

Numerical Investigations Related to the Derivatives of the L -Series of Certain Elliptic Curves

C. Delaunay and S. Duquesne

CONTENTS

- 1. Introduction and Motivations
 - 2. Elliptic Curves Associated to Simplest Cubic Fields
 - 3. Numerical Results
 - 4. Nontrivial Tate-Shafarevich Groups of Curves with Rank 3 and 5
- Acknowledgments
References

In [Zagier and Kramarz 87], the authors computed the critical value of the L -series of the family of elliptic curves $x^3 + y^3 = m$ and they pointed out some numerical phenomena concerning the frequency of curves with a positive rank and the frequency of occurrences of the Tate-Shafarevich groups III in the rank 0 case (assuming the Birch and Swinnerton-Dyer conjecture). In this paper, we give a similar study for the family of elliptic curves associated to simplest cubic fields. These curves have a nonzero rank and we discuss the density of curves of rank 3 that occurs. We also remark on a possible positive density of nontrivial Tate-Shafarevich groups in the rank 1 case. Finally, we give examples of curves of rank 3 and 5 for which the group III is nontrivial.

1. INTRODUCTION AND MOTIVATIONS

Let E be an elliptic curve defined over \mathbb{Q} . From the work of [Wiles 95], [Taylor and Wiles 95], and [Breuil et al. 2001], E is known to be modular. This implies that its L -function $L(E, s)$ can be analytically continued to the whole complex plane. Furthermore, if N is the conductor of E , then the following functional equation holds:

$$\Lambda(E, 2 - s) = \varepsilon \Lambda(E, s), \quad (1-1)$$

where $\varepsilon = \pm 1$ is the sign of the functional equation and

$$\Lambda(E, s) = \left(\frac{\sqrt{N}}{2\pi} \right)^s \Gamma(s) L(E, s).$$

In this paper, we are interested in computing the analytic order of the Tate-Shafarevich group III of certain elliptic curves E defined over \mathbb{Q} using the Birch and Swinnerton-Dyer (BSD) conjecture:

Conjecture 1.1. (Birch and Swinnerton-Dyer.) *Let r denote the rank of the Mordell-Weil group $E(\mathbb{Q})$. We have*

$$\lim_{s \rightarrow 1} \frac{L(E, s)}{(s-1)^r} = \frac{c \Omega R}{|E(\mathbb{Q})_{tors}|^2} |\text{III}|, \quad (1-2)$$

2000 AMS Subject Classification: Primary 11G40;
Secondary 11Y35, 15A52

Keywords: Elliptic curves, simplest cubic fields, analytic rank, Tate-Shafarevich group, L -series

where c denotes the product of the Tamagawa numbers, Ω the real period, and R the regulator of E .

In [Zagier and Kramarz 87], Kramarz and Zagier carried out some numerical computations related to the family of elliptic curves given by equations $x^3 + y^3 = m$ (the so-called Sylvester cubics). They computed the critical value of the L -functions of the curves having an even functional equation (i.e., $\varepsilon = 1$) for $m \leq 70000$ and they pointed out some numerical phenomena concerning the frequency of curves with a positive rank and the frequencies of occurrences of $|\text{III}|$ in the rank 0 case (with Formula (1–2)). More precisely, concerning the rank, their numerical data suggest a possible positive density of curves with positive rank. In [Watkins 00], Watkins extended the computations to $m = 10^7$, the results being that the density of positive rank is finally decreasing and probably tends to zero like $x/(x^{5/6} \log(x)^C)$ (with some constant $C \approx 3/5$). The behaviour $x^{5/6}$ was already mentioned in [Zagier and Kramarz 87], and stronger models using random matrix theory as in [Conrey et al. 00] should give $x^{5/6} \log(x)^C$ for some constant C .

