Journal of Number Theory **79**, 115–163 (1999)
Article ID jnth.1999.2395, available online at http://www.idealibrary.com on IDEAL®

Erdős and the Integers

Imre Z. Ruzsa[1]

Mathematical Institute of the Hungarian Academy of Sciences,
Pf. 127, H-1364 Budapest, Hungary
E-mail: ruzsa@math-inst.hu

Communicated by Alan C. Woods

Received June 2, 1997; published online October 8, 1999

INTRODUCTION

It is a difficult task to do justice to the memory of Pál (Paul) Erdős for three reasons. One is the sheer volume of his work: about 500 papers in number theory alone. Another is the diversity of his work; when looking into his papers for this survey I was surprised to see subjects I never imagined he was interested in. The third reason is its peculiar character. A major source of his impact on mathematics came indirectly, through others' work inspired by his questions and conjectures. He was perhaps more proud when he mentioned others' proofs (or disproofs) of his conjectures than when he related his own advances. Thus, in his spirit, I will not restrict myself to his results but describe later achievements that grew out of his ideas.

I started this paper with the idea of being comprehensive—I did not mean, of course, to mention every paper, but at least to touch every important subject. Then I realized that even this was impossible, and that I had to stop sometime; thus this paper is, despite its size, in many aspects incomplete. The most glaring omissions are the statistical theory of partitions and questions of irrationality—I hope that someone, more competent than I, will write about them. The selection and relative coverage of topics often reflect, besides their importance, the fact that I am better informed in some areas than in others.

A final caveat is that when I select or miss one of the later improvements or related results, this is by no means intended as a judgement on the importance of these works; I wanted to give a typical example, or a starting point where the interested reader might find further references, nothing else.

[1] Supported by the Hungarian National Foundation for Scientific Research under Grant T 017433.

0022-314X/99 $30.00

Whenever I say something is "the record up to date," this reflects my knowledge, which may be deficient; corrections are welcome.

This paper deals only with the work of Erdős, not his life or personality. In the short time since his death many obituaries, personal recollections about him etc., have appeared, and the bibliography cites some of these. I mention his biography by Babai (1996), which was written during his life and is based on long interviews with him and on thorough research. I also wrote my personal reminiscences (Ruzsa, 1996b). A complete list of his papers in number theory appeared in *Acta Arithmetica* **81** (1997), 319–343.

I will delve more into his early work which can now be seen in better perspective. I was tempted to say "his most important work was done up to 1970"; I am sure this is true statistically, but I would be reluctant to brand any single result or question of his as unimportant. The reason is his penchant for considering seemingly irrelevant particular cases, which may be like the mustard seed. For instance, his obstinate repetition of the question whether almost all integers have a pair of divisors satisfying $d<d'<2d$ was certainly the main driving force leading to a statistical theory of divisors. (See Section 6.)

As an important contribution to the development of number theory in Hungary (with a decisive impact also on the writer of these lines) I mention here his beautiful book with Surányi (1960) (an English translation will finally appear in the near future).

The treatment is divided into the following main topics:

I. Primes.
II. Divisors, sets of multiples, primitive sequences.
III. Arithmetical functions.
IV. Additive problems.
V. Miscellaneous.

Notation. In citations if no author is given (or can be inferred), the author is Erdős.

$\log_k$ denotes k times iterated logarithm.
$f \asymp g$ for functions f, g means that f/g is between positive bounds.

I. PRIMES

1. *The Number of Primes*

The mathematical career of Erdős started remarkably conventionally, with a variation on an old theme, Chebyshev's theorem (Erdős, 1930/1932). He was very fond of this piece, so let us say a few words about it.

When we say "'Chebyshev's theorem," we think of one (or more) of the following claims.

(a) $c_1(x/\log x) < \pi(x) < c_2(x/\log x)$ for large x, with positive constants c_1, c_2. Here $\pi(x)$ is the number of primes up to x.

(b) $c_1 x < \psi(x) < c_2 x$ for large x. Here

$$\psi(x) = \sum_{p,\,k:\,p^k \leqslant x} \log p = \sum_{n \leqslant x} \Lambda(n).$$

(c) In the words of N. J. Fine[2] "Cheyshev said it, I'll say it again: There's always a prime between n and $2n$."

Here (a) and (b) are equivalent by an obvious partial summation, and if we have either of them with $c_2 < 2c_1$ then we can deduce (c).

Now with

$$L(n) = \sum_{k=1}^{n} \log k = \log n!$$

we have

$$L(x) = \sum \psi(x/k) \tag{1.1}$$

(Legendre's formula for the prime decomposition of $n!$). By a subtraction we get

$$L(x) - 2L(x/2) = \psi(x) - \psi(x/2) + \psi(x/3) - \psi(x/4) + \cdots \begin{cases} \leqslant \psi(x) \\ \geqslant \psi(x) - \psi(x/2). \end{cases} \tag{1.2}$$

Since $L(x) - 2L(x/2) \sim (\log 2)\, x$, we immediately get that $\psi(x) > (\log 2 - \varepsilon)\, x$ and

$$\psi(x) = (\psi(x) - \psi(x/2)) + (\psi(x/2) - \psi(x/4)) + \cdots < (2 \log 2 + \varepsilon)\, x. \tag{1.3}$$

Thus we have (a) and (b) with $c_2 = (2 + \varepsilon)\, c_1$, which is just too weak for (c).

Chebyshev took the more complicated expression

$$L(x) - L(x/2) - L(x/3) - L(x/5) + L(x/30) = \psi(x) - \psi(x/6) + \cdots,$$

which enabled him to obtain (a), (b) with $c_2 = (6/5 + \varepsilon)\, c_1$ and to deduce (c). No doubt his starting point was (1.2), though he kept this secret.

[2] I heard this rhyme attributed to Erdős; Professor P. Bateman informed me that Fine is the author.

Erdős observed that we can get (c) from (1.2) as follows. Equation (1.2) shows

$$L(x) - 2L(x/2) \leqslant \psi(x) - \psi(x/2) + \psi(x/3);$$

hence we get

$$\psi(x) - \psi(x/2) \geqslant L(x) - 2L(x/2) - \psi(x/3) \geqslant \left(\frac{\log 2}{3} - \varepsilon\right) x$$

by estimating $\psi(x/3)$ via (1.3).

His other observation was that

$$L(x) - 2L(x/2) = \log \binom{x}{x/2}$$

if x is an even integer, which simplifies the task of estimating this quantity.

A few years later he extended his method to primes in certain arithmetical progressions (1935g), using products of consecutive terms of an arithmetic progression in the place of factorials. These results were made numerically explicit by Moree (1993). For instance, for any $x \geqslant 130$ the interval $(x, 4630x)$ contains a prime from each reduced residue class modulo 840.

These results point in three directions:

— estimate $\pi(x)$, $\psi(x)$ elementarily;

— estimate the gaps between primes (see the next section);

— the multiplicative structure of binomial coefficients (see Section 14).

In the first direction an aim more ambitious than that of improving the values of c_1, c_2 is to make them arbitrarily near, that is, to prove the prime number theorem. Erdős (1997) wrote:

> In 1937, Kalmár and I proved that for every ε there is an elementary proof for
>
> $$(1-\varepsilon)\frac{n}{\log n} < \pi(n) < (1+\varepsilon)\frac{n}{\log n}, \qquad n > n_0(\varepsilon).$$
>
> Our proof did not give an elementary proof of the prime number theorem since it was based on the following fact. Let $\delta = \delta(\varepsilon)$ be small but fixed. Then one can find a k so that for every $k < t < k^2$,
>
> $$\sum_{n=1}^{t} \mu(n) < \delta t, \tag{1.4}$$
>
> where μ is the usual Möbius function. That such a k exists follows from the prime number theorem, but (1.4) can be shown by a finite computation.

Somehow this escaped publication at that time. Forty years later Diamond and Erdős (1980), in a paper dedicated to the memory of Kalmár, reconstructed this proof, that is, they showed for every $\varepsilon > 0$ the existence of a finite combination (with weights) of $L(x)$, $L(x/2)$, ..., $L(x/k)$ for which a Chebyshev-type argument yields constants satisfying $c_2 - c_1 < \varepsilon$.

For a good numerical example see Costa Pereira (1989).

The elementary proof of the prime number theorem became possible a decade later, with Selberg's invention of the formula

$$\sum_{p \leqslant x} (\log p)^2 + \sum_{pq \leqslant x} \log p \log q = 2x \log x + O(x); \tag{1.5}$$

here p, q run over the primes. The prime number theorem was deduced from this by Selberg himself and by Erdős. The relationship of their proofs is discussed in Ingham's review in the *Mathematical Reviews* (10-595bc).

Since then many elementary proofs have been found, most of them based on Selberg's formula. An elementary proof without Selberg's formula was found by Daboussi (1984), and another by Hildebrand (1986). There are several attempts to obtain elementary proofs with an error term. The first was by P. Kuhn (1955). The record to date is held by Lavrik and Shobirov (1973); it is

$$\psi(x) - x \ll x \exp\{-(\log x)^{1/6 - \varepsilon}\}.$$

2. *Gaps Between Primes*

The previous arguments show that to estimate the number of primes between x and $x + y$ we do not need to know $\pi(x)$ and $\pi(x + y)$ separately. Indeed,

$$\pi(x + y) - \pi(x) \sim \frac{y}{\log(x + y)} \tag{2.1}$$

is known to hold for $y = x^{7/12 + \varepsilon}$, a bound much smaller than the error term for $\pi(x)$. In Erdős' approach to the prime number theorem an intermediary step was the deduction of a lower bound similar to (2.1) for arbitrary $y = cx$ from Selberg's formula. Erdős should have asked (but seemingly he did not) whether there is an elementary proof of (2.1) for values of y smaller than the elementary error term in the prime number theorem.

He was very much interested in values of y for which the left side of (2.1) vanishes, that is, gaps between consecutive primes. With p_n denoting the

nth prime and $d_n = p_{n+1} - p_n$, the prime number theorem is equivalent to saying

$$\sum_{i=1}^{n} d_i \sim n \log n;$$

thus d_n is about $\log n$ on average. Erdős (1940) proved that smaller values do exist, namely

$$\liminf \frac{d_n}{\log n} < 1$$

(this was established on the Riemann hypothesis earlier by Hardy and Littlewood). Several numerical values were given, the record being Maier's (1988).

About large values of d_n, the first to prove

$$\limsup \frac{d_n}{\log n} > 1$$

was Backlund (1929). His value was 2; Brauer and Zeitz (1929) improved this to 4, and then Westzynthius (1931) proved that the value was infinite.

To measure the degree of improvement here, put

$$g(n) = \max_{k \leqslant n} \frac{d_n}{\log(n+1)}.$$

For $g(n)$ Westzynthius found the lower estimate $c \log_3 n / \log_4 n$; Ricci (1934) removed the $\log_4$; Erdős (1935a) improved this to $\log_2 n/(\log_3 n)^2$, an exponential increase. Rankin (1938) added a further $\log_4$, and since then only the value of the constant was been improved; the record of $2e^\gamma$, where γ is Euler's constant, is due to Pintz (1997).

This is also famous as the Erdős problem with the highest prize. Originally Erdős offered \$10,000 for any factor going to infinity; recently he reduced this to \$5000, reserving the \$10,000 for a power of logarithm.

If we build a moronic random model for the primes, including any number n with probability $1/\log n$, then the maximal gap up to n will be asymptotic to $(\log n)^2$; that is, we have $g(n) \sim \log n$ (Cramér's conjecture). Observe that in this model $d_n = 1$ infinitely often, which is a marked difference from the case of primes. Another consequence of this model would be that (2.1) holds as soon as $y/(\log x)^2 \to \infty$, while in reality it fails even for $y = (\log x)^c$ with arbitrary constant c (Maier, 1985). In this connection let me quote some (I think unpublished) conjectures of Erdős from a letter to me.

Let $D(x) = \max_{p_k < x}(p_{k+1} - p_k)$. It is obviously true that

$$\max_{p_k < x} (p_{k+1} - p_k)(p_k - p_{k-1})/D(x)^2 \to 0, \tag{2.2}$$

but of course I cannot prove (2.2). One could ask the same for squarefree numbers rather than primes, but it can't be done either. Perhaps if $n_k = 2 \cdot 3 \cdot \cdots \cdot p_k$ and $1 = a_1 < \cdots < a_{\phi(n_k)} = n_k - 1$ are coprime to n_k and $J(n_k) = \max(a_{i+1} - a_i)$, then

$$\max(a_{i+1} - a_i)(a_i - a_{i-1})/J(n_k)^2 < \varepsilon$$

for $k > k_0(\varepsilon)$, and perhaps this is not so difficult.

Let $x/2 < y < x$. It is certainly not true that

$$\pi(y + (1+c)\, D(x)) - \pi(y) = (1 + o(1))\, \frac{(1+c)\, D(x)}{\log y},$$

but can one disprove this? Again, one could ask this for the squarefree numbers; that can't be done, but perhaps for the numbers coprime to n_k it can.

In the random model the limit in (2.2) will be 1/4 with probability 1. So, if this is true, (2.2) is a very strong indicator for the non-randomness of primes. Perhaps it would be interesting to carry out some numerical investigations of (2.2).

Erdős (1949a) also proved that

$$\limsup \frac{\min(d_n, d_{n+1})}{\log n} = \infty.$$

It is easy to see that the sequence d_n cannot be monotonic (in other words, p_n is not convex) from a point on. Erdős (1948c) proved the following stronger result: with some $c > 0$ the sequences

$$\{n: d_{n+1}/d_n > 1 + c\}, \qquad \{n: d_{n+1}/d_n < 1 - c\}$$

both have positive lower density. Erdős and Turán (1948c) showed that p_n^t is not ultimately convex or concave either, for any choice of the constant t.

From the prime number theorem we know that $p_n/n \sim \log n$. Erdős and Prachar (1961/1962) showed that p_n/n is not monotonic from a point onward, and found the stronger result

$$\sum_{p_n \leqslant x} \left| \frac{p_{n+1}}{n+1} - \frac{p_n}{n} \right| \asymp (\log x)^2.$$

(The symbol $\asymp$ means that the quotient of the left and right sides stays between positive bounds.) They also proved that a subsequence for which p_{n_i}/n_i is monotonic has $o(\pi(x))$ elements up to x. This was improved by Rieger (1966).

Erdős often mentioned that "he and Ricci" proved that the set of limit points of $d_n/\log n$ has positive measure, but so far no one has identified a single element of this set. I was unable to find whether he published anything on this; Ricci (1955) considers left and right limit points, and shows each to have measure $\geqslant 1/8$.

He was also interested in gaps between products of k primes. I quote from another letter:

> It is an old question of mine whether, if $u_1 < u_2 < \cdots$ is the sequence of those numbers that have at most two prime factors, it is true that
>
> $$\overline{\lim} \frac{u_{k+1} - u_k}{\log k} = \infty. \tag{2.3}$$
>
> It can be done with $> c$ instead of ∞, but if we take those u's that have at most three prime factors, even this cannot be done any more.

II. DIVISORS, SETS OF MULTIPLES, PRIMITIVE SEQUENCES

These fields have grown so large that by now two monographs have been published (on different aspects): "Divisors," by Hall and Tenenbaum (1988), and "Sets of Multiples," by Hall (1996). We refer the reader to them for a systematic account. Here we mention only a couple of points.

3. *Abundant Numbers*

An integer is *perfect*, if it satisfies $\sigma(n) = 2n$, with $\sigma(n)$ denoting the sum of divisors of n. It is an easy exercise to show that the number of perfect numbers up to x is $O(\sqrt{x})$ (which was improved by Wirsing (1959) to $x^{c/\log\log x}$); thus most numbers satisfy either $\sigma(n) > 2n$, in which case they are called *abundant*, or $\sigma(n) < 2n$, and then they are *deficient*.

