

The Tails of Infinitely Divisible Laws and a Problem in Number Theory

P. D. T. A. ELLIOTT¹

Department of Mathematics, University of Colorado, Boulder, Colorado 80309

AND

P. ERDÖS

*Mathematical Institute of the Hungarian Academy of Science,
1053 Budapest, Reáltanoda utca 13-15, Hungary*

Communicated by H. Zassenhaus

Received May 31, 1978; revised November 14, 1978

The authors show that if the tail of an infinitely divisible probability law approaches zero sufficiently rapidly, then it must be the Normal Law. An application is made to a problem of number theory.

A probability distribution function is said to be *infinitely divisible* if for every positive integer n it may be expressed as the convolution of n copies of some other distribution function. It was proved by Khinchine that the class of such laws coincides with the class of all limit laws of sums of independent infinitesimal random variables. For this reason they play an important rôle in many applications of the theory of probability.

A function $f(n)$, defined on the positive integers, is said to be additive if it satisfies the relation $f(ab) = f(a) + f(b)$ whenever the integers a and b have no common prime factors. Supposing that for each prime p , $f(p^m) = f(p)$ and $|f(p)| \leq 1$, that

$$B(N) = \left(\sum_{p < N} p^{-1} |f(p)|^2 \right)^{1/2} \rightarrow \infty, \quad (N \rightarrow \infty),$$

and that

$$A(N) = \sum_{p < N} p^{-1} f(p),$$

¹ Partially supported by N.S.F. Contract No. MCS78-04374.

then Erdős and Kac [3], in 1939, proved that

$$N^{-1} \sum_{\substack{n \leq N \\ f(n) - A(N) \leq uB(N)}} 1 \rightarrow \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^u e^{-t^2/2} dt, \quad N \rightarrow \infty.$$

Their method, which was much developed by Kubilius [6] amongst others, depended upon approximating the additive function $f(n)$ with sums of independent random variables. In particular it always led to a limit law which was infinitely divisible.

Let α be a positive real number, $\alpha \neq 1$, and consider the additive function defined by $f(p^m) = (\log p^m)^\alpha$. Although this function is not susceptible to the method of Erdős-Kac [3], already in 1946 Erdős [2] had remarked that the proper limiting distribution

$$K_\alpha(u) = (\text{weak}) \lim_{N \rightarrow \infty} N^{-1} \sum_{\substack{n \leq N \\ f(n) < u(\log N)^\alpha}} 1$$

existed. A distribution function is said to be *proper* if it does not consist of a single jump, and to be *improper* otherwise. If $\alpha = 1$ then the limit law $K_\alpha(u)$ still exists, but is easily seen to be improper.

In a paper of 1955, Halberstam [5] pointed out that the existence of the limiting distribution $K_\alpha(u)$ could be deduced by evaluating the moments

$$\lim_{N \rightarrow \infty} N^{-1} \sum_{n \leq N} \left(\frac{f(n)}{\log N} \right)^k, \quad (k = 0, 1, \dots).$$

The nature of the limit law was obscured, however, since it satisfied a non-trivial integral equation.

Other (later) treatments (Levin and Timofeev [7], Elliott [1]) only give partial help in the study of this limit law. However, Levin and Timofeev, in a short note [8], pointed out that when $\alpha > 1$, then

$$f(n) \leq (\log n)^{\alpha-1} \sum_{p^m || n} \log p^m = (\log n)^\alpha$$

so that $K_\alpha(u) = 0$ for $u < 0$, and $= 1$ for $u \geq 1$. More succinctly, $K_\alpha(u)$ is concentrated on the interval $0 \leq u \leq 1$ for $\alpha > 1$. In particular, a proper such law cannot be infinitely divisible. (They did not indicate a proof.)

It turns out that for $0 < \alpha < 1$ the law $K_\alpha(u)$ is not concentrated on a finite interval. Nevertheless, we shall show that it is still not infinitely divisible. Thus the behaviour of the additive function $\sum (\log p^m)^\alpha$, $\alpha \neq 1$, cannot be investigated (at least in any obvious manner) by the applications of sums of independent random variables.

We shall prove two results to the effect that the tail of an infinitely divisible law cannot decrease to zero too rapidly. The first of these will be applied to the study of the distribution function $K_\alpha(u)$.

THEOREM 1. *Let the proper infinitely divisible law $F(u)$ satisfy*

$$\max(F(-u), 1 - F(u)) \leq e^{-Au \log u} \quad (1)$$

for each $A > 0$ for all sufficiently large values of u . Then it must be a normal law.

