73/21

J. N. Srivastava et al., eds., *A Survey of Combinatorial Theory*

CHAPTER 12

Problems and Results on Combinatorial Number Theory

P. ERDŐS

Hungarian Academy of Sciences, Budapest, Hungary

I will discuss in this paper number theoretic problems which are of combinatorial nature. I certainly do not claim to cover the field completely and the paper will be biased heavily towards problems considered by me and my collaborators. Combinatorial methods have often been used successfully in number theory (e.g. sieve methods), but here we will try to restrict ourselves to problems which themselves have a combinatorial flavor. I have written several papers in recent years on such problems and in order to avoid making this paper too long, wherever possible, will discuss either problems not mentioned in the earlier papers or problems where some progress has been made since these papers were written.

Before starting the discussion of our problems I give a few of the principal papers where similar problems were discussed and where further literature can be found.

I. P. Erdös, On unsolved problems, *Publ. Math. Inst. Hung. Acad.* **6** (1961) 229–254; Some unsolved problems, *Michigan Math. J.* **4** (1957) 291–300.

II. P. Erdös, Remarks on number theory IV and V. Extremal problems in number theory I and II *Mat. Lapok* **13** (1962) 28–38; **17** (1966) 135–166. See also: P. Erdös, *Proc. Symp. Pure Math.*, vol. 8 (Am. Math. Soc., Providence, R.I.), pp. 181–189.

III. P. Erdös, Some recent advances and current problems in number theory, *Lectures on modern mathematics*, vol. III (L. Saaty, ed.), pp. 196–244.

IV. P. Erdös, Some extremal problems in combinatorial number theory, *Math. Essays dedicated to A. J. Macintyre* (H. Shankar, ed.; Ohio Univ. Press, Athens, Ohio, 1971), pp. 123–133.

V. P. Erdös, Some problems in number theory, *Computers in Number Theory* (Academic Press, London, 1971), pp. 406–414.

VI. H. Halberstam and K. F. Roth, *Sequences* (Oxford Univ. Press, London, 1966).

VII. A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I and II, *J. Reine Angew. Math.* **194** (1955) 40–65, 111–140.

Many interesting unsolved problems of a combinatorial and number theoretic nature are mentioned in the proceedings of the meetings on number theory held in Boulder, Colorado, in 1959 and 1963. See also a forthcoming book of Croft and Guy.

1. Denote by $r_k(n)$ the maximum number of integers not exceeding n which do not contain an arithmetic progression of k terms. The first publication on $r_k(n)$ was due to Turán and myself (Erdös and Turán [1936]). We were lead to this problem by the following two facts: $r_k(n) < \frac{1}{2}n$ for $n > n_0(k)$ would immediately imply the well known theorem of Van der Waerden that if we split the integers into two classes, then at least one class contains arbitrarily long arithmetic progressions. If we could prove $r_k(n) < \pi(n)$ ($\pi(n)$ is the number of primes not exceeding n) for every k if $n > n_0(k)$, we would obtain that there are arbitrarily long arithmetic progressions among the primes. Unfortunately, none of these results have been proved so far. The best inequalities for $r_3(n)$ are due to Behrend [1946] and Roth [1953]:

$$n^{1-c_1/(\log n)^{\frac{1}{2}}} < r_3(n) < c_2 n/\log\log n.$$

A weaker lower bound has been proved earlier by Salem and Spencer.

L. Moser constructed an infinite $a_1 < \cdots$ of integers not containing an arithmetic progression of three terms so that for every n

$$\sum_{a_i \leqslant n} 1 > n^{1-c/(\log n)^{\frac{1}{2}}}.$$

Moser also raised the following interesting problem: Denote by $f_3(n)$ the largest integer so that one can find $f(n)$ lattice points in the n-dimensional cube

$$\{x_1^{(r)}, \ldots, x_n^{(r)}\},\ x_i^{(r)} \text{ is } 0, 1 \text{ or } 2,\ 1 \leqslant i \leqslant n;\ 1 \leqslant r \leqslant f_3(n)$$

no three of which are on a straight line. Clearly $f_3(n) \geqslant r_3(3^n)$. Moser showed that

$$f_3(n) > c3^n/\sqrt{n} \tag{1.1}$$

and asks: is it true that $f_3(n) = o(3^n)$? (1.1) has never been improved. It is easy to see that $\lim f_3(n)/3^n$ exists. One can easily generalize this question when the x_i can take k integral values, but nothing seems to be known.

The following problem is due to Straus: Let $a_1 < \cdots < a_k \leqslant x$ be such that no a_i is the arithmetic mean of any subset of the a's consisting of two or more elements. Put max $k = F(x)$. We have

$$\exp (2 \log x)^{\frac{1}{2}} < F(x) < cx^{\frac{2}{3}}. \tag{1.2}$$

The lower bound in (1.2) is due to Straus [1967] and the upper bound to Erdös and Straus [1970] (these papers contain other related problems and results on combinatorial number theory). Straus conjectures that in (1.2) the lower bound is the correct one, but even $F(x) = o(x^{\varepsilon})$ seems very difficult to obtain.

Recently, Szemerédi [1969] (see also Behrend [1946]) proved $r_4(n) = o(n)$; his very complicated proof is a masterpiece of combinatorial reasoning.

Recently, Roth [1970] obtained a more analytical proof of $r_4(n) = o(n)$. $r_5(n) = o(n)$ remains undecided. Very recently, Szemerédi proved $r_5(n) = o(n)$.

Rankin [1962] proved that for every $k \geqslant 3$ ($\exp z = e^z$)

$$r_k(n) > n \exp\left(-c(\log n)^{1/(k-1)}\right)$$

and also investigated the question of the densest sequence of integers which do not contain a geometric progression of k terms. Riddell [1969] obtains sharper results, but many interesting questions remain unsettled.

Riddell [1969] defines $g_k(n)$ as the largest integer so that among any n real numbers one can always find $g_k(n)$ of them which do not contain an arithmetic progression of k terms. It is not hard to see that without loss of generality we can always assume that the real numbers are in fact positive integers. $r_3(5) = 4$, but Riddell showed $g_3(5) = 3$ (from the set 1, 3, 4, 5, 7 one can select only 3 integers not containing an arithmetic progression of three terms). $r_3(14) = 8$, but Riddell recently showed $g_3(14) \leqslant 7$ (he feels that $g_3(14) = 7$). Riddell, with the help of a computer, showed that any subset of 8 elements of

$$0, 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15, 16, 18$$

contains an arithmetic progression of three terms, thus $g_3(14) \leqslant 7$.

Trivially, $g_k(n) \leqslant r_k(n)$, and we cannot disprove that for large n, $g_3(n) = r_3(n)$. Riddell proved very simply that $g_3(n) > c\sqrt{n}$ and for $k > 3$, $g_k(n) > cn^{1-(2/k)}$. Riddell and I recently slightly improved this, e.g., we showed $g_4(n) > cn^{\frac{2}{3}}$. It seems certain that $g_3(n) > n^{1-\varepsilon}$ for every ε if $n > n_0(\varepsilon)$, but even the proof of $\lim g_3(n)/n^{\frac{1}{2}} = \infty$ seems to present difficulties. (Szemerédi just writes that he proved $g_3(n) > n^{1-\varepsilon}$.)

The following problem might be of interest in this connection: Let $f_k(n)$, $k > 3$, be the largest integer so that there is a sequence of integers $a_1 < \cdots < a_n$ which contains $f_k(n)$ arithmetic progressions of three terms but no progression of k terms. It is easy to see that $f_4(3^n) \geqslant 5^{n-1}$ and G. Simmons considerably improved this estimate. We proved that for every $k > 3$

$$\lim_{n\to\infty} \log f_k(n)/\log n = c_k$$

exists, but we do not know if $c_k < 2$. In fact, we do not know if $f_4(n) = o(n^2)$.

