1) holds for the family of rank zero quadratic twists of any particular elliptic curve provided the Birch and Swinnerton-Dyer Conjecture holds for every member of that family.

The Birch and Swinnerton-Dyer Conjecture combined with the following consequence of the Generalised Lindelöf Hypothesis (see [GHP], p. 154)

$$\lim_{d\to\infty} \frac{L^{(r_d)}(E_d,1)}{N(E_d)^{\epsilon}} = 0 \qquad (d \text{ square-zero}),$$

where r_d denotes the rank of the group $E_d(\mathbb{Q})$, and the following conjecture of Lang (see [L])

[3] In this article we adhere to the following notational convention. Let $A(E)$ and $B(E)$ be some quantities $A(E)$ and $B(E)$ dependent on a curve E belonging to a specified class $\mathcal{C}$ of elliptic curves defined over $\mathbb{Q}$. We say that $A(E) \ll B(E)$ if, for any $K > 0$, there exists N_0 such that $A(E) < KB(E)$ for all curves in $\mathcal{C}$ with conductor $N(E) > N_0$. This is meaningful only if $\mathcal{C}$ contains infinitely many nonisomorphic curves. If either $A(E)$ or $B(E)$ depend on some parameter ϵ, then the choice of N_0 is allowed to depend on ϵ.

$$R(E) \gg N(E)^{-\epsilon},$$

easily imply that

$$|Ш(E_d)| \ll N(E_d)^{1/4+\epsilon}.$$

The following unconditional bounds

$$|Ш(E)| \ll \begin{cases} N(E)^{79/120+\epsilon} & \text{if } \ j(E)=0 \\ N(E)^{37/60+\epsilon} & \text{if } \ j(E)=1728 \\ N(E)^{59/120+\epsilon} & \text{otherwise,} \end{cases}$$

where $j(E)$ denotes the j-invariant of E, are known for curves of rank zero with complex multiplication [GL].

In general, for elliptic curves satisfying the Birch and Swinnerton-Dyer Conjecture, Goldfeld and Szpiro [GS] show that the Goldfeld-Szpiro-Mai-Murty Conjecture is equivalent to the Szpiro Conjecture:

$$|\Delta(E)| \ll N(E)^{6+\epsilon},$$

where $\Delta(E)$ denotes the discriminant of the minimal model of E. Masser proves in [Ma] that 6 in the exponent of (2) cannot be improved; in [We] de Weger conjectures that the exponent in (1) is also, in a certain sense, the best possible.

Conjecture 3 (de Weger). *For any $\epsilon > 0$ and any $C > 0$, there exists an elliptic curve over $\mathbb{Q}$ with*

$$|Ш(E)| > CN(E)^{1/2-\epsilon}.$$

He shows [We] that Conjecture 3 is a consequence of the following three conjectures: the Birch and Swinnerton-Dyer Conjecture for curves of rank zero, the Szpiro Conjecture, and the Riemann Hypothesis for Rankin-Selberg zeta functions associated to certain modular forms of weight $\frac{3}{2}$.

On the other hand, de Weger demonstrates that the following variant of Conjecture 3 which involves the minimal discriminant instead of the conductor, is a consequence of just the Birch and Swinnerton-Dyer Conjecture for elliptic curves with $L(E,1) \neq 0$.

Conjecture 4 (de Weger). *For any $\epsilon > 0$ and any $C > 0$, there exists an elliptic curve over $\mathbb{Q}$ with*

$$|Ш(E)| > C|\Delta(E)|^{1/12-\epsilon}.$$

For the purpose of the present article the quantity

$$GS(E) := \frac{|Ш(E)|}{\sqrt{N(E)}}$$

will be referred to as the *Goldfeld-Szpiro ratio* of E. Eleven examples of elliptic curves with $GS(E) \geqslant 1$ are given in [We], the largest value being 6.893... . Further forty seven examples with $GS(E) \geqslant 1$ are produced by Nitaj [Ni], his largest value of $GS(E)$ being 42.265. Note that curves of small conductor with $GS(E) > 1$ were already known from Cremona's tables [Cr_2]. In all these examples $GS(E)$ is calculated by using the formula for $|Ш(E)|$ which is predicted by the Birch and Swinnerton-Dyer conjecture, see (4) below.

