1. Problems and Results in Number Theory

P. ERDÖS

Mathematical Institute, Hungarian Academy of Sciences, Reáltanoda-u. 13–15, H-1053, Budapest, Hungary

I will mainly discuss somewhat unconventional problems on sieves, primes and congruences. First some questions on sieves. Let $B_k(x)$ (B for Brun) be the smallest integer so that we can assign k residues $a_i^{(p)}$, $i = 1, \ldots, k$, mod p for every p, $k < p < B_k(x)$ so that every integer $n < x$ should satisfy at least one of the congruences

$$n \equiv a_i^{(p)} (\mathrm{mod}\ p).$$

This problem is of course not new, it goes back at least to Brun, but I am not sure if and when it has been formulated explicitly. For references see the well-known, recent book of Halberstam–Richert, *Sieve Methods*. As far as I know the sharpest current results are

$$\frac{c_1 x^{\frac{1}{2}}}{\log x} < B_1(x) < \frac{c_2 x (\log\log x)^2}{\log x \log\log\log x}. \tag{1}$$

The lower bound is due to Iwaniec and the upper bound to Rankin. Rankin's result immediately gives that for infinitely many k

$$p_{k+1} - p_k > c \frac{\log k \log\log k \log\log\log\log k}{(\log\log\log k)^2}. \tag{2}$$

Inequality (2) was proved more than 40 years ago and the only improvement since then was to increase the value of c. Clearly any improvement of the upper and lower bounds in (1) and (2) would be of great importance in

the theory of the distribution of primes. I offer 10 000 dollars for a proof that (2) holds for every c and infinitely many k. This will probably require a new idea since (2) seems to be the natural boundary of the method used there. I refer to the book of Halberstam and Richert for the results on $B_k(x)$ for $k>1$. The case $k=1$ connects up with an interesting problem of Jacobstahl. Let $1=a_1<\cdots<a_{\varphi(n)}=n-1$ be the sequence of integers relatively prime to n. Put

$$g(n)=\max(a_{k+1}-a_k), \qquad G(n)=\max_{1\leqslant m\leqslant n} g(m).$$

Rankin's result (2) implies that

$$G(n)>\frac{c\log n\log\log n\log\log\log\log n}{(\log\log\log n)^2} \tag{2'}$$

and Jacobstahl conjectured

$$G(n)<c\left(\frac{\log n}{\log\log n}\right)^2.$$

It is perhaps more illuminating to put

$$\max g(n)=C(r)$$

where the maximum is taken over all integers n which have r distinct prime factors. Jacobstahl conjectured

$$C(r)<c_2r^2, \tag{3}$$

and he further conjectured that $C(r)$ is assumed if n is the product of the first r primes. Perhaps the true order of magnitude of $C(r)$ is $r(\log r)^c$.

It is easy to see that for every n ($\nu(n)$ denotes the number of distinct prime factors of a)

$$g(n)\geqslant(1+o(1))\nu(n)\prod_{p/n}\left(1-\frac{1}{p}\right)^{-1}. \tag{2''}$$

I often tried to find two integers $m_1<m_2\leqslant n$, $(m_1,m_2)=1$ for which

$$\min(g(m_1),g(m_2))>\log n.$$

I was not successful; perhaps $g(m)$ can be abnormally large, i.e. larger than the bound given by (2'') only if m is divisible by all (or most) of the small primes. The strongest form of this conjecture would state: Let $m_1<m_2\leqslant n$, $(m_1,m_2)=1$. Then

$$\min(g(m_1),g(m_2))<c\frac{\log n}{\log\log n}(\log\log\log n)^{\frac{1}{2}}. \tag{2'''}$$

The conjecture (2‴) may very well go too far. I hope to be able to investigate these questions, but I am not very optimistic of success.

