Acta Mathematica Academiae Scientiarum Hungaricae
Tomus 33 (1–2), (1979), pp. 71–80.

SOME UNCONVENTIONAL PROBLEMS IN NUMBER THEORY

By

P. ERDŐS (Budapest), member of the Academy

Dedicated to the 80th birthday of my friend George Alexits

In the paper, we will mostly deal with arithmetic functions, primes, divisors, sieve processes and consecutive integers.

1. Let f be an arithmetic function. The integer n is called a *barrier* for f if

$$m+f(m)\le n \tag{1}$$

for every $m<n$.

Perhaps I should explain why I considered (1). In the early 1950's, van Wijngaarden told me the following conjecture. Put $\sigma_1(n)=\sigma(n)$, the sum of divisors of n, and $\sigma_k(n)=\sigma_1(\sigma_{k-1}(n))$. Is it true that there is essentially only one sequence $\sigma_k(n)$ $(k=1,2,3,\dots)$? In other words, if m and n are distinct integers, are there integers k and l such that $\sigma_k(m)=\sigma_l(n)$? Such a conjecture is usually hopeless to prove or disprove. Selfridge and others made some computer experiments and believe that the conjecture is false. I tried to find an airthmetic function for which an analogous conjecture is true and can be proved. Put $f_1(n)=n+\nu(n)$, where $\nu(n)$ is the number of distinct prime factors of n, and $f_k(n)=f_1(f_{k-1}(n))$. Is it true that for any two integers m and n there are integers k and l for which $f_k(m)=f_l(n)$?. This would follow immediately if we could prove that $\nu(n)$ has infinitely many barriers. This problem seems more interesting than my original question. It is easy to find with a pocket computer and a little patience (I do not have either of these) a large number of integers which are barriers for $\nu(n)$, but I am afraid that the question of the existence of infinitely many barriers is hopeless at present. I could not even prove that $\varepsilon\nu(n)$ has infinitely many barriers for some $\varepsilon>0$. Sieve methods seem the right method of attack, but there are great technical difficulties which I could not overcome.

The following theorem gives a result of this type which can actually be proved.

THEOREM 1. *For $n=\Pi p_i^{\alpha_i}$ set $d_0(n)=\Pi\alpha_i$. Then $d_0(n)$ has infinitely many barriers, that is there are infinitely many n such that*

$$m+d_0(m)\le n \quad \textit{for every} \quad m<n. \tag{2}$$

In fact, the density of integers satisfying (2) *is positive.*

I will outline the simple (but slightly messy) proof of Theorem 1 at the end of the paper.

Let me now state a few other difficult problems. Let $\Omega(n)$ denote the total number of prime factors of n, that is $\Omega(n)=\Sigma\alpha_i$ when $n=\Pi p_i^{\alpha_i}$. Probably $\Omega(n)$ has infinitely marry barriers, but this is clearly hopeless at present, since a barrier n would have to satisfy $n-1=p$ and $n-2=2q$ for primes p and q and we are not likely to be able to prove the existence of infinitely many such n in the near future. Selfridge found that 99840 is the largest barrier for $\Omega(n)$ below 10^5. Selfridge and I then investigated whether $d(n)$, the number of divisors of n, has any barriers. Here one has to redefine the barrier a little bit: n is a barrier for $d(n)$ if

$$m+d(m)\leqq n+2$$

for every $m<n$. This is satisfied by $n=24$ and we convinced ourselves that if there is any other solution then it is enormously large, far beyond our tables and computers.

