ACTA ARITHMETICA
123.1 (2006)

# Intersective sets given by a polynomial

by

Jason Lucier (Waterloo, ON)

**1. Introduction.** L. Lovász conjectured that any set of natural numbers of positive upper density must contain distinct elements $a$ and $b$ such that the difference $a-b$ is a perfect square. In the late 1970s, Furstenberg [5] and Sárközy [15] independently proved Lovász's conjecture. Furstenberg used ergodic theory, whereas Sárközy used the circle method. Sárközy actually proved a stronger result which we will describe shortly.

Let $H$ denote a set of natural numbers. We say that $H$ is *intersective* if any set of natural numbers of positive upper density must contain distinct elements $a$ and $b$ such that the difference $a-b$ is in $H$. Thus, Lovász conjectured that the set of positive squares is an intersective set. For any positive integer $N$ we define $D(H,N)$ to be the maximal size of a subset $A$ of $\{1,\dots,N\}$ such that if $a$ and $b$ are in $A$ then $a-b$ is not in $H$. Notice that if $D(H,N)=o(N)$ then $H$ is an intersective set. The converse implication is also true; Ruzsa [13, Theorem 1] has given a proof of this.

Let $S$ denote the set of positive squares. Sárközy proved Lovász's conjecture by proving the stronger statement

$$D(S,N) \ll N\,\frac{(\log\log N)^{2/3}}{(\log N)^{1/3}}.$$

He also proved [16] that the set $P=\{p-1 : p \text{ a prime}\}$ is intersective. In particular, he proved that

$$D(P,N) \ll N\,\frac{(\log\log\log N)^2(\log\log\log\log N)}{(\log\log N)^2}.$$

Inspired by Sárközy's results, Kamae and Mendès France [8] obtained in 1978, by means of harmonic analysis, a general criterion for determining when a set of positive integers is intersective.

Theorem A (Kamae and Mendès France). *Let $H$ be a set of natural numbers such that for every positive integer $m$ there are infinitely many*

2000 *Mathematics Subject Classification*: 11P55, 11N56.

*elements in $H$ divisible by $m$. Denote by $\{h_{i,m}\}_{i=1}^{\infty}$ the increasing sequence whose terms are the elements of $H$ which are divisible by $m$. If for every positive integer $m$ and every irrational number $\theta$ the sequence $\{\theta h_{i,m}\}_{i=1}^{\infty}$ is uniformly distributed modulo* 1, *then the set $H$ is intersective.*

For any polynomial $f$ let $V(f) = \{f(x) : x \geq 1,\, f(x) > 0\}$. As an application of their criterion Kamae and Mendès France proved the following result.

THEOREM B (Kamae and Mendès France). *Let $h$ be a nonconstant polynomial, with integer coefficients, and positive leading coefficient. The set $V(h)$ is intersective if and only if for every integer $m \geq 2$ the congruence equation*

$$h(x) \equiv 0 \pmod{m} \tag{1}$$

*has a solution.*

We remark that if the polynomial $h$ has an integer root, then the congruence equation $h(x) \equiv 0 \pmod{m}$ plainly has a solution for every integer $m \geq 2$. There are polynomials without an integer root that also have this property, for example $(x^3 - 19)(x^2 + x + 1)$. D. Berend and Y. Bilu [2] have given a procedure for determining when a polynomial $h(x) \in \mathbb{Z}[x]$ has a root modulo $m$ for every integer $m \geq 2$.

For brevity, given any positive integer $N$ and polynomial $f$ we write $D(f, N)$ in place of $D(V(f), N)$. For any integer $k \geq 2$, let $f_k(x) = x^k$. So in terms our earlier notation $V(f_2)$ is the set $S$ of positive squares.

In 1985 Srinivasan [18] used the circle method to prove $V(f_k)$ is intersective for every integer $k \geq 2$. In fact, Srinivasan was able to conclude that

$$D(f_k, N) \ll_k N/(\log\log N)^{c_k}$$

for some $c_k > 0$.

In 1988 Pintz, Steiger, and Szemerédi [12] improved Sárközy's estimate for $D(f_2, N)$ by proving that

$$D(f_2, N) \ll N/(\log N)^{(\log\log\log\log N)/4}.$$

In 1994 Balog, Pelikán, Pintz, and Szemerédi [1] showed that for $k \geq 3$ the previous estimate also holds for $D(f_k, N)$ with the implicit constant depending on $k$.

Green [7] has given a different proof that $S = V(f_2)$ is intersective. Green's argument, which follows the methodology of Gowers [6], gives a weaker bound for $D(f_2, N)$.

Slijepčević [17] proved in 2003 the following result: If $h(x) \in \mathbb{Z}[x]$ has degree greater than or equal to 3 and satisfies $h(0) = 0$, then

$$D(h, N) \ll N/\log\log\log N.$$

The purpose of this paper is to provide a quantitative version of Theorem B by estimating $D(h,N)$ whenever $h$ is a polynomial such that $V(h)$ is intersective. We remark that when $h$ is linear it is trivial to estimate $D(h,N)$ and thus we will concern ourselves only with polynomials of degree 2 or greater. We will obtain the following result.

THEOREM 1. *Let $h$ be a polynomial with integer coefficients, a positive leading coefficient, degree $k \geq 2$, and such that for every integer $m \geq 2$ the congruence equation*

$$h(x) \equiv 0 \pmod{m}$$

*has a solution. Set*

$$\mu = \begin{cases} 3 & \text{if } k = 2, \\ 2 & \text{if } k \geq 3. \end{cases} \tag{2}$$

*Then*

$$D(h,N) \ll_h N \frac{(\log\log N)^{\mu/(k-1)}}{(\log N)^{1/(k-1)}}.$$

Working in the other direction Ruzsa [14] has given a lower bound for $D(f_k,N)$ which in particular gives $D(f_2,N) \geq (1/65)N^{0.733}$.

For any finite set $A$ of integers and any integer $n$, let

$$r(A,n) = |\{(a,b) \in A \times A : a - b = n\}|.$$

Furthermore, if $H$ is a set of integers let

$$R(H,A) = \sum_{n \in H} r(A,n).$$

In other words, $R(H,A)$ is the number of solutions to $a-b=h$ with $a,b \in A$ and $h \in H$. Note that if $A$ is a subset of $\{1,\dots,N\}$ and $|A| > D(H,N)$, then $R(H,A) \geq 1$. For brevity, given any polynomial $f$ we write $R(f,A)$ in place of $R(V(f),A)$.

Using the circle method R. C. Vaughan [20, Theorem 10.2] proved that if $B$ is any set of positive integers with positive upper density, then

$$\limsup_{N\to\infty} \frac{R(f_2, B \cap \{1,\dots,N\})}{N^{3/2}} > 0.$$

This result gives another proof that $V(f_2)$ (the set of positive squares) is intersective. A second purpose of this paper is to generalize this result by proving the following theorem.

THEOREM 2. *Let $h$ be a polynomial as in Theorem 1 with leading coefficient $b$. Let $N$ be a sufficiently large integer in terms of $h$, and let $A$ be a subset of $\{1,\dots,N\}$ with size $\delta N$. Let $\mu$ be as in (2). There exist positive*

*numbers $C$ and $C'$ which depend only on $h$ such that if*

$$|A| \geq CN \frac{(\log\log N)^{\mu/(k-1)}}{(\log N)^{1/(k-1)}},$$

*then*

$$R(h,A) \gg_k \frac{|A|^2}{b^{1/k}N^{1-1/k}} \exp(-C'\delta^{-(k-1)}(\log 2\delta^{-1})^{\mu}). \tag{3}$$

Note that for $|A| \gg N$, this theorem implies $R(h,A) \gg_h N^{1+1/k}$. Apart from the implied constant this is best possible since

$$R(h,A) = \sum_{h(x)\leq N} r(A,h(x)) \leq |A| \sum_{h(x)\leq N} 1 \ll_h N^{1+1/k}.$$

Observe that since $R(h,A)$ is an integer and the right hand side of (3) is positive, the conclusion of Theorem 2 implies $R(h,A) \geq 1$. Thus Theorem 1 follows from Theorem 2.

The author would like to thank his doctoral advisor, Cameron Stewart, for his valuable guidance in the preparation of this paper, the results of which are part of the author's Ph.D. thesis [9].

**2. Preliminaries.** Let $h(x) \in \mathbb{Z}[x]$ be a polynomial with a positive leading coefficient and set $f(x) = h(x+d)$ where $d$ is some positive integer. Then $R(f,A) \leq R(h,A)$, and hence any lower bound for $R(f,A)$ is a lower bound for $R(h,A)$. The integer $d$ can be taken to be large enough, in terms of $h(x)$ alone, so that $f(x)$ and $f'(x)$ are positive and increasing for $x \geq 0$. Therefore to prove Theorem 2 we may assume $h$ also has this property.

For any finite set $A$ we define

$$W(h,A) = \sum_{x\geq 1} h'(x) r(A,h(x)).$$

In order to prove Theorem 2 it will be technically more convenient to work with the weighted function $W(h,A)$ in place of $R(h,A)$.

Given any polynomial $f(x) = b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0$, we define

$$B(f) = \frac{2}{|b_k|}(|b_{k-1}| + |b_{k-2}| + \cdots + |b_0|). \tag{4}$$

The next lemma, which contains some elementary properties regarding $B(f)$, can be proved easily thus we leave the details to the reader.

LEMMA 3. *Let $f$ be a polynomial of degree $k$ and with leading coefficient $b > 0$. If $x \geq 1$, then*

$$bx^k\left(1 - \frac{B(f)}{2x}\right) \leq f(x) \leq bx^k\left(1 + \frac{B(f)}{2x}\right).$$

*As a consequence, if* $x \geq B(f)$, *then*

$$\frac{1}{2}\, bx^k \leq f(x) \leq \frac{3}{2}\, bx^k.$$

*Furthermore,* $f'$, *the derivative of* $f$, *satisfies*

$$B(f') \leq B(f).$$

We relate the counting functions $R(h, A)$ and $W(h, A)$.

LEMMA 4. *Let* $h$ *be a polynomial with integer coefficients, degree* $k$, *and positive leading coefficient* $b$. *Furthermore, suppose that* $h(x)$ *and* $h'(x)$ *are positive and increasing for* $x \geq 1$. *If* $A$ *is a subset of* $\{1, \ldots, N\}$, *then*

$$W(h, A) \leq 3kb^{1/k} N^{1-1/k} R(h, A)$$

*provided* $N$ *is sufficiently large in terms of* $h$.

*Proof.* We first note that

$$W(h, A) \leq (\max h'(x)) R(h, A),$$

where the maximum is taken over all $x \geq 1$ such that $h(x) \leq N$. Let $m = (2N/b)^{1/k}$, and suppose that $N$ is large enough so that $m \geq B(h)$. Then

$$h(m) \geq \frac{1}{2}\, bm^k \geq N.$$

By the assumptions made on $h$ we are able to deduce that $W(A, h) \leq h'(m) R(A, h)$. Since $B(h') \leq B(h)$ we find that $h'(m) \leq 3kb^{1/k} N^{1-1/k}$. Therefore

$$W(h, A) \leq 3kb^{1/k} N^{1-1/k} R(h, A). \quad \blacksquare$$

By the remark made at the beginning of this section and by Lemma 4 we see that Theorem 2 follows from the following.

THEOREM 5. *Let* $h$ *be a polynomial satisfying the hypothesis in Theorem* 2. *Suppose further* $h(x)$ *and* $h'(x)$ *are positive and increasing for* $x \geq 0$. *Let* $N$ *be a sufficiently large integer in terms of* $h$, *and let* $A$ *be a subset of* $\{1, \ldots, N\}$ *of size* $\delta N$. *Let* $\mu$ *be as in* (2). *There exist positive numbers* $C$ *and* $C'$ *which depend only on* $h$ *such that if*

$$\delta \geq C\, \frac{(\log \log N)^{\mu/(k-1)}}{(\log N)^{1/(k-1)}},$$

*then*

$$W(h, A) \geq \frac{1}{64}\, |A|^2 \exp(-C' \delta^{-(k-1)} (\log 2\delta^{-1})^{\mu}).$$

**3. Outline of the proof.** In this section we sketch the major features in our proof of Theorem 5. The proof is an adaptation of Sárközy's method in [15] and [16]. This method is indirect and involves an iterative construction

to produce a contradiction. In our application of the circle method we will use the discrete Fourier transform in a fashion similar to the approach taken by Green [7].

