BOUNDED GAPS BETWEEN PRODUCTS OF PRIMES WITH APPLICATIONS TO IDEAL CLASS GROUPS AND ELLIPTIC CURVES

FRANK THORNE

Abstract. In the recent papers [12, 13], Goldston, Graham, Pintz, and Yıldırım use a variant of the Selberg sieve to prove the existence of small gaps between E_2 numbers, that is, square-free numbers with exactly two prime factors. We apply their techniques to prove similar bounds for E_r numbers for any $r \geq 2$, where these numbers are required to have all of their prime factors in a set of primes $\mathcal{P}$. Our result holds for any $\mathcal{P}$ of positive density that satisfies a Siegel-Walfisz condition regarding distribution in arithmetic progressions. We also prove a stronger result in the case that $\mathcal{P}$ satisfies a Bombieri-Vinogradov condition. We were motivated to prove these generalizations because of recent results of Ono [22] and Soundararajan [25]. These generalizations yield applications to divisibility of class numbers, nonvanishing of critical values of L-functions, and triviality of ranks of elliptic curves.

1. Introduction and Statement of Results

In a recent series of papers [11, 12, 13], Goldston, Graham, Pintz, and Yıldırım (GGPY) considered the problem of bounding gaps between primes and almost primes. Goldston, Pintz, and Yıldırım proved in [11] that

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log n} = 0, \tag{1.1}$$

and Goldston, Graham, Pintz, and Yıldırım gave an alternate proof [12] of (1.1) based on the Selberg sieve. In the latter paper, the authors also observed that their method could be successfully applied to E_2 numbers, that is, square-free numbers with exactly two prime factors. In [13] these authors proved that

$$\liminf_{n\to\infty} \big(q_{n+1}-q_n\big) \leq 6, \tag{1.2}$$

where q_n denotes the nth E_2 number. They further showed that their method was highly adaptable, and obtained bounds between nonconsecutive almost-primes q_n and $q_{n+\nu}$ for any ν, and between E_2 numbers whose prime factors are both congruent to 1 modulo 4.

The reason for this adaptability is the following. The proofs in [11, 12, 13] proceed by considering a sum of the shape

$$S = \sum_{n=N}^{2N} \left(\sum_{h\in\mathcal{H}} \chi(n+h) - 1 \right) \left(\sum_{d \mid \prod_h (n+h)} \lambda_d \right)^2, \tag{1.3}$$

where $\chi(n)$ is the characteristic function of the primes or of a related sequence, $\mathcal{H}$ is a finite set of integers, and the λ_d are (real-valued) Selberg sieve coefficients, which have the property that the squared term is very small if $\prod_h (n+h)$ is divisible by many small primes. If $S > 0$ asymptotically for large N and a fixed choice of $\mathcal{H}$, then this argument proves the existence of bounded gaps between the integers counted by $\chi(n)$.

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

In this paper we will exploit this adaptability and prove the following rather general theorem:

Theorem 0. *Suppose $\mathcal{P}$ is an infinite set of primes of positive density satisfying certain conditions to be described later. Let ν and r be positive integers with $r \geq 2$, and let q_n denote the nth E_r number whose prime factors are all in $\mathcal{P}$. Then*

$$\liminf_{n\to\infty}(q_{n+\nu} - q_n) < C(r, \nu, \mathcal{P}),$$

for an effectively computable constant $C(r, \nu, \mathcal{P})$.

"Theorem 0" is the general statement of our main results, and a precise formulation will be given as Theorems 2.1, 2.2, and 2.3. The conditions on $\mathcal{P}$ are the Bombieri-Vinogradov or (for $r \geq 3$) Siegel-Walfisz conditions, which require that the primes of $\mathcal{P}$ be well-distributed in arithmetic progressions; these conditions will be defined precisely in Section 2. The constant $C(r, \nu, \mathcal{P})$ may be easily computed in particular cases.

We remark that some related results have also been obtained independently by Jimenez-Urroz [15].

Our work was largely motivated by the case where $\mathcal{P}$ has *Frobenius density*. This means that there exists a Galois extension $K/\mathbb{Q}$ with the property that those primes $p \in \mathcal{P}$, up to finitely many exceptions, are distinguished as those primes for which the $\mathrm{Frob}(p)$ constitute a fixed conjugacy class or a union of conjugacy classes in $\mathrm{Gal}(K/\mathbb{Q})$. The Chebotarev Density Theorem implies such a set indeed has a positive density in the set of all primes, and a result of Murty and Murty [19] (see Lemma 3.1) implies that $\mathcal{P}$ satisfies our Bombieri-Vinogradov condition.

We can use Theorem 0 to prove several corollaries. The first of these, a number field analogy of (1.2), is immediate:

Corollary 1.1. *Suppose that $K/\mathbb{Q}$ is a Galois extension, and $r \geq 2$ is an integer. Then there exist a constant $C(K)$ and infinitely many nonconjugate pairs of ideals $\mathfrak{a}$ and $\mathfrak{b}$, each with exactly r distinct prime factors, whose norms differ by at most $C(K)$.*

Another application is suggested by the work of Ono [22] and Balog and Ono [1] regarding elliptic curves and non-vanishing of modular L-functions. We start by recalling some notation (see, e.g., [17, 24] for definitions). Given an elliptic curve $E/\mathbb{Q}$, we denote by $L(E, s)$ its Hasse-Weil L-function, and we define the Mordell-Weil rank $\mathrm{rk}(E) := \mathrm{rk}(E, \mathbb{Q})$ to be the rank of the (abelian) group of rational points on E over $\mathbb{Q}$. By Kolyvagin's work [18] on the Birch and Swinnerton-Dyer conjecture, we have $\mathrm{rk}(E) = 0$ for any E for which $L(E, 1) \neq 0$.

If E is given by the equation

$$E: \quad y^2 = x^3 + ax^2 + bx + c$$

we define, for a fundamental discriminant D, the *D-quadratic twist* $E(D)$ by the equation

$$E(D): \quad Dy^2 = x^3 + ax^2 + bx + c.$$

It is natural to consider the set of D for which $L(E(D), 1)) \neq 0$. Goldfeld [10] conjectured that for an elliptic curve $E/\mathbb{Q}$ with conductor N, we have

$$\sum_{\substack{|D|\leq X,\\ \gcd(D,N)=1}} \mathrm{ord}_{s=1}(L(E(D), s)) \sim \frac{1}{2} \sum_{\substack{|D|\leq X,\\ \gcd(D,N)=1}} 1, \tag{1.4}$$

where D ranges over all fundamental discriminants D with $-X \leq D \leq X$. The strongest known result in this direction is due to Ono and Skinner [23], who proved the lower bound

$$\#\{|D| \leq X \ : \ L(E(D), 1) \neq 0 \text{ and } \gcd(D, N) = 1\} \gg \frac{X}{\log X}. \tag{1.5}$$

Moreover, for elliptic curves $E/\mathbb{Q}$ without a $\mathbb{Q}$-rational torsion point of order 2, Ono [22] improved (1.5) to

$$\#\{|D| \leq X \ : \ L(E(D),1) \neq 0 \text{ and } \gcd(D,N)=1\} \gg \frac{X}{\log^{1-\alpha} X}, \tag{1.6}$$

where α is the density of a certain set of primes S_E. Although these results are strong, they do not imply the existence of infinitely many bounded gaps between such D.

However, Ono's proof of (1.6) gives an explicit description of a set of D satisfying the above conditions. Specifically, there is an integer D_E and a set of primes S_E with positive Frobenius density (see Section 3) with the property that for every positive integer j we have

$$L(E(D_E p_1 p_2 \dots p_{2j}),1) \neq 0$$

and

$$\mathrm{rk}(E(D_E p_1 p_2 \dots p_{2j}),\mathbb{Q}) = 0$$

whenever $p_1, p_2, \dots, p_{2j} \in S_E$ are distinct primes not dividing N. Taking $j=1$, Theorem 2.1 then implies the existence of bounded gaps:

Theorem 1.2. *Let $E/\mathbb{Q}$ be an elliptic curve without a $\mathbb{Q}$-rational torsion point of order 2. Then there is a constant C_E and infinitely many pairs of square-free integers m and n for which the following hold:*

(i) $L(E(m),1) \cdot L(E(n),1) \neq 0$,
(ii) $\mathrm{rk}(E(m)) = \mathrm{rk}(E(n)) = 0$,
(iii) $|m-n| < C_E$.

The constant C_E can be explicitly computed, and in Section 6 we give an example of this result for the elliptic curve $X_0(11)$.

Remark. The analog of Theorem 1.2 (i) holds for any even weight modular L-function associated to a newform with non-trivial mod 2 Galois representation (see Theorem 1 of [22]).

We also consider the work of Balog and Ono [1]. For a large class of elliptic curves E, Balog and Ono prove lower bounds on the number of quadratic twists $E(n)$ with zero rank, with the additional property that their Shafarevich-Tate groups contain an element of order $\ell \in \{3,5,7\}$. For "good" curves E, they prove that these properties hold for the quadratic twists $E(-Mp_1 \dots p_{2\ell})$, whenever there is a solution to the Diophantine equation

$$Mcp_1 \dots p_{2\ell} = m^{2\ell} - n^2 \tag{1.7}$$

for certain values M and c, where the primes p_i are restricted to a set $\mathcal{P}$ satisfying a Siegel-Walfisz condition. Balog and Ono then use the "circle method" to prove a lower bound for the number of solutions of (1.7). It is natural to ask whether a result similar to Theorem 1.2 can be proved in this situation. Such a result would follow immediately if we could extend the result of Theorem 2.3 to the situation where we impose the additional condition (1.7). This problem is more difficult, and it suggests a potential application of bounding gaps between E_r numbers for larger values of r.

Although we do not currently have a proof, we can apply our methods to a related question concerning divisibility of class groups of quadratic fields. Balog and Ono's proof in [1] proceeds by using a result of Soundararajan [25], which shows that for any integer $g \geq 3$, the ideal class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ contains an element of order g for any d satisfying a condition similar to (1.7). In the case $g=4$, Soundararajan gives a simple classification of such d, and thereby proves that for any positive square-free $d \equiv 1 \pmod 8$ whose prime factors are all congruent to $\pm 1 \pmod 8$, the class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ contains an element of order 4.

Theorem 2.1 implies the existence of bounded gaps, and we can easily obtain an explicit bound. (See Section 2 for the definitions of Hypothesis BV and admissible tuples of linear forms.)

Let $\mathcal{P}$ be the set of primes $\equiv 1 \pmod 8$, and let $\mathcal{P}'$ be the set of primes $\equiv 7 \pmod 8$. $\mathcal{P}$ and $\mathcal{P}'$ each satisfy Hypothesis $BV(\frac{1}{2}, 8)$; i.e., they have level of distribution $1/2$ and are well-distributed in arithmetic progressions to moduli coprime to 8. We now choose a k-tuple $\mathcal{L} = \{8n + b_j\}$ with each $b_j \equiv 1 \pmod 8$. Then half of the E_2 numbers represented by linear forms in $\mathcal{L}$ will have both prime factors either in $\mathcal{P}$ or in $\mathcal{P}'$. (In the notation of Theorem 2.1, we have $\delta\varphi(M) = 1/2$, and we are appealing to the remark following Theorem 2.3.)

Applying Theorem 2.1 with $\delta = 1/8$ and $M = 8$, we may take $k = 6$. One 8-admissible 6-tuple with each $b_j \equiv 1 \pmod 8$ is $\{8n + 49, 8n + 65, 8n + 73, 8n + 89, 8n + 97, 8n + 113\}$. We therefore obtain the following result concerning ideal class groups of imaginary quadratic fields.