Kleitman and I observed that 1, 2, 3 and 1, 3, 4, 5, 7 are essentially the only sets of integers where every pair is contained in a three term arithmetic progression. It is not clear to us at this moment if there are sequences $a_1, \ldots, a_n$ which do not form an arithmetic progression but where every pair is contained in some arithmetic progression other than arithmetic progressions of even length and even difference with the middle integer (this example is due to Jeffrey Lagaris).

Denote by $P(n, k)$ (Riddell [1969]) the largest integer so that amongst n points in k-dimensional space one can always find $P(n, k)$ which do not contain an isosceles triangle. Clearly $P(n, 1) = g_3(n)$. It is not hard to prove by induction with respect to k that

$$P(n, k) > n^{\varepsilon_k},$$

but it is not easy to determine (or estimate) the best value of ε_k. I expect $P(n, 2) < n^{1-c}$. In fact, it seems probable that amongst the lattice points (x, y), $0 \leqslant x, y \leqslant n$, x, y integer, one cannot select $n^{2-\varepsilon}$ of them which do not determine an isosceles triangle. A technique used by Guy and myself (Erdös and Guy [1959]) seems to give that one can give cn such points — I would guess that one can give more than n^{1+c} for some $c > 0$.

As far as I know, questions of the following type have not yet been investigated: Let there be given cn^2 lattice points (x_i, y_i) $(0 \leqslant x_i, y_i \leqslant n)$. Is it true that they determine four vertices of a square whose sides are parallel to the axes? Clearly many generalizations are possible which we leave to the reader. Improving a previous result of Rennie Abbott and Hanson recently proved that one can give $n^{\log 5/\log 3}$ lattice points (x_i, y_i), $0 \leqslant x_i, y_i \leqslant n$ which do not contain four vertices of a square whose sides are parallel to the axes. Very recently Aytai found $n^{2-\varepsilon}$ such lattice points.

Before ending this chapter, I mention a problem considered in Riddell [1969]. Let $a_1 < \cdots < a_n$ be any set of real numbers. Denote by $l(n)$ the largest integer so that one can always find $l(n)$ of them, $a_{i_1}, \ldots, a_{i_r}$, $r \geqslant l(n)$ so that all the sums $a_{i_{j_1}} + a_{i_{j_2}}$, $1 \leqslant j_1 \leqslant j_2 \leqslant r$ are distinct. It is known that

$$cn^{\frac{1}{3}} < l(n) \leqslant (1+o(1))n^{\frac{1}{2}}. \tag{1.3}$$

In (1.3), probably the upper bound is the right one. Szemerédi and Komlós proved a slightly weaker upper bound $cn^{\frac{1}{2}}$. Many generalizations are possible for more than two summands or vectors in higher dimensions.

2. The theorem of Van der Waerden states that there is a smallest integer $f(n)$ so that if we split the integers from 1 to $f(n)$ into two classes, at least one contains an arithmetic progression of n terms. Van der Waerden obtains a very poor upper bound for $f(n)$ and it would be very desirable to obtain a more reasonable upper bound for it. The best lower bound for $f(n)$ is due to Berlekamp [1968] who proved $f(p) > p2^p$, sharpening previous results of Rado, Schmidt and myself. It would be very interesting to decide whether $f(n) < c^n$ holds for a certain constant c.

Perhaps the following modification of the problem is more amenable to attack: Denote by $f(c, n)$, $\frac{1}{2} < c \leqslant 1$, the smallest integer so that if we split the integers from 1 to $f(c, n)$ into two classes, there is an arithmetic progression of n terms so that at least cn of its terms belong to the same class. $f(1, n)$ clearly equals $f(n)$. By probability methods it is not hard to show that for every $c > \frac{1}{2}$, $f(c, n) > (1+\varepsilon_c)^n$. I never could get a good upper bound for $f(c, n)$. Perhaps $f(c, n) < c^n$, at least if c is sufficiently close to $\frac{1}{2}$ (Erdös [1963]).

A related problem was considered by Roth [1964, 1967]. Let $g(n) = \pm 1$ be an arbitrary number theoretic function. Put

$$F(x) = \min_{g(n)} \max |\sum g(a+kd)|,$$

where the maximum is to be taken over all arithmetic progressions whose terms are positive integers not exceeding x and the minimum is to be taken over all the functions $g(n) = \pm 1$. Roth proved that

$$F(x) > cx^{\frac{1}{4}}$$

and conjectured $F(x) > x^{\frac{1}{2}-\varepsilon}$ for every $\varepsilon > 0$ if $x > x_0(\varepsilon)$.

Y. Spencer recently proved

$$F(x) < cx^{\frac{1}{2}} \frac{\log \log x}{\log x},$$

he uses probabilistic methods, his proof will be published soon. These results will also be treated in the forthcoming booklet of Y. Spencer and myself on probabilistic methods in combinatorial analysis.

Many years ago, Cohen asked the following question. Determine or estimate a function $f(d)$ so that if we split the integers into two classes, at least one class contains for infinitely many values of d an arithmetic progression of length $f(d)$. I showed $f(d) < cd$. To see this, let α be a quadratic irrationality, say $\sqrt{5}$. n belongs to the first class if the fractional part of $n\alpha$ is less than $\frac{1}{2}$ and in the second class otherwise. From the well known fact that $|\alpha - p/q| > c_1/q^2$, it easily follows that $f(d) < cd$. I have not been able to show that $f(d) < \varepsilon d$ for sufficiently small ε and I have not succeeded in getting a lower estimation for $f(d)$. Van der Waerden's theorem certainly implies that $f(d) \to \infty$.

Let $g(n) = \pm 1$ be an arbitrary number theoretic function. Cantor, Schreiber, Straus and I [II] proved that there is such a $g(n)$ for which

$$\max_{a,m,1 \leqslant b \leqslant d} \left| \sum_{k=1}^{m} g(a+kb) \right| < h(d)$$

for a certain function $h(d)$. Van der Waerden's theorem implies $h(d) \to \infty$ as $d \to \infty$. We showed $h(d) < (cd)!$. We have no good lower bound for $h(d)$ and are not sure how good our upper bound is. As far as I know the following related more general question is still unsolved: Let

$$A_k = \{a_1^{(k)} < \cdots\},\ k = 1, 2, \ldots$$

be infinitely many infinite sequences of integers. Does there exist a function $F(d)$ (which depends on the sequences A_k) so that for a suitable $g(n) = \pm 1$

$$\max_{m,1 \leqslant k \leqslant d} \left| \sum_{i=1}^{m} g(a_i^{(k)}) \right| < F(d)?$$

It seems certain that the answer is affirmative.

I conjectured more than thirty years ago that if $f(n) = +1$ and $f(n)$ is multiplicative then

$$\lim_{n=\infty} \frac{1}{n} \sum_{k=1}^{n} f(k)$$

exists and is 0 if and only if $\sum_{f(p)=-1} 1/p = \infty$. Wintner observed that the conjecture fails if we only assume $|f(n)| = 1$ and $f(n)$ is multiplicative. Wirsing [1967] proved (and generalized) my conjecture and Halász [1968] obtained a still more general result.

Finally, I would like to mention an old conjecture of mine: let $f(n) = \pm 1$ be an arbitrary number theoretic function. Is it true that to every c there is a d and an m so that

$$\left|\sum_{k=1}^{m} f(kd)\right| > c?$$

I have made no progress with this conjecture.

Sanders and Folkman proved the following result (which also follows from earlier results of Rado [1933]): For every n there is a $g(n)$ so that if we split the integers not exceeding $g(n)$ into two classes, there always is a sequence $a_1 < \cdots < a_n$ so that all the sums

$$\sum_{i=1}^{n} \varepsilon_i a_i,\ \varepsilon_i = 0 \text{ or } 1 \text{ (not all } \varepsilon_i = 0)$$

belong to the same class. As far as I know there are no good upper or lower bounds for $g(n)$. The result of Sanders and Folkman also follows from the general theorems of Graham and Rotschild.

