Heuristics on class groups and on Tate-Shafarevich groups: The magic of the Cohen-Lenstra heuristics

Christophe Delaunay

When we have to study a number field or an elliptic curve defined over $\mathbb{Q}$, some groups may appear which make the explicit computations more complicated and which are, in a way, not very “welcome”. These groups are the class groups of number fields and the Tate-Shafarevich groups of elliptic curves. A direct study of their general behavior is a very difficult problem. In [3], Cohen and Lenstra explained how to obtain precise conjectures for this purpose using a general fundamental heuristic principle. In [6], it is shown how to adapt the Cohen-Lenstra idea to Tate-Shafarevich groups using the analogy between number fields and elliptic curves. Understanding the behavior of Tate-Shafarevich groups is important in itself first but it may also be useful for studying the distribution of the special values of the L-functions $L(E, s)$ attached to elliptic curves. Indeed, the Birch and Swinnerton-Dyer conjecture relates the value $L(E, 1)$ to natural invariants of E including the order of the Tate-Shafarevich group. This paper sketches the Cohen-Lenstra philosophy in both cases of class groups and of Tate-Shafarevich groups. It is organized as follows:

In the first section, we describe the analogy between number fields and elliptic curves defined over $\mathbb{Q}$. In the second section, we recall the Cohen-Lenstra heuristic for class groups. Using the analogy of the first section, we adapt, in the third section, the heuristic for Tate-Shafarevich groups. Finally, we restrict the heuristic to the case of families of quadratic twists of an elliptic curve.

Acknowledgements. I am very pleased to be able to thank here the organizers of the Clay Mathematics Institute Special Week on Ranks of Elliptic Curves and Random Matrix Theory, held at the Isaac Newton Institute for Mathematical Sciences, for the invitation to participate and to give a lecture on the heuristics. I could benefit from many interesting discussions with participants whom I want to thank. I am very happy to thank H. Cohen very much for his availability and his many suggestions. I am also grateful to C. Liebendörfer for her remarks and advice she kindly gave me.

This text was prepared during a post-doctoral position at the École Polytechnique Fédérale de Lausanne in Switzerland. I am grateful to all the members of the Eva Bayer’s “Chaire des structures algébriques et géométriques”.

1 Analogy between number fields and elliptic curves defined over $\mathbb{Q}$

In [6], we made a study of Tate-Shafarevich groups of elliptic curves defined over $\mathbb{Q}$ similar to the one made in [3] about class groups of number fields. To do this, we used the deep analogy between number fields and elliptic curves defined over $\mathbb{Q}$ on the one hand and class groups and Tate-Shafarevich groups on the other hand. This analogy is summarized in this section. First, we give the following table which states the correspondences between the main invariants of number fields and of elliptic curves defined over $\mathbb{Q}$:

Elliptic curve $E/\mathbb{Q}$		Number field K
$E(\mathbb{Q})_{\text{tors}}$ rational torsion points	$\leftrightarrows$	$U(K)_{\text{tors}}$ roots of unity
$E(\mathbb{Q})$ Mordell-Weil group of E	$\leftrightarrows$	$U(K)$ unit group of K
$N(E)$ conductor of E	$\leftrightarrows$	$\lvert D_K \rvert$ absolute value of the discriminant of K
$Ш(E)$ Tate-Shafarevich group of E	$\leftrightarrows$	$Cl(K)$ class group of K
$R(E)$ regulator of E	$\leftrightarrows$	$R(K)$ regulator of K
$E(\mathbb{Z})$ integer points on E	$\leftrightarrows$	exceptional units of K

The torsion parts of the groups $E(\mathbb{Q})$ and $U(K)$ are both finite and easy to determine; furthermore they play the same role. For a number field K, the unit group $U(K)$ is a finitely generated abelian group and it is not difficult to compute its rank r since we have $r = r_1 + r_2 - 1$ where r_1 (resp. r_2) is the number of real (resp. complex) places of K. However, it may be difficult to find the units of K. The Mordell-Weil group of an elliptic curve $E(\mathbb{Q})$ is a finitely generated abelian group, its rank can be predicted by the Birch and Swinnerton-Dyer conjecture and it may also be difficult to compute rational points on $E(\mathbb{Q})$ if they have large denominators. The primes dividing the absolute value of the discriminant or the conductor are rather special in both cases. Another property is that there are only finitely many number fields (resp. elliptic curves/$\mathbb{Q}$) up to isomorphism with a bounded absolute value of the discriminant (resp. conductor). The class group of a number field is a finite abelian group and measures in a way the obstruction of the ideals to be principal. Whenever this group is non-trivial, the arithmetic in K is more complicated. Similarly, the Tate-Shafarevich group Ш of an elliptic curve is a finite abelian group (here the finite part is only conjectural but we assume this conjecture to be true) and it measures the obstruction of the "local-global" principle. When Ш is non-trivial, it can be more difficult to study the elliptic curve. The regulator of a number field (resp. an elliptic curve) is the absolute value of the determinant of a certain matrix which is defined with the help of a basis of the unit group (resp. a basis of the Mordell-Weil group). In the case of a real quadratic field (the rank of the unit group of such a field is 1), as well as in the case of a rank 1 elliptic curve, there exist analytic processes to find a unit of the number field and a non-torsion point of the elliptic curve (the processes are the Gauss construction for number fields and the Heegner point construction for elliptic curves). The integer points on an elliptic curve form a finite subset of the Mordell-Weil group and are exact analogues of the exceptional units of a number field; exceptional units are units u such that $1-u$ is also a unit and they form a finite subset of the unit group (this analogy was pointed out by H. Cohen). Finally, for a number field, we have the following exact sequence:

$$1 \to U(K)/U(K)^p \to S_p(K) \to Cl(K)[p] \to 1$$

where $S_p(K) = V_p(K)/K^{*p}$ with $V_p(K) = \{\gamma \in K^* | \gamma\mathbb{Z}_K = \mathcal{I}^p$ for some ideal $\mathcal{I} \subset K\}$ and where $\mathbb{Z}_K$ is the ring of integers of K. The set $V_p(K)$ is indeed a subgroup of the multiplicative group K^*: it is called the group of p-virtual units. The group $S_p(K)$ is called the p-Selmer group of the number field K (we refer to [2] for all this terminology and for some more information about those groups).

If $L(K,s)$ is the L-function associated to K (i.e. the Dedekind zeta function), we have:

$$L(K,s) \sim_{s=0} -s^r \frac{R(K)|Cl(K)|}{|U(K)_{\text{tors}}|}$$

where $r = r_1 + r_2 - 1$ is the the rank of $U(K)$.

For an elliptic curve E:

$$1 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to S_p(E) \to Ш(E)[p] \to 1$$

where $S_p(E)$ is the p-Selmer group of E (cf. [11]), and if $L(E,s)$ is the L-function attached to E, then the Birch and Swinnerton-Dyer conjecture predicts that:

$$L(E,s) \sim_{s=1} (s-1)^r \frac{R(E)|Ш(E)|}{(|E(\mathbb{Q})_{\text{tors}}|)^2} \, c\,\Omega \tag{1.1}$$

where r is the rank of the Mordell-Weil group, c is the product of the Tamagawa numbers (it is a small integer) and Ω is the real period of E.

The exact sequences and the estimates of the L-functions are exact analogues. However, we should note that the main terms in the right-hand side of (1.1) are perfect squares:

- $R(E)$ is the determinant of a Gram matrix and so is naturally the square of a determinant.
- The order of the group $Ш(E)$ is a square (we assume it is finite).
- In the denominator, there is the square of the order of $E(\mathbb{Q})_{\text{tors}}$.

Cassels proved that there exists a bilinear alternating pairing:

$$\beta \,:\, Ш \times Ш \longrightarrow \mathbb{Q}/\mathbb{Z}$$

which is non-degenerate if the Tate-Shafarevich group is finite; we assume Ш to be a finite group. Then we will say that a couple (G,β) is a group of type S, if G is a finite abelian group and:

$$\beta \,:\, G\times G \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is a non-degenerate alternating bilinear pairing.
Two groups (G_1,β_1) and (G_2,β_2) of type S are said to be isomorphic if there exists an isomorphism $\sigma \,:\, G_1 \rightarrow G_2$ such that:

$$\beta_2(\sigma(x),\sigma(y)) = \beta_1(x,y) \quad \text{for all } x,y\in G_1.$$

If (G,β) is a group of type S, then $G \simeq H\times H$ where H is a finite abelian group; in particular, this explains why the order of a Tate-Shafarevich group is a perfect square. Conversely, every group $G\simeq H\times H$, where H is a finite abelian group, can be endowed with a unique (up to isomorphism) structure of group of type S.

In the sequel, the letter p will always denote a prime number. For G a finite abelian group, we denote by G_p the p-part of G: that is G_p is the subgroup of G consisting of elements of order a power of p. Note that every finite abelian group can be written as the direct sum of its p-group. The subgroup G_p is thus a p-group (i.e. $|G_p| = p^n$ for some $n\in\mathbb{N}$) and then can be uniquely written as:

$$G_p \simeq \mathbb{Z}/p^{a_1}\mathbb{Z}\times\mathbb{Z}/p^{a_2}\mathbb{Z}\cdots\times\mathbb{Z}/p^{a_r}\mathbb{Z}$$

for some (unique) positive integers $a_1 \leqslant a_2 \leqslant \ldots \leqslant a_r \in \mathbb{N}$. The number r is called the p-rank of G. It is denoted by $r_p(G)$ and is also equal to the dimension over $\mathbb{Z}/p\mathbb{Z}$ of the $\mathbb{Z}/p\mathbb{Z}$-vector space G/pG.

The symbol $\sum_{G(n)}$ (resp. $\sum_{G^S(n)}$) means that the sum is over all isomorphism classes of finite abelian groups (resp. groups of type S) of order n. Note that $\sum_{G^S(n)} \equiv 0$ if n is not a perfect square. Finally, $\mathrm{Aut}(G)$ denotes the group of automorphisms of G and $\mathrm{Aut}^S(G)$ the group of automorphisms of (G,β) which preserve the pairing β.

2 Heuristics on class groups of quadratic number fields

The class group measures in a way how difficult it is to perform the explicit computations related to some underlying arithmetical problem. Then, we would like to understand how it behaves in general; are we lucky if, for example, the p-part of the class group of some number field is trivial or are they often trivial? In fact, for those questions, we have to restrict our study to natural families of number fields whose unit groups have the same rank. Unfortunately, and even for such natural families, a direct study of this problem is completely out of reach nowadays. In [3], however, Cohen and Lenstra proposed a wonderful heuristic principle that allows to give conjectural answers to many questions related to the general behavior of class groups in a natural family. We now sketch their philosophy in the first case, that is, in the case of class groups attached to quadratic imaginary number fields.