THEOREM 2. *Let the proper infinitely divisible law $F(u)$ have a lattice distribution concentrated on a half-line $u > u_0$, and satisfy*

$$1 - F(u) < e^{-cu \log u} \quad (2)$$

for some $c > 0$ and all sufficiently large values of u . Then it must be the convolution of finitely many laws of Poisson type.

Concerning the additive arithmetic function

$$f(n) = \sum_{p^m | n} (\log p)^m$$

we prove:

THEOREM 3. *The distribution function $K_\alpha(u)$ is not infinitely divisible for any positive value of α , $\alpha \neq 1$. For $0 < \alpha < 1$ we have*

$$\begin{aligned} \alpha^{2/(1-\alpha)} &\leq \liminf_{u \rightarrow \infty} \frac{-\log(1 - K_\alpha(u))}{u^{1/(1-\alpha)} \log u} \\ &\leq \limsup_{u \rightarrow \infty} \frac{-\log(1 - K_\alpha(u))}{u^{1/(1-\alpha)} \log u} \leq \frac{1}{1-\alpha}. \end{aligned} \quad (3)$$

Proof of Theorem 1. Let the inequality (1) hold for $u \geq U > 0$. Then for any positive reals r , and $w \geq U$,

$$\begin{aligned} \int_w^{2w} e^{ru} dF(u) &\leq \exp(2wr)(1 - F(w)) \\ &\leq \exp(2wr - \frac{1}{2}Aw \log w) \cdot \exp(-\frac{1}{2}Aw \log w). \end{aligned}$$

The expression in the first of these exponents is greatest when $2r = \frac{1}{2}A$

$(\log w + 1)$, and so (uniformly in w) does not exceed $\exp(\exp(4rA^{-1}))$. Setting $w = 2^k U$, $k = 0, 1, 2, \dots$, in turn, and adding, noting that the series

$$\sum_{k=0}^{\infty} \exp(-\frac{1}{2}A \cdot 2^k U \log 2^k U)$$

converges, we see that

$$\int_{-\infty}^{\infty} e^{xu} dF(u) \leq c_1 \exp(\exp(4rA^{-1})). \quad (4)$$

It follows from a result of Raikov (see, for example, Linnik [9], [10], or Lukacs [11]) that $\varphi(t)$, the characteristic function of the distribution function $F(u)$, coincides on the real axis with an integral function $\varphi(z)$ of the complex variable z . A further result of Raikov (*loc. cit.*) asserts that the Lévy-Khinchine representation

$$\varphi(z) = \exp\left(i\gamma z + \int_{-\infty}^{\infty} \left(e^{izu} - 1 - \frac{izu}{1+u^2}\right) \frac{1+u^2}{u^2} dH(u)\right)$$

of the characteristic function of an infinitely divisible law, initially valid for all real values of z , then holds over the whole complex z -plane. Here the function $H(u)$ is non-decreasing and of finite total variation. In particular $\varphi(z)$ never vanishes and

$$g(z) = i\gamma z + \int_{-\infty}^{\infty} \left(e^{izu} - 1 - \frac{izu}{1+u^2}\right) \frac{1+u^2}{u^2} dH(u) = \log \varphi(z) \quad (5)$$

the value of the logarithm being the principal one when z is near to zero.

It follows from our result (4) that

$$\operatorname{Re}(g(z)) = \log |\varphi(z)| \leq \exp(4|z|A^{-1}) + c_2.$$

An application of the Borel-Carathéodory theorem (see Titchmarsh [12, Section 5.5, p. 174]) allows us to extend this to an upper bound

$$|g(z)| \leq c_3 \exp(8|z|A^{-1}).$$

If $|z| > 1$ then from Cauchy's integral representation theorem

$$g^n(z) = \frac{2!}{2\pi i} \int_{|s-z|=|z|/2} \frac{f(s)}{(s-z)^3} ds$$

so that

$$|g^n(z)| \leq c_4 \exp(12|z|A^{-1}).$$

By adjusting the value of c_4 , if necessary, we may assume that this bound is also satisfied when $|z| \leq 1$.

However, the representation

$$-g''(z) = \int_{-\infty}^{\infty} e^{iz^2u} (1+u^2) dQ(u)$$

which may be deduced from (5) shows that for every imaginary number iy

$$\int_{-\infty}^{\infty} e^{-yu^2} (1+u^2) dH(u) \leq c_4 \exp(12|y|A^{-1}).$$

In this step we have implicitly made another application of the first theorem of Raikov to which we referred earlier.

