INTERSECTIVE POLYNOMIALS AND DIOPHANTINE APPROXIMATION

THÁI HOÀNG LÊ AND CRAIG V. SPENCER

Abstract. We extend results on Diophantine approximation modulo 1 to intersective polynomials, and by applying Schmidt's lattice method, we obtain results on simultaneous Diophantine approximation modulo 1 for systems of jointly intersective polynomials. We also study prime analogues of these topics.

1. Introduction

In 1927, Vinogradov [21] proved the following result, confirming a conjecture of Hardy and Littlewood [8].

Theorem 1. *For every positive integer k, there exists an exponent $\theta_k > 0$ such that*

$$\min_{1\leq n\leq N} \|\alpha n^k\| \ll_k N^{-\theta_k}$$

for any positive integer N and real number α, where $\|\cdot\|$ denotes the distance to the nearest integer.

Vinogradov showed that one could take $\theta_k = \frac{k}{k2^{k-1}+1} - \epsilon$ for any $\epsilon > 0$. In particular one can take $\theta_2 = 2/5 - \epsilon$. Heilbronn [11] improved this to $\theta_2 = 1/2 - \epsilon$. The best result to date is due to Zaharescu [25], who showed we can take $\theta_2 = 4/7 - \epsilon$, though his method is not applicable to higher powers. It is an open conjecture that we can choose θ_2 (and more generally, θ_k) to be $1 - \epsilon$.

Natural generalizations of Vinogradov's result have been made. Davenport [7] obtained an analog of Theorem 1 when αn^k is replaced by a polynomial $f(n)$ of degree k without constant term (the corresponding bound being uniform in the coefficients of f and depending only on k). Danicic [6] was the first to address the question of simultaneous approximation. He showed that

$$\min_{1\leq n\leq N} \max(\|\alpha n^2\|, \|\beta n^2\|) \ll N^{-1/9+\epsilon},$$

uniformly in N, α and β. This was generalized by Cook [5] to a system of polynomials without constant terms.

Theorem 2. *There is an exponent $\theta = \theta(k,l) > 0$ such that whenever $f_1, \dots, f_l \in \mathbf{R}[x]$ are polynomials without constant terms of degree at most k, we have*

$$\min_{1\leq n\leq N} \max_{1\leq j\leq l} \|f_j(n)\| \ll N^{-\theta}$$

for every positive integer N.

The research of the second author is supported in part by NSA Young Investigators Grants #H98230-10-1-0155 and #H98230-12-1-0220.

This problem was also addressed by Schmidt in [17]. Though he only worked with quadratic polynomials, his methods provided a very general framework for this type of problem, which we utilize in this paper.

Conjecturally, $\theta(k,l) = 1/l - \epsilon$, but again this is wide open. On the quantitative side, quite a lot of effort has been put into obtaining explicit and optimal values of θ under different circumstances. There are various bounds for θ of different qualities, depending on extra conditions imposed on the system $f_1, \dots, f_l$ (e.g., when each f_i is a monomial, or when k or l is in a certain range). We refer the reader to Baker's book [1] which discusses in depth techniques and results for this kind of problem. Notably, when $l = 1$, the best bound is due to Wooley, who showed that we can choose $\theta_k = \frac{1}{4k(k-2)} - \epsilon$ for $k \geq 4$, as a consequence of his recent breakthrough [22, 23] on Vinogradov's mean value theorem.

In contrast, the emphasis in this paper will be put on the qualitative side. We are interested in generalizing Theorems 1 and 2. For instance, can we replace n^k in Theorem 1 with a polynomial $h \in \mathbf{Z}[x]$? That is, for which polynomials $h \in \mathbf{Z}[x]$ do we have

$$\min_{1\leq n\leq N} \|\alpha h(n)\| \ll_h N^{-\theta}$$

for some $\theta = \theta(h)$, uniformly in α and N? By Theorem 2, this is the case if h is without constant term, but apparently these are not all the polynomials enjoying this property. By considering $\alpha = 1/q$, we see that in order for such a bound to exist, h must have a root modulo q for every $q \in \mathbf{Z}^+$. It turns out that this condition is also sufficient. We will prove the following theorem.

Theorem 3. *Let h be a polynomial with the property that for every $q \neq 0$, there exists an $n \in \mathbf{Z}$ such that $h(n) \equiv 0 \pmod q$. Then there is an exponent $\theta > 0$ depending only on the degree of h such that*

$$\min_{1\leq n\leq N} \|\alpha h(n)\| \ll_h N^{-\theta}$$

for any positive integer N and real number α.

In the same spirit, we come up with the following generalization of Theorem 2 under a similar hypothesis.

Theorem 4. *Let l be a positive integer and $h_1, h_2, \dots, h_k$ be polynomials of distinct degree satisfying the following property: if $f_i = \sum_{j=1}^k c_{ij} h_j$ for $i = 1, \dots, l$ are any l linear combinations of $h_1, \dots, h_k$ with coefficients $c_{ij} \in \mathbf{Z}$, and q is any non-zero integer, there exists $n \in \mathbf{Z}$ such that $f_i(n) \equiv 0 \pmod q$ for every $i = 1, \dots, l$. Then there is an exponent $\theta > 0$ depending only on l and the polynomials h_i such that the following holds. Let A be an arbitrary $l \times k$ matrix with real entries. Write $A \begin{pmatrix} h_1(n) \\ \vdots \\ h_k(n) \end{pmatrix} = \begin{pmatrix} v_1(n) \\ \vdots \\ v_l(n) \end{pmatrix}$. Then*

$$\min_{1\leq n\leq N} \max_{1\leq i\leq l} \|v_i(n)\| \ll_{h_1,\dots,h_k} N^{-\theta},$$

where the bound is uniform in N and A.

Remark 1.1.

- Theorem 2 is a special case of Theorem 4 when $h_i = x^i$ for all $i = 1, \dots, k$.

- One can see that θ depends at most on k, l and $\max\limits_{1\leq i\leq k} \deg h_i$, but not on the coefficients of h_i.
- The divisibility condition on the polynomials $h_1, h_2, \dots, h_k$ is necessary. This can be seen by taking A to be $\frac{1}{q}$ times an integral $l \times k$ matrix.
- The dependency of the implied constants in Theorem 3 and 4 on h and $h_1, \dots, h_k$ is necessary. For example, in Theorem 3, consider the case when $h(n) = (n + M)^k$ and $\alpha = \frac{1}{2M^k}$. By taking M large compared to N, we can ensure that $\min\limits_{1\leq n\leq N} \|\alpha h(n)\|$ is greater than $\frac{1}{3}$.
- The assumption that $h_1, \dots, h_k$ are of distinct degree is by no means necessary. This assumption makes the details of the proof easier. In the general case, any family of polynomials can be reduced to a family of polynomials of distinct degree by applying a suitable linear transform.