Let $A(x)$ denote the number of abundant numbers up to x. It is easy to see that $c_1 x < A(x) < c_2 x$ with constants $0 < c_1 < c_2 < 1$, but does $A(x)/x$ tend to a limit? (Or, in other words, do the abundant numbers have an asymptotic density?) Erdős attributes this question to Bessel-Hagen (I was unable to locate this work). The affirmative answer was given independently by Davenport (1933), Chowla (1934), and Erdős (1934). This early work so perfectly shows the Erdősian way of thinking that I shall say more about it.

Since $\sigma(n)/n = \sum_{d \mid n} 1/d$, we always have $\sigma(kn)/(kn) \geqslant \sigma(n)/n$, with strict inequality if $k > 1$. Thus the set $\mathscr{A} = \{n : \sigma(n) \geqslant 2n\}$ has the property that for every number in the set,it contains all its multiples (it is a multiplicative ideal, a word Erdős never used).

Now for every set $\mathscr{B}$ we can build its *set of multiples*

$$M(\mathscr{B}) = \{n : d \mid n \text{ for some } d \in \mathscr{B}\}.$$

Does a set of multiples (an ideal) always have an asymptotic density? Besicovitch (1934) gave an example for which it does not. However, if $\mathscr{B}$ is so small that the sum of reciprocals of its elements converges, then an elementary argument shows that $M(\mathscr{B})$ has an asymptotic density. For a given ideal the smallest set that generates it is the set of its *primitive elements*, those numbers that have no nontrivial divisor within the set. For the set of abundant and perfect numbers this is the set

$$\mathscr{B} = \{n : \sigma(n) \geqslant 2n, \sigma(d) < 2d \text{ for all } d \mid n, d < n\}$$

of *primitive abundant numbers*. Erdős proved that the number of primitive abundant numbers up to x is $O(x/(\log x)^2)$, which immediately shows the convergence of the sum of reciprocals.

To achieve this, he first shows that all but $O(x/(\log x)^2)$ numbers up to x have the following three properties:

(1) If $p^k \mid n$, p prime, $k \geqslant 2$, then $p^k < (\log x)^{10}$;

(2) $\Omega(n) < 10 \log\log x$, where Ω stands for the number of prime divisors, counted with multiplicity;

(3) the maximal prime factor of n is $> x^{1/(20 \log\log x)}$.

Then he proved that if a primitive abundant number has properties (1)–(3), then it must have a prime factor in the range

$$(\log x)^{10} < p < x^{1/(20 \log\log x)},$$

and if we pick up such a prime for each primitive abundant n, then the quotients n/p are all different. This immediately gives the required upper estimate.

The secret of Erdős lies somewhere here. He saw the structure of "a typical integer"; numbers were his friends (as were graphs and infinite cardinalities).

Observe that if we consider abundant numbers only, excluding the perfect numbers, then the definition of primitive abundant changes into $\sigma(n) > 2n$ but $\sigma(d) \leqslant 2d$ for all nontrivial divisors. This includes all numbers of the form $6p$, $p \geqslant 5$ prime, and the sum of reciprocals will diverge. We also run into difficulties if we try to extend this result to the numbers satisfying $\sigma(n)/n \geqslant \alpha$ for any given α. We can define α-abundant and primitive α-abundant numbers analogously, and Erdős (1958a) showed that their number up to x is $o(x/\log x)$. This is essentially best possible and their sum of reciprocals need not converge.

For the number $B(x)$ of primitive abundant numbers up to x he found the sharper estimates (1935b)

$$xe^{-c_1\sqrt{\log x \log\log x}} < B(x) < xe^{-c_2\sqrt{\log x \log\log x}}$$

with certain positive constants c_1, c_2. The values of c_1, c_2 were improved by Ivič and recently by Avidon (1996).

Since every multiple of 6 is abundant, a block of consecutive deficient numbers can have at most five elements (and it is easy to see that this happens infinitely often). On the other hand if $g(n)$ denotes the maximal length of a block of abundant numbers $\leqslant n$, then we have (Erdős, 1935e)

$$g(n) \asymp \log_3 n.$$

The story of abundant numbers points also toward the theory of arithmetical functions, (see Part III).

4. *The Existence of Density*

Since from Besicovitch (1934) we know that a set of multiples need not have an asymptotic density, the question arises whether they have a density in another sense, and what additional assumptions will guarantee the existence of asymptotic density. Davenport and Erdős (1937, 1951) answer the first question as follows. The *logarithmic density* of a set $\mathscr{A}$ is the quantity

$$\lambda(\mathscr{A}) = \lim_{x\to\infty} \frac{1}{\log x} \sum_{a\in A,\, a\leqslant x} \frac{1}{a}$$

if it exists. Now take an arbitrary set $\mathscr{B}$, and let $\mathscr{A} = M(\mathscr{B})$ be the set of multiples. Furthermore put $\mathscr{B}_n = \mathscr{B} \cap [1, n]$ and $\mathscr{A}_n = M(\mathscr{B}_n)$. The sets $\mathscr{A}_n$ (are periodic, hence obviously) have an asymptotic density. The set $\mathscr{A}$ has a logarithmic density and it satisfies

$$\lambda(\mathscr{A}) = \underline{d}(\mathscr{A}) = \lim d(\mathscr{A}_n).$$

The first paper proves this via the simple Tauberian theorem

$$\lambda(\mathscr{A}) = \lim_{s\to 1^+} \frac{1}{\zeta(s)} \sum_{a\in A} a^{-s},$$

the second with elementary considerations.

Warlimont (1991) extended this result to certain abstract semigroups. I found (Ruzsa, 1996a) a third approach, based on convolutions of measures on certain semigroups. This also yields the following generalization.

I call a set A a *weak ideal*, if it has the following property. If for an integer n we can find an $a_0 \in A$ such that $a_0 n \in A$, then $an \in A$ for all $a \in A$. Weak ideals also always have a logarithmic density.

In general it is a difficult problem to decide for a given set $\mathscr{B}$ whether its set of multiples has an asymptotic density (after Hall, we call a set a *Besicovitch set* if it does), and whether it is equal to 1 or not.

Erdős (1948b) gave a sort of necessary and sufficient criterion for the existence, the application of which for concrete cases, however, may not be easy. A remarkable corollary is that this is always the case if $B(x) = O(x/\log x)$.

Erdős, Hall, and Tenenbaum (1994) show that the union of two Besicovitch sets is a Besicovitch set again, but their intersection need not be one. As an interesting sufficient criterion for this property they provide the following: if the number of prime divisors of all $\gcd(a, a')$, $a, a' \in \mathscr{A}$, is bounded, then $\mathscr{A}$ is a Besicovitch set.

5. *Primitive Sequences*

Different sets may generate the same set of multiples. Among the sets $\mathscr{B}$ such that $M(\mathscr{B}) = \mathscr{A}$ there is a largest, $\mathscr{A}$ itself, and a smallest, namely

$$\mathscr{B} = \{a \in A\colon \text{there is no } d \in A, d \mid a, d < a\},$$

the set of primitive elements of $\mathscr{A}$. We call a set that is the set of primitive elements of another set a *primitive set*. This definition immediately implies that a set is primitive if and only if no element divides any other element.

A primitive set may be quite dense: it can have upper density $1/2 - \varepsilon$. This follows from the facts that a finite set $\mathscr{A}_n = \{n+1, n+2, ..., 2n\}$ is primitive, but $d(M(\mathscr{A}_n)) \to 0$. The same observation leads to a construction for which $d(M(\mathscr{A}))$ does not exist; these are due to Besicovitch. However, this cannot happen frequently. If $\mathscr{A}$ is primitive, then with an absolute constant c we have for all x

$$\sum_{a \in \mathscr{A},\, a < x} 1/a \leqslant c \frac{\log x}{\sqrt{\log \log x}} \tag{5.1}$$

(Behrend, 1935). The best value of c is $\sim 1/(2\pi)$ for large x; here the lower estimate comes from Erdős (1948a), the upper one from Erdős, Sárközy, and Szemerédi (1967a).

It is interesting to remark that the finite and infinite cases differ. If we take an infinite primitive set A, then, as $x \to \infty$, the $\leqslant c \cdots$ in (5.1) can be replaced by $= o(\cdots)$ (Erdős, Sárközy, and Szemerédi, 1967b). Later the same authors (1969) proved that the same conclusion follows from the much weaker hypothesis that the set does not contain three distinct elements, say a, b, c, such that $\mathrm{lcm}[a, b] = c$.

Erdős (1935d) proved that for a primitive sequence $\sum 1/(a \log a)$ is always convergent and the value is bounded from above by an absolute constant. He conjectured that the extremal set is that of the primes; currently the best bound is that of Clark (1995), equal to $e^{\gamma} \approx 1.7811$.

6. *Statistical Theory of Divisors*

In (1948b), as an application of his criterion on the existence of density for certain sets of multiples, Erdős showed that the set of integers which have a pair of divisors satisfying $d < d' < 2d$ has asymptotic density, and conjectured that it is 1. In (1964a) he announced cautiously that he thought he had a proof, which he later recalled. This became one of his favourite problems, which he repeated ostentatiously. The solution was finally given by Maier and Tenenbaum (1984); this led to the much stronger result that almost all integers n have a pair of divisors such that

$$1 < d'/d < 1 + (\log n)^{1 - \log 3 + \varepsilon},$$

where the exponent is best possible (this form was also conjectured by Erdős).

An interesting generalization is studied by Raouj (1995). For a given n and λ he considers the set of multiples of the finite set

$$\bigcup_{d \mid n} (d, d(1 + 1/\log n)^{\lambda}).$$

He exactly describes the asymptotic behaviour of the density of this set.

As a contrast to the above, the density of those integers that have a triple of pairwise coprime divisors (observe that this does not restrict generality for a couple) satisfying $d_1 < d_2 < d_3 < 2d_1$ exists and it is < 1 (Erdős, 1970a). In the same paper we find the following result: the integers with the property that all the $2^{\tau(n)}$ sums formed from divisors of n are all distinct again has a positive density.

He considered the question, How many of the integers up to x are expressible as a product of two factors $\leqslant \sqrt{x}$ first in (1955). He returned to this in (1960), prompted by Linnik and Vinogradov, and gave the following estimate: this number is about

$$x(\log x)^{-c}, \qquad c = 1 - \frac{1 + \log \log 2}{\log 2} \approx 0.086071332.$$

We still do not have an asymptotic formula (the "about" above means that this is correct up to a factor $(\log x)^{o(1)}$).

In his letter to me of October 25, 1981, he asks:

> Let
>
> $$f(n) = \sum_{(d_i, d_{i+1})=1} d_i/d_{i+1}.$$
>
> ($1 = d_1 < d_2 < \cdots < d_{\tau(n)} = n$ are the divisors of n.) Is it true that
>
> $$\frac{1}{x} \sum_{n=1}^{x} f(n) \to C < \infty?$$
>
> Does the sequence $f(n)$ have a limiting distribution?

Later he and Tenenbaum (1989) found that

$$f(n) = (\log n)^{\log 3 - 1 + o(1)}$$

for almost all n. The following, related result is worth mentioning:

$$g(n) = \sum_{(d_i, d_{i+1})=1} 1$$

satisfies $g(n) \leqslant \tau(n)^c$ with a certain constant $1/2 < c < 1$, while $g(n) > \tau(n)^{1/2}$ infinitely often (Tenenbaum, 1991).

III. ARITHMETICAL FUNCTIONS

7. *Foundations of Probabilistic Number Theory*

To prove that abundant numbers have a density, Erdős used the fact that this set is a multiplicative ideal. This property alone is insufficient, and he had to resort to further particular considerations. With this approach it is difficult to handle even the slightly more general problem of the density of the set $\{n: \sigma(n)/n > \alpha\}$ for general α, and even more difficult to turn to other functions.

We remind the reader that an arithmetical function (a function defined on the positive integers) is *multiplicative*, if it satisfies $f(mn) = f(m) f(n)$ for all pairs of coprime integers m, n, and it is *additive*, if it satisfies $f(mn) = f(m) + f(n)$ instead. If these equations are assumed to hold for all (rather than only coprime) pairs of integers, the function is completely multiplicative or completely additive, respectively.

In the above case, we are interested in the density of the set $\{n: g(n) > \alpha\}$ for the multiplicative function $g(n) = \sigma(n)/n$. By an obvious transformation this is equivalent to the analogous question for the additive function $f(n) = \log g(n)$. Some notations will be more appropriate for additive functions, so we will speak about additive rather than multiplicative functions. Note, however, that this logarithmic transformation is possible only for positive multiplicative functions, and for multiplicative functions assuming also negative (or even complex) values further difficulties will arise. The starting case had one more pecularity; $\sigma(n)/n$ was always $\geqslant 1$, whence the resulting additive function f was nonnegative.

One could ask what further properties a set of the form $\{n: f(n) \leqslant a\}$ possesses. It is not difficult to exhibit such properties; say, if f is completely additive and $n_1, ..., n_k, m$ are such integers that satisfy an equation $m = \prod n_i^{r_i}$ with positive rational exponents whose sum is 1, then if all the n_i are in our set, so must m be. I do not know whether such properties can be of any use in establishing the existence of density, but seemingly the whole approach is a dead end. The real idea is to look at all the sequences arising from different values of a together, that is, to ask about the *limiting distribution* of the function. If exploring the structure of these sets is of any use, it is likely to be in the opposite way: with some luck we can reduce a question about sequences to one about functions. An instance of this is the following question of Erdős (1969b). Suppose a set A of natural numbers has the property that $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_n$ with $a_i, b_j \in A$ can occur only when $k = n$. (An example is all the numbers $\equiv 2 \pmod 4$.) How dense can such a set be? I proved (1977) that given such a set we can find an additive function such that $f(a) = 1$ for all $a \in A$, and this led to the answer that the upper density is always $< 1/e$, which is tight. This sort of application of additive functions to multiplicative properties of sets of integers was extensively studied by Elliott (1985); we quote a result later.

Let us say that an arithmetical function f has a *density limiting distribution*, if the sets $\{n: f(n) \leqslant a\}$ always have an asymptotic density. The early works on the distribution of arithmetical function used this concept. Later it was realized that it is better to require this for almost all values of a only (I do not know who first proposed this step). This is equivalent to the now common formulation which requires that the finite distributions

$$F_N(u) = \frac{1}{N} \# \{n \leqslant N: f(n) \leqslant u\}$$

converge weakly. The existence of a limiting distribution was first proved by Schoenberg (1928), for the function $\phi(n)/n$; the next proof was by Davenport (1933), with $\sigma(n)/n$.

In (1935c) Erdős makes a leap forward by proving the existence for a class of functions, namely, for the additive functions satisfying $f(n) \geqslant 0$ and

$f(p_1) \neq f(p_2)$ for all pairs $p_1 \neq p_2$ of primes; the second condition was removed in Erdős (1937a). It can be remarked that this class is in a sense "too general", the density is often identically 0. Schoenberg (1936) proved this for functions which are not necessarily of constant sign, but satisfy

$$\sum_p \frac{\min(1, |f(p)|)}{p} < \infty.$$

Schoenberg also showed that the distribution is discrete if $\sum_{f(p)\neq 0} 1/p < \infty$ and continuous if there is a sequence p_j of primes such that $\sum 1/p_j = \infty$ and $f(p_i) \neq f(p_j)$ whenever $i \neq j$. This is a rather restrictive condition, but it includes (after obvious transformations) the classical funtions $\phi(n)/n$, $\sigma(n)/n$. Continuity is also important because then the existence of density follows from the existence of limiting distribution in the usual sense. In general it does not, just imagine a function $f(n) = \pm 1/n$ with long blocks of identical sign. For additive functions with $\sum_{f(p)\neq 0} 1/p < \infty$ the existence of densities can be easily shown directly.

