Can. J. Math., Vol. XL, No. 4, 1988, pp. 788-816

# ON DIVISORS OF SUMS OF INTEGERS IV

A. SÁRKÖZY AND C. L. STEWART

**1. Introduction.** Throughout this article $c_0, c_1, c_2, \dots$ will denote effectively computable positive absolute constants. Denote the cardinality of a set $X$ by $|X|$. Let $N$ be a positive integer and let $A$ and $B$ be non-empty subsets of $\{1, \dots, N\}$. Put

$$A_0 = \{a \in A | (N/2) < a \leqq N\} \text{ and}$$

$$B_0 = \{b \in B | (N/2) < b \leqq N\}.$$

In [**3**], Balog and Sárközy proved that if $N > c_0$ and

(1) $\quad ( |A_0||B_0| )^{1/2} > c_1 N^{12/13} (\log N)^{21/13},$

then there exist $a_0$ and $b_0$ with $a_0 \in A_0$ and $b_0 \in B_0$ and a prime number $p$ such that

$$p^2 | (a_0 + b_0)$$

and

(2) $\quad p^2 > c_2 ( |A_0| \, |B_0| )^{5/2} / (N^4 (\log N)^7).$

If follows from this result that if $|A| \gg N$ and $|B| \gg N$ then there exist $a$ in $A$ and $b$ in $B$ and a prime $p$ such that $p^2 | (a + b)$ with

$$p^2 \gg N/(\log N)^7.$$

Let $k$ be an integer with $k \geqq 2$. We shall prove that if $|A| \gg N$ and $|B| \gg N$ then there exist $\gg_k N^{1+(1/k)}/\log N$ pairs $(a, b)$ with $a$ in $A$ and $b$ in $B$ for which $a + b$ is divisible by $p^k$ with $p$ a prime and

$$p^k \gg_k N.$$

This result is best possible, up to determination of constants, both with respect to the number of pairs $(a, b)$ and also with respect to the lower bound for $p^k$. It follows from Theorem 1 below.

The case $k = 1$ was considered by Balog and Sárközy in [**2**]. They proved, by means of the large sieve inequality, that if $|A| \gg N$ and $|B| \gg N$ then there exist $a$ in $A$ and $b$ in $B$ and a prime $p$ with $p | (a + b)$ and

Received February 5, 1987. The research of the second author was supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

$$p \gg N/\log N.$$

In part II of this series [**9**] we showed, by means of the Hardy-Littlewood method, that if $|A| \gg N$ and $|B| \gg N$ then there exist $\gg N^2/\log N$ pairs $(a, b)$ with $a$ in $A$ and $b$ in $B$ for which $a + b$ is divisible by a prime $p$ with

$$p \gg N.$$

Put

$$R = 3N/(|A|\,|B|)^{1/2},$$

and

$$(3) \quad \theta_k = (1 + 2k4^{k-1})^{-1},$$

for $k \geqq 2$.

THEOREM 1. *Let $N$ and $k$ be positive integers with $k \geqq 2$, let $A$ and $B$ be subsets of $\{1, \dots, N\}$ and let $\epsilon$ be a positive real number. There exist effectively computable positive absolute constants $c_3$ and $c_4$ and positive numbers $C_0$, $C_1$ and $N_0$ which are effectively computable in terms of $\epsilon$ and $k$ such that if $N > N_0$ and*

$$(4) \quad (|A|\,|B|)^{1/2} > N^{1-\theta_k+\epsilon},$$

*then there exist at least*

$$(5) \quad C_0(((|A|\,|B|)^{1/2})^{1+(1/k)}/\log N)\exp(c_3(\log k \log R)/\log\log R)$$

*pairs $(a, b)$ with $a$ in $A$ and $b$ in $B$, (respectively pairs $(a_1, b_1)$ with $a_1$ in $A$ and $b_1$ in $B$), such that for each pair there exists a prime $p$ for which $p^k|(a+b)$, (respectively $p^k|(a_1 - b_1)$), with*

$$(6) \quad \frac{2C_1(|A|\,|B|)^{1/2}}{\exp(c_4(\log k \log R)/\log\log R)} \geqq p^k > \frac{C_1(|A|\,|B|)^{1/2}}{\exp(c_4(\log k \log R)/\log\log R)}.$$

In particular if (4) holds then for $N$ sufficiently large there exist $a$ in $A$ and $b$ in $B$ and a prime $p$ such that $p^k|(a + b)$ with

$$(7) \quad p^k > C_1(|A|\,|B|)^{1/2}/\exp(c_4(\log k \log R)/\log\log R).$$

Note that if $k = 2$, (4) is a more stringent requirement that (1), however the lower bound for $p^2$ given by (7) is better than the one given by (2). In fact the lower bound for $p^k$ given by (7) is best possible apart from the factor

$$\exp(c_4(\log k \log R)/\log\log R)$$

as the following example shows. Let $A$ and $B$ consist of all multiples of a positive integer $t$ with $t \leqq N^{1/(k+1)}$. Then

$$|A| = |B| = [N/t].$$

If $p^k|(a + b)$ with $a$ in $A$ and $b$ in $B$, (or indeed if $p^k|(a - b)$ with $a$ in $A$, $b$ in $B$ and $a \neq b$), then either $p|t$ in which case

$$p^k \leqq N^{k/(k+1)} \leqq N/t \leqq 2(|A|\,|B|)^{1/2}$$

or $p \nmid t$ in which case

$$p^k \leqq 2[N/t] = 2(|A|\,|B|)^{1/2}.$$

We shall derive Theorem 1 from the following result of independent interest. For any real number $x$ let $[x]$ denote the greatest integer less than or equal to $x$, let $\{x\} = x - [x]$ denote the fractional part of $x$ and let

$$||x|| = \min(\{x\}, 1 - \{x\}).$$

THEOREM 2. *Let $k$ be an integer greater than one and let $\epsilon$ be a positive real number. Let $N$ be a positive integer and let $y$ be a real number with*

$$(8) \qquad 3 \leqq y < N^{\gamma_k - \epsilon}$$

*where $\gamma_k = (2k4^{k-1})^{-1}$. For any real number $\alpha$ with*

$$y^{k-1}/N \leqq \alpha \leqq 1 - (y^{k-1}/N),$$

*we have*

$$\sum_{p^k \leqq N} \min(y, ||p^k\alpha||^{-1})$$

$$< C_2(N^{1/k}/\log N)\exp(c_5(\log k \log y)/\log\log y),$$

*for $N > N_1$, where $c_5$ is an effectively computable positive absolute constant and $C_2$ and $N_1$ are real numbers which are effectively computable in terms of $\epsilon$ and $k$.*

In [**10**] we established the analogue of Theorem 2 for the case $k = 1$.

**2. Preliminary lemmas.** For any real number $x$ denote $e^{2\pi ix}$ by $e(x)$.

LEMMA 1. *Let $X$ and $Y$ be positive integers with $X < Y$. Then for any real number $\alpha$ we have*

$$\left|\sum_{X<n\leqq Y} e(n\alpha)\right| \leqq \min(Y - X, 2||\alpha||^{-1}).$$

*Proof.* See [**8**], p. 189.

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

LEMMA 2. *Let $V$ be a positive integer. Then for any real number $\alpha$ we have*

$$\left|\sum_{n=0}^{V-1} e(n\alpha) - V\right| \leqq 4V^2|\alpha|.$$

*Proof.* See [**1**], Lemma 2.

For any positive integer $n$ let $\omega(n)$ denote the number of distinct prime factors of $n$.

LEMMA 3. *There exists an effectively computable positive real number $c_6$ such that*

(9) $\omega(n) < c_6(\log n)/\log \log n,$

*for $n \geqq 3$.*

*Proof.* This estimate is well known. It can be derived easily from the prime number theorem. In fact for any positive real number $\epsilon$, (9) holds with $c_6 = 1 + \epsilon$ provided that $n$ is sufficiently large in terms of $\epsilon$.

We shall next record four additional well known elementary results. For any positive integer $n$, denote the number of integers less than or equal to $n$ and coprime with $n$ by $\phi(n)$. $\phi$ is Euler's phi function.

LEMMA 4. *There exists an effectively computable positive real number $c_7$ such that*

$$\phi(n) > c_7 n/\log \log n,$$

*for $n \geqq 3$.*

*Proof.* See [**8**], p. 24.

For any positive integer $n$, denote the number of positive integers which divide $n$ by $\tau(n)$.

LEMMA 5. *Let $q$ be a positive integer and let $u$ and $v$ be real numbers with $v > 0$. Then*

$$\left|\sum_{\substack{u<a\leqq u+v\\(a,q)=1}} 1 - v\phi(q)/q\right| \leqq 2\tau(q).$$

*Proof.* This is Lemma 4 of [**9**].