We begin by describing a nonuniformity result which is at the core of our argument. Let $A$ be a subset of $\{1,\dots,N\}$ with size $\delta N$, and let $f$ be some increasing polynomial of degree 2 or greater. For any real $\alpha$ we define the exponential sums

$$F(\alpha)=\sum_{a\in A} e(\alpha a), \qquad T(\alpha)=\sum_{f(x)\le N/2} f'(x)e(\alpha f(x)),$$

where as usual $e(\alpha)$ denotes $\exp(2\pi i\alpha)$. In Section 6 we use these exponential sums and some basic Fourier analysis to compare $W(f,A)$ with its "expected" size

$$\delta^2 \sum_{f(x)\le N} f'(x) r(\{1,\dots,N\}, f(x)) \approx |A|^2.$$

We suppose that $W(f,A)\le |A|^2/32$. Then provided $\delta$ is not too small we deduce that there exists a positive real number $\theta(f,\delta)$, that depends only of $f$ and $\delta$, such that

$$\sum |F(t/N)|^2 \gg \theta(f,\delta)|A|^2,$$

where this sum is over a set of nonzero $t$ such that $t/N$ belongs to certain "major arcs" used in our application of the circle method. This result, together with a standard argument given in Section 7, allows us to deduce that $A$ is nonuniform in the sense that there exists a large arithmetic progression $P$ in $\{1,\dots,N\}$ that contains more elements from $A$ than the expected amount $\delta|P|$. In fact, we find that there is a positive number $C$ such that

$$|A\cap P|\ge \delta(1+C\theta(f,\delta))|P|.$$

We remark that the size of the increment $\theta(f,\delta)$ will depend on estimates of the exponential sum $T(\alpha)$. Section 5 is devoted to estimating $T(\alpha)$ in a way that is suitable for our purposes. Our estimates will allow us to express the increment $\theta(f,\delta)$ as a function of $\delta$ and the content of the polynomial $f(x)-f(0)$ (the *content* of a polynomial is defined as the greatest common divisor of its coefficients).

Let $h$ be a polynomial as in Theorem 5. Following the method laid out in [16] we need to consider intersective sets other than $V(h)$. For any set of integers $H$ and integer $m$, we set

$$H_m=\{k/m : k\in H,\ k\equiv 0 \pmod m\}.$$

If $H$ is intersective then so is $H_m$ (see [17, Proposition 1.3]). The set $H_m$ has the following property: If $B$ is a finite set of integers and $C$ =

$\{c + mb : b \in B\}$, then

$$R(H, C) = R(H_m, B).$$

When $H = V(h)$ we can write

$$V(h)_m = \bigcup_{\substack{-m<r\le 0 \\ h(r)\equiv 0 \,(\mathrm{mod}\, m)}} \{h(r + mx)/m : x \ge 1\}.$$

Notice that $V(h)_m$ is nonempty since $h$ has at least one root modulo $m$.

The condition that $h(x) \equiv 0 \pmod m$ has a solution for every $m \ge 2$ is equivalent to the existence of a $p$-adic root of $h$ for every prime $p$. For each prime $p$ we fix a $p$-adic root $z_p$ of $h$. By the Chinese Remainder Theorem the $p$-adic roots $z_p$ determine for every positive integer $d$ a unique integer $r_d$ in the interval $(-d, 0]$ such that $h(r_d) \equiv 0 \pmod d$. Furthermore $r_{dq} \equiv r_d \pmod d$ for all positive integers $q$. The $p$-adic roots $z_p$ also determine an arithmetic function $\lambda$ such that $d \,|\, \lambda(d)$ and

$$h(r_d + dx) \equiv 0 \pmod{\lambda(d)}$$

for every integer $x$. In Section 8 we define the polynomial $h_d$ by

$$h_d(x) = \frac{h(r_d + dx)}{\lambda(d)}.$$

These auxiliary polynomials $h_d(x)$ have the property that

$$V(h_{dq}) \subseteq V(h_d)_{\lambda(d)} \subseteq V(h)_{\lambda(dq)} \tag{5}$$

for all positive integers $d$ and $q$.

A technical aspect of the proof requires us to show that for every positive integer $d$ the content of the polynomial $h_d(x) - h_d(0)$ is bounded above in terms of $h(x)$ alone. We accomplish this by introducing in this context the semidiscriminant of Chudnovsky [4].

We can now describe the first step of the iteration. We begin by assuming that $\delta$ is not too small and that $W(h, A)$ is much smaller than $|A|^2/32$. Then by applying the nonuniformity result described above we deduce that there is an arithmetic progression $P$ in $\{1, \dots, N\}$ of length $N' \le N$ such that

$$|A \cap P| \ge \delta_0(1 + C\theta(h, \delta))|P|.$$

The arithmetic progression can be chosen to have the form

$$P = \{c + \lambda(q), \dots, c + \lambda(q)N'\},$$

with $q$ a relatively small integer. We define the set $A' \subseteq \{1, \dots, N'\}$ by

$$A \cap P = \{c + \lambda(q)b : b \in A'\}.$$

Then

$$R(V(h)_{\lambda(q)}, A') = R(V(h), A) = R(h, A).$$

Since $V(h_q) \subseteq V(h)_{\lambda(q)}$, we obtain $R(h_q, A') \leq R(h, A)$. In fact we will have

$$W(h_q, A') \leq W(h, A).$$

If we denote the size of $A'$ by $\delta' N'$, then $\delta' = |A \cap P|/N'$, and thus

$$\delta' \geq \delta(1 + C\theta(h, \delta)).$$

By taking $W(h, A)$ to be small enough, $W(h_q, A')$ will also be smaller than $|A'|^2/32$. We can then repeat the argument with $A'$ and $h_d$. The number of times we can repeat the argument depends on the size of $\delta$ and $W(A, h)$. By making $\delta$ large enough and $W(A, h)$ small enough we can repeat this iteration enough times to eventually obtain a set whose density is greater than 1. This contradiction will imply the estimates on $\delta$ and $W(h, A)$ found in the statement of Theorem 5.

Finally, we remark that it is the use of the $p$-adic numbers which allows us to treat polynomials $h$ that do not have an integer root. If $h$ has zero as a root, say with multiplicity $l$, then we can take the $p$-adic roots to be $z_p = 0$ for every prime $p$. In this case our auxiliary polynomials will become

$$h_d(x) = \frac{h(xd)}{d^l},$$

and these are the polynomials used by Slijepčević [17] to give his bound on $D(h, N)$ when $h(0) = 0$.

**4. Complete exponential sums.** In this section we present some preliminary lemmas dealing with complete exponential sums. Given any polynomial $f$ with integer coefficients and any positive integer $q$, we write $S(f, q)$ to denote the complete exponential sum given by

$$S(f, q) = \sum_{r=1}^{q} e\left(\frac{f(r)}{q}\right).$$

Let us write $c(f)$ to denote the content of the polynomial $f(x) - f(0)$. The following result, obtained independently by Chen [3] and Nechaev [10], gives an estimate for $S(f, q)$ which is the best possible up to the implicit constant.

LEMMA 6. *Let $f$ be a polynomial with integer coefficients and degree $k \geq 2$. Then*

$$S(f, q) = O_k((c(f), q)^{1/k} q^{1-1/k}).$$

Let us note the following "orthogonality" relation: For any positive integer $m$ and integer $x$ we have

$$\frac{1}{m} \sum_{t=0}^{m-1} e\left(\frac{xt}{m}\right) = \begin{cases} 1 & \text{if } m \mid x, \\ 0 & \text{if } m \nmid x. \end{cases} \tag{6}$$

We define $c'(f)$ to be the content of the polynomial $f(x)-f'(0)x-f(0)$.

LEMMA 7. *Let $f$ be a polynomial with integer coefficients and degree $k \geq 2$. Let $q \geq 2$ be a positive integer, and set $d = \gcd(c'(f), q)$. If $d \nmid f'(0)$, then $S(f,q) = 0$.*

*Proof.* Let $a_0$ and $a_1$ be integers and $h(x)$ a polynomial in $\mathbb{Z}[x]$ such that $f(x) = h(x) + a_1x + a_0$. Then $c'(f) = c'(h)$. Define $h_1(x) = (1/d)h(x)$ and $q_1 = q/d$. By (6) we find that

$$\begin{aligned} S(f,q) &= e\Big(\frac{a_0}{q}\Big)\sum_{r=1}^{q_1} e\Big(\frac{h_1(r)}{q_1}\Big) \sum_{\substack{s=1 \\ y\equiv x \,(\mathrm{mod}\, q_1)}}^{q} e\Big(\frac{a_1 s}{q}\Big) \\ &= e\Big(\frac{a_0}{q}\Big)\sum_{r=1}^{q_1} e\Big(\frac{h_1(r)}{q_1}\Big)\sum_{s=1}^{q} e\Big(\frac{a_1 s}{q}\Big)\Big(\frac{1}{q_1}\sum_{t=1}^{q_1} e\Big(\frac{(r-s)t}{q_1}\Big)\Big) \\ &= de\Big(\frac{a_0}{q}\Big)\sum_{t=1}^{q_1}\sum_{r=1}^{q_1} e\Big(\frac{h_1(r)+tr}{q_1}\Big)\Big(\frac{1}{q}\sum_{s=1}^{q} e\Big(\frac{(a_1-dt)s}{q}\Big)\Big). \end{aligned}$$

Suppose that $d \nmid f'(0)$. Then $q \nmid (a_1 - dt)$ for every integer $t$. Therefore by (6) the sum in the last pair of brackets above is zero. Thus $S(f,q) = 0$. ∎

LEMMA 8. *Let $f$ be a polynomial with integer coefficients, and $q \geq 2$ an integer. Then*

$$\frac{1}{q}\sum_{s=1}^{q} |S(f(x)+sx, q)| \leq q^{1/2}.$$

*Proof.* By using (6) we are able to deduce that

$$\sum_{s=1}^{q} |S(f(x)+sx,q)|^2 = \frac{1}{q}\sum_{r=1}^{q}\Big|\sum_{s=1}^{q} S(f(x)+sx,q)e\Big(\frac{-rs}{q}\Big)\Big|^2.$$

Also by (6), we find that for every integer $t$,

$$\begin{aligned} \sum_{s=1}^{q} S(f(x)+sx,q)e_q(-ts) &= \sum_{s=1}^{q}\sum_{r=1}^{q} e\Big(\frac{f(r)+sr}{q}\Big)e\Big(\frac{-ts}{q}\Big) \\ &= \sum_{r=1}^{q} e\Big(\frac{f(r)}{q}\Big)\sum_{s=1}^{q} e\Big(\frac{(r-t)s}{q}\Big) = qe\Big(\frac{f(t)}{q}\Big). \end{aligned}$$

The equations above imply

$$\sum_{s=1}^{q} |S(f(x)+sx,q)|^2 = q^2.$$

Thus, by the Cauchy–Schwarz inequality we obtain

$$\sum_{s=1}^{q} |S(f(x)+sx,q)| \le q^{1/2}\Big(\sum_{s=1}^{q} |S(f(x)+sx,q)|^2\Big)^{1/2} \le q^{3/2}.$$

The result then follows. ∎

**5. Incomplete exponential sums.** Throughout this section we let $f$ denote a polynomial with integer coefficients, degree $k$, and positive leading coefficient $b$. Furthermore, we assume that $f(x)$ and $f'(x)$ are positive and increasing for $x \ge 1$.

For any real number $n \ge 1$ and real number $\alpha$ we define

$$S(\alpha,n) = \sum_{1\le x\le n} e(\alpha f(x)), \qquad T(\alpha,n) = \sum_{1\le x\le n} f'(x)e(\alpha f(x)).$$

In this section we will estimate these two exponential sums. For applications later on, any implicit constant appearing in our estimates must depend only on the degree of the polynomial $f$. In order to obtain estimates of this nature we will take $n$ to be large enough in terms of the polynomial $f$.

**5.1.** *A general estimate.* In Lemma 11 below we give an estimate for $S(\alpha,n)$ and $T(\alpha,n)$ which generalises a result due to Vaughan (Theorem 4.1 in [20]). The proof of Lemma 11 follows closely the proof of Theorem 4.1 in [20] except for the treatment of the error term. Before presenting Lemma 11 we state two preliminary lemmas.

