Heuristics on Tate–Shafarevitch Groups of Elliptic Curves Defined over $\mathbb{Q}$

Christophe Delaunay

CONTENTS

In a well-known paper, Cohen and Lenstra gave conjectures on class groups of number fields. We give here similar conjectures for Tate–Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. For such groups (if they are finite), there exists a nondegenerate, alternating, bilinear pairing. We give some properties of such groups and then formulate heuristics which allow us to give precise conjectures.

1. INTRODUCTION

We make a study of Tate–Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$ similar to the one made in [Cohen and Lenstra 1984] of class groups of number fields. Part of our motivation is the deep analogy that exists between these groups.

In this paper, we will assume the truth of the conjecture asserting that the Tate–Shafarevitch group Ш of an elliptic curve over $\mathbb{Q}$ is finite. Under this conjecture, there exists a nondegenerate, alternating, bilinear pairing

$$\beta : Ш \times Ш \to \mathbb{Q}/\mathbb{Z};$$

see [Silverman 1986], for example. We will say that a pair (G, β) is a group of type S if G is a finite abelian group and β is a nondegenerate alternating bilinear pairing $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$. We will also have to consider isomorphism classes of groups of type S, where two groups (G_1, β_1) and (G_2, β_2) of type S are said to be isomorphic if there exists an isomorphism $\sigma : G_1 \to G_2$ such that $\beta_2(\sigma(x), \sigma(y)) = \beta_1(x, y)$ for all $x, y \in G_1$.

In [Cohen and Lenstra 1984], the groups considered are simply finite abelian groups, and the main idea is to give each group G a weight proportional to $1/|\mathrm{Aut}\, G|$. Here we must replace $\mathrm{Aut}\, G$ by its analog $\mathrm{Aut}^s\, G$, the group of automorphisms of (G, β) that preserve β.

1058-6458/2001 \$0.50 per page

We will use the following notation: $\sum_{G^s(n^2)}$ is as an abbreviation for a sum over all isomorphism classes of groups (G,β) of type S of order n^2. We denote by $\mathbb{P}$ the set of prime numbers and, for $p \in \mathbb{P}$, we denote by $r_p(G)$ the p-rank of G. If (G,β) is a group of type S, we define

$$w^s(G) = \frac{1}{|\mathrm{Aut}^s G|},$$
$$w_a^s(G) = \frac{1}{|\mathrm{Aut}^s G|} \prod_{p||G|} \frac{(1/p^2)_a}{(1/p^2)_{a-r_{p(G)/2}}},$$

where $(q)_a = \prod_{1\le i\le a}(1-q^i)$ for $a \in \mathbb{N}\cup\{\infty\}$. Finally, we set $w^s(n^2) = \sum_{G^s(n^2)} w^s(G)$ and $w_a^s(n^2) = \sum_{G^s(n^2)} w_a^s(G)$, and note that $w_a^s(G)$ tends to $w^s(G)$ when a tends to infinity.

We give some properties of groups of type S. We start with an example. Let

$$G = (\mathbb{Z}/p^{a_1}\mathbb{Z} \oplus \mathbb{Z}/p^{a_1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{a_2}\mathbb{Z} \oplus \mathbb{Z}/p^{a_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{a_j}\mathbb{Z} \oplus \mathbb{Z}/p^{a_j}\mathbb{Z}),$$

with $a_1 \le a_2 \le \cdots \le a_j$. Denote by $e_1, e_2, \ldots, e_{2j}$ a "canonical basis" (for example the i-th component of e_i is taken to be invertible mod p, and the others are taken equal to zero). Define β on this basis by:

$$\beta(e_{2i-1}, e_{2i}) = -\beta(e_{2i}, e_{2i-1}) = 1/p^{a_i} \in \mathbb{Q}/\mathbb{Z},$$
$$\beta(e_i, e_j) = 0 \quad \text{elsewhere}.$$

Then (G,β) is a group of type S. Hence, if a finite group G is isomorphic to $H \times H$ for a suitable group H, we can define, as above, a nondegenerate, alternating, bilinear pairing (the p-components of (G,β) are orthogonal). We now show the converse.

