

# EXPECTED MORDELL-WEIL RANK HEURISTICS THROUGH SATO-TATE, BIRCH AND SWINNERTON-DYER CONJECTURES

DINESH S. THAKUR

ABSTRACT. We present an heuristic argument for the prediction of expected Mordell-Weil rank of elliptic curves over number fields, using Birch and Swinnerton-Dyer's original conjecture and Sato-Tate conjectures. We do calculations in some cases and raise questions about their relations, if any, with the predictions of various average rank models that have been considered.

For an elliptic curve  $E$  over the rational number field  $\mathbb{Q}$ , write  $N_p$  for the cardinality of  $E(\mathbb{F}_p)$ , and let  $P_x = \prod_{p \leq x} N_p/p$ .

Then the strong original form of Birch and Swinnerton-Dyer (BSD) conjecture [BSD63-65] says that there is a positive constant  $C = C(E)$  such that  $P_x$  is asymptotic to  $C(\log x)^r$ , as  $x$  tends to infinity, where  $r$  is the (Mordell-Weil) rank of  $E$ , i.e., the rank of the finitely generated group  $E(\mathbb{Q})$ .

Goldfeld [Goldfeld82] showed that this implies the usual  $L$ -function form of this conjecture as well as the Riemann hypothesis for this function. The finite field-function field Riemann Hypothesis, i.e., Hasse bounds imply much weaker result  $\log(P_x) = O(x^{1/2+\epsilon})$ , for any  $\epsilon > 0$ , instead of the asymptotics  $r \log \log(x) + B$  expected from above. But they also imply that we can write  $N_p = p + 1 - 2\sqrt{p} \cos(\theta_p)$ ,  $\theta_p \in [0, \pi]$

The distribution of  $\theta_p$  is predicted by the Sato-Tate (ST) conjecture [Tate63] as equidistribution wrt.  $(2/\pi) \sin^2(\theta) d\theta$ , for  $E$  with no complex multiplications (non-CM). This is now a theorem [BGHT11] ([Taylor08] for such  $E$  with non-integral  $j$ -invariant.)

Now let us first calculate the expected value of  $\log(P_x)$  under the Sato-Tate distribution on  $\theta_p$  for non-CM elliptic curve. We write  $\mathbb{E}$  for the expectation.

Using  $\log(1+y) = y - y^2/2 + \dots$ , and  $\sum_{p \leq x} 1/p = \log \log(x) + B + O(1/\log(x))$ , for some constant  $B$ , we get

$$\begin{aligned} \mathbb{E}(\log(P_x)) &= \sum \mathbb{E}(\log(1 + 1/p - 2 \cos(\theta_p)/\sqrt{p})) = \log \log(x) - \frac{1}{2} \log \log(x) + O(1) \\ &= \frac{1}{2} \log \log(x) + O(1), \end{aligned}$$

using  $\int_0^\pi 2 \cos(\theta) \sin^2(\theta) d\theta = 0$  and  $\int_0^\pi 2 \cos^2(\theta) \sin^2(\theta) d\theta = \pi/4$  to get the first two terms from the first 2 terms of the Taylor expansion, and putting the error from the remaining convergent series in the big  $O$  term.

Comparison with the strong original BSD conjecture asymptotics of  $r \log \log(x)$  implies heuristically that *the expected value of the Mordell-Weil rank of  $E(\mathbb{Q})$  in non-CM case is  $1/2$ .*

