

Moments of the orders of Tate-Shafarevich groups

C. Delaunay

March 14, 2005

Abstract

We give some conjectures for the moments of the orders of the Tate-Shafarevich groups of elliptic curves belonging to a family of quadratic twists. These conjectures follow from the predictions on L -functions given by the random matrix theory ([K-S], [CFKRS]) and from the Birch and Swinnerton-Dyer conjecture. Furthermore, including the Cohen-Lenstra type heuristics for Tate-Shafarevich groups, we obtain some conjectural estimates for the regulator of rank 1 elliptic curves in a family of quadratic twists.

1 Introduction and notations

We use the methods and conjectures coming from random matrix theory and their link with L -functions (as developed in [K-S], [CFKRS]) in order to give conjectures related to the size of the orders of Tate-Shafarevich groups of elliptic curves in a family of quadratic twists. Let E be an elliptic curve defined over \mathbb{Q} with conductor $N(E)$. The associated L -function of E is:

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

and converges for $\Re(s) > 3/2$. From the work of Wiles, Taylor ([Wil], [Tay-Wil]) and Breuil, Conrad, Diamond, Taylor ([Bre et al.]), $L(E, s)$ can be continued to the whole complex plane and satisfies a functional equation:

$$\Lambda(E, s) = \left(\frac{\sqrt{N(E)}}{2\pi} \right)^s \Gamma(s)L(E, s) = \varepsilon(E)\Lambda(E, 2-s) \quad (1)$$

where $\varepsilon(E) = \pm 1$ is the sign of the functional equation. Furthermore, the function $f(\tau) = \sum_n a(n)q^n$, $q = \exp(2i\pi\tau)$, is a newform of weight 2 on the congruence subgroup $\Gamma_0(N)$. Let $d \in \mathbb{Z}$ be a fundamental discriminant and $\left(\frac{d}{\cdot}\right)$ the associated quadratic character. We denote by E_d the quadratic twist of E by d , for simplicity we always assume that all the discriminants d we consider are coprime with $N(E)$. In this case, the conductor of E_d is $N(E)d^2$ and its

L -function is given by:

$$L(E_d, s) = \sum_{n \geq 1} a(n) \left(\frac{d}{n} \right) n^{-s}$$

The function $L(E_d, s)$ satisfies a functional equation of the same type as equation (1) but its sign is:

$$\varepsilon(E_d) = \varepsilon(E) \left(\frac{d}{-N(E)} \right)$$

Assuming that $\varepsilon(E_d) = 1$ we can write:

$$L(E_d, 1) = \frac{\Omega(E_d) Tam(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} S(E_d) \quad (2)$$

where $\Omega(E_d)$ is the real period of (a minimal model for) E_d , $E_d(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup of E_d and $Tam(E_d) = \prod_p Tam_p(E_d)$ is the product of the Tamagawa numbers. The Birch and Swinnerton-Dyer conjecture predicts that $S(E_d)$ is given by:

$$S(E_d) = \begin{cases} |\text{III}(E_d)| & \text{if } L(E_d, 1) \neq 0 \\ 0 & \text{else} \end{cases}$$

Let k be a positive integer (we will see later that in fact k can be a real positive number). We are interested in evaluating (conjecturally) the k -th moment of the $S(E_d)$ which is defined by:

$$\frac{1}{T^*} \sum_{\substack{|d| \leq T \\ \varepsilon(E_d) = 1}} S(E_d)^k$$

where the sum is over all fundamental discriminants $d < 0$ coprime with $N(E)$ and T^* denotes the number of terms in the sum. In fact, an asymptotic evaluation of this k -th moment should actually be an asymptotic evaluation of the moment of the orders of the Tate-Shafarevich groups of the elliptic curves E_d with rank 0 since classical conjectures ([CKRS]) imply that the d , for which $S(E_d) = 0$, are very rare and so do not contribute in the averages. We should mention that if we apply the heuristic principle of [De1] for the average of $|\text{III}|^k$ in the rank 0 case, we only obtain that if $k > 0$ then $M_E(k, T) \rightarrow \infty$ as $T \rightarrow \infty$. In this paper, we use the predictions on L -functions coming from random matrix theory to give conjectures for the leading-order asymptotics for $M_E(k, T)$.

2 General case

First, we have to restrict the discriminants we will consider in our family of twists. For this purpose, we fix once and for all a sign $\varepsilon_p = \pm 1$ for each prime p

dividing $N(E)$, such that $\prod \varepsilon_p = -\varepsilon(E)$, and we consider the family:

$$\mathcal{F}(E) = \{d < 0 \text{ fundamental discriminant with } \left(\frac{d}{p}\right) = \varepsilon_p \text{ for all } p|N(E)\}$$

We also note:

$$\mathcal{F}(E, T) = \{d \in \mathcal{F}(E) \mid |d| < T\}$$

And we consider the corresponding family of elliptic curves:

$$\{E_d \mid d \in \mathcal{F}(E)\}$$

Since we only deal with even-rank elliptic curves (at least in the first parts), we must have $\varepsilon(E_d) = 1$ for all $d \in \mathcal{F}(E)$; that is the reason why we imposed $\prod \varepsilon_p = -\varepsilon(E)$. Finally, we let $M_E(k, T)$ be the k -th moment of the $S(E_d)$ for E_d belonging to our family:

$$M_E(k, T) := \frac{1}{|\mathcal{F}(E, T)|} \sum_{d \in \mathcal{F}(E, T)} S(E_d)^k$$

The starting point of our study is the work of Keating and Snaith ([K-S]) which suggests that the moment:

$$\frac{1}{|\mathcal{F}(E, T)|} \sum_{d \in \mathcal{F}(E, T)} L(E_d, 1)^k \tag{3}$$

behave (as $T \rightarrow \infty$) as the moment of characteristic polynomials evaluated at 1 of matrices in $SO(2N)$ where N is of size $\log(T)$. We will also use the work of [CFKRS], where there is obtained a more precise asymptotic for these moments (still conjectural based on random matrix theory). In fact, what we will obtain is a conjectured formula for the first leading order asymptotic for $M_E(k, T)$. Nevertheless, it is probably possible to use the full work of [CFKRS] to obtain other leading orders. Finally, we can state the conjecture of Keating and Snaith:

Conjecture 1 (Keating-Snaith) *We have as $T \rightarrow \infty$*

$$\frac{1}{|\mathcal{F}(E, T)|} \sum_{d \in \mathcal{F}(E, T)} L(E_d, 1)^k \sim g_k(O^+) a_k(E) \log(T)^{k(k-1)/2}$$

In this conjecture, the coefficient $g_k(O^+)$ comes from the random matrix theory model and is defined by:

$$g_k(O^+) = 2^{k(k+1)/2} \prod_{j=1}^{k-1} \frac{j!}{(2j)!}$$

The factor $a_k(E)$ is an arithmetic factor and can be expanded as an Euler product: $a_k(E) = \prod_p a_k(E, p) (1 - 1/p)^{k(k-1)/2}$ with:

$$a_k(E, p) = \left(\frac{1}{p} + \frac{(1 - a(p)/p + 1/p)^{-k} + (1 + a(p)/p + 1/p)^{-k}}{2} \right) \left(1 + \frac{1}{p} \right)$$

if $p \nmid N(E)$ and:

$$a_k(E, p) = (1 - \varepsilon_p a(p)/p)^{-k}$$

if $p \mid N(E)$.

In fact, Conjecture 1 can be stated for all real $k > 0$. For this we must extend the definition of $g_k(O^+)$ for $k \in \mathbb{R}$ which can indeed be done by using Barnes' double gamma function G (cf. [K-S]):

$$g_k(O^+) = 2^{k^2/2} \frac{G(1+k)\Gamma(1+2k)^{1/2}}{(G(1+2k)\Gamma(1+k))^{1/2}}$$

Now we would like to replace the term $L(E_d, 1)$ in (3) by its value predicted by the Birch and Swinnerton-Dyer conjecture (cf. equation (2)) and then isolate the term $S(E_d)$. We need the:

Proposition 2 *Let c_4 be the usual c_4 -invariant for a minimal model of E . There exist $\Omega_E > 0$ such that for all fundamental discriminants $d < 0$ coprime to $N(E)$ with $|d|$ large enough we have:*

$$\frac{\Omega(E_d)Tam(E_d)}{|E_d(\mathbb{Q})_{tors}|^2} = \delta_8(d, c_4) \frac{\Omega_E}{\sqrt{|d|}} \prod_{p|d} Tam_p(E_d) \quad (4)$$

where $\delta_8(d, c_4) = 2$ if $8 \mid d$ and $2 \mid c_4$ and $\delta_8(d, c_4) = 1$ otherwise.

