Reprinted from

Séminaire de Théorie des Nombres, Paris 1984–85

Edited by Catherine Goldstein

Progress in Mathematics, Volume 63

© Birkhäuser Boston, Inc., 1986
Printed in the U.S.A.

Birkhäuser
Boston · Basel · Stuttgart

SOME REMARKS ON PRIME DIVISORS OF SUMS OF INTEGERS

C.L. Stewart

Denote the cardinality of a set X by $|X|$ and for any integer n let $P(n)$ denote the greatest prime factor of n with the convention $P(0) = P(\pm 1) = 1$. In [1], Balog and Sárközy proved that if N is a sufficiently large positive integer and A and B are subsets of $\{1,\ldots,N\}$ with $(|A||B|)^{1/2} > 10N^{1/2}\log N$ then there exist integers a in A and b in B such that

$$P(a+b) > (|A||B|)^{1/2}/(16\log N). \tag{1}$$

The key ingredient in the proof of their result is the large sieve inequality. More generally let N be a positive integer and let $A_1,\ldots,A_k$ be non-empty subsets of $\{1,\ldots,N\}$. Recently Sárközy and Stewart [9] derived estimates for the greatest prime factor of terms of the form $a_1 + \ldots + a_k$ where $a_1,\ldots,a_k$ are chosen from the sets $A_1,\ldots,A_k$ respectively. Of particular use in this connection is the Cauchy-Davenport lemma, see [2].

Cauchy-Davenport Lemma. Let p be a prime number, let A and B be subsets of $\mathbb{Z}/p\mathbb{Z}$ and put $A+B = \{a+b \mid a\in A,\ b\in B\}$. Then

$$|A+B| \geq \min\{|A| + |B| - 1, p\}.$$

Let ϵ be a positive real number. Using the Cauchy-Davenport lemma Sárkozy and Stewart [9] proved that if

$$\sum_{i=1}^{k} |A_i| > (1+\epsilon)N,$$

then for any prime number p with $N < p < (1+\epsilon/2)N$ there exist a_i in A_i, for $i = 1,\ldots,k$, such that

$$P(a_1 + \ldots + a_k) = p,$$

whenever N is larger than a number which is effectively computable in terms of ε and k. Denote the geometric mean of $|A_1|,\ldots,|A_k|$ by T, so that

$$T = \Big(\prod_{i=1}^{k} |A_i|\Big)^{1/k}.$$

By combining the Cauchy-Davenport lemma with the large sieve inequality Sárközy and Stewart [9] were able to generalize the result of Balog and Sárközy referred to earlier. In particular, if N is larger than a number which is effectively computable in terms of k and

$$T > 8N^{1/2} \log N,$$

then there exist a_i in A_i, for $i = 1,\ldots,k$, such that

$$P(a_1 + \ldots + a_k) > k\,T/(14 \log T).$$

Further, by combining the Cauchy-Davenport lemma with Gallagher's larger sieve, Sárközy and Stewart [9] showed that if $|A_1| \le |A_i|$ for $i = 1,\ldots,k$ and ε is any positive real number then there exist a_i in A_i for $i = 1,\ldots,k$ such that

$$P(a_1 + \ldots + a_k) > |A_1|/N^{1/k+\varepsilon},$$

provided that N is larger than a number which is effectively computable in terms of ε and k.

Notice from (1) that if $|A| \gg N$ and $|B| \gg N$ then there exist a in A and b in B such that

$$P(a+b) \gg N/\log N \tag{2}$$

Balog and Sárközy [1] also employed the Hardy-Littlewood circle method in this context and they established a somewhat weaker result by this approach; in place of $N/\log N$ in (2) their argument yielded $N/(\log N)^2$. Recently Sárközy and Stewart [10] were able to show by means of the circle method that if $|A| \gg N$ and $|B| \gg N$ then there exist a in A and b in B such that