**Remarks** (1) Note that we have not taken averages or expectations of actual ranks under any family, but just matched the asymptotics of the expectation of the quantity  $\log(P_x)$  under ST for non-CM case with the asymptotics conjectured (a conjecture is, in fact, basically just an ‘expectation’!) and called the result heuristic expected value just because it comes from such a matching (and [Birch68] connection with the averages mentioned below). Interestingly, this seems to fit well with the predictions (and some evidence and bounds in some cases) by Dorian Goldfeld [Goldfeld79, Conjecture B] (for quadratic twists) and others (e.g., [PR11, Conjecture 1.2] over global fields) for the average rank as  $1/2$  in various ‘averages scenarios’ when you take averages by ordering the elliptic curves by the heights (normalized coefficients sizes) or use families of quadratic twists ordered by the twist parameter. (I do not know of any predictions (or rather results?) specifically mentioning ordering by minimal discriminants or conductors, apart from Katz-Sarnak function field work [KS99]). We refer to [BS15, PPVW19, Poonen18, Poonen13] for some results and surveys. Is this a coincidence or is there a better explanation? In the Sato-Tate original case [Tate63], one fixes  $E$  and averages over primes, but as Birch [Birch68] proved, one gets the same probability distribution when we fix  $p$  and average over curves  $E$  over  $\mathbb{F}_p$ . So there might be an explanation of the coincidence.

Andrew Sutherland suggested that probably the ordering of  $E$ ’s over  $\mathbb{Q}$  by naive height has the property that for any fixed  $p$  and all sufficient large  $M$  the first  $M$  of the  $E$ ’s have reductions mod  $p$  that are equidistributed over the isomorphism classes of  $E$  over  $\mathbb{F}_p$ , and Birch might apply to connect with actual averages.

Peter Sarnak suggested that going from one curve (as in the expectation calculation) to a family, a serious complicated issue is how big the parameter  $x$  is compared to the conductors of the family one is supposed to be averaging over.

(2) Similar calculation gives the same expectation  $1/2$  for non-CM elliptic curves over any number field, by exactly the same argument and using that sum of the reciprocals of the norms of primes (up to  $x$ ) still grows like  $\log \log x$ . Only the constants seem to depend on the number field. In contrast to [PR11, Conjecture 1.2] for global fields, Dorian Goldfeld suggested to the author that  $1/2$  may not now be expected to be the average rank for the elliptic curves over number fields with many complex places, since the discrepancy is known [DD09] for some quadratic twist families. The ‘expectations’ and predictions by experts of the rank distributions have changed a few times over the time. The ‘Infinite family Rank at most 21’ heuristics of Granville [W15] and [PPVW19] for elliptic curves over  $\mathbb{Q}$  also seems to go wrong when generalized naively for general number fields, as pointed out in [PPVW19, Sec. 12], [Poonen18, Sec. 4].

Next we look at CM  $E/Q$ , a similar calculation now with the predicted uniform distribution of  $\theta_p$  for ordinary primes and  $a_p = 0$  for super-singular  $p$  gives

$\mathbb{E}(\log(P_x)) = 1/2 \log \log(x) + O(1)$ , now  $1/2$  coming from the density of super-singular primes, the ordinary primes contribution being  $O(1)$  term: as  $(1/2) \log \log(x)$  from the  $y$  term (since  $\int_0^\pi \cos(\theta) d\theta = 0$ ) cancels from the  $(1/2) \log \log(x)$  from  $-y^2/2$  term (since  $\int_0^\pi 2 \cos^2(\theta) d\theta = \pi$ .)

Again, this heuristically gives the expected rank as  $1/2$ . This argument shows that the expected rank is  $1/2$  for CM  $E$  over field not containing the CM field and 0 for CM  $E$  over field containing the CM field.

I do not know whether these are the ‘expected’ averages in these cases. In fact, I could not find any published predictions. I would love to know references, if any.

Let us now calculate higher moments  $\mathbb{E}((\log P_x)^n)$ 's.

Write  $x_i$  for  $1/p_i - 2 \cos(\theta_p)/\sqrt{p_i}$ , where  $p_i$  is  $i$ -th prime. Then  $\mathbb{E}(x_i) = 1/p_i$  and  $\mathbb{E}(x_i^2) = 1/p_i$ , so that  $\sum \mathbb{E}(x_i) = \log \log(x) + O(1)$  and  $\sum \mathbb{E}(x_i^2/2) = (1/2) \log \log(x) + O(1)$  by the calculations done above. Since third and higher powers of  $x_i$  can be ignored as they give convergent sums, we have, up to  $O(1)$ ,  $\mathbb{E}((\log P_x)^n) = \mathbb{E}((\sum \log(1 + x_i))^n) = \mathbb{E}(\sum \prod_{i=1}^n (x_i - x_i^2/2))$  since terms with some repeated indices  $i_1 = i_2$  again contribute bounded quantities as they involve at least  $3/2$  powers of primes in denominator.