Watkins computations confirm the remark on Kramarz and Zagier that the frequency of occurrences of $|\text{III}| = 1$, $|\text{III}| = 4$, etc. among rank 0 curves is decreasing. Heuristics in [Delaunay 01] predict that these frequencies should be 0 (but note that these heuristics predict a general behaviour for all elliptic curves and that we are only concerned here with very specific families). Furthermore, the numerical results of Watkins about the question of how often a given prime p divides $|\text{III}|$ seem to be not too much discordant with the predictions in [Delaunay 01] (at least for $p \neq 3$).

Here, we make a similar experimental study, but in the case of a family of elliptic curves with positive rank. It is quite natural and interesting to wonder if the same phenomena will occur or not and, in fact, as far as we know, there is no such study in the literature. In the case of positive rank, heuristics in [Delaunay 01] predict that there is a positive density of curves with a nontrivial Tate-Shafarevich group but, in practice, they are quite sparsely observed. For example, the tables of Cremona ([Cremona 03b]) found only 196 such curves among all elliptic curves of conductor less than 20000; furthermore all of these 196 curves have rank 1 and most of them have $\text{III} = 4$. Indeed, there are infinitely many rational points on such curves, so that it is more difficult to find p -adic points not corresponding to rational points. In fact, nontrivial Tate-Shafarevich groups appear for large conductors.

The problem of computing $|\text{III}|$ using Formula (1–2) when the rank is positive is much more complicated because on the one hand we have to determine the regulator R (in the rank-0 case, the regulator is simply $R = 1$) and on the other hand we have to deal with quite large conductors to be able to detect nontrivial III .

Here, we are concerned with the family of elliptic curves associated to the simplest cubic fields (see below) which were introduced by Shanks in [Shanks 74] and were studied by Washington ([Washington 1987]) and more recently in [Duquesne 01]. This family has properties interesting for our purpose. Each of these curves has an odd rank and an explicit generator so that the regulator is easily computable when the rank is 1. The conductor grows fast so that we can hope to find nontrivial Tate-Shafarevich groups. We compute, using the GP-Pari software ([PARI 02]), values of $L'(E, 1)$ for many of these curves and deduce from them and from Formula (1–2) analytic orders of Tate-Shafarevich groups for the rank-1 case. The methods we used are well known since we have to evaluate a rapidly converging series (see Formula (2–4)), and are explained in [Cohen 93] and [Cremona 97]. Furthermore, several GP-programs are available, for example, a program by Cremona and Womack ([Cremona and Womack]), which computes the derivatives of L -functions of elliptic curves or by Dokchitser ([Dokchitser 03]); this program deals with general L -function having a classical functional equation.

According to our numerical data, we first observe an experimental positive-like density of curves with high ranks. With regard to the above Zagier-Kramarz extension by Watkins, we must be careful; indeed, the fact that the growth of the regulator can be well estimated allows us to use the same argument-principle as in the case of the Sylvester cubics and it suggests that the density of curves with ranks ≥ 3 may tend to 0. We also discuss the density of occurrences of $|\text{III}|$ when the rank is 1 (with the same reticence as above). Finally, we find examples of nontrivial Tate-Shafarevich groups for some curves of rank 3 and 5 by computing $L^{(3)}(E, 1)$ and $L^{(5)}(E, 1)$.

2. ELLIPTIC CURVES ASSOCIATED TO SIMPLEST CUBIC FIELDS

In the sequel, m will always denote a positive integer such that the number $\Delta = m^2 + 3m + 9$ is square-free. Let E be the elliptic curve:

$$E : Y^2 = X^3 + mX^2 - (m + 3)X + 1. \quad (2-1)$$

The field defined by the polynomial of the right-hand side of (2-1) is said to be a simplest cubic field. These fields were introduced by Shanks in [Shanks 74].