LEMMA 9 ([19, Lemma 4.3]). *Let $F(x)$ be real-valued differentiable function on the interval $[m,n]$ that never takes on the value 0. Let $G(x)$ be a real-valued function on the interval $[m,n]$ such that $G(x)/F'(x)$ is monotonic and $|G(x)/F'(x)| \le B$ for some positive real number $B$. Then*

$$\int_m^n G(t)e(F(t))\,dt = O(B).$$

LEMMA 10. *Let $F(x)$ be a real-valued function on the interval $[m,n]$ such that $F(x)$ has a continuous second derivative, $F'(x)$ is monotonic, and $|F'(x)| \le 3/4$. Let $G(x)$ be a real-valued differentiable function on $[m,n]$ such that both $G(x)$ and $G'(x)$ are positive and increasing. Then*

$$\sum_{m\le x\le n} G(x)e(F(x)) = \int_m^n G(t)e(F(t))\,dt + O(G(n)+G'(n)).$$

*Proof.* This can be viewed as a weighted version of Lemma 4.2 in [20]. Adapting the proof of Lemma 4.2 in [20] to handle the weight $G(x)$ is fairly straightforward. The result can also be seen as a variation of Lemma 4.10 in [19]. ∎

LEMMA 11. *Let $n \geq 1$ be a real number such that $n \geq B(f)$. Let $a$ and $q$ be relatively prime integers with $q \geq 2$, and let $\alpha$ and $\beta$ be real numbers such that $\alpha = a/q + \beta$ and $|\beta| \leq (3qkbn^{k-1})^{-1}$. Then*

$$S(\alpha, n) = \frac{1}{q}\, S(af, q) \int_1^n e(\beta f(t))\, dt + O_k(q^{1-1/k} \log q),$$

$$T(\alpha, n) = \frac{1}{q}\, S(af, q) \int_1^n f'(t) e(\beta f(t))\, dt + O_k(bn^{k-1} q^{1-1/k} \log q).$$

*Proof.* We prove the result for $T(\alpha, n)$ only, the estimate for $S(\alpha, n)$ is proved in a similar fashion. Using the expression $\alpha = a/q + \beta$ we find by using (6) that

$$T(\alpha, n) = \frac{1}{q} \sum_{-q/2 < s \leq q/2} S(af(x) + sx, q) \sum_{1 \leq x \leq n} f'(x) e\left(\beta f(x) - \frac{s}{q}\, x\right). \tag{7}$$

We now approximate the inner sum appearing in (7). Since $n \geq B(f)$ we are able to deduce from Lemma 3 that

$$|f'(t)| \leq f'(n) \leq \frac{3}{2}\, kbn^{k-1} \tag{8}$$

for every $t \in [1, n]$. Thus for every integer $s$ in $(-q/2, q/2]$, the bound on $|\beta|$ implies

$$\left|\beta f'(t) - \frac{s}{q}\right| \leq |\beta f'(t)| + \frac{|s|}{q} \leq \frac{1}{2q} + \frac{1}{2} \leq \frac{3}{4}.$$

These observations and the hypotheses on $h$ indicate that we can apply Lemma 10 with $F(x) = \beta f(x) - sx/q$ and $G(x) = f'(x)$ to obtain

$$\sum_{1 \leq x \leq n} f'(x) e\left(\beta f(x) - \frac{s}{q}\, x\right) = \int_1^n f'(t) e\left(\beta f(t) - \frac{s}{q}\, t\right) dt + O_k(f'(n) + f''(n)).$$

Since $n \geq B(f)$, Lemma 3 implies $f'(n) + f''(n) = O_k(bn^{k-1})$. Thus if we set

$$I(s) = \int_1^n f'(t) e\left(\beta f(t) - \frac{s}{q}\, t\right) dt,$$

then

$$\sum_{1 \leq x \leq n} f'(x) e\left(\beta f(x) - \frac{s}{q}\, x\right) = I(s) + O_k(bn^{k-1}). \tag{9}$$

By (7) and (9) we have

$$T(\alpha, n) = \frac{1}{q} \sum_{-q/2 < s \leq q/2} S(af(x) + sx, q)(I(s) + O_k(bn^{k-1})).$$

By Lemma 8 this implies

$$T(\alpha,n)=\frac{1}{q}\sum_{-q/2<s\le q/2} S(af(x)+sx,q)I(s)+O_k(bn^{k-1}q^{1/2}). \tag{10}$$

For any nonzero integer $s$, (8) and the bound on $|\beta|$ imply

$$\left|\beta f'(t)-\frac{s}{q}\right|\ge\frac{|s|}{q}-|\beta f'(t)|\ge\frac{|s|}{q}-\frac{1}{2q}\ge\frac{|s|}{2q} \tag{11}$$

for all $t\in[1,n]$. Hence when $s\neq 0$ the function $\beta f'(t)-s/q$ is nonzero on the interval $[1,n]$. In this case we can apply Lemma 9, together with (8) and (11), to obtain

$$I(s)=O\left(\frac{f'(n)}{\min|\beta f'-s/q|}\right)=O_k\left(\frac{q}{|s|}\,bn^{k-1}\right). \tag{12}$$

Estimates (10) and (12) imply

$$\begin{aligned}T(\alpha,n)-\frac{1}{q}\,S(af,q)\int_1^n f'(t)e(\beta f(t))\,dt\\ =O_k\left(\left(\sum_{\substack{-q/2<s\le q/2\\ s\neq 0}}\frac{|S(af(x)+sx,q)|}{|s|}+q^{1/2}\right)bn^{k-1}\right).\end{aligned} \tag{13}$$

Let $d=(c'(f),q)$. Since $a$ and $q$ are relatively prime, it follows that for any integer $s$,

$$(c'(af(x)+sx),q)=(c'(af),q)=d.$$

If $d\nmid(af'(0)+s)$, then Lemma 7 implies $S(af(x)+sx,q)=0$. Therefore

$$\sum_{\substack{-q/2<s\le q/2\\ s\neq 0}}\frac{|S(af(x)+sx,q)|}{|s|}=\sum_{\substack{-q/2<s\le q/2\\ s\neq 0\\ s\equiv -af'(0)\,(\mathrm{mod}\,d)}}\frac{|S(af(x)+sx,q)|}{|s|}. \tag{14}$$

If $d\,|\,(af'(0)+s)$ then

$$(c(af(x)+sx),q)=((c'(af),af'(0)+s),q)=(d,af'(0)+s)=d.$$

Lemma 6 then implies $S(af(x)+sx,q)=O_k(d^{1/k}q^{1-1/k})$. Thus by (14),

$$\sum_{\substack{-q/2<s\le q/2\\ s\neq 0}}\frac{|S(af(x)+sx,q)|}{|s|}\ll_k d^{1/k}q^{1-1/k}\sum_{\substack{-q/2<s\le q/2\\ s\neq 0\\ s\equiv -af'(0)\,(\mathrm{mod}\,d)}}\frac{1}{|s|}.$$

This last sum can be estimated by using partial summation to find that

$$\sum_{\substack{-q/2<s\le q/2\\ s\neq 0}}\frac{|S(af(x)+sx,q)|}{|s|}\ll_k q^{1-1/k}\,\frac{\log q}{d}. \tag{15}$$

Finally, (13) and (15) imply

$$T(\alpha,n)=\frac{1}{q}\,S(af,q)\int_1^n g(t)e(\beta f(t))\,dt+O_k(bn^{k-1}q^{1-1/k}\log q),$$

which is the desired result. ∎

**5.2.** *Estimates for the major arcs*

LEMMA 12. *Let $n\ge 1$ be a real number such that $n\ge B(f)$. Let $a,q$ be relatively prime integers with $q\ge 1$, and let $\alpha$ be a real number such that $|\alpha-a/q|\le (3kbqn^{k-1})^{-1}$. If*

$$q\ll\frac{n}{\log n}$$

*then*

$$S(\alpha,n)\ll_k (c(f),q)^{1/k}nq^{-1/k},\qquad T(\alpha,n)\ll_k (c(f),q)^{1/k}bn^kq^{-1/k}.$$

*Proof.* We prove the result for $T(\alpha,n)$ only. Let us assume first that $q\ge 2$ and put $\beta=\alpha-a/q$. We can apply Lemma 11 to obtain

$$T(\alpha,n)=\frac{1}{q}\,S(af,q)\int_1^n f'(t)e(\beta f(t))\,dt+O_k(bn^{k-1}q^{1-1/k}\log q).$$

The upper bound on $q$ implies

$$q^{1-1/k}\log q\ll (q\log n)q^{-1/k}\ll nq^{-1/k}.$$

Since $(a,q)=1$ we deduce that $(c(af),q)=(c(f),q)$, and hence Lemma 6 implies

$$S(af,q)=O_k((c(f),q)^{1/k}q^{1-1/k}).$$

To deal with the integral we note that since $n\ge B(f)$,

$$\Big|\int_1^n f'(t)e(\beta f(t))\,dt\Big|\le\int_1^n f'(t)\,dt\le f(n)\le\frac{3}{2}\,bn^k.$$

Combining the above estimates we obtain

$$T(\alpha,n)\ll_k (c(f),q)^{1/k}bn^kq^{-1/k}.$$

Thus, we have proved the lemma for $q\ge 2$. For $q=1$ we use Lemma 3 to obtain the trivial estimate

$$|T(\alpha,n)|\le\sum_{1\le x\le n}f'(x)\le\int_1^{n+1}f'(t)\,dt\ll_k bn^k.\ \blacksquare$$

**5.3.** *Estimates for the minor arcs.* To obtain estimates for $S(\alpha,n)$ and $T(\alpha,n)$ when $\alpha$ does not satisfy the hypothesis of Lemma 12 we use a result (Lemma 13 below) due to Vinogradov. To state this result we introduce some notation.

For real numbers $R$ and $Q$ such that $1 \le R \le Q$ we write $\mathfrak{s}(R,Q)$ to denote the set of all real numbers $\alpha$ such that there do not exist relatively prime integers $a$ and $q$ that satisfy $1 \le q \le R$ and $|\alpha - a/q| < q^{-1}Q^{-1}$.

If $\boldsymbol{\alpha}$ is an element of $\mathbb{R}^k$, say $\boldsymbol{\alpha} = (\alpha_k, \alpha_{k-1}, \dots, \alpha_1)$, then we define the polynomial $P(\boldsymbol{\alpha}, x)$ in the variable $x$ by

$$P(\boldsymbol{\alpha}, x) = \alpha_k x^k + \alpha_{k-1} x^{k-1} + \cdots + \alpha_1 x. \tag{16}$$

Let $\varrho = \varrho(k)$ be defined by

$$\varrho = \begin{cases} 1/4 & \text{if } k = 2, \\ 1/(8k^2(\log k + 1.5 \log\log k + 4.2)) & \text{if } k \ge 3. \end{cases} \tag{17}$$

LEMMA 13. *Let $k$ and $m$ be positive integers with $k \ge 3$. Let $\boldsymbol{\alpha} = (\alpha_k, \dots, \alpha_1)$ be an element of $\mathbb{R}^k$, and let $c$ be a positive integer such that $c \le m^{2\varrho}$. If $\alpha_k$ is an element of $\mathfrak{s}(m^{1/k}, m^{k-2/k})$ then*

$$\sum_{x=1}^{m} e(P(\boldsymbol{\alpha}, x)) \ll m^{1-\varrho}.$$

*Proof.* This follows from a result of Vinogradov: Theorem 3 of Chapter 4, Section II in [21]. One just needs to note that if $\boldsymbol{\alpha} = (\alpha_k, \dots, \alpha_1)$ is such that $\alpha_k \in \mathfrak{s}(m^{1/k}, m^{k-2/k})$, then $\boldsymbol{\alpha}$ is a point in class II of Vinogradov's theorem. ∎

LEMMA 14. *Suppose that $k$, the degree of $f$, satisfies $k \ge 3$. Let $n \ge 1$ be a real number, sufficiently large in terms of $k$, such that $n \ge B(f)$ and*

$$b \le n^{\varrho}. \tag{18}$$

*Let $R \ge 1$ be a real number such that*

$$R \ll n^{k\varrho}. \tag{19}$$

*Then for every $\alpha \in \mathfrak{s}(R, 4kbn^{k-1})$,*

$$\sup_{1 \le m \le n} |S(\alpha, m)| \ll_k c(f)^{1/k} n R^{-1/k}.$$

*Proof.* If $m \le n^{1-\varrho}$ then the trivial bound implies $|S(\alpha, m)| \le n^{1-\varrho}$. Thus by (19) we obtain

$$|S(\alpha, m)| \ll nR^{-1/k} \ll c(f)^{1/k} n R^{-1/k},$$

the required result. We assume then throughout the rest of the proof that $m$ satisfies

$$n^{1-\varrho} < m \le n. \tag{20}$$

Let $f(x) = bx^k + b_{k-1}x^{k-1} + \cdots + b_0$, and set

$$\boldsymbol{\alpha} = \left(\alpha, \frac{b_{k-1}}{b}\,\alpha, \dots, \frac{b_1}{b}\,\alpha\right).$$

By (16) we can write $P(b\cdot\boldsymbol{\alpha},x)=\alpha(f(x)-f(0))$, hence

$$S(\alpha,m)=e(b_0\alpha)\sum_{x=1}^{m}e(P(b\cdot\boldsymbol{\alpha},x)). \tag{21}$$

The current assumption in (20) implies $n<m^{1/(1-\varrho)}$, and therefore the bound on $b$ in (18) implies $b<m^{\varrho/(1-\varrho)}$. Since $\varrho<1/2$ we deduce that $\varrho/(1-\varrho)<2\varrho$, and therefore the previous inequality involving $b$ implies

$$b<m^{2\varrho}. \tag{22}$$

We now break the proof into two cases.