Graham and Rotschild ask the following beautiful question: split the integers into two classes. Is there always an infinitive sequence so that all the finite sums

$$\sum \varepsilon_i a_i,\ \varepsilon_i = 0 \text{ or } 1 \text{ (not all } \varepsilon_i = 0) \tag{2.1}$$

all belong to the same class? It is not even known if there is an infinite sequence so that all the sums (2.1) with $\sum \varepsilon_i = k$, $k = 1, 2, \ldots$, belong to the same class where the class may depend on k.

This problem seems very difficult. As far as I know, the following simpler question is also unsolved: Does there exist an infinite sequence $a_1 < \cdots$ so that all the numbers

$$a_i,\ i = 1, 2, \ldots \quad \text{and} \quad a_i + a_j,\ 1 \leqslant i < j < \infty$$

all belong to the same class? Galvin recently asked the following question: Does there exist a sequence $a_1 \cdots a_n$, $a_1 \leqslant n$ so that all the numbers $a_1 < \cdots < a_n$ and $a_i + a_j$, $1 \leqslant i < j \leqslant n$ belong to the same class?

3. Denote by $f(k, x)$ the largest integer r so that there is a sequence $a_1 < \cdots < a_r \leqslant x$ no $k+1$ of which are pairwise relatively prime. It seems certain that we obtain $f(k, x)$ by considering the set of multiples of the first r primes. The proof seems to present unexpected difficulties — recently, Szemerédi states that he proved this conjecture for sufficiently large r.

A more general conjecture would be: Denote by $f(p_s, k, x)$ the largest integer r so that there is a sequence $a_1 < \cdots < a_r \leqslant x$ all prime factors of the a's are $\geqslant p_s$ and no $k+1$ of them are relatively prime. One would expect to obtain $f(p_s, k, x)$ by considering the set of integers not exceeding x of the form $p_{s+i}t$, $1 \leqslant i \leqslant k$, where all prime factors of t are $\geqslant p_{s+i}$. I have not even been able to show this for $k = 1$ and all s.

A problem of Graham and myself states: Let $a_1 < \cdots < a_k = n$, $(a_i, a_j) = 1$. What is the maximum of k? A reasonable guess seems to be that max k either equals n/p where p is the smallest prime factor of n or it is the number of integers of the form $2t$, $t \leqslant \frac{1}{2}n$, $(t, n) = 1$. (See a forthcoming paper of Graham and myself in *Acta Arithmetica.*)

4. Let $a_1 < \cdots < a_k \leqslant x$. Assume that no r ($r \geqslant 3$) a's have pairwise the same greatest common divisor. Put max $k = f_r(x)$. I proved $f_r(x) < x^{\frac{3}{4}+\varepsilon}$ (Erdös [1964a]). This was improved to $x^{\frac{1}{2}+\varepsilon}$ by Abbott and Hanson [1970]. In Erdös [1964a], I showed that

$$f_3(x) > \exp(c_1 \log x/\log\log x)$$

and I stated in Erdös [1964a] that it is likely that

$$f_3(x) < \exp(c_2 \log x/\log\log x). \tag{4.1}$$

(4.1) is intimately connected with the following purely combinatorial problem of Erdös and Rado [1960]: Let $g_r(n)$ be the smallest integer with the following property: Let $|A_i| = n$, $1 \leqslant i \leqslant g_r(n)$; then there are always r A's which have pairwise the same intersection. Rado and I proved $g_r(n) < c_r^n n!$ and conjectured

$$g_r(n) < c_r^n. \tag{4.2}$$

(4.2) would have many applications in combinatorial number theory. It is easy to see that (4.2) if true is best possible apart from the value of c_r. Abbott [1966] improved our upper and lower bounds for $g_r(n)$, but no real progress has been made with the conjecture (4.2).

I stated in Erdös [1964a] that (4.2) would imply (4.1). Abbott pointed out to me that (4.2) does not seem to suffice. The following slightly stronger conjecture is easily seen to imply (4.1): Let $g_r'(n)$ be the smallest integer so that if u_i, $1 \leqslant i \leqslant g_r(n)$, are integers satisfying

$$u_i = \prod_j p_j^{\alpha_j}, \qquad \sum \alpha_j = n \qquad (p_j \text{ prime}, \alpha_j \geqslant 0 \text{ integer})$$

then there are always r u's, say $u_{i_1}, \ldots, u_{i_r}$, which have pairwise the same greatest common divisor d and $(u_{i_j}/d, d) = 1$, $1 \leqslant j \leqslant r$. The method of Rado and myself gives $g_r'(n) < c_r^n h!$, and it seems likely that

$$g_r'(n) < c_r^n. \tag{4.3}$$

Let $a_1 < \cdots < a_k \leqslant n, k > cn$. Is it true that for $n > n_0(c)$ there are always three a's which have pairwise the same least common multiple? I do not know the answer to this question, but showed that there do not have to be four a's which have pairwise the same least common multiple [IV].

Let $a_1 < \cdots < a_k < n, k > cn$. Is it true that there always is an m so that $pa_i = m$ (p prime) has at least three solutions? If the answer would be yes then the least common multiple of the three a's would be m (since it is easy to see that one could assume $(p, a_i) = 1$). I.Ruzsa (a 16-year-old Hungarian mathematician) found the following simple construction of a sequence $a_1 < \cdots < a_k \leqslant n, k > cn$ so that the equation $pa_i = m$ has at most two solutions. Consider the set of all squarefree numbers of the form

$$q_1 q_2 \cdots q_r, q_{i+1} > 2q_i, i = 1, \ldots, r-1; \qquad r = 1, 2, \ldots \tag{4.4}$$

It is easy to see that the density of the integers (4.4) is positive. Therefore there are cn of them in the interval $(\frac{1}{2}n, n)$ and it is easy to see that for this set of integers $pa_i = m$ has at most two solutions.

Assume that $pa_i = m$ has at most r solutions. Then clearly

$$\sum_{a_i \leqslant n} \frac{1}{a_i} \sum_{p \leqslant n} \frac{1}{p} \leqslant r \sum_{m=1}^{n^2} \frac{1}{m} < cr \log n$$

or

$$\sum_{a_i \leqslant n} \frac{1}{a_i} < \frac{c_1 r \log n}{\log \log n} \tag{4.5}$$

I do not know whether (4.5) can be improved.

Let $a_1 < \cdots < a_k \leqslant n$ be such that for every m, $pa_i = m$ has at most one solution (i.e., the numbers $\{pa_i\}$ are all distinct). It can be shown that there is a c so that

$$\max k = n \exp(-(1+o(1))c(\log n \log \log n)^{\frac{1}{2}}).$$

5. R. L. Graham posed the following interesting problem: Let $1 \leqslant a_1 < \cdots < a_n$ be n integers. Prove

$$\max_{1 \leqslant i,j \leqslant n} \frac{a_j}{(a_i, a_j)} \geqslant n. \tag{5.1}$$

Szemerédi proved that (5.1) holds if $n = p$. It is easy to see that in this case either $a_i \equiv a_j \pmod p$, or $a_i \equiv 0 \pmod p$ and $a_j \not\equiv 0 \pmod p$ for two indices $i \neq j$ (we can of course assume that not all the a's are multiples of p). (5.1) now follows easily. For composite n, the proof of (5.1) seems to present difficulties.

Winterle [1970] proved (5.1) if a_1 is a prime. Marcia and Schönheim [1969] proved that if the a's are squarefree then there are at least n distinct ratios of the form $a_j/(a_i, a_j)$, thus (5.1) follows.