Define

$$H_f(n)=\max_{m<n}\big(m+f(m)-n\big).$$

It is quite possible that $H_d(n)\to\infty$ as $n\to\infty$,but these questions are clearly hopeless at the present "state of the art". On the other hand, it would not be very difficult to prove that, for almost all n, $H_\nu(n)/\log\log n(\log\log\log n)^{1/2}\to c(>0)$ as $n\to\infty$. (I have not carried out the details.) The strongest possible conjecture which has a chance of being true is as follows: for every $\varepsilon>0$, there are infinitely many values of n so that

$$(3)\qquad \nu(n-k)<(1+\varepsilon)\log k/\log\log k \ \text{ and } \ \Omega(n-k)<(1+\varepsilon)\log k/\log 2$$

for every k satisfying $k_0(\varepsilon)<k<n$. In may opinion, this has some chance of being true, but there is no chance at all of proving it in the forseeable future. At the present moment, I cannot disprove the following strengthening of (3): there are infinitely many values of n so that

$$(4)\qquad \nu(n-k)<\frac{\log k}{\log\log k}+C \quad\text{and}\quad \Omega(n-k)<\frac{\log k}{\log 2}+C$$

for every k satisfying $k_0(C)<k<n$. I am convinced that (4) is false for every C and $n>n_0(C)$; perhaps (4) and (3) can be disproved. It seems certain that for every k there are infinitely many values of n for which

$$\max_{n-k<m<n}\big(m+d(m)\big)\leqq n+2,$$

though this is hopeless with our present methods. It would easily follow from Hypothesis H of Schinzel.

Let $f(n)$ be a non-negative additive or multiplicative function which has a bounded average, that is $\sum_{1\leqq n\leqq x}f(n)<cx$. Then $\liminf_{n\to\infty}H(n)<\infty$. (We suppress the proof since it is very similar to that of Theorem 1.) For $n=\Pi p_i^{\alpha_i}$ define $d_r(n)=\Pi(r+\alpha_i)$. It is not hard to show that if (3) holds then $\liminf_{n\to\infty}H_{d_r}(n)<\infty$.

To conclude this section, we observe that $\sigma(n)$ and $\phi(n)$ increase too fast to have barriers. In fact, it is easy to prove that $\max\limits_{m<n}\big(m+\phi(m)\big)=2n+o(n)$ and if we make plausible (but at present inaccessible) assumptions on the difference of consecutive primes, then it is easy to see that $\max\limits_{m<n}\big(m+\phi(m)\big)=2Q_n-1$ for all $n>n_0$, where Q_n is the largest prime not exceeding n. Finally a little elementary manipulation with the primes gives $\max\limits_{m<n}\big(m+\sigma(m)\big)=\max\limits_{m<n}\sigma(m)+n-o(n)$.

2. Now we discuss some unconventional problems on primes. Denote by $p(m)$ the least and by $P(m)$ the largest of the prime factors of m. Put $F(n)=\max\{m+p(m)\colon 1\leqq m<n,\ m \text{ composite}\}$. Is it true that $F(n)\leqq n$ for infinitely many n? Many related questions occur in a forth-coming triple paper of Eggleton, Selfridge and myself. We conclude that plausible conjectures on primes imply that $F(n)\leqq n$ has only a finite number of solutions. Trivially, $F(n)>n+\sqrt{n}$, but it is quite possible that $F(n)>n+(1-\varepsilon)\sqrt{n}$ for $n>n_0(\varepsilon)$.

Further questions can be posed if we do not want to ignore the primes, as in the definition of $F(n)$, but perhaps it is more natural in this case to consider the numbers $n+i$ instead of $n-i$. Thus, let g be a non-decreasing arithmetic function and let $B(n,g)$ be the smallest i for which $p(n+i)>g(i)$. If such an i does not exist, put $B(n,g)=\infty$. First, take $g(i)=i+1$. It is easy to see that $B(n,i+1)$ is just the smallest prime not dividing $n-1$ and, by the prime number theorem, $B(n,i+1)\leqq\big(1+o(1)\big)\log n$. I could not get such a simple estimate for $B(n,g)$ if $g(i)=i+c$, or say $2i+1$. It follows from plausible assumptions on the distribution of primes that $B(n,i^k+1)<\infty$ for $n>n_0(k)$. I wonder if one can prove without any assumptions on the primes that, for every $n>n_0$, there is an i with $p(n+i)>i^2+1$. It follows from Huxley's well-known result on gaps between consecutive primes that, for every $n>n_0(\varepsilon)$, there is an i with $p(n+i)>i^{12/7+\varepsilon}$. It easily follows from well-known results on large gaps between consecutive primes that $p(n+i)<e^{\varepsilon i}+c(\varepsilon)$ $(i=1,2,3,\dots)$, that is $B\big(n,e^{\varepsilon i}+c(\varepsilon)\big)=\infty$ holds for infinitely many n. The additive constant $c(\varepsilon)$ is needed to take care of the very small values of i. In fact, $e^{\varepsilon i}$ can be replaced by $\exp\{ci(\log\log i)^2/\log i\log\log\log i\}$. A well-known conjecture of Cramer states that