Erdős (1938) generalized Schoenberg's result in as follows. If an additive function satisfies

$$\sum \frac{\min(1, f(p)^2)}{p} < \infty$$

and the series

$$\sum_{|f(p)|<1} f(p)/p$$

is convergent, then f has a limiting distribution. The importance of this condition is that it is also necessary, which was established soon afterward by Erdős and Wintner (1939) and thus became known as the Erdős–Wintner theorem, the first completely general result on the limiting distribution of additive functions. It is also perhaps the first application of Turán's method. To prove Hardy and Ramanujan's (1917) theorem that $\omega(n)$, the number of prime divisors of n, is about $\log\log n$ for almost all n, Turán (1934) showed that one can easily estimate the second moment

$$\sum_{n \leqslant N} (\omega(n) - \log\log N)^2.$$

In 1936 he extended this to a class of additive functions. The most general form, which became known later as the Turán–Kubilius inequality, was found by Kubilius (1959, 1962, 1964). This asserts that for every additive function f we have

$$\sum_{n \leqslant N} (f(n) - A)^2 \leqslant cN \sum_{p^k \leqslant N} p^{-k} f(p^k)^2,$$

where c is an absolute constant and A can be any of the quantities

$$\frac{1}{N} \sum_{n \leqslant N} f(n), \qquad \sum_{p^k \leqslant N} (p^{-k} - p^{-(k+1)}) \, f(p^k),$$

$$\sum_{p^k \leqslant N} p^{-k} f(p^k), \qquad \sum_{p \leqslant N} p^{-1} f(p).$$

Many proofs, variants, and extensions of the Erdős–Wintner theorem have been given. De la Cal (1992) extended it to functions with values in a Banach space.

Erdős (1937b) showed that $\omega(n) > \log\log n$ holds for a set of integers of asymptotic density 1/2, To do so he de facto proved, though did not state, a central limit theorem for ω. What he proved was the following.

(a) A sufficiently truncated ω—let us call it ω'—satisfies a local limit theorem. He defines $\omega'(n)$ as the number of prime factors of n in the range $((\log N)^6, n^{1/(\log\log\log N)^3})$, when the numbers $n \leqslant N$ are considered. Then

$$\#\{n \leqslant N : \omega'(n) = k\} \sim \frac{(\log\log N)^{k-1}}{k!} \frac{N}{\log N}$$

for $k \sim \log\log N$.

(b) The average of $\omega(n) - \omega'(n)$ is $O(\log\log\log N)$; hence

$$\omega(n) - \omega'(n) = o(\sqrt{\log\log N})$$

for almost all n.

Statements (a) and (b) immediately imply that

$$\frac{1}{N} \#\{n \leqslant N : \omega(n) - \log\log N < u\sqrt{\log\log N}\}$$

$$\to \Phi(u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{u} e^{-t^2/2} \, \mathrm{d}t, \tag{7.1}$$

a usual central limit law, but Erdős was content with stating only the case $u = 0$.

These results hint at a close parallelism between additive functions and results of probability theory like Chebyshev's inequality, the additivity of the variance for independent variables, or the central limit theorems. The pioneers quoted above seemingly did not notice this connection. Elliott (1980, pp. 18–20) interviewed Turán about this. Turán writes:

> When writing Hardy first in 1934 on my proof of Hardy–Ramanujan's theorem I did not know what Tchebycheff's inequality was and a fortiori on central limit theorem. Erdős, to my best knowledge, was at that time not aware too. It was Mark Kac who wrote to me a few years later that he discovered when reading my proof in J. L. M. S. that this is basically probability and so was his interest turned to this subject. He asked me whether or not I can do the same for
>
> $$H_k = \frac{1}{x} \sum_{n \leqslant x} (\omega(n) - \log\log x)^k,$$
>
> $k = 3, 4, \ldots$ too, and *perhaps* he made even a hint as to the Gaussian value distribution of $\omega(n)$.

Thus it was Kac who introduced the probabilistic point of view to the theory of arithmetic functions. The first result of this was the celebrated Erdős–Kac theorem (Erdős and Kac, 1939, 1940). Consider any additive function f which is bounded on the primes. Put

$$A_N = \sum_{p \leqslant N} f(p)/p, \qquad B_N = \left(\sum_{p \leqslant N} f(p)^2/p \right)^{1/2}.$$

If $B_N \to \infty$, then we have

$$\frac{1}{N} \# \{ n \leqslant N \colon f(n) - A_N < u B_N \} \to \Phi(u), \tag{7.2}$$

which reduces to (7.1) in the case $f(n) = \omega(n)$.

The systematic exploration of connections to probability was done by Kubilius in a series of papers in the fifties, which he summarized in his monograph (1959, 1964). The term "probabilistic number theory" is likely also his invention. Among others, (7.2) can be further extended to a full analog of the central limit theorem involving Lindeberg's condition. For details we refer the reader to Elliott's books (1979, 1980).

Perhaps the most important results of Erdős are given in his paper (1946). One result concerns the limiting distribution of additive functions with centering but without norming. Let f be an additive function such that for some constant λ we have

$$\sum_p \frac{\min(1, (f(p) - \lambda \log p)^2)}{p} < \infty. \tag{7.3}$$

Then with a suitable choice of the quantities A_N the frequencies

$$\frac{1}{N}\#\{n \leqslant N: f(n) - A_N < u\}$$

converge to a proper distribution function. A possible choice of A_N is

$$A_N = \lambda \log N + \sum_{p \leqslant N, \, |f(p) - \lambda \log p| \leqslant 1} \frac{f(p) - \lambda \log p}{p}.$$

It is stated as a conjecture that condition (7.3) is also necessary for the existence of such a centering.

Another result is the first (ineffective) *concentration estimate* for additive functions. Let f be an additive function and put

$$Q_N = \max_u \frac{1}{N}\#\{n \leqslant N: u \leqslant f(n) < u + 1\}.$$

Then $Q_N \to 0$ as $N \to \infty$, unless the series (7.3) converges for some λ. This obviously implies the above conjecture; strangely this connection was overlooked not only by Erdős himself, but by everyone else for the next 25 years. Thus, while de facto established by Erdős in 1946, the necessity of condition (7.3) for the existence of a limiting distribution with centering was first proclaimed by Elliott and Ryavec (1971) and Levin and Timofeev (1971). Elliott and Ryavec apply Erdős's concentration result, but rather than observing the immediate connection they find an indirect way (I could not check Levin and Timofeev for this point). Erdős himself did much to conceal the real nature of this result by the terminology. He writes (1946):

> THEOREM V. *Let the additive function be such that there exist two constants c_1 and c_2 and infinitely many n, so that there exists $a_1 < a_2 < \cdots < a_x \leqslant n$, $x > c_1 n$, $|f(a_i) - f(a_j)| < c_2$. Then there exists a constant c such that if we write*
>
> $$f^+(p) = f(p) - c \log p,$$
>
> $\sum_p (f^+(p))^2/p$ *converges.*
>
> In other words, if for many integers the values of $f(m)$ are close together, then $f(m)$ is almost equal to $c \log m$. If $f(m)$ satisfies the conditions of Theorem V we shall say that it is *finitely distributed.*

Another result from this paper reads as follows. The ε-concentration

$$Q_N(\varepsilon) = \max_u \frac{1}{N}\#\{n \leqslant N: u \leqslant f(n) < u + \varepsilon\}$$

satisfies $Q_N(\varepsilon) \to 0$ as $\varepsilon \to 0$ and $N \to \infty$, unless

$$\sum_{f(p) \neq 0} 1/p < \infty.$$

If f happens to have a limiting distribution, this is equivalent to the continuity of the distribution function (this case was mentioned above). Erdős liked to state this result in the form that "The limiting distribution tries to be continuous even when it does not exist."

Erdős obtained his concentration estimates by extremely tricky elementary means. I would say the natural approach is via the analytic method of Halász (1975) (which is, of course, three decades later). One can have the following effective estimate for the concentration (Ruzsa, 1980). We have

$$Q_N \ll \max_{\lambda} \left(\lambda^2 + \sum_{p \leqslant N} p^{-1} \min(1, |f(p) - \lambda \log p|^2) \right)^{-1/2},$$

an analog of Kolmogorov and Rogozin's inequality (with the "proper" multiple of the logarithm first subtracted).

This result readily implies that the set $\{n: f(n) = a\}$ always has an asymptotic density. Erdős, Ruzsa, and Sárközy (1973) showed that for $a \neq 0$ this density is at most 1/2.

The previous result hints at the special place of $\log n$ among the additive functions. There are two further results Erdős (1946) in this direction, which since then have generated many responses. These results say that if f is an additive function, and is either monotonic or satisfies

$$f(n+1) - f(n) \to 0,$$

then it must be $c \log n$ for some constant c. We mention a few among the rich collection of generalizations and improvements.

Wirsing (1981) proved that if f is completely additive and $f(n+1) - f(n) = o(\log n)$, then f is a logarithm. Wirsing, Tang, and Shao (1996) proved that if $f(n+1) - f(n) \to 0 \pmod 1$, then $f(n) \equiv c \log n \pmod 1$ for all n with some c. This made it possible (via characters) to extend some of these results to groups. Let f be an additive function with values in a locally compact group. If $f(n+1) - f(n) \to 0$ (which means now the neutral element of the group), then f is the restriction of a continuous homomorphism of the multiplicative group of positive reals to the group (Mauclaire, 1994); for a narrower class of groups this was established earlier by Daróczy and Kátai (1986)).

Katalin Kovács (1986) proved that if f is an additive function with values in $\mathbb{R}^d$ and $|f(n)|$ is monotonic, then $f(n)=c\log n$ with suitable $c\in\mathbb{R}^d$. The interesting feature is that if we replace the finite dimensional space by an infinite dimensional Hilbert space, then the corresponding statement fails. A different kind of additive function with monotonic norm arises from $f(p_j)=e_j\sqrt{\log p_j}$, where p_j is the sequence of primes and the e_j are orthogonal unit vectors. Probably every example is a combination of the above two, but this has not been established.

Elliott (1985) devoted a monograph to these questions and their applications to representations of integers. He considers the more general expressions $f(an+b)-f(An+B)$; what is more important, he can treat the square mean rather than the maximum of these quantities and obtain effective results, while most previous work considered only a fixed function and $n\to\infty$. We quote Theorem 10.1. We have

$$\max_{x\leqslant w\leqslant x^c}\frac{1}{W}\sum_{n\leqslant w}|f(an+b)-f(An+B)|^2$$

$$\gg\min_{\lambda}\sum_{p^k\leqslant x,\ p\nmid D}p^{-k}\,|f(p^k)-\lambda\log p^k|^2,$$

where $D=aA\,|aB-Ab|$. To indicate what sort of representations can be obtained, we mention Theorem 18.1. Given a rational function $R(x)=\prod(x+a_i)^{b_i}$ with integers $a_i\geqslant 0$ and b_i, for any pair m_1, m_2 of positive integers we find positive integer $n_1, ..., n_r$ and $\varepsilon_1, ..., \varepsilon_r=\pm 1$ such that

$$m_1=\prod R(n_j)^{\varepsilon_j},\qquad m_2=\prod R(n_j+1)^{\varepsilon_j}.$$

8. *Individual Functions*

Erdős kept his interest in questions about concrete functions like the number of divisors, Euler's function, etc., throughout his career—and, indeed, the previous accounts indicate that his interest in general additive functions arose from these concrete examples. In Erdős (1935f) we find the following results. (Here $\omega(n)$ is the number of prime divisors of n, $\tau(n)$ is the number of all divisors, and $\phi(n)$ is Euler's function, the number of reduced residue classes modulo n.)

(a) $\omega(p-1)\sim\log\log p$ for almost all primes p.

(b) $\sum_{p<x}\tau(p-1)\gg x(\log x)^{\log 2-1-\varepsilon}$.

(c) The number of integers up to x that occur as values of Euler's ϕ function is $\ll x(\log x)^{-1+\varepsilon}$ but it is $\gg x\log\log\log x/\log x$. After improvements by Erdős, Hall, and Pomerance, it was proved by Maier and Pomerance (1988) that this number is

$$\frac{x}{\log x}\exp((c+o(1))(\log_3 x)^2)$$

with a certain positive constant c.

(d) There are integers n that are assumed by $\phi(m)$ for $\gg n^c$ values of m with suitable $c>0$.

Number of prime factors. From the Erdős–Kac theorem we know that the integers have about $\log\log n$ prime factors; more exactly, the integers are normally distributed around that value with standard deviation $\sqrt{\log\log n}$. What happens if we take only the primes between u and v? As soon as $\log\log v - \log\log u \to \infty$ (say, as functions of x, when we consider the integers $n \leqslant x$), most numbers will have about $\log\log v - \log\log u$ prime divisors in (u, v). What happens if u, v may also vary with n? Erdős (1969a) gave a precise answer to this question. Let $\omega(n; u, v)$ be the number of prime factors of n satisfying $u < p \leqslant v$. If $u = u(n)$, $v = v(n)$ and

$$\frac{\log\log v - \log\log u}{\log\log\log n} \to \infty,$$

then for almost all n we have

$$\frac{\omega(n; u, v)}{\log\log v - \log\log u} \to 1.$$

If the limit is c rather than ∞, then this will no longer be valid.

Euler's function. Erdős (1958b) shows that if there is a number n such that the number of solutions of the equation $\phi(x) = n$ is exactly k, then there are infinitely many such numbers. It is a still undecided conjecture of Carmichael that there is no such number for $k = 1$. Recently K. Ford proved that there are such values for any $k \geqslant 2$ (unpublished), which was conjectured by Sierpinski.

Everyone knows that $\phi(n)/n$ can be arbitrarily small; and it is not too difficult to see that k consecutive values also can be simultaneously small. Erdős (1956a) describes the exact extent of this phenomenon. Put $L_n = [\log_3 n/\log_4 n]$. Then

$$\liminf \frac{\phi(n)+\phi(n+1)+\cdots+\phi(n+L_n)}{n} = 0,$$

but for every $\varepsilon > 0$ we have

$$\lim \frac{\phi(n) + \phi(n+1) + \cdots + \phi(n + [(1+\varepsilon)\, L_n])}{n} = \infty,$$

The transition at the threshold proceeds as

$$\liminf \frac{\phi(n) + \phi(n+1) + \cdots + \phi\left(n + \left[\dfrac{\log_3 n}{\log_4 n - \log_5 n} + c\, \dfrac{\log_3 n}{(\log_4 n)^2}\right]\right)}{n} = e^c/\alpha,$$

where

$$\alpha = \prod_p \left(1 - \frac{1}{p}\right)^{-1/p}.$$

It is a classical fact that

$$\Phi(x) = \sum_{n \leqslant x} \phi(n) = \frac{3}{\pi^2} x^2 + O(x \log x).$$

Saltykov and Walfisz improved the error term to $x(\log x)^{2/3+\varepsilon})$, while Chowla and Pillai showed that it is $\neq O(x \log_3 x)$. Erdős and Shapiro (1951) proved that it changes sign infinitely often, and it is $\Omega_{\pm}(x \log_4 x)$. Montgomery (1987) improved this to $\Omega_{\pm}(x \sqrt{\log \log x})$. For an account of the method and further developments see Adhikari (1998).

