COMPOSITIO MATHEMATICA

K. GYÖRY
C. L. STEWART
R. TIJDEMAN

On prime factors of sums of integers I

Compositio Mathematica, tome 59, nº 1 (1986), p. 81-88
<http://www.numdam.org/item?id=CM_1986__59_1_81_0>

Compositio Mathematica 59 (1986) 81–88

ON PRIME FACTORS OF SUMS OF INTEGERS I

K. Győry, C.L. Stewart * and R. Tijdeman

§1. Introduction

For any integer n larger than one let $\omega(n)$ denote the number of distinct prime factors of n and let $P(n)$ denote the greatest prime factor of n. For any set X let $|X|$ denote the cardinality of X. In 1934 Erdös and Turán [4] proved that if A is a finite set of positive integers with $|A| = k$ then, for $k \geqslant 2$,

$$\omega\Big(\prod_{a,a' \in A} (a + a')\Big) > C_1 \log k, \tag{1}$$

where C_1 is an effectively computable positive constant. By the prime number theorem this implies that there exist integers a_1 and a_2 in A for which

$$P(a_1 + a_2) > C_2 \log k \log\log k,$$

where C_2 is an effectively computable positive constant.

Erdös and Turán (cf. [3, p. 36] conjectured that for every w there is an $f(w)$ so that if A and B are finite sets of positive integers with $|A| = |B| = k \geqslant f(w)$ then

$$\omega\Big(\prod_{a \in A, b \in B} (a + b)\Big) > w.$$

We shall prove this conjecture with $f(w) = e^{C_3 w}$. Moreover, it suffices that one set has at least k elements and the other at least two.

THEOREM 1: *Let A and B be finite sets of positive integers with $|A| \geqslant |B| \geqslant 2$. Put $k = |A|$. Then*

$$\omega\Big(\prod_{a \in A, b \in B} (a + b)\Big) > C_4 \log k, \tag{2}$$

where C_4 is an effectively computable positive constant.

* The research of the second author was supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

Note that Theorem 1 covers (1). For the proof of Theorem 1 we shall make use of a result of Evertse [6] proved by applying a modification of a method of Thue and Siegel involving hypergeometric functions. The proof of Erdös and Turán of (1) is elementary. Stewart and Tijdeman [12] have given an elementary proof of a weaker version of Theorem 1 where, in (2), $C_4 \log k$ is replaced by $C_5(\log l)/\log\log l$ with $l = |B|$. This suffices to establish the conjecture of Erdös and Turán with $f(w) = w^{C_6 w}$.

On combining the prime number theorem with Theorem 1 we obtain the following result. (In fact the nth prime exceeds $n \log n$, see Rosser and Schoenfeld [9], formula (3.12).)

COROLLARY 1: *Let A and B be finite sets of positive integers with $|A| \geqslant |B| \geqslant 2$ and put $|A| = k$. Then there exist a in A and b in B such that*

$$P(a+b) > C_7 \log k \log\log k, \tag{3}$$

where C_7 is an effectively computable positive constant.

We are able to improve upon (3) if there are sufficiently large terms of the form $a+b$ and the greatest common divisor of all such terms is one. By adding the smallest term of B to the terms of A and subtracting it from the terms of B we may suppose, without loss of generality, that the smallest term of B is zero. We shall state our next theorem with this observation in mind.

THEOREM 2: *Let ϵ be a positive real number, let k be an integer with $k \geqslant 2$ and let $a_1 < a_2 < \ldots < a_k$ and b be positive integers. If*

$$\text{g.c.d.}\ (a_1, \ldots, a_k, b) = 1, \tag{4}$$

then

$$P(a_1 \ldots a_k(a_1+b)\ldots(a_k+b)) > \min((1-\epsilon)k \log k,\ C_8 \log\log(a_k+b)), \tag{5}$$

for $k > k_0(\epsilon)$, where $k_0(\epsilon)$ is a positive real number which is effectively computable in terms of ϵ and C_8 is an effectively computable positive constant. Further, if a_1, a_2, b run through positive integers such that

$$a_1 < a_2 \quad \textit{and}\ \text{g.c.d.}\ (a_1, a_2, b) = 1$$

then

$$\lim_{a_2+b\to\infty} P\big(a_1a_2(a_1+b)(a_2+b)\big)=\infty. \tag{6}$$

For the proof of (5) we use estimates for linear forms in the logarithms of algebraic numbers due in the complex case to Baker [1] and in the p-adic case to van der Poorten [7]. For the proof of (6) we appeal to a result of Evertse [5]; alternatively we could use a similar result of van der Poorten and Schlickewei [8]. These results depend in turn on the work of Schlickewei on the p-adic version of the Thue-Siegel-Roth-Schmidt theorem.