$$\limsup_{k\to\infty}\,(p_{k+1}-p_k)/(\log k)^2=1 \tag{5}$$

where $p_1<p_2<p_3<\dots$ is the sequence of consecutive primes. Let us assume that (5) holds. Then we obtain $B\big(n,e^{(1-\varepsilon)i^{1/2}}\big)<\infty$ for every $n>n_0(\varepsilon)$. But I cannot conclude from (5) that $B\big(n,e^{(1+\varepsilon)i^{1/2}}+c(\varepsilon)\big)=\infty$ for infinitely many n because, of course, $p(n+i)$ can be very large even if $n+i$ is not a prime. There is clearly not much hope to settle these questions in the near future. Let us therefore be more modest for the moment and try to determine when the integers n satisfying $p(n+i)<g(i)$ $(i=1,2,3,\dots)$ have positive density. A more or less routine sieve process

shows that a necessary and sufficient condition for the non-decreasing function g to have this property is that

$$\sum_{i=1}^{\infty} \prod_{p<g(i)} \left(1-\frac{1}{p}\right) < \infty .$$

Now let us investigate what can be said about the large values of $p(n+i)$ for $n+i$ composite. First, is it true that for $n > n_0$, there is always an i for which $n+i$ is composite and $p(n+i) > i^2$? This is closely related to questions which we considered with Eggleton and Selfridge. Perhaps it is true that for every k and $n > n_0(k)$, there is an i for which $n+i$ is composite and $p(n+i) > i^k$. Clearly it is hopeless to prove this at present. I thought that for $k > k_0$, there is always an m satisfying $p_k < m < p_{k+1}$ and $p(m) \geqq p_{k+1} - p_k$, with equality say for prime twins. I am now sure that this is not true and I "almost" have a counterexample. Pillai and Szekeres observed that for every $t \leqq 16$, a set of t consecutive integers always contains one which is relatively prime to the others. This is false for $t = 17$, the smallest counterexample being 2184, 2185, . . ., 2200. Consider now the two arithmetic progressions $2183 + d \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ and $2201 + d \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. There certainly will be infinitely many values of d for which the progressions simultaneously represent primes; this follows at once from hypothesis H of Schinzel, but cannot at present be proved. These primes are consecutive and give the required counterexample. I expect that this situation is rather exceptional and that the integers k for which there is no m satisfying $p_k < m < p_{k+1}$ and $p(m) > p_{k+1} - p_k$ have density 0.

Things become much easier if we study $P(m)$. A well-known theorem of Sylvester and Schur states that $P\left(\binom{n}{k}\right) > k$ if $k \leqq \frac{1}{2} n$. In other words, for every k and n with $k \leqq n$, there is an m satisfying $n+1 < m \leqq n+k$ and $P(m) > k$. This is certainly not true for $p(m)$. There are many extensions and sharpenings of the Sylvester–Schur theorem. Although we are very far from being able to prove it, there is no doubt that

$$P\left(\binom{n}{k}\right) > \min \{n-k+1,\ k^{1+c}\} \tag{6}$$

for some absolute constant c. Ramachandra, Shorey and Tijdeman have many results in this direction. It seems certain that (6) actually holds for every c with a finite number of exceptions (depending on c). Cramer's conjecture (5) suggests that perhaps

$$P\left(\binom{n}{k}\right) > \min \{n-k+1,\ e^{(1-\varepsilon)k^{1/2}}\}$$

holds if we disregard a finite number of values of k and n. Let

$$\binom{n}{k} = u_k^{(n)} v_k^{(n)} \quad \text{where} \quad P\left(u_k^{(n)}\right) < k,\ p\left(v_k^{(n)}\right) \geqq k . \tag{7}$$

