Functiones et Approximatio
57.1 (2017), 77–91
doi: 10.7169/facm/1618

A BOMBIERI–VINOGRADOV THEOREM WITH PRODUCTS OF GAUSSIAN PRIMES AS MODULI

Karin Halupczok

Abstract: We prove a version of the Bombieri–Vinogradov Theorem with certain products of Gaussian primes as moduli, making use of their special form as polynomial expressions in several variables. Adapting Vaughan's proof of the classical Bombieri–Vinogadov Theorem, cp. [10] to this setting, we apply the polynomial large sieve inequality that has been proved in [7] and which includes recent progress in Vinogradov's mean value theorem due to Parsell *et al.* in [9]. From the benefit of these improvements, we obtain an extended range for the variables compared to the range obtained from standard arguments only.

Keywords: polynomial large sieve inequality, Bombieri–Vinogradov Theorem, polynomial moduli in several variables, Gaussian primes

1. Introduction

The classical theorem of Bombieri–Vinogradov states that

Theorem 1.1 (Theorem of E. Bombieri [2] and A. I. Vinogradov [11, 12]). *For any $A, Q, x > 1$ we have*

$$\sum_{q \leqslant Q} \sup_{y \leqslant x} \max_{a \bmod q} |E(y; q, a)| \ll_A \frac{x}{(\log x)^A} + Q\sqrt{x}(\log(Qx))^3$$

where

$$E(y; q, a) := \psi(y; q, a) - \frac{y}{\varphi(q)} \text{ and } \psi(y; q, a) := \sum_{\substack{n \leqslant y \\ n \equiv a \bmod q}} \Lambda(n),$$

so the nontrivial upper bound $\ll_A x(\log x)^{-A}$ is obtained for $Q \leqslant x^{1/2}(\log x)^{-3-A}$. It is well known to be a difficult task to break the "1/2-barrier", which means to show the estimate for q bigger that $x^{1/2}$. The famous Elliott–Halberstam conjecture in [5] states that the estimate should hold even with $Q \ll x^{1-\varepsilon}$. Many

2010 Mathematics Subject Classification: primary: 11N36; secondary: 11N05

applications, especially recent progress in the solution of the small gap conjecture, rely on such improvements on the bound Q for certain moduli sets for q. It has been found by Y. Zhang in [13] that a restriction to certain smooth moduli breaks the 1/2-barrier.

A standard approach to prove Bombieri–Vinogradov's theorem is the proof of Vaughan, cp. [10], by making use of the large sieve inequality. In [7], nontrivial improvements of the large sieve inequality with polynomial moduli have been achieved, based on the work of Parsell *et al.* in [9] in connection with progress in Vinogradov's mean value theorem. The results of [7] are superior to standard approaches in a number of applications where the degree of the considered polynomial is bigger than the number of variables.

In this article, we use Vaughan's approach to prove a variant of the Bombieri–Vinogradov Theorem with polynomial moduli having certain properties. The polynomial behavior of the moduli is exploited in the proof by using the result in [7]. Our main result is the following:

Theorem 1.2 (A Bombieri–Vinogradov Theorem with special polynomial moduli). *Let $A, Q, x > 1$ be real and $\ell, k \geqslant 1$ be integers. Consider two maps $u, v : \{1, \dots, k\} \to \{1, \dots, \ell\}$ such that $\{u(i), v(i)\} \neq \{u(j), v(j)\}$ for $i \neq j$, and let $P \in \mathbb{Z}[x_1, \dots, x_\ell]$ be the polynomial $P(\mathbf{x}) := \prod_{i=1}^{k}(x_{u(i)}^2 + x_{v(i)}^2)$.*

Let $\sigma = 1/(4kr)$ with $r := \binom{2k+\ell-1}{\ell} - 1$ and suppose that

$$x^{\varepsilon/\sigma} \ll Q \leqslant x^{(1/3-2\varepsilon)/(2k-\sigma)} \tag{1}$$

for an arbitrary $\varepsilon > 0$. Then we have the estimate

$$\sum_{\mathbf{q}\sim Q} G_{\mathbf{q}} \frac{\varphi(P(\mathbf{q}))}{Q^\ell} \sup_{y\leqslant x} \max_{\substack{a \bmod P(\mathbf{q}) \\ \gcd(a,P(\mathbf{q}))=1}} |E(y; P(\mathbf{q}), a)| \ll_{A,\ell,k,\varepsilon} \frac{x}{(\log x)^A},$$

where

$$G_{\mathbf{q}} := \mu^2(P(\mathbf{q}))\Lambda(q_{u(1)}^2 + q_{v(1)}^2) \cdots \Lambda(q_{u(k)}^2 + q_{v(k)}^2),$$

and the sum runs over all $\mathbf{q}$ with $Q < q_i \leqslant 2Q$, $i = 1, \dots, k$.

In the weights $G_{\mathbf{q}}$, the Λ-arguments are all primes $\equiv 1 \bmod 4$ by Gauss' theorem on the sum of two squares, and $P(\mathbf{q})$ is a squarefree number composed of such Gaussian primes. Hence we consider certain subsets of

$$\{p_1 \cdots p_k;\ \text{all } p_i \equiv 1 \bmod 4 \text{ prime, pairwise different and } 2Q^2 < p_i \leqslant 8Q^2\}$$

as moduli, which is the set of squarefree products of k Gaussian primes from a certain interval of length $6Q^2$. Note that the subsets we consider become quite sparse if the degree $2k$ of P is bigger than the number ℓ of variables. In that case, the estimate in Theorem 1.2 can not be deduced directly by applying the classical Theorem 1.1 due to the assigned weights that reflect the sparsity of the moduli. In other words, Theorem 1.2 takes the distribution of the moduli into account, whereas the classical theorem only sees the size of the moduli.

It is clear from the proof that the range with exponent $1/6k$ in (1) could also be obtained using a standard approach. The improvement here is the term 3σ coming from the benefit of the polynomial large sieve inequality from [7]. So to speak, it breaks the "$1/6k$-barrier". Whether this "$1/6k$-barrier" is really such a hard barrier is not that clear since by the classical theorem, one might heuristically expect a hard barrier at $1/4k$.

