CHAPTER 20

Combinatorial Number Theory

Carl POMERANCE[1]

Department of Mathematics, University of Georgia, Athens, GA 30602, USA

András SÁRKÖZY[2]

Mathematical Institute of the Hungarian Academy of Sciences, Reáltanoda utca 13–15, Budapest 1364, Hungary

Contents

[1] Research partially supported by an NSF grant.
[2] Research partially supported by the Hungarian National Foundation for Scientific Research, Grant No. 1811.

HANDBOOK OF COMBINATORICS
Edited by R. Graham, M. Grötschel and L. Lovász

... 1008
... 1011
... 1013
... 1014
... 1015

1. Introduction

What is the cardinality of the largest subset of $\{1, 2, \ldots, N\}$ that does not contain two relatively prime numbers? This is a typical problem in combinatorial number theory. That the problem is one in number theory, there is no doubt. But someone who leans towards combinatorics might prefer to think of it as a question of the largest complete subgraph of that graph on $\{1, 2, \ldots, N\}$ with edges that connect two numbers when they are not coprime.

The above question illustrates a common theme in combinatorial number theory. Namely, what arithmetic properties must a "dense" subset of the integers possess? One of the greatest theorems of this type, Szemerédi's theorem, is discussed in section 6. But combinatorial number theory also deals with other issues. For example, under what conditions is a subset of the natural numbers a basis, i.e., for some h, every number can be represented as a sum of h or fewer elements from the subset. Such issues are discussed in section 3. Combinatorial sieve methods, the subject of section 2, takes its starting point at the inclusion–exclusion principle. Its simpler aspects might be described as a device for controlling the "combinatorial explosion" in the number of terms involved in an inclusion–exclusion argument.

Combinatorial number theory can also deal with some classical problems of number theory when the methods used have a strong combinatorial flavor. In section 7 we present a proof of Wirsing's theorem on perfect numbers. This gem uses nothing but simple counting arguments from elementary combinatorics.

Combinatorial number theory is a relatively young field. In 1850, P. L. Chebyshev proved that

$$c_1 \frac{x}{\log x} < \pi(x) < c_2 \frac{x}{\log x} \quad \text{for } x \geq 2\,, \tag{1.1}$$

where $\pi(x)$ denotes the number of primes up to x, and c_1, c_2 are positive constants. This result constituted important progress towards the prime number theorem, $\pi(x) = (1 + o(1))x/\log x$, which was not proved until some 45 years later. Chebyshev's proof of (1.1) (which was later analyzed and simplified by Landau, Erdős and Diamond) had a certain combinatorial flavor.

In the period 1915–1924, V. Brun essentially single-handedly began the subject of combinatorial sieve methods. In 1927, B.L. van der Waerden proved his famous theorem that whenever the set of natural numbers is partitioned into two sets, then one set contains arbitrarily long arithmetic progressions. L.G. Schnirelmann, in 1930, used both Brun's results and his own ideas on the relationship between density and bases to prove that the set consisting of one and the primes is a basis. Inspired by these works, combinatorial number theory came into full flower in the 1930s and 1940s. Certainly the most significant force to shape and define the subject both then and now has been P. Erdős. We are much indebted to him for his generous help with this chapter.

In writing a chapter such as this, certain hard choices were necessarily forced

upon us. The subject is very broad and does not have clearly delineated boundaries. It soon became clear that we had no chance of covering it all. Moreover, our philosophy for this chapter mandated the inclusion of representative proofs. Thus even the few areas that we do cover are not done encyclopaedically. Fortunately there are several excellent books that treat various aspects of combinatorial number theory with great thoroughness, books that we refer to frequently throughout for further problems, details, and references. These are *Sequences* by Halberstam and Roth (1983), *Old and New Problems and Results in Combinatorial Number Theory* by Erdős and Graham (1980), and *Unsolved Problems in Number Theory*, 2nd edition, by Guy (1994).

Some may consider the subject of integer partitions an important part of combinatorial number theory. Unfortunately, though, it is a subject we completely ignore. The interested reader is referred to the excellent monograph of Andrews (1976).

We now say a word about notation. If $n \in \mathbb{N}$ (the set of positive integers), then $\tau(n)$ is the number of positive divisors of n, $\nu(n)$ is the number of prime divisors of n, and $\Omega(n)$ is the number of prime and prime power divisors of n. For example, $\tau(12) = 6$, $\nu(12) = 2$, and $\Omega(12) = 3$. We say $n \in \mathbb{N}$ is *squarefree* if n has no square factor exceeding 1. We define the Möbius function $\mu(n)$ by $\mu(n) = (-1)^{\nu(n)}$ if n is squarefree, and $\mu(n) = 0$ if n is not squarefree. The sum of the positive divisors of n is denoted $\sigma(n)$. The number of integers in $\{1, 2, \ldots, n\}$ that are coprime to n is denoted $\varphi(n)$; this is Euler's function, of course.

The symbols $\mathscr{A}, \mathscr{B}, \ldots$ are reserved for sets of non-negative integers. If $\mathscr{A}$ is such a set, then $A(x)$ denotes the number of members of $\mathscr{A}$ not exceeding x. By $\mathscr{A} + \mathscr{B}$ we mean the set of numbers representable as $a + b$ with $a \in \mathscr{A}$, $b \in \mathscr{B}$. By $2\mathscr{A}$ we mean $\mathscr{A} + \mathscr{A}$, by $3\mathscr{A}$ we mean $2\mathscr{A} + \mathscr{A}$, etc. By $\mathscr{A} - \mathscr{A}$ we mean the set of numbers $a - a'$, where $a, a' \in \mathscr{A}$. By $|\mathscr{A}|$ we mean the cardinality of $\mathscr{A}$.

The letters p, q shall always denote primes. The function $\log x$ is the natural logarithm. When we say $f(x) \sim g(x)$ as $x \to \infty$, we mean $f(x) = (1 + o(1))g(x)$.

So as not to have too long a reference section, we often give only one or a few later references on a particular problem so that an interested reader may begin a literature search. We do not mean to imply that the articles for which we give bibliographic data are necessarily the most important ones. Sometimes we defer all references to the extensive listings in Erdős and Graham (1980) or Guy (1994).

Have you solved the problem at the start of the introduction? Suppose $N > 1$. If $\mathscr{A}$ is the set of even numbers in $\{1, 2, \ldots, N\}$, then $|\mathscr{A}| = \lfloor \frac{1}{2}N \rfloor$ and no two members of $\mathscr{A}$ are coprime. Moreover, if a set $\mathscr{B} \subset \{1, 2, \ldots, N\}$ has more than $\lfloor \frac{1}{2}N \rfloor$ members, then either $1 \in \mathscr{B}$ or $\mathscr{B}$ contains two consecutive numbers (which are clearly coprime). Thus the answer is $\lfloor \frac{1}{2}N \rfloor$ if $N > 1$; the case $N = 1$ is clearly degenerate. See section 7.4 for more on this problem.

2. Combinatorial sieve methods

Many number-theoretic problems can be reduced to a problem of the following type. A finite set $\mathscr{A} \subset \mathbb{N}$ and a finite set $\mathscr{P}$ of prime numbers are given. Estimate

the number of of members of $\mathscr{A}$ that are not divisible by any primes belonging to $\mathscr{P}$. In other words, we "sift out" the multiples of the prime numbers belonging to $\mathscr{P}$ from $\mathscr{A}$ leaving the residual set whose cardinality $S(\mathscr{A}, \mathscr{P})$ we wish to estimate. As an illustration, we are going to consider the following three problems:

(i) Estimate $\pi(x)$;

(ii) Estimate the number of prime twins q, q' with $q' = q + 2$ and $q' \leqslant x$;

(iii) For each $x \in \mathbb{N}$, estimate the number of prime pairs q, r with $q + r = x$.

Problem (ii) is connected with the famous twin prime conjecture which asserts that there are infinitely many such pairs q, $q + 2$. Problem (iii) is connected with Goldbach's conjecture which asserts that if x is an even integer at least 4, then x is a sum of two primes. These are among the most famous unsolved problems in mathematics.

For any set $\mathscr{A} \subset \mathbb{N}$, let

$$\mathscr{A}(d) = \{n \in \mathscr{A} : d \mid n\} . \tag{2.1}$$

First we are going to study problem (i). Let $x \geqslant 1$, and let us write

$$\mathscr{A} = \{n \in \mathbb{N} : n \leqslant x\} , \tag{2.2}$$

so that

$$|\mathscr{A}(d)| = \lfloor x/d \rfloor . \tag{2.3}$$

Furthermore, let us write

$$\mathscr{P} = \{p \text{ prime} : p \leqslant \sqrt{x}\} . \tag{2.4}$$

Consider the following simple fact: an integer n with $\sqrt{x} < n \leqslant x$ is a prime if and only if there is no prime $p \in \mathscr{P}$ with $p \mid n$. Thus if we start out from the set $\mathscr{A}$ in (2.2) and we sift by the primes in the set $\mathscr{P}$ in (2.4), then the set left after the sifting procedure consists of the number 1 and the primes q with $\sqrt{x} < q \leqslant x$ [so that $S(\mathscr{A}, \mathscr{P}) = 1 + \pi(x) - \pi(\sqrt{x})$].

On the other hand, the number of integers left after the sifting procedure can be computed by the well-known inclusion–exclusion principle of elementary combinatorics (cf. chapter 21). In this way, we get the following formula:

$$\begin{aligned} &|\{1\} \cup \{q \text{ prime} : \sqrt{x} < q \leqslant x\}| \\ &\quad = |\mathscr{A}| + \sum_{k=1}^{\pi(\sqrt{x})} (-1)^k \sum_{p_1 < p_2 < \cdots < p_k \leqslant \sqrt{x}} |\mathscr{A}(p_1 p_2 \cdots p_k)| . \end{aligned} \tag{2.5}$$

In fact, to prove this identity, we have to show two facts:

(a) the contribution of 1 and of each prime q with $\sqrt{x} < q \leqslant x$ to the right-hand side of (2.5) is 1;

(b) if $n \leqslant x$ and it is divisible by at least one $p \in \mathscr{P}$, then its contribution to the right-hand side of (2.5) is 0.

[Note that only positive integers $n \leqslant x$ contribute to the right-hand side of (2.5).]

We have (a) immediately since in the first term, $|\mathscr{A}|$, every positive integer

$n \leqslant x$ is counted exactly once, while 1 and the primes q with $\sqrt{x} < q \leqslant x$ are not multiples of any prime $p \leqslant \sqrt{x}$, so are counted in none of the terms $(-1)^k |\mathscr{A}(p_1 p_2 \cdots p_k)|$.

To show (b), assume that $1 < n \leqslant x$ and $p_1', p_2', \ldots, p_l'$ are all the distinct prime divisors not exceeding $\sqrt{x}$ of n, where $l \geqslant 1$. Then the first term $|\mathscr{A}|$ on the right-hand side of (2.5) contributes with a weight 1. Any other term $(-1)^k |\mathscr{A}(p_1 p_2 \cdots p_k)|$ contributes with a weight $(-1)^k$ if and only if $p_1, p_2, \ldots, p_k$ are chosen from $p_1', p_2', \ldots, p_l'$; for a fixed k there are $\binom{l}{k}$ such terms with this property. Thus the total contribution of this n to the right-hand side of (2.5) is

$$1 + \sum_{k=1}^{l} (-1)^k \binom{l}{k}.$$

By the identity

$$\sum_{k=0}^{l} (-1)^k \binom{l}{k} = (1-1)^l = 0, \tag{2.6}$$

this contribution is 0, which completes the proof of (2.5).

Writing

$$\prod_{p \leqslant z} p = P(z), \tag{2.7}$$

we rewrite (2.5) in the following equivalent form:

$$1 + \pi(x) - \pi(\sqrt{x}) = \sum_{d | P(\sqrt{x})} \mu(d) |\mathscr{A}(d)|, \tag{2.8}$$

where μ is defined section 1. In view of (2.3), we obtain:

Theorem 2.9. *If $x \geqslant 1$, then*

$$1 + \pi(x) - \pi(\sqrt{x}) = \sum_{d | P(\sqrt{x})} \mu(d) \lfloor x/d \rfloor .$$

In fact, Legendre used this formula in his numerical studies of $\pi(x)$. The sieve method described above is called the *sieve of Eratosthenes*.

By choosing the set $\mathscr{A}$ in an appropriate way, problems (ii) and (iii) can be studied similarly. For example, in the case of problem (ii) we choose

$$\mathscr{A} = \{n(n+2) : n \in \mathbb{N}, n \leqslant x - 2\}, \qquad \mathscr{P} = \{p \text{ prime} : p \leqslant \sqrt{x}\}. \tag{2.10}$$

Then by using the inclusion–exclusion principle, one may similarly derive the following formula analogous to (2.8), where $\mathscr{A}$ is now defined by (2.10) rather than (2.2):

$$|\{q : q, q+2 \text{ are primes}, \sqrt{x} < q \leqslant x - 2\}| = \sum_{d | P(\sqrt{x})} \mu(d) |\mathscr{A}(d)|. \tag{2.11}$$

Here we have

$$|\mathscr{A}(d)| = |\{n(n+2): n \in \mathbb{N}, n \leqslant x-2, d \mid n(n+2)\}| .$$

It is easy to see that $|\mathscr{A}(d)| \approx \omega(d)x/d$, where

$$\omega(d) = |\{n \in \mathbb{N}: 0 \leqslant n < d, n(n+2) \equiv 0 \pmod{d}\}| . \tag{2.12}$$

Clearly, $\omega(p) = 1$ for $p = 2$, $\omega(p) = 2$ for any odd prime p, and by the Chinese Remainder Theorem, the function $\omega(n)$ is multiplicative [i.e., $\omega(mn) = \omega(m)\omega(n)$ when $(m, n) = 1$]. Thus for $\mu(d) \neq 0$, i.e., for d squarefree, we have

$$|\,|\mathscr{A}(d)| - \omega(d)x/d\,| \leqslant \omega(d) \leqslant 2^{\nu(d)} , \tag{2.13}$$

where $\nu(d)$ is defined in section 1.

Finally, to attack problem (iii), one may choose

$$\mathscr{A} = \{n(x-n): n \in \mathbb{N}, n \leqslant x\} \tag{2.14}$$

and $\mathscr{P}$ as in (2.4) and (2.10). We leave the further details to the reader.

The main problem with the sieve of Eratosthenes is that as in (2.8) and (2.12), it gives the number of integers left after the sifting in the form of a sum, and this sum has "too many" terms. For example, the sum on the right-hand side of (2.8) has $\tau(P(\sqrt{x})) = 2^{\pi(\sqrt{x})}$ terms and, in view of (1.1), this is much bigger than the number $\pi(x)$ which is being computed. As a consequence, one cannot use Theorem 2.9 for estimating $\pi(x)$ as $x \to \infty$. Indeed, the best we can do is use the approximation

$$\lfloor x/d \rfloor \approx x/d ,$$

whose error is less than 1 so that, in view of $|\mu(d)| \leqslant 1$, the total error would be bounded by the number of terms, namely $2^{\pi(\sqrt{x})}$.

Ignoring the error, this approximation would lead to the estimate

$$\pi(x) \approx \sum_{d \mid P(\sqrt{x})} \mu(d)\frac{x}{d} = x \sum_{d \mid P(\sqrt{x})} \frac{\mu(d)}{d} = x \prod_{p \leqslant \sqrt{x}} \left(1 - \frac{1}{p}\right) . \tag{2.15}$$

We now recall Mertens' theorem, an elementary result in prime number theory:

$$\prod_{p \leqslant z} \left(1 - \frac{1}{p}\right) \sim \frac{1}{e^{\gamma} \log z} \quad \text{as } z \to \infty , \tag{2.16}$$

where γ is Euler's constant. Thus, from (2.15) and (2.16), we get the approximation

$$\pi(x) \approx c\,\frac{x}{\log x} , \tag{2.17}$$

where $c = 2e^{-\gamma} \approx 1.123$, but we get this approximation with an error term bounded only by $2^{\pi(\sqrt{x})}$ which is much greater than the approximating function. This error term is certainly not negligible since, by the prime number theorem, we

have

$$\pi(x) = (1 + o(1))\frac{x}{\log x},$$

while the constant c appearing in (2.17) is larger than 1. The heuristic (2.17) does give the correct order of magnitude for $\pi(x)$, a fact that we shall see can be expected (at least for upper bounds) from sieve methods.

The situation is even slightly worse in case of problems (ii) and (iii). For example, in the case of problem (ii), if we replace $|\mathcal{A}(d)|$ by $\omega(d)x/d$, our only bound for the error in each term of (2.11) is $2^{\nu(d)}$ as given by (2.13). This is worse than the error bound of 1 per term in our analysis of $\pi(x)$. [Note that the number of terms in (2.8) and in (2.11) are the same.] If we nevertheless make the approximation $|\mathcal{A}(d)| \approx \omega(d)x/d$ in (2.11) we get

$$|\{q: q, q+2 \text{ are primes}, q \leqslant x-2\}| \approx \sum_{d|P(\sqrt{x})} \mu(d)\omega(d)x/d\,. \tag{2.18}$$

Using the fact that $\mu(d)\omega(d)/d$ is a multiplicative function of d, we have for any z that

$$\sum_{d|P(z)} \mu(d)\omega(d)/d = \prod_{p \leqslant z}\left(1 - \frac{\omega(p)}{p}\right). \tag{2.19}$$

Then, using Mertens' theorem (2.16) and the fact that $\omega(2) = 1$, and $\omega(p) = 2$ for $p > 2$, we have by an easy calculation that

$$\prod_{p \leqslant z}\left(1 - \frac{\omega(p)}{p}\right) \sim e^{-2\gamma}\alpha/\log^2 z \quad \text{as } z \to \infty\,, \tag{2.20}$$

where

$$\alpha = 2\prod_{p>2}[1 - (p-1)^{-2}] = 1.3202\ldots, \tag{2.21}$$

the so-called "twin prime constant". Putting (2.19) and (2.20) (with $z = \sqrt{x}$) into the heuristic approximation (2.18), we have the "conclusion" that the number of twin primes up to x is of order of magnitude $x/\log^2 x$ with the "suggestion" that the asymptotic constant is $4e^{-2\gamma}\alpha$. In fact, this is not far from the strong twin prime conjecture which asserts that the number of twin primes up to x is $(\alpha + o(1))x/\log^2 x$. That is, the above heuristic gives the conjectured order of magnitude, but not the conjectured constant.

In general, the above attempts at using a sieve lead us to the following thoughts. There is no hope of giving asymptotics for the number of integers left after the sifting process if we sieve by a "large" set of primes $\mathcal{P}$. On the other hand, one may hope to get good bounds for the number of these integers (even if $\mathcal{P}$ is "large") by some sort of refinement that reduces the number of terms in the sum $\sum_d \mu(d)|\mathcal{A}(d)|$.

V. Brun, working in the period 1915–1924 and at least in part basing his work

on that of J. Merlin, was the first to succeed in modifying the sieve of Eratosthenes to prove highly non-trivial results with a sieve. First we are going to discuss a relatively simple version of Brun's method which is called *Brun's simple* (or *pure*) *sieve*. As we shall see it enables one to derive estimates very close to the conjectured best possible one in a quite cheap way.