In a forthcoming paper, Ecklund, Eggleton, Selfridge and I prove that, for $n \geqq 2k$, we have $v_k^{(n)} > u_k^{(n)}$ except for 12 cases, namely $\binom{8}{3}, \binom{9}{4}, \binom{10}{5}, \binom{12}{5}, \binom{21}{7}, \binom{21}{8}, \binom{30}{7}, \binom{33}{13}, \binom{33}{14}, \binom{36}{13}, \binom{36}{17}$, and $\binom{56}{13}$. If in (7) we modify the definition to $P(u_k^{(n)}) \leqq k, p(v_k^{(n)}) > k$, we can still prove that $v_k^{(n)} > u_k^{(n)}$ for $n \geqq 2k$ for all but a finite number of pairs n and k, but we cannot prove that we have all the exceptional cases. (The unresolved cases correspond to $k = 3$, 5 and 7.) We now give a further result of this type.

THEOREM 2. *Write* $\binom{n}{k} = u_k^{(n)} w_k^{(n)} \pi_k^{(n)}$ *where the prime factors* p *of* $u_k^{(n)}$, $w_k^{(n)}$ *and* $\pi_k^{(n)}$ *satisfy the respective inequalities* $2 \leqq p \leqq k$, $k < p < n-k+1$ *and* $n-k+1 \leqq p \leqq n$.

(i) *Except for a finite number of cases,* $w_k^{(n)} > 1$ *if* $4 \leqq k < Q$, *where* Q *is the largest prime not exceeding* $\frac{1}{2}n$.

(ii) *For sufficiently large* C *and* $n > Ck$, $w_k^{(n)} > \max\{u_k^{(n)}, \pi_k^{(n)}\}$.

The proof is fairly easy since we make no attempt (which would be hopeless in any case) to give all the exceptional k and n. Before we give the proof, let us investigate some of the exceptional cases in (i). For $k = 2$, we have $w_k^{(n)} = 1$ if and only if $n-1$ is a Mersenne prime or n is a Fermat prime. There are probably infinitely many cases with $k = 3$ and $w_k^{(n)} = 1$ arising when $n = 2^\alpha 3^\beta + 1$ and $2^\alpha 3^\beta - 1$ are a prime twin. $\binom{9}{3}$ and $\binom{18}{3}$ are not of this form and give $w_k^{(n)} = 1$, but it is easy to see that there are only a finite number of such exceptional cases and it would be easy to tabulate all of them. Finally, if $k \geqq Q$, then $w_k^{(n)} = 1$ clearly holds.

PROOF OF THEOREM 2. We distinguish several cases.

(a) Assume first that $\frac{n}{20} \leqq k < Q \leqq \frac{n}{2}$ It easily follows from elementary results on primes that $2Q > n-k+1$ for $n > n_0$, as $Q \,\Big|\, \binom{n}{k}$, that is $w_k^{(n)} \geqq Q > 1$.