Let us say a few words about the order of the Tate-Shafarevich group for those curves when it is known. The results by Stein and his collaborators [GJPST, Thm. 4.4] imply that $|Ш(E)| = 7^2$ for the curves denoted `546f2` and `858k2`, respectively, in Cremona's tables [Cr_2]. No other curve of rank zero and conductor less than 1000 has larger $|Ш(E)|$ if the Birch and Swinnerton-Dyer conjecture holds for such curves. Gonzalez-Avilés demonstrated [GA, Thm. B], that formula (4) for the order of the Tate-Shafarevich group holds for all the quadratic twists

$$E_d : \quad y^2 = x^3 + 21dx^2 + 112d^2x$$

with $L(E_d, 1) \neq 0$. The largest value of $|Ш(E_d)|$ for such curves, when $d \leqslant 2000$, is $|Ш(E_{1783})| = 8^2$ (cf. [Le, Table I]).

Assuming the validity of the Birch and Swinnerton-Dyer conjecture, one can compute $|Ш(E)|$ for an elliptic curve of rank zero E by evaluating $L(E, 1)$ with sufficient accuracy. (In practice, this is possible only for curves with not too big conductors.) We shall be referring to this number as the *analytic order* of the Tate-Shafarevich group of E. In what follows $|Ш(E)|$ will denote exclusively the analytic order of $Ш(E)$.

It is rather surprising how small is the analytic order in all known examples: de Weger [We] produced one with $|Ш(E)| = 224^2$, Rose [Rs] produced another one with $|Ш(E)| = 635^2$; finally, Nitaj [Ni] found a curve with

$$|Ш(E)| = 1832^2$$

and that seems to be the largest known value prior to year 2002.

For the family of cubic twists considered by Zagier and Kramarz [ZK]

$$E'_d : \quad x^3 + y^3 = d \qquad (d \text{ cubic-free}),$$

the value of $|Ш(E'_d)|$ does not exceed 21^2 for $d \leqslant 70000$. In this case, the Birch and Swinnerton-Dyer, the Lang, and the Generalised Lindelöf conjectures imply that

$$|Ш(E'_d)| \ll N(E'_d)^{1/3+\epsilon}.$$

For quadratic twists of a given curve one can calculate the analytic order of the Tate-Shafarevich group by using a well known theorem of Waldspurger [W] in conjunction with purely combinatorial methods. The details for some curves with complex multiplication can be found in [Fr_1],[Fr_2],[Le],[N],[T]. Here we shall consider only one example, the family

$$E_d: \quad y^2 = x^3 - d^2x \qquad (d \geqslant 1 \text{ an odd square-free integer})$$

of so called congruent-number elliptic curves. Define the sequence $a(d)$ by

$$\sum_{n=1}^{\infty} a(n)q^n := \eta(8z)\eta(16z)\Theta(2z)$$

where

$$\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n), \qquad \Theta(z) = \sum_{n=-\infty}^{\infty} q^{n^2} \qquad (q = e^{2\pi i z}),$$

When curve E_d is of rank zero then, assuming as usual the Birch and Swinnerton-Dyer conjecture, we have (see [T]):

$$|\text{Ш}(E_d)| = \left(\frac{a(d)}{\tau(d)}\right)^2$$

where $\tau(d)$ denotes the number of divisors of d. (Coefficients $a(d)$ can also be calculated using a formula of Ono [O].) Conjecturally, one expects that

$$|\text{Ш}(E_d)| \ll N(E_d)^{1/4+\epsilon},$$

hence the sequence of curves E_d (and, more generally, the family of quadratic twists of *any* curve) is not a likely candidate to produce curves with large Goldfeld-Szpiro ratio.

The primary aim of this article is to present the results of our search for curves with exceptionally large analytic orders of the Tate-Shafarevich group. We exhibit 134 examples of curves of rank zero with $|\text{Ш}(E)| > 1832^2$ which was the largest previously known value for any explicit curve. For our record curve we have

$$|\text{Ш}(E)| = 63,408^2.$$

For the reasons explicated in the last section, we focused on the family

$$E(n,p): \quad y^2 = x(x+p)(x+p-4\cdot 3^{2n+1}),$$

and three families of isogeneous curves, for n and p being integers within the bounds $3 \leqslant n \leqslant 19$ and $0 < |p| < 1000$. Compared to the previously published results, in our work we faced dealing with curves of very big conductor. A big conductor translates into a very slow convergence rate of the approximation to $L(E,1)$. The main difficulty was to design a successful search strategy for curves with an exceptionally large Goldfeld-Szpiro ratio, (3), which is usually accompanied by a large value of the analytic order of the Tate-Shafarevich group.

Our explorations brought out also a number of unplanned discoveries: curves of rank zero with the value of $L(E,1)$ much smaller, or much bigger, than in any previously known example (see Tables 6 and 5 below). A particularly notable case involves a pair of non-isogeneous curves whose values of $L(E, 1)$ coincide in their first 11 digits after the decimal!

Details of the computations, tables and related comments are contained in Sections 1 - 3. Further remarks on Conjecture 3 are the subject of Section 4.