I now state one of my favorite old conjectures:

$$\sum_{k=1}^{\varphi(n)} (a_{k+1}-a_k)^2 < C\frac{n^2}{\varphi(n)}. \tag{4}$$

It is surprising that (4) is probably really difficult—I offer 500 dollars for a proof or disproof. Hooley has several results which indicate that (4) is probably true. In particular Hooley proved (4) if 2 is replaced by an exponent less than 2. It seems certain that for every n

$$\sum_{k=1}^{\varphi(n)} (a_{k+1}-a_k)^r < C_r\frac{n^r}{\varphi(n)^{r-1}}. \tag{4'}$$

Perhaps

$$\sum_{k=1}^{\varphi(n)} e^{a_{k+1}-a_k} < Ce^{G(n)}.$$

Now I state a few problems on unconventional sieves. Let $f(m)$ be a number theoretic function. n is said to be a barrier for $f(m)$ if for every $m<n$ we have $m+f(m)\leqslant n$. A function can only have a barrier if it does not increase fast. I wanted to prove that $\sum_{k=1}^{\infty} \nu(n)2^{-n}$ is irrational (this problem is still open) and this led me to the problem whether $\nu(n)$ has infinitely many barriers. The answer is almost certainly yes, but a proof can perhaps not be expected, since if n is a barrier than $n-1=p$ and $n-2=2q$ where p and q are primes. It is a well-known, unsolved problem whether infinitely many pairs of such primes exist. Faced with this situation I hoped that I could prove that for some $\varepsilon>0$ $\varepsilon\nu(n)$ has infinitely many barriers. I failed to do so, but if we would know a little more about sieves where the number of omitted residues mod p is a slowly increasing function of p we would probably succeed. Selfridge and I investigated if $d(n)$ has infinitely many barriers. Observe that $\max(n-1+d(n-1),\ n-2+d(n-2))\geqslant n+2$. Thus the best one can hope here is that for infinitely many n

$$\max_{m<n}(m+d(m))=n+2. \tag{5}$$

For example $n=24$ satisfies (5). We convinced ourselves that if there is any $n>24$ which satisfies (5) it must be enormous—far beyond the reach of our computers and tables (and unfortunately probably our brains). Perhaps it would be more reasonable to conjecture that

$$\max_{m<n}(m+d(m))-n\to\infty \tag{6}$$

as $n\to\infty$. I feel that (5) if true is completely hopeless; (6) if true could perhaps be attacked.

I was often blocked in my work by sieve problems of the following kind: Let $p_k < n$ be any set of primes satisfying $\sum (1/p_i) > c$. Is it true that to every $\varepsilon > 0$ there is a k (k depends only on c and ε and not on n or the set of primes p_i), so that if $\{a_j^{(i)}\}$, $j = 1, \ldots, k$ is an arbitrary set of k residues mod p_i then the number of integers $x < n$

$$x \not\equiv a_j^{(i)} (\mathrm{mod}\ p_i), \qquad j = 1, \ldots, k$$

is less than εx? For many related problems and results see our forthcoming paper with I. Ruzsa in the *Journal of Number Theory*.

Is it true that to every ε there is a k so that if we omit $(p_i - 1)/2$ residues mod p_i where $p_1, \ldots, p_k$ are any k primes satisfying $p_i = o(n)$ then all but εn integers $\leqslant n$ have been omitted?

Let $f(x)$ be the smallest integer so that there are $(p_i + 1)/2$ residues

$$a_j^{(i)} (\mathrm{mod}\ p_i), \qquad j = 1, \ldots, \frac{p_i + 1}{2}, \qquad p_i \leqslant f(x) \tag{7}$$

so that every integer $n \leqslant x$ satisfies at least one of the congruences (7). Determine or estimate $f(x)$ as accurately as possible. On the one hand it is easy to see that we must have $\prod_{p/f(x)} p > x$, on the other hand

$$2^{\pi(f(x))} < x,$$

where π is the prime counting function. These two inequalities imply

$$(1 + o(1)) \log x < f(x) < (1 + o(1)) \frac{\log x \log \log x}{\log 2}. \tag{8}$$

I would be interested in any improvement—however small—of (8). I have no guess for an asymptotic formula for $f(x)$.

