PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 146, Number 8, August 2018, Pages 3191–3202
http://dx.doi.org/10.1090/proc/13900
Article electronically published on April 17, 2018

A REMARK ON THE LANG-TROTTER AND ARTIN CONJECTURES

M. RAM MURTY AND AKSHAA VATWANI

(Communicated by Matthew A. Papanikolas)

Abstract. We use recent advances in sieve theory to show that conditional upon the generalized Elliott-Halberstam conjecture, at least one of the following is true:

(i) Artin's primitive root conjecture holds for all a not equal to ± 1 or a perfect square
(ii) The Lang-Trotter conjecture holds for all CM elliptic curves $E/\mathbb{Q}$ with rank $E(\mathbb{Q}) \geq 1$ and CM field $k \neq \mathbb{Q}(\omega), \mathbb{Q}(i)$, where ω is a primitive cube root of unity.

1. Introduction

The breakthrough work of Yitang Zhang [23] about bounded gaps between primes has inspired new and spectacular developments in sieve theory. Foremost in this direction is the work of Maynard [10] and the Polymath project [18] who initiated the development of a 'higher rank Selberg sieve' that led to substantial simplification of parts of Zhang's work and improved numerical results. This new sieve method has been axiomatized, generalized and formulated into a flexible method by the authors in [20], [16] and applied to an assortment of problems, most notably to the study of almost-prime k-tuples which improves upon the earlier work of Heath-Brown [5]. This method has also been applied in [21] to the ring of integers of imaginary quadratic fields with class number 1.

In this paper, we want to study the implications of this new sieve method to Artin's primitive root conjecture and the Lang-Trotter conjectures for CM elliptic curves. These conjectures have a long history and the reader may find a description in [14]. However, we give a brief description here so as to introduce and explain our main result.

In 1927, Artin (see [1]) predicted that any natural number a not equal to ± 1 or a perfect square is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ for infinitely many primes p. This is called Artin's conjecture (or more precisely Artin's primitive root conjecture, to distinguish it from Artin's other conjecture concerning the holomorphy of non-abelian L-series). Artin further conjectured an asymptotic formula for the number $N_a(x)$ of such primes $p \leq x$. Both of Artin's conjectures are still open, though some advances have been made on both.

Received by the editors June 1, 2016.
2010 *Mathematics Subject Classification.* Primary 11N35, 11N36; Secondary 11N05.
Key words and phrases. Lang-Trotter conjecture, Artin's primitive root conjecture.
Research of the first author partially supported by an NSERC Discovery grant.

In 1967, Hooley [7] assumed the generalized Riemann hypothesis (for the Dedekind zeta functions of all number fields $\mathbb{Q}(e^{2\pi i/q}, a^{1/q})$ with q prime) to derive an asymptotic formula for $N_a(x)$. In 1984, Gupta and Murty [3], using sieve theory, showed that there exists a finite set S of 13 elements such that for some $a \in S$, Artin's conjecture holds. This was further refined by Heath-Brown [6] who showed that if a_1, a_2, a_3 are mutually coprime, none of which equal ± 1 or a perfect square, then Artin's conjecture holds for at least one of a_1, a_2, a_3.

In 1977, Lang and Trotter [8] formulated an elliptic analogue of Artin's primitive root conjecture. To describe this, let E be an elliptic curve defined over $\mathbb{Q}$. By a well-known theorem of Mordell [12], the abelian group of rational points $E(\mathbb{Q})$ is finitely generated, and thus by the structure theorem for finitely generated abelian groups, we can write

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$$

where $E(\mathbb{Q})_{\text{tor}}$ denotes the torsion subgroup and r is called the rank of E over $\mathbb{Q}$. By a celebrated theorem of Mazur [11],

$$|E(\mathbb{Q})_{\text{tor}}| \leq 16$$

so that if $r = 0$, there are only finitely many rational points on the curve. This can also be deduced using the more elementary theorem of Lutz and Nagell (see for example, p. 240 of [19]). In any case, Lang and Trotter suggested that if $r \geq 1$ and a is a point of infinite order, an elliptic analogue of Artin's conjecture would be to study under what conditions the reduction of $a \pmod p$ generates $E(\mathbb{F}_p)$ and how often this can happen. Using Galois theory, algebraic number theory and the Chebotarev density theorem, they formulated precise conjectures concerning the infinitude of such primes and predicted their densities (see [9]). Attempts to modify Hooley's approach to study these elliptic analogues failed because of large error terms in their applications of the Chebotarev density theorem.