2.1 Imaginary quadratic number fields

Imaginary quadratic number fields have the form $K = \mathbb{Q}(\sqrt{D_K})$ where $D_K < 0$ is a fundamental discriminant. The unit group is a finite group (its rank is 0) and the discriminant of K is D_K.

For our purpose, we let F be a $\mathbb{C}$-valued function defined on isomorphism classes of finite abelian groups (because class groups are finite abelian groups).

Examples. We will look at the following ones:

$$\begin{aligned} F_{p\text{-}triv}(G) &= \begin{cases} 1 & \text{if } G_p \simeq \{0\} \\ 0 & \text{else} \end{cases} \\ F_{cyclic}(G) &= \begin{cases} 1 & \text{if } G \text{ is cyclic} \\ 0 & \text{else} \end{cases} \\ F_{p-rank}(G) &= p^{r_p(G)} \end{aligned}$$

Then we consider the following limit:

$$M_{Cl,0}(F) = \lim_{X\to\infty} \left(\frac{\sum\limits_{|D_K|\leqslant X} F(Cl(K))}{\sum\limits_{|D_K|\leqslant X} 1} \right) \tag{2.1}$$

where the sums are over all quadratic imaginary number fields K whose absolute value of the discriminant is bounded by X. Note that there are only finitely many such number fields, so that the term in the brackets of (2.1) is meaningful.

We have two problems: does the limit exist? If yes, what is its value? One moment's thought tells us that, in fact, this is exactly what we want to answer. For example, if we consider the function $F = F_{p\text{-}triv}$, then if the limit in (2.1) exists for F, this limit is precisely the frequency of class groups with trivial p-parts. But, as we mentioned above we cannot study this limit directly. The fundamental idea of Cohen and Lenstra is to say that class groups behave as random finite abelian groups G except that they have to be weighted by:

$$\frac{1}{|\operatorname{Aut}(G)|} \tag{2.2}$$

More precisely, we consider the following average:

Definition 1. *Let F be as above. The 0-average of F over finite abelian groups is defined by:*

$$M_{G,0}(F) = \lim_{X\to\infty}\left(\frac{\displaystyle\sum_{n\leqslant X}\sum_{G(n)}\frac{F(G)}{|\operatorname{Aut}(G)|}}{\displaystyle\sum_{n\leqslant X}\sum_{G(n)}\frac{1}{|\operatorname{Aut}(G)|}}\right).$$

If F is the characteristic function of a property $\mathcal{P}$, we will speak of 0-probability instead of 0-average.

From the theory of genera, the 2-part of the class group $Cl(K)$ behaves in a very special way and so we have to exclude it from our discussion and we denote by:

$$Cl_0(K) = \{x \in Cl(K) \text{ such that } x \text{ has odd order}\}$$

the odd part of $Cl(K)$.
If F is a function as above, we define the function $F\circ odd$ to be the function: $F\circ odd\ :\ G \mapsto F(G_0)$, where G_0 denotes the odd part of G. We can now formulate the Cohen-Lenstra heuristic:

Fundamental heuristic assumption for imaginary quadratic fields. *For all reasonable functions F, we have:*

$$M_{Cl,0}(F\circ odd) = M_{G,0}(F\circ odd)$$

The magic of the Cohen-Lenstra heuristic is that it works! Indeed, there are strong evidences to believe in this assumption. Furthermore, the value of $M_{G,0}(F\circ odd)$ can be computed for many interesting functions and we can be confident enough in the results it produces. In practice, in order to compute $M_{G,0}(F)$, we treat the numerator and the denominator of the definition of $M_{G,0}(F)$ separately. For this purpose we need the following Tauberian theorem:

Theorem 2. *Let $(c(n))_{n\geqslant 1}$ be a sequence of non-negative numbers and $D(z) = \sum_n c(n)/n^z$. If $D(z)$ converges for $\Re(z) > 0$ and if there exists $C \in \mathbb{C}$ such that $D(z) - C/z$ can be analytically continued to an open subset containing $\Re(z) \geqslant 0$, then, as X tends to infinity, we have:*

$$\sum_{n\leqslant X} c(n) \sim C\log(x)$$

In view of the definition 1 we would like to apply this theorem with $c(n) = \sum_{G(n)} F(G)/|\operatorname{Aut}(G)|$, leading to:

Definition 3. *Let F be a function as above. We define the two following Dirichlet series:*

$$\begin{aligned}\zeta_G(z) &= \sum_{n\geqslant 1}\frac{1}{n^z}\sum_{G(n)}\frac{1}{|\operatorname{Aut}(G)|}\\ \zeta_{G,F}(z) &= \sum_{n\geqslant 1}\frac{1}{n^z}\sum_{G(n)}\frac{F(G)}{|\operatorname{Aut}(G)|}\end{aligned}$$

Cohen and Lenstra proved (cf. [3]):

Theorem 4. *We have:*

$$\zeta_G(z)=\prod_{j=1}^{\infty}\zeta(z+j)$$

where ζ is the Riemann zeta function.