LEMMA 6. *There exists an effectively computable positive real number $c_8$ such that for any integer $b$ with $b \geqq 2$,*

$$\sum_{\substack{1\leqq n\leqq b\\(n,b)=1}} 1/n < c_8(\phi(b)/b) \log b.$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

*Proof.* This is Lemma 5 of [**9**].

Let $a$, $k$ and $q$ be integers with $k$ and $q$ positive. We define the function $f(a, k, q)$ by

$$(10)\quad f(a, k, q) = \sum_{\substack{0 \leqq x < q \\ (x,q)=1 \\ x^k \equiv a (\mathrm{mod}\, q)}} 1.$$

LEMMA 7. *Let $a$, $k$ and $q$ be integers with $k$ and $q$ positive.*
(i) *If $(a, q) = 1$ and $f(a, k, q) \neq 0$ then*

$$(11)\quad f(a, k, q) = f(1, k, q).$$

(ii) *If $p$ is a prime number, $r$ and $k$ are positive integers and $(a, p) = 1$ then*

$$(12)\quad f(a, k, p^r) \leqq \begin{cases} 2k & \text{for } p = 2 \\ k & \text{for } p > 2. \end{cases}$$

(iii) *There exists an effectively computable positive real number $c_9$ such that for $k \geqq 2$, $q \geqq 3$ and $(a, q) = 1$,*

$$f(a, k, q) < \exp(c_9(\log k \log q)/\log \log q).$$

*Proof.* Let $x_1, \ldots, x_t$ denote a complete set of incongruent solutions modulo $q$ of

$$x^k \equiv 1 \pmod{q},$$

and let $x_0$ be a solution of

$$(13)\quad x^k \equiv a \pmod{q}.$$

Then $x_0x_1, \ldots, x_0x_t$ is a complete set of incongruent solutions of (13) and this implies (11).

(ii) follows easily from the theory of binomial congruences.

Let

$$q = p_1^{r_1} \ldots p_l^{r_l}$$

with $r_1, \ldots, r_l$ positive integers and $p_1, \ldots, p_l$ distinct primes. By the Chinese Remainder Theorem

$$f(a, k, q) = f(a, k, p_1^{r_1}) \ldots f(a, k, p_l^{r_l}).$$

Thus by (ii) and Lemma 3

$$f(a, k, q) \leqq 2k^l$$
$$= 2 \exp( (\log k)\omega(q) ) < \exp(c_9(\log k \log q)/\log \log q)$$

as required.

Let $i$, $n$ and $q$ be integers with $q \geqq 2$. Put

$$(14) \quad \xi(i, n, q) = \begin{cases} 1 & \text{if } i \equiv n \pmod{q} \\ 0 & \text{if } i \not\equiv n \pmod{q}. \end{cases}$$

LEMMA 8. *Let $a$, $b$, $k$ and $q$ be integers with $k \geqq 2$, $q \geqq 3$ and $(a, q) = 1$ and let $u$ and $v$ be real numbers with $v > 0$. Then*

$$\left| \sum_{u<i \leqq u+v} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} \xi(i, an^k + b, q) - v\phi(q)/q \right|$$

$$< q^{1/2} \exp(c_{10}(\log k \log q)/\log\log q),$$

*where $c_{10}$ is an effectively computable positive real number.*

*Proof.* We have, for $(n, q) = 1$,

$$\xi(i, n, q) = (1/\phi(q)) \sum_{\chi} \bar{\chi}(i)\chi(n),$$

where the summation is taken over all characters $\chi$ modulo $q$. We shall denote the principal character modulo $q$ by $\chi_0$. Thus

$$\sum_{u<i \leqq u+v} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} \xi(i, an^k + b, q)$$

$$= \sum_{u<i \leqq u+v} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} \xi(i - b, an^k, q)$$

$$= \sum_{u-b<j \leqq u+v-b} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} \xi(j, an^k, q)$$

$$= \sum_{u-b<j \leqq u+v-b} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} (1/\phi(q)) \sum_{\chi} \bar{\chi}(j)\chi(an^k)$$

$$= (1/\phi(q)) \sum_{\chi} \left( \chi(a) \sum_{u-b<j \leqq u+v-b} \bar{\chi}(j) \sum_{n=0}^{q-1} \chi^k(n) \right)$$

$$= (1/\phi(q))\chi_0(a) \sum_{u-b<j \leqq u+v-b} \bar{\chi}_0(j) \sum_{n=0}^{q-1} \chi_0^k(n)$$

$$+ (1/\phi(q)) \sum_{\chi \neq \chi_0} \left( \chi(a) \sum_{u-b<j \leqq u+v-b} \bar{\chi}(j) \sum_{n=0}^{q-1} \chi^k(n) \right)$$

$$= \sum_{\substack{u-b<j \leqq u+v-b \\ (j,q)=1}} 1 + \sum_{\substack{\chi \neq \chi_0 \\ \chi^k = \chi_0}} \left( \chi(a) \sum_{u-b<j \leqq u+v-b} \bar{\chi}(j) \right).$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

Therefore

$$\left| \sum_{u<i\leqq u+v} \sum_{\substack{0\leqq n<q \\ (n,q)=1}} \xi(i, an^k + b, q) - v\phi(q)/q \right|$$

$$\leqq \left| \sum_{\substack{u-b<j\leqq u+v-b \\ (j,q)=1}} 1 - v\phi(q)/q \right| + \sum_{\substack{\chi\neq\chi_0 \\ \chi^k=\chi_0}} \left| \sum_{u-b<j\leqq u+v-b} \bar{\chi}(j) \right|$$

which, by Lemma 5, the Pólya-Vinogradov inequality [7], [**11**] and the trivial inequality $\tau(q) \leqq 2q^{1/2}$, is

$$< 2\tau(q) + \sum_{\substack{\chi\neq\chi_0 \\ \chi^k=\chi_0}} c_{11}q^{1/2} \log q$$

$$\leqq 4q^{1/2} + c_{11}q^{1/2} \log q \sum_{\chi^k=\chi_0} 1$$

$$= 4q^{1/2} + c_{11}q^{1/2} \log q \sum_{\chi} (1/\phi(q)) \sum_{n=0}^{q-1} \chi^k(n)$$

$$= 4q^{1/2} + c_{11}q^{1/2} \log q \sum_{n=0}^{q-1} (1/\phi(q)) \sum_{\chi} \chi(n^k)$$

$$= 4q^{1/2} + c_{11}q^{1/2} \log q \sum_{\substack{0\leqq n<q \\ n^k\equiv 1(\mathrm{mod}\, q)}} 1$$

$$= 4q^{1/2} + c_{11}q^{1/2} \log q\, f(1, k, q).$$

The result now follows from Lemma 7.

LEMMA 9. *Let $h$, $a$ and $q$ be integers with $a > 0$, $q > 1$ and $(a, q) = 1$. Let $\rho(n)$ be a real valued function defined for those integers $n$ with $h \leqq n \leqq h + q$ and $(n, q) = 1$. Put*

$$\lambda = \max_{\substack{h\leqq n<h+q \\ (n,q)=1}} \rho(n) - \min_{\substack{h\leqq n<h+q \\ (n,q)=1}} \rho(n)$$

*and*

$$\eta(n) = (an + \rho(n))/q.$$

*There is an effectively computable positive absolute constant $c_{12}$ such that if $\lambda \leqq 1$ and if $E$ is a real number satisfying $2 \leqq E \leqq q$ then*

$$\sum_{\substack{h\leqq n<h+q \\ (n,q)=1}} \min(E, \|\eta(n)\|^{-1}) < c_{12}\phi(q) \log E.$$

*Proof.* This is Lemma 6 of [**9**].