Are there infinitely many integers n not of the form

$$ak^2 + b, \qquad k > 1, \qquad a \geqslant 1, \qquad 0 \leqslant b < k\,? \tag{9}$$

Selfridge and Wagstaff made some numerical calculations which seem to indicate that the number of these n is indeed infinite. Perhaps (9) should be replaced by

$$ak^2 + b, \qquad k > 1, \qquad a \geqslant 1, \qquad -k < b < k. \tag{9'}$$

(9') implies that $n \equiv 0 \pmod 4$. I would expect that there are by infinitely many integers n not of the form (9'). Denote $F_1(x)$ (respectively $F_2(x)$) the number of integers $\leqslant x$ not of the form (9) (respectively (9')). The computations of Selfridge and Wagstaff seem to indicate that

$$x^{\alpha_1} < F_1(x) < x^{\alpha_2}$$

and perhaps the same holds for $F_2(x)$.

One final question of this type: Let $a_1 \leqslant a_2 \leqslant \cdots$. Consider the integers of the form

$$ak^2+b, \qquad a \geqslant 1, \qquad k>1, \qquad -a_k<b<a_k. \tag{9''}$$

How fast must a_k increase that if $h(n)$ denotes the number of representations of n in the form (9'') then $h(n) \to \infty$ as $n \to \infty$? Does $a_k/k \to \infty$ suffice? I doubt it. Many further questions could be asked but we leave this to the reader—I hope (against hope) that at least some of them he will be able to answer.

Now let us discuss some problems on primes. The prime k-tuple conjecture of Hardy and Littlewood states as follows: Let $a_1<a_2<\cdots<a_k$ be k integers. Then the necessary and sufficient condition that there should be infinitely many values of n for which all the integers $n+a_i$, $i=1, \ldots, k$ are primes is that for no prime p should the set $a_1, \ldots, a_k$ form a complete set of residues mod p. The condition is clearly necessary; the proof of the sufficiency seems hopeless at present since e.g. the conjecture that there are infinitely many prime twins is a special case. The analogous question about squarefree numbers is easy and well known. The necessary and sufficient condition that for infinitely many n all the integers $n+a_i$, $i=1, \ldots, k$ should be squarefree is that the a's do not form a complete set of residues (mod p^2) for any prime p. The reason for this difference is that $\sum_p (1/p^2)<\infty$ is convergent and therefore we have no difficulty with the sieve. Let us now return to the prime k-tuple conjecture. There are some interesting extremal problems here. First of all observe that if $\{a_1, \ldots, a_k\}$ is a sequence of residues which do not form a set of complete residues mod p for every p—let us call such a set of integers a P_k set—then clearly it suffices to restrict ourselves to the primes $p \leqslant k$. First of all how many distinct P_k sequences are there? Two P_k sequences are identical if they are identical mod p for every $p \leqslant k$. It is not clear if there is a nice formula for this number. Much more interesting and infinitely more difficult are the following extremal problems: Determine or estimate

$$\min a_k = f(k) \quad \text{and} \quad \min \sum_{i=1}^{k} a_i = F(k) \tag{10}$$

where the minimum is to be taken over all the P_k-sequences $0 \leqslant a_1 < \cdots < a_k$. There is no reason to assume that the extremal sequences giving the solutions of these two problems coincide. It would be of interest to determine these extremal sequences for small values of k. The sequences for $k \geqslant 4$ will probably begin to be interesting. Clearly many other related extremal problems could be asked; we restrict ourselves to state one more problem: Consider all the sequences of one of the classes of P_k (i.e. the sequences of

our class are all congruent mod p for all $p \leq k$). Consider

$$\max_{P_k} \min a_k = G(k).$$

Estimate $G(k)$ as well as possible. In other words: in each class consider the sequence $a_1 < \cdots < a_k$ which minimizes a_k and then take the class for which this minimum is maximum. I never considered this problem before and I hope the reader will forgive me if it turns out to be trivial or uninteresting.