PROOF. One can see that for $|d|$ large enough $|E_d(\mathbb{Q})_{tors}|$ does not depend on d , and we denote by T this number (we have $T = 1, 2$ or 4). For the product of the Tamagawa numbers we have:

$$Tam(E_d) = \prod_{p|N(E)d^2} Tam_p(E_d)$$

with $Tam_p(E_d) = [E_d(\mathbb{Q}_p) : E_d^0(\mathbb{Q}_p)]$ and where $E_d^0(\mathbb{Q}_p)$ is the subgroup of points of $E_d(\mathbb{Q}_p)$ with non-singular reduction mod p ([Sil]). For each prime p dividing $N(E)$, fix $c_p \in \mathbb{Z}$ which is a square (resp. a non-square) mod p if $\varepsilon_p = 1$ (resp. $\varepsilon_p = -1$) (if $p = 2$ replace mod p by mod 8). Then, the curve E_d and the curve E_{c_p} are isomorphic over \mathbb{Q}_p . Hence, $Tam_p(E_d) = Tam_p(E_{c_p})$ and so $Tam_p(E_d)$ does not depend on p for $p \mid N(E)$. Finally, for $\Omega(E_d)$ we have to compute the real period of a minimal model of E_d . Let $d_0 < 0$ be a fundamental discriminant coprime to $N(E)$. Using Tate's algorithm and the fact that d is coprime to $N(E)$, one can see that we have $\Omega(E_d) = (|d_0|/|d|)^{1/2} \Omega(E_{-d_0})$ if $2 \nmid c_4$ or if $8 \nmid d$ and that the last quantity must be multiplied by 2 whenever $2 \mid c_4$ and $8 \mid d$. Now, we let $\Omega_E = \prod_{p|N(E)} Tam_p(E_{c_p}) \Omega/T^2$ and the proposition holds. \square

We will also need an upper bound for $S(E_d)$:

Proposition 3 *Assuming the Lindelöf hypothesis, we have:*

$$S(E_d) \ll_{\varepsilon, E} |d|^{1/2+\varepsilon} \quad (5)$$

PROOF. Since for all p we have $Tam_p(E_d) \geq 1$, proposition 2 and equation (2) imply that $S(E_d) \ll_E L(E_d, 1)|d|^{1/2}$. Furthermore, the Lindelöf hypothesis predicts that $L(E_d, 1) \ll_\varepsilon N(E_d)^\varepsilon \ll_{E, \varepsilon} |d|^\varepsilon$ because $N(E_d) = N(E)d^2$. \square

Remarks. 1- One could also obtain the same upper bound as (5) using the Ramanujan conjecture for weight $3/2$ modular forms instead of the Lindelöf hypothesis. Indeed, in many cases one can apply a Waldspurger-like theorem which relates the value $L(E_d, 1)$ to the coefficient $c(|d|)$ of a certain modular form of weight $3/2$. Roughly speaking, we can write $L(E_d, 1) = \kappa_E c(|d|)^2 / |d|^{1/2}$ for a convenient constant κ_E . The Ramanujan conjecture predicts that $c(|d|) \ll |d|^{1/4+\varepsilon}$ giving the desired bound.

2- In fact, the proposition above asserts that if $L(E_d, 1) \neq 0$ then $|\text{III}(E_d)| \ll N(E_d)^{1/4+\varepsilon}$ (assuming the Birch and Swinnerton-Dyer conjecture and the Lindelöf hypothesis). Goldfeld and Szpiro ([Go-Sz]) proposed a general conjecture saying that for any elliptic curve E defined over \mathbb{Q} (that is not necessarily in a family of quadratic twists) we have $|\text{III}(E)| \ll N(E)^{1/2+\varepsilon}$. As a consequence of classical conjectures, de Weger ([We]) proved that the upper bound conjectured by Goldfeld and Szpiro is optimal. Hence, the specific situation of family of quadratic twists should differ from the general case.

Now, we are concerned with the product of the Tamagawa numbers over the primes p dividing the discriminant d :

$$\prod_{p|d} Tam_p(E_d)$$

Let F be a polynomial of degree 3 such that the curve E can be defined by

$$E : y^2 = F(x) \tag{6}$$

and where this model is minimal except maybe for the prime 2. We have by Tate's algorithm:

$$Tam_p(E_d) = 1 + \text{the number of roots of } F \text{ in } \mathbb{F}_p$$

Thus, there are three cases:

- The polynomial F has three roots in \mathbb{Q} . Then, for all odd prime $p|d$ we have $Tam_p(E_d) = 4$.
- The polynomial F has only one root $a \in \mathbb{Q}$. Let $F(X) = (X - a)Q(X)$ and denote by K the quadratic number field defined by Q and Δ the discriminant of K/\mathbb{Q} . Then, for $p|d$ odd, either $\left(\frac{\Delta}{p}\right) = -1$ and $Tam_p(E_d) = 2$ or $\left(\frac{\Delta}{p}\right) = +1$ and $Tam_p(E_d) = 4$.
- The polynomial F is irreducible over \mathbb{Q} . Let K be the number field defined by it and Δ the discriminant of K/\mathbb{Q} . Then, for $p|d$ odd if $\left(\frac{\Delta}{p}\right) = -1$ then

$Tam_p(E_d) = 2$ and if $\left(\frac{\Delta}{p}\right) = 1$ then either p splits in K and $Tam_p(E_d) = 4$ or p is inert and $Tam_p(E_d) = 1$.

3 Family of twists restricted to prime discriminants

First, we would like to avoid to control precisely the product $\prod_{p|d} Tam_p(E_d)$ in (2). For this purpose, we only consider odd prime discriminants and the associated family of elliptic curves. Hence, we define:

$$\mathcal{F}'(E) = \{d < 0 \text{ odd prime discriminant with } \left(\frac{d}{p}\right) = \varepsilon_p \text{ for all } p|N(E)\}$$

We also note:

$$\mathcal{F}'(E, T) = \{d \in \mathcal{F}'(E) \mid |d| < T\}$$

Note that the conditions $\left(\frac{d}{p}\right) = \varepsilon_p$ for all $p|N(E)$ and d is a discriminant are only congruence conditions on d (d is prime) so we have by the Dirichlet density theorem:

$$|\mathcal{F}'(E, T)| \sim b \frac{T}{\log(T)} \quad \text{as } T \rightarrow \infty \quad (7)$$

for a certain $b > 0$.

We need a similar conjecture as conjecture 1 but where the discriminants d are restricted to prime discriminants. For this purpose we have to slightly adapt the work in [CFKRS]. In fact, only the arithmetic factor $a_k(E)$ will be affected. Copying the method of [CFKRS][eqs (4.4.8)-(4.4.16)], we must compute the averages of:

$$\sum_{n_1, \dots, n_k} \frac{a(n_1) \dots a(n_k)}{n_1^s \dots n_k^s} \left(\frac{d}{n_1}\right) \dots \left(\frac{d}{n_k}\right)$$

as d is varying in $\mathcal{F}'(E)$.

Using the notations in [CFKRS], only the terms of the form $n_1 n_2 \dots n_k = g \square$ will contribute where the prime factors of g are also prime factors of $N(E)$ and \square is a square coprime with $N(E)$. In this case, the average of $\left(\frac{d}{n_1}\right) \dots \left(\frac{d}{n_k}\right)$ is $\prod_{p^\alpha || g} \varepsilon_p^\alpha$. Then the factor $R_{k,N}(s; 0, \dots, 0)$ in [CFKRS][eq. (4.4.11)] has to be replaced by:

$$R'_{k,N}(s) = \sum_{\substack{g \square \\ \text{as above}}} \prod_{p^\alpha || g} \varepsilon_p^\alpha \sum_{n_1 \dots n_k = g \square} \frac{a(n_1) \dots a(n_k)}{n_1^s \dots n_k^s} = \prod_p R'_{k,N,p}(s)$$

where if $p \nmid N(E)$:

$$R'_{k,N,p}(s) = \frac{1}{2} \left(\left(1 - \frac{a(p)}{p^s} + \frac{1}{p^{2s-1}} \right)^{-k} + \left(1 + \frac{a(p)}{p^s} + \frac{1}{p^{2s-1}} \right)^{-k} \right)$$

and if $p \mid N(E)$:

$$R'_{k,N,p}(s) = \left(1 - \varepsilon_p \frac{a(p)}{p^s}\right)^{-k}$$

And then the arithmetic factor $a_k(E)$ in conjecture 1 has to be changed to:

$$a'_k(E) = \prod_p (1 - 1/p)^{k(k-1)/2} R_{k,N,p}(1)$$

(note that in [CFKRS], we have to take $s = 1/2$ for the argument in $R_{k,N}(s)$; the difference comes in fact from our normalization of the L -functions).