In [Washington 1987], Washington studied these fields and deduced some properties of the related elliptic curves (2-1), including the following result:

Theorem 2.1. (Washington.) *The rank of the elliptic curve E is odd, assuming that the Tate-Shafarevitch group is finite.*

In [Duquesne 01], the second author studies the structure of the Mordell-Weil group of these curves, and in particular proves:

Theorem 2.2. *The Mordell-Weil group $E(\mathbb{Q})$ is torsion-free and the point $(0, 1)$ can always be taken as an element of a system of generators for $E(\mathbb{Q})$. In particular, if the rank of E is one, the point $(0, 1)$ generates $E(\mathbb{Q})$.*

Let us now write down the classical invariants attached to these curves. The discriminant of E is $16\Delta^2$; its j -invariant is 256Δ . Note that $16\Delta^2$ is the discriminant of (2-1) and is the minimal discriminant of E whereas Equation (2-1) does not give the minimal Weierstrass model. In fact, the minimal model is given by a slightly more complicated equation,

$$Y^2 = X^3 + \varepsilon X^2 - (3(k^2 + k + 1) + (2k + 1)\varepsilon) X + (2k + 1)(k^2 + k + 1) + k(k + 1)\varepsilon,$$

where $m = 3k + \varepsilon$ with $\varepsilon = \pm 1$ (if $\varepsilon = 0$, m does not define a simplest cubic field). Moreover, Tate’s algorithm also allows us to compute the conductor and the Tamagawa numbers:

	$m \equiv 0 \pmod{2}$	$m \equiv 1 \pmod{4}$	$m \equiv 3 \pmod{4}$
N	$16\Delta^2$	$8\Delta^2$	$4\Delta^2$
c	1	2	3

The table above shows that N is about m^4 and grows sufficiently quickly as mentioned in the introduction.

In our case, the BSD conjecture predicts that

$$L'(E, 1) = c \widehat{h}((0, 1)) S, \tag{2-2}$$

where \widehat{h} is the canonical height on E and is computed using GP-Pari, Ω is the real period of E (which is easily computable using the AGM method), and

$$S = \begin{cases} 0 & \text{if } \text{rank}(E) > 1, \\ |\text{III}| & \text{if } \text{rank}(E) = 1. \end{cases}$$

From the work of [Duquesne 01], one can see that $\widehat{h}((0, 1))$ behaves like $\log(m)$ and that $\Omega \simeq m^{-1/2} \log(m)$. Since, under GRH, $L'(E, 1) = O(m^\varepsilon)$, using Formula (2-2), we obtain

$$S = O(m^{1/2+\varepsilon}). \tag{2-3}$$

Furthermore, the value of $L'(E, 1)$ is computed by:

$$L'(E, 1) = 2 \sum_{n \geq 1} \frac{a_n}{n} \int_{\frac{2\pi n}{\sqrt{N}}}^{\infty} e^{-t} \frac{dt}{t}, \tag{2-4}$$

where $L(E, s) = \sum_{n \geq 1} a_n n^{-s}$.

Thus, we compute S using (2-2). From the well-known work of Gross and Zagier ([Gross and Zagier 86]) S is known to be a rational number. All the values that we find in our numerical calculations are near to perfect squares of integers as required by the BSD conjecture. This gives a check of our numerical computations.

3. NUMERICAL RESULTS

We computed S for all integers m less than 14000 defining simplest cubic fields. For this, we need about $O(\sqrt{N})$ coefficients in the right-hand side of Formula (2-4) to obtain a reasonable accuracy for $L'(E, 1)$. Since the conductor grows as m^4 , we were led to consider sums with about m^2 terms (and so sums with about 2×10^8 terms for the largest values of m we considered). For this, the strategy that we used to get a sufficiently good approximation for $L'(E, 1)$ is the following (the same sort of strategy is used in [Zagier and Kramarz 87]):

- We compute and store the values of the coefficients a_n for n less than some bound B of the order of \sqrt{N} ($B = 1.67 \times 10^7$ for large values of m).
- We compute the partial sum in (2-4) using these first coefficients.
- Beyond B , we compute on the fly the coefficients a_n (if $n = n_1 n_2$ with $n_1, n_2 \leq B$, we can deduce a_n from a_{n_1} and a_{n_2}) and add their contributions to the sum. At each step, we add 10^6 new terms in the partial sum.
- We repeat the last step until two successive sums Σ_1 and Σ_2 satisfy:

$$|\Sigma_1 - \Sigma_2| < 0.02 \text{ and } |\Sigma_2 - s^2| < 0.02 \text{ for some } s \in \mathbb{Z}.$$

Note that for each prime p dividing the conductor, we have $p^2|N$. Thus, from the Atkin-Lehner theory ([Atkin and Lehner 70]), $(n, N) \neq 1 \Rightarrow a_n = 0$, and in particular, $a_n = 0$ if n is even. This remark is helpful for computations.