Suppose now that the function $H(u)$ has a point-of-increase at $u = a > 0$. Then $\delta = H(3a/2) - H(a/2) > 0$ and for every $y < 0$

$$e^{iy|a/2} \cdot \delta \leq c_4 \exp(12|y|A^{-1}).$$

Letting $|y| \rightarrow \infty$ shows that $a \leq 24A^{-1}$, and if A is sufficiently large (see the hypothesis) a contradiction is obtained.

Hence $H(u)$ is concentrated at $u = 0$, and

$$\varphi(t) = \exp(it\gamma t - \frac{1}{2}\sigma^2 t^2)$$

for some $\sigma \geq 0$. The distribution function is then a law of either normal or improper type.

This completes the proof of Theorem 1.

Proof of Theorem 2. Without loss of generality the lattice on which $F(u)$ is concentrated may be assumed to contain the origin, and its maximum span may be taken to be 2π . Then $\varphi(t)$, the characteristic function of $F(u)$ satisfies $\varphi(t+1) = \varphi(t)$ for all real values of t .

Arguing as in the proof of Theorem 1 we see that an integral function $\varphi(z)$ exists, of the form $\exp(g(z))$; and a bound

$$|g(z)| \leq c_1 \exp(c_2|z|)$$

holds for some $c_2 > 0$, this time *fixed*.

Then for real values of t

$$\exp(g(t+1)) = \varphi(t+1) = \varphi(t) = \exp(g(t))$$

so that $g(t+1) - g(t) = 2\pi ni$ for some integer n . Since $g(t)$ is a continuous function of t , n must be a constant, and $g'(t)$, $g''(t)$ will be periodic, of period 1. By analytic continuation this will also be true of the integral function $g''(z)$.

We next note, following the proof of Theorem 1, that

$$|g''(z)| \leq c_3 \exp(c_4 |z|)$$

for some positive constants c_3, c_4 .

However, if $z = x + iy$

$$\begin{aligned} | -g''(x + iy) | &= \left| \int_{-\infty}^{\infty} e^{i(x+iy)u} (1 + u^2) dH(u) \right| \\ &\leq \int_{-\infty}^{\infty} e^{-yu} (1 + u^2) dH(u) = -g''(iy), \end{aligned}$$

(ridge property), so that

$$| -g''(z) | \leq -g''(iy) \leq c_3 \exp(c_4 |y|). \quad (6)$$

For $w \neq 0$ the function $-g''((i/2\pi) \log w)$ is well defined and analytic in the complex w -plane punctured at the origin. It satisfies

$$\begin{aligned} \left| -g'' \left(\frac{i}{2\pi} \log w \right) \right| &\leq c_3 \exp(c_4 | \log |w| |) \\ &\leq \begin{cases} c_3 |w|^{\alpha_4} & \text{if } |w| \geq 1, \\ c_3 |w|^{-\alpha_4} & \text{if } |w| < 1. \end{cases} \end{aligned}$$

Let m be a positive integer, $m > c_4$. It is now easy to extend the definition of $-w^m g''((i/2\pi) \log w)$ to an integral function, and then to deduce that it must be a polynomial in w .

Hence

$$-g''(z) = \sum_{0 < |k| < m} a_k e^{2\pi i k z}.$$

Integrating twice gives

$$g(z) = \sum_{0 < |k| < m} (2\pi k)^{-2} a_k e^{2\pi i k z} + P(z)$$

where $P(z)$ is a polynomial in z of degree at most two.

Suppose now that $(2\pi m)^{-2} |a_{-m}| = 2\delta > 0$. Then choosing θ suitably, $0 \leq \theta \leq m^{-1}$, we see that for all real negative values of y

$$\operatorname{Re} g(iy + \theta) = 2\delta e^{-2\pi m y} + O(e^{-2\pi(m-1)y})$$

and

$$| \varphi(iy + \theta) | \geq \exp(\delta e^{-2\pi m y})$$

if y is large enough. But, by hypothesis

$$|\varphi(iy + \theta)| \leq \int_{\alpha_0}^{\infty} e^{-yu} dF(u) \leq e^{-y\alpha_0}$$

which leads to a contradiction as $-y \rightarrow \infty$.

