AN IMPROVED RESULT TOWARDS THE LANG-TROTTER CONJECTURE

FRANK THORNE

Abstract. In [2], Cojocaru, Fouvry, and Murty prove [some partial results towards the Lang-Trotter conjecture]. Here we sketch a proof of improved versions of their results. We proceed separately in the GRH and non-GRH cases. Conditionally on GRH, we introduce a new step into their proof and postpone the use of the Chebotarev density theorem until a certain sum S has been analyzed further. Unconditionally, we use an improvement to the Chebotarev density theorem which we describe in [5].

In both cases the improved results described here turn out to be inferior to subsequent results by Cojocaru and David [1] and Zywina [6].

These notes are a rough draft.

1. Introduction

In this note we will sketch the proof of the following theorem:

Theorem 1.1. *For a fixed elliptic curve E without CM, and a fixed imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$, let $P_E(x)$ denote the number of primes $p \leq x$ which are of good reduction, and for which $\sqrt{a_p}$ generates K (i.e., for which K is the splitting field of Frobenius). Then, conditional on GRH,*

$$P_E(x) \ll_{N(E)} x^{9/10} \log x.$$

Unconditionally, we obtain

$$P_E(x) \ll_{N(E)} \frac{x}{(\log x)^{11/10-\epsilon}}.$$

Remark. This improves on results of $x^{17/18} \log x$ and $x(\log\log x)^{13/12}(\log x)^{-25/24}$ found in [2], but is inferior to the results in [1] and [6].

We also will discuss how we can improve the unconditional result slightly further (still falling well short of [6]).

To prove this we will introduce an improvement to the proof in [2]. We won't describe their argument or try to motivate this problem; rather, we presume our reader has access to their paper.

2. Setup and notation

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. We want to consider the Galois groups $\mathrm{Gal}(\mathbb{Q}(E[lq])/\mathbb{Q})$, for primes l and q. It is known that for all but finitely many primes, these groups are isomorphic to $\mathrm{GL}_2(\mathbb{Z}/lq\mathbb{Z})$, and we shall assume throughout that these primes are avoided. Moreover, we shall assume that these primes are asymptotically of size z (say, $z < l, q < 2z$) for a parameter z to be determined.

We will write $G_n = \mathrm{GL}_2(Z/nZ)$ throughout, and note that if $n = lq$ for distinct primes l and q then $G_{lq} = G_l \times G_q$.

2000 *Mathematics Subject Classification.* 11N25, 11N36.

The setup for our paper is that of [2], as indeed we are picking up their proof from the middle and introducing improvements. There may be additional assumptions there which I have neglected to mention here, but we assume all that they do.

3. Some technical details

We take as our starting point the expression

$$S_0 := \sum_{t \pmod{lq}} \sum_{\substack{d \pmod{lq} \\ (d,lq)=1}} \left(\frac{4d-t^2}{lq}\right) \pi_E(x, lq, t, d). \tag{3.1}$$

Here $\pi_E(x, lq; t, d)$ counts the number of primes $p \leq x$ which are congruent to d mod lq and for which a_p is congruent to t mod q. These are conditions on the determinant and trace of the Frobenius element at p in G_{lq}.

We will replace this with

$$S := \sum_{t \pmod{lq}} \sum_{\substack{d \pmod{lq} \\ (d,lq)=1}} \left(\frac{4d-t^2}{lq}\right) \psi_E(x, lq, t, d). \tag{3.2}$$

Then S is asymptotic to $S_0 \log x$. Without attempting to motivate our estimate for the time being, we will prove the following estimate:

Proposition 3.1. *Conditional on GRH, and assuming (as before) that l and q are of size asymptotic to z, we have*

$$S \ll xz^{-6} + x^{1/2} z^4 \log^2 x.$$

Unraveling Lagarias and Odlyzko's effective version of the Chebotarev density theorem [4], we obtain that

$$S = \frac{-1}{2\pi i |G_{lq}|} \sum_{\phi \in \mathrm{Irr}(G_{lq})} \left(\int_{\sigma_0} \frac{L'}{L}(s, \phi, \mathbb{Q}(E[lq])/\mathbb{Q}) \frac{x^s}{s} ds \right) \left(\sum_{\sigma \in G_{lq}} \left(\frac{4 \det \sigma - (\mathrm{tr}\ \sigma)^2}{lq} \right) \overline{\phi}(\sigma) \right)$$