Polynomials h satisfying the hypothesis of Theorem 3 are known as *intersective polynomials* in the literature. If a polynomial has an integer root, then it is necessarily intersective, but there are examples of intersective polynomials without rational roots, such as $(x^3 - 19)(x^2 + x + 1)$ [2]. A system of polynomials $(h_1, \dots, h_k)$ is called *jointly intersective* if for every $q \neq 0$, there exists an $n \in \mathbf{Z}$ such that $h_i(n) \equiv 0 \pmod q$ for $i = 1, \dots, k$.[1] Thus the condition in Theorem 4 says that any l linear combinations with integral coefficients of $h_1, \dots, h_k$ are jointly intersective. This is quite a strong requirement. It turns out (Proposition 1) that if $l \geq 2$, then this condition implies that $h_1, \dots, h_k$ are jointly intersective themselves, but this is not necessary in the case $l = 1$.

The notions of intersective polynomials and jointly intersective polynomials also come up naturally when studying related problems in combinatorial number theory. Let $h, h_1, \dots, h_k \in \mathbf{Z}[x]$ be polynomials. It follows from the work of Kamae and Mendès France [12] that configurations $\{a, a + h(n)\}$ exist in any set of positive relative density[2] A if and only if h is intersective. Bergelson, Leibman, and Lesigne proved in [4] that configurations $\{a + h_1(n), a + h_2(n), \dots, a + h_k(n)\}$ exist in any set of positive relative density if and only if $h_1, \dots, h_k$ are jointly intersective. For any $\alpha_1, \dots, \alpha_k$ and $\epsilon > 0$, the Bohr set $B(\alpha_1, \dots, \alpha_k; \epsilon) = \{m \in \mathbf{Z} : \|\alpha_i m\| < \epsilon \text{ for all } i = 1, \dots, k\}$ is a set of positive relative density, and Theorem 4 implies that configurations $\{a + h_1(n), a + h_2(n), \dots, a + h_k(n)\}$ can be found in such sets. Thus Theorem 4 may be regarded as a qualitative step towards the Bergelson-Leibman-Lesigne theorem. Obtaining a bound for the Bergelson-Leibman-Lesigne theorem in the general case is a very difficult problem.

We note that the techniques used to prove Theorem 1 can be adapted to study the set $\{p - 1 : p \text{ prime}\}$ in place of $\{n^k\}$. One has a corresponding bound

$$\min_{\substack{1\leq p\leq N \\ p \text{ prime}}} \|\alpha(p-1)\| \ll N^{-\theta},$$

[1] In the journal version of this paper, the definition of joint intersectivity is not correctly stated.

[2] That is, $\overline{\lim\limits_{N\to\infty}} \dfrac{|A \cap \{1, \dots, N\}|}{N} > 0$.

uniformly in α and N, for some exponent $\theta > 0$. Curiously enough, this doesn't seem to have been observed before in the literature. Slijepcevic [18] obtained a weaker bound

$$\min_{\substack{1\le p\le N\\ p \text{ prime}}} \|\alpha(p-1)\| \ll (\log N)^{-1+o(1)}$$

as a consequence of his construction of special trigonometric polynomials (the "van der Corput" property of the set $\{p-1\}$). We prove a generalization of this fact, which is similar to Theorem 3.

Theorem 5. *Let h be a polynomial with the property that for every $q \neq 0$, there is an $n \in \mathbf{Z}$ such that $h(n) \equiv 0 \pmod q$ and furthermore q is coprime to n. Then there is an exponent $\theta > 0$, depending only on the degree of h, such that*

$$\min_{\substack{1\le p\le N\\ p \text{ prime}}} \|\alpha h(p)\| \ll N^{-\theta}$$

for any positive integer N and real number α.

Again, the condition on h is easily seen to be necessary. In [13], we call such polynomials *intersective of the second kind.* Examples of intersective polynomials of the second kind include $p-1, (p-3)(p-5)$, and it is interesting to give examples of intersective polynomials of the second kind without rational roots. Note that much work has been done to show that Diophantine inequalities of the form

$$\left\|\eta + \sum_{i=1}^{s} \nu_i p_i^k\right\| < (\max p_i)^{-\sigma} \quad \text{or} \quad \|\eta + \nu p^k\| < p^{-\sigma}$$

have infinitely many solutions, where the variables p_i and p are prime. See, for example, [9, 20]. However, the techniques used when studying such problems frequently have implicit constants depending on the constants η, ν, and ν_i.

A prime analog of Theorem 4 should certainly exist, and we will return to this topic in a future paper. It follows from the work of Vinogradov that if we have a large exponential sum $\sum_{n=1}^{N} e(f(n))$, where $e(x) = e^{2\pi i x}$ and $f \in \mathbf{R}[x]$, then there is a good simultaneous approximation to all the coefficients of f (except the constant term). This is one of the main ingredients of the proof of Theorem 4. In order to have a prime analog of Theorem 4, we need a similar result for exponential sums over primes, e.g.

$$\sum_{\substack{1\le p\le N\\ p \text{ prime}}} (\log p)\, e(f(p)).$$

Such a result is plausible, but not explicitly available in the literature. However, we do have an approximation to the leading coefficient of f, and this enables us to prove Theorem 5.

In the proofs of our results, we do not obtain the best exponents possible with the given methods. On the one hand, this gives a clean exposition of the methods used. The proof of Theorem 4 gives a bound $\theta \le C_{h_1,\dots,h_k}^{-l}$, and there are reasons to expect that it may be very hard to obtain bounds for θ in the general case that are of the same quality as the special case $h_i(x) = x^i$. Indeed, suppose that h is a polynomial of degree k and that we want to find n such that $h(n)$ is divisible by a modulus q^k (which naturally occurs when we look at the values of h along a congruence class modulo q). If $h(x) = x^k$, then we can simply choose n to be a multiple of q. However, if h is a general intersective polynomial, we are only guaranteed to find an n in a congruence class modulo q^k.

The structure of the paper is as follows: In Section 2, we gather some general facts, especially on intersective polynomials. In Section 3, we prove Theorems 3 and 5. While Theorem 3 is superseded by the one-dimensional version of Theorem 4 (Theorem 6), we provide the relatively short proof since it demonstrates some themes that occur in the proof of Theorem 4. Theorem 4 is proved in Section 5 by induction on the dimension, and the base case is proved in Section 4.

Acknowledgement. We would like to thank the referee for detailed comments which helped improve the presentation of the paper.