We deduce that $a_{-m} = 0$, and, likewise, $a_{-k} = 0$ for $k < 0$. Hence

$$g(t) = \sum_{k=1}^m (2\pi k)^{-2} a_k e^{2\pi i k t} + P(t).$$

For every integer $r \geq 1$ the function obtained by differentiating $-g^r(t)$ $2r$ times has a real value when $t = 0$. Hence

$$\sum_{k=1}^m (2\pi k)^{2r} \operatorname{Im}(a_k) = 0.$$

If, for example, $b = \operatorname{Im}(a_m)$, then

$$m^{2r} |b| \leq (m-1)^{2r} \sum_{k=1}^{m-1} |\operatorname{Im}(a_k)|.$$

Dividing by m^{2r} and letting $r \rightarrow \infty$ shows that $b = 0$.

In this way we see that every a_k is real.

Since $g'(t)$ has period 1, $P(t)$ can be at most linear. By considering the size of $|\varphi(t)|$ as $|t|$ becomes unbounded through integer values we deduce that for some real number α ,

$$\varphi(t) = \exp \left(\sum_{k=1}^m (2\pi k)^{-2} a_k (e^{2\pi i k t} - 1) + i \alpha t \right).$$

This completes the proof of Theorem 2.

Proof of Theorem 3. Assume that $0 < \alpha < 1$. We first prove that $K_\alpha(u)$ is not concentrated on a finite interval. Clearly $K_\alpha(u) = 0$ when $u < 0$, so that only the positive values of u are of interest.

Let k be a positive integer. Let N be a further positive integer to be thought of as "large". Let q run through the primes p which lie in the interval $N^{1/(4k)} < p \leq N^{1/(2k)}$. Then for all sufficiently large values of N (see Hardy and Wright [4])

$$\sum \frac{1}{q} = \log 2 + O\left(\frac{1}{\log N}\right) > \frac{1}{2} \log 2.$$

Let m denote a typical integer which is made up of k distinct primes chosen from amongst the q , thus $N^{1/4} < m \leq N^{1/2}$.

Consider the integers n_i , not exceeding N , which are of the form ml , where l is not divisible by any of the (above) primes q . Their number is at least

$$\sum_m \sum_{l \leq N/m} 1.$$

A straightforward application of the Brun or Selberg sieve method shows that if k is fixed at a sufficiently large value, then a typical innersum is at least

$$c_1 \frac{N}{m} \prod \left(1 - \frac{1}{q}\right) + O(N^{1/4}) \geq c_2 \frac{N}{m}.$$

Here the constant c_2 does not depend upon k . Therefore the number of n_i is at least

$$\begin{aligned} c_2 N \sum \frac{1}{m} &\geq c_2 N \left\{ \frac{1}{k!} \left(\sum \frac{1}{q}\right)^k - \frac{1}{(k-2)!} \left(\sum \frac{1}{q}\right)^{k-2} \sum \frac{1}{q^2} \right\} \\ &\geq N \exp(-k \log k - c_3 k). \end{aligned}$$

Moreover,

$$\sum_{p^a | n_i} (\log p)^a \geq k \left(\frac{1}{4k} \log N \right)^a,$$

so that

$$1 - K_\alpha(4^{-\alpha} k^{1-\alpha}) \geq \exp(-k \log k - c_3 k). \quad (7)$$

This shows that $K_\alpha(u) < 1$ for every positive value of u . Indeed, a more careful treatment of details, confining the primes q to an interval $N^{(1-2\epsilon)/k} < q \leq N^{(1-\epsilon)/k}$ and then letting ϵ approach zero enables one to prove that

$$\limsup_{u \rightarrow \infty} \frac{-\log(1 - K_\alpha(u))}{u^{1/(1-\alpha)} \log u} \leq \frac{1}{1-\alpha}.$$

We now obtain a result going in the direction opposite to that of (7). We continue to assume that $0 < \alpha < 1$.

Consider those integers n not exceeding N for which

$$\sum_{p^a | n} (\log p)^a > k(\log N)^\alpha.$$

Let $T = \exp((2 \log N)/k^{1/(1-\alpha)})$. For each integer n under consideration

$$\sum_{p^r | n, p^r > T} (\log p^r)^\alpha \leq (\log T)^{\alpha-1} \sum_{p^r | n} \log p^r \leq 2^{-1+\alpha} k (\log N)^\alpha,$$

so that

$$\sum_{p^r | n, p^r < T} (\log p^r)^\alpha > k(1 - 2^{-1+\alpha})(\log N)^\alpha. \quad (8)$$

Let ω be a positive real number which satisfies

$$\omega \left(1 - \frac{1}{2^\alpha}\right)^{-1} \cdot (2k^{-1/(1-\alpha)}) \leq k(1 - 2^{-1+\alpha}) \quad (9)$$

