

SOME PROBLEMS ON NUMBER THEORY

P. ERDÖS

In this little note I discuss mainly problems on prime numbers some of which occupied me for a long time, but I mention also some new questions. The quality of the problems considered will be very uneven, some are more exercises, some certainly serious problems, unfortunately I am not always sure into which category the problems belong.

First I discuss some problem which arose during our meeting. An old and very difficult conjecture of mine states that $(d(n) = d(n+1))$ has infinitely many solutions. It is probably presumptions to call this "my conjecture" it probably was asked long ago. I only call it my conjecture since it is mentioned in one of my papers. Brun's method easily gives that for infinitely many n , $c_1 < d(n)/d(n+1) < c_2$ and in fact the set of limit points of $d(n)/d(n+1)$ contains intervals $[1] [2]$. No doubt the sequence $d(n)/d(n+1)$ is everywhere dense in $(0, \infty)$, but the only limit points known are 0 and ∞ . My original conjecture on $d(n) = d(n+1)$ may very well be unattackable and it was a great surprise to me when Claudia Spiro (unpublished) proved that $d(n) = d(n+5040)$ has infinitely many solutions. It is based on the fact that there are 8 primes p_i , $i=1, \dots, 8$ so that the least common multiple of the differences $p_j - p_i$, $1 \leq i \leq 8$ is 5040. This led Narkiewicz and me to consider the following problem: Denote by $D(p_1, \dots, p_n)$ the least common multiple of the $\binom{n}{2}$ numbers $p_j - p_i$. Put

$$f(n) = \min_{p_1, \dots, p_n} D(p_1, \dots, p_n)$$

and $F(n)$ is the smallest value of $D(p_1, \dots, p_n)$ assumed for infinitely many p_1, p_2, \dots, p_n . We of course can not even prove that $F(2)$ is finite since this would imply that $p_{k+1} - p_k < C$ has infinitely many solutions for some C , but we will assume the prime k -tuple conjecture of Hardy and Littlewood which of course implies $F(n) < \infty$. Put

$$g(n) = \prod_{q < m} q^{\alpha_q}$$

where α_q is the largest integer for which $\phi(q^{\alpha_q}) = (q-1)q^{\alpha_q-1} < n$.

A simple argument shows that $F(n) \geq g(n)$ since if q is not one of the p 's then $q^{\alpha_q} \mid D(p_1, \dots, p_n)$. If q is one of the p 's then $q^{\alpha_q} \mid D(p_1, \dots, p_n)$ if $(q-1)q^{\alpha_q-1} < n-1$. We conjectured that $f(n)/g(n) \rightarrow \infty$ and that $f(n) = g(n)$

is possible only for every small values of n . Very likely $f(n) = F(n)$ for $n > n_0$. We could not even show that $f(8) = 5040$. It could be 2520 if all the 8 p's are incongruent mod 16. We only could exclude this by long computations which we did not carry out. It follows from the prime number theorem that $\log g(n) = (n + o(1))$. We think that perhaps

$$(1) \quad \lim_{n \rightarrow \infty} \frac{\log f(n)}{n} < \infty, \quad \lim_{n \rightarrow \infty} \frac{\log F(n)}{n} < \infty.$$

It might be of some interest to obtain an asymptotic formula for $\log D(2,3,\dots,p_n)$ probably

$$(2) \quad \log D(2,3,\dots,p_n) / n \log n = c, \text{ for some } 0 < c < 1.$$

In a recent letter Claudia Spiro deduced from the prime k -tuple conjecture that

$$(3) \quad F(n) \sim (g(n))^{1+c} \frac{\log \log n}{\log n}.$$

The conjecture $f(n)/g(n) \rightarrow \infty$ remains open. In view of her result (3) it would perhaps be of interest to study

$$\max_{p_1, \dots, p_n} \{ (\max_{1 \leq i \leq n} p_i) D(p_1, \dots, p_n) \} = A_n.$$

Is it true that $A_n^{1/n} \rightarrow \infty$? or at least $A_n > (1+\epsilon)^n$ i.e.

A related function is

$$\min_{p_1, \dots, p_n} \prod_{i=1}^n p_i D(p_1, \dots, p_n) = B_n.$$

$B_n > (n!)^{1+c}$ or $B_n > n!^c$ for every c if $n > n_0(c)$ would perhaps be of some interest.

These problems can be considered for other sequences than the primes

a_1, a_2, \dots, a_n are n square-free numbers what can be said about $\min D(a_1, \dots, a_n)$? At the moment I can say nothing non-trivial about this problem.