The actual calculations were carried out by the second author in the Summer and early Fall 2002 on a variety of computers, almost all of them located in the Department of Mathematics in Berkeley. Supplemental computations were conducted also in 2003 and the Summer 2004.

The results were reported by M.W. at the conference *Geometric Methods in Algebra and Number Theory* which took place in December 2003 in Miami, and by A.D. at the Number Theory Seminar at the Max-Planck-Institut in October 2006; A.D. would like to thank the Department of Mathematics in Berkeley and the Max-Planck-Institut in Bonn, for their support and hospitality during his visits in 2006 when the revised version of this article was prepared; M.W. would like to thank the Institute of Matematics at the University of Szczecin for its hospitality during his visits there in the Summer 2002, when the project started, and in the Summer 2003. The second author was partially supported by NSF Grants DMS–9707965 and DMS–0503401.

1 Examples of elliptic curves with large $|Ш(E)|$

Consider the family

$$E(n, p): \quad y^2 = x(x+p)(x+p-4\cdot 3^{2n+1}),$$

with $(n, p) \in \mathbb{N} \times \mathbb{Z}$ and $p \neq 0,\ 4\cdot 3^{2n+1}$. Any member of this family is isogeneous over $\mathbb{Q}$ to three other curves $E_i(n, p)$ $(i = 2, 3, 4)$:

$$E_2(n, p): \quad y^2 = x^3 + 4(2\cdot 3^{2n+1} - p)x^2 + 16\cdot 3^{4n+2}x, \tag{1}$$

$$E_3(n, p): \quad y^2 = x^3 + 2(4\cdot 3^{2n+1} + p)x^2 + (4\cdot 3^{2n+1} - p)^2 x, \tag{2}$$

and

$$E_4(n, p): \quad y^2 = x^3 + 2(p - 8\cdot 3^{2n+1})x^2 + p^2 x. \tag{3}$$

The L-series and ranks of isogeneous curves coincide, while the orders of $E(\mathbb{Q})_{\mathrm{tors}}$ and $Ш(E)$, the real period, ω, and the Tamagawa number c_{fin} may differ. The curves being 2-isogeneous, the analytic orders of $Ш(E_i)$ may differ from $|Ш(E(n, p)|$ only by a power of 2.

All the examples we found where *at least one* of the four analytic orders of $Ш(E(n, p)$ and $Ш(E_i(n, p))$ $(i = 2, 3, 4)$ is greater or equal to 1000^2 are listed in Table 1. Notation used: $|Ш| = |Ш(E)|$ and $|Ш_i| = |Ш(E_i)|$.

For a curve E of rank zero, we compute the analytic order of Ш(E), i.e., the quantity

$$|Ш(E)| = \frac{L(E,1)\cdot|E(\mathbb{Q})_{\mathrm{tors}}|^2}{c_\infty(E)c_{\mathrm{fin}}(E)},$$

by using the following approximation to $L(E,1)$, cf. [Co]:

$$S_m = 2\sum_{l=1}^{m}\frac{a_l}{l}e^{-\frac{2\pi l}{\sqrt{N}}},$$

which, for

$$m \geqslant \frac{\sqrt{N}}{2\pi}\left(2\log 2 + k\log 10 - \log(1-e^{-2\pi/\sqrt{N}})\right),$$

differs from $L(E,1)$ by less than 10^{-k}.

It seems that the currently available techniques of n-descent for $n=3$, 4, and 5 (cf. [CFNS^2], [MS^2], [Be], [F]), can be utilized to see that 60^2 divides the actual order of Ш(E) for $E = E_3(15,12)$. On the other hand, the results of Kolyvagin and Kato could be used to prove that the actual order of Ш(E) divides $|$Ш$(E)|$. This would establish validity of the exact form of the Birch and Swinnerton-Dyer Conjecture in this case. The Birch and Swinnerton-Dyer conjecture is invariant under isogeny, hence this would establish validity of this conjecture for each of its three isogeneous relatives. In particular, this would show that Ш$(E_4(15,12))$ is indeed a group of order 3840^2.

Table 1. Examples of elliptic curves $E(n,p)$ ($n \leqslant 19$; $0 < |p| \leqslant 1000$) with $\max(|Ш|, |Ш_2|, |Ш_3|, |Ш_4|) \geqslant 1000^2$.