For large values of the parameter (say $m \geq 8000$), the computation of $L'(E, 1)$ requires a lot of time and memory. We needed several months of CPU time on a Pentium III at 1GHz to deal with the values of m less than 14000.

In order to give the numerical data that we obtained, we set

$$N(x) = \#\{m \leq x \mid m^2 + 3m + 9 \text{ is square-free}\},$$

$$N_s(x) = \#\{m \leq x \mid m^2 + 3m + 9 \text{ is square-free and } S_m = s\}.$$

The results are summarized in the following table:

x	2000	4000	6000	8000	10000	12000	14000
$N(x)$	1246	2492	3739	4986	6234	7477	8722
$N_0(x)$	363	700	1031	1347	1681	2026	2328
$N_1(x)$	728	1384	2025	2677	3267	3828	4402
$N_4(x)$	101	235	389	522	703	868	1035
$N_9(x)$	45	141	227	326	427	540	674
$N_{16}(x)$	5	19	42	67	91	116	150
$N_{25}(x)$	3	11	17	32	46	72	97
$N_{36}(x)$	1	2	7	13	13	15	21
$N_{49}(x)$			1	1	3	7	9
$N_{64}(x)$					1	2	3
$N_{81}(x)$				1	2	3	3

3.1 Density of High Rank Curves

The discussion we give here is founded on experimental data; several interpretations are possible, so we must be careful that the behaviour of the curves for $m \leq 14000$ may not mirror the general one when m tends to ∞ (as is the case for the Zagier-Kramarz computations). A first approach concerning the frequency of occurrences of curves with $L'(E, 1) = 0$ (and so of curves with rank ≥ 3) suggests that there is a positive density of such curves. Indeed, as it can be seen in Figure 1, the ratio $N_0(x)/N(x)$ is fairly nearly constant (the constant being ≈ 0.27).

Such an observation should provide, as asked in [Zagier and Kramarz 87], an example of a family of curves with an expected positive density of curves with high rank. Note that in the case of the simplest cubic fields, and contrary to the Fermat cubics, the curves are not isomorphic over any number field (their j -invariant is not constant). We should compare this 27% of extra-rank curves

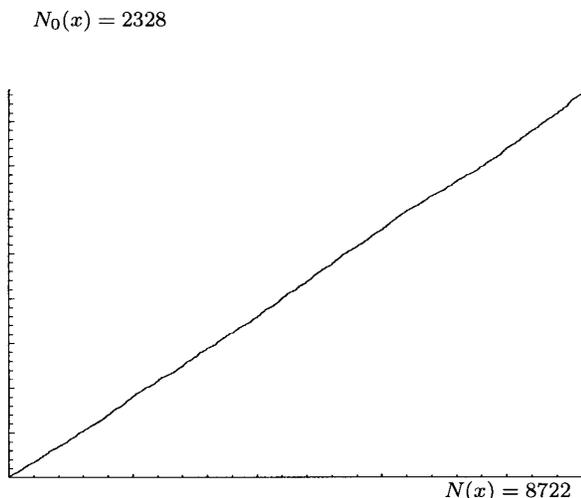


FIGURE 1. The points $(N(x), N_0(x))$ (and joined).

we obtained with the large table of Stein and Watkins in [Stein and Watkins 02] extending the Brumer-McGuinness one ([Brumer and McGuinness 90]) and for which 92.5% of their curves with odd functional equation have rank 1 (their database contains million of curves, and their conductors do not exceed 10^{10}). In fact, one of the current opinions about the rank of elliptic curves is that asymptotically, the rank is the lowest one compatible with the sign of the functional equation ([Brumer and McGuinness 90]). So, it would be very surprising if a positive density really occurs for our family.