Some questions which Nicolas and I considered lead to the following question: let p_1, p_2, \dots, p_n be an arbitrary set of n primes. Is it true that

$$(4) \quad \sum_{1 \leq i < j \leq n} \frac{1}{p_j - p_i} < Cn?$$

(4) is still open. It follows from the prime k -tuple conjecture that (4) if true is best possible i.e. there are infinitely many n -tuples of primes

p_{i_1}, \dots, p_{i_k} for which

$$\sum_{1 \leq j < j' \leq n} \frac{1}{p_{i_j} - p_{i_{j'}}} > Cn.$$

I thought for a while that instead of (4) the following stronger result may hold :
 Let $a_1 < a_2 < \dots < a_n$ be a sequence of integers for which every interval of length t contain for every t fewer than $c_1 t / \log t$ a's . Is it then true that

$$(5) \quad \sum_{1 \leq i < j \leq n} \frac{1}{a_j - a_i} < Cn ?$$

Unfortunately, Ruzsa gave a simple counterexample to (5) . Let the a's be the integers of the form $\sum_{i=1}^s \epsilon_i 2^i$, where $\epsilon_i = 0$ or 1 but $\epsilon_i = 0$ if i is a power of 2 and s is chosen so that $s - \frac{\log s}{\log 2} = \frac{\log n}{\log 2} + O(1)$.

It is easy to see that the a's satisfy our condition but

$$(6) \quad \sum_{1 \leq i < j \leq n} \frac{1}{a_j - a_i} > c n \log \log n$$

(6) contradicts (5) and is easily seen to be best possible. Probably a counterexample to (4) can also be found (i.e. the a's can be chosen to be primes).

Put $d_k = p_{k+1} - p_k$; d_k seems to behave very irregularly. Put

$$D(x) = \max_{p_k < x} (p_{k+1} - p_k) .$$

Cramer [3] conjectured that $\lim_{k \rightarrow \infty} \frac{d_k}{(\log k)^2} = 1$. A slight strengthening of Cramer conjecture states

$$(7) \quad \lim_{x \rightarrow \infty} \frac{D(x)}{(\log x)^2} = 1 .$$

It is quite possible though that Cramer's conjecture holds but (7) is false. (7) in particular would imply that

$$\frac{D(2x)}{D(x)} \rightarrow 1$$

and there certainly is no real evidence that this holds. In fact I suspect that it fails. There is no doubt that every even d is of the form $p_{k+1} - p_k$ but the smallest k for which $p_{k+1} - p_k = d$ probably tends to infinity exponentially in d but I can not prove that it tends to infinity faster than polynomially, perhaps this is not hopeless and I overlook a simple argument.

Denote by $U(x)$ the number of even integers of the form $p_j - p_i$, $3 \leq p_i < p_j \leq x$. $U(x) > cx$ follows immediately by Brun's method, but perhaps, $U(x) > \frac{x}{2} - (\log x)^\alpha$, for some α and all $x > x_0(\alpha)$ and perhaps for infinitely many x : $U(x) > \frac{x}{2} - C$ for some absolute constant C . Both of these conjectures are of course unattainable in the foreseeable future (the second one can perhaps be disproved).

Denote by $V(x)$ the number of integers of the form $a_j - a_i$ where $1 < a_i < a_j \leq x$ are squarefree numbers. $V(x) > x - x^\alpha$ is easy to prove for some $\alpha < 1$, also

$V(x) > x - C$ holds for infinitely many x and it seems to be easy to prove that for every t the density of the integers, for which $V(x) = x - t$, exists and the density of integers for which $V(x) < x - t$ tends to 0 as $t \rightarrow \infty$. The reason for the vagueness of my statement is that I did not think the proof over in all details.

Rankin [4] proved in 1938 that

$$(8) \quad D(x) > c \log x \log \log x \log \log \log x (\log \log \log x)^{-2} = L(x) .$$

Since then the only improvement of (8) was that the original value of c has been replaced by a larger one by Schönhage and Rankin. This fact lead me to offer a reward of 10^4 dollars for a proof that (8) holds for every c and infinitely many x (in fact it no doubt holds for all x). I am so sure that this conjecture is true that I offer 25 000 dollars for a disproof. I really feel like offering 10^6 dollars, but contrary to rumours [5], I never offer a prize if I could not pay it.