Denote by $h(n)$ the greatest integer so that there are at least $h(n)$ distinct ratios of the form (5.1). Szemerédi and I showed

$$n^{\frac{1}{2}} < h(n) < n^{1-c_1}. \tag{5.2}$$

It would be interesting to improve (5.2). The determination of

$$\lim_{n=\infty} \frac{\log h(n)}{\log n}$$

will perhaps not be too difficult.

6. *On covering congruences.* A system of congruences

$$a_i (\text{mod } n_i),\ n_1 < \cdots < n_k \tag{6.1}$$

is called covering if every integer satisfies at least one of the congruences (6.1). The simplest covering system is: 0 (mod 2), 0 (mod 3), 1 (mod 4), 5 (mod 6), 7 (mod 12). I asked if for every n_1 there is a covering system (6.1). $n_1 = 20$ is the largest number for which this is known. This is an unpublished result of Choi. An affirmative answer to my question would imply that for every k there is an arithmetic progression no term of which is of the form $2^r + u$, where u has at most k distinct prime factors.

It is easy but not quite trivial to prove that for a covering congruence $\sum_{i=1}^{k} 1/n_i > 1$ (Erdös [1950]; L. Mirsky and D. Newman). It is easy to see that this is best possible if $n_1 = 3$ or $n_1 = 4$. Selfridge and I feel that for $n_1 > 4$, $\sum_{i=1}^{k} 1/n_i > 1 + c_{n_1}$ where $c_{n_1} \to \infty$ as n_1.

It is not known if there is a covering system where all the moduli are odd. As far as I know, it has never been proved that for every c there is an m so that $\sigma(m)/m > c$, but one can not form a covering system from the divisors of m. It would be nice to have a usable necessary and sufficient condition on the sequence $n_1 < \cdots < n_k$ which would decide whether they can be the moduli of a covering set, but perhaps this is too much to hope for. Selfridge informs me that it is easy to see that the n_k can not all be squarefree integers having at most two prime factors and very likely the same result holds for three prime factors.

Selfridge and Dewar investigated the following problems: An infinite system

$$a_i (\text{mod } n_i),\ n_1 < \cdots \tag{6.2}$$

is called covering if every integer satisfies at least one of the congruences (6.2) and the density of integers which do not satisfy any of the first k congruences of (6.2) goes to 0 as $k \to \infty$. This can clearly be done if $\sum 1/n_i = \infty$. A system (6.2) is called perfect if every integer satisfies exactly one of the congruences (6.2).

Recently, several interesting results were obtained on covering congruences by Burshtein and Schónheim [1970] and Znám [1969], some of which are not yet published. The recent thesis of C. E. Krukenberg (Urbana, Illinois) also contains many interesting results and also many numerical examples of covering systems and a fairly complete literature on the subject. Several problems and results on this subject are also stated in [V]. Here I just want to state one more problem which is also stated in [V] but which is still far from being completely solved; so perhaps it deserves to be restated.

A system of congruences (6.1) is called disjoint if no integer satisfies two of them. Let $n_k \leqslant x$ and put max $k = f(x)$. Stein and I conjectured that $f(x) = o(x)$; Szemerédi and I proved this. In fact we showed

$$x \exp\left(-c_1(\log x \log\log x)^{\frac{1}{2}}\right) < f(x) < \frac{x}{(\log x)^{c_2}}. \tag{6.3}$$

In the proof of the lower bound, Stein collaborated. The lower bound seems to give the true order of magnitude of $f(x)$, but by our method the upper bound can not be improved (Erdös and Szeméredi [1968]).

7. Heilbronn and I conjectured that if n is any integer and $a_1, \ldots, a_k$, $k > c\sqrt{n}$, are k distinct residues mod n then

$$\sum_{i=1}^{k} \varepsilon_i a_i \equiv 0 \pmod{n}, \qquad \varepsilon_i = 0 \text{ or } 1 \text{ (not all } \varepsilon_i \text{ are } 0)$$

is always solvable. This conjecture has recently been proved by Szemerédi [1970]. The right value of c is perhaps $\sqrt{2}$. Szemerédi's proof works for Abelian groups having n elements. The result may hold for non-Abelian groups too, but this is not yet settled.

A theorem of Ginsburg, Ziv and myself states (Mann [1967]): Let G_n be an Abelian group of n elements and let $a_1, \ldots, a_{2n-1}$ be $2n-1$ elements of G_n (of course they are not all distinct). Then the 0 element of G_n can be represented in the form

$$\sum_{i=1}^{2n-1} \varepsilon_i a_i, \qquad \sum_{i=1}^{n} \varepsilon_i = n, \qquad \varepsilon_i = 0 \text{ or } 1.$$

This result holds perhaps for non-Abelian groups too, but this has not been settled.

I would like to mention two interesting problems of Graham: Let $a_1, \ldots, a_p$ be p not necessarily distinct residues mod p. Assume that if

$$\sum_{i=1}^{p} \varepsilon_i a_i \equiv 0 \pmod{p}, \qquad \varepsilon_i = 0 \text{ or } 1$$

then $\sum_{i=1}^{p} \varepsilon_i = r$. Does it then follow that there are at most two distinct residues amongst the a's?

Let $a_1, \ldots, a_k$ be k distinct residues mod p, $k < p$. Is it true that there is a permutation $a_{i_1}, \ldots, a_{i_k}$ so that none of the sums $a_{i_1} + \cdots + a_{i_r}$, $1 \leqslant r \leqslant k$ are $\equiv \pmod p$? Graham proved this if $k = p-1$, but the general case is not yet settled.

Rényi and I proved the following result (Erdös and Rényi [1965]): Let G_n be an Abelian group of n elements (n large). Let $k > \log n/\log 2 + c \log\log n$. Then for all but $o(\binom{n}{k})$ choices of k elements $a_1, \ldots, a_k$ of G_n all elements of G_n can be written in the form $\sum_{i=1}^{k} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1. It seems likely that the summand $c \log\log n$ cannot be replaced by $o(\log\log n)$, but as far as I know, nothing has been done in this direction.

We also proved that if

$$k > 2\frac{\log n}{\log 2} + c$$

then for all but $o(\binom{n}{k})$ choices of $a_1, \ldots, a_k$ the number of representations of every element of G in the form $\sum_{i=1}^{k} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1 is $(1+o(1))2^k/n$. It is not impossible that this result remains true for $k > (1+o(1)) \log n/\log 2$.

Some progress in this direction has been made by Miech [1967] and Bognár [1972]. Rényi and I proved (unpublished) that if $k > (1+o(1)) \log n/\log 2$ then for all but $o(\binom{n}{k})$ choices of $a_1, \ldots, a_k$ every element has at least $(1+o(1))2^k/n$ representations in the form $\sum_{i=1}^{k} {}_i a_i$, but we have not succeeded in getting an upper bound.

For further problems and results of this kind see [V] and [VI]; also a forthcoming paper of Eggleton and myself (*Acta Arithmetica*) and for a comprehensive treatment Mann [1965].

8. Some problems in additive number theory. Not very much progress has been made on these problems and they have been published several times, but because of their attractiveness it is worthwhile to repeat them (see [I], [III]).

1. Let $0 < a_1 < \cdots < a_r \leqslant 2^k$ be a sequence of integers so that all the sums $\sum_{i=1}^{r} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1, are distinct. L. Moser and I both asked: Can r be greater than $k+1$. This was answered affirmatively by Conway and Guy for every $k > 21$. It is not known if $r = k+3$ is possible.