A similar phenomenon is already known from the literature in the case of polynomials in one variable of degree d; in that case, heuristically, $1/2d$ might be reached. This has been investigated by Elliott in [4], who proved such a Bombieri–Vinogradov-type theorem with exponent $1/4d$ and gave evidence that one might be able to reach $1/3d$ by further improvements, though the barrier of the method seems to be at $1/4d$. Later, Mikawa and Peneva [8] improved the exponent to $8/19d$, and Baker [1] to $9/20d$.

For the polynomials of degree $d = 2k$ considered in this article, Theorem 1.2 confirms the exponent $1/3d$, even improving it in a way depending on σ. Note however, that we always have at least two variables. It is not clear yet whether the improvements in [8, 1] can be extended to a several variable setting as in the present article. The proof of Theorem 1.2 relies on the classical Fourier Analysis approach, whereas deeper such techniques are used in [8] and [1]. Elliott's argument in [4] is a largely self-contained careful application of Linnik's Dispersion Method, without appeal to Fourier Analysis.

We continue by giving some important comments on our choice of the moduli.

Firstly, the proof of the polynomial version of the Basic Mean Value Theorem in Section 4 does *not* depend on this choice: it works for arbitrary polynomials P of degree k in ℓ variables, assuming only that the biggest value M_Q and smallest value m_Q of P in the dyadic Q-box $\mathbf{q} \sim Q$ are such that $Q^k \ll m_Q \leqslant M_Q \ll Q^k$ holds for P. In the proof, one needs primes $p = q_u^2 + q_v^2$ with q_u, q_v of similar size. But then, Theorem 1.2 and its proof rely on the special structure of the moduli: we use that each divisor is again of such a form so that the polynomial basic mean value theorem can be used iteratively.

Secondly, one should make clear that the estimate in our Theorem 1.2 is non-trivial in the sense that the number of moduli is big enough and not too sparse, so that it can not be deduced using the trivial estimate $E(y; P(\mathbf{q}), a) \ll y/\varphi(\mathbf{q})$.

This would indeed follow from the following conjecture.

Conjecture 1.3 (Number of moduli). *Consider u, v, P as in Theorem 1.2. There exists a constant $C > 0$ depending on k and ℓ only such that*

$$\sum_{\mathbf{q}\sim Q} \mu^2(P(\mathbf{q}))\Lambda(q_{u(1)}^2 + q_{v(1)}^2)\cdots\Lambda(q_{u(k)}^2 + q_{v(k)}^2) \gg_{k,\ell} \frac{Q^\ell}{(\log Q)^C}.$$

As a second result of this article, we confirm this conjecture in certain cases, namely when not too many of the Gaussian primes share a summand q_i^2.

Theorem 1.4 (Special cases). *Assume that the maps $u, v : \{1, \dots, k\} \to \{1, \dots, \ell\}$ are such that for each $i \leqslant k$, one of the numbers $u(i)$ and $v(i)$ does not occur in the set $\{u(i+1), \dots, u(k), v(i+1), \dots, v(k)\}$. Then the assertion in Conjecture 1.3 holds true.*

To give an example, if the sequence of the pairs $(u(i), v(i))$ is $(1,2)$, $(2,3)$, $(3,4)$, we deal with the polynomial $P(\mathbf{x}) = (x_1^2 + x_2^2)(x_2^2 + x_3^2)(x_3^2 + x_4^2)$. On the other hand, the sequence of pairs $(1,2), (2,3), (3,1)$ does not comply with the condition. Clearly, if this condition holds, then $\ell \geqslant k+1$. However, the degree $2k$ of the polynomial may still be bigger than the number ℓ of variables, so that Theorem 1.2 is nontrivial.

We prove Theorem 1.4 in Section 6 by making use of the main theorem of Fouvry and Iwaniec in [6].

Some other additional remarks on Theorem 1.2:

(i) Further improvements of Theorem 1.2 could be made if the relevant term $Q^{\ell-\sigma}N$ in the polynomial large sieve inequality, which is dominant in the relevant ranges, could be further improved. Ideas how this could be reached, but showing also its difficulty, are discussed in [7, Sec. 5].

(ii) The restriction $\mathbf{q} \sim Q$ can be generalized to $R \ll \mathbf{q} \ll Q$. In that case the estimate in Theorem 1.2 holds with upper bound $Q \ll x^{1/6k-\varepsilon} R^{\sigma/2k}$. Therefore the benefit coming from σ melts if R decreases. The theorem gives the biggest possible upper bound for Q if $Q/R \ll 1$.

(iii) It should be possible to obtain a power of $\log x$ instead of the term x^ε in the range for Q by working more precisely. This would require a refinement of the used theorem [9, Thm. 10.1] of Parsel *et al.* where Q^ε is replaced by a power of $\log Q$.

Notation. Let k, ℓ denote positive integers and let ε denote a positive real number. In this article, we suppress the dependence of the implicit constants on k, ℓ or ε in our notation and simply write $\ll$ for $\ll_{k,\ell,\varepsilon}$ or $\ll_{k,\ell}$.

For a real number $Q > 1$ the symbol $q \sim Q$ means $Q < q \leqslant 2Q$, and the notation $\mathbf{q} \sim Q$ means that the ℓ-tuple $\mathbf{q} = (q_1, \dots, q_\ell)$ of integers is contained in a dyadic Q-box, that is $q_i \sim Q$ for $i = 1, \dots, \ell$.

For $\alpha \in \mathbb{R}$, the symbol $\mathrm{e}(\alpha) := \exp(2\pi i \alpha)$ denotes the complex exponential function. The greatest common divisor is abbreviated by gcd. As usual, we denote the von Mangoldt function by Λ, Euler's totient function by φ, and the Möbius function by μ.

2. Auxiliary tools

Assumptions 2.1. *Let ℓ be a positive integer and let $P \in \mathbb{Z}[x_1, \dots, x_\ell]$ be a polynomial in ℓ variables of degree $k \geqslant 2$. Let $\sigma := 1/(2rk)$ with $r := \binom{k+\ell-1}{\ell} - 1$, and for a real number $Q > 1$ consider the ℓ-tuples in the dyadic Q-box $\mathbf{q} \sim Q$.*

Assume that P takes only positive values in the Q-box and that the biggest value M_Q and smallest value m_Q of P in this box are such that $Q^k \ll m_Q \leqslant M_Q \ll Q^k$ holds for P.

