61. Y. Sampei, On the uniformization of the complement of an analytic set, *Comment. Math. Univ. St. Paul*, **10** (1962) 57–62.
62. D. Scott, Measurable cardinals and constructible sets, *Bull. Ac. Pol. Sc.*, **9** (1961) 521–524.
63. J. R. Shoenfield, The problem of predicativity, pp. 132–139 in *Essays on the foundations of mathematics*, Jerusalem (1961) Magnes Press.
64. R. Solovay, Independence results in the theory of cardinals, *Notices of the Am. Math. Soc.*, **10** (1963) 595.
65. C. Spector, Recursive well-orderings, *J.S.L.*, **20** (1955) 151–163.
66. C. Spector, Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles formulated in current intuitionistic mathematics, *Proc. Symp. Pure Maths.*, **5** (1962) 1–27.
67. W. W. Tait, Infinitely long terms of transfinite types, pp. 176–185 in *Formal systems and recursive functions*, Amsterdam (1964) North Holland Publ. Co.
68. W. W. Tait, The ϵ-substitution method, *J.S.L.*, to appear.
69. W. W. Tait, The no-counterexample interpretation, *Archiv für math. Logik und Grundlagenforschung*, to appear.
70. G. Takeuti, Construction of the set theory from the theory of ordinal numbers, *J. Math. Soc. Japan*, **6** (1954) 196–220.
71. G. Takeuti, On the theory of ordinal numbers, *J. Math. Soc. Japan*, **9** (1957) 93–113.
72. G. Takeuti, On the fundamental conjecture of GLC, GLC (I–V), *J. Math. Soc. Japan*, **10** (1958) 121–134, and earlier papers quoted there.
73. J. Ax, S. Kochen, Diophantine problems over local fields, *Amer. J. Math.*, to appear.
74. A. Lévy, Measurable cardinals and the continuum hypothesis, *Notices Amer. Math. Soc.*, **11** (1964) 769–770.
75. R. Solovay, The measure problem, *Annals of Mathematics*, to appear.

Offprints from
LECTURES ON MODERN MATHEMATICS, VOL. III
Edited by T.L. Saaty
Published by John Wiley & Sons, Inc., 1965

4

Some Recent Advances and Current Problems in Number Theory

Paul Erdös

The subject of number theory is very extensive and has intimate links with other branches of mathematics. Analysis has been applied with great success to various problems of number theory for 200 years and there is every reason to expect that such applications will continue. Algebraic methods have also been applied to number theory and have in turn developed out of number theory. Recently algebraic geometry and probability theory have been applied with success to problems which previously seemed intractable. In this chapter I clearly cannot hope even to attempt to give a complete survey of recent developments in number theory, and in quite a few of its branches I am not particularly competent to do so—for example, in the branches involving algebraic geometry. My paper will be highly subjective; I shall write mainly about questions which have interested me personally, and I certainly do not wish to suggest that any problems and results which I omit to mention are less important or interesting than the ones I shall write about a great deal. For instance, I overemphasize problems on primes and problems of a combinatorial type; also, of course, I overemphasize my own work. I shall not write much about Waring's

problem since it has been dealt with in recent books [1]; I shall omit the geometry of numbers, and also Diophantine approximation since I recently wrote about this subject (see my forthcoming paper in *Compositio Math.*). The same fate will overtake many applications of probability to number theory, but several survey articles have appeared recently on this subject (some of them written by me) and there is also a recent book by Kubilius and a forthcoming book by Rényi and myself [2]. Most of the questions with which I shall deal will have a combinatorial flavor or will relate to primes (or both); these are the subjects which have interested me most for the last thirty-three years. To quote from the introduction to the well-known and excellent book of Hardy and Wright: "I cannot fail completely in making the paper interesting, since the subject is so attractive that this would need extravagant incompetence."

There will be some overlap between this paper and my recent paper "On unsolved problems" [2a].

I wish to thank my friends Davenport, Schinzel, and Turan for their valuable assistance.

1. First, I shall discuss problems and results on the distribution of prime numbers (the letters p, q will denote primes throughout).

Denote by $\pi(x)$ the number of primes not exceeding x and by c, c_1, . . . absolute constants, not always the same. The Prime Number Theorem states that

$$\lim_{x=\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1. \tag{1}$$

(1) was first proved in 1896 by Hadamard and de la Vallée Poussin. In 1948 Selberg and I obtained [3] an elementary proof of (1). Our starting point was the following remarkable formula of Selberg, which he proved in an elementary way:

If $\vartheta(x) = \sum_{p \le x} \log p$ then

$$\vartheta(x) \log x + \sum_{p<x} \log p \, \vartheta\left(\frac{x}{p}\right) = 2x \log x + O(x). \tag{2}$$

We then proved by elementary arguments that if $1 < p_1 < p_2 <$

. . . is any sequence of real numbers which satisfies (2) and further satisfies

$$\vartheta(x) > ax, \qquad \sum_{p<x} \frac{\log p}{p} = \log x + O(1), \tag{3}$$

then

$$\vartheta(x) = x + o(x). \tag{4}$$

This is well known to be equivalent to (1).

Beurling [4] gave the following interesting generalization of the prime number theorem. Let $1 < p_1 < p_2 < \cdots$ be any sequence of real numbers, which will be called generalized primes. Denote by $N(x)$ the number of solutions of

$$\prod_i p_i^{\alpha_i} \leq x \qquad (\alpha_i = 0, 1, \ldots).$$

Assume that

$$N(x) = x + o\left(\frac{x}{(\log x)^{3/2}}\right). \tag{5}$$

Then it follows that

$$\sum_{p_i \leq x} 1 = (1 + o(1)) \frac{x}{\log x}. \tag{6}$$

Beurling also observed that (6) cannot be deduced from a weaker error term than that in (5). Selberg observed that one can make the deduction of (6) from (5) by our elementary method if in (5) a slightly better error term is assumed (unpublished). Nyman and Malliavin [4] sharpened Beurling's results in various ways. I later proved [3] that (2) alone implies (4) and Shapiro [3] proved that (2) with an error term $o(x \log x)$ instead of $O(x)$ also implies (4).

My deduction of (4) from (2) was based on the following Tauberian theorem, which seems of independent interest:

Suppose $a_k \geq 0$ and assume that $\left(\text{with } s_n = \sum_{k=1}^{n} a_k\right)$

$$\sum_{k=1}^{n} a_k(s_{n-k} + k) = n^2 + O(n). \tag{7}$$

Then

$$s_n = n + O(1). \tag{8}$$

My original proof was very complicated; Siegel simplified it (unpublished) and later Shapiro [3] simplified my proof considerably.

Bombieri and Wirsing [5] succeeded independently in proving in an elementary way that for every $k > 0$

$$\vartheta(x) = x + o\left(\frac{x}{(\log x)^k}\right). \tag{9}$$

This, as is well known, implies that

$$\pi(x) = \int_o^x \frac{dy}{\log y} + o\left(\frac{x}{(\log x)^k}\right).$$

This is a considerable advance on previous results of Van der Corput, Kuhn, Breusch, and others.

In my opinion the simplest deduction of (4) from (2) and (3) is that due to V. Nevanlinna [6], who somewhat simplifies the proof of Wright [1].

Put $\psi(x) = \sum_{n<x} \Lambda(n)$, $\Lambda(n) = \log n$ if $n = p^\alpha$ and is 0 otherwise. Tchebicheff observed that

$$\sum_{n=1}^{x} \psi\left(\frac{x}{n}\right) = x \log x - x + o(x) \tag{10}$$

The proof of (10) is elementary; in fact (10) easily follows from a weak form of Stirling's formula.

It would be very desirable to deduce the prime number theorem from (10) as far as possible in an elementary way. Sharpening a previous result of Landau, Ingham [7] proved by using Wiener's theory that (10) implies $\psi(x) = x + o(x)$ which is equivalent to the prime number theorem. Recently Ingham and I proved the following theorem (our paper will appear in *Acta Arithmetica*): Let $1 < a_1 < a_2 \cdots$ be a sequence of real numbers with $\sum_i 1/a_i < \infty$. Assume that $f(x)$ is an increasing function for which

$$f(x) + \sum_i f\left(\frac{x}{a_i}\right) = x\left(1 + \sum_i \frac{1}{a_i}\right) + o(x). \tag{11}$$

(11) implies $f(x) = x + o(x)$ if and only if $\sum_i 1/(a_i)^s = 1$ has no root of the forms $1 + it$, $t \neq 0$. It is possible that if the a_i are integers this condition is always satisfied. The simplest case for which we cannot decide this question is $a_1 = 2$, $a_2 = 3$, $a_3 = 5$. Several related problems are discussed in our paper.

The sharpest estimation of $\vartheta(x)$ is at present

$$\vartheta(x) = x + O(x \exp(-(\log x)^{3/5-\epsilon})),$$

obtained by Korobov and Vinogradoff [8]. The Riemann Hypothesis would imply

$$\vartheta(x) = x + O(x^{1/2} \log x)$$

Now I go on to state some problems and results about the distribution of primes. Let $2 = p_1 < p_2 < \cdots$ be the sequence of consecutive primes. A well-known theorem of Tchebicheff states that $p_{n+1} < 2p_n$ for all n, and the prime number theorem implies that $p_{n+1}/p_n \to 1$. The sharpest upper bound for $p_{n+1} - p_n = d_n$ is due to Haneke [9]; he proved, sharpening previous results of Hoheisel, Haneke, Heilbronn, Ingham, and Min, that

$$d_n < p_n^{61/80+\epsilon}.$$

The Riemann Hypothesis would imply

$$d_n < p_n^{1/2+\epsilon}.$$

It has been conjectured that between two consecutive squares there is always a prime. This conjecture can probably not be deduced from the Riemann Hypothesis and seems to be very deep. Piltz conjectured that for every $\epsilon > 0$ and $n > n_0(\epsilon)$

$$d_n < n^{\epsilon}.$$

Cramer [10] conjectured that

$$\overline{\lim_{n=\infty}} \frac{d_n}{(\log n)^2} = 1. \tag{12}$$

Cramer was lead to his conjecture by probabilistic reasoning; the proof or disproof of (12) seems hopeless by the methods which are at our disposal at present. It has been known for a very long time

that $\overline{\lim}\, d_n = \infty$ (the $n-1$ integers $n!+2, n!+3, \ldots, n!+n$ are all composite).

Sharpening previous results of Backlund, Brauer-Zeitz, and Westzynthius, I proved [11] by using Brun's method that for infinitely many n

$$d_n > c \log n \log\log n/(\log\log\log n)^2. \tag{13}$$

Chang [11] succeeded by a simple further idea in dispensing with Brun's method in the proof of (13), and Rankin using an improvement of our method proved that for infinitely many n and every $\epsilon > 0$

$$d_n > (\tfrac{1}{3} - \epsilon) \log n \log\log n \log\log\log\log n/(\log\log\log n)^2. \tag{14}$$

(14) seems to be the natural boundary of our method; the only improvement of (14) in the last 26 years is due to Schönhage and Rankin, who replaced the constant $\frac{1}{3}$ by e^{γ} [11].

A well-known and probably very difficult conjecture on primes asserts that

$$\pi(x+y) \leq \pi(x) + \pi(y). \tag{15}$$

Hardy and Littlewood [12] proved by Brun's method that

$$\pi(x+y) - \pi(x) < \frac{cy}{\log y}. \tag{16}$$

As far as I know this is the only time Hardy and Littlewood used Brun's method. Selberg [12] improved (16) to

$$\pi(x+y) - \pi(x) < \frac{2y}{\log y} + O\left(\frac{y \log\log y}{(\log y)^2}\right). \tag{17}$$

It would be very important if one would replace 2 in (17) by a smaller constant, but this seems to be difficult. A slightly weaker conjecture than (15) states that, for every ϵ and $y > y_0(\epsilon)$,

$$\pi(x+y) - \pi(x) < \frac{(1+\epsilon)y}{\log y}.$$

Selberg's investigations [12] on the limits of the efficiency of the sieve methods indicate that (17) cannot be improved by Brun's method except possibly if very essential changes are made in the estimation of the error terms.

It seems likely that $d_n/\log n$ is everywhere dense in $(0, \infty)$. Ricci [13] and I proved independently that the limit points of $d_n/\log n$ form a set of positive Lebesgue measure, but the only known limit point of this set is ∞. In particular I do not know if $d_n/\log n$ has a rational limit point. It seems certain that $d_n/\log n$ has a continuous distribution function $\psi(t)$. In fact, Bombieri conjectures that $\psi(t) = 1 - e^{-t}$, in other words, the density of integers n for which $d_n < t \log n$ equals $1 - e^{-t}$. There does not seem to be much hope of attacking this conjecture at present, but later in this paper I will state a modification which can probably be settled.

Ricci [13] proved by Brun's method that the lower density of the integers n for which $d_n < \log n$ is positive, and in fact it is not hard to show that there is an $\epsilon > 0$ such that the lower density of the integers n for which $d_n < (1 - \epsilon) \log n$ is also positive. Unfortunately I cannot prove that the upper density of the integers n for which

$$d_n > \log n$$

is positive. It is not hard to deduce from Brun's method that

$$\Sigma' d_n > cx,$$

where the dash indicates that the summation is extended over those $p_n < x$ for which $d_n > \log n$. But unfortunately nothing can be deduced from this because of possible very large values of d_n. In fact I just observe to my annoyance that I cannot show that $d_n/\log n$ has at least one finite limit point greater than or equal to 1. One could give by Brun's method a rough estimation for a constant c so that $d_n/\log n$ certainly has a finite limit point $\geq c$, but as far as I know nobody has given an explicit value for c.