From theorem 4 and theorem 2 we deduce a very good estimate for the denominator of $M_{G,0}(F)$:

Corollary 5. *We have:*

$$\sum_{n\leqslant X}\ \sum_{G(n)}\frac{1}{|\operatorname{Aut}(G)|}\sim\prod_{j=2}^{\infty}\zeta(j)\ \log(X).$$

For the numerator of $M_{G,0}(F)$ we do the same; in general for reasonable functions F, the Dirichlet series $\zeta_{G,F}$ satisfies the conditions of theorem 2, and we can deduce that:

$$\sum_{n\leqslant X}\sum_{G(n)}\frac{F(G)}{|\operatorname{Aut}(G)|}\sim C\log(X)$$

(for convenience $C=0$ means that the left hand-side is $O(1)$). We then obtain:

$$M_{G,0}(F)=\frac{C}{\prod_{j=2}^{\infty}\zeta(j)}$$

By the same method we can compute $M_{G,0}(F\circ \mathit{odd})$ and by the heuristic assumption this is the average of F over class groups.

2.2 Real quadratic fields

This case is a little bit more subtle since the rank of the unit group is 1. More generally, when the unit group is not a finite group, the Cohen-Lenstra heuristic is more technical ([3], [4]). In our case, the philosophy is to say that the odd part of a class group associated to a real quadratic field behaves as a random finite abelian group G of odd order divided by a random cyclic subgroup (we still have the weight $1/|\operatorname{Aut}(G)|$). With this idea we can also define a "1-average" over finite abelian group $M_{G,1}(F)$ and the heuristic predicts that:

Fundamental heuristic assumption for real quadratic fields: *For all reasonable functions F we have:*

$$M_{Cl,1}(F \circ odd) = M_{G,1}(F \circ odd)$$

where $M_{Cl,1}(F)$ is defined as in (2.1) except that the sums are over real quadratic number fields.

In fact, Cohen and Lenstra defined the u-average $M_{G,u}(F)$ of F over finite abelian groups for all $u \in \mathbb{N}$. In general, the u-average can be computed by a straightforward generalization of the method explained above ([3]):

Theorem 6. *Let F be a function as above, $u \in \mathbb{N}$ and suppose that $\zeta_{G,F}$ satisfies the conditions of theorem 2 then:*

$$\begin{aligned} \text{if } u = 0 \text{ then } M_{G,0}(F) &= \lim_{z\to 0} \frac{\zeta_{G,F}(z)}{\zeta_G(z)}, \\ \text{if } u > 0 \text{ then } M_{G,u}(F) &= \frac{\zeta_{G,F}(u)}{\zeta_G(u)}. \end{aligned}$$

2.3 Examples

Let us consider the function $F = F_{p\text{-}triv}$, where $p \neq 2$; then $F \circ odd = F$. The function $\zeta_{G,F}$ is exactly the function ζ_G without its p-part. From theorem 4 we have:

$$\begin{aligned} \zeta_G(z) &= \prod_{j=1}^{\infty} \zeta(z+j) \\ &= \prod_{j} \prod_{q \text{ prime}} \left(1 - \frac{1}{q^{z+j}}\right)^{-1} \\ &= \prod_{q \text{ prime}} \prod_{j} \left(1 - \frac{1}{q^{z+j}}\right)^{-1}. \end{aligned}$$

So the term $\prod_j \left(1 - \frac{1}{p^{z+j}}\right)^{-1}$ is exactly the p-Euler factor of $\zeta_G(z)$. Then we deduce:

$$\begin{aligned} \zeta_{G,F}(z) &= \prod_{q \neq p} \prod_{j} \left(1 - \frac{1}{q^{z+j}}\right)^{-1} \\ &= \zeta_G(z) \prod_{j} \left(1 - \frac{1}{p^{z+j}}\right). \end{aligned}$$

Finally, we obtain:

$$\begin{aligned} M_{G,0}(F) &= \prod_{j=1}^{\infty}\left(1-\frac{1}{p^j}\right) \\ M_{G,1}(F) &= \prod_{j=1}^{\infty}\left(1-\frac{1}{p^{j+1}}\right). \end{aligned}$$

By the Cohen-Lenstra heuristic, we deduce the conjecture:

Conjecture 7. *Let $p \neq 2$.*
The probability that p divides the order of the class group of an imaginary quadratic field is equal to:

$$1-\prod_{j=1}^{\infty}\left(1-\frac{1}{p^j}\right)=\frac{1}{p}+\frac{1}{p^2}-\frac{1}{p^5}\cdots$$

The probability that p divides the order of the class group of a real quadratic field is equal to:

$$1-\prod_{j=1}^{\infty}\left(1-\frac{1}{p^{j+1}}\right)=\frac{1}{p^2}+\frac{1}{p^3}+\frac{1}{p^4}\cdots$$

Let us consider some other examples that can be found in [3] (they are a little more technical because they involve the p-rank of finite abelian groups).
- The u-average of the function $F = F_{cyclic} \circ odd$ is equal to:

$$M_{G,u}(F)=\frac{\prod_{j\geqslant u+2}(1-1/2^j)}{1+1/2^{u+1}}\prod_p\left(\frac{1-1/p+1/p^{u+2}}{1-1/p}\right)\prod_{j\geqslant 2}\frac{1}{\zeta(u+j)}$$

In particular, $M_{G,0}(F) \approx 0.98$.
- The u-average of the function $F(G) = p^{r_p(G)}$ is $1+1/p^u$ (note that $F\circ odd = F$ if $p \neq 2$). In particular, if $p = 3$, the 0-average of F is equal to 2 and the 1-average of F is 4/3.