Corollary 1.3. *There are infinitely many pairs of E_2 numbers, say m and n, such that the class groups $\mathrm{Cl}(\mathbb{Q}(\sqrt{-m}))$ and $\mathrm{Cl}(\mathbb{Q}(\sqrt{-n}))$ each contain elements of order 4, with*

$$|m - n| \leq 64.$$

There are other applications of these results, and we conclude by briefly describing an application to the nonvanishing of Fourier coefficients of modular forms. By the theory of Deligne and Serre [8], if $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_1(\Gamma_0(N), \chi)$ is a weight 1 newform, then the set of primes p for which $a(p) = 0$ has Frobenius density δ with $0 < \delta < 1$. By the multiplicativity of Fourier coefficients of newforms, almost all of the $a(n)$ (as n ranges over all integers) are zero. However, our results prove the existence of bounded gaps between those n for which $a(n)$ does not vanish. Moreover, for newforms of higher integer weight, the theory of p-adic Galois representations implies that almost all of the $a(n)$ vanish modulo p, for any prime p. In this case, we obtain bounded gaps between those $a(n)$ that do not vanish modulo p.

Acknowledgements

I would like to thank Kevin Ford, Dan Goldston, Andrew Granville, M. Ram Murty, Robert Rhoades, Jeremy Rouse, Cem Yıldırım, and the referee for many useful suggestions regarding this paper. I would particularly like to thank Ken Ono for suggesting and supervising this project, and Sid Graham for his encouragement and for answering my many questions about his work.

2. Preliminaries, Notation, and Precise Statement of Results

In order to properly formulate our main results we need to introduce some hypotheses and notation.

2.1. **Distribution conditions on $\mathcal{P}$.** We start by defining the Bombieri-Vinogradov ($BV(\vartheta, M)$) and Siegel-Walfisz conditions that our set of primes $\mathcal{P}$ may satisfy. These conditions are analogous to the Bombieri-Vinogradov and Siegel-Walfisz theorems on the distribution of primes (see [7]), but we will require something slightly more than the direct analogues of these theorems.

Assume an infinite set of primes $\mathcal{P}$ is given. We will require that $\mathcal{P}$ be well-distributed in arithmetic progressions modulo m for every m coprime to a fixed modulus M. For any m coprime to M, let $\mathcal{P}_m$ denote the set of primes in $\mathcal{P}$ congruent to m modulo M. For each m, assume that $\mathcal{P}_m$ has a (natural) density $\delta(m) \geq 0$, and for any N and q, and any a coprime to q, define an error term $\Delta_{\mathcal{P}_m}(N; q, a)$ by the equation

$$\Delta_{\mathcal{P}_m}(N; q, a) := \sum_{\substack{N < p \leq 2N \\ p \equiv a \pmod q \\ p \in \mathcal{P}_m}} 1 - \frac{1}{\varphi(q)} \sum_{\substack{N < p \leq 2N \\ p \in \mathcal{P}_m}} 1. \tag{2.1}$$

We say that $\mathcal{P}$ *satisfies Hypothesis* $BV(\vartheta, M)$, or equivalently, has *level of distribution* ϑ, if for each m coprime to M, and for any positive ϵ and A,

$$\sum_{\substack{q\le N^{\theta-\epsilon}\\(q,M)=1}} \max_{\substack{a\\(a,q)=1}} \Delta_{\mathcal{P}_m}(N;q,a) \ll_{\epsilon,A} N\log^{-A} N. \tag{2.2}$$

We say that $\mathcal{P}$ satisfies a *Siegel-Walfisz condition* for M if for each m we have

$$\Delta_{\mathcal{P}_m}(N;q,a) \ll_{\epsilon,A} N\log^{-A} N \tag{2.3}$$

uniformly for all q with $(q, Ma) = 1$. If (2.3) holds, we may readily check that the same bound holds with the condition $p \le N$ substituted for $N < p \le 2N$ in (2.1).

We will not need assumptions about products of primes of $\mathcal{P}$. Instead, we will use a result of Motohashi [20] and Bombieri, Friedlander, and Iwaniec [3] to prove that an appropriate result of Bombieri-Vinogradov type will hold for a sufficiently large set of almost-primes formed from $\mathcal{P}$.

2.2. **Linear forms and admissibility.** Following [13], we shall prove our results for k-tuples of linear forms

$$L_i(x) := a_i x + b_i \quad (1 \le i \le k) \quad a_i, b_i \in \mathbb{Z}, \quad a_i > 0. \tag{2.4}$$

Our results take the shape that for any admissible k-tuple with k sufficiently large, there are infinitely many x for which at least two $L_i(x)$ simultaneously represent E_r numbers with all prime factors in $\mathcal{P}$.

Our admissibility constraint is as in [13]. Specifically we require that for every prime p there exists $x_p \in \mathbb{Z}$ such that

$$p \nmid \prod_{i=1}^{k}(a_i x_p + b_i). \tag{2.5}$$

Equivalently, $\{L_i(x)\}$ is admissible if there is no x such that the $L_i(x)$ represent all congruence classes modulo p for any prime p.

As we are considering sets of primes $\mathcal{P}$ which may fail to be well-distributed modulo M, we must introduce a further constraint and restrict attention to k-tuples for which the dependence modulo M can be controlled. We will say that a k-tuple is M-admissible if each a_j is "exactly" divisible by M:

Definition: An admissible k-tuple $\mathcal{L} = \{L_1, \dots, L_k\}$ is *M-admissible* if for each i, M divides a_i and is coprime to a_i/M.

We will be primarily interested in the case $a_1 = \cdots = a_k = M$.

In fact, as we will argue, we may assume without loss of generality that an M-admissible k-tuple $\mathcal{L}$ may be replaced by one satisfying a stronger condition which we label *Hypothesis* $A(M)$. This condition is a combination of M-admissibility and the condition Hypothesis A occurring in [13].

Hypothesis $A(M)$: *$\mathcal{L} = \{L_1, \dots, L_k\}$ is an M-admissible k-tuple of linear forms. The functions $L_i(n) = a_i n + b_i$ $(1 \le i \le k)$ have integer coefficients with $a_i > 0$. Each of the coefficients a_i is composed of the same primes, none of which divides any of the b_i. If $i \ne j$, then any prime factor of $a_i b_j - a_j b_i$ divides each of the a_i.*

We may justify the introduction of this hypothesis using the renormalization argument in [13], incorporating a variation suggested by S. Graham. We sketch the proof here, highlighting the variation.

We define a quantity A_0 by the expression

$$A_0 := A_0(\mathcal{L}) = \prod_{i=1}^{k} a_i \prod_{1 \le i < j \le k} |a_i b_j - a_j b_i| \tag{2.6}$$

and choose a number A which is divisible by the same prime factors as A_0, is divisible by M, and such that M and A/M are coprime. For each prime $p|A/M$, there is an integer n_p such that $p \nmid P_{\mathcal{L}}(n_p)$, where $P_{\mathcal{L}}(n_p)$ is defined in (2.8). We use the Chinese Remainder Theorem to choose an integer B such that $B \equiv n_p \pmod{p}$ for all $p|A/M$, and write

$$L_i'(n) := L_i((A/M)n + B) = a_i' n + b_i', \tag{2.7}$$

where $a_i' = a_i A/M$ and $b_i' = a_i B + b_i$. We then relabel each $L_i'(n)$ as $L_i(n)$; $\mathcal{L}$ will be M-admissible by our selection of A, and will satisfy Hypothesis $A(M)$.

We also define related quantities

$$P_{\mathcal{L}}(n) := \prod_{i=1}^{k} L_i(n) = (a_1 n + b_1) \cdots (a_k n + b_k), \tag{2.8}$$

$$\Omega_d(\mathcal{L}) := \{n : 1 \le n \le d;\ P_{\mathcal{L}}(n) \equiv 0 \pmod{d}\}, \tag{2.9}$$

$$\nu_d(\mathcal{L}) := \#\Omega_d(\mathcal{L}), \tag{2.10}$$

$$A := \mathrm{lcm}_i(a_i). \tag{2.11}$$

By the Chinese Remainder Theorem, ν_d is multiplicative, and moreover, by our normalization we have for any prime p

$$\nu_p(\mathcal{L}) := \begin{cases} k & \text{if } p \nmid A, \\ 0 & \text{if } p \mid A. \end{cases} \tag{2.12}$$

We also associate to $\mathcal{L}$ the *singular series*

$$\mathfrak{S}(\mathcal{L}) := \prod_{p|A} \left(1 - \frac{1}{p}\right)^{-k} \prod_{p \nmid A} \left(1 - \frac{k}{p}\right) \left(1 - \frac{1}{p}\right)^{-k} \tag{2.13}$$

which will be positive when $\mathcal{L}$ is admissible. In particular, all primes $\le k$ will divide A.

Densities of linear forms: Assume that a set of primes $\mathcal{P}$ satisfying the Siegel-Walfisz or Bombieri-Vinogradov condition for an integer M is given. Also assume that $r \ge 2$ is fixed, and that an M-admissible k-tuple $\mathcal{L} = \{L_1(n), \dots, L_k(n)\}$ is given. By Lemma 3.2, the E_r numbers formed from $\mathcal{P}$ have a density (in the set of all E_r numbers) when restricted to arithmetic progressions modulo M. This motivates the following definition:

Definition: Assume the notation and hypotheses above. We define the *density* δ_j of a linear form $L_j(n) = a_j n + b_j$ to be the density of E_r numbers with prime factors in $\mathcal{P}$ that are congruent to b_j modulo M, as a proportion of all E_r numbers. We also define the *minimum density* δ of $\mathcal{L}$ to be the minimum of the densities of the L_j.

These densities occur naturally in the statements of our results. In particular, each of our main theorems contains the expression $\delta\varphi(M)$, which gives the density of "good" E_r numbers as a proportion of those represented by forms in $\mathcal{L}$.

Construction of k-tuples of linear forms: To prove the existence of bounded gaps we need to

construct M-admissible k-tuples of linear forms $Mn+b_i$ and bound $|b_j-b_i|$ from above in terms of k. The density of each linear form will in general depend on the residue class of b_i modulo M, so that we might need to restrict the b_i to lie in certain residue classes modulo M.

Here is a simple recipe which can be readily applied to examples: For given k and m, let $b_1, b_2, \dots, b_k$ denote the k smallest primes larger than k, with restrictions on the residue class(es) of the b_i as needed. Then $\{Mx+b_i\}$ forms an M-admissible k-tuple, which we then may normalize to satisfy Hypothesis $A(M)$. The constant $C(r,\nu,\mathcal{P})$ of Theorem 0 is then given by b_k-b_1.

It is therefore easy to determine $C(r,\nu,\mathcal{P})$ in particular examples, as we do in Section 6. To compute a general value for $C(r,\nu,\mathcal{P})$ we could use quantitative versions of Linnik's theorem (see Chapter 18 of [14]), but we do not do this here.

2.3. **Precise statement of results.** We are now prepared to give precise statements of our results. Our results are separated into three cases, depending on whether $r=2$ or $r>2$, and if $r>2$, which condition is assumed on $\mathcal{P}$.

Our first result is for E_2 numbers, and is the natural generalization of Theorem 1 of [13]:

Theorem 2.1. *Let $\mathcal{P}$ be an infinite set of primes satisfying Hypothesis $BV(\vartheta,M)$ with $\vartheta \le 1/2$, and let $L_i(x)$ $(1\le i\le k)$ be an M-admissible k-tuple of linear forms with minimum density δ. There are at least $\nu+1$ forms among them which infinitely often simultaneously represent E_2 numbers with prime factors in $\mathcal{P}$, provided that*

$$k > \frac{4e^{-\gamma}(1+o(1))}{B} e^{B\nu/4\delta\varphi(M)}. \tag{2.14}$$

Here $B := 2/\vartheta$, as in [13].