I proved [14] that

$$\underline{\lim}\, d_n/\log n < 1$$

(the prime number theorem immediately implies that the $\underline{\lim}$ is ≤ 1). Rankin [14] proved that the limit in question is $\leq \frac{57}{59}$; Ricci [13] showed that it is $\leq \frac{15}{16}$, and finally Bombieri proved that it is $\leq \frac{29}{32}$ (unpublished). There seems to be no doubt that the $\underline{\lim}$ in question is 0, but this seems very hard to prove; the well-known conjecture that there are infinitely many prime twins, that is, that $d_n = 2$ has infinitely many solutions, would of course imply this.

The sequence d_n, $n = 1, 2, \ldots$, behaves very irregularly.

Turán and I [15] proved that the inequalities $d_{n+1} > d_n$ and $d_{n+1} < d_n$ both have infinitely many solutions. We have not been able to prove that $d_n > d_{n+1} > d_{n+2}$ or $d_n < d_{n+1} < d_{n+2}$ have infinitely many solutions. In fact we cannot disprove the existence of an integer n_0 so that for every $k \geq 0$, $d_{n_0} + 2k > d_{n_0} + 2k + 1$ and $d_{n_0} + 2k + 1 < d_{n_0} + 2k + 2$. It is not known that $d_n = d_{n+1}$ has infinitely many solutions; Rényi and I [15] proved that the number of solutions of $d_n = d_{n+1}$, $1 \leq n \leq x$ is less than $cx/(\log x)^{1/2}$; very likely the true order is $cx/\log x$ but this seems difficult.

It is not difficult to show that for infinitely many indices n, $d_n > d_{n+1}$, $d_n > d_{n-1}$ and for infinitely many indices m, $d_m < d_{m+1}$, $d_m < d_{m-1}$.

Sierpinski [16] observed that

$$\overline{\lim_n} \min (d_n, d_{n+1}) = \infty. \tag{18}$$

It is perhaps surprising that though the proof of $\overline{\lim}\, d_n = \infty$ is trivial the proof of (18) is much more difficult.

Walfisz and Prachar [16] proved that the upper density of the integers n for which

$$\min (d_n, d_{n+1}, \ldots, d_{n+k}) < \epsilon \log n$$

tends to 0 for fixed k together with ϵ (I slightly modified their result). Also I observed [16] that for every $c_1 > 0$ there exists a $c_2 > 0$ so that there are at least $c_2 \log n$ consecutive values $d_k, \ldots, d_{k+r}$, $(k < n)$, all of which are $> c_1$, but I do not know if this holds for every c_1 and c_2. Rényi and I [15] also showed that

$$\frac{c_1 n}{\log n} < \sum_{k=1}^{n} \frac{1}{d_k} < \frac{c_2 n \log\log n}{\log n};$$

probably the upper bound is nearly best possible.

Prachar and I [17] proved that

$$c_1 (\log x)^2 < \sum_{p_k < x} \left| \frac{p_{k+1}}{k+1} - \frac{p_k}{k} \right| < c_2 (\log x)^2.$$

We further showed that if k_i is a subsequence of the integers for

which

$$\frac{p_{k_i}}{k_i} < \frac{p_{k_{i+1}}}{k_{i+1}},$$

then the density of this sequence is 0.

Put $p_k/k = u_k$. We further observed that the prime number theorem implies, for $k > k_0(\epsilon)$,

$$u_{[k(1+\epsilon)]} > u_k; \tag{19}$$

on the other hand to every l there are infinitely many values of k for which

$$u_k > u_{k+l}. \tag{20}$$

There is a big gap between (19) and (20) which we cannot fill. In our paper we state the following further problems on the structure of the sequence u_k:

There are only a finite number of values of k (possibly none) for which

$$\max_{1\le i\le k} u_{k-i} < u_k < \min_{1\le i\le\infty} u_{k+i}.$$

We easily show that the density of the integers k for which $u_k > u_{k+1}$ is positive. We cannot show that the same holds for the k for which $u_k < u_{k+1}$.

We do not know if $u_k < u_{k+1} < u_{k+2}$ or $u_k > u_{k+1} > u_{k+2}$ has infinitely many solutions.

Returning to the question of d_n, I may mention that by using Brun's method I proved [18] that

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

but I cannot prove that

$$\underline{\lim}\, \max \frac{(d_n, d_{n+1})}{\log n} < 1 \text{ or } \overline{\lim}\, \min \frac{(d_n, d_{n+1}, d_{n+2})}{\log n} = \infty,$$

also I cannot prove that

$$\underline{\lim}\, \frac{d_n + \cdots + d_{n+k-1}}{k \log n} < 1 - c$$

where c does not depend on k.

It seems certain that the density of the indices n for which $d_n > d_{n+1}$ is $\frac{1}{2}$, but this seems very hard to prove. I proved [19] though that for a sufficiently small $\epsilon > 0$ the lower density of the indices n for which $d_n > (1+\epsilon)d_{n+1}$ is positive, and the same result holds for $(1+\epsilon)d_n < d_{n+1}$.

Define $n_1 < n_2 < \cdots$ as follows:

$$d_{n_i} > d_n \qquad \text{for all } n < n_i.$$

Very little is known about the sequence n_i, for example, I cannot prove that $n_{i+1} > n_i + 1$ for $i > i_0$. It is easy though to see that the density of the n_i is 0.

Cramér [10] proved, assuming the Riemann hypothesis, that

$$\sum_{n<x} d_n^2 < cx(\log x)^4.$$

Very probably

$$\sum_{n<x} d_n^2 < cx(\log x)^2,$$

but this seems hopeless. It may even be true that

$$\lim_{x=\infty} \frac{1}{(\log x)^2} \sum_{n=x} d_n^2 = c. \tag{21}$$

It is not hard to prove that the lower limit in (21) is positive.

Similar questions can be asked for other sequences of numbers. For example, let $s_1 < s_2 < \cdots$ be the sequence of squarefree numbers; it is well known and easy to prove that their density is $6/\pi^2$. I proved [20] that

$$\sum_{s_i<n} (s_{i+1} - s_i)^2 = c_2 n + o(n).$$

It seems very probable that for every $\alpha > 0$

$$\sum_{s_i<n} (s_{i+1} - s_i)^\alpha = c_\alpha n + o(n). \tag{22}$$

(22) if true must be very difficult, since it would imply $s_{i+1} - s_i = o(s_i^\epsilon)$ for every $\epsilon > 0$. My method breaks down for $\alpha > 2$ but it proves (22) for $\alpha \leq 2$. The best upper bound for $s_{i+1} - s_i$ is due to Richert [20] who proved (sharpening a previous result of

K. F. Roth)

$$s_{i+1} - s_i < cs_i^{3/4} \log s_i.$$

It is easy to prove [20] that

$$s_{i+1} - s_i > (1 + o(1)) \frac{\pi^2}{6} \log s_i / \log \log s_i, \tag{23}$$

but as far as I know nobody has succeeded in replacing $1 + o(1)$ by $1 + c$ in (23).

Denote by $Q(x)$ the number of squarefree integers not exceeding x. It is easy to prove that

$$Q(x) = \frac{6}{\pi^2} x + O(x^{1/2}), \tag{24}$$

and the prime number theorem gives $o(x^{1/2})$ in (24). One would expect the Riemann Hypothesis to give $o(x^{1/4+\epsilon})$, but it seems that one can only deduce $o(x^{3/4+\epsilon})$. The true order of magnitude of the error term in (24) is unknown.

One could try to generalize (22) as follows. Let $a_1 < a_2 < \cdots$ be an infinite sequence of integers satisfying $a_k/k^2 \to \infty$ and let $b_1 < b_2 < \cdots$ be the sequence of integers no one of which is a multiple of any a. Is it then true that

$$\sum_{b_i \le n} (b_{i+1} - b_i)^2 = Cn + o(n)? \tag{25}$$

If $a_i = p_i^2$ we obtain (22). If instead of $a_k/k^2 \to \infty$ only $a_k < ck^2$ is assumed it is easy to see that (25) cannot hold; at present I cannot disprove that in this case

$$\sum_{b_i < n} (b_{i+1} - b_i)^2 < An$$

remains true for a suitable A.

In [14] I conjectured that if $1 = a_1 < a_2 < \cdots < a_{\varphi(n)} = n - 1$ are the integers relatively prime to n then

$$\sum_{i=1}^{\varphi(n)-1} (a_{i+1} - a_i)^2 < \frac{cn^2}{\varphi(n)}. \tag{26}$$

This conjecture seems to be an elementary version of (21) and should not be too difficult to prove.

Hooley [20] in fact proved that for every $\alpha < 2$

$$\sum_{i=1}^{\varphi(n)-1} (a_{i+1} - a_i)^\alpha < \frac{c_\alpha n^\alpha}{\varphi(n)^{\alpha-1}}$$

and

$$\sum_{i=1}^{\varphi(n)-1} (a_{i+1} - a_i)^2 < cn^2 \frac{\log\log n}{\varphi(n)}.$$

Put $n_k = 2, 3, \ldots p_k$. The $\varphi(n_k)$ integers relatively prime to n_k in the interval $(1, n_k)$ might be expected to show a somewhat similar behavior to the primes. Let

$$1 = a_1^{(k)} < a_2^{(k)} < \cdots < a_{\varphi(n_k)}^{(k)} = n_k - 1$$

be the integers relatively prime to n_k. Let us investigate to what extent this sequence satisfies the conjectures we stated about primes. First of all, it is not hard to deduce from Brun's method that there are constants c_1 and c_2 such that every interval of length $c_1(\log n)^{c_2}$ contains an integer relatively prime to n_k.

A theorem of Mertens implies that

$$\frac{n_k}{\varphi(n_k)} = \frac{(1 + o(1))e^{-\gamma}}{\log\log n_k} = \frac{(1 + o(1)e^{-\gamma}}{\log k}.$$

It is not hard to prove that (if $a_{i+1}^{(k)} - a_i^{(k)} = d_i^{(k)}$) the sequence

$$\frac{d_i^{(k)}}{\log k}$$

is everywhere dense in $(0, \infty)$; in other words to every ϵ and η there is a k_0 such that for $k > k_0$ every interval of length η in $(\epsilon, 1/\epsilon)$ contains a number of the form $d_i^{(k)}/\log k$. I have not been able to prove that

$$\frac{d_i^{(k)}}{\log k}$$

has a distribution function (the precise meaning of this statement is obvious and is left to the reader).

It seems probable that the number of integers $1 \leq s < \varphi(n_k)$ for which $d_{i+1}^{(k)} > d_i^{(k)}$, is $[\frac{1}{2} + o(1)]\varphi(n_k)$, but as far as I know this has

not been proved. I do not know the number of solutions of $d_{i+1}^{(k)} = d_i^{(k)}$, but it would be easy to obtain crude upper and lower bounds.

It is easy to see that for every t and all $k > k_0(t)$

$$d_i^{(k)} > d_{i+1}^{(k)} > \cdots > d_{i+t-1}^{(k)}$$

is solvable.

Sivasankaranarayana Pillai conjectured that

$$\sum_{\substack{p_n < x \\ n \equiv 0 \pmod 2}} d_n = [\tfrac{1}{2} + o(1)]x. \tag{27}$$

(27) seems very hard to prove; Brun's method easily gives

$$\sum_{\substack{p_n < x \\ n \equiv 0 \pmod 2}} d_n > cx.$$

One can also conjecture that

$$\sum_{i \equiv 0 \pmod 2} d_i^{(k)} = [\tfrac{1}{2} + o(1)]n_k, \tag{28}$$

but I have not been able to prove this.

Jacobsthal defines $g(n)$ to be the least integer such that among any $g(n)$ consecutive integers there is at least one relatively prime to n. Put

$$\max g(n) = C(r) + 1,$$

where the maximum is taken over all the integers n with $\nu(n) \leq r$ (where $\nu(n)$ denotes the number of distinct prime factors of n). We have

$$\frac{c_1 r(\log r)^2 \log\log\log r}{(\log\log r)^2} < C(r) < c_2 r^{c_3}. \tag{29}$$

The left side of (29) follows from (13) and the right side can be easily obtained by Brun's method. Jacobsthal conjectured that

$$C(r) < c_4 r^2. \tag{30}$$

The exponent in (29) can be reduced by Selberg's improvement of Brun's method, but (30) seems hopeless at present [21].

Now we discuss primes in arithmetic progressions. Dirichlet was the first to prove that every arithmetic progression $\{a + kd\}$ with $(a, d) = 1$ represents infinitely many primes. Many mathematicians attempted without success to find an elementary proof, but

finally Selberg [22] was successful. Denote by $\pi(a, d, x)$ the number of primes $\leq x$ of the form $a + kd$. The prime number theorem for arithmetic progressions states that

$$(31) \quad \pi(a, d, x) = [1 + o(1)] \frac{x}{\varphi(d) \log x} \qquad (d \text{ fixed}, x \to \infty).$$

It is not difficult to prove (31) by the method of Selberg and myself [22]. The generalized Riemann Hypothesis for L-functions would imply that

$$\pi(a, d, x) = \frac{1}{\varphi(d)} \int_2^x \frac{dy}{\log y} + O(x^{1/2} \log x)$$

uniformly in d, and also that the least prime $p(a, d)$ in $a + kd$ is less than $d^{2+\epsilon}$.

