COLLOQUIUM MATHEMATICUM

Online First version

ELLIPTIC CURVES WITH EXCEPTIONALLY LARGE ANALYTIC ORDER OF THE TATE–SHAFAREVICH GROUPS

BY

ANDRZEJ DĄBROWSKI and LUCJAN SZYMASZKIEWICZ (Szczecin)

Abstract. We exhibit 88 examples of rank zero elliptic curves over the rationals with $|Ш(E)| > 63408^2$, which was the largest previously known value for any explicit curve. Our record is an elliptic curve E with $|Ш(E)| = 1029212^2 = 2^4 \cdot 79^2 \cdot 3257^2$. We use deep results by Kolyvagin, Kato, Skinner–Urban and Skinner to prove that, in some cases, these orders are the true orders of Ш. For instance, 410536^2 is the true order of Ш(E) for $E = E_4(21, -233)$ from the table in Section 2.3.

1. Introduction. Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N_E, and let $L(E,s)$ denote its L-series. Let Ш(E) be the Tate–Shafarevich group of E, $E(\mathbb{Q})$ the group of rational points, and $R(E)$ the regulator with respect to the Néron–Tate height pairing. Finally, let Ω_E be the least positive real period of the Néron differential of a global minimal Weierstrass equation for E, and define $C_\infty(E) = \Omega_E$ or $2\Omega_E$ according as $E(\mathbb{R})$ is connected or not, and let $C_{\text{fin}}(E)$ denote the product of the Tamagawa factors of E at the bad primes. The Euler product defining $L(E,s)$ converges for $\operatorname{Re} s > 3/2$. The modularity conjecture, proven by Wiles–Taylor–Diamond–Breuil–Conrad, implies that $L(E,s)$ has an analytic continuation to an entire function. The Birch and Swinnerton-Dyer conjecture relates the arithmetic data of E to the behaviour of $L(E,s)$ at $s=1$.

Conjecture 1 (Birch and Swinnerton-Dyer).

(i) *The L-function $L(E,s)$ has a zero of order $r = \operatorname{rank} E(\mathbb{Q})$ at $s=1$.*
(ii) Ш(E) *is finite, and*

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

If Ш(E) is finite, the work of Cassels and Tate shows that its order must be a square.

2020 *Mathematics Subject Classification*: Primary 11G05, 11G40, 11Y50.
Key words and phrases: elliptic curves, Tate–Shafarevich group, central L-values.
Received 11 August 2019; revised 25 August 2020.
Published online 22 March 2021.

DOI: 10.4064/cm8008-9-2020

The first general result in the direction of this conjecture was proven in 1976 for elliptic curves E with complex multiplication by Coates and Wiles [6], who showed that if $L(E,1) \neq 0$, then the group $E(\mathbb{Q})$ is finite. Gross and Zagier [16] showed that if $L(E,s)$ has a first-order zero at $s=1$, then E has a rational point of infinite order. Rubin [28] proved that if E has complex multiplication and $L(E,1) \neq 0$, then $Ш(E)$ is finite. Let g_E be the rank of $E(\mathbb{Q})$ and r_E the order of the zero of $L(E,s)$ at $s=1$. Kolyvagin [18] proved that if $r_E \leq 1$, then $r_E = g_E$ and $Ш(E)$ is finite. Very recently, Bhargava, Skinner and Zhang [1] proved that at least 66.48% of all elliptic curves over $\mathbb{Q}$, when ordered by height, satisfy the weak form of the Birch and Swinnerton-Dyer conjecture, and have finite Tate–Shafarevich group.