Case 1: $\alpha\in\mathfrak{s}(m^{1/k},m^{k-2/k})$. By (22) we can apply Lemma 13 to obtain $S(b\cdot\boldsymbol{\alpha},m)\ll m^{1-\varrho}$. Then by (21) we obtain

$$\sum_{x=1}^{m}e(P(b\cdot\boldsymbol{\alpha},x))\ll m^{1-\varrho}.$$

Using the inequality $m\le n$ and (19), we find that $S(\alpha,m)\ll nR^{-1/k}$, which implies the desired result.

Case 2: $\alpha\notin\mathfrak{s}(m^{1/k},m^{k-2/k})$. Then there exist relatively prime integers $a$ and $q$ such that

$$1\le q\le m^{1/k} \tag{23}$$

and

$$\left|\alpha-\frac{a}{q}\right|\le\frac{1}{qm^{k-2/k}}. \tag{24}$$

We will now show, provided $n$ is sufficiently large in terms of $k$, that

$$\left|\alpha-\frac{a}{q}\right|\le(4qkbn^{k-1})^{-1}. \tag{25}$$

Since $\varrho<1/2$ we have $1/(1-\varrho)<1+2\varrho$, and thus (20) implies

$$n<m^{1+2\varrho}.$$

This inequality and (22) imply

$$bn^{k-1}<m^{k+2k\varrho-1}. \tag{26}$$

A calculation shows that $k+2k\varrho-1<k-2/k$. It follows from (20) that as $n$ approaches infinity so does $m$. Therefore (26) implies for $n$ to be large enough in terms of $k$ that

$$4kbn^{k-1}\le m^{k-2/k}.$$

It then follows from (24) that (25) is true. Since $m\le n$, (23) implies

$$q\le m^{1/k}\le\frac{m}{\log m}\le\frac{n}{\log n}. \tag{27}$$

We can apply Lemma 12 in these circumstances to obtain

$$S(\alpha, m) \ll_k (c(f), q)^{1/k} m q^{-1/k} \ll_k c(f)^{1/k} n q^{-1/k}.$$

Since $(a, q) = 1$ and $\alpha \in \mathfrak{s}(R, 4kbn^{k-1})$ we deduce from (25) that $q > R$, and therefore the last estimate implies

$$S(\alpha, m) \ll_k c(f)^{1/k} n R^{-1/k}.$$

This completes the proof. ∎

LEMMA 15. *Let $n \geq 1$ be a real number, sufficiently large in terms of $k$, such that $n \geq B(f)$ and*

$$n^{\varrho} \geq b. \tag{28}$$

*Let $R$ and $Q$ be real numbers such that $1 \leq R < Q$,*

$$R \ll n^{k\varrho}, \tag{29}$$

*and*

$$4kbn^{k-1} \leq Q \ll bn^k/R. \tag{30}$$

*Then for every $\alpha \in \mathfrak{s}(R, Q)$,*

$$T(\alpha, n) \ll_k c(f)^{1/k} b n^k R^{-1/k}.$$

*Proof.* Let $\alpha$ be an element of $\mathfrak{s}(R, Q)$. It can be seen that

$$\mathfrak{s}(R, 4kbn^{k-1}) \subseteq \mathfrak{s}(R, Q).$$

We break the proof into cases.

CASE 1: $\alpha \notin \mathfrak{s}(R, 4kbn^{k-1})$. Then there exist integers $a$ and $q$ such that $(a, q) = 1$,

$$1 \leq q \leq R, \tag{31}$$

and

$$|\alpha - a/q| \leq (4kqbn^{k-1})^{-1}. \tag{32}$$

Let $\beta = \alpha - a/q$. We can apply Lemma 11 to obtain

$$T(\alpha, n) = \frac{1}{q} S(af, q) \int_1^n f'(t) e(\beta f(t))\, dt + O_k(bn^{k-1} q^{1-1/k} \log q). \tag{33}$$

By (29) and (31) we obtain

$$q^{1-1/k} \log q \leq (R \log n) R^{-1/k} \ll n R^{-1/k}.$$

Therefore

$$bn^{k-1} q^{1-1/k} \log q \ll bn^k R^{-1/k}. \tag{34}$$

We now estimate the main term on the right hand side of (33). Since $\alpha \in \mathfrak{s}(R,Q)$ it follows that

$$|\beta| = \left|\alpha - \frac{a}{q}\right| > \frac{1}{qQ}. \tag{35}$$

Thus $\beta$ is nonzero, and therefore

$$\int_1^n f'(t)e(\beta f(t))\,dt = \frac{1}{2\pi i\beta}\left(e(\beta f(n)) - e(\beta f(1))\right) = O(1/|\beta|).$$

This last estimate together with (30) and (35) implies

$$\int_1^n f'(t)e(\beta f(t))\,dt = O_k(qbn^kR^{-1}). \tag{36}$$

From Lemma 6 and the fact that $(a,q)=1$, we deduce

$$S(af,q) = O_k(c(f)^{1/k}q^{1-1/k}). \tag{37}$$

The estimates (31), (36), and (37) imply

$$\frac{1}{q}\,S(af,q)\int_1^n f'(t)e(\beta f(t))\,dt \ll_k c(f)^{1/k}bn^kR^{-1/k}. \tag{38}$$

Finally, by (33), (34), and (38) we obtain

$$T(\alpha,n) \ll_k c(f)^{1/k}bn^kR^{-1/k}.$$

Case 2: $\alpha \in \mathfrak{s}(R,4kbn^{k-1})$. This case is further divided according to the degree of $f$. Assume for now that $k \geq 3$. By partial summation we have

$$T(\alpha,n) = S(\alpha,n)f'(n) - \int_1^n S(f)(\alpha,t)f''(t)\,dt.$$

Hence

$$|T(\alpha,n)| \leq \max_{1\leq m\leq n}|S(\alpha,m)|\Big(|f'(n)| + \int_1^n |f''(t)|\,dt\Big). \tag{39}$$

Since we are assuming $n \geq B(f)$ we have

$$|f'(n)| \ll kbn^{k-1}, \tag{40}$$

$$\int_1^n |f''(t)|\,dt \ll 2kbn^{k-1}. \tag{41}$$

By (39)–(41) we have

$$|T(\alpha,n)| \ll_k bn^{k-1}\max_{1\leq m\leq n}|S(\alpha,m)|.$$

This inequality and Lemma 14 imply

$$T(\alpha,n) \ll_k c(f)^{1/k}bn^kR^{-1/k}.$$

Thus the result is true for $k \geq 3$.

Assume now that $k = 2$. By Dirichlet's approximation theorem there exist integers $a$ and $q$ such that $(a, q) = 1$,

$$1 \le q \le 4bn \tag{42}$$

and

$$\left|\alpha - \frac{a}{q}\right| \le \frac{1}{4qbn}.$$

Set $\beta = \alpha - a/q$. We can apply Lemma 11 to obtain

$$T(\alpha, n) = \frac{1}{q}\, S(af, q) \int_1^n f'(t) e(\beta f(t))\, dt + O(bnq^{1/2} \log q). \tag{43}$$

Inequality (42) and the fact that $\varrho(2) = 1/4$ imply

$$q^{1/2} \log q \ll n^{1/2+\varrho/2} \log n \ll n^{1-\varrho}.$$

Thus

$$q^{1/2} \log q \ll nR^{-1/2}. \tag{44}$$

By the same argument we used in the case $k \ge 3$ we obtain

$$\frac{1}{q}\, S(af, q) \int_1^n f'(t) e(\beta f(t))\, dt \ll c(f)^{1/2} bn^2 q^{-1/2}. \tag{45}$$

Since we are assuming that $\alpha \in \mathfrak{s}(R, 4kbn^{k-1})$, we must have $q > R$. Thus (45) implies

$$\frac{1}{q}\, S(af, q) \int_1^n f'(t) e(\beta f(t))\, dt \ll bn^2 R^{-1/2}. \tag{46}$$

Finally, (43), (44) and (46) imply

$$T(\alpha, n) \ll c(f)^{1/2} bn^2 R^{-1/2}.$$

This completes the proof. ∎

**6. A nonuniformity result.** For any positive integer $q$ and positive real number $\eta$ we let

$$\mathfrak{M}(q, \eta) = \bigcup_{\substack{a=0 \\ (a,q)=1}}^{q} \{\alpha \in [0, 1] : |\alpha - a/q| \le q^{-1}\eta\}.$$

Let $f$ be a polynomial as in Section 5. Throughout this section we let $N$ denote a positive integer such that

$$b \le N^{\varrho/2k}. \tag{47}$$

Define the integer $n$ by

$$f(n) \le N/2 < f(n + 1). \tag{48}$$

We can deduce from Lemma 3 that

$$n \sim (N/2b)^{1/k}, \tag{49}$$

where in this asymptotic relation the implicit constants depend only on $k$ and $B(f)$. For any real number $\alpha$ we let

$$T(\alpha) = T(\alpha, n) = \sum_{x=1}^{n} f'(x)e(\alpha f(x)).$$

LEMMA 16. *Let $N$ be a positive integer sufficiently large in terms of $k$ and $B(f)$. Let $R$ be a real number such that*

$$1 \le R \ll_k N^{\varrho/2}. \tag{50}$$

*If there exists an integer $q$ such that $1 \le q \le R$ and $\alpha \in \mathfrak{M}(q, R/N)$, then*

$$T(\alpha) \ll_k c(f)^{1/k} N q^{-1/k}.$$

*Otherwise*,

$$T(\alpha) \ll_k c(f)^{1/k} N R^{-1/k}.$$

*Proof.* By (47) and (49) we can deduce that

$$N^{1/2k} < n \tag{51}$$

for $N$ sufficiently large in terms of $k$ and $B(f)$. Therefore (50) implies

$$R \ll_k n^{k\varrho} \quad (\ll n/\log n). \tag{52}$$

We can apply Lemma 12 to obtain

$$T(\alpha) \ll_k (c(f), q)^{1/k} b n^k q^{-1/k}.$$

By (49) this implies for $N$ sufficiently large that

$$T(\alpha) \ll_k c(f)^{1/k} N q^{-1/k}.$$

Suppose now that $\alpha$ is not in any of the sets $\mathfrak{M}(q, R/N)$ with $1 \le q \le R$. Then we find that $\alpha \in \mathfrak{s}(R, RN^{-1})$. From the definition of $n$ and (52) we are able to deduce that

$$4kbn^{k-1} \le R^{-1}N \ll bn^k/R.$$

Note that (47) and (51) imply $b < n^{\varrho}$. We can apply Lemma 15 (with $Q = R^{-1}N$) to obtain

$$T(\alpha) \ll_k c(f)^{1/k} b n R^{-1/k}.$$

By (49) this implies

$$T(\alpha) \ll_h N R^{-1/k}$$

for $N$ sufficiently large. ∎

LEMMA 17. *For $N$ sufficiently large in terms of $k$ and $B(f)$ we have*

$$|T(0)| \ge N/8.$$

*Proof.* By Lemma 3 we find that

$$|T(0)| = \sum_{x=1}^{n} f'(x) \geq kb \sum_{x=1}^{n} \left( x^{k-1} - \frac{B(f)}{2}\, x^{k-2} \right).$$

Since $x^{k-1} - (B(h)/2)x^{k-2}$ is an increasing function we have

$$\begin{aligned} \sum_{x=1}^{n} \left( x^{k-1} - \frac{B(f)}{2}\, x^{k-2} \right) &\geq \int_{0}^{n} \left( t^{k-1} - \frac{B(f)}{2}\, t^{k-2} \right) dt \\ &= \frac{1}{k}\, n^k - \frac{B(f)}{2(k-1)}\, n^{k-1}. \end{aligned}$$

Therefore

$$|T(0)| \geq bn^k \left( 1 - \frac{kB(f)}{2(k-1)n} \right).$$

We can assume that $n \geq 2B(f)$ and thus

$$|T(0)| \geq bn^k/2.$$

It then follows from (49) that $|T(0)| \geq N/8$ for $N$ large enough in terms of $k$ and $B(f)$. ∎