The Cohen-Lenstra heuristics have been checked by many numerical computations and they are very useful for understanding the behavior of class groups, even if the results are conjectural. For example, they explain why it is so difficult to find a non-cyclic $Cl_0(K)$.
The first theoretical result was obtained by Davenport and Heilbronn who proved (before the heuristics were formulated) that the average of the function $3^{r_3(Cl(K))}$ is equal to 2 (resp. 4/3) in the case of imaginary (resp. real) quadratic fields.
The Cohen-Lenstra heuristics extend to many other families of number fields, and we refer to [3], [4], [15] for some generalizations.

3 Heuristics on Tate-Shafarevich groups of elliptic curves

As with class groups, we are annoyed by Tate-Shafarevich groups of elliptic curves. Thus, we use the analogy described in the first section and sketch the work in [6] which shows how the Cohen-Lenstra philosophy can be adapted to our case. To do this, we take into account the particular structure of Tate-Shafarevich groups, i.e., the structure of groups of type S.

3.1 Rank 0 case

By analogy, we consider a $\mathbb{C}$-valued function F defined on the isomorphism classes of groups of type S.

Examples. We will look at the following ones:

$$\begin{aligned} F_{p\text{-}triv}(G) &= \begin{cases} 1 & \text{if } G_p \simeq \{0\} \\ 0 & \quad\text{else} \end{cases} \\ F_{cyclic}(G) &= \begin{cases} 1 & \text{if } G \text{ is the square of a cyclic group} \\ 0 & \qquad\qquad\text{else} \end{cases} \\ F_{p\text{-}rank=2r}(G) &= \begin{cases} 1 & \text{if } r_p(G) = 2r \\ 0 & \quad\text{else} \end{cases} \end{aligned}$$

Note that we simply write G for a group of type S instead of (G, β), since there is only one group structure of type S for each group (up to isomorphism). We consider the following limit:

$$M_{\text{Ш},0}(F) = \lim_{X \to \infty} \left(\frac{\displaystyle\sum_{N(E) \leqslant X} F(\text{Ш}(E))}{\displaystyle\sum_{N(E) \leqslant X} 1} \right) \tag{3.1}$$

where the sums are over all isomorphism classes of rank 0 elliptic curves whose conductor is bounded by X (there are only finitely many such isomorphism classes). As for class groups, we have two questions: does the limit exist? If yes, what is its value? Furthermore, questions of this type are exactly what we would like to answer...

Definition 8. *We define:*

$$\begin{aligned}\zeta_{G^S}(z) &= \sum_{n\geqslant 1}\frac{1}{n^z}\sum_{G^S(n)}\frac{1}{|\operatorname{Aut}^S(G)|}\\ \zeta_{G^S,F}(z) &= \sum_{n\geqslant 1}\frac{1}{n^z}\sum_{G^S(n)}\frac{F(G)}{|\operatorname{Aut}^S(G)|}\end{aligned}$$

We can prove:

Theorem 9. *We have:*

$$\zeta_{G^S}(z)=\prod_{j=1}^{\infty}\zeta(2z+2j+1).$$

The main difference with finite abelian groups is that the function $\zeta_{G^S}(z)$ converges for $z=0$ and that we have:

Corollary 10.

$$\zeta_{G^S}(0)=\sum_{n\geqslant 1}\sum_{G^S(n)}\frac{1}{|\operatorname{Aut}^S(G)|}=\prod_{j=1}^{\infty}\zeta(2j+1).$$

So, we have to adapt the definition for average over groups of type S:

Definition 11. *Let F be as above and $\alpha\geqslant 1$ (we will see later why we need α). Then, the 0-average of F over groups of type S is defined by:*

$$M_{G^S,0}(F,\alpha)=\lim_{X\to\infty}\left(\frac{\displaystyle\sum_{n\leqslant X}\sum_{G^S(n)}\frac{F(G)|G|^{\alpha}}{|\operatorname{Aut}^S(G)|}}{\displaystyle\sum_{n\leqslant X}\sum_{G^S(n)}\frac{|G|^{\alpha}}{|\operatorname{Aut}^S(G)|}}\right).$$

The exact analogue of definition 1 would have been to take $\alpha=0$. But as we have shown before, the denominator converges for $\alpha=0$ and this does not give a relevant average. For $\alpha\geqslant 1$ the denominator diverges. Another reason to insert α in definition 11 is that for reasonable functions F, the limit $M_{G,0}(F,\alpha)$ *does not depend on* α if $\alpha\geqslant 1$ (this fact is an application of a generalization of theorem 2). In particular, it is not true that the limit does not depend on α if $\alpha<1$. The *same phenomenon* already occurred for finite abelian groups; we could take the weight $|G|^{\alpha}/|\operatorname{Aut}(G)|$ in (2.2) and the results would not have depended on α for $\alpha\geqslant 0$. Once again, the situation is analogous to the one of class groups.