Gupta and Murty [4] began a systematic study to see how these difficulties can be circumvented. They first proved that for CM elliptic curves, Hooley's methods can be modified to derive analogous results in this case. Namely, they showed that the Lang-Trotter conjecture in the CM case is true assuming the generalized Riemann hypothesis for Dedekind zeta functions of certain algebraic number fields. They also noted that in the CM case, a lower bound sieve technique can be used to show that if E is a CM elliptic curve over $\mathbb{Q}$ with an irrational 2-division point and rank $E(\mathbb{Q}) \geq 6$, then there is a set S of 2^{18} rational points such that for at least one $a \in S$, we have $E(\mathbb{F}_p)$ cyclic and generated by a for infinitely many primes p.

In unpublished work, the stringent condition that $r \geq 6$ has been reduced to $r \geq 3$ by the first author, assuming the Elliott-Halberstam conjecture. This conjecture can be explained as follows. Let $\pi(x, q, a)$ be the number of primes $p \leq x$ with $p \equiv a \pmod q$. Then for any $\theta < 1$ and any $A > 0$, we have

$$\text{(EH)} \qquad \sum_{q<x^\theta} \max_{y \leq x} \max_{(a,q)=1} \left| \pi(y, q, a) - \frac{\text{li}(y)}{\phi(q)} \right| \ll \frac{x}{(\log x)^A}.$$

Recently, a generalized version of the Elliott-Halberstam conjecture has emerged in [18] where the authors prove using it, a "disjunction theorem", namely that either the twin prime conjecture holds or the "near miss" Goldbach conjecture holds (that is, for n with $6|n$, either n or $n-2$ can be written as a sum of two primes).

We describe the generalized Elliott-Halberstam conjecture (denoted GEH) below and then proceed to state our central result.

2. The generalized Elliott-Halberstam conjecture

We use the letter p to denote primes. Given a "reasonable" arithmetical function $f \to \mathbb{N}$, one expects that its values are equidistributed over primitive residue classes. For any $(a, q) = 1$, we set

$$\Delta_f(y, q, a) := \sum_{\substack{n \le y \\ n \equiv a \pmod q}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n \le y \\ (n,q)=1}} f(n). \tag{1}$$

In the case when f is the von Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^\alpha \text{ with } \alpha \ge 1, \\ 0 & \text{otherwise,} \end{cases}$$

the average estimate

$$\sum_{q < x^\theta} \max_{y \le x} \max_{(a,q)=1} |\Delta_\Lambda(y, q, a)| \ll \frac{x}{(\log x)^A},$$

holds for any $\theta < 1/2$ and $A > 0$. This is called the Bombieri-Vinogradov theorem. Analogues of the Bombieri-Vinogradov theorem for multiplicative arithmetic functions satisfying certain restrictions were proved by Siebert and Wolke [22].

In 1976, Motohashi [13] proved a general result showing that the analogue of the Bombieri-Vinogradov theorem holds for any arithmetical function f which can be represented as a linear combination of convolutions of two sequences (α_m) and (β_n) satisfying certain properties. Such a formulation of his result is given by Bombieri, Friedlander and Iwaniec in [2], where the authors also conjecture that such functions should satisfy an Elliott-Halberstam type conjecture. Following the notation of Claim 12 of [18], we assume that the estimate

$$\sum_{q < x^\theta} \max_{(a,q)=1} |\Delta_f(x, q, a)| \ll \frac{x}{(\log x)^A}, \tag{2}$$

holds for any $\theta < 1$ and $A > 0$ for all functions of the above type. As an application of such conjectured equidistribution estimates, the authors derive some interesting results regarding the parity problem in [17].

A variant of the Bombieri-Vinogradov theorem that plays a key role in our discussion is due to M. Ram Murty and V. Kumar Murty [15]. Let $\mathcal{P}$ be a set of primes. We use the standard notation

$$\pi_{\mathcal{P}}(x) = \#\{p \in \mathcal{P} \mid p \le x\},$$

and

$$\pi_{\mathcal{P}}(x, q, a) = \#\{p \in \mathcal{P} \mid p \le x, \ \ p \equiv a \pmod q\}.$$

A subset $\mathcal{P}$ of the set of rational primes $\mathbb{P}$ is called a Chebotarev set if there is a Galois extension $K/\mathbb{Q}$ of number fields with Galois group G and absolute discriminant d_K such that

$$\mathcal{P} = \left\{ p \in \mathbb{P} \mid p \text{ is unramified with } \left(\frac{K/\mathbb{Q}}{p}\right) \subseteq C \right\}.$$

Here, for p unramified (or equivalently, $p \nmid d_K$), $\left(\frac{K/\mathbb{Q}}{p}\right)$ denotes the Artin symbol at p, and C is a union of conjugacy classes of G. It is clear that a Chebotarev set $\mathcal{P}(K, C)$ is determined by K and C. A Chebotarev set $\mathcal{P} = \mathcal{P}(K, C)$ is said to have a level of distribution θ if there exists a natural number M such that

$$\sum_{\substack{q \leq x^{\theta} \\ (q, M)=1}} \max_{y \leq x} \max_{(a,q)=1} \left| \pi_{\mathcal{P}}(y, q, a) - \frac{\pi_{\mathcal{P}}(y)}{\phi(q)} \right| \ll \frac{x}{(\log x)^A}, \tag{3}$$

holds for any $A > 0$. In [15], the authors prove the following.