In [7, Cor. 3], we obtained the following polynomial large sieve inequality.

Theorem 2.2 (Polynomial large sieve inequality). *Let P be a polynomial as in Assumptions 2.1, let (v_n) be a complex sequence, and let*

$$S(\alpha) := \sum_{M<n\leqslant M+N} v_n \mathrm{e}(\alpha)$$

and

$$\Sigma = \Sigma_{Q,N,P} := \sum_{\mathbf{q}\sim Q} \sum_{\substack{1\leqslant a\leqslant P(\mathbf{q}) \\ \gcd(a,P(\mathbf{q}))=1}} \Big| S\Big(\frac{a}{P(\mathbf{q})}\Big)\Big|^2.$$

Then we have the bound

$$\Sigma \ll (QN)^{\varepsilon} \cdot \Delta(Q,N) \cdot \sum_{M<n\leqslant M+N} |v_n|^2 \tag{2}$$

with $\Delta(Q,N) := Q^{k+\ell} + Q^{\ell-\sigma}N + Q^{\ell+k\sigma}N^{1-\sigma}$.

Further, the following Lemmas are standard tools in the proof of the classical Bombieri–Vinogradov Theorem: their proofs can be found in the literature, see e. g. [10].

Lemma 2.3 (Consequence of Vaughan's identity). *Let $U, x \geqslant 1$, $U^2 \leqslant x$, $f : \mathbb{N} \to \mathbb{C}$. Then*

$$\sum_{U<n\leqslant x} f(n)\Lambda(n) \ll (\log x)T_1 + T_2 + T_3$$

with

$$T_1 = \sum_{\ell\leqslant U} \max_{w} \Big| \sum_{w<k\leqslant x/\ell} f(k\ell)\Big|$$

and

$$T_i = \Big| \sum_{U<m\leqslant \max\{x/U,U^2\}} a_i(m)b_i(k)f(mk)\Big| \text{ for } i = 2,3,$$

where $a_i(m)$, $b_i(k)$ are arithmetic functions depending on U only and $|b_i(k)| \leqslant \sum_{d|k} 1$, $|a_i(k)| \leqslant \log k$ for all $k \in \mathbb{N}$.

Lemma 2.3 is presented as [3, Satz 6.1.1] in the book of Brüdern. It can be deduced easily from the widely-known Vaughan identity.

Lemma 2.4 (Polya–Vinogradov's inequality). *Let $w < z$ be real. For any nonprincipal character χ mod $q > 1$ we have*

$$\sum_{w<k\leqslant z} \chi(k) \ll q^{1/2}\log q.$$

Lemma 2.5 (Formula for $\chi(n)$). *Let $q \geqslant 1$. Then for all $n \in \mathbb{Z}$ and all primitive characters χ mod q we have*

$$\chi(n)\tau(\overline{\chi}) = \sum_{h \bmod q} \overline{\chi}(h)\mathrm{e}(hn/q),$$

where $\tau(\chi) := \sum_{a=1}^{q} \chi(a)e(a/q)$ is the Gaussian sum. We have $|\tau(\chi)| = \sqrt{q}$ for primitive χ mod q.

Lemma 2.6 (Get rid of $mn \leqslant X$). *Let $T, X > 1$ be real, $M, N \geqslant 1$ be integers and let (γ_n), (η_n) be complex sequences. Then*

$$\sum_{\substack{m\leqslant M, n\leqslant N\\ mn\leqslant X}} \gamma_m\eta_n \ll \int_{-T}^{T} \Big|\sum_{m\leqslant M} \gamma_m m^{it} \sum_{n\leqslant N} \eta_n n^{it}\Big| \min(|t|^{-1}, \log(2MN))dt + MNT^{-1} \sum_{m\leqslant M, n\leqslant N} |\gamma_m\eta_n|. \tag{3}$$

3. The polynomial large sieve inequality for characters and its bilinear version

Lemma 3.1 (Polynomial large sieve inequality with characters). *Let $Q, x > 1$ and (v_n) be a complex sequence. Then*

$$\sum_{\mathbf{q}\sim Q} \frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))} \sideset{}{^*}\sum_{\chi(P(\mathbf{q}))} \Big|\sum_{n\leqslant x} v_n\chi(n)\Big|^2 \ll (Qx)^{\varepsilon} \cdot \Delta(Q, x) \cdot \sum_{n\leqslant x} |v_n|^2,$$

where the star means that the sum is stretched over all primitive characters χ mod $P(\mathbf{q})$.

Proof. If χ mod $P(\mathbf{q})$ is primitive, Lemma 2.5 gives

$$\Big|\sum_{n\leqslant x} v_n\chi(n)\Big|^2 = \frac{1}{P(\mathbf{q})}\Big|\sum_{a=1}^{P(\mathbf{q})} \sum_{n\leqslant x} \overline{\chi}(a)\mathrm{e}\Big(\frac{an}{P(\mathbf{q})}\Big)v_n\Big|^2.$$

We sum this equation on the right hand side over all characters, and on the left hand side over all primitive characters. We obtain

$$\sum_{\chi(P(\mathbf{q}))}^{*}\Big|\sum_{n\leqslant x}v_n\chi(n)\Big|^2 \leqslant \frac{1}{P(\mathbf{q})}\sum_{\chi(P(\mathbf{q}))}\Big|\sum_{a=1}^{P(\mathbf{q})}\sum_{n\leqslant x}\overline{\chi}(a)\mathrm{e}\Big(\frac{an}{P(\mathbf{q})}\Big)v_n\Big|^2$$
$$= \frac{1}{P(\mathbf{q})}\sum_{a,c=1}^{P(\mathbf{q})}\sum_{m,n\leqslant x}\sum_{\chi(P(\mathbf{q}))}\overline{\chi}(a)\chi(c)\mathrm{e}\Big(\frac{an-cm}{P(\mathbf{q})}\Big)v_n\overline{v_m}$$
$$= \frac{\varphi(P(\mathbf{q}))}{P(\mathbf{q})}\sum_{\substack{a \bmod P(\mathbf{q})\\ \gcd(a,P(\mathbf{q}))=1}}\sum_{m,n\leqslant x}\mathrm{e}\Big(\frac{a(n-m)}{P(\mathbf{q})}\Big)v_n\overline{v_m}$$
$$= \frac{\varphi(P(\mathbf{q}))}{P(\mathbf{q})}\sum_{\substack{a \bmod P(\mathbf{q})\\ \gcd(a,P(\mathbf{q}))=1}}\Big|S\Big(\frac{a}{P(\mathbf{q})}\Big)\Big|^2,$$