Finally, we are led to conjecture the following:

Conjecture 4 (Keating-Snaith for prime discriminants) *As $T \rightarrow \infty$*

$$\frac{1}{|\mathcal{F}'(E, T)|} \sum_{d \in \mathcal{F}'(E, T)} L(E_d, 1)^k \sim g_k(O^+) a'_k(E) \log(T)^{k(k-1)/2} \quad (8)$$

Since d is prime there is just one factor for the d part of the Tamagawa numbers. Recall that we have:

$$\text{Tam}_{-d}(E_d) = 1 + \text{the number of roots of } F \text{ in } \mathbb{F}_{-d}$$

where F is the polynomial in equation (6).

Proposition 5 *Assume that the polynomial F has three roots in \mathbb{Q} . Then for all $d \in \mathcal{F}'(E)$ we have $\text{Tam}_{-d}(E_d) = 4$.*

Proposition 6 *Assume that the polynomial F has only one root $a \in \mathbb{Q}$. Let $F(X) = (X - a)Q(X)$ and denote by K the quadratic number field defined by Q and Δ the discriminant of K . Furthermore, suppose that the power of 2 occurring in Δ is even or that $2 \mid N(E)$. Then $\text{Tam}_{-d}(E_d)$ does not depend on d for $d \in \mathcal{F}'(E)$. So, we have either $\text{Tam}_{-d}(E_d) = 2$ or $\text{Tam}_{-d}(E_d) = 4$.*

PROOF. First, we note that the primes dividing Δ also divide $N(E)$ or 2. We let α_2 such that $2^{\alpha_2} \parallel \Delta$ and we can write:

$$\begin{aligned} \left(\frac{\Delta}{-d}\right) &= \prod_{q^\alpha \parallel \Delta, q \neq 2} \left(\frac{q}{-d}\right)^\alpha \times \left(\frac{2}{-d}\right)^{\alpha_2} \\ &= \prod_{q^\alpha \parallel \Delta, q \neq 2} \varepsilon_q^\alpha \times \begin{cases} \varepsilon_2^{\alpha_2} & \text{if } 2 \mid N(E) \\ 1 & \text{otherwise (since here } \alpha_2 \text{ is even)} \end{cases} \end{aligned}$$

Hence, $\left(\frac{\Delta}{-d}\right)$ does not depend on d and $\text{Tam}_{-d}(E_p) = 2$ (resp. 4) if $\left(\frac{\Delta}{-d}\right) = -1$ (resp. 1). \square

Remark: if the hypothesis of the proposition about the power of 2 occurring in Δ does not hold then we have to fix a value for ε_2 and to modify $R'_{k,N,2}(s)$.

Proposition 7 *Assume that the polynomial $F(X)$ is irreducible over \mathbb{Q} . Let K be the number field defined by F , Δ its discriminant. Then, the number $\left(\frac{\Delta}{-d}\right)$ does not depend on d for $d \in \mathcal{F}'(E)$. So, if $\left(\frac{\Delta}{-d}\right) = -1$ then $Tam_{-d}(E_d) = 2$ and if $\left(\frac{\Delta}{-d}\right) = 1$ then $-d$ splits or is inert and we have respectively $Tam_{-d}(E_d) = 4$ or $Tam_{-d}(E_d) = 1$.*

PROOF. As above we note that the primes dividing Δ also divide $N(E)$ or 2. Now the power of 2 occurring in Δ is even or $2 \mid N(E)$. Indeed, suppose that $2 \nmid N(E)$. The power of 2 occurring in Δ has the same parity as the power of 2 occurring in the discriminant of the model (6) which is even because E admits a model with good reduction at 2. The rest of the proof is the same as above. \square

Remarks: With the notations of proposition 7, suppose that K is cyclic and so we must have $\left(\frac{\Delta}{-d}\right) = 1$. Then, by Tchebotarev's density theorem, the density of primes $\in \mathbb{Z}$ which totally split (resp. are inert) in \mathbb{Z}_K is $1/3$ (resp. $2/3$). If there are no arithmetic incompatibilities (and there can exist such incompatibilities since the conductor of K is not coprime to the conductor of K/\mathbb{Q}) with the congruence conditions on $d \pmod{N(E)}$ then $Tam_{-d}(E_d)=4$ (resp. $Tam_{-d}(E_d)=1$) should also occur with a density equal to $1/3$ (resp. $2/3$). In fact, a similar reasoning applies if K is non-abelian and $\left(\frac{\Delta}{-d}\right) = 1$ giving the same density as above for the occurrence of $Tam_{-d}(E_d) = 1$ or 4 (for this purpose, consider the Galois closure of K and the fact that we only consider p that are inert or split in \mathbb{Z}_K which avoids half of the primes).

4 Moment of $S(E_d)$

We want to estimate:

$$M'_E(k, T) = \frac{1}{|\mathcal{F}'(E, T)|} \sum_{d \in \mathcal{F}'(E, T)} S(E_d)^k$$

Let S be the (finite) set of values taken by $Tam_{-d}(E_d)$ for $d \in \mathcal{F}'(E)$. For $\ell \in S$ let b_ℓ be the density of the d in $\mathcal{F}'(E)$ such that $Tam_{-d}(E_d) = \ell$ (see the discussion above). Then, by equations (2) and (4), we have:

$$M'_E(k, T) = \frac{1}{\Omega_E^k} \frac{1}{|\mathcal{F}'(E, T)|} \sum_{\ell \in S} \frac{1}{\ell^k} \sum_{\substack{d \in \mathcal{F}'(E, T) \\ Tam_{-d}(E_d) = \ell}} |d|^{\frac{k}{2}} L(E_d, 1)^k$$

We fix $\ell \in S$ and for simplicity, we write for $t > 0$:

$$t^* = \sum_{\substack{d \in \mathcal{F}'(E, t) \\ Tam_{-d}(E_d) = \ell}} 1$$

So that:

$$t^* \sim bb_\ell \frac{t}{\log(t)}$$

And we have:

$$A := \frac{1}{|\mathcal{F}'(E, T)|} \sum_{\substack{d \in \mathcal{F}'(E, T) \\ Tam_{-d}(E_d) = \ell}} |d|^{\frac{k}{2}} L(E_d, 1)^k \sim \frac{b_\ell}{T^*} \sum_{\substack{d \in \mathcal{F}'(E, T) \\ Tam_{-d}(E_d) = \ell}} |d|^{\frac{k}{2}} L(E_d, 1)^k$$

Now, we assume that we can apply equation (8) for each class of d such that $Tam_{-d}(E_d) = \ell$. Then, using the Abel transform we deduce that:

$$A \sim b_\ell \left(T^{\frac{k}{2}} g_k(O^+) a'_k(E) \log(T)^{\frac{k(k-1)}{2}} - \frac{1}{T^*} \frac{k}{2} \int_2^T t^{\frac{k}{2}-1} \sum_{\substack{d \in \mathcal{F}'(E, t) \\ Tam_{-d}(E_d) = \ell}} L(E_d, 1)^k dt \right)$$

Once again, we use (8) in the integral and by integration by parts we see that the member of the right-hand side of the above formula is equal to:

$$b_\ell g_k(O^+) a'_k(E) \left(T^{\frac{k}{2}} \log(T)^{\frac{k(k-1)}{2}} - \frac{k}{k+2} \frac{bb_\ell}{T^*} T^{\frac{k}{2}+1} \log(T)^{\frac{k(k-1)}{2}-1} \right) + O\left(T^{\frac{k}{2}-1} \log(T)^{\frac{k(k-1)}{2}-1}\right)$$

Now, from the fact that $T^* \sim bb_\ell T / \log(T)$, we have:

$$A \sim b_\ell \frac{2}{k+2} g_k(O^+) a'_k(E) T^{\frac{k}{2}} \log(T)^{\frac{k(k-1)}{2}}$$

Finally, taking the sum over $\ell \in S$ and dividing by Ω_E^k we obtain the following conjecture:

Conjecture 8 *We have as $T \rightarrow \infty$:*

$$M'_E(k, T) \sim \frac{1}{\Omega_E^k} g_k(O^+) a'_k(E) \frac{2}{k+2} \left(\sum_{\ell \in S} \frac{b_\ell}{\ell^k} \right) T^{\frac{k}{2}} \log(T)^{\frac{k(k-1)}{2}} \quad (9)$$

In the next section, we will give some numerical evidence supporting this conjecture. In fact, it also seems to be correct if k is real and not only in \mathbb{N} . Furthermore, classical conjectures predict that:

$$|\{d \in \mathcal{F}'(E, T) \text{ with } L(E_d, 1) = 0\}| = o(|\mathcal{F}'(E, T)|) \quad (10)$$

and since we let $S(E_d) = 0$ if $L(E_d, 1) = 0$, we deduce that conjecture 8 is equivalent to (under equation (10)):

Conjecture 9 *We have as $T \rightarrow \infty$:*

$$\frac{1}{T'^*} \sum_{\substack{d \in \mathcal{F}'(E, T) \\ L(E_d, 1) \neq 0}} |\mathbb{III}(E_d)|^k \sim \frac{1}{\Omega_E^k} g_k(O^+) a'_k(E) \frac{2}{k+2} \left(\sum_{\ell \in S} \frac{b_\ell}{\ell^k} \right) T^{\frac{k}{2}} \log(T)^{\frac{k(k-1)}{2}}$$

where T'^* denotes the number of terms in the sum.

So the conjecture above gives precise informations about the size of $|\text{III}(E_d)|$ of the elliptic curves E_d with rank 0. One can also use the upper bound in (5) to estimate $M'_E(k, T)$; we obtain:

$$\begin{aligned} M'_E(k, T) &\ll \frac{1}{|\mathcal{F}'(E, T)|} \sum_{d \in \mathcal{F}'(E, T)} |d|^{k/2+\varepsilon} \\ &\ll T^{k/2+\varepsilon} \end{aligned}$$

If we compare this upper bound with (9), we deduce:

Conjecture 10 *There exists a positive density of $d \in \mathcal{F}'(E)$ with $L(E_d, 1) \neq 0$ such that $|\text{III}(E_d)| \gg |d|^{1/2-\varepsilon}$.*

5 Example and numerical check of Conjecture 8

In this example, we choose the elliptic curve E of conductor $N = 11$ that is defined by:

$$E : y^2 = F(x) := x^3 - 4x^2 - 160x - 1264 \quad (11)$$

This is a minimal model for E except for the prime $p = 2$. The polynomial F is irreducible over \mathbb{Q} ; let K be the number field defined by it, \mathbb{Z}_K its ring of integers and $D_{K/\mathbb{Q}} = -44$ its discriminant. We consider prime discriminants $d < 0$ such that the functional equation of E_d has sign $\varepsilon(E_d) = 1$, hence we must have $d \equiv 2, 6, 7, 8, 10 \pmod{11}$. Note that in this case, $\left(\frac{D_{K/\mathbb{Q}}}{-d}\right) = 1$ so the prime $-d$ is inert or splits in K (cf. proposition 7). Furthermore, there are no arithmetical restrictions for the density of d with $Tam_{-d}(E_d) = 4$ or 1 ; by Tchebotarev's theorem these densities are respectively $1/3$ and $2/3$, so:

$$\sum_{\ell \in S} \frac{b_\ell}{\ell^k} = \frac{2}{3} + \frac{1}{3 \times 4^k}$$

Furthermore, a little calculation shows that:

$$\Omega_E \approx 2.917633233876990458661779$$

We used the huge numerical data computed by Rubinstein ([Rub]) in order to check the conjectured formula (9). For this, we computed $M'_E(k, T)$ for $T = 10^6, 2 \times 10^6, \dots, 99 \times 10^6$ and $k = 1, 2, 3$ in figure (1) and (2). We plotted the graph $(T, M'_E(k, T)T^{1-k/2}/\log(T)^{k(k-1)/2})$ (in order to get something looking like a line), and we compare the graph with the prediction (9).

As a consequence of a theorem of Waldspurger, the numbers $S(E_d)$ are related to the coefficients $c(n)$ of a weight $3/2$ modular form. This modular form has the following q -expansion computed by Rodriguez-Villegas (cf.[CFKRS]):

$$\sum_{n \geq 1} c(n)q^n = \frac{\theta_1(q) - \theta_2(q)}{2}$$

where

$$\begin{aligned}\theta_1(q) &= \sum_{\substack{(x,y,z) \in \mathbb{Z}^3 \\ x \equiv y \pmod{2}}} q^{x^2+11y^2+11z^2} \\ \theta_2(q) &= \sum_{\substack{(x,y,z) \in \mathbb{Z}^3 \\ x \equiv y \pmod{3} \\ z \equiv y \pmod{2}}} q^{(x^2+11y^2+33z^2)/3}\end{aligned}$$

And we have:

$$S(E_d) = \begin{cases} c(|d|)^2 & \text{if } -d \text{ is inert in } K \\ \left(\frac{c(|d|)}{2}\right)^2 & \text{if } -d \text{ splits in } K \end{cases}$$

As a consequence of the Birch and Swinnerton-Dyer conjecture $S(E_d)$ must be an integer, we deduce that:

$$-d \text{ splits in } K \Rightarrow c(|d|) \text{ is even}$$

In fact, we have in full generality:

Theorem 11 *Let p be a prime number such that $-p$ is a fundamental discriminant and such that $\left(\frac{-11}{p}\right) = 1$ (so p is inert or splits in K), then:*

$$p \text{ splits in } K \Leftrightarrow c(|p|) \equiv 0 \pmod{2}$$

First, we proof the following lemma:

Lemma 12 *Let p be as in the theorem. Either p is of the form $3x^2 + 2xy + 4y^2$ and $c(p)$ is odd or p is of the form $x^2 + 11y^2$ and $c(p)$ is even.*

PROOF OF THE LEMMA. We consider the two following sets:

$$\begin{aligned}R_1 &= \{(x, y, z) \in \mathbb{Z}^3 \mid x \equiv y \pmod{2} \text{ and } x^2 + 11y^2 + 11z^2 = p\} \\ R_2 &= \{(x, y, z) \in \mathbb{Z}^3 \mid x \equiv y \pmod{3}, z \equiv y \pmod{2} \text{ and } x^2 + 11y^2 + 33z^2 = 3p\}\end{aligned}$$

and we compute $|R_1|$ and $|R_2| \pmod{4}$. For R_1 , we see that if $(x, y, z) \in R_1$ then $(\pm x, \pm y, \pm z) \in R_1$ and since there is at most one of y, z which can vanish we deduce that $|R_1| \equiv 0 \pmod{4}$.

For R_2 , if $(x, y, z) \in R_2$ with $z \neq 0$ then $x \neq 0$ and the points $(x, y, \pm z)$, $(-x, -y, \pm z)$ belong to R_2 ; hence $|\{(x, y, z) \in R_2 \mid z \neq 0\}| \equiv 0 \pmod{4}$. Now if $z = 0$, we must compute:

$$|\{(x, y) \in \mathbb{Z}^2 \mid x \equiv y \pmod{3} \text{ and } x^2 + 11y^2 = 3p\}|$$

(the condition $y \equiv 0 \pmod{2}$ is here automatic since we have $p \equiv 3 \pmod{4}$). Eliminating the condition $x \equiv y \pmod{3}$ (by the change of variables $x = y + 3x'$), we see that we have to compute the number of solutions of:

$$p = 3x'^2 + 2xy + 4y^2 \tag{12}$$

There are 3 classes of primitive binary quadratic forms of discriminant -44 modulo $SL_2(\mathbb{Z})$. As a set of representatives we can choose the 3 following forms:

$$\begin{aligned} Q_1(x, y) &= 3x^2 + 2xy + 4y^2 \\ Q_2(x, y) &= 3x^2 - 2xy + 4y^2 \\ Q_3(x, y) &= x^2 + 11y^2 \end{aligned}$$

Since p splits in $L = \mathbb{Q}(\sqrt{-11})$, either p can be represented by Q_1 (and Q_2) (with only 2 solutions for each quadratic form) or p can be represented by Q_3 . If p is represented by Q_1 , there are 2 solutions in (12); so $|R_2| \equiv 2 \pmod{4}$ and $c(p)$ is odd. If p is represented by Q_3 , there are no solutions in (12) so $|R_2| \equiv 0 \pmod{4}$ and $c(p)$ is even. \square