Theorem 1. *The average result* (3) *holds if* $M = d_K$ *and* $0 < \theta < \min\left(\frac{2}{|G|}, \frac{1}{2}\right)$. *Moreover, assuming a special case of the Artin conjecture (AC) that all L-functions attached to all abelian twists of any non-trivial character of* G *are entire, and setting*

$$\eta = \max_{\chi \neq \chi_0} |\chi(1) - 2|,$$

where the maximum runs over all non-trivial characters of G*, one can improve the estimate* (3) *with a larger level of distribution* $0 < \theta < \min\left(\frac{1}{\eta}, \frac{1}{2}\right)$.

Let ω be a primitive cube root of unity and a be a natural number not equal to ± 1 or a perfect square. In the context of our result, we will be interested in applying Theorem 1 to the primes p which do not split completely in $K = \mathbb{Q}(\omega, a^{1/3})$. In this case, the Galois group G is the symmetric group S_3 and the special case of the Artin conjecture required in Theorem 1 holds. As $\eta = 0$ in this case, the above theorem yields a level of distribution $\theta < 1/2$ for such primes.

Henceforth in this paper, the generalized Elliott-Halberstam conjecture (GEH) will refer to a level of distribution $\theta < 1$ for primes which do not split completely in $\mathbb{Q}(\omega, a^{1/3})$, as well as the inequality (2) for functions f of the type as stated above.

Our main theorem is:

Theorem 2. *Assuming GEH, at least one of the following is true:*

(i) *Artin's primitive root conjecture holds for all* a *not equal to* ± 1 *or a perfect square.*
(ii) *The Lang-Trotter conjecture holds for all CM elliptic curves* $E/\mathbb{Q}$ *with rank* $E(\mathbb{Q}) \geq 1$ *and CM field* $k \neq \mathbb{Q}(\omega), \mathbb{Q}(i)$.

3. Notation

We use notation introduced in [20]. We include the same briefly here for the sake of completeness. We denote the k-tuple of integers $(d_1, \ldots, d_k)$ by $\underline{d}$. A tuple is said to be square-free if the product of its components is square-free. For $R \in \mathbb{R}$, the inequality $\underline{d} \leq R$ means that $\prod_i d_i \leq R$. The notions of divisibility and congruence among tuples are defined component-wise. Divisibility relations between a tuple and a scalar are defined in terms of the product of the components of the tuple. For example,

$$q | \underline{d} \iff q | \prod_i d_i.$$

We define the multiplicative vector function $f(\underline{d})$ as the product of its component (multiplicative) functions acting on the corresponding components of the tuple,

that is,

$$f(\underline{d}) = \prod_{i=1}^{k} f_i(d_i).$$

We use $[\cdot,\cdot]$ and $(\cdot,\cdot)$ to denote lcm and gcd respectively. In the case of tuples, this means the product of the lcms (or gcds) of the corresponding components. We employ the following multi-index notation to denote mixed derivatives of a function on k-tuples, $\mathcal{F}(\underline{t})$. Then

$$\mathcal{F}^{(\underline{\alpha})}(\underline{t}) := \frac{\partial^{\alpha}\mathcal{F}(t_1,\dots,t_k)}{(\partial t_1)^{\alpha_1}\dots(\partial t_k)^{\alpha_k}}, \tag{4}$$

for any k-tuple $\underline{\alpha}$ with $\alpha := \sum_{j=1}^{k}\alpha_j$.

We use the convention $n \sim N$ to mean $N \le n < 2N$. In practice we have $N \to \infty$. We fix $D_0 = \log\log\log N$ and let $W = \prod_{p<D_0} p$. Then $W \sim \log\log N$ by an application of the prime number theorem. Let $\omega(n)$ denote the number of distinct prime factors of n. The greatest integer less than or equal to x is denoted as $\lfloor x \rfloor$. Throughout this paper, δ denotes a positive quantity which can be made as small as needed.

4. The higher rank Selberg sieve

We give a brief summary of the general higher rank Selberg sieve developed in [20]. The exposition given here is concise for the sake of brevity and the reader is encouraged to peruse Section 3.2 of the above mentioned paper.