Erdős and Shapiro (1955) consider the related function

$$H(x) = \sum_{n \leqslant x} \frac{\phi(n)}{n} - \frac{6}{\pi^2} x,$$

and prove that it has a continuous limiting distribution.

The average of $\phi(n)/n$ is $6/\pi^2$, with a continuous limiting distribution which is nowhere constant on $[0, 1]$. If we iterate Euler's function, we get a rather different picture (Erdős, 1961a). Write $\phi_k(n) = \phi(\phi(\cdots(n)\cdots))$. Then for $k \geqslant 2$ we have for almost all n

$$\frac{\phi_k(n)}{\phi_{k-1}(n)} \sim \frac{1}{e^\gamma \log_3 n}.$$

The number of integers $n \leqslant x$ such that $(n, \phi(n)) = 1$ is asymptotically $e^{-\gamma} x/\log_3 x$, with γ denoting the Euler–Mascheroni constant (Erdős, 1948d).

The most famous property of Euler's function is the congruence $a^{\phi(n)} \equiv 1 \pmod{n}$ for $(a, n) = 1$. For most values of n it is not the smallest such number; the smallest number with this property is given by

$$\lambda(n) = \text{lcm}[\phi^*(p^k) \colon p^k \,\|\, n],$$

where $\phi^*(p^k) = \phi(p^k)$ except for $p = 2$, $k \geqslant 3$ when it is $\phi(p^k)/2$. This function is called Carmichael's lambda function. Erdős, Pomerance, and Schmutz (1991) show that its behaviour is rather different from that of ϕ. Its minimal value is around $(\log n)^{c \log_3 n}$, and its average satisfies

$$\sum_{n \leqslant x} \lambda(n) = \frac{x^2}{\log x} \exp \frac{(c + o(1)) \log_2 x}{\log_3 x}$$

with a suitable positive constant c.

Sum of divisors. $\sigma(n)$ denotes the sum of divisors of n.

The maximal possible order of $\sigma(n)/n = \sum_{d \mid n} 1/d$ is $\log \log n$. If we consider only the numbers $n = 2^k - 1$, we have $\sigma(n)/n \ll \log \log k (\sim \log_3 n)$, which is best possible (1971). Erdős, Kiss, and Pomerace (1991) extend this as follows. Write $f(k) = \sigma(2^k - 1)/(2^k - 1)$ and $f_m(k) = \min(f(k), f(k+1), \ldots, f(k+m))$. For a fixed m the function f_m will remain unbounded, but it satisfies

$$f_m(k) \ll \log_{m+2}(k).$$

On the assumption of a certain generalized Riemann hypothesis this is best possible.

And the others. Erdős and Sárközy (1994) consider, for various functions f, the largest number G such that

$$f(n) > \sum_{0 < |i| \leqslant G} f(n+i)$$

is possible for some $n \leqslant x$. They show that for the function σ, G is asymptotic to $(3e^{\gamma}/\pi^2) \log \log x$, for ω it is between $\log x (\log_2 x)^{-2}$ and $\log x (\log_2 x \log_3 x)^{-1}$. In the same paper we find the following striking question. Is it true that

$$\max_{n \leqslant x} (\omega(n) + \omega(n-1)) - \max_{n \leqslant x} \omega(n) \to \infty?$$

Erdős and Szekeres (1934) consider the function $f_i(n)$, which counts the number or representations of n as a product (of an arbitrary number of terms, order ignored) of factors of the form p^j, $j \geqslant i$. In particular, $f_1(n)$ is the number of Abelian groups of order n. They show that

$$\sum_{n \leqslant x} f_i(n) = A_i n^{1/i} + O(n^{1/(i+1)}), \qquad A_i = \prod_{k=1}^{i} \zeta(1+k+i).$$

IV. ADDITIVE PROBLEMS

9. *Classical Additive Theory*

Classical number theory studies the representations of integers as sums from a nice set, the principal examples being the primes (Goldbach) and the kth powers (Waring). Out of this, notably from Schnirelmann's approach to the Goldbach problem, grew a new branch in the thirties, combinatorial number theory. Erdős was a central figure in this from the onset, as we shall soon see. He devoted less attention to the classical part; still, there are a few results worth mentioning.

In connection with Waring's problem one often needs an upper bound for the number of solutions of the equation

$$x_1^k + \cdots + x_s^k = y_1^k + \cdots + y_s^k. \tag{9.1}$$

Davenport and Erdős (1939) call a sequence $\lambda_1 \geqslant \cdots \geqslant \lambda_s$ of positive numbers *admissible exponents* for k if the number of solutions of (9.1) under the restriction $P^{\lambda_i} < x_i,\ y_i < 2P^{\lambda_1}$ is $O(P^{\lambda_1 + \cdots + \lambda_s + o(1)})$ (roughly the number of trivial solutions). They find the following collections of admissible exponents: $1, \lambda, \lambda\vartheta, ..., \lambda\vartheta^{s-2}$, where $\vartheta = 1 - 1/k$ and λ is any number satisfying $k\lambda - (k-1) \leqslant \lambda\vartheta^{s-2}$; and the numbers 1, $1 - k^{-2}$, $1 - k^{-1} - k^{-2}$ in the case $s = 3$. The latter was recently extended by Thanigasalam (1994).

Erdős and Mahler (1938) proved that for any binary form $F(x, y)$ of degree $k \neq 3$, the number of integers $\leqslant N$ assumed by F is $\gg N^{2/k}$. Erdős (1939c) found an elementary proof for the particularly interesting case of the form $x^k + y^k$.

Romanov proved that the integers of the form $2^k + p$, p prime, have a positive lower density, a remarkable feat since there are "just enough" sums for that, and he asked whether every sufficiently large odd number is of this form. Erdős (1950) proved that this is not the case, they miss complete arithmetic progressions. Crocker proved (1971) that there are infinitely many odd numbers not representable as a sum of a prime and two powers of two.

How do you prove that $n \neq 2^k + p$? This means that no $n - 2^k$ can be prime, and a way to guarantee that is that it is always divisible by at least one of certain primes $q_1, ..., q_m$. The divisibility $q \mid n - 2^k$ kills a residue class modulo $o(q)$, the order of 2 modulo q (which we can choose by fixing the residue of n modulo q). Thus if we can find a collection of primes $q_1, ..., q_m$ and numbers $a_1, ..., a_m$ so that every integer satisfies at least one of the congruences

$$n \equiv a_i \pmod{o(q_i)},$$

then we are done. Erdős found such a covering system, and this gave him the occasion to ask many questions about covering systems. The favourite two are: Is there a covering system of congruences with distinct odd moduli? Is there one with arbitrary large distinct moduli?

With $r(n)$ denoting the number of solutions of $n = 2^k + p$, Romanov based his theorem on the assertion that $r(n)$ is bounded in the square mean. Erdős (1950) proved that it is bounded in every sth mean, that is,

$$\sum_{n \leqslant N} r(n)^s = O(N),$$

but it is not bounded everywhere, even

$$\limsup \frac{r(n)}{\log \log n} > 0.$$

As a dessert, he shows how the powers of 2 can be replaced by a general sequence satisfying $a_i \mid a_{i+1}$.

10. *Bases*

We say that a set $\mathscr{B}$ of integers is a *basis* of order k if every positive integer can be expressed as a sum of at most k elements of $\mathscr{B}$ (sometimes one requires exactly k summands, which makes no difference if we include 0 in $\mathscr{B}$); it is an *asymptotic basis* of order k, if every sufficiently large integer has such a representation. Goldbach's conjecture asserts that the set of primes and 1 is a basis of order 3. As a first unconditional result toward this conjecture, Schnirelmann proved that this set is at least indeed a basis of some order. An important tool for achieving this goal was his concept of density (Schnirelmann density)

$$\sigma(\mathscr{B}) = \inf_{n \in \mathbb{N}} B(n)/n,$$

where $B(n)$ is the number of elements of $\mathcal{B} \cap [1, n]$ (and in the sequel we use the same convention for other letters of the alphabet).

Schnirelmann himself proved the inequality

$$\sigma(\mathcal{A} + \mathcal{B}) \geqslant \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\, \sigma(\mathcal{B}), \tag{10.1}$$

provided $0 \in \mathcal{A} \cup \mathcal{B}$. (Under the stronger condition that $0 \in \mathcal{A} \cap \mathcal{B}$, Mann improved (10.1) to

$$\sigma(\mathcal{A} + \mathcal{B}) \geqslant \min(1, \sigma(\mathcal{A}) + \sigma(\mathcal{B})),$$

which is best possible. About the possibility of improving (10.1) under the weaker condition, see Hegedűs, Piroska, Ruzsa (1998).) The next question was: Is there a similar inequality for at least *some* sets of density 0? Such an inequality was first found by Khinchin, for the case when $\mathcal{B}$ is the set of squares, with an analytic (and specific) proof. Erdős (1936a, b) found the following result, which was sensational because of both its generality and the simplicity of the proof: whenever $\mathcal{B}$ is a basis of order k and $0 \in \mathcal{B}$, we have

$$\sigma(\mathcal{A} + \mathcal{B}) \geqslant \sigma(\mathcal{A}) + \frac{1}{2k}\, \sigma(\mathcal{A})(1 - \sigma(\mathcal{A})). \tag{10.2}$$

(There is a similar inequality for asymptotic density.) Plünnecke (1970) improved (10.2) to

$$\sigma(\mathcal{A} + \mathcal{B}) \geqslant \sigma(\mathcal{A})^{1 - 1/k}, \tag{10.3}$$

which is better for every value of $\sigma(\mathcal{A})$ and much better for small values. He also determined the order of magnitude for the case of squares (the exponent 3/4, which follows from (10.3) and Legendre's theorem, can be improved to 1/2, (Plünnecke, (1957)). It can be observed, however, that while $\mathcal{A} + \mathcal{B}$ is the union of all the translates $\mathcal{A} + b$, $b \in \mathcal{B}$, to estimate the number of elements of the sumset up to a limit Erdős uses only the union of *two* such sets, and for this quantity (10.2) is essentially optimal. Let $f(\alpha)$ denote, for $0 < \alpha < 1$, the maximal number with the following property: if $\sigma(\mathcal{A}) = \alpha$, then for every n there is an integer k such that the set $\mathcal{A} \cup (k + \mathcal{A})$ contains $\geqslant (\alpha + f(\alpha))\, n$ elements. In the course of the proof of (10.2) it is shown that $f(\alpha) \geqslant \alpha(1 - \alpha)/2$, and in Erdős (1961b) this is complemented by $f(\alpha) \leqslant \alpha(1 - \alpha)$, which is achieved by considering a random set.

Take a set $\mathcal{A}$, which is a basis of order two. This means that $r(n)$, the number of representations of $n = a + a'$ with $a, a' \in \mathcal{A}$, must satisfy $r(n) \geqslant 1$.

It is not difficult to construct bases (say, via considering odd and even places in the binary decomposition of integers) for which $r(n)$ is bounded on the average (which is just another way of saying that the number of elements in the basis up to N is $O(\sqrt{N})$). In these examples, however, the maximal size of $r(n)$ is as high as N^c. Is there a basis for which $r(n)$ stays bounded? Erdős and Turán (1941) conjectured it cannot. Erdős (1954b) proved the existence of a basis for which $r(n) = O(\log n)$, more exactly,

$$c_1 \log n < r(n) < c_2 \log n$$

for all n with certain positive constants c_1, c_2. This is done by a random construction; if we make a set by deciding over each natural number n independently, so that

$$\mathbf{P}(n \in \mathscr{A}) = c \sqrt{\frac{\log n}{n}},$$

then we get such a set with positive probability for large enough c.

I proved (Ruzsa, 1990) that $r(n)$ can be bounded in the square mean.

It is interesting to remark that the multiplicative analog of the boundedness problem can be solved. Let $\mathscr{B}$ be a set of integers, and let $g(n)$ denote the number of representations of n in the form $n = bb'$, $b, b' \in \mathscr{B}$. If $g(n) > 0$ for all $n > n_0$, then g is unbounded; even $g(n) > (\log n)^c$ occurs infinitely often with some $c > 0$. On the other hand, again by a random construction, $g(n) \ll (\log n)^C$ is possible (Erdős, 1964b). For an extension to products of more than two factors see Nešetřil and Rödl (1985).

Another aspect of regularity is monotonicity; Erdős, Sárközy, and Sós (1987) study how near $r(n)$ can get to being monotonic.

How regular can $r(n)$ be on the average; in other words, how well can the function

$$R(x) = \sum_{n \leqslant x} r(n) = \#\{(a, a') : a, a' \in A, a + a' \leqslant x\}$$

behave? (Here we do not suppose that $r(n) \geqslant 1$ always.) If for A we take the squares (with proper multiplicities), we arrive at the classical circle problem; it is generally believed that

$$R(x) = \pi x + O(x^{1/4 + \varepsilon}),$$

though the best known exponent is just a bit below 1/3. Hardy and Littlewood showed that the 1/4, if true, is best possible (for the squares).

Erdős and Fuchs (1956) proved that this is, rather than a property of the squares, a universal phenomenon:

$$R(x) = cx + o(x^{1/4}(\log x)^{-1/2})$$

is impossible for *any* set A with $c > 0$. Jurkat (unpublished), and later Montgomery and Vaughan (1990) removed the power of logarithm. On the other hand,

$$R(x) = cx + O(x^{1/4} \log x)$$

already can occur for a suitable sequence (Ruzsa, 1997). This is a random construction, and it seems difficult to construct a concrete example.

Erdős and Graham (1980) show that if we omit an element from an asymptotic basis, then, with possibly a finite number of exceptions, the new set will be an asymptotic basis as well. If the original set had order h, the order of the smaller set can be estimated as $O(h^2)$; see Deleglise (1991) and Nash (1993).

11. *Sidon Sets*

Take a set $\mathscr{A} = \{a_1, ..., a_n\}$ of integers and write

$$f(t) = \sum e(a_j t).$$

No matter what these integers are, we always have $\int |f(t)|^2 \, dt = n$, while

$$2n^2 - n \leqslant \int |f(t)|^4 \, dt \leqslant \frac{n(2n^2+1)}{3}.$$

The upper bound is attained for arithmetic progressions, the lower bound whenever all the sums of pairs are distinct (so there is the maximal possible number $n(n+1)/2$ of them), or equivalently, all the differences are distinct, which makes $n(n-1)+1$. These sets were called B_2 sets by Sidon (1932), and generally bear his name today. A B_h set is required to have distinct sums of h terms, which is again related to the minimality of $\int |f(t)|^{2h}$.

Sidon asked how many elements such a set can have in the interval $[1, x]$. Erdős and Turán (1941) proved that this amount is $\leqslant \sqrt{x} + O(x^{1/4})$, which is still the best result, save the coefficient of $x^{1/4}$ (Lindström (1969) found the value 1, still the record; as R. Freud observed, even this could be obtained by the Erdős–Turán method with a careful calculation), but it is $> (1/\sqrt{2} - o(1)) \sqrt{x}$. The lower bound has been improved to $\sqrt{x} - x^c$, where the value of c depends on our actual knowledge of gaps between primes, so at present we can take $c = 11/40 + \varepsilon$. Somehow all known constructions of dense Sidon sets involve the primes. They are based on constructions of Sidon sets modulo m for certain values of m, that is, sets of residues such that $x+y \equiv u+v \pmod m$ can only hold trivially among elements of the set. The known constructions are $p+1$ residues modulo p^2+p+1 (Singer, 1938), p residues modulo p^2-1 (Bose, 1942), where p is a power of a prime, and $p-1$ residues modulo $p(p-1)$, where p is a prime (Ruzsa, 1993). Singer and Bose were not interested in Sidon sets; the relationship between their constructions and Sidon sets was observed by Erdős (1944) and Chowla (1944). (Proofs of these results and further information can be found in Halberstam and Roth (1966/1983).)