2. Preliminaries

2.1. **On intersective polynomials.** A polynomial $h \in \mathbf{Z}[x]$ is intersective if and only if it has a root in $\mathbf{Z}_p$ for any prime p, where $\mathbf{Z}_p$ is the ring of p-adic integers. We can fix, for each $d \in \mathbf{Z}^+$, an integer $-d < r_d \leq 0$ such that $h(n) \equiv 0 \pmod{d}$ whenever $n \equiv r_d \pmod{d}$. Moreover, $r_{dq} \equiv r_d \pmod{d}$ for any $d, q \in \mathbf{Z}^+$ (see [16, p. 82]).

By [4, Proposition 6.1], polynomials $h_1, \dots, h_k \in \mathbf{Z}[x]$ are jointly intersective if and only if they are all multiples of an intersective polynomial $h \in \mathbf{Z}[x]$. Thus $h_1, \dots, h_k \in \mathbf{Z}[x]$ are jointly intersective if and only if they have a common root in $\mathbf{Z}_p$ for any prime p. Also, corresponding to any system of jointly intersective polynomial $(h_1, \dots, h_k)$, we can associate a sequence $(r_d)_{d \in \mathbf{Z}^+}$ such that

$$-d < r_d \leq 0,\ r_{dq} \equiv r_d \pmod{d} \text{ for any } d, q \in \mathbf{Z}^+, \text{ and } h_i(n) \equiv 0 \pmod{d} \text{ for all } i = 1, \dots, k. \tag{1}$$

We now turn to the claim made in the introduction regarding the condition in Theorem 4.

Proposition 1. *Let $h_1, \dots, h_k \in \mathbf{Z}[x]$ be polynomials such that any two linear combinations of $h_1, \dots, h_k$ with coefficients in $\mathbf{Z}$ are jointly intersective. Then $h_1, \dots, h_k$ are jointly intersective themselves.*

Proof. Let us induct on k. If $k = 2$, then the conclusion follows immediately. Suppose we have proved the statement for an integer $k \geq 2$ polynomials, and $h_1, \dots, h_{k+1} \in \mathbf{Z}[x]$ are such that any two linear combinations of them are jointly intersective. For any integer t, the k polynomials $h_1, \dots, h_{k-1}, h_k + th_{k+1}$ also have the property that any two linear combinations of them are jointly intersective. By the induction hypothesis, $h_1, \dots, h_{k-1}, h_k + th_{k+1}$ are jointly intersective. That is, for each prime p, the polynomials $h_1, \dots, h_{k-1}, h_k + th_{k+1}$ have a common root x_t in $\mathbf{Z}_p$. Clearly, the number of possible values of x_t is finite, thus there are distinct integers t, t' such that $x_t = x_{t'}$. Therefore x_t is a common root in $\mathbf{Z}_p$ of $h_1, \dots, h_{k-1}, h_k, h_{k+1}$. It follows that $h_1, \dots, h_{k-1}, h_k, h_{k+1}$ are jointly intersective. □

Conversely, for any $l \geq 1$, it is trivially true that for any jointly intersective polynomials $h_1, \dots, h_k$, any l linear combinations of $h_1, \dots, h_k$ with coefficients in $\mathbf{Z}$ are jointly intersective. Curiously enough, when $l = 1$, Bergelson and Lesigne [3, Appendix] gave an example of two polynomials that are not jointly intersective, but any integral linear combination of them is intersective. Motivated by their construction, we show that this can be extended to any number of polynomials.

Proposition 2. *For any natural number $k \geq 2$, there exist polynomials $h_1, \ldots, h_k \in \mathbf{Z}[x]$ such that any two of them are not jointly intersective, but any linear combination of $h_1, \ldots, h_k$ with coefficients in $\mathbf{Z}$ is intersective.*

Proof. It suffices to show this when $k = p$ is prime. Let $G(x) = (x+1)\cdots(x+p)$, and let

$$h_i(x) = (px+1)(x^{i-1}G(x) + p) \qquad (1 \leq i \leq p).$$

Clearly, any two of the h_i do not have a common root in $\mathbf{Z}_p$; thus they are not jointly intersective. Given any integers $a_1, \ldots, a_p$, we will show that the polynomial $f(x) = a_1h_1(x) + \ldots + a_ph_p(x)$ is intersective. Since f is divisible by $px+1$, f has a root in $\mathbf{Z}_q$ for any prime $q \neq p$. Thus it suffices to show that f has a root in $\mathbf{Z}_p$. We may assume that $\gcd(a_1, \ldots, a_p) = 1$ and, in particular, that the a_i are not all divisible by p.

For any $x \in \mathbf{Z}/p\mathbf{Z}$, we have $G(x) \equiv 0 \pmod{p}$, implying that $f(x) \equiv 0 \pmod{p}$. By Hensel's lemma, it suffices to find $x \in \mathbf{Z}/p\mathbf{Z}$ such that $f'(x) \not\equiv 0 \pmod{p}$. For any $x \in \mathbf{Z}/p\mathbf{Z}$,

$$h_i'(x) \equiv (x^{i-1}G(x))' \equiv x^{i-1}G'(x) \equiv -x^{i-1} \pmod{p}$$

by Wilson's theorem. Hence

$$f'(x) \equiv -\sum_{i=1}^{p} a_i x^{i-1} \pmod{p}.$$

Since the a_i are not all divisible by p, there exists $x \in \mathbf{Z}/p\mathbf{Z}$ such that $f'(x) \not\equiv 0 \pmod{p}$, and the proposition follows. □

Two questions naturally arise from this construction.

Question 1. *If two (or more) polynomials are such that any integral linear combination of them is intersective, must they have a common factor?*

Question 2. *Is there an infinite sequence of polynomials such that any two of them are not jointly intersective, but any integral linear combination of them (where only finitely many coefficients are non-zero) is intersective?*

In view of Proposition 1, throughout this paper, we will work with a fixed intersective polynomial h and a fixed system of polynomials $h_1, \ldots, h_k$, where $h_1, \ldots h_k$ have the property that any integral linear combination of them is intersective if $l = 1$, and that they are jointly intersective if $l \geq 2$. Also, in the latter case, we can fix a sequence (r_d) such that (1) holds. We can assume furthermore that $h_1, \ldots, h_k$ are linearly independent and that our $\deg h_i = d_i$ satisfy $d_1 < d_2 < \cdots < d_k$. For a polynomial h, let us denote by $\mathrm{lead}(h)$ the leading coefficient of h.

We say that a system of polynomials $(g_1, \ldots, g_k)$ is *nice* if $\deg g_1 < \deg g_2 < \cdots < \deg g_k$ and the coefficient of $x^{\deg g_i}$ in g_j is 0 for $i \neq j$ (it is obviously 0 if $j < i$). Such a definition is useful when we want to apply results about simultaneous approximation to all the coefficients, in the spirit of Vinogradov, to a linear combination of the g_i. The following lemma is useful when one needs to convert a system of polynomials into a nice one. Basically, it says that given a system of polynomials $(f_i)_{i=1}^k$, if we are looking at the polynomials along an arithmetic progression $dx+r$, we can change them in such a way to have a nice system while the involved coefficients can grow but are still in control.