Given a set $\mathcal{S}$ of k-tuples (not necessarily finite),

$$\mathcal{S} = \{\underline{n} = (n_1,\dots,n_k)\},$$

in [20], we undertook a systematic study of sums of the form

$$\sum_{\underline{n}\in\mathcal{S}} w_{\underline{n}}\Big(\sum_{\underline{d}|\underline{n}}\lambda_{\underline{d}}\Big)^2, \tag{5}$$

satisfying certain hypotheses. Here $w_{\underline{n}}$ is a 'weight' attached to the tuples $\underline{n}$ and $\lambda_{\underline{d}}$'s are sieve parameters chosen in terms of a fixed positive real number R and a smooth real valued test function $\mathcal{F}$ supported on the simplex

$$\Delta_k(1) := \{(t_1,\dots,t_k) \in [0,\infty)^k : t_1 + \dots + t_k \le 1\}.$$

More precisely, we chose:

$$\lambda_{\underline{d}} = \mu(\underline{d})\mathcal{F}\left(\frac{\log d_1}{\log R},\dots,\frac{\log d_k}{\log R}\right). \tag{6}$$

The sum (5) was assumed to satisfy the following hypotheses.

H1. If a prime p divides a tuple $\underline{n}$ such that p divides n_i and n_j, with $i \ne j$, then p must lie in some fixed finite set of primes $\mathcal{P}_0$.

This allows us to perform the 'W trick', that is, restrict $\underline{n}$ in the above sum to be congruent to a residue class $\underline{b} \pmod W$ such that $(b_i, W) = 1$ for all i.

H2. The function $w_{\underline{n}}$ satisfies

$$\sum_{\substack{\underline{d}|\underline{n}\\ \underline{n}\equiv\underline{b}\,(\mathrm{mod}\ W)}} w_{\underline{n}} = \frac{X}{f(\underline{d})} + r_{\underline{d}},$$

for some multiplicative function f and some quantity X depending on the set $\mathcal{S}$.

H3. The components of f satisfy

$$f_j(p) = \frac{p}{\alpha_j} + O(p^t), \text{ with } t < 1$$

for some fixed $\alpha_j \in \mathbb{N}$.

We denote the tuple $(\alpha_1, \ldots, \alpha_k)$ as $\underline{\alpha}$ and the sum of the components $\sum_{j=1}^{k} \alpha_j$ as α.

H4. There exists $\theta > 0$ and $Y \ll X$ such that

$$\sum_{[\underline{d},\underline{e}]<Y^\theta} |r_{[\underline{d},\underline{e}]}| \ll \frac{Y}{(\log Y)^A},$$

for any $A > 0$.

With all this in place, we state below the main result of the higher rank sieve obtained in [20].

Theorem 3. *Let $\lambda_{\underline{d}}$'s be as chosen in* (6)*. Suppose hypotheses H1 to H3 hold and H4 holds with $Y = X$. Set $R = X^{\theta/2-\delta}$ for small $\delta > 0$. Then,*

$$\sum_{\underline{n} \equiv \underline{b} \pmod{W}} w_n \left(\sum_{\underline{d} | \underline{n}} \lambda_{\underline{d}} \right)^2 = (1 + o(1)) C(\mathcal{F}, \mathcal{F})^{(\underline{\alpha})} c(W) \frac{X}{(\log R)^\alpha},$$

with

$$c(W) := \frac{W^\alpha}{\phi(W)^\alpha},$$

and

$$C(\mathcal{F}, \mathcal{F})^{(\underline{\alpha})} = \int_0^\infty \cdots \int_0^\infty \left(\prod_{j=1}^{k} \frac{t_j^{\alpha_j - 1}}{(\alpha_j - 1)!} \right) \left(\mathcal{F}^{(\underline{\alpha})}(\underline{t}) \right)^2 d\underline{t}.$$

Here $\mathcal{F}(\underline{t})^{\underline{\alpha}}$ denotes the mixed partial derivative as given in (4)*.*

5. An application of the higher rank sieve

We apply the theory of the previous section to the set of 3-tuples

$$\mathcal{S} = \{(n, 6n + 1, 12n + 1) : N < n \leq 2N\}.$$

There exists $n_p \in \mathbb{N}$ so that the set $\{(n_p, 6n_p + 1, 12n_p + 1)\}$ is not the complete set of residues modulo p for any prime p, as can be seen by checking for the primes $2, 3$. More generally, to check the admissibility of a k-element set, one need only check admissibility for all primes $p \leq k$. Hence, this set is indeed admissible. In order to set up the sieve for this set, we need to check hypothesis H1 for $\mathcal{S}$. This condition is vacuous for $\mathcal{S}$ because for any n, the elements of $\mathcal{S}$ are pairwise co-prime. We set $W = \prod_{p < D_0} p$, with $D_0 = \log\log\log N$, so that $W \ll (\log\log N)^2$ by an application of the Chebycheff's estimate for the prime counting function. We choose $b \pmod W$ such that each component of $\underline{b} = (b, 6b + 1, 12b + 1)$ is co-prime to W.

