DISCUSSION OF c_E

CHRISTOPHE DELAUNAY

ABSTRACT. ***Any errors should solely be attributed to the typist, Steven J. Miller. The cyrillic package did not load, so Sha is denoted by ω.***

1. COMMENTS ON AN EARLIER TALK

Earlier in the week I was wrong to say that Ono conjectured that if $E/\mathbb{Q}$ is an elliptic curve then there are infinitely many primes p such that the rank of either E_p or E_{-p} is at least two. In fact, Silverman conjectured that there are infinitely many primes p such that the rank of either E_p or E_{-p} is zero. Ono proved that for all E with conductor at most 100, Silverman's result is true, more precisely, he proved that there is a positive density of primes satisfying Silverman 's conjecture.

We can ask whether or not for $E/\mathbb{Q}$ an elliptic curve there are infinitely many primes p such that the rank of either E_p or E_{-p} is at least two.

2. FIRST THOUGHTS ON c_E

We discuss c_E and the kind of complexities that arise when we try to compute it. Let $E/\mathbb{Q}$ be an elliptic curve: $y^2 = f(x)$. Let $d < 0$ be a fundamental discriminant, and consider the twisted curve $E_d : dy^2 = f(x)$. By the B-SD conjecture,

$$L(E_d, 1) \ = \ \frac{\Omega}{\sqrt{|d|}}\, c(E_d)|\omega(E_d)|. \tag{2.1}$$

We will study those with $|\omega(E_d)| = 0$ (this only a convention for saying that $L(E_d, 1) = 0$). At a first study, we only consider prime discriminants so that the contribution $c(E_d)$ in (2.1), coming from the Tamagawa numbers, is simply 1. So, in the following, d will denote a prime fundamental discriminant such that the sign of the functional equation of E_d is $+1$.

By Random matrix theory and the probability model,

$$\text{Prob}\left(L(E_d, 1) < x\right) \ \sim \ c(E)x^{1/2}\log^{3/8}|d| \tag{2.2}$$

as $x \to \ 0$. By applying a discretization procedure, we find

$$\begin{aligned} \text{Prob}\left(L(E_d, 1) = 0\right) &= \text{Prob}\left(|\omega(E_d)| \approx 0\right) \\ &= \text{Prob}\left(|\omega(E_d)| < r\right) \text{ , for some } r < 1 \\ &= c(E)r|d|^{-1/2}\log^{3/8}|d|. \end{aligned} \tag{2.3}$$

The conclusion is that

$$\#\left\{|d| < T : L(E_d, 1) = 0, \epsilon(E_d) = 1, d \text{ primefund. disc.}\right\} \ \sim \ c_E T^{3/4}\log^{\frac{3}{8}-1} T. \tag{2.4}$$

To understand c_E there is an interplay between the arithmetics on E, the behavior of ω, our probability model, and the value of the parameter r.

2.1. **Arithmetic.** We have to pay attention to the arithmetic coming from E. For example, if $E = 17\mathrm{a}_1$, the $|\omega(E_d)|$ is odd and thus $L(E_d, 1) \neq 0$. This is not really a program. But consider $E = 11\mathrm{a}_1$. Letting $y^2 = f(x)$, look at the degree three field defined by any root of $f(x)$, call this K. Note K is a non-Galois extension of $\mathbb{Q}$. If $d = -p$ is a prime fundamental discriminant such that the sign of the functional equation of E_d is $+1$ then $\left(\frac{D_{K/\mathbb{Q}}}{p}\right) = \left(\frac{-44}{p}\right) = 1$ so p is inert or split in K. If p is inert then $|\omega(E_d)|$ is odd and thus $L(E_d, 1) \neq 0$. This happens 66% of the time, and must probably be taken into account.

2.2. **Behavior of ω.** We assume the following conjecture: ω is finite. Hence ω is a finite Abelian group and there is a bilinear pairing $\beta : \omega \times \omega \to \mathbb{Q}/\mathbb{Z}$ (alternating and non-degenerate). We say G is a group of type S if G is finite Abelian group with a bilinear alternating non-degenerate pairing $\beta : G \times G \to \mathbb{Q}/\mathbb{Z}$. .