Erdős conjectured that the size of the maximal Sidon set in $[1, N]$ is $\sqrt{N}+O(1)$. Some numerical evidence against this was offered by Zhang (1994).

Erdős (1968/1969) considers the multiplicative analog: How many integers can one select from $[1, x]$ so that all pairwise products are distinct? The primes have this property, even the stronger one that products of any number of factors are distinct. Still, the answer is here between $\pi(x)+c_1 x^{3/4}/(\log x)^{3/2}$ and $\pi(x)+c_2 x^{3/4}/(\log x)^{3/2}$ with certain positive constants c_1, c_2.

Infinite Sidon sets are more problematic. Already in their 1941 paper Erdős and Turán write ($\phi(x)$ below is the number of elements up to x):

> It is easy to see that, for every *infinite* B_2 sequence, $\underline{\lim}\ \phi(n)/\sqrt{n}=0$. On the other hand, it is not difficult to give an example of a B_2 sequence with $\overline{\lim}\ \phi(n)/\sqrt{n}>0$.

Their proof of the first claim appeared in Stöhr (1955), in the stronger form

$$\liminf \frac{A(x)\sqrt{\log x}}{\sqrt{x}} < \infty.$$

Concerning the second, Krückeberg (1961) proved it with $1/\sqrt{2}$, and Erdős conjectures that it could be $1-\varepsilon$.

It is more difficult to construct an infinite Sidon set for which $A(x)$ is always large. Chowla and Mian (1944) considered the greedy algorithm: we start with 1, and we always include the smallest positive integer which does not spoil the Sidon property. It is easy to see that this satisfies $A(x) \geqslant x^{1/3}$. Erdős (I cannot imagine why) conjectured that there should be a Sidon set with $A(x) \gg x^{1/2-\varepsilon}$. He and Rényi (1960) proved the existence, for every fixed positive ε, of a set such that $A(x) \gg x^{1/2-\varepsilon}$ and the number of representations $n=a+a'$, $a, a' \in A$ is bounded, the bound depending on ε. For Sidon sets, the trivial bound $x^{1/3}$ was improved to $(x \log x)^{1/3}$ by Ajtai, Komlós, and Szemerédi (1981), and recently to $x^{1/\sqrt{2}-o(1)}$ by me (1998).

As a generalization of the above result, Erdős conjectured that any infinite B_h set $\mathscr{A}$ satisfies

$$\liminf A(n)\, n^{-1/h} = 0.$$

This was proved for $h = 4$ by Nash (1989) and for general even h by Jia (1994) and Helm (1993). Improving a result of Chen, Helm (1994) found the estimate

$$\liminf A(n)\, n^{-1/h} (\log n)^{1/(3h/2-1)} < \infty.$$

Curiously nothing is known for odd values of h.

Erdős, Sárközy, and Sós (1995) studied the longest interval that can be contained in $A + A$, where $A \subset [1, N]$ is a Sidon set. They proved that its length $h(N)$ satisfies $N^{1/3} \ll h(N) \ll N^{1/2}$. Ruzsa (1996c) proved that the upper bound gives the correct order of magnitude.

12. *Random Sets*

This paper is organized around different subjects, and "random sets" means a perspective or a method rather than a topic. Random sets can be investigated from many aspects, some of which were discussed above, and some results were claimed to be found by a "random method." Random sets are often not investigated for their own sake, but with the aim that they provide the key to an existence problem where attempts at construction fail.

This is frequently called a "random construction," a phrase the meaning of which is somewhat obscure. One can debate whether such a proof is a construction or only a proof of existence. A proof of existence often immediately leads to an algorithm for finding the desired object (by trial and error), typically a very slow one. In connection with the basis with $r(n) \asymp \log n$ (see Section 10), Kolountzakis (1994) gives an algorithm, based on Erdős' proof, that constructs the first n elements in polynomial time. Such a "derandomization" is likely to be possible for many applications of the random method.

Erdős did not invent the random construction, but he applied it masterfully and became perhaps its chief popularizer.

Given a set $\mathscr{A}$, we can ask for another set $\mathscr{B}$, possibly thin, with the property that $\mathscr{A} + \mathscr{B}$ contains all but finitely many integers. Such a set is called an *additive complement* of $\mathscr{A}$. A general result on the existence of thin additive complements was proved by Lorentz (1954). This applies nothing more than a lower estimate for the counting function of $\mathscr{A}$, and an application to the primes, or to any set with $\gg x/\log x$ elements up to x, yields the existence of a complement $\mathscr{B}$ with $B(x) \ll (\log x)^3$. Erdős

(1954a) proved that this can be improved to $(\log x)^2$; this applies the further property of primes that

$$\pi(x+y)-\pi(x)\sim\frac{y}{\log x} \tag{12.1}$$

holds for a range $x^c\leqslant y\leqslant x$ with a certain $c<1$.

Lorentz' and Erdős' proofs both apply the "random construction" in its simplest form, which can be described as a counting argument (Lorentz' even as a greedy algorithm).

Recently Dufner and Wolke (1994) applied these ideas to the construction of a thin set $\mathscr{P}'$ of *primes*, having $\ll(\log x)^2$ elements up to x, such that all but $O(x(\log x)^{-C})$ even integers up to x are of the form $p+p'$, with both p, p' primes and $p'\in\mathscr{P}'$. Wolke (1996) found that by allowing more, but still $o(x)$, exceptions, $\mathscr{P}'$ can be made even thinner.

Erdős (1954a) also proved that with only a lower estimate for the counting function (that is, without further properties like (12.1)), Lorentz' estimates are best possible up to a constant factor. Rather than the primes, this concerns sets of positive density. Lorentz' theorem implies that when $\mathscr{A}$ has positive lower density, we can find a complement $\mathscr{B}$ with $B(x)\ll(\log x)^2$, and Erdős shows that this cannot be improved.

This is also done by a probabilistic method, and here a reduction to counting seems to be (at the least) difficult.

In the first step, we consider a random set $\mathscr{A}_0$, constructed so that the positive integers are selected into it independently, with probability $\mathbf{P}(n\in\mathscr{A}_0)=1/2$. By the law of large numbers the counting function of this set satisfies, with probability 1, $A_0(x)\sim x/2$.

Next, we try to estimate the probability of existence, for a fixed x, of a set $\mathscr{B}\subset[1,x]$, $|\mathscr{B}|<\alpha\log x$, such that $\mathscr{A}_0+\mathscr{B}$ contains all integers in $[x/2,x]$. This can be done by estimating for each $\mathscr{B}$ separately and summing, though these events are far from disjoint. For a given $\mathscr{B}$ this estimation is still not obvious. The event "$\mathscr{A}_0+\mathscr{B}$ contains every $x/2\leqslant n\leqslant x$" is the intersection of these individual events for each n. These are not independent, and it seems (to me) impossible to calculate the degree of dependence even by new tools like Janson's inequality. Erdős cut through the knot by selecting an independent subset; seemingly a loss, since from the $x/2$ events only $x/(\log x)^2$ remain, but the final result is miraculously not affected.

The proof is completed by applying the above argument for a sequence like $x_j=10^j$, and trimming $\mathscr{A}_0$ into, say,

$$\mathscr{A}=\mathscr{A}_0\cap\left(\bigcup[10^j,2\cdot10^j]\right)$$

so that the sets $\mathscr{B}$ corresponding to $x=x_j$ could not interfere.

This method can easily be adapted to different situations. Kolountzakis (1996) proved that for a simple random model of primes $(\log x)^2$ is the actual size of a minimal additive completion; thus if there is a thinner complement for the primes (which Erdős believed to be the case), this must be based on properties in addition to (12.1).

Erdős and Rényi devoted two papers (1960, 1970) to the study of random sets. In the first they consider, among others things, how the number of sums changes if we replace the squares by a random set of comparable counting function. They show that with probability one, the set of sums of pairs will have positive density, so that the squares are atypical. In fact, they find the density of this set, together with the density of numbers having exactly k representations, an analog of the law of iterated logarithms and much more. It is worth mentioning that Atkin (1965) found a sequence that is even more square-like, namely $a_k = k^2 + O(\log k)$; still, the set of sums has positive density.

Another result, on dense sets with a bounded number of additive representations, was mentioned in the previous section. In the second paper they find a set $\mathscr{A}$ of density α (a random set, of course) with the property that for any finite $\mathscr{B}$ of k elements $\mathscr{A} + \mathscr{B}$ has density $1-(1-\alpha)^k$, which is the smallest possible value for *any* set, and thus random sets are again extremal.

Erdős and Ulam (1971) consider the possibility of solving the equation $a_1 + a_2 = a_3$ in a random set $\mathscr{A}$ whose counting function satisfies $A(x) \sim x^\alpha$. If $\alpha \geqslant 1/3$, then, with probability 1, this equation has infinitely many solutions, while for $\alpha < 1/3$ it has only finitely many. Thus, the case $k=3$ of Fermat's last theorem is surprising, while the cases $k \geqslant 4$ could be expected.

A set $\mathscr{V}$ is an *essential component*, if for every set $\mathscr{A}$ with $0 < \sigma(\mathscr{A}) < 1$ we have $\sigma(\mathscr{A} + \mathscr{V}) > \sigma(\mathscr{A})$ (or an analogous requirement with asymptotic density). A consequence of Erdős' inequality (11.2) is that every basis is an essential component. The converse is not true. In Halberstam and Roth (1966, p. 35) we read the following.

> Linnik constructed an essential component $\mathscr{V}$ which is exceedingly thin; so thin, indeed, that it satisfies $V(n) = O(n^\varepsilon)$ for every ε and thus could not (on trivial combinatorial grounds) be a basis. Linnik's highly ingenious method is based on the use of exponential sums....
>
> Erdős and Roth have recently (unpublished) found that, by the use of probability methods, it is possible to prove the existence of a sequence of the required kind, without the use of any deep result (other than the central limit theorem), and that Linnik's method can be much simplified in this way.

The above lines were written before 1966, when the book appeared. This proof was never published—even Erdős' thousand papers do not include everything he did. When I picked up this idea a quarter of a century later, I found that it not only yields a simpler proof of Linnik's result, but leads to a complete answer about the possible size of essential components: for every fixed $\varepsilon > 0$ we can find an essential component with $V(x) = O((\log x)^{1+\varepsilon})$, but $V(x) = O((\log x)^{1+o(1)})$ is impossible (Ruzsa, 1987). The simplest set with a chance to be an essential component is the collection of numbers in the form $2^m 3^n$, and Erdős often asked whether it is an essential component or not; I do not even have a plausible guess.

13. *Further Additive–Combinatorial Questions*

Arithmetical progressions. Erdős and Turán (1936) ask how many integers we can select from the first N so that there are no three in an arithmetical progression (equivalently, the equation $x + y = 2z$ is not solvable in the set). They denote this number by $r(N)$, and use $r_k(N)$ for the corresponding quantity defined with arithmetic progressions of length k.

This paper had an enormous impact, despite its containing almost no results (only the easy $r(N) < (4/9 + \varepsilon) N$), and led (four decades later) to Erdős' paying \$1000 to Szemerédi for the proof that $r_k(N) = o(N)$ for all k (Szemerédi, 1975). Van der Waerden's celebrated theorem (a decade earlier) told us that in any partition of the integers into finitely many classes at least one class contains arbitrary long arithmetical progressions. $r_k(N) = o(N)$ obviously implies this; the general connection between these two types of results is still not completely clarified.

This paper also states the conjecture, attributed to Szekeres, that $r((3^k + 1)/2) = 2^k$, which would mean that $r(N) \asymp N^{\log 2/\log 3}$. Here the example comes from the integers which contain only the digits 0, 1 in their development in base 3. It is somewhat surprising that the authors did not observe that minimal changes give more elements; say, by taking integers with only 0, 1, 2 in the base 5 development and fixing the number of 1's we can have

$$\binom{k}{l} 2^{k-l}$$

integers up to $(5^k + 1)/2$. The optimal choice $l = [k/3]$ increases the exponent to $(\log 3)/\log 5 - \varepsilon$, and leads directly to further improvements. This was done by Salem and Spencer (1942) and was further improved by Behrend (1946) to

$$r(N) > N e^{-c\sqrt{\log N}},$$

which is still the record, save the value of c. In the other direction, Roth (1953) proved $r(N) = o(N)$. His method was improved by Heath-Brown

(1987) and Szemerédi (1990) to $N/(\log N)^c$; my calculations indicate that the best value of c that can be obtained by their method is between 0.3 and 1/3.

The first upper estimate for $k=4$ was obtained recently by Gowers (1998) (of type $r_4(N) \ll N(\log\log N)^{-c}$). He also announced estimates for larger k.

Erdős and Spencer (1995) consider the following problem. How many numbers need we take from $\{1, ..., n\}$ so that it necessarily contains a k term arithmetical progression of the special form $\{x, 2x, ..., kx\}$? The answer is $d_k n + o(n)$ with a certain constant $d_k \in (0, 1)$, and as $k \to \infty$ we have

$$1 - d_k \asymp \frac{1}{k \log k}.$$

Erdős, Ginsburg, and Ziv. Erdős, Ginsburg, and Ziv (1961) proved that from a collection of $2n-1$ integers we can select n, whose sum is a multiple of n (this bound is easily seen to be exact). See Alon and Dubiner (1993) for an anthology of proofs. Alon and Dubiner (1995) estimate the least number $f(n, d)$ with the property that among f d-dimensional vectors we can always find n in whose sum all coordinates are divisible by n; they show $f(n, d) \leqslant c_d n$. Mann (1967) and Gao (1996) find conditions for the subsums to represent every residue.

Erdős and Heilbronn. If $\mathscr{A}, \mathscr{B}$ are finite sets of integers, say $|\mathscr{A}| = m$, $|\mathscr{B}| = n$, it is an easy exercise to show that

$$|\mathscr{A} + \mathscr{B}| \geqslant m + n - 1.$$

The extension to sets of residues modulo a prime p is the familiar Cauchy–Davenport theorem (the right side must be replaced by $\min(p, m+n-1)$). Now what happens if we are allowed to count only the numbers represented as $a+b$ with $a \neq b$? Erdős and Heilbronn (1964) formulated the conjecture that, in the case $\mathscr{A} = \mathscr{B}$, we get at least $\min(p, 2m-3)$ residues. The analogous quesion for integers also is easy; but this simple piece proved surprisingly hard, and was finally proved by Dias da Silva and Hamidoune (1994). (See Alon, Nathanson, and Ruzsa (1995) for a simpler proof and generalizations.)

V. MISCELLANEOUS

14. *Consecutive Integers, Binomial Coefficients*

Products of consecutive integers and binomial coefficients are clearly closely related. Erdős (1939a, b) started early to work on the question, "When will these be perfect powers?" In the first case he conjectured the answer to be "never." After much sweat and toil, this was completed by Erdős and Selfridge (1975).

Erdős (1939b, 1951) asked whether a binomial coefficient $\binom{n}{k}$, $n \geqslant 2k$, can be a perfect power, say $=x^l$, and proved that for $k \geqslant 4$ it cannot. (The case $l=3$ was solved previously by Niven, $l=4, 5$ by Obláth.) The remaining cases, $k=2, 3$, needed much work. (For $k=l=2$ the problem reduces to a Pell equation with infinitely many solutions.) Based mainly on the work of R. Tijdeman, H. Darmon, L. Merel, and N. Terai, the last step was done by Győry (1997); the interested reader is referred to this work for further details and history. The only solution with $k>2$ is $\binom{50}{3}=140^2$.

