NUMBER THEORY WEEK 2017
BANACH CENTER PUBLICATIONS, VOLUME 118
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2019

ORDERS OF TATE–SHAFAREVICH GROUPS FOR THE CUBIC TWISTS OF $X_0(27)$

ANDRZEJ DĄBROWSKI

Institute of Mathematics, University of Szczecin
Wielkopolska 15, 70-451 Szczecin, Poland
E-mail: andrzej.dabrowski@usz.edu.pl, dabrowskiandrzej7@gmail.com

LUCJAN SZYMASZKIEWICZ

Institute of Mathematics, University of Szczecin
Wielkopolska 15, 70-451 Szczecin, Poland
E-mail: lucjansz@gmail.com

Dedicated to Jerzy Kaczorowski
on his sixtieth birthday

Abstract. This paper continues the authors' previous investigations concerning orders of Tate–Shafarevich groups in quadratic twists of a given elliptic curve, and for the family of the Neumann–Setzer type elliptic curves. Here we present the results of our search for the (analytic) orders of Tate–Shafarevich groups for the cubic twists of $X_0(27)$. Our calculations extend those given by Zagier and Kramarz (1987) and by Watkins (2007). Our main observations concern the asymptotic formula for the frequency of orders of Tate–Shafarevich groups. In the last section we propose a similar asymptotic formula for the class numbers of real quadratic fields.

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

2010 *Mathematics Subject Classification*: 11G05, 11G40, 11Y50.
Key words and phrases: elliptic curves, cubic twists, Tate–Shafarevich group, Cohen–Lenstra heuristics, distribution of central L-values, class numbers of real quadratic fields.
The paper is in final form and no version of it will be published elsewhere.

DOI: 10.4064/bc118-8

connected or not, and let $C_{\mathrm{fin}}(E)$ 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) *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*

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

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

The first general result in the direction of this conjecture was proven for elliptic curves E with complex multiplication by Coates and Wiles in 1976 [3], who showed that if $L(E,1) \neq 0$, then the group $E(\mathbb{Q})$ is finite. Gross and Zagier [11] showed that if $L(E,s)$ has a first-order zero at $s=1$, then E has a rational point of infinite order. Rubin [16] proves 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 let r_E the order of the zero of $L(E,s)$ at $s=1$. Then Kolyvagin [13] 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 a 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 [17] for all primes p which do not divide the order of the group of roots of unity of K. Coates et al. [2], and Gonzalez-Avilés [10] 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 Skinner–Urban ([18], Theorem 2) allow, in specific cases (still assuming $L(E,1)$ is non-zero), to establish p-part of the Birch and Swinnerton-Dyer conjecture for elliptic curves without complex multiplication for all odd primes p.

This paper continues the authors' previous investigations concerning orders of Tate–Shafarevich groups in quadratic twists of a given elliptic curve, and for the family of the Neumann–Setzer type elliptic curves. Here we present the results of our search for the (analytic) orders of Tate–Shafarevich groups for the cubic twists E_m of $E : x^3 + y^3 = 1$. These analytic orders $|Ш(E_m)|$ are the true ones if $|Ш(E_m)|$ are coprime to 6 (by [17]). Our calculations extend those given by Zagier and Kramarz [20] and by Watkins [19]. Our main observations concern the asymptotic formulae in Sections 3 (frequency of orders of Ш) and 4 (asymptotics for the sums $\sum |Ш(E_m)|$ in the rank zero case), and the distributions of $\log L(E_m,1)$ and $\log(|Ш(E_m)|/\sqrt[t]{m})$ $(t=2,3)$ in Sections 6 and 7. In Section 8 we propose a variant of the asymptotic formula from Section 3 for the class numbers of real quadratic fields.

This research was supported in part by the PL-Grid Infrastructure. Our computations were carried out in 2016 and 2017 on the Prometheus supercomputer via the PL-Grid infrastructure.