It was often conjectured that

$$\pi(x+y) \leq \pi(x) + \pi(y) \tag{11}$$

holds for every $x \geq y > 0$. It was a great surprise to me when a few years ago Hensley and Richards proved that (11) is incompatible with the prime k-tuple conjecture. More precisely they proved that if the prime k-tuple conjecture holds, then there is an absolute constant c so that for all sufficiently large y and infinitely many x

$$\pi(x+y) - \pi(x) - \pi(y) > \frac{cy}{(\log y)^2}. \tag{12}$$

Very recently Richards and I wrote a paper on this subject at the end of which we disagree about a conjecture. Richards believes that (12) holds for every c and suitable x and y and I believe that for sufficiently large c and all x, y

$$\pi(x+y) - \pi(x) - \pi(y) < cy/(\log y)^2. \tag{13}$$

I repeat my meta-conjecture: None of us will ever know the answer, at least not in this world.

In conversation a few years ago somebody (let us refer to him or her as S) pointed it out to me that the conjecture $\pi(x+y) \leq \pi(x) + \pi(y)$ was not reasonable. The "correct" conjecture should have been

$$\pi(x+y) \leq \pi(x) + 2\pi\left(\frac{y}{2}\right). \tag{14}$$

S argued that amongst all the intervals of length y the interval $(-y/2 + y/2)$ can be expected to contain the largest number of primes. I agree with S; (14) would of course imply (13).

Montgomery–Vaughan and Selberg proved

$$\pi(x+y) - \pi(x) < \frac{2y}{\log y}. \tag{15}$$

This sharpens a previous result of Selberg. It would be very nice if in (15) one could replace 2 by $2 - \varepsilon$, but at the moment this seems far beyond our reach.

X and I asked: Are there infinitely many $2k$-tuples ($k > 1$) of consecutive primes $p_{n+1} < \cdots < p_{n+2k}$ satisfying $p_{n+i} + t = p_{n+k+i}$, for some $t = t(k)$ and $i = 1, \ldots, k$? The prime k-tuple conjecture of course implies this; the point is to try to prove this without any hypotheses. We were unable to make any progress with this problem.

One could try to extend the prime k-tuple conjecture for infinite subsequences. It is easy to see that there are sequences $a_1 < a_2 < \cdots$ which increase as fast as we wish and which do not form a complete set of residues mod p for any p and nevertheless there is no integer n for which all the numbers $a_1 + n$, $i = 1, 2, \ldots$ are all primes (or are all squarefree). On the other hand it follows from the prime k-tuple conjecture that there are two infinite sequences $a_1 < a_2 < \cdots$; $b_1 < b_2 < \cdots$ so that all the sums $a_i + b_j$ $1 < i < j < \infty$ are all primes. It is not hard to prove that there is an infinite sequence $u_1 < u_2 < \cdots$ for which all the sums $u_i + u_j$ are all squarefree. Can these sequences be of polynomial growth? I am sure that the answer is negative. Perhaps they can be of exponential growth. Let more generally $a_1 < a_2 < \cdots$ be any sequence of positive identity. Is it true that there is an infinite sequence $b_1 < b_2 < \cdots$ and a fixed integer t so that all the sums $b_i + b_j + t$ $i \neq j$ are as?

In various problems on primes it would often be useful to obtain non-trivial estimations about the smallest solutions of systems of congruences, e.g. Ecklund, Selfridge and I tried to estimate the smallest integer n_k for which $\binom{n_k}{k}$ has no prime factor $\leq k$ or the smallest N_k for which all primes $p \leq k$ divide $\binom{N_k}{k}$; we only obtained crude upper and lower bounds. Another related question: let m_k be the smallest integer greater than k for which no prime factor of $\prod_{i=1}^{k}(m_k + i)$ is in $(k, 2k)$, or alternatively let M_k be the smallest integer greater than $2k$ for which $\prod_{i=1}^{k}(M_k + i)$ is a multiple of all the primes q, $k < q < 2k$. Again only rough upper and lower bounds are available.