Erdős and Graham (1980, p. 71) conjectured that $\binom{2n}{n}$ is never squarefree for $n>4$. This was proved for large n by Sárközy (1985) and for all n by Velammal (1995) and by Granville and Ramaré (1996). Sander (1995) proved that the maximal exponent $E(n)$ of a prime in $\binom{2n}{n}$ satisfies

$$E(n) \gg (\log n)^{1/10-\varepsilon}.$$

Among a consecutive integers there is exactly one multiple of a. The reader may spend a few minutes to prove that for $a<b$, from b consecutive integers we can select two whose product is a multiple of ab. What happens if we take more? Define $f(n)$ as the smallest positive number with the following property: for any collection $1<a_1<\cdots<a_n$ of n integers, in any interval of length $f(n)\,a_n$ we can find n integers whose product is a multiple of $a_1 \cdots a_n$; so $f(1)=f(2)=1$. Erdős and Surányi (1959), prompted by a question of Gallai, show that $f(3)=\sqrt{2}$ and that

$$(\log n)^{\alpha} \ll f(n) \ll \sqrt{n}$$

with some positive α.

15. *Uniform Distribution, Discrepancy*

A sequence x_j of real numbers is *uniformly distributed* modulo one if we have

$$\frac{1}{N}\,\#\{j \leqslant N : u \leqslant \{x_j\} < v\} \to v-u$$

as $n \to \infty$, for all $0 \leqslant u \leqslant v \leqslant 1$. By a famous criterion of Weyl, this is equivalent to

$$\frac{1}{N}\sum_{j \leqslant N} e^{2\pi i k x_j} \to 0$$

for every integer $k \neq 0$. Erdős and Turán (1948a, b) gave an effective version of this result as follows. We define the *discrepancy* Δ of a (finite) sequence $x_1, ..., x_N$ by

$$\Delta = \sup_{1 \leqslant u \leqslant v < 1} \left| \frac{1}{N} \# \{ 1 \leqslant j \leqslant N : u \leqslant \{x_j\} < v \} - (v - u) \right|, \qquad (15.1)$$

where $\{x\}$ denotes the fractional part of x. (Some authors use this term for the quantity $N\Delta$.) Put

$$\alpha_k = \frac{1}{N} \sum e^{2\pi i k x_j}, \qquad (15.2)$$

the *Fourier coefficients* of this sequence. Then we have

$$\Delta \ll B = \min_k \left(\frac{1}{k} + \sum_{j=1}^{k-1} \frac{|\alpha_j|}{j} \right). \qquad (15.3)$$

This is remarkable for several things. One is the masterful use of the Jackson mean in the proof (for more on this, including a new method of Vaaler, see Chapter 1 of Montgomery (1994)). Second is its close resemblance to the Berry–Esseen inequality; see Niederreiter and Philipp (1973). (This is another meeting point with probability theory, besides the theory of additive functions, which was not recognized as such at the time.) A third is its sharpness. “Probably our result is not very far from being best possible,” Erdős writes (in his reminiscences of Turán in Turán’s “Collected Papers,” 1990). I proved (Ruzsa, 1992) that it indeed is best possible, up to a constant factor, if we are allowed to use only an upper estimate for the Fourier coefficients.

This result found wide response in the literature. Koksma (1950) gave a generalization to several dimensions.

Erdős continues: “Turán and I obtained a very much stronger result on the error terms by using interpolatory properties—these papers are very little used and seem to have been forgotten. While the condition above is easy to check, i.e., it is easy to apply, our interpolatory conditions are very hard to verify and this is the reason why they almost never have been used.”

Discrepancy is not the only possible method for grasping the goodness of distribution. Let $a_1, a_2, ...$ be a sequence of reals; the first n elements divide the the unit interval modulo one into n arcs. Let M_n and m_n denote the length of the longest and the shortest of these, respectively. De Bruijn and Erdős (1949) calculate the largest possible value of $\liminf nm_n$, and the smallest possible values of $\limsup nM_n$ and $\limsup M_n/m_n$. The following sequence attains the extremal values in all. In the first step we have one point and one interval of length $1 = {}^2\log 2$. We split it into two intervals of lengths ${}^2\log 3/2$ and ${}^2\log 4/3$; in the next step we split ${}^2\log 3/2 = {}^2\log 6/4$ into ${}^2\log 5/4$ and ${}^2\log 6/5$, and so on.

16. *The Kitchen Sink*

"The kitchen sink" is the title Erdős and Spencer (1974) gave the last chapter of their book. This includes, under the subheading "A $300 problem," the question about the maximal number k of integers $0 < a_1 < \cdots < a_k \leqslant n$ such that all the 2^k subsums are distinct. The example of the powers of 2 and an easy counting argument give for $\max k = g(n)$ the inequalities

$$1 + [{}^2\log n] \leqslant g(n) \leqslant {}^2\log n + {}^2\log {}^2\log n + o(1).$$

Erdős and Moser (published in Erdős, 1956b) halved the ${}^2\log {}^2\log$ of the upper estimate, and Conway and Guy (see Guy, 1982) improved the lower estimate by *one* for $n \geqslant 2^{21}$.

It is a rich kitchen where such things go to the sink, so this title is respectfully copied here.

Factorisatio numerorum. Let $f(n)$ denote the number of factorizations of the natural number n into factors larger than 1, where the order of the factors does not count. (For instance, $12 = 2 \cdot 6 = 3 \cdot 4 = 2 \cdot 2 \cdot 3$, thus $f(12) = 4$.) Canfield, Erdős, and Pomerance (1983) determined the maximal order of this function. With $F(n) = \max_{k \leqslant N} f(k)$ we have

$$F(n) = n \exp\{(1 + 0(1)) \log n \log_3 n/\log \log n\}.$$

Few multiples of primes in an interval. Let $p_1 < \cdots < p_u$ be primes (now just any u primes, not necessarily the first ones), and take an interval of length αp_u. How many multiples must these primes have in this interval at the least? If $\alpha > 1$, each p_i has at least one multiple, but they may all coincide. If $\alpha > 2$, then each has at least two multiples, and these pairs are different; hence a lower estimate $c\sqrt{u}$ easily follows. Erdős and Selfridge (1975) found for $2 < \alpha < 3$ the exact bound; it is $\sqrt{u/2}$ if u is of the form $2m^2$. We make a graph on the multiples by connecting the first two multiples of each p_i by an edge. If $p_1 > 2$, this will be a bipartite graph, which easily yields the lower estimate. To learn how the complete bipartite graph is realized see Erdős (1978).

If $\alpha > 3$, then the (first three) multiples of each prime form an arithmetical progression of length 3, each with a different difference. Of course, not every such configuration can be realized with primes, and to tell which are we may need to resort to unproved hypotheses about primes. But we are concerned with the following problem: How many arithmetical progressions of length 3 with distinct differences can lie in a set of k integers? I am sure an answer to this would lead to a deeper understanding of the additive structure of sets of integers.

Cyclotomic polynomials. Let

$$\Phi_n(z) = \sum_{m=0}^{\phi(n)} a_{m,n} z^m$$

be the nth cyclotomic polynomial. The first few polynomials have mainly 0, ± 1 coefficients, and this induces one to think that they remain generally small. Still, Erdős conjectured that $A(n) = \max |a(m, n)|$ tends to ∞ for almost all n. This was established by Maier (1990); later (Maier, 1993) he added that it is $> n^c$ on a set of positive density. Sometimes it is much larger: Erdős (1949b) proved that it can be as big as $\exp\exp(c \log n / \log\log n)$, which is best possible, save the value of c, by a result of Bateman (1949). (As a general reference, the reader can consult Bachmann (1993).)

Quadratic residues. Davenport and Erdős (1952) proved, improving a result of Vinogradov, that the smallest quadratic nonresidue modulo a prime p is $\ll p^{(1/2\sqrt{e})+\varepsilon}$, which is still the record. The conjecture is, naturally, $p^{o(1)}$. Surprisingly, better exponents are known for cubic and quintic residues; see Jordan (1966).

Values of L-functions. Consider the Dirichlet series

$$L_d(s) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-s}$$

(an L-function corresponding to a real character) for a real $s > 3/4$. Chowla and Erdős (1951) show that for a fixed s this series, as a function of d, has a limiting distribution $g(u)$, which is continuous, satisfies $g(0) = 0$, and is strictly increasing for $u > 0$ (in particular, $L_d(s) > 0$ for almost all d). The distribution was descibed and the speed of convergence estimated by Elliott (1970).

Euclidean algorithm in number fields. Erdős and Ko (1938a) proved that there is no Euclidean algorithm with respect to the norm in the quadratic field $\mathbb{Q}(\sqrt{p})$, if p is a prime, $p \equiv 1 \pmod 8$ or $p \equiv 13 \pmod{24}$. This was the last undecided case.

Quadratic forms. Consider a quadratic form (with integral coefficients) $f=\sum a_{ij}x_ix_j$ of determinant D. Mordell proved that if f is positive definite and $D>(2/\pi)^n$, then f can be decomposed as a sum of two positive semi-definite forms. Erdős and Ko (1938b, c) showed that the limit cannot be reduced below 1.1^n.

Diophantine approximation. For every irrational α there are infinitely many a, q such that $(a, q)=1$ and $|\alpha-a/q|<1/q^2$. To what degree can this be improved if we are content to approximate almost all (rather than all) α? In other words, given a sequence $\delta_q \geqslant 0$, when is it true that for almost all α we can find infinitely many a, q such that $|\alpha-a/q|<\delta_q/q^2$? By familiar measure-theoretic arguments (Borel–Cantelli) a necessary condition is that

$$\sum \delta_q \frac{\phi(q)}{q^2}=\infty.$$

Erdős (1970b) solves the important case when $\delta_q=0$ or 1. More exactly, for any sequence $q_1<q_2<\cdots$ of integers the following three are equivalent:

(1) $\sum \phi(q_i)/q_i^2=\infty$,

(2) $\liminf q_i \,\|\alpha q_i\|=0$ for almost all α,

(3) for almost all α there are infinitely many elements of the sequence q_i among the denominators of the convergents in the continued fraction development of α.

Connection between additive and multiplicative properties. Erdős and Turán (1934) proved that for any collection of positive integers $a_1, ..., a_n$, the numbers a_i+a_j, $1\leqslant i, j\leqslant n$, have altogether at least k prime divisors if $n\geqslant 3\cdot 2^{k-2}$. This was extended to numbers of the form a_i+b_j, $1\leqslant i\leqslant n$, $1\leqslant j\leqslant m$, by Győry, Stewart, and Tijdeman (1988); this works even for $m=2$.

The following result of Erdős and Sárközy (1970) connects primitive sequences (Section 5) with additive questions. If a sequence has the property that no element divides the sum of any two larger elements, then it must have density 0.

Another type of connection is studied by Erdős, Maier, and Sárközy (1987). They show that if we take two dense sets $\mathscr{A}, \mathscr{B}\subset[1, x]$, then an analog of the Erdős–Kac theorem holds for the distribution of $\omega(a+b)$, $a\in\mathscr{A}$, $b\in\mathscr{B}$. See Tenenbaum (1989) for an improved error term.

None of the above, but still beautiful. The following charming small finger-exercise was proposed as a problem in the Monthly in 1937. Let $a_1 < \cdots < a_n \leqslant 2n$ be integers. We have

$$\max_{i \neq j} \gcd(a_i, a_j) > \tfrac{38}{147} n - c,$$

where 38/147 is best possible.

This is from a letter of his to me around 1980:

> Let $1 \leqslant a_1 < \cdots < a_k \leqslant n$, $(a_j - a_i) \nmid a_j$. Then it is trivial that $\max k = [(n+1)/2]$, namely $a_{i+1} - a_i > 1$ and $a_i \equiv 1 \pmod 2$ is good. But suppose that $(a_j - a_i) \nmid a_j$ for $a_j - a_i \geqslant t$. How large is $\max k$? I don't know this even for $t = 2$, maybe just because My Oldness is stupid and My Stupidity is old.
>
> $k > n/2 + c \log n$ is possible for $t = 2$, for instance $a_i \equiv 1 \pmod 2$ and $a_i = 2^{2l+1}$. $\max k = n/2 + o(n)$?

ACKNOWLEDGMENTS

I am grateful to Róbert Freud for carefully reading my manuscript and pointing out many inaccuracies.

REFERENCES

D. S. Adhikari, The average behaviour of the number of solutions of a Diophantine equation and an averaging technique, *in* "Number Theory: Diophantine, Computational and Algebraic Aspects, Eger, Hungary, July 29–Aug. 2, 1996" (K. Győry, A. Pettho, and V. Sós, Eds.), pp. 1–8, de Gruyter, Berlin, 1998.

M. Ajtai, J. Komlós, and E. Szemerédi, A dense infinite Sidon sequence, *Europ. J. Combin.* **2** (1981), 1–11.

N. Alon and M. Dubiner, Zero-sum sets of prescribed size, *in* "Combinatorics, Paul Erdős Is Eighty, Keszthely, Hungary, 1993," Vol. 1, pp. 33–50, János Bolyai Mathematical Society, Budapest, 1993. [MR 94j:11016]

N. Alon and M. Dubiner, A lattice point problem and additive number theory, *Combinatorica* **15** (1995), 301–309.

N. Alon, M. B. Nathanson, and I. Z. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly* **102** (1995), 250–255. [MR 95k:11009]

A. O. L. Atkin, On pseudo-squares, *Proc. London Math. Soc. Sec. A* **14** (1965), 22–27.

M. R. Avidon, On the distribution of primitive abundant numbers, *Acta Arith.* **77** (1996), 195–205.

L. Babai, In and out of Hungary: Paul Erdős, his friends, and times, *in* "Combinatorics: Paul Erdős Is Eighty, Keszthely, Hungary, 1993," Vol. 2, pp. 7–95, János Bolyai Mathematics Society, Budapest, 1996.

G. Bachmann, On the coefficients of cyclotomic polynomials, *Mem. Amer. Math. Soc.* **106** (1993), No. 510.

R. J. Backlund, Über die Differenzen zwischen den Zahlen, die zu den *n* ersten Primzahlen teilerfremd sind, *Ann. Acad. Sci. Fenn.* **32**, No. 9 (1929).

P. T. Bateman, Note on the coefficients of the cyclotomic polynomial, *Bull. Amer. Math. Soc.* **55** (1949), 1180–1181.

F. Behrend, On sequences of numbers not divisible one by another, *J. London Math. Soc.* **10** (1935), 42–44.

F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.* **32** (1946), 331–333.

A. S. Besicovitch, On the density of certain sequences of integers, *Math. Ann.* **110** (1934), 336–341.

R. C. Bose, An affine analogue of Singer's theorem, *J. Indian Math. Soc.* **6** (1942), 1–15.

A. Brauer and H. Zeitz, Über eine Zahlentheoretische Behauptung von Legendre, *Sitzungsber. Berlin Math. Ges.* **29** (1929), 116–125.

N. G. de Bruijn and P. Erdős, Sequences of points on a circle, *Indag. Math.* **11** (1949), 46–49.

J. de la Cal, On the Erdős–Wintner theorem in Banach spaces, *in* "New Trends in Probability and Statistics II" (F. Schweiger and E. Manstavičius, Eds.), pp. 201–209, VSP TEV, Vilnius/Utrecht, 1992. [MR 94a:11126]

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning 'factorisatio numerorum', *J. Number Theory* **17** (1983), 1–28. [MR 85j:11012]

S. Chowla, On abundant numbers, *J. Indian Math. Soc.* **1** (1934), 41–44.

S. Chowla, Solution of a problem of Erdős in additive number theory, *Proc. Nat. Acad. Sci. India Sect. A* **14** (1944), 1–2.