Lemma 1. *Suppose $r, d \in \mathbf{Z}$ and $f_1, \dots, f_k \in \mathbf{Z}[x]$ with $\deg f_1 < \deg f_2 < \cdots < \deg f_k$. There exists a $k \times k$ matrix T and polynomials $g_1, \dots, g_k \in \mathbf{Z}[x]$, depending on d and r, satisfying the following properties:*

(1) $T \begin{pmatrix} f_1(dx+r) \\ \vdots \\ f_k(dx+r) \end{pmatrix} = \begin{pmatrix} g_1(x) \\ \vdots \\ g_k(x) \end{pmatrix}.$

(2) *T is lower triangular with integer entries. All its diagonal entries are equal to c, where c is an integer constant (depending only on the coefficients of f_i). Actually, the (i,j) entry of T is $c_{ij} r^{\deg f_j - \deg f_i}$ if $i \le j$ and 0 otherwise, where c_{ij} is an integer depending only on the coefficients of $f_1, \dots, f_k$.*

(3) *$g_1, \dots, g_k$ form a nice system. Also, $\operatorname{lead}(g_i) = c d^{\deg f_i} \operatorname{lead}(f_i)$ for all $1 \le i \le k$.*

Proof. Let $A = (a_{ij})$ be a lower triangular matrix with all entries on the main diagonal equal to 1. For each $1 \le j \le k$, one can successively select rational numbers $a_{j,j-1}, \dots, a_{j,1}$ so that in the polynomial

$$a_{j1} f_1(dx+r) + a_{j2} f_2(dx+r) + \cdots + a_{j,j-1} f_{j-1}(dx+r) + f_j(dx+r),$$

the coefficient of x^{d_i} is 0 for every $i < j$. Let c be the common denominator of the entries in A; the matrix $T = cA$ satisfies the desired properties. □

Thus for any real numbers $(\alpha_1, \dots, \alpha_k)$, we can write

$$\alpha_1 f_1(dx+r) + \cdots + \alpha_k f_k(dx+r) = \beta_1 g_1(x) + \cdots + \beta_k g_k(x)$$

where

$$(\beta_1 \cdots \beta_k) = (\alpha_1 \cdots \alpha_k) T^{-1}. \tag{2}$$

2.2. **Notation.** We will use Vinogradov's notation $\ll, \gg$. Throughout the paper, ϵ stands for a positive number, which can be made arbitrarily small and may change from line to line (at the cost of changing the implied constants).

3. The case of a single polynomial

In this section we prove Theorems 3 and 5. Our main tool is the following (weighted version of a) lemma due to Montgomery.

Lemma 2 (Theorem 2.2, [1])**.** *Let M and N be a positive integers. Consider a sequence of real numbers $x_1, \dots, x_N$ and weights $c_1, \dots, c_N \ge 0$. Suppose $\|x_j\| \ge M^{-1}$ for all $j = 1, \dots, N$. Then there exists $1 \le m \le M$ such that*

$$\left| \sum_{n=1}^{N} c_n e(m x_n) \right| \ge \frac{1}{6M} \sum_{n=1}^{N} c_n.$$

Before proving Theorem 3, we also recall Weyl's inequality, a theorem due to Harman [9], and Linnik's Theorem [14, 15].

Lemma 3 (Weyl's inequality)**.** *Let f be a polynomial of degree k with leading coefficient c. Suppose that $q \in \mathbb{N}$ and $\|qc\| < q^{-1}$. Then,*

$$\sum_{n=1}^{N} e(f(n)) \ll N^{1+\epsilon} \left(q^{-1} + N^{-1} + qN^{-k}\right)^{2^{1-k}}.$$

Lemma 4. *Let f be a polynomial of degree k with leading coefficient c. Suppose that $q \in \mathbb{N}$ and $\|qc\| < q^{-1}$. For $k > 1$,*

$$\sum_{\substack{1 \le p \le N \\ p \text{ is prime}}} (\log p)\, e(f(p)) \ll N^{1+\epsilon} \left(q^{-1} + N^{-1/2} + qN^{-k}\right)^{4^{1-k}},$$

and for $k = 1$,

$$\sum_{\substack{1 \le p \le N \\ p \text{ is prime}}} (\log p)\, e(f(p)) \ll N^{1+\epsilon} \left(q^{-1/2} + N^{-1/5} + N^{-1/2}q^{1/2}\right).$$

Proof. This is a combination of [9, Theorem 1] due to Harman and [19, Theorem 3.1] due to Vinogradov. □

Lemma 5 (Linnik's Theorem)**.** *There exist positive real numbers U and V such that for any relatively prime positive integers q and r, the smallest prime congruent to r (mod q) is less than Uq^V.*

The current record is $V = 5.2$ [24], but we are not concerned in this paper with optimal constants.

Proof of Theorem 3. Let $M = \lfloor N^\theta \rfloor$, where θ is a sufficiently small exponent to be chosen later. We will show that for N sufficiently large, $\min_{1 \le n \le N} \|\alpha h(n)\| \le M^{-1} \ll N^{-\theta}$. Suppose for a contradiction that $\|\alpha h(n)\| \ge M^{-1}$ for all $n = 1, \dots, N$. Then, by Lemma 2, there exists $1 \le m \le M$ such that

$$\left| \sum_{n=1}^{N} e(m\alpha h(n)) \right| \gg \frac{N}{M}.$$

Let c be the leading coefficient of h, and let $\tau > 2^{k-1}$, where k is the degree of h. We assume that $\theta < \frac{1}{\tau}$, so that $M^\tau < N$. By Dirichlet's theorem on Diophantine approximation and Weyl's inequality, there exists $1 \le q \ll M^\tau$ such that $\|qm\alpha c\| \ll \frac{M^\tau}{N^k}$. Since h is intersective, there exists $1 \le n \le qmc$ such that $h(n)$ is divisible by qmc. On the one hand, we have $1 \le n \ll M^{\tau+1} \le N$ if $\theta < \frac{1}{\tau+1}$. We have

$$\|\alpha h(n)\| \le \left| \frac{h(n)}{qmc} \right| \|qm\alpha c\| \ll (qm)^{k-1} \|qm\alpha c\| \ll \frac{M^{k\tau+k-1}}{N^k}.$$

If θ is sufficiently small and N is sufficiently large, $\|\alpha h(n)\| < M^{-1}$, which is a contradiction. □

Remark 3.1. From a careful analysis of the argument above, one finds that for a polynomial h of degree k, Theorem 3 holds for any value $\theta < (2^{k-1} + 1)^{-1}$.