Let now $0 < a_1 < \cdots < a_r \leqslant x$, and $\sum_{i=1}^{r} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1, are all distinct. Put $f(x) = \max r$. Is it true that

$$f(x) = \frac{\log x}{\log 2} + o(1)? \tag{8.1}$$

It is trivial that

$$f(x) < \frac{\log x}{\log 2} + \frac{\log\log x}{\log 2} + o(1).$$

L. Moser and I (Erdös [1955]) proved that

$$f(x) < \frac{\log x}{\log 2} + \frac{\log \log x}{2 \log 2} + o(1). \tag{8.2}$$

I offered (and still offer) 300 dollars for a proof or disproof of (8.1). I would pay something for any improvement of (8.2). Graham recently asked: Does (8.1) remain true if we only require the a_i to be positive,

$$1 \leqslant a_1 < \cdots < a_r \leqslant x,\ a_{i+1} - a_i \geqslant 1,$$

and any two of the sums $\sum_{i=1}^{r} \varepsilon_i a_i$, $\varepsilon_i = 0$ or 1 differ by at least one? (8.2) remains true.

2. Let $a_1 < \cdots < a_k \leqslant x$ be a sequence of integers. Assume that all the sums

$$\sum_{i=1}^{r} \varepsilon_i a_{j_i}, \qquad \varepsilon_i = 0 \text{ or } 1, \qquad 1 \leqslant j_1 < \cdots < j_r \leqslant k,$$

are all distinct. Put $\max k = f_r(x)$. Turán and I proved $f_2(x) < x^{\frac{1}{2}} + cx^{\frac{1}{4}}$, and recently Lindstrom proved (Krückeberg [1961])

$$f_2(x) \leqslant x^{\frac{1}{2}} + x^{\frac{1}{4}} + 1.$$

Recently, Szemerédi proved $f_2(x) < x^{\frac{1}{2}} + o(x^{\frac{1}{4}})$. That $f_2(x) > (1-\varepsilon)x^{\frac{1}{2}}$ for every $\varepsilon > 0$ if $x > x_0(\varepsilon)$ easily follows from the classical result of Singer on difference sets (as observed by Chowla and myself). Turán and I conjectured

$$f_2(x) = x^{\frac{1}{2}} + o(1). \tag{8.3}$$

I offer 250 dollars for the proof or disproof of (8.3).

Bose and Chowla proved that for every r

$$f_r(x) \geqslant (1 + o(1))x^{1/r},$$

and they conjecture that

$$\lim_{x=\infty} f_r(x)/x^{1/r} = 1 \tag{8.4}$$

(8.4) has never been proved for $r > 2$ and is a very attractive conjecture. I offer 100 dollars for a proof or disproof.

Let now $a_1 < \cdots$ be an infinite sequence so that all the sums $a_i + a_j$ are distinct (i.e., A is a B_2 sequence of Sidon). It is easy to see that there is a B_2 sequence for which $a_k < ck^3$ for every k. It seems certain to me that there is a B_2 sequence $a_1 < \cdots$ satisfying $a_k < k^{2+\varepsilon}$ for every ε if $k > k_0$, but as far as I know, nobody constructed a B_2 sequence satisfying $a_k = o(k^3)$. (I offer 25 dollars for this and 50 for $a_k < k^{2+\varepsilon}$.) Rényi and I proved by probabilistic methods that to every ε there is a c so that there is a sequence $a_k < k^{2+\varepsilon}$ so that the number of solutions of $n = a_i + a_j$ is less than c_ε (see [VI]).

There is a B_2 sequence for which (Krückeberg [1961])

$$\liminf_{k \to \infty} \frac{a_k}{k^2} \leqslant \sqrt{2}. \tag{8.5}$$

It is not known if $\sqrt{2}$ can be decreased, perhaps it can be replaced by 1. On the other hand, for a B_2 sequence [VII]

$$\limsup_{h\to\infty} \frac{a_k}{k^2 \log k} > 0.$$

Let $a_1 < \cdots$ be any sequence of integers. Denote by $f(n)$ the number of solutions of $n = a_i + a_j$. Turán and I conjectured that if $f(n) > 0$ for all n then

$$\limsup_{n\to\infty} f(n) = \infty. \tag{8.6}$$

Perhaps $a_k < ck^2$ suffices to imply (8.6). I offer 250 dollars for (8.6). The multiplicative analogue of (8.6) I succeeded to prove (Erdös [1964b]).

Let $a_1 < \cdots$ be an infinite sequence of integers. Assume that no a is the distinct sum of other a's. Then the a's have density 0 and $\sum 1/a_i < \infty$ (Erdös [1962]).

Let $a_1 < \cdots < a_n$ be n distinct numbers; L. Moser and I proved that the number solutions of (see [II])

$$t = \sum_{i=1}^{n} \varepsilon_i a_i, \qquad \varepsilon_i = 0 \text{ or } 1, \tag{8.7}$$

is less than $c2^n (\log n)^{\frac{3}{2}}/n^{\frac{3}{2}}$. We conjectured that it is in fact less than $c2^n/n^{\frac{3}{2}}$ (which apart from the value of c is best possible). Sárközi and Szemerédi [1965] proved this conjecture. It seems that the number of solutions of

$$t = \sum_{i=1}^{n} \varepsilon_i a_i, \qquad \sum_{i=1}^{n} \varepsilon_i = l, \tag{8.8}$$

is less than $c2^n/n^2$ (where c is an absolute constant independent of t, l, n and our sequence). (8.8) has never been proved.

It is likely that for $n = 2m+1$ the number of solutions of (8.7) is largest when the a's are the integers in $(-m, +m)$, but this has never been proved (Van Lint [1967]).

9. I first mention a few special problems considered in [II], especially those where some progress has been made. Let $a_1 < \cdots < a_n$ be n real numbers all different from 0. Denote by $f(n)$ the largest integer so that for every sequence $a_1, \ldots, a_n$ one can always select $k = f(n)$ of them, $a_{i_1}, \ldots, a_{i_k}$, so that

$$a_{i_{j_1}} + a_{i_{j_2}} \neq a_{i_{j_3}}, \qquad 1 \leqslant j_1 \leqslant j_2 < j_3 \leqslant k. \tag{9.1}$$

It is not hard to see that $f(n) \geqslant \frac{1}{3}n$. This is almost certainly not best possible but Klarner and Hilton showed $f(n) < \frac{1}{2}n$ even if we exclude $j_1 = j_2$.

Independently of this, Diananda, Yap, Rhentulla and Street considered in several papers the problem of determining in an Abelian group of order n the maximal sum free set, i.e., the largest set for which (9.1) holds. The most difficult case is when all prime factors of n are $\equiv 1 \pmod 3$, and in this case there are several unsolved problems. For a complete literature on this subject, see the two forthcoming papers of H. P. Yap, 'Maximal sum free sets in finite abelian groups I and II,' *Bull. Austral. Math. Soc.*

Denote by $g(n)$ the largest number such that from every sequence of n numbers one can always select $g(n)$ of them with the property that no sum of two distinct integers of this subsequence belongs to the original sequence. It is known that

$$c \log n < g(n) < n^{2/5+\varepsilon}. \tag{9.2}$$

The lower bound is due to Klarner, the upper bound to S. L. G. Choi. (Choi's paper is not yet published but will soon appear.)

The lower bound in (9.2) can probably be improved very much.

In Choi's paper the following interesting problem is raised: A set C of natural numbers is said to be admissible relative to a set of natural numbers B if the sum of two distinct elements of C is always outside B. Let B be any set of integers in $(2n, 4n)$ and let C be a maximal admissible subset of $(n, 2n)$ relative to B. Put

$$f(n) = \min_{\mathrm{B}} (|C| + |B|).$$

Choi conjectures $f(n) < n^{\frac{1}{2}+\varepsilon}$, but can only show $f(n) < cn^{\frac{3}{4}}$. Choi's conjecture perhaps could be proved by probabilistic arguments, but I have not succeeded in this.