Brun's first idea is to reduce the number of terms in the sum $\sum_d \mu(d)|\mathscr{A}(d)|$ by reducing the number of sifting primes. The simplest way to do this is to replace the condition $p \leqslant \sqrt{x}$ in the definitions (2.4) and (2.10) of $\mathscr{P}$ by $p \leqslant z$, where z is a parameter much smaller than $\sqrt{x}$ whose exact value should be fixed as some function of x depending on the problem being studied. This means that, for example, in the case of the twin prime problem, we sift out only those integers n for which $n(n+2)$ has a small prime factor (i.e., at most z). Since the remaining integers include all the twin primes larger than z, in this way we get an upper bound for the number of twin primes between z and x. On the other hand we do not get any lower bound for this number. We might only hope to get a lower bound for the number of twin "almost primes" up to x, where q in an "almost prime" if it has no prime factor up to z. (Usually in sieve methods the term "almost prime" is reserved for the case when $\log z/\log x$ is bounded away from 0, so that if $q \leqslant x$ is an almost prime, it has a bounded number of prime factors. We do not follow this convention here.)

So let us now study the general sieve problem: given $\mathscr{A} \subset \mathbb{N}$ finite and

$$\mathscr{P} = \{p \text{ prime}: p \leqslant z\}, \tag{2.22}$$

estimate

$$S(\mathscr{A}, \mathscr{P}) := |\{n \in \mathscr{A}: (n, P(z)) = 1\}|, \tag{2.23}$$

where $P(z)$ is defined by (2.7). Then by using the inclusion–exclusion principle, we get in the now familiar way that

$$S(\mathscr{A}, \mathscr{P}) = \sum_{d|P(z)} \mu(d)|\mathscr{A}(d)|,$$

where $\mathscr{A}(d)$ is given by (2.1).

The inclusion–exclusion formula is based on the identity (2.6). This identity is only a special case of the following more general identity:

$$\sum_{k=0}^{j} (-1)^k \binom{l}{k} = (-1)^j \binom{l-1}{j} \quad \text{for all } j, l \in \mathbb{N}, \tag{2.24}$$

which can be proved easily by induction on j. This identity implies that the sum on the left-hand side is $\geqslant 0$ for even j and $\leqslant 0$ for odd j.

The second idea of Brun is to utilize this alternation of sign for the sum in (2.24). We are going to show that for every $t \in \mathbb{N}$ we have both

$$S(\mathscr{A}, \mathscr{P}) \leqslant \sum_{\substack{d|P(z) \\ \nu(d) \leqslant 2t}} \mu(d)|\mathscr{A}(d)| \tag{2.25}$$

and

$$S(\mathcal{A}, \mathcal{P}) \geqslant \sum_{\substack{d|P(z) \\ \nu(d)\leqslant 2t-1}} \mu(d)|\mathcal{A}(d)| \,. \tag{2.26}$$

To prove (2.25) we will show that if $n \in \mathcal{A}$, then the contribution of n to the right-hand side of (2.25) is

(a) 1 for $(n, P(z)) = 1$,

(b) $\geqslant 0$ for $(n, P(z)) > 1$.

The assertion (a) is trivial since if $n \in \mathcal{A}$ and $(n, P(z)) = 1$, then n is counted only in the term $d = 1$ with weight $\mu(1) = 1$. To show (b), write $(n, P(z)) = p_1 p_2 \cdots p_l$, so that $p_1, p_2, \ldots, p_l$ are distinct primes up to z and $l \geqslant 1$. Then n is counted on the right-hand side of (2.25) only for d's of the form

$$d = p_1' p_2' \cdots p_k' | p_1 p_2 \cdots p_l \,, \quad k \leqslant 2t \,.$$

For a fixed $k \leqslant 2t$, the number of these d's is $\binom{l}{k}$, and they get counted with weight $(-1)^k$. Thus the total contribution of n to the right-hand side of (2.25) is

$$\sum_{k=0}^{2t} (-1)^k \binom{l}{k} \,.$$

By (2.24), this sum is non-negative, which completes the proof of (b) and (2.25). In a similar way we can prove (2.26).

As an application of Brun's simple sieve we adapt (2.25) and (2.26) to the twin prime problem, getting a relatively sharp bound in a relatively simple way.

Theorem 2.27. *The number N of integers $n \leqslant x - 2$ such that both n and $n + 2$ are free of prime factors up to z satisfies*

$$N \sim \mathrm{e}^{-2\gamma} \alpha x / \log^2 z \,,$$

where α is the constant defined in (2.21), *and where the asymptotic relation holds as $x, z \to \infty$ in the region $z \leqslant x^{1/(20 \log\log x)}$.*

Thus Brun's simple sieve actually gives an asymptotic formula for the number of twin "almost primes" up to x. Moreover, by making the largest choice of z allowed, it gives a non-trivial upper estimate for the distribution of twin primes:

Corollary 2.28. *The number of primes $p \leqslant x$ with $p + 2$ also prime is* $O(x(\log\log x)^2 / \log^2 x)$. *In particular, the sum $\sum 1/p$ for primes p with $p + 2$ prime is either convergent or finite.*

The number $\sum 1/p$ described in the corollary is referred to as *Brun's constant*. Note that the O-estimate in the corollary is only off by a factor $(\log\log x)^2$ from the conjectured order of magnitude.

On the other hand, Theorem 2.27 does not give any lower bound for the

distribution of twin primes. We still do not know if there are infinitely many; as mentioned above, this is one of the great unsolved problems in mathematics. We have witnessed a general pattern with sieve methods: they often give good upper bounds, but no or weak lower bounds, unless one is interested in "almost primes" of some kind.

Proof of Theorem 2.27. Define $\mathscr{A}$ by (2.10), $\mathscr{P}$ by (2.22), and $S(\mathscr{A}, \mathscr{P})$ by (2.23). Then the quantity N in the theorem is just $S(\mathscr{A}, \mathscr{P})$. In view of (2.19) and (2.20) it is thus sufficient to prove

$$S(\mathscr{A}, \mathscr{P}) = x \sum_{d|P(z)} \mu(d)\omega(d)/d + o(x/\log^2 z) . \tag{2.29}$$

Note that from the upper bound and lower bound for $S(\mathscr{A}, \mathscr{P})$ given by (2.25) and (2.26), we have

$$S(\mathscr{A}, \mathscr{P}) = \sum_{\substack{d|P(z) \\ \nu(d)\leqslant 2t}} \mu(d)|\mathscr{A}(d)| + O\left(\sum_{\substack{d|P(z) \\ \nu(d)=2t}} |\mathscr{A}(d)|\right)$$

for any choice of $t \in \mathbb{N}$. Thus by (2.13) we have

$$\begin{aligned} S(\mathscr{A}, \mathscr{P}) &= x \sum_{\substack{d|P(z) \\ \nu(d)\leqslant 2t}} \mu(d)\frac{\omega(d)}{d} + O\left(x \sum_{\substack{d|P(z) \\ \nu(d)=2t}} \frac{\omega(d)}{d}\right) + O\left(\sum_{\substack{d|P(z) \\ \nu(d)\leqslant 2t}} 2^{\nu(d)}\right) \\ &= x \sum_{d|P(z)} \mu(d)\frac{\omega(d)}{d} + O\left(x \sum_{\substack{d|P(z) \\ \nu(d)\geqslant 2t}} \frac{\omega(d)}{d}\right) + O\left(\sum_{\substack{d|P(z) \\ \nu(d)\leqslant 2t}} 2^{\nu(d)}\right) \\ &= x \sum_{d|P(z)} \mu(d)\frac{\omega(d)}{d} + O(E_1) + O(E_2) , \end{aligned} \tag{2.30}$$

say.

We shall show that E_1, E_2 are $O(x/\log^6 z)$, $O(x^{1/2})$, respectively, if we choose

$$t = \lfloor 5 \log\log z \rfloor$$

(and z large enough so that $t \geqslant 1$). Thus (2.30) will imply a strong version of (2.29) and thus prove the theorem.

To estimate E_1, we use a weak form of Mertens' theorem. In fact, by taking the logarithm of (2.16), we have

$$\sum_{p\leqslant z} \frac{1}{p} \leqslant \log\log z + c$$

for some constant c and all large z. (This inequality is actually a weak form of a much older theorem of Euler.) Thus using $\omega(d) \leqslant 2^{\nu(d)}$ and the multinomial

theorem,

$$E_1 = x \sum_{\substack{d \mid P(z) \\ \nu(d) \geqslant 2t}} \frac{\omega(d)}{d} \leqslant x \sum_{l \geqslant 2t} 2^l \sum_{\substack{d \mid P(z) \\ \nu(d) = l}} \frac{1}{d}$$

$$\leqslant x \sum_{l \geqslant 2t} \frac{2^l}{l!} \left(\sum_{p \leqslant z} \frac{1}{p} \right)^l \leqslant x \sum_{l \geqslant 2t} \frac{1}{l!} (2 \log\log z + 2c)^l .$$

The terms in this last sum are decaying at least geometrically with a common ratio bounded below 1, so that the sum is majorized by its first term. Thus

$$E_1 = O\left(\frac{x}{[2t]!} [2 \log\log z + 2c]^{2t} \right) = O\left(x \left[\frac{2e \log\log z + 2ce}{2t} \right]^{2t} \right)$$

$$= O(x(\tfrac{1}{5}e)^{10 \log\log z}) = O(x/\log^6 z) .$$

The majorization of E_2 is easier. We have

$$E_2 = \sum_{\substack{d \mid P(z) \\ \nu(d) \leqslant 2t}} 2^{\nu(d)} \leqslant 2^{2t} \sum_{\substack{d \mid P(z) \\ \nu(d) \leqslant 2t}} 1 = 2^{2t} \sum_{l=0}^{2t} \binom{\pi(z)}{l} \leqslant 2^{2t} \pi(z)^{2t} .$$

For large z, we have $\pi(z) \leqslant \frac{1}{2} z$ (in fact, $z \geqslant 8$ will do), so that

$$E_2 \leqslant z^{2t} = O(x^{1/2}) .$$

This estimate concludes our proof of Theorem 2.27. □

To eliminate the unwanted $(\log\log x)^2$ factor in Corollary 2.28, one needs *Brun's sieve* in its complete form. To explain the crucial idea of Brun's sieve we start out from the inequalities (2.25) and (2.26). These inequalities can be rewritten in the form

$$\sum_{d \mid P(z)} \chi_1(d) \mu(d) |\mathcal{A}(d)| \leqslant S(\mathcal{A}, \mathcal{P}) \leqslant \sum_{d \mid P(z)} \chi_2(d) \mu(d) |\mathcal{A}(d)| , \tag{2.31}$$

where

$$\chi_1(d) = \begin{cases} 1 & \text{for } \nu(d) \leqslant 2t-1 \\ 0 & \text{for } \nu(d) > 2t-1 , \end{cases}$$

$$\chi_2(d) = \begin{cases} 1 & \text{for } \nu(d) \leqslant 2t , \\ 0 & \text{for } \nu(d) > 2t . \end{cases} \tag{2.32}$$

The idea is to replace these two functions by certain other functions $\chi_1(d)$, $\chi_2(d)$ with the following properties:

(a) $\chi_1(d)$, $\chi_2(d)$ satisfy (2.31),

(b) $\chi_1(1) = \chi_2(1) = 1$,

(c) $\chi_i(d) = 0$ or 1 if $d \mid P(z)$ for $i = 1, 2$.

The goal is to make the choice for χ_1, χ_2 so that we get better upper and lower bound estimates than that afforded by (2.32).

Brun succeeded in constructing functions $\chi_1(d)$, $\chi_2(d)$ with all these properties and giving very good estimates for $S(\mathscr{A}, \mathscr{P})$. The construction is too complicated to describe here; see, e.g., Halberstam and Richert (1974) for further details.

We now cite one general theorem that may be proved by Brun's sieve – it is a special case of Theorem 2.3 in Halberstam and Richert (1974).

Theorem 2.33. *Let $k \in \mathbb{N}$, let a_i, b_i be pairs of integers for $i = 1, \ldots, k$ such that each $(a_i, b_i) = 1$ and*

$$E = \left(\prod_{i=1}^{k} a_i\right)\left(\prod_{1 \leqslant r < s \leqslant k} (a_r b_s - a_s b_r)\right) \neq 0 .$$

Let $1 > \varepsilon > 0$, x, $y \in \mathbb{R}$ be arbitrary with $2 \leqslant y \leqslant x$, and let $z = y^{\varepsilon}$. Let

$$\mathscr{A} = \left\{\prod_{i=1}^{k} (a_i n + b_i) : n \in \mathbb{N}, x - y < n \leqslant x\right\} \tag{2.34}$$

and denote the number of solutions of $\prod_{i=1}^{k} (a_i n + b_i) \equiv 0 \pmod{p}$ by $\omega(p)$ for each prime p. Then if $\mathscr{P} = \{p \text{ prime}: p \leqslant z\}$,

$$S(\mathscr{A}, \mathscr{P}) \leqslant c\left(\prod_{\substack{p \mid E \\ p \leqslant y}} \left(1 - \frac{1}{p}\right)^{\omega(p)-k}\right)\frac{y}{\log^k y},$$

where the constant c depends only on k and ε.

Note that all of the sets $\mathscr{A}$ as in (2.2), (2.10), and (2.14) are of the form (2.34). For example, by choosing $k = 2$, $a_1 = 1$, $b_1 = 0$, $a_2 = 1$, $b_2 = 2$, $y = x$, and $z = \sqrt{x}$ we obtain:

Corollary 2.35. *There is a positive constant c such that if $x \geqslant 2$, then*

$$|\{q: q, q+2 \text{ are primes}, q \leqslant x - 2\}| \leqslant c\frac{x}{\log^2 x} .$$

Similarly, if we let $k = 2$, $a_1 = 1$, $b_1 = 0$, $a_2 = -1$, $b_2 = n$, $x = y = n$, and $z = \sqrt{n}$, we get:

Corollary 2.36. *There is a positive constant c such that if $n \in \mathbb{N}$ and n is even, then*

$$|\{p: p \text{ and } n - p \text{ are primes}\}| \leqslant c\left(\prod_{p \mid n}\left(1 - \frac{1}{p}\right)^{-1}\right)\frac{n}{\log^2 n} .$$

Even for the simpler problem (i) where the prime number theorem gives us an asymptotic formula for $\pi(x)$, Theorem 2.33 can tell us something non-trivial when

y is small compared to x. By choosing $k=1$, $a_1=1$, and $b_1=0$, we have the following result originally due to Hardy and Littlewood.

Corollary 2.37. *If $2 \leqslant y \leqslant x$, there is an absolute constant c such that*

$$\pi(x) - \pi(x-y) \leqslant c\frac{y}{\log y}.$$

Brun's sieve has numerous applications and many of these are due to P. Erdős who, perhaps more than any other person, showed that sieve methods are indeed a powerful tool in number theory. For example, Erdős used Brun's sieve to estimate the differences between the consecutive primes. Let p_i denote the ith prime (so that $p_1=2$, $p_2=3$, $p_3=5$, etc.), write $d_n = p_n - p_{n-1}$ for $n>1$, and let $d_1=2$. It follows easily from the prime number theorem that

$$\liminf_{n\to\infty} d_n/\log n \leqslant 1.$$

We now prove the following result due to Erdős (1940).

Theorem 2.38. *There is a constant $c<1$ such that*

$$\liminf_{n\to\infty} d_n/\log n \leqslant c. \tag{2.39}$$

Proof. Let $\varepsilon>0$ be arbitrary, but fixed. Suppose that

$$\liminf_{n\to\infty} d_n/\log n > 1-\tfrac{1}{2}\varepsilon. \tag{2.40}$$

Then there is some x_0 such that for $x \geqslant x_0$, if $n > \pi(x/\log x)$ we have $d_n > (1-\varepsilon)\log x$. Let $L = \pi(x) - \pi(x/\log x)$ and assume $\delta = \delta(x,\varepsilon)$ is such that there are exactly δL values of n with $\pi(x/\log x) < n \leqslant \pi(x)$ and d_n is between $(1-\varepsilon)\log x$ and $(1+\varepsilon)\log x$. Then for $x \geqslant x_0$, there are $(1-\delta)L$ values of n in this range with $d_n \geqslant (1+\varepsilon)\log x$. Thus

$$\delta L(1-\varepsilon)\log x + (1-\delta)L(1+\varepsilon)\log x \leqslant \sum_{n\leqslant\pi(x)} d_n \leqslant x,$$

so that

$$\varepsilon(1-2\delta) \leqslant \frac{x}{L\log x} - 1. \tag{2.41}$$

By the prime number theorem, $L\log x = (1+o(1))x$, so that (2.41) implies (since $\varepsilon>0$ is fixed) there is some $x_1(\varepsilon)$ such that if $x \geqslant x_1(\varepsilon)$ we have $\delta > \frac{1}{3}$.

We now use Theorem 2.33 to show that $\delta = O(\varepsilon)$ so that if ε is sufficiently small, (2.40) cannot hold. This will prove the theorem. For any $t \in \mathbb{N}$, let $D(t,x)$ denote the number of primes $p \leqslant x$ with $p+t$ prime. Thus

$$\delta L \leqslant \sum_{(1-\varepsilon)\log x < t < (1+\varepsilon)\log x} D(t,x). \tag{2.42}$$

But by Theorem 2.33 with $k=2$, $a_1=1$, $b_1=0$, $a_2=1$, $b_2=t$, $y=x$, and $z=\sqrt{x}$,

we have some absolute constant c' with

$$D(t,x) \leqslant c'\left(\prod_{\substack{p\mid t\\ p\leqslant x}}\left(1-\frac{1}{p}\right)^{-1}\right)\frac{x}{\log^2 x}. \tag{2.43}$$

From elementary arguments it is not difficult to prove that

$$\sum_{t\leqslant u}\prod_{p\mid t}\left(1-\frac{1}{p}\right)^{-1} \sim c''u \quad \text{as } u\to\infty$$

for some constant c''. Thus

$$\sum_{(1-\varepsilon)\log x<t<(1+\varepsilon)\log x} D(t,x) \leqslant c'(c''+o(1))2\varepsilon \log x \frac{x}{\log^2 x}.$$

Since $L\sim x/\log x$, (2.42) thus implies for $x\geqslant x_2(\varepsilon)$

$$\delta \leqslant 3c'c''\varepsilon,$$

which is what we wanted to prove. □

Since 1942, the value of the constant c in (2.39) has been improved by several authors. The best estimate (derived by both combinatorial and analytic tools) has $c<\frac{1}{4}$ and is due to Maier (1988). Of course the twin prime conjecture implies that $c=0$.

Theorem 2.33 can be proved also by another sieve method of less combinatorial nature which is due to A. Selberg. In some applications, Selberg's sieve is slightly superior to Brun's.

Returning to the three problems at the beginning of this section, note that in problem (i) we counted integers $n\not\equiv 0 \pmod p$ for primes $p\leqslant z$, in problem (ii) we counted integers satisfying $n\not\equiv 0 \pmod p$ and $n\not\equiv 2 \pmod p$, and in problem (iii) the excluded classes were $n\not\equiv 0 \pmod p$, $n\not\equiv x \pmod p$. In other words, there are 1, 2 and 2 "forbidden" residue classes, respectively. Brun's sieve and Selberg's sieve have a common feature: both methods can be used only in the case that the number of forbidden residue classes is bounded or it grows only very slowly in terms of p. If the number of forbidden residue classes grows rapidly (for example, more than cp residue classes for each p), then other sieve methods must be used. The most important sieve method of this type is the *large sieve* of Linnik and Rényi.

See Halberstam and Richert (1974) for detailed discussion of "small sieves" (Brun's and Selberg's sieves) and Montgomery (1971) for the large sieve. The former reference also contains proofs of J. Chen's remarkable theorems that (1) there are infinitely many primes p such that $p+2$ is either prime or the product of two primes, and (2) every sufficiently large even number is the sum of a prime and another number which is either prime or the product of two primes.

Finally we mention Rosser's sieve, a general principle for a combinatorial small

sieve. Iwaniec (1981) has done extensive work developing this general principle and has given details for some important special cases.