Idea of the heuristic: $\omega(E)$ of rank 0 elliptic curves E behave as random group G of type S weighted by $|G|/|\mathrm{Aut}^S G|$. More precisely, if f is a function,

$$M(f) := \lim_{T\to\infty} \frac{\sum_{|d|\leq T, r(E_d)=0} f(\omega(E_d))}{\sum_{|d|\leq T, r(E_d)=0} 1} \tag{2.5}$$

is the average of f over the Tate-Shavarevich groups of $\omega(E_d)$. It is not known, in general, if the limit exists. The heuristic asserts that for reasonable functions f the average exist and is given by

$$\begin{aligned} M(f) &= \lim_{x\to\infty} \frac{\sum_{n\leq x} \sum_{G^S(n)} \frac{f(G)|G|}{|\mathrm{Aut}^S G|}}{\sum_{n\leq x} \sum_{G^S(n)} \frac{|G|}{|\mathrm{Aut}^S G|}} \\ &= \lim_{s\to 0} \frac{\sum_{n\geq 1} n^{-s} \sum_{G^s(n)} f(G)|G|/|\mathrm{Aut}^S G|}{\sum_{n\geq 1} n^{-s} \sum_{G^S(n)} |f|/\mathrm{Aut}^S G|} \\ &= \lim_{s\to 0} \frac{\text{same}}{\prod_{j\geq 1} \zeta(2s+2j-1)}. \end{aligned} \tag{2.6}$$

For example, take

$$f(G) \;=\; \begin{cases} 1 & \text{if } |G| \leq N \\ 0 & \text{otherwise.} \end{cases} \tag{2.7}$$

Then $M(f) = \mathrm{Prob}(|\omega(E_d)| < N) = 0$. This suggests that, maybe, we have to consider $r < N$ in (2.3). Worse, we can prove (under BSD) that

$$\frac{1}{T^*} \sum_{|d|<T} |\omega(E_d)| \;\sim\; dT^{1/2}. \tag{2.8}$$

Hence, this suggests that in fact $r < |d|^{1/2-\varepsilon}$ have to be considered for probably some twists.

The computation in (2.3) can be done for more general size of $|\omega(E_d)|$, obtaining that if $r < |d|^{1/2-\epsilon}$ we should have

$$\mathrm{Prob}(|\omega(E_d)|^{1/2} \;\approx\; \ell) \approx (*)|d|^{-1/4} \log^{\mathrm{power}} |d|. \tag{2.9}$$

2.3. **Another example.** Fix a prime ℓ, and let

$$f(G) \;=\; \begin{cases} 1 & \text{if } G_\ell = \{0\} \\ 0 & \text{otherwise.} \end{cases} \tag{2.10}$$

Set

$$\begin{aligned} M(f) &= \mathrm{Prob}(\ell \nmid |\omega(E_d)|) \\ &= \lim_{s\to 0} \prod_{p\neq \ell}(*) \prod_p \prod_{j\geq 1}(1-p^{-(2s+2j-1)})^{-1} \\ &= \prod_{j\geq 1}(1-p^{-(2j-1)})^{-1}. \end{aligned} \tag{2.11}$$

We end up getting

$$\begin{aligned} \mathrm{Prob}\,(\ell||\omega_d(E_d)|) &= 1-\prod_{j\geq 1}(1-p^{-(2j-1)})^{-1} \\ &= \frac{1}{\ell}+\frac{1}{\ell^3}-\frac{1}{\ell^4}\cdots, \end{aligned} \tag{2.12}$$

where the $1/\ell^3$ and higher terms are the difference between the classical arguments and (probably) 'reality'.

I think one of the key points is the following question: Can random matrix theory predict the above result? Maybe up to a constant? Of course, as 'up to a constant' has no meaning in predicting a constant, we need to be a bit more precise.

Let consider the following heuristic computation. We have

$$\begin{aligned} \mathrm{Prob}\,(\ell||\omega(E_d)|) &= \mathrm{Prob}(|\omega(E_d)|\approx 0) \\ &\quad + \mathrm{Prob}(|\omega(E_d)|^{1/2}\approx \ell) + \mathrm{Prob}(|\omega(E_d)|^{1/2}\approx 2\ell)+\cdots \\ &\quad + \mathrm{Prob}(|\omega(E_d)|^{1/2}\approx \lfloor |d|^{1/4}\rfloor \ell) \\ &= (*)|d|^{-1/4}+(*)|d|^{-1/4}+\cdots+(*)|d|^{-1/4} \\ &= \text{Average of } (*), \end{aligned} \tag{2.13}$$

where the last is known in advance by the heuristics. This could be useful to adjust the 'approximations' in the computations...

For doing this, we would need a more precise probabilistic model:

$$\mathrm{Prob}\,(L(E_d,1)<x) \;=\; c(E)x^{1/2}\log^{3/8}|d| + \cdots + o(x^{\frac{1}{2}-\epsilon}) \tag{2.14}$$

for $x \ll 1$. Or something like that.

Another useful fact is that we can use other test primes than ℓ or other functions. Unfortunately, the heuristic is not right for all primes. For some primes (depending on E and probably just on the order of the torsion sub-group of $E(\mathbb{Q})$) we rather have to apply the original Cohen-Lenstra for class-group (this is discussed in M. Rubinstein talk).