hence

$$\sum_{\mathbf{q}\sim Q}\frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))}\sum_{\chi(P(\mathbf{q}))}^{*}\Big|\sum_{n\leqslant x}v_n\chi(n)\Big|^2 \ll (Qx)^{\varepsilon}\cdot\Delta(Q,x)\cdot\sum_{n\leqslant x}|v_n|^2$$

by Theorem 2.2. ∎

Lemma 3.2 (Bilinear inequality). *Let $x, Q, M, N > 1$, let (a_m) and (b_n) be complex sequences. Then*

$$\sum_{\mathbf{q}\sim Q}\frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))}\sum_{\chi(P(\mathbf{q}))}^{*}\max_{X}\Big|\sum_{\substack{m\leqslant M\\ n\leqslant N\\ mn\leqslant X}}a_mb_n\chi(mn)\Big|$$
$$\ll (QMN)^{\varepsilon}\cdot\Big(\Delta(Q,M)\Delta(Q,N)\cdot\sum_{m\leqslant M}|a_m|^2\sum_{n\leqslant N}|b_n|^2\Big)^{1/2},$$

where the star means that the sum runs over all primitive characters.

Proof. Let $A(t,\chi) := \sum_{m\leqslant M}a_m\chi(m)m^{it}$, $B(t,\chi) := \sum_{n\leqslant N}b_n\chi(n)n^{it}$ and write $\|a\| := (\sum_{m\leqslant M}|a_m|^2)^{1/2}$ and $\|b\| := (\sum_{n\leqslant N}|b_n|^2)^{1/2}$. Then using Lemma 2.6 with $\gamma_m = a_m\chi(m)$, $\eta_n = b_n\chi(n)$ and summing up, we bound the left hand side of the lemma by

$$\ll \int_{-T}^{T}\sum_{\mathbf{q}\sim Q}\frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))}\sum_{\chi(P(\mathbf{q}))}^{*}|A(t,\chi)B(t,\chi)|\min(|t|^{-1},\log(2MN))dt$$
$$+\sum_{q\leqslant Q}P(\mathbf{q})MNT^{-1}\sum_{m\leqslant M,n\leqslant N}|a_mb_n|$$
$$\ll (QMN)^{\varepsilon}\Delta(Q,M)^{1/2}\Delta(Q,N)^{1/2}\|a\|\|b\|\int_{-T}^{T}\Xi(t)dt$$
$$+Q^{k+\ell}(MN)^{3/2}T^{-1}\|a\|\|b\|,$$

where Lemma 3.1 and the Cauchy–Schwarz inequality has been used in the second estimate. The assertion follows with $T = (MN)^{3/2}$. ∎

4. Proof of the polynomial Basic Mean Value Theorem

In this section, we prove the polynomial version of the Basic Mean Value Theorem using the polynomial large sieve.

Theorem 4.1 (Polynomial Basic Mean Value Theorem). *Let $Q, x > 1$, let P be a polynomial and $\sigma > 0$ as in Assumptions 2.1, and for a primitive character χ mod q we write $\psi(x,\chi) := \sum_{n\leqslant x}\chi(n)\Lambda(n)$. Then*

$$\sum_{\mathbf{q}\sim Q}\frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))}\sideset{}{^*}\sum_{\chi(P(\mathbf{q}))}\sup_{y\leqslant x}|\psi(y,\chi)| \ll (Qx)^{\varepsilon}\cdot\tilde{\Delta}(Q,x) \tag{4}$$

with

$$\tilde{\Delta}(Q,x) := Q^{\ell-\sigma}x + Q^{\ell+(k-\sigma)/2}x^{5/6} + Q^{\ell+(k-1)\sigma/2}x^{1-\sigma/6}, \qquad \text{if } \ x \geqslant Q^{2k+\sigma},$$

and

$$\tilde{\Delta}(Q,x) := Q^{\ell+5k/6-\sigma/3}x^{2/3}, \qquad \text{if } \ Q^{k+3-\sigma} \leqslant x \leqslant Q^{2k+\sigma}.$$

The second range for $x \leqslant Q^{2k+\sigma}$ is not relevant in the proof of Theorem 1.2, but the result and proof in this case is included here for completeness.

Proof. Let $y = y(\chi) \leqslant x$ be such that $|\psi(y,\chi)| = \max_{z\leqslant x}|\psi(z,\chi)|$. Let $U \geqslant 1$, $U^2 \leqslant x$. Then Vaughan's identity in the form of Lemma 2.3 yields

$$|\psi(y,\chi)| \ll U + (\log x)T_1(\chi) + T_2(\chi) + T_3(\chi),$$

where

$$T_1(\chi) = \sum_{r\leqslant U}\max_{w}\Big|\sum_{w<s\leqslant y/r}\chi(sr)\Big|,$$

with

$$T_i(\chi) = \Big|\sum_{\substack{m>U,\\ m\leqslant\max(U^2,x/U)}}\ \sum_{s\leqslant x/m} a_i(m)b_i(s)\chi(sm)\Big|, \ i = 2,3.$$

Choosing U such that it depends on Q and x only, we can sum over all primitive χ and $\mathbf{q}$. We obtain

$$\sum_{\mathbf{q}\sim Q}\frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))}\sideset{}{^*}\sum_{\chi(P(\mathbf{q}))}|\psi(y(\chi),\chi)| \ll (UQ^{\ell+k} + K_1\log x + K_2 + K_3)\log x,$$

where

$$K_j := \sum_{\mathbf{q}\sim Q}\frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))}\sideset{}{^*}\sum_{\chi(P(\mathbf{q}))}T_j(\chi), \qquad j = 1,2,3.$$

We estimate K_1 using Polya–Vinogradov's inequality Lemma 2.4 as

$$K_1 \ll U\sum_{\mathbf{q}\sim Q}P(\mathbf{q})^{3/2}\log^2 x \ll Q^{\ell+3k/2}U\log^2 x,$$

which already dominates the term $UQ^{\ell+k}\log x$ above.