(n,p)	$N(n,p)$	$\lvert Ш\rvert$	$\lvert Ш_2\rvert$	$\lvert Ш_3\rvert$	$\lvert Ш_4\rvert$
$(11,-489)$	1473152464197864	680^2	680^2	1360^2	680^2
$(11,163)$	1473152461647240	346^2	1384^2	173^2	1384^2
$(11,301)$	5440722586421136	576^2	1152^2	576^2	288^2
$(11,336)$	15816054028824	529^2	1058^2	529^2	1058^2
$(11,865)$	15635299103673360	617^2	1234^2	617^2	617^2
$(12,-605)$	4473683858657640	1031^2	1031^2	1031^2	2062^2
$(12,-257)$	20904304573762872	1545^2	1545^2	3090^2	3090^2
$(12,-56)$	569377945555104	1049^2	1049^2	2098^2	1049^2
$(12,22)$	143157883450560	416^2	1664^2	416^2	1664^2
$(12,24)$	81339706505952	603^2	1206^2	603^2	1206^2
$(12,63)$	63264216170568	554^2	1108^2	554^2	1108^2
$(12,262)$	42622006206125760	468^2	1872^2	234^2	1872^2
$(12,382)$	62143535763983040	648^2	2592^2	324^2	2592^2
$(12,466)$	75808606453660608	1435^2	5740^2	1435^2	5740^2
$(12,694)$	112899512607942336	576^2	2304^2	288^2	2304^2
$(12,934)$	151942571712321216	512^2	2048^2	256^2	2048^2

(n,p)	$N(n,p)$	$\lvert Ш\rvert$	$\lvert Ш_2\rvert$	$\lvert Ш_3\rvert$	$\lvert Ш_4\rvert$
$(13,-672)$	1281100377506040	389^2	1556^2	389^2	778^2
$(13,-160)$	915071698203240	1079^2	1079^2	2158^2	1079^2
$(13,-125)$	3660286792808760	639^2	1278^2	639^2	2556^2
$(13,-69)$	16837319246889384	516^2	516^2	258^2	1032^2
$(13,-42)$	20497606039673280	502^2	2008^2	251^2	2008^2
$(13,-17)$	12444975095505720	348^2	1392^2	348^2	2784^2
$(13,-5)$	3660286792794360	1583^2	1583^2	1583^2	3166^2
$(13,-3)$	1464114717117648	2364^2	2364^2	1182^2	2364^2
$(13,60)$	457535849098320	552^2	1104^2	276^2	552^2
$(13,66)$	32210523776515392	618^2	2472^2	309^2	2472^2
$(13,73)$	610744996281840	494^2	1964^2	247^2	988^2
$(13,96)$	10765549390536	588^2	1176^2	294^2	588^2
$(13,136)$	264786704158368	258^2	1032^2	258^2	1032^2
$(13,544)$	3111243773819208	929^2	1858^2	929^2	929^2
$(13,708)$	21595692076981920	812^2	3248^2	406^2	1624^2
$(13,876)$	835002924582096	340^2	1360^2	85^2	1360^2
$(13,928)$	5307415849389480	470^2	1880^2	470^2	940^2
$(14,-948)$	2033174929441680	312^2	1248^2	156^2	624^2
$(14,-800)$	8235645283809960	390^2	1560^2	195^2	1560^2
$(14,-672)$	11529903397328568	2310^2	4620^2	2310^2	2310^2
$(14,-596)$	61355557364338608	598^2	1196^2	598^2	2392^2
$(14,-281)$	15300603799975032	253^2	1012^2	253^2	2024^2
$(14,-212)$	21824460002049648	560^2	560^2	560^2	1120^2
$(14,-33)$	72473678497325160	1002^2	2004^2	1002^2	4008^2
$(14,-12)$	3294258113514528	1077^2	2154^2	1077^2	2154^2
$(14,-11)$	144947356994638704	1806^2	3612^2	903^2	3612^2
$(14,-3)$	775119556121040	588^2	1176^2	294^2	1176^2
$(14,12)$	205891132094640	564^2	2256^2	282^2	4512^2
$(14,96)$	1647129056756616	306^2	1224^2	153^2	612^2
$(14,100)$	16471290567565920	1186^2	2372^2	593^2	2372^2
$(14,240)$	8235645283778760	1184^2	2368^2	592^2	1184^2
$(14,268)$	726037150017264	858^2	1716^2	429^2	1716^2
$(14,528)$	18118419624294264	356^2	1424^2	356^2	712^2
$(14,652)$	33560254531348080	268^2	2144^2	67^2	2144^2

Table 2. Examples of elliptic curves $E(n,p)$ ($n = 14, 15$; $0 < |p| \leqslant 1000$) with $\max_{1\leqslant i\leqslant 4} |Ш_i| \geqslant 1000^2$.