Since $M_{G,0}(F,\alpha)$ does not depend on α for $\alpha\geqslant 1$, we let:

$$M_{G^S,0}(F)=M_{G^S,0}(F,1).$$

Then we can compute $M_{G,0}(F)$ by using theorem 2 as for finite abelian groups. For instance, the function $\zeta_{G^S}(z-1) = \sum_n \frac{1}{n^z} \sum_{G^S(n)} \frac{|G|}{|\operatorname{Aut}^S(G)|}$ converges for $\Re(z) > 0$ and satisfies the conditions of theorem 2. Thus we deduce the following estimate for the denominator of $M_{G,0}(F)$:

Corollary 12. *As X tends to ∞ we have:*

$$\sum_{n \leqslant X} \sum_{G^S(n)} \frac{|G|}{|\operatorname{Aut}^S(G)|} \sim \frac{1}{2} \prod_{j=1}^{\infty} \zeta(2j+1) \ \log(X).$$

As regards the numerator, we expect that the function $\zeta_{G^S,F}(z-1)$ satisfies the conditions of theorem 2 so that:

$$\sum_{n \leqslant X} \sum_{G^S(n)} \frac{F(G)|G|}{|\operatorname{Aut}^S(G)|} \sim C \log(X).$$

And we would have:

$$M_{G^S,0}(F) = \frac{2C}{\prod_{j=1}^{\infty} \zeta(2j+1)}.$$

Now the heuristic idea is to assert that Tate-Shafarevich groups of rank 0 elliptic curves behave as random groups G of type S except that they have to be weighted by the weight $|G|/|\operatorname{Aut}^S(G)|$.

Fundamental heuristic assumption for rank 0 elliptic curves. *For all reasonable functions F we have:*

$$M_{Ш,0}(F) = M_{G^S,0}(F).$$

3.2 Rank 1 case

As for class groups, the higher rank cases are a little bit more technical. In case of rank 1, we are interested in the following limit:

$$M_{Ш,1}(F) = \lim_{X \to \infty} \left(\frac{\displaystyle\sum_{N(E) \leqslant X} F(Ш(E))}{\displaystyle\sum_{N(E) \leqslant X} 1} \right) \tag{3.2}$$

where now the sums are over all isomorphism classes of rank 1 elliptic curves with conductor bounded by X.

Definition 13. *Let F be as above and $u \geqslant 0$. We define $(c_u(F,n))_{n\geqslant 1}$ by:*

$$\sum_{n\geqslant 1} \frac{c_u(F,n)}{n^z} = \frac{\zeta_{G^S,F}(z+u)\zeta_{G^S}(z)}{\zeta_{G^S}(z+u)}.$$

The u-average of F over groups of type S is:

$$M_{G^S,u}(F) = \lim_{X\to\infty} \left(\frac{\displaystyle\sum_{n\leqslant X} nc_u(F,n)}{\displaystyle\sum_{n\leqslant X} \sum_{G^S(n)} \frac{|G|}{|\operatorname{Aut}^S(G)|}} \right).$$

Remarks. For reasonable functions F, the average $M_{G^S,u}(F)$ does not depend on $\alpha \geqslant 1$ if we replace in the definition $nc_u(F,n)$ by $n^\alpha c_u(F,n)$ and $|G|$ by $|G|^\alpha$. For $u=0$, this is the same definition as in the section above.

Theorem 2 allows us to compute u-averages in many cases:

Proposition 14. *Let F be as above and suppose that $\zeta_{G^S,F}(z-1)$ satisfies the conditions of theorem 2. We have:*

$$\textit{if } u=0 \textit{ then } M_{G^S,0} = \lim_{z\to 0} \frac{\zeta_{G^S,F}(z-1)}{\zeta_{G^S}(z-1)}$$

$$\textit{if } u>0 \textit{ then } M_{G^S,u}(F) = \frac{\zeta_{G^S,F}(u-1)}{\zeta_{G^S}(u-1)}$$

Fundamental heuristic assumption for rank 1 elliptic curves. *For all reasonable functions F we have:*

$$M_{Ш,1}(F) = M_{G^S,1}(F).$$

Note that in [6], we formulated the heuristic for higher ranks by taking the $u/2$-average for the family of rank u elliptic curves. So the heuristic assumption here *is a correction of [6] in the rank 1 case.*

3.3 Examples

Let us consider the function $F = F_{p\text{-}triv}$. Then, as for finite abelian groups, we have:

$$\zeta_{G^S,F}(z) = \zeta_{G^S}(z) \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^{2z+2j+1}}\right).$$

So we obtain the u-average of F:

$$M_{G^S,u}(F) = \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^{2u+2j-1}}\right).$$

Then, we deduce:
-The 0-probability that p divides the order of a group of type S is equal to:

$$f_0(p) = 1 - \prod_{j=1}^{\infty}\left(1 - \frac{1}{p^{2j-1}}\right) = \frac{1}{p} + \frac{1}{p^3} - \frac{1}{p^4} + \frac{1}{p^5} - \frac{1}{p^6}\cdots \tag{3.3}$$

In particular $f_0(2) \approx 0.58$, $f_0(3) \approx 0.36$ and $f_0(5) \approx 0.21$.

-The 1-probability that p divides the order of a group of type S is equal to:

$$f_1(p) = 1 - \prod_{j=1}^{\infty}\left(1 - \frac{1}{p^{2j+1}}\right) = \frac{1}{p^3} + \frac{1}{p^5} + \frac{1}{p^7} - \frac{1}{p^8}\cdots \tag{3.4}$$

In particular $f_1(2) \approx 0.16$, $f_1(3) \approx 0.04$ and $f_1(5) \approx 0.01$.