We maintain that each of the integers n satisfying (8) must have at least ω exact prime-power factors p^r in at least one of the intervals

$$T^{2^{-(j+1)}} < p^r \leq T^{2^{-j}} \quad (j = 0, 1, 2, \dots). \quad (10)$$

Otherwise

$$\begin{aligned} \sum_{p^r | n, p^r < T} (\log p^r)^\alpha &\leq \sum_{j=0}^{\infty} \omega (\log T^{2^{-j}})^\alpha \\ &= \omega \sum_{j=0}^{\infty} 2^{-j\alpha} \left(\frac{2}{k^{1/(1-\alpha)}} \log N\right)^\alpha \leq k(1 - 2^{-1+\alpha})(\log N)^\alpha, \end{aligned}$$

contradicting (8).

Those integers n for which the j th interval in (10) contains at least ω prime-powers are in number at most

$$\begin{aligned} \sum_{\substack{n < N \\ (10) \text{ holds for } j}} \frac{N}{n} &\leq \frac{N}{\omega!} A^\omega \left(1 + \frac{A}{\omega + 1} + \frac{A^2}{(\omega + 1)(\omega + 2)} \dots\right) \\ &\leq N \exp(-\omega \log \omega + c_4 \omega); \end{aligned}$$

here

$$A = \sum \frac{1}{p^r} \leq \sum \frac{1}{p} + \sum_{p, d \geq 2} \frac{1}{p^d} \leq \log \left(\frac{2^{-j} \log T}{2^{-j-1} \log T}\right) + c_3 \leq c_4.$$

Since the intervals in (10) contain no prime-powers unless $j = O(\log k)$ we see that

$$1 - K_\alpha(k) \leq \exp(-c_7 k^{1/(1-\alpha)} \log k). \quad (11)$$

A more careful treatment of this proof leads to the bound

$$\liminf_{u \rightarrow \infty} \frac{-\log(1 - K_\alpha(u))}{u^{1/(1-\alpha)} \log u} \gg \alpha^{2/(1-\alpha)}.$$

It follows from the bound (11) and Theorem 1 that the distribution $K_\alpha(u)$ can be infinitely divisible only if it is a normal law. Since this is clearly not the case, Theorem 3 is established.

Concluding Remarks. The proof that $K_\alpha(u)$ is not infinitely divisible when $0 < \alpha < 1$ depends only upon weak upper bounds of the form $|f(p)| \leq c(\log p)^\alpha$, so that the method is applicable to many other functions $f(n)$ for which a limiting distribution exists.

Perhaps

$$\lim_{n \rightarrow \infty} \frac{-\log(1 - K_\alpha(u))}{u^{1/(1-\alpha)} \log u}$$

exists.

REFERENCES

1. P. D. T. A. ELLIOTT, On the limiting distribution of additive arithmetic functions: Logarithmic Renormalization, *Proc. London Math. Soc.* **31** (1975), 364-384.
2. P. ERDŐS, On the distribution function of additive functions, *Ann. of Math.* **47** (2) (1946), 1-20.
3. P. ERDŐS AND M. KAC, On the Gaussian law of errors in the theory of additive functions, *Proc. Nat. Acad. Sci. U.S.A.* **25** (1939), 206-207.
4. G. H. HARDY AND E. M. WRIGHT, "An Introduction to the Theory of Numbers," Oxford Univ. Press, London/New York, 4th ed., 1960.
5. H. HALBERSTAM, Über additive zahlentheoretische Funktionen, *J. reine angew. Math.* **195** (1955), 210-214.
6. J. KUBILIUS, Probabilistic Methods in the Theory of Numbers, Amer. Math. Soc. Translations of Math. Monographs, 11, Providence, R. I., 1964.
7. B. V. LEVIN AND N. M. TIMOFEEV, On the distribution of values of additive functions, *Acta Arith.* **26** (1975), 333-364.
8. B. V. LEVIN AND N. M. TIMOFEEV, The distribution of values of additive functions, *Uspehi Mat. Nauk.* **28** (1) (169) (1973), 243-244.
9. U. V. LINNIK, "Décompositions des Lois de Probabilités," Gauthier-Villars, Paris, 1962.
10. U. V. LINNIK, "Decomposition of Probability Distributions," Oliver and Boyd, Edinburgh/London.
11. E. LUKACS, "Characteristic Functions," 2nd ed., Griffin, London, 1970.
12. E. C. TITCHMARSH, "The Theory of Functions," 2nd ed., Oxford Univ. Press, London/New York, 1939/1968.