(n,p)	$N(n,p)$	$\lvert Ш\rvert$	$\lvert Ш_2\rvert$	$\lvert Ш_3\rvert$	$\lvert Ш_4\rvert$
$(15,-852)$	8222777088032880	562^2	1124^2	281^2	1124^2
$(15,-248)$	141399694410862368	1185^2	4740^2	1185^2	4740^2
$(15,-240)$	74120807554080840	965^2	3860^2	965^2	3860^2
$(15,-212)$	280600200026160	498^2	1992^2	249^2	3984^2
$(15,-116)$	107475170953411824	2368^2	4736^2	2368^2	9472^2
$(15,-96)$	14824161510815304	1434^2	2838^2	717^2	2838^2
$(15,-84)$	3242785330490832	775^2	1650^2	775^2	1650^2
$(15,-80)$	74120807554076040	679^2	1358^2	679^2	1358^2
$(15,-48)$	14824161510815016	3057^2	3057^2	3057^2	3057^2
$(15,-12)$	5929664604325920	576^2	1152^2	288^2	1152^2
$(15,-6)$	237186584173036224	3705^2	3705^2	3705^2	7410^2
$(15,-1)$	59296646043258936	162^2	648^2	81^2	1296^2
$(15,1)$	118593292086517776	4032^2	8064^2	2016^2	8064^2
$(15,12)$	336912761609424	240^2	1920^2	60^2	3840^2
$(15,60)$	37060403777035920	2299^2	4598^2	2299^2	2299^2
$(15,88)$	130452621295164960	1232^2	2464^2	1232^2	2464^2
$(15,172)$	2489995878769488	1258^2	2516^2	629^2	1258^2
$(15,375)$	26953020928749960	1143^2	4572^2	1143^2	4572^2
$(16,-408)$	72579094756950240	1863^2	3726^2	3726^2	3726^2
$(16,-96)$	133417453597333128	3804^2	7608^2	1902^2	7608^2
$(16,-33)$	234814718331305640	3717^2	7437^2	3717^2	14868^2
$(16,-32)$	133417453597332744	5463^2	10926^2	5463^2	10926^2
$(16,-8)$	106733962877866080	891^2	891^2	891^2	1782^2
$(16,12)$	2084647712458320	792^2	3168^2	396^2	6336^2
$(16,48)$	7021971241964856	4608^2	9216^2	2304^2	9216^2
$(16,92)$	61372028654772720	1064^2	2128^2	532^2	2128^2
$(16,268)$	279342793469411664	2916^2	11664^2	1458^2	11664^2
$(16,300)$	166771816996663440	1018^2	4072^2	509^2	4072^2
$(16,472)$	186310763603371680	3119^2	12476^2	3119^2	12476^2
$(16,588)$	116740271897662896	549^2	2196^2	549^2	1098^2
$(16,592)$	17950711938549720	2221^2	8884^2	2221^2	4442^2
$(16,624)$	102025111574427912	1100^2	2200^2	550^2	1100^2
$(17,-404)$	118434048164038608	3246^2	6492^2	1623^2	12948^2
$(17,-68)$	10206435200195943696	8284^2	33136^2	4142^2	33136^2
$(19,-32)$	19452264734491086120	31704^2	63408^2	31704^2	63408^2

Table 3. Examples of elliptic curves $E(n,p)$ ($16 \leqslant n \leqslant 19$; $0 < |p| \leqslant 1000$) with $\max_{1\leqslant i\leqslant 4} |Ш_i| \geqslant 1000^2$.

2 Values of the Goldfeld-Szpiro ratio $GS(E)$

The Goldfeld-Szpiro ratio was defined in (3). The articles of de Weger [We] and Nitaj [Ni] produce altogether 58 examples of elliptic curves with $GS(E)$ greater than 1 (the record value being 42.265...). For all of these examples the conductor does not exceed 10^{10}. The largest values of $GS(E)$ that we observed for our curves are tabulated in Table 4.

E	$\lvert Ш(E)\rvert$	$GS(E)$
$E_2(9,544)$	344^2	1.20290...
$E_{2,4}(16,48)$	9216^2	1.01357...
$E_2(10,204)$	504^2	0.98366...
$E_4(15,-212)$	3984^2	0.94753...
$E_{2,4}(19,-32)$	63408^2	0.91159...
$E_4(16,12)$	6336^2	0.87925...
$E_4(15,12)$	3840^2	0.80334...
$E_2(16,592)$	8882^2	0.58908...
$E_2(11,160)$	322^2	0.57131...
$E_4(17,-404)$	12984^2	0.48986...
$E_4(16,-33)$	14868^2	0.45618...
$E_2(13,96)$	1176^2	0.42149...
$E_{2,4}(16,472)$	12476^2	0.36060...
$E_{2,4}(17,-68)$	33136^2	0.34368...
$E_{2,4}(16,-32)$	10926^2	0.32682...
$E_2(11,336)$	1058^2	0.28146...
$E_4(15,-116)$	9472^2	0.27367...
$E_{2,4}(16,268)$	11664^2	0.25741...