Thanks to the estimate of Formula (2–3), we can adapt the argument of Zagier and Kramarz: Assuming S is, in fact, a random perfect square between 0 and \sqrt{m} for each value of m , then the number of curves with $m \leq x$ that have rank greater than 1 should be about $x^{3/4}$. Moreover, a naïve extension of the conjecture [Conrey et al. 00] to our case should provide the more precise estimate $x^{3/4} \log(x)^C$ for some constant C . However, it does not seem obvious how to extend the work of [Conrey et al. 00] to the derivatives of L -functions even if, as in our case, the regulator can be well estimated. The interpretation above is corroborated by taking the best linear fit to a log-log graph of Figure 1. We find thus that the number of curves with $m < x$ that have rank greater than 1 appear to grow like $x^{0.967}$, which is close enough to $x^{3/4} \log(x)^{0.91}$ when $x \leq 14000$.

3.2 Frequency of Occurrences of S

We also compute the frequency of occurrences of each analytic order of Tate-Shafarevich groups among curves

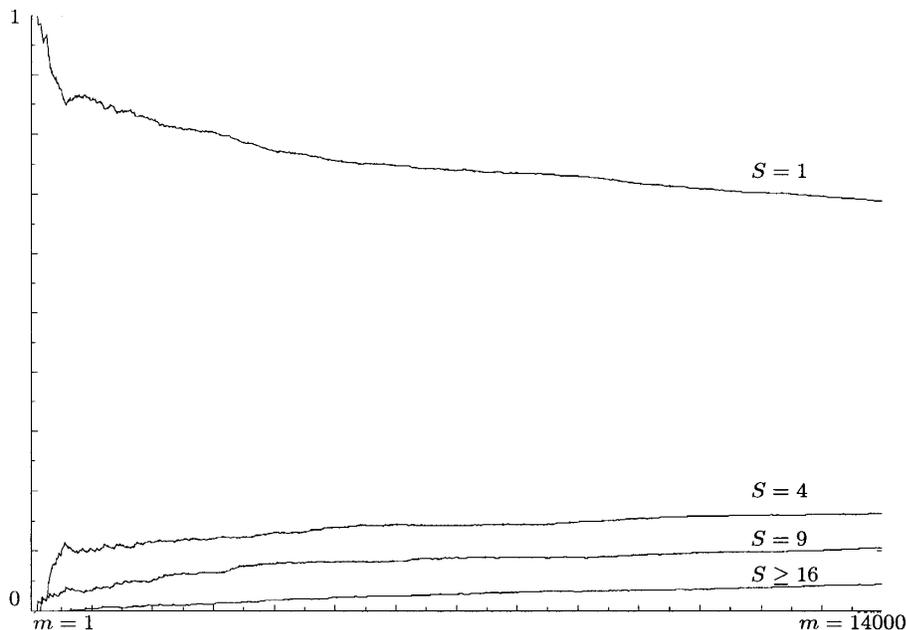


FIGURE 2. Frequencies of occurrence of S .

of (analytic) rank 1. Figure 2 illustrates the results that we obtained.

Although we cannot produce sufficient data, we seem to have a positive density for each order. This is in accordance with the heuristics in [Delaunay 01]. However, the densities could differ from the predicted ones since we only consider a specific family of elliptic curves. For instance, 68.8% (respectively, 18.9%, 10.9%) of rank 1 curves with $m \leq 14000$ have trivial III (respectively, have 2 dividing S , have 3 dividing S) whereas [Delaunay 01] would predict 54.9% (respectively, 31.1%, respectively, 12.3%).

Furthermore, the same heuristic argument as for $S = 0$ could also be used here and predicts that $N_S(x)/(N(x) - N_0(x))$ should tend to zero like $x^{-1/4}$ and so clashes with the heuristics and seems to be discordant with our numerical data.