Using the notation $\underline{d}$ to represent a 3-tuple, we are now ready to set up the sums

$$S_1 = \sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W)}} \left(\sum_{\underline{d}|\underline{n}} \lambda_{\underline{d}}\right)^2, \tag{7}$$

and

$$S_2 = \sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W)}} (\chi_{\mathbb{P}}(n) + \chi_{\mathbb{P}}(6n+1) + \chi_{\mathbb{P}}(12n+1)) \left(\sum_{\underline{d}|\underline{n}} \lambda_{\underline{d}}\right)^2, \tag{8}$$

where $\lambda_{\underline{d}}$'s are chosen as in (6).

The key idea of this approach is then as follows. For some $\rho > 1$, if $S_2(N,\rho) - \rho S_1 > 0$, as $N \to \infty$, then there are infinitely many integers n such that at least 2 of $n, 6n+1, 12n+1$ are prime. We refer the reader to Proposition 4.1 of [20] for a proof of this fact.

We proceed to give asymptotic formulas for the sums S_1 and S_2. The asymptotic formula for S_1 is given in Lemma 4.2 of [20], which we restate here in the case $k = 3$ for convenience.

Lemma 4. *Choose $\theta < 1$ and $R = N^{\theta/2-\delta}$ for some small $\delta > 0$ to be chosen later. Then, as $N \to \infty$,*

$$S_1 := \sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W)}} \left(\sum_{\underline{d}|\underline{n}} \lambda_{\underline{d}}\right)^2 = (1+o(1))\frac{W^2}{\phi(W)^3}\frac{N}{(\log R)^3} I(\mathcal{F}),$$

where

$$I(\mathcal{F}) = \int_{\mathbb{R}^3} \left(\mathcal{F}^{(\underline{1})}(\underline{t})\right)^2 dt_1 dt_2 dt_3,$$

with $\mathcal{F}^{(\underline{1})}(\underline{t})$ as in (4).

We also have an asymptotic formula for the sum

$$S_2^{(1)} := \sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W)}} \chi_{\mathbb{P}}(n) \left(\sum_{\underline{d}|\underline{n}} \lambda_{\underline{d}}\right)^2,$$

originally derived by Maynard and Tao, stated in Lemma 4.3 of [20] as follows.

Lemma 5. *With $\theta < 1/2 - \delta$ and $R = N^{\theta/2-\delta}$, we have as $N \to \infty$,*

$$S_2^{(1)} := \sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W)}} \chi_{\mathbb{P}}(n) \left(\sum_{\underline{d}|\underline{n}} \lambda_{\underline{d}}\right)^2 = (1+o(1))\frac{W^2}{\phi(W)^3}\frac{(\pi(2N)-\pi(N))}{(\log R)^2} J_1(\mathcal{F}),$$

with $J_1(\mathcal{F})$ given by the integral

$$\int_{\mathbb{R}^2} \left(\mathcal{F}_1^{(\underline{1})}(t_2,t_3)\right)^2 dt_2 dt_3.$$

Here $\mathcal{F}_1$ is the function $\mathcal{F}$ restricted to tuples with the first component zero, that is, $\mathcal{F}_1(t_2,t_3) = \mathcal{F}(0,t_2,t_3)$, and $\mathcal{F}_1^{(\underline{1})}(t_2,t_3)$ is as given in (4).

We will show that the sums involving $\chi_{\mathbb{P}}(6n+1)$ and $\chi_{\mathbb{P}}(12n+1)$ give the same asymptotic formulas as $S_2^{(1)}$.

Theorem 6. *With $\theta < 1/2 - \delta$ and $R = N^{\theta/2-\delta}$, we have as $N \to \infty$,*

$$S_2^{(2)} := \sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W)}} \chi_{\mathbb{P}}(6n+1)\left(\sum_{\underline{d}|\underline{n}} \lambda_{\underline{d}}\right)^2 = (1+o(1))\frac{W^2}{\phi(W)^3}\frac{(\pi(2N)-\pi(N))}{(\log R)^2} J_2(\mathcal{F}),$$

and

$$S_2^{(3)} := \sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W)}} \chi_{\mathbb{P}}(12n+1)\left(\sum_{\underline{d}|\underline{n}} \lambda_{\underline{d}}\right)^2 = (1+o(1))\frac{W^2}{\phi(W)^3}\frac{(\pi(2N)-\pi(N))}{(\log R)^2} J_3(\mathcal{F}),$$

where

$$J_2(\mathcal{F}) = \int_{\mathbb{R}^2} (\mathcal{F}_2^{(1)}(t_1,t_3))^2 dt_1 dt_3, \qquad J_3(\mathcal{F}) = \int_{\mathbb{R}^2} (\mathcal{F}_3^{(1)}(t_1,t_2))^2 dt_1 dt_2$$

with notation as in Lemma 5.