LEMMA 10. *Let $k$, $h$, $a$ and $q$ be integers with $k \geqq 2$, $a \geqq 1$, $q \geqq 3$ and $(a, q) = 1$. Let $\rho(n)$ be a real valued function defined for those integers $n$ with $h \leqq n < h + q$, $(n, q) = 1$ and $f(n, k, q) > 0$. Put*

$$\lambda = \max_{\substack{h \leqq n < h+q \\ (n,q)=1 \\ f(n,k,q)>0}} \rho(n) - \min_{\substack{h \leqq n < h+q \\ (n,q)=1 \\ f(n,k,q)>0}} \rho(n)$$

*and*

$$\eta(n) = (an + \rho(n))/q.$$

*There exists an effectively computable positive absolute constant $c_{13}$ and a positive real number $C_3$ which is effectively computable in terms of $k$ such that if $\lambda \leqq 1$ and if $E$ is a real number satisfying $3 \leqq E \leqq q$, then*

$$(15) \quad \sum_{\substack{h \leqq n < h+q \\ (n,q)=1}} f(n, k, q) \min(E, \|\eta(n)\|^{-1})$$

$$< C_3 \phi(q) \exp(c_{13}(\log k \log E)/\log \log E).$$

*Proof.* If $q^{1/3} \leqq E \leqq q$ then, by Lemmas 7 and 9,

$$(16) \quad \sum_{\substack{h \leqq n < h+q \\ (n,q)=1}} f(n, k, q) \min(E, \|\eta(n)\|^{-1})$$

$$\leqq \left( \max_{\substack{0 \leqq n < q \\ (n,q)=1}} f(n, k, q) \right) \sum_{\substack{h \leqq n < h+q \\ (n,q)=1}} \min(E, \|\eta(n)\|^{-1})$$

$$< \exp(c_9(\log k \log q)/\log \log q) c_{12} \phi(q) \log E$$

$$< \phi(q) \exp(c_{14}(\log k \log E)/\log \log E).$$

Thus we may assume that

$$(17) \quad 3 \leqq E < q^{1/3}.$$

Put

$$r = \left[ \min_{\substack{h \leqq n < h+q \\ (n,q)=1 \\ f(n,k,q)>0}} \rho(n) \right],$$

and $\rho_1(n) = \rho(n) - r$. Note that

$$0 \leqq \rho_1(n) < \lambda + 1 \leqq 2.$$

We have

$$\eta(n) = ((an + r) + \rho_1(n))/q$$

and so

$$(an + r)/q \leqq \eta(n) < (an + r + 2)/q,$$

hence

$$\|\eta(n)\|^{-1} \leqq \max( \|(an + r)/q\|^{-1}, \|(an + r + 1)/q\|^{-1}, \|(an + r + 2)/q\|^{-1}),$$

subject to the convention that

$$a \leqq \max(1/0, b) \quad \text{and} \quad 1/0 \leqq \max(1/0, a)$$

for all real numbers $a$ and $b$. Thus, on recalling (14), we find that

$$\sum_{\substack{h \leqq n < h+q \\ (n,q)=1}} f(n, k, q) \min(E, \|\eta(n)\|^{-1})$$

$$\leqq \sum_{\substack{h \leqq n < h+q \\ (n,q)=1}} f(n, k, q) \sum_{i=0}^{2} \min(E, \|(an + r + i)/q\|^{-1})$$

$$\leqq 3 \max_{j \in \mathbf{Z}} \sum_{\substack{h \leqq n < h+q \\ (n,q)=1}} f(n, k, q) \min(E, \|(an + j)/q\|^{-1})$$

$$= 3 \max_{j \in \mathbf{Z}} \sum_{\substack{h \leqq n < h+q \\ (n,q)=1}} f(n, k, q) \sum_{i=0}^{q-1} \xi(i, an + j, q) \min(E, \|i/q\|^{-1})$$

$$= 3 \max_{j \in \mathbf{Z}} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} \sum_{i=0}^{q-1} \xi(i, an^k + j, q) \min(E, \|i/q\|^{-1})$$

$$\leqq 3 \max_{j \in \mathbf{Z}} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} \sum_{i=0}^{[q/2]} (\xi(i, an^k + j, q) + \xi(q - i, an^k + j, q))$$

$$\times \min(E, q/i) \leqq 3 \max_{j \in \mathbf{Z}} \Bigg( E \sum_{0 \leqq i \leqq q/E} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} (\xi(i, an^k + j, q) + \xi(q - i, an^k + j, q))$$

$$+ \sum_{u=1}^{[E]} (E/u) \sum_{uq/E < i \leqq (u+1)q/E} \sum_{\substack{0 \leqq n < q \\ (n,q)=1}} (\xi(i, an^k + j, q) + \xi(q - i, an^k + j, q)) \Bigg)$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

which, by Lemma 8, is

$$\leqq 6E((1 + (q/E))(\phi(q)/q)$$
$$+ q^{1/2}\exp(c_{10}(\log k \log q)/\log\log q))$$
$$+ 6\sum_{u=1}^{[E]} (E/u)((1 + (q/E))(\phi(q)/q)$$
$$+ q^{1/2}\exp(c_{10}(\log k \log q)/\log\log q))$$

and, by (17), is

$$\leqq 12\phi(q) + 6q^{5/6}\exp(c_{10}(\log k \log q)/\log\log q)$$
$$+ 12(1 + \log E)(\phi(q) + q^{5/6}\exp(c_{10}(\log k \log q)/\log\log q)),$$

whence, by Lemma 4, is

$$(18) \quad < C_4\phi(q)\log E,$$

where $C_4$ is a positive number which is effectively computable in terms of $k$. Lemma 10 now follows from (16) and (18).

LEMMA 11. *Let $\theta$ be a positive real number and let $k$ be an integer larger than one. If $\alpha$ is a real number and $a$, $q$ and $N$ are positive integers with $(a, q) = 1$ and $|\alpha - (a/q)| < q^{-2}$ then*

$$\left|\sum_{p\leqq N} e(\alpha p^k)\right| < C_5N^{1+\theta}(q^{-1} + N^{-1/2} + qN^{-k})^{4^{1-k}},$$

*where $C_5$ is a real number which is effectively computable in terms of $k$ and $\theta$; the summation above is over primes $p$ with $p \leqq N$.*

*Proof.* This follows from Theorem 1 of **[4]** by partial summation.

LEMMA 12. *Let $\delta$ be a real number satisfying*

$$0 < \delta \leqq 1/2.$$

*Then there exists a periodic function $\psi(x, \delta)$, with period 1, such that*
(i) *$\psi(x, \delta) \geqq 1$ in the interval $-\delta \leqq x \leqq \delta$,*
(ii) *$\psi(x, \delta) \geqq 0$ for all $x$,*
(iii) *$\psi(x, \delta)$ has a Fourier series expansion of the form*

$$\psi(x, \delta) = a_0 + \sum_{0<j\leqq(1/2\delta)-1} a_j \cos 2\pi jx,$$

*where*

$$|a_0| \leqq \pi^2\delta,$$

*and*

$$|a_j| < 2\pi^2\delta,$$

*for* $0 < j \leqq (1/2\delta) - 1$.

*Proof.* This is Lemma 4 of **[10]**. In fact in **[10]** it is shown that one may take

$$\psi(x, \delta) = (\pi^2/(4N^2))|(1 - e(Nx))/(1 - e(x))|^2$$

where $N = [1/(2\delta)]$. Of course results of this character are well known. They were introduced in this setting by Weyl and have often been used by Vinogradov and others.

Let $x$ be a real number and let $l$ and $k$ be positive integers. As usual we denote the number of primes less than or equal to $x$ by $\pi(x)$ and the number of primes less than or equal to $x$ and congruent to $l$ modulo $k$ by $\pi(x, k, l)$.

LEMMA 13. *There exist effectively computable positive real numbers* $c_{15}$ *and* $c_{16}$ *such that if* $X$ *and* $Y$ *are real numbers with* $X > c_{15}$ *and* $Y \geqq X^{23/42}$ *then*

$$\pi(X + Y) - \pi(X) > c_{16}Y/\log X.$$

*Proof.* This is the main theorem of **[5]**.

In fact we only require Lemma 13 for the range $Y \geqq X^{(5/8)+\epsilon}$ for $\epsilon$ an arbitrary positive real number and so Ingham's Theorem would suffice here.

LEMMA 14. (Brun-Titchmarsh Theorem). *Let* $x$ *and* $y$ *be positive real numbers and let* $k$ *and* $l$ *be relatively prime positive integers with* $y > k$. *Then*

$$\pi(x + y, k, l) - \pi(x, k, l) < 2y/(\phi(k) \log(y/k)).$$

*Proof.* This is Theorem 2 of **[6]**.