$$P(a+b) \gg N.$$

This is an immediate consequence of the following theorem. Put

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

Theorem 1 (Sárközy and Stewart [10]). Let N be a positive integer, let A and B be subsets of $\{1,\dots,N\}$ and let ϵ be a positive real number. There exist effectively computable positive absolute constants c_0 and c_1 and a positive number N_1 which is effectively computable in terms of ϵ such that if N is greater than N_1 and

$$(|A||B|)^{1/2} > N^{5/6+\epsilon},$$

then there exist atleast $c_0(|A||B|)/\log N$ pairs (a,b) with a in A and b in B for which

$$P(a+b) > c_1(|A||B|)^{1/2}/(\log R \log\log R). \tag{3}$$

Notice that if t is a positive integer with t at most $N^{1/2}$ and we put $A = B = \{nt \mid n \in \mathbb{Z}^+, nt \le N\}$ then for all a in A and b in B,

$$P(a+b) \le \max\{P(t), 2[N/t]\} \le 2[N/t]$$

$$\le 2(|A||B|)^{1/2},$$

and thus (3) is close to best possible.

Put $y = c_2 R \log R \log\log R$, where c_2 is an effectively computable positive constant. For each positive integer n define d_n to be 1 if n can be written as mp with $1 \le m \le y$ and p a prime number with $2N/y < p \le 4N/y$ and 0 otherwise. For any real number x denote $e^{2\pi i x}$ by $e(x)$ and put

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

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

and

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

with

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

Next define J by

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

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

Notice that if d_n is positive then $P(n) > \frac{2N}{y}$ while if h_n is positive there exist a in A and b in B such that $n = a+b$. To establish Theorem 1 it suffices to show that

$$J > c_3|A||B|/\log N, \tag{4}$$

where c_3 is an effectively computable positive constant. We remark that in [1], Balog and Sárközy studied essentially the same integral J. For the proof of (4) we employ a result of Heath-Brown and Iwaniec on the difference between consecutive prime numbers, a refinement, due to Vaughan, of Vinogradov's fundamental lemma on exponential sums over prime numbers and, on several occasions, the Brun-Titchmarsh theorem.

The above results apply only when A and B or $A_1,\ldots,A_k$ are fairly "dense" subsets of $\{1,\ldots,N\}$. When this is not the case sieve methods and the circle method must be replaced by elementary arguments or methods from Diophantine approximation. For any positive integer n let $\omega(n)$ denote the number of distinct prime factors of n. In 1934, Erdös and Turán [4] proved that if A is a finite set of positive integers with $|A| = k$ then, for $k > 2$,

$$\omega\Big(\prod_{a,a'\in A}(a+a')\Big) \geq (\log(k/3))/\log 2. \tag{5}$$

Thus, by the prime number theorem there exist integers a_1 and a_2 in A such that

$$P(a_1+a_2) > c_4 \log k \log\log k ,$$

where c_4 is an effectively computable positive constant. The proof given by Erdös and Turán is elementary and ingenious. Erdös and Turán conjectured that a similar result to (5) should hold when the summands are drawn from two different sets A and B. In particular, see [3], they conjectured that to every s there is an $f(s)$ so that if $k \geq f(s)$ and $1 \leq a_1 < \ldots < a_k$ and $1 \leq b_1 < \ldots < b_k$ are any two sets of positive

integers then

$$\omega\Big(\prod_{\substack{1\le i\le k\\ 1\le j\le k}} (a_i+b_j)\Big) \ge s. \tag{6}$$

In [11] Stewart and Tijdeman resolved the conjecture by an elementary argument. They showed that one can replace s on the right hand side of inequality (6) by $c_5 \log k/\log\log k$, where c_5 is an effectively computable positive constant. In fact it is possible to improve this further by using a result by Evertse [5].

Theorem 2 (Győry, Stewart and Tijdeman [7]). Let A and B be sets of positive integers with $k = |A| \ge |B| \ge 2$. Then

$$\omega\Big(\prod_{a\in A, b\in B} (a+b)\Big) > c_6 \log k,$$

where c_6 is an effectively computable positive constant.