2. Formula for the order of $Ш(E_m)$, when $L(E_m,1)\neq 0$. Let m be any cube-free positive integer. Let $E_m : x^3+y^3=m$ denote the cubic twist of $E: x^3+y^3=1$. Then it is plain to see that E_m has the Weierstrass equation $y^2=x^3-432m^2$, and $E_1=X_0(27)$. Let $L(E_m,s)=\sum_{n=1}^{\infty} a_m(n)n^{-s}$ $(\mathrm{Re}(s)>3/2)$ denote its L-series. If $L(E_m,1)\neq 0$, then the analytic order of $Ш(E_m)$ may be expressed as follows (see [20]):

$$|Ш(E_m)| = \frac{L(E_m,1)\cdot T_m}{C_{\mathrm{fin}}(E_m)\cdot C_\infty(E_m)},$$

where

(i) $T_1=9$, $T_2=4$, and $T_m=1$ for any $m>2$;
(ii) $C_\infty(E_m)=\frac{\Gamma(1/3)^3}{2\pi\sqrt{3}\sqrt[3]{m}}$ if $9\nmid m$, and $C_\infty(E_m)=\frac{3\Gamma(1/3)^3}{2\pi\sqrt{3}\sqrt[3]{m}}$ if $9|m$;
(iii) $C_{\mathrm{fin}}(E_m)=\prod_p C_p(E_m)$, where $C_p(E_m)=1$ if $p\nmid m$, $C_p(E_m)=2\pm 1$ if $p\equiv \pm 1 \pmod 3$, $C_3(E_m)=3$ if $m\equiv \pm 1 \pmod 9$, $C_3(E_m)=2$ if $m\equiv \pm 2 \pmod 9$, and $C_3(E_m)=1$ if $m\equiv \pm 4 \pmod 9$ or $3|m$.

If $\epsilon(E_m)=+1$, then the central L-value $L(E_m,1)$ is given by the sum of the approximating series

$$L(E_m,1)=2\sum_{n=1}^{\infty}\frac{a_m(n)}{n}\,e^{-2\pi n/\sqrt{N_{E_m}}},$$

where N_{E_m} is the conductor of E_m. The coefficients $a_m(n)$ can be computed as in [20] and [19]. In order to compute $L(E_m,1)$ with appropriate accuracy, we need to calculate $c\sqrt{N_{E_m}}$ terms of the approximating series (and, hence the same number of coefficients $a_m(n)$) for some constant c.

Definition. We say that a positive cube-free integer d *satisfies condition* $(*)$, if $\epsilon(E_d)=+1$.

3. Frequency of orders of Ш. Our data contain values of $|Ш(E_d)|$ for all positive cubic-free integers $d\le 10^8$ satisfying $(*)$. Our calculations strongly suggest that for any positive integer k there are infinitely many positive cube-free integers d satisfying $(*)$, such that E_d has rank zero and $|Ш(E_d)|=k^2$. Below we will state a more precise conjecture.

Let $f(X)$ denote the number of cube-free integers $d\le X$, satisfying $(*)$ and such that $|Ш(E_d)|=1$. Let $g(X)$ denote the number of cube-free integers $d\le X$, satisfying $(*)$ and such that $L(E_d,1)=0$. We obtain the following graph of the function $f(X)/g(X)$ (Fig. 1).

We expect that $f(X)/g(X)$ tends to a constant (≈ 0.7). Using ([19], Question 1.4.1, and [4]), we believe the following asymptotic formula holds

$$g(X)\sim c\cdot X^{5/6}(\log X)^d, \qquad X\to\infty,$$

with some positive c and real d. We therefore expect a similar asymptotic formula for $f(X)$. Compare this to similar phenomena for the cases of quadratic twists of elliptic curves [5], [6] and a family of Neumann–Setzer type elliptic curves [7].

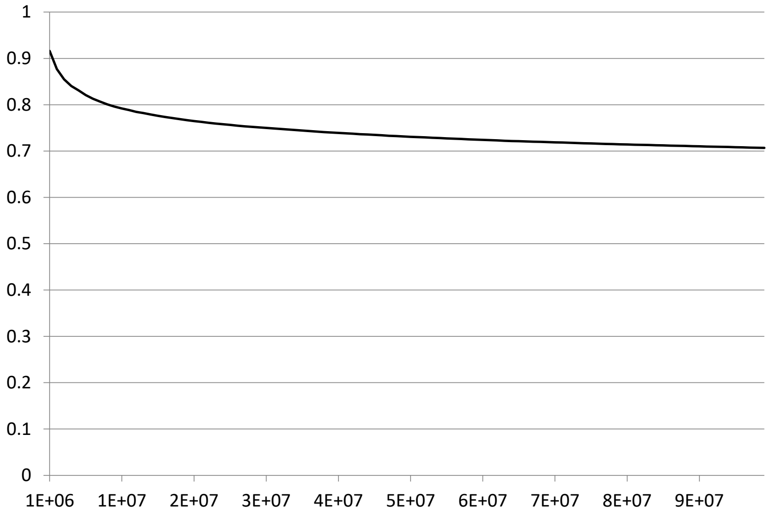

Fig. 1. Graph of the function $f(X)/g(X)$.