Remark. The constant implied by $o(1)$ may be made explicit. Based on a careful analysis of Section 8 of [13], we may replace $o(1)$ by

$$\frac{1}{3}\left(\frac{5}{k}+\frac{1}{\sqrt{k}}\right).$$

In the case of E_r numbers for $r\ge 3$, we will prove the following bound subject to Hypothesis $BV(\vartheta,M)$:

Theorem 2.2. *Let $\mathcal{P}$ be an infinite set of primes satisfying Hypothesis $BV(\vartheta,M)$ with $\vartheta \le 1/2$, and let $L_i(x)$ $(1\le i\le k)$ be an M-admissible k-tuple of linear forms with minimum density δ. For any $r\ge 3$, there are at least $\nu+1$ forms among them which infinitely often simultaneously represent E_r numbers with prime factors in $\mathcal{P}$, provided that*

$$k > 3\exp\big(\big[\frac{29B\nu(r-1)!}{\delta\varphi(M)}\big]^{\frac{1}{r-1}}\big)+2, \tag{2.15}$$

where

$$B := \max\left(\frac{2}{\vartheta}, r\right). \tag{2.16}$$

For $\mathcal{P}$ satisfying the Siegel-Walfisz condition, we will prove the following bound:

Theorem 2.3. *Let $\mathcal{P}$ be an infinite set of primes satisfying a Siegel-Walfisz condition for an integer M, and let $L_i(x)$ $(1\le i\le k)$ be an M-admissible k-tuple of linear forms with minimum density δ. For any $r\ge 3$, there are at least $\nu+1$ forms among them which infinitely often simultaneously represent E_r numbers with prime factors in $\mathcal{P}$, provided that*

$$k > 3\exp\big(\big[\frac{29\nu(r+4)(r-2)!}{\delta\varphi(M)}\big]^{\frac{1}{r-2}}\big)+2. \tag{2.17}$$

Remark. We obtain similar results for somewhat more general situations. In particular, using an appropriate generalization of Lemma 3.2, we obtain the same result for E_r numbers $p_1 p_2 \cdots p_r$, with $p_i \in \mathcal{P}_i$ for each i. As will be clear from the proof, we may also combine disjoint sets of E_r numbers and add the appropriate densities.

2.4. **Setup for the proof.** We will prove our results closely following the approach of Goldston, Graham, Pintz, and Yıldırım [13] by establishing the positivity of a sum

$$S := \sum_{N<n\leq 2N} \left(\sum_{i=1}^{k} \beta_{r,\mathcal{P}}(L_i(n)) - \nu \right) \left(\sum_{d | P_{\mathcal{L}}(n)} \lambda_d \right)^2, \tag{2.18}$$

where the $L_i(n)$ are our linear forms, $P_{\mathcal{L}}(n)$ is as in (2.8), the λ_d real numbers are to be described momentarily, and $\beta_{r,\mathcal{P}}$ is a characteristic function which selects the almost-primes of interest. Let $E_{r,\mathcal{P}}$ denote the set of square-free E_r numbers whose prime factors are restricted to $\mathcal{P}$, and let $E_{r,\mathcal{P}(N)}$ denote the set of $E_{r,\mathcal{P}}$ numbers whose prime factors are each larger than $\exp(\sqrt{\log N})$. We define

$$\beta_{r,\mathcal{P}}(n) := \begin{cases} 1 & \text{if } n \in E_{r,\mathcal{P}(N)} \\ 0 & \text{otherwise.} \end{cases} \tag{2.19}$$

Later, we will make additional restrictions to the support of $\beta_{r,\mathcal{P}}$ as needed in our analysis. If S is asymptotically positive for large N, it will follow that infinitely often $\nu + 1$ of the $L_i(n)$ represent $E_{r,P}$ numbers.

Our choice of the sieve coefficients λ_d will be identical to that in [13]. We refer to [13] for an overview and discussion; we will simply recall the relevant notation and definitions here. We remark that all the arithmetic functions that we will define will only be supported on integers coprime to A.

For square-free d with $(d, A) = 1$, we define a multiplicative function $f(d)$ by

$$f(d) := \frac{d}{\nu_d(\mathcal{L})} = \frac{d}{\tau_k(d)} \tag{2.20}$$

where

$$\tau_k(d) := \prod_{p|d} k. \tag{2.21}$$

We further define the function $f_1 := f * \mu$. In other words,

$$f_1(d) := \prod_{p|d} \frac{p-k}{k}. \tag{2.22}$$

To define the Selberg sieve coefficients, we let P be a polynomial with positive coefficients to be determined later (for the proofs of Theorems 2.2 and 2.3 we will take $P(x) = 1$), and we will define a polynomial $\tilde{P}$ by

$$\tilde{P}(x) := \int_0^x P(t)dt. \tag{2.23}$$

We will fix a level of support $R = N^{1/B}$ for our sieve coefficients, for a parameter B that will satisfy $B > 4$, $B \geq r$, and if Hypothesis $BV(\vartheta, M)$ is assumed, $B > 2/\vartheta$. Eventually, we will obtain the bounds in Theorems 2.1 and 2.2 for each such B, and therefore for $B = \max(4, r, 2/\vartheta)$ as these theorems claim.

We define a quantity y_s by

$$y_s := \begin{cases} \mu^2(s)\mathfrak{S}(\mathcal{L})P\Big(\frac{\log R/s}{\log R}\Big) & \text{if } s < R \text{ and } (s,A)=1, \\ 0 & \text{otherwise.} \end{cases} \tag{2.24}$$

Then, for square-free d with $(d,A)=1$ we define our coefficients λ_d by

$$\lambda_d := \mu(d)f(d)\sum_s \frac{y_{sd}}{f_1(sd)}. \tag{2.25}$$

The sum is over all s for which $y_{sd} \neq 0$. With this definition we have the usual (see, e.g., [6]) Selberg diagonalization relation

$$\sum_{d,e} \frac{\lambda_d\lambda_e}{f([d,e])} = \sum_s \frac{y_s^2}{f_1(s)} \tag{2.26}$$

which will allow us to evaluate S. We remark that with the choice $P(x)=1$, the quantity y_s is constant for all s for which it is defined, so that the λ_d are essentially the same as in the usual Selberg sieve. In various numerical experiments, different choices of $P(x)$ have yielded mild improvements on our results.

Finally, we introduce functions

$$f^*(d) := \frac{\phi(d)}{\tau_{k-1}(d)}, \tag{2.27}$$

$$f_1^*(d) := \mu * f^*(d) = \prod_{p|d} \frac{p-k}{k-1}, \tag{2.28}$$

$$y_s^* := \frac{\mu^2(s)s}{\phi(s)} \sum_m \frac{y_{ms}}{\phi(m)}. \tag{2.29}$$

Our proof proceeds from an analysis of the quantity S defined in (2.18). We decompose S as

$$\sum_{j=1}^k S_{1,j} - \nu S_0,$$

where

$$S_{1,j} := \sum_{N<n\le 2N} \beta_{r,\mathcal{P}}(L_j(n)) \left(\sum_{d|P_{\mathcal{L}}(n)} \lambda_d\right)^2, \tag{2.30}$$

and

$$S_0 := \sum_{N<n\le 2N} \left(\sum_{d|P_{\mathcal{L}}(n)} \lambda_d\right)^2. \tag{2.31}$$

The sum S_0 is evaluated in [13]. Choosing a level of support $R < N^{1/2-\epsilon}$ for the λ_d (for any ϵ), Theorem 7 of [13] gives the estimate

$$S_0 = (1+o_N(1))\frac{\mathfrak{S}(L)N\log^k R}{(k-1)!}\int_0^1 P(1-x)^2x^{k-1}dx.$$

The sum $S_{1,j}$ is similar to the one evaluated in Theorem 8 of [13], but is somewhat more complicated, and we will prove a lower bound for it. Before stating this bound we recall our assumptions: $r \ge 2$

is an integer, $\mathcal{L} = \{L_i(n)\}$ is an M-admissable k-tuple of linear forms satisfying Hypothesis $A(M)$, $\mathcal{P}$ is a set of primes of positive density satisfying either Hypothesis $BV(\vartheta, M)$ or (for $r \geq 3$ only) the Siegel-Walfisz condition for M, and B is a real number satisfying $B > 4$, $B \geq r$, and if Hypothesis $BV(\vartheta, M)$ is assumed, $B > 2/\vartheta$.

Proposition 2.4. *With these assumptions, $S_{1,j}$ satisfies the lower bound*

$$S_{1,j} \geq (\delta_j \varphi(M) - o_N(1)) \frac{N\mathfrak{S}(L)\log^k R}{B(k-2)!} \int_{y=0}^{1} \tilde{P}(1-y)^2 y^{k-2} dy \int_{u_1} \dots \int_{u_{r-1}} \frac{1}{\prod_i u_i} du_{r-1} \dots du_1.$$

The bounds of integration on the u_i are

$$1 - y < u_1 < u_2 < \dots < u_{r-1}; \tag{2.32}$$

$$u_1 + u_2 + \dots + u_{r-2} + 2u_{r-1} < B. \tag{2.33}$$

In the case that Hypothesis $BV(\vartheta, M)$ is not assumed, we have the additional bound

$$u_{r-1} > 1.$$

Remark. Theorems 2.2 and 2.3 are established by proving a general lower bound on the integral occurring in Proposition 2.4. For small r it is possible to numerically evaluate this integral and improve our results. For example, suppose that $\mathcal{P}$ is any subset of the primes of (relative) density 1, and let q_n denote the nth E_3 number with all prime factors in $\mathcal{P}$. Then our (numerical) calculations allow $k = 3$, so that $\liminf_{n\to\infty}(q_{n+1} - q_n) \leq 6$.

We will establish Proposition 2.4 in Section 4, and then give the proofs of Theorems 2.2 and 2.3 in Section 5. The proof of Theorem 2.1 depends on the analysis given in [13], as we describe at the end of Section 5.

3. Well-distribution of Primes and Almost Primes

Before beginning the proof of Proposition 2.4, we establish a couple of preliminary results concerning well-distribution of primes and almost primes. We recall (as stated in the introduction) that a set of primes $\mathcal{P}$ has *Frobenius density* if there is a Galois extension $K/\mathbb{Q}$ with the property that those primes $p \in \mathcal{P}$, up to finitely many exceptions, are distinguished as those primes for which the $\mathrm{Frob}(p)$ constitute a fixed conjugacy class or a union of conjugacy classes in $\mathrm{Gal}(K/\mathbb{Q})$.

We remark that the case where $\mathcal{P}$ is a union of arithmetic progressions modulo M is a special case of this, with $K = \mathbb{Q}(\zeta_M)$.

Lemma 3.1. *If $\mathcal{P}$ has Frobenius density, then $\mathcal{P}$ satisfies Hypothesis $BV(\vartheta, M)$ for some ϑ and M.*

In fact, we may take M to be the smallest integer such that $K \cap \mathbb{Q}(\zeta_M)$ is maximal, and

$$\vartheta = \min\left(\frac{2}{[K:\mathbb{Q}]}, \frac{1}{2}\right). \tag{3.1}$$

Moreover, see (3.4) for a value of ϑ which may be greater depending on the structure of $\mathrm{Gal}(K(\zeta_M)/\mathbb{Q})$.

Proof. By the classical Chebotarev Density Theorem, $\mathcal{P}$ will be well-distributed modulo q for any q for which $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$. Choosing M as above, $\mathcal{P}$ will then be well-distributed in residue classes coprime to M.

The Bombieri-Vinogradov condition (2.2) follows from work of Murty and Murty [19]. Murty and Murty prove that (2.2) holds with $\mathcal{P}$ in place of $\mathcal{P}_m$, for any $\mathcal{P}$ that has Frobenius density. The level of distribution ϑ depends on the choice of conjugacy class(es), but satisfies the lower bound (3.1).

Therefore, we must prove that each $\mathcal{P}_m$ has Frobenius density. To see this, let C denote the conjugacy class(es) defining $\mathcal{P}$ in $\mathrm{Gal}(K/\mathbb{Q})$, and let $\left[\frac{\mathbb{Q}(\zeta_M)/\mathbb{Q}}{m}\right] \in \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ denote the Artin symbol of any prime $\equiv m \pmod q$, which will not depend on the prime chosen. There is an injection

$$\iota : \mathrm{Gal}(K(\zeta_M)/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q}) \tag{3.2}$$

which satisfies the relation

$$\iota\left(\left[\frac{K(\zeta_M)/\mathbb{Q}}{p}\right]\right) = \left(\left[\frac{K/\mathbb{Q}}{p}\right], \left[\frac{\mathbb{Q}(\zeta_M)/\mathbb{Q}}{p}\right]\right). \tag{3.3}$$

Letting C' denote the (possibly empty) conjugacy class of $\mathrm{Gal}(K(\zeta_M)/\mathbb{Q})$ defined by $C' = \iota^{-1}\big(C \times \left[\frac{\mathbb{Q}(\zeta_M)/\mathbb{Q}}{m}\right]\big)$ we see that a prime p will satisfy $\left[\frac{K/\mathbb{Q}}{p}\right] \in C$ and $p \equiv m \pmod q$ exactly when $\left[\frac{K(\zeta_M)/\mathbb{Q}}{p}\right] \in C'$. Therefore $\mathcal{P}_m$ has Frobenius density as desired.