Proof of Theorem 5. Let $M = \lfloor N^{\theta} \rfloor$, where θ is a sufficiently small exponent to be chosen later. We will show that for N sufficiently large,

$$\min_{\substack{1 \le p \le N \\ p \text{ is prime}}} \|\alpha h(p)\| \le M^{-1} \ll N^{-\theta}.$$

Suppose for a contradiction that $\|\alpha h(p)\| \ge M^{-1}$ for all primes $p \le N$. Then, by Lemma 2 and the Prime Number Theorem, there exists $1 \le m \le M$ such that

$$\left| \sum_{\substack{1 \le p \le N \\ p \text{ is prime}}} (\log p)\, e(m\alpha h(p)) \right| \gg \frac{1}{M} \sum_{\substack{1 \le p \le N \\ p \text{ is prime}}} \log p \gg \frac{N}{M}.$$

Let c be the leading coefficient of h, and let $\eta > 4^{k-1}$ $(k > 1)$ or $\eta > 2$ $(k = 1)$, where k is the degree of h. Let U and V be given by Lemma 5. For θ sufficiently small depending on η, by Dirichlet's theorem on Diophantine approximation and Lemma 4, there exists $1 \le q \ll M^{\eta}$ such that $\|qm\alpha c\| \ll \frac{M^{\eta}}{N^k}$. By the hypothesis on the polynomial h, there exists $1 \le n \le qmc$ with $(qmc, n) = 1$ such that $h(n)$ is divisible by qmc. By Linnik's Theorem, there exists a prime $\tilde{p} \le U(qmc)^V$ with $\tilde{p} \equiv n \pmod{qmc}$. Note that $h(\tilde{p})$ is divisible by qmc. If θ is sufficiently small, we have $1 \le \tilde{p} \ll M^{(\eta+1)V} \le N$. Then

$$\|\alpha h(\tilde{p})\| \le \left| \frac{h(\tilde{p})}{qmc} \right| \|qm\alpha c\| \ll (qm)^{Vk-1} \|qm\alpha c\| \ll \frac{M^{Vk\eta + Vk - 1}}{N^k}.$$

If θ is sufficiently small and N is sufficiently large, $\|\alpha h(\tilde{p})\| < M^{-1}$, which is a contradiction. □

Remark 3.2. From a careful analysis of the argument above, one finds that for a polynomial h of degree k, Theorem 5 holds for any

$$\theta < \begin{cases} \min\left((3V)^{-1}, 5^{-1}\right), & \text{if } k = 1, \\ \min\left((4^{k-1}V + V)^{-1}, 2^{1-2k}\right), & \text{if } k > 1, \end{cases}$$

where V is given by Lemma 5. It is reasonable to conjecture that in Theorem 5, θ can be made arbitrarily close to 1. However, we cannot expect to improve vastly on our value of θ. Indeed, in the case $h(p) = p - 1$, if we have an inequality of the form

$$\min_{\substack{1 \le p \le N \\ p \text{ prime}}} \|\alpha(p-1)\| \ll N^{-\theta},$$

then by taking $\alpha = 1/q$ and $N \ll q^{1/\theta}$, this implies that the least prime congruent to 1 modulo q is $\ll q^{1/\theta}$. This gives a value of $1/\theta$ for Linnik's constant V (at least in the case $r = 1$), but it is presumably very difficult to show that $V = 2 + \epsilon$, which has only been established under the generalized Riemann hypothesis [10].

4. The one-dimensional case

In this section, we prove the one-dimensional case of Theorem 4.

Theorem 6. *Suppose the polynomials $h_1, \ldots, h_k$ of distinct degree are such that any linear combination of them with integer coefficients is intersective. Then there is an exponent $\theta > 0$ (depending at most on $h_1, \ldots, h_k$) such that*

$$\|\alpha_1 h_1(n) + \cdots + \alpha_k h_k(n)\| \ll N^{-\theta}$$

uniformly in $\alpha_1, \dots, \alpha_k, N$.

We need the following result due to Wooley, in place of Weyl's inequality.

Lemma 6. [22, Theorem 1.6] *Let* l *be an integer with* $l \geq 2$*, and let* τ *and* δ *be real numbers with* $\tau^{-1} > 4l(l-1)$ *and* $\delta > l\tau$*. Suppose that* N *is a sufficiently large integer in terms of* l*,* δ*, and* τ *and that*

$$\left| \sum_{1 \leq x \leq N} e\left(\alpha_1 x + \cdots + \alpha_l x^l\right) \right| \geq N^{1-\tau}.$$

Then, there exist an integer $1 \leq q \leq N^\delta$ *satisfying* $\|q\alpha_j\| \leq N^{\delta - j}$ $(1 \leq j \leq l)$*.*

The current record is $\tau(l) = \frac{1}{4l(l-2)}$ for $l \geq 4$ in [23], but we are not concerned in this paper with optimal exponents.

Proof of Theorem 6. By Theorem 3, we may assume that $k \geq 2$. Suppose for a contradiction that for every $1 \leq n \leq N$, we have

$$\|\alpha_1 h_1(n) + \cdots + \alpha_k h_k(n)\| \geq M^{-1},$$

where $M = \lfloor N^\theta \rfloor$ and θ is a sufficiently small exponent to be chosen later. Let the matrix T and polynomials $g_1, \dots, g_k$ be obtained by applying Lemma 1 for the polynomials $h_1, \dots, h_k$ with $d = 1$ and $r = 0$, and let $\beta_1, \dots, \beta_k$ be given by (2). Then for all $1 \leq n \leq N$, we have

$$\|\beta_1 g_1(n) + \cdots + \beta_k g_k(n)\| \geq M^{-1}.$$

By Lemma 2, there exists $1 \leq m \leq M$ with

$$\left| \sum_{n=1}^{N} e\left(m\beta_1 g_1(n) + \cdots + m\beta_k g_k(n)\right) \right| \gg \frac{N}{M}.$$

Recall that $\deg(g_i) = \deg(h_i) = d_i$ $(1 \leq i \leq k)$. Applying Lemma 6 with $\tau = \theta - \epsilon$ and $\delta = d_k\tau + \epsilon$, for N sufficiently large, there exists $1 \leq q \leq N^\delta$ with $\|qm\beta_i \mathrm{lead}(g_i)\| \leq N^{\delta - d_i}$ $(1 \leq i \leq k)$.