We proceed to estimate $K_2 + K_3$. Let $M \leqslant x$. We will use dyadic summation over M. For arithmetic functions a, b we consider the expression

$$K_M := \sum_{\mathbf{q}\sim Q} \frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))} \sideset{}{^*}\sum_{\chi(P(\mathbf{q}))} \Big| \sum_{m\sim M} \sum_{s\leqslant x/m} a(m)b(s)\chi(sm)\Big|.$$

Writing the conditions of summation over s as $s \leqslant x/M$, $ms \leqslant x$, we apply the bilinear inequality of Lemma 3.2 (choosing $a(m) = 0$ for $m \leqslant M$) which yields

$$K_M \ll (Qx)^{\varepsilon}\Big(\Delta(Q,M)\Delta(Q,x/M) \sum_{m\sim M} |a(m)|^2 \sum_{s\leqslant x/M} |b(s)|^2\Big)^{1/2}.$$

Now use $\sum_{m\leqslant 2M} |a(m)|^2 \ll M(\log M)^2$, $\sum_{s\leqslant z} |b(s)|^2 \ll z(\log z)^3$: this yields

$$K_M \ll x^{1/2+\varepsilon}\Delta(Q,M)^{1/2}\Delta(Q,x/M)^{1/2} \text{ for } M \leqslant x,$$

hence

$$\begin{aligned} K_M &\ll x^{1/2+\varepsilon}(Q^{\ell+k} + Q^{\ell-\sigma}M + Q^{\ell+k\sigma}M^{1-\sigma})^{1/2} \\ &\quad \times (Q^{\ell+k} + Q^{\ell-\sigma}xM^{-1} + Q^{\ell+k\sigma}(x/M)^{1-\sigma})^{1/2} \\ &\ll x^{1/2+\varepsilon}(Q^{2\ell+2k} + Q^{2\ell+k-\sigma}xM^{-1} + Q^{2\ell+k+k\sigma}(x/M)^{1-\sigma} \\ &\quad + Q^{2\ell+k-\sigma}M + Q^{2\ell-2\sigma}x + Q^{2\ell+(k-1)\sigma}x^{1-\sigma}M^{\sigma} \\ &\quad + Q^{2\ell+k+k\sigma}M^{1-\sigma} + Q^{2\ell+(k-1)\sigma}xM^{-\sigma} + Q^{2\ell+2k\sigma}x^{1-\sigma})^{1/2}. \end{aligned}$$

Now the dyadic summation for $M = 2^{\nu}U$, $M \leqslant W \leqslant x$, with $\nu = 0, 1, 2, \ldots$ yields

$$\begin{aligned} &\sum_{\mathbf{q}\sim Q} \frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))} \sideset{}{^*}\sum_{\chi(P(\mathbf{q}))} \Big| \sum_{U<m\leqslant W} \sum_{s\leqslant x/m} a(m)b(s)\chi(sm)\Big| \\ &\qquad \ll x^{1/2+\varepsilon}(Q^{2\ell+2k} + Q^{2\ell+k-\sigma}xU^{-1} + Q^{2\ell+k+k\sigma}(x/U)^{1-\sigma} \\ &\qquad\quad + Q^{2\ell+k-\sigma}W + Q^{2\ell-2\sigma}x + Q^{2\ell+(k-1)\sigma}x^{1-\sigma}W^{\sigma} \\ &\qquad\quad + Q^{2\ell+k+k\sigma}W^{1-\sigma} + Q^{2\ell+(k-1)\sigma}xU^{-\sigma} + Q^{2\ell+2k\sigma}x^{1-\sigma})^{1/2}. \end{aligned}$$

Choosing $W = \max(U^2, x/U)$, $a = a_i$, $b = b_i$ for $i = 2, 3$, we bound K_2 and K_3 by

$$\begin{aligned} K_2 + K_3 &\ll x^{1/2+\varepsilon}(Q^{2\ell+2k} + Q^{2\ell-2\sigma}x + Q^{2\ell+2k\sigma}x^{1-\sigma} \\ &\quad + Q^{2\ell+k-\sigma}xU^{-1} + Q^{2\ell+k+k\sigma}(x/U)^{1-\sigma} + Q^{2\ell+(k-1)\sigma}xU^{-\sigma} \\ &\quad + Q^{2\ell+k-\sigma}U^2 + Q^{2\ell+k+k\sigma}U^{2(1-\sigma)} + Q^{2\ell+(k-1)\sigma}x^{1-\sigma}U^{2\sigma})^{1/2}. \end{aligned}$$

Together with $K_1 \ll x^{\varepsilon}Q^{\ell+3k/2}U$, we optimize the terms depending on the two ranges $Q \ll x^{1/(2k+\sigma)}$ and $x^{1/2k+\sigma} \ll Q \ll x^{1/(k+3-\sigma)}$ by choosing U suitably to obtain the bounds stated in the theorem.

First range: $Q^{2k+\sigma} \leqslant x$. In that case, we choose $U = x^{1/3}$ so that $U^2 = x/U$, this yields

$$K_2 + K_3 \ll x^{\varepsilon}(Q^{\ell+k}x^{1/2} + Q^{\ell-\sigma}x + Q^{\ell+k\sigma}x^{1-\sigma/2} + Q^{\ell+(k-\sigma)/2}x^{5/6} + Q^{\ell+k/2+k\sigma/2}x^{5/6-\sigma/3} + Q^{\ell+(k-1)\sigma/2}x^{1-\sigma/6}),$$

and this also bounds K_1 since $K_1 \ll x^{\varepsilon}Q^{\ell+3k/2}x^{1/3} \ll Q^{\ell+k/2-\sigma/2}x^{5/6}$ holds in the assumed first range. Further, in this bound for $K_2 + K_3$, we can leave out the first, third and fifth summand since a simple calculation shows that they are dominated by the fourth and sixth.