Lemma 1. *Let (G,β) be a p-group of type S, and let $x \in G$ be an element of maximal order, say p^k. Then:*

- *There exists $y \in G$ of order p^k with $\beta(x,y) = 1/p^k \in \mathbb{Q}/\mathbb{Z}$.*
- *There exists a subgroup H of G with $(H, \beta|_{H\times H})$ of type S, such that $G = (\langle x\rangle \oplus \langle y\rangle) \oplus^\perp H$, where $\oplus^\perp$ denotes an orthogonal direct sum.*

Proof. The element y exists because β is nondegenerate. We can then set

$$H = \{z \in G : \beta(x,z) = \beta(y,z) = 0\}. \qquad \square$$

By induction on the order of the group, this lemma allows us to prove the following proposition.

Proposition 2. *If (G,β) is a p-group of type S, then (G,β) is isomorphic to the group of the example given above, for appropriate (a_i). In particular, $G \simeq H \times H$ and the structure of $\mathrm{Aut}^s G$ is independent of β.*

Recall that abelian groups of order p^n are in one-to-one correspondence with partitions of n. If (ν) is a partition of n, we denote by λ_i the number of occurrences of i in (ν). Clearly

$$n = \lambda_1 + 2\lambda_2 + \cdots + j\lambda_j,$$

where j is the largest integer with $\lambda_j \ne 0$.

Further, we denote by $\mu_1, \mu_2, \ldots, \mu_j$ the parts of the associated partition of n defined by $\mu_k = \lambda_k + \lambda_{k+1} + \cdots + \lambda_j$. Clearly $n = \mu_1 + \mu_2 + \cdots + \mu_j$.

Theorem 3. *Let (G,β) be a group of type S of order p^{2n} with $G \simeq H \times H$ and*

$$H = (\mathbb{Z}/p)^{\lambda_1} \oplus (\mathbb{Z}/p^2)^{\lambda_2} \oplus \cdots \oplus (\mathbb{Z}/p^j)^{\lambda_j}.$$

Then, with the preceding notation,

$$|\mathrm{Aut}^s G| = p^{2(\mu_1^2+\cdots+\mu_j^2)+n} \prod_{1\le i\le j} \left(\frac{1}{p^2}\right)_{\lambda_i}.$$

Proof. We reason by induction on n. Let $e_1, e_2, \ldots$ be a "canonical basis" with e_1, e_2 of order p^j. Take e_1 and e_2 to be the elements of G with 1 on the last and penultimate components, respectively, and zero elsewhere. Let β be the pairing of the example. An automorphism g is given by the image of a basis. Let x be the image of e_1. There exist $p^{2n}(1-1/p^{2\lambda_j})$ possibilities for x, this being the number of elements of order p^j in G. If z is the image of e_2, we must have $\beta(x,z) = 1/p^j$. Writing

$$G = (\langle x\rangle \oplus \langle y\rangle) \oplus^\perp H,$$

we deduce that there are p^{2n-j} possibilities for $z = g(e_2)$.

Finally, note that $e_3, e_4, \ldots$ form a "canonical basis" of a group of type S which is isomorphic to $(H, \beta_{|H\times H})$ and that $g(e_3), g(e_4), \ldots$ must belong to H. So there are $|\mathrm{Aut}^s H|$ possibilities; we then use our induction hypothesis since $|H| < |G|$. $\square$

Remark. Taking $\lambda_1 = n$, we obtain the order of the symplectic group $S_p(2n,p)$.