LEMMA 18. *Let $N$ be a positive integer sufficiently large in terms of $k$, $B(f)$, and $c(f)$. Suppose that $A$ is a subset of $\{1, \dots, N\}$ with size $\delta N$ such that*

$$\delta \geq N^{-\varrho/4k} \tag{53}$$

*and*

$$W(f, A) \leq \frac{1}{64}\, |A|^2. \tag{54}$$

*Then there exist a real number $R$ $(\geq 1)$ and an integer $q$ such that*

$$c(f)\delta^{-k} \ll_k R \ll_k c(f)\delta^{-k}, \tag{55}$$

$$1 \leq q \leq R, \tag{56}$$

$$\sum_{\substack{t=1 \\ t/N \in \mathfrak{M}(q, R/N)}}^{N-1} |F(t/N)|^2 \gg_k \theta(f, \delta)|A|^2, \tag{57}$$

*where*

$$\theta(f, \delta) = \begin{cases} \delta/\log(2c(f)\delta^{-1}) & \text{if } k = 2, \\ c(f)^{-2/k}\delta^{k-1} & \text{if } k \geq 3. \end{cases} \tag{58}$$

*Proof.* Let $A_1 = \{a \in A : a \leq N/2\}$ and $A_2 = \{a \in A : a > N/2\}$. Then $A$ is the disjoint union of $A_1$ and $A_2$, and we must have $|A_i| \geq |A|/2$ for some $i \in \{1, 2\}$. Without loss of generality let us assume that $|A_1| \geq |A|/2$,

otherwise the proof can easily be adapted for the other case. For any real $\alpha$ we define

$$F_1(\alpha) = \sum_{a \in A_1} e(\alpha a).$$

Note that for any $a \in A$, $b \in A_1$, and integer $x \in \{1, \dots, n\}$, we have

$$-N < a - b - f(x) < N.$$

It follows from (6) that

$$W(f, A) \geq \frac{1}{N} \sum_{t=0}^{N-1} F_1(t/N) F(-t/N) T(t/N).$$

Then by the triangle inequality we obtain

$$\frac{1}{N} |F_1(0)F(0)T(0)| - W(f, A) \leq \frac{1}{N} \sum_{t=1}^{N-1} |F_1(t/N)F(t/N)T(t/N)|.$$

It follows from Lemma 17 and (54) that

$$\frac{1}{64} |A|^2 \leq \frac{1}{N} \sum_{t=1}^{N-1} |F_1(t/N)F(t/N)T(t/N)|. \tag{59}$$

Let

$$R = C(k) \cdot c(f) \delta^{-k},$$

where $C(k)$ is a real number greater than or equal to 1 and whose size we will determine implicitly in terms of $k$. Put

$$\mathfrak{M} = \bigcup_{1 \leq q \leq R} \mathfrak{M}(q, R/N), \qquad \mathfrak{m} = [0, 1] \setminus \mathfrak{M}.$$

By the definition of $R$ and (53) we deduce that

$$R \ll_k N^{\varrho/2}$$

for $N$ sufficiently large in terms of $c(f)$. We can then apply Lemma 16 to deduce that

$$|T(\alpha)| \ll_k c(f)^{1/k} N R^{-1/k}$$

for all $\alpha$ in $\mathfrak{m}$.

It follows from the Cauchy–Schwarz inequality that

$$\begin{aligned} \frac{1}{N} \sum_{\substack{t=1 \\ t/N \in \mathfrak{m}}}^{N-1} & |F_1(t/N)F(t/N)T(t/N)| \\ & \leq \frac{1}{N} \sup_{\alpha \in \mathfrak{m}} |T(\alpha)| (N|A_1|)^{1/2} (N|A|)^{1/2} \ll_k c(f)^{1/k} N |A| R^{-1/k}. \end{aligned} \tag{60}$$

By the definition of $R$ we have

$$c(f)^{1/k}N|A|R^{-1/k} \ll_k C(k)^{-1/k}|A|^2.$$

Therefore we can ask that $C(k)$ be large enough so that (60) implies

$$\frac{1}{N}\sum_{\substack{t=1\\ t/N\in\mathfrak{m}}}^{N-1} |F_1(t/N)F(t/N)T(t/N)| \le \frac{|A|^2}{128}. \tag{61}$$

Since $\mathfrak{m} = [0,1]\setminus\mathfrak{M}$, it follows from (59) and (61) that

$$|A|^2 \ll \frac{1}{N}\sum_{\substack{t=1\\ t/N\in\mathfrak{M}}}^{N-1} |F_1(t/N)F(t/N)T(t/N)|. \tag{62}$$

By the Cauchy–Schwarz inequality and Parseval's relation this implies

$$|A|^2 \ll (|A|/N)^{1/2}\Big(\sum_{\substack{t=1\\ t/N\in\mathfrak{M}}}^{N-1} |F(t/N)T(t/N)|^2\Big)^{1/2}.$$

By squaring both sides and rearranging some terms we find that

$$N|A|^3 \ll \sum_{\substack{t=1\\ t/N\in\mathfrak{M}}}^{N-1} |F(t/N)T(t/N)|^2. \tag{63}$$

Let

$$\mathcal{C}(q) = \sum_{\substack{t=1\\ t/N\in\mathfrak{M}(q,R/N)}}^{N-1} |F(t/N)|^2.$$

Then the definition of $\mathfrak{M}$ and (63) imply

$$N|A|^3 \ll \max_{q\le R}\mathcal{C}(q)\sum_{q\le R}\sup_{\alpha\in\mathfrak{M}(q,R/N)}|T(\alpha)|^2. \tag{64}$$

By Lemma 16 we have $T(\alpha) \ll_k c(f)^{1/k}Nq^{-1/k}$ for all $\alpha\in\mathfrak{M}(q,R/N)$ with $1\le q\le R$. Thus, we can deduce that

$$\sum_{q\le R}\sup_{\alpha\in\mathfrak{M}(q,R/N)}|T(\alpha)|^2 \ll_k \begin{cases} c(f)^{2/k}N^2\log 2R & \text{if } k=2,\\ c(f)^{2/k}N^2R^{1-2/k} & \text{if } k\ge 3.\end{cases}$$

Since $R\ll_k c(f)\delta^{-k}$, this implies

$$\sum_{q\le R}\sup_{r\in\mathfrak{M}(q,R/N)}|T(\alpha)|^2 \ll_k \begin{cases} N^2\log(2c(f)\delta^{-1}) & \text{if } k=2,\\ N^2c(f)^{2/k}\delta^{-k+2} & \text{if } k\ge 3.\end{cases} \tag{65}$$

From (64) and (65) we deduce that

$$\max_{q\le R}\mathcal{C}(q) \gg_k \theta(f,\delta)|A|^2,$$

where $\theta(f,\delta)$ is given by (58). By the definition of $\mathcal{C}(q)$ this completes the proof. ∎

**7. A density increment.** In this section we prove a result, Lemma 20 below, which roughly says that if the generating function for some finite set takes on large values, then the set has a higher density in some arithmetic progression.

LEMMA 19. *Let $L$ and $m$ be positive integers, and $\alpha$ a real number. Set*

$$G(\alpha)=\sum_{k=1}^{L} e(\alpha mk).$$

*Let $q$ be a positive integer such that $q\,|\,m$. If there exists an integer $a$ such that*

$$\left|\alpha-\frac{a}{q}\right| \le \frac{1}{2\pi mL}, \tag{66}$$

*then $|G(\alpha)|\ge L/2$.*

*Proof.* We begin by noting that

$$|G(\alpha)| = \left|L-\sum_{k=0}^{L-1}(1-e(\alpha mk))\right| \ge L-\sum_{k=1}^{L-1}|e(\alpha mk)-1|. \tag{67}$$

Given any real number $x$ let $\|x\|$ denote the distance from $x$ to the nearest integer. For all real $x$ we have $|e(x)-1|\le 2\pi\|x\|$. Thus (67) implies

$$|G(\alpha)| \ge L-2\pi\sum_{k=1}^{L-1}\|\alpha mk\|. \tag{68}$$

If $l$ is a nonnegative integer then (66) implies

$$\left|\alpha ml-\frac{aml}{q}\right| \le \frac{l}{2\pi L}.$$

Since $q\,|\,m$ this implies $\|\alpha ml\|\le l/2\pi L$. Therefore

$$2\pi\sum_{k=1}^{L-1}\|\alpha mk\| \le \frac{1}{L}\sum_{k=1}^{L-1}k \le \frac{L}{2}.$$

It then follows from (68) that $|G(\alpha)|\ge L/2$. ∎

For any subset $X$ of $\{1,\dots,N\}$ and integer $t$, we define the subset $X(t)$ of $\{1,\dots,N\}$ by

$$X(t)=\{z\in\{1,\dots,N\} : z\equiv x+t \pmod N \text{ for some } x\in X\}.$$

If $0 \le t \le N-1$, then

$$X(t) = (t + X) \cap (t - N + X) \cap \{1, \dots, N\}.$$

LEMMA 20. *Let $N$ be a positive integer and $A$ a subset of $\{1, \dots, N\}$ with size $\delta N$. For any real $\alpha$ set*

$$F(\alpha) = \sum_{a \in A} e(\alpha a).$$

*Let $m$ be a positive integer and let $\varepsilon$ be a positive real number such that*

$$m \le 2\pi\varepsilon N \le N. \tag{69}$$

*Let $q$ be a positive integer such that $q \,|\, m$, and let $E = E(q, m, \varepsilon)$ denote the subset of $[0,1]$ defined by*

$$E = \{\alpha \in [0,1] : |\alpha - a/q| \le \varepsilon/m \text{ for some } 0 \le a \le q\}.$$

*If $\theta$ is a positive number such that*

$$\sum_{\substack{t=1 \\ t/N \in E}}^{N-1} |F(t/N)|^2 \ge \theta |A|^2, \tag{70}$$

*then there exists an arithmetic progression $P$ in $\{1, \dots, N\}$ with difference $m$, length $|P| \ge (\delta\theta\varepsilon^{-1})/32\pi$, and such that*

$$|A \cap P| \ge \delta(1 + \theta/8)|P|.$$

*Proof.* Let $L = [(2\pi\varepsilon)^{-1}]$ and $Q = \{mk : k = 1, \dots, L\}$. By (69) we are able to deduce that $L \ge 1$ and $mL \le N$. Thus the arithmetic progression $Q$ is a subset of $\{1, \dots, N\}$ and has length $L \ge \varepsilon^{-1}/4\pi$.

For any real $\alpha$ let $G(\alpha)$ be the exponential sum defined as in the statement of Lemma 19. By Parseval's relation we have

$$\sum_{t=0}^{N-1} |F(t/N)\overline{G(t/N)}|^2 = \frac{1}{N} \sum_{t=0}^{N-1} \Big| \sum_{s=0}^{N-1} F(s/N)\overline{G(s/N)} e(-ts/N) \Big|^2.$$

By (6) we find that

$$\sum_{s=0}^{N-1} F(s/N)\overline{G(s/N)} e(-ts/N) = N|A \cap Q(t)|.$$

It follows that

$$\sum_{t=0}^{N-1} |A \cap Q(t)|^2 = \frac{1}{N} \sum_{t=0}^{N-1} |F(t/N)G(t/N)|^2. \tag{71}$$

From the definition of $L$ we can deduce that $\varepsilon \le (2\pi L)^{-1}$. Thus Lemma 19 implies $|G(\alpha)| \ge L/2$ for any $\alpha \in E$. This estimate together with (70)

and (71) implies

$$\sum_{t=0}^{N-1} |A \cap Q(t)|^2 \geq \frac{1}{N} |F(0)|^2 |G(0)|^2 + \frac{1}{N} \sum_{\substack{t=1 \\ t/N \in E}}^{N-1} |F(t/N)|^2 |G(t/N)|^2$$

$$\geq \delta |A| L^2 + \frac{1}{4} \delta\theta |A| L^2.$$

Let $t' \in \{0, \ldots, N-1\}$ be such that $|A \cap Q(t')|$ is maximal. Then

$$\sum_{t=0}^{N-1} |A \cap Q(t)|^2 \leq |A \cap Q(t')| \sum_{t=0}^{N-1} |A \cap Q(t)| = |A \cap Q(t')|\, |A|\, |Q|.$$

The above inequalities imply

$$|A \cap Q(t')|\, |A| L \geq \delta(1 + \theta/4) |A| L^2.$$

Dividing this inequality through by $|A|L$ we obtain

$$|A \cap Q(t')| \geq \delta(1 + \theta/4) L. \tag{72}$$

If $Q(t')$ is an arithmetic progression, then the result follows from (72) by taking $P$ to be $Q(t')$. If $Q(t')$ is not an arithmetic progression, then it can be verified that $Q(t') = P_1 \cup P_2$, where $P_1$ and $P_2$ are disjoint arithmetic progressions both with difference $m$. Then by (72), we obtain

$$(|A \cap P_1| - \delta |P_1|) + (|A \cap P_2| - \delta |P_2|) \geq \frac{1}{4} \delta\theta L.$$

Thus there exists an index $i \in \{1, 2\}$ such that

$$|A \cap P_i| - \delta |P_i| \geq \frac{1}{8} \delta\theta L.$$

From this inequality we find that $|P_i| \geq (\delta\theta/8) L$ and

$$|A \cap P_i| \geq \delta(1 + \theta/8) |P_i|.$$

The result then follows by taking $P$ to be $P_i$. ∎

**8. Auxiliary polynomials.** Let $h$ be the polynomial given in Theorem 5. Then for every prime $p$ and integer $l$ the congruence equation $h(x) \equiv 0 \pmod{p^l}$ has a solution. It follows by Proposition 1.4 in [11] that $h$ has a root in $\mathbb{Z}_p$, the ring of $p$-adic integers. For each prime $p$ let $z_p$ be a fixed $p$-adic integer which is a root of $h$.