Remark. Watkins claims ([19], Question 1.4.1 and comments after it), that if we restrict to the cubic twists by primes congruent to 1 modulo 9, then we can take $d = -5/8$ and $c \approx 1/6 \approx 0.16666$. Our calculations suggest (see Figures 2 and 3 below) that the constant c is ≈ 0.175. Let $g^*(X)$ denote the number of primes $d \le X$, satisfying $(*)$ and such that $L(E_d, 1) = 0$.

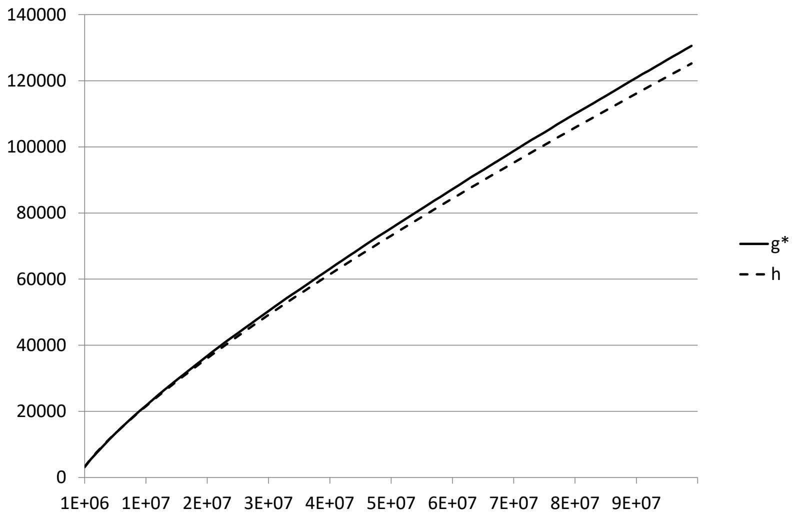

Fig. 2. Graphs of the functions $g^*(X)$ and $h(X) = \frac{1}{6}X^{5/6}(\log X)^{-5/8}$.

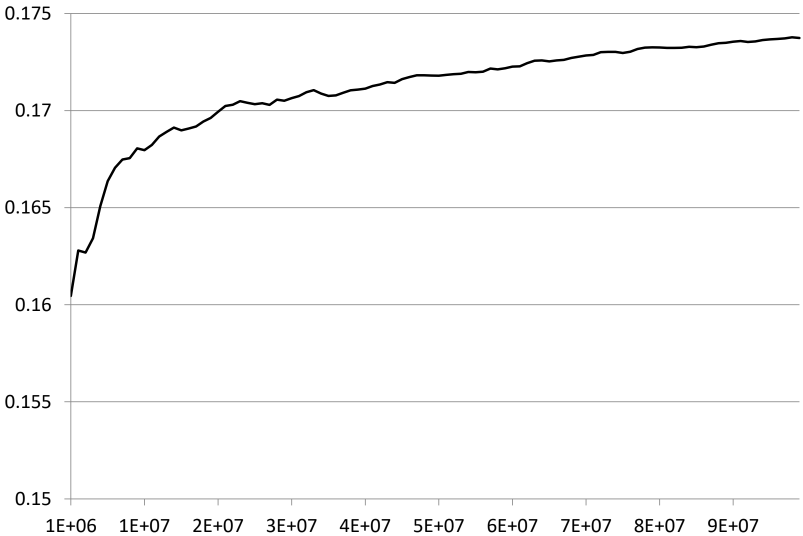

Fig. 3. Graph of the function $g^*(X)/(X^{5/6}(\log X)^{-5/8})$.

Let us also include the graph of the function $g(X)/(X^{5/6}(\log X)^{-5/8})$ (Fig. 4) .