Denote by $h(n)$ the largest integer so that from any set of n integers one can always find a subset of $h(n)$ integers with the property that any two sums formed from the elements of the subset are equal only if they have the same number of summands. We have

$$c_1 n^{\frac{1}{3}} < h(n) < c_2 n^{\frac{1}{2}}$$

The upper bound is due to Straus [1966]. Recently, Choi proved $h(n) > c(n \log n)^{\frac{1}{3}}$; his proof will soon appear.

Denote by $l(n)$ the largest integer so that from any set $a_1, \ldots, a_n$ of real numbers one can always select $l(n)$ of them, $a_{i_1}, \ldots, a_{i_k}$, $k \geqslant l(n)$, so that no a_{i_j} is the distinct sum of other a_{i_r}'s. I observed $l(n) \geqslant \sqrt{(\frac{1}{2}n)}$; this was improved by Choi to $l(n) > (1+c)\sqrt{n}$. Probably $l(n)/\sqrt{n} \to \infty$, but Choi's method does not even seem to give $l(n) > 2\sqrt{n}$. I claimed $l(n) = o(n)$, but have difficulties in reconstructing my proof. Probably $l(n) < n^{1-c}$ holds for some $c > 0$.

Several very interesting problems on additive number theory are discussed in the papers of Rohrbach and Stöhr [VII]. Here I would like to mention one problem of Rohrbach: Let $0 \leqslant a_1 < \cdots < a_k \leqslant n$ be a sequence of integers so that every integer $0 \leqslant m \leqslant n$ can be written in the form $a_i + a_j$. Put $g(n) = \min k$. Rohrbach observed:

$$\sqrt{2n} \leqslant g(n) \leqslant 2\sqrt{n}.$$

He proved $g(n) > (1+\varepsilon)\sqrt{2n}$ for some $\varepsilon > 0$; Moser improved this result but his ε is still very small. Rohrbach conjectured $g(n) = 2\sqrt{n} + o(1)$. We are very far from being able to prove this.

10. Let $1 \leqslant a_1 < \cdots < a_k \leqslant x$ be a sequence of integers so that the product of any two integers $a_i a_j$ is distinct. Then

$$\pi(x) + \frac{c_2 x^{\frac{3}{4}}}{(\log x)^{\frac{3}{2}}} < \max k < \pi(x) + \frac{c_1 x^{\frac{3}{4}}}{(\log x)^{\frac{3}{2}}}. \tag{10.1}$$

Perhaps

$$\max k = \pi(x) + \frac{c x^{\frac{3}{4}}}{(\log x)^{\frac{3}{2}}} + o\left(\frac{x^{\frac{3}{4}}}{(\log x)^{\frac{3}{2}}}\right) \tag{10.2}$$

for a certain constant $c > 0$, but I have not been able to prove (10.2).

Assume that $1 \leqslant a_1 < \cdots < a_k \leqslant x$ is such that all products $a_{i_1} \cdots a_{i_r}$ are distinct. Perhaps in this case

$$\max k < \pi(x) + c x^{\frac{1}{2}(1+1/r)}, \tag{10.3}$$

but I could prove this only for $r = 2$.

Now let $1 \leqslant a_1 < \cdots < a_k \leqslant x$ so that all the products

$$\prod_{i=1}^{k} a_i^{\varepsilon_i}, \qquad \varepsilon_i = 0 \text{ or } 1,$$

are distinct. Then

$$\max k \leqslant \pi(x) + c\,\frac{x^{\frac{1}{2}}}{\log x};$$

perhaps

$$\max k = \pi(x) + \pi(\sqrt{x}) + o\left(\frac{x^{\frac{1}{2}}}{\log x}\right).$$

All these questions become very much more difficult if the a's do not have to be integers. Let, e.g., $1 \leqslant a_1 < \cdots < a_k \leqslant x$ be a sequence of real numbers and assume that $|a_i a_j - a_r a_s| \geqslant 1$. Does (10.1) remain true? I can not even prove $k = o(x)$, though this may be simple, and perhaps I overlook a simple idea.

An old conjecture of mine states: Let $1 \leqslant a_1 < \cdots < a_k \leqslant x$, $1 \leqslant b_1 < \cdots < b_l \leqslant y$ be two sequences of integers. Assume that the products $a_i b_j$ are all distinct. Is it true that

$$kl < \frac{cx^2}{\log x}? \tag{10.4}$$

It is easy to see that if true, (10.4) is best possible. The weaker result

$$kl < \frac{x^2}{(\log x)^\alpha} \text{ for some } \alpha > 0$$

is not very hard to prove. (10.4) was recently proved by Szemerédi.

Is it true that to every $\varepsilon > 0$ there is an infinite sequence of integers of density $> 1-\varepsilon$ so that two products $a_{i_1} \cdots a_{i_r} = a_{j_1} \cdots a_{j_s}$ can only hold if $r = s$? Selfridge constructed such a sequence of density $1/e$. Is it true that one can give $x - o(x)$ such integers not exceeding x? By taking the integers not exceeding x having a prime factor $> x^{\frac{1}{2}}$, it is easy to see that one can give $x \log 2$ such integers not exceeding x and that the constant $\log 2$ can be slightly improved.

For the literature on these questions, see [II] and Erdös [1968, 1964].

11. A sequence of integers is called primitive if no one divides any other. Chapter 5 of [VI] is devoted to the study of primitive sequences. Sárközi, Szemerédi and I wrote about ten papers on primitive sequences and related questions (see our paper at the Debrecen meeting of the Bólyai Math. Soc. 1968). The following question which I formulated nearly forty years ago is still unsolved:

Let $1 \leqslant a_1 < \cdots$ be a sequence of positive numbers. Assume that for every integer i, j and k

$$|ka_i - a_j| \geqslant 1. \tag{11.1}$$

Is it then true that

$$\sum_i \frac{1}{a_i \log a_i} < \infty \tag{11.2}$$

and

$$\sum_{a_i < x} \frac{1}{a_i} < \frac{c \log x}{(\log \log x)^{\frac{1}{2}}}? \tag{11.3}$$

If the a's are integers then (11.1) means that no a divides any other, and in this case (11.3) is an old result of Behrend and (11.2) is an old result of mine (see [VI]). But in the general case I can not even prove that (11.1) implies $\liminf A(x)/x = 0$ ($A(x) = \sum_{a_i < x} 1$). Recently, Haight [unpublished] proved that if the a's are rationally independent then (11.1) implies $\lim A(x)/x = 0$. An old result of Besicovitch states that if the a's are integers then (11.1) does not imply $\lim A(x)/x = 0$ [VI].

Let $a_1 < \cdots$ be an infinite sequence of integers where no a_i divides the sum of two greater a's. Sárközi and I proved that the a's then have density

0 and this result is best possible (Erdös and Sárközi [1970]). Probably $\sum 1/a_i < \infty$ holds.

Let $a_1 < \cdots < a_k \leqslant x$ be a sequence of integers where no a divides the sum of two larger a's. Probably

$$\max k = x/3 + o(1).$$

12. Let $a_1 < a_2 < \cdots$ be an infinite sequence of integers. Straus and I conjectured that there is a sequence of density 0, $b_1 < \cdots$ so that every integer is of the form $a_i + b_j$. Lorentz [1954] proved this conjecture. In fact, he showed that $b_1 < \cdots$ can be chosen so that for every x

$$B(x) < c \sum_{k=1}^{x} \frac{\log A(k)}{A(k)}. \tag{12.1}$$

(12.1) is surprisingly close to being best possible (Erdös [1954]). We will call $b_1 < \cdots$ the complementary sequence to $a_1 < \cdots$

Lorentz observed that if the a's are the primes then (12.1) gives $B(x) < c(\log x)^3$. I proved that this can be improved to $B(x) < c(\log x)^2$ (Erdös [1954]). Clearly every complimentary sequence to the primes must satisfy

$$\liminf \frac{B(x)}{\log x} \geqslant 1. \tag{12.2}$$

I am certain that (12.2) can be improved, but I could not even show

$$\limsup \frac{B(x)}{\log x} > 1.$$

In the other direction I could not find a complementary sequence to the primes satisfying $B(x) = o((\log x)^2)$. Further I could not decide whether there is a complementary sequence to the primes $b_1 < \cdots$ for which the number of solutions of $n = p + b_i$ is bounded.