We define the arithmetic function $\lambda$ on the positive integers as follows. We ask that $\lambda$ be completely multiplicative and that its value at the prime $p$ be given by $\lambda(p) = p^m$, where $m$ is the multiplicity of $z_p$ as a root of $h$ over $\mathbb{Q}_p$. It follows that

$$d \mid \lambda(d), \qquad \lambda(d) \mid d^k. \tag{73}$$

Let $v_p$ denote the $p$-adic valuation on $\mathbb{Q}_p$ normalized so that $v_p(p) = 1$. For every positive integer $d$ we define $r_d$ to be the unique integer that satisfies

$$-d < r_d \leq 0 \tag{74}$$

and

$$r_d \equiv z_p \pmod{p^{v_p(d)}\mathbb{Z}_p} \tag{75}$$

for every prime $p$.

For any positive integer $d$ we define $h_d$ to be the polynomial given by

$$h_d(x) = \frac{h(r_d + dx)}{\lambda(d)}. \tag{76}$$

By Taylor's expansion formula we find that

$$h_d(x) = \sum_{j=0}^{k} \frac{h^{(j)}(r_d)}{j!} \left(\frac{d^j}{\lambda(d)}\right) x^j. \tag{77}$$

The leading coefficient of $h$ is $b$, thus by (77) the leading coefficient of $h_d$ is $b(d^k/\lambda(d))$.

LEMMA 21. *Let $d$ be a positive integer. Then $h_d$ is a polynomial with integer coefficients and degree $k$.*

*Proof.* The polynomial $h_d(x)$ clearly has rational coefficients and is of degree $k$. Let $p$ be any prime number. We will show that the coefficients of $h_d(x)$ are $p$-adic integers.

Denote by $m$ the multiplicity of $z_p$ as a root of $h_d(x)$ over $\mathbb{Q}_p$. Then by Gauss' Lemma there exists a polynomial $g(x) \in \mathbb{Z}_p[x]$ such that

$$h(x) = (x - z_p)^m g(x) \quad \text{and} \quad g(z_p) \neq 0.$$

From the definition of $\lambda$ we have $\lambda(p) = p^m$. Let $l$ and $d_1$ be the unique integers such that $d = p^l d_1$ and $p \nmid d_1$. Then by (76) we find that

$$h_d(x) = \frac{(r_d + dx - z_p)^m g(r_d + dx)}{\lambda(d)} = \frac{(p^l d_1 x + r_d - z_p)^m g(r_d + dx)}{p^{lm}\lambda(d_1)}.$$

By (75) we have $z_p \equiv r_d \pmod{p^l\mathbb{Z}_p}$. Hence there exists a $p$-adic integer $y$ such that $z_p = r_d + p^l y$. Using this expression for $z_p$ we can rewrite $h_d(x)$ as

$$h_d(x) = \frac{(d_1 x - y)^m g(r_d + dx)}{\lambda(d_1)}.$$

Since $p \nmid d_1$ we see that $\lambda(d_1)$ is a unit in $\mathbb{Z}_p$. Thus, the above expression for $h_d(x)$ implies that its coefficients are $p$-adic integers.

Since $p$ is an arbitrary prime it follows that $h_d$ is a polynomial with integer coefficients. ∎

LEMMA 22. *Let $d$ and $q$ be positive integers. Then there exists an integer $s$ such that $-q < s \le 0$ and*

$$h_{dq}(x) = \frac{h_d(s+qx)}{\lambda(q)}.$$

*Proof.* It follows from (75) that $r_{dq} \equiv r_d \pmod d$, and hence there exists an integer $s$ such that $r_{dq} = r_d + ds$. Thus by (76) we obtain

$$h_{dq}(x) = \frac{h(r_{dq}+(dq)x)}{\lambda(dq)} = \frac{h(r_d + d(s+qx))}{\lambda(d)\lambda(q)} = \frac{h_d(s+qx)}{\lambda(q)}.$$

We now prove the inequality $-q < s \le 0$. By (74) we know that $-d < r_d \le 0$ and $-dq < r_{dq} \le 0$. From this it follows that

$$s = \frac{r_{dq}-r_d}{d} \le 1 - \frac{1}{d}$$

and

$$s = \frac{r_{dq}-r_d}{d} \ge -q + \frac{1}{d}.$$

Since $s$ is an integer these two inequalities imply $-q < s \le 0$. ∎

LEMMA 23. *Let $d$ and $q$ be positive integers, and let $B$ be a finite set of integers. Put $C = \{c + \lambda(q)b : b \in B\}$. Then*

$$W(h_{dq}, B) \le W(h_d, C).$$

*Proof.* By Lemma 22 there exists an integer $s$ such that $-q < s \le 0$ and

$$h_{dq}(x) = \frac{h_d(s+qx)}{\lambda(q)}.$$

Therefore $b, b' \in B$ satisfy $b - b' = h_{dq}(x)$ if and only if

$$(c + \lambda(q)b) - (c - \lambda(q)b') = h_d(s+qx).$$

Thus $r(B, h_{dq}(x)) = r(C, h_d(s+qx))$, and it follows that

$$W(h_{dq}, B) = \sum_{x\ge 1} h'_{dq}(x) r(B, h_{dq}(x)) = \frac{q}{\lambda(q)} \sum_{x\ge 1} h'_d(s+qx) r(C, h_d(s+qx))$$
$$\le W(h_d, C). \ ∎$$

We recall from Section 4 that $c(f)$ denotes the content of the polynomial $f(x) - f(0)$. We will estimate the numbers $c(h_d)$ and show that as $d$ varies they are uniformly bounded above in terms of $h$ alone. Our estimate for $c(h_d)$ will be obtained by estimating $v_p(c(h_d))$ in terms of $h$ for an arbitrary prime $p$. We begin by giving a relation between $c(h_d)$ and $c(h)$.

LEMMA 24. *Let $d$ be a positive integer. Then $c(h)$ divides $\lambda(d)c(h_d)$, and $c(h_d)$ divides $(d^k/\lambda(d))c(h)$.*

*Proof.* Let us write $h(x) = b_k x^k + \cdots + b_0$ and $h_d(x) = s_k x^k + \cdots + s_0$. So $c(h) = \gcd(b_k, \ldots, b_1)$ and $c(h_d) = \gcd(s_k, \ldots, s_1)$. By (77) we have

$$s_j = \frac{h^{(j)}(r_d)}{j!} \frac{d^j}{\lambda(d)} \tag{78}$$

for $j = 0, \ldots, k$. Now

$$\frac{h^{(j)}(x)}{j!} = \sum_{l=j}^{k} \binom{l}{j} b_l x^{l-j},$$

and thus we deduce that

$$\lambda(d) s_j = d^j \sum_{l=j}^{k} \binom{l}{j} b_l r_d^{l-j}$$

for $j = 0, \ldots, k$. Therefore $c(h)$ divides $\lambda(d)s_j$ for $j = 1, \ldots, k$, and hence $c(h)$ divides $\lambda(d)c(h_d)$.

Now we prove the second result. For $l = 0, \ldots, k$ we have

$$b_l = \frac{h^{(l)}(0)}{l!}.$$

By Taylor's expansion formula,

$$h^{(l)}(x+y) = \sum_{i=0}^{k-l} \frac{h^{(l+i)}(x)}{i!}\, y^i = \sum_{j=l}^{k} \frac{h^{(j)}(x)}{(j-l)!}\, y^{j-l}.$$

Therefore

$$b_l = \frac{h^{(l)}(r_d - r_d)}{l!} = \sum_{j=l}^{k} \frac{h^{(j)}(r_d)}{l!(j-l)!} (-r_d)^{j-l} = \sum_{j=l}^{k} \binom{j}{l} \left( \frac{h^{(j)}(r_d)}{j!} \right) (-r_d)^{j-l}$$

for $l = 0, \ldots, k$. It follows by (78) that

$$\frac{d^k}{\lambda(d)}\, b_l = \sum_{j=l}^{k} \binom{j}{l} (-r_d)^{j-l} d^{k-j} s_j$$

for $l = 0, \ldots, k$. Therefore $c(h_d)$ divides $(d^k/\lambda(d))b_l$ for $l = 1, \ldots, k$, and hence $c(h_d)$ divides $(d^k/\lambda(d))c(h)$. ∎

A prime $p$ divides $\lambda(d)$ if and only if it divides $d$. Therefore the previous lemma implies the following result.

LEMMA 25. *Let $d$ be a positive integer and $p$ a prime number such that $p \nmid d$. Then*

$$v_p(c(h_d)) = v_p(c(h)).$$

To approximate $v_p(c(h_d))$ when $p$ divides $d$ we use the notion of the semi-discriminant introduced by Chudnovsky [4, p. 63]. Let $f(x)$ be a polynomial

of degree $k \geq 1$ with coefficients from a field $K$. Suppose that in some splitting field,

$$f(x) = a(x-\eta_1)^{e_1} \cdots (x-\eta_r)^{e_r},$$

where all the $\eta_i$ are distinct. Then the semidiscriminant of $f$, which we denote by $\Delta(f)$, is given by

$$\Delta(f) = a^{2k-2} \prod_{i \neq j} (\eta_i - \eta_j)^{e_i e_j}.$$

An important feature of the semidiscriminant is that it is never zero. It can be shown that $\Delta(f)$ is an element of $K$ and is independent of the splitting field over which $f(x)$ factors. Furthermore, if $f(x) = a_n x^n + \cdots + a_0$ then $\Delta(f)$ can be expressed as $G(a_0, \ldots, a_n)$, where $G(x_0, \ldots, x_n)$ is a polynomial with integer coefficients. As a consequence, if the coefficients of $f(x)$ are algebraic over $K$ then so is $\Delta(f)$.