3. Bases and density theorems on addition of sets

As mentioned in the preceding section, it is conjectured that every even number exceeding 2 is a sum of two primes. This conjecture, which was stated by Goldbach in a letter to Euler in 1742, has the immediate corollary that *every* number exceeding 5 is a sum of three primes and that every number exceeding 1 is a sum of at most three primes.

In 1770, Waring stated without proof that for every n there is some number $g(n)$ such that every natural number is the sum of at most $g(n)$ positive nth powers. In that same year, Lagrange solved Waring's problem for $n=2$, showing that every natural number is the sum of at most four squares. In 1909, Waring's conjecture was finally proved by Hilbert using a combinatorial argument.

Let $\mathbb{N}_0=\mathbb{N}\cup\{0\}$ denote the set of non-negative integers. A set $\mathcal{A}\subseteq\mathbb{N}_0$ is said to be a *basis of order* k if every natural number can be represented as the sum of at most k elements of $\mathcal{A}$. If every sufficiently large integer can be represented as the sum of at most k elements of $\mathcal{A}$, then $\mathcal{A}$ is said to be an *asymptotic basis of order* k. Thus Goldbach's conjecture implies that the set of primes is an asymptotic basis of order 3 and that the set of primes together with 1 is a basis of order 3. Not only has Waring's problem been settled, the minimal choices for the numbers $g(n)$ are "known" for every n. If $G(n)$ is the least number such that the positive nth powers form an asymptotic basis of order $G(n)$, then *no* value of $G(n)$ is known except for $n=1$, 2, and 4. See Vaughan (1981) and Balasubramanian et al. (1986) for more details.

If $\mathcal{A}\subseteq\mathbb{N}_0$, then the *lower asymptotic density* $\underline{d}(\mathcal{A})$, the *upper asymptotic density* $\overline{d}(\mathcal{A})$, and, if it exists, the *asymptotic density* $d(\mathcal{A})$ of $\mathcal{A}$ are defined by:

$$\underline{d}(\mathcal{A})=\liminf_{n\to\infty} A(n)/n\,,$$

$$\overline{d}(\mathcal{A})=\limsup_{n\to\infty} A(n)/n\,,$$

$$d(\mathcal{A})=\lim_{n\to\infty} A(n)/n\,,$$

respectively.

Assuming the Riemann hypothesis, Hardy and Littlewood proved in 1922 that every sufficiently large odd integer can be represented as the sum of three primes, which would imply, of course, that the set of primes is an asymptotic basis of order 4. The Hardy and Littlewood theorem was proved unconditionally in 1937 by Vinogradov. But the first to unconditionally prove that the set of primes is an asymptotic basis of some finite order was Schnirelmann in 1930.

This work of Schnirelmann opened up an important chapter in combinatorial number theory. His starting point was the following simple corollary of Brun's sieve and, in particular, Theorem 2.33.

Corollary 3.1. *The set of integers which can be represented as the sum of two primes has positive lower asymptotic density. That is, if $\mathscr{P}$ denotes the set of primes, then $\underline{d}(2\mathscr{P})>0$.*

Thus to prove that $\mathscr{P}$ is an asymptotic basis of finite order, it would be sufficient to show that any set of positive lower asymptotic density must necessarily be an asymptotic basis of finite order. Unfortunately, this is not so, as the set

$$\mathscr{A}=\{0,2,4,\ldots\} \tag{3.2}$$

of even non-negative integers show. This set has asymptotic density $\frac{1}{2}$, but no odd integer is a sum of members of $\mathscr{A}$.

However, Schnirelmann was able to save this idea with his concept of *Schnirelmann density*. If $\mathscr{A}\subseteq\mathbb{N}_0$ and we write $A^*(n)$ for the number of *positive* members of $\mathscr{A}$ up to n, then the Schnirelmann density $\sigma(\mathscr{A})$ of $\mathscr{A}$ is defined by:

$$\sigma(\mathscr{A})=\inf_{n\in\mathbb{N}} A^*(n)/n\,.$$

Thus $\sigma(\mathscr{A})>0$ holds if and only if both $1\in\mathscr{A}$ and $\underline{d}(\mathscr{A})>0$ hold. In addition, $\sigma(\mathscr{A})=1$ if and only if $\mathscr{A}=\mathbb{N}$ or $\mathbb{N}_0$. Schnirelmann proved the following theorems on the Schnirelmann density of sum sets.

Theorem 3.3. *If $\mathscr{A}$, $\mathscr{B}\subseteq\mathbb{N}_0$ with $0\in\mathscr{A}\cap\mathscr{B}$, then*

$$\sigma(\mathscr{A}+\mathscr{B})\geqslant\sigma(\mathscr{A})+\sigma(\mathscr{B})-\sigma(\mathscr{A})\sigma(\mathscr{B})\,.$$

Proof. We may assume $\sigma(\mathscr{A})>0$. Let n be an arbitrary natural number and suppose

$$1=a_1<a_2<\cdots<a_k\leqslant n$$

are the positive members of $\mathscr{A}$ that do not exceed n. Since $0\in\mathscr{B}$, we have also $a_1,\ldots,a_k\in\mathscr{A}+\mathscr{B}$. What other members in $\mathscr{A}+\mathscr{B}$ do not exceed n? We now count those members of $\mathscr{A}+\mathscr{B}$ of the form a_i+b, where $i<k$, $b\in\mathscr{B}$, and $a_i<a_i+b<a_{i+1}$. This number is $B^*(a_{i+1}-a_i-1)\geqslant(a_{i+1}-a_i-1)\sigma(\mathscr{B})$. Similarly the number of a_k+b, where $b\in\mathscr{B}$ and $a_k<a_k+b\leqslant n$, is $B^*(n-a_k)\geqslant(n-a_k)\sigma(\mathscr{B})$. Thus the number of positive members of $\mathscr{A}+\mathscr{B}$ up to n is at least

$$\begin{aligned}
&A^*(n)+(n-a_k)\sigma(\mathscr{B})+\sum_{i<k}(a_{i+1}-a_i-1)\sigma(\mathscr{B})\\
&\quad=A^*(n)+(n-a_1-k+1)\sigma(\mathscr{B})\\
&\quad=A^*(n)+(n-A^*(n))\sigma(\mathscr{B})\\
&\quad=(1-\sigma(\mathscr{B}))A^*(n)+n\sigma(\mathscr{B})\\
&\quad\geqslant n(1-\sigma(\mathscr{B}))\sigma(\mathscr{A})+n\sigma(\mathscr{B})\,,
\end{aligned}$$

which proves the theorem. □

Theorem 3.4. *If* $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}_0$ *with* $0 \in \mathcal{A} \cap \mathcal{B}$ *and* $\sigma(\mathcal{A}) + \sigma(\mathcal{B}) \geq 1$, *then* $\sigma(\mathcal{A} + \mathcal{B}) = 1$. *That is, every non-negative integer can be represented in the form* $a + b$ *with* $a \in \mathcal{A}$, *and* $b \in \mathcal{B}$.

Proof. If $n \in \mathcal{A} \cup \mathcal{B}$, then $n \in \mathcal{A} + \mathcal{B}$. So suppose $n \in \mathbb{N}_0$ and $n \notin \mathcal{A} \cup \mathcal{B}$. Then $n > 1$. We have

$$n \leq A^*(n) + B^*(n) = A^*(n-1) + B^*(n-1) .$$

Consider the positive integers $a \in \mathcal{A}$ for $a < n$, and $n - b$ for $b \in \mathcal{B}$, $0 < b < n$. There are at least n of these numbers and they all lie in $\{1, 2, \ldots, n-1\}$. Thus we have $a = n - b$ for some $a \in \mathcal{A}$, $b \in \mathcal{B}$, so that $n = a + b \in \mathcal{A} + \mathcal{B}$. □

Corollary 3.5. *If* $\mathcal{A} \subseteq \mathbb{N}_0$ *with* $\sigma(\mathcal{A}) > 0$, *then* $\mathcal{A}$ *is a basis of some finite order.*

Proof. Write $\mathcal{A}_0 = \mathcal{A} \cup \{0\}$. Then by Theorem 3.3 and induction, $\sigma(k\mathcal{A}_0) \geq 1 - (1 - \sigma(\mathcal{A}_0))^k$ for every $k \in \mathbb{N}$. Thus there is some k with $\sigma(k\mathcal{A}_0) \geq \frac{1}{2}$. Thus by Theorem 3.4, with $\mathcal{A} = \mathcal{B} = k\mathcal{A}_0$, we have $2k\mathcal{A}_0 = \mathbb{N} \cup \{0\}$. Thus $\mathcal{A}$ is a basis of order $2k$. □

Schnirelmann's theorem on the set of primes $\mathcal{P}$ follows easily from Corollaries 3.1 and 3.5 as we now see.

Theorem 3.6. *The set of primes is an asymptotic basis of finite order.*

Proof. Write $\mathcal{P}_1 = \mathcal{P} \cup \{0, 1\}$. Then by Corollary 3.1, $\sigma(2\mathcal{P}_1) > 0$, so that by Corollary 3.5, $2\mathcal{P}_1$ is a basis of some finite order. Thus $\mathcal{P}_1$ is a basis of some order k. Thus every $n \in \mathbb{N}$ may be represented in the form $s + v$, where s is a sum of at most k primes and $0 \leq v \leq k$.

We now show that every $n > 2$ may be represented as a sum of at most $\frac{3}{2}k + 1$ primes. Indeed, $n - 2 \in \mathbb{N}$, so we may write $n - 2 = s + v$, where s is a sum of at most k primes and $0 \leq v \leq k$. Then $n = s + (v + 2)$ and $2 \leq v + 2 \leq k + 2$. But it is trivial that every integer $m \geq 2$ can be represented as a sum of 2's and 3's with at most $\frac{1}{2}m$ summands. Thus $v + 2$ is a sum of at most $\frac{1}{2}(k + 2)$ primes, each prime being 2 or 3. Thus $n = s + (v + 2)$ is a sum of at most $\frac{3}{2}k + 1$ primes. □

In 1942, Mann improved on Schnirelmann's theorems 3.3 and 3.4 by proving the following result which had come to be known as the $\alpha + \beta$ conjecture.

Theorem 3.7. *If* $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}_0$ *with* $0 \in \mathcal{A} \cap \mathcal{B}$, *then* $\sigma(\mathcal{A} + \mathcal{B}) \geq \min\{1, \sigma(\mathcal{A}) + \sigma(\mathcal{B})\}$.

Thus in the case $\sigma(\mathcal{A}) > 0$, $\sigma(\mathcal{B}) > 0$, and $\sigma(\mathcal{A}) + \sigma(\mathcal{B}) < 1$, Theorem 3.7 gives a sharper result than Theorems 3.3 and 3.4. As we saw above, these latter

theorems can be proved relatively easily. However, Mann's theorem 3.7 is much deeper.

A disadvantage of Schnirelmann's and Mann's theorems is that in both cases, the statement is formulated in terms of Schnirelmann density which is a fairly artificial concept. In particular, if we use these results for estimating the order of a basis, then we often get rather poor estimates. Thus in many applications it would be preferable to have an addition theorem involving asymptotic (lower) density. In 1953, Kneser proved the following (very deep) theorem.

Theorem 3.8. *If $\mathcal{A}_0, \dots, \mathcal{A}_k \subseteq \mathbb{N}_0$ are infinite, then either*

$$\underline{d}(\mathcal{A}_0 + \cdots + \mathcal{A}_k) \geqslant \liminf_{n\to\infty} (A_0(n) + \cdots + A_k(n))/n$$

or there are natural numbers $g, a_0, \dots, a_k$, such that

(i) *each $\mathcal{A}_i$ is contained in the union $\mathcal{A}_i'$ of a_i distinct congruence classes* (mod g),

(ii) *there are at most finitely many positive members of $\mathcal{A}_0' + \cdots + \mathcal{A}_k'$ not in $\mathcal{A}_0 + \cdots + \mathcal{A}_k$,*

(iii) $d(\mathcal{A}_0 + \cdots + A_k) \geqslant (a_0 + \cdots + a_k - k)/g$.

The following result of Nathanson and Sárközy (1989) gives a particularly simple application of Kneser's theorem 3.8.

Theorem 3.9. *If $\mathcal{A} \subseteq \mathbb{N}$ is an asymptotic basis of order h and if $\underline{d}(\mathcal{A}) > 1/h$, then for every β with $1/h < \beta < \underline{d}(\mathcal{A})$, there is a set $\mathcal{B} \subset \mathcal{A}$ with $\underline{d}(\mathcal{B}) = \beta$ and with $\mathcal{B}$ also an asymptotic basis of order h.*

Proof. Let $\mathcal{A}$ be as described and choose β with $1/h < \beta < \underline{d}(\mathcal{A})$. Let $\mathcal{C}$ be any subset of $\mathcal{A}$ with $\underline{d}(\mathcal{C}) = \beta$. Let $H = (h-1)/(h\beta - 1)$ and let $\mathcal{A}_0 \subset \mathcal{A}$ be a finite set such that for each $j \leqslant H$, $\mathcal{A}_0$ contains a representative of each residue class (mod j) that has at least one representative in $\mathcal{A}$. We claim that $\mathcal{B} = \mathcal{C} \cup \mathcal{A}_0$ fulfills the conditions of the theorem.

First, it is clear that $\underline{d}(\mathcal{B}) = \beta$, since $\mathcal{A}_0$ is finite. To show $\mathcal{B}$ is an asymptotic basis of order h, we apply Kneser's theorem 3.8 with h copies of $\mathcal{B}$. Since $\underline{d}(\mathcal{B}) > 1/h$, the first condition cannot hold. Thus there is some number g and a set $\mathcal{B}'$ of a residue classes (mod g) such that $\mathcal{B} \subseteq \mathcal{B}'$, all sufficiently large members of $h\mathcal{B}'$ are in $h\mathcal{B}$, and

$$1 \geqslant d(h\mathcal{B}) \geqslant \frac{ha - (h-1)}{g} \geqslant h\beta - \frac{h-1}{g}.$$

Thus $g \leqslant H$, so that $\mathcal{B}$ contains representatives of exactly the same residue classes (mod g) as does $\mathcal{A}$. Since $\mathcal{B} \subseteq \mathcal{B}'$ and $\mathcal{B}'$ is a union of complete residue classes (mod g), we have $\mathcal{A} \subseteq \mathcal{B}'$. Thus $\mathcal{B}'$ is an asymptotic basis of order h, as is $\mathcal{B}$. □

Kneser's theorem 3.8 serves a unifying role in additive number theory in that certain prior results with longer proofs can also be seen as fairly immediate corollaries of Theorem 3.8. For example, it is possible to prove via Schnirelmann's theorem 3.3 that if $\mathcal{A} \subseteq \mathbb{N}$, $\underline{d}(\mathcal{A}) > 0$, and $\mathcal{A}$ contains a finite subset that is relatively prime, then $\mathcal{A}$ is an asymptotic basis of some order – this is essentially what is done in the proof of Theorem 3.6. But assuming Kneser's theorem, the result is virtually immediate.

As one further example, we state the following corollary of Kneser's theorem, leaving the proof for the reader. [The proof is not completely trivial – for help, consult Halberstam and Roth (1983, pp. 54–55).] Parts of this result are due independently to Cauchy in 1813, Davenport in 1935, and I. Chowla in 1935. It is also possible to give a (relatively simple) direct proof, not using Kneser's theorem.

Theorem 3.10. (The Cauchy–Davenport–Chowla Theorem). *If $\mathcal{A}$, $\mathcal{B} \subseteq \mathbb{Z}/g$ with $|\mathcal{A}| = r$, $|\mathcal{B}| = s$, $0 \in \mathcal{B}$, and every other member of $\mathcal{B}$ is coprime to g, then $|\mathcal{A} + \mathcal{B}| \geq \min\{g, r + s - 1\}$.*

When we are studying a finite set $\mathcal{A} \subseteq \mathbb{N}$ and we need an addition theorem, then the only assumption that one might like to use is that $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ and $|\mathcal{A}|/N$ is large. Improving on a joint theorem with Nathanson, Sárközy has recently proved the following addition theorem of this type, see Sárközy (1989/1994).

Theorem 3.11. *Assume that $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ and that $|\mathcal{A}| > (N/k) + 1$, where $k \in \mathbb{N}$. Then there are d, $l \in \mathbb{N}$ with $d < k$, $l < 118/k$ such that $l\mathcal{A}$ contains an N-term arithmetic progression of multiples of d.*

Bourgain (1990) and Freiman et al. (1992) have recently shown that if $\mathcal{A}$ is "dense", then there are "long" arithmetic progressions in $2\mathcal{A}$ and considerably longer ones in $3\mathcal{A}$.

Using exponential sums and methods from the geometry of numbers, Freiman (1973) gave a deep analysis of the structure of sum sets of the form $k\mathcal{A}$ for finite sets $\mathcal{A}$ assuming that $|k\mathcal{A}|$ is not much greater than $|\mathcal{A}|$. Indeed, suppose $k_1, \ldots, k_d$ are integers at least 2, $u, v_1, \ldots, v_d$ are integers, and there are $k_1 \cdots k_d$ distinct integers of the form

$$n = u + \sum_{i=1}^{d} x_i v_i \quad \text{where } x_i \in \{1, \ldots, k_i\} \text{ for } i = 1, \ldots, d\,.$$

Then the set $\mathcal{P}$ of such numbers n is called a d-dimensional arithmetic progression of size $|\mathcal{P}| = k_1 \cdots k_d$. Freiman's most important result, the so-called "doubling theorem", says that if $|2\mathcal{A}|$ is not much greater than $|\mathcal{A}|$, then $|\mathcal{A}|$ can be well-covered by a generalized arithmetic progression:

Theorem 3.12. *For all $\alpha > 1$ there are constants $c_1 = c_1(\alpha)$, $c_2 = c_2(\alpha)$ such that if $|2\mathcal{A}| < \alpha|\mathcal{A}|$, then there is a generalized arithmetic progression $\mathcal{P}$ of dimension $d < c_1$ with $\mathcal{A} \subseteq \mathcal{P}$ and $|\mathcal{P}| < c_2|\mathcal{A}|$.*

Many further details, results, and problems on addition theorems and bases can be found in Halberstam and Roth (1983), Stöhr (1955), and Ostmann (1956).

A set $\mathcal{A} \subseteq \mathbb{N}_0$ is said to be a *minimal basis of order k* if $\mathcal{A}$ is a basis of order k, but no proper subset of $\mathcal{A}$ is a basis of order k. A set $\mathcal{A} \subseteq \mathbb{N}_0$ is said to be a *maximal nonbasis of order k* if $\mathcal{A}$ is not a basis of order k, but $A \cup \{a\}$ is a basis of order k for every $a \in \mathbb{N}_0 \setminus \mathcal{A}$. Stöhr, Härtter, Erdős, Nathanson and others have studied properties of minimal bases and maximal nonbases, see Stöhr (1955), Erdős and Nathanson (1987) and Nathanson (1989).

Similarly one can define the concept of a minimal asymptotic basis or maximal asymptotic nonbasis. Note that an immediate corollary of Theorem 3.9 is that if $\mathcal{A}$ is a minimal asymptotic basis of order h, then $\underline{d}(\mathcal{A}) \leqslant 1/h$. That this result is sharp is shown in Erdős and Nathanson (1988).

If $\mathcal{B} \subseteq \mathbb{N}_0$ is such that

$$\mathcal{A} \subseteq \mathbb{N}_0 \text{ and } 0 < \sigma(\mathcal{A}) < 1 \text{ imply } \sigma(\mathcal{A} + \mathcal{B}) > \sigma(\mathcal{A}),$$

then $\mathcal{B}$ is said to be an *essential component*. In 1933, Khintchin proved that the set of squares is an essential component. In 1936, Erdős generalized this theorem as follows by proving that every basis is an essential component.