I asked: Let $a_k = 2^k$. Is there a complementary sequence for which $B(x) < cx/\log x$? The 17-year-old Ruzsa gave a very ingenious proof that the answer is affirmative and he also observed that for his sequence the number of solutions of $2^k + b_i = n$ is bounded. Clearly

$$B(x) \geqslant (1+o(1))\frac{x \log 2}{\log 2}.$$

It seems certain that

$$B(x) > (1+c)\frac{x \log 2}{\log 2} \tag{12.3}$$

must hold for a complementary sequence of the powers of 2, but this has never been proved. Ruzsa's proof will appear in the *Bull. Canad. Math.*

Soc. Ruzsa also finds a sequence $a_1 < \cdots$ with $A(x) > c \log x$ so that for every complementary sequence

$$B(x) > \frac{cx \log \log x}{\log x};$$

or, (12.1) is best possible in this case. It is not clear that if $a_k = r^k$, then there is a complementary sequence satisfying $B(x) < cx/\log x$. (By the way, earlier I referred to Ruzsa as being 16 years old; this is no contradiction, since he did the other work one year earlier.)

Complementary sequences of the rth powers were studied by L. Moser [1965], but several interesting unsolved problems remain.

13. Let $a_1 < \cdots; b_1 < \cdots$ be two infinite sequences of integers. Assume that every sufficiently large integer is of the form $a_i + b_j$. Clearly

$$\liminf \frac{A(x)B(x)}{x} \geqslant 1$$

and Hanani conjectured that

$$\limsup \frac{A(x)B(x)}{x} > 1. \tag{13.1}$$

Narkiewicz [1960] proved that (13.1) holds under fairly general conditions, but Danzer [1964] disproved Hanani's conjecture. Danzer and I then conjectured that if every $n > n_0$ is of the form $a_i + b_j$ and

$$\lim \frac{A(x)B(x)}{x} = 1 \tag{13.2}$$

then

$$\lim (A(x)B(x) - x) \to \infty \tag{13.3}$$

(It is easy to see that (13.3) does not hold in general). Sárközi and Szemerédi recently proved (13.3); their proof is not yet published. It is not clear how fast $A(x)B(x) - x$ must tend to infinity if (13.2) holds.

14. Before finishing this report, I would like to mention a few miscellaneous problems and results of a combinatorial flavor. No doubt I will omit many very interesting questions, but this is inevitable since both space and time and my memory and judgement are limited.

1. Let $a_1 < \cdots < a_k \leqslant n$ be a sequence of integers satisfying

$$[a_i, a_j] > n,\ 1 \leqslant i < j \leqslant k. \tag{14.1}$$

In other words, no $m \leqslant n$ is divisible by two or more a's.

I conjectured that

$$\max k = (1 + o(1)) \frac{3}{2\sqrt{2}} n^{\frac{1}{2}}$$

and that the extremal sequence is given by the numbers $1 \leqslant i \leqslant (\frac{1}{2}n)^{\frac{1}{2}}$, $(\frac{1}{2}n)^{\frac{1}{2}} \leqslant 2j \leqslant (2n)^{\frac{1}{2}}$. Perhaps these conjectures are trivially true or false and I overlook an obvious idea.

I further conjectured that (13.1) implies

$$\sum_{i=1}^{k} \frac{1}{a_i} \leqslant \frac{31}{30}, \tag{14.2}$$

with equality only if $n = 5$, $a_1 = 2$, $a_2 = 3$, $a_3 = 5$. Schinzel and Szekeres proved this conjecture. I thought that (14.1) implies the existence of an absolute constant c so that there are cn integers $m \leqslant n$ which do not divide any of the a's. To my great surprise this was disproved by Schinzel and Szekeres. It is probable that (14.1) implies for $n > n_0(\varepsilon)$, $\sum_{i=1}^{k} 1/a_i < 1+\varepsilon$.

Let $a_1 < \cdots < a_k \leqslant n$ satisfying $\sum_{i=1}^{k} 1/a_i < c_1$. It is true that there is a c_2 so that there are at least $n/(\log n)^{c_2}$ integers m not exceeding n which are not divisible by any of the a's. The example of Schinzel and Szekeres [1959] shows that apart from the value of c_2 this is best possible if true.

Assume now

$$\sum_{i=1}^{k} \frac{1}{a_i} < c_1, \qquad (a_i, a_j) = 1, \qquad 1 < a_i \leqslant n. \tag{14.3}$$

For what choice of the a's satisfying (14.3), the number of integers $m \leqslant n$ not divisible by any a is minimal? Let q_1 be the greatest prime not exceeding n and $q_1 > q_2 > \cdots$ the consecutive primes in decreasing order. Put

$$\sum_{i=1}^{j} \frac{1}{q_i} \leqslant c_1 < \sum_{i=1}^{j+1} \frac{1}{q_i}. \tag{14.4}$$

The q's defined by (14.4) satisfy (14.3) and it seems to me that (14.4) either gives the extremal sequence (or at least nearly gives the minimum). I made no progress with this question.

2. A sequence $n_1 < n_2 < \cdots$ is called an essential component if for any sequence $1 = a_1 < \cdots$ of Schnirelman density α, the Schnirelman sum of the two sequences $\{a_i + n_j\}$ always has density greater than α. I conjectured that if $n_{i+1}/n_i > c > 1$ then the sequence is never an essential component.

Essential components have been investigated a great deal for the older literature; see [VI] and Edrös [1961]. Also in the *J. Reine Angew. Math.*, several recent interesting papers appeared, e.g., Tülnnecke [1960].

3. Let $1 = a_1 < \cdots < a_{\phi(n)} = n-1$ be the set of integers relatively prime to n. An old conjecture of mine states that

$$\sum_{i=1}^{\phi(n)-1} (a_{i+1}-a_i)^2 < c\frac{n^2}{\phi(n)}. \tag{14.5}$$

C. Hooley made some progress towards the proof of (14.5), but at the moment (14.5) is not yet settled. It seems certain that for every k

$$\sum_{i=1}^{\phi(n)-1} (a_{i+1}-a_i)^k < c_k \frac{n^k}{\phi(n^{k-1})}. \tag{14.6}$$

Hooley in fact proved (14.6) for $k < 2$. I conjectured (14.5) and (14.6) more than thirty years ago and never expected it to be so difficult.

4. Let $f(n)$ be the largest integer so that for every $1 \leqslant i \leqslant f(n)$ there is a $p_i | n+i$, $p_{i_1} \neq p_{i_2}$ for $1 \leqslant i_1 < i_2 \leqslant f(n)$.

Grimm conjectured (*Am. Math. Monthly*, Dec. 1969) that for every j, $f(p_j) > p_{j+1} - p_j$. Selfridge and I proved that for all n

$$f(n) \geqslant (1+o(1)) \log n \tag{14.7}$$

and for infinitely many n

$$f(n) < \exp c\, (\log n \log\log\log n / \log\log n)$$

It would be interesting to find out more about $f(n)$. Grimm's conjecture if true will be very hard to prove. Ramachandra just informed me that he improved (14.7) to

$$f(n) > c \log n\, (\log\log n)^{1/2} / (\log\log\log n)^{1/2}.$$

5. A problem in set theory lead R. O. Davies and myself to the following question: Denote by $f(n, k)$ the largest integer so that if there are given in k dimensional space n points which do not contain the vertices of an isosceles triangle, then they determine at least $f(n, k)$ distinct distances. Determine or estimate $f(n, k)$. In particular, is it true that

$$\lim_{n=\infty} \frac{f(n, k)}{n} = \infty\, ? \tag{14.8}$$

(14.8) is unproved even for $k = 1$. Straus observed that if $2^k \geqslant n$ then $f(n, k) = n-1$.