S. Chowla and P. Erdős, A theorem on the distribution of the values of L-functions, *J. Indian Math. Soc. (N.S.)* **15** (1951), 11–18. [MR 13,439a]

S. Chowla and A. M. Mian, On the B_2 sequences of Sidon, *Proc. Nat. Acad. Sci. India Sect. A* **14** (1944), 3–4.

D. A. Clark, An upper bound of $\sum 1/(a_i \log a_i)$ for primitive sequences, *Proc. Amer. Math. Soc.* **123** (1995), 363–365. [MR 95c:11026]

N. Costa Pereira, Elementary estimates for the Chebyshev function $\psi(x)$ and for the Mobius function $M(x)$, *Acta Arith.* **52** (1989), 307–337. [MR 91e:11099]

R. Crocker, On the sum of a prime and of two powers of two, *Pacific J. Math.* **36** (1971), 103–107.

H. Daboussi, Sur le théorème des nombres premiers, *C. R. Acad. Sci. Paris Ser. I Math.* **298** (1984), 161–164. [MR 85f:11065]

Z. Daróczy and I. Kátai, On additive arithmetical functions with values in topological groups, I, *Publ. Math. Debrecen* **33** (1986), 287–291. [MR 88e:11093]

H. Davenport, Über Numeri Abundantes, *Sitzungsber. Preuss. Akad. Wiss.* (1933), 830–837.

H. Davenport and P. Erdős, On sequences of positive integers, *Acta Arith.* **2** (1937), 147–151.

H. Davenport and P. Erdős, On sums of positive integral kth powers, *Ann. Math.* **40** (1939), 553–536. [MR 1,5d]

H. Davenport and P. Erdős, On sequences of positive integers, *J. Indian Math. Soc. (N.S.)* **15** (1951), 19–24. [MR 13,326c]

H. Davenport and P. Erdős, The distribution of quadratic and higher residues, *Publ. Math. Debrecen* **2** (1952), 252–265. [MR 14,1063h]

M. Deleglise, Recouvrement optimal du cercle par les multiples d'un intervalle, *Acta Arith.* **59** (1991), 21–35. [MR 92m:11011]

H. G. Diamond and P. Erdős, On sharp elementary prime number estimates, *Enseign. Math. (2)* **26** (1980), 313–321. [MR 83i:10055]

J. A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (1994), 140–146. [MR 95i:11007]

G. Dufner and D. Wolke, Einige Bemerkungen zum Goldbachschen Problem, *Monatsh. Math.* **118** (1994), 75–82. [MR 95h:11106]

P. D. T. A. Elliott, The distribution of the quadratic class number, *Liet. Mat. Rinkinys* **10** (1970), 189–197.

P. D. T. A. Elliott, “Probabilistic Number Theory I,” Springer-Verlag, New York/Berlin, 1979.

P. D. T. A. Elliott, “Probabilistic Number Theory II,” Springer-Verlag, New York/Berlin, 1980.

P. D. T. A. Elliott, “Arithmetic Functions and Integer Products,” Grundlehren der Mathematischen Wissenschaften (Fundamental Principles of Mathematical Science), Vol. 272, Springer-Verlag, New York/Berlin, 1985. [MR #86j:11095]

P. D. T. A. Elliott, and C. Ryavec, The distribution of the values of additive arithmetical functions, *Acta Math.* **126** (1971), 143–164.

P. Erdős, Beweis eines Satzes von Tschebischeff, *Acta Litt. Sci. Szeged Sect. Math.* **5** (1930/1932), 194–198.

P. Erdős, On the density of the abundant numbers, *J. London Math. Soc.* **9** (1934), 278–282.

P. Erdős, On the difference of consecutive primes, *Quart. J. Math. Oxford* **6** (1935a), 124–128.

P. Erdős, On primitive abundant numbers, *J. London Math. Soc.* **10** (1935b), 49–58.

P. Erdős, On the density of some sequences of numbers, I, *J. London Math. Soc.* **10** (1935c), 120–125.

P. Erdős, Note on sequences of integers none of which is divisible by any other, *J. London Math. Soc.* **10** (1935d), 126–128.

P. Erdős, Note on consecutive abundant numbers, *J. London Math. Soc.* **10** (1935e), 128–131.

P. Erdős, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ function, *Quart. J. Math. Oxford* **6** (1935f), 205–213.

P. Erdős, Über die Primzahlen gewisser arithmetischer Reihen, *Math. Z.* **39** (1935g), 473–491.

P. Erdős, On the arithmetical density of the sum of two sequences, one of which forms a basis for the integers, *Acta Arith.* **1** (1936a), 201–207.

P. Erdős, On the arithmetical density of the sum of two sequences, one of which forms a basis for the integers, II, *Travaux Inst. Math. Tbilisi* (1936b), 217–224.

P. Erdős, On the density of some sequences of numbers, II, *J. London Math. Soc.* **12** (1937a), 7–11.

P. Erdős, Note on the number of prime divisors of integers, *J. London Math. Soc.* **12** (1937b), 308–314.

P. Erdős, On the density of some sequences of numbers, III, *J. London Math. Soc.* **13** (1938), 119–127.

P. Erdős, Note on products of consecutive integers, *J. London Math. Soc.* **14** (1939a), 194–198. [MR 1,4e]

P. Erdős, Note on the product of consecutive integers, II, *J. London Math. Soc.* **14** (1939b), 245–249. [MR 1,39d]

P. Erdős, On the integers of the form $x^k + y^k$, *J. London Math. Soc.* **14** (1939c), 250–254. [MR 1,42b]

P. Erdős, The difference of consecutive primes, *Duke Math. J.* **6** (1940a), 438–441. [MR 1,292h]

P. Erdős, On a problem of Sidon in additive number theory and on some related problems. Addendum, *J. London Math. Soc.* **19** (1944a), 208. [MR 7,242f]

P. Erdős, On the distribution of additive functions, *Ann. of Math.* **47** (1946), 1–20.

P. Erdős, On the integers having exactly K prime factors, *Ann. of Math. (2)* **49** (1948a), 53–66. [MR 9,333b]

P. Erdős, On the density of some sequences of integers, *Bull. Amer. Math. Soc.* **54** (1948b), 685–692. [MR 10,105b].

P. Erdős, On the difference of consecutive primes, *Bull. Amer. Math. Soc.* **54** (1948c), 885–889. [MR 10,235b].

P. Erdős, Some asymptotic formulas in number theory, *J. Indian Math. Soc. (N.S.)* **12** (1948d), 75–78. [MR 10,594d]

P. Erdős, Problems and results on the differences of consecutive primes, *Publ. Math. Debrecen* **1** (1949a), 33–37. [MR 11,84a]

P. Erdős, On the coefficients of the cyclotomic polynomial, *Portugal. Math.* **8** (1949b), 63–71. [MR 12,11f]

P. Erdős, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.* **2** (1950a), 113–123. [MR 13,437i]

P. Erdős, On a Diophantine equation, *J. London Math. Soc.* **26** (1951a), 176–178. [MR 12,804d]

P. Erdős, Some results on additive number theory, *Proc. Amer. Math. Soc.* **5** (1954a), 847–853. [MR 16,336b]

P. Erdős, On a problem of Sidon in additive number theory, *Acta Sci. Math. Szeged* **15** (1954b), 255–259. [MR 16,336c]

P. Erdős, Some remarks on number theory, *Riv. Lemat.* **9** (1955a), 45–48. [MR 17,460d]

P. Erdős, Megjegyzések a Matematikai Lapok két problémájához, *Mat. Lapok* **7** (1956a), 10–17.

P. Erdős, Problems and results in additive number theory, *in* "Colloque sur la Théorie des Nombres, Bruxelles, 1955," pp. 127–137, Thone, Liège & Masson, Paris, 1956b. [MR 18,18a]

P. Erdős, Remarks on number theory. I. On primitive α-abundant numbers, *Acta Arith.* **5** (1958a), 25–33. [MR 21 # 24]

P. Erdős, Some remarks on Euler's φ function, *Acta Arith.* **4** (1958b), 10–19. [MR 22 # 1539].

P. Erdős, An asymptotic inequality in the theory of numbers, *Vestnik Leningrad. Univ. Math.* **15**, No. 13 (1960a), 41–49 [in Russian].

P. Erdős, Some remarks on number theory, II, *Mat. Lapok* **12** (1961a), 161–169. [MR 26 # 2411]

P. Erdős, Über einige Probleme der additiven Zahlentheorie, *J. Reine Angew. Math.* **206** (1961b), 61–66. [MR 24 # A707]

P. Erdős, On some applications of probability to analysis and number theory, *J. London Math. Soc.* **39** (1964a), 692–696. [MR 30 # 1997]

P. Erdős, On the multiplicative representation of integers, *Israel J. Math.* **2** (1964b), 251–261. [MR 31 # 5847]

P. Erdős, On some applications of graph theory to number theoretic problems, *Publ. Ramanujan Inst.* **1** (1968/1969), 131–136. [MR 42 # 4520]

P. Erdős, On the distribution of prime divisors, *Aequationes Math.* **2** (1969a), 177–183.

P. Erdős, Some applications of graph theory to number theory, *in* "The Many Facets of Graph Theory: Conference Proceedings, Western Michigan University, Kalamazoo, 1968," pp. 77–82, Springer-Verlag, Berlin, 1969b. [MR 40 # 4149]

P. Erdős, Some extremal problems in combinatorial number theory, *in* "Mathematical Essays Dedicated to A. J. Macintyre," pp. 123–133, Ohio Univ. Press, Athens, 1970a. [MR 43 # 1942]

P. Erdős, On the distribution of the convergents of almost all real numbers, *J. Number Theory* **2** (1970b), 425–441. [MR 42 # 5941]

P. Erdős, On the sum $\sum_{d2^n-1} d^{-1}$, *Israel J. Math.* **9** (1971), 43–48. [MR 42 # 4508]

P. Erdős, Problems and results in combinatorial analysis and combinatorial number theory, *in* "Congressus Numerantium XXI: Proceedings Ninth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Boca Raton, 1978," pp. 29–40, Utilitas Math., Winnipeg, 1978.

P. Erdős, Some of my favorite problems and results, *in* "The Mathematics of Paul Erdős" (R. L. Graham and J. Nešetřil, Eds.), pp. 47–67, Springer-Verlag, Berlin/New York, 1997.

P. Erdős and W. H. J. Fuchs, On a problem of additive number theory, *J. London Math. Soc.* **31** (1956), 67–73. [MR 17,586d]

P. Erdős, A. Ginsburg, and A. Ziv, Theorem in the additive number theory, *Bull. Res. Council Israel* **10** (1961), 41–43.

P. Erdős and R. L. Graham, On bases with an exact order, *Acta Arith.* **37** (1980), 201–207. [MR 82e:10093]

P. Erdős, R. R. Hall, and G. Tenenbaum, On the densities of sets of multiples, *J. Reine Angew. Math.* **454** (1994), 119–141. [MR 95k:11115]

P. Erdős and H. Heilbronn, On the addition of residue classes mod p, *Acta Arith.* **9** (1964), 149–159. [MR 29#3463]

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.

P. Erdős and M. Kac, The Gaussian law of errors in the theory of additive number theoretic functions, *Amer. J. Math.* **62** (1940), 738–742. [MR 2,42c]

P. Erdős, P. Kiss, and C. Pomerance, On prime divisors of Mersenne numbers, *Acta Arith.* **57** (1991), 267–281. [MR 92d:11104]

P. Erdős and C. Ko, Note on the Euclidean algorithm, *J. London Math. Soc.* **13** (1938a), 3–3.

P. Erdős and C. Ko, On the definite quadratic forms which are not the sum of definite or semidefinite forms, *Acta Arith.* **3** (1938b), 102–121.

P. Erdős and C. Ko, Some results on definite quadratic forms, *J. London Math. Soc.* **13** (1938c), 217–224.

P. Erdős and K. Mahler, On the number of integers which can be represented by a binary form, *J. London Math. Soc.* **13** (1938), 134–139.

P. Erdős, H. Maier, and A. Sárközy, On the distribution of the number of prime factors of sums $a+b$, *Trans. Amer. Math. Soc.* **302** (1987), 269–280. [MR 88d:11090]

P. Erdős, C. Pomerance, and E. Schmutz, Carmichael's lambda function, *Acta Arith.* **58** (1991), 363–385. [MR 92g:11093]

P. Erdős and K. Prachar, Sätze und Probleme über p_k/k, *Abh. Math. Sem. Univ. Hamburg* **25** (1961/1962), 251–256. [MR 25#3901]

P. Erdős and A. Rényi, Additive properties of random sequences of positive integers, *Acta Arith.* **6** (1960), 83–110. [MR 22#10970]

P. Erdős and A. Rényi, On some applications of probability methods to additive number theoretic problems, *in* "Contributions to Ergodic Theory and Probability: Proceedings of Conference held at Ohio State University, Columbus, 1970," pp. 37–44, Springer-Verlag, Berlin, 1970. [MR 43#1938]

P. Erdős, I. Ruzsa, Jr., and A. Sárközy, On the number of solutions of $f(n)=a$ for additive functions, "Collection of Articles Dedicated to Carl Ludwig Siegel on the Occasion of His Seventy-Fifth Birthday, I," *Acta Arith.* **24** (1973), 1–9. [MR 48#11013]

P. Erdős and A. Sárközy, On the divisibility properties of sequences of integers, *Proc. London Math. Soc. (3)* **21** (1970), 97–101. [MR 42#222]

P. Erdős and A. Sárközy, On isolated, respectively consecutive large values of arithmetic functions, *Acta Arith.* **66** (1994), 269–295. [MR 95c:11111]

P. Erdős, A. Sárközy, and V. T. Sós, Problems and results on additive properties of general sequences, III, *Studia Sci. Math. Hungar.* **22** (1987), 53–63. [MR 89b:11015]

P. Erdős, A. Sárközy, and V. T. Sós, On sum sets of Sidon sets, II, *Israel J. Math.* **90** (1995), 221–233.

P. Erdős, A. Sárközy, and E. Szemerédi, On an extremal problem concerning primitive sequences, *J. London Math. Soc.* **42** (1967a), 484–488. [MR 36#1412]

P. Erdős, A. Sárközy, and E. Szemerédi, On a theorem of Behrend, *J. Austral. Math. Soc.* **7** (1967b), 9–16. [MR 35#148]

P. Erdős, A. Sárközy, and E. Szemerédi, Über Folgen ganzer Zahlen, *in* "Number Theory and Analysis (Papers in Honor of Edmund Landau)," pp. 77–86, Plenum, New York, 1969. [MR 41#8372]

P. Erdős and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292–301. [MR 51/12692]

P. Erdős and H. N. Shapiro, On the changes of sign of a certain error function, *Canad. J. Math.* **3** (1951), 375–385. [MR 13,535i]

P. Erdős and H. N. Shapiro, The existence of a distribution function for an error term related to the Euler function, *Canad. J. Math.* **7** (1955), 63–75. [MR 16,448f]

P. Erdős and J. Spencer, "Probabilistic Methods in Combinatorics," Akadémiai Kiadó, Budapest, 1974.

P. Erdős and J. Spencer, A problem in covering progressions, *Studia Sci. Math. Hungar.* **30** (1995), 149–154.

P. Erdős and J. Surányi, Bemerkungen zu einer Aufgabe eines mathematischen Wettbewerbs, *Mat. Lapok* **10** (1959), 39–48. [MR 26#2388]

P. Erdős and J. Surányi, "Válogatott fejezetek a számelméletből (Selected Chapters from Number Theory)," Tankönyvkiadó Vállalat, Budapest, 1960; (2nd ed.), Polygon, Szeged, 1996. [MR 28#5022]

P. Erdős and G. Szekeres, Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem, *Acta Sci. Math. Szeged* **7** (1934), 95–102.