Theorem 3.13. *If $\mathcal{B} \subseteq \mathbb{N}_0$ is a basis of order h and $\mathcal{A} \subseteq \mathbb{N}_0$ is arbitrary, then*

$$\sigma(\mathcal{A} + \mathcal{B}) \geqslant \sigma(\mathcal{A}) + \frac{1}{2h}(1 - \sigma(\mathcal{A}))\sigma(\mathcal{A}).$$

Landau slightly sharpened this result. Using a complicated graph-theoretic argument, Plünnecke improved the conclusion of Theorem 3.13 to the much sharper $\sigma(\mathcal{A} + \mathcal{B}) \geqslant \sigma(\mathcal{A})^{1-1/h}$. Ruzsa (1990/91) analyzed Plünnecke's method and gave further applications.

In 1942, Linnik proved the existence of a "thin" essential component $\mathcal{B}$ with

$$B(x) < \exp[(\log x)^{9/10+\varepsilon}].$$

This shows that an essential component need not be a basis. Wirsing improved on this estimate and Ruzsa (1987), using exponential sums, proved the following theorem (which settles the problem).

Theorem 3.14. *For every $\varepsilon > 0$ there is an essential component $\mathcal{B}$ with $B(x) = O((\log x)^{1+\varepsilon})$. Moreover, if $\mathcal{B}$ is any essential component, then there is some $c > 0$ such that $B(x) > (\log x)^{1+c}$ for all sufficiently large x.*

It is not known if $\mathcal{B} = \{2^i 3^j : i, j \in \mathbb{N}_0\}$ is an essential component. Note that $B(x) \sim c \log^2 x$ for some $c > 0$.

4. Other additive problems

4.1. Sidon sets

As before, let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. If $\mathcal{A} \subseteq \mathbb{N}_0$, let $s(\mathcal{A}, n)$ denote the number of solutions of

$$a + a' = n \quad \text{with } a, a' \in \mathcal{A}\ ,\ a \leqslant a'\ .$$

In 1931, S. Sidon posed the following two problems:

(i) How "dense" can $\mathcal{A}$ be if $s(\mathcal{A}, n) \leqslant 1$ for all n?

(ii) What is the slowest growing function $f(n)$ such that for some $\mathcal{A}$, $1 \leqslant s(\mathcal{A}, n) \leqslant f(n)$ holds for all $n \in \mathbb{N}_0$?

The first question motivates the following definition. If a set $\mathcal{A} \subseteq \mathbb{N}_0$ satisfies $s(\mathcal{A}, n) \leqslant 1$ for all n, then it is called a *Sidon set*. The first remarkable fact about Sidon sets is that the greedy algorithm provides a simple way to show the existence of relatively dense, finite Sidon sets.

Theorem 4.1. *If $N \in \mathbb{N}$, then there is a Sidon set $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ with $|\mathcal{A}| \geqslant [N^{1/3}]$.*

Proof. Clearly it suffices to show that if $\{a_1, a_2, \ldots, a_t\} \subseteq \{1, 2, \ldots, N\}$ is a Sidon set of cardinality t and

$$t \leqslant N^{1/3} - 1\ , \tag{4.2}$$

then there is an integer b such that

$$1 \leqslant b \leqslant N\ , \qquad b \notin \{a_1, a_2, \ldots, a_t\}\ , \tag{4.3}$$

and

$$\{a_1, a_2, \ldots, a_t\} \cup \{b\} \text{ is a Sidon set}\ . \tag{4.4}$$

To show this, note that if an integer b satisfying (4.3) does not satisfy (4.4), then there are a_i, a_j, a_k with

$$a_i + b = a_j + a_k\ ,$$

or there are a_u, a_v with

$$b + b = a_u + a_v\ .$$

There are at most t^3 choices for triples a_i, a_j, a_k and at most t^2 choices for pairs a_u, a_v, so there are at most $t^3 + t^2$ "bad" b's. Thus in view of (4.2), the number of "good" b's satisfying (4.3) and (4.4) is at least

$$N - t - (t^3 + t^2) \geqslant N - (t+1)^3 + 1 \geqslant 1\ ,$$

so there is at least one "good" b. □

This argument can be modified easily to give the existence of a dense *infinite* Sidon set.

Theorem 4.5. *There is a Sidon set* $\mathcal{A} \subseteq \mathbb{N}$ *such that* $A(n) \geq \lfloor n^{1/3} \rfloor$ *for all* $n \in \mathbb{N}$.

In the finite case, the estimate obtained in this way can be improved considerably. In fact, by using Singer's theorem on perfect difference sets, Erdős and Chowla independently proved in 1944 the following result.

Theorem 4.6. *For infinitely many* $N \in \mathbb{N}$, *there is a Sidon set* $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ *with* $|\mathcal{A}| > N^{1/2}$. *For all* $N \in \mathbb{N}$, *there is a Sidon set* $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ *with* $|\mathcal{A}| > N^{1/2} - cN^{5/16}$ (*for some absolute positive constant* c).

On the other hand, in 1941 Erdős and Turán had proved the following.

Theorem 4.7. *There is an absolute, positive constant* c *such that if* $N \in \mathbb{N}$ *and* $A \subseteq \{1, 2, \ldots, N\}$ *is a Sidon set, then* $|\mathcal{A}| < N^{1/2} + cN^{1/4}$.

Erdős conjectures that the expression $cN^{5/16}$ in Theorem 4.6 can be replaced with c and that the expression $cN^{1/4}$ in Theorem 4.7 can be replaced with $N^{o(1)}$.

Much less is known in the infinite case. The best-known lower bound, due to Ajtai et al. (1981) is annoyingly only slightly better than the near-trivial Theorem 4.5.

Theorem 4.8. *There is a Sidon set* $\mathcal{A} \subseteq \mathbb{N}$ *such that* $A(n) > 10^{-3}(n \log n)^{1/3}$ *for all sufficiently large* n.

We can do much better if we only want an Ω-result. Improving on a result of Erdős, Krückeberg showed the following in 1961.

Theorem 4.9. *There is a Sidon set* $\mathcal{A} \subseteq \mathbb{N}$ *such that*

$$\limsup_{n \to \infty} A(n)/\sqrt{n} \geq 1/\sqrt{2}\,.$$

Erdős conjectures that this lim sup is 1. Note that by Theorem 4.7, it is at most 1.

We do know the lim sup in Theorem 4.9 cannot be replaced by lim inf, as the following result of Erdős in 1955 shows.

Theorem 4.10. *There is an absolute constant* c *such that if* $\mathcal{A} \subseteq \mathbb{N}$ *is any infinite Sidon set, then*

$$\liminf_{n \to \infty} A(n)/\sqrt{n/\log n} \leq c\,.$$

The gap between Theorems 4.8 and 4.10 remains an important unsolved problem in the subject.

We can obtain interesting problems and results if we relax the condition $s(\mathcal{A}, n) \leqslant 1$ of a Sidon set to $s(\mathcal{A}, n) \leqslant g$. In 1960, using probability theory, Erdős and Rényi proved, among other interesting results, the following.

Theorem 4.11. *For every $\varepsilon > 0$, there is a number $g = g(\varepsilon)$ and an infinite set $\mathcal{A} \subseteq \mathbb{N}$ with $s(\mathcal{A}, n) \leqslant g$ for all $n \in \mathbb{N}$ and*

$$\lim_{n\to\infty} A(n)/n^{1/2-\varepsilon} = \infty .$$

In connection with problem (ii), in 1956 Erdős, using a probabilistic method, proved the following.

Theorem 4.12. *There are positive constants c_1, c_2 and a set $\mathcal{A} \subseteq \mathbb{N}$ such that*

$$c_1 \log n < s(\mathcal{A}, n) < c_2 \log n \quad \text{for all } n \in \mathbb{N} .$$

It is not known if $s(\mathcal{A}, n) \sim c \log n$ for some positive constant c is possible. Another attractive problem is whether $s(\mathcal{A}, n) \geqslant 1$ for all $n \in \mathbb{N}$ implies $s(\mathcal{A}, n)$ is unbounded.

The following result due to Erdős and Fuchs in 1956 involves analytic methods. Let $r(\mathcal{A}, n)$ denote the total number of solutions of $a + a' = n$ with $a, a' \in \mathcal{A}$, where now, we do not require $a \leqslant a'$.

Theorem 4.13. *If $c > 0$ and $\mathcal{A} \subseteq \mathbb{N}$, then*

$$\sum_{n\leqslant N} r(\mathcal{A}, n) = cN + o(N^{1/4}(\log N)^{-1/2})$$

cannot hold.

As a corollary one can get an Ω-result for the error term in the circle problem; that is, for the quantity

$$\pi r^2 - \sum_{\substack{(i,j)\in\mathbb{Z}^2 \\ i^2+j^2\leqslant r^2}} 1 .$$

Recently, Montgomery and Vaughan (1990) have shown that the factor $(\log N)^{-1/2}$ in Theorem 4.13 may be dropped. See Halberstam and Roth (1983, including the footnote on p. 106) and Erdős (1956) for further information.

The results and problems discussed so far have been extended and generalized by many people. For further references, see Hayashi (1981) and Erdős et al. (1986).

4.2. The arithmetic structure of sum sets and difference sets

In 1934, Erdős and Turán proved the following theorem.

Theorem 4.14. *There is a positive constant c such that if* $\{a_1, a_2, \ldots, a_n\} \subset \mathbb{N}$, *then*

$$\nu\Big(\prod_{1 \leq i, j \leq n} (a_i + a_j)\Big) \geq c \log n .$$

Thus the set of integers with prime factors coming from a small set cannot contain a subset of the form $2\mathscr{A}$ with $|\mathscr{A}|$ large.

Since then many papers have been written on the arithmetic properties of sum sets $\mathscr{A} + \mathscr{B}$ and difference sets $\mathscr{A} - \mathscr{A}$. For example, in 1978–79, Fürstenberg and Sárközy (independently) studied the solvability of the equation $a - a' = n^2$ for a, $a' \in \mathscr{A}$. In these papers written on "hybrid" problems (i.e., problems involving both general sets and special sets of integers), combinatorial, analytic, and ergodic methods are used. See Sárközy (1989) for a survey of these results; see also Pintz et al. (1988) and György et al. (1988) for further recent efforts.

Recently it has been proved that if $\mathscr{A}$, $\mathscr{B}$ are "dense", then (i) the sum set $\mathscr{A} + \mathscr{B}$ contains an element $a + b$ all whose prime factors are "small" (Balog and Sárközy), (ii) there is a sum $a + b$ which is "almost prime" in the strong sense that it is the product of a prime and a bounded integer (Sárközy and Stewart), (iii) there is a sum $a + b$ with "many" distinct prime factors (Erdős et al. 1993), (iv) the members of $\mathscr{A} + \mathscr{B}$, weighted with respect to the number of their representations, behave like normal integers for the function $\nu(n)$ (Erdős et al. 1987). This last result has been sharpened and extended in various directions by Elliott and Sárközy and by Tenenbaum. Several authors have studied the structure of the difference set $\mathscr{A} - \mathscr{A}$ for "dense" sets $\mathscr{A}$; see Stewart and Tijdeman (1983) for references.

4.3. Complete sets and subset sums

For references, see Erdős and Graham (1980, pp. 53–60).

A set $\mathscr{A} \subseteq \mathbb{N}$ is said to be *complete* if every large integer can be written as the sum of the elements in some finite subset of $\mathscr{A}$. For example, the powers of 2 form a complete set. It is less well known that the squares form a complete set – indeed, every integer greater than 128 can be represented as a sum of distinct squares.

Must a dense enough set be complete? Improving on a result of Erdős, Folkman proved in 1966 the following result.

Theorem 4.15. *Suppose* $\mathscr{A} \subseteq \mathbb{N}$ *is such that* $A(x) > x^{1/2+\varepsilon}$ *for some* $\varepsilon > 0$ *and all large x. Suppose further that the set of subset sums from* $\mathscr{A}$ *contains a complete residue system* (mod m) *for every* $m \in \mathbb{N}$. *Then* $\mathscr{A}$ *is complete.*

A somewhat stronger statement, that is still open, was conjectured by Erdős in 1962. In some sense, though, Theorem 4.15 is best possible, for in 1960 Cassels showed that "1/2" cannot be replaced with any smaller number in the theorem. By using Theorem 3.11, Sárközy (1989/1994) proved a finite analog of Theorem 4.15 which has many applications. (Slightly later, Freiman independently proved nearly the same theorem.)

Let $s(\mathscr{A})$ be the largest number of subsets of $\mathscr{A}$ with the same sum. Improving on a result of Erdős and Moser, Sárközy and Szemerédi proved (by using Sperner's theorem) that if $\mathscr{A}$ is a set of positive reals with $|\mathscr{A}| = n$, then $s(\mathscr{A}) \leqslant c2^n n^{-3/2}$ for some absolute constant c. This result has since been improved by Nicolas, Beck, van Lint, and Stanley. In particular, Stanley showed that $s(\mathscr{A})$ is maximized over all sets $\mathscr{A}$ of n positive reals when $\mathscr{A}$ is an arithmetic progression and in this case the most popular subset sum is a subset sum closest to the average of the members of $\mathscr{A}$.

How dense can $\mathscr{A} \subseteq \{1, 2, \ldots, N\}$ be if the subset sums from $\mathscr{A}$ are distinct? One of Erdős's first conjectures is that

$$\max|\mathscr{A}| = \frac{\log N}{\log 2} + O(1).$$

Towards this conjecture, Erdős and Moser proved that

$$\max|\mathscr{A}| \leqslant \frac{\log N}{\log 2} + \frac{\log\log N}{2\log 2} + O(1).$$

In 1969, Conway and Guy gave the lower bound $(\log N)/(\log 2) + 2$ for $N = 2^k$ which is just 1 better than the trivial example of taking the powers of 2. However, no one has succeeded in giving *any* example that is 2 better than the trivial. Ryavec showed that

$$\sum_{a \in \mathscr{A}} \frac{1}{a} < 2$$

if $\mathscr{A}$ is a finite set of natural numbers with distinct subset sums.

In 1969, Erdős and Heilbronn showed that if $\mathscr{A} \subseteq \mathbb{Z}/p$, where p is prime and $|\mathscr{A}| > 3\sqrt{6p}$, then the subset sums of $\mathscr{A}$ cover all of $\mathbb{Z}/p$. Olson improved on the constant $3\sqrt{6}$ and Szemerédi (1970) extended the result to arbitrary finite Abelian groups. Sárközy (1989/1994) studied the case when the elements of $\mathscr{A}$ are not necessarily distinct.

5. Multiplicative problems

5.1. *Primitive sets*

For many references, see chapter V of Halberstam and Roth (1983) and Hall and Tenenbaum (1988).

Say $\mathscr{B} \subseteq \mathbb{N}$ has the property that whenever $b \in \mathscr{B}$, every positive multiple of b

is in $\mathcal{B}$. Examples of sets with this property include the set of even natural numbers, the set of composites, and the set of natural numbers with a divisor between 100 and 200. An example with historic interest is the set of abundant numbers, i.e., natural numbers n such that the sum of the positive divisors of n (other than n) exceeds n.

More generally, if $\mathcal{A} \subseteq \mathbb{N}$ is arbitrary, then the set $\mathcal{B}(\mathcal{A})$ of all positive multiples of members of $\mathcal{A}$ evidently has the property that if $b \in \mathcal{B}(\mathcal{A})$, then all positive multiples of b are in $\mathcal{B}(\mathcal{A})$. Is every set $\mathcal{B}$ with this property in the form $\mathcal{B}(\mathcal{A})$ for some $\mathcal{A}$? The answer is clearly yes. In fact, if $\mathcal{B}$ has this property and $\mathcal{A}$ is the set of primitive elements of $\mathcal{B}$, i.e., members of $\mathcal{B}$ not divisible by any other members of $\mathcal{B}$, then $\mathcal{B} = \mathcal{B}(\mathcal{A})$.

We say a set $\mathcal{A} \subseteq \mathbb{N}$ is *primitive* if no member of $\mathcal{A}$ divides another member of $\mathcal{A}$. Thus $\mathcal{A} \leftrightarrow \mathcal{B}(\mathcal{A})$ is a one-to-one correspondence between primitive sets and sets $\mathcal{B} \subseteq \mathbb{N}$ such that $kb \in \mathcal{B}$ whenever $b \in \mathcal{B}$.

The set of prime numbers is a primitive set. More generally, the set of $n \in \mathbb{N}$ with $\Omega(n) = k$ is primitive for any fixed $k \in \mathbb{N}$. The case $k = 2$ is the primitive set for the set of composites. If $N \in \mathbb{N}$, then

$$\mathcal{I}_N = \{n: \tfrac{1}{2}N < n \leqslant N\}$$

is primitive. Clearly any subset of a primitive set is primitive.

These considerations suggest several questions:

(i) Is $\mathcal{I}_N$ the most numerous primitive subset of $\{1, 2, \ldots, N\}$?

(ii) Must a primitive set have asymptotic density of 0?

(iii) Must a set $\mathcal{B}(\mathcal{A})$ have asymptotic density?

At least one of these questions is fairly easy as is seen in the following result.

Proposition 5.1. *$\mathcal{I}_N$ is the most numerous primitive subset of* $\{1, 2, \ldots, N\}$.

Proof. For each $n \in \mathbb{N}$, let n' denote the largest odd divisor of n. Clearly if $m' = n'$ and $m < n$, then $m \mid n$. Thus the mapping $n \to n'$ must be one-to-one on any primitive set $\mathcal{A}$. There are exactly $N - \lfloor \frac{1}{2}N \rfloor$ odd integers in $\{1, 2, \ldots, N\}$, so no primitive subset of $\{1, 2, \ldots, N\}$ can have more than $N - \lfloor \frac{1}{2}N \rfloor = |\mathcal{I}_N|$ members. □

The sets $\mathcal{I}_N$ can be essentially glued together to get a counter-example to question (ii). The key tool is the following, perhaps surprising, result of Erdős from 1935. We first note that, concerning question (iii), if $\mathcal{A} \subseteq \mathbb{N}$ is *finite*, then clearly $d(\mathcal{B}(\mathcal{A}))$ exists.

Theorem 5.2. *Let $\varepsilon_N = d(\mathcal{B}(\mathcal{I}_N))$; that is, ε_N is the asymptotic density of the integers with a divisor in $(\frac{1}{2}N, N]$. Then* $\lim_{N\to\infty} \varepsilon_N = 0$.

This result can be proved by consideration of the "normal" number of prime factors below N of a random integer. We still do not have an asymptotic formula

for ε_N; the best results to date are due to Tenenbaum. Finally, it should be remarked that Erdős actually proved a stronger version of Theorem 5.2 where $(\frac{1}{2}N, N]$ is replaced by $(N^{1-\delta_N}, N]$ and $\delta_N \to 0$ arbitrarily slowly.

The following result is due to Besicovitch in 1934.

Theorem 5.3. *For each $\varepsilon > 0$, there is a primitive set $\mathcal{A}$ with $\overline{d}(\mathcal{A}) \geqslant \frac{1}{2} - \varepsilon$.*

Proof. We use Theorem 5.2; the original proof of Besicovitch used a weaker form of this result. Let $N_1 < N_2 < \cdots$ be a sequence of natural numbers with $\varepsilon_{N_i} \leqslant 2^{-i-1}\varepsilon$ and such that the number of integers up to N_i divisible by some member of $\mathcal{I}_{N_1} \cup \cdots \cup \mathcal{I}_{N_{i-1}}$ is at most

$$(2\varepsilon_{N_1} + \cdots + 2\varepsilon_{N_{i-1}})N_i < \varepsilon N_i . \tag{5.4}$$

Thus if we denote by $\mathcal{I}'_{N_i}$ the set of members of $\mathcal{I}_{N_i}$ not divisible by any member of $\mathcal{I}_{N_1} \cup \cdots \cup \mathcal{I}_{N_{i-1}}$, then $|\mathcal{I}'_{N_i}| > (\frac{1}{2} - \varepsilon)N_i$.