**3. The proof of theorem 2.** As before, $C_0, C_1, \ldots$ and $N_0, N_1, \ldots$ denote positive real numbers which are effectively computable in terms of $\epsilon$ and $k$ and $c_0, c_1, \ldots$ denote effectively computable positive absolute constants. We shall assume, without loss of generality, that

$$0 < \epsilon < (2k4^{k-1})^{-1}.$$

Put

$$P = (yN^{\epsilon/2})^{4^{k-1}} \quad \text{and} \quad Q = N/P.$$

Let $T_1$ denote the set of those $\alpha$ in the interval

$$(y^{k-1}/N, 1 - (y^{k-1}/N))$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

for which for all integers $n$ with $1 \leqq n \leqq y$ there exist positive integers $r_n$ and $s_n$ with $(r_n, s_n) = 1$,

(19) $|n\alpha - (r_n/s_n)| < 1/s_n^2$

and

(20) $P \leqq s_n \leqq Q.$

Put

$$T' = (y^{k-1}/N, 1 - (y^{k-1}/N)) - T_1,$$

so that $T'$ consists of the real numbers $\alpha$ in $(y^{k-1}/N, 1 - (y^{k-1}/N))$ which are not in $T_1$. If $\alpha \in T'$ then for some integer $n^*$ with $1 \leqq n^* \leqq y$ there exist no coprime positive integers $r_{n^*}$, $s_{n^*}$ satisfying (19) and (20) with $n^*$ in place of $n$. By Dirichlet's Theorem there exist integers $u$ and $v$ with

(21) $|n^*\alpha - (u/v)| < 1/(vQ),$

$0 \leqq u$, $0 < v \leqq Q$ and $(u, v) = 1$. Note that

$$|n^*\alpha - (u/v)| < 1/v^2,$$

and therefore that $v < P$. It follows directly from (21) that

$$|\alpha - (u/n^*v)| < 1/(n^*vQ),$$

hence, on writing $u/(n^*v)$ in the form $a/b$ with $a$ and $b$ coprime $a \geqq 0$ and $b > 0$ we see that

(22) $|\alpha - (a/b)| < 1/(bQ),$

with

(23) $b \leqq n^*v \leqq yP.$

To each $\alpha$ in $T'$ we shall associate a pair of coprime integers $a$ and $b$ with $a \geqq 0$ and $b > 0$ satisfying (22) and (23) and we shall put

$$\beta = \alpha - (a/b).$$

Let us define subsets $T_2$ and $T_3$ of $T'$ by

$$T_2 = \{\alpha \in T' | b \leqq y\},$$

$$T_3 = \{\alpha \in T' | y < b\}.$$

Put

$$S_0(\alpha) = \sum_{p^k \leqq N} \min(y, ||p^k\alpha||^{-1}).$$

Since

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

$$(y^{k-1}/N, 1 - (y^{k-1}/N)) = T_1 \cup T_2 \cup T_3$$

it suffices to show that for $N > N_1$,

(24) $$\max_{\alpha \in T_i} S_0(\alpha) < C_2(N^{1/k}/\log N) \exp(c_5(\log k \log y)/\log \log y),$$

for $i = 1, 2, 3$. We shall establish (24) for $i = 1$, the case of the "minor arcs" in Section 4 and for $i = 2, 3$, the "major arcs" in Section 5.

**4. Minor arcs.** Assume that $\alpha \in T_1$. For $\beta > 0$, put

$$Z(N, \alpha, \beta) = \sum_{\substack{p^k \leqq N \\ \|p^k\alpha\| < \beta}} 1.$$

Then

$$\begin{aligned}
S_0(\alpha) &= \sum_{p^k \leqq N} \min(y, \|p^k\alpha\|^{-1}) \\
&= \sum_{\substack{p^k \leqq N \\ \|p^k\alpha\| < 1/y}} \min(y, \|p^k\alpha\|^{-1}) \\
&\quad + \sum_{j=2}^{[y/2]+1} \sum_{\substack{p^k \leqq N \\ (j-1)/y \leqq \|p^k\alpha\| < j/y}} \min(y, \|p^k\alpha\|^{-1}) \\
&\leqq \sum_{\substack{p^k \leqq N \\ \|p^k\alpha\| < 1/y}} y + \sum_{j=2}^{[y/2]+1} \sum_{\substack{p^k \leqq N \\ (j-1)/y \leqq \|p^k\alpha\| < j/y}} y/(j-1) \\
&= yZ(N, \alpha, 1/y) \\
&\quad + \sum_{j=2}^{[y/2]+1} (y/(j-1))(Z(N, \alpha, j/y) - Z(N, \alpha, (j-1)/y)) \\
&= y \sum_{j=2}^{[y/2]} Z(N, \alpha, j/y)(1/(j-1) - 1/j) \\
&\quad + (y/[y/2])Z(N, \alpha, ([y/2] + 1)/y) \\
&\leqq y \sum_{j=2}^{[y/2]} Z(N, \alpha, j/y)/(j(j-1)) + 3 \sum_{p^k \leqq N} 1.
\end{aligned}$$

Thus, by the prime number theorem,

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

(25) $$S_0(\alpha) < y \sum_{j=2}^{[y/2]} Z(N, \alpha, j/y)/(j(j-1)) + 4kN^{1/k}/\log N,$$

for $N > N_2$.

On applying Lemma 12 with $\delta = j/y$ and $1 \leqq j \leqq y/2$ we find that

$$\begin{aligned} &Z(N, \alpha, j/y) \\ &= \sum_{\substack{p^k \leqq N \\ \|p^k\alpha\| < j/y}} 1 \leqq \sum_{p^k \leqq N} \psi(p^k\alpha, j/y) \\ &= \sum_{p^k \leqq N} \left(a_0 + \sum_{0 < m \leqq (y/2j)-1} a_m \cos(2\pi m p^k \alpha)\right) \\ &= a_0\pi(N^{1/k}) + \sum_{0 < m \leqq (y/2j)-1} a_m R_e\left(\sum_{p^k \leqq N} e(mp^k\alpha)\right) \\ &\leqq |a_0|\pi(N^{1/k}) + \sum_{0 < m \leqq (y/2j)-1} |a_m| \left|\sum_{p^k \leqq N} e(mp^k\alpha)\right| \\ &\leqq (\pi^2 j/y)\pi(N^{1/k}) + \sum_{0 < m \leqq (y/2j)-1} (2\pi^2 j/y) \left|\sum_{p^k \leqq N} e(mp^k\alpha)\right|. \end{aligned}$$

Thus, by the prime number theorem, for $N > N_3$,

(26) $$\begin{aligned} &Z(N, \alpha, j/y) \\ &\leqq (20kj/y)N^{1/k}/\log N \\ &+ \left(\max_{0 < m \leqq (y/2j)-1} \left|\sum_{p^k \leqq N} e(mp^k\alpha)\right|\right) \sum_{0 < m \leqq (y/2j)-1} 20j/y \\ &\leqq (20kj/y)N^{1/k}/\log N + 10 \max_{0 < m \leqq (y/2j)-1} \left|\sum_{p^k \leqq N} e(p^k m\alpha)\right|. \end{aligned}$$

If $0 < m \leqq (y/2j) - 1$ then, since $(y/2j) - 1 \leqq y$, for $\alpha \in T_1$ there exist, by (19), positive integers $r_m$ and $s_m$ with $(r_m, s_m) = 1$,

$$|m\alpha - (r_m/s_m)| < 1/s_m^2,$$

and $P \leqq s_m \leqq N/P$. Thus, on applying Lemma 11 with $\theta = \epsilon/2$, we find that

$$\left|\sum_{p^k \leqq N} e(p^k(m\alpha))\right| < C_6 N^{(1+(\epsilon/2))/k}((2/P) + N^{-(1/2k)})^{4^{1-k}}$$

which, for $N > N_4$, is, by (8),

$$< C_7 N^{1/k}/(y \log N).$$

Therefore, by (26), for $1 \leqq j \leqq y/2$ and $N > N_5$,

$$Z(N, \alpha, j/y) < C_8(j/y)N^{1/k}/\log N.$$

Thus, from (25), for $\alpha \in T_1$,

$$(27) \quad S_0(\alpha) < C_8(N^{1/k}/\log N) \sum_{j=2}^{[y/2]} 1/(j-1) + 4kN^{1/k}/\log N$$
$$< C_9(N^{1/k}/\log N) \log y,$$

provided that $N > N_5$.