So, in the assumed range, we obtain

$$K_2 + K_3 \ll x^{\varepsilon}(Q^{\ell-\sigma}x + Q^{\ell+k/2-\sigma/2}x^{5/6} + Q^{\ell+(k-1)\sigma/2}x^{1-\sigma/6}).$$

Second range: $Q^{k+3-\sigma} \leqslant x \leqslant Q^{2k+\sigma}$. There, we choose $U = x^{2/3}Q^{-B}$ with $B = (\sigma + 2k)/3$. Hence

$$\begin{aligned} K_2 + K_3 \ll x^{\varepsilon}(&Q^{\ell+k}x^{1/2} + Q^{\ell-\sigma}x + Q^{\ell+k\sigma}x^{1-\sigma/2} \\ &+ Q^{\ell+(k-\sigma)/2}x^{2/3}Q^{B/2} + Q^{\ell+k/2+k\sigma/2}x^{2/3-\sigma/6}Q^{B(1-\sigma)/2} \\ &+ Q^{\ell+(k-1)\sigma/2}x^{1-\sigma/3}Q^{B\sigma/2}). \end{aligned}$$

Now the dominating summand in this bound is $Q^{\ell+(k-\sigma)/2+B/2}x^{2/3}$ within this range, and it also dominates the bound for K_1.

This shows the theorem. ∎

5. Proof of Theorem 1.2

Before starting with the proof of Theorem 1.2, we deduce an auxiliary result from the previous sections.

Lemma 5.1. *For a polynomial P as in Assumptions 2.1 of degree k in ℓ variables we have*

$$E := Q^{-\ell} \sum_{\mathbf{q} \sim Q} \frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))} \sum_{\chi_1 (P(\mathbf{q}))}^{*} \sup_{y \leqslant x} |\psi(x, \chi_1)| \ll x^{1-\delta}$$

for any small value $\delta > 0$, assuming that $x^{\varepsilon/\sigma} \ll Q \leqslant x^{(1/3-2\varepsilon)/(k-\sigma)}$ for any fixed $\varepsilon > \delta$.

Proof. Theorem 4.1 yields the bound $E \ll Q^{-\ell}x^{\varepsilon}\tilde{\Delta}(Q, x)$ with

$$\tilde{\Delta}(Q, x) := Q^{\ell-\sigma}x + Q^{\ell+(k-\sigma)/2}x^{5/6} + Q^{\ell+(k-1)\sigma/2}x^{1-\sigma/6}$$

assuming that $Q \leqslant x^{1/(2k+\sigma)}$: hence

$$E \ll x^{\varepsilon}(Q^{-\sigma}x + Q^{(k-\sigma)/2}x^{5/6} + Q^{(k-1)\sigma/2}x^{1-\sigma/6}) \ll x^{1-\delta}$$

holds in the range $x^{(\varepsilon+\delta)/\sigma} \ll Q \leqslant x^{(1/3-2(\varepsilon+\delta))/(k-\sigma)}$ for Q. Now replace $\varepsilon + \delta$ by $\varepsilon > \delta$ in the upper and lower bound. ∎

Now we give the main proof.

Proof of Theorem 1.2. Let P be the polynomial of degree $2k$ as in the statement and $\sigma = 1/(4rk)$ with $r = \binom{2k+\ell-1}{\ell} - 1$, $\varepsilon' = 2\varepsilon/(2k-\sigma)$.

Let $Q, x > 1$, and for a character $\chi \bmod P(\mathbf{q})$, we set $\psi'(x,\chi) := \psi(x,\chi)$ if χ is different from the principal character χ_0, and $\psi'(x,\chi_0) := \psi(x,\chi_0) - x$ otherwise. So for $y \leqslant x$ we have

$$E(y; P(\mathbf{q}), a) = \psi(y; P(\mathbf{q}), a) - \frac{y}{\varphi(P(\mathbf{q}))} = \frac{1}{\varphi(P(\mathbf{q}))} \sum_{\chi(P(\mathbf{q}))} \overline{\chi}(a)\psi'(y,\chi),$$

and hence

$$\max_{\substack{a \bmod P(\mathbf{q}) \\ \gcd(a,P(\mathbf{q}))=1}} |E(y; P(\mathbf{q}), a)| \leqslant \frac{1}{\varphi(P(\mathbf{q}))} \sum_{\chi(P(\mathbf{q}))} |\psi'(y; P(\mathbf{q}), a)|.$$

If χ is induced by the primitive character χ_1 modulo d with $d \mid P(\mathbf{q})$, then $\psi(y,\chi) - \psi'(y,\chi_1) \ll (\log(yP(\mathbf{q})))^2$. Thus

$$\max_{\substack{a \bmod P(\mathbf{q}) \\ \gcd(a,P(\mathbf{q}))=1}} |E(y; P(\mathbf{q}), a)| \ll \frac{1}{\varphi(P(\mathbf{q}))} \sum_{\substack{\chi(P(\mathbf{q})) \\ \text{ind. of } \chi_1 \\ \bmod d \mid P(\mathbf{q})}} |\psi'(y,\chi_1)| + (\log x)^2,$$

and so

$$\sum_{\mathbf{q}\sim Q} G_{\mathbf{q}} \frac{\varphi(P(\mathbf{q}))}{Q^\ell} \sup_{y\leqslant x} \max_{\substack{a \bmod P(\mathbf{q}) \\ \gcd(a,P(\mathbf{q}))=1}} |E(y; P(\mathbf{q}), a)|$$
$$\ll \sum_{\mathbf{q}\sim Q} \frac{G_{\mathbf{q}}}{Q^\ell} \sum_{\substack{\chi(P(\mathbf{q})) \\ \text{ind. of } \chi_1 \\ \bmod d \mid P(\mathbf{q})}} \sup_{y\leqslant x} |\psi'(y,\chi_1)| + Q^{2k}(\log x)^{2+k},$$

where the term $Q^{2k}(\log x)^{2+k}$ is clearly admissible in the considered Q-range, since there, $Q \ll x^{1/4k}$.

Now due to the assigned weight $G_{\mathbf{q}}$, each $P(\mathbf{q})$ is squarefree, so $\mathbf{q}$ is so that each $q_{u(i)}^2 + q_{v(i)}^2 = p_i$ is a prime, $1 \leqslant i \leqslant k$, and these primes are pairwise different. Hence, for a divisor d of $P(\mathbf{q})$, we have $d = 1$ or $d = \tilde{P}(\mathbf{q})$ for a polynomial $\tilde{P}$ that divides P which is of a similar shape as P itself. We split the sum over χ according to these two cases.