Let $R = qm \prod_{i=1}^{k} \mathrm{lead}(g_i)$, then $R \ll qm \leq N^\delta M \leq N$ if θ is sufficiently small and N is sufficiently large. We have $\|R\beta_i\| \ll N^{\delta - d_i}$ for all i. It follows that we can find integers a_i such that $|\beta_i - \frac{a_i}{R}| \ll N^{\delta - d_i} R^{-1}$ for all i. Let us now choose $1 \leq n \leq R$ such that

$$a_1 g_1(n) + \cdots + a_k g_k(n) \equiv 0 \pmod{R},$$

which is possible because each g_i is a linear combination of the h_i. Then we have

$$\begin{aligned} \left\| \sum_{i=1}^{k} \beta_i g_i(n) \right\| &\leq \left| \sum_{i=1}^{k} \beta_i g_i(n) - \frac{1}{R} \sum_{i=1}^{k} a_i g_i(n) \right| \leq \sum_{i=1}^{k} \left| \left(\beta_i - \frac{a_i}{R}\right) g_i(n) \right| \\ &\ll \sum_{i=1}^{k} N^{\delta - d_i} R^{d_i - 1} \ll N^{\delta - 1}. \end{aligned}$$

If θ is sufficiently small and N is sufficiently large, then this is smaller than M^{-1}, which is a contradiction. □

For the remainder of the paper, we will study jointly intersective polynomials $h_1, \dots, h_k$, and we will prove Theorem 4 by induction under this hypothesis. For technical reasons, we work with these polynomials along arithmetic progressions $dx + r_d$, where the sequence (r_d) is given by (1), and the modulus d may be as large as a small power of N.

Theorem 7. *Let $h_1, \dots, h_k$ be jointly intersective polynomials of distinct degree. There are exponents $\theta, \sigma > 0$ (depending on the h_i) such that the following holds. If d is a modulus smaller than N^σ and $\alpha_1, \dots, \alpha_k$ are arbitrary real numbers, then there exists $1 \le n \le N$ such that $n \equiv r_d \pmod{d}$ and*

$$\|\alpha_1 h_1(n) + \cdots + \alpha_k h_k(n)\| \ll N^{-\theta},$$

where the implied constant does not depend on $\alpha_1, \dots, \alpha_k, N, d$.

Proof of Theorem 7. Let θ and σ be small positive real numbers to be chosen later. Suppose for a contradiction that for every $1 \le x \le M = \lfloor N^{1-\sigma} \rfloor - 1$, we have

$$\|\alpha_1 h_1(dx + r_d) + \cdots + \alpha_k h_k(dx + r_d)\| \ge N^{-\theta} > M^{-2\theta}.$$

Let the matrix T and polynomials $g_1, \dots, g_k$ be obtained by applying Lemma 1 to the polynomials $h_1, \dots, h_k$ for d and $r = r_d$, and let $\beta_1, \dots, \beta_k$ be given by (2). Then for all $1 \le x \le M$, we have

$$\|\beta_1 g_1(x) + \cdots + \beta_k g_k(x)\| > M^{-2\theta}.$$

By Lemma 2, there exists $1 \le m \ll M^{2\theta}$ with

$$\left| \sum_{n=1}^{M} e\left(m\beta_1 g_1(n) + \cdots + m\beta_k g_k(n)\right) \right| \gg \frac{M}{M^{2\theta}}.$$

Recall that $\deg(g_i) = \deg(h_i) = d_i$ $(1 \le i \le k)$. Applying Lemma 6 with $\tau = 2\theta - \epsilon$ and $\delta = d_k \tau + \epsilon$, for M sufficiently large, there exists $1 \le q \le M^\delta$ with $\|qm\beta_i \mathrm{lead}(g_i)\| \le M^{\delta - d_i}$ $(1 \le i \le k)$.

Let $R = qm \prod_{i=1}^k \mathrm{lead}(g_i)$, then $R \ll qmd^C \ll M^{2\theta+\delta} d^C$, where $C = \sum_{i=1}^k d_i$. If θ and σ are sufficiently small, then we have $R \le N$. We also have $\|R\beta_i\| \le d^C M^{\delta - d_i}$ $(1 \le i \le k)$. Let us now choose $1 \le n \le R$ such that whenever

$$n \equiv r_R \pmod{R}$$

then $h_i(n)$ is divisible by R for any $1 \le i \le k$. We also have $n \equiv r_d \pmod{d}$, since R is divisible by d. If we write $n = dx + r_d$ for some $1 \le x \le R$, then $g_i(x)$ is divisible by R for any $1 \le i \le k$, since each $g_i(x)$ can be written as a linear combination of the $h_i(dx + r_d)$.

Then we have

$$\begin{aligned} \left\| \sum_{i=1}^k \beta_i g_i(x) \right\| &\le \sum_{i=1}^k \|\beta_i g_i(x)\| \le \sum_{i=1}^k \|R\beta_i\| \left| \frac{g_i(x)}{R} \right| \\ &\ll \sum_{i=1}^k d^C M^{\delta - d_i} R^{d_i - 1} \ll \sum_{i=1}^k d^C M^{\delta - d_i} (M^{2\theta+\delta} d^C)^{d_i - 1} \\ &\ll d^{C^2} \sum_{i=1}^k M^{-2\theta + d_i(2\theta + \delta - 1)} \end{aligned}$$

If θ and σ are sufficiently small and N is sufficiently large, then this is smaller than $M^{-2\theta}$, which is a contradiction. □

5. The general case

In this section, we prove Theorem 4. Following Schmidt [17], we reformulate the problem in the language of lattices and prove a more general statement that allows us to perform induction. Precisely, we will prove the following theorem.

Theorem 8. *Let $h_1, \dots, h_k$ be polynomials satisfying the conditions in Theorem 4. For every natural number l, there are exponents θ_l, σ_l such that the following holds. If Λ is a lattice with determinant $\det(\Lambda) \leq N^{\theta_l}$, d is a modulus with $d \leq N^{\sigma_l}$, and A is any real $l \times k$ matrix, then there exists $1 \leq n \leq N$ such that*

$$A \begin{pmatrix} h_1(n) \\ \vdots \\ h_k(n) \end{pmatrix} \in \Lambda + B_l,$$

where B_l is the unit ball in $\mathbf{R}^l$. Furthermore, $n \equiv r_d \pmod{d}$.

It is easy to see that Theorem 8 implies Theorem 4 (where θ can be taken to be θ_l/l) by setting $\Lambda = N^{\theta_l/l}\mathbf{Z}^l$ and replacing the matrix A in Theorem 4 by $N^{\theta_l/l}A$. Before proving Theorem 8, let us first recall the following lemma, which is reminiscent of Lemma 2 and can be found in the proof of [17, Lemma 14A].