Linnik [23] proved without using any hypothesis that

$$p(a, d) < c_1 d^{c_2}.$$

Linnik's proof has been simplified first by Rodosskij and still further recently by Turán and Knapowski [22].

Turán [24] proved using the generalized Riemann Hypothesis that for all but $o[\varphi(d)]$ arithmetic progressions $a + kd$

$$(32) \qquad p(a, d) < cd(\log d)^{2+\epsilon}.$$

Perhaps the exponent $2 + \epsilon$ can be replaced by $1 + \epsilon$ but this is very deep if true. I proved [24] using Brun's method that for every $c_1 > 0$

$$p(a, d) < c_1 \varphi(d) \log d$$

for at least $c_2 \varphi(d)$ [where $c_2 = c_2(c_1)$] values of a. In the opposite direction, I could only show that there exists a constant c_3 and an infinite sequence $d_1 < d_2 < \cdots$ such that

$$(33) \qquad p(a, d_i) > (1 + c_1) \varphi(d_i) \log d_i$$

for at least $c_4 \varphi(d_i)$ values of a. There seems no doubt that this holds for all sufficiently large d, but I could not prove it. The proof of (33) used Brun's methods and thus strongly used special properties of primes. Perhaps the following general result holds: Let $a_1 < a_2 < \cdots$ be a sequence of integers for which

$$A(x) = \sum_{a_i \leq x} 1 = [1 + o(1)] \frac{x}{\log x}.$$

Denote by $f(a, d, n)$ the smallest $a_i \equiv d \pmod{n}$. Then there is an infinite sequence $n_1 < n_2 < \cdots$ so that, for at least $c_1 n_i$ values of d in $0 \leq d < n_i$,

$$f(a, d, n_i) > (1 + c_2) n_i \log n_i. \tag{34}$$

Perhaps (34) holds for all sufficiently large n.

Using the results of [24] Turán proved that for every irrational $\alpha > 1$ the sequence $p\alpha \pmod 1$ is uniformly distributed; later Vinogradov [24] proved this without any hypothesis, and by using his powerful methods of estimating trigonometric sums, he also obtains a fairly good estimation of the discrepancy of the sequence $p\alpha \pmod 1$. It follows easily from the uniformity of distribution that for every irrational $\alpha > 1$, $[n\alpha] = p$ has infinitely many solutions. As far as I know it is not known whether there are infinitely many primes p for which $[p\alpha] = q$.

Now I want to say something about the comparative theory of prime numbers; a subject recently developed by Turán and Knapowski [25]. The origin of this subject is to be found in the following conjecture of Tchebicheff: put

$$f(x) = \sum_p (-1)^{p-1/2} e^{-px}.$$

Then Tchebicheff stated that $f(x) \to -\infty$ as x tends to 0. This conjecture is still unproved and must be very deep since Hardy, Littlewood, and Landau [25] showed that it is equivalent to the Riemann Hypothesis for the L-function $1 - \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \cdots$ belonging to the modulus 4.

Tchebicheff stated that his conjecture implies a preponderance of the primes $\equiv 3 \pmod 4$ over those $\equiv 1 \pmod 4$. Littlewood [25] proved on the other hand that

$$\pi(1, 4, x) - \pi(3, 4, x)$$

changes sign infinitely often.

Turán and Knapowski [25] recently took up this subject and obtained a whole series of interesting results which seemed unattainable previously. I just state here a few of them and must refer to their joint papers and to their forthcoming book on this subject.

A modulus d is called good if the L-functions $L(s, \chi)$ belonging to this modulus d have no real root in the critical strip. The values $3 \leq d \leq 12$ are all good and possibly every modulus is good, but it is not even known that there are infinitely many good moduli.

1. If d is good and T is sufficiently large, then the interval[1] $(\log_3 T, T)$ always contains an x_1 and an x_2 for which for any l with $(l, d) = 1$ and $l \not\equiv 1 \pmod{d}$,

$$\pi(1, d, x_1) - \pi(l, d, x_1) > \frac{\sqrt{x_1}}{\log x_1} \log_5 x_1,$$

$$\pi(1, d, x_2) - \pi(l, d, x_2) < \frac{\sqrt{x_2}}{\log x_2} \log_5 x_2;$$

further $\pi(1, d, x) - \pi(l, d, x)$ has at least $c \log_4 T$ changes of sign in $(0, T)$.

2. For good d the interval $(\log_3 T, T)$ always contains an x_1 and x_2 for which

$$\pi(1, d, x_1) - \frac{\pi(x_1)}{\varphi(d)} > \frac{\sqrt{x_1}}{\log x_1} \log_5 x_1,$$

$$\pi(1, d, x_2) - \frac{\pi(x_2)}{\varphi(d)} < -\frac{\sqrt{x_2}}{\log x_2} \log_5 x_2.$$

3. If d is good and $T > T_0$ and l is a quadratic residue (mod d) then the interval $(T^{1/4}, T)$ contains values x_1 and x_2 for which

$$\pi(1, d, x_1) - \pi(l, d, x_1) > T^{1/2} \exp\left(-\frac{\log T \log_3 T}{\log_2 T}\right),$$

$$\pi(1, d, x_2) - \pi(l, d, x_2) < -T^{1/2} \exp\left(-\frac{\log T \log_3 T}{\log_2 T}\right).$$

4. If d is good and $T > T_0$ then for every two distinct values l_1 and l_2

$$\sum_{\substack{n \equiv l_1 \pmod{d} \\ n \leq x}} \Lambda(n) - \sum_{\substack{n \equiv l_2 \pmod{d} \\ n \leq x}} \Lambda(n)$$

changes sign in $(T, e^{2\sqrt{T}})$.

[1] We write $\log_2$ for log log, and so on.

5. Knapowski [26] proved that for sufficiently large T

$$\pi(x) - \int_2^x \frac{dy}{\log y}$$

changes sign at least $c \log_4 T$ times in $(0, T)$. (Riemann conjectured that

$$\pi(x) < \int_2^x \frac{dy}{\log y}$$

for all x and Littlewood disproved this conjecture by showing that

$$\pi(x) - \int_2^x \frac{dy}{\log y}$$

$L_i(x)$ changes sign infinitely often [26].)

Knapowski and Turán use the new and surprising inequalities of Turán which he developed in several of his papers and in his book [25]. A new English edition of the book will soon appear and will contain many interesting problems and new results. The inequalities are analytic in nature but can also be considered as part of the theory of Diophantine approximation, and in a certain sense they can be considered as generalizations of Dirichlet's theorem. Here I want to state only two problems in this theory, on which I also worked.

Let $z_1 = 1$ and $|z_i| \leq 1$ for $2 \leq i \leq n$. Put $s_k = \sum_{i=1}^{n} z_i^k$. Turán conjectured that there exists an absolute constant c such that, for all n and all choices of the z's,

$$\max_{1 \leq k \leq n} |s_k| \geq c. \tag{35}$$

Atkinson [27] recently proved this conjecture, and in an unpublished manuscript he showed that c can be chosen to be $\frac{1}{3}$. Turán further conjectured that to every ϵ there is an n_0 such that for $n > n_0$

$$\max_{1 \leq k \leq n} |s_k| > 1 - \epsilon.$$

I observed [25] that there is a constant $c > 0$ and a sequence with $z_1 = 1$, $|z_i| \leq 1$ for $2 \leq i \leq n$ such that

$$\max_{2 \leq k \leq n+1} |s_k| < \frac{1}{(1 + c)^n}. \tag{36}$$

The contrast between (35) and (36) is striking. I was unable to decide the existence of a sequence with $|z_i| \geq 1$ for $1 \leq i \leq n$ which satisfies (36).

Very recently Turán told me the following conjecture: Assume that the infinite sequence s_k, $1 \leq k < \infty$, contains infinitely many consecutive $n-1$-tuples which are all 0. Then (essentially)

$$z_j = e^{2\pi ij/n}, \qquad 1 \leq j \leq n. \tag{37}$$

Perhaps (37) can be deduced if we know only that the sequence s_k contains two consecutive $n-1$-tuples which are 0.

Before I leave the subject of prime numbers I would like to call attention to some related questions: E. Jabotinsky and I and independently and simultaneously V. Gardiner, R. Lazarus, N. Metropolis, and S. Ulam considered a modification of the sieve of Eratostenes and we were lead to several interesting questions, but for this I must refer to our papers on this subject [28].

Very interesting questions are raised in a paper by Hawkins on the so-called random sieve [29]; since this is perhaps not very well known I give the necessary definitions. We define a "random" sequence $a_i(t)$ as follows: Put $a_1 = 2$, and cross out each integer $3, 4, \ldots$ with probability $\frac{1}{2}$. Let a_2 be the first integer which has not been crossed out. Then cross out each of the integers $a_2 + 1$, $a_2 + 2, \ldots$ with probability $1/a_2$ and let a_3 be the first integer not crossed out, then cross out each of the integers $a_3 + 1, \ldots$ with probability $1/a_3$, and so on. Thus we obtain the "random" sequence $a_i = a_i(t)$, and Hawkins conjectured that for almost all t $a_i/(i \log i) \to 1$, but as far as I know this has never been satisfactorily proved [29].

Finally, I would like to call attention to the following result: Let $p_1 = 3$, $p_2 = 5$, and let p_k be the smallest prime for which

$$p_k \not\equiv 1 (\mathrm{mod}\ p_i), \qquad 1 \leq i < k.$$

Then I prove that

$$\lim_{k=\infty} \frac{p_k}{k \log k \log \log k} = 1. \tag{38}$$

The proof of (38) uses Tauberian arguments which are simpler than those used in the elementary proof of the prime number theorem [30].

6. Now I discuss some results in the arithmetic theory of polynomials. Let $f(x) = a_0 x^n + \cdots + a_n$ be an irreducible poly-

nomial with integral coefficients. Denote by $\nu(p)$ the number of solutions of the congruence

$$f(x) \equiv 0 \pmod{p}.$$

The prime ideal theorem [22] states that

$$\sum_{p<x} \nu(p) = (1 + o(1)) \frac{x}{\log x}. \tag{39}$$

Shapiro [22] proved (39) by the method of Selberg and myself in an elementary way. The proof is elementary in the sense that it does not use function theory, but as in all the other proofs of (39) he has to use algebraic number theory, that is, the theory of ideals. It would of course be interesting to prove (39) without the use of ideal theory, but perhaps this is not possible. I often tried without success to prove without using ideal theory that

$$\sum_{\nu(p)>0} 1/p = \infty.$$

Knapowski and Turán (unpublished; see [25]) proved the following theorem: Suppose $T > T_0(f)$. Then there are four numbers u_1, u_2, u_3, u_4 satisfying

$$\log_3 T \leq u_2 \exp(-8(\log u_2)^{5/6}) \leq u_1 \leq u_2 \leq T,$$

$$\log_3 T \leq u_4 \exp(-8(\log u_4)^{5/6}) \leq u_3 \leq u_4 \leq T,$$

for which

$$\sum_{u_1 \leq p \leq u_2} \nu(p) - \int_{u_1}^{u_2} \frac{du}{\log u} > \frac{u_2^{1/2}}{\log u_2},$$

$$\sum_{u_3 \leq p \leq u_4} \nu(p) - \int_{u_3}^{u_4} \frac{du}{\log u} < -\frac{u_4^{1/2}}{\log u_4}.$$

This theorem is new even for the case $f(x) = x$.

Denote by $\nu(m)$ the number of distinct prime factors of m. The prime ideal theorem immediately implies that

$$\sum_{n=1}^{x} \nu[f(n)] = [1 + o(1)]x \log\log x.$$

Turán [31] proved the following surprising result: Let $h(n)$ tend to infinity together with n as slowly as we please; then the density of the integers n for which the inequality

$$\log\log n - h(n)(\log\log n)^{\frac{1}{2}} < \nu[f(n)] < \log\log n + h(n)(\log\log n)^{\frac{1}{2}}$$

does not hold is 0. The special case $f(x) = x$ is a classical result of Hardy and Ramanujan [31].

Halberstam [31] proved that the density of integers n for which

$$\nu[f(n)] < \log\log n + c(\log\log n)^{\frac{1}{2}}$$

equals $(2\pi)^{-\frac{1}{2}} \int_{-\infty}^{c} e^{-x^2/2}\,dx$. The special case $f(x) = x$ is contained in a theorem of Kac and myself.