2. DIRICHLET SERIES AND AVERAGES

Study of $w_a^s(n^2)$ and $w^s(n^2)$

Theorem 4. $\displaystyle\sum_{G^s(p^{2n})} w_a^s(G) = \frac{1}{p^{3n}} \frac{(1/p^2)_{n+a-1}}{(1/p^2)_{a-1}(1/p^2)_n}.$

Proof. In [Cohen and Lenstra 1984] we find the formula

$$\sum_{G(p^n)} \frac{1}{|\mathrm{Aut}\, G|} \frac{(1/p)_a}{(1/p)_{a-r_p(G)}} = \frac{1}{p^n} \frac{(1/p)_{n+a-1}}{(1/p)_{a-1}(1/p)_n},$$

where the sum is over all abelian groups of order p^n up to isomorphism. Furthermore, it is well-known (and can be proved as Theorem 3) that for a p-group G corresponding to (ν) we have

$$|\mathrm{Aut}\, G| = p^{\mu_1^2+\cdots+\mu_j^2} \prod_{1\le i\le j} \left(\frac{1}{p}\right)_{\lambda_i};$$

see [Hall 1938]. We deduce that

$$\sum_{(\nu)=n} \frac{(1/p)_n}{(1/p)_{a-r(\nu)}} \frac{(1/p)^{\mu_1^2+\cdots+\mu_j^2}}{(1/p)_{\lambda_1}\cdots(1/p)_{\lambda_j}} = \frac{1}{p^n} \frac{(1/p)_{n+a-1}}{(1/p)_{a-1}(1/p)_n},$$

where the sum is over all partitions (ν) of n and $r(\nu)$ is the number of parts in (ν). The above formula is in fact a formal identity. It follows that we can substitute p^2 for p and multiply by $1/p^n$, proving the theorem. $\square$

Corollary 5. $\displaystyle\sum_{G^s(n^2)} w_a^s(G) = \frac{1}{n^3} \prod_{p^\alpha \| n} \frac{(1/p^2)_{\alpha+a-1}}{(1/p^2)_{a-1}(1/p^2)_\alpha}.$

Letting a tend to ∞, we obtain:

Corollary 6. $\displaystyle\sum_{G^s(n^2)} \frac{1}{\mathrm{Aut}^s(G)} = \frac{1}{n^3} \prod_{p^\alpha \| n} \frac{1}{(1/p^2)_\alpha}.$

Definition 7. We define the functions ζ_a^s and ζ^s by the Dirichlet series

$$\zeta^s(z) = \sum_{n=1}^{\infty} \frac{w^s(n)}{n^z}, \quad \zeta_a^s(z) = \sum_{n=1}^{\infty} \frac{w_a^s(n)}{n^z},$$

with $w^s(n) = w_a^s(n) = 0$ if n is not a perfect square.

The next lemma can be proved by induction on a:

Lemma 8. *Let a be a nonnegative integer. Then*

$$\sum_{\beta=0}^{\infty} X^\beta \frac{(X)_{\beta+a}}{(X)_\beta (X)_a} Y^\beta = \prod_{j=1}^{a+1} \frac{1}{1-X^j Y}.$$

Remark. Letting a tend to ∞, we obtain a formula of Euler:

$$\sum_{\beta=0}^{\infty} \frac{X^\beta}{(X)_\beta} Y^\beta = \prod_{j=1}^{\infty} \frac{1}{1-X^j Y}.$$

Theorem 9. *We have:*

$$\zeta_a^s(z) = \sum_{n=1}^{\infty} \frac{w_a^s(n)}{n^z} = \prod_{j=1}^{a} \zeta(2z+2j+1),$$

$$\zeta^s(z) = \sum_{n=1}^{\infty} \frac{w^s(n)}{n^z} = \prod_{j=1}^{\infty} \zeta(2z+2j+1).$$

Proof. It is sufficient to prove the first formula, the second following by letting $a \to \infty$. We first write $\zeta_a^s(z) = \prod_p \sum_{\nu=0}^{\infty} p^{-2\nu z} w_a^s(p^{2\nu})$ and replace $w_a^s(p^{2\nu})$ by the formula of Theorem 4. We obtain

$$\zeta_a^s(z) = \prod_p \left(\sum_{\nu=0}^{\infty} \frac{1}{p^{2\nu}} \frac{(1/p^2)_{\nu+a-1}}{(1/p^2)_{a-1}(1/p^2)_\nu} \frac{1}{p^{\nu(2z+1)}} \right),$$

and we use Lemma 8 to conclude. $\square$

Averages

Let f be a complex-valued function defined on isomorphism classes of groups of type S.