LEMMA 26. *Let $f$ be a polynomial of degree $k$ ($\geq 1$). Suppose that $\alpha$ is a root of $f(x)$ with multiplicity $m \geq 1$, and that $g$ is a polynomial such that $f(x) = (x-\alpha)^m g(x)$. Then*

$$\Delta(f) = (-1)^{(k-m)m} g(\alpha)^{2m} \Delta(g).$$

*Proof.* Suppose that $f$ has leading coefficient $a$. Then the polynomial $g$ has degree $k-m$ and leading coefficient $a$. Let $\eta_1, \ldots, \eta_r$ be the distinct roots of $g$. Then

$$g(x) = a(x-\eta_1)^{e_1} \cdots (x-\eta_r)^{e_r},$$

where $e_1, \ldots, e_r$ are positive integers satisfying

$$e_1 + \cdots + e_r = k - m. \tag{79}$$

The semidiscriminant of $f$ can be written as

$$\Delta(f) = a^{2k-2} \prod_{i=1}^{r} (\alpha - \eta_i)^{me_i} \prod_{i=1}^{r} (\eta_i - \alpha)^{e_i m} \prod_{i \neq j} (\eta_i - \eta_j)^{e_i e_j}.$$

By (79) the middle product on the right can be written as

$$\prod_{i=1}^{r} (\eta_i - \alpha)^{e_i m} = (-1)^{(k-m)m} \prod_{i=1}^{r} (\alpha - \eta_i)^{me_i}.$$

Thus

$$\begin{aligned}\Delta(f) &= (-1)^{(k-m)m} \Big( a \prod_{i=1}^{r} (\alpha - \eta_i)^{e_i} \Big)^{2m} \Big( a^{2(k-m)-2} \prod_{i \neq j} (\eta_i - \eta_j)^{e_i e_j} \Big) \\ &= (-1)^{(k-m)m} g(\alpha)^{2m} \Delta(g). \ \blacksquare\end{aligned}$$

LEMMA 27. *Let $p$ be a prime divisor of the positive integer $d$. Then*

$$v_p(c(h_d)) \leq v_p(c(h)) + \frac{k-1}{2}\, v_p(\Delta(h)).$$

*Proof.* Denote by $m$ the multiplicity of $z_p$ as a root of $h_d(x)$ over $\mathbb{Q}_p$. Then $1 \leq m \leq k$ and by Taylor's expansion formula $h_d^{(m)}(0)/m!$ is a coefficient of $h_d(x)$ which is not the constant term. It follows that

$$v_p(c(h_d)) \leq v_p(h_d^{(m)}(0)/m!). \tag{80}$$

Let $l$ and $d_1$ by the unique positive integers such that $d = p^l d_1$ and $p \nmid d_1$. There exists a polynomial $g(X)$ in $\mathbb{Z}_p[X]$ such that $g(z_p) \neq 0$ and

$$h(x) = (x - z_p)^m g(X). \tag{81}$$

As in the proof of Lemma 21 there exists a $p$-adic integer $y$ such that

$$h_d(x) = \frac{(d_1 x - y)^m g(r_d + p^l d_1 x)}{\lambda(d_1)}.$$

By Leibniz's formula,

$$h_d^{(m)}(x) = \frac{1}{\lambda(d_1)} \sum_{j=0}^{m} \binom{m}{j} \frac{\partial^{m-j}}{\partial x} (xd_1 - y)^m \frac{\partial^j}{\partial x} g(r_d + p^l d_1 x).$$

Now

$$\frac{\partial^{m-j}}{\partial x} (d_1 x - y)^m = d_1^{m-j} \frac{m!}{j!} (d_1 x - y)^j,$$

$$\frac{\partial^j}{\partial x} g(r + p^l d_1 x) = d_1^j p^{lj} g^{(j)}(r + d_1 p^l x).$$

Therefore

$$\frac{h_d^{(m)}(0)}{m!} = \frac{d_1^m}{\lambda(d_1)} \sum_{j=0}^{m} p^{lj} \binom{m}{j} (-y)^j \frac{g^{(j)}(r_d)}{j!}.$$

Inspecting the sum in the previous equation we see that all of its summands corresponding to a positive index are divisible by $p^l$. Therefore

$$\frac{h_d^{(m)}(0)}{m!} \equiv \frac{d_1^m}{\lambda(d_1)}\, g(r_d) \pmod{p^l \mathbb{Z}_p}.$$

From (75) we have $r_d \equiv z_p \pmod{p^l \mathbb{Z}_p}$. By the previous two congruence equations there exists a $p$-adic integer $y$ such that

$$\frac{h_d^{(m)}(0)}{m!} = \frac{d_1^m}{\lambda(d_1)}\, g(z_p) + p^l y. \tag{82}$$

By (81) and Lemma 26 we obtain $\Delta(h) = \pm g(z_p)^{2m} \Delta(g)$, and therefore

$$v_p(\Delta(h)) = 2m v_p(g(z_p)) + v_p(\Delta(g)).$$

Since $g(X) \in \mathbb{Z}_p[X]$ it follows that $\Delta(g) \in \mathbb{Z}_p$, and hence $v_p(\Delta(g)) \geq 0$. Therefore the previous equation implies

$$2mv_p(g(z_p)) \leq v_p(\Delta(h)).$$

Recall that $p \nmid d_1$; therefore $v_p(d_1^m/\lambda(d_1)) = 0$. It then follows that

$$v_p\left(\frac{d_1^m}{\lambda(d_1)}\, g(z_p)\right) \leq \frac{1}{2m}\, v_p(\Delta(h)). \tag{83}$$

Assume now that $v_p(\Delta(h)) < 2ml$. Then

$$v_p\left(\frac{d_1^m}{\lambda(d_1)}\, g(z_p)\right) < l. \tag{84}$$

By (82)–(84) we deduce that

$$v_p\left(\frac{h_d^{(m)}(0)}{m!}\right) = v_p\left(\frac{d_1^m}{\lambda(d_1)}\, g(z_p)\right) \leq \frac{1}{2m}\, v_p(\Delta(h)).$$

Therefore by (80) we have

$$v_p(c(h_d)) \leq \frac{1}{2m}\, v_p(\Delta(h)).$$

Since $m \geq 1$, this implies the result of the lemma when $v_p(\Delta(h)) < 2ml$.

Let us now assume that

$$v_p(\Delta(h)) \geq 2ml. \tag{85}$$

By Lemma 24 we see that $c(h_d)$ divides $(d^k/\lambda(d))c(h)$. Therefore

$$v_p(c(h_d)) \leq v_p(d^k/\lambda(d)) + v_p(c(h)).$$

Since $d = p^l d_1$ with $p \nmid d_1$, we have

$$v_p(d^k/\lambda(d)) = v_p(p^{kl}/p^{ml}) = (k-m)l.$$

Therefore

$$v_p(c(h_d)) \leq (k-m)l + v_p(c(h)).$$

By (85) this implies

$$v_p(c(h_d)) \leq \frac{k-m}{2m}\, v_p(\Delta(h)) + v_p(c(h)).$$

Since $m \geq 1$, it follows that

$$v_p(c(h_d)) \leq \frac{k-1}{2}\, v_p(\Delta(h)) + v_p(c(h)).$$

This completes the proof. ∎

LEMMA 28. *For any positive integer $d$,*

$$c(h_d) \leq |\Delta(h)|^{(k-1)/2} c(h).$$

*Proof.* This follows from Lemmas 25 and 27. ∎

We end this section with two technical lemmas which we need in the next section. For the next result we remind the reader of the notation introduced in (4).

LEMMA 29. *For any positive integer $d$,*

$$B(h_d) \le 2^{k-1} k (B(h) + 2).$$

*Proof.* Let us put $h(x) = b_k x^k + b_{k-1} x^{k-1} + \cdots + b_0$ and $h_d(x) = s_k x^k + s_{k-1} x^{k-1} + \cdots + s_0$. By (77) we have that

$$s_j = \frac{h^{(j)}(r_d)}{j!} \frac{d^j}{\lambda(d)}$$

for $j = 0, \ldots, k$. Now

$$\frac{h^{(j)}(x)}{j!} = \sum_{l=j}^{k} \binom{l}{j} b_l x^{l-j},$$

so that

$$|s_j| = \left| \sum_{l=j}^{k} \binom{l}{j} b_l r_d^{l-j} \frac{d^j}{\lambda(d)} \right| \le \frac{d^j}{\lambda(d)} \sum_{l=j}^{k} \binom{l}{j} |b_l| \, |r_d|^{l-j}$$

for $j = 0, \ldots, k$. Since $|r_d| < d$, this implies

$$|s_j| \le \frac{d^k}{\lambda(d)} \sum_{l=j}^{k} \binom{l}{j} |b_l| \le 2^k \frac{d^k}{\lambda(d)} \sum_{l=0}^{k} |b_l| = 2^{k-1} \frac{d^k}{\lambda(d)} b_k (B(h) + 2)$$

for $j = 0, \ldots, k$. By (77) the leading coefficient of $h_d$ is $s_k = b_k (d^k / \lambda(d))$, thus the above implies

$$B(h_d) = \frac{2}{|s_k|} (|s_0| + \cdots + |s_{k-1}|) = 2^k k (B(h) + 2). \ ∎$$

LEMMA 30. *For every positive integer $d$ the polynomials $h_d(x)$, $h_d'(x)$, and $h_d''(x)$ are positive and increasing for $x \ge 1$.*

*Proof.* Let $d$ be a positive integer and $j$ an integer from $\{0, 1, 2\}$. Then

$$h_d^{(j)}(x) = \frac{d^j}{\lambda(d)} h^{(j)}(r_d + dx).$$

By definition $-d < r_d \le 0$, therefore $r_d + dx > 0$ whenever $x \ge 1$. Since $h^{(j)}(x)$ is positive and increasing for $x \ge 1$, it follows that $h_d^{(j)}(x)$ is positive and increasing for $x \ge 1$. ∎

**9. The iteration step.** The results of Sections 6–8 will now be used to prove a lemma which will be the basis for our proof of Theorem 5. Before stating the lemma we define the ($k$-dependent) real-valued function $\theta$ on the positive reals by

$$\theta(x) = \begin{cases} \dfrac{x}{2\log(2x^{-1})} & \text{if } k = 2, \\ x^{k-1} & \text{if } k \geq 3. \end{cases} \tag{86}$$

Note that $\theta(x) \in (0,1]$ whenever $x \in (0,1]$.

LEMMA 31. *Let $N$ be a positive integer sufficiently large in terms of $h$, and let $d$ be a positive integer such that*

$$d \leq N^{\varrho/4k^2}. \tag{87}$$

*Suppose $A$ be a subset of $\{1,\dots,N\}$ with size $\delta N$ such that*

$$\delta \geq N^{-\varrho/2k} \tag{88}$$

*and*

$$W(h_d, A) \leq \frac{1}{64}\,|A|^2. \tag{89}$$

*Then there exist positive integers $d'$ and $N'$, and a set $A' \subseteq \{1,\dots,N'\}$ of size $\delta' N'$, such that*

$$W(h_{d'}, A') \leq W(h_d, A), \qquad \delta' \geq \delta(1 + C_1\theta(\delta)),$$
$$C_2\delta^{2k^2} N \leq N' \leq N, \qquad d \leq d' \leq C_3\delta^{-k} d.$$

*Here, $C_1$, $C_2$, and $C_3$ are positive constants that depend only on $h$.*

*Proof.* Note that by Lemmas 28 and 29, by taking $N$ sufficiently large in terms of $h$ alone we can consider $N$ to be sufficiently large in terms of $B(h_d)$ and $c(h_d)$ regardless of the value of $d$.

Let $b_{(d)}$ denote the leading coefficient of $h_d$. By (77) we have $b_{(d)} = bd^k/\lambda(d)$, and from (73) we find that $b_{(d)} \leq bd^{k-1}$. It then follows by (87) that we can take $N$ large enough in terms of $h$ so that

$$b_{(d)} \leq N^{\varrho/2k}. \tag{90}$$

By Lemma 30, (88)–(90), and the remark made at the begining of this proof, we can apply Lemma 18 with $f$ replaced by $h_d$ to obtain a real number $R$ ($\geq 1$) and an integer $q$ such that

$$c(h_d)\delta^{-k} \ll_k R \ll_k c(h_d)\delta^{-1}, \tag{91}$$

$$1 \leq q \leq R, \tag{92}$$

$$\sum_{\substack{t=1 \\ t/N \in \mathfrak{M}(q,R/N)}}^{N-1} |F(t/N)|^2 \gg_k \theta(h_d,\delta)|A|^2. \tag{93}$$

We note that (58), (86), and Lemma 28 imply

$$\theta(h_d, \delta) \gg_h \theta(\delta). \tag{94}$$

Let us set $m = \lambda(q)$ and $\varepsilon = \lambda(q)R/qN$. Then the set $E = E(q, m, \varepsilon)$ defined in Lemma 20 satisfies $\mathfrak{M}(q, R/N) \subseteq E$. Therefore (93) and (94) imply

$$\sum_{\substack{t=1 \\ t/N \in E}}^{N-1} |F(t/N)|^2 \gg_h \theta(\delta)|A|^2.$$

We will apply Lemma 20 to this estimate. To do so we must show that the values given to $m$ and $\varepsilon$ satisfy the conditions in (69), that is,

$$\lambda(q) \le 2\pi \frac{\lambda(q)R}{qN} N \le N.$$

The first inequality here is true by (92). The second inequality follows for $N$ sufficiently large in terms of $h$ since by (17), (73), (88), (91), and (92),

$$\frac{\lambda(q)R}{q} \le R^k \ll_h \delta^{-k^2} \ll_h N^{1/2}.$$

Therefore we can apply Lemma 20 to deduce that there exists an arithmetic progression $P$ in $\{1, \dots, N\}$, with difference $m = \lambda(q)$, length

$$|P| \gg \delta\theta(\delta)\varepsilon^{-1}, \tag{95}$$

and such that

$$|A \cap P| \ge \delta(1 + C_1\theta(\delta))|P|, \tag{96}$$

where $C_1$ is some positive number that depends only on $h$.