**5. Major arcs.** For any real number $\alpha$ in $T'$ and associated positive integer $b \leqq N$ we put

$$S_0(\alpha, b) = \sum_{\substack{p^k \leqq N \\ (p,b)=1}} \min(y, \|p^k\alpha\|^{-1}).$$

Then, by Lemma 3,

$$S_0(\alpha) \leqq \sum_{p|b} y + S_0(\alpha, b) \leqq c_{17} y \log b + S_0(\alpha, b)$$
$$\leqq c_{17} y \log N + S_0(\alpha, b).$$

Thus, by (8), for $N > N_6$,

$$(28) \quad S_0(\alpha) < N^{1/k}/\log N + S_0(\alpha, b).$$

In this section we shall establish (24) for $\alpha \in T_2$ and $\alpha \in T_3$. Assume first that $\alpha \in T_2$. Put

$$L = \min(N, 1/(2b|\beta|)),$$

where $\min(N, 1/0) = N$ by definition. Then we have

$$(29) \quad N \geqq L \geqq Q/2 = N/(2P).$$

Put

$$S_1(\alpha, b) = \sum_{\substack{p^k \leqq L \\ (p,b)=1}} \min(y, \|p^k\alpha\|^{-1}) \quad \text{and}$$

$$S_2(\alpha, b) = \sum_{\substack{L < p^k \leqq N \\ (p,b)=1}} \min(y, \|p^k\alpha\|^{-1}),$$

so that

(30) $S_0(\alpha, b) = S_1(\alpha, b) + S_2(\alpha, b).$

Notice that the sum $S_2(\alpha, b)$ is empty for $N \leqq 1/(2b|\beta|)$ hence for

(31) $|\beta| \leqq 1/(2bN).$

We shall now estimate $S_1(\alpha, b)$. Suppose that $b = 1$. Then $|\beta| = \|\alpha\|$ and since $\alpha \in T'$, $|\beta| > y^{k-1}/N$. Thus $L < N/y^{k-1}$ and so $L|\beta| = 1/2$. We have, just as in our estimation (25) for $S(\alpha)$,

$$S_1(\alpha, 1) \leqq y \sum_{j=2}^{[y/2]} Z(L, \alpha, j/y)/(j(j-1)) + 4kN^{1/k}/\log N.$$

Now, since $L|\beta| = 1/2$, we have, by Lemma 14,

$$Z(L, \alpha, j/y) \leqq \pi((2jL/y)^{1/k}) \leqq 8k(jN)^{1/k}/(y \log N).$$

Therefore,

(32) $S_1(\alpha, 1) \leqq C_{10}(N^{1/k}/\log N).$

Next suppose that $b > 1$. In this case we may assume, since $a$ and $b$ are coprime, that $a > 0$. If $(p, b) = 1$ and $p^k \leqq L$ then

$$\begin{aligned} \|p^k\alpha\| &= \|p^k((a/b) + \beta)\| = \|ap^k/b\| - p^k|\beta| \\ &\geqq \|ap^k/b\| - 1/(2b) \geqq (1/2)\|ap^k/b\|, \end{aligned}$$

since $b > 1$ and $(ap^k, b) = 1$. Thus

$$\begin{aligned} &S_1(\alpha, \beta) \\ &\leqq \sum_{\substack{p^k \leqq L \\ (p,b)=1}} \min(y, 2\|ap^k/b\|^{-1}) \\ &\leqq \sum_{\substack{0<h<b \\ (h,b)=1}} \sum_{\substack{0<x<b \\ (x,b)=1 \\ x^k \equiv h (\mathrm{mod}\, b)}} \sum_{\substack{p \leqq L^{1/k} \\ p \equiv x (\mathrm{mod}\, b)}} 2\|ah/b\|^{-1} \\ &= 2 \sum_{\substack{0<h<b \\ (h,b)=1}} \sum_{\substack{0<x<b \\ (x,b)=1 \\ x^k \equiv h (\mathrm{mod}\, b)}} \pi(L^{1/k}, b, x)\|ah/b\|^{-1} \\ &< 2\left(\max_{\substack{0<x<b \\ (x,b)=1}} \pi(L^{1/k}, b, x)\right) \sum_{\substack{0<h<b \\ (h,b)=1}} \sum_{\substack{0<x<b \\ (x,b)=1 \\ x^k \equiv h (\mathrm{mod}\, b)}} \|ah/b\|^{-1} \\ &= 2\left(\max_{\substack{0<x<b \\ (x,b)=1}} \pi(L^{1/k}, b, x)\right) \sum_{\substack{0<h<b \\ (h,b)=1}} f(h, k, b)\|ah/b\|^{-1} \end{aligned}$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

$$\leqq 2\left(\max_{\substack{0<x<b\\(x,b)=1}} \pi(L^{1/k}, b, x)\right)\left(\max_{\substack{0<h<b\\(h,b)=1}} f(h, k, b)\right) \sum_{\substack{0<h<b\\(h,b)=1}} ||ah/b||^{-1}$$

$$\leqq 4\left(\max_{\substack{0<x<b\\(x,b)=1}} \pi(L^{1/k}, b, x)\right)\left(\max_{\substack{0<h<b\\(h,b)=1}} f(h, k, b)\right) \sum_{\substack{0<l\leqq[b/2]\\(l,b)=1}} b/l.$$

Employing Lemmas 6 and 7 and recalling that since $\alpha \in T_2$, $b \leqq y$, we find

(33) $$S_1(\alpha, b) \leqq C_{11}\left(\max_{\substack{0<x<b\\(x,b)=1}} \pi(L^{1/k}, b, x)\right) \exp(c_{18}(\log k \log y)/\log\log y)\phi(b).$$

Now, by (29),

$$L^{1/k}/b \geqq N^{1/k}/(2yP^{1/k})$$

hence by (8),

$$L^{1/k}/b > N^{1/2k},$$

for $N > N_7$. Thus we may apply Lemma 14 to conclude that

(34) $$\max_{\substack{0<x<b\\(x,b)=1}} \pi(L^{1/k}, b, x) < C_{12}L^{1/k}/(\phi(b) \log N).$$

Thus, since $L \leqq N$, it follows from (33) and (34) that

(35) $$S_1(\alpha, b) < C_{13}(N^{1/k}/\log N) \exp(c_{18}(\log k \log y)/\log\log y),$$

for $N > N_8$.

We shall now estimate $S_2(\alpha, b)$. We may assume that

(36) $$1/(2bN) < |\beta| < 1/(bQ),$$

since otherwise, recall (31), the sum is empty. Thus also

(37) $$L = 1/(2b|\beta|).$$

We have

$$S_2(\alpha, b) = \sum_{\substack{L<p^k\leqq N\\(p,b)=1}} \min(y, ||p^k\alpha||^{-1})$$

$$\leqq \sum_{j=1}^{[N/L]} \sum_{\substack{jL<p^k\leqq(j+1)L\\(p,b)=1}} \min(y, ||p^k\alpha||^{-1})$$

$$= \sum_{j=1}^{[N/L]} \sum_{h=1}^{[2y]+1} \sum_{\substack{jL<p^k \leqq (j+1)L \\ (p,b)=1 \\ (h-1)/([2y]+1) \leqq \{p^k\alpha\} < h/([2y]+1)}} \min(y, \|p^k\alpha\|^{-1}).$$

Note that

$$(h - 1)/([2y] + 1) \leqq \{p^k\alpha\} < h/([2y] + 1)$$

implies that

$$\|p^k\alpha\|^{-1} \leqq \|(h - 1)/([2y] + 1)\|^{-1} + \|h/([2y] + 1)\|^{-1},$$

where we write $x \leqq (1/0) + z$ and $(1/0) \leqq (1/0) + z$ for all real numbers $x$ and $z$. Thus

$$(38) \quad S_2(\alpha, b) \leqq \sum_{j=1}^{[N/L]} \sum_{h=1}^{[2y]+1} (\min(y, \|(h - 1)/([2y] + 1)\|^{-1}$$
$$+ \min(y, \|h/([2y] + 1)\|^{-1})) \sum_{\substack{jL<p^k \leqq (j+1)L \\ (p,b)=1 \\ (h-1)/([2y]+1) \leqq \{p^k\alpha\} < h/([2y]+1)}} 1.$$

If $p_0$ and $p_1$ are primes with

$$jL < p_i^k \leqq (j + 1)L \quad \text{and}$$
$$(h - 1)/([2y] + 1) \leqq \{p_i^k\alpha\} < h/([2y] + 1)$$

for $i = 0, 1$ then, by (37),

$$1/(2y) > 1/([2y] + 1)$$
$$\geqq \|(p_1^k - p_0^k)\alpha\| = \|(p_1^k - p_0^k)((a/b) + \beta)\|$$
$$\geqq \|(p_1^k - p_0^k)a/b\| - |p_1^k - p_0^k|\,|\beta| > \|(p_1^k - p_0^k)a/b\| - L|\beta|$$
$$= \|(p_1^k - p_0^k)a/b\| - 1/(2b).$$

Thus

$$\|(p_1^k - p_0^k)a/b\| < 1/(2y) + 1/(2b) \leqq 1/b,$$

whence

$$p_1^k \equiv p_0^k \pmod{b}.$$

Therefore

$$(39) \quad 1/(2y) > \|p_1^k\alpha - p_0^k\alpha\| = \|(p_1^k - p_0^k)a/b + (p_1^k - p_0^k)\beta\|$$
$$= \|(p_1^k - p_0^k)\beta\|.$$