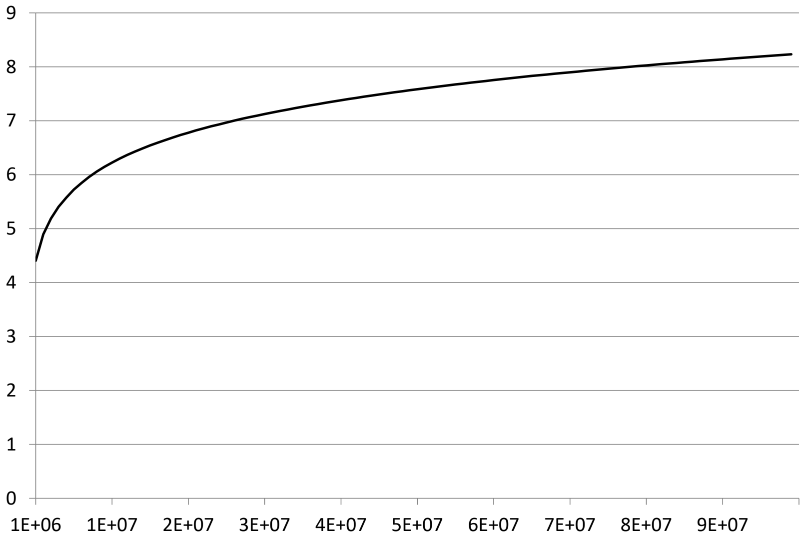

Fig. 4. Graph of the function $g(X)/(X^{5/6}(\log X)^{-5/8})$.

Now let $f(k,X)$ denote the number of cube-free integers $d \le X$, satisfying $(*)$ and such that $|Ш(E_d)| = k^2$. Let $F(k,X) := f(X)/f(k,X)$. We obtain the following graphs of the functions $F(k,X)$ for $k = 2,3,4,5,6,7$ (Fig. 5).

The above calculations suggest the following general conjecture (compare [5], [6] for the case of quadratic twists of elliptic curves, and [7] for the case of a family of Neumann–Setzer type elliptic curves).

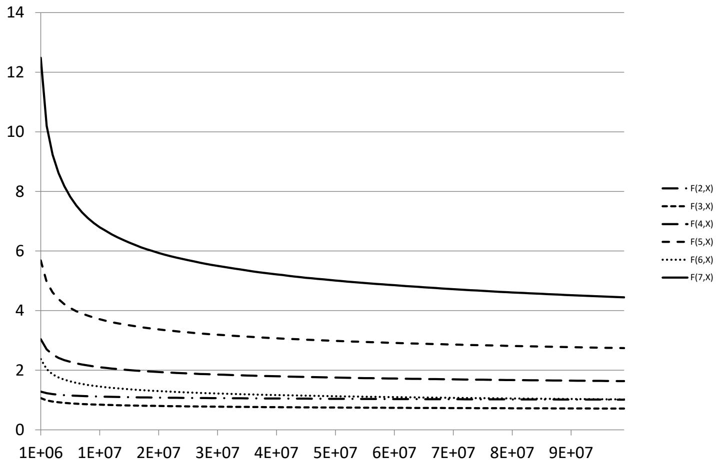

Fig. 5. Graphs of the functions $F(k, X)$ for $k = 2, 3, 4, 5, 6, 7$.

Conjecture 2. *For any positive integer k there are constants $c_k \geq 0$ and d_k such that*

$$f(k, X) \sim c_k X^{5/6} (\log X)^{d_k}, \qquad X \to \infty.$$

Remark. Park, Poonen, Voight and Wood [15] have formulated an analogous (but less precise) conjecture for the family of all elliptic curves over the rationals, ordered by height.

4. Variant of Delaunay's asymptotic formula. Let $M^*(T) := \frac{1}{T^*} \sum |Ш(E_d)|$, where the sum is over primes $d \leq T$, satisfying $(*)$ and $L(E_d, 1) \neq 0$, and T^* denotes the number of terms in the sum. Similarly, let $N^{**}(T) := \frac{1}{T^{**}} \sum |Ш(E_d)|$, where the sum is over positive cube-free integers $d \leq T$, satisfying $(*)$ and $L(E_d, 1) \neq 0$, and T^{**} denotes the number of terms in the sum. Let $f(T) := \frac{M^*(T)}{T^{1/2}}$, and $g(T) := \frac{N^{**}(T)}{T^{1/2}}$. We obtain the following picture (Fig. 6).