In the first case, when $d = 1$, we have $\chi_1 \equiv 1$ (the constant 1 character) and $\chi = \chi_0 \bmod P(\mathbf{q})$ is unique, hence

$$\sum_{\mathbf{q}\sim Q} \frac{G_{\mathbf{q}}}{Q^\ell} \sup_{y\leqslant x} |\psi(y,\chi_0) - y| \ll x(\log x)^{-A}$$

for any $A > 0$ by the prime number theorem.

In the second case, we obtain the expression

$$\sum_{1<d\leqslant P(\mathbf{q})} \sum_{\substack{\mathbf{q}\sim Q\\ d\mid P(\mathbf{q})}} \frac{G_{\mathbf{q}}}{Q^\ell} \sideset{}{^*}\sum_{\chi_1(d)} \sup_{y\leqslant x} |\psi'(y,\chi_1)| \ \ll \ \sum_{\tilde P\mid P} \sum_{\mathbf{q}\sim Q} \frac{G_{\mathbf{q}}}{Q^\ell} \sideset{}{^*}\sum_{\chi_1(\tilde P(\mathbf{q}))} \sup_{y\leqslant x} |\psi'(y,\chi_1)|.$$

Now for every $\tilde P$, we apply Lemma 5.1 and together with the trivial observation $\#\{\mathbf{q}\sim Q\}\ll Q^\ell$, we bound this expression by

$$\ll \sum_{\tilde P\mid P} x^{1-\delta}(\log x)^{k+1},$$

which holds for $x^{\varepsilon/\sigma}\ll Q\ll x^{(1/3-2\varepsilon)/(2k-\sigma)}$ and $\varepsilon>\delta>0$. We used that the exponents $(1/3-2\varepsilon)/(2k(\tilde P)-\sigma(\tilde P))$ are all $\geqslant (1/3-2\varepsilon)/(2k-\sigma)$, since for $\tilde P\mid P$ with $\tilde P\neq P$, we have $\deg\tilde P\leqslant \deg P-2$. This yields the desired estimate of the theorem since there are only $\ll_k 1$ many divisor polynomials of P in $\mathbb{Z}[\mathbf{x}]$. ■

6. Proof of Theorem 1.4

The proof depends on the following result of Fouvry and Iwaniec in [6].

Theorem 6.1 (Fouvry and Iwaniec). *Let (λ_ℓ) be a complex sequence with $|\lambda_\ell|\leqslant 1$. Then, if $A,x>1$, we have*

$$\sum_{\ell^2+m^2\leqslant x} \lambda_\ell \Lambda(\ell^2+m^2) = \sum_{\ell^2+m^2\leqslant x} \lambda_\ell \frac{4c}{\pi}\theta(\ell) + O_A\Big(\frac{x}{(\log x)^A}\Big)$$

with $\theta(\ell):=\prod_{p\mid\ell}(1-\chi(p)/(p-1))^{-1}$ and $c:=\prod_p(1-\frac{\chi(p)}{(p-1)(p-\chi(p))})$.

Note that $\theta(\ell)\geqslant\varphi(\ell)/\ell\gg 1/(\log\log\ell)$ holds.

Using this theorem, the proof of Theorem 1.4 can be worked out by induction on k.

Proof of Theorem 1.4. It suffices to prove Theorem 1.4 without the factor $\mu^2(P(\mathbf{q}))$, that is

$$\sum_{\mathbf{q}\sim Q} \Lambda(q_{u(1)}^2+q_{v(1)}^2)\cdots\Lambda(q_{u(k)}^2+q_{v(k)}^2) \gg \frac{Q^\ell}{(\log Q)^C} \tag{5}$$

for some constant $C>0$, what can be seen as follows: In the difference of the left hand sides, at least one of the Λ-arguments must be a prime power, say, that this is in the i-th Λ-factor. Let $\mathbf{q}'$ denote the $(\ell-2)$-tuple obtained from $\mathbf{q}$ by deleting the coordinates with $u(i)$ and $v(i)$. Then the deviation can be bounded by

$$\sum_{\substack{m\leqslant 8Q^2\\ m=p^k\\ k\geqslant 2}} \Lambda(m) \sum_{\substack{q_{u(i)},q_{v(i)}\sim Q\\ q_{u(i)}^2+q_{v(i)}^2=m}} \sum_{\mathbf{q}'\sim Q} \prod_{\substack{j=1\\ j\neq i}}^{k} \Lambda(q_{u(j)}^2+q_{v(j)}^2) \ll Q\log Q\cdot Q^{\ell-2}(\log Q)^{k-1},$$

what is admissible for the desired lower bound of the theorem.

Now we give the proof of (5) by induction. Let $k = 1$: then we have to show that

$$\sum_{q_1,q_2\sim Q} \Lambda(q_1^2+q_2^2) \gg \frac{Q^2}{(\log Q)^C}$$

holds for a constant $C > 0$. A simple geometric argument shows that

$$\sum_{q_1,q_2\sim Q} \Lambda(q_1^2+q_2^2) = \sum_{2Q^2<q_1^2+q_2^2\leqslant 8Q^2} \Lambda(q_1^2+q_2^2) - 2 \sum_{\substack{2Q^2<q_1^2+q_2^2\leqslant 8Q^2\\ q_1>2Q}} \Lambda(q_1^2+q_2^2)$$
$$- 2\left(\sum_{\substack{2Q^2<q_1^2+q_2^2\leqslant 5Q^2\\ q_1\leqslant Q}} \Lambda(q_1^2+q_2^2) - \sum_{\substack{2Q^2<q_1^2+q_2^2\leqslant 5Q^2\\ q_1\geqslant 2Q}} \Lambda(q_1^2+q_2^2) \right).$$

Each sum is of the form $\sum_{y<q_1^2+q_2^2\leqslant x} \lambda_{q_1}\Lambda(q_1^2+q_2^2)$ where λ_{q_1} is the characteristic function of the conditions on q_1. Hence, to each sum, Theorem 6.1 applies giving

$$\sum_{y<q_1^2+q_2^2\leqslant x} \lambda_{q_1} \frac{4c}{\pi}\theta(q_1) + O_A\Big(\frac{Q^2}{(\log Q)^A}\Big),$$

and the main terms combine again. In such a way, we obtain

$$\sum_{q_1,q_2\sim Q} \Lambda(q_1^2+q_2^2) = \sum_{q_1,q_2\sim Q} \frac{4c}{\pi}\theta(q_1) + O_A\Big(\frac{Q^2}{(\log Q)^A}\Big)$$
$$\gg \sum_{q_1,q_2\sim Q} \frac{1}{\log\log q_1} + O_A\Big(\frac{Q^2}{(\log Q)^A}\Big) \gg \frac{Q^2}{\log Q},$$

fixing $A > 1$ in the last step.