I proved [31] that the number of primes $p \leq x$ for which

$$(40) \qquad (1-\epsilon)\log\log p < \nu(p-1) < (1+\epsilon)\log\log p$$

is not satisfied is $o(x/\log x)$. Halberstam [31] proved the following very much more general and more precise result. Suppose $f(x) \neq cx$. Then the number of primes $p \leq x$ for which

$$\nu[f(p)] < \log\log p + c(\log\log p)^{\frac{1}{2}}$$

equals

$$[1 + o(1)](2\pi)^{-\frac{1}{2}}\left(\int_{-\infty}^{c} e^{-y^2/2}\,dy\right)\frac{x}{\log x}.$$

Denote by $d(n)$ the number of divisors of n. Titchmarsh [31] proved that

$$\frac{c_2 x}{(\log x)^{\frac{1}{2}}} < \sum_{p<x} d(p-1) < c_1 x.$$

I proved [31] using (40) that

$$(41) \qquad \sum_{p<x} d(p-1) > \frac{x}{\log x}\, 2^{(1-\epsilon)\log\log x},$$

and Haselgrove [32] proved that

$$\sum_{p<x} d(p-1) > \frac{cx}{\log\log x}.$$

Finally, Linnik [31], using his powerful new dispersion method, proved that

$$\sum_{p<x} d(p-1) = (1+o(1))\frac{315\zeta(3)}{2\pi^4}x + o(x).$$

Van der Corput [32] proved that

$$c_1 x \log x < \sum_{n=1}^{x} d[f(n)] < c_2 x (\log x)^{\alpha}.$$

I proved [32] that

$$\sum_{n=1}^{x} d[f(n)] < c_3 x \log x \tag{42}$$

The proof is elementary but not simple. Very likely

$$\sum_{n=1}^{x} d[f(n)] = cx \log x + o(x \log x). \tag{43}$$

If true (43) must be very hard to prove, since the prime factors greater than x make the sharp estimation of the sum (43) very difficult. The constant c in (43) will perhaps depend on the polynomial $f(x)$. Bellmann and Shapiro [32] proved (43) if $f(x)$ is of degree 2, and in this case $c = 2$. Recently Hooley [32] proved that if $f(x)$ is of degree 2 then

$$\sum_{n=1}^{x} d[f(n)] = 2x \log x + O(x^{\alpha}), \qquad \alpha < 1.$$

Using Brun's method and the one with which I proved (42), I can show that

$$\sum_{p<x} d[f(p)] < c_4 x.$$

Perhaps if $f(x) \neq cx$ one can show by Linnik's method that

$$\Sigma\, d[f(p)] > c_5 x.$$

Denote by $P(n)$ the greatest prime factor of n. Tchebicheff [33] proved that

$$\lim_{x=\infty} P\Big[\prod_{n=1}^{x}(1+n^2)\Big]/x = \infty.$$

Nagell and Ricci [33] proved that if $f(x)$ is of degree greater than 1 then

$$P\Big[\prod_{n=1}^{x} f(n)\Big] > cx \log x,$$

and I [33] proved that

$$P\Big[\prod_{n=1}^{x} f(n)\Big] > c_1 x\,(\log x)^{\log_2 x}.$$

By more complicated methods I can prove that

$$P\Big[\prod_{n=1}^{x} f(n)\Big] > c_3 x \exp\,(\log x)^{c_4}. \tag{44}$$

I never published the proof of (44), which is fairly complicated. The proof could be simplified a great deal if I could prove the following purely combinatorial theorem [33]. To every c_1 there exists a c_2 so that if $A_1, \ldots, A_l$, where $l = [c_2{}^k]$, are sets each having at most k elements, then there are c_1 of them $A_{i_1}, \ldots, A_{i_{c_1}}$ which have pairwise the same intersection. Rado and I [33] proved this with $k!(c_1 - 1)^k$ instead of $[c_2{}^k]$. (44) seems to be the natural boundary of my method. Very likely

$$P\Big[\prod_{n=1}^{x} f(n)\Big] > x^{1+d}, \tag{45}$$

but this seems very difficult. (44) would follow easily if we could prove that the number of integers $n \leq x$ for which all prime factors of $f(n)$ are $\leq x$ is greater than cx, but this has not even proved for $f(x) = 1 + x^2$.

It seems probable in fact that

$$P\Big[\prod_{n=1}^{x} f(n)\Big] > cx^k$$

when $f(x)$ is a polynomial of degree k.

A well-known result of Pólya [34] states that if the degree of $f(x)$ is > 1 then

$$\lim_{n=\infty} P[f(n)] = \infty. \tag{46}$$

If $f(x) = 1 + x^2$ Mahler and Chowla [34] (independently) proved that

$$P[f(n)] > c \log \log n. \tag{47}$$

(47) is certainly very far from being best possible, but I do not know of any reasonable upper bound for $P[f(n)]$ which is valid for infinitely many n. [Added in proof: Schinzel just informed me that he showed that for every t there are infinitely many n for which $P(n^2 + t) < \exp(c \log n/\log \log \log n)$.]

Another result of Pólya [34], related to (41), states that if $p_1, \ldots, p_k$ is any finite set of primes and $a_1 < a_2 < \cdots$ is the set of all integers composed of the p's, then $a_{i+1} - a_i$ tends to infinity. This was improved by Siegel [34] to

$$a_{i+1} - a_i > a_i^{1-\epsilon} \tag{48}$$

for every $\epsilon > 0$ if $i > i_0(\epsilon)$. It is easy to see that if $k > 1$ then

$$\frac{a_{i+1}}{a_i} \to 1 \tag{49}$$

as $i \to \infty$. There is a gap between (48) and (49) which as far as I know has not yet been filled.

Here I would like to mention a problem of Wintner which he communicated to me orally. Does there exist an infinite sequence of primes $p_1 < p_2 < \cdots$ such that if $a_1 < a_2 < \cdots$ is the set of all the integers composed of the p's then

$$\lim_{i=\infty} (a_{i+1} - a_i) = \infty ? \tag{50}$$

It seems certain that such a sequence exists, but I was unable to prove this.

One final result about greatest prime factors. It is not difficult to prove that for every n

$$P(2^n - 1) > n.$$

Schinzel [34] recently proved that for $n > 12$

$$P(2^n - 1) > 2n. \tag{51}$$

The proof of (51) is surprisingly complicated. Very likely

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

As far as I know $P(n! + 1)$ has not yet been investigated.

The polynomial $x^2 + x + 2$ is even for all integral values of x, thus it cannot represent any odd prime. A well known elementary theorem states that if $f(x)$ is of degree k and $f(x) \equiv O(\text{mod } n)$ for all integral values of x then $n \mid k!$. One could conjecture that $f(n)$ represents infinitely many integers of the form $a \cdot p$ where $a \mid k!$. As already stated Dirichlet proved this for polynomials of degree 1 in 1837. But the conjecture has never been proved even for a single polynomial of degree greater than 1. The only result for expressions of degree greater than 1 is due to I. I. Pjatezkij-Schapiro [35]. He proved that the number of primes of the form $[n^c]$ in $1 \leq n \leq x$ is $(1 + o(1))x/(1 + c) \log x$ if $1 \leq c \leq \frac{12}{11}$.

The result very likely holds for all nonintegral $c \geq 1$.

Heilbronn [36] proved using Brun's method that the number of integers $n \leq x$ for which $f(n)$ is a prime is less than $cn/\log n$; also it follows from Brun's method that there is an absolute constant c_1, depending only on the degree of $f(x)$, such that $f(n)$ represents infinitely many integers having fewer than c_1 prime factors.

Another conjecture states that $f(x)$ represents infinitely many integers of the form aQ, where $a \mid k!$ and Q is squarefree. It is well known and easy to prove that $f(x)$ represents infinitely many kth power-free integers, and in fact the density of the integers n for which $f(n)$ is kth power-free is positive (k being the degree of $f(x)$).

I proved [37] that if $k > 2$ then $f(x)$ represents infinitely many $(k-1)$-th power-free integers, the only exception being that if $k = 2^l$ then it may happen that $f(n) \equiv O(\text{mod } 2^{l-1})$ for all n, but then $f(x)$ represents infinitely many integers of the form $2^{l-1}Q$ where Q is odd and $(k-1)$-th power-free. The proof is fairly complicated. We would expect that the density of the integers for which $f(n)$ is $(k-1)$-th power-free is positive, but I could not prove this. I could prove nothing about the representation of $(k-2)$-th power-free numbers, for example, I cannot show that $n^4 + 2$ represents infinitely many squarefree numbers.

As far as I know the question whether $2^n \pm 1$ represents infinitely many kth power-free integers, is intractable at present, and the same is true for $n! \pm 1$.

7. Now I want to discuss a set of problems which could be said to belong to combinatorial number theory, that is, the questions have both number-theoretic and combinatorial character. These problems perhaps do not all have great importance but they are very

close to my heart (or rather I should say to my brain) since two of my main interests are number theory and combinatorial analysis.

I will start with Van der Waerden's theorem [38]. This asserts that if one splits the integers into two classes in any way then at least one of them contains an arbitrary long arithmetic progression. We shall be more concerned here with the finite form of this theorem, also proved by Van der Waerden: For every k there exists a smallest integer $f(k)$ such that if we split the integers $1 \leq t \leq f(k)$ into two classes then at least one of them contains an arithmetic progression of k terms. The upper bound obtained for $f(k)$ is enormously large; the reason for this is that all proofs use a double induction. Denote by $f(k, l)$ the smallest integer such that if we split the integers $1 \leq t \leq f(k, l)$ into l classes then at least one of them contains an arithmetic progression of k terms. The induction is carried out with respect to k and l and so gives a very poor estimation for $f(k, l)$ and in particular for $f(k) = f(k, 2)$. At least I believe that the estimation is very bad, though no one succeeded in obtaining any better one. Rado and I [38] obtained the first nontrivial lower bound for $f(k)$, by proving that $f(k) > ((k-1)2^k)^{1/2}$. The proof is based on the following simple consideration: The total number of ways of splitting n integers into two classes is clearly 2^n, and the number of splittings such that one of the two sets contains a given arithmetic progression of k terms is easily seen to be 2^{n-k+1}, and since there are fewer than n^2 arithmetic progressions all of whose terms are $\leq n$ we obtain that the total number of ways of splitting the integers $1 \leq t \leq n$ so that one of the sets will contain an arithmetic progression of k terms is at most $n^2 2^{n-k+1}$. This is less than 2^n if $n < 2^{(k-1)/2}$, whence $f(k) \geq 2^{(k-1)/2}$, and a more careful estimation of the number of arithmetic progressions gives $f(k) > [(k-1)2^k]^{1/2}$.

W. Schmidt [38] obtained by a difficult and ingenious improvement of our method

$$f(k) > 2^{k-c(k \log k)^{1/2}}, \tag{52}$$

and this is the best known lower bound for $f(k)$ up to the present time.

Using Van der Waerden's theorem, A. Brauer [39] proved that to every k there is a $p_0(k)$ so that if $p > p_0(k)$ then p has k consecutive quadratic residues and also k consecutive quadratic nonresidues (in fact Brauer proved a somewhat more general theorem).

Probably the right order of magnitude of $p_0(k)$ is $\exp ck$. It can be deduced from the results of A. Weil on congruences in two variables that $p_0(k) < \exp ck$.

In the same way as for the well-known theorem of Ramsey, define $g(k, l)$ as the smallest integer for which if we split the integers $1 \leq t \leq g(k, l)$ into two classes then either the first class contains an arithmetic progression of k terms or the second an arithmetic progression of l terms. If $k \leq l$ then clearly $f(k) \leq g(k, l) \leq f(l)$, but I do not know of any nontrivial estimation of $g(k, l)$; in particular it would be interesting to have upper and lower estimations of $g(3, l)$.

Let $h(n)$ be an arbitrary number-theoretic function which takes on the values $+1$ and -1. Van der Waerden's theorem asserts that for every k there is an arithmetic progression for which $h(a) = h(a + d) = \cdots = h[a + (k - 1)d]$. For a long time I conjectured that for every c there exist a d and an m such that

$$\left| \sum_{k=1}^{m} h(kd) \right| > c; \tag{53}$$

more precisely, perhaps there exists a constant c such that for every function $h(n)$ and every x there exist d and m with $md \leq x$ such that

$$\left| \sum_{k=1}^{m} h(kd) \right| > c_1 \log x. \tag{54}$$

It is easy to see that (54) if true is best possible. (53) requires much less than Van der Waerden's theorem but the arithmetic progressions are much more restricted. K. F. Roth recently proved (to appear in *Acta Arithmetica*) that there exist $a > 0$, $d < n^{1/2}$, $a + md < n$ for which

$$\left| \sum_{k=0}^{m} h(a + kd) \right| > cn^{1/4}. \tag{54'}$$

Roth in fact proves a more general theorem. In conversation Roth raised the question whether if we drop the condition $d < n^{1/2}$, then $cn^{1/4}$ can perhaps be replaced by $n^{1/2-\epsilon}$. I showed by probabilistic reasoning that (54′) is false in general with $cn^{1/2}$ when c is sufficiently large. It is probably false with $cn^{1/2}$ for every $c > 0$ if $n > n_0(c)$, but I have not been able to show this.

Assume now that $h(n) = \pm 1$ is multiplicative, that is, $h(a \cdot b) = h(a) \cdot h(b)$. Then (53) would imply that

$$\left| \sum_{k=1}^{m} h(k) \right| \tag{55}$$

is unbounded. (55) seems quite difficult [38]. If $h(p^\alpha) = (-1)^\alpha$ we obtain Liouville's function $\lambda(n)$ and (55) is well known in this case, in fact

$$\sum_{k=1}^{n} \lambda(k) \neq o(n^{\frac{1}{2}-\epsilon}).$$

An interesting and beautiful conjecture on multiplicative functions $h(n) = \pm 1$ states that

$$\lim_{x=\infty} \frac{1}{x} \sum_{n=1}^{x} h(n) \tag{56}$$

always exists and that the limit of (56) is 0 if and only if

$$\sum_{h(p)=-1} \frac{1}{p} = \infty. \tag{57}$$

If (57) does not hold it is easy to see that the limit (56) exists and is different from 0. The conjecture (56) does not seem easy; it certainly contains the prime number theorem, for if $h(n) = \lambda(n)$, (56) is well known to be equivalent to the prime number theorem.

Wintner observed that if we only assume $|h(n)| = 1$ then (56) does not have to hold. Rényi recently observed that $h(n) = e^{i \log n}$ provides a simple counterexample. [Added in proof: Wirsing just informs me that he proved (56).]