Table 4. Elliptic curves $E_i(n,p)$ ($9 \leqslant n \leqslant 19$; $0 < |p| \leqslant 1000$; $1 \leqslant i \leqslant 4$) with the largest $GS(E)$. Notation $E_{i,j}(n,p)$ means that the given values of $\lvert Ш(E)\rvert$ and $GS(E)$ are shared by the isogeneous curves $E_i(n,p)$ and $E_j(n,p)$.

3 Large and small (nonzero) values of $L(E,1)$

In this section we produce elliptic curves of rank zero with $L(E,1)$ either much smaller or much bigger than in all previously known examples (Tables 5 and 6).

E	$L(E,1)$
$E(11,-733)$	88.203561907255071...
$E(13,-160)$	71.523635814751843...
$E(12,466)$	56.224807584564927...
$E(7,-433)$	36.275918867296195...
$E(10,687)$	30.274774697662334...
$E(9,767)$	29.638568367562609...
$E(9,-93)$	28.032198538875886...
$E(11,336)$	22.922225180212583...

Table 5. Elliptic curves $E(n,p)$ ($n \leqslant 19$; $0 < |p| \leqslant 1000$) with the largest values of $L(E,1)$ known to us.

E	$L(E,1)$
E(12,800)	0.0001706491750110...
E(10,142)	0.0002457348122099...
E(11,168)	0.0003276464160384...
E(14,672)	0.0006067526222261...
E(9,160)	0.0007372044423472...
E(10,-534)	0.0009829392448696...
E(10,408)	0.0009829392504019...

Table 6. Elliptic curves $E(n,p)$ ($n \leqslant 19$; $0 < |p| \leqslant 1000$) with the smallest positive values of $L(E,1)$ known to us.

Note that

$$L(E(10,408),1) - L(E(10,-534),1) = 0.00000000000553237117\ldots .$$

This is the *smallest known* difference between the values of $L(E,1)$ of two elliptic curves of rank zero. The analytic orders of the Tate-Shafarevich group are 2^2, 4^2, 1^2, 4^2 for the isogeneous curves $E(10,408)$ and $E_i(10,408)$, respectively, and 2^2, 8^2, 8^2, 8^2 for the curves $E(10,-534)$ and $E_i(10,-534)$, repectively, where $i = 2$, 3, or 4.

We observed that for a large percentage of rank zero curves $E_i(n,p)$ with $7 \leqslant n \leqslant 19$ and $0 < |p| \leqslant 1000$, one has

$$L(E,1) \geqslant \frac{1}{(\log N(E))^2}.$$

We verified, in particular, that (5) holds for every single curve $E(7,p)$ of rank zero when $0 < |p| \leqslant 1000$. This is consistent with results of Iwaniec and

Sarnak who proved [IS] that

$$L(f,1) \geqslant \frac{1}{(\log N)^2},$$

for a large percentage of newforms of weight 2, with the *level* N of a newform f playing the role of the conductor of an elliptic curve.

On the other hand, we have

$$L(E(8,-131),1) = 0.0002764516... < 0.0012048710... = (\log N(8,-131))^{-2},$$

$$L(E(9,160),1) = 0.0007372044... < 0.0015186182... = (\log N(9,160))^{-2},$$

$$L(E(10,142),1) = 0.0002457384... < 0.0009026601... = (\log N(10,142))^{-2},$$

$$L(E(11,168),1) = 0.0003276464... < 0.0009902333... = (\log N(11,168))^{-2},$$

$$L(E(12,800),1) = 0.0001706491... < 0.0009613138... = (\log N(12,800))^{-2}.$$

An estimate much weaker than (5) was proposed by Hindry [H], see Conjecture 6 below.

4 Remarks on Conjecture 3

Below we sketch how to utilize curves $E(n,p)$ in order to establish the first of the two conjectures of de Weger (Conjecture 3 above).