Definition 10. Define

$$w^s(f, n^2) = \sum_{G^s(n^2)} w^s(G) f(G),$$

$$\zeta^s(f, z) = \sum_{n} \frac{w^s(f, n)}{n^z},$$

$$w_a^s(f, n^2) = \sum_{G^s(n^2)} w_a^s(G) f(G),$$

$$\zeta_a^s(f, z) = \sum_{n} \frac{w_a^s(f, n)}{n^z},$$

with $w^s(f,n) = w_a^s(f,n) = 0$ if n is not a perfect square. When $u \ge 0$, define $c_{a,u}(f,n)$ by

$$\sum_{n=1}^{\infty} \frac{c_{a,u}(f,n)}{n^z} = \frac{\zeta_a^s(f, z+u)\zeta_a^s(z)}{\zeta_a^s(z+u)}.$$

Definition 11. The (a,u)-*average of* f is defined by

$$M_{a,u}^s(f) = \lim_{x\to\infty} \frac{\sum_{n\le x} n c_{a,u}(f,n)}{\sum_{n\le x} n w_a^s(n)}.$$

If $a = \infty$, we will speak of the u-average of f, and we will write $M_u^s(f)$ instead of $M_{\infty,u}^s(f)$.

Remarks. This definition is analogous to that of the (a,u)-average in [Cohen and Lenstra 1984, Definition 5.1 and Proposition 5.4]. In particular, the (a,u)-average of f, if it exists, is an average (that is, the (a,u)-average of a constant function is equal to that constant).

If f is the characteristic function of a property P, we will speak of the (a,u)-probability of P or simply of the u-probability of P.

Important: we have included the factor n in the definition so that the denominator diverges as $x \to \infty$. Moreover, we can see that the average of f is unchanged (for a reasonable class of functions) if we replace n by n^l for $l \geq 1$. This is *not* true if we replace n by n^l for $l < 1$, in particular if we replace n by the constant 1.

We also need the following Tauberian theorem:

Proposition 12 [Tenenbaum 1995]. *Let $(c(n))_n$ be nonnegative real numbers. If $D(z) = \sum_n c(n)/n^z$ converges for $\operatorname{Re} z > 0$ and if $D(z) - C/z$ can be analytically continued to $\operatorname{Re} z \geq 0$, then*

$$\sum_{n \leq x} c(n) \sim C \log x.$$

Applying this to $\zeta_a^s(z-1)$ (i.e., to $c(n) = n w_a^s(n)$), we obtain

$$\sum_{n \leq x} n w_a^s(n) \sim \frac{\prod_{2 \leq k \leq a} \zeta(2k-1)}{2} \log x.$$

The Tauberian theorem immediately implies:

Proposition 13. *Let f be a nonnegative function defined on isomorphism classes of groups of type S. If $\zeta_a^s(f, z-1)$ converges for $\operatorname{Re} z > 0$ and $\zeta_a^s(f, z-1) - C/z$ can be analytically continued to $\operatorname{Re} z \geq 0$, then*:

1. *For $u = 0$,*

$$M_{a,0}^s(f) = \frac{2C}{\prod_{2 \leq k \leq a} \zeta(2k-1)} = \lim_{z \to 0} \frac{\zeta_a^s(f, z-1)}{\zeta_a^s(z-1)}.$$

2. *For $u \neq 0$, $M_{a,u}^s(f) = \dfrac{\zeta_a^s(f, u-1)}{\zeta_a^s(u-1)}$.*

For our applications, we need to be able to restrict our attention to $\mathcal{P}$-parts of groups of type S, where $\mathcal{P}$ is a set of prime numbers. For this, we denote by $f \circ \mathcal{P}$ the function $G \mapsto f(G_{\mathcal{P}})$, where $G_{\mathcal{P}}$ is the $\mathcal{P}$-part of G. We also write $\mathbb{N}_{\mathcal{P}} = \{n \in \mathbb{N} : p | n \Longrightarrow p \in \mathcal{P}\}$.