If $h(n)^k = 1$ for some k, (56) probably remains true.

Another variant of Ván der Waerden's theorem is the following: Define $f(k, c)$ $(0 < c \leq 1)$ as the smallest integer such that for every $h(n) = \pm 1$ there exists an arithmetic progression

$$0 < a < a + d < \cdots < a + (k-1)d < f(k, c)$$

for which

$$\left| \sum_{l=0}^{k-1} h(a + ld) \right| \geq ck.$$

Clearly $f(k, 1) = f(k)$. Using the same method as that which Rado and I used, I showed [38] that for every $c > 0$

$$f(k, c) > (1 + \alpha_c)^k,$$

where $\alpha_c \to 0$ as $c \to 0$ and $\alpha_c \to \sqrt{2} - 1$ as $c \to 1$ (perhaps the method of Schmidt would allow one to prove that $\alpha_c \to 1$ as $c \to 1$, but this has not been done). I would expect that for every $c < 1$

$$f(k, c) < (1 + \alpha_c')^k.$$

I am doubtful whether the same inequality holds for $f(k)$ (that is, for $c = 1$). Possibly

$$\lim_{k=\infty} [f(k, c)]^{1/k} = \alpha(c), \qquad 0 < c < 1.$$

The problem of obtaining a good upper bound for $f(k)$ led Turán and myself [40] to the following question: Let $1 \leq a_1 \leq \cdots \leq a_l \leq n$ and assume that the sequence $\{a_i\}$ does not contain an arithmetic progression of k terms. Put

$$\max l = \gamma_k(n).$$

If we could show that, for a certain n, $\gamma_k(n) < n/2$, we would immediately obtain $f(k) \leq n$. Unfortunately this has been shown only for $k = 3$, $n = 20$. In our paper [40] we only obtain crude inequalities for $\gamma_3(n)$, and Szekeres conjectured that $\gamma_k(n) = o(n)$ and that $\gamma_k(n) < n^{1-\epsilon_k}$. Behrend [40] observed that $\lim_{k=\infty} \gamma_k(n)/n = c_k$ exists; he further showed that either all $c_k = 0$ or $\lim_{k=\infty} c_k = 1$. Salem and Spencer [40] disproved $\gamma_k(n) < n^{1-\epsilon_k}$, in fact they showed that $\gamma_3(n) > n^{1-c/\log\log n}$, and Behrend showed [40] that

$$\gamma_3(n) > n^{1-c/\sqrt{\log n}}. \tag{58}$$

This is still the best known lower bound for $\gamma_3(n)$. Rankin [40] improved (58) for $k > 3$.

Roth [40] proved $\gamma_3(n) = o(n)$, in fact he showed that

$$\gamma_3(n) < \frac{cn}{\log\log n}.$$

Unfortunately Roth's method does not seem to give $\gamma_4(n) = o(n)$. It would be of great interest if one could prove that $\gamma_k(n) < \pi(n)$ for every k if $n > n_0(k)$ since this would imply that for every k there

are k primes in an arithmetic progression. Sevedinskij observed that $23143 + l \cdot 30030$ is a prime for $0 \leq l \leq 11$. Chowla [40] proved that there are infinitely many triplets of primes in arithmetic progression. His proof does not use $\gamma_k(n)$, but runs as follows. As is well known Vinogradoff proved that every sufficiently large odd number is the sum of three primes, and Van der Corput, Esterman, and Tchudakoff proved using Vinogradoff's method that the number of even numbers not exceeding x which are not of the form $p + q$ $(p \neq q)$ is $o(x/(\log x)^k)$ for every k. Thus for infinitely many primes r, $p + q = 2r$ is solvable, hence there are infinitely many triplets of primes in arithmetic progression. This proof no longer works for quadruplets, and I do not see how a proof could be obtained except through an estimation of $\gamma_k(n)$. If $\gamma_k(n) < \pi(n)$ could be proved, then the fact that the primes contain arbitrarily long arithmetic progressions would be deduced just from the fact that the primes are numerous and would not use any special properties of the primes. This method is sometimes successful, for example, I proved [41] in this way that to every k there is an n_k such that $n_k = p^2 - q^2$ has more than k solutions.

Denote by $f_k(n)$ the number of solutions of

$$\sum_{i=1}^{k} p_i^k = n.$$

I proved in [41] that $\limsup f_2(n) = \infty$; the proof used special properties of primes, but it could be modified so as to use only $\pi(n) > n/(\log n)^k$. I can also prove that $\limsup_{n=\infty} f_3(n) = \infty$ (unpublished), and the proof of this seems to need some special properties of the primes. I can prove nothing for $k > 3$.

Now I have to break my word given in the introduction, since I have to mention a conjecture of Hardy and Littlewood which is of importance in Waring's problem: Denote by $\psi_k(n)$ the number of solutions in positive integers of

$$\sum_{i=1}^{k} x_i^k = n.$$

The famous K-hypothesis of Hardy and Littlewood asserts that $\psi_k(n) = o(n^\epsilon)$ for every $\epsilon > 0$.

It is well known that this would imply $G(k) < ck$, in other words

every sufficiently large integer is the sum of at most ck positive integral kth powers (more precisely the K-hypothesis would imply $G(k) \leq 4k$ for all k, and $G(k) \leq 2k + 1$ if k is not a power of 2).

For $k = 2$ the K-hypothesis is well known to hold. For $k = 3$ Mahler [42] disproved the K-hypothesis; he showed by an identity that

$$\psi_3(n^{12}) > cn. \tag{59}$$

As far as I know $\overline{\lim}_{n=\infty} \psi_3(n)/\log n$ has not been determined. The K-hypothesis is probably wrong for $k > 3$ too but this has never been proved.

For the applications to Waring's problem it would suffice to show that for every $\epsilon > 0$:

$$\sum_{k=1}^{x} \psi_k(n)^2 = o(x^{1+\epsilon}). \tag{60}$$

(60) is probably true but this has never been proved.

Chowla, Pillai, and I [42] proved that for every k and infinitely many n

$$\psi_k(n) > \exp(c_k \log n/\log\log n). \tag{61}$$

(61) is of course not enough to disprove the K-hypothesis.

Let A be a sequence of integers of positive density. Denote by $\psi_k(A; n)$ the number of solutions of

$$\sum_{j=1}^{k} a_{i_j}{}^k = n.$$

I can prove (unpublished) that

$$\limsup \psi_k(A; n) = \infty. \tag{62}$$

More generally if c_1 and c_2 are given and $n > n_0(c_1, c_2)$, then if $a_1 < a_2 < \cdots < a_l$, where $l > c_1 n$, there always exists an m such that the number of solutions of

$$m = \sum_{j=1}^{k} a_{i_j}{}^k$$

is greater than c_2. The proof is similar to the proof of (61) but is considerably more tricky.

Turán and I conjectured that if $a_1 < a_2 < \cdots, a_k < ck^2$, is an infinite sequence of integers, then the number of solutions of $n = a_i + a_j$ cannot be bounded. I could only prove that the sums $a_i + a_j$ cannot all be different [43]. One would expect that $a_l < cl^k$ implies that the sums of the a's taken k at a time cannot all be different. Unfortunately the proof works only for even k, and though the result is undoubtedly true for odd k, I cannot prove it. The reason for this difficulty is very simple. For $k = 2$, if the sums $a_i + a_j$ are all distinct, then the differences $a_i - a_j$ are also all distinct. It is easy to see that $a_k < ck^2$ implies that the number of solutions $S(x)$ of $a_i - a_j \leq x$ satisfies $\overline{\lim} S(x)/x = \infty$, and therefore the differences $a_i - a_j$ cannot all be distinct. This argument breaks down for $k = 3$. For further problems and results on this subject I have to refer to my paper on unsolved problems [2a] and to the interesting review article by Stöhr [43].

Varnavides [40] proved using Roth's theorem that if $1 \leq a_1 < \cdots < a_l \leq n$, where $l > \alpha n$, $\alpha > 0$ fixed, n sufficiently large, then the a's contain more than $c_\alpha n^2$ arithmetic progressions of three terms. Except for the value of c_α this result is best possible since the total number of arithmetic progressions $0 < a < a + d < a + 2d \leq n$ is:

$$\binom{\left[\frac{n}{2}\right]}{2} + \binom{\left[\frac{n+1}{2}\right]}{2} = \frac{n^2}{4} + 0(n).$$

It would be interesting to determine the best value of c_α and to find the structure of the extremal sequence.

Many problems of combinatorial and numbertheoretical nature are discussed in my paper on unsolved problems [2a], and here I only wish to mention a few of them in which some progress has been made since I wrote the paper.

Denote by $a_1 < \cdots < a_k \leq x$ a sequence of integers for which all the sums $\sum_{i=1}^{k} \epsilon_i a_i$, $\epsilon_i = 0$ or 1, are distinct, and put

$$\max k = A(x).$$

Many years ago I asked whether

$$A(x) = \frac{\log x}{\log 2} + 0(1) \tag{64}$$

holds. (64) seems surprisingly resistant to any attack.

I also asked whether $A(2^k) \geq k + 2$ is possible. This was answered affirmatively a few years ago by Guy and Conway (independently). Their example is unpublished. Moser and I proved (see [2], *Colloque . . . Bruxelles*, 136–134) that

$$A(x) < \frac{\log x}{\log 2} + \frac{(1+\epsilon)\log\log x}{2\log 2},$$

and recently Moser showed (to appear in the report of the A.M.S. Pasadena Conference, 1963) that

$$\sum_{i=1}^{k} a_i^2 \geq \frac{4^k - 1}{3}, \tag{65}$$

with equality only for $a_i = 2^{i-1}$. Moser easily deduces from (65) that

$$A(x) < \frac{\log x}{\log 2} + \frac{\log\log x}{2\log 2} + O(1).$$

This is the best upper bound for $A(x)$ known up to the present. It is quite easy to see that if $a_1 < a_2 < \cdots$ is an infinite sequence of integers for which all the sums $\sum \epsilon_i a_i$, $\epsilon_i = 0$ or 1, are distinct then for infinitely many i, $a_i \leq 2^{i-1}$. Another somewhat related result states that if $A(x)$ denotes the number of solutions of $\sum_i \epsilon_i a_i \leq x$ and if $A(x) = x + O(1)$ then $a_i = 2^{i-1}$ for $i \geq i_0$. (This is proved in a paper, which will soon appear in *Acta Arithmetica*, by P. Erdös, B. Gordon, L. A. Rubel, and E. Straus.)

Lorenz [44] proved the following conjecture of Straus and myself: Let $a_1 < a_2 < \cdots$ be an infinite sequence of integers; then there always exists a sequence $b_1 < b_2 < \cdots$ of density 0 such that every integer n can be written in the form $a_i + b_j$. In particular he proved that if the a's are the primes then the b's can be chosen so that $B(x) < c(\log x)^3 \left(B(x) = \sum_{b_i \leq x} 1\right)$. By using probabilistic arguments [44] I improved this to $B(x) < c(\log x)^2$. The prime number theorem trivially implies $B(x) \geq (1 + o(1))\log x$ and I cannot disprove that $B(x) = (1 + o(1))\log x$. In 1956 Hanani stated the following conjecture: If $a_1 < \cdots$; $b_1 < \cdots$ are two infinite sequences such that every integer can be written in the form

$a_i + b_j$ then

$$\limsup A(x)B(x)/x > 1 \tag{66}$$

Special cases of (66) were proved by Narkiewicz [44]. Recently Danzer disproved (66) (Danzer's paper has just appeared in *J. für reine und angew. Math*). It easily follows from the result of Narkiewicz that to every $\epsilon > 0$ there is an infinite sequence $x_i \to \infty$ such that

$$A(x_i)B(x_i) - x_i > x_i^{1-\epsilon}. \tag{67}$$

The example of Danzer implies the existence of two sequences satisfying

$$x \leq A(x)B(x) \leq x + o(x). \tag{68}$$

There is a gap between (67) and (68) which as far as I know has not yet been filled. Danzer and I conjectured that (68), for two sequences such that every integer can be expressed as $a_i + b_j$, would imply that

$$A(x)B(x) - x \to \infty,$$

but as far as I know this has not yet been proved.

Lorenz's result implies that there exists a sequence $a_1 < a_2 \cdots$ satisfying $A(x) < cx \log\log x/\log x$ such that every integer is of the form $2^k + a_i$. One would expect that this can be improved to $cx/\log x$, but this seems to present unexpected difficulties.

Davenport and I [45] proved that if $a_1 < \cdots$ is an infinite sequence of positive lower density then there exists an infinite subsequence $a_{i_1}, a_{i_2} \cdots$ satisfying $a_{i_k} \mid a_{i_{k+1}}$. I conjectured that there are infinitely many triples a_i, a_j, a_l of distinct integers of the sequence satisfying $[a_i, a_j] = a_l$. This would follow from the following purely combinatorial theorem: Let $A_1, \ldots A_r$ be subsets of a set S of n elements and assume that there are no three distinct sets A_i, A_j, A_l for which

$$A_i \cup A_j = A_l.$$

Put $\max r = f(n)$. Then

$$f(n) = o(2^n). \tag{69}$$

Recently Sárközy and Szemerédi proved (69) (unpublished);

in fact they showed that $f(n) < c2^n/\log\log n$. Perhaps

$$f(n) < c2^n/\sqrt{n},$$

in fact perhaps $f(n) = (1 + o(1))\binom{n}{\left[\frac{n}{2}\right]}$. Thus the above conjecture about triples is now proved. A well-known combinatorial theorem of Sperner [46] should be mentioned here: If the A_i's are such that no one of them contains any other, then their number is at most $\binom{n}{\left[\frac{n}{2}\right]}$. This theorem has many applications in number theory and analysis.