Before I turn to covering congruences let me state two problems on the difference of consecutive primes. First an old problem of Turán and myself: Put $d_n = p_{n+1} - p_n$. There is no doubt that for every k there are infinitely many n for which $d_{n+1} > \cdots > d_{n+k}$ and $d_{n+1} < d_{n+2} < \cdots < d_{n+k}$ both have infinitely solutions; we can only prove this for $k = 2$. Surely $d_{n+1} = \cdots = d_{n+k}$ also has infinitely many solutions, but this we can not even prove for $k = 2$, and is probably hopeless at present. We could not even prove that there is no n_0 so that for every $i \geq 1$, $(d_{n_0+i} - d_{n_0})(-1)^i \geq 0$. Perhaps here we overlook a trivial point and I offer 100 dollars for a proof that no such n_0 exists. (I am of course so sure that such an n_0 does not exist that I do not even offer anything for finding an n_0.)

Define n_i to be the smallest integer for which $t_i = d_{n_i+1} - d_{n_i} > d_{u+1} - d_u$, for all $u < n_i$.

It seems likely that the sequence n_i increases very rapidly and surely $n_{i+1} > n_i + 1$ for all $i > i_0$. Similarly the sequence t_i seems to increase rapidly but I certainly cannot prove that the sequence t_i has density 0 and in fact cannot even prove that there are infinitely many even numbers not equal to one of the t_i. There again I may be overlooking a trivial point.

Similar questions can be asked about squarefree numbers. Let $q_1 < q_2 < \cdots$ be the sequence of consecutive squarefree numbers. It is a simple exercise to prove that for every r there are infinitely many values of k for which

$$q_{k+1} - q_k = q_{k+2} - q_{k+1} = \cdots = q_{k+r+1} - q_{k+r}.$$

The only problem which remains is: How fast can r increase as a function of k?

On the other hand n_i and t_i can be defined here too, and I can do as little here as with the primes. No doubt $q_{n+1} - q_n = o(n^\varepsilon)$ but we are very far from being able to prove this. Put

$$F(n) = \max_{q_k < n} (q_{k+1} - q_k).$$

A simple argument using the Chinese Remainder Theorem and the Prime Number Theorem gives

$$\limsup_{n>\infty} F(n)\left\{\frac{\pi^2}{12}\frac{\log n}{\log\log n}\right\}^{-1} \geqslant 1. \tag{16}$$

I never was able to improve (16) and I am not absolutely sure that (16) is not best possible—though I frankly doubt it. Let $1 < a_1 < \cdots (a_i, a_j) = 1$, and assume that the as tend to infinity sufficiently fast. Denote by $1 = b_1 < b_2 < \cdots$ the sequence of integers not divisible by any of the a's. Define $\phi(n)$ as the integer t for which

$$\prod_{i=1}^{t} a_i \leqslant n < \prod_{i=1}^{t+1} a_i.$$

Then a simple sieve process gives ($F(n) = \max_{b_i < n} (b_{i+1} - b_i)$)

$$\limsup_{n\to\infty} F(n)\left(\phi(n)\prod\left(1-\frac{1}{a_i}\right)\right)^{-1} = 1. \tag{17}$$

If $a_i = p_i^2$, then (17) becomes (16), but I doubt very much whether p_i^2 increases fast enough to insure equality in (16). I expect that the as have to increase faster than polynomially to insure that (17) should hold. I hope to investigate this problem in the near future.

Now I state a few problems connected with covering congruences. Some of these problems are in my opinion among the most interesting ones I ever

invented. Van der Corput and I proved that there are infinitely many odd integers not of the form 2^k+p; in fact there is an arithmetic progression consisting entirely of odd numbers no term of which is of the form 2^k+p.