According to Chen [Ch], every sufficiently large even integer can be represented as the sum $p+q$ where p is an odd prime and q is the product of at most two primes. Apply this, for sufficiently large n, to the number

$$4 \cdot 3^{2n+1} = p + q.$$

The factors $c_\infty(E(n,p))$ and $c_{\text{fin}}(E(n,p))$ on the right-hand-side of the formula for the analytic order of the Tate-Shafarevich group, (4), are given by the following lemma.

lemma Assume $p < q$, with q having at most two prime factors. Then we have

$$c_\infty(E(n,p)) = \frac{\pi}{3^{n+1/2} \cdot \mathrm{AGM}(1, \sqrt{q/(p+q)})} \tag{4}$$

and

$$c_{\text{fin}}(E(n,p)) = 2c_2c_3c_q, i \tag{5}$$

(6)

where $AGM(a,b)$ denotes the arithmetico-geometric mean of a and b,

$$c_2 = \begin{matrix} 2 \text{ if } p \equiv 1 \mod 4 \\ 4 \text{ if } p \equiv 3 \mod 4 \end{matrix}, \qquad c_3 = \begin{matrix} 2(2n+1) \text{ if } p \equiv 2 \mod 3 \\ 4 \text{ if } p \equiv 1 \mod 3 \end{matrix},$$

and

$$c_q = \begin{cases} 2 \text{ if } q \text{ is a prime} \\ 4 \text{ if } q \text{ is a product of two primes} \end{cases}.$$

The conductor is given by the formula

$$N(E(n,p)) = 2^{f_2} \cdot 3 \cdot p \cdot \mathrm{rad}(q),$$

where $\mathrm{rad}(q)$ denotes the product of prime factors, and

$$f_2 = \begin{cases} 3 \text{ if } p \equiv 1 (\mathrm{mod}\ 4) \\ 4 \text{ if } p \equiv 3 (\mathrm{mod}\ 4)\ . \end{cases}$$

lemma

This is easily proven by using calculations of Nitaj [Ni, Propositions 2.1, 3.1 and 3.2]. The following then seems to be a plausible conjecture.

Conjecture 5. *For any $\epsilon > 0$ there exists $c(\epsilon) > 0$ and infinitely many n admitting a decomposition* (6) *with*

$$p \leqslant c(\epsilon) q^{\epsilon}$$

such that curve $E(n,p)$ has rank zero.

If we accept Conjecture 5, then

$$\frac{1}{c_\infty(E(n,p))} \gg N(E(n,p))^{1/2-\epsilon} \quad \text{and} \quad \frac{1}{c_{\mathrm{fin}}(E(n,p))} \gg N(E(n,p))^{-\epsilon}.$$

on an infinite set of curves $E(n,p)$.

Since $|E(\mathbb{Q})_{\mathrm{tors}}| \geqslant 1$ (in fact, $|E(\mathbb{Q})_{\mathrm{tors}}|$ can take only twelve values between 1 and 16, cf[Mz]) it remains to estimate $L(E,1)$. The result of Iwaniec and Sarnak mentioned in section 3 provides a support for the following conjecture recently proposed by Hindry [H, Conjecture 5.4].

Conjecture 6 (Hindry). *One has*

$$L^{(r)}(E,1) \gg N(E)^{-\epsilon} \qquad (r \text{ being the rank of } E).$$

Hindry observed that (8) implies that the distance from 1 to the nearest zero of $L(E,s)$ is $\gg N(E)^{-\epsilon}$.

The combination of (7) and (8), for curves of rank zero, yields the assertion of Conjecture 3 for the analytic order of the Tate-Shafarevich group. In order to pass to the actual order, one needs, of course, the equality of the two, as predicted by the Birch and Swinnerton-Dyer Conjecture.

References

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$: *wild 3-adic exercises,* J. Amer. Math. Soc. **14** (2001), 843–939

[Be] C. D. Beaver, *5-torsion in the Shafarevich-Tate group of a family of elliptic curves,* J. Number Theory **82** (2000), 25–46

[C] J. W. S. Cassels, *Arithmetic on curves of genus 1. VI. The Tate-Šafarevič group can be arbitrarily large,* J. reine angew. Math. **214/215** (1964), 65–70

[Ch] J. R. Chen, *On the representation of a large even number as the sum of a prime and the product of at most two primes,* Sc. Sinica **16** (1973), 157–176

[Co] H. Cohen, *A course in Computational Algebraic Number Theory.* Graduate Texts in Math. **138** Springer-Verlag (1993)

[Cr_1] J. E. Cremona, *Algorithms for modular elliptic curves.* Cambridge University Press 1997

[Cr_2] J. E. Cremona, Elliptic Curve Data (*an online resource*)

[CFNS^2] J. E. Cremona, T. A. Fischer, C. O'Neil, D. Simon, M. Stoll, *Explicit n-descent on elliptic curves. I. Algebra, II. Geometry,* preprints 2006

[F] T. Fisher, *Some examples of 5 and 7 descent for elliptic curves over* $\mathbb{Q}$*,* J. Eur. Math. Soc. **3** (2001), 169–201