We remark that it is possible to improve upon the estimates (3) and (5) if A and B are dense subsets of $\{1,\dots,N\}$ for some integer N. For example, Sárközy and Stewart [11] have used the Hardy-Littlewood circle method to prove that if $|A|\gg N$ and $|B|\gg N$ then there exist a in A and b in B for which $(P(a+b)\gg N$. Further, Balog and Sárközy [2], see also [10], have used the large sieve inequality to prove that if $|A|\,|B|>100\ N(\log N)^2$ and N is sufficiently large then there exist a in A and b in B for which

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

The second author would like to thank the University of Leiden for the hospitality he received during a visit in the fall of 1984, at which time the greater part of this paper was written.

§2. Preliminary lemmas

Let $a_1,\dots,a_n$ be non-zero integers with absolute values at most $A_1,\dots,A_n$ respectively and let $b_1,\dots,b_n$ be integers with absolute values at most B. We shall assume that $A_1,\dots,A_n$ and B are all at least 3. Put

$$\Lambda=b_1\log a_1+\dots+b_n\log a_n,$$

where, for any real number x, $\log x$ denotes the principal branch of the logarithm of x. Further, put

$$\Omega=\log A_1\dots\log A_n.$$

LEMMA 1: *If* $\Lambda\neq 0$ *then*

$$|\Lambda|>\exp\big(-(2n)^{C_9 n}\Omega\log\Omega\log B\big),$$

where C_9 *is an effectively computable positive constant.*

PROOF: This follows from Theorem 2 of [1]. □

For any non-zero rational number x and any prime number p there is a unique integer a such that $p^{-a}x$ is the quotient of two integers coprime with p. We denote a by $\operatorname{ord}_p x$.

LEMMA 2: *Let p be a prime number. If $a_1^{b_1}\dots a_n^{b_n}-1\neq 0$ then*

$$\operatorname{ord}_p\left(a_1^{b_1}\dots a_n^{b_n}-1\right)<(p/\log p)(2n)^{C_{10}n}\Omega(\log B)^2,$$

where C_{10} is an effectively computable positive constant.

PROOF: This follows from Theorem 2 of [7]. □

LEMMA 3: *Let S be a finite set of prime numbers and let n be a positive integer. There are only finitely many n-tuples $(x_1,\dots,x_n)$ of rational integers composed of primes from S such that*

$$\text{g.c.d. }(x_1,\dots,x_n)=1,$$

$$x_1+\dots+x_n=0,$$

and

$$x_{i_1}+\dots+x_{i_k}\neq 0,$$

for each proper, non-empty subset $\{i_1,\dots,i_k\}$ of $\{1,\dots,n\}$.

PROOF: This follows from Corollary 1 of [5], see also [8]. □

Evertse [6] proved a result on the number of solutions of the equation $\lambda x+\mu y=1$ in S-units x, y from any fixed algebraic number field. We state and use this result for the rational number field only.

LEMMA 4: *Let λ, μ and ν be non-zero integers. Let $p_1,\dots,p_w$ be distinct prime numbers. There are at most $3\times 7^{2w+3}$ triples of relative prime integers x, y, z each composed of $p_1,\dots,p_w$ such that $\lambda x+\mu y=\nu z$.*

§3. Proof of Theorem 1

Let $a_1,\dots,a_k$ denote the elements of A and let b_1, b_2 be elements of B. Let $p_1,\dots,p_w$ be the primes which divide

$$\prod_{i=1}^{k}\prod_{j=1}^{2}(a_i+b_j).$$

Each element a_i yields a solution $x = a_i + b_1$, $y = a_i + b_2$, $z = 1$ of the equation $x - y = (b_1 - b_2)z$. By Lemma 4, there are at most $3 \times 7^{2w+3}$ such triples $(a_i + b_1, a_i + b_2, 1)$. Hence $k \leqslant 3 \times 7^{2w+3}$. Thus $w > C_4 \log k$ for some effectively computable positive constant C_4. □

§4. Proof of Theorem 2

We shall establish (5) first. Let $c_1, c_2, \ldots$ denote effectively computable positive constants and denote $P(a_1 \ldots a_k(a_1 + b) \ldots (a_k + b))$ by P for brevity. We shall assume that P is at most the $k - 1$ st prime since otherwise, by the prime number theorem, $P > (1 - \epsilon)k \log k$ for $k > k_0(\epsilon)$ and (5) holds. Let $p_1, \ldots, p_w$ be the distinct prime factors of $a_1 \ldots a_k(a_1 + b) \ldots (a_k + b)$. Then

$$w \leqslant k - 1. \tag{7}$$

Further, by the prime number theorem,

$$w < c_1 P / \log P. \tag{8}$$

First, we shall estimate b from below in terms of $a_k + b$. Since $|\log(1 + x)| \leqslant x$ for $x \geqslant 0$,