In 1934 Romanoff proved that the lower density of the integers of the form 2^k+p is positive. Presumably the density of these integers exists, but this has never been proven and probably can not be proven by the methods at our disposal at present. In 1934 Romanoff wrote to me asking if I can prove that there are infinitely many odd integers not of the form 2^k+p. Using covering congruences I proved that there is an arithmetic progression of odd numbers no term of which is of the form 2^k+p. A system of congruences

$$a_i \pmod{n_i}, \qquad n_1 < \cdots < n_k \tag{18}$$

is said to be covering if every integer satisfies at least one of the congruences (18). The simplest such system is 0 (mod 2), 0 (mod 3), 1 (mod 4), 5 (mod 6), 7 (mod 12). To prove the theorem I had to find a covering system which does not contain the modulus 6, which is easy. The most interesting problem which can be posed states: Is there a system (18) for every t satisfying $t \leqslant n_1$? The present record is held by Choi who constructed such a system with $n_1 = 20$. I offer 1000 dollars for a proof or disprove of the existence of a covering system (18) with n_1 arbitrarily large. If systems (18) exist for every t then it is easy to see that for every r there is an arithmetic progression no term of which is of the form $2^k+\theta_r$ where θ_r has r or fewer distinct prime factors.

Linnik proved that there is an r so that every integer is the sum of two primes and r powers of 2. Gallagher proved that for every $\varepsilon > 0$ there is an r so that the lower density of the integers n which are the sum of a prime p and r powers of 2 is greater than $1-\varepsilon$. This result of course implies Linnik's result. Is it true that there is an r so that every integer is the sum of a prime p and r powers of 2? Crocker proved that there are infinitely many odd integers which are not of the form $p+2^{u_1}+2^{u_2}$. The numbers not of this form given by Crocker's construction form a very thin sequence. I suspect that covering congruences cannot be applied here. More precisely: Let $q_1, \ldots, q_s$ be any set of odd primes and let $n > n_0(q_1, \ldots, q_s)$ be a sufficiently large odd integer. Then there are integers u and v satisfying

$$2^u + 2^v < n, \quad \left(n - 2^u - 2^v \prod_{i=1}^{s} q_i\right) = 1. \tag{19}$$

(19) if true would of course show that covering congruences cannot be used here.

I do not have any guess if in fact there is an r so that every n is the sum of a prime and r or fewer powers of 2.

I conjectured that every $n \not\equiv 0 \pmod 4$ is of the form $2^k + \theta$ where θ is squarefree. This conjecture if true will be certainly very hard to prove. It is not even known that every $n > n_0(k)$ is the sum of a k-th power and a squarefree number. There might be some chance of proving that almost all integers $n \not\equiv 0 \pmod 4$ are of the form

$$2^k + \theta \qquad \theta \text{ squarefree}. \tag{20}$$

In any case I do not believe that (20) can be disproved by covering congruences. As far as I know it has never been proven that every sufficiently large n can be written in the form $2^k + \theta$ where $v(\theta) < \log\log n$ ($v(n)$ is the number of distinct prime factors of n). In fact one would perhaps expect that to every ε there is an n_0 so that for every $n > n_0$

$$n = 2^k + \theta, \qquad v(\theta) < \varepsilon \log\log\theta$$

is solvable.

An integer n is called covering if one can form a covering system from the division $2 \leqslant d_1 < \cdots < d_{r(n)} = n$ of n. It is not hard to show that the covering numbers have a density. I conjectured and J. Haight recently proved that for every C there are integers n for which $\sigma(n)/n > C$ and n is not a covering number. This is one of the few theorems on covering systems. A possible refinement would be: Put

$$g_1(x) = \max_{n<x} \frac{\sigma(n)}{n}, \qquad g_2(x) = \max_{n'<x} \frac{\sigma(n')}{x}$$

where n' runs through the integers which are not covering numbers. By Haight's theorem $g_2(x) \to \infty$. Is it true that

$$|g_1(x) - g_2(x)| < C\,?$$

The paper of Haight will appear in Matematika very soon.