When C' is empty, the conclusion (2.2) is vacuous. When C' is nonempty, the bound (3.1) follows from the criterion given in Section 7.2 of [19]. We have more precisely

$$\vartheta = \frac{1}{\max(2, i-2)}, \tag{3.4}$$

where i is the index in $\mathrm{Gal}(K(\zeta_M)/\mathbb{Q})$ of the largest abelian subgroup H whose intersection with C' is nontrivial. As $\mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ is abelian, we check that $i \le \frac{1}{2}[K : \mathbb{Q}]$ (if $K \neq \mathbb{Q}$), and so (3.1) follows for any nonempty C'. □

Our next result is a version of Hypothesis $BV(\vartheta, M)$ for almost-primes in $[N, 2N]$ formed from $\mathcal{P}$. The result follows readily from work of Bombieri, Friedlander, and Iwaniec ([3], Theorem 0; see also [2]), and gives a level of distribution $\vartheta = 1/2$ with only the assumption that $\mathcal{P}$ satisfies a Siegel-Walfisz condition.

Lemma 3.2. *Suppose that $\mathcal{P}$ satisfies the Siegel-Walfisz condition (2.3) for an integer M. For any $r \ge 2$, any N, any $x \ge \exp((\log N)^{1/4})$, and any residue class m modulo M, let $\mathcal{P}(x)$ denote the subset of $\mathcal{P}$ consisting of primes $\ge x$, and let $\beta_{r,\mathcal{P}_m(x)}$ denote the characteristic function of the E_r numbers congruent to m modulo M, with prime factors in $\mathcal{P}(x)$. Then $\beta_{r,\mathcal{P}_m(x)}$ has level of distribution 1/2 in the following sense:*

With the notation

$$\Delta_{r,\mathcal{P}_m(x)}(N; q, a) := \sum_{\substack{N < n \le 2N \\ n \equiv a \pmod q}} \beta_{r,\mathcal{P}_m(x)}(n) - \frac{1}{\varphi(q)} \sum_{N < n \le 2N} \beta_{r,\mathcal{P}_m(x)}(n), \tag{3.5}$$

we have for any A and some $B = B(A) > 0$ the inequality

$$\sum_{\substack{q \le N^{1/2}\log^{-B} N \\ (q,M)=1}} \max_{a} {}^{(a,q)=1} |\Delta_{r,\mathcal{P}_m(x)}(N; q, a)| \ll_A N \log^{-A} N, \tag{3.6}$$

uniformly in x.

Proof. This is a variant of a result of Motohashi [20]. We will appeal to the aforementioned Bombieri-Friedlander-Iwaniec result, following the exposition in ([2], Theorem 22). We will prove our result for integers of the form $n = p_1 \dots p_r$, where for each i, $p_i \equiv m_i \pmod M$ for fixed residue classes m_i modulo M, and $p_i \ge x$. The result then follows by summing over all possibilities for the m_i.

For simplicity, let α_r denote the characteristic function of such integers, suppressing the dependence on N and the m_i. Similarly, let α_{r-1} denote the characteristic function of E_{r-1} numbers $n = p_1 \dots p_{r-1}$ with the same restrictions.

To apply the Bombieri-Friedlander-Iwaniec result, we will approximate α_r by a sum h of convolutions $f * g$, where f and g will be supported in $[X, 2X]$ and $[Y, 2Y]$ respectively, for some X, Y with $XY = N$ and $X, Y \geq x$, and g will satisfy a Siegel-Walfisz condition. Estimate (3.6) will then follow for h, which we will show is sufficiently close to α_r to establish (3.6) for α_r as well.

Fixing $\epsilon > 0$, we split the interval $[x, 2N/x]$ into $\ll \frac{\log N}{\epsilon}$ intervals of the type $[t, (1+\epsilon)t)$. For a given t, let f denote the restriction of α_{r-1} to $[t, (1+\epsilon)t)$, and let g denote the restriction of $\beta_{1,\mathcal{P}_{m_i}}$ to $[N/t, \frac{2N}{(1+\epsilon)t})]$. We then let h denote the sum over all t of $f*g$. The Siegel-Walfisz condition applies to $\beta_{1,\mathcal{P}_{m_i}}$ and therefore to its restriction g, and so by Bombieri-Friedlander-Iwaniec, (3.6) holds for each $f * g$. Summing over t, we obtain (3.6) for h with a total error

$$\ll (1/\epsilon) N \log^{-A+1} N. \tag{3.7}$$

Let c equal the number of m_i $(i \leq r)$ for which $m_i = m_r$, so that c counts the number of times that an integer n counted by α_r will be counted by some $f * g$. We claim that $(1/c)h$ closely approximates the restriction of α_r to $[N, 2N]$. Both functions are supported in $[N, 2N]$ and identical on $[N(1+\epsilon), 2N(\frac{1}{1+\epsilon})]$. The difference on the intervals $[N, N(1+\epsilon))$ and $(2N(\frac{1}{1+\epsilon}), 2N]$ contributes $\ll \frac{\epsilon N}{\varphi(q)}$ to each $\Delta_{r,\mathcal{P}_m(x)}(N; q, a)$; summing over q (and over the m_i) the total contribution to the error in (3.6) is

$$\ll \epsilon N \sum_{q \leq N^{1/2} \log^{-B} N} \frac{1}{\varphi(q)} \ll \epsilon N \log N. \tag{3.8}$$

Choosing $\epsilon \sim \log^{-A/2} N$ (depending also on x, so that $\log(2N/x^2)/\log(1+\epsilon)$ is an integer), the errors in (3.7) and (3.8) are both $\ll N \log^{-(A/2)+1} N$ for any A, and this completes the proof.

We remark that the result in [2] is stated for $M = 1$ and an ordinary Siegel-Walfisz condition. However, an examination of the proof in [2] reveals that this result remains valid as long as we introduce the restriction $(q, M) = 1$ in the sum in (3.6). □

4. Proof of Proposition 2.4

The proof of Proposition 2.4 will consist of a careful analysis of the quantity $S_{1,j}$. We recall that $S_{1,j}$ is defined by the formula

$$S_{1,j} = \sum_{N < n \leq 2N} \beta_{r,\mathcal{P}}(L_j(n)) \left(\sum_{d | P_{\mathcal{L}}(n)} \lambda_d \right)^2.$$

Switching the order of summation, we have

$$S_{1,j} = \sum_{d,e} \lambda_d \lambda_e \sum_{\substack{N < n \leq 2N \\ [d,e] | P_{\mathcal{L}}(n)}} \beta_{r,\mathcal{P}}(L_j(n)). \tag{4.1}$$

We now decompose the inner sum over E_r numbers according to how many prime factors of $L_j(n)$ divide $[d, e]$. Write

$$S_{1,j} = T_r + T_{r-1} + \cdots + T_0, \tag{4.2}$$

where T_h is the sum over those E_r's with h factors not dividing $[d, e]$.

To get a handle on these sums, we introduce a restriction on the support of $\beta_{r,\mathcal{P}}$. If $\mathcal{P}$ is known to have a level of distribution ϑ, we restrict to those E_r numbers whose largest prime factor is larger than the level of support R. If only the Siegel-Walfisz condition is known for $\mathcal{P}$, we restrict further to those E_r numbers whose largest two prime factors are larger than R.

With this restriction, the quantities T_0 and possibly T_1 will be absent from (4.2). We have the formula

$$T_h = \sum_{d,e} \lambda_d \lambda_e \sum_{\substack{p_1<\cdots<p_{r-h} \\ p_i|[d,e]}}{}' \sum_{\substack{N<n\le 2N \\ (\prod p_i)|L_j(n);\ \frac{[d,e]}{\prod p_i}|\frac{P_{\mathcal{L}}(n)}{L_j(n)}}} \beta_{r,\mathcal{P}}(L_j(n)). \tag{4.3}$$

The dash on the second sum indicates that all primes must be in $\mathcal{P}$. In the case $h = r$, the second sum is omitted with $\prod p_i$ understood to be 1.

As products over primes will occur frequently in our analysis we introduce the notation $q := \prod_i p_i$, where the range of i should be clear from the context.

The condition $\frac{[d,e]}{q}|\frac{P_{\mathcal{L}}(n)}{L_j(n)}$ depends only on the residue class of n modulo $[d,e]/q$. For any square-free x coprime to A, let $\Omega^*(x)$ denote the set of residue classes modulo x for which $x|\frac{P_{\mathcal{L}}(n)}{L_j(n)}$, and write $\nu^*(x) := |\Omega^*(x)|$. We claim that

$$\nu^*(x) = \tau_{k-1}(x). \tag{4.4}$$

To see this, we first observe that by the Chinese Remainder Theorem, ν^* is multiplicative. If x is prime, then we will have $x|P_{\mathcal{L}}(n)/L_j(n)$ whenever $x|P_i(n)$ for any $i \neq j$. By Hypothesis $A(M)$, this happens for one residue class modulo x for each i, and moreover, these residue classes are all distinct. Accordingly, for x prime we have $\nu^*(x) = k-1$, and (4.4) follows.

We rewrite (4.3) as

$$T_h = \sum_{d,e} \lambda_d \lambda_e \sum_{\substack{p_1<\cdots<p_{r-h} \\ p_i|[d,e]}}{}' \sum_{a\in\Omega^*([d,e]/q)} \sum_{\substack{N<n\le 2N \\ q|L_j(n);\ n\equiv a \pmod{[d,e]/q}}} \beta_{r,\mathcal{P}}(L_j(n)). \tag{4.5}$$

Write $n' = L_j(n) = a_j n + b_j$, so that $a_j N + b_j < n' \le 2a_j N + b_j$, with congruence conditions on n' modulo $[d,e]/q$ and a_j. By our choice of sieve coefficients, $[d,e]/q$ and a_j will be coprime. Moreover, we may write $a_j = M \cdot (a_j/M)$, where M and a_j/M are coprime by Hypothesis $A(M)$. We thus obtain independent congruence conditions modulo $[d,e]/q$, M, and a_j/M. We introduce the notation

$$u := \frac{[d,e]a_j}{qM}, \tag{4.6}$$

and we use the Chinese Remainder Theorem to combine the congruence conditions modulo $[d,e]/q$ and a_j/M into a single condition modulo u. We thus sum over the n' such that $n' \equiv b_j \pmod M$, and such that n' satisfies one of the congruences modulo u determined by $\Omega^*([d,e]/q)$. We will denote the appropriate moduli by $\Omega_1^*([d,e]/q)$, and we observe that $|\Omega_1^*([d,e]/q)| = |\Omega^*([d,e]/q)|$. Accordingly, we rewrite the above sum as

$$T_h = \sum_{d,e} \lambda_d \lambda_e \sum_{\substack{p_1<\cdots<p_{r-h} \\ p_i|[d,e]}}{}' \sum_{a\in\Omega_1^*([d,e]/q)} \sum_{\substack{a_jN+b_j<n'\le 2a_jN+b_j \\ q|n';\ n'\equiv a \pmod u \\ n'\equiv b_j \pmod M}} \beta_{r,\mathcal{P}}(n'). \tag{4.7}$$

As q is coprime to both u and M, we write $\bar{q}_u$ and $\bar{q}_M$ for the multiplicative inverses of q modulo u and M respectively. Writing t for n'/q, we rewrite the above as

$$T_h = \sum_{d,e} \lambda_d \lambda_e \sum_{\substack{p_1<\cdots<p_{r-h} \\ p_i|[d,e]}}{}' \sum_{a\in\Omega_1^*([d,e]/q)} \sum_{\substack{(a_jN+b_j)/q<t\le(2a_jN+b_j)/q \\ t\equiv a\bar{q}_u \pmod u \\ t\equiv b_j\bar{q}_M \pmod M}} \beta_{h,\mathcal{P}}(t). \tag{4.8}$$