[Fr_1] G. Frey, *Der Rang der Lösungen von $y^2 = x^3 \pm p^3$ über* $\mathbb{Q}$*,* Manuscr. math. **48** (1984), 71–101

[Fr_2] G. Frey, *A relation between the value of the L-series of the curve $y^2 = x^3 - k^3$ in $s = 1$ and its Selmer group,* Arch. Math. **45** (1985), 232–238

[GHP] D. Goldfeld, J. Hoffstein, S. J. Patterson, *On automorphic functions of half-integral weight with applications to elliptic curves.* In: Number Theory Related to Fermat's Last Theorem (Birkhäuser, Boston, MA, 1982), pp 153–193

[GL] D. Goldfeld and D. Lieman, *Effective bounds on the size of the Tate-Shafarevich group,* Math. Res. Letters **3** (1996), 309–318

[GS] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevich group,* Compos. math. **97** (1995), 71–87

[GA] C. Gonzalez-Avilés, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. **349** (1997), 4181-4200

[GJPST] G. Grigorov, A. Jorza, S. Patrikis, W.A. Stein, C. Tarniţă, *Verification of the Birch and Swinnerton-Dyer conjecture for specific elliptic curves*, Math. Comput. (to appear)

[H] M. Hindry, *Why it is difficult to compute the Mordell-Weil group?* In: Diophantine Geometry. Proceedings (ed. Umberto Zannier, Edizioni della Normale, Pisa, 2007)

[HL] J. Hoffstein, W. Luo, *Nonvanishing of L-series and the combinatorial sieve,* Math. Res. Letters **4** (1997), 435–442

[IS] H. Iwaniec and P. Sarnak, *The non-vanishing of central values of automorphic L-functions and Landau-Siegel zeros,* Israel J. Math. **120** (2000), 155–177

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

[L] S. Lang, *Conjectured diophantine estimates on elliptic curves.* In: Arithmetic and Geometry – Papers dedicated to I. R. Shafarevich. Vol. 1 (Birkhäuser, Boston, MA, 1983), pp. 155–171

[Le] J. L. Lehman, *Rational points on elliptic curves with complex multiplication by the ring of integers in* $\mathbb{Q}(\sqrt{-7})$*,* J. Number Theory **27** (1987), 253–272

[MM1] L. Mai and M. R. Murty, *On the Shafarevich-Tate group.* (unpublished, reported in [R])

[MM2] L. Mai and M. R. Murty, *A note on quadratic twists of an elliptic curve.* In: Elliptic Curves and Related Topics. CRM Proceed. and Lecture Notes **4** (1994), 121–124

[Ma] D. W. Masser, *Note on a conjecture of Szpiro,* Astérisque **183** (1990), 19–23

[Mz] B. Mazur, *Modular curves and the Eisenstein ideal,* Publ. Math. IHES **47** (1977), 33–186

[MS] J. R. Merriman, S. Siksek, N. P. Smart, *Explicit* 4*-descents on an elliptic curve,* Acta arithmetica **77** (1996), 385–404

[N] J. Nekovář, *Class numbers of quadratic fields and Shimura's correspondence,* Math. Ann. **287** (1990), 577–594

[Ni] A. Nitaj, *Invariants des courbes de Frey-Hellegouarch et grands groupes de Tate-Shafarevich,* Acta arithmetica **93** (2000), 303–327

[O] K. Ono, *Tate-Shafarevich groups of the congruent number elliptic curves,* Acta arithmetica **81** (1997), 247–252

[R] C. S. Rajan, *On the size of the Shafarevich-Tate group of elliptic curves over function fields,* Compos. math. **105** (1997), 29–41

[Ro] D. E. Rohrlich, *Unboundedness of the Tate-Shafarevich group in families of quadratic twists* (an appendix to [HL]), Math. Res. Letters **4** (1997), 443–444

[Rs] H. E. Rose, *On some elliptic curves with large Sha,* Experimental Math. **9** (2000), 85–89

[Ru] K. Rubin, *Tate-Shafarevich groups and* L*-functions of elliptic curves with complex multiplication.* Invent. math **89** (1987), 527–559

[S] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Math. **106**, Springer, New York 1986

[T] J. Tunnell, *A classical diophantine problem and modular forms of weight* 3/2*,* Invent. math. **72** (1983), 323–334

[W] J. L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entiers,* J. Math. Pure et Appl. **60** (1981), 375–484

[We] B. M. M. de Weger, $A + B = C$ *and big* Ш*'s,* Quart. J. Math. **49** (1998), 105–128

[ZK] D. Zagier and G. Kramarz, *Numerical investigations related to the* L*-series of certain elliptic curves,* Journal of the Indian Math. Soc. **52** (1987), 51–69