Let us do  $n = 2$  case first. Then up to  $O(1)$  again, with  $i \neq j$  below, we have

$$\begin{aligned} \mathbb{E}((\log(P_x))^2) &= \mathbb{E}\left(\sum \log(1 + x_i) \log(1 + x_j)\right) = \sum \mathbb{E}((x_i - x_i^2/2)(x_j - x_j^2/2)) \\ &= \sum \mathbb{E}(x_i x_j - x_i x_j^2/2 - x_i^2 x_j/2 + x_i^2 x_j^2/4) \\ &= \sum [1/(p_i p_j) - 1/(2p_i p_j) - 1/(2p_j p_i) + 1/(4p_i p_j)] \\ &= \sum 1/(4p_i p_j) = (\log \log(x))^2/4 \end{aligned}$$

For general  $n$ , we get, by the simplification above that

$\mathbb{E}((\log P_x)^n) = \sum \mathbb{E}(\prod x_i) (\prod (-x_j^2/2)) = \sum \prod \mathbb{E}(x_i) \mathbb{E}(-x_j^2/2)$ , where we take  $k$  of  $x_i$  terms and  $n - k$  of  $-x_j^2/2$  terms, so we get

$$\left(\sum_{k=0}^n (-1)^k \binom{n}{k} / 2^k\right) (\log \log(x))^n = (1 - 1/2)^n (\log \log(x))^n = (\log \log(x))^n / 2^n$$

**Remarks** The expectations (in the generic non-CM case that we only worked out so far) now seem ‘unexpected’:  $n$ -th moment is basically  $(\log \log x)/2^n$ , rather than  $(\log \log x)/2$ , which would be ‘expected’, if it is supposed to be the just average of  $r^n$ , since half are expected to be of rank 0 and half of rank 1, in the widely believed conjecture. Are the expectations not supposed to be reasonable averages or is there some other good explanation for higher moments discrepancy with average considerations?

Finally, we mention another (unrelated to above) observation regarding the rank conjectures. In a beautiful work [Poonen02], Bjorn Poonen showed (among other things) that Hilbert’s tenth problem over  $\mathcal{O}_K$  is undecidable for every number field  $K$ , if for every number field  $K$ , there exists elliptic curve  $E$  over  $\mathbb{Q}$  with MW rank of  $E$  over  $\mathbb{Q}$  and over  $K$  being one. But the optimistic conjecture [Poonen02, 2.6] that the if part is always true is incompatible with the BSD conjecture, since for some number fields  $K$ , e.g.,  $K = \mathbb{Q}(\sqrt{-1}, \sqrt{17})$  it is known (by Karl Rubin see e.g., [Dokchitser13, Sec. 8.1]) that the analytic rank of  $E$  over  $K$  is always even for all  $E$  over  $\mathbb{Q}$ , by root number calculations. Bjorn Poonen tells me that he and Alexandra Shlapentokh proved later that for this application to Hilbert’s tenth problem, it is enough to know that for every quadratic extension of number fields  $L/K$ , there is an elliptic curve  $E$  of a positive rank over  $K$  (not necessarily 1) that has the same rank over  $L$ . In fact, Karl Rubin and Barry Mazur [MR10] have proved that such  $E$  exists, assuming that the Tate-Shafarevich group for elliptic curves is always finite.

**Acknowledgments** I thank Dorian Goldfeld, Peter Sarnak, Bjorn Poonen (especially for pointing out a wrong comment), Andrew Sutherland for their comments.