This sum is now in a form for which our Bombieri-Vinogradov conditions can be applied. We recall that we have restricted to almost primes whose prime factors are all greater than $\exp(\sqrt{\log N})$, so that we may use Lemma 3.2 and (when it applies) Hypothesis $BV(\vartheta, M)$. We write

$$\sum_{\substack{(a_jN+b_j)/q<t\leq(2a_jN+b_j)/q\\ t\equiv a\bar{q}_u \pmod u\\ t\equiv b_j\bar{q}_M \pmod M}} \beta_{h,\mathcal{P}}(t) = \frac{1}{\varphi(u)} \sum_{\substack{a_jN/q<t\leq 2a_jN/q\\ t\equiv b_j\bar{q}_M \pmod M}} \beta_{h,\mathcal{P}}(t) + \Delta_h\left(\frac{a_jN}{q}; u, a\bar{q}_u\right) + O_{b_j}(1). \tag{4.9}$$

We denote as usual

$$\Delta_h(X, u) = \max_a \Delta_h(X; u, a) \tag{4.10}$$

and write

$$T_h = M_h + E_h,$$

where the main term M_h is given by

$$M_h = \sum_{d,e} \lambda_d\lambda_e \sideset{}{'}\sum_{p_1,\dots,p_{r-h}|[d,e]} \frac{\tau_{k-1}([d,e]/q)}{\varphi(u)} \sum_{\substack{a_jN/q<t\leq 2a_jN/q\\ t\equiv b_j\bar{q}_M \pmod M}} \beta_{h,\mathcal{P}}(t), \tag{4.11}$$

and the error E_h satisfies

$$|E_h| \leq \sum_{d,e} \lambda_d\lambda_e \sideset{}{'}\sum_{p_1,\dots,p_{r-h}|[d,e]} \tau_{k-1}([d,e]/q)(\Delta_h(a_jN/q, u) + O(1)). \tag{4.12}$$

We start off by showing that the error is within acceptable limits. In particular, we prove the following lemma:

Lemma 4.1. *If E_h is defined as in (4.12), we have for any U*

$$E_h \ll_U N\log^{-U} N.$$

The implied constant is allowed to depend on all parameters other than N. It follows from this lemma that the error from each of the E_h may be absorbed into the $N\cdot o_N(1)$ term of Proposition 2.4.

Proof. In (4.3) of [13] it is proved that

$$\lambda_d \ll \log^k R \leq \log^k N.$$

We write $v = [d, e]$, and for any fixed v there are at most $3^{\omega(v)}$ choices of d and e so that $v = [d, e]$. Therefore, we have

$$\begin{aligned}|E_h| &\ll \log^{2k} N \sum_{v<R^2} \sideset{}{'}\sum_{p_1,\dots,p_{r-h}|v} 3^{\omega(v)}\tau_{k-1}\left(\frac{v}{q}\right)\left(\Delta_h\left(\frac{a_jN}{q}, \frac{a_jv}{qM}\right) + O(1)\right)\\ &\leq \log^{2k} N \sideset{}{'}\sum_{p_1<\dots<p_{r-h}<R} \sum_{\substack{v<R^2\\ p_1\cdots p_{r-h}|v}} (3k-3)^{\omega(v)}\left(\Delta_h\left(\frac{a_jN}{q}, \frac{a_jv}{qM}\right) + O(1)\right).\end{aligned}$$

Again writing $u = a_j[d, e]/qM$, we thus obtain

$$|E_h| \ll \log^{2k} N \sideset{}{'}\sum_{p_1<\dots<p_{r-h}<R} \sum_{u<a_jR^2/qM} (3k-3)^{\omega(u)}\left(\Delta_h\left(\frac{a_jN}{q}, u\right) + O(1)\right).$$

(Here we have allowed our implied constant to depend on k and r, so that $(3k-3)^{\omega(v)-\omega(u)} \ll 1$.)

We now use Lemma 3.2 as well as (when appropriate) Hypothesis $BV(\vartheta, M)$ to estimate the inner sum. To justify the use of Lemma 3.2 we observe first that for large N, $(a_j R^2/qM) < (a_j N/q)^{2/(B+B_0)}$, where $B_0 < B$ is our lower bound on B (e.g., $B_0 = 2/\vartheta$ if $BV(\vartheta, M)$ is assumed, and $B_0 = 4$ otherwise). We also recall that we are estimating almost primes with prime factors $> \exp(\sqrt{\log N})$, and Lemma 3.2 allows this uniformly as a cutoff for all choices of q.

Therefore, Lemma 3.2 together with Cauchy's inequality, implies (see, e.g., Lemma 2 of [12]) that for any U we have

$$\sum_{u<a_j R^2/qM} (3k-3)^{\omega(u)} \Delta_h(a_j N/q, u) \ll_U (a_j N/q) \log^{-U}(a_j N/q).$$

Moreover, the contribution of the $O(1)$ term is trivial (see Lemma 1 of [12]). Therefore,

$$E_h \ll \log^{2k} N \sideset{}{'}\sum_{p_1,\dots,p_{r-h}} N/q \log^{-U}(a_j N/q). \tag{4.13}$$

We now make the simple estimates

$$\log(a_j N/q) \geq \log R = \frac{1}{B}\log N \gg \log N$$

and (recalling that q stands for $\prod_{i=1}^{r-h} p_i$),

$$\sideset{}{'}\sum_{p_1,\dots,p_{r-h}} 1/q \leq \Big(\sum_{n=2}^{R} \frac{1}{n}\Big)^{r-h} \leq \log^{r-h} R \leq \log^{r-h} N,$$

so that putting these estimates together gives

$$E_h \ll N(\log N)^{2k+r-h-U}.$$

This completes the proof. □

Having dealt with the error for each h separately, we combine the main terms

$$M_h = \sum_{d,e} \lambda_d \lambda_e \sideset{}{'}\sum_{p_1,\dots,p_{r-h} | [d,e]} \frac{\tau_{k-1}([d,e]/q)}{\varphi(u)} \sum_{\substack{a_j N/q < t \leq 2a_j N/q \\ t \equiv b_j \bar{q}_M \pmod M}} \beta_{h,\mathcal{P}}(t),$$

and we use the fact that

$$\varphi(u) = \varphi(a_j[d,e]/qM) = \frac{\varphi(a_j[d,e]/q)}{\varphi(M)}$$

to write

$$S_{1,j} \sim T := \sum_h M_h = \sum_{d,e} \lambda_d \lambda_e \sideset{}{'}\sum_{p_1 < \cdots < p_{r-1}} \frac{\tau_{k-1}([d,e,q]/q)}{\varphi(a_j[d,e,q]/q)} \varphi(M) \sum_{\substack{a_j N/q < n \leq 2a_j N/q \\ n \equiv b_j \bar{q}_M \pmod M}} \beta_{1,\mathcal{P}}(n). \tag{4.14}$$

The sum over the p_i is over those primes in $\mathcal{P}$ such that $p_1 < \cdots < p_{r-1} < n$, with the restriction $p_1 \geq \exp(\sqrt{\log N})$ as before. We have $n > R$, which will be automatic because $B \geq r$ and therefore $R \leq N^{1/r}$. For convenience, we make the restriction $N/q > p_{r-1}$, excluding E_r numbers whose largest two prime factors are nearly equal. With this restriction, the only condition on n will be the range written in the inner sum of (4.14).

We remark that in case only the Siegel-Walfisz condition is assumed we also have $p_{r-1} > R$, and so in fact p_{r-1} will never divide $[d,e]$. Although this will be reflected in the bounds of integration in Proposition 2.4, there is no need to reflect this explicitly in the notation.

At this point, we need to break up the contribution to $S_{1,j}$ and T by residue classes modulo M. In particular, for $i = 1, \dots, r$, choose residue classes m_i modulo M, and let $\mathfrak{m} = \{m_1, \dots, m_r\}$

denote the set of residue classes chosen. Let $T_{\mathfrak{m}}$ denote the contribution to T of those E_r numbers with $p_i \in \mathcal{P}_{m_i}$ for each i. Proposition 2.4 will then follow by summing over $\mathfrak{m}$.

For fixed $\mathfrak{m}$, we change the order of summation to write

$$T_{\mathfrak{m}} = \frac{\varphi(M)}{\varphi(a_j)} \sideset{}{'}\sum_{p_1<\cdots<p_{r-1}} \left(\sum_{a_jN/q<n\le 2a_jN/q} \beta_{1,\mathcal{P}_{m_r}}(n) \right) \sum_{d,e} \frac{\lambda_d \lambda_e \tau_{k-1}([d,e,q]/q)}{\varphi([d,e,q]/q)}.$$

The sum over d and e is evaluated in Lemma 6 of [13]:

$$\sum_{d,e} \frac{\lambda_d \lambda_e \tau_{k-1}([d,e,q]/q)}{\varphi([d,e,q]/q)} = \sum_{\substack{a \\ (a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)} \left(\sum_{s|q} \mu(s) y_{as}^* \right)^2. \tag{4.15}$$

(Recall that the expressions $f_1^*(a)$ and y_{as}^* were defined in (2.28) and (2.29), respectively.) We have thus written M as a sum of nonnegative terms.

Accordingly, we may now use the density of $\mathcal{P}_{m_r}$ and the Prime Number Theorem to incorporate the estimate

$$\sum_{a_jN/q<n\le 2a_jN/q} \beta_{1,\mathcal{P}_{m_r}}(n) \ge (1-\epsilon)\delta_r \frac{a_jN/q}{\log(a_jN/q)}$$

uniformly in $q < N^{1-1/r}$, for any ϵ, provided N is sufficiently large. Here δ_r is the (possibly zero) density of $\mathcal{P}_{m_r}$. The contribution from ϵ will be absorbed into the $o_N(1)$ term of Proposition 2.4, so we may disregard it and evaluate

$$T' := \delta_r \varphi(M) \frac{a_j}{\phi(a_j)} \sideset{}{'}\sum_{p_1<\cdots<p_{r-1}} \frac{N/q}{\log(a_jN/q)} \sum_{\substack{a \\ (a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)} \left(\sum_{s|q} \mu(s) y_{as}^* \right)^2. \tag{4.16}$$

We make a couple of further simplifications. In the first place, by Hypothesis $A(M)$, a_j and A have the same prime divisors, so that $a_j/\varphi(a_j) = A/\varphi(A)$. Furthermore, we have, for any $\epsilon > 0$,

$$\log(a_jN/q) \le (1+\epsilon)\log(N/q)$$

uniformly in q for sufficiently large N, so that we may replace $\log(a_jN/q)$ by $\log(N/q)$ in (4.16) and again absorb the error into the $o_N(1)$ term in Proposition 2.4.

In conclusion, we have $T' \ge (1-o_N(1))T''$, where the main term T'' is defined by

$$T'' := \delta_r \varphi(M) \frac{A}{\varphi(A)} \sideset{}{'}\sum_{p_1<\cdots<p_{r-1}} \frac{N/q}{\log(N/q)} \sum_{\substack{a \\ (a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)} \left(\sum_{s|q} \mu(s) y_{as}^* \right)^2. \tag{4.17}$$

We will thus prove a general lower bound for T''. It is, of course, possible to derive an asymptotic formula (in terms of a sum of integrals) for any fixed value of r. Unfortunately, the resulting integrals are too unwieldy to effectively evaluate in Section 5. We did, however, numerically evaluate the resulting integrals in several special cases. In particular, we determined that our lower bound for T'' is reasonably sharp. (The bounds in Section 5 are less so.)

We begin by restricting the sum over a to the range $a > R/p_1$. As $y_{as}^* = 0$ whenever $as > R$, we will only get a contribution to the innermost sum for $s = 1$. We have

$$T'' \ge T^{(3)} := \delta_r \varphi(M) \frac{A}{\varphi(A)} \sideset{}{'}\sum_{p_1<\cdots<p_{r-1}} \frac{N/q}{\log(N/q)} \sum_{\substack{a>R/p_1 \\ (a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)} (y_a^*)^2. \tag{4.18}$$

We will use several estimates from [13] to evaluate $T^{(3)}$. The first of these is a combination of Lemma 7 and (7.1) from [13].