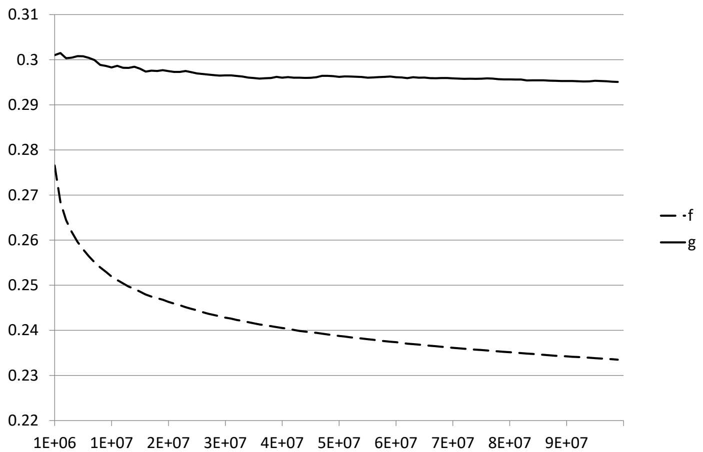

Fig. 6. Graphs of the functions $f(T)$ and $g(T)$.

Note the similarity to the predictions by Delaunay [8] for the case of quadratic twists of a given elliptic curve (and numerical evidence in [5], [6]), and to a variant of this phenomenon in the case of the family of Neumann–Setzer type elliptic curves [7].

5. Cohen–Lenstra heuristics for the order of Ш. Delaunay [9] has considered Cohen–Lenstra heuristics for the order of the Tate–Shafarevich group. He predicts, among others, that in the rank zero case the probability that $|Ш(E)|$ of a given elliptic curve E over $\mathbb{Q}$ is divisible by a prime p should be $f_0(p) := 1 - \prod_{j=1}^{\infty}(1 - p^{1-2j}) = \frac{1}{p} + \frac{1}{p^3} + \ldots$. Hence, $f_0(2) \approx 0.580577$, $f_0(3) \approx 0.360995$, $f_0(5) \approx 0.206660$, $f_0(7) \approx 0.145408$, and so on.

Let $F(X)$ denote the number of cube-free $d \le X$ satisfying $(*)$ and $L(E_d, 1) \neq 0$, and let $F_p(X)$ denote the number of such d's satisfying $p \mid \bigl|Ш(E_d)\bigr|$. Let $f_p(X) := \frac{F_p(X)}{F(X)}$. We obtain the following table (in the last row we restrict the computation to prime twists).

X	$f_2(X)$	$f_3(X)$	$f_5(X)$	$f_7(X)$	$f_{11}(X)$
10000000	0.4574860107	0.4528351278	0.0797229512	0.0365187357	0.0107055908
20000000	0.4667861427	0.4665902606	0.0856954224	0.0406883829	0.0126964802
30000000	0.4720389372	0.4743395107	0.0891666909	0.0430854869	0.0138608186
40000000	0.4755325884	0.4797263355	0.0916462006	0.0448302849	0.0147494390
50000000	0.4782835292	0.4838047688	0.0935546233	0.0461842060	0.0154253689
60000000	0.4804365024	0.4870412651	0.0950607348	0.0472714454	0.0160042804
70000000	0.4821166758	0.4897452073	0.0963909035	0.0482264317	0.0164998297
80000000	0.4836581573	0.4920588749	0.0974999561	0.0490436597	0.0169344117
90000000	0.4849849695	0.4940653891	0.0984979769	0.0497487127	0.0173190511
100000000	0.4861728066	0.4958441463	0.0993871375	0.0503845401	0.0176658729
100000000	0.5474977246	0.0713684943	0.1628461726	0.0993604813	0.0467913704

The numerical values of $f_3(X)$ exceed the expected value $f_0(3)$, but for $p \neq 3$ the values $f_p(X)$ seem to tend to $f_0(p)$; additionally restricting to prime twists tends to speed convergence to the expected values.

6. Distributions of $L(E_m, 1)$. It is a classical result (due to Selberg) that the values of $\log|\zeta(\frac{1}{2} + it)|$ follow a normal distribution.