PROOF OF THE THEOREM. By the lemma, we need to prove that p splits if and only if p can be represented by Q_3 . For this purpose, let M be the Galois closure of K . Then $[M : \mathbb{Q}] = 6$ and M is the compositum of K and of L . Since $\left(\frac{-11}{p}\right) = 1$, p splits in L and we can write $(p) = \mathfrak{p}_p \overline{\mathfrak{p}_p}$ in L . Furthermore, we see that p is inert (resp. splits) in K/\mathbb{Q} if and only if \mathfrak{p}_p is inert (resp. splits) in M/L . One can also see that M is, in fact, the ray class field of L for the modulus (2) (2 is inert in L/\mathbb{Q}). Let $I_{(2)}$ be the group of ideals coprime to (2) in \mathbb{Z}_L and $P_{(2)}$ the ray group of (2) so that we have $Gal(M/L) \simeq I_{(2)}/P_{(2)} \simeq \mathbb{Z}/3\mathbb{Z}$. Suppose that p can be represented by the quadratic form Q_1 . Then $3p = x^2 + 11y^2$ and we can assume without loss of generality that:

$$\mathfrak{p}_3 \mathfrak{p}_p = \left(\frac{2x + 2y\sqrt{-11}}{2} \right) \in \mathbb{Z}_L$$

where \mathfrak{p}_3 is a prime above (3). We deduce that $\mathfrak{p}_3 \mathfrak{p}_p \in P_{(2)}$, and so we have $Art_{M/L}(\mathfrak{p}_3 \mathfrak{p}_p) = 1 \in Gal(M/L)$, where the symbol Art stands for the Artin map. Furthermore, we also have $\mathfrak{p}_3 = \left(\frac{1 + \sqrt{-11}}{2} \right) \notin P_{(2)}$ so $Art_{M/L}(\mathfrak{p}_3) \neq 1$, and we must have $Art_{M/L}(\mathfrak{p}_p) \neq 1$. Then \mathfrak{p}_p is inert in M .

Suppose that p can be represented by the quadratic form Q_3 . Then $p = x^2 + 11y^2$ and we easily check that $Art_{M/L}(\mathfrak{p}_p) = 1$; hence \mathfrak{p}_p splits in M . \square

Corollary 13 *The density of $d \in \mathcal{F}'(E)$, such that $S(E_d)$ is divisible by 2 is $\leq 1/3$.*

PROOF. By Tchebotarev's density theorem, the density of the primes p which split in K inside the set of primes which are inert or split in K is $1/3$. \square

Remark: This is in contradiction with the heuristic in [De1] which would have suggested a density of about 58%. Numerically, it appears that half of the $d \in \mathcal{F}'(E)$ with $-d$ split in K are such that $2 \mid S(E_d)$. Thus the density of $S(E_d)$ that are divisible by 2 should be $1/6$ in the whole family. In fact, the effect of taking only prime discriminants $d \in \mathcal{F}(E)$ has a large consequence on

the 2-divisibility of $S(E_d)$. This effect seems to disappear if we consider all discriminants $d \in \mathcal{F}(E)$. For example, the density of $d \in \mathcal{F}(E, 10^7)$ for which $S(E_d) \equiv 0 \pmod{2}$ is about ≈ 0.38 . We expect that the correct density is the one predicted by the heuristic but that the convergence is slow (cf. [De2]). For example, it is the case for the curve $y^2 = x^3 - x^2$ (due to the results of [H-B1], [H-B2]).

Corollary 14 5 *If $d \in \mathcal{F}'(E)$ is inert in K then the rank of E_d is 0.*

Remarks: 1- This corollary means that if we restrict the discriminants to be inert, the constant c_E in conjecture 1 of [CKRS] is 0. Of course, we must consider also the discriminants which split in K and the contradiction disappears. But, there may exist an elliptic curve E such that an arithmetic restriction of the same type as in theorem 11 is valid for all the prime discriminants. It is in fact the case, for example, for the curve 17A ([De3]). However, if we consider all discriminants and not only primes, there is no contradiction any more with the conjecture.

2- The corollary as well as the result about the curve 17A mentioned in the remark above can also be obtained by 2-descent (cf. [An-Bu-Fr][example 1.15]).

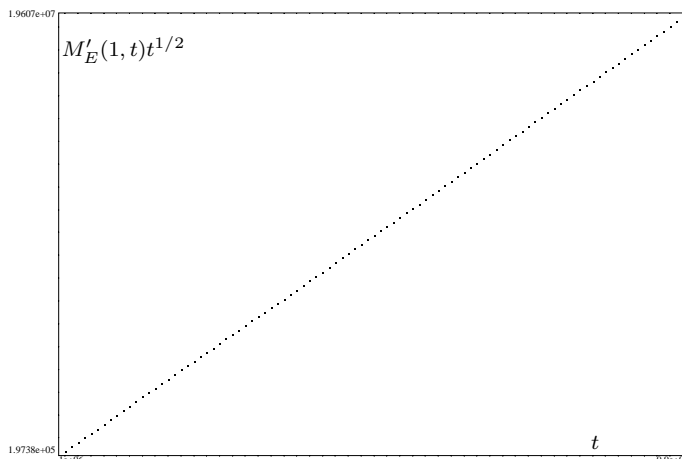


Figure 1: The points $(t, M'_E(1, t)t^{1/2})$ for $t/10^6 = 1, 2, \dots, 99$ and for the curve of conductor 11. The correlation coefficient is ≈ 0.999992 . The best fitting line has a slope ≈ 0.198 . The conjectural value given by formula (9) is ≈ 0.202 .

6 Family of twists over fundamental discriminants

In this section, we obtain conjectures for the moments of the orders of Tate-Shafarevich groups in a family of twists as in the section 4 except that the discriminants are not restricted to be prime, so, our discriminants run now over

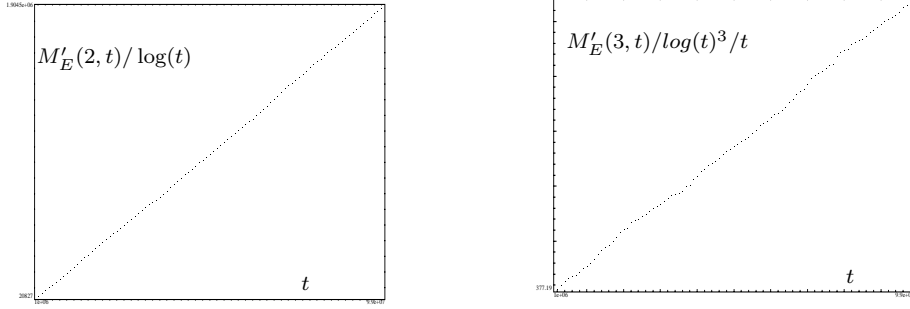


Figure 2: The analogue of figure 1 for the moments of order 2 (on the left) and of order 3 (on the right). The correlation coefficients are respectively 0.99993 and 0.9995. The slope of the best fitting lines are respectively ≈ 0.0192 and ≈ 0.00027 . The conjectural values given by formula (9) are respectively ≈ 0.0157 and ≈ 0.000094 .

$\mathcal{F}(E)$. The idea is first to control on average the contribution coming from the product of the Tamagawa numbers over the primes dividing d . More precisely, we will obtain below the following estimate as $T \rightarrow \infty$:

$$\sum_{d \in \mathcal{F}(E, T)} \delta_8(c_4, d)^{-k} \prod_{p|d} Tam_p(E_d)^{-k} \sim A T \log(T)^a \quad (13)$$

for some explicit constants A and a both depending on k and E . Second, using the same technique as above and the conjecture 1, we should have:

$$\frac{1}{|\mathcal{F}(E, T)|} \sum_{d \in \mathcal{F}(E, T)} |d|^{k/2} L(E_d, 1)^k \sim B T^{k/2} \log(T)^{k(k-1)/2}$$

where:

$$B = g_k(O^+) a_k(E) \frac{2}{k+2}$$

Then, in order to estimate:

$$\frac{1}{|\mathcal{F}(E, T)|} \sum_{d \in \mathcal{F}(E, T)} |d|^{k/2} L(E_d, 1)^k \delta_8(c_4, d)^{-k} \prod_{p|d} Tam_p(E_d)^{-k}$$

we use the empirical argument that consists in replacing in the sum above the term $\delta_8(c_4, d)^{-k} \prod_{p|d} Tam_p(E_d)^{-k}$ by its average over d (since the power of T in (13) is equal to 1). Finally, we obtain:

$$\frac{1}{|\mathcal{F}(E, T)|} \sum_{d \in \mathcal{F}(E, T)} S(E_d)^k \sim \frac{1}{\Omega_E^k} A B T^{k/2} \log(T)^{k(k-1)/2+a}$$

Hence,

Conjecture 15 *There exist $A_E > 0$ and c_E such that as $T \rightarrow \infty$:*

$$M_E(k, T) \sim A_E T^{k/2} \log(T)^{c_E} \quad (14)$$

and we also have:

$$\frac{1}{T^*} \sum_{\substack{d \in \mathcal{F}(E, T) \\ L(E_d, 1) \neq 0}} |\mathfrak{III}(E_d)|^k \sim A_E T^{k/2} \log(T)^{c_E} \quad (15)$$

where T^* denotes the number of terms in the sum.