I conjectured that for every system (18) we must have $\sum_{i=1}^{k} (1/n_i) > 1$. In other words: A covering system can never be exact. L. Mirsky and D. Newman (independently) proved this conjecture in a very simple and ingenious way. Herzog and Schönheim have the following interesting conjecture which is a far reaching generalization: Let G be a finite group (if necessary assume it to be abelian). Let $H_1, H_2, \ldots, H_k$ be cosets of G satisfying

$$H_i \cap H_j = \phi, \qquad 1 < |H_1| < \cdots < |H_k| < |G|.$$

Then $G \neq \bigcup_{i=1}^{k} H_i$. In other words G is not the union of disjoint cosets of different sizes. As far as I know this conjecture has not yet been settled.

To end the paper I state a few miscellaneous problems. A well-known theorem of van der Waerden states that if we divide the integers into two

classes then at least one of them contains an arbitrarily long arithmetic progression. Let $f(n)$ be the smallest integer so that if we divide the integers from 1 to $f(n)$ into two classes then at least one of them contains an arithmetic progression of n terms. Almost nothing is known about $f(n)$; perhaps it increases faster than any primitive recursive function, but it is not even known that $f(n) > c^n$ for every c if $n > n_0(c)$. I offer one hundred dollars for a proof or disproof of this conjecture.

More than 45 years ago Turán and I conjectured that every sequence of positive upper density contains arbitrarily long arithmetic progressions. I offered a few years ago one thousand dollars for a proof of this conjecture. Szemerédi proved this conjecture by a masterpiece of combinatorial reasoning. Recently Fürstenberg obtained a proof using ergodic theory. Let now $f_c(n)$ be the smallest integer so that if

$$1 \leq a_1 < \cdots < a_r \leq f_c(n), \qquad r = [cf_c(n)],$$

is any sequence of integers then the a's contain an arithmetic progression of n terms. Nothing significant is known about the growth properties of $f_c(n)$. In particular it is not known to what extent it depends on c and in particular it is not known if $f_{\frac{1}{2}}(n)$ increases significantly faster than $f(n)$. It might be worth while to investigate this question but unfortunately methods seem to be lacking.

An old conjecture states that the set of primes contains arbitrarily long arithmetic progressions. I conjectured many decades ago that if $\sum_i (1/a_i) = \infty$ then the a's contain arbitrarily long arithmetic progressions. I offer 3000 dollars for a proof or disproof. It is known that there are infinitely many triples of primes in an arithmetic progression i.e. $p + q = 2r$ is solvable in primes infinitely often, but it is not known if there are infinitely many quadruples of primes in an arithmetic progression and no proof is in sight.

Sierpinski proved, by using covering congruences, that if $N(x)$ is the number of odd positive integers $k \leq x$ such that $k \cdot 2^n + 1$ is composite for every positive integer n then $N(x) > cx$. Bateman asked if the number of odd integers for which this property does not hold is also $> cx$. In other words: is it true that the number of odd integers $k < x$ of the form $(p-1)/2^n$ is greater than cx? Odlyzko and I proved this. We also conjectured that every integer $k \equiv 1$ or $5 \pmod 6$ is of the form $(p-1)/2^\alpha 3^\beta$. Odlyzko showed this for every $k < 10^5$. There does not seem to be much hope to prove our general conjecture.

The following somewhat vague question could be posed: Are there odd integers k for which $k2^n + 1$ is composite but which can not be obtained by covering congruences? Perhaps the following formulation is less vague: Is there an integer k for which $k2^n + 1$ is composite for every n but if $p_1, \ldots, p_r$ is any finite set of primes then there always is an n for which

$(k2^n+1, \prod_{i=1}^{r} p_i)=1$? These type of questions arise in several situations—so far all of them were unattackable.

Turán and I asked: Let $a_1, \ldots, a_k$ be real numbers. What are necessary and sufficient conditions that

$$\sum_{i=1}^{k} a_i p_{n+1}, \qquad n=1,2,\ldots \tag{21}$$

should have infinitely many changes of sign? We have observed that $\sum_{i=1}^{k} a_i = 0$ is clearly necessary and Polya observed that if (21) has infinitely many changes of sign then the k numbers $\alpha_j = \sum_{i=1}^{j} a_i$ cannot all have the same sign. Polya, Turán and I then conjectured that if the α_1 are not all of the same sign then (21) has infinitely many changes of sign. We are very far from being able to prove this, in fact I cannot even prove that $d_n > d_{n+1} + d_{n+2}$ $(d_n = p_{n+1} - p_n)$ has infinitely many solutions. I proved the following much easier theorem: Assume that $\sum_{i=1}^{k-1} \alpha_i = 0$ and $\alpha_{k-1} \neq 0$. Then (21) changes sign infinitely often. If the primes are replaced by squarefree numbers then it is easy to see that our conjecture holds.