Lemma 4.2. *We have the estimate*

$$y_a^* = \frac{\varphi(A)}{A}\mathfrak{S}(\mathcal{L})(\log R)\tilde{P}\Big(\frac{\log R/a}{\log R}\Big) + O(\log\log R). \tag{4.19}$$

The next estimate is a variation of Lemma 8 of [13].

Lemma 4.3. *We have the estimate*

$$\sum_{\substack{a<t\\(a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)} = C(q)\frac{A}{\varphi(A)}\frac{1}{(k-1)!\mathfrak{S}(\mathcal{L})}\log^{k-1} t + O(\log^{k-2} t), \tag{4.20}$$

for a constant $C(q)$ satisfying

$$C(q) = 1 - o_N(1). \tag{4.21}$$

For sufficiently large N, the constant implied by $O(\log^{k-2} t)$ may be chosen uniformly in q.

Proof. In Lemma 8 of [13] it is proved that

$$\sum_{a<t} \frac{\mu^2(a)}{f_1^*(a)} = \frac{A}{\varphi(A)}\frac{1}{(k-1)!\mathfrak{S}(\mathcal{L})}\log^{k-1} t + O(\log^{k-2} t). \tag{4.22}$$

Introducing the condition $(a,q)=1$ on the left is equivalent to replacing A with qA, which has the effect of multiplying the main term by a factor of

$$C(q) := \prod_{p|q}\Big(1 - \frac{k-1}{p-1}\Big).$$

The claim (4.21) follows because all $r-1$ prime factors of q are larger than $\exp(\sqrt{\log N})$.

To justify that the $O(\log^{k-2} t)$ term may be chosen uniformly in q (and N), we observe that the implied constant in (4.22) depends on constants L, A_1, A_2, κ occurring in Lemma 3 of [13]. Checking the definitions of these constants, they may easily be chosen uniformly for sufficiently large N. □

We now begin our evaluation of $T^{(3)}$. By Lemma 4.2, we have

$$(y_a^*)^2 = \bigg(\frac{\varphi(A)}{A}\mathfrak{S}(\mathcal{L})(\log R)\tilde{P}\Big(\frac{\log R/a}{\log R}\Big)\bigg)^2 + O(\log R\log\log R).$$

We thus write

$$T^{(3)} = T^{(4)} + O(E^{(4)}), \tag{4.23}$$

where

$$T^{(4)} := \delta_r\varphi(M)\frac{\varphi(A)}{A}\mathfrak{S}(\mathcal{L})^2\log^2 R \sideset{}{'}\sum_{p_1<\cdots<p_{r-1}} \frac{N/q}{\log(N/q)} \sum_{\substack{a>R/p_1\\(a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)}\tilde{P}^2\Big(\frac{\log R/a}{\log R}\Big) \tag{4.24}$$

and

$$E^{(4)} := \log R\log\log R \sideset{}{'}\sum_{p_1<\cdots<p_{r-1}} \frac{N/q}{\log(N/q)} \sum_{\substack{a>R/p_1\\(a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)}. \tag{4.25}$$

We analyze the error term $E^{(4)}$ first. Recalling that $\log(N/q) \geq \log R$, we use Lemma 4.3 to write

$$E^{(4)} \ll N\log^{k-1} R\log\log R\bigg(\sideset{}{'}\sum_{p_1<\cdots<p_{r-1}} \frac{1}{\prod_i p_i}\bigg).$$

We use Mertens' estimate $\sum_{p\le x} 1/p \ll \log\log x$ to write

$$\sum_{p_1<\dots<p_{r-1}}{}' \frac{1}{\prod_i p_i} \le \left(\sum_{p<N}\frac{1}{p}\right)^{r-1} \ll (\log\log N)^{r-1} \ll (\log\log R)^{r-1} \tag{4.26}$$

so that

$$E^{(4)} \ll N\log^{k-1} R(\log\log R)^r$$

which is negligible compared to the main term of Proposition 2.4.

To tackle $T^{(4)}$, we write the inner sum as a Stieltjes integral

$$\sum_{\substack{a>R/p_1\\(a,q)=1}} \frac{\mu^2(a)}{f_1^*(a)}\tilde{P}^2\left(\frac{\log R/a}{\log R}\right) = \int_{R/p_1}^R \tilde{P}^2\big(\frac{\log R/t}{\log R}\big)d\left(\sum_{\substack{a<t\\(a,q)=1}}\frac{\mu^2(a)}{f_1^*(a)}\right). \tag{4.27}$$

We define an error term $E(t)$ by

$$\sum_{\substack{a<t\\(a,q)=1}}\frac{\mu^2(a)}{f_1^*(a)} = C(q)\frac{A}{\varphi(A)}\frac{1}{(k-1)!\mathfrak{S}(\mathcal{L})}\log^{k-1} t + E(t),$$

where $E(t)\ll \log^{k-2} R$ by Lemma 4.3. The contribution of $E(t)$ to (4.27) is

$$\int_{R/p_1}^R \tilde{P}^2\left(\frac{\log R/t}{\log R}\right)dE(t) = \left[E(t)\tilde{P}^2\left(\frac{\log R/t}{\log R}\right)\right]_{R/p_1}^R - \int_{R/p_1}^R E(t)\frac{d}{dt}\left(\tilde{P}^2\left(\frac{\log R/t}{\log R}\right)\right)dt. \tag{4.28}$$

As $E(t)\ll\log^{k-2} R$, the first term above is $\ll\log^{k-2} R$ as well, and as $\tilde{P}$ is monotone the second is

$$\ll \log^{k-2} R\int_{R/p_1}^R \frac{d}{dt}\left(\tilde{P}^2\left(\frac{\log R/t}{\log R}\right)\right)dt \ll \log^{k-2} R.$$

Therefore, the expression in (4.27) is

$$(1-o_N(1))\frac{A}{\varphi(A)}\frac{1}{(k-1)!\mathfrak{S}(\mathcal{L})}\int_{R/p_1}^R \tilde{P}^2\left(\frac{\log R/t}{\log R}\right)d(\log^{k-1} t) + O(\log^{k-2} R).$$

Thus,

$$T^{(4)} \ge (\delta_r\varphi(M)-o_N(1))\frac{\mathfrak{S}(\mathcal{L})\log^2 R}{(k-1)!}\sum_{p_1<\dots<p_{r-1}}{}'\frac{N/q}{\log(N/q)}\left(\int_{R/p_1}^R \tilde{P}^2\left(\frac{\log R/x}{\log R}\right)d(\log^{k-1} x)+O(\log^{k-2} R)\right). \tag{4.29}$$

The O-term will contribute

$$\ll \log^k R\sum_{p_1<\dots<p_{r-1}}{}'\frac{N/q}{\log(N/q)}$$

which, by the same argument given in (4.26), is $O(N\log^{k-1} R(\log\log R)^{r-1})$ and therefore negligible.

We will introduce the notation

$$I(t) := \int_{R/t}^R \tilde{P}^2\left(\frac{\log R/x}{\log R}\right)d(\log^{k-1} x), \tag{4.30}$$

and rewrite the main term of $T^{(4)}$ (without the constants) as

$$I_1 := \int_{t_1}\dots\int_{t_{r-1}}\frac{N/q}{\log(N/q)}I(t_1)d(\pi_1'(t_{r-1}))\dots d(\pi_{r-1}'(t_1)), \tag{4.31}$$

where $\pi_i'(x)$ refers to the number of primes in $\mathcal{P}_{m_i}$ less than x, and q now corresponds to the product of the t_i. The bounds of integration in the integrals over t_i correspond to the restrictions made earlier; we have $t_{i+1} > t_i$ for each i and $t_1 t_2 \dots t_{r-2} t_{r-1}^2 < N$. We will continue to suppress these from the notation for the time being.

Using the approximation $\pi_i'(t) \sim \delta_i \frac{t}{\log t}$, where δ_i is the (relative) density of $\mathcal{P}_{m_i}$, we would like to substitute $\delta_i dt_i / \log t_i$ for each $d\pi_i'(t_i)$. The content of the next proposition is that we may make this substitution at only a mild cost.

Proposition 4.4. *Let $\epsilon > 0$ be fixed, and let I_1 be defined as in (4.31). Then we have*

$$I_1 \geq (\delta_1 \dots \delta_{r-1} - \epsilon) I_1', \tag{4.32}$$

where

$$I_1' := \int_{t_1} \dots \int_{t_{r-1}} \frac{N/q}{\log(N/q)} I(t_1) d(\text{li } t_{r-1}) \dots d(\text{li } t_1). \tag{4.33}$$

The bounds of integration on I_1' are the same as those on I_1, with the additional condition that $t_{i+1} > (1+\epsilon)t_i$ for each i with $1 \leq i \leq r-2$.

With Proposition 4.4, we will have proved a lower bound for $S_{1,j}$ in the form of an integral of a smooth function; a change of variables will lead quite directly to the integral given in Proposition 2.4.

We begin the proof of Proposition 4.4 with two lemmas.

Lemma 4.5. *Let g be a positive, nonincreasing, and differentiable function. Then, with the notation above, we have for any A and B*

$$\int_{t=A}^{B} g(t) d\pi_i'(t) \geq (\delta_i - \epsilon) \int_{t=A(1+\epsilon)}^{B} g(t) d(\text{li } t) \tag{4.34}$$

for any $\epsilon > 0$ satisfying

$$\pi_i'(t) - \pi_i'(A) \geq (\delta_i - \epsilon)(\text{li } t - \text{li } A) \tag{4.35}$$

for all $t \in [A(1+\epsilon), B]$.

We remind the reader that the notation $\pi_i'(t)$ is used to restrict to the set of primes $\mathcal{P}_{m_i}$, and in particular does not denote a derivative.

Proof. The left side of (4.34) is

$$\int_{t=A}^{B} g(t) d\big(\pi_i'(t) - \pi_i'(A)\big) = \Big[g(t)\big(\pi_i'(t) - \pi_i'(A)\big) \Big]_A^B - \int_A^B \big(\pi_i'(t) - \pi_i'(A)\big) \frac{dg}{dt} dt. \tag{4.36}$$

Certainly if (4.35) holds, then we also have the weaker bound

$$\pi_i'(t) - \pi_i'(A) \geq (\delta_i - \epsilon)\big(\text{li } t - \text{li}(A(1+\epsilon))\big).$$

As $\frac{dg}{dt} \leq 0$, we conclude that (4.36) is

$$\geq g(B)(\delta_i - \epsilon)\big(\text{li}(B) - \text{li}(A(1+\epsilon))\big) - \int_{A(1+\epsilon)}^{B} (\delta_i - \epsilon)\big(\text{li}(t) - \text{li}(A(1+\epsilon))\big) \frac{dg}{dt} dt.$$

Undoing the integration by parts, the above is

$$(\delta_i - \epsilon) \int_{A(1+\epsilon)}^{B} g(t) d\big(\text{li } t - \text{li}(A(1+\epsilon))\big) = (\delta_i - \epsilon) \int_{A(1+\epsilon)}^{B} g(t) d(\text{li } t).$$

□

Our next lemma shows that the condition (4.35) indeed holds in the case of interest.

Lemma 4.6. *Suppose $\epsilon > 0$ is given. Then for sufficiently large A and arbitrary $B > (1+\epsilon)A$, the condition*

$$\pi_i'(t) - \pi_i'(A) \geq (\delta_i - \epsilon)(\text{li } t - \text{li } A)$$

of Lemma 4.5 holds whenever $t \in [A(1+\epsilon), B]$.