Lemma 3.2. *Let $G = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Then, we have (as an equality of class functions on G)*

$$\sum_{\phi \in \mathrm{Irr}(G)} \left(\sum_{\sigma \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})} \left(\frac{4 \det \sigma - (\mathrm{tr}\ \sigma)^2}{n} \right) \right) \phi = |G| \left(\frac{4 \det - \mathrm{tr}^2}{n} \right).$$

Proof. This follows by switching the order of summation and using the orthogonality relations. □

Furthermore, if $n = l$ is a prime, then the class function above is easily described: it is equal to 0 for matrices with repeated eigenvalues in $\mathbb{F}_l$, $|G|$ for matrices with distinct eigenvalues in $\mathbb{F}_l$, and $-|G|$ for matrices whose eigenvalues are not in $\mathbb{F}_l$. are conjugate to an upper triangular matrix.

We let $D_l \subseteq \mathrm{GL}_2(\mathbb{F}_l)$ denote the (abelian) subgroup of diagonal matrices, and let K_l the subgroup described on p. 68 of [3]. (to do: describe here.)

For a subgroup H of G, we write $\mathrm{Ind}(H)$ for the character induced on G by the trivial character on H.

Lemma 3.3. *If $n = l$ is a prime, then the class function above is*

$$\frac{|G|}{2}\mathrm{Ind}(D) - \frac{|G|}{2}\mathrm{Ind}(K) - l \cdot \mathrm{Ind}(1). \tag{3.3}$$

Proof. Computation. □

Remark. It is possible that there are other formulas for this class function which will yield better results. However, this appears doubtful.

By putting all of this together with $n = lq$, we obtain

$$S := \frac{-1}{2\pi i|G|}\sum_{\phi}\int_{\sigma_0}\frac{L'}{L}(s,\phi,G_{lq})\frac{x^s}{s}ds,$$

where ϕ ranges over the products of the characters above. We recall that $G_{lq} = G_l \times G_q$, and we check that for subgroups $H_q \subseteq G_q, H_l \subseteq G_l$ we have

$$\mathrm{Ind}(H_q) \times \mathrm{Ind}(H_l) = \mathrm{Ind}(H_q \times H_l).$$

Furthermore, if H is a subgroup of G, and $\phi = \mathrm{Ind}(H)$, then by invariance of Artin L-functions under induction we have

$$L(s,\phi,G) = L(s,1,H) = \zeta_{\mathrm{Fix}(H)}(s).$$

This shows that

$$S := \frac{-1}{2\pi i}\sum_{1\le i\le 9}\alpha_i\int_{\sigma_0}\frac{\zeta'_{E_i}}{\zeta_{E_i}}(s)\frac{x^s}{s}ds, \tag{3.4}$$

where the α_i range over each pairwise product of $1/2, -1/2, l/|G_l|$ with $1/2, -1/2, q/|G_q|$, and the fields E_i are the fixed fields (as subfields of $\mathbb{Q}(E[lq])$) of the direct products of $D_l, K_l, 1_l$ with $D_q, K_q, 1_q$.

Conditional on the GRH, if E is an extension of degree d whose ramified primes include only l, q, and fixed primes depending on our choice of elliptic curve, then we have

$$\int_{\sigma_0}\frac{\zeta'_E}{\zeta_E}(s)\frac{x^s}{s}ds = x + O\big(x^{1/2}d\log^2 x\big), \tag{3.5}$$

if we assume that $l, q \ll x$. This bound uses the discriminant estimate given as Lemma 2.6 of [2].

By (3.3), the main terms in (3.5) all cancel except for the term coming from the trivial subgroup of G_{lq}. This term contributes

$$\frac{lq}{|G_{lq}|}x \ll xz^{-6}.$$

We obtain an error term from each of the nine integrals of $O(\alpha_i d_i x^{1/2}\log^2 x)$. The products of the D and K subgroups yield $\alpha_i = \pm\frac{1}{4}$ for each i, and $d_i := [E_i : \mathbb{Q}] = O((lg)^2) = O(z^4)$ Thus, these four terms contribute

$$\ll z^4 x^{1/2}\log^2 x.$$

The products of one of the D and K subgroups with the trivial subgroup for the other prime yield $\alpha_i \ll z^{-3}$ and $d_i = O(z^6)$, for a total contribution of $\ll z^3 x^{1/2}\log^2 x$. Similarly, the product of the two trivial subgroups yields a contribution $\ll z^2 x^{1/2}\log^2 x$.