When E has complex multiplication by the ring of integers of an imaginary quadratic field K and $L(E,1)$ is non-zero, the p-part of the Birch and Swinnerton-Dyer conjecture has been established by Rubin [29] for all primes p which do not divide the order of the group of roots of unity of K. Coates et al. [5], [4] and Gonzalez-Avilés [13] showed that there is a large class of explicit quadratic twists of $X_0(49)$ whose complex L-series does not vanish at $s=1$, and for which the full Birch and Swinnerton-Dyer conjecture is valid (covering the case $p=2$ when $K=\mathbb{Q}(\sqrt{-7})$). The deep results by Kato, Skinner and Urban [32, Theorem 2] and Skinner [31, Theorem C] allow one, in specific cases (still assuming $L(E,1)$ is non-zero), to establish the p-part of the Birch and Swinnerton-Dyer conjecture for elliptic curves without complex multiplication for all odd primes p.

It has long been known that the order of $Ш(E)[p]$ can be arbitrarily large for elliptic curves E defined over $\mathbb{Q}$ and $p=2,3$; for $p=3$, the result is due to Cassels [3], and for $p=2$ it is due to McGuinness [24]. It was later extended for $p=5$ by Fisher [12], and for $p=7$ and 13 by Matsuno [21], but no similar result is known for $p=11$ or $p>13$. Let us mention that all those authors used the fact that there are infinitely many elliptic curves defined over $\mathbb{Q}$ with rational p-isogenies. We also stress that it has not yet been proven that there exist elliptic curves E defined over $\mathbb{Q}$ for which $Ш(E)[p]$ is non-zero for arbitrarily large primes p.

In earlier papers (see [11], [7], [8], [9], [10]), we have investigated some numerical examples of E defined over $\mathbb{Q}$ for which $L(E,1)$ is non-zero and the order of $Ш(E)$ is large.

We extend these numerical results in this paper, with the largest proved example of $Ш(E)$ having order $410536^2 = 2^6 \cdot 7^2 \cdot 7331^2$. We exhibit 88 examples of rank zero elliptic curves over the rationals with $|Ш(E)| > 63408^2$, which was the largest previously known value for any explicit curve. For some of these examples we use deep results by Kolyvagin, Kato, Skinner–Urban and Skinner to prove that these orders are the true orders of Ш.

Our idea was to use the family $E_i(n,p)$ from [11] (see Section 2.1 below), within the bounds $20 \le n \le 24$ and $0 < |p| \le 5000$ (the calculations in [11] were focused on the pairs (n,p) with $3 \le n \le 19$ and $0 < |p| \le 1000$). The first step was to find good candidates, i.e. the curves $E_i(n,p)$ with rank zero and $\max_i |Ш(E_i(n,p))| > 50000^2$. The next step was to calculate $|Ш(E_i(n,p))|$ exactly for all these good candidates. In these steps, we computed (or estimated) the analytic orders of $Ш(E)$, using the approximations to $L(E,1)$. The computations were performed using the computer package PARI/GP [27]. The total running time for the various computational parts was about 9 months.

2. Results. The previously largest value for $|Ш(E)|$ was 63408^2, found by Dąbrowski and Wodzicki [11]. In [7, Section 5] we proposed a candidate with $|Ш(E)| > 100000^2$. Below we present the results of our recent search for elliptic curves with exceptionally large analytic order of the Tate–Shafarevich group. We exibit 88 examples of rank zero elliptic curves with $|Ш(E)| > 63408^2$. Our record is an elliptic curve $E = E_2(23,-348)$ with $|Ш(E)| = 1029212^2$. Also note that the prime 19861 divides the order of $Ш(E_i(22,304))$, the largest (at the moment) prime dividing the order of $Ш(E)$ of an elliptic curve over $\mathbb{Q}$.