Turán and I conjectured that if $a_1 < \cdots$ is an infinite sequence of integers, and if $F(n)$ denotes the number of solutions of $a_i + a_j \leq n$, then

$$F(n) = cn + O(1)$$

is impossible. Fuchs and I [47] proved that for $c > 0$

$$F(n) = cn + o\left(\frac{n^{1/4}}{(\log n)^{1/2}}\right) \tag{70}$$

is impossible. In the case $a_k = k^2$ Hardy and Landau [47] proved that

$$F(n) = \pi n + o(n \log n)^{1/4} \tag{71}$$

is impossible. This is the classical problem of the number of lattice points in a large circle. It has been conjectured that in (71) the error term is $o(n^{1/4+\epsilon})$, but this seems very deep. It is surprising that in our much more general case we obtain a lower bound for the error term which is nearly as good as (71) and our proof is very much simpler. Recently Jurkat proved that the error term in (70) cannot be $o(n^{1/4})$ (unpublished). Fuchs and I suspected a long time ago that a sequence $a_1 < \cdots$ can be constructed for which

$$F(n) = cn + O(n^{1/4}); \tag{72}$$

this would show that Jurkat's result is best possible, but we have not succeeded in constructing a sequence satisfying (72). Bateman, Kohlbecker, and Tull [47] generalized (70) by replacing c by a slowly oscillating function, but as far as I know the following simple

conjecture has not yet been proved: There does not exist a sequence $a_1 < a_2 \cdots$ for which the number of solutions of $a_i + a_j + a_s \leq x$ is of the form $cx + 0(1)$. My proof with Fuchs breaks down.

Heilbronn and I (our paper will appear in *Acta Arithmetica* [added in proof: 9 (1964), 149–159]) proved that if $a_1, \ldots, a_k$ are distinct residues (mod p), and $k > 3.6\sqrt{n}$, then every residue class (mod p) can be written in the form

$$\sum_{i=1}^{k} \epsilon_i a_i, \qquad \epsilon_i = 0 \text{ or } 1.$$

This result probably holds for $k > 2\sqrt{n}$. To show this it would be sufficient to show that if $a_1, \ldots, a_k$ are k distinct residues (mod p) then the number of distinct residues which can be written as the sum of at most r distinct a's is at least

$$\min (p, rk - r^2 + 1). \tag{73}$$

Taking the a's to be the residues $-\left[\frac{k-1}{2}\right], \ldots, +\left[\frac{k}{2}\right]$ we see that (73) if true is best possible. (73) is not even known for $r = 2$. A special case of a well-known theorem of Cauchy-Davenport [48] states that the number of distinct residues which can be written as the sum of r a's (not necessarily distinct) is at least

$$min\ (p, rk - r + 1).$$

Heilbronn and I further proved that if $k/p^{2/3} \to \infty$ then the number of solutions of

$$\sum_{i=1}^{k} \epsilon_i a_i = u (\text{mod } p), \qquad \epsilon_i = 0 \text{ or } 1$$

is $(1 + o(1))2^k/p$. The condition $k/p^{2/3} \to \infty$ is best possible, and $k > cp^{2/3}$ does not suffice.

We further conjectured that if $a_1, \ldots, a_k$ are distinct residues (mod n) and $k > cn^{1/2}$, then

$$\sum_{i=1}^{k} \epsilon_i a_i \equiv 0 (\text{mod } n), \qquad \epsilon_i = 0 \text{ or } 1 \tag{74}$$

is always solvable. Perhaps (74) is solvable for every $c > \sqrt{2}$

if $n > n_0(c)$. Flohr and I could only prove that (74) is solvable if

$$k > n^{\gamma+\epsilon}, \qquad \gamma = \frac{1}{1 + \log 2/\log 3};$$

our proof is unpublished.

A famous unsolved problem in number theory asks for the estimation of the least quadratic nonresidue of p. This problem goes back to Gauss who proved that the least quadratic nonresidue is $< 2p^{\frac{1}{2}} + 1$ if $p \equiv 1 (\mathrm{mod}\ 8)$; he used this estimation in his first proof of the law of quadratic reciprocity [49]. The first result which used the modern methods of analytic number theory is due to Vinogradov [49], who proved that the least quadratic nonresidue $n_2(p)$ satisfies

$$n_2(p) < cp^{\frac{1}{2}\sqrt{e}}(\log p)^2. \tag{75}$$

Davenport and I [49] improved the exponent of $\log p$ to $1/\sqrt{e}$. The first significant improvement on (75) was found by Burgess [49] who proved

$$n_2(p) < cp^{\frac{1}{4}\sqrt{e}}(\log p)^{\alpha}. \tag{76}$$

The ingenious proof of Burgess uses the following deep result of A. Weil [50]. Let $f(x)$ be an irreducible polynomial of degree n; then $\left(\left(\frac{f(x)}{p}\right)\right.$ is the Legendre symbol$\Big)$

$$\left|\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\right| < (n-1)\sqrt{p}. \tag{77}$$

André Weil used the methods of algebraic geometry in the proof of (74). For polynomials of degree 3 and 4, (77) was proved by Hasse [50] and weaker inequalities that (77) were proved by Davenport, Mordell, and others [50].

It seems certain that $n_2(p) < p^{\epsilon}$ and in fact perhaps $n_2(p) < c \log p$. Turán observed that $n_2(p) > c' \log p$.

Linnik [49] proved that there is a c_ϵ so that there are at most c_ϵ primes in $x < p < x^2$ which do not satisfy $n_2(p) < p^{\epsilon}$. Linnik developed his famous large sieve for the purpose of proving this result.

Davenport and I [49] observed the trivial result that there exists a constant $c > 0$ so that every interval of length $cp^{\frac{1}{2}}$ contains

both a residue and a nonresidue (mod p). We were not able to prove that this holds for every $c > 0$, but Burgess [49] proved the stronger result that every interval of length $p^{\frac{1}{4}+\epsilon}$ contains both a residue and a nonresidue. It seems probable that $p^{\frac{1}{4}+\epsilon}$ can be replaced by p^{ϵ} or even by $c \log p$.

I proved [51] that

$$\sum_{p<x} n_2(p) = (1 + o(1)) \frac{x}{\log x} \sum_{k=1}^{\infty} \frac{p_k}{2^k}. \tag{78}$$

Very likely, if $n_k(p)$ denotes the least kth power nonresidue of p, one has

$$\sum_{p<x} n_k(p) = c_k \frac{x}{\log x} + o\left(\frac{x}{\log x}\right), \tag{79}$$

but my knowledge of algebraic number theory was not sufficient to enable me to prove (79). The proof of (78) is surprisingly complicated; I needed to use the prime number theorem for airthmetic progressions, Brun's method, and the large sieve of Linnik and Rényi.

Denote by $f(\epsilon, p)$ the smallest integer such that, for every $l \geq f(\epsilon, p)$

$$\sum_{n=1}^{l} \left(\frac{n}{p}\right) < \epsilon l.$$

I expect that

$$\sum_{p<x} f(\epsilon, p) = (1 + o(1)) c_\epsilon \frac{x}{\log x}, \tag{80}$$

but I do not see how to attack (80).

Denote by $r(p)$ the least primitive root of p. Vinogradov proved $r(p) < p^{\frac{1}{2}+\epsilon}$; Hua, Shapiro, and I [52] improved this to

$$(\nu(p-1))^c p^{\frac{1}{2}}.$$

The first significant improvement on Vinogradoff's result is due to Burgess [52] who proved

$$r(p) < p^{\frac{1}{4}+\epsilon}.$$

Very likely $r(p) < c \log p$. Ankeny [52] deduced from the general-

ized Riemann Hypothesis that $n_2(p) < c(\log p)^2$, and obtained a weaker result for $r(p)$.

It seems very hard to prove that

$$\sum_{p<x} r(p) = (1 + o(1)) \frac{cx}{\log x},$$

in fact I cannot even show that $\lim r(p) < \infty$. Artin conjectured that there are infinitely many primes p for which 2 is a primitive root, in fact he made a plausible conjecture about their density. As far as I know it is not even known whether to every p there is a prime $q < p$ which is a primitive root of p.

In the last 35 years significant new results were obtained in the additive theory of prime numbers, also in Waring's problem, but I do not wish to speak much of these since several excellent books discussed them recently in great detail. I only wish to state the closest approaches known to the famous Goldbach conjecture: Selberg and Wang [53] proved, using Selberg's improvement of Brun's method, that every sufficiently large integer can be written in the form $a + b$ where a has at most 2 prime factors and b at most 3. Rényi proved [53] that there is an absolute constant c such that every integer is the sum of a prime and an integer which has at most c prime factors. Rényi used the large sieve of Linnik and Rényi and new results about the distribution of the roots of L-functions. I have been informed that recently Barban proved that every large integer can be written in the form $p + a$ where $\nu(a) \leq 4$. One of the main new ideas of Barban's proof is a remarkable improvement of the Linnik-Rényi large sieve.

Another remarkable recent result is due to Linnik [31]. He proved by his dispersion method the following conjecture of Hardy and Littlewood: The number of solutions of $n = p + u^2 + v^2$ is of the form

$$(1 + o(1))c_n \frac{n}{\log n}, \qquad c_n > \frac{c}{\log \log n}$$

where c_n is a complicated constant which depends only on n. He also obtains asymptotic formuls for sums of the form $\left(d_k(m) = \sum_{x_1 \cdots x_k = m} 1\right)$

$$\sum_{m \leq n} d_{k_1}(m)\, d_{k_2}(m + a)$$

and

$$\sum_{m \leq n} d_{k_1}(m)\, d_{k_2}(n-m)$$

for $k_1 = 2$ and k_2 arbitrary. For the details and the history of this problem I have to refer to Linnik's book.

Many of the results mentioned in this chapter can be proved by Brun's method, which is perhaps our most powerful elementary tool in number theory. Recently Selberg [12] obtained a significant improvement of Brun's method and in a certain sense showed that further improvement is impossible beyond a certain limit. As far as I know the following question has not yet been investigated. Determine or estimate the smallest $f_1(x)$ with the following property: there exists a set of residue classes $a_i (\mathrm{mod}\ p_i)$, for $p_i < f_1(x)$, such that every $1 \leq u \leq x$ satisfies at least one of the congruences $u \equiv a_i (\mathrm{mod}\ p_i)$. Similarly for $f_2(x)$, defined as follows: there is a set of residue classes $a_i (\mathrm{mod}\ p_i)$, $p_i < f_2(x)$ so that the number of integers $u \leq x$ which do not satisfy any of the congruences $u \equiv a_i (\mathrm{mod}\ p_i)$ is $o(x/\log x)$.

Here I would like to call attention to another problem on sieve methods which as far as I know has not yet been investigated. The essential result proved by Viggo Brun was the following. Let $p < n^{\epsilon}$, $\epsilon = \epsilon(k)$ and consider $k_p \leq k$ congruences:

$$x \equiv a_j^{(p)} \ (\mathrm{mod}\ p), \qquad 1 \leq j \leq k_p \leq k. \tag{81}$$

Then the number of integers $x \leq n$ which do not satisfy any of the congruences (81) is between

$$c_1 n \prod_{p<n^{\epsilon}} \left(1 - \frac{k_p}{p}\right) \quad \text{and} \quad c_2 n \prod_{p<n^{\epsilon}} \left(1 - \frac{k_p}{p}\right). \tag{82}$$

(82) was improved by Selberg [12] in two ways; he permitted a larger choice of $\epsilon = \epsilon(k)$, and he brought c_1 and c_2 closer together.

Linnik and Rényi investigated the other extreme; in their case the number of congruences (81) is very large, and roughly speaking they prove that if "many" integers are given up to x then, with the exception of a few primes, each residue class mod p contains "nearly" the same number of integers if we neglect a "few" exceptional residue classes. For a precise statement I have to refer to the papers of Rényi and Linnik [53].

As far as I know nobody investigated what happens if in (81) the

number of congruences increases with p but not very quickly, say like $\log p$ or like $\log \log p$. I have not been able to find a reasonable application for the estimation which would correspond to (82) and this may be the reason why this question was neglected.

Now I would like to call attention to another group of problems on congruences. A set of congruences:

$$(83) \qquad a_i \pmod{n_i}, \qquad n_1 < n_2 < \cdots < n_k$$

is called a covering set if every integer satisfies at least one of the congruences (83). The simplest covering set is $0 \pmod 2$, $0 \pmod 3$, $1 \pmod 4$, $5 \pmod 6$, $7 \pmod{12}$. I asked if for every choice of n_1 there is a covering set (83). This problem seems very difficult and has been solved only for $n_1 \leq 8$ (by Selfridge and others). Many similar questions can be asked, for example, it is not known if there exists a covering set with all the n_i odd. A simple but not quite trivial result about covering sets of congruences states that $\sum_{i=1}^{k} \frac{1}{n_i} > 1$ [54].

Two congruences are called disjoint if no integer satisfies both of them. Stein and I asked: let (83) be a system of pairwise disjoint congruences for which $n_k \leq x$. Put $\max k = f(x)$. We conjectured that $f(x) = o(x)$. We proved that for every $\epsilon > 0$ and $x > x_0(\epsilon)$

$$f(x) > x \exp\left(-(\log x)^{\frac{1}{2}-\epsilon}\right).$$

It is surprising that the proof of $f(x) = o(x)$ presents difficulties and this perhaps due to our overlooking an obvious idea [54].