A slightly weaker version of Theorem 2 can be deduced from earlier work of Lewis and Mahler, see [12]. As before, we see, on applying the prime number theorem, that if A and B are sets of positive integers with $k = |A| \ge |B| \ge 2$ then there exist a in A and b in B for which

$$P(a+b) > c_7 \log k \log\log k, \tag{7}$$

where c_7 is an effectively computable positive constant. Stewart and Tijdeman have proved that (7) is close to best possible by showing that, in general, it is not possible to replace the right hand side of inequality (7) by $(\log k)^{2+\varepsilon}$ for any positive real number . It is however possible to improve upon (7) if there are sufficiently large terms of the form $a+b$ and the greatest common divisor of all a's and b's is one, as the next result shows.

Theorem 3 (Győry, Stewart and Tijdeman [7]). Let ε be a positive real number, let k be an integer with $k \ge 2$ and let $a_1 < a_2 < \ldots < a_k$ and b be positive integers. If the greatest common divisor of $a_1,\ldots,a_k$ and b is one then

$$P(a_1 \ldots a_k (a_1+b) \ldots (a_k+b)) > \min((1-\varepsilon)k \log k, c_8 \log\log (a_k+b)),$$

for $k > k_0(\varepsilon)$, where $k_0(\varepsilon)$ is a positive real number which is effecti-

vely computable in terms of ε and c_8 is an effectively computable positive constant.

The proof of Theorem 3 depends upon estimates for linear forms in the logarithms of algebraic numbers due to Baker and, in the p-adic case, due to van der Poorten. Finally we mention that Győry, Stewart and Tijdeman [9] have shown that if a_1, a_2 and b run through positive integers with $g.c.d(a_1, a_2, b) = 1$ then $P(a_1a_2(a_1+b)(a_2+b))$ tends to infinity with the maximum of a_1, a_2 and b. This is proved by appealing to results of Evertse [6] or van der Poorten and Schlickewei [8] which in turn depend upon the work of Schlickewei on the p-adic version of the Thue-Siegel-Roth-Schmidt theorem.

BIBLIOGRAPHY

[1] A. Balog and A. Sárközy.- On sums of sequences of integers II, Acta Math. Hung., to appear.

[2] H. Davenport.- A historical note, J. London Math. Soc. 22 (1947), 100-101.

[3] P. Erdös.- Problems in number theory and combinatorics, Proc. Sixth Manitoba Conf. Numerical Math. (Univ. Manitoba, Winnipeg, Man., 1976), 35-58, Congress Numer., 18, Utilitas Math., Winnipeg, Man., 1977.

[4] P. Erdös and P. Turán.- On a problem in the elementary theory of numbers, Amer. Math. Monthly 41 (1934), 608-611.

[5] J.H. Evertse.- On equations in S-units and the Thue-Mahler equation, Invent. Math. 75 (1984), 561-584.

[6] J.H. Evertse.- On sums of S-units and linear recurrences, Compositio Math. 53 (1984), 225-244.

[7] K. Györy, C.L. Stewart and R. Tijdeman.- On prime factors of sums of integers, to appear.

[8] A.J. van der Poorten and H.P. Schlickewei.- The growth conditions for recurrence sequences, Macquarie Math. Report 82-0041 (1982).

[9] A. Sárközy and C.L. Stewart.- On divisors of sums of integers I, Acta Math. Hung., to appear.

[10] A. Sárközy and C.L. Stewart.- On divisors of sums of integers II, J. reine angew. Math., to appear.

[11] C.L. Stewart and R. Tijdeman.- On prime factors of sums of integers II, Proc. Number Theory Conf. Sydney, to appear.

[12] C.L. Stewart and R. Tijdeman.- On prime factors of sums of integers, Univ. Leiden Math. Inst. Report 11 (1985).

C.L. Stewart
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
CANADA
N2L 3G1