$$|\log((a_k + b)/a_k)| < b/a_k \tag{9}$$

and, since a_k and $a_k + b$ are composed of primes from $\{p_1, \ldots, p_w\}$,

$$|\log((a_k + b)/a_k)| = |m_1 \log p_1 + \ldots + m_w \log p_w|,$$

where $m_1, \ldots, m_w$ are integers of absolute value at most $2\log(a_k + b)$. By Lemma 1,

$$\begin{aligned} &|\log((a_k + b)/a_k)| \\ &\qquad > \exp\left(-(2w)^{c_2 w} \log p_1 \ldots \log p_w \log(\log p_1 \ldots \log p_w)\right. \\ &\qquad\qquad \left.\times \log(2\log(a_k + b))\right). \end{aligned}$$

Thus, by (8)

$$|\log((a_k + b)/a_k)| > (\log(a_k + b))^{-c_3^P}. \tag{10}$$

Therefore, from (9) and (10)

$$b > a_k / (\log(a_k + b))^{c_3^P},$$

and, since either $b > (a_k + b)/2$ or $a_k \geqslant (a_k + b)/2$,

$$b > \tfrac{1}{2}(a_k + b)/(\log(a_k + b))^{c_3^P}. \tag{11}$$

Next, we shall estimate $\operatorname{ord}_{p_i} b$ from above for $i = 1, \dots, w$. Accordingly, assume that $\operatorname{ord}_{p_i} b$ is positive. By (4), there exists an integer t with $1 \leqslant t \leqslant k$ such that a_t or $a_t + b$ is coprime with p_i. Since $\operatorname{ord}_{p_i} b$ is positive both a_t and $a_t + b$ are coprime with p_i. Thus

$$\operatorname{ord}_{p_i} b = \operatorname{ord}_{p_i}((a_t + b) - a_t) = \operatorname{ord}_{p_i}((a_t + b)/a_t - 1).$$

We may write

$$(a_t + b)/a_t = p_1^{l_1} \dots p_{i-1}^{l_{i-1}} p_{i+1}^{l_{i+1}} \dots p_w^{l_w},$$

where the integers l_m, $m = 1, \dots, w$, $m \neq i$, are of absolute value at most $2 \log(a_k + b)$. Then, by Lemma 2,

$$\operatorname{ord}_{p_i} b < e^{c_4 P}(\log \log(a_k + b))^2, \tag{12}$$

for $i = 1, \dots, w$. Certainly (12) also holds if $\operatorname{ord}_{p_i} b$ is not positive.

To each integer $a_j + b$ with $1 \leqslant j \leqslant k$ we associate a prime $p = p^{(j)}$ such that

$$p^{\operatorname{ord}_p(a_j + b)} \geqslant (a_j + b)^{1/w}, \tag{13}$$

as is possible since at most w distinct primes divide $a_j + b$. The primes $p^{(j)}$ for $j = 1, \dots, k$ are elements of $\{p_1, \dots, p_w\}$ and so, by (7), there are two integers $a_r + b$ and $a_s + b$ with $1 \leqslant r < s \leqslant k$ which are associated to the same prime. Denote that prime by p_i. By (13),

$$\min\{p_i^{\operatorname{ord}_{p_i}(a_r + b)}, p_i^{\operatorname{ord}_{p_i}(a_s + b)}\} \geqslant (a_1 + b)^{1/w}.$$

Therefore, by (8) and (11),

$$\min\{\operatorname{ord}_{p_i}(a_r + b), \operatorname{ord}_{p_i}(a_s + b)\}$$
$$> \frac{c_5}{P} \log\left((a_k + b)/(\log(a_k + b))^{c_6^P}\right). \tag{14}$$

Since $\operatorname{ord}_{p_i}(a_r - a_s) = \operatorname{ord}_{p_i}((a_r + b) - (a_s + b)) \geqslant \min\{\operatorname{ord}_{p_i}(a_r + b), \operatorname{ord}_{p_i}(a_s + b)\}$, we also have

$$\operatorname{ord}_{p_i}(a_r - a_s) > \frac{c_5}{P} \log\left((a_k + b)/(\log(a_k + b))^{c_6^P}\right). \tag{15}$$

Observe that if $\operatorname{ord}_{p_i}(a_r+b) > \operatorname{ord}_{p_i} b$ then $\operatorname{ord}_{p_i} a_r = \operatorname{ord}_{p_i} b$ and similarly if $\operatorname{ord}_{p_i}(a_s+b) > \operatorname{ord}_{p_i} b$ then $\operatorname{ord}_{p_i} a_s = \operatorname{ord}_{p_i} b$. Thus, by (12) and (14), $\operatorname{ord}_{p_i} a_r = \operatorname{ord}_{p_i} a_s = \operatorname{ord}_{p_i} b$ provided that

$$\frac{c_5}{P}\log\Big((a_k+b)/\big(\log(a_k+b)\big)^{c_6^P}\Big) > e^{c_4^P}\big(\log\log(a_k+b)\big)^2. \qquad (16)$$