Let $H(x)/D(x) \rightarrow \infty$. Is it true that $(\pi(y)$ is the number of primes not exceeding y)

$$(9) \quad \pi(x+H(x)) - \pi(x) = (1+o(1)) H(x)/\log x ?$$

(9) if true, is no doubt unattackable at present. Let $H_1(x)/L(x) \rightarrow \infty$. I noticed that I could not disprove that

$$(10) \quad \pi(x+H_1(x)) - \pi(x) = (1+o(1)) H_1(x)/\log x .$$

H.Meier wrote me that he proved that if (10) holds then $H_1(x) > (\log x)^{1+\epsilon}$. I hope Meier will soon publish the proof of his interesting result. In the mean time Maier in fact proved that $H_1(x)$ must tend to infinity faster than any fixed power of $\log x$. His proof will be published soon. Denote by $A(x)$ the number of distinct integers of the form $p_{k+1} - p_k < x$. Is it true that

$$(11) \quad A(x)/D(x) \rightarrow 0 ?$$

I have no intuition about (11) and it is quite possible that the limit in (11) does not exist. I expect that

$$(12) \quad \max_{p_k < x} \min (p_{k+1} - p_k, p_k - p_{k-1}) / \max_{p_k < x} (p_{k+1} - p_k) \rightarrow 0$$

(12) is certainly true, but is probably very deep. All these questions can be formulated for the sequence $q_1 < q_2 < \dots$ of square-free numbers, unfortunately these questions seem to me nearly as difficult as the questions about primes, with a few exception. It is a simple exercise in the use of the siefe of Eratosthenes that for every d there are infinitely many indices k for which $q_{k+1} - q_k = d$. k probably increases exponentially in d , we can at least show that it does not increases faster. Let $p_1 < p_2 < \dots$ be an infinite sequence of primes, $a_1 < a_2 < \dots$ is the sequence of integers not divisible by any of the p 's.

We can ask the same question about $a_{i+1} - a_i$ but can answer them only if the p 's tend to infinity very fast.

Perhaps we have more chance for success if we consider the integers relatively prime to n . Let $1 = a_1 < \dots < a_{\phi(n)} = n-1$ be the integers relatively prime to n and put $J(n)$ after Jacobstahl [6]:

$$J(n) = \max_{a_i < n} (a_{i+1} - a_i) .$$

Jacobstahl conjectured $J(n) < c(\log n)^2$ and this was proved by Iwaniec [7], but perhaps $J(n) < (\log n)^{1+\epsilon}$, this would require very much better sieve methods than the ones at our disposal at present.

Let n_k be the product of the first k primes, Jacobstahl conjectured that for $m \leq n_k, J(m) < J(n_k)$. Perhaps $J(m) < J(n_k)$ for all $m < n_{k+1}$, with possibly a finite number of exceptions. Clearly $J(n_{k+1}) > J(n_k)$ and probably

$$(13) \quad J(n_{k+1}) - J(n_k) \rightarrow \infty \quad \text{but} \quad J(n_{k+1})/J(n_k) \rightarrow 1 .$$

The second conjecture of (13) seems certain to be true. The following conjecture seems important to me. Let $n_k < x < n_{k+1}$, then

$$(14) \quad J(n_k)/D(x) \rightarrow 0 .$$

(14) seems important to me, all our information on large values of $p_{k+1} - p_k$ comes from our information on $J(n_k)$. I feel confident that (14) is true but see no way of an attack. I offer a record of 1000 dollars for any relevant information on (14) and 3000 dollars for a proof or disproof.

I expect that

$$(15) \quad \max_{1 \leq i < \phi(n_k)} \min(a_{i+1} - a_i, a_i - a_{i-1})/J(n_k) \rightarrow 0 .$$

Perhaps (15) will not be very difficult in any case it should be much easier than (12). (15) certainly is false for almost all integers, but may remain true for the sequence of integers satisfying $\phi(n'_k)/n'_k \rightarrow 0$ i.e. $\prod_{p|n'_k} (1 - \frac{1}{p}) \rightarrow 0$.

It is true that if $H(n)/J(n) \rightarrow \infty$ then

$$(16) \quad \phi_n(x, x+H(n)) = (1+o(1)) \frac{\phi(n)}{n} H(n)$$

where $\phi_n(u, v)$ is the number of integers $u < m < v$ $(m, n) = 1$. (16) is related to (9) but is probably much easier. (16) certainly holds for almost all n but I can not prove it for the n_k 's, but in any case I am sure it is much easier than (9).