Finally I would like to call attention to the following curious situation: Ricci and I proved that the set of limit points of $d_n/\log n$ has positive Lebesgue measure; the same is true for d_n/d_{n+1} and also for $\tau(n)/\tau(n+1)$ ($\tau(n)$ denotes the number of divisors of n). In the case of $\tau(n)/\tau(n+1)$ I proved that the set of limit points contains intervals. Nevertheless in none of these cases could we (or anybody else) decide if a given positive real number is a limit point of elements of our set. Perhaps I overlook a simple argument.

REFERENCES

I published several papers which contain unsolved problems. My latest paper entitled: Problems and Results on Combinatorial Number Theory, Number Theory Day, Proceedings, New York 1976, M. Nathanson editor, Springer-Verlag, Lecture Notes in Math. 626, 43–72 contains an extensive bibliography and also references to some of my other problem papers. I will give references only to papers not quoted there.

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

[2] Ecklund, E. F., Erdös, P. and Selfridge, J. L.
A new function associated with the prime factor of $\binom{n}{k}$. *Math. Computation* **28** (1974), 647–649.

[3] Erdös, P.
Some problems and results in elementary number theory. *Publ. Math. Debrecen* **2** (1951), 103–109.

[4] Erdös, P.
On the integers relatively prime to n and on a number theoretic function considered by Jacobstahl. *Math Scand.* **10** (1962), 163–170.

[5] Erdös, P.
Some problems on consecutive prime numbers. *Mathematika* **19** (1972), 91–95.

[6] Erdös, P. and Odlyzko, A. M.
On the density of odd integers of the form $(p-1)2^{-n}$ and related questions. *J. of Number Theory*, **11** (1979), 257–263.

[7] Erdös, P. and Richards, I.
Density functions for prime and relatively prime numbers. *Monatshefte für Math.* **83** (1977), 99–112.

[8] Fürstenberg, H. and Katznelson, Y.
An ergodic Szemerédi theorem for commuting transformations. *Journal d'Analyse* **34** (1978), 275–291.

[9] Gallagher, P. X.
Primes and powers of 2. *Inventiones Math.* **29** (1975), 125–142.

[10] Hensley, D. and Richards, I.
Primes in intervals. *Acta Arith.* **25** (1973–74), 375–391.

[11] Hooley, C.
On the difference between consecutive numbers prime to n. I, II and III, *Acta Arithmetica* **8** (1962/1963), 343–347, *Publ. Math. Debrecen* **12** (1965), 39–49; *Math. Zeitschrift* **90** (1965), 39–49. See also "Applications of sieve methods to the theory of numbers", Cambridge Tracts in *Math* **70** and "On a new technique and its applications to the theory of numbers", *Proc. London Math Soc.* **38** (1970), 115–151.

[12] Montgomery, H. L.
Topics in multiplicative number theory. Lecture Notes in *Math* **227**, Springer-Verlag, 1971.

[13] Rankin, R. A.
The difference between consecutive prime numbers. *J. London Math. Soc.* **13** (1938), 242–244.

[14] Richert, H. E.
On the difference between consecutive squarefree numbers. *J. London Math. Soc.* **29** (1953), 16–20. The strongest result on this subject is due to P. G. Schmidt, Abschätzungen bei unsymmetrischen Gitterpunktproblemen, *Dissertation*, Göttingen 1964.

[15] Szemerédi, E.
On sets of integers containing no k elements in arithmetic progression. *Acta Arith.* **27** (1975), 299–345.