(b) Assume next that $e^{14} < k < \frac{n}{20}$. It is well-known that if $p^\alpha \,\Big\|\, \binom{n}{k}$, then $p^\alpha \leqq n$. If $w_k^{(n)} = 1$, we therefore have

$$\binom{n}{k} < n^{\pi(k)+\pi(n)-\pi(n-k)} < n^{7k/2\log k},$$

using Montgomery's result $\pi(n) - \pi(n-k) < 2k/\log k$ and the estimate $\pi(k) < < 3k/2 \log k$. On the other hand, trivially

$$\binom{n}{k} > n^k e^k / k^{k+1}.$$

On combining the last two inequalities and taking a k-th root, we obtain

$$\frac{2n}{k} < \frac{en}{k^{1+1/k}} < n^{7/2 \log k}$$

and this leads to a contradiction for $e^{14} < k < \frac{n}{20}$ and $n > n_0$. This part of the argument could easily be made effective and the n and k with $k < e^{14}$ and $w_k^{(n)} = 1$ could be enumerated. (In fact, I am sure that there are no such values of n and k.) The cases $k \leqq e^{14}$ considered below cannot at present be made effective, but $k \leqq e^{14}$ could be greatly reduced by more careful computations.

(c) Finally assume $4 \leqq k \leqq e^{14}$. Write

$$\prod_{i=1}^{k} (n+i) = \Pi_1 \Pi_2 \quad \text{where} \quad P(\Pi_1) \leqq l,\ p(\Pi_2) > l.$$

A classical theorem of Mahler states that to every $\varepsilon > 0$ there is an $n_0(\varepsilon, k, l)$ so that $\Pi_1 < n^{1+\varepsilon}$ whenever $n > n_0(\varepsilon, k, l)$. Mahler's theorem is not effective and it is a very important open problem to obtain effective bounds. From Mahler's theorem, we obtain

$$\frac{n^k e^k}{k^{k+1}} < \binom{n}{k} = u_k^{(n)} w_k^{(n)} \pi_k^{(n)} < w_k^{(n)} n^{\frac{3}{2} + \pi(n) - \pi(n-k)} \leqq w_k^{(n)} n^{k - \frac{1}{2}}$$

for $n > n_0(k)$, since $\pi(n) - \pi(n-k) \leqq k - 2$ for $k \geqq 4$. Thus $w_k^{(n)} > 1$ for $n > n_0$. This completes the proof of (i). We suppress the proof of (ii) since it is similar to that of (i).

We observe that $u_k^{(n)} > \pi_k^{(n)}$ and $\pi_k^{(n)} > u_k^{(n)}$ both hold for infinitely many n for every k. In fact, it is easy to see that for every k, $\pi_k^{(n)} = 1$ for almost all n. If $\pi(n) - \pi(n-k) \geqq 2$, then by Mahler's theorem, $\pi_k^{(n)} > u_k^{(n)}$ for $n > n_0(k)$; perhaps this holds always, or at least with very few exceptions. The reason for this bold and somewhat unmotivated conjecture is that it is not hard to prove $\pi_k^{(n)} > u_k^{(n)}$ for all $n > k^{1+c}$ and $k > k_0$, and I hoped that the first failure of $\pi_k^{(n)} > u_k^{(n)}$ occurs when $\pi(n) = \pi(n-k)$ for the first time. This is certainly false for $k = 4$, since the first failure occurs for $n = 9$. Perhaps it fails for all k. There is not much hope to decide any of these questions in the foreseeable future. It follows easily by elementary methods and a little computation that $\pi_k^{(2k)} > u_k^{(2k)}$ for all k except $k = 5$ and 6. It is also easy to see that if $\pi(n) - \pi(n-k) \geqq 1$, then $\pi_k^{(n)} > u_k^{(n)}$ for all but $o\big(\pi(x)\big)$ values of $n < x$. Presumably there are infinitely many values of n with $\pi(n) - \pi(n-k) \geqq 1$ and $\pi_k^{(n)} < u_k^{(n)}$, but if true, this will surely be very hard to prove.

It is not difficult to prove that the density $f(c)$ of integers n for which $\big(u_k^{(n)}\big)^{1/k} > c$ exists and is a continuous strictly decreasing function of c with $f(1) = 1, f(\infty) = 0$. However, the two questions which follow cannot be answered at present because Mahler's theorem is not effective. Denote by $A(n)$ the smallest k for which $u_k^{(n)} > n^2$. By Mahler's theorem, $A(n) \to \infty$ as $n \to \infty$, but we do not know how fast. Perhaps

Baker's results will yield a crude estimate for $A(n)$. Denote by $B(n, k)$ the smallest integer for which

$$\prod_{p^\alpha \| \binom{n}{k},\, p \leqq B(n,k)} p^\alpha > n^2 .$$

Estimate $B(n, k)$ as well as possible.