We also consider some other examples that can be found in [6].
-The u-average of the function $F = F_{cyclic}$ is equal to:

$$M_{G^S,u}(F) = \prod_p \left(1 - \frac{1}{p^2} + \frac{1}{p^{2u+3}}\right) \frac{\zeta(2)}{\prod_{j\geqslant 1}\zeta(2u+2j+1)}.$$

In particular, $M_{G^S,0}(F) \approx 0.98$.
-The u-average of $F(G) = p^{r_p(G)}$ is equal to:

$$1 + p^{1-2u}. \tag{3.5}$$

-The u-average of the function $F = F_{p\text{-}rank=2r}$ is equal to:

$$M_{G^S,u}(F) = \frac{p^{-r(2u+2r-1)}}{\prod_{j\geqslant 1}(1 - 1/p^{2r})} \prod_{j\geqslant r+1}(1 - 1/p^{2u+2j-1}). \tag{3.6}$$

The heuristics as well as their consequences are out of reach. Furthermore it is difficult to check them numerically because there are too many elliptic curves and Tate-Shafarevich groups seem to appear for large conductors. There is no algorithm known to compute Tate-Shafarevich groups. The only thing we can do is to compute the (conjectural) order of Tate-Shafarevich groups using the Birch and Swinnerton-Dyer conjecture. Indeed all members in equation (1.1) are easily computable except $R(E)$ and $|Ш(E)|$. So if for some reason one can compute $R(E)$ (for rank 0 curves we simply have $R(E) = 1$), then we can deduce $|Ш(E)|$. If we have many data we can compare them with the heuristic predictions of type (3.3). We can also restrict the heuristics to some natural sub-families of elliptic curves (quadratic twists) for which the analogy with number fields seems to be even more deeper.

4 Quadratic twist families

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and let $L(E,s) = \sum_n a(n)n^{-s}$ be its L-function. From the work in [14], [12] and [1] E is known to be modular. This implies that its L-function can be analytically continued to the whole complex plane and satisfies a functional equation:

$$\Lambda(E, 2-s) = \varepsilon\Lambda(E,s) \tag{4.1}$$

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

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

Note that the Birch and Swinnerton-Dyer conjecture implies $\varepsilon = (-1)^r$ where r is the rank of $E(\mathbb{Q})$. Let D be a fundamental discriminant (for simplicity we assume $(N,D) = 1$). Then the twisted L-function:

$$L(E,D,s) = \sum_n \left(\frac{D}{n}\right) a(n)n^{-s}$$

where $\left(\frac{D}{\cdot}\right)$ is the Kronecker symbol, corresponds to the quadratic twist E_D of E by D and has conductor $N_D = ND^2$. Then the function $L(E,D,s)$ satisfies a functional equation as (4.1) whose sign is $\varepsilon_D = \left(\frac{D}{-N}\right)$.

In this section, we consider the family of elliptic curves:

$(E_D)_D$ where D runs over all fundamental discriminant.

In fact, there is another analogy between this family and the family of quadratic imaginary number fields. Indeed, from the work of Waldsurger ([13]), the values $L(E,D,1)$ are related to the coefficients $c(|d|)$ of a 3/2-weight modular form; more precisely:

$$L(E,D,1) = \kappa_E|D|^{-1/2}c(|D|)^2 \tag{4.2}$$

where κ_E is a constant depending only on E. Suppose that $c(|d|) \neq 0$ so that E_D has rank 0. Then replacing $L(E,D,1)$ by its value predicted by the Birch and Swinnerton-Dyer conjecture, we deduce that the order $|Ш(E_D)|$ of the Tate-Shafarevich group of the rank 0 curve E_D is, up to some factors (namely the Tamagawa numbers), the square of the coefficients of a 3/2-weight modular form. We have exactly the same phenomenon for class groups (without the square). Indeed, the order of class groups of imaginary quadratic fields are, up to some normalization (namely, we have to consider the Hurwitz class numbers instead of the class numbers), the coefficients of a 3/2-weight modular form.
Furthermore, using (4.2), Rubinstein ([10]) performed huge numerical experimentations and computed how often a given prime p divides the (conjectural)

order of $\text{Ш}(E_D)$ for rank 0 quadratic twists of many elliptic curves E. His numerical results are in close agreement with the prediction (3.3) given by the heuristic except maybe for some "special" primes. These lead us to restrict the heuristics to the family (E_D).

If $\mathcal{T}$ is a set of prime numbers and F a function defined on isomorpism classes of groups of type S, then we define the function $F \circ \mathcal{T}$ by $F \circ \mathcal{T} \,:\, G \mapsto F(G_{\mathcal{T}})$, where $G_{\mathcal{T}}$ is the $\mathcal{T}$-part of G.

Heuristic assumption for rank 0 quadratic twists. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then there exists a finite set $\mathcal{S}$ of prime numbers such that for all reasonable functions F we have:*

$$\lim_{X\to\infty}\left(\frac{\displaystyle\sum_{\substack{|D|<X\\ rk(E_D)=0}} F\circ\mathcal{T}(\text{Ш}(E_D))}{\displaystyle\sum_{\substack{|D|<X\\ rk(E_D)=0}} 1}\right) = M_{G^S,0}(F\circ\mathcal{T}) \tag{4.3}$$

where the sum is over fundamental discriminants D such that the rank of E_D is 0 and where $\mathcal{T}$ is the set of prime numbers p with $p \notin \mathcal{S}$.