Arithmetic effects on m could also modify the frequencies we considered. In view of the invariants of E , it is natural to fit m into three cases: m even, $m \equiv 1 \pmod 4$, and $m \equiv 3 \pmod 4$ (in fact, other cases were considered as Δ prime for example, but gave nearly the same results as in the general case). We sum up the results for all curves with $m \leq 14000$ in the following table. It follows from the data that the densities are, as in the general case, nearly constant for $m \leq 14000$, but depend on the class of m .

m	$\#\{S = 0\}$	$\#\{S = 1\}$	$\#\{S = 4\}$	$\#\{S = 9\}$	$\#\{S \geq 16\}$
$\equiv 0 \pmod 2$	964	2040	628	490	239
$\equiv 1 \pmod 4$	649	1133	256	110	32
$\equiv 3 \pmod 4$	715	1229	151	74	12

For $m \equiv 0 \pmod 2$ (respectively, $m \equiv 1 \pmod 4$, $m \equiv 3 \pmod 4$), there are about 22.1% (respectively, 29.7%, 32.7%) of elliptic curves with $S = 0$. This difference could be explained by the fact that Formula (2-2) and the invariant c force S to be smaller when m is odd, and so S is more often equal to 0 or 1 in this case. We also remark that all parametrizations of [Duquesne 01], in order to have elliptic curves with large rank, give odd values of m .

4. NONTRIVIAL TATE-SHAFAREVICH GROUPS OF CURVES WITH RANK 3 AND 5

Among the 27% of our curves of rank 3 or more, we find some curves of analytic rank 3 with nontrivial Tate-Shafarevich group. For this, we use Conjecture 1.1 and compute $L'''(E, 1)$ by the method of Buhler, Gross, and Zagier ([Buhler et al. 85]).

The first example of rank greater than 1 for which the program `mwrnk` of Cremona ([Cremona 03a]) is not able to determine the rank completely is obtained with $m = 157$. As `mwrnk` uses a 2-descent, this suggests a

nontrivial 2-part in the Tate-Shafarevich group. In order to compute the regulator, we check that the points

$$P_1 = [-12, 151], P_2 = [0, 1], \text{ and } P_3 = [3, 31]$$

form a basis for $E(\mathbb{Q})$ using Siksek's method ([Siksek 95]). Finally, we get $|\text{III}| = 4$, thus providing a nontrivial Tate-Shafarevich group for an elliptic curve of rank 3 (assuming BSD). Other such examples are given by $m = 617, 830, 856, 943, 961$.

We can also obtain similar results for rank 5. In this case, the first value for which the `mwrnk` program does not seem to determine the rank completely is $m = 3461$. Thus, this suggests a nontrivial 2-part. Indeed, we can check that the points

$$[0, 1], [-4, 263], [-40, 2369], [-124, 7193],$$

and

$$\left[\frac{-12}{169}, \frac{35725}{2197} \right]$$

give a basis for $E(\mathbb{Q})$ and that $|\text{III}| = 4$ (under BSD).

ACKNOWLEDGMENTS

We are very grateful to the anonymous referees for their comments and suggestions which improved this paper. We are very pleased to thank them here.