I investigated if there is a prime $p > k$ so that $p^2 \left| \binom{n}{k} \right.$. Ordinarily, this does not happen. A simple averaging process shows that, for every $\varepsilon > 0$, there is a $k_0(\varepsilon)$ so that when $k > k_0(\varepsilon)$ the density of integers n for which $p^2 \left| \binom{n}{k} \right.$ for some $p > k$ is less than ε. Also, for every k, there are infinitely many n for which $\binom{n}{k}$ is squarefree, but the density of these n tends to 0 as $k \to \infty$. The questions connected with $p^2 \left| \binom{n}{k} \right.$, $p > k$, lead to the following problem which is of independent interest. Is it true that for every $n > n_0$ there is a prime p for which

$$n = up^2 + v,\ u \geqq 1,\ 0 \leqq v < p? \tag{8}$$

It easily follows from the sieve of Eratosthenes that (8) is satisfied for almost all n, but it seems likely that (8) has no solution for infinitely many n. More generally, for every $p \leqq \sqrt{n}$, write $n = up^2 + v$ with $0 \leqq v < p^2$ and define $\varepsilon_n = \min_{p \leqq \sqrt{n}} \frac{v}{p}$. Almost certainly $\limsup_{n \to \infty} \varepsilon_n = \infty$ (but $\varepsilon_n \to 0$ as $n \to \infty$ for almost all n). Probably $\varepsilon_n < n^\varepsilon$ for $n > n_0(\varepsilon)$ and every $\varepsilon > 0$.

In a previous paper, I studied the number of prime factors of $\binom{n}{k}$. Trivially,

$$v\left(\binom{n}{k}\right) > \log \binom{n}{k} \Big/ \log n . \tag{9}$$

It is easy to see that if $k > n^{1-o(1)}$, then (9) becomes an asymptotic equality and we have

$$v\left(\binom{n}{k}\right) = \big(1 + o(1)\big) \log \binom{n}{k} \Big/ \log n \qquad \big(k > n^{1-o(1)}\big).$$

I conjecture that, for "large" k,

$$v\left(\binom{n}{k}\right) = \big(1 + o(1)\big)k \sum_{k<p<n} \frac{1}{p}.$$

I obtained this conjecture by a simple averaging process. I cannot even prove it if $k > n^\varepsilon$, but perhaps it is true for every $k \geqq (\log n)^c$.

3. I discuss a few miscellaneous problems mostly about consecutive integers. Pomerance and I considered the following problem. Put $A(n, k) = \prod_{1 \leqq i \leqq k} (n+i)$ and denote by $q(n, k)$ the least prime which does not divide $A(n, k)$. Clearly,

$$q(n, k) < \big(1 + o(1)\big)\, k \log n \, . \tag{10}$$

This is clearly very crude. For bounded k and, more generally, for $k = o(\log n)$, the factor $k \log n$ in (10) can perhaps be replaced by $\log n$. An interesting special case is $k = [\log n]$. By choosing n so that it is the product of the primes between $\log n$ and $\big(2 + o(1)\big) \log n$, we see that $q(n, [\log n])$ can be as large as $\big(2 + o(1)\big) \log n$. Is it true that $q(n, [\log n]) < (2 + \varepsilon) \log n$ for $n > n_0(\varepsilon)$? We could not even prove that $q(n, [\log n]) < (1 - \varepsilon)(\log n)^2$. It seems certain that, to every $\varepsilon > 0$, there is a $k(\varepsilon)$ so that the density of integers n for which $P\big(A(n, k(\varepsilon))\big) < n^{1-\varepsilon}$ is less than ε. On probabilistic grounds, one would expect that the density of these integers is asymptotic to