Further, if $\mathcal{A}$ is the union of all $\mathcal{I}'_{N_i}$, then $\mathcal{A}$ is evidently primitive and

$$A(N_i) \geqslant |\mathcal{I}'_{N_i}| \geqslant (\tfrac{1}{2} - \varepsilon)N_i$$

for each i. Thus $\overline{d}(\mathcal{A}) \geqslant \frac{1}{2} - \varepsilon$. □

The set $\mathcal{A}$ just constructed (with $0 < \varepsilon < \frac{1}{6}$) also answers question (iii) in the negative. Indeed,

$$\overline{d}(\mathcal{B}(\mathcal{A})) \geqslant \overline{d}(\mathcal{A}) \geqslant \tfrac{1}{2} - \varepsilon > \tfrac{1}{3} ,$$

and since the number of members of $\mathcal{B}(\mathcal{A})$ up to $\frac{1}{2}N_i$ is by (5.4) at most εN_i, we have

$$\underline{d}(\mathcal{B}(\mathcal{A})) \leqslant 2\varepsilon < \tfrac{1}{3} .$$

Thus $\mathcal{B}(\mathcal{A})$ does not possess asymptotic density.

It is a simple exercise to show the following.

Proposition 5.5. *If $\mathcal{A} \subseteq \mathbb{N}$ is such that $\sum_{a \in \mathcal{A}} 1/a < \infty$, then $d(\mathcal{B}(\mathcal{A}))$ exists.*

It is a slightly more difficult exercise to show that if furthermore $1 \notin \mathcal{A}$, then $d(\mathcal{B}(\mathcal{A})) < 1$; see Pomerance and Sárközy (1988).

As we have seen, a primitive set $\mathcal{A}$ need not have density 0. However, if one considers a weaker density than asymptotic density, namely logarithmic density, then every primitive set has density 0. The logarithmic density of a set $\mathcal{A} \subseteq \mathbb{N}$ is defined by

$$\delta(\mathcal{A}) = \lim_{N \to \infty} \frac{1}{\log N} \sum_{\substack{a \in \mathcal{A} \\ a \leqslant N}} \frac{1}{a} , \tag{5.6}$$

should this limit exist. It is not hard to show that if $d(\mathcal{A})$ exists, then so does $\delta(\mathcal{A})$ and it is equal to $d(\mathcal{A})$.

In 1935, Erdős proved the following result.

Theorem 5.7. *There is an absolute constant c such that*

$$\sum_{a\in\mathcal{A}} \frac{1}{a\log a} < c$$

for every primitive set $\mathcal{A}\subseteq\mathbb{N}$ except $\mathcal{A}=\{1\}$.

(Erdős conjectures that the maximal value of the sum in this theorem is attained when $\mathcal{A}$ is the set of primes.) It follows immediately that $\delta(\mathcal{A})=0$ for every primitive set $\mathcal{A}$. Since $\underline{d}(\mathcal{A})\leq\delta(\mathcal{A})$ always (this is easy), another corollary is that the lower asymptotic density of any primitive set is 0.

In 1937, Davenport and Erdős proved the following result.

Theorem 5.8. (i) *If $\mathcal{A}\subseteq\mathbb{N}$ has positive upper logarithmic density, then $\mathcal{A}$ contains an infinite sequence $a_1<a_2<\cdots$ with $a_i|a_{i+1}$ for $i=1, 2, \ldots$.*

(ii) *For any $\mathcal{A}\subseteq\mathbb{N}$, $\delta(\mathcal{B}(\mathcal{A}))$ exists.*

Of course, by "upper logarithmic density" we mean that the lim in (5.6) is replaced with lim sup. These results really underline the fact that logarithmic density is the "correct" measure when considering primitive sets and sets of multiples.

How large can $\sum_{\mathcal{A}} 1/a$ be for a primitive set $\mathcal{A}\subseteq\{1, 2, \ldots, N\}$? This question is partially answered by the following result of Behrend from 1935.

Theorem 5.9. *There is a positive constant c_1 such that if $N\geq 3$, then*

$$\sum_{a\in\mathcal{A}} \frac{1}{a} < c_1(\log N)(\log\log N)^{-1/2}$$

for any primitive set $\mathcal{A}\subseteq\{1, 2, \ldots, N\}$.

Proof. Let $s(u)$ denote the cardinality of the largest primitive set made up of divisors of u. We begin our proof by using Sperner's theorem (see chapter 24) to compute $s(u)$ when u is squarefree. Indeed, if u is squarefree and $\nu(u)=k$, then each divisor of u corresponds to a subset of the k primes of u. Thus Sperner's theorem immediately gives

$$s(u)=\binom{k}{\lfloor\frac{1}{2}k\rfloor}. \tag{5.10}$$

We now show the connection of $s(u)$ to our problem. Let u' denote the largest squarefree divisor of u. If $\mathcal{A}\subseteq\{1, 2, \ldots, N\}$ is primitive and every member of $\mathcal{A}$

is squarefree, then

$$\sum_{u\leqslant N} s(u') \geqslant \sum_{u\leqslant N} \sum_{\substack{a|u \\ a\in\mathscr{A}}} 1 = \sum_{a\in\mathscr{A}} \sum_{\substack{u\leqslant N \\ a|u}} 1 = \sum_{a\in\mathscr{A}} \left[\frac{N}{a}\right]$$

$$> N \sum_{a\in\mathscr{A}} \frac{1}{a} - N .$$

Thus it will suffice to prove that

$$\sum_{u\leqslant N} s(u') \leqslant cN(\log N)(\log\log N)^{-1/2} \tag{5.11}$$

for some constant c and all $N \geqslant 3$.

To do this, we apply Stirling's formula to (5.10), getting

$$s(u) \leqslant c2^{\nu(u)}(\nu(u))^{-1/2}, \quad u \text{ squarefree}$$

for some constant c. Since $\nu(u) = \nu(u')$, we thus have (with $l = \lfloor \log\log N \rfloor$)

$$\begin{aligned}\sum_{u\leqslant N} s(u') &\leqslant c \sum_{u\leqslant N} 2^{\nu(u)}(\nu(u))^{-1/2} \\ &= c \sum_{\substack{u\leqslant N \\ \nu(u)\leqslant l}} 2^{\nu(u)}(\nu(u))^{-1/2} + c \sum_{\substack{u\leqslant N \\ \nu(u)>l}} 2^{\nu(u)}(\nu(u))^{-1/2} \\ &\leqslant c\cdot 2^l N + cl^{-1/2} \sum_{u\leqslant N} 2^{\nu(u)} \\ &\leqslant cN(\log N)^{\log 2} + cl^{-1/2} \sum_{u\leqslant N} \tau(u) ,\end{aligned} \tag{5.12}$$

where $\tau(u)$ is defined in section 1. The final sum in (5.12) is easily majorized. We have

$$\sum_{u\leqslant N} \tau(u) = \sum_{u\leqslant N} \sum_{d|u} 1 = \sum_{d\leqslant N} \sum_{\substack{u\leqslant N \\ d|u}} 1 = \sum_{d\leqslant N} \lfloor N/d \rfloor$$

$$\leqslant N \sum_{d\leqslant N} 1/d \leqslant N(\log N + 1) .$$

Putting this estimate in (5.12) gives (5.11) and thus the theorem for the case when every member of $\mathscr{A}$ is squarefree.

Now suppose $\mathscr{A} \subseteq \{1, 2, \ldots, N\}$ is an arbitrary primitive set. For each $k \in \mathbb{N}$, let $\mathscr{A}_k$ denote the set of $a \in \mathscr{A}$ with largest square divisor being k^2. Thus $\{a/k^2 : a \in \mathscr{A}_k\}$ is a primitive set of squarefree numbers not exceeding N/k^2. Thus

$$\sum_{a\in\mathscr{A}} \frac{1}{a} = \sum_{k=1}^{\infty} \sum_{a\in\mathscr{A}_k} \frac{1}{a} = \sum_{k=1}^{\infty} \frac{1}{k^2} \sum_{a\in\mathscr{A}_k} \frac{1}{a/k^2}$$

$$\leqslant c(\log N)(\log\log N)^{-1/2} \sum_{k=1}^{\infty} \frac{1}{k^2} ,$$

by our theorem for primitive sets of squarefree numbers. Since $\sum 1/k^2$ is convergent, the general case of our theorem follows. □

That Theorem 5.9 is essentially best possible was shown by Pillai in 1939. Namely, Pillai showed that there is a positive constant c_2 such that for each large N there is a primitive set $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ with

$$\sum_{a \in \mathcal{A}} \frac{1}{a} > c_2 (\log N)(\log\log N)^{-1/2}. \tag{5.13}$$

The gap between Theorem 5.9 and eq. (5.13) was eliminated by Erdős, Sárközy and Szemerédi in 1967. They show that if $L(N)$ is the maximum value of $\sum_{\mathcal{A}} 1/a$ for all primitive sets $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$, then

$$L(N) = ((2\pi)^{-1/2} + o(1))(\log N)(\log\log N)^{-1/2}. \tag{5.14}$$

The lower bound in (5.14) had already been shown by Erdős in 1948 by taking $\mathcal{A}$ to be the set of $m \in \{1, 2, \ldots, N\}$ with $\Omega(m) = \lfloor \log\log N \rfloor$.

Interestingly, if $\mathcal{A}$ is an infinite primitive set, then we have

$$\sum_{\substack{a \in \mathcal{A} \\ a \leq N}} \frac{1}{a} = o((\log N)(\log\log N)^{-1/2}) \tag{5.15}$$

and no statement stronger than (5.15) is true, a result of Erdős, Szemerédi and Sárközy in 1967. For references, see Erdős et al. (1970).

5.2. *Product sets and other multiplicative problems*

If $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}$, we denote by $\mathcal{AB}$ the set of products ab where $a \in \mathcal{A}$, $b \in \mathcal{B}$. Also we write $\mathcal{A}^2$ for $\mathcal{AA}$, $\mathcal{A}^3$ for $\mathcal{A}^2\mathcal{A}$, etc.

In 1960, Erdős proved the following remarkable theorem.

Theorem 5.16. *If* $\mathcal{A} = \{1, 2, \ldots, N\}$, *then* $|\mathcal{A}^2| = N^2(\log N)^{-\alpha + o(1)}$, *where* $\alpha = 1 - (1 + \log\log 2)/\log 2$.

Thus there are only $o(N^2)$ distinct integers in the $N \times N$ multiplication table! This seeming paradox is explained by the fact that a "normal product" of integers $a_1, a_2 \leq N$ has about $2 \log\log N$ prime factors, which is quite *abnormal* for integers below N^2. The idea of looking at the normal number of prime factors of an integer is often fruitful; in fact this idea was mentioned above in connection with Theorem 5.2 whose proof is actually quite similar to the proof of Theorem 5.16.

What can one say about $|\mathcal{AB}|$ if $\mathcal{A}$ and $\mathcal{B}$ are just "dense" subjects of $\{1, 2, \ldots, N\}$? This question is addressed in a recent paper of Pomerance and Sárközy (1990).

Theorem 5.17. *If* $\varepsilon > 0$ *is arbitrary and* $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \ldots, N\}$ *with* $|\mathcal{A}|, |\mathcal{B}| > \varepsilon N$,

then $|\mathcal{AB}| \geqslant N^2(\log N)^{1-2\log 2+o_\varepsilon(1)}$. *Moreover, there is a set* $\mathcal{A}_N \subseteq \{1, 2, \ldots, N\}$ *with* $|\mathcal{A}_N| \sim N$ *and* $|\mathcal{A}_N^2| = N^2(\log N)^{1-2\log 2+o(1)}$.

We say a set $\mathcal{A} \subseteq \mathbb{N}$ is a *multiplicative basis of order k* if $\mathcal{A}^k = \mathbb{N}$. See Wirsing (1957) for a study of density properties of multiplicative bases.

Following Theorem 4.12 we asked the Sidon problem: if $\mathcal{A}$ is a basis (additive) of order 2, must $s(n)$, the number of representations of n as $a_1 + a_2$ with a_1, $a_2 \in \mathcal{A}$, be unbounded? The multiplicative analog of this problem was solved by Erdős in 1965 (see Erdős and Graham 1980, p. 100).

Theorem 5.18. *If* $\mathcal{A}$ *is a multiplicative basis of order* 2, *then* $t(n)$, *the number of representations of* n *as* a_1a_2 *with* a_1, $a_2 \in \mathcal{A}$, *must be unbounded.*

How large a set $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ can we choose with all of the products a_1a_2 (with a_1, $a_2 \in \mathcal{A}$, $a_1 < a_2$) distinct? If $k(N)$ denotes the maximal cardinality of such a set $\mathcal{A}$, then Erdős has shown (with graph-theoretic tools) that

$$\pi(N) + c_1N^{3/4}/\log^{3/2}N < k(N) < \pi(N) + c_2N^{3/4}/\log^{3/2}N$$

for certain positive constants c_1, c_2 and all large N. Erdős and Posa have considered the analogous problem where all of the subset products from $\mathcal{A}$ are distinct. See Erdős and Graham (1980, p. 98) for references and a proof.

In 1976, Szemerédi proved the following attractive result (see Erdős and Graham 1980, pp. 98–99).

Theorem 5.19. *There is a constant* c *such that if* $\mathcal{A}$, $\mathcal{B} \subseteq \{1, 2, \ldots, N\}$ *and* $|\mathcal{AB}| = |\mathcal{A}||\mathcal{B}|$, *then* $|\mathcal{AB}| < cN^2/\log(N+1)$.

In contrast, it is easy to construct sets $\mathcal{A}$, $\mathcal{B} \subseteq \mathbb{N}$ such that each $n \in \mathbb{N}$ has a unique representation $n = ab$ with $a \in \mathcal{A}$, $b \in \mathcal{B}$. For example, we may choose $\mathcal{A}$ to be the powers of 2 and $\mathcal{B}$ to be the odd natural numbers, or more generally, $\mathcal{A}$ the natural numbers all of whose primes come from $\mathcal{P}_1$ and $\mathcal{B}$ the natural numbers all of whose primes come from $\mathcal{P}_2$, where $\mathcal{P}_1 \cup \mathcal{P}_2$ is an arbitrary partition of the set of primes. Erdős, Saffari, Vaughan, and Daboussi have studied this problem.

In 1975, Erdős and Selfridge (see Erdős and Graham 1980, p. 66) showed the following striking result.

Theorem 5.20. *The product of two or more consecutive positive integers is never a non-trivial power.*

There are many other problems and results concerning blocks of consecutive integers in Erdős and Graham (1980, section 8).

6. Van der Waerden's theorem and generalizations

For many references, see chapters 1 and 2 of Graham et al. (1980), and section 2 of Erdős and Graham (1980).

How much of the structure of the natural numbers must be preserved in a "dense" subset? In 1927, B. L. van der Waerden showed that if the natural numbers are partitioned into two subsets, then one subset contains arbitrarily long arithmetic progressions. In one sense, this theorem is best possible, since it is an easy exercise to partition the natural numbers into two subsets, neither of which contains an infinite arithmetic progression. But the theorem still leaves us wondering about our opening question, which we now repeat more specifically. How dense must a subset of the natural numbers be for it to contain arbitrarily long arithmetic progressions?

In particular, in 1936 Erdős and Turán conjectured that if $\mathscr{A} \subseteq \mathbb{N}$ has positive upper asymptotic density, then $\mathscr{A}$ contains arbitrarily long APs (we abbreviate "arithmetic progression" as AP). In 1952, Roth used the Hardy–Littlewood circle method from analytic number theory to prove the Erdős–Turán conjecture for three-term APs. In 1969, via a combinatorial argument, Szemerédi showed the conjecture for four-term APs, and in 1974, in what must be one of the most complex proofs in combinatorial number theory, he proved the complete conjecture. A few years later, Fürstenberg, using ergodic theory, gave another proof (also complicated) of what is now known as Szemerédi's theorem.

How much can Szemerédi's theorem be improved? An old conjecture of Erdös is that if $\mathscr{A} \subseteq \mathbb{N}$ satisfies only the weaker hypothesis

$$\sum_{a \in \mathscr{A}} \frac{1}{a} = \infty,$$

rather than positive upper asymptotic density, then this is enough to force $\mathscr{A}$ to have arbitrarily long APs.

A corollary to this conjecture of Erdős is that the set of primes would contain arbitrarily long APs. It is unclear, though, that one should think of this prime number problem in terms of the Erdős conjecture. That is, Erdős is suggesting that the set of prime numbers contains arbitrarily long APs only because the prime numbers are fairly numerous and not because of any special properties of the prime numbers. This technique of generalizing a hard problem to put it in proper perspective is of course an often-successful trick in mathematics. However, the only progress we have had so far on showing the set of primes contains arbitrarily long APs is through intrinsic properties of the primes.

For example, Chudakov, Estermann, and van der Corput independently in 1937–38 used the circle method to show the following strengthening of Corollary 3.1: for any $A > 0$, the number of even integers up to x not the sum of two distinct primes is $O(x/\log^A x)$. From this we can prove the following result.

Corollary 6.1. *The set of primes contains infinitely many three-term APs.*

Proof. By the prime number theorem, the number of even integers up to x of the form $2p$ with p prime is $\sim x/(2\log x)$. Thus by the above-mentioned theorem, most of these numbers $2p$ can be represented as $q+r$, where $q<r$ are primes. But then q, p, r form a three-term AP of prime numbers. □

It is still unknown if there are infinitely many four-term APs of primes. The longest AP of primes ever found has length 22, a result of Pritchard et al. (1995).

We now look at several "equivalent" formulations of van der Waerden's theorem. The reason for the quotation marks is that logically, all theorems are equivalent. Here we mean it in the subjective sense that the proofs of interdependence are simple and fairly transparent.

Theorem 6.2. *The following statements are equivalent*:

(i) *If* $\mathbb{N}$ *is partitioned into two subsets, then one subset contains arbitrarily long APs.*

(ii) *For each* $k\in\mathbb{N}$, *there is a number* $W(k)$ *such that if* $\{1, 2, \ldots, W(k)\}$ *is partitioned into two subsets, then one subset contains a* k*-term AP.*

(iii) *For each* k, $r\in\mathbb{N}$, *there is a number* $W(k,r)$ *such that if* $\{1, 2, \ldots, W(k, r)\}$ *is partitioned into* r *subsets, then one subset contains a* k*-term AP.*

(iv) *For each* $r\in\mathbb{N}$, *if* $\mathbb{N}$ *is partitioned into* r *subsets, then one subset contains arbitrarily long APs.*

(v) *If* $\{a_n\}$ *is an infinite subsequence of* $\mathbb{N}$ *with* $\{a_{n+1}-a_n\}$ *bounded, then* $\{a_n\}$ *contains arbitrarily long APs.*

Proof. We first show that (i) $\Rightarrow$ (ii), which is probably the most difficult of the implications. It is an example of the "compactness principle" in Ramsey theory (cf. chapter 42). Suppose k is such that $W(k)$ does not exist. Thus for every N there is a subset $\mathcal{A}_N$ of $\{1, 2, \ldots, N\}$ such that neither $\mathcal{A}_N$ nor its complement contains a k-term AP. Obviously there is an infinite subsequence $N_{11}<N_{12}<\cdots$ of $\mathbb{N}$ such that

$$\mathcal{S}_1 := \mathcal{A}_{N_{11}}\cap\{1\} = \mathcal{A}_{N_{12}}\cap\{1\} = \cdots;$$

that is, either 1 is in each $\mathcal{A}_{N_{1j}}$ or 1 is in no $\mathcal{A}_{N_{1j}}$. By passing to an infinite subsequence $N_{21}<N_{22}<\cdots$ of $\{N_{1j}\}$, we have

$$\mathcal{S}_2 := \mathcal{A}_{N_{21}}\cap\{1,2\} = \mathcal{A}_{N_{22}}\cap\{1,2\} = \cdots$$

and $\mathcal{S}_1\subseteq\mathcal{S}_2$. Continuing in this fashion we find $\mathcal{S}_1\subseteq\mathcal{S}_2\subseteq\cdots\subseteq\mathbb{N}$ and an infinite subsequence $N_1<N_2<\cdots$ of $\mathbb{N}$ ($N_1=N_{11}$, $N_2=N_{21}$, etc.) with $\mathcal{S}_j=\mathcal{A}_{N_j}\cap\{1, 2, \ldots, j\}$ for each j. Thus if $\mathcal{S}=\bigcup\mathcal{S}_j$, then neither $\mathcal{S}$ nor $\mathbb{N}\backslash\mathcal{S}$ contains a k-term AP, contradicting (i).