Stein conjectured that if (83) is a disjoint system then there always exists a $0 < u \leq 2^k$ for which $u \not\equiv a_i \pmod{n_i}$, $(i = 1, 2, \ldots, k)$. This conjecture was recently proved by Selfridge (unpublished). The system

$$2^{i-1} \pmod{2^i}, \qquad 1 \leq i \leq k$$

shows that this conjecture is best possible.

I conjectured that if $a_i \pmod{n_i}$, $1 \leq i \leq k$ is any system of congruences such that there is a u for which $u \not\equiv a_i \pmod{n_i}$ $(i = 1, \ldots, k)$, then there is such a u for which $0 < u \leq 2^k$. I could only prove that there is such a u for which $0 < u < f(k)$ where $f(k)$

depends only on k, but I did no give an explicit estimation for $f(k)$ [54].

Recently Elliott (in publication in *Quart. J. of Math.*) proved that if $a_1 < a_2 < \cdots < a_k < n$ and $k > cn/(\log n)$, where $c > 2$, then there exists a prime q such that every residue class (mod q) is represented among the a_i. He uses Selberg's sieve.

8. I now refer briefly to a body of recent work on Diophantine equations and Diophantine inequalities in many variables. We consider equations first.

The treatment of equations of additive type, such as

$$f(x_1) + \cdots f(x_n) = N$$

where $f(x)$ is an integer-valued polynomial, is possible by the Hardy-Littlewood method, and presents no essentially new difficulty. In particular a homogeneous additive equation:

$$a_1 x_1^k + \cdots + a_n x_n^k = 0$$

always has an infinity of solutions, provided n is greater than a suitable function of k, and provided $a_1, \ldots, a_n$ are not all of the same sign if k is even.

The general homogeneous equation

$$f(x_1, \ldots, x_n) = 0$$

of degree k, offers much more difficulty. The first method of reducing such an equation to additive equations (in a smaller number of variables) was given by Richard Brauer in 1945. This method was not directly applicable in the rational number field, because it required the solubility of all additive equations of every degree $k' \leq k$, and this cannot be ensured for even values of k'. But Lewis (1957) modified Brauer's method to obtain a proof that when $k = 3$ the equation is always soluble if n is sufficiently large. Birch (1957) generalized Brauer's method to prove the following remarkable theorem: every system of simultaneous equations, of odd degrees $k_1, \ldots, k_r$, is soluble in integers (not all 0) provided n is greater than a certain function of $k_1, \ldots, k_r$.

Davenport (1959 and 1963) attacked the problem of a single homogeneous cubic equation directly by the Hardy-Littlewood method, and proved that the condition $n \geq 16$ is sufficient to ensure solubility. It is conjectured that $n \geq 10$ suffices and it is known

that this would be best possible. A treatment on similar general lines of homogeneous equations of higher degree, and simultaneous systems of such equations, was given by Birch (1962), but here it becomes necessary (and it is indeed essential) to impose further conditions.

A connected account of much of this work, with references, is available in Davenport's notes: *Analytic Methods for Diophantine Equations and Diophantine Inequalities* (Ann Arbor Publishers, 1963).

There is a close connection between these problems and the problem of the solubility of homogeneous equations in p-adic numbers. In several recent papers, Birch and Lewis have established, for particular values of k, the conjecture of Artin that for such equations the condition $n > k^2$ is sufficient to ensure solubility.

As regard Diophantine inequalities, the principal result of a general character proved so far is the following: if $Q(x_1, \ldots, x_n)$ is any indefinite quadratic form with real coefficients, then the inequality

$$|Q(x_1, \ldots, x_n)| < \epsilon$$

is soluble for every $\epsilon > 0$ provided $n \geq 21$. (For references see Davenport's notes, mentioned above.) The proof is complicated. It is conjectured that $n \geq 5$ suffices, and it may even be true that $n \geq 3$ would suffice if one excluded forms which are proportional to forms with integral coefficients. A similar result (but with a very large lower bound for n) can probably be proved for cubic forms, but further extension seems to present great difficulties.

REFERENCES

1. I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, translated from the Russian by K. F. Roth and Ann Davenport, New York (1954) Interscience Publishers.

L. K. Hua, *Additive Primzahltheorie*, Leipzig (1959) Teubner. For the older results see the excellent book of E. Landau, *Vorlesungen über Zahlentheorie*, vols. 1–3; Leipzig (1927).

Hardy and Wright, *Introduction to the theory of numbers*, Oxford, Clarendon Press.

L. K. Hua, Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie, *Enz. Math. Wiss.*, Band I 2 Heft 13 Teil I (1959).

For the most modern results on prime number theory, see K. Prachar, *Primzahlverteilung*, Berlin (1957) Springer.

2. M. Kac, Probability methods in some problems of analysis and number theory, *Bull. Amer. Math. Soc.*, **55** (1949) 641–665.
Kubilius, Probabilistic methods in the theory of numbers (Russian), *Uspehi Matem. Nauk*, **11** (1956) 31–66. See also Probabilistic methods in the theory of numbers, *Transl. Math. Monog.* **11** (1964) Amer. Math. Soc.
P. Erdös, On additive arithmetical functions and applications of probability to number theory, *Proc. Int. Congress of Math. Amsterdam*, **3** (1954) 13–19.
P. Erdös, On the distribution function of additive arithmetical functions and on some related problems, *Rend. Sem. Math. Fis. Milano*, **27** (1958) 3–7.
E. V. Novoselov, A new method in probabilistic number theory, *Izv. Akad. Nauk U.S.S.R.*, **28** (1964) 307–364.
See also a forthcoming review article by me in the *London Math. Soc. Journal*, On applications of probability methods to number theory. For applications of probability methods to additive number theory see, for example, A. Rényi, Probabilistic methods in number theory, *Proc. I.C.M. Edinburgh* (1958) 529–539.
P. Erdös, Problems and results in additive number theory, *Colloque sur la théorie des nombres*, 127–137, Bruxelles (1955); P. Erdös and A. Rényi, Additive properties of random sequences of positive integers, *Acta Arithmetica*, **6** (1960) 83–110; see also a forthcoming book on sequences of integers by K. F. Roth and H. Halberstam.

2a. P. Erdös, On unsolved problems, *Publ. Math. Inst. Hung. Acad.*, **6** (1961) 221–254.

3. A. Selberg, An elementary proof of the prime number theorem, *Annals of Math.*, **50** (1949) 305–313.
P. Erdös, On a new method in elementary number theory which leads to an elementary proof of the prime number theorem, *Proc. Nat. Acad. Sci. U.S.A.*, **35** (1949) 379–384.
P. Erdös, On a Tauberian theorem connected with the new proof of the prime number theorem, *Journ. Ind. Math. Soc.*, **13** (1949) 133–147.
H. N. Shapiro, Tauberian theorems and elementary prime number theory, *Comm. Pure Appl. Math.*, **12** (1959) 579–610.

4. A. Beurling, Analyse asymptotique de la distribution des nombres premiers generalisés, *Acta Math.*, **68** (1937) 255–299.
B. Nyman, A general prime number theorem, *ibid.* **81** (1949), 299–307.
P. Malliavin, Sur la reste de la loi asympotique de répartition des nombres premiers généralisés de Beurling, *ibid.* **106** (1961) 281–298.

5. E. Bombieri, Sulle formule di A. Selberg generalizzate per classi di funzioni aritmetiche e le applicazioni al problema del resto nel Primzahlsatz, *Riv Mat. Univ. Parma Ser II*, **3** (1962), 393–440. This paper has a very good bibliography of the literature of the elementary proofs of the prime number theorem and their generalizations.
E. Wirsing, Elementare Beweise des Primzahlsatzes mit Restglied I, *J. reine und angew. Math.*, **211** (1962), 205–214; and **214–215** (1964), 1–18.

6. T. V. Nevanlinna, Über den Elementaren Beweis des Primzahlsatzes, *Soc. Sci. Fenn. Comment. Phys. Math. 27*, **3** (1962); and Über die elementaren

Beweise der Primzahlsätze und deren aequivalente Fassungen, *Ann. Acad. Sci. Fennicae Ser. A. I. Math*, **343** (1964).

7. A. E. Ingham, Some Tauberian theorems connected with the prime number theorem, *J. London Math. Soc.*, **20** (1945) 171–180.
8. N. M. Korobov, Weyl's sums estimates and the distribution of primes, *Doklady Akad. Nauk. U.S.S.R.*, **123** (1959) 28–31; I. M. Vinogradov, *Akad. Nauk. U.S.S.R. Ser Mat.*, **22** (1958) 161–164.
9. W. Haneke, Verschärfung der Abschätzung von $\xi(\frac{1}{2} + it)$, *Acta Arith.* **8** (1962/63), 357-430.
10. H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, *Acta Arith.*, **2** (1936) 23–46.
11. P. Erdös, On the difference of consecutive primes, *Quart. J. Math. Oxford*, **6**, 124–128.
    T. H. Chang, Über aufeinanderfolgende Zahlen von denen jede mindestens einer von n linearen Kongruenzen genügt, deren Moduln die ersten n Primzahlen sind, *Schriften Math. Sem. und Inst. Angew. Math. Univ. Berlin*, **4** (1938) 35–55.
    R. A. Rankin, The difference between consecutive prime numbers, *J. London Math. Soc.*, **13** (1938) 242–247.
    A. Schönhage, Eine Bemerkung zur Konstruktion grosser Primzahllücken, *Arch. Math.*, **14** (1963) 29–30.
    R. A. Rankin, The difference between consecutive prime numbers V, *Proc. Edinburgh Math. Soc.*, **13** (1963) 331–332.
12. G. H. Hardy and J. E. Littlewood, Some problems of partitio numerorum III, *Acta Math.*, **44** (1923) 1–70.
    A. Selberg, On elementary methods in prime number theory and their limitations, *Den 11-te Skand. Mat. Kongress* (1952) 13–22; see also The general sieve method and its place in prime number theory, *Proc. Int. Congr. Math. Harvard*, **1** (1950) 286–292.
13. G. Ricci, Recherches sur l'allure de la suite $(p_{n+1} - p_n)/\log p_n$, *Colloque sur la théorie des nombres, Bruxelles* (1955) 93–96; Sull, andamento della differenza di numeri primi consecutivi, *Riv. Math. Univ. Parma*, **5** (1954) 3–54.
14. P. Erdös, The difference of consecutive prime numbers, *Duke Math. J.*, **6** (1940) 438–441.
    R. A. Rankin, The difference between consecutive prime numbers, II, III, IV, *Proc. Cambridge Phil. Soc.*, **36** (1940) 255–266; *J. London Math. Soc.*, **22** (1947) 226–230; *Proc. Amer. Math. Soc.*, **1** (1950) 143–150.
15. P. Erdös and P. Turán, On some new questions in the distribution of prime numbers, *Bull. Amer. Math. Soc.*, **54** (1948) 271–278.
    P. Erdös and A. Rényi, Some problems and results on consecutive primes, *Simon Stevin* (1949) 115–126.
    K. Blarner, Zur Abschätzung von Reihen deren Glieder von rationalen Funktionen einer festen Anzahl sukzessiver Primzahlen gebildet werden, *Monatshefe für Math.*, **68** (1964) 1–16.
    W. Schwarz, Weitere mit einer Methode von Erdös-Prachar erzielte Ergebnisse, *ibid.* 75–80.

16. W. Sierpinski, Remarque sur la répartition des nombres premiers, *Colloquium Math.*, **1** (1948) 193–194.
A. Walfisz, Isolierte Primzahlen, *Doklady Akad. Nauk. U.S.S.R.*, **90** (1953) 711–713.
K. Prachar, Über ein Resultat von A. Walfisz, *Monatshefte Math.*, **58** (1954) 114–116.
P. Erdös, On some applications of Brun's method, *Acta Szeged*, **13** (1949) 57–63.
17. P. Erdös and K. Prachar, Sätze und Probleme über p_k/k, *tbh. Math. Sem. Univ. Hamburg*, **25** (1962) 51–56.
18. P. Erdös, Problems and results on the differences of consecutive primes, *Publ. Math. Debrecen* **1** (1949) 33–37.
19. P. Erdös, On the difference of consecutive primes, *Bull. Amer. Math. Soc.*, **54** (1948) 885–889.
20. P. Erdös, Some problems and results in elementary number theory, *Publ. Math. Debrecen*, **2** (1951) 103–109.
H. E. Richert, On the difference between consecutive squarefree numbers, *J. London Math. Soc.*, **29** (1954) 16–20. [*Added in proof:* It was pointed out to me that Richert's result was improved by Rankin (*Quart. J. Math., Ser.* 2, **6** (1955) 147–153) who replaced the exponent $\frac{2}{3}$ by 0.22198215. The best result to date is due to P. G. Schmidt who in his dissertation (Göttingen, 1964) obtained the exponent $\frac{10955}{49419} = 0.22158534$.]
C. Hooley, On the difference of consecutive numbers prime to n, *Acta Arith.*, **8** (1963) 343–347.
21. P. Erdös, On the integers relatively prime to n and on a number theoretic function considered by Jacobsthal, *Math. Scand.*, **10** (1962) 163–170.
22. A. Selberg, An elementary proof of Dirichlet's theorem about primes in an arithmetic progression, *Ann. of Math.*, **50** (1949) 297–307.
A. Selberg, An elementary proof of the prime number theorem for arithmetic progressions, *Canadian J. Math.*, **2** (1950) 66–78.
H. N. Shapiro, On primes in arithmetic progressions I, *Ann. of Math.* (2) (52) (1950) 217–230; II ibid. (2) (52) (1950) 231–243.
W. E. Briggs, An elementary proof of a theorem about the representation of primes by quadratic forms, *Canadian J. Math.* **6** (1954) 353–363.
H. N. Shapiro, An elementary proof of the prime ideal theorem, *Comm. Pure Appl. Math.*, **2** (1949) 309–323.
W. Forman and H. N. Shapiro, Abstract prime number theorem, *ibid.* **7** (1954) 587–619.
23. For an easily accessible exposition of the work of Linnik and Rodosskij, see K. Prachar's book *Primzahlverteilung*, Berlin (1957) Springer.
P. Turán, On a density theorem of Ju. V. Linnik, *Publ. Math. Inst. Hung. Acad.*, **6** (1961) 165–178.
S. Knapowski, On Linnik's theorem concerning exceptional L-zeros, *Publ. Math. Debrecen*, **9** (1962) 168–178.
24. P. Turán, Über die Primzahlen der arithmetischen Progression, *Acta Szeged*, **8** (1937) 226–235.
P. Erdös, On some applications of Brun's method, *ibid.* **13** (1949) 57–63.