Proposition 14. *Let $\mathcal{P} \subset \mathbb{P}$ be a set of prime numbers. Then*

$$w_a^s(f \circ \mathcal{P}, n) = w_a^s(f, n_1) w_a^s(n_2),$$

where $n = n_1 n_2$ and n_1 is the $\mathcal{P}$-part of n. In particular, $\zeta_a^s(f \circ \mathcal{P}, z)$ equals

$$\left(\sum_{n \in \mathbb{N}_{\mathcal{P}}} \frac{w_a^s(f,n)}{n^z} \right) \prod_{p \notin \mathcal{P}} \prod_{k=1}^{a} \frac{1}{1 - (1/p)^{2z+2k+1}}.$$

Proof. Immediate consequence of the definitions. ☐

We now give some examples of averages, with follow from Propositions 13 and 14. For simplicity we assume $a = \infty$.

Example A. Let $\alpha \in \mathbb{R}$ and $u > \alpha$. The u-average of $|G|^\alpha$ is equal to

$$\frac{\prod_{j=1}^{\infty} \zeta(2u - 2\alpha + 2j - 1)}{\prod_{j=1}^{\infty} \zeta(2u + 2j - 1)}.$$

In particular, if $u \geq 2$, the u-average of $|G|$ equals $\zeta(2u-1)$.

Example B. Let L be a group of type S with L a $\mathcal{P}$-group. The u-probability that the $\mathcal{P}$-part of a group of type S is isomorphic to L is equal to

$$\frac{|L|^{1-u}}{|\operatorname{Aut}^s L|} \prod_{p \in \mathcal{P}} \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2u+2k-1}}\right).$$

Example C. Assume that all prime divisors p of n are in $\mathcal{P}$. The u-probability that the $\mathcal{P}$-part of a group of type S has cardinality equal to n is equal to

$$n^{1-u} w^s(n) \prod_{p \in \mathcal{P}} \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2u+2k-1}}\right).$$

Example D. The u-probability that $G_p \neq \{0\}$ is equal to

$$1 - \prod_{k=1}^{\infty} \left(1 - (1/p)^{2u+2k-1}\right).$$

Example E. The u-probability that the $\mathcal{P}$-part of a group of type S is isomorphic to the square of a cyclic group is

$$\prod_{p \in \mathcal{P}} \frac{1 - 1/p^2 + 1/p^{2u+3}}{(1 - 1/p^2)} \prod_{k=2}^{\infty} \left(1 - (1/p)^{2u+2k-1}\right).$$

In particular, when $\mathcal{P} = \mathbb{P}$ this probability equals

$$\prod_{p \in \mathbb{P}} (1 - 1/p^2 + 1/p^{2u+3}) \frac{\zeta(2)}{\zeta(2u+3)\zeta(2u+5)\zeta(2u+7)\dots}.$$

Averages Involving p-Ranks

We can also obtain results on the p-rank of a group of type S. For simplicity, we assume $a = \infty$ but the results can also be given for finite values of a.