The second estimate of the conjecture above come from classical conjectures which predict that the density of $d \in \mathcal{F}(E)$ such that $L(E_d, 1) = 0$ is 0 (as in equation (10)). One can also use the upper bound in (5) to estimate $M_E(k, T)$; we obtain $M_E(k, T) \ll T^{k/2+\varepsilon}$ and with (15):

Conjecture 16 *There exists a positive density of $d \in \mathcal{F}(E)$ with $L(E_d, 1) \neq 0$ such that $|\mathfrak{III}(E_d)| \gg |d|^{1/2-\varepsilon}$.*

In the rest of this section, we compute the numbers A and a of equation (13).

6.1 Average of the product of the Tamagawa numbers

We need some technical results

Theorem 17 *Let $N \in \mathbb{N}$ and $J = (\mathbb{Z}/N\mathbb{Z})^*$ so that $|J| = \varphi(N)$. For all $j \in J$, we define the arithmetical function w_j by:*

$$\omega_j(n) = |\{p|N, p \equiv j \pmod{N}\}|$$

Furthermore, suppose that for all $j \in J$ we are given a nonnegative real number t_j and let $t = |J|^{-1} \sum_{j \in J} t_j$. If $a \in J$, we have, as $T \rightarrow \infty$:

$$\begin{aligned} \sum_{\substack{n \leq T \\ n \equiv a \pmod{N} \\ n \text{ squarefree}}} \prod_{j \in J} t_j^{\omega_j(n)} &\sim \frac{1}{|J|\Gamma(t)} T \log(T)^{t-1} \prod_{p|N} \left(1 - \frac{1}{p}\right)^t \\ &\times \prod_{j \in J} \prod_{p \equiv j \pmod{N}} \left(1 + \frac{t_j}{p}\right) \left(1 - \frac{1}{p}\right)^{t_j} \end{aligned}$$

Remark: in the formula above, the product over the prime $p \equiv j \pmod{N}$ is absolutely converging.

Let ξ be a character \pmod{N} , we define the Dirichlet serie G_ξ by:

$$G_\xi(s) = \sum_{\substack{(n, N)=1 \\ n \text{ squarefree}}} \frac{\xi(n)}{n^s} \prod_{j \in J} t_j^{\omega_j(n)} \quad (16)$$

Hence, we have:

$$\sum_{\substack{n \equiv a \pmod N \\ n \text{ squarefree}}} \frac{1}{n^s} \prod_{j \in J} t_j^{\omega_j(n)} = \frac{1}{\varphi(N)} \sum_{\xi} \overline{\xi(a)} G_{\xi}(s) \quad (17)$$

where the last sum is over all character $\pmod N$. In order to get an estimate of the sum of the coefficients of the Dirichlet serie of the left hand size of (17) it suffices to estimate the sum of the coefficients of each G_{ξ} .

Lemma 18 *With the notations above, we have:*

$$\sum_{\substack{(n, N)=1 \\ n \text{ squarefree} \\ n \leq T}} \xi(n) \prod_{j \in J} t_j^{\omega_j(n)} \sim C_{\xi} X \log(X)^{t_{\xi}-1} + O\left(\frac{\log \log(X)}{\log(X)}\right) \quad (18)$$

where $t_{\xi} = |J|^{-1} \sum_{j \in J} t_j \xi(j)$,

$$\begin{aligned} C_{\xi} &= \frac{\prod_{p|N} (1 - 1/p)^{t_{\xi}}}{\Gamma(t_{\xi})} \prod_{j \in J} \prod_{p \equiv j \pmod N} \left(1 + \frac{t_j \xi(p)}{p}\right) \left(1 - \frac{\xi(p)}{p}\right)^{t_j} \\ &\times \exp\left(\sum_{j \in J} \frac{t_j}{|J|} \left(G_{j, \xi}(1) + \sum_{\chi \neq \overline{\xi}} \chi(j) \log(L(1, \chi))\right)\right) \end{aligned}$$

the function $G_{j, \xi}(s)$ is a certain serie absolutely converging for $\Re(s) > 1/2$ and can also be defined by:

$$G_{j, \xi}(s) = -\varphi(N) \sum_{p \equiv j \pmod N} \log\left(1 - \frac{\xi(p)}{p^s}\right) - \sum_{\chi} \overline{\chi(j)} \log(L(s, \chi \xi))$$

PROOF OF THE LEMMA 18. We follow the paper of F. Ben Saïd and J. L. Nicolas ([BS-Ni]) where the authors proof a more general result except that in their article the prime p satisfies congruences modulo k (with their notations) which is coprime to N (ξ is a charater modulo N), whereas in our case we have $k = N$ and so there are just slight modifications to perform. The assertions about the functions $G_{j, \xi}$ is exactly the Lemme 2 of [BS-Ni].

We have:

$$\begin{aligned} G_{\xi}(s) &= \prod_{j \in J} \prod_{p \equiv j \pmod N} \left(1 + \frac{t_j \xi(p)}{p^s}\right) \\ &= H_{\xi}(s) \prod_{j \in J} \prod_{p \equiv j \pmod N} \left(1 - \frac{\xi(p)}{p^s}\right)^{-t_j} \end{aligned}$$

where:

$$H_{\xi}(s) = \prod_{j \in J} \prod_{p \equiv j \pmod N} \left(1 + \frac{t_j \xi(p)}{p^s}\right) \left(1 - \frac{\xi(p)}{p^s}\right)^{t_j}$$

is absolutely converging for $\Re(s) > 1/2$. Then:

$$\begin{aligned} G_\xi(s) &= H_\xi(s) \exp \left(- \sum_j t_j \sum_{p \equiv j \pmod N} \log(1 - \xi(p)/p^s) \right) \\ &= H_\xi(s) \exp \left(\frac{1}{\varphi(N)} \sum_j t_j \left(G_{j,\xi}(s) + \sum_{\chi \neq \bar{\xi}} \overline{\chi(j)} \log(L(s, \chi\xi)) \right) \right) \\ &\times \zeta(s)^{t_\xi} \prod_{p|N} \left(1 - \frac{1}{p^s} \right) \end{aligned}$$

Now, following the proof of “Théorème 1, Deuxième cas” in [BS-Ni], we have that:

$$|G_\xi(s)/\zeta(s)^{t_\xi}| \leq M_\xi(3 + |\Im(s)|)^{1/2}$$

Furthermore, the absolute values of the coefficients of G_ξ are bounded by the coefficients of G_{ξ_0} , where ξ_0 denote the trivial character modulo N . Hence one can apply the “théorème A” of [BS-Ni] and the lemma follows. \square

PROOF OF THE THEOREM 17. We remark that if the character ξ is not trivial there is at least one $j \in J$ such that $\xi(j) \neq 1$ and we have $|t_\xi| < |t_{\xi_0}|$ (since for all j , $t_j \geq 0$). So, when we sum the coefficients of the series G_ξ using the equation 17, we see that the main term is obtained for the trivial character ξ_0 and we have:

$$\sum_{\substack{n \leq T \\ n \equiv a \pmod N \\ n \text{ squarefree}}} t^{\omega_j(n)} \sim T \log(T)^{t-1} \frac{C_{\xi_0}}{|J|\Gamma(t)}$$

Adapting the proof of “lemme 4” of [BS-Ni], we obtain that:

$$\exp \left(\sum_{j \in J} \frac{t_j}{|J|} \left(G_{j,\xi_0}(1) + \sum_{\chi \neq \bar{\xi_0}} \overline{\chi(j)} \log(L(1, \chi)) \right) \right) = 1$$

and the theorem follows. \square

We deduce from theorem 17 the two corollaries:

Corollary 19 *Let $N \in \mathbb{N}$, $t \in \mathbb{R}_+$ and $a \in \mathbb{N}$ coprime with N , we have:*

$$\sum_{\substack{n \leq T \\ n \equiv a \pmod N \\ n \text{ squarefree}}} t^{\omega(n)} \sim \frac{1}{\varphi(N)\Gamma(t)} T \log(T)^{t-1} P(N, t)$$

where $P(N, t) = \prod_{p|N} \left(1 - \frac{1}{p} \right)^t \times \prod_{(p,N)=1} \left(1 + \frac{t}{p} \right) \left(1 - \frac{1}{p} \right)^t$ and $\omega(n)$ is the number of prime dividing n .