I. M. Vinogradov, Über die Abschätzung trigonometrischer Summen mit Primzahlen, *Izv. Akad. Nauk, U.S.S.R. Ser. Mat,* **12** (1948) 225–248.

25. S. Knapowski and P. Turán, Comparative prime-number theory I–VIII, *Acta Math. Hung.* **XIII** (1962), **XIV** (1963) and also forthcoming papers in *Acta Arithmetica.* A first exposition of the methods in question can be found in Turán's book *Eine neue Methode in der Analysis und deren Anwendungen;* a completely rewritten English edition will be published in the Interscience Tracts series. For the older literature, see the papers of Turán and Knapowski and the book of Turán.
26. S. Knapowski, On sign-changes in the remainder-term in the prime number formula, *J. London Math. Soc.,* **36** (1961) 451–460.
27. F. V. Atkinson, On sums of powers of complex numbers, *Acta Hung. Acad.,* **12** (1961) 185–188.
28. W. E. Briggs, Prime-like sequences generated by a sieve process, *Duke Math. J.,* **30** (1963) 297–311. This paper contains the sharpest results known up to the present and has references to the previous literature.
29. D. Hawkins, The random sieve, *Math. Mag.,* **31** (1957–1958) 1–3.
30. P. Erdös, On a problem of S. Golomb, *J. Australian Math. Soc.,* **2** (1961) 1–8.
31. P. Turán, Uber einige Verallgemeinungen eines Satzes von Hardy und Ramanujan, *J. London Mat. Soc.,* **11** (1936) 125–133.
    S. Ramanujan, *Collected papers,* 262–275.
    H. Halberstam, On the distribution of additive number-theoretic function, II and III, *J. London Math. Soc.,* **31** (1956) 1–11, 14–31.
    P. Erdös, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's function, *Quart. J. Math. Oxford,* **6** (1935) 205–213.
    E. C. Titchmarsh, On a divisor problem, *Rend. Circ. Mat. Palermo,* **54** (1930) 414–419.
    C. B. Haselgrove, Some theorems in the analytic theory of numbers, *J. London Math. Soc.,* **26** (1951) 273–277.
    Yu. V. Linnik, The dispersion method in binary additive problems, *Trans. Math. Monog.* **4** (1963) Amer. Math. Soc.
32. J. G. van der Corput, Une inégalité rélative au nombre des diviseurs, *Proc. Neder. Akad. Wet. Amsterdam,* **42** (1939) 547–553.
    P. Erdös, On the sum $\sum_{k=1}^{n} d(f(k))$, *J. London Math. Soc.,* **27** (1952) 7–15.
    R. Bellman, Ramanujan sums and the average value of arithmetic functions, *Duke Math. J.,* **17** (1950) 159–168.
    C. Hooley, On the number of divisors of quadratic polynomials, *Acta Math.,* **110** (1963) 97–114.
33. P. Erdös, On the greatest prime factor of $\prod_{k=1}^{x} f(k)$, *J. London Math. Soc.,* **27** (1952) 379–384. The references to the older literature can be found in this paper.
    P. Erdös and R. Rado, Intersections theorems for systems of sets, *J. London Math. Soc.,* **35** (1960) 85–90.

34. A. Schinzel, On primitive prime factors of $a^n - b^n$, *Proc. Cambridge Phil. Soc.*, **58** (1962) 555–562.
G. Pólya, Zur arithmetischen Untersuchung der Polynome, *Math. Zeitschrift*, **1** (1918) 143–148.
C. Siegel, Über Näheringswerte algebrascher Zahlen, *Math. Annalen*, **84** (1921) 80–99; see also K. Mahler, *Math. Annalen*, **107** (1933) 691–730.
S. Chowla, The greatest prime factor of $x^2 + 1$, *J. London Math. Soc.*, **10** (1935) 117–120.
K. Mahler, Über den grössten Primteiler der Polynome $x^2 \pm 1$, *Arch. Math. og Naturvid.*, **41** (1935) 1–8.
35. I. I. Pjatezkij-Schapiro, On the distribution of primes in the sequences of the form $[f(n)]$, *Mat. Sbornik*, **33** (1953) 559–566.
36. H. Heilbronn, Über die Verteilung der Primzahlen in Polynomen, *Math. Ann.*, **104** (1931) 794–799.
37. P. Erdös, Arithmetical properties of polynomials, *J. London Math. Soc.*, **28** (1953) 416–425.
38. B. L. van der Waerden, Beweis einer Baudetschen Vermutung, *Nieuw Archiefvoor Wiskunde*, (2) **15** (1928), 212–216.
P. Erdös and R. Rado, Combinatorial theorems on classifications of subsets of a given set, *Proc. London Math. Soc.*, **2** (1952) 438–439.
W. Schmidt, Two combinatorial theorems on arithmetic progressions, *Duke Math. J.*, **29** (1962) 129–140.
P. Erdös, On some combinatorial problems connected with the theorems of Ramsey and Van der Waerden (in Hungarian), *Mat. Lapok*, **14** (1963) 29–37.
R. Rado, Studien zur Kombinatorik, *Math. Zeitsch.*, **36** (1933) 424–480; see also Khintchine's delightful book *Three pearls of number theory*, English translation (Graylock) (1952).
N. G. Tchudakoff, Theory of the characters of number semigroups, Report Internat. Coll on Zeta Function, Bombay (1956), also *J. Indian Math. Soc.* **20** (1956) 11–17.
39. A. Brauer, Über sequenzen von Potenzresten I and II, *Sitzungsber. Preuss. Akad. Wiss. Phys.-Math. kl.* **19** (1931) 329–341.
40. P. Erdös and P. Turán, On some sequences of integers, *J. London Math. Soc.*, **11** (1936) 261–264.
F. Behrend, On sequences of integers containing no arithmetic progression, *Cas. Mat. fys.*, **67** (1938) 235–238.
R. Salem and D. C. Spencer, On sets of integers which contain no three terms in an arithmetic progression, *Proc. Nat. Acad. Sci. U.S.A.*, **28** (1942) 561–563.
F. Behrend, On sets of integers which contain no three terms in an arithmetical progression, *ibid.* **32** (1946) 331–332.
R. A. Rankin, Sets of integers containing not more than a given number of terms in arithmetical progression, *Proc. Royal Soc. Edinburgh A*, **65** (1960–1961) 332–344.
K. F. Roth, On certain sets of integers, *J. London Math. Soc.*, **28** (1953) 104–109.
P. Varnavides, On certain sets of positive density, *J. London Math. Soc.*, **341** (1959) 358–360.

L. Chowla, There exists an infinity of 3-combinations of primes in A, *P. Proc. Lahore Philos. Soc.* **6**, No. 2 (1944) 15–16.
See also J. G. van der Corput, Über Summen von Primzahlen und Primzahlquadraten, *Math. Ann.* **113** (1939) 1–50.

41. P. Erdös, On the sum and difference of squares of primes, I and II, *J. London Math. Soc.*, **12** (1937) 133–136, 168–171.
42. P. Erdös, On the representation of an integer as the sum of k kth powers, *J. London Math. Soc.*, **11** (1936) 133–136.
S. Chowla and S. S. Pillai, The number of representations of a number as a sum of non-negative nth powers, *Quart. J. Math. Oxford*, **7** (1936) 56–59.
K. Mahler, Note on hypothesis K of Hardy and Littlewood, *J. London Math. Soc.*, **11** (1936) 136–138.
43. A. Stöhr, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe, I and II, *J. reine u. angew. Math.*, **194** (1955) 40–65, 111–140. Many interesting unsolved problems can be found in this paper. For a review of additive number theory, see H. H. Ostmann, *Additive Zahlentheorie, Ergeb. der Math.*, Heft 7 and 11.
44. G. G. Lorenz, On a problem of additive number theory, *Proc. Am. Math. Soc.*, **5** (1954) 838–841.
P. Erdös, Some results on additive number theory, *ibid.* 847–853.
W. Narkiewicz, Remarks on a conjecture of Hanani in number theory, *Coll. Math.*, **7** (1960) 161–165.
45. P. Erdös and H. Davenport, On sequences of positive integers, *Acta Arithmetica*, **2** (1936) 147–151; and *J. Indian Math. Soc.*, **15** (1951) 19–24.
46. A. Sperner, Ein Satz über Untermengen einer endlichen Menge, *Math. Zeitsch.*, **27** (1928) 544–548.
47. P. Erdös and W. H. J. Fuchs, On a problem of additive number theory, *J. London Math. Soc.*, **31** (1956) 67–73.
P. T. Bateman, E. E. Kohlbeiker, and J. P. Tull, In a theorem of Erdös and Fuchs in additive number theory, *Proc. Amer. Math. Soc.* **14** (1963) 278–284.
48. H. Davenport, On the addition of residue classes, *J. London Math. Soc.*, **10** (1935) 30–32; A historical note, *ibid.* **22** (1947) 100–101.
49. C. F. Gauss, *Disquisitiones arithmeticae*, art. 125 and 129; see also Dirichlet-Dedekind, *Vorlesungen über Zahlentheorie*, 4th edition (1894), p. 116.
A. Brauer, Über den kleinsten quadratischen Nichtrest, *Math. Zeitsch.*, **33** (1931) 162–176.
J. M. Vinogradoff, On the bound of the least non-residue of kth powers, *Trans. Amer. Math. Soc.*, **29** (1927) 218–226; see also *Journal of the Physico-Mathematical Soc. of Perm.* (1919).
H. Davenport and P. Erdös, The distribution of quadratic and higher residues, *Publ. Math. Debrecen*, **2** (1952) 252–265.
D. A. Burgess, The distribution of quadratic residues and nonresidues, *Mathematika*, **4** (1957) 106–112.
Yu. V. Linnik, A remark on the least quadratic non-residue, *Doklady Acad. Sci. U.S.S.R.* (*N.S.*), **36** (1942) 119–120.
50. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Math. Sci. No.* 1041, Paris 1945.

H. Hasse, Theorie der relativ-zyklischen algebraischen Funktionenkörper inbesondere bei endlichem Konstantenkörper, *J. reine u. angew. Math.*, **172** (1935) 37–59.
H. Davenport, On character sums in finite fields, *Acta Math.*, **71** (1939) 99–121.

51. P. Erdös, Remarks on number theory I, *Mat. Lapok*, **12** (1961) 10–17.
52. P. Erdös and H. N. Shapiro, On the least primitive root of a prime, *Pacific J. of Math.*, **7** (1957) 861–865.
N. C. Ankeny, The least quadratic non-residue, *Annals of Math.*, **55** (1952) 65–71.
D. A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc.*, (3) **12** (1962) 179–192.
Wang Yuan, A note on the least primitive root of a prime, *Science Record, New Ser.*, **3** (1959) 174–207.
53. Wang Yuan, On sieve methods and some of their applications, *Scientia Sinica*, **8** (1959) 357–381.
A. Rényi, On the large sieve of Yu. V. Linnik, *Comp. Mat.*, **8** (1950) 68–75; see also On the probabilistic generalisation of the large sieve of Linnik, *Publ. Math. Inst. Hung. Acad.*, **3** (1958) 199–206.
54. P. Erdös, On a problem of systems of congruences (in Hungarian), *Mat. Lapok*, **3** (1952) 122–128.
S. K. Stein, Unions of arithmetic sequences, *Math. Annalen*, **134** (1957) 289–294.
P. Erdös, External problems in number theory (in Hungarian), *Mat. Lapok*, **13** (1962) 228–255; see also my forthcoming paper in the report of the A.M.S. Pasadena conference (1963). For problems and conjectures on prime numbers, see A. Schinzel and W. Sierpinski, Sur certaines hypothèses concernant les nombres premiers, *Acta Arithmetica*, **4** (1958) 185–207. Several unsolved problems are stated in a recent paper of Sierpinski, On some unsolved problems of arithmetics, *Scripta Math.*, **25** (1960) 125–136; see also P. Erdös, *Quelques problèmes de la théorie des nombres, Monographies de l' Enseignement Math.*, No. 6 (1963), 81–135.