REFERENCES

- [Atkin and Lehner 70] A. O. L. Atkin and J. Lehner. "Hecke Operators on $\Gamma_0(N)$." *Math. Ann.* 185 (1970), 134–160.
- [PARI 02] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. GP-Pari. Available from World Wide Web (<http://www.math.u-psud.fr/~belabas/pari/>), 2002.
- [Buhler et al. 85] J. Buhler, B. Gross, and D. Zagier. "On the Conjecture of Birch and Swinnerton-Dyer for an Elliptic Curve of Rank 3." *Math. Comp.* 44:170 (1985), 473–481.
- [Breuil et al. 2001] 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.* 14:4 (2001), 843–939 (electronic).
- [Brumer and McGuinness 90] A. Brumer and O. McGuinness. "The Behaviour of the Mordell-Weil group of Elliptic Curves." *Bull. Amer. Soc.* 23:2 (1990), 375–382.
- [Cohen 93] H. Cohen. *A Course in Computational Algebraic Number Theory*, Fourth corrected printing, Graduate Texts in Math., 138. New York: Springer-Verlag, 2000.
- [Conrey et al. 00] J. Conrey, J. Keating, M. Rubinstein, and N. Snaith. "On the Frequency of Vanishing of Quadratic Twists of Modular L -Functions." In *Number Theory for the Millennium, I*, pp. 301–315. Natick, MA: A K Peters, Ltd., 2002.
- [Cremona 97] J. Cremona. *Algorithms for Modular Elliptic Curves*, Second edition. Cambridge, UK: Cambridge University Press, 1997.
- [Cremona 03a] J. Cremona. `mwrnk`. Available from World Wide Web (<http://www.maths.nott.ac.uk/personal/jec/>), 2003.
- [Cremona 03b] J. Cremona. "Elliptic Curve Data for Conductors up to 20000." Available from World Wide Web (<http://www.maths.nott.ac.uk/personal/jec/>), 2003.
- [Cremona and Womack] J. Cremona and T. Womack. Buhler-Gross Algorithm for Computing L -Series Derivatives. Available from World Wide Web (<http://www.maths.nott.ac.uk/personal/pmxtow/BG.gp>).
- [Delaunay 01] C. Delaunay. "Heuristics on Tate-Shafarevich Groups of Elliptic Curves Defined over \mathbb{Q} ." *Exp. Math.* 10:2 (2001), 191–196.
- [Dokchitser 03] T. Dokchitser. `computeL`. Available from World Wide Web (<http://maths.dur.ac.uk/~dma0td/computel/>), 2003.
- [Duquesne 01] S. Duquesne. "Integral Points on Elliptic Curves Defined by Simplest Cubic Fields." *Exp. Math.* 10:1 (2001), 91–102.
- [Gross and Zagier 86] B. Gross and D. Zagier. "Heegner Points and Derivatives of L -series." *Invent. Math.* 84, (1986), 225–320.
- [Shanks 74] D. Shanks. "The Simplest Cubic Fields." *Math. Comp.* 28 (1974), 1137–1152.
- [Siksek 95] S. Siksek. "Infinite Descent on Elliptic Curves." *Rocky Mountain Journal of Math.* 25:4 (1995), 1501–1538.
- [Stein and Watkins 02] W. Stein and M. Watkins. "A Database of Elliptic Curves — First Report." In *ANTS-V*, LNCS 2369, pp. 267–275. Berlin: Springer-Verlag, 2002.
- [Taylor and Wiles 95] R. Taylor and A. Wiles. "Ring-Theoretic Properties of Certain Hecke Algebras." *Ann. of Math. (2)* 141:3 (1995), 553–572.
- [Washington 1987] L. C. Washington. "Class Numbers of the Simplest Cubic Fields." *Math. Comp.* 48:177 (1987), 371–384.
- [Watkins 00] M. Watkins. "Rank Distribution of Cubic Twists." Preprint. Available from World Wide Web (www.math.psu.edu/watkins/zk.dvi), 2000.
- [Wiles 95] A. Wiles. "Modular Elliptic Curves and Fermat's Last Theorem." *Ann. of Math. (2)* 141:3 (1995), 443–551.
- [Zagier and Kramarz 87] 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.

Christophe Delaunay, École Polytechnique Fédérale de Lausanne, Faculté des sciences de Base, CSAG,
1015 Lausanne, Switzerland (christophe.delaunay@epfl.ch)

Sylvain Duquesne, Département des Sciences Mathématiques, Université Montpellier II - Case Courrier 051,
Place Eugène Bataillon, 34095 Montpellier cedex 5, France (duquesne@math.univ-montp2.fr)

Received September 19, 2002; accepted in revised form September 16, 2003.