Since

$$|(p_1^k - p_0^k)\beta| < L|\beta| = 1/(2b) \leqq 1/2$$

it follows from (39) that

$$1/(2y) > |p_1^k - p_0^k|\,|\beta|,$$

hence

$$|p_1 - p_0| < \left(2|\beta|y\left(\sum_{i=0}^{k-1} p_1^i p_0^{k-1-i}\right)\right)^{-1} \leqq (2|\beta|yp_0^{k-1})^{-1}$$
$$< (2|\beta|y(jL)^{(k-1)/k})^{-1}.$$

Thus, by (37),

$$|p_1 - p_0| < L^{1/k}b/(yj^{(k-1)/k}).$$

Therefore, either there are no primes $p$ with

$$jL < p^k \leqq (j + 1)L, \quad (p, b) = 1 \quad \text{and}$$
$$(h - 1)/([2y] + 1) \leqq \{p^k\alpha\} < h/([2y] + 1),$$

or for some $p_0$ with $(p_0, b) = 1$ we have

$$(40)\qquad \sum_{\substack{jL<p^k\leqq(j+1)L\\ (p,b)=1\\ (h-1)/([2y]+1)\leqq\{p^k\alpha\}<h/([2y]+1)}} 1$$
$$\leqq \sum_{\substack{p^k\equiv p_0^k(\mathrm{mod}\,b)\\ |p-p_0|<L^{1/k}b/(yj^{(k-1)/k})}} 1$$
$$= \sum_{\substack{0\leqq t<b\\ t^k\equiv p_0^k(\mathrm{mod}\,b)}} \sum_{\substack{p\equiv t(\mathrm{mod}\,b)\\ |p-p_0|<L^{1/k}b/(yj^{(k-1)/k})}} 1$$
$$\leqq \sum_{\substack{0\leqq t<b\\ t^k\equiv p_0^k(\mathrm{mod}\,b)}} (\pi(p_0 + (L^{1/k}b/(yj^{(k-1)/k})), b, t)$$
$$- \pi(p_0 - (L^{1/k}b/(yj^{(k-1)/k})), b, t)).$$

Now, since $1 \leqq j \leqq N/L$ and $L > Q/2$,

$$(2L^{1/k}b/(yj^{(k-1)/k}))/b \geqq 2L/(yN^{(k-1)/k})$$
$$> Q/(yN^{(k-1)/k}) = N^{1/k}/(yP),$$

and, by (8),

$$N^{1/k}/(yP) \geqq N^{3/(8k)}.$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

Thus, the right hand side of (40) is, by Lemma 14,

$$< \sum_{\substack{0 \leqq t < b \\ t^k \equiv p_0^k (\mathrm{mod}\, b)}} C_{14} L^{1/k} b/(yj^{(k-1)/k} \phi(b) \log N)$$

and, by Lemma 4,

$$< C_{15}(L^{1/k} \log\log b/(yj^{(k-1)/k} \log N)) \sum_{\substack{0 \leqq t < b \\ t^k \equiv p_0^k (\mathrm{mod}\, b)}} 1$$

$$= C_{15}(L^{1/k} \log\log b/(yj^{(k-1)/k} \log N)) f(p_0^k, k, b)$$

and, by Lemma 7 and the fact that $b \leqq y$,

$$< C_{15}(L^{1/k}/(yj^{(k-1)/k} \log N)) \exp(c_{19}(\log k \log y)/\log\log y).$$

Therefore, by (38),

(41) $S_2(\alpha, b)$

$$\leqq \sum_{j=1}^{[N/L]} \sum_{h=1}^{[2y]+1} (\min(y, \|(h-1)/([2y]+1)\|^{-1})$$

$$+ \min(y, \|h/([2y]+1)\|^{-1}))$$

$$\times C_{15}(L^{1/k}/(yj^{(k-1)/k} \log N)) \exp(c_{19}(\log k \log y)/\log\log y)$$

$$\leqq C_{16}(L^{1/k}/(y \log N)) \exp(c_{19}(\log k \log y)/\log\log y)$$

$$\times \sum_{j=1}^{[N/L]} j^{-(k-1)/k} \sum_{h=0}^{[2y]+1} \min(y, \|h/([2y]+1)\|^{-1})$$

$$\leqq C_{17}(L^{1/k}/(y \log N)) \exp(c_{19}(\log k \log y)/\log\log y)(N/L)^{1/k}$$

$$\times \left(y + \sum_{h=1}^{[y]+1} (2y+1)/h\right)$$

$$\leqq C_{18}(N^{1/k}/\log N) \exp(c_{20}(\log k \log y)/\log\log y).$$

Appealing to (28), (30), (32), (35) and (41) we find that for $\alpha \in T_2$,

(42) $S_0(\alpha) < C_{19}(N^{1/k}/\log N) \exp(c_{21}(\log k \log y)/\log\log y)$,

provided that $N > N_9$.

Finally, we assume that $\alpha$ is in $T_3$. Put

$$M = \min(N, (|\beta| y)^{-1}).$$

Then

(43) $$S_0(\alpha, b) \leqq \sum_{j=0}^{[N/M]} \sum_{\substack{jM<p^k\leqq(j+1)M \\ (p,b)=1}} \min(y, \|p^k\alpha\|^{-1}).$$

Now if $\|p^k\alpha\|^{-1} < y$ with $jM < p^k \leqq (j+1)M$, and $n$ is defined by $p^k \equiv n \pmod b$ with $(j+1)M - b < n \leqq (j+1)M$, then

$$\begin{aligned}\|p^k\alpha\| &= \|p^k((a/b) + \beta)\| = \|(an/b) + n\beta + (p^k - n)\beta\| \\ &\geqq \|(an + nb\beta)/b\| - |p^k - n|\,|\beta|.\end{aligned}$$

Note that $N > b$ and

$$(|\beta|y)^{-1} > bQ/y \geqq Q > b$$

by (8) and (23). Thus $|p^k - n| < M$ and so

$$|p^k - n|\,|\beta| < M|\beta| \leqq 1/y < \|p^k\alpha\|.$$

Therefore

$$2\|p^k\alpha\| \geqq \|(an + nb\beta)/b\|,$$

whence

$$\min(y, \|p^k\alpha\|^{-1}) \leqq 2\min(y, \|(an + nb\beta)/b\|^{-1}).$$

Consequently, by (43),

(44) $$S_0(\alpha, b) \leqq \sum_{j=0}^{[N/M]} \sum_{\substack{(j+1)M-b<n\leqq(j+1)M \\ (n,b)=1}} \times 2\min(y, \|(an + nb\beta)/b\|^{-1}) \sum_{\substack{jM<p^k\leqq(j+1)M \\ p^k\equiv n \pmod b}} 1.$$

By (22), $(|\beta|y)^{-1} > Qb/y$ and by (23), $N \geqq Qb/y$ hence $M \geqq Qb/y$. Thus, since $b > y$,

$$\begin{aligned}&(((j+1)M)^{1/k} - (jM)^{1/k})/b \\ &\geqq M^{1/k}/(k(j+1)b) \geqq M^{1/k}/(2bk(N/M)) \\ &= M^{1+(1/k)}/(2bkN) \geqq Q^{1+(1/k)}b^{1/k}/(2kNy^{1+(1/k)}) \\ &\geqq N^{1/k}/(2kyP^{1+(1/k)})\end{aligned}$$

which is, by (8),

(45) $$\geqq N^{1/(8k)},$$

for $N > N_{10}$. Therefore, by (45) and Lemma 14,

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

(46)
$$\sum_{\substack{jM<p^k\leqq(j+1)M\\ p^k\equiv n(\mathrm{mod}\, b)}} 1$$

$$= \sum_{\substack{0\leqq t<b\\ t^k\equiv n(\mathrm{mod}\, b)}} \sum_{\substack{(jM)^{1/k}<p\leqq((j+1)M)^{1/k}\\ p\equiv t(\mathrm{mod}\, b)}} 1$$

$$< \sum_{\substack{0\leqq t<b\\ t^k\equiv n(\mathrm{mod}\, b)}} (16k(((j+1)M)^{1/k} - (jM)^{1/k})/(\phi(b)\log N))$$

$$< (C_{20}M^{1/k}((j+1)^{1/k} - j^{1/k})/(\phi(b)\log N)) \sum_{\substack{0\leqq t<b\\ t^k\equiv n(\mathrm{mod}\, b)}} 1.$$

But the sum in the expression on the right hand side of inequality (46) is $f(n, k, b)$ and so on combining (44) and (46) we obtain

$$S_0(\alpha, b)$$
$$\leqq \sum_{j=0}^{[N/M]} (C_{20}M^{1/k}((j+1)^{1/k} - j^{1/k})/(\phi(b)\log N))$$
$$\times \sum_{\substack{(j+1)M-b<n\leqq(j+1)M\\ (n,b)=1}} f(n, k, b)\min(y, \|(an + nb\beta)/b\|^{-1}).$$