Lemma 7. *Suppose Λ is a lattice of full rank in $\mathbf{R}^l$ such that $\Lambda \cap B_l = \{0\}$. Suppose $\vec{x}_1, \dots, \vec{x}_N \in \mathbf{R}^l$ are vectors not in $\Lambda + B_l$. Let $\epsilon > 0$ and*

$$S_{\vec{p}} = \sum_{n=1}^{N} e(\vec{x}_n \cdot \vec{p}).$$

Then, provided N is sufficiently large in terms of ϵ, there is a primitive point $\vec{p}$ in the dual lattice Π of Λ such that $|\vec{p}| \leq N^{\epsilon}$ and an integer $1 \leq t \leq \frac{N^{\epsilon}}{|\vec{p}|}$ such that

$$|S_{t\vec{p}}| \geq N^{1-\epsilon} \det(\Lambda)^{-1}.$$

Proof of Theorem 8. We prove this theorem by induction on l. The case when $l = 1$ follows from Theorem 7. Suppose that $l \geq 2$ and that we have determined appropriate values for θ_{l-1} and σ_{l-1}. Let θ_l and σ_l be two exponents, which will be selected later, and suppose that

$$A \begin{pmatrix} h_1(dn + r_d) \\ \vdots \\ h_k(dn + r_d) \end{pmatrix} \notin \Lambda + B_l$$

for all $1 \leq n \leq M = \lfloor N^{1-\sigma_l} \rfloor - 1$. Let T be the matrix and $g_1, \dots, g_k$ be the polynomials resulting from an application of Lemma 1 for the polynomials $h_1, \dots, h_k$ with respect to d and $r = r_d$. Then

$$B \begin{pmatrix} g_1(n) \\ \vdots \\ g_k(n) \end{pmatrix} \notin \Lambda + B_l \tag{3}$$

for all $n = 1, \ldots, M$, where $B = AT^{-1}$. Let $\epsilon > 0$ be any number, and assume that N is sufficiently large in terms of ϵ. Let $\vec{b}_1, \ldots, \vec{b}_k$ be the columns of B. Applying Lemma 7 to the vectors $\vec{x}_n = g_1(n)\vec{b}_1 + \cdots + g_k(n)\vec{b}_k$, we find a primitive point $\vec{p}$ in the dual lattice Π of Λ with $|\vec{p}| \le M^\epsilon$ and an integer $1 \le t \le \frac{M^\epsilon}{|\vec{p}|}$ such that

$$\left|\sum_{n=1}^{M} e(tg_1(n)\vec{b}_1 \cdot \vec{p} + \cdots + tg_k(n)\vec{b}_k \cdot \vec{p})\right| \ge M^{1-\epsilon} \det(\Lambda)^{-1}.$$

Let $\tau < \frac{1}{4d_k(d_k-1)}$ be a parameter to be chose later, and let $\delta = d_k\tau + \epsilon$. Applying Theorem 6 (in the case that $k = 1$ and $d_k = 1$, one could instead apply Weyl's inequality), provided M is sufficiently large and $M^{\tau-\epsilon} \ge \det(\Lambda)$, we can find $1 \le q \le M^\delta$ such that

$$\|qt\text{lead}(g_i)\vec{b}_i \cdot \vec{p}\| < M^{\delta - d_i}$$

for all $i = 1, \ldots, k$, since $(g_1, \ldots, g_k)$ is a nice system with d_i being the degree of g_i.

There are integers n_i such that $\|qt\text{lead}(g_i)\vec{b}_i \cdot \vec{p}\| = |qt\text{lead}(g_i)\vec{b}_i \cdot \vec{p} - n_i|$. Since $\vec{p}$ is a primitive point in Π, there are vectors $\vec{v}_i \in \Lambda$ such that $n_i = \vec{p} \cdot \vec{v}_i$. Thus we have $|(qt\text{lead}(g_i)\vec{b}_i - \vec{v}_i) \cdot \vec{p}| < M^{\delta - d_i}$. Roughly speaking, this means that the vectors $\vec{u}_i = qt\text{lead}(g_i)\vec{b}_i - \vec{v}_i$ almost lie in the orthogonal complement of $\vec{p}$, and we will exploit this fact to move to a space of smaller dimension. Before proceeding, let us state our goal. Let $R = cqtd^{d_k} \prod_{i=1}^{k} \text{lead}(h_i)$, where c is the constant in Property (3) of Lemma 1. Then R is divisible by $qt\text{lead}(g_i)$ for every i.

Claim: There exists $1 \le m \le \sqrt{N} \le M$ such that $g_i(m)$ are all divisible by R and

$$\frac{g_1(m)}{qt\text{lead}(g_1)}\vec{u}_1 + \cdots + \frac{g_k(m)}{qt\text{lead}(g_k)}\vec{u}_k \in \Lambda + B_l. \tag{4}$$

Since

$$\frac{g_1(m)}{qt\text{lead}(g_1)}\vec{u}_1 + \cdots + \frac{g_k(m)}{qt\text{lead}(g_k)}\vec{u}_k = g_1(m)\vec{b}_1 + \cdots + g_k(m)\vec{b}_k - \frac{g_1(m)}{qt\text{lead}(g_1)}\vec{v}_1 - \cdots - \frac{g_k(m)}{qt\text{lead}(g_k)}\vec{v}_k$$

and the $\vec{v}_i$ are in Λ, this immediately implies that $g_1(m)\vec{b}_1 + \cdots + g_k(m)\vec{b}_k \in \Lambda + B_l$, which contradicts (3). (The claim makes it clear why we need to include the extra divisibility requirement in our induction hypothesis.)

Let Λ' be the intersection of Λ and the $(l-1)$-dimensional space $V = \vec{p}^{\perp}$. Since $\vec{p}$ is a primitive point in the dual lattice of Π, Λ' is a sublattice of Λ of dimension $l - 1$. In order to achieve (4), we want to have

$$\frac{g_1(m)}{qt\text{lead}(g_1)}\vec{w}_1 + \cdots + \frac{g_k(m)}{qt\text{lead}(g_k)}\vec{w}_k \in \Lambda' + \frac{1}{2}B_l, \tag{5}$$

where $\vec{w}_i$ is the orthogonal projection of $\vec{u}_i$ onto V, and

$$\frac{g_1(m)}{qt\text{lead}(g_1)}(\vec{u}_1 - \vec{w}_1) + \cdots + \frac{g_k(m)}{qt\text{lead}(g_k)}(\vec{u}_k - \vec{w}_k) \in \frac{1}{2}B_l. \tag{6}$$

Since $|\vec{p}| \gg \det(\Lambda)^{-1}$ (see [17, p. 28]), we have $|\vec{u}_i - \vec{w}_i| = \frac{|\vec{u}_i \cdot \vec{p}|}{|\vec{p}|} \le \frac{M^{\delta - d_i}}{|\vec{p}|} \ll \det(\Lambda)M^{\delta - d_i} \le N^{\theta_l}M^{\delta - d_i}$. It is easy to see from Lemma 1 that we also have the bound $g_i(m) \ll (dm)^{d_i}$.