Let $N' = |P|$. Then there exist an integer $c$ and a set $A' \subseteq \{1, \dots, N'\}$ such that $A \cap P = \{c + \lambda(q)b : b \in A'\}$. An application of Lemma 23 (with $B = A'$ and $C = A \cap P$) shows that

$$W(h_{dq}, A') \le W(h_d, A \cap P).$$

Put $d' = dq$; then the above implies

$$W(h_{d'}, A') \le W(h_d, A).$$

Let the size of $A'$ be $\delta' N'$. Then (96) implies

$$\delta' \ge \delta(1 + C_1\theta(\delta)).$$

All that is left to do is to estimate $N'$ $(= |P|)$ and $d'$. Using (73), (86), (91), and (95) we are able to infer for $k \ge 2$ and for $N$ sufficiently large in terms of $h$ that

$$N' \gg_h \delta\theta(\delta)\varepsilon^{-1} \gg_h N\delta^{2k^2}.$$

Thus there exists a positive number $C_2$ that depends only on $h$ such that

$$C_2 N\delta^{2k^2} \le N' \le N.$$

Since $d' = dq$ it follows from (92) that $d \leq d' \leq Rd$. Then by Lemma 28 and (91) we can deduce that there exists a positive number $C_3$ that depends only on $h$ such that

$$d \leq d' \leq C_3 \delta^{-1} d.$$

This completes the proof. ∎

**10. The proof of Theorem 5.** We are now ready to prove Theorem 5, which we remind the reader implies both Theorem 1 and Theorem 2.

*Proof of Theorem 5.* Let $N$ be a positive integer which is sufficiently large in terms of $h$. Let $A$ be a subset of $\{1, \ldots, N\}$ and size $\delta N$. Let $\mu$ be defined as in (2). Suppose that

$$\delta \geq C \frac{(\log \log N)^{\mu/(k-1)}}{(\log N)^{1/(k-1)}}, \tag{97}$$

where $C$ is a positive number that depends only on $h$. Let $C_1$, $C_2$ and $C_3$ be the positive numbers given in Lemma 31. We define the positive integer $Z$ by

$$Z = [8C_1^{-1}\delta^{-(k-1)}(\log 2\delta^{-1})^{\mu-1}]. \tag{98}$$

For $N$ sufficiently large in terms $h$ it follows from (97) that

$$Z \leq 8C^{-1}C_1^{-1} \frac{\log N}{\log \log N}. \tag{99}$$

Assume that

$$W(h, A) \leq \frac{1}{64} (C_2^2 \delta^{4k^2})^Z |A|^2. \tag{100}$$

We will show that this assumption leads to a contradiction. Set

$$N_0 = N, \quad A_0 = A, \quad \delta_0 = \delta, \quad d_0 = 1.$$

We will inductively construct a finite sequence of quadruples

$$\{(N_i, A_i, \delta_i, d_i)\}_{i=0}^{Z},$$

where for each $1 \leq i \leq Z$, $N_i$ and $d_i$ are positive integers, $A_i \subseteq \{1, \ldots, N_i\}$, and $\delta_i = |A_i|/N_i$. Furthermore:

$$W(h_{d_i}, A_i) \leq \frac{1}{64} (C_2^2 \delta_i^{4k^2})^{Z-i} |A_i|^2, \tag{101}$$

$$\delta_i \geq \delta_{i-1}(1 + C_1\theta(\delta_{i-1})), \tag{102}$$

$$C_2 \delta_{i-1}^{2k^2} N_{i-1} \leq N_i \leq N_{i-1}, \tag{103}$$

$$d_{i-1} \leq d_i \leq C_3 \delta_i^{-k} d_{i-1}. \tag{104}$$

Let $0 \leq l \leq Z - 1$, and suppose we have obtained the first $l$ terms of the sequence. We will use Lemma 20 to find the succeeding $(l+1)$th term.

We begin by estimating $N_l$ in terms of $N$. By (103) and (102) we can deduce that

$$N_l \geq \Big( \prod_{j=0}^{l-1} C_2 \delta_j^{2k^2} \Big) N_0 \geq (C_2 \delta^{2k^2})^Z N.$$

Taking logarithms we find that

$$\log N_l \geq \log N - Z \log (C_2 \delta^{2k^2})^{-1}. \tag{105}$$

By (97) and (99) we have, for large $N$,

$$Z \log (C_2 \delta^{2k^2})^{-1} \ll_h C^{-1} \log N.$$

Therefore we can take $C$ to be large enough so that (105) implies

$$\log N_l \geq \frac{1}{2} \log N. \tag{106}$$

Hence $N_l \geq N^{1/2}$, and thus we can assume that $N_l$ is large in terms of $h$ whenever $N$ is.

We now give an estimate for $d_l$. Since $C_3 \geq 1$ we deduce from (104) that

$$d_l \leq \Big( \prod_{j=1}^{l} C_3 \delta_j^{-k} \Big) d_0 \leq (C_3 \delta^{-k})^Z.$$

Thus

$$\log d_l \leq Z \log (C_3 \delta^{-k}).$$

By (97) and (99) we deduce that

$$\log d_l \ll_h C^{-1} \log N.$$

We ask that $C$ be large enough so that this implies

$$\log d_l \leq \frac{\varrho}{8k^2} \log N.$$

By (106) this implies $\log d_l \leq (\varrho/4k^2) \log N_l$, and hence

$$d_l \leq N_l^{\varrho/4k^2}. \tag{107}$$

We now estimate $\delta_l$. By (102) we deduce that $\delta_l \geq \delta_0^Z$, and therefore

$$\log \delta_l^{-1} \leq Z \log \delta^{-1}.$$

By taking $C$ to be large enough, an argument similar to the one used to estimate $d_l$ shows that, for large $N$,

$$\delta_l \geq N_l^{-\varrho/2k}. \tag{108}$$

Since $l < Z$ and $C_2 < 1$ it follows from (101) that

$$W(h_{d_l}, A_l) \leq \frac{1}{64} |A_l|^2. \tag{109}$$

By (107)–(109) we can apply Lemma 18 with $N$, $d$, and $A$ replaced by $N_l$, $d_l$ and $A_l$ respectively. By relabeling the results of Lemma 18, we obtain an integer $N_{l+1}$ and a subset $A_{l+1}$ of $\{1,\dots,N_{l+1}\}$ of size $|A_{l+1}| = \delta_{l+1}N_{l+1}$ such that

$$C_2\delta_l^{2k^2}N_l \le N_{l+1} \le N_l, \tag{110}$$

$$\delta_{l+1} \ge \delta_l(1 + C_1\theta(\delta_l)). \tag{111}$$

Furthermore, there exists an integer $d_{l+1}$ such that

$$d_l \le d_{l+1} \le C_3\delta_l^{-k}d_l, \tag{112}$$

$$W(h_{d_{l+1}}, A_{l+1}) \le W(h_{d_l}, A_l). \tag{113}$$

It follows from (101) that

$$W(h_{d_{l+1}}, A_{l+1}) \le \frac{1}{64}\,(C_2^2\delta_l^{4k^2})^{Z-l}|A_l|^2. \tag{114}$$

From (110) and (111) we can deduce that

$$|A_l| = \delta_l N_l \le \delta_{l+1}C_2^{-1}\delta_l^{-2k^2}N_{l+1} = C_2^{-1}\delta_l^{-2k^2}|A_{l+1}|. \tag{115}$$

Then (114) and (115) imply

$$W(h_{d_l+1}, A_{l+1}) \le \frac{1}{64}\,(C_2^2\delta_{l+1}^{4k^2})^{Z-(l+1)}|A_{l+1}|^2. \tag{116}$$

By induction we can conclude that there exist a finite sequence of quadruples $\{(N_i, A_i, \delta_i, d_i)\}_{i=1}^{Z}$ whose components satisfy the properties in (101)–(104). Since $\theta(x)$ is increasing for $x > 0$, repeated applications of (102) imply

$$\delta_Z \ge \delta_0(1 + C_1\theta(\delta_0))^Z = \delta(1 + C_1\theta(\delta))^Z.$$

Taking the logarithm we obtain

$$\log\delta_Z \ge Z\log(1 + C_1\theta(\delta)) - \log\delta^{-1} \ge Z\,\frac{C_1\theta(\delta)}{2} - \log 2\delta^{-1}. \tag{117}$$

(Here we used the fact that $\log(1+x) \ge x/2$ whenever $0 \le x \le 1$.)

Assume now that $k \ge 3$. Then (98) and (117) imply

$$\log\delta_Z \ge 4C_1^{-1}\delta^{-(k-1)}(\log 2\delta^{-1})C_1\delta^{k-1}/2 - \log 2\delta^{-1},$$

and thus

$$\log\delta_Z \ge \log 2\delta^{-1} > 0. \tag{118}$$

A calculation shows that (118) is also true when $k = 2$. From (118) we find that $\delta_Z > 1$, a contradiction. Therefore (100) is false, and thus

$$W(A, h) \ge \frac{1}{64}\,(C_2^2\delta^{4k^2})^Z N^2\delta^2. \tag{119}$$

By (98) we have

$$(C_2^2\delta^{4k^2})^Z = \exp(-Z\log C_2^{-2}\delta^{-4k^2})$$
$$= \exp([-8C_1^{-1}\delta^{-(k-1)}(\log 2\delta^{-1})^{\mu-1}]\log C_2^{-2}\delta^{-4k^2}).$$

Thus there exists a positive number $C'$ such that

$$(C_2^2\delta^{4k^2})^Z \geq \exp(-C'\delta^{-(k-1)}(\log 2\delta^{-1})^{\mu}). \tag{120}$$

By (119) and (120) we obtain

$$W(A,h) \geq \frac{1}{64}\,|A|^2\exp(-C'\delta^{-(k-1)}(\log 2\delta^{-1})^{\mu}).$$

This completes the proof. ∎

## References


[1] A. Balog, J. Pelikán, J. Pintz and E. Szemerédi, *Difference sets without $\kappa$-th powers*, Acta Math. Hungar. 65 (1994), 165–187.

[2] D. Berend and Y. Bilu, *Polynomials with roots modulo every integer*, Proc. Amer. Math. Soc. 124 (1996), 1663–1671.

[3] J. R. Chen, *On Professor Hua's estimate of exponential sums*, Sci. Sinica 20 (1977), 711–719.

[4] G. V. Chudnovsky, *Contributions to the Theory of Transcendental Numbers*, Math. Surveys Monogr. 19, Amer. Math. Soc., Providence, RI, 1984.

[5] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. 31 (1977), 204–256.

[6] W. T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. 11 (2001), 465–588.

[7] B. Green, *On arithmetic structures in dense sets of integers*, Duke Math. J. 114 (2002), 215–238.

[8] T. Kamae and M. Mendès France, *Van der Corput's difference theorem*, Israel J. Math. 31 (1978), 335–342.

[9] J. Lucier, *Polynomials and intersective sets*, doctoral thesis, Univ. of Waterloo, 2004.

[10] V. I. Nečaev [V. I. Nechaev], *An estimate of the complete rational trigonometrical sum*, Mat. Zametki 17 (1975), 839–849 (in Russian); English transl.: Math. Notes 17 (1975), 504–511.

[11] J. Neukirch, *Algebraic Number Theory*, Springer, Berlin, 1999.

[12] J. Pintz, W. L. Steiger and E. Szemerédi, *On sets of natural numbers whose difference set contains no squares*, J. London Math. Soc. 37 (1988), 219–231.

[13] I. Z. Ruzsa, *On measures of intersectivity*, Acta Math. Hungar. 43 (1984), 335–340.

[14] —, *Difference sets without squares*, Period. Math. Hungar. 15 (1984), 205–209.

[15] A. Sárközy, *On difference sets of sequences on integers I*, Acta Math. Acad. Sci. Hungar. 31 (1978), 125–149.

[16] —, *On difference sets of sequences on integers III*, ibid., 355–386.

[17] S. Slijepčević, *A polynomial Sárközy–Furstenberg theorem with upper bounds*, Acta Math. Hungar. 98 (2003), 111–128.

[18] S. Srinivasan, *On a result of Sárközy and Furstenberg*, Nieuw Arch. Wisk. (4) 3 (1985), 275–280.

[19] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford Univ. Press, Oxford, 1951.
[20] R. C. Vaughan, *The Hardy–Littlewood Method*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.
[21] I. M. Vinogradov, *Selected Works*, Springer, Heidelberg, 1985.

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada N2L 3GI
E-mail: jlucier@uwaterloo.ca

*Received on 9.9.2005*
*and in revised form on 31.1.2006* (5066)