We may estimate the inner sum above by means of Lemma 10 with $h = (j + 1)M - b + 1$, $q = b$ and $\rho(n) = nb\beta$. Then, by (8), (22) and (23),

$$\lambda = \max_{\substack{(j+1)M-b<n\leqq(j+1)M\\ (n,b)=1}} nb\beta - \min_{\substack{(j+1)M-b<n\leqq(j+1)M\\ (n,b)=1}} nb\beta$$
$$\leqq b^2|\beta| < b/Q < 1.$$

Thus

(47) $S_0(\alpha, b)$
$$\leqq \sum_{j=0}^{[N/M]} C_{21}(M^{1/k}((j+1)^{1/k} - j^{1/k})/\log N)$$
$$\times \exp(c_{13}(\log k \log y)/\log\log y)$$
$$= C_{21}(M^{1/k}/\log N)\exp(c_{13}(\log k\log y)/\log\log y)$$
$$\times \sum_{j=0}^{[N/M]} ((j+1)^{1/k} - j^{1/k})$$

$$= C_{21}(M^{1/k}/\log N) \exp(c_{13}(\log k \log y)/\log\log y)$$
$$\times ([N/M] + 1)^{1/k}$$
$$< C_{22}(N^{1/k}/\log N) \exp(c_{13}(\log k \log y)/\log\log y).$$

By (28) and (47), for $\alpha$ in $T_3$,

(48) $S_0(\alpha) < C_{23}(N^{1/k}/\log N) \exp(c_{13}(\log k \log y)/\log\log y)$,

provided that $N > N_{10}$.

Thus (24) follows from (27), (42) and (48) and this completes the proof of Theorem 2.

**6. Further preliminaries to the proof of theorem 1.** Let $\epsilon$ be a positive real number less than $\theta_k$ and let $C_0, C_1, \ldots$ denote positive real numbers which are effectively computable in terms of $\epsilon$ and $k$ and $c_0, c_1, \ldots$ denote effectively computable positive absolute constants. Let $C$ and $c$ be real numbers, with $C \geqq 20$ and $c \geqq 1$, to be specified later and let $N_{11}, N_{12}, \ldots$ denote numbers which are effectively computable in terms of $C$, $c$, $\epsilon$ and $k$. We shall choose $C$ and $c$ later so that $C$ is effectively computable in terms of $\epsilon$ and $k$ and so that $c$ is an effectively computable positive absolute constant. Put

$$y = CR \exp(c(\log k \log R)/\log\log R).$$

Since $R \geqq 3$ we have $y \geqq 3$ and if (4) holds and $N > N_{11}$ then

(49) $y < N^{\theta_k - (\epsilon/2)}$.

We shall first establish Theorem 1 for the case of sums $a + b$; the case $a - b$ is treated in a similar way. To do so it suffices to show that there exist at least

$$C_{24}|A|\,|B|(N/y)^{(1/k)-1}/\log N$$

pairs $(a, b)$ with $a$ in $A$ and $b$ in $B$ for which there exists a prime $p$ with $p^k|(a + b)$ and

(50) $4N/y \geqq p^k > 2N/y$.

We now introduce the following notation. Put

$$\lambda = y^k/N \quad \text{and} \quad U = [N/y^{k+1}]$$

and, for each positive integer $n$,

$$d_n = \begin{cases} 1 & \text{if } n = mp^k \text{ with } 1 \leqq m \leqq y,\ p \text{ a prime and } 2N/y < p^k \leqq 4N/y \\ 0 & \text{otherwise.} \end{cases}$$

Next put

$$S(\alpha) = \sum_{n=1}^{4N} d_n e(n\alpha),$$

$$S = S(0) = \sum_{n=1}^{4N} d_n,$$

$$U(\alpha) = \sum_{n=0}^{U-1} e(n\alpha),$$

and, since $d_n = 0$ if $n < 1$ or $n > 4N$, write

$$S(\alpha)U(\alpha) = \sum_{n=1}^{4N+U-1} v_n e(n\alpha) \quad \text{where } v_n = \sum_{j=n-U+1}^{n} d_j.$$

Further, put

$$F(\alpha) = \sum_{a\in A} e(a\alpha), \quad G(\alpha) = \sum_{b\in B} e(b\alpha)$$

and

$$H(\alpha) = F(\alpha)G(\alpha) = \sum_{a\in A, b\in B} e((a+b)\alpha) = \sum_{n=1}^{2N} h_n e(n\alpha)$$

where

$$h_n = \sum_{\substack{a+b=n \\ a\in A, b\in B}} 1.$$

Finally, define $J$ by

$$J = \int_0^1 F(\alpha)G(\alpha)S(-\alpha)d\alpha.$$

Observe that

$$J = \int_0^1 H(\alpha)S(-\alpha)d\alpha = \int_0^1 \sum_{n=1}^{2N} \sum_{m=1}^{4N} h_n d_m e((n-m)\alpha)d\alpha$$

$$= \sum_{n=1}^{2N} h_n d_n.$$

Note that $d_n > 0$ implies that $p^k | n$ with $2N/y < p^k \leqq 4N/y$, while $h_n > 0$ implies that $n = a + b$, for $a \in A$, $b \in B$. Thus to establish our result it suffices to show that

(51) $J > C_{24}|A|\,|B|(N/y)^{(1/k)-1}/\log N.$

In order to prove (51) we first require some estimates for $S$, $S(\alpha)$ and $v_n$.

We remark that by (49), $y < (2N/y)^{1/k}$, provided that $N > N_{11}$ and therefore that

(52) $$S(\alpha) = \sum_{m \leqq y} \sum_{2N/y < p^k \leqq 4N/y} e(mp^k\alpha).$$

LEMMA 15. *For* $N > N_{11}$,

(53) $S < C_{25}y(N/y)^{1/k}/\log N.$

*Proof.* By (52),

$$S = \sum_{n=1}^{4N} d_n = \left(\sum_{1 \leqq m \leqq y} 1\right)\left(\sum_{2N/y < p^k \leqq 4N/y} 1\right) \leqq y\pi(\,(4N/y)^{1/k}),$$

which, by (49) and Lemma 14, is

$$< C_{25}y(N/y)^{1/k}/\log N.$$

LEMMA 16. *If* $N > N_{12}$, *then for* $\lambda \leqq \alpha \leqq 1 - \lambda$,

(54) $|S(\alpha)| < C_{26}(\,(N/y)^{1/k}/\log N)\exp(c_5(\log k \log y)/\log\log y).$

*Proof.* By (52), for $N > N_{11}$,

$$|S(\alpha)| < \sum_{2N/y < p^k \leqq 4N/y} \left|\sum_{m \leqq y} e(mp^k\alpha)\right|,$$

which, by Lemma 1, is

$$\leqq \sum_{2N/y < p^k \leqq 4N/y} \min(y, 2\|p^k\alpha\|^{-1})$$

$$\leqq 2 \sum_{p^k \leqq 4N/y} \min(y, \|p^k\alpha\|^{-1}).$$

The lemma now follows from Theorem 2.

LEMMA 17. *If* $N > N_{13}$ *and* $n$ *is an integer satisfying* $30N/y < n \leqq 2N$ *then*

(55) $v_n > C_{27}(N/y)^{(1/k)-1}U/\log N.$

*Proof.* If $n$ satisfies $30N/y < n \leqq 2N$ then, for $N > N_{11}$,

$$v_n = \sum_{j=n-U+1}^{n} d_j = \sum_{\substack{n-U < mp^k \leqq n \\ m \leqq y \\ 2N/y < p^k \leqq 4N/y}} 1$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

$$= \sum_{m \leqq y} \sum_{\max((n-U)/m, 2N/y) < p^k \leqq \min(n/m, 4N/y)} 1.$$

Notice that if $m \leqq 11ny/(30N)$ then

$$(n - U)/m \geqq 30N/(11y) - U/m \geqq 30N/(11y) - N/y^{k+1}$$

and, since $y \geqq 3$,

$$(n - U)/m > 2N/y.$$

Further, if $9ny/(30N) < m$ then $n/m < 30N/(9y) < 4N/y$. Since

$$11ny/(30N) \leqq 22y/30 < y$$

we conclude that

$$(56) \quad v_n > \sum_{9ny/(30N) < m \leqq 11ny/(30N)} \sum_{(n-U)/m < p^k \leqq n/m} 1$$

$$= \sum_{9ny/(30N) < m \leqq 11ny/(30N)} \pi((n/m)^{1/k}) - \pi(((n - U)/m)^{1/k}).$$