Now we show (ii) $\Rightarrow$ (iii). We do this by induction on r, (ii) being the statement for $r=2$ (and the case $r=1$ being trivial). Suppose $W(k, r)$ exists for all k for some fixed $r\geq 2$. Say $\{1, 2, \ldots, N\}$ is partitioned into $r+1$ sets $\mathcal{A}_1, \ldots, \mathcal{A}_{r+1}$. If $N\geq W(l, r)$, then one of $\mathcal{A}_1\cup\mathcal{A}_2, \mathcal{A}_3, \ldots, \mathcal{A}_{r+1}$ contains an

l-term AP, call it $\mathcal{B}$. If $\mathcal{B} \subseteq \mathcal{A}_1 \cup \mathcal{A}_2$, then $\mathcal{A}_1 \cap \mathcal{B}$, $\mathcal{A}_2 \cap \mathcal{B}$ is a partition of $\mathcal{B}$ into two parts. Thus if $l = W(k, 2)$, then one part contains a k-term AP. Since clearly $W(k, 2) \geq k$, if $\mathcal{B}$ is contained in one of $\mathcal{A}_3, \ldots, \mathcal{A}_{r+1}$, then one of these sets contains a k-term AP. Thus, not only have we shown that $W(k, r+1)$ exists, but we have shown that the least choice for $W(k, r+1)$ is at most $W(W(k, 2), r)$.

It is obvious that (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i).

It is also clear that (v) $\Rightarrow$ (i), since if $\mathbb{Z} = \mathcal{A}_1 \cup \mathcal{A}_2$, $\mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset$, and $k \in \mathbb{N}$, then either $\mathcal{A}_1$ contains k consecutive integers or the maximal gap between consecutive members of $\mathcal{A}_2$ is at most k.

Finally we show (iv) $\Rightarrow$ (v), which will complete our proof. Suppose $\mathcal{A} \subseteq \mathbb{N}$ has maximal gap r between consecutive members. Let $\mathcal{A}_i = \mathcal{A} + \{i\}$ for $i = 0, 1, \ldots, r-1$. Then $\mathcal{A}_0 \cup \cdots \cup \mathcal{A}_{r-1} = \mathbb{N}$. Although these sets may not be disjoint, (iv) still implies that one of them contains a k-term AP. Then so does $\mathcal{A}_0 = \mathcal{A}$. □

Van der Waerden's theorem, as we originally stated it, is statement (i) of Theorem 6.2. We now give a proof of van der Waerden's theorem.

We begin with two definitions. If $x_1, x_2, \ldots, x_m$ and $x_1', x_2', \ldots, x_m'$ are two sequences where each term is in $\{0, 1, \ldots, l\}$, we say $\{x_i\}$ is *l-equivalent* to $\{x_i'\}$ if either l does not appear in either sequence or there is some k with $x_i = x_i'$ for $i \leq k$ and each $x_j, x_j' < l$ for $j > k$. That is, $\{x_i\}$ and $\{x_i'\}$ agree at least up to the last appearance of l.

Next, we define the statement $S(l, m)$ (where $l, m \in \mathbb{N}$) as the following assertion: for each $r \in \mathbb{N}$ there is a number $N(l, m, r)$ such that whenever $\{1, 2, \ldots, N(l, m, r)\}$ is partitioned into r parts $\mathcal{A}_1, \ldots, \mathcal{A}_r$, there exist $a, d_1, \ldots, d_m \in \mathbb{N}$ such that

$$a + l(d_1 + \cdots + d_m) \leq N(l, m, r) \tag{6.3}$$

and such that whenever $\{x_i\}$ and $\{x_i'\}$ are m-term sequences from $\{0, 1, \ldots, l\}$ that are l-equivalent, $a + x_1 d_1 + \cdots + x_m d_m$ and $a + x_1' d_1 + \cdots + x_m' d_m$ are in the same $\mathcal{A}_j$.

Note that the condition (6.3) guarantees that $a + \sum x_i d_i$ and $a + \sum x_i' d_i$ are in $\{1, 2, \ldots, N(l, m, r)\}$.

Note also that the assertion $S(l, 1)$ is essentially the same as statement (iii) of Theorem 6.2. Indeed, two integers $x, x' \in \{0, 1, \ldots, l\}$, considered as 1-term sequences, are l-equivalent if and only if both $x, x' < l$ or $x = x' = l$. The assertion $S(l, 1)$ says that there is some number $N(l, 1, r)$ such that if $\{1, 2, \ldots, N(l, 1, r)\}$ is partitioned into r subsets, then there are positive integers a, d with a, $a + d, \ldots, a + (l-1)d$ all in one of the parts. That is, one part contains an l-term AP. [Note that $S(l, 1)$ also carries the extra stipulation, not found in statement (iii) of Theorem 6.2, that $a + ld \leq N(l, 1, r)$.] Thus van der Waerden's theorem will follow from the following result.

Theorem 6.4. *For each $l, m \in \mathbb{N}$, the assertion $S(l, m)$ is a theorem.*

Proof. Our plan is as follows. First we show that if $S(l, k)$ is a theorem for $k = 1, \ldots, m$, then so too is $S(l, m+1)$. Next we show that if $S(l, m)$ is a theorem for all m, then so too is $S(l+1, 1)$. Thus our theorem will follow from this double induction and the fact that $S(1, 1)$ is trivially true.

Suppose l, $m \in \mathbb{N}$ and $S(l, k)$ is a theorem for $k = 1, \ldots, m$. Let $r \in \mathbb{N}$ be arbitrary, let $M = N(l, m, r)$, $M' = N(l, 1, r^M)$. We shall show that we may choose $N(l, m+1, r) = MM'$. Let $\mathscr{A}_1, \ldots, \mathscr{A}_r$ be a partition of $\{1, 2, \ldots, MM'\}$ and let C be the function that assigns to $i \in \{1, 2, \ldots, MM'\}$ the number $j \in \{1, 2, \ldots, r\}$ with $i \in \mathscr{A}_j$.

Consider now the matrix

$$A = \begin{bmatrix} C(1) & C(2) & \cdots & C(M) \\ C(M+1) & C(M+2) & & C(2M) \\ \vdots & & \ddots & \vdots \\ C((M'-1)M+1) & C((M'-1)M+2) & \cdots & C(M'M) \end{bmatrix}.$$

Each row of A is one of the r^M M-term sequences from $\{1, 2, \ldots, r\}$. We now partition $\{1, 2, \ldots, M'\}$ into r^M subsets where i, j are in the same subset if and only if the ith row and jth row of A are identical. Since $S(l, 1)$ is true and by our choice of M', one of these subsets contains an l-term arithmetic progression b, $b+d, \ldots, b+(l-1)d$, where b, d are positive integers with $b + ld \leqslant M'$. That is, rows $b + id$ for $i = 1, \ldots, l-1$ of A are identical.

We now apply $S(l, m)$ to $\{(b-1)M+1, (b-1)M+2, \ldots, bM\}$ (a translate of $\{1, 2, \ldots, M\}$) and the partition we already have of $\{1, 2, \ldots, MM'\}$ restricted to this subset. Thus there are natural numbers a, $d_1, \ldots, d_m$ such that

(1) $a \geqslant (b-1)M + 1$, $a + l(d_1 + \cdots + d_m) \leqslant bM$;

(2) whenever $\{x_i\}$, $\{x_i'\}$ are l-equivalent, m-term sequences from $\{0, 1, \ldots, l\}$, then $C(a + \sum x_i d_i) = C(a + \sum x_i' d_i)$.

Let $d_{m+1} = dM$. To prove assertion $S(l, m+1)$, we will show

(1′) $a + l(d_1 + \cdots + d_{m+1}) \leqslant MM'$;

(2′) whenever $\{x_i\}$, $\{x_i'\}$ are l-equivalent, $(m+1)$-term sequences from $\{0, 1, \ldots, l\}$, then $C(a + \sum x_i d_i) = C(a + \sum x_i' d_i)$.

For (1′), note that the left-hand side is

$$a + l(d_1 + \cdots + d_m) + ld_{m+1} \leqslant bM + ldM$$

by (1). But we noted above that $b + ld \leqslant M'$, so we have (1′).

For (2′) we may clearly assume that the l-equivalent sequences $\{x_i\}$ and $\{x_i'\}$ are not identical. Thus $x_{m+1}, x_{m+1}' < l$. Let

$$j = a - (b-1)M + \sum_1^m x_i d_i, \qquad j' = a - (b-1)M + \sum_1^m x_i' d_i. \tag{6.5}$$

Then j, $j' \in \{1, 2, \ldots, M\}$. We look now at columns j and j' of matrix A and how they intersect rows b, $b+d, \ldots, b+(l-1)d$. Of course, column j is constant on

these rows, as is column j'. But from (6.5),

$$(b-1)M+j=a+\sum_1^m x_i d_i\,, \qquad (b-1)M+j'=a+\sum_1^m x_i' d_i\,,$$

and since $x_1,\dots,x_m$ is l-equivalent to $x_1',\dots,x_m'$, (2) implies $C((b-1)M+j)=C((b-1)M+j')$. Thus the constant value on the l special rows of column j is the same constant value as in column j'. Note that one of these rows is $b+x_{m+1}d$, whose jth entry is

$$C((b+x_{m+1}d-1)M+j)=C\left(a+\sum_1^{m+1} x_i d_i\right)$$

by (6.5). Another special row is $b+x_{m+1}'d$, whose j'th entry is

$$C((b+x_{m+1}'d-1)M+j')=C\left(a+\sum_1^{m+1} x_i' d_i\right).$$

Thus (2′) holds and we have proved $S(l, m+1)$.

For our second induction, assume $l\in\mathbb{N}$ and $S(l, m)$ is a theorem for all $m\in\mathbb{N}$. Choose $r\in\mathbb{N}$, $r\geq 2$ (since we clearly can take $N(l+1, 1, 1)=l+2$). Let $N=N(l\ r, r)$. We shall show we may take $N(l+1, 1, r)=2N$. Indeed take any partition of $\{1, 2, \dots, 2N\}$ into r subsets $\mathscr{A}_1,\dots,\mathscr{A}_r$. Let $a, d_1,\dots,d_r\in\mathbb{N}$ be such that $a+l(d_1+\cdots+d_r)\leq N$ and such that whenever $\{x_i\}$, $\{x_i'\}$ are l-equivalent, m-term sequences from $\{0, 1, \dots, l\}$, $a+\sum x_i d_i$ is in the same $\mathscr{A}_j$ as $a+\sum x_i' d_i$.

Since $r\geq 2$, we have $\binom{r+1}{2}>r$, so there are integers $u<v$ with $0\leq u<v\leq r$ and such that

$$a+\sum_{i=1}^u l d_i\,, \qquad a+\sum_{i=1}^v l d_i$$

are in the same subset from $\mathscr{A}_1,\dots,\mathscr{A}_r$, say $\mathscr{A}_j$. Let

$$a'=a+\sum_{i=1}^u l d_i\,, \qquad d'=\sum_{i=u+1}^v d_i\,.$$

We now claim that the $(l+1)$-term arithmetic progression $a', a'+d', \dots, a'+ld'$ lies wholly in $\mathscr{A}_j$ and that $a'+(l+1)d'\leq 2N$. Indeed, we know already that a' and $a'+ld'$ both lie in $\mathscr{A}_j$ and if $x\in\{1, 2, \dots, l-1\}$, then

$$\{\underbrace{l,\dots,l}_{u},\underbrace{0,\dots,0}_{r-u}\} \quad\text{and}\quad \{\underbrace{l,\dots,l}_{u},\underbrace{x,\dots,x}_{v-u},\underbrace{0,\dots,0}_{r-v}\}$$

are l-equivalent, so that a' and $a'+xd'$ both lie in $\mathscr{A}_j$. The assertion about $a'+(l+1)d'$ is trivial since $a'+ld'\leq a+l(d_1+\cdots+d_r)\leq N$. Thus $S(l+1, 1)$ is proved, as is the theorem. □

The above proof is a "fleshed-out" version of the short proof presented in

Graham et al. (1980, p. 32). It shows that the function $W(k, r)$ defined in statement (iii) of Theorem 6.2 is recursive, but it does not show it is primitive recursive. This has recently been done by Shelah (1988), thus solving a problem that had been outstanding for a long time.

For the record we now formally state Szemerédi's theorem.

Theorem 6.6. *If $\mathcal{A} \subseteq \mathbb{N}$ has positive upper asymptotic density, then $\mathcal{A}$ contains arbitrarily long APs.*

As van der Waerden's theorem contains several essentially equivalent forms, the following result which is superficially stronger than Szemerédi's theorem is easily proved to follow from it.

Corollary 6.7. *Let $k \in \mathbb{N}$ and $\varepsilon > 0$. For each sufficiently large N, depending on the choice of k and ε, if $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ with $|A| > \varepsilon N$, then $\mathcal{A}$ contains a k-term AP.*

Proof. We may assume $k \geqslant 3$. If the corollary is untrue, then there is an infinite sequence $N_1, N_2, \ldots$ and sets $\mathcal{A}_{N_i} \subseteq \{1, \ldots, N_i\}$ with $|\mathcal{A}_{N_i}| > \varepsilon N_i$ and $\mathcal{A}_{N_i}$ does not contain any k-term AP. Let $\mathcal{B}_{N_i} = \mathcal{A}_{N_i} + \{2N_i\}$, so that $|\mathcal{B}_{N_i}| > \varepsilon N_i$, $\mathcal{B}_{N_i} \subseteq \{2N_i + 1, \ldots, 3N_i\}$ and $\mathcal{B}_{N_i}$ does not contain any k-term AP. By passing to an infinite subsequence if necessary, we may assume $N_{i+1} \geqslant 5N_i$ for $i = 1, 2, \ldots$. Let

$$\mathcal{A} = \bigcup_{i=1}^{\infty} \mathcal{B}_{N_i}.$$

Then $\mathcal{A}$ has upper asymptotic density at least $\frac{1}{3}\varepsilon$. Furthermore, $\mathcal{A}$ contains no k-term AP, since no $\mathcal{B}_{N_i}$ does and since $\mathcal{A}$ does not contain any 3-term AP that is not wholly in some $\mathcal{B}_{N_i}$. However, Theorem 6.6 denies the existence of any such set $\mathcal{A}$, which proves the corollary. □

An interesting and still unsolved problem that is perhaps connected with these considerations is the following old problem of Erdős. Is there a sequence ε_n of 1's and -1's with

$$g(k, N) = \sum_{n=1}^{N} \varepsilon_{kn}$$

bounded for all $k, N \in \mathbb{N}$? Another form of this problem asks if $g(1, N)$ can be bounded for all N for some sequence ε_n of 1's and -1's that is also a multiplicative function.

The integers

$$4030, 4131, 4232, 4333, 4434, 4535, 4636, 4737, 4838, 4939 \tag{6.8}$$

obviously form an AP of length 10. We generalize this idea as follows. Let C_t^N denote the set of N-term sequences from $\{0, 1, \ldots, t-1\}$. Then t distinct points

$P_1, P_2, \ldots, P_t$ in C_t^N are said to form a *line* if the sequence of jth terms $P_1^j, P_2^j, \ldots, P_t^j$ is either constant or is $0, 1, \ldots, t-1$. Thus the quadruplets formed by the digits of the integers in (6.8), viewed as members of C_{10}^4, form a line. The following result is due to Hales and Jewett in 1963.

Theorem 6.9. *For each $r, t \in \mathbb{N}$, there is a number $\mathrm{HJ}(r, t)$ such that if $N \geqslant \mathrm{HJ}(r, t)$ and C_t^N is partitioned into r subsets, then one subset contains a line.*

By writing the integers below t^N in base-t notation, we see that if $\{0, 1, \ldots, t^N - 1\}$ is partitioned into r subsets, where $N \geqslant \mathrm{HJ}(r, t)$, then one subset contains a t-term AP. That is, the Hales–Jewett theorem implies van der Waerden's theorem. In fact, Shelah's recent result mentioned above, that $W(k, r)$ is primitive recursive, was obtained by proving the stronger theorem that the function $\mathrm{HJ}(r, t)$ is primitive recursive.

In the 1930s, Gallai proved the following generalization of van der Waerden's theorem as a corollary of the latter. It is also possible to prove this result as a simple corollary of the Hales–Jewett theorem.

Theorem 6.10. *For all $u, r, k \in \mathbb{N}$, if $\mathbb{Z}^u$ is partitioned into r subsets, then one subset contains a set of the form $\mathcal{B}^u$ where $\mathcal{B} \subseteq \mathbb{Z}$ is an AP of length k.*

By $\mathcal{B}^u$ we mean of course all the points of $\mathbb{Z}^u$ whose coordinates lie in $\mathcal{B}$.

It is natural to ask if Theorems 6.9 and 6.10 can be generalized to "dense" sets. For Hales–Jewett, the following theorem was recently announced by Fürstenberg in the Abstracts of the 1990 International Congress of Mathematicians.

Theorem 6.11. *For each $t \in \mathbb{N}$, $\varepsilon > 0$, if N is sufficiently large and $\mathcal{A} \subseteq C_t^N$ with $|\mathcal{A}| > \varepsilon t^N$, then $\mathcal{A}$ contains a line.*

The proof is by ergodic methods. The following result is a Szemerédi-type analog of Gallai's theorem 6.10. It was first proved by Fürstenberg and Katznelson in 1978. However, it now may be viewed as a corollary of Theorem 6.11.

Theorem 6.12. *For each $k, u \in \mathbb{N}$ and each $\varepsilon > 0$, if N is sufficiently large and $\mathcal{A} \subseteq [-N, N]^u \cap \mathbb{Z}^u$ with $|\mathcal{A}| > \varepsilon N^u$, then $\mathcal{A}$ contains a subset $\mathcal{B}^u$ where $\mathcal{B} \subseteq \mathbb{Z}$ is an AP of length k.*

Another question one may attack is that of sequences of lattice points in $\mathbb{Z}^u$. If a sequence $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots$ in $\mathbb{Z}^u$ has "small gaps", what may be said? We should not expect to find long APs as can be seen from the following result of Dekking (1979).

Theorem 6.13. *There is an infinite sequence $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots$ in $\mathbb{Z}^2$ with each $\boldsymbol{v}_{i+1} - \boldsymbol{v}_i =$ (0, 1) or (1, 0) and such that no five of the $\boldsymbol{v}$'s form an AP of vectors.*

However, we may expect a large subset to be collinear, at least for $\mathbb{Z}^2$ (we mean "collinear" in the ordinary, geometric sense). The following result is due to Ramsey and Gerver (1979).