$$\exp\left(-k \sum_{n^{1-\varepsilon} < p < n} \frac{1}{p}\right) = \exp\big(-\big(1 + o(1)\big) k\varepsilon\big)$$

as $n \to \infty$ and $\varepsilon \to 0$, but no sieve method at present applies here. Let $f(c)$ denote the density of integers n for which there is an m with $b < m \leqq n + k$ and $p(m) > e^{ck}$. Using elementary sieve methods, we can prove that $f(c)$ is continuous and strictly decreasing with $f(0) = 1$, $f(\infty) = 0$. This $f(c)$ could, of course, be determined explicitly. Several times during my long life, I was led to questions of the following type. Estimate, as well as you can, the size of the smallest integer $m_n \geqq n$ for which $\prod_{1 \leqq i \leqq n} (m_n + i)$ has no prime factor p satisfying $n < p < 2n$. I would expect that $m_n > n^k$ for every k if $n > n_0(k)$, but that $m_n < e^{\varepsilon n}$ for every $\varepsilon > 0$ if $n > n_1(\varepsilon)$. However, I could prove nothing non-trivial.

To end this section, I state some older problems. I conjectured more than a year ago that if $m \geqq n + k$, then $[n+1, n+2, \ldots, n+k] \neq [m+1, m+2, \ldots, m+k]$ where the square brackets denote least common multiple. Is it true that $\prod_{1 \leqq i \leqq k} (n+i)$ and $\prod_{1 \leqq i \leqq k} (m+i)$ cannot have the same prime factors for $k > 2$ and $m \geqq n + k$, except for a finite number of values of n, m and k? Put

$$\alpha(m, n, k) = \prod_{i=1}^{k} (m+i) \Big/ \prod_{i=1}^{k} (n+i)$$

and assume $k \geqq 2$ and $m \geqq n + k$. Is it true that $\alpha(m, n, k) = I$ is solvable for every integer $I > 1$? Now let n and k be fixed. Can one say anything about the integers of the form $\alpha(m, n, k)$?

Let me restate an old and very attractive conjecture of Turán and myself on the differences $d_n = p_{n+1} - p_n$ between consecutive primes. We easily proved that $d_{n+1} > d_n$ and $d_{n+1} < d_n$ both have infinitely many solutions. Presumably, $d_n = d_{n+1}$

also holds for infinitely many n but this is well-known to be very difficult. We conjectured that all the $k!$ inequalities of the form $d_{n+i_1} > d_{n+i_2} > \dots > d_{n+i_k}$ have infinitely many solutions, where $i_1, i_2, \dots, i_k$ is an arbitrary permutation of $1, 2, \dots, k$. We certainly could not prove this even for $k = 3$. We could not even prove that there is no n_0 so that $d_{n+1} - d_n$ changes sign when n is replaced by $n + 1$ for every $n > n_0$. Perhaps we overlooked a trivial argument; in any case, I offer a hundred dollars for a proof or disproof.

Finally let $B(n)$ (where B stands for Brun) be the smallest integer so that there is a residue a_p for every prime p with $2 \leqq p \leqq B(n)$, and every positive integer $x \leqq n$ satisfies at least one of the congruences $x \equiv a_p (\operatorname{mod} p)$. The exact determination of $B(n)$ is probably hopeless, but a good estimate for $B(n)$ would be of the greatest importance for the application of Brun's method. As far as I know, Iwaniec's result $B(n) > c\sqrt{n}$ is the best lower bound known at present. It would be very nice if one could prove that $B(n) > Cn^{1/2}$ for every C and $n > n_0(C)$. It is likely that $B(n) > n^{1-\varepsilon}$ for every $\varepsilon > 0$ and $n > n_1(\varepsilon)$. The method of Rankin (used to give a lower bound on the difference of consecutive primes) gives

$$B(n) < cn(\log\log\log n)^2/\log n \cdot \log\log n \cdot \log\log\log\log n\,.$$