Hence for every $1 \leq m \leq \sqrt{N}$,

$$\begin{aligned}\left|\frac{g_1(m)}{qt\mathrm{lead}(g_1)}(\vec{u}_1 - \vec{w}_1) + \cdots + \frac{g_k(m)}{qt\mathrm{lead}(g_k)}(\vec{u}_k - \vec{w}_k)\right| &\leq \sum_{i=1}^{k} N^{\theta_l} M^{\delta - d_i} (dm)^{d_i} \\ &\ll \sum_{i=1}^{k} N^{\theta_l} M^{\delta - d_i} N^{d_i(1/2+\sigma_l)},\end{aligned}$$

which can be made smaller than 1/2 if, say, $\theta_l + 2\sigma_l + \delta < 1/2$. Thus (6) is achieved.

Let us now turn our attention to (5). This is satisfied if we can find $1 \leq x \leq \sqrt{N}$ such that $x \equiv r_R \pmod{R}$ and

$$h_1(x)\vec{s}_1 + \cdots + h_k(x)\vec{s}_k \in \Lambda' + \frac{1}{2}B_l, \tag{7}$$

where

$$(\vec{s}_1 \vec{s}_2 \cdots \vec{s}_k) = \begin{pmatrix} \frac{\vec{w}_1}{qt\mathrm{lead}(g_1)} & \frac{\vec{w}_2}{qt\mathrm{lead}(g_2)} & \cdots & \frac{\vec{w}_k}{qt\mathrm{lead}(g_k)} \end{pmatrix} T.$$

Once such an x is found, upon setting $m = \frac{x - r_d}{d}$, (5) holds. (Note that R is divisible by d.)

We are working in the $(l-1)$-dimensional space V with a lattice of full rank Λ'. By our induction hypothesis, we can find $1 \leq x \leq \sqrt{N}$ satisfying $x \equiv r_R \pmod{R}$ and (7) provided that $R \leq N^{\sigma_{l-1}/2}$ and $\det(\Lambda') \ll N^{\theta_{l-1}/2}$. By definition,

$$R \ll qtd^{d_k} \ll M^{\delta+\epsilon} N^{d_k \sigma_l},$$

so the first condition is always satisfied if $\delta + d_k \sigma_l \leq \sigma_{l-1}/3$. As for the second condition, note that $\det(\Lambda') = |\vec{p}| \det(\Lambda) \ll N^{\theta_l + \epsilon}$, implying that the condition is satisfied if $\theta_l \leq \theta_{l-1}/3$. In summary, if we choose τ, θ_l, and σ_l sufficiently small in terms of σ_{l-1} and θ_{l-1}, then (5) is achieved, and the theorem holds. □

References

[1] R. C. Baker, **Diophantine inequalities**, London Mathematical Society Monographs, vol. 1, Oxford University Press, Oxford, 1986.

[2] D. Berend and Y. Bilu, *Polynomials with roots modulo every integer*, Proc. Amer. Math. Soc. **124** (1996), no. 6, 1663–1671.

[3] V. Bergelson and E. Lesigne, *Van der Corput sets in* $\mathbf{Z}^d$, Colloq. Math. **110** (2008), no. 1, 1–49.

[4] V. Bergelson, A. Leibman, and E. Lesigne, *Intersective polynomials and the polynomial Szemerédi theorem*, Adv. Math. **219** (2008), no. 1, 369–388.

[5] R. J. Cook, *On the fractional parts of a sets of points. III*, J. London Math. Soc. (2) **9** (1975), 490–494.

[6] I. Danicic, *Contributions to number theory*, PhD Thesis, University of London, 1957.

[7] H. Davenport, *On a theorem of Heilbronn*, Quart. J. Math. Oxford, Ser. 2, **18** (1967), 339–344.

[8] G. H. Hardy and J. E. Littlewood, *Some problems of diophantine approximation Part I. The fractional part of* $n^k\theta$, Acta Math. **37** (1914), no. 1, 155–191.

[9] G. Harman, *Trigonometric sums over primes I*, Mathematika **28** (1981), no. 2, 249–254.

[10] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. **64** (1992), 265–338.

[11] H. Heilbronn, *On the distribution of the sequence* $n^2\theta$ (mod 1), Quart. J. Math., Oxford Ser. **19** (1948), 249–256.

[12] T. Kamae and M. Mendès France, *Van der Corput's difference theorem*, Israel J. Math. **31** (1978), no. 3-4, 335–342.

[13] T. H. Lê, *Problems and results on intersective sets*, preprint, 14pp.

[14] U. V. Linnik, *On the least prime in an arithmetic progression, I*, Rec. Math (Mat. Sbornik) N.S. **15(57)** (1944), 139–178.

[15] U. V. Linnik, *On the least prime in an arithmetic progression, II*, Rec. Math (Mat. Sbornik) N.S. **15(57)** (1944), 347–368.

[16] J. Lucier, *Intersective sets given by a polynomial*, Acta Arith. **123** (2006), 57–95.

[17] W. M. Schmidt, **Small fractional parts of polynomials**, Regional Conference Series in Mathematics, no. 32, American Mathematical Society, Providence, 1977.

[18] S. Slijepcevic, *On van der Corput property of shifted primes*, http://arxiv.org/abs/1003.3783, 12pp.

[19] R. C. Vaughan, **The Hardy-Littlewood method**, 2nd ed., Cambridge University Press, Cambridge, 1997.

[20] R. C. Vaughan, *Diophantine approximation by prime numbers, II*, Proc. London Math. Soc. **28** (1974), 385–401.

[21] I. M. Vinogradov, *Analytischer Beweis des Satzes über die Verteilung der Bruchteile eines ganzen Polynoms*, Bull. Acad. Sci. USSR (6) **21** (1927), 567–578.

[22] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing*, Annals of Math. **175** (2012), 1575–1627.

[23] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing, II*, to appear in Duke Math. J., 46pp.

[24] T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, Acta Arith. **150** (2011), 65–91.

[25] A. Zaharescu, *Small values of $n^2\alpha$ (mod 1)*, Invent. Math. **121** (1995), no. 2, 379–388.

T. H. Lê, Department of Mathematics, The University of Texas at Austin, 1 University Station, C1200 Austin, TX 78712

E-mail address: `leth@math.utexas.edu`

C. V. Spencer, Department of Mathematics, Kansas State University, 138 Cardwell Hall, Manhattan, KS 66506

E-mail address: `cvs@math.ksu.edu`