Theorem 6.14. *If $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots$ is an infinite sequence in $\mathbb{Z}^2$ with $|\boldsymbol{v}_{i+1} - \boldsymbol{v}_i|$ bounded, then for every k there are k of the $\boldsymbol{v}$'s which are collinear.*

As is also shown by Ramsey and Gerver, this result is not true for $\mathbb{Z}^3$.

Theorem 6.14 bears a similarity in appearance to statement (v) of Theorem 6.2 and thus may be thought of as an analog of van der Waerden's theorem. The following result of Pomerance (1980) would thus be a Szemerédi-analog.

Theorem 6.15. *If $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots$ is an infinite sequence in $\mathbb{Z}^2$ with*

$$\liminf_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} |\boldsymbol{v}_{i+1} - \boldsymbol{v}_i| < \infty,$$

then for every k there are k of the $\boldsymbol{v}$'s that are collinear.

An old result of Schur says that if $\mathbb{N}$ is partitioned into finitely many classes, then one class must contain infinitely many triples x, y, z with $x + y = z$. This result has been starting point of many interesting Ramsey-type problems on the integers. One particularly interesting result is due to Hindman in 1974 who showed that if $\mathbb{N}$ is partitioned into finitely many classes, then one class contains an *infinite* set $\mathcal{A}$ such that all finite subset sums from $\mathcal{A}$ belong to the same class. For more on problems of this type, see chapter 3 of Graham et al. (1980).

7. Miscellaneous problems

As with combinatorics as a whole, combinatorial number theory is rich in attractive problems that defy precise classification. It is from the wealth of such problems in an area that we are sometimes able to discern patterns that become the broad outlines of a more mature branch of mathematics. In this section we take a very brief glimpse at a few of these problems.

7.1. Covering congruences

For references see section 3 of Erdős and Graham (1980) and section F13 of Guy (1994).

In 1934, Romanoff posed the following problem. Can every sufficiently large odd integer be written as a sum of a power of 2 and a prime? In 1950, Erdős and van der Corput independently answered this problem in the negative by showing that in fact there is an infinite arithmetic progression of positive odd numbers m not of the form $2^n + p$. Erdős's solution begins with the observation that *every*

integer n is in at least one of the following residue classes:

$$\begin{aligned} &0 \pmod 2, \quad 0 \pmod 3, \quad 1 \pmod 4, \\ &3 \pmod 8, \quad 7 \pmod{12}, \quad 23 \pmod{24}. \end{aligned} \tag{7.1}$$

From this he was able to deduce that if n is a positive integer and m simultaneously satisfies

$$\begin{aligned} &m \equiv 1 \pmod{32}, \quad m \equiv 2^0 \pmod 3, \quad m \equiv 2^0 \pmod 7, \\ &m \equiv 2^1 \pmod 5, \\ &m \equiv 2^3 \pmod{17}, \quad m \equiv 2^7 \pmod{13}, \quad m \equiv 2^{23} \pmod{241}, \end{aligned} \tag{7.2}$$

then m is odd and not representable as $2^n + p$. Moreover, by the Chinese Remainder Theorem from elementary number theory, the set of integers m which satisfy all of the congruences in (7.2) form an infinite arithmetic progression with common difference $32 \cdot 3 \cdot 7 \cdot 5 \cdot 17 \cdot 14 \cdot 241$. (It is still not known if a positive odd integer m which is not representable as $2^n + p$ must belong to an infinite arithmetic progression of such integers.)

A finite system of residue classes, such as (7.1), which have *distinct* moduli and such that every integer belongs to at least one class, is called a *covering system of congruences*. Another example that is simpler than (7.1) (but that does not have relevance to the $2^n + p$ problem) is

$$0 \pmod 2, \quad 0 \pmod 3, \quad 3 \pmod 4, \quad 1 \pmod 6, \quad 5 \pmod{12}. \tag{7.3}$$

In both (7.1) and (7.3) the least modulus is 2. The following problem of Erdős from 1950 is the major unsolved problem in the area.

Problem 7.4. It is true that for every k there is a covering system of congruences with least modulus at least k?

An example due to Choi has least modulus 20. There are numerous other problems and some results concerning covering systems of congruences. We mention two more problems, the first due to Selfridge, the second to Erdős.

Problem 7.5. Is there a covering system of congruences with all moduli squarefree and greater than 2?

Problem 7.6. Is there a covering system of congruences with all moduli odd and greater than 1?

7.2. Graham's conjecture

If $\mathcal{S} \subseteq \mathbb{N}$, let $F(\mathcal{S}) = \{a/b\colon a, b \in \mathcal{S}\}$. Graham conjectured in 1970 that if $\mathcal{S}$ is

finite, then

$$F(\mathcal{S}) \not\subseteq F(\{1, 2, \ldots, |\mathcal{S}| - 1\}).$$

That is, there are $a, b \in \mathcal{S}$ with $a/(a, b) \geq |\mathcal{S}|$. This problem has attracted much attention and there have been numerous partial results. One of the easier ones is due to Szemerédi who has proved Graham's conjecture in the case $|\mathcal{S}| = p$, a prime. Indeed, we may assume not every member of $\mathcal{S}$ is divisible by p (if not, replace each $a \in \mathcal{S}$ with a/p) so that there are two members $a, b \in \mathcal{S}$ with either $a \equiv b \not\equiv 0 \pmod{p}$ or $a \not\equiv b \equiv 0 \pmod{p}$. In either case, $a/b \notin F(\{1, 2, \ldots, p - 1\})$.

Recently Graham's conjecture was independently proved by Szegedy (1986) and Zaharescu (1987) for all sufficiently large values of $|\mathcal{S}|$. They were even able to describe those sets $\mathcal{S}$ with $F(\mathcal{S}) = F(\{1, 2, \ldots, |\mathcal{S}|\})$.

Theorem 7.7. *There is some number n_0 such that if $n \geq n_0$, $\mathcal{S} \subseteq \mathbb{N}$, $|\mathcal{S}| = n$, then $F(\mathcal{S}) \not\subseteq F(\{1, 2, \ldots, n-1\})$. If $F(\mathcal{S}) \subseteq F(\{1, 2, \ldots, n\})$, then there is some $k \in \mathbb{N}$ with either*

$$\mathcal{S} = \{k, 2k, \ldots, nk\} \quad \text{or} \quad \mathcal{S} = \left\{\frac{k}{1}, \frac{k}{2}, \ldots, \frac{k}{n}\right\}.$$

In Cheng and Pomerance (1994) it is shown that we may take $n_0 = 10^{50\,000}$ and in Balasubramanian and Soundararajan (1995) it is shown that we may take $n_0 = 5$. Note that the first claim in Theorem 7.7 is true for $n < 5$, but the second claim fails for $n = 4$, since $\mathcal{S} = \{2, 3, 4, 6\}$ has $F(\mathcal{S}) = F(\{1, 2, 3, 4\})$.

7.3. Perfect numbers – Wirsing's theorem

Let $\sigma(n)$ denote the sum of the positive divisors of n. If $\sigma(n) = 2n$, then n is said to be *perfect*. The first few examples are 6, 28, and 496. It has been known since Euclid that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect. The three examples just cited fit this formula with $p = 2, 3, 5$. In fact, it has been shown by Euler that every *even* perfect number comes from Euclid's formula. The two big questions are: (1) are there infinitely many perfect numbers?, and (2) are there any odd perfect numbers?

From the Euclid–Euler results, the first question is equivalent to the existence of infinitely many Mersenne primes, that is, primes of the form $2^p - 1$. This is a very hard problem about which very little is known. We know 33 values of p for which $2^p - 1$ is prime, the largest being $p = 859\,433$.

We are still far from solving the second problem too. Numerous partial results are known, however. One of the more interesting theorems in the subject is due to Wirsing (1959), a paper which extends earlier joint work with Hornfeck.

Theorem 7.8. *There are absolute constants c_0, x_0 such that if $x \geq x_0$ and α is any rational number, then the number of $n \leq x$ with $\sigma(n) = \alpha n$ is at most $x^{c_0/\log\log x}$.*

Proof. We begin with the observation that $\sigma(n)$ is a multiplicative function [$\sigma(mn) = \sigma(m)\sigma(n)$ when $(m, n) = 1$]. Suppose α is given; write α in reduced form u/v. Suppose x is large, $n \leqslant x$, and $\sigma(n) = \alpha n$. Write $n = ab$, where b is the largest divisor of n all of whose prime factors p satisfy $p \leqslant \log x$ or $p \mid v$. Then αb is an integer. The idea of the proof is to use the equation

$$\sigma(n) = \sigma(ab) = \sigma(a)\sigma(b) = a \cdot \alpha b\,. \tag{7.9}$$

The plan is to show that we must have $\sigma(b) \nmid \alpha b$, and use this to show that b just about determines a.

Suppose the prime factorization of a is $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$. Let l be the least integer $\geqslant \log x/\log\log x$. Since each $p_i > \log x$ and since $a \leqslant n \leqslant x$, we have

$$\beta_1 + \beta_2 + \cdots + \beta_k \leqslant l\,, \tag{7.10}$$

so that, in particular, $k \leqslant l$. Then

$$1 \leqslant \frac{\sigma(a)}{a} = \prod_{i=1}^{k} (1 + p_i^{-1} + \cdots + p_i^{-\beta_i}) < \prod_{i=1}^{k} \left(1 + \frac{1}{p_i - 1}\right)$$
$$< \exp\left(\sum_{i=1}^{k} \frac{1}{p_i - 1}\right) < \exp\left(\frac{l}{(\log x) - 1}\right) < 2 \tag{7.11}$$

for $x \geqslant x_1$. Thus for $x \geqslant x_1$ we have $a \mid \sigma(a)$ if and only if $a = 1$. Putting this into (7.9) we see that for $x \geqslant x_1$ we have either $a = 1$ or $\sigma(b) \nmid \alpha b$. In fact we get even more. If $a' \mid a$, $(a', a/a') = 1$, and $a' < a$, then applying (7.11) to a/a' we have $\sigma(a'b) \nmid a' \cdot \alpha b$.

Let us see how we can reconstruct the number a given only b and an ordered k-tuple (with $k \geqslant 0$) of positive integers $\beta_1, \beta_2, \ldots, \beta_k$ satisfying (7.10). First if $k = 0$, then $a = 1$, and we are done. So suppose $k > 0$. Then $\sigma(b) \nmid \alpha b$ (if this fails then there can be no a at all), so let p_1 be the least prime that divides $\sigma(b)$ to a higher power than it divides αb. If $k = 1$, then $a = p_1^{\beta_1}$, so suppose $k > 1$. Let $b' = bp_1^{\beta_1}$. Then as before we may assume $\sigma(b') \nmid \alpha b'$; let p_2 be the least prime that divides $\sigma(b')$ to a higher power than it divides $\alpha b'$. If $k = 2$, then $a = p_1^{\beta_1} p_2^{\beta_2}$. If $k > 2$, we let $b'' = bp_1^{\beta_1} p_2^{\beta_2}$ and continue as before. This procedure either terminates with an integer $a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ or proves no a can exist satisfying (7.9). If a is constructed, it may or may not satisfy (7.9). But if some a satisfying (7.9) does exist, this procedure will find it.

Thus for $x \geqslant x_1$ the number of $n \leqslant x$ satisfying $\sigma(n) = \alpha n$ is at most BC, where B is the number of $b \leqslant x$ such that $v \mid b$ and for every prime p in b we have $p \leqslant \log x$ or $p \mid v$ and C is the number of ordered tuples of natural numbers satisfying (7.10).

From elementary combinatorics we have $C = 2^l$.

Note that we have $B \leqslant B_1 B_2 B_3$, where B_1 is the number of $b_1 \leqslant x$ of the form $q_1^{\gamma_1} q_2^{\gamma_2} \cdots q_t^{\gamma_t}$ where $q_1, q_2, \ldots, q_t$ are all of the primes in v exceeding $\log x$ and $\gamma_1, \gamma_2, \ldots, \gamma_t$ are natural numbers, B_2 is the number of $b_2 \leqslant x$ such that every

prime in b_2 is in the interval $(\log^{3/4}x, \log x]$, and B_3 is the number of $b_3 \leqslant x$ divisible by no prime exceeding $\log^{3/4}x$.

An upper bound for B_1 is the number of sequences $\gamma_1, \gamma_2, \ldots, \gamma_t$ of natural numbers such that

$$\gamma_1 + \gamma_2 + \cdots + \gamma_t \leqslant l .$$

Thus $B_1 \leqslant \binom{l}{t-1} \leqslant 2^l$.

The total number of prime factors in a choice for b_2 is at most $(\log x)/\log(\log^{3/4}x) \leqslant 2l$. Say the primes in $(\log^{3/4}x, \log x]$ are $r_1, r_2, \ldots, r_m$. Then B_2 is at most the number of sequences $\delta_1, \delta_2, \ldots, \delta_m$ of non-negative integers with

$$\delta_1 + \delta_2 + \cdots + \delta_m \leqslant 2l .$$

Thus again using elementary combinatorics, we have

$$B_2 \leqslant \binom{m+2l}{m} \leqslant 2^{m+2l} .$$

However, $m = \pi(\log x) - \pi(\log^{3/4}x)$, so that from the prime number theorem we have $m \sim (\log x)/\log\log x$. Since we have yet to use such a "big gun", we could rely instead on the more elementary inequality (1.1). To be specific, we use $\pi(z) < 2z/\log z$, which holds for all $z > 1$. Thus we have $m < 2l$, so that $B_2 \leqslant 2^{4l}$. (In fact, the inequality $\pi(z) < 2z/\log z$ can be proved by a very easy argument involving binomial coefficients, but we suppress the details.)

If p is a prime and p^β divides some choice for b_3, then $p^\beta \leqslant x$ so that $\beta \leqslant (\log x)/\log 2$. Thus B_3 is at most the number of ordered $\pi(\log^{3/4}x)$-tuples with each coordinate a non-negative integer at most $(\log x)/\log 2$. Thus

$$B_3 \leqslant (1 + (\log x)/\log 2)^{\pi(\log^{3/4}x)} \leqslant (1 + (\log x)/\log 2)^{\log^{3/4}x} \leqslant 2^l$$

for $x \geqslant x_2$.

From the above, if $x \geqslant x_2$, then $B \leqslant B_1 B_2 B_3 \leqslant 2^{6l}$. Since $C = 2^l$, if we have $x \geqslant x_0 = \max\{x_1, x_2\}$, then the number of $n \leqslant x$ with $\sigma(n) = \alpha n$ is at most 2^{7l}, proving the theorem. □

While it is clear that a smaller value of c_0 may be found from a more careful proof, it would be more interesting to replace c_0 with some function tending to 0, perhaps only in the special case $\alpha = 2$ corresponding to perfect numbers. As for lower bounds, we know of no α for which we can prove $\sigma(n) = \alpha n$ has infinitely many solutions. In fact, we cannot even prove that the number of solutions is unbounded as α varies. It is known that if for some α and k there are infinitely many solutions to $\sigma(n) = \alpha n$ with $\nu(n) = k$, then there are infinitely many even perfect numbers, a result due to Kanold in 1956. Pomerance (1977a) proved the following effective form of this theorem.

Theorem 7.12. *For any α and k there is an effectively computable constant $N(\alpha, k)$*

such that if $n > N(\alpha, k)$, $\sigma(n) = \alpha n$, *and* $\nu(n) = k$, *then* $n = em$, *where* e *is an even perfect number* $(e, m) = 1$, *and* $m \leq N(\alpha, k)$.

The bound $N(\alpha, k)$ is not very friendly, although it is primitive recursive as a function of k. In the special case of odd solutions n, there is a somewhat more reasonable bound. For example, if n is an odd perfect number with $\nu(n) = k$, then Heath-Brown (1994), improving on a result in Pomerance (1977a) showed

$$n \leq 4^{4^k}.$$

That n is bounded by some function of k (for odd perfect numbers) was first shown by L. E. Dickson in 1913.

In 1932, D. H. Lehmer proposed the following problem that is similar in flavor to the odd perfect number problem. Lehmer asked if there are any composite natural numbers n with $\varphi(n) \mid n-1$, where φ is Euler's function from elementary number theory. This is still unsolved today. We do know that the number of composite integers $n \leq x$ with $\varphi(n) \mid n-1$, is $O(x^{1/2}\log^{3/4} x)$, and that if $\varphi(n)$ divides $n-1$, $\nu(n) = k$, and $k > 1$, then

$$n \leq k^{2^k},$$

see Pomerance (1977b). This can be improved to $n \leq 4^{2^k}$ using the method of Heath-Brown (1994).

Consider the function $s(n) = \sigma(n) - n$, the sum of the proper divisors of n. Thus a perfect number n satisfies $s(n) = n$. For any natural number n, one may consider the *aliquot sequence* for n: $n, s(n), s(s(n)), \ldots$. An old conjecture of Catalan and Dickson is that any such sequence either terminates at 0 (by hitting a prime and becoming 0 two steps later) or becomes periodic. This has been proved for all $n \leq 275$. Guy and Selfridge (1975) instead conjecture that the set of n whose aliquot sequence is unbounded has positive lower asymptotic density.

A cycle of length 2 for the function $s(n)$ is called an *amicable pair*. Namely, this is a pair of distinct integers a, b such that $s(a) = b$ and $s(b) = a$. Such numbers have been studied since Pythagoras who noted that 220 and 284 are an amicable pair. In 1955, Erdős showed that the numbers which belong to an amicable pair have asymptotic density 0. In Pomerance (1981) it is shown that the number of integers up to x which belong to an amicable pair is at most $x \cdot \exp(-(\log x)^{1/3})$ if x is sufficiently large.

7.4. *Graphs on the integers*

Consider the coprime graph on $\mathbb{Z}$. This is the graph whose vertex set is $\mathbb{Z}$ and two integers a, b are connected by an edge if $(a, b) = 1$.

The problem that opens this chapter can be reworded as follows. What is the largest set $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ such that the induced coprime graph on $\mathcal{A}$ contains no edges? This is the case $k = 2$ of the following famous problem of Erdős. Namely, what is the largest set $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ such that the induced coprime

graph on $\mathcal{A}$ does not contain a complete graph on k vertices? Of course, the set of integers $n \leq N$ which have a prime factor among the first $k-1$ primes is such a set, and Erdős conjecture was that this set gives the maximum. This conjecture is fairly easily proved for $k=3$. The case $k=4$ was proved by Szabó and Tóth (1985). Finally this long-standing problem has been very recently settled completely by Ahlswede and Khachatrian (1995). First, they showed that there is a pair k, N for which the conjecture fails, and their example suggests that probably there are infinitely many integers k such that the conjecture fails for these k and certain small values of N. On the other hand, they proved that the following slightly weaker form of the conjecture is true: for every k there is a number $N_0 = N_0(k)$ such that for $N > N_0(k)$, up to N the set of multiples of the first $k-1$ primes gives the largest set with no k numbers pairwise coprime.

If $\mathcal{A} \subseteq \{1, 2, \ldots, N\}$ has $|\mathcal{A}| \geq \lfloor \frac{1}{2}N \rfloor + 1$, then we have seen that the coprime graph on $\mathcal{A}$ must contain an edge. Must it already contain many edges? The answer is yes, for as Erdős et al. (1980) show, there must be some $a \in \mathcal{A}$ with valence at least $cN/\log\log N$. Moreover, if $|\mathcal{A}| \geq (\frac{1}{2} + \varepsilon)N$, then the coprime graph on $\mathcal{A}$ contains at least $c(\varepsilon)N^2$ edges. They also show that if $|A| \geq (\frac{2}{3} + \varepsilon)N$, then the coprime graph on $\mathcal{A}$ contains at least $c(\varepsilon)N^3$ triangles, i.e. triplets a_1, a_2, a_3 with $(a_1, a_2) = (a_1, a_3) = (a_2, a_3) = 1$.