Proof. This is readily implied by the Siegel-Walfisz Condition, which states that for any U that

$$\pi_i'(t) - \pi_i'(A) \geq \delta_i(\text{li } t - \text{li } A) - O(t \log^{-U} t) - O(A \log^{-U} A).$$

We may combine the error terms to write

$$\pi_i'(t) - \pi_i'(A) \geq \delta_i(\text{li } t - \text{li } A) - C_1 t \log^{-U} t$$

for some C_1 depending on U and A (but not t). Our claim then follows from the chain of inequalities

$$C_1 t \log^{-U} t \leq \frac{\epsilon^2}{3} \text{li } t \leq \epsilon(\text{li } t - \text{li } A).$$

The first inequality is obvious, and the second is true if li $A \leq (1 - \frac{\epsilon}{3})\text{li}(A(1+\epsilon))$. This relation follows in turn from the asymptotic li $x \sim \frac{x}{\log x}$. □

Proof of Proposition 4.4. To begin, we apply Lemma 4.5 to the variables t_{r-1} through t_2 in order. The inner integrals define a positive, decreasing function of t_i for each $i \geq 2$, and after $\delta_{i+1}\text{li } t_{i+1}$ has been substituted for $\pi_{i+1}'(t_{i+1})$, the t_i integrand will be differentiable in t_i as well. We thus obtain the formula

$$I_1 \geq (\delta_2 \cdots \delta_{r-2} - \epsilon) \int_{t_1} I(t_1) \int_{t_2} \dots \int_{t_{r-1}} \frac{N/q}{\log(N/q)} d(\text{li } t_{r-1}) \cdots d(\text{li } t_2) d(\pi_1'(t_1)) \tag{4.37}$$

where in the limits of integration, we have $t_{i+1} \geq (1+\epsilon)t_i$ for each i with $1 \leq i \leq r-2$.

To analyze the (more complicated) dependence on t_1, we choose an arbitrary small $\epsilon_1 > 0$, and rewrite the above as

(4.38)

$$I_1 \geq (\delta_2 \dots \delta_{r-2} - \epsilon) \int_{t_1} \frac{1}{t_1^{1-\epsilon_1}} I(t_1) \left[\int_{t_2} \dots \int_{t_{r-1}} \frac{1}{t_1^{\epsilon_1}} \frac{N/(\prod_{i=2}^{r-1} t_i)}{\log(N/(\prod_{i=1}^{r-1} t_i))} d(\text{li } t_{r-1}) \dots d(\text{li } t_2) \right] d(\pi_1'(t_1)).$$

We wish to prove that for sufficiently large N, the integrand defines a decreasing function of t_1. The quantity in square brackets is, because $t_1^{\epsilon_1} \log(N/(\prod_{i=1}^{r-1} t_i))$ is an increasing function of t_1 and because the bounds of integration shrink as t_1 grows. It therefore suffices to prove that

$$\frac{1}{t_1^{1-\epsilon_1}} I(t_1) = \frac{1}{t_1^{1-\epsilon_1}} \int_{R/t_1}^{R} \tilde{P}^2\Big(\frac{\log R/x}{\log R}\Big) d(\log^{k-1} x) \tag{4.39}$$

is also a decreasing function of t_1, for $t_1 > \exp(\sqrt{\log N})$. To prove this, we make the change of variables $u = \log t_1 / \log R$, $y = \log x / \log R$ to rewrite (4.39) as

$$(k-1)(\log^{k-1} R) e^{-(1-\epsilon_1)u \log R} \int_{1-u}^{1} \tilde{P}^2(1-y) y^{k-2} dy.$$

The derivative with respect to u is

$$(k-1)(\log^{k-1} R) e^{-(1-\epsilon_1)u \log R} \left[\tilde{P}^2(u)(1-u)^{k-2} + \left(\int_{1-u}^{1} \tilde{P}^2(1-y) y^{k-2} dy \right) (-(1-\epsilon_1) \log R) \right]. \tag{4.40}$$

We wish to prove that when N (and thus R) are sufficiently large, this will be negative for those u allowed by the condition $t_1 > \exp(\sqrt{\log N})$. With this condition, u will satisfy

$$u > \frac{\sqrt{\log N}}{\log R} > (\log N)^{-1/2}.$$

Recalling that $\log N \gg \log R$, (4.40) will be negative if

$$(\log N)\int_{1-u}^{1} \tilde{P}^2(1-y)y^{k-2}dy \gg \tilde{P}^2(u)(1-u)^{k-2}. \tag{4.41}$$

We break the proof of this into two cases. Let α be the real solution to $(1-\alpha)^{k-2} = \frac{1}{2}$ with $0 < \alpha < 1$. When $u \geq \alpha$, (4.41) follows from the fact that

$$\int_{1-\alpha}^{1} \tilde{P}^2(1-y)y^{k-2}dy \gg \tilde{P}^2(u)(1-u)^{k-2}$$

uniformly for all u; this last inequality follows as the right side is bounded and the left side is fixed. When $u < \alpha$, it is enough to show that

$$(\log N)\int_{1-u}^{1} \tilde{P}^2(1-y)dy \gg \tilde{P}^2(u). \tag{4.42}$$

We prove this when $\tilde{P}^2(x) = x^c$ for a positive integer c, and then the result for general $\tilde{P}$ follows by linearity. The quantity on the left is

$$(\log N)\int_{0}^{u} y^c dy = \frac{u^c}{c+1}\cdot(u\log N) \gg u^c(\log N)^{1/2} \gg u^c, \tag{4.43}$$

which proves (4.42) and therefore the fact that the integrand in (4.38) is decreasing. Accordingly, Lemma 4.5 applies, and Proposition 4.4 follows. □

In summary, we have proved the inequality

$$T_{\mathfrak{m}} \geq (\delta_1\cdots\delta_r\varphi(M) - o_N(1))\frac{N\mathfrak{S}(\mathcal{L})\log^2 R}{(k-1)!}\times \tag{4.44}$$
$$\int_{t_1}\cdots\int_{t_{r-1}} \frac{1}{\prod(t_i\log t_i)\log(N/\prod t_i)}\left(\int_{R/t_1}^{R}\tilde{P}^2\big(\frac{\log R/x}{\log R}\big)d(\log^{k-1}x)\right)dt_{r-1}\ldots dt_1.$$

We have slightly shrunk the bounds of integration to introduce the condition $t_{i+1} > (1+\epsilon)t_i$, where $\epsilon > 0$ is a constant that may be chosen arbitrarily small for sufficiently large N. The constant implied by $o_N(1)$ depends on this ϵ; we shall control this dependence by choosing $\epsilon = \epsilon(N)$ so that ϵ approaches 0 as N grows.

We obtain a similar inequality for $S_{1,j}$ by summing over all $\mathfrak{m}$. We write

$$\delta_j := \sum_{\mathfrak{m}} \delta_1\cdots\delta_r. \tag{4.45}$$

The sum is over all $\mathfrak{m} = \{m_1,\ldots,m_r\}$ for which $m_1\cdots m_r \equiv b_j \pmod m$. Then δ_j is simply the density of $E_{r,\mathcal{P}}$ numbers congruent to b_j modulo m as a proportion of all E_r numbers, as defined earlier. We make the change of variables $u_i = \log t_i/\log R$ (for each i) and $y = \log x/\log R$ to obtain

$$S_{1,j} \geq (\delta_j\varphi(M) - o_N(1))\frac{N\mathfrak{S}(\mathcal{L})\log^k R}{(k-2)!}\times \tag{4.46}$$
$$\int_{u_1}\cdots\int_{u_{r-1}} \frac{1}{(B-\sum_i u_i)\prod_i u_i}\big(\int_{y=1-u_1}^{1}\tilde{P}(1-y)^2y^{k-2}dy\big)du_{r-1}\ldots du_1.$$

For convenience, we introduce the further simplification

$$\frac{1}{B-\sum_i u_i} \geq \frac{1}{B},$$

and we switch the order of integration to write

$$S_{1,j} \geq (\delta_j \varphi(M) - o_N(1)) \frac{N\mathfrak{S}(\mathcal{L}) \log^k R}{B(k-2)!} \int_{y=0}^1 \tilde{P}(1-y)^2 y^{k-2} dy \int_{u_1} \dots \int_{u_{r-1}} \frac{1}{\prod_i u_i} du_{r-1} \dots du_1.$$

The bounds of integration are

$$u_1 > 1-y,$$

$$u_1 > \frac{\sqrt{\log N}}{\log R}, \tag{4.47}$$

$$u_{i+1} > u_i + \log(1+\epsilon) \quad (1 \leq i \leq r-2), \tag{4.48}$$

$$u_1 + \dots + u_{r-2} + 2u_{r-1} < B.$$

In case Hypothesis $BV(\vartheta, M)$ is not assumed, the condition $p_{r-1} > R$ imposes the bound

$$u_{r-1} > 1. \tag{4.49}$$

The integrand is nonnegative, so we may pass to the limit as $N \to \infty$ and $\epsilon \to 0$, so that (4.47) is superfluous and in place of (4.48) we have $u_{i+1} > u_i$. This is the claim of Proposition 2.4.

5. Proofs of Theorems 2.2 and 2.3

The proofs of Theorem 2.2 and 2.3 will proceed by establishing lower bounds for the integral in Proposition 2.4,

$$I^{\pm}(r,k,P,B) := \int_{y=0}^1 \tilde{P}(1-y)^2 y^{k-2} dy \int_{u_1} \dots \int_{u_{r-1}} \frac{1}{\prod_i u_i} du_{r-1} \dots du_1. \tag{5.1}$$

We let I^- denote the integral with the restriction that $u_{r-1} > 1$, and we let I^+ denote the same integral without this restriction.

These integrals seem somewhat difficult to estimate closely, so we shall content ourselves with somewhat simple estimates.

We begin with the following identity:

Lemma 5.1. *For $r \geq 2$ and $0 < t < 1$, we have*

$$\int_{u_1=t}^1 \dots \int_{u_{r-1}=u_{r-2}}^1 \frac{1}{\prod_i u_i} du_{r-1} \dots du_1 = \frac{(-\log t)^{r-1}}{(r-1)!}.$$

Proof. This follows easily by induction on r. □

As the integrand of $I^{\pm}(r,k,P,B)$ is positive, we may derive a lower bound by restricting the range of integration. We consider the bounds

$$\int_{u_1=t}^1 \dots \int_{u_{r-2}=u_{r-3}}^1 \int_{u_{r-1}=u_{r-2}}^1 \frac{1}{\prod_i u_i} du_{r-1} \dots du_1 \tag{5.2}$$

for I^+, and

$$\int_{u_1=t}^1 \dots \int_{u_{r-2}=u_{r-3}}^1 \int_{u_{r-1}=1}^3 \frac{1}{\prod_i u_i} du_{r-1} \dots du_1 \tag{5.3}$$

for I^-. Considering the bound (2.33), these will be a subset of our original bounds of integration if $B \geq r$ for I^+, and $B \geq r+4$ for I^-. The restricted bound for I^+ limits attention to almost-primes whose smallest $r-1$ factors are less than R; the bound for I^- limits attention to almost-primes whose smallest $r-2$ factors are less than R, and whose next largest factor is between R and R^3.