Heuristic assumption for rank 1 quadratic twists. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then there exists a finite set $\mathcal{S}$ of prime numbers such that for all reasonable functions F we have:*

$$\lim_{X\to\infty}\left(\frac{\displaystyle\sum_{\substack{|D|<X\\ rk(E_D)=1}} F\circ\mathcal{T}(\text{Ш}(E_D))}{\displaystyle\sum_{\substack{|D|<X\\ rk(E_D)=1}} 1}\right) = M_{G^S,1}(F\circ\mathcal{T}) \tag{4.4}$$

where the sum is over fundamental discriminants D such that the rank of E_D is 1 and where $\mathcal{T}$ is the set of prime numbers p with $p \notin \mathcal{S}$.

Remark: It is actually not clear which prime numbers have to be excluded form the discussion. Rubinstein's huge numerical data show that some primes behave in a rather special way. More precisely, those primes appear to be maybe the prime 2 and the odd primes ℓ dividing the order of the torsion sub-group of the curves belonging to the isogeny class of the curve E with the smallest conductor in the family in question (perhaps due to the fact that, in this case, the ℓ-part of the class group of $\mathbb{Q}(\sqrt{d})$ should have a weight on the ℓ-Selmer group of E_d. This is, indeed, what had been proved by Frey for some curves E [7]). However, the convergence for the prime 2 may be simply slower than for the others and so seems to be a special prime even if it is not.

In [8] and [9], Heath-Brown [1] studied the Selmer groups of the family of quadratic twists:

$$E_D \ : \ Dy^2 = x^3 - x.$$

When the rank of E_D is 0 or 1, it is not difficult to obtain information about the Tate-Shafarevich groups of E_D from its Selmer group. Furthermore, Heath-Brown considered all curves E_D and not only those that have rank 0 or 1. Nevertheless, there is a classical conjecture (the density conjecture) asserting that on average the curves E_D have either rank 0 or rank 1 (of course, this can be true only on average). The random matrix theory predicts very precise statements refining the density conjecture ([5]). Finally, the density conjecture and Heath-Brown's works imply the following rank 0 and rank 1 results:

Rank 0 case. Here we consider only D such that E_D has rank 0.

- The average of the function $2^{r_p(\text{Ш}(E_D))}$ over the curves E_D that have rank 0 is equal to 3.
- Let $r \in \mathbb{N}$. The probability that $r_2(\text{Ш}(E_D)) = 2r$ is equal to:

$$\prod_{j=1}^{\infty}(1+2^{-n})^{-1}\frac{2^r}{\prod_{1\leqslant j\leqslant r}(2^j-1)} \tag{4.5}$$

Rank 1 case. Here we consider only D such that E_D has rank 1.

- The average of the function $2^{r_p(\text{Ш}(E_D))}$ over the curves E_D that have rank 1 is equal to 3/2.
- Let $r \in \mathbb{N}$. The probability that $r_2(\text{Ш}(E_D)) = 2r$ is equal to ([9]):

$$\prod_{j=1}^{\infty}(1+2^{-n})^{-1}\frac{2^{r-1}}{\prod_{1\leqslant j\leqslant r-1}(2^j-1)}. \tag{4.6}$$

These results should be compared with (3.5) and (3.6) with $p = 2$, $u = 0$ and $u = 1$. In fact, a little computation shows that they all agree! (Heath Brown's results and the link with the heuristics have been pointed out to me by E. Kowalski whom I thank here). In Heath-Brown's paper, it is suggested that the convergence should be extremely slow, so it would not be very surprising if the prime 2 behaved like a special prime in numerical computations although it is not. Heath-Brown's results and Rubinstein's data make the heuristics on Tate-Shafarevich groups even more believable in the case of quadratic twist families.

[1] Editors' comment: See also the article by D.R. Heath-Brown in this volume.

References

[1] 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), no. 4, 843–939

[2] H. Cohen, *Advanced topics in computational algebraic number theory*, Graduate texts in Math. **193**, Springer-Verlag, New-York, (2000).

[3] H. Cohen and H. W. Lenstra, *Heuristics on class groups of number fields*, in Number theory (Noordwijkerhout, 1983), ed. H. Jager, Lecture Notes in Math. **1068**, Springer-Verlag (1984), pp. 33-62.

[4] H. Cohen and J. Martinet, *Etude heuristiques des groupes de classes des corps de nombres*, J. Reine Angew. Math. **404** (1990), pp. 39-76.

[5] J. Conrey, J. Keating, M. Rubinstein and N. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 301–315.

[6] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Exp. Math. **10** (2001), no. 2, 191–196.

[7] G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. ,**XL**, (1988), 649–665.

[8] D. R. Heath-Brown, *The size of the Selmer group for the congruent number problem, I*, Invent. Math. **111**, (1993), pp. 111-125.

[9] D. R. Heath-Brown, *The size of the Selmer group for the congruent number problem, II*, Invent. Math. **118**, (1994), pp. 331-370.

[10] M. Rubinstein, *Numerical data*, available at
www.math.uwaterloo.ca/∼mrubinst/L_function/VALUES/DEGREE_2/
ELLIPTIC/QUADRATIC_TWISTS/WEIGHT_THREE_HALVES/

[11] J. Silverman, *The arithmetic of elliptic curves*, Graduate texts in Math. **106**, Springer-Verlag, New-York, (1986).

[12] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[13] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. (9) **60** (1981), pp. 375-484.

[14] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no.3, 443–551.

[15] C. Wittmann, *p-class groups of certain extensions of degree p*, Math. Comp. **74** (2005), no. 250, 937–947.

Institut Camille Jordan
Université Claude Bernard Lyon 1
43, avenue du 11 novembre 1918
69622 Villeurbanne Cedex - France