Now let $k \geqslant 2$ and assume that estimate (5) holds for $k-1$: we proceed to show it for k. Surely, $\ell \geqslant 2$, and we divide the left hand side in (5) by $(\log Q)^{k-1}Q^{\ell-2}$ and obtain

$$\sum_{\mathbf{q}\sim Q} (\log Q)^{1-k}Q^{2-\ell}\Big(\prod_{i=2}^{k} \Lambda(q_{u(i)}^2+q_{v(i)}^2)\Big)\Lambda(q_{u(1)}^2+q_{v(1)}^2).$$

Let $\mathbf{q}'$ be obtained from $\mathbf{q}$ by deleting the coordinates with index $u(1)$ and $v(1)$. By assumption, one of the indices $u(1)$ and $v(1)$ does not occur in $\{u(2),\dots,u(k), v(2),\dots,v(k)\}$, assume w.l.o.g. that this is $u(1)$. Then the considered sum transforms into

$$\sum_{q_{u(1)},q_{v(1)}\sim Q} \lambda_{q_{v(1)}}\Lambda(q_{u(1)}^2+q_{v(1)}^2)$$

with

$$\lambda_{q_{v(1)}} := (\log(8Q^2))^{1-k} Q^{2-\ell} \sum_{\mathbf{q}' \sim Q} \prod_{i=2}^{k} \Lambda(q_{u(i)}^2 + q_{v(i)}^2) \leqslant 1,$$

which does not depend on $u(1)$. By induction hypothesis, we have

$$\sum_{q_{v(1)} \sim Q} \lambda_{q_{v(1)}} \gg (\log Q)^{1-k} Q^{2-\ell} \frac{Q^{\ell-1}}{(\log Q)^C} = Q(\log Q)^{1-k-C} \tag{6}$$

for some constant $C > 0$.

We apply Theorem 6.1 similarly to the case $k = 1$, which yields

$$\begin{aligned}
&\sum_{q_{u(1)}, q_{v(1)} \sim Q} \lambda_{q_{v(1)}} \Lambda(q_{u(1)}^2 + q_{v(1)}^2) \\
&\qquad \geqslant \sum_{\substack{13Q^2/4 < q_{u(1)}^2 + q_{v(1)}^2 \leqslant 5Q^2 \\ Q < q_{v(1)} \leqslant 3Q/2}} \lambda_{q_{v(1)}} \Lambda(q_{u(1)}^2 + q_{v(1)}^2) \\
&\qquad = \sum_{\substack{13Q^2/4 < q_{u(1)}^2 + q_{v(1)}^2 \leqslant 5Q^2 \\ Q < q_{v(1)} \leqslant 3Q/2}} \lambda_{q_{v(1)}} \frac{4c}{\pi} \theta(q_{v(1)}) + O_A\Big(\frac{Q^2}{(\log Q)^A}\Big) \\
&\qquad \gg \sum_{\substack{13Q^2/4 < q_{u(1)}^2 + q_{v(1)}^2 \leqslant 5Q^2 \\ Q < q_{v(1)} \leqslant 3Q/2}} \frac{\lambda_{q_{v(1)}}}{\log\log q_{v(1)}} + O_A\Big(\frac{Q^2}{(\log Q)^A}\Big) \\
&\qquad \gg \frac{Q^2}{(\log Q)^{C'}}
\end{aligned}$$

for a constant $C' > 0$ and a $A > 1$ chosen large enough, where we used (6) in the last estimate (adjusted to an appropriate scaled box that is contained in the considered region). This concludes the proof of (5) and therefore of Theorem 1.4. ∎

References

[1] R.C. Baker, *Primes in arithmetic progressions to spaced moduli*, Acta Arith. **153** (2012), no. 2, 133–159.

[2] E. Bombieri, *On the large sieve*, Mathematika **12**, 201–225.

[3] J. Brüdern, *Einführung in die analytische Zahlentheorie*, Springer Lehrbuch, 1995.

[4] P.D.T.A. Elliott, *Primes in short arithmetic progressions with rapidly increasing differences*, Trans. Amer. Math. Soc. **353** (2001), no. 7, 2705–2724.

[5] P.D.T.A. Elliott and H. Halberstam, *A conjecture in prime number theory*, in Symposia Mathematica, Vol. IV (INDAM, Rome, 1968/69), pages 59–72, Academic Press, London, 1970.

[6] E. Fouvry and H. Iwaniec, *Gaussian primes*, Acta Arith. **79** (1997), no. 3, 249–287.

[7] K. Halupczok, *Large sieve inequalities with general polynomial moduli*, Q. J. Math **66** (2015), no. 2, 529–545.

[8] H. Mikawa and T.P. Peneva, *Primes in arithmetic progressions to spaced moduli*, Arch. Math. (Basel) **84** (2005), no. 3, 239–248.

[9] S.T. Parsell, S.M. Prendiville and T.D. Wooley, *Near-optimal mean value estimates for multidimensional Weyl sums*, Geom. Funct. Anal. **23** (2013), no. 6, 1962–2024.

[10] R.C. Vaughan, *The Bombieri–Vinogradov Theorem*, AIM discussion paper, November 2005, available at http://www.personal.psu.edu/rcv4/Bombieri.pdf

[11] A.I. Vinogradov, *On the density hypothesis for Dirichlet L-series*, Izv. Akad. Nauk SSSR, Ser. Mat. **29** (1965), 903–934.

[12] A.I. Vinogradov, *Corrections to the work of A. I. Vinogradov 'On the density hypothesis for Dirichlet L–series'*, Izv. Akad. Nauk SSSR, Ser. Mat. **30**, 719–729.

[13] Y. Zhang, *Bounded gaps between primes*, Ann. Math. (2) **179** (2014), no. 3, 1121–1174.

Address: Karin Halupczok: Mathematisches Institut, WWU Münster, Einsteinstraße 62, D-48149 Münster, Germany.

E-mail: karin.halupczok@uni-muenster.de

Received: 24 April 2015; **revised:** 25 July 2016