The coprime graph on $\mathbb{Z}$ has many edges so we might expect that if I_1 and I_2 are disjoint intervals of n consecutive integers, then the induced coprime graph on $I_1 \cup I_2$ contains a matching from I_1 to I_2. This is not the case, however. Suppose $I_1 = \{2, 3, 4\}$ and $I_2 = \{8, 9, 10\}$. Then any one-to-one correspondence between I_1 and I_2 must have at least one pair of even numbers in the correspondence. Another example: $I_1 = \{2, 3, 4, 5\}$, $I_2 = \{30, 31, 32, 33\}$. Here nothing can correspond with 30.

About 25 years ago, D. J. Newman conjectured that if $I_1 = \{1, 2, \ldots, n\}$ and I_2 is any interval of n consecutive integers, then there is a coprime matching from I_1 to I_2. (If $I_1 \cap I_2 \neq \emptyset$, we mean there is a one-to-one correspondence from I_1 to I_2 with corresponding numbers coprime. This can still be thought of as a matching in the coprime graph if we replace I_2 by $I_2 + \{n!\}$.) In Pomerance and Selfridge (1980), Newman's conjecture is proved by giving an algorithm for constructing a coprime matching and proving it works for every n. The proof involves effective estimates for the cardinality of the sets $S(x, u) = \{n \leq x: \varphi(n)/n \leq u\}$, where φ is Euler's function.

Consider now the divisor graph on $\mathbb{N}$. Here two distinct numbers a, b are connected by an edge if either $a \mid b$ or $b \mid a$. There are many attractive problems concerning the divisor graph; few of them are completely solved. The divisor graph is not as dense with edges as the coprime graph, so in general two n-element subsets of $\mathbb{N}$ should not be expected to contain a matching. Rather, we might consider the following. Let $f(n)$ be the least integer such that the divisor graph contains a matching from $\{1, 2, \ldots, n\}$ into $\{n+1, n+2, \ldots, f(n)\}$. The following result is due to Erdős and Pomerance (1980).

Theorem 7.13. *There are positive constants c_0, c_1 such that for all large n,*

$$c_0 n((\log n)/\log\log n)^{1/2} \leq f(n) \leq c_1 n(\log n)^{1/2}.$$

Proof. We present only the proof of the upper bound; the lower bound proof is much harder and not particularly combinatorial in flavor. We shall show that we may take c_1 as any number larger than 2.

Let $\varepsilon > 0$ be arbitrary. The divisor graph clearly contains a matching from the integers in $(n/\sqrt{\log n}, n]$ into the integers in $(n, n\lceil\sqrt{\log n}\rceil]$ – indeed, just multiply each number in the first interval by $\lceil\sqrt{\log n}\rceil$. It will thus be sufficient to show the divisor graph contains a matching from I to J, where

$$I = [1, n/\sqrt{\log n}] \cap \mathbb{N}, \qquad J = (n\lceil\sqrt{\log n}\rceil, (2+\varepsilon)n\sqrt{\log n}] \cap \mathbb{N}.$$

We consider in fact only the subgraph where $a \in I$, $b \in J$ are connected by an edge if b/a is prime.

If $a \in I$, the number of primes p such that $pa \in J$ is, by the prime number theorem,

$$\begin{aligned}
&\pi\left(\frac{1}{a}(2+\varepsilon)n\sqrt{\log n}\right) - \pi\left(\frac{1}{a}n\lceil\sqrt{\log n}\rceil\right) \\
&> (1+\tfrac{1}{2}\varepsilon)\frac{n\sqrt{\log n}}{a\log(a^{-1}n\sqrt{\log n})} \\
&\geqslant (1+\tfrac{1}{2}\varepsilon)\frac{\log n}{\log\log n}
\end{aligned}$$

if $n \geqslant n_0$, uniformly for al $a \in I$. On the other hand, if $b \in J$, the maximal number of $a \in I$ that can correspond to b is at most the number of primes p that divide b with $p \geqslant \log n$. Since $b \leqslant (2+\varepsilon)n\sqrt{\log n}$, this number evidently is at most

$$\frac{\log((2+\varepsilon)n\sqrt{\log n})}{\log\log n} < (1+\tfrac{1}{2}\varepsilon)\frac{\log n}{\log\log n}$$

for $n \geqslant n_1$. Thus for $n \geqslant \max\{n_0, n_1\}$, the König–Hall marriage lemma (see chapter 3) implies there is a matching from I into J. □

What is the length $H(n)$ of the longest simple path in the divisor graph on $\{1, 2, \ldots, n\}$? Hegyvári conjectured $H(n) = o(n)$ and this was proved by Pomerance (1983). It would be nice to get an asymptotic formula for $H(n)$. Recently, Saias and Tenenbaum have obtained fairly sharp estimates for $H(n)$. Other problems of a similar nature are considered in Erdős et al. (1983).

7.5. Egyptian fractions

The ancient Egyptians thought fractions $1/a$ where $a \in \mathbb{N}$ were especially nice. There is today a wide body of literature and many problems and results concerning Egyptian fractions – see section 4 in Erdős and Graham (1980) and section D11 of Guy (1994).

It has been known since Fibonacci that every positive rational r can be expressed as a finite sum of distinct Egyptian fractions. In fact, the greedy algorithm of choosing a_{n+1} minimal with $a_{n+1} > a_n$ and $1/a_1 + \cdots + 1/a_{n+1} \leqslant r$

always terminates. However, a representation of r as a sum of distinct Egyptian fractions is certainly not unique and this fact leads to many questions. For example, what is the fewest number of summands for r? Or, how many ways are there to write r as a sum of n distinct Egyptian fractions as $n \to \infty$? For the latter question, the case $r = 1$ has special interest.

It has been conjectured by Erdős and Straus that for every integer $n > 1$, $4/n$ can be written as a sum of three Egyptian fractions. This has been verified numerically for small values of n and has been shown true for all n but for a possible exceptional set of asymptotic density 0. More generally, Schinzel and Sierpiński have conjectured that every positive rational a/b can be expressed as a sum of three Egyptian fractions provided the denominator b is sufficiently large as a function of the numerator a. This is easily seen not to be true for a sum of two Egyptian fractions. For example, if p is a prime with $p \equiv 1 \pmod 3$, then $3/p = 1/x + 1/y$ is not solvable in integers.

7.6. *Pseudoprimes*

From Fermat's little theorem, if n is prime and $a \not\equiv 0 \pmod n$, then

$$a^{n-1} \equiv 1 \pmod n . \tag{7.14}$$

The congruence (7.14) is very useful for testing large numbers n for primality. Indeed, even if n is very large, it is a relatively simple matter to compute the least non-negative residue of $2^{n-1} \pmod n$; if this is not 1 (and $n > 2$), then n is composite. The residue may be found in $O(\log n)$ multiplications $(\bmod n)$ using the repeated squaring method. However, this method is not perfect – sometimes we come across composite numbers n that nevertheless satisfy (7.14) for some a. The least example with $a = 2$ is $n = 341$, and with $a = 3$ is $n = 91$. We say n is a *pseudoprime to the base a* if n is a composite natural number and (7.14) holds.

Let $P_a(x)$ denote the number of base a pseudoprimes up to x. Can we prove that for a fixed a we have $P_a(x) = o(\pi(x))$; that is, that base a pseudoprimes are rare compared with primes? Certainly not for $a = \pm 1$, since then (7.14) has many composite solutions. However, for $|a| > 1$, Erdős showed in 1956 that $P_a(x) = o(\pi(x))$ does in fact hold. The best result in this direction is due to Pomerance in 1981.

Theorem 7.15. *For each integer a with $|a| > 1$, there is a number $x_0(a)$ such that for $x \geq x_0(a)$ we have $P_a(x) \leq x^{1-\varepsilon(x)/2}$, where*

$$\varepsilon(x) = (\log\log\log x)/\log\log x . \tag{7.16}$$

In 1956, Erdős conjectured that $P_a(x) > x^{1-c\varepsilon(x)}$ for some $c > 0$ and x sufficiently large and where $\varepsilon(x)$ is defined in (7.16). This conjecture was refined by Pomerance to the following.

Conjecture 7.17. For each integer a with $|a|>1$, we have

$$P_a(x) = x^{1-(1+o_a(1))\varepsilon(x)}.$$

One might wonder if a number n can be simultaneously a pseudoprime to the bases 2 and 3. This in fact can happen; the least example is $n = 1105$. It is not known if there are infinitely many such n. There are numbers n which are a pseudoprime to *every* base a with $(a, n) = 1$. Such numbers are called *Carmichael numbers*; the smallest example is $n = 561$. If $C(x)$ is the number of Carmichael numbers up to x, it is known that $C(x) \leqslant x^{1-\varepsilon(x)}$ for x sufficiently large and it is conjectured that $C(x) = x^{1-(1+o(1))\varepsilon(x)}$. Alford et al. (1994) recently proved there are infinitely many Carmichael numbers. In fact they showed the following.

Theorem 7.18. *For all sufficiently large values of* x, $C(x) > x^{2/7}$.

The proof, which roughly follows a heuristic argument given by Erdős in 1956, has some strong combinatorial elements.

We remark that any composite number n with $\varphi(n) \mid n-1$ must also be a Carmichael number, but no such n are known to exist (see the earlier remarks on perfect numbers).

Acknowledgements

As mentioned in the Introduction, Paul Erdős played an important role in the writing of this chapter. In addition we gratefully acknowledge assistance from Adolf Hildebrand, Helmut Maier, and Melvyn Nathanson. We also thank the editors of this Handbook for their patience and encouragement.

References

Ahlswede, R., and L.H. Khachatrian
[1995] Maximal sets of numbers not containing $k+1$ pairwise coprime integers, *Acta Arithm.*, to appear.
Ajtai, M., J. Komlós and E. Szemerédi
[1981] A dense infinite Sidon sequence, *European J. Combin.* **2**, 1–11.
Alford, W.R., A. Granville and C. Pomerance
[1994] There are infinitely many Carmichael numbers, *Ann. of Math.* **140**, 703–722.
Andrews, G.E.
[1976] *The Theory of Partitions* (Addison-Wesley, Reading, MA).
Balasubramanian, R., and K. Soundararajan
[1995] On a conjecture of R.L. Graham, to appear.
Balasubramian, R., J.-M. Deshouillers and F. Dress
[1986] Probleme de Waring pour les bicarrés. I. Schéma de la solution, *C.R. Acad. Sci. Paris Sér. I Math.* **303**(4), 85–88.
Bourgain, J.
[1990] On arithmetic progressions in sums of sets of integers, in: *A Tribute to Paul Erdős*, eds. A. Baker, B. Bollobás and A. Hajnal (Cambridge University Press, Cambridge) pp. 105–109.

Cheng, F.Y., and C. Pomerance
[1994] On a conjecture of R.L. Graham, *Rocky Mountains J. Math.* **24**, 961–975.
Dekking, F.M.
[1979] Strongly non-repetitive sequences and progression-free sets, *J. Combin. Theory A* **27**, 181–185.
Erdős, P.
[1940] The difference of consecutive primes, *Duke Math. J.* **6**, 438–441.
[1956] Problems and results in additive number theory, in: *Colloque sur la Thórie des Nombres, Bruxelles, 1955* (Georges Thone/Masson and Cie, Liège/Paris) pp. 127–137.
Erdős, P., and R.L. Graham
[1980] *Old and New Problems and Results in Combinatorial Number Theory* (L'Enseignement Mathématique, Université de Genève, Monographie No. 28).
Erdős, P., and M.B. Nathanson
[1987] Problems and results on minimal bases in additive number theory, in: *Number Theory, New York 1984/1985, Lecture Notes in Mathematics*, Vol. 124, eds. D.V. Chudnovsky et al. (Springer, Berlin) pp. 87–96.
[1988] Minimal asymptotic bases with prescribed densities, *Ill. J. Math.* **32**, 562–574.
Erdős, P., and C. Pomerance
[1980] Matching the natural numbers up to n with distinct multiples in another interval, *Nederl. Akad. Wetensch. Proc. A* **83**, 147–161.
[1986] On the number of false witnesses for a composite number, *Math. Comp.* **46**, 259–279.
Erdős, P., A. Sárközy and E. Szemerédi
[1970] On divisibility properties of sequences of integers, in: *Number Theory, Colloq. Math. Soc. János Bolyai* **2**, 35–49.
[1980] On some extremal properties of sequences of integers. II, *Publ. Math. Debrecen* **27**, 117–125.
Erdős, P., R. Freud and N. Hegyvári
[1983] Arithmetical properties of permutations of integers, *Acta Math. Acad. Sci. Hungar.* **41**, 169–176.
Erdős, P., A. Sárközy and V.T. Sós
[1986] Problems and results on additive properties of general sequences, V, *Monatsh. Math.* **102**, 183–197.
Erdős, P., H. Maier and A. Sárközy
[1987] On the distribution of the number of prime factors of sums $a+b$, *Trans. Amer. Math. Soc.* **302**, 269–280.
Erdős, P., C. Pomerance, A. Sárközy and C.L. Stewart
[1993] On elements of sumsets with many prime factors, *J. Number Theory* **44**, 93–104.
Freiman, G.A.
[1973] *Foundations of a Structural Theory of Set Additions, Translations of Mathematical Monographs*, Vol. 37 (American Mathematical Society, Providence, RI).
Freiman, G.A., H. Halberstam and I.Z. Rusza
[1992] Integer sums containing long arithmetic progressions, *J. London Math. Soc.* **46**, 193–201.
Graham, R.L., B.L. Rothschild and J.H. Spencer
[1980] *Ramsey Theory* (Wiley, New York).
Guy, R.K.
[1994] *Unsolved Problems in Number Theory*, 2nd Ed. (Springer, New York).
Guy, R.K., and J.L. Selfridge
[1975] What drives an aliquot sequence? *Math. Comp.* **29**, 101–107. Corrigendum: 1980, **34**, 319–321.
György, K., C.L. Stewart and R. Tijdeman
[1988] On prime factors of sums of integers, III, *Acta Arithm.* **49**, 307–312.
Halberstam, H., and H.-E. Richert
[1974] *Sieve Methods* (Academic Press, London).
Halberstam, H., and K.F. Roth
[1983] *Sequences*, 2nd Ed. (Springer, New York).
Hall, R.R., and G. Tenenbaum
[1988] *Divisors* (Cambridge University Press, Cambridge).

Hayashi, E.K.
[1981] Omega theorems for the iterated additive convolution of a nonnegative arithmetic function, *J. Number Theory* **13**, 176–191.
Heath-Brown, D.R.
[1994] Odd perfect numbers, *Math. Proc. Cambridge Philos. Soc.* **115**, 191–196.
Iwaniec, H.
[1981] Rosser's sieve-bilinear forms of the remainder terms – some applications, in: *Recent Progress in Analytic Number Theory, Durham 1979*, Vol. 1, eds. H. Halberstam and C. Hooley (Academic Press, London) pp. 203–230.
Maier, H.
[1988] Small differences between prime numbers, *Michigan Math. J.* **35**, 323–344.
Montgomery, H.L.
[1971] *Topics in Multiplicative Number Theory, Lecture Notes in Mathematics*, Vol. 27 (Springer, New York).
Montgomery, H.L., and R.C. Vaughan
[1990] On the Erdős–Fuchs theorem, in: *A Tribute to Paul Erdős*, eds. A. Baker, B. Bollobás and A. Hajnal (Cambridge University Press, Cambridge) pp. 331–338.
Nathanson, M.B.
[1989] Additive problems in combinatorial number theory, in: *Number Theory, New York 1985/1988, Lecture Notes in Mathematics*, Vol. 1383, eds. D.V. Chudnovsky et al. (Springer, Berlin) pp. 123–139.
Nathanson, M.B., and A. Sárközy
[1989] On the maximum density of minimal asymptotic bases, *Proc. Amer. Math. Soc.* **105**, 31–33.
Ostmann, H.
[1956] *Additive Zahlentheorie*, Vols. I, II (Springer, Berlin).
Pintz, J., W.L. Steiger and E. Szemerédi
[1988] On sets of natural numbers whose difference set contains no squares, *J. London Math. Soc. (2)* **37**, 219–231.
Pomerance, C.
[1977a] Multiply perfect numbers, Mersenne primes and effective computability, *Math. Ann.* **226**, 195–206.
[1977b] On composite n for which $\varphi(n)|n-1$, II, *Pacific J. Math.* **69**, 177–186.
[1980] Collinear subsets of lattice point sequences – an analog of Szemerédi's theorem, *J. Combin. Theory A* **28**, 140–149.
[1981] On the distribution of amicable numbers, II, *J. Angew. Math.* **325**, 183–188.
[1983] On the longest simple path in the divisor graph, *Congress. Numerantium* **40**, 291–304.
Pomerance, C., and A. Sárközy
[1988] On homogeneous multiplicative hybrid problems in number theory, *Acta Arithm.* **49**, 291–302.
[1990] On products of sequences of integers, in: *Number Theory, Budapest 1987*, eds. K. György and G. Halász, Vol. 1, *Colloq. Math. Soc. János Bolyai* **51**, 447–467.
Pomerance, C., and J.L. Selfridge
[1980] Proof of D.J. Newman's coprime mapping conjecture, *Mathematika* **27**, 69–83.
Pritchard, P.A., A. Moran and A. Thyssen
[1995] Twenty-two primes in arithmetic progression, *Math. Comp.*, to appear.
Ramsey, L.T., and J.L. Gerver
[1979] On certain sequences of lattice points, *Pacific J. Math.* **83**, 357–363.
Ruzsa, I.Z.
[1987] Essential components, *Proc. London Math. Soc. (3)* **54**, 38–56.
[1990/91] An application of graph theory to additive number theory, *Scientia (Chile)* **4**, 93–94.
Sárközy, A.
[1989a] Hybrid problems in number theory, in: *Number Theory, New York 1985/1988, Lecture Notes in Mathematics*, Vol. 1383, eds. D.V. Chudnovsky et al. (Springer, Berlin) pp. 146–169.
[1989b] Finite addition theorems, I, *J. Number Theory* **32**, 114–130.
[1994] Finite addition theorems, II, *J. Number Theory* **48**, 197–218.

Shelah, S.
[1988] Primitive recursive bounds for van der Waerden numbers, *J. Amer. Math. Soc.* **1**, 683–697.
Stewart, C.L., and R. Tijdeman
[1983] On density-difference sets of integers, in: *Studies in Pure Mathematics – to the Memory of Paul Turán* (Birkhäuser/Hungarian Academy of Science, Basel/Budapest) pp. 701–710.
Stöhr, A.
[1955] Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I, II, *J. Reine Angew. Math.* **194**, 40–65; 111–140.
Szabó, C., and G. Tóth
[1985] Maximal sequences not containing 4 pairwise comprime integers (in Hungarian), *Mat. Lapok* **32**, 253–257.
Szegedy, M.
[1986] The solution of Graham's greatest common divisor problem, *Combinatorica* **6**, 67–71.
Szemerédi, E.
[1970] On a conjecture of Erdős and Heilbronn, *Acta Arithm.* **17**, 227–229.
Vaughan, R.C.
[1981] *The Hardy–Littlewood Method* (Cambridge University Press, Cambridge).
Wirsing, E.
[1957] Über die Dichte multiplikativer Basen, *Arch. Math.* **8**, 11–15.
[1959] Bemerkung zu der Arbeit über vollkommene Zahlen, *Math. Ann.* **137**, 316–318.
Zaharescu, A.
[1987] On a conjecture of Graham, *J. Number Theory* **27**, 33–40.