An old (more than 40 years) and striking conjecture of mine asserts that there is an absolute constant C so that for every n

$$(17) \quad \sum_{k=1}^{\phi(n)-1} (a_{k+1} - a_k)^2 = c \frac{n^2}{\phi(n)} .$$

Hooley [8] has many nice results on the conjecture (17), but (17) is still open even if we assume that $\phi(n) < cn$.

Now let me state some more conjectures on the integers relatively prime to n . Many of these conjectures become trivial for the integers n which have few prime factors. Therefore we will usually restrict ourselves to state the problems for the integers n_k . Let $r = r(k)$ be the smallest index for which

$$(18) \quad a_{r+1} = J(n_k)$$

i.e. r is smallest index for which $a_{\ell+1} - a_\ell$ assumes its maximum. I am sure that r increases exponentially in k but can not even prove that increases faster than polynomially. I would like to get an estimation for the number of solution of (18), also it is not clear to me that

$$(9) \quad a_{t+1} - a_t = s$$

is solvable for every even $s < J(n_k)$. Perhaps the proof of this will be easy. A formula for the number of solutions and an estimation for the smallest solution would perhaps be of some interest. I just thought of these questions and have to ask for the indulgence of the reader if some of these problems are trivial or false. I conjectured some time ago that if $(a,b) = 1$, $a < b < x$ then

$$(20) \quad \min(J(a), J(b)) < c \log x .$$

(20) is certainly a "serious" conjecture and if true, might give some insight into the mysterious behaviour of $p_{k+1} - p_k$.

A related old conjecture of mine states that if we consider the congruences

$$(21) \quad n \equiv a_p \pmod{p}, \quad p < x,$$

then for every choice of the a_p there always is an integer $n < x$ which satisfies at most one of the congruences (21).

Unfortunately I can make no contribution to the solution of these problems. During our meeting Hildebrandt and I proved that for every $\epsilon > 0$ if $x > x_0(\epsilon)$ one can find congruences

$$(22) \quad n \equiv a_p, \\ \exp(1-\epsilon) \log x \log \log \log x / \log \log x < p < x$$

so that every integer $n < x$ satisfies at least one of the congruences (22), and that this becomes false if in (22) $1-\epsilon$ is replaced by $1+\epsilon$. One could try to make the result more precise by asking for the largest p_1 for which there are con-

gruences (22) for $p_1 \leq p \leq x$ so that every integer $n \leq x$ satisfies at least one of them. The exact determination of p_1 is of course hopeless but no doubt (22) could be made more precise.

Denote by $a_1^{(r)} < a_2^{(r)} < \dots$ the set of integers which have at most r prime factors. It is a simple exercise to prove that for $r = 2$ [9]

$$(23) \quad \overline{\lim} (a_{i+1}^{(r)} - a_i^{(r)}) / \log(a_i^{(r)}) > 0 .$$

I could never prove that the limit in (23) is ∞ , also I could get no satisfactory result for $r > 2$. The limit could very well be 0 for $r > 2$.

Now I would like to restate some old problems of Selfridge and myself [10] which seem interesting to us but which have been completely neglected partly because our paper has been made to some extent obsolete by the results of Hensley and Richards [11]. Let

$$(24) \quad n < a_1 < a_2 < \dots < a_t \leq n+k, \quad (a_i, a_j) = 1, \\ 1 \leq i < j \leq t .$$

The sequence (24) is called complete if for every $n < s \leq n+k$, $(s, a_i) > 1$ for some $1 \leq i \leq t$. Put $\max t = F(n;k)$ and $\min t = f(n;k)$ where the maximum and minimum is to be taken for all complete sequences (24). Consider the four functions

$$\max_n F(n;k), \quad \min_n F(n;k), \quad \max_n f(n;k), \quad \min_n f(n;k) .$$

Our results on $\max F(n;k)$ have been made obsolete by Hensley and Richards, but perhaps it is remarkable that we could only prove

$$25 k^{\frac{1}{2} - \epsilon} < \min F(n;k) < c k (\log \log k)^2 (\log k)^{-2} (\log \log \log k)^{-1} .$$

The upper bound in (25) is clearly related to Rankin's result (8) and will be hard to improve but the lower bound should surely be improved to $k^{1-\epsilon}$ or at least to $k^{1/2+\epsilon}$ perhaps even $\min F(n;k)/k^{1/2} \rightarrow \infty$ would be of some interest.