References

H. L. Abbott, 1966, Some remarks on a combinatorial theorem of Erdös and Rado, *Canad. Math. Bull.* **9**, 155–160.

H. L. Abbott and B. Gardiner, 1967, *Canad. Math. Bull.* **10**, 173–177.

H. L. Abbott and D. Hanson, 1970, An extremal problem on number theory, *Bull. London Math. Soc.* **2**, 324–326. *See also* Abbott and Gardiner [1967].

F. Behrend, 1946, On sets of integers which contain no three terms in an arithmetic progression, *Proc. Natl. Acad. Sci. USA* **32**, 331–332.

E. R. Berlekamp, 1968, A construction for partitions which avoid long arithmetic progressions, *Canad. Math. Bull.* **11**, 409–414.

K. Bognár, On a problem of statistical group theory, *Studia Sci. Math. Hung.*

N. Burshtein and J. Schönheim, 1970, On a conjecture concerning exactly covering systems of congruences, *Israel J. Math.* **8**, 28–29.

L. Danzer, 1964, Über eine Frage von Hanani aus der additiven Zahlentheorie, *J. Reine Angew. Math.* **214/215**, 392–394.

P. Erdös, 1950, On integers of the form 2^n+p and some related problems, *Summa Brasil Math.* **2**, 113–123.

P. Erdös, 1952, On a problem concerning congruence systems, *Mat. Lapok* **3**, 122–128 (in Hungarian).

P. Erdös, 1954, Some results on additive number theory, *Proc. Am. Math. Soc.* **5**, 847–853.

P. Erdös, 1955, Problems and results in additive number theory, *Coll. sur la theorie des nombres*, (Bruxelles), pp. 127–137.

P. Erdös, 1957, On some geometrical problems, *Mat. Lapok* **8**, 86–92 (MR 20 6056 [1959]) (in Hungarian).

P. Erdös, 1961, Über einige Probleme der additiven Zahlentheorie, *J. Reine Angew. Math.* **206**, 61–66.

P. Erdös, 1962, Remarks on number theory III, *Mat. Lapok* **13**, 28–38 (in Hungarian).

P. Erdös, 1963, On some combinatorial theorems connected with the theorems of Ramsey and Van der Waerden, *Mat. Lapok* **14**, 29–37 (in Hungarian).

P. Erdös, 1964a, On a problem in elementary number theory and on a combinatorial problem, *Math. Comp.* **18**, 644–646.

P. Erdös, 1964b, On the multiplicative representation of integers, *Israel J. Math.* **2**, 251–261.

P. Erdös, 1968, On some applications of graph theory to number theoretic problems, *Bull. Ramanujan Inst.* **1.**

P. Erdös and R. Guy, 1970, Distinct distances between lattice points, *Elemente Math.* **25**, 121–123.

P. Erdös and R. Rado, 1960, Intersection theorems for systems of sets, *J. London Math. Soc.* **35**, 85–90.

P. Erdös and A. Rényi, 1965, Probabilistic methods in group theory, *J. Analyse Math.* **14**, 127–138.

P. Erdös and A. Sárközi, 1970, On the divisibility properties of sequences of integers, *Proc. London Math. Soc.* **21**, 97–101.

P. Erdös and E. G. Straus, 1970, Non-averaging sets II, *Combinatorial Theory and its Applications* (P. Erdös et al., eds.; North-Holland, Amsterdam), pp. 405–411.

P. Erdös and E. Szemerédi, 1968, On a problem of P. Erdös and S. Stein, *Acta Arithmetica* **15**, 85–90.

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

G. Halász, 1968, Über Mittelwerte multiplikativer zahlentheoretischer Funktionen, *Acta Math. Acad. Sci. Hung.* **19**, 365–403.

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

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

H. B. Mann, 1965, *Addition Theorems*, Tracts in Math. **18** (Wiley-Interscience, New York).

H. B. Mann, 1967, Two addition theorems, *J. Combin. Theory* **3**, 233–235.

J. Marcia and J. Schönheim, 1969, Difference of sets and a problem of Graham, *Canad. Math. Bull.* **12**, 635–637.

R. J. Miech, 1967, On a conjecture of Erdös and Rényi, *Illinois J. Math.* **11**, 114–127.

L. Moser, 1965, On the additive completion of sets of integers, *Proc. Symp. Pure Math.* **8** (Am. Math. Soc. Providence, R.I.), pp. 175–180.

W. Narkiewicz, 1960, Remarks on a conjecture of Hanani in additive number theory, *Colloq. Math.* **7,** 161–165.

R. Rado, 1933, Studien über Kombinatorik, *Math. Z.* **36,** 429–480.

R. A. Rankin, 1962, Sets of integers containing not more than a given number of terms in arithmetical progression, *Proc. Roy. Soc. Edinburgh* **A65,** 332–344.

J. Riddell, 1969, On sets of numbers containing no l terms in arithmetic progression, *Nieuw Archief voor Wiskunde*, **17,** 204–209.

K. F. Roth, 1953, On certain sets of integers, *J. London Math. Soc.* **28,** 104–109.

K. F. Roth, 1964, Remark concerning integer sequences, *Acta Arithmetica* **9,** 257–260.

K. F. Roth, 1967, Irregularities of sequences relative to arithmetic progressions, *Math. Ann.* **169**, 1–25.

K. F. Roth, 1970, Irregularities of sequences relative to arithmetic progressions III, *J. Number Theory* **2,** 125–142.

A. Sárközi and Z. Szemerédi, 1965, Über ein Problem von Erdös und Moser, *Acta Arithmetica* **11,** 205–208.

A. Schinzel and G. Szekeres, 1959, Sur un problème de M. P. Erdös, *Acta Sci. Math. Szeged* **20,** 221–229.

E. G. Straus, 1966, On a problem in combinatorial number theory, *J. Math. Sci.* **1,** 77–80.

E. G. Straus, 1967, Non averaging sets, *Proc. Symp. Pure Math.* (Am. Math. Soc., Providence, R.I.).

E. Szemerédi, 1969, On sets of integers containing no four elements in arithmetic progression, *Acta Math. Acad. Sci. Hung.* **20,** 89–104.

E. Szemerédi, 1970, On a conjecture of Erdös and Heilbronn, *Acta Arithmetica* **17,** 227–229.

J. H. van Lint, 1967, Representation of 0 as $\sum_{k=-N}^{N} \varepsilon_k k$, *Proc. Am. Math. Soc.* **18,** 182–184.

H. Tülnnecke, 1960, Über die Dichte der Summen zweier Mengen deren eine die Dichte 0 hat, *J. Reine Angew. Math.* **205,** 1–20.

B. L. van der Waerden, 1927, Beweis einer Baudetschen Vermutung, *Nieuw Archief voor Wiskunde* (2) **15,** 212–216. *See also* Rado [1933].

A. Winterle, 1970, A problem of R. L. Graham in combinatorial number theory, *Proc. Louisiana Conf. on Combinatorics, Graph Theory and Computing* (Louisiana State Univ., Baton Rouge, La.), pp. 357–361.

E. Wirsing, 1967, Das asymptotische Verhalten von Summen über multiplikative Funktionen, *Acta Math. Acad. Sci. Hung.* **18,** 411–467.

S. Znám, 1969, On exactly covering systems of arithmetic sequences, *Math. Ann.* **180,** 227–232.