2.1. Preliminaries. In this section we compute the analytic order of $Ш(E)$, i.e., the quantity

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

for certain special curves of rank zero. We use the following approximation of $L(E,1)$:

$$S_m = 2\sum_{n=1}^{m}\frac{a_n}{n}e^{-2\pi n/\sqrt{N}},$$

which, for

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

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

Consider (as in [11]) the family

$$E_1(n,p):\quad y^2 = x(x+p)(x+p-4\cdot 3^{2n+1})$$

with $(n,p)\in\mathbb{N}\times(\mathbb{Z}\setminus\{0\})$. Any member of the family admits three isogenous (over $\mathbb{Q}$) curves $E_i(n,p)$ $(i=2,3,4)$:

$$\begin{aligned}
E_2(n,p):&\quad y^2 = x^3 + 4(2\cdot 3^{2n+1}-p)x^2 + 16\cdot 3^{4n+2}x,\\
E_3(n,p):&\quad y^2 = x^3 + 2(4\cdot 3^{2n+1}+p)x^2 + (4\cdot 3^{2n+1}-p)^2x,\\
E_4(n,p):&\quad y^2 = x^3 + 2(p-8\cdot 3^{2n+1})x^2 + p^2x.
\end{aligned}$$

In our calculations, we focused on the pairs of integers (n,p) within the bounds $20 \le n \le 24$ and $0 < |p| \le 5000$. Recall that the calculations in [11] were focused on (n,p) with $3 \le n \le 19$ and $0 < |p| \le 1000$.

The conductors, L-series and ranks of isogenous curves coincide; what may differ is the orders of $E(\mathbb{Q})_{\text{tors}}$ and $Ш(E)$, the real period Ω_E, and the Tamagawa number $C_{\text{fin}}(E)$. In our situation we are dealing with 2-isogenies, thus the analytic order of $Ш(E)$ can only change by a power of 2.

Notation. Let $N(n,p)$ denote the conductor of the curve $E_i(n,p)$. We put $|Ш_i| = |Ш(E_i)|$.

2.2. Elliptic curves $E_i(n,p)$ with $50000^2 \le \max(|Ш_i|) < 250000^2$

(n,p)	$N(n,p)$	$\|Ш_1\|$	$\|Ш_2\|$	$\|Ш_3\|$	$\|Ш_4\|$
$(20,-756)$	42551829106699251024	27993^2	55986^2	27993^2	27993^2
$(20,-2000)$	190293894141760627320	15081^2	60324^2	15081^2	60324^2
$(20,192)$	109418989131512359065	3780^2	60480^2	945^2	60480^2
$(22,-692)$	11978814802342833513168	15194^2	30388^2	7597^2	60776^2
$(21,-128)$	1969541804367222465954	34234^2	68468^2	34234^2	68468^2
$(20,-180)$	60788327295284644080	20970^2	41940^2	10485^2	83880^2
$(21,3)$	31512668869875559452120	10962^2	43848^2	5481^2	87696^2
$(20,-2448)$	1653442502431742344680	22028^2	88112^2	22028^2	88112^2
$(20,2704)$	11379574869677285146824	48538^2	97076^2	97076^2	48538^2
$(21,12)$	281363114909603209392	12768^2	102144^2	3192^2	102144^2
$(20,-608)$	16631686347989878669080	25787^2	103148^2	51574^2	51574^2
$(21,192)$	984770902183611232737	54648^2	109296^2	27324^2	109296^2
$(20,4788)$	25871512096873143639456	27745^2	110980^2	27745^2	27745^2
$(20,2680)$	23938195173261478962720	14474^2	115792^2	14474^2	57896^2
$(20,-801)$	34625031227394133415352	29338^2	58676^2	29338^2	117352^2
$(22,1344)$	62040566837567507664447	60930^2	121860^2	30465^2	60930^2
$(20,-1436)$	1832369310703810488288	32455^2	129820^2	32455^2	129820^2
$(20,4768)$	10032879618827902147272	16254^2	130032^2	8127^2	65016^2
$(21,-24)$	31512668869875559452768	34092^2	68184^2	17046^2	136368^2
$(20,-1376)$	37640132261240251922904	70010^2	140020^2	140020^2	70010^2
$(22,64)$	8862938119652501095881	72306^2	144612^2	36153^2	144612^2
$(21,-1536)$	1969541804367222468066	75897^2	151794^2	75897^2	151794^2
$(20,-6)$	14005630608833581979328	19248^2	76992^2	4812^2	153984^2
$(22,304)$	27493195799738370745848	39722^2	158888^2	19861^2	79444^2
$(21,1516)$	11663380372737145525968	25866^2	206928^2	12933^2	103464^2
$(21,480)$	39390836087344449300840	54110^2	216440^2	27055^2	108220^2
$(23,1452)$	6451697601805864768272	55698^2	222792^2	27849^2	222792^2