We may assume that (16) holds since otherwise

$$a_k+b < \big(\log(a_k+b)\big)^{e^{c_7 P}\log\log(a_k+b)},$$

hence

$$P > c_8 \log\log(a_k+b),$$

as required. Therefore

$$\operatorname{ord}_{p_i}(a_r-a_s) = \operatorname{ord}_{p_i} b + \operatorname{ord}_{p_i}(a_r/a_s - 1),$$

and we may employ Lemma 2 as before to estimate $\operatorname{ord}_{p_i}(a_r/a_s-1)$. Combining this estimate with (12) we obtain

$$\operatorname{ord}_{p_i}(a_r-a_s) < e^{c_4 P}\big(\log\log(a_k+b)\big)^2 + e^{c_9 P}\big(\log\log(a_k+b)\big)^2$$
$$< e^{c_{10} P}\big(\log\log(a_k+b)\big)^2.$$

A comparison of the above estimate with (15) reveals that

$$P > c_{11}\log\log(a_k+b),$$

and this completes the proof of (5).

To prove (6) we shall suppose that there is an integer h and there are infinitely many triples (a_1, a_2, b) of positive integers with g.c.d. $(a_1, a_2, b) = 1$ for which

$$P\big(a_1 a_2 (a_1+b)(a_2+b)\big) < h, \qquad (17)$$

and we shall show that this leads to a contradiction. Let S be the set of prime numbers smaller than h. For each triple (a_1, a_2, b) as above we put $x_1 = a_1$, $x_2 = -a_2$, $x_3 = -(a_1+b)$ and $x_4 = a_2+b$. By (17), x_1, x_2, x_3 and x_4 are composed only of primes from S and since g.c.d. $(a_1, a_2, b) = 1$ we have g.c.d. $(x_1, x_2, x_3, x_4) = 1$. Further, $x_1+x_2+x_3+x_4 = 0$ and no non-empty sum of three or fewer terms from $\{x_1, x_2, x_3, x_4\}$ is zero. There are infinitely many quadruples (x_1, x_2, x_3, x_4) as above. However, by Lemma 3 with $n=4$, there are only finitely many such quadruples and this contradiction establishes (6).

References

[1] A. BAKER: The theory of linear forms in logarithms. In: A. Baker and D.W. Masser (eds.), *Transcendence theory: Advances and applications*, London and New York: Academic Press (1977), pp. 1–27.

[2] A. BALOG and A. SÁRKÖZY: On sums of sequences of integers, II, *Acta Math. Hungar.*, to appear.

[3] P. ERDŐS: Problems in number theory and combinatorics. Proc. 6th Manitoba Conference on Numerical Math. (1976), pp. 35–58.

[4] P. ERDŐS and P. TURÁN: On a problem in the elementary theory of numbers. *Amer. Math. Monthly* 41 (1934), 608–611.

[5] J.-H. EVERTSE: On sums of S-units and linear recurrences. *Compositio Math.* 53 (1984) 225–244.

[6] J.-H. EVERTSE: On equations in S-units and the Thue-Mahler equation. *Invent. Math.* 75 (1984) 561–584.

[7] A.J. VAN DER POORTEN: Linear forms in logarithms in the p-adic case. In: A. Baker and D.W. Masser (eds.), *Transcendence theory: Advances and applications*, London and New York: Academic Press (1977), pp. 29–57.

[8] A.J. VAN DER POORTEN and H.P. SCHLICKEWEI: The growth conditions for recurrence sequences. *Macquarie Math. Report* 82-0041 (1982).

[9] J. BARKLY ROSSER and L. SCHOENFELD: Approximate formulas for some functions of prime numbers. Illinois J. Math. 6 (1962), 64–94.

[10] A. SÁRKÖZY and C.L. STEWART: On divisors of sums of integers I. *Acta Math. Hungar.*, to appear.

[11] A. SÁRKÖZY and C.L. STEWART: On divisors of sums of integers II. *J. Reine Angew. Math.*, to appear.

[12] C.L. STEWART and R. TIJDEMAN: On prime factors of sums of integers II, In: J.H. Loxton and A.J. van der Poorten (eds.), Diophantine Analysis, Cambridge University Press, to appear.

(Oblatum 28-X-1985)

K. Győry
Mathematical Institute
Kossuth Lajos University
4010 Debrecen
Hungary

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

R. Tijdeman
Mathematical Institute
Leiden University
2300 RA Leiden
The Netherlands