Putting this together we conclude that

$$S \ll xz^{-6} + x^{1/2}z^4\log^2 x.$$

We now refer to the quantity $S(\mathcal{A})$ referred to in (9) of Section 3 of [2]. In particular, we have (with the assumption that $\log D \ll \log x$) that

$$S(\mathcal{A}) \ll S_0 + \frac{x\log z}{z} + \frac{x\log^4 x}{z^2},$$

and by choosing $z = x^{1/10}$ we obtain that

$$P_E \ll x^{9/10} \log x,$$

where the implied constant depends on our elliptic curve.

4. Unconditional results

It seem that we are also able to improve on the unconditional result in [2], in a different way. The method above does not appear to be helpful, because the main bottleneck in [2] originates from the unconditional version of the Chebotarev density theorem in [4]: in particular, this result is only proved when x is sufficiently large in relation to the underlying field. By Lemma 3.3, we are still obliged to use a prime number theorem for the Dedekind zeta function associated to the same field as in [2]. As the choice of z in [2] is only just small enough to allow the use of CDT, we are obliged to lower the threshold for x to proceed.

To our surprise, this proved possible. In particular, we proved the following result. (We assume the reader is familiar with the notation used; L is the field of definition, and $G = \mathrm{Gal}(L/\mathbb{Q})$.)

Theorem 4.1. *There exist absolute effectively computable constants C_1, C_2, C_3 such that if*

$$x \geq \exp\left(C_1 \frac{(\log n_L)^3}{n_L} (\log d_L)^2\right), \tag{4.1}$$

then

$$\left|\pi_C(x) - \frac{|C|}{|G|}\mathrm{li}(x)\right| \leq \frac{|C|}{|G|}\mathrm{li}(x^{\beta_0}) + C_2 x \exp(-C_3 n_L^{-1/2} (\log x)^{1/2}). \tag{4.2}$$

The conclusion is the same as that in [4]; the improvement is in the condition (4.1), which replaces the condition

$$x \geq \exp(10 n_L (\log d_L)^2) \tag{4.3}$$

given in [4].

The proof essentially consists of one line. We follow [4] exactly, and then replace (9.6) in [4] with the choice

$$T = \exp\left(n_L^{-1/2} (\log x)^{1/2} - \frac{1}{n_L} \log d_L\right). \tag{4.4}$$

We then check that everything works. This is written up separately in [5], although in truth there is not much to say.

Remark. Although I carefully checked my work, it still seems wise to be very skeptical. I recently sent this paper to Lagarias and Odlyzko and am awaiting their comments.

Turning back to [2], we check that we may take

$$z := (\log x)^{1/10 - \epsilon}$$

for any fixed $\epsilon > 0$, in place of the choice $z = c(\log x)^{1/24}/(\log\log x)^{1/12}$ in [2]. We check that the condition (4.2) allows this choice (or, in fact, the choice $z = c(\log x)^{1/8}(\log\log x)^{-5/8}$). We also have the condition in (22) to worry about, which is why we choose the smaller value of z above. We have further exactly similar estimates, but the remainder of the argument in [2] appears to work out, and we obtain our result.

Remark. It appears that we could improve this still further to $z = (\log x)^{1/8-\epsilon}$, or indeed to $z = (\log x)^{1/8}(\log\log x)^{-5/8}$, by improving the first estimate in (15) in [2]. In any case, Zywina [6] obtains the much better result

$$P_E(x) \ll_{N(E)} x(\log\log x)^2/(\log x)^2.$$

5. Concluding remarks and questions

Question 5.1. *Are the improvements made here compatible with the "mixed representations" methods in Cojocaru and David's* [1] *and Zywina's* [6] *work?*

A cursory look at these papers does not suggest anything obvious.

Question 5.2. *Are the methods here applicable to other problems?*

Nothing occurs to the author at present.

Question 5.3. *Does the expression of our class function in Lemma 3.3 "mean anything"?*

The class function we obtained was very nice, and quite simply described. One gets the feeling that the ideas described here could be further pursued, but nothing occurs to the author.

References

[1] A. C. Cojocaru and C. David, *Frobenius fields for elliptic curves.*
[2] A. C. Cojocaru, E. Fouvry, and M. R. Murty, *The square sieve and the Lang-Trotter conjecture.*
[3] W. Fulton and J. Harris, *Representation theory.*
[4] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem.*
[5] F. Thorne, *An improved version of the effective Chebotarev density theorem*, in preparation.
[6] D. Zywina, *The Lang-Trotter conjecture and mixed representations.*

Department of Mathematics, Stanford University
E-mail address: fthorne@math.stanford.edu