Recently, I considered the following modification of the above problem. Denote by ε_n the smallest number so that there is a residue b_p for every prime p with $n^{\varepsilon_n} < p \leqq n$, and every positive integer $x \leqq n$ satisfies at least one of the congruences $x \equiv b_p (\operatorname{mod} p)$. Is it true that $\varepsilon_n \to 0$ as $n \to \infty$? I can prove that $\varepsilon_n > c \log\log\log n/\log\log n$. Are there residues c_p for every prime p with $2 \leqq p \leqq n$ so that every positive integer $x \leqq n$ satisfies at least 2 (or at least r) of the congruences $x \equiv c_p (\operatorname{mod} p)$?

4. Proof of Theorem 1. The proof will use a simple averaging process, some of the details of which will be left to the reader. Let $\varepsilon > 0$, k be a sufficiently large integer and A be a multiple of $p_1, p_2, \dots, p_k$. We shall show that the density of integers n which are barriers for d_0 is greater than $(1 - \varepsilon)/A^k$ by considering the integers $n \leqq x$ with $n \equiv 0 (\operatorname{mod} A^k)$. First, we observe that the density of integers t for which

$$d_0(tA^k - i) > i\,, \tag{11}$$

for some i with $1 \leqq i \leqq k$, is less than $\frac{1}{2}\varepsilon$. Indeed, (11) can only hold if $tA^k - i \equiv \equiv 0 (\operatorname{mod} p^2)$ for some $p > p_k$ and this easily implies our assertion for $k > k_0(\varepsilon)$. Next, by a simple computation, we obtain

$$\sum_{t=1}^{x} d_0(tA^k - i)^2 > cd_0(i)\,x\,,$$

and from this, the density of integers t satisfying (11) is less than $cd_0(i)/i^2 < c/i^{3/2}$.

Hence, for $k > k_0(\varepsilon)$, the density of integers t for which (11) holds for some $i > k$ is less than

$$\sum_{i>k} \frac{c}{i^{3/2}} < \frac{\varepsilon}{2}.$$

Thus the density of integers t for which tA^k is not a barrier for d_0 is less than ε. This proves Theorem 1.

With a little more trouble, I can prove that the density of integers n for which n is a barrier for $d_0(n)$ exists. More generally let α_i be the density of integers n for which $\max_{m<n} \big(m + d_0(m)\big) = n + i$. Then α_i exists for every i and $\sum_{i\geqq 0} \alpha_i = 1$. To end the paper, I state a somewhat special problem. Denote by S_i the set of integers m for which the number of solutions of $n + d_0(n) = m$ is i. I believe that it can be proved that the set S_i has a density $\beta_i \geqq 0$ and $\sum_{i\geqq 0} \beta_i = 1$. (I have not carried out the details and perhaps it is more difficult than I think it is). I am not sure that $\beta_i > 0$ always holds, but $\beta_0 > 0$ seems to hold. I certainly cannot settle the analogous questions for $n + v(n)$, $n + d(n)$, $n + \Phi(n)$, or $n + \sigma(n)$.

References

For a collection of some older problems of this and related type, see P. Erdős, "Some recent advances and current problems in number theory", Lectures in modern mathematics (ed. Saaty), vol. 3 (Wiley, New York, 1965), 196—244. This contains an extensive bibliography.

Some more recent problems on consecutive integers are discussed in P. Erdős, "Problems and results on number theoretic properties of consecutive integers and related problems", Proceedings of the 5th Manitoba conference on numerical mathematics (1975). See also P. Erdős, "Problems and results on combinatorial number theory III." Number theory day Proc., New York, 1976, Lecture Notes in Math. 26, Springer Verlag, 43—72, finally P. Erdős, "Some unconventional problems in number theory", will soon appear in Math. Magazine.

(Received April 6, 1978)

MATHEMATICAL INSTITUTE
OF THE HUNGARIAN ACADEMY OF SCIENCES
1053 BUDAPEST, REÁLTANODA U. 13—15.