Let E be any elliptic curve defined over $\mathbb{Q}$. Let $\mathcal{E}$ denote the set of all fundamental discriminants d with $(d, 2N_E) = 1$ and $\epsilon_E(d) = \epsilon_E \chi_d(-N_E) = 1$, where ϵ_E is the root number of E and $\chi_d = (d/\cdot)$. Keating and Snaith [12] have conjectured that, for $d \in \mathcal{E}$, the quantity $\log L(E_d, 1)$ has a normal distribution with mean $-\frac{1}{2}\log\log|d|$ and variance $\log\log|d|$.

Now we consider the case of cubic twists E_m of $E = X_0(27)$. Our data suggest that the values $\log L(E_m, 1)$ also follow an approximate normal distribution. Let $W_E = \{m \le 10^8 : m \text{ satisfies } (*)\}$, and $I_x = [x, x + 0.1)$ for $x \in \{-10, -9.9, -9.8, \ldots, 10\}$. We create histograms with bins I_x from the data $\bigl\{\bigl(\log L(E_m, 1) + \frac{1}{2}\log\log m\bigr)/\sqrt{\log\log m} : m \in W_E\bigr\}$. Below we present this histogram (Fig. 7).

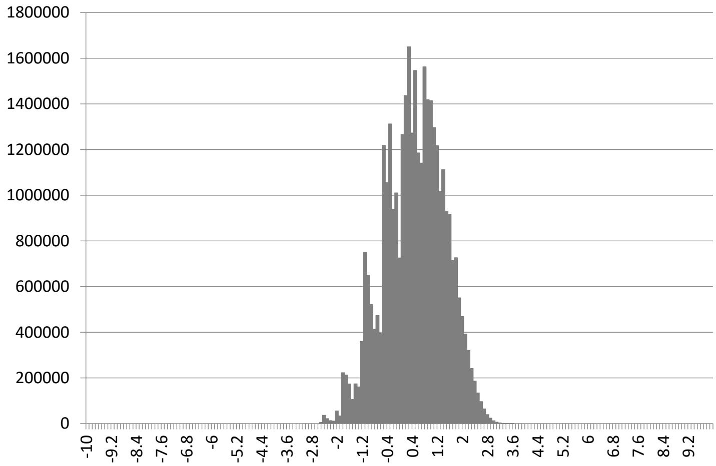

Fig. 7. Histogram of values $\left(\log L(E_m,1)+\frac{1}{2}\log\log m\right)/\sqrt{\log\log m}$ for $m\in W_E$.

7. Distribution of $|Ш(E_m)|$. It is an interesting question to find results (or at least a conjecture) on the distribution of the order of the Tate–Shafarevich group in a family of elliptic curves. It turns out that in the case of rank zero quadratic twists E_d of a fixed elliptic curve E the values of $\log(|Ш(E_d)|/\sqrt{d})$ are the natural ones to consider (compare the numerical experiments in [5], [6]). We also have a good conjecture for a family of rank zero Neumann–Setzer type elliptic curves [7].

Now let us consider the family E_m of cubic twists of the Fermat curve $E=X_0(27)$. In this case we will create histograms for the values $\log(|Ш(E_m)|/\sqrt[t]{m})$, $t=2,3$, separately. Let $W_E=\{m\le 10^8 : m \text{ satisfies } (*)\}$ and $I_x=[x,x+0.1)$ for $x\in\{-10,-9.9,\dots,10\}$.

Below (Figures 8 and 9) we create these histograms with bins I_x from the data $\left\{\left(\log(|Ш(E_m)|/\sqrt[t]{m})+\frac{1}{2}\log\log m\right)/\sqrt{\log\log m} : m\in W_E\right\}$.