2.3. Elliptic curves $E_i(n,p)$ with $\max(|Ш_i|) \geq 250000^2$

(n,p)	$N(n,p)$	$\|Ш_1\|$	$\|Ш_2\|$	$\|Ш_3\|$	$\|Ш_4\|$
$(21,4)$	15756334434937779726048	130614^2	261228^2	65307^2	261228^2
$(21,1248)$	102416173827095568122280	70375^2	281500^2	70375^2	70375^2
$(20,-201)$	234594312697962498467304	141540^2	141540^2	283080^2	141540^2
$(23,960)$	398832215384362549313205	96254^2	385016^2	48127^2	192508^2
$(24,832)$	373306953599763346160205	75780^2	303120^2	37890^2	151560^2
$(20,1120)$	30637316956823460343320	20440^2	327040^2	20440^2	81760^2
$(23,-84)$	17448909423065861532624	184991^2	369982^2	184991^2	184991^2
$(22,480)$	354517524786100043822760	99938^2	399752^2	49969^2	199876^2
$(23,-8)$	7441767284139709375008	102120^2	204240^2	51060^2	408480^2
$(21,-233)$	149845956054714394972728	51317^2	205268^2	51317^2	410536^2
$(23,-96)$	638131544614980078907464	264696^2	529392^2	132348^2	529392^2
$(24,-96)$	302272836922885300534872	412146^2	824292^2	206073^2	824292^2
$(23,-348)$	37011629587668844576720608	514606^2	1029212^2	257303^2	1029212^2

2.4. Birch and Swinnerton-Dyer conjecture for elliptic curves with exceptionally large analytic order of Tate–Shafarevich group. In this subsection, we will use the deep results by Kato, Skinner–Urban and Skinner to prove the full version of the Birch and Swinnerton-Dyer conjecture for some elliptic curves $E_i(n,p)$ with exceptionally large analytic order of Tate–Shafarevich groups.

Let $\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ denote the Galois representation on the p-torsion of E. Assume $p \geq 3$. As mentioned in [14], the work of Kato [17] together with the works of Mazur and Rubin [23] and Matsuno [20] implies the following result.

Theorem 2. *Let E be an optimal elliptic curve over $\mathbb{Q}$ with conductor N_E. Assume that $p \nmid 6N_E$, and $\overline{\rho}_{E,p}$ is surjective. If $L(E,1) \neq 0$, then $Ш(E)$ is finite and*

$$\mathrm{ord}_p(|Ш(E)|) \leq \mathrm{ord}_p\left(\frac{L(E,1)}{C_\infty(E)}\right). \tag{1}$$

For elliptic curves without complex multiplication, the following theorem of Skinner–Urban and Skinner implies that the p-part of the Birch and Swinnerton-Dyer conjecture holds for nice primes p in the rank zero case.

Theorem 3 ([32, Theorem 2]; [31, Theorem C]). *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Suppose:* (i) *E has good ordinary or multiplicative reduction at p;* (ii) *there exists a prime $q \neq p$ such that $q \,\|\, N_E$ and $\overline{\rho}_{E,p}$ is ramified at q;* (iii) *$\overline{\rho}_{E,p}$ is surjective. If moreover $L(E,1) \neq 0$, then* *the p-part of the Birch and Swinnerton-Dyer conjecture holds true, that is,*

$$\operatorname{ord}_p(|Ш(E)|) = \operatorname{ord}_p\left(\frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2 L(E,1)}{C_\infty(E) C_{\mathrm{fin}}(E)}\right). \tag{2}$$

Remark 4. The condition (ii) can be removed in the good ordinary case by the results of X. Wan [33], so we will omit it in the calculations below. Further, surjectivity of $\overline{\rho}_{E,p}$ implies its irreducibility.