Proof. Expanding the square and interchanging summation gives

$$\sum_{\underline{d},\underline{e}} \lambda_{\underline{d}}\lambda_{\underline{e}} \Bigg(\sum_{\substack{n\sim N \\ n\equiv b \,(\mathrm{mod}\ W) \\ [\underline{d},\underline{e}]|\underline{n}}} \chi_{\mathbb{P}}(6n+1) \Bigg)$$

For the above sum to be non-trivial, we must have $[d_2, e_2] = 1$. Writing $6n+1$ as n', the congruence condition $n \equiv b \,(\mathrm{mod}\ W)$ implies that $n' \equiv 6b+1 \,(\mathrm{mod}\ W)$ but is *not* equivalent to it. Instead we have

$$n \equiv b \,(\mathrm{mod}\ W) \Leftrightarrow n' \equiv 6b+1 \,(\mathrm{mod}\ 6W).$$

Note that this condition ensures that n' is of the form $6n+1$ for some integer n.

We observe that $[d_1, e_1]$ must be co-prime to W because $[d_1, e_1]$ divides n which is in the residue class $b \,(\mathrm{mod}\ W)$ and is hence co-prime to W. In particular, the co-primality of $[d_1, e_1]$ and 6 gives

$$n \equiv 0 \,(\mathrm{mod}\ [d_1, e_1]) \Leftrightarrow n' \equiv 1 \,(\mathrm{mod}\ [d_1, e_1]).$$

Similarly, $[d_3, e_3]$ is co-prime to W, so that

$$12n+1 \equiv 0 \,(\mathrm{mod}\ [d_3, e_3]) \Leftrightarrow n' \equiv \bar{2}(-1)+1 \,(\mathrm{mod}\ [d_3, e_3]),$$

where $\bar{2}$ is the inverse class of 2 $(\mathrm{mod}\ [d_3, e_3])$. Using the Chinese remainder theorem to write this system of congruence equations as a single congruence relation, we have for the sum above

$$\sum_{\substack{\underline{d},\underline{e} \\ d_2=e_2=1}} \lambda_{\underline{d}}\lambda_{\underline{e}} \Bigg(\sum_{\substack{n'\sim 6N \\ n'\equiv a \,(\mathrm{mod}\ q)}} \chi_{\mathbb{P}}(n') \Bigg),$$

where $q = 6W[d_1, e_1][d_3, e_3]$ and a is some residue class co-prime to q. This sum now is the same as S_1 with W, N replaced by $6W, 6N$ respectively. We can proceed as in Lemma 4.3 of [20] to obtain

$$S_2 = (1 + o(1))\frac{(6W)^2}{\phi(6W)^3}\frac{6(\pi(2N) - \pi(N))}{(\log R)^2}J_2(\mathcal{F}).$$

As

$$\frac{\phi(6W)}{6W} = \prod_{p|6W}\left(1 - \frac{1}{p}\right) = \frac{\phi(W)}{W},$$

we see that $\phi(6W) = 6\phi(W)$, thus giving the required asymptotic formula for $S_2^{(2)}$. This argument can be repeated mutatis mutandis for the sum $S_2^{(3)}$. □

Putting the above formulae together and using the prime number theorem, we have the following result.

Theorem 7. *Choosing $\theta < 1/2 - \delta$ and $R = N^{\theta/2-\delta}$, we have as $N \to \infty$,*

$$S(N, \rho) := S_2 - \rho S_1 \sim \frac{W^2}{\phi(W)^3}\frac{N}{(\log R)^3}I(\mathcal{F})\left(\left(\frac{\theta}{2} - \delta\right)M_3(\mathcal{F}) - \rho\right),$$

where $M_3(\mathcal{F})$ is defined as the functional

$$\frac{J_1(\mathcal{F}) + J_2(\mathcal{F}) + J_3(\mathcal{F})}{I(\mathcal{F})},$$

which is the same as $3J_1(\mathcal{F})/I(\mathcal{F})$ because of the symmetry of the function $\mathcal{F}$.

In order to show $S(N, \rho) > 0$ for some $\rho > 0$, it is necessary to have good numerical estimates for

$$M_3 = \sup_{\mathcal{F}}\frac{3J_1(\mathcal{F})}{I(\mathcal{F})}, \tag{9}$$

where the supremum is taken over all square integrable functions supported on $\Delta_3(1)$. More precisely, assuming the Elliott-Halberstam conjecture, that is, $\theta = 1-\epsilon$ for some $\epsilon > 0$ in (2), if one can show that $M_3(\mathcal{F}) > 2$, this gives $S(N, \rho) > 0$ as $N \to \infty$, for some $\rho > 1$. This would prove conditionally that there are infinitely many $n \in \mathbb{N}$ such that at least two of $n, 6n + 1, 12n + 1$ are prime. Unfortunately, we do not have good enough numerical estimates for M_3 currently, leading us to assume the stronger generalized Elliott-Halberstam conjecture.