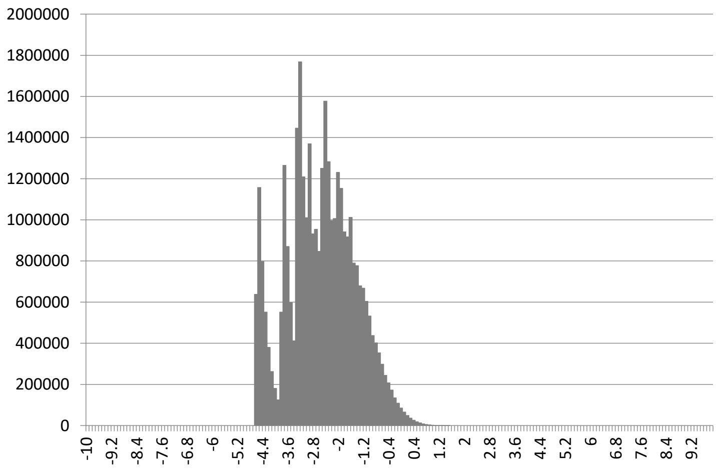

Fig. 8. Histogram of values $\left(\log(|Ш(E_m)|/\sqrt{m})+\frac{1}{2}\log\log m\right)/\sqrt{\log\log m}$ for $m\in W_E$.

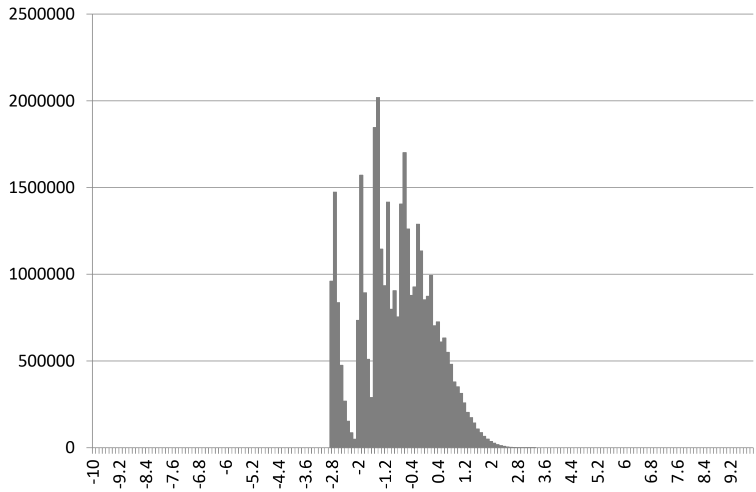

Fig. 9. Histogram of values $\left(\log(|Ш(E_m)|/\sqrt[3]{m}) + \frac{1}{2}\log\log m\right)/\sqrt{\log\log m}$ for $m \in W_E$.

8. Observations concerning the class numbers of real quadratic fields. Consider a real quadratic field $K = \mathbb{Q}(\sqrt{d})$ (d a positive square-free integer); let $h(d)$ denote its class number. We calculated the values $h(d)$ for all positive square-free integers $d \le 3\cdot 10^{10}$. Our observations suggest that $h(d)$'s behave in a way similar to the orders of Tate–Shafarevich groups in some families of rank zero elliptic curves (i.e. quadratic or cubic twists of a given one).

Let $h(k, X)$ denote the number of positive square-free integers $0 < d \le X$ such that $h(d) = k$. Let $H(k, X) := \frac{h(1,X)}{h(k,X)}$. We obtain the following graphs of the functions $H(k, X)$ for $2 \le k \le 10$ (Fig. 10).

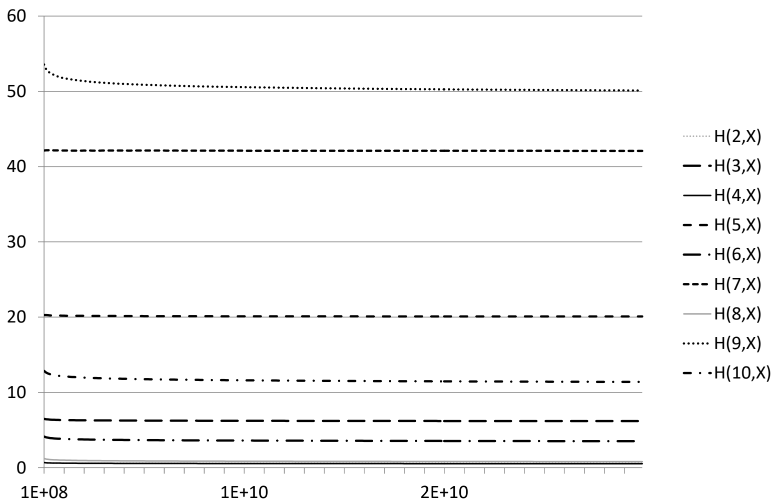

Fig. 10. Graphs of the functions $H(k, X)$ for $2 \le k \le 10$.