Using Lemma 5.1, we thus obtain

$$I^+(r,k,P,B) \geq \frac{1}{(r-1)!}\int_{y=0}^1 \tilde{P}(1-y)^2 y^{k-2}(-\log(1-y))^{r-1}dy \tag{5.4}$$

$$I^-(r,k,P,B) \geq \frac{1}{(r-2)!}\int_{y=0}^1 \tilde{P}(1-y)^2 y^{k-2}(-\log(1-y))^{r-2}dy. \tag{5.5}$$

Here we have made the simple estimate $\log 3 > 1$ in (5.5). Write a for $r-1$ or $r-2$, and fix $P(x)=1$, $\tilde{P}(x)=x$, so that we need to bound

$$J(a,k) := \int_{y=0}^1 (1-y)^2 y^{k-2}(-\log(1-y))^a dy. \tag{5.6}$$

Fix a parameter $\alpha \in (0,1)$, to be determined later, and restrict the range of integration to those α where $y^{k-2} > \alpha$. We obtain

$$J(a,k) > \alpha \int_{y=\alpha^{\frac{1}{k-2}}}^1 (1-y)^2(-\log(1-y))^a dy$$

$$= \alpha \int_{y=0}^{1-\alpha^{\frac{1}{k-2}}} y^2(-\log y)^a dy.$$

Integrating by parts, this is

$$\alpha y^3\big[\frac{1}{3}(-\log y)^a + \frac{a}{9}(-\log y)^{a-1} + \frac{(a)(a-1)}{27}(-\log y)^{a-2} + \cdots + \frac{a!}{3^{a+1}}\big]\Big|_0^{1-\alpha^{\frac{1}{k-2}}}$$

$$= \alpha(1-\alpha^{\frac{1}{k-2}})^3\big[\frac{1}{3}(-\log(1-\alpha^{\frac{1}{k-2}}))^a + \frac{a}{9}(-\log(1-\alpha^{\frac{1}{k-2}}))^{a-1} + \cdots + \frac{a!}{3^{a+1}}\big].$$

We thus obtain the crude estimate

$$J(a,k) > \frac{\alpha}{3}(1-\alpha^{\frac{1}{k-2}})^3(-\log(1-\alpha^{\frac{1}{k-2}}))^a. \tag{5.7}$$

To estimate the quantity $1-\alpha^{\frac{1}{k-2}}$, observe that

$$1-\alpha^{\frac{1}{k-2}} = \frac{1-\alpha}{1+\alpha^{\frac{1}{k-2}}+\cdots+\alpha^{\frac{k-1}{k-2}}},$$

so that

$$\frac{1-\alpha}{k-2} < 1-\alpha^{\frac{1}{k-2}} < \frac{1-\alpha}{\alpha(k-2)}. \tag{5.8}$$

We thus estimate

$$(1-\alpha^{\frac{1}{k-2}})^3 > \big(\frac{1-\alpha}{k-2}\big)^3,$$

$$-\log(1-\alpha^{\frac{1}{k-2}}) > -\log\left(\frac{1-\alpha}{\alpha(k-2)}\right) = \log\left(\frac{\alpha(k-2)}{1-\alpha}\right),$$

and deduce that

$$J(a,k) > \frac{\alpha}{3}\left(\frac{1-\alpha}{k-2}\right)^3 \log^a\left(\frac{\alpha(k-2)}{1-\alpha}\right).$$

Therefore we have established the estimate

$$S_{1,j} \geq (1-o_N(1))\frac{\delta_j \varphi(M) N \mathfrak{S}(\mathcal{L}) \log^k R}{B(k-2)!a!}\frac{\alpha}{3}\left(\frac{1-\alpha}{k-2}\right)^3 \log^a\left(\frac{\alpha(k-2)}{1-\alpha}\right), \tag{5.9}$$

where $a = r-1$ if $BV(\vartheta, M)$ is assumed, and $a = r-2$ otherwise. We multiply by k, the number of terms, replace δ_j with δ (which is the minimum of the δ_j), and subtract νS_0 to obtain

$$S = N\mathfrak{S}(\mathcal{L})\log^k R\left[(1-o_N(1))\frac{k\delta\varphi(M)}{B(k-2)!a!}\frac{\alpha}{3}\left(\frac{1-\alpha}{k-2}\right)^3 \log^a\left(\frac{\alpha(k-2)}{1-\alpha}\right) - (1+o_N(1))\frac{\nu}{k!}\right]. \tag{5.10}$$

To prove that this is positive for large N, it suffices to prove that

$$\frac{k\delta\varphi(M)}{B(k-2)!a!}\frac{\alpha}{3}\left(\frac{1-\alpha}{k-2}\right)^3 \log^a\left(\frac{\alpha(k-2)}{1-\alpha}\right) > \frac{\nu}{k!}. \tag{5.11}$$

We sort this out a bit to obtain the condition

$$\frac{k^2(k-1)}{(k-2)^3}\log^a\left(\frac{\alpha(k-2)}{1-\alpha}\right) > \frac{3\nu B a!}{\delta\varphi(M)\alpha(1-\alpha)^3}.$$

The ratio of k terms at left is greater than 1, and just slightly so as k gets large, so that we can replace this with

$$\log^a\left(\frac{\alpha(k-2)}{1-\alpha}\right) > \frac{3\nu B a!}{\delta\varphi(M)\alpha(1-\alpha)^3}$$

and thus

$$\log(k-2) > \Big[\frac{3\nu B a!}{\delta\varphi(M)\alpha(1-\alpha)^3}\Big]^{\frac{1}{a}} - \log\left(\frac{\alpha}{1-\alpha}\right).$$

Choosing $\alpha = 1/4$, we have

$$\log(k-2) > \Big[\frac{256}{9}\frac{\nu B a!}{\delta\varphi(M)}\Big]^{\frac{1}{a}} + \log 3$$

and thus

$$k > 3\exp\big(\Big[\frac{29\nu B a!}{\delta\varphi(M)}\Big]^{\frac{1}{a}}\big) + 2.$$

To prove Theorem 2.3 we take $B = r+4, a = r-2$. To prove Theorem 2.2 we take $a = r-1$, thereby obtaining (2.15) for each $B > \max(2/\vartheta, r)$ and thus for $B = \max(2/\vartheta, r)$ as well.

We conclude with a sketch of the proof of Theorem 2.1. In the case of E_2 numbers, (4.14) remains valid, and reads

$$S_{1,j} \sim \sum_{d,e}\lambda_d\lambda_e \sideset{}{'}\sum_{p}\frac{\tau_{k-1}([d,e,p]/p)}{\varphi(a_j[d,e,p]/p)}\varphi(M)\sum_{\substack{a_j N/p < n \leq 2a_j N/p \\ n \equiv b_j\bar{p}_M \pmod M}}\beta_{1,\mathcal{P}}(n).$$

This is the same as the sum occurring immediately before (5.6) in [13], except for the restrictions on n and p. As the sum over n is immediately estimated using the prime number theorem, we obtain a factor of δ_2 corresponding to this restriction.

We also need to take into account the restrictions on p. In the evaluation of the analogous sum in [13], the authors use the estimation

$$\sum_{p\leq u}\log p = u + Z(u)$$

for an error term $Z(u)$ satisfying

$$Z(u) \ll u\exp(-c\sqrt{\log u})$$

by the prime number theorem. In our case, we have

$$\sum_{p\le u}{}' \log p = \delta_1 u + Z(u)$$

where $Z(u)$ satisfies the weaker Siegel-Walfisz condition

$$Z(u) \ll u \log^{-A} u. \tag{5.12}$$

One checks that the estimates in Lemmas 10-12 of [13] remain valid with the weaker error term (5.12), so that the estimate for $S_{1,j}$ holds with an additional density factor of $\delta_j\varphi(M)$. The remainder of the analysis in [13] then proves Theorem 2.1 for any $B > 2/\vartheta$, and thus for $B = 2/\vartheta$ as well.

6. An Example

In this section we use work of Ono [21] to give an example of how the constant C_E of Theorem 1.2 can be made explicit. We consider the elliptic curve $E := X_0(11)$, given by the equation

$$y^2 = x^3 - 4x^2 - 160x - 1264. \tag{6.1}$$

(For an illuminating discussion of some interesting properties of this curve see [16], Ch. 11). Ono establishes the existence of a set of primes S_1 of Frobenius density $\frac{1}{3}$, so that for any square-free integer q whose prime factors are all in S_1, we have

$$\mathrm{rk}(E(-11q), \mathbb{Q}) = 0.$$

Moreover, Ono explicitly describes S_1 as follows: The natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the 2-division points of $E(-11)$ induces the surjective representation

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}),$$

which satisfies

$$\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) \equiv a(p) \pmod 2$$

for all but finitely many primes p. (Here $a(p) := p + 1 - \#E(\mathbb{F}_p)$, Frob_p denotes the Frobenius at p in $\mathrm{Gal}(\mathbb{Q}[f(x)]/\mathbb{Q})$, and $f(x)$ is the cubic in (6.1).) The set S_1 is the set of those primes p such that $\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) \equiv 1 \pmod 2$, and the Chebotarev density theorem implies that S_1 has density $\frac{1}{3}$.

By Murty and Murty's theorem [19], S_1 satisfies Hypothesis $BV(\vartheta, M)$. To compute M, we calculate that the discriminant of $f(x)$ is $-2^8 \cdot 11^5$, and the only subfield of $\mathbb{Q}(f(x))$ that will be contained in any cyclotomic field is $\mathbb{Q}(\sqrt{-11})$. This field has discriminant -11, and so will in fact be contained in $\mathbb{Q}(\zeta_{11})$, so $M = 11$. We may then use (3.4) to compute $\vartheta = 1/2$.

We will forgo a detailed analysis of the density of S_1 in arithmetic progressions, and instead easily obtain a somewhat large upper bound. We will choose an admissible k-tuple with each b_j in the same residue class modulo 11. For some choice of residue class we will have $\delta\varphi(M) \ge \frac{1}{9}$, so we may apply Theorem 2.1 with $B = 4$ and $\delta\varphi(M) = \frac{1}{9}$, obtaining $k = 4574$. Let $p_1, p_2, \dots$ denote the primes larger than 4574; choosing a subset $\{p_i\}$ of 4574 of these in the same residue class modulo 11, $\{11n + p_i\}$ will form an 11-admissible 4574-tuple.

We may guarantee that 4574 of the p_i are in the same residue class by choosing from the first $4574 \cdot \varphi(11) + 1 = 45741$ primes larger than 4574. Referring to a table [4] of the primes, we conclude that there are infinitely pairs of square-free m and n with

$$\mathrm{rk}(E(-11m)) = \mathrm{rk}(E(-11n)) = 0,$$

and

$$|m - n| \le 559286.$$

References

[1] A. Balog and K. Ono, *Elements of class groups and Shafarevich-Tate groups of elliptic curves*, Duke Math J. **120** (2003), 35-63.

[2] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, 2nd ed., Astérisque 18. Société Mathématique de France, Paris, 1987.

[3] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in progression to large moduli*, Acta Math., **156** (1986), 203-251.

[4] A. Booker, *The nth prime page*, http://primes.utm.edu/nthprime/index.php#nth

[5] J.-R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica, **16** (1973), 157-176.

[6] A. C. Cojocaru and M. R. Murty, *An introduction to sieve methods and their applications*, Cambridge University Press, Cambridge, 2005.

[7] H. Davenport, *Multiplicative number theory*, GTM 74, Springer-Verlag, New York, 2000.

[8] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507-530.

[9] T. J. Engelsma, *k-tuple permissible patterns*, http://www.opertech.com/primes/k-tuples.html.

[10] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Springer Lect. Notes **751** (1979), 108-118.

[11] D. A. Goldston, J. Pintz, and C.Y. Yıldırım, *Primes in tuples I*, preprint.

[12] D. A. Goldston, S. W. Graham, J. Pintz, and C. Y. Yıldırım, *Small gaps between primes or almost primes*, preprint.

[13] D. A. Goldston, S. W. Graham, J. Pintz, and C. Y. Yıldırım, *Small gaps between products of two primes*, preprint.

[14] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society, Providence, 2005.

[15] J. Jiménez Urroz, *Bounded gaps between almost prime numbers representable as sum of two squares*, preprint.

[16] A. Knapp, *Elliptic curves*, Princeton University Press, Princeton, 1992.

[17] N. Koblitz, *Introduction to elliptic curves and modular forms*, GTM 97, Springer-Verlag, New York, 1993.

[18] V. Kolyvagin, *Finiteness of* $E(\mathbb{Q})$ *and* $Ш_{E/\mathbb{Q}}$ *for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk., USSR, ser. Matem. **52** (1988), 522-540.

[19] M. R. Murty and V. K. Murty, *A variant of the Bombieri-Vinogradov theorem*, Canadian Math. Soc. Conf. Proc., Vol. 7 (1987), 243-272.

[20] Y. Motohashi, *An induction principle for the generalization of Bombieri's prime number theorem*, Proc. Japan Acad., **52** (1976), 273-275.

[21] K. Ono, *Twists of elliptic curves*, Compositio Math., **106** (1997), 349-360.

[22] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. reine angew. math., **533** (2001), 81-97.

[23] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, Invent. Math. **134**, 1998, 651-660.

[24] J. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, New York, 1986.

[25] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc., **61** (2000), 681-690.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: thorne@math.wisc.edu