Assuming GEH, Theorems 28, 29 of [18] show that for any $0 < \epsilon \leq 1/2$, one can consider instead of M_3, the functional

$$M_{3,\epsilon}(F) = \frac{3J_{1,1-\epsilon}(F)}{I(F)}, \tag{10}$$

where

$$J_{1,1-\epsilon}(\mathcal{F}) := \int\limits_{\Delta_2(1-\epsilon)}\left(\mathcal{F}_1^{(1)}(t_2, t_3)\right)^2 dt_2 dt_3, \tag{11}$$

and F is now a non-zero square integrable function supported on the enlarged simplex

$$\Delta_3(3/2) = \{(t_1, t_2, t_3) \in [0, \infty)^3 : t_1 + t_2 + t_3 \leq 3/2\}.$$

Moreover, F satisfies the condition

$$\int_0^\infty F(t_1, t_2, t_3)dt_1 = 0,$$

whenever $t_1 + t_2 > 1 + 1/4$. Theorem 29 of [18] also establishes that there exists a piecewise polynomial function F satisfying the above conditions such that $M_{3,1-\epsilon} > 2$. This gives the following theorem.

Theorem 8. *Assuming GEH, there are infinitely many $n \in \mathbb{N}$ such that at least two of $n, 6n+1, 12n+1$ are prime.*

6. The disjunction theorem

We first prove the following result below.

Theorem 9. *Assuming GEH, at least one of the following is true:*

(i) *For all a not equal to ± 1 or a perfect square, there are infinitely many primes q such that the index of $a \pmod q$ is bounded by 3.*
(ii) *The Lang-Trotter conjecture holds for all CM elliptic curves $E/\mathbb{Q}$ with rank $E(\mathbb{Q}) \geq 1$ and CM field $k \neq \mathbb{Q}(\omega), \mathbb{Q}(i)$.*

Proof. In order to prove this, we examine in turn each of the three cases arising in Theorem 8.

Case 1. n and $6n+1$ are prime infinitely often:

This means that there are infinitely many primes p and q such that $q = 6p+1$. Fix $b \in \mathbb{N}$ not equal to ± 1 or a perfect square. We consider the order of a modulo q, denoted by $o(a) \pmod q$. If $o(a) = q-1$, we are done. So assume otherwise. As $o(a)|q-1 = 6p$, the only other possibilities for $o(a)$ are $2, 3, 6, p, 2p$ and $3p$. If the order of $a \pmod q$ is 2 we have $q|a^2 - 1$. As a is fixed, there can only be finitely many such primes q and we eliminate these from our discussion. The same can be done if the order of $a \pmod q$ is 3 or 6.

On the other hand, if the order of $a \pmod q$ is p or $3p$, then we have

$$a^{\frac{q-1}{2}} \equiv 1 \pmod q,$$

which means that a is a quadratic residue modulo q. It is possible to eliminate this possibility by imposing a suitable congruence condition on n (and hence q) throughout the discussion of Section 4. We are left with the possibility that the order of a is $2p$, which means that $a^{\frac{q-1}{3}} \equiv 1 \pmod q$. This means that the index of $a \pmod q$ is bounded by 3.

Case 2. n and $12n+1$ are prime infinitely often:

This gives infinitely many primes p, q with $q = 12p+1$. Given $a \in \mathbb{N}$ not equal to ± 1 or a perfect square, if $a \pmod q$ does not generate $\mathbb{F}_q$, the order of $a \pmod q$ can only be $2, 3, 4, 6, 12, p, 2p, 3p, 4p$ or $6p$. We consider each of these cases in turn. If the order of $a \pmod q$ is $2, 3, 4, , 6$ or 12, we see as before that the number of such primes q is finite and can be removed from the set of primes under consideration.

If the order of $a \pmod q$ is $p, 2p, 3p$ or $6p$, we have

$$a^{\frac{q-1}{2}} \equiv 1 \pmod q,$$

so that a is a quadratic residue modulo q. As before, it is possible to get rid of this possibility. We are left with the case

$$a^{4p} = a^{\frac{q-1}{3}} \equiv 1 \pmod{q},$$

which means that the index of $a \pmod{q}$ is bounded by 3.

Case 3. $6n+1$ and $12n+1$ are prime infinitely often:

This means that there are infinitely many primes p, q, with $q = 2p-1$. Given an elliptic curve $E/\mathbb{Q}$, with CM field $k \neq \mathbb{Q}(\omega), \mathbb{Q}(i)$, we are ensured that q is inert in the ring of integers O_k, so that $a_q = 0$. This can be done by imposing a suitable congruence condition on n. Fix a point $a \in E(\mathbb{Q})$ having infinite order and consider its image modulo q, denoted $\bar{a}$. Then $\bar{a} \in E(\mathbb{F}_q)$. We want to show that $\bar{a}$ generates the group $E(\mathbb{F}_q)$. As $|E(\mathbb{F}_q)| = q + 1 - a_q = 2p$, we see that the order of $\bar{a}$ can either be 2, p or $q+1$. If it is 2, then $\bar{a}$ is a two-torsion point in $E(\mathbb{F}_q)$, giving only finitely many such q. If the order is p, then $\bar{a} = 2\bar{m}$ for some $\bar{m} \in E(\mathbb{F}_q)$. Writing $a = (a_1, a_2)$, we see that a_1 must be the solution of a quartic polynomial modulo q. This leads to a quartic polynomial having a solution $\pmod{q}$. Since the splitting field of a quartic polynomial contains a quadratic extension, we can impose congruence conditions on q so that q does not split in this extension. This means that the order of $\bar{a}$ must be $q+1$. □

7. Concluding remark

In the previous section, we obtained a conditional disjunction result concerning the bounded index problem and the Lang-Trotter conjecture for CM elliptic curves. The proof of Theorem 2 can be obtained by a slight variation of this argument. In Cases 1 and 2 of the above proof, it is possible to get rid of the possibility that $a^{\frac{q-1}{3}} \equiv 1 \pmod{q}$ by noticing that this means that q splits in the field $K = \mathbb{Q}(\omega, a^{1/3})$. For any $\epsilon > 0$, we can apply Theorem 1 with level of distribution $\theta = 1 - \epsilon$ (assumed under GEH), to get rid of the contribution from such primes q. This gives a positive proportion of primes q for which a is a primitive root modulo q. One could also modify these arguments to treat elliptic curves which have CM by $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$.

References

[1] Emil Artin, *Collected papers*, Springer-Verlag, New York-Berlin, 1982. Edited by Serge Lang and John T. Tate; Reprint of the 1965 original. MR671416

[2] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in arithmetic progressions to large moduli*, Acta Math. **156** (1986), no. 3-4, 203–251, DOI 10.1007/BF02399204. MR834613

[3] Rajiv Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130, DOI 10.1007/BF01388719. MR762358

[4] Rajiv Gupta and M. Ram Murty, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), no. 1, 13–44. MR834046

[5] D. R. Heath-Brown, *Almost-prime k-tuples*, Mathematika **44** (1997), no. 2, 245–266, DOI 10.1112/S0025579300012584. MR1600529

[6] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38, DOI 10.1093/qmath/37.1.27. MR830627

[7] Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220, DOI 10.1515/crll.1967.225.209. MR0207630

[8] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), no. 2, 289–292, DOI 10.1090/S0002-9904-1977-14310-3. MR0427273

[9] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. MR0568299

[10] James Maynard, *Small gaps between primes*, Ann. of Math. (2) **181** (2015), no. 1, 383–413, DOI 10.4007/annals.2015.181.1.7. MR3272929

[11] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[12] L. J. Mordell, *On the rational solutions of indeterminate equations of the third and fourth degree*, Proc. Cambridge Philos. Soc, 21 (1922), 179-192.

[13] Yoichi Motohashi, *An induction principle for the generalization of Bombieri's prime number theorem*, Proc. Japan Acad. **52** (1976), no. 6, 273–275. MR0422179

[14] M. Ram Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), no. 4, 59–67, DOI 10.1007/BF03023749. MR966133

[15] M. Ram Murty and V. Kumar Murty, *A variant of the Bombieri-Vinogradov theorem*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 243–272. MR894326

[16] M. Ram Murty and A. Vatwani, A higher rank Selberg sieve with an additive twist and applications, *Funct. Approx. Comment. Math.*, 2017, to appear.

[17] M. Ram Murty and Akshaa Vatwani, *Twin primes and the parity problem*, J. Number Theory **180** (2017), 643–659, DOI 10.1016/j.jnt.2017.05.011. MR3679820

[18] D. H. J. Polymath, *Variants of the Selberg sieve, and bounded intervals containing many primes*, Res. Math. Sci. **1** (2014), Art. 12, 83, DOI 10.1186/s40687-014-0012-7. MR3373710

[19] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[20] A. Vatwani, A higher rank Selberg sieve and applications, *Czechoslovak Mathematical Journal*, 2017, to appear.

[21] Akshaa Vatwani, *Bounded gaps between Gaussian primes*, J. Number Theory **171** (2017), 449–473, DOI 10.1016/j.jnt.2016.07.008. MR3556693

[22] Hartmut Siebert and Dieter Wolke, *Über einige Analoga zum Bombierischen Primzahlsatz*, Math. Z. **122** (1971), no. 4, 327–341, DOI 10.1007/BF01110168. MR0409391

[23] Yitang Zhang, *Bounded gaps between primes*, Ann. of Math. (2) **179** (2014), no. 3, 1121–1174, DOI 10.4007/annals.2014.179.3.7. MR3171761

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, Canada K7L 3N6

E-mail address: murty@mast.queensu.ca

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: avatwani@uwaterloo.ca