P. Erdős and G. Tenenbaum, Sur les fonctions arithmétiques liées aux diviseurs consecutifs, *J. Number Theory* **31** (1989), 285–311. [MR 90i:11103]

P. Erdős and P. Turán, On a problem in the elementary theory of numbers, *Amer. Math. Monthly* **41** (1934), 608–611.

P. Erdős and P. Turán, On some sequences of integers, *J. London Math. Soc.* **11** (1936), 261–264.

P. Erdős and P. Turán, On a problem of Sidon in additive number theory, and on some related problems, *J. London Math. Soc.* **16** (1941), 212–215. [MR 3,270e]

P. Erdős and P. Turán, On a problem in the theory of uniform distribution, I, *Indag. Math.* **10** (1948a), 370–378.

P. Erdős and P. Turán, On a problem in the theory of uniform distribution, II, *Indag. Math.* **10** (1948b), 406–413.

P. Erdős and P. Turán, On some new questions on the distribution of prime numbers, *Bull. Amer. Math. Soc.* **54** (1948c), 371–378. [MR 9,498k]

P. Erdős and S. Ulam, Some probabilistic remarks on Fermat's last theorem, *Rocky Mountain J. Math.* **1** (1971), 613–616. [MR 44#2724]

P. Erdős and A. Wintner, Additive arithmetical functions and statistical independence, *Amer. J. Math.* **61** (1939), 713–721. [MR 1,40c]

W. D. Gao, Two addition theorems on groups of prime order, *J. Number Theory* **56** (1996), 211–213.

W. T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, *Geom. Funct. Anal.* **7** (1998), 322–337.

A. Granville and O. Ramaré, Explicit bounds on exponential sums and the scarcity of squarefree binomial coefficients, *Mathematika* **43** (1996), 73–107.

R. K. Guy, Sets of integers whose subsets have distinct sums, *in* "Theory and Practice of Combinatorics," North-Holland Math. Studies, Vol. 60, pp. 141–154, North-Holland, Amsterdam/New York, 1982. [MR 86m:11009]

K. Győry, On the diophantine equation $\binom{n}{k}=x^l$, *Acta Arith.* **80** (1997), 289–295.

K. Győry, C. L. Stewart, and R. Tijdeman, On prime factors of sums of integers, III, *Acta Arith.* **49** (1988), 307–312. [MR 89g:11094]

G. Halász, On the distribution of additive arithmetical functions, *Acta Arith.* **27** (1975), 143–152.

H. Halberstam and K. F. Roth, "Sequences," Clarendon, London, 1966; (2nd ed.), Springer-Verlag, New York/Berlin, 1983.

R. R. Hall, "Sets of Multiples," Cambridge Univ. Press, Cambridge, UK, 1996.

R. R. Hall and G. Tenenbaum, "Divisors," Cambridge Tracts in Mathematics, Vol. 90, Cambridge Univ. Press, Cambridge/New York, UK, 1988. [MR 90a:11107]

G. H. Hardy and S. Ramanujan, The normal number of prime factors of a number n, *Quart. J. Math. (Oxford)* **48** (1917), 76–92.

D. R. Heath-Brown, Integer sets containing no arithmetic progression, *J. London Math. Soc.* **35** (1987), 385–394.

P. Hegedűs, G. Piroska, and I. T. Ruzsa, On the Schnirelmann density of sumsets, *Publ. Math. Debrecen* **53** (1998), 333–345.

M. Helm, On B_{2k}-sequences, *Acta Arith.* **63** (1993), 367–371. [MR 95c:11029]

M. Helm, A generalization of a theorem of Erdős on asymptotic basis of order 2, *J. Theoret. Nombres Bordeaux* **6** (1994), 9–19. [MR 95i:11008]

A. Hildebrand, The prime number theorem via the large sieve, *Mathematika* **33** (1986), 23–30. [MR 88a:11085]

X.-D. Jia, On B_{2k}-sequences, *J. Number Theory* **48** (1994), 183–196. [MR 95d:11027]

J. H. Jordan, The distribution of cubic and quintic non-residues, *Pacific J. Math.* **16** (1966), 77–85.

N. M. Khodzhaev, Some multiplicative properties of products of natural numbers in short intervals, *Moscow Univ. Math. Bull.* **48** (1993), 36–39 [in English]; *Vestnik Moskov. Univ. Ser. Mat.* **119** (1993), 40–43 [in Russian].

J. F. Koksma, "Some Theorems on Diophantine Inequalities," Math. Centrum Scriptum, Vol. 5, Math Centrum, Amsterdam, 1950.

M. N. Kolountzakis, An effective additive basis for the integers, *in* "Proceedings, Fifth Annual ACM–SIAM Symposium on Discrete Algorithms, Arlington, VA, 1994," pp. 44–47, Assoc. Comput. Mach., New York, 1994. [MR 95d:11009]

M. N. Kolountzakis, On the additive complements of the primes and sets of similar growth, *Acta Arith.* **77** (1996), 1–8.

K. Kovács, On the characterization of additive functions with monotonic norm, *J. Number Theory* **24** (1986), 298–304. [MR 88d:11075]

F. Krückeberg, B_2-Folgen und verwandte Zahlenfolgen, *J. Reine Angew. Math.* **206** (1961), 53–60.

J. Kubilius, "Probabilistic Methods in the Theory of Numbers," Vilnius, 1959; (2nd ed.), 1962 [in Russian].

J. Kubilius, "Probabilistic Methods in the Theory of Numbers," AMS Translations of Math. Monographs, Vol. 11, American Math. Society, Providence, RI, 1964.

P. Kuhn, Ein Verbesserung des Restgliedes beim elementaren Beweis des Primzahlsatzes, *Math. Scand.* **3** (1955), 75–89.

A. F. Lavrik and A. Sh. Shobirov, The remainder term in the elementary proof of the prime number theorem, *Dokl. Akad. Nauk. SSSR* **211** (1973), 534–536 [in Russian]; *Soviet Mat. Dokl.* **14** (1973), 1063–1066 [in English]. [MR 48/2092]

B. V. Levin and N. M. Timofeev, An analytic method in probabilistic number theory, *Uchen Zap. Vladimirskogo Gos. Ped. Inst. (Mat.)* **57**, No. 2 (1971), 57–150 [in Russian].

B. Lindström, An inequality for B_2-sequences, *J. Combin. Theory* **6** (1969), 211–212.

G. G. Lorentz, On a problem of additive number theory, *Proc. Amer. Math. Soc.* **5** (1954), 838–841.

H. Maier, Primes in short intervals, *Michigan Math. J.* **32** (1985), 221–225. [MR 86i:11049]
H. Maier, Small differences between prime numbers, *Michigan Math. J.* **35** (1988), 323–344. [MR 90e:11126]
H. Maier, The coefficients of cyclotomic polynomials, *in* "Analytic Number Theory, Allerton Park, IL, 1989," Progress in Mathematics, Vol. 85, pp. 349–366, Birkhäuser Boston, Cambridge, MA, 1990. [MR 92a:11110]
H. Maier, Cyclotomic polynomials with large coefficients, *Acta Arith.* **64** (1993), 227–235. [MR 94g:11074]
H. Maier and C. Pomerance, On the number of distinct values of Euler's ϕ-function, *Acta Arith.* **49** (1988), 263–275. [MR 89d:11083]
H. Maier and G. Tenenbaum, On the set of divisors of an integer, *Invent. Math.* **76** (1984), 121–128. [MR 86b:11057]
H. Maier and G. Tenenbaum, On the normal concentration of divisors, *J. London Math. Soc.* **31** (1985), 393–400.
H. B. Mann, Two addition theorems, *J. Combin. Theory* **3** (1967), 233–235.
J. L. Mauclaire, On the regularity of group-valued additive arithmetical functions, *Publ. Math. Debrecen* **44** (1994), 285–290. [MR 95f:11077]
H. L. Montgomery, Fluctuations in the mean of Euler's phi function, *Proc. Indian Acad. Sci. Math. Sci.* **97** (1987), 239–245. [MR 90e:11138]
H. L. Montgomery, "Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis," CBMS Regional Conference Series in Math., Vol. 84, American Math. Society, Providence, RI, 1994.
H. L. Montgomery and R. C. Vaughan, On the Erdős–Fuchs theorem, *in* "A Tribute to Paul Erdős" (A. Baker, B. Bollobás, and A. Hajnal, Eds.), pp. 331–388, Cambridge Univ. Press, Cambridge, UK, 1990. [MR #92f:11128]
P. Moree, Bertrand's postulate for primes in arithmetical progressions, *Comput. Math. Appl.* **26** (1993), 35–43.
J. C. M. Nash, On B_4-sequences, *Canad. Math. Bull.* **32** (1989), 446–449. [MR 91e:11025]
J. C. M. Nash, Some applications of a theorem of M. Kneser, *J. Number Theory* **44** (1993), 1–8. [MR 94k:11015]
J. Nešetřil and V. Rödl, Two proofs in combinatorial number theory, *Proc. Amer. Math. Soc.* **93** (1985), 185–188. [MR 86c:11083]
H. Niederreiter and W. Philipp, Berry–Esseen bounds and a theorem of Erdős and Turán on uniform distribution *mod* 1, *Duke Math. J.* **40** (1973), 633–649.
J. Pintz, Very large gaps between consecutive primes, *J. Number Theory* **63** (1997), 286, 301.
H. Plünnecke, Über ein metrisches Problem der additiven Zahlentheorie, *J. Reine Angew. Math.* **197** (1957), 97–103.
H. Plünnecke, Eine zahlentheoretische Anwendung der Graphentheorie, *J. Reine Angew. Math.* **243** (1970), 171–183.
R. A. Rankin, The difference between consecutive prime numbers, *J. London Math. Soc.* **13** (1938), 242–247.
A. Raouj, Sur la densité de certains ensembles de multiples, I, II, *Acta Arith.* **69** (1995), 121–152, 171–188. [MR 96b:11126]
G. Ricci, Ricerche arithmetiche sui polinomi. II. Intorno a una proposizione non vera di Legendre, *Rend. Circ. Mat. Palermo* **58** (1934), 190–207.
G. Ricci, Recherches sur l'allure de la suite $\{(p_{n+1}-p_n)/\log p_n\}$, *in* "Colloque sur la Théorie des Nombres, Bruxelles, 1955," pp. 93–106, Thone, Liège, & Masson, Paris, 1955.
G. J. Rieger, Über p_k/k und verwandte Folgen, *J. Reine Angew. Math.* **221** (1966), 14–19.
K. F. Roth, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 104–109.
I. Z. Ruzsa, General multiplicative functions, *Acta Arith.* **32** (1977), 313–347.

I. Z. Ruzsa, On the concentration of additive functions, *Acta Math. Acad. Sci. Hungar.* **36** (1980), 215–232.
I. Z. Ruzsa, Essential components, *Proc. London Math. Soc.* **54** (1987), 38–56.
I. Z. Ruzsa, A just basis, *Monatsh. Math.* **109** (1990), 145–151.
I. Z. Ruzsa, On an inequality of Erdős and Turán concerning uniform distribution modulo one, *in* "International Colloque Math. Society J. Bolyai 60: Sets, Graphs and Numbers, Budapest, 1991," pp. 621–630, János Bolyai Mathematical Society, Budapest, 1992.
I. Z. Ruzsa, Solving a linear equation in a set of integers, I, *Acta Arith.* **65** (1993), 259–282.
I. Z. Ruzsa, Logarithmic density and measures on semigroups, *Manuscripta Math.* **89** (1996a), 307–317.
I. Z. Ruzsa, Paul Erdős—From an epsilon's eye view, *Period. Math. Hung.* **33** (1996b), 73–81.
I. Z. Ruzsa, Sumsets of Sidon sets, *Acta Arith.* **77** (1996c), 353–359.
I. Z. Ruzsa, A converse to a theorem of Erdős and Fuchs, *J. Number Theory* **62** (1997), 397–402.
I. Z. Ruzsa, An infinite Sidon sequence, *J. Number Theory* **68** (1998), 63–71.
A. Sárközy, On divisors of binomial coefficients, I, *J. Number Theory* **20** (1985), 70–80.
R. Salem and D. C. Spencer, On sets of integers which contain no three terms in arithmetical progression, *Proc. Nat. Acad. Sci. U.S.A.* **28** (1942), 561–563.
J. W. Sander, On the order of prime powers dividing $\binom{2n}{n}$, *Acta Math.* **174** (1995), 85–118.
I. J. Schoenberg, , Über die asymptotische Verteilung reellen Zahlen mod 1, *Math. Z.* **28** (1928), 171–200.
I. J. Schoenberg, On asymptotic distribution of arithmetic functions, *Trans. Amer. Math. Soc.* **39** (1936), 315–330.
S. Sidon, Ein Satz über trigonometrische Polynome und seine Anwendung in der Theorie der Fourier-Reihen, *Math. Ann.* **106** (1932), 536–539.
J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.
A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe, *J. Reine Angew. Math.* **19** (1955), 40–65, 111–140.
E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975), 199–245.
E. Szemerédi, Integer sets containing no arithmetic progressions, *Acta Math. Hungar.* **56** (1990), 155–158.
G. Tenenbaum, Facteurs premiers de sommes d'entiers (Prime factors of sums of integers), *Proc. Amer. Math. Soc.* **106** (1989), 287–296. [MR 89k:11091]
G. Tenenbaum, Une inégalite de Hilbert pour les diviseurs, *Indag. Math. (N.S.)* **2** (1991), 105–114. [MR 92i:11102]
K. Thanigasalam, On admissible exponents for kth powers, *Bull. Calcutta Math. Soc.* **86** (1994), 175–178.
P. Turán, On a theorem of Hardy and Ramanujan, *J. London Math. Soc.* **9** (1934), 274–276.
P. Turán, "Collected Papers" (P. Erdős, Ed.), Akadémiai Kiadó, Budapest, 1990.
G. Velammal, Is the binomial coefficient $\binom{2n}{n}$ squarefree?, *Hardy Ramanujan J.* **18** (1995), 23–45. [MR 95j:11016]
R. Warlimont, Arithmetical semigroups. II. Sieving by large and small prime elements. Sets of multiples, *Manuscripta Math.* **71** (1991), 197–221. [MR 92c:11098]
E. Westzynthius, Über die Verteilung der Zahlen, die zu den n ersten Primzahlen teilerfremd sind, *Comm. Phys.-Math. Soc. Sci. Fenn. (Helsingfors)* **5** (1931), Nr. 25, 1–37.
E. Wirsing, Bemerkung zu der Arbeit über vollkommene Zahlen, *Math. Ann.* **137** (1959), 316–318.

E. Wirsing, Additive and completely additive functions with restricted growth, *in* "Recent Progress in Analytic Number Theory: Proceedings of the Symposium held in Durham, 1979," Vol. 2, pp. 231–280, Academic Press, London, 1981.

E. Wirsing, Y. Sh. Tang, and P. Shao, On a conjecture of Kátai for additive functions, *J. Number Theory* **56** (1996), 391–395.

D. Wolke, On a problem of Erdős in additive number theory, *J. Number Theory* **59** (1996), 209–213.

Z. X. Zhang, Finding finite B_2-sequences with larger $m - a^1/2_m$, *Math. Comp.* **63** (1994), 403–414. [MR 94i:11109]