Proposition 15. *Let α and r be two nonnegative integers with $r \le \alpha$. We have:*

$$\sum_{\substack{G^s(p^{2\alpha})\\ r_p(G)=2r}} w^s(G) = w^s(p^{2\alpha}) \times \frac{(1/p^2)_{\alpha-1}(1/p^2)_\alpha}{(1/p^2)_{r-1}(1/p^2)_r(1/p^2)_{\alpha-r}} p^{-2r^2+2r}.$$

Proof. We use exactly the same methods as in the proof of Theorem 4, using the formula of [Cohen and Lenstra 1984, Theorem 6.1]. □

Corollary 16. *Let $n \in \mathbb{Z}$ with $p^\alpha \| n$. Then:*

$$\sum_{\substack{G^s(n^2)\\ r_p(G)=2r}} w^s(G) = w^s(n^2) \times \frac{(1/p^2)_{\alpha-1}(1/p^2)_\alpha}{(1/p^2)_{r-1}(1/p^2)_r(1/p^2)_{\alpha-r}} p^{-2r^2+2r}.$$

Proof. Write $n = p^\alpha n_2$ and use the multiplicativity of w^s. □

Proposition 17. *Let r be a nonnegative integer. Then*

$$\sum_{G^s(p,2r)} \frac{w^s(G)}{|G|^z} = \frac{p^{-r(2r+2z+1)}}{(1/p^2)_r} \prod_{j=1}^{r} \frac{1}{1-1/p^{2z+2j+1}},$$

where the sum is over all p-groups (G, f) of type S with $r_p(G) = 2r$.

Proof. We write

$$\sum_{G^s(p,2r)} \frac{w^s(G)}{|G|^z} = \sum_{\alpha=0}^{\infty} \frac{1}{p^{2\alpha z}} \sum_{\substack{G(p^{2\alpha})\\ r_p(G)=2r}} w^s(G),$$

and we obtain the formula by using Proposition 15, Theorem 4 and Lemma 8. □

We thus obtain:

Example F. The u-probability that the p-rank of a group of type S is $2r$ equals

$$\frac{p^{-r(2u+2r-1)}}{(1/p^2)_r} \prod_{k=r+1}^{\infty} \left(1 - 1/p^{2u+2k-1}\right).$$

The next result is proved using [Cohen and Lenstra 1984, Theorem 6.4]:

Proposition 18. *If $\alpha \le \beta$ are two nonnegative integers, then*

$$\sum_{G^s(p^{2\beta})} w^s(G) \prod_{0 \le i < \alpha} \left(p^{r_p(G)} - p^{2i}\right) = \frac{w^s(p^{2\beta-2\alpha})}{p^\alpha}.$$

Corollary 19. *If n is a nonnegative integer with $p^\alpha | n$, then*

$$\sum_{G^s(n^2)} w^s(G) \prod_{0 \le i < \alpha} \left(p^{r_p(G)} - p^{2i}\right) = \frac{w^s(n^2/p^{2\alpha})}{p^\alpha}.$$

This corollary gives:

Example G. The 0-average of the function $p^{r_p(G)}$ is $1 + p$.

3. HEURISTICS ON TATE–SHAFAREVITCH GROUPS

Using the analogy between units of number fields and rational points on elliptic curves, we can now give a "Cohen–Lenstra"-type heuristic assumption for Tate–Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$, and deduce from them and the above results on groups of type S a number of conjectures on Tate–Shafarevitch groups. Let $\mathcal{E}_u$ be the set of isomorphism classes of elliptic curves E of rank u defined over $\mathbb{Q}$, which we assume to be ordered by the conductor $N(E)$. For a function f defined on isomorphism classes of groups of type S, we define

$$\omega_u(f, x) = \sum_{\substack{E \in \mathcal{E}_u\\ N(E) \le x}} f(\text{Ш}(E)), \quad \omega_u(x) = \sum_{\substack{E \in \mathcal{E}_u\\ N(E) \le x}} 1.$$

We can define an average of f by setting

$$M_u(f) = \lim_{x \to \infty} \frac{\omega_u(f, x)}{\omega_u(x)}.$$

The basic heuristic assumption is then the following:

Heuristic Assumption. $M_u(f) = M^s_{u/2}(f)$.

We now give some consequences of this assumption.