Now let us consider graphs of the functions $h(1,X)/(X^{5/6}(\log X)^r)$, $r=0,1$ (Fig. 11).

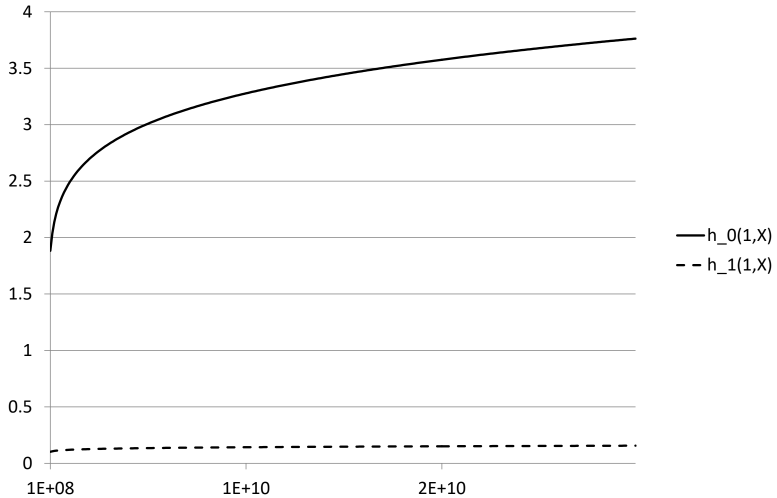

Fig. 11. Graphs of the functions $h_r(1,X) := h(1,X)/(X^{5/6}(\log X)^r)$, $r=0,1$.

The above calculations suggest the following (optimistic) conjecture.

Conjecture 3. *For any positive integer k there are positive constants r_k, s_k such that*

$$h(k,X) \sim r_k X^{5/6}(\log X)^{s_k}, \qquad X \to \infty.$$

Remark. The Gauss' class-number one problem for real quadratic fields states that there are infinitely many real quadratic fields with trivial ideal class group. It is still an open problem; note that it is not even known if there are infinitely many number fields with a given class number. Therefore the above conjecture is a highly optimistic version of these open questions.

References

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

[2] J. Coates, Y. Li, Y. Tian, S. Zhai, *Quadratic twists of elliptic curves*, Proc. Lond. Math. Soc. (3) 110 (2015), 357–394.

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

[4] J. B. Conrey, J. P. Keating, M. O. Rubinstein, N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, in: Number Theory for the Millennium, I (Urbana, IL, 2000), 301–315.

[5] A. Dąbrowski, T. Jędrzejak, 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. Stat. 188, Springer, Cham, 2016, 125–159.

[6] A. Dąbrowski, L. Szymaszkiewicz, *Behaviour of the order of Tate–Shafarevich groups for the quadratic twists of elliptic curves*, arXiv: 1611.07840.

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

[8] C. Delaunay, *Moments of the orders of Tate–Shafarevich groups*, Int. J. Number Theory 1 (2005), 243–264.

[9] C. Delaunay, *Heuristics on class groups and on Tate–Shafarevich groups: the magic of the Cohen–Lenstra heuristics*, in: Ranks of Elliptic Curves and Random Matrix Theory, London Math. Soc. Lecture Ser. 341, Cambridge Univ. Press, Cambridge, 2007, 323–340.

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

[11] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225–320.

[12] J. P. Keating, N. C. Snaith, *Random matrix theory and $\zeta(1/2+it)$*, Comm. Math. Phys. 214 (2000), 57–89.

[13] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш(E,\mathbb{Q})$ for a class of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522–540; English transl.: Math. USSR Izv. 32 (1989), 523–541.

[14] The PARI Group, PARI/GP version 2.7.2, Bordeaux, 2014, pari.math.u-bordeaux.fr/.

[15] J. Park, B. Poonen, J. Voight, M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, www-math.mit.edu/~poonen/papers/bounded-ranks.pdf.

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

[17] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. 103 (1991), 25–68.

[18] Ch. Skinner, E. Urban, *The Iwasawa main conjectures for GL_2*, Invent. Math. 195 (2014), 1–277.

[19] M. Watkins, *Rank distributions in a family of cubic twists*, in: Ranks of Elliptic Curves and Random Matrix Theory, London Math. Soc. Lecture Ser. 341, Cambridge Univ. Press, Cambridge, 2007, 237–246.

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