We may now apply Lemma 13 with

$$X = ((n - U)/m)^{1/k} \quad \text{and} \quad Y = (n/m)^{1/k} - ((n - U)/m)^{1/k}$$

for

$$9ny/(30N) < m \leqq 11ny/(30N).$$

For we have

$$(57) \quad X = ((n - U)/m)^{1/k} < (n/m)^{1/k} < (30N/(9y))^{1/k}$$

while

$$(58) \quad Y = (n/m)^{1/k}(1 - (1 - (U/n))^{1/k}) > C_{28}(N/y)^{(1/k)}U/n,$$

since $U/n < y^{-k} < 1/2$ for $N > N_{14}$. By (57) and (58)

$$(X^{3/5}/Y)^{5k/2} < C_{29}y^{1+(5k(k+1)/2)}/N,$$

which, by (49), is

$$< C_{29}/N^{1/17}.$$

Thus for $N > N_{15}$, $X^{3/5} < Y$ whence, by Lemma 13,

$$v_n > \sum_{9ny/(30N) < m \leqq 11ny/(30N)} C_{30}(N/y)^{(1/k)}U/(n \log N)$$

$$> ((2ny/(30N)) - 1)C_{30}(N/y)^{(1/k)}U/(n \log N).$$

Since $n > 30N/y$ the result follows.

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

**7. The proof of theorem 1.** We shall establish (51) now. We have, for $N > N_{16}$,

$$|J - U^{-1}\int_0^1 F(\alpha)G(\alpha)S(-\alpha)U(-\alpha)d\alpha|$$

$$\leqq \int_{-\lambda}^{\lambda} |F(\alpha)|\,|G(\alpha)|\,|S(-\alpha)|\,|(U - U(-\alpha))/U|d\alpha$$

$$+ \int_{\lambda}^{1-\lambda} |F(\alpha)|\,|G(\alpha)|\,|S(-\alpha)|\,(1 + |U(-\alpha)/U|)d\alpha$$

which, by Lemma 2, is

$$\leqq \int_{-\lambda}^{\lambda} |F(\alpha)|\,|G(\alpha)|\,|S4U|\alpha|d\alpha$$

$$+ \int_{-\lambda}^{\lambda} |F(\alpha)|\,|G(\alpha)|\left(\max_{\lambda\leqq\beta\leqq 1-\lambda} |S(\beta)|\right)2d\alpha$$

by Lemmas 15 and 16, is

$$< \int_{\lambda}^{\lambda} |F(\alpha)|\,|G(\alpha)|\,C_{31}(y(N/y)^{1/k}/\log N)U\lambda d\alpha$$

$$+ \int_{\lambda}^{1-\lambda} |F(\alpha)|\,|G(\alpha)|\,2C_{26}((N/y)^{1/k}/\log N)$$

$$\times \exp(c_5(\log k \log y)/\log\log y)d\alpha,$$

$$\leqq (C_{31}(N/y)^{1/k}/\log N + C_{32}((N/y)^{1/k}/\log N)$$

$$\times \exp(c_5(\log k \log y)/\log\log y))$$

$$\times \int_0^1 |F(\alpha)|\,|G(\alpha)|d\alpha,$$

and, by Cauchy's inequality, is

$$\leqq C_{33}((N/y)^{1/k}/\log N)\exp(c_5(\log k \log y)/\log\log y)$$

$$\times \left(\left(\int_0^1 |F(\alpha)|^2 d\alpha\right)\left(\int_0^1 |G(\alpha)|^2 d\alpha\right)\right)^{1/2}.$$

Thus, by Parseval's formula,

$$(59)\quad \left|J - U^{-1}\int_0^1 F(\alpha)G(\alpha)U(-\alpha)S(-\alpha)d\alpha\right|$$

$$\leqq C_{33}((N/y)^{1/k}(|A|\,|B|)^{1/2}/\log N)$$

$$\times \exp(c_5(\log k \log y)/\log\log y).$$

Furthermore,

$$I = \int_0^1 F(\alpha)G(\alpha)U(-\alpha)S(-\alpha)d\alpha$$

https://doi.org/10.4153/CJM-1988-035-3 Published online by Cambridge University Press

$$= \int_0^1 \left( \sum_{n=1}^{2N} h_n e(n\alpha) \right) \left( \sum_{m=1}^{4N+U-1} v_m e(-m\alpha) \right) d\alpha$$

$$= \sum_{n=1}^{2N} h_n v_n.$$

Since $h_n$ and $v_n$ are non-negative for $n = 1, \ldots, 2N$,

$$I \geqq \sum_{30N/y < n \leqq 2N} h_n v_n,$$

and, by Lemma 17,

$$I \geqq C_{27}(N/y)^{(1/k)-1}(U/\log N) \sum_{30N/y < n \leqq 2N} h_n$$

$$= C_{27}(N/y)^{(1/k)-1}(U/\log N) \sum_{\substack{a \in A, b \in B \\ 30N/y < a+b \leqq 2N}} 1.$$

Observe that since $C \geqq 20$,

$$30N/y \leqq (\,|A|\,|B|\,)^{1/2}/2 \leqq (1/2) \max(\,|A|, |B|\,)$$

and thus

$$\sum_{\substack{a \in A, b \in B \\ 30N/y < a+b \leqq 2N}} 1 \geqq |A|\,|B|/2.$$

Therefore

(60) $I \geqq C_{34}|A|\,|B|(N/y)^{(1/k)-1}U/\log N.$

It follows, from (59) and (60), that

(61) $$|J| \geqq |I|/U - C_{33}(\,(N/y)^{1/k}(\,|A|\,|B|\,)^{1/2}/\log N) \times \exp(c_5(\log k \log y)/\log\log y)$$
$$\geqq C_{34}|A|\,|B|(\,(N/y)^{(1/k)-1}/\log N)(1 - (C_{35}N/(y(\,|A|\,|B|\,)^{1/2})\,) \times \exp(c_5(\log k \log y)/\log\log y)\,).$$

Recall that

$$y = CR \exp(c(\log k \log R)/\log\log R).$$

We now choose $c = 2c_5$. Put

(62) $W = C_{35}(N/(y(\,|A|\,|B|\,)^{1/2})\,) \exp(c_5(\log k \log y)/\log\log y).$

Provided that $C > C_{36}$ we have $y < (CR)^2$ and

$$\log y/\log\log y < 2(\log CR)/\log\log CR$$
$$< 2(\,(\log C/\log\log C) + (\log R/\log\log R)\,)$$

hence

$$W < C_{35}\exp(2c_5(\log k \log C)/\log\log C)/C$$

and so we may choose $C = C_{37}$ sufficiently large so that $W < 1/2$. Then, by (61) and (62),

$$|J| \geqq (C_{34}/2)(\,|A|\,|B|/\log N)(N/y)^{(1/k)-1}.$$

Since $J$ is non-negative (51) holds and this completes the proof of Theorem 1 for the case of sums $a + b$. The proof of Theorem 1 for terms of the form $a - b$ is essentially the same as that given above. We estimate

$$J' = \int_0^1 F(\alpha)G(-\alpha)S(-\alpha)d\alpha$$

in place of $J$; see pp. 190-191 of **[9]** for details.

## References


1. A. Balog and A. Sárközy, *On sums of sequences of integers, I*, Acta Arith. *44* (1984), 73-86.
2. ——— *On sums of sequences of integers, II*, Acta Math. Hung. *44* (1984), 169-179.
3. ——— *On sums of sequences of integers, III*, Acta Math. Hung. *44* (1984), 339-349.
4. G. Harman, *Trigonometric sums over primes, I*, Mathematika *29* (1981), 249-254.
5. H. Iwaniec and J. Pintz, *Primes in short intervals*, Monatshefte Math. *98* (1984), 115-143.
6. H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika *20* (1973), 119-134.
7. G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttinger Nachrichten (1918), 21-29.
8. K. Prachar, *Primzahlverteilung* (Springer-Verlag, 1957).
9. A. Sárközy and C. L. Stewart, *On divisors of sums of integers, II*, J. reine angew Math. *365* (1986), 171-191.
10. ——— *On exponential sums over prime numbers*, J. Austral. Math. Soc. Series A, to appear.
11. I. M. Vinogradov, *An asymptotic equality in the theory of quadratic forms*, Zh. fiz.-matem. Obshch. Permsk universitet *1* (1918), 18-28.


*Hungarian Academy of Science,*
*Budapest, Hungary;*
*University of Waterloo,*
*Waterloo, Ontario*