## REFERENCES

- [BGHT11] Barnet-Lamb, T., Geraghty, D., Harris, M., Taylor, R. *A family of Calabi-Yau varieties and potential automorphy II*. Publ. Res. Inst. Math. Sci. 47 (2011), no. 1, 29-98.
- [BS15] Bhargava, M., Shankar, A. *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*. Ann. of Math. (2) 181 (2015), no. 1, 191-242.
- [Birch68] Birch, B.J., *How the number of points of an elliptic curve over a fixed prime field varies*. J. London Math. Soc. 43 (1968), 57-60.
- [BSD63-65] Birch B.J., and Swinnerton-Dyer H. P. F. *Notes on elliptic curves I and II*. I. J. Reine Angew. Math. 212 (1963), 7-25 and 218 (1965), 165-172.
- [Dokchitser13] Dokchitser, Tim. *Notes on the parity conjecture*. Elliptic curves, Hilbert modular forms and Galois deformations, 201-249, Adv. Courses Math. CRM Barcelona, Birkhauser/Springer, Basel, 2013.
- [DD09] Dokchitser, T., and Dokchitser, V. *Elliptic curves with all quadratic twists of positive rank*. Acta Arith. 237 no. 2 (2009), 193-197.
- [Goldfeld79] Goldfeld Dorian. *Conjectures on elliptic curves over quadratic fields*. Number Theory, Carbondale 1979, Lecture Notes in Math., vol. 751, Springer, (1979), 108-118.
- [Goldfeld82] Goldfeld Dorian. *Sur les produits partiels eulériens attaches aux courbes elliptiques*. C. R. Acad. Sci. Paris Ser. I Math. 294 (1982), no. 14, 471-474.
- [KS99] Katz, N.M., Sarnak, P. *Random matrices, Frobenius eigenvalues, and Monodromy*. AMS Colloq. Pub. vol. 45, AMS (1999).
- [MR10] Mazur, B., Rubin, K. *Ranks of twists of elliptic curves and Hilbert's tenth problem*. Invent. Math. 181 (2010), no. 3, 541-575.
- [PPVW19] Park, J., Poonen, B., Voight, J., Wood, M. *A heuristic for boundedness of ranks of elliptic curves*. J. Eur. Math. Soc. (JEMS) 21 (2019), no. 9, 2859-2903.
- [PR11] Poonen, B., Rains, E. *Random maximal isotropic subspaces and selmer groups* J. Amer. Math. Soc. vol. 25, no. 1, (2012) 245-269.
- [Poonen02] Poonen, Bjorn. *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*. Algorithmic Number Theory, Ed. by C. Fieker, D. Kohel, Lecture Notes in Comp. Sci. 2369, Springer (2002), 33-42.
- [Poonen13] Poonen, Bjorn. *Average rank of elliptic curves [after Manjul Bhargava and Arul Shankar]*. Seminaire Bourbaki. Vol. 2011/2012. Exposes 1043-1058. Asterisque No. 352 (2013), Exp. No. 1049, viii, 187-204.
- [Poonen18] Poonen, Bjorn. *Heuristics for the arithmetic of elliptic curves*. Proceedings of the International Congress of Mathematicians- Rio de Janeiro 2018. Vol. II. Invited lectures, 399-414, World Sci. Publ., Hackensack, NJ, 2018.
- [Tate63] Tate, John T. *Algebraic cycles and poles of zeta functions. Arithmetical Algebraic Geometry*. (Proc. Conf. Purdue Univ., 1963) pp. 93-110 Harper & Row, New York 1965.
- [Taylor08] Taylor, Richard. *Automorphy for some  $l$ -adic lifts of automorphic mod  $l$  Galois representations. II*. Publ. Math. Inst. Hautes Etudes Sci. No. 108 (2008), 183-239.
- [W15] Watkins, Mark. *A discursus on 21 as a bound for ranks of elliptic curves over  $\mathbb{Q}$  and sundry related topics*. August 20, 2015. Available at <http://magma.maths.usyd.edu.au/watkins/papers/DISCURSUS.pdf>