For the following curves from the tables in Sections 2.2 and 2.3, we can apply the above results by Kato, Skinner–Urban and Skinner: $E_i(22,-692)$, $E_i(20,-608)$, $E_i(20,-1436)$, $E_i(20,4788)$, $E_i(22,304)$, $E_i(22,64)$, $E_i(21,1516)$, $E_i(21,4)$, $E_i(21,-233)$.

Let us give some details for the curves $E_i = E_i(20,-1436)$. We can use the above results to show that $|Ш_1| = 5^2 \times 6491^2$ is the true order of $Ш(E_1)$ (and hence all $|Ш_i|$ are the true orders of $Ш(E_i)$).

(i) We have $N_{E_1} = 2^5 \times 3 \times 7 \times 31 \times 257 \times 359 \times 107323 \times 8883041$.

(ii) We have $j_{E_1} = \frac{2^6 285451^3 4660272567723053424015171049538317^3}{3^{82} 7^8 31^2 257^2 359^2 107323^2 8883041^2}$. The representation $\overline{\rho}_{E_1,p}$ is surjective for any prime $p \geq 19$ by [35, Prop. 1.8]. On the other hand, [35, Prop. 6.1] gives a criterion to determine whether $\overline{\rho}_{E,p}$ is surjective or not for any non-CM elliptic curve E and any prime $p \leq 11$. For instance, the representation $\overline{\rho}_{E,5}$ is not surjective if and only if

$$j_E = \frac{5^3(t+1)(2t+1)^3(2t^2-3t+3)^3}{(t^2+t-1)^5} \quad \text{or}$$
$$\frac{5^2(t^2+10t+5)^3}{t^5} \quad \text{or} \quad t^3(t^2+5t+40)$$

for some $t \in \mathbb{Q}$. We have checked, using Pari/GP, that these three cases are impossible.

For the primes $p = 13$ and $p = 17$ (actually for any $p \geq 5$), we can give a less computational proof of surjectivity as follows (suggested by the referee). First, it is due to B. Mazur (see [22, Theorem 3] or [25, Theorem 1.3]) that for any elliptic curve E over $\mathbb{Q}$ with all its 2-division points defined over $\mathbb{Q}$, the representation $\overline{\rho}_{E,p}$ is absolutely irreducible for any prime $p \geq 5$. Using the irreducibility, and the fact that the denominator of j_{E_1} is not a pth power, we can apply [30, Lemmas 1 and 2, Chapter IV, Section 3.2].

(iii) E_1 has good ordinary reduction at 5 and 6491: $(N_{E_1},5) = (N_{E_1},6491) = 1$, and $a_5(E_1) = 2$, $a_{6491}(E_1) = 108$.

(iv) E_1 has multiplicative reduction at any $p \in \{3,7,31,257,359,107323,8883041\}$. Take $q = 7$. Then $7 \,\|\, N_{E_1}$, and $\overline{\rho}_{E_1,p}$ is ramified at 7 for these $p \neq 7$, since they satisfy $p \nmid \operatorname{ord}_7(\Delta_{E_1})$. Take $q = 31$. Then $31 \,\|\, N_{E_1}$, and $\overline{\rho}_{E_1,7}$ is ramified at 31, since $7 \nmid \operatorname{ord}_{31}(\Delta_{E_1})$.

(v) Using Magma [2] we see that $Ш(E_1)[2]$ is trivial, and it is easy to conclude that the order of $Ш(E_1)$ is odd.