The Rank-Zero Case

The probability that Ш is isomorphic to the square of a cyclic group is

$$\prod_{p \in \mathbb{P}} (1 - 1/p^2 + 1/p^3) \frac{\zeta(2)}{\zeta(3)\zeta(5)\zeta(7)\ldots},$$

or approximately 0.977076. The probability that p divides $|\text{Ш}|$ is

$$f_0(p) = 1 - \prod_{k=1}^{\infty} \left(1 - (1/p)^{2k-1}\right).$$

In particular, $f_0(2) \simeq 0.580577$, $f_0(3) \simeq 0.360995$, and $f_0(5) \simeq 0.20666$.

We give here the probability that the p-part of Ш is isomorphic to a group G:

G/p	$(\mathbb{Z}/p\mathbb{Z})^2$	$(\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z})^2$	$(\mathbb{Z}/p^2\mathbb{Z})^2$
2	0.387	0.0129	0.1935
3	0.1354	0.00056	0.045

The probability that $r_p(\text{Ш}) = 2r$ is

$$\frac{p^{-r(2r-1)}}{(1/p^2)_r} \prod_{k=r+1}^{\infty} \left(1 - 1/p^{2k-1}\right).$$

The Rank-One Case

The probability that Ш is isomorphic to the square of a cyclic group is

$$\frac{1}{\zeta(12)} \prod_{k=4}^{\infty} \frac{1}{\zeta(2k)} \sim 0.99437$$

The probability that p divides $|\text{Ш}|$ is

$$f_1(p) = 1 - \prod_{k=1}^{\infty} \left(1 - (1/p)^{2k}\right).$$

In particular, $f_1(2) \simeq 0.31146$, $f_1(3) \simeq 0.12344$, and $f_1(5) \simeq 0.0416$.

Let L be a group of type S. The probability that Ш is isomorphic to L is

$$\frac{\sqrt{|L|}}{|\mathrm{Aut}^s L|} \frac{1}{\zeta(2)\zeta(4)\zeta(6)\dots}.$$

In particular, $|\text{Ш}| = 1$ with probability close to 0.54914.

A proof of the heuristic assumption (and of its consequences) is presently out of reach. It is also difficult to check numerically our conjectures, since nontrivial Tate–Shafarevitch groups seem to appear whenever the conductor is very large and tables of elliptic curves have been done "only" for $N \leq 6000$ [Cremona 1992]. Nevertheless, we make some comments that point toward the truth of the heuristic assumption above.

First, we note that the nature of the results are different according to the parity of the rank (in the sense that they involve values of the Riemann zeta function at odd positive integers or at even positive integers). This seems quite natural since elliptic curves can be naturally split into two parts according to the sign of the functional equation, in other words according to the parity of the rank if we assume the Birch and Swinnerton-Dyer conjecture. The conjectures also predict that the p-rank of a Tate–Shafarevitch group with a nontrivial p-part is often equal to 2. Indeed, all the nontrivial p-parts of Tate–Shafarevitch groups in Cremona's table have a p-rank equal to 2 [Cremona and Mazur 2000].

REFERENCES

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number theory* (Noordwijkerhout, 1983), edited by H. Jager, Lecture notes in Math. **1068**, Springer, Berlin, 1984.

[Cremona 1992] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, Cambridge, 1992. Second edition, 1997.

[Cremona and Mazur 2000] J. E. Cremona and B. Mazur, "Visualizing elements in the Shafarevich-Tate group", *Experiment. Math.* **9**:1 (2000), 13–28.

[Hall 1938] P. Hall, "A partition formula connected with Abelian groups", *Comment. Math. Helv.* **11** (1938), 126–129.

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

[Tenenbaum 1995] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, 2nd ed., Cours spécialisés **1**, Soc. math. France, Paris, 1995.

Christophe Delaunay, Université Bordeaux I, Laboratoire A2X, 351 Cours de la Libération, 33 405 Talence, France (delaunay@math.u-bordeaux.fr)

Received April 24, 2000; accepted in revised form October 10, 2000