Corollary 20 *Let $N \in \mathbb{N}$ such that N is not a square, let t_+, t_- two nonnegative real numbers. Define ω_+ and ω_- by:*

$$\omega_{\pm}(n) = |\{p|n, \left(\frac{N}{p}\right) = \pm 1\}|$$

Then, if $(a, N) = 1$, we have:

$$\sum_{\substack{n \leq T \\ n \equiv a \pmod{N} \\ n \text{ squarefree}}} t_+^{\omega_+(n)} t_-^{\omega_-(n)} \sim \frac{1}{\varphi(N)\Gamma\left(\frac{t_++t_-}{2}\right)} T \log(T)^{\frac{t_++t_-}{2}-1} Q(N, t_+, t_-)$$

$$\text{where } Q(N, t_+, t_-) = \prod_{p|N} \left(1 - \frac{1}{p}\right)^{\frac{t_++t_-}{2}} \times \prod_{\substack{(p, N)=1 \\ \left(\frac{N}{p}\right)=\varepsilon}} \left(1 + \frac{t_{\varepsilon}}{p}\right) \left(1 - \frac{1}{p}\right)^{t_{\varepsilon}}.$$

We apply the results above to the study of the product of the Tamagawa numbers. For this, we need some notations. Let $N(E)$ be the conductor of the elliptic curve E then we note:

$$\tilde{N} = \prod_{p|N} p \times \begin{cases} 1 & \text{if } N(E) \text{ is odd} \\ 4 & \text{if } N(E) \text{ is even} \end{cases}.$$

The conditions $\left(\frac{d}{p}\right) = \varepsilon_p$ restricted to the discriminants $d \in \mathcal{F}(E)$ are in fact congruence conditions on d modulo \tilde{N} ; there exist $A \subset \mathbb{Z}/\tilde{N}\mathbb{Z}$ such that:

$$d \in \mathcal{F}(E) \Leftrightarrow d \text{ is a fundamental discriminant } < 0 \text{ and } \bar{d} \in A$$

where \bar{d} denotes the image of d in $\mathbb{Z}/\tilde{N}\mathbb{Z}$. Since each odd prime $p | \tilde{N}$ implies exactly $(p-1)/2$ congruences, one can see that:

$$|A| = \prod_{\substack{(p|\tilde{N} \\ p \neq 2}} \frac{p-1}{2} \quad (\times 2 \text{ if } \tilde{N} \text{ is even})$$

We let $\delta_8(c_4) = 1$ if c_4 is odd and $\delta_8(c_4) = 2$ otherwise. Finally, we define $T_2(k, E)$ by:

$$T_2(k, E) = \left(1 + \frac{Tam_2(E_{-4})^{-k} + \delta_8(c_4)^{-k} Tam_2(E_{-8})^{-k}}{2}\right)$$

Theorem 21 *With the notations above, suppose that the polynomial F in (6) has three roots in \mathbb{Q} , then if \tilde{N} is odd:*

$$\sum_{d \in \mathcal{F}(E, T)} \delta_8(d, c_4)^{-k} \prod_{p|d} Tam_p(E_d)^{-k} \sim T \log(T)^{\frac{1}{4k}-1} \frac{|A| P(2\tilde{N}, 1/4)}{2\Gamma(1/4^k)\varphi(\tilde{N})} T_2(k, E)$$

And if \tilde{N} is even:

$$\sum_{d \in \mathcal{F}(E, T)} \prod_{p|d} Tam_p(E_d)^{-k} \sim T \log(T)^{\frac{1}{4^k}-1} \frac{|A|P(\tilde{N}, 1/4)}{\Gamma(1/4^k)\varphi(\tilde{N})}$$

PROOF. We let $t = 1/4^k$. If \tilde{N} is odd we separate the odd and even discriminants. We remark that if $4||d$ (resp. $8||d$) then $Tam_2(E_d) = Tam_2(E_{-4})$ (resp. $= Tam_2(E_{-8})$). So we can write:

$$\begin{aligned} \sum_{d \in \mathcal{F}(E, T)} \delta_8(d, c_4)^{-k} \prod_{p|d} Tam_p(E_d)^{-k} &= \sum_{\substack{d < T \\ \bar{d} \in A \\ d \equiv 1, 5 \pmod{8} \\ d \text{ squarefree}}} t^{\omega(d)} \\ &+ Tam_2(E_{-4}) \sum_{\substack{d < T/4 \\ \bar{d} \in 4^{-1}A \\ d \equiv 3, 7 \pmod{8} \\ d \text{ squarefree}}} t^{\omega(d)} \\ &+ \delta_8(c_4) Tam_2(E_{-8}) \sum_{\substack{d < T/8 \\ \bar{d} \in 8^{-1}A \\ d \equiv 1 \pmod{2} \\ d \text{ squarefree}}} t^{\omega(d)} \end{aligned}$$

Now, we use Corollary 19 for each of the sum above: the congruence conditions are modulo $8\tilde{N}$ (resp. $2\tilde{N}$) for the first two sums (resp. the last sum), we have $2|A|$ (resp. $|A|$) possible congruences and $\varphi(8\tilde{N}) = 4\varphi(\tilde{N})$. Whenever \tilde{N} is even the discriminants must be odd and a single use of the Corollary 19 is needed. \square

Theorem 22 *Suppose that the polynomial F in (6) has only one root a in \mathbb{Q} . We denote by Δ the discriminant of the quadratic number field defined by $F(X)/(X-a)$. Furthermore, we suppose that the 2-adic valuation of \tilde{N} has the same parity as the 2-adic valuation of Δ . We let $t = (1/4^k + 1/2^k)/2$. If \tilde{N} is odd, we have:*

$$\sum_{d \in \mathcal{F}(E, T)} \delta_8(d, c_4)^{-k} \prod_{p|d} Tam_p(E_d)^{-k} \sim T \log(T)^{t-1} \frac{|A|Q(2\tilde{N}, 1/4, 1/2)}{2\Gamma(t)\varphi(\tilde{N})} T_2(k, E)$$

And if \tilde{N} is even:

$$\sum_{d \in \mathcal{F}(E, T)} \prod_{p|d} Tam_p(E_d)^{-k} \sim T \log(T)^{t-1} \frac{|A|Q(\tilde{N}, 1/4, 1/2)}{\Gamma(t)\varphi(\tilde{N})}$$

PROOF. With the conditions of the theorem, then if p is an odd prime we have $Tam_p(E_d) = 2$ (resp. 4) if $\left(\frac{\Delta}{p}\right) = -1$ (resp. $\left(\frac{\Delta}{p}\right) = 1$). So, we can apply Corollary 20 with $t_+ = 1/4^k$ and $t_- = 1/2^k$. \square

Remarks. 1. Using the same technique, one can obtain a similar result without the conditions of the theorem about the 2-adic valuation of Δ .

2. If the polynomial F is irreducible over \mathbb{Q} and the extension K/\mathbb{Q} is Galois then one can obtain also a similar result since in this case we will have $Tam_p(E_d) = 1$ or 4 and the exact value will be determined by some congruence conditions modulo the conductor of K/\mathbb{Q} .

7 Rank 1 case

In this section, we consider a family of quadratic twists of E with rank 1. Thus, we define:

$$\mathcal{F}_-(E) = \{d < 0 \text{ fundamental discriminant}, \varepsilon(E_d) = -1\}$$

and

$$\mathcal{F}_-(E, T) = \{d \in \mathcal{F}_-(E), |d| < T\}$$

Remark. One could also restrict our discriminants with some additional conditions as in the rank 0 case. We would have obtain a similar study.