REMARK. The curves $E = E_i(23, -348)$ have additive reduction at 3, and the above results by Kolyvagin, Kato, Skinner–Urban and Skinner are not enough to prove that the analytic orders of Ш are the true ones in these cases. These methods only show that, say, the true order of $Ш(E_2(23, -348))$ is $1029212^2 \cdot 3^{2k} = 2^4 \cdot 3^{2k} \cdot 79^2 \cdot 3257^2$ for some non-negative integer k. To have $k = 0$, we additionally need to prove that $Ш(E)[3]$ is trivial. One way is to use Magma [2] to show that $\mathrm{Sel}(E)[3] = 0$. We ran `ThreeSelmerGroup(E)` subroutine for about 2.5 months, but without success, and we stopped the calculations. A second way is to use a result of Gross (see [15, Props. 2.1, 2.3] or [19, Theorem 0.5]) and some Magma computations. Let $y_K \in E(K)$ be the basic Heegner point attached to E and a suitable imaginary quadratic field K. If $y_K \notin 3E(K)$, then we obtain $Ш(E/K)[3^\infty] = 0$ as desired. But we have not managed to compute y_K, since all our attempts required recomputing $L(E, 1)$.

2.5. Values of the Goldfeld–Szpiro ratio. Let

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

denote the *Goldfeld–Szpiro ratio* of an elliptic curve E. Eleven examples of elliptic curves with $GS(E) \geq 1$ are given by de Weger [34], the largest value being 6.893 . . . . Another forty-seven examples with $GS(E) \geq 1$ are produced by Nitaj [26], his largest value of $GS(E)$ being 42.265 . . . . For all of these examples the conductor does not exceed 10^{10}. The article of Dąbrowski and Wodzicki [11] produces two examples with $GS(E) \geq 1$ for curves with much larger conductors.

The largest values of $GS(E)$ that we observed for our curves are given below. The notation $E_{i,j}(n, p)$ means that the given values of $|Ш(E)|$ and $GS(E)$ are shared by the isogeneous curves $E_i(n, p)$ and $E_j(n, p)$.

E	$\lvert Ш(E)\rvert$	$GS(E)$
$E_4(23, -8)$	408480^2	1.9342096803...
$E_{2,4}(24, 96)$	824292^2	1.2358410273...
$E_2(23, -84)$	369982^2	1.0362798350...
$E_4(20, -180)$	83880^2	0.9024159172...
$E_{2,4}(21, 12)$	102144^2	0.6220025144...
$E_{2,4}(23, 1452)$	222792^2	0.6179625870...
$E_2(20, 1120)$	327040^2	0.6110494864...
$E_{2,4}(21, 4)$	261228^2	0.5436405656...
$E_{2,4}(21, -1536)$	151794^2	0.5191903468...

Note that our record elliptic curves $E = E_{2,4}(23, -348)$ have relatively small Goldfeld–Szpiro ratio: $GS(E) = 0.1741167606\ldots$.

Acknowledgements. We thank an anonymous referee for the constructive criticism and comments which improved the final version.

This research was supported in part by PLGrid Infrastructure. Our computations were carried out in 2016 on the Prometheus supercomputer via PLGrid infrastructure. We also used the HPC cluster HAL9000 and desktop computers Core(TM) 2 Quad Q8300 4GB/8GB, all located at the Department of Mathematics and Physics of Szczecin University.

REFERENCES

[1] M. Bhargava, Ch. Skinner and W. Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, arXiv:1407.1826 (2014).

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[3] 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.

[4] J. Coates, *Lectures on the Birch–Swinnerton-Dyer conjecture*, ICCM Notices 1 (2013), no. 2, 29–46.

[5] J. Coates, Y. Li, Y. Tian and S. Zhai, *Quadratic twists of elliptic curves*, Proc. London Math. Soc. 110 (2015), 357–394.

[6] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223–251.

[7] A. Dąbrowski, T. Jędrzejak and L. Szymaszkiewicz, *Behaviour of the order of Tate–Shafarevich groups for the quadratic twists of $X_0(49)$*, in: Elliptic Curves, Modular Forms and Iwasawa Theory (in honour of John Coates' 70th birthday), Springer Proc. Math. Statist. 188, Springer, 2016, 125–158.

[8] A. Dąbrowski and L. Szymaszkiewicz, *Orders of Tate–Shafarevich groups for the quadratic twists of elliptic curves*, arXiv:1611.07840 (2016).

[9] A. Dąbrowski and L. Szymaszkiewicz, *Orders of Tate–Shafarevich groups for the Neumann–Setzer type elliptic curves*, Math. Comput. 87 (2018), 1509–1522.

[10] A. Dąbrowski and L. Szymaszkiewicz, *Orders of Tate–Shafarevich groups for the cubic twists of $X_0(27)$*, in: Banach Center Publ. 118, Inst. Math., Polish Acad. Sci., 2019, 125–135.

[11] A. Dąbrowski and M. Wodzicki, *Elliptic curves with large analytic order of* Ш(E), in: Algebra, Arithmetic and Geometry (in honour of Yu. I. Manin), Vol. I, Progr. Math. 269, Birkhäuser Boston, 2009, 407–421.

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

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

[14] G. Grigorov, A. Jorza, S. Patrikis, W. A. Stein and C. Tarnita, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Math. Comput. 78 (2009), 2397–2425.

[15] B. Gross, *Kolyvagin's work on modular elliptic curves*, in: L-functions and Arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser. 153, Cambridge Univ. Press, 1989, 235–256.
[16] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225–320.
[17] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in: P. Berthelot et al. (eds.), Cohomologies p-adiques et applications arithmétiques, III, Astérisque 295 (2004), 117–290.
[18] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E)$ for a class of Weil curves*, Math. USSR-Izv. 32 (1989), 523–541.
[19] A. Matar and J. Nekovář, *Kolyvagin's result on the vanishing of $Ш(E/K)[p^\infty]$ and its consequences for anticyclotomic Iwasawa theory*, J. Théor. Nombres Bordeaux 31 (2019), 455–501.
[20] K. Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory 99 (2003), 415–443.
[21] K. Matsuno, *Construction of elliptic curves with large Iwasawa lambda-invariants and large Tate–Shafarevich groups*, Manuscripta Math. 122 (2007), 289–304.
[22] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–162.
[23] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. 168 (2004), no. 799, viii + 96 pp.
[24] F. McGuinness, *The Cassels pairing in a family of elliptic curves*, PhD thesis, Brown Univ., 1982.
[25] L. Merel, *Arithmetic of elliptic curves and diophantine equations*, J. Théor. Nombres Bordeaux 11 (1999), 173–200.
[26] A. Nitaj, *Invariants des courbes de Frey–Hellegouarch et grands groupes de Tate–Shafarevich*, Acta Arith. 93 (2000), 303–327.
[27] The PARI Group, *PARI/GP version 2.7.2*, Bordeaux, 2014, http://pari.math.u-bordeaux.fr/.
[28] K. Rubin, *Tate–Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. 89 (1987), 527–560.
[29] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25–68.
[30] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, W. A. Benjamin, New York, 1968.
[31] Ch. Skinner, *Multiplicative reduction and the cyclotomic main conjecture for* GL_2, Pacific J. Math. 283 (2016), 171–200.
[32] Ch. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. 195 (2014), 1–277.
[33] X. Wan, *The Iwasawa main conjecture for Hilbert modular forms*, Forum Math. Sigma 3 (2015), art. e18, 95 pp.
[34] B. M. M. de Weger, *$A + B = C$ and big $Ш$'s*, Quart. J. Math. 49 (1998), 105–128.
[35] D. Zywina, *On the surjectivity of mod l representations associated to elliptic curves*, arXiv:1508.07661 (2015).

Andrzej Dąbrowski, Lucjan Szymaszkiewicz
Institute of Mathematics, University of Szczecin
Wielkopolska 15, 70-451 Szczecin, Poland
E-mail: andrzej.dabrowski@usz.edu.pl
dabrowskiandrzej7@gmail.com
lucjan.szymaszkiewicz@usz.edu.pl
lucjansz@gmail.com