The Birch and Swinnerton-Dyer conjecture can now be stated as:

$$L'(E_d, 1) = \frac{\Omega(E_d)Tam(E_d)}{|E_d(\mathbb{Q})_{\text{tors}}|^2} R(E_d)S(E_d)$$

where $R(E_d)$ is the regulator of E_d and $S(E_d)$ the order of the Tate-Shafarevich group of E_d if $L'(E_d, 1) \neq 0$ and $S(E_d) = 0$ otherwise. By proposition 2 we deduce:

$$L'(E_d, 1) = \frac{\Omega_E}{\sqrt{|d|}} \prod_{p|d} Tam_p(E_d) R(E_d) S(E_d) \delta_8(c_4, d)$$

Furthermore, as we saw before $Tam_p(E_d) \leq 4$ ([Sil]) and

$$\prod_{p|d} Tam_p(E_d) \leq 4^{\omega(d)} \ll_{\varepsilon} |d|^{\varepsilon} \quad (19)$$

where $\omega(d)$ is the number of primes dividing d . Hence we obtain:

$$L'(E_d, 1) \ll_{\varepsilon} R(E_d)S(E_d)|d|^{\varepsilon-1/2} \quad (20)$$

The philosophy of Keating and Snaith suggests that the moments of $L'(E_d, 1)$ should behave as the moments of the derivative of characteristic polynomials of $SO(2N+1)$ evaluated at 1 ([Sna]). More precisely, this implies that we should have:

$$\frac{1}{|\mathcal{F}_-(E, T)|} \sum_{d \in \mathcal{F}_-(E, T)} L'(E_d, 1)^k \sim \tilde{a}_E(k) \log(T)^{k(k+1)/2} \quad (21)$$

for some constant $\tilde{a}_E(k) > 0$. Note that for $k = 1$ this is in accordance with the results in ([Mu-Mu]). Furthermore, it is also conjectured that the number

of $d \in \mathcal{F}_-(E, T)$ such that $L'(E_d, 1) = 0$ is $o(T)$. Now using (20) and the same technique as the rank 0 case, we have:

$$\begin{aligned} \frac{1}{T^*} \sum_{\substack{d \in \mathcal{F}'_-(E, T) \\ L'(E_d, 1) \neq 0}} R(E_d)^k S(E_d)^k &\gg \frac{1}{T^*} \sum_{\substack{d \in \mathcal{F}'_-(E, T) \\ L'(E_d, 1) \neq 0}} L'(E_d, 1)^k |d|^{k/2-\varepsilon} \\ &\gg T^{k/2-\varepsilon} \end{aligned} \quad (22)$$

Where T^* denotes the number of terms in the sum. Note that the constant involved in this lower bound depends on k , ε and on E . By the inequality of Hölder we have:

$$\begin{aligned} \left(\sum R(E_d)^{k\ell} \right)^{1/\ell} &\gg \frac{\sum R(E_d)^k S(E_d)^k}{\left(\sum S(E_d)^{kp} \right)^{1/p}} \quad \text{where } \frac{1}{p} + \frac{1}{\ell} = 1 \\ &\gg \frac{T^{1+k/2-\varepsilon-1/p}}{\left(\frac{1}{T^*} \sum S(E_d)^{kp} \right)^{1/p}} \end{aligned} \quad (23)$$

where \sum stands for the sum over $d \in \mathcal{F}'_-(E, T)$ such that $L'(E_d, 1) \neq 0$. Now by the heuristic in [De1] in the rank 1 case (see [De2] for a modification in this case), the average:

$$\frac{1}{T^*} \sum S(E_d)^{kp}$$

should tend to a finite value $b(kp) > 0$ as T tends to ∞ whenever $kp < 1$. In fact, there could be some special primes ([De2]) which have an effect on $b(kp)$ and so this number could depend on E . Nevertheless, this suggests that we can include the denominator of equation (23) in the constant and

$$\frac{1}{T^*} \sum R(E_d)^{k\ell} \gg_{\varepsilon, k, \ell} T^{\frac{k\ell}{2}-\varepsilon} \quad \text{where } k < \frac{\ell-1}{\ell}$$

Taking for example $\ell = a + 1 + 1/a$ and $k = a/\ell$, we conjecture:

Conjecture 23 *With the notations above we have for all $a > 0$, as $T \rightarrow \infty$:*

$$\frac{1}{T^*} \sum_{\substack{d \in \mathcal{F}'_-(E, T) \\ L'(E_d, 1) \neq 0}} R(E_d)^a \gg_{\varepsilon, a, E} T^{\frac{a}{2}-\varepsilon}$$

We can also use the empirical argument of replacing in the left-hand side of:

$$\sum_{\substack{d \in \mathcal{F}'_-(E, T) \\ L'(E_d, 1) \neq 0}} S(E_d)^k R(E_d)^k = \frac{1}{\Omega_E^k} \sum_{\substack{d \in \mathcal{F}'_-(E, T) \\ L'(E_d, 1) \neq 0}} |d|^{k/2} L'(E_d, 1)^k \delta_8(d, c_4)^{-k} \prod_{p|d} Tam_p(E_d)^{-k}$$

the term $S(E_d)^k$ by its average (that is, if $k < 1$, by some number which is predicted by the heuristic principle) and to estimate the right-hand side by the

same methods as in the rank 0 case. We should have obtained the following: if $k < 1$ then:

$$\frac{1}{T^*} \sum_{\substack{d \in \mathcal{F}'(E, T) \\ L'(E_d, 1) \neq 0}} R(E_d)^k \sim a_E T^{k/2} \log(T)^{b_E} \quad (24)$$

for some constants $a_E > 0$ and b_E (with for example $b_E = k(k+1)/2$ if we restrict to prime discriminants). By the lack of numerical experiments, we do not know what to think of equation (24).

References

- [An-Bu-Fr] J. A. Antoniadis M. Bungert and G. Frey, *Properties of twists of elliptic curves*, J. Reine Angew. Math. **405** (1990), 1–28.
- [BS-Ni] F. Ben Saïd and J.-L. Nicolas, *Sur une application de la formule de Selberg-Delange*, Coll. Math. **98** (2003) no.2, 223-247.
- [Bre et al.] 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.
- [CKRS] J. B. Conrey, J. P. Keating, M. O. Rubinstein and N. C. Snaith, *On the frequency of vanishing of quadratic twists of modular L-functions*, Number theory for the millennium, I (Urbana, IL, 2000), 301–315, A K Peters, Natick, MA, 2002.
- [CFKRS] J. B. Conrey, D. W. Farmer J. P. Keating, M. O. Rubinstein and N. C. Snaith, *Integral moments of L-functions*, preprint.
- [De1] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over \mathbb{Q}* , Exp. Math. **10** (2001), no. 2, 191–196.
- [De2] C. Delaunay, *The magic of the Cohen-Lenstra heuristics*, preprint.
- [De3] C. Delaunay, *Vanishing of L-functions of elliptic curves in certain families of quadratic twists*, in preparation.
- [We] B. M. M. de Weger, *A + B = C and big III's*, Quart. J. Math. Oxford **49** (1998), 105–128.
- [H-B1] D. R. Heath-Brown, *The size of the Selmer group for the congruent number problem, I*, Invent. Math. **111**, (1993), pp. 111-125.
- [H-B2] D. R. Heath-Brown, *The size of the Selmer group for the congruent number problem, II*, Invent. Math. **118**, (1994), pp. 331-370.
- [K-S] J. P. Keating and N. .C. Snaith, *Random matrix theory and L-functions at $s = 1/2$* , Comm. Math. Phys. **214** (2000), 91–110.

- [Go-Sz] D. Goldfeld and L. Szpiro, *Bounds for the order of the Tate-Shafarevitch group*, *Comp. Math.* **97** (1995), 71–87.
- [Ma-Mu] L. Mai and M. R. Murty, *A note on quadratic twists of an elliptic curve*, In *Elliptic curves and related topics*, 121–124, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, RI, 1994.
- [Mu-Mu] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L -series*, *Annals of Math.* **133** (1991), 447–475.
- [Rub] M. Rubinstein, *Numerical data*, available at www.math.uwaterloo.ca/~mrubinst/L_function/VALUES/DEGREE_2/ELLIPTIC/QUADRATIC_TWISTS/WEIGHT_THREE_HALVES/
- [Sil] J. H. Silverman *Advanced topics in the arithmetic of elliptic curves*, Graduate text in Math. **151**, Springer-Verlag, New-York (1994).
- [Sna] N. Snaith, *Derivatives of random matrix characteristic polynomials with applications to elliptic curves*, in preparation.
- [Tay-Wil] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, *Ann. of Math. (2)* **141** (1995), no. 3, 553–572.
- [Wal] 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.
- [Wil] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, *Ann. of Math. (2)* **141** (1995), no.3, 443–551.

Christophe Delaunay, École Polytechnique Fédérale de Lausanne, Faculté des Sciences de Base, CSAG, 1015 Lausanne, Switzerland.
e-mail : christophe.delaunay@epfl.ch