Both $\max_n F(n;k)$ and $\min_n F(n;k)$ are clearly monotonic but $\max_n f(n;k)$ is not monotonic since $\max_n f(n;6) = 3$ and $\max_n f(n;5) = 4$, this is the only such case we found, but we only computed $\max_n f(n;k)$ for $k \leq 45$. Put

$$(26) \quad \min_n (F(n;k) - f(n;k)) = g(k) .$$

We conjectured that $g(k) \rightarrow \infty$ as $k \rightarrow \infty$. Perhaps (26) can be proved algorithmically and will not be difficult. Clearly all the integers all whose prime factors are $\geq k$ must occur in every complete sequence. Perhaps

$$(27) \quad \lim_{k \rightarrow \infty} \max_n \frac{F(n;k)}{k/\log k} > 1$$

but as far as I know (27) is still open, we only can prove that the \limsup is finite and the $\liminf \geq 1$.

It is trivial that $\min f(n;k) = 2$. Denote by n_k the smallest integer for which $f(n_k;k) = 2$. Trivially $n_k \leq \prod_{p_i \leq k} p_i - k$. We have a non-trivial proof that

for some k there is strict inequality.

Denote further by n'_k the smallest integer for which there are two integers a and b , $n'_k < a < b < n'_k + k$ so that $(n+j, ab) > 1$ for $1 \leq j \leq k$. The difference between n'_k and n_k is that in the definition of n'_k we do not require $(a,b) = 1$.

We show that for all sufficiently large $k < n'_k < \frac{1}{2} \prod_{p < k} p$ and probably

$$n'_k = O\left(\prod_{p < k} p\right).$$

For which k is it true that if $(a,b) = 1$, $1 < b-a = k$, then there always is a c , $a < c < b$ such that $(a,b,c) = 1$? Perhaps for $k > k_0$ there is no such k . If such a k exists then for this k , $n_k = \prod_{p < k} p - k$.

Is there a k so that for some set of k consecutive integers $n+1, \dots, n+k$

$$\left(n+i, \prod_{\substack{j=1 \\ j \neq i}}^k (n+j)\right) = A(n;i)$$

is complete for every i , $1 \leq i \leq k$? Is there a k so that every $A(n;i)$ has more than r distinct prime factors? For $r=0$ every sufficiently large k has this property. This is a well known result of Brauer, Pillai and Szekeres [12]. For $r > 0$ we do not know the answer which may very well be yes for $r=1$ and no for $r > 1$. This problem is related to (23).

In another paper Selfridge and I [13] prove the following surprising theorem: For every $\epsilon > 0$ and k there is a set of k^2 primes $p_1 > \dots > p_{k^2}$ and an interval $I = \{x, x + (3-\epsilon)p_1\}$ so that the number of distinct integers m in I which are multiples of any the p 's is $2k$. This theorem is surprising since one would expect that the number of these integers is $> ck^2$. Since our proof is not easily accessible I give it here in full detail. First we prove that our result is best possible. In fact we show that any interval I' of length $> 2p_1$ contains at least $2k$ distinct multiples of the p 's. This is essentially best possible.

The interval $\left\{ \prod_{i=1}^{k^2} p_i - \frac{p_{k^2}}{k^2} + 1, \prod_{i=1}^{k^2} p_i + \frac{p_{k^2}}{k^2} - 1 \right\}$ has length $2p_{k^2} - 2$ and contains only one multiple of the p 's. Let I' be the interval $\{a,b\}$, $b-a > 2p_1$. I'_1 is the interval $\{a, a + \frac{1}{2}(b-a)\}$ and I'_2 the interval

$\{a + \frac{1}{2}(b-a), b\}$ both of these intervals contains at least

$$\sum_{i=1}^{k^2} \left[\frac{b-a}{2p_i} \right] \geq k^2$$

multiples of the p 's (counted by multiplicity). If no m in I is a multiple of more than k of the p 's then clearly there are at least $2k$ distinct multiples of the p 's in I . Thus assume say that there is an m in I'_1 which is a multiple of $r > k$, p 's, where r is the largest such integer.

Let p_{i_1}, \dots, p_{i_r} , $r > k$ be the prime factors of m . This in I'_1 there are at least $\frac{k^2}{r}$ distinct multiples of the p 's. For every p_{i_j} let s_j be the smallest integer for which $m + 2^{s_j} \cdot p_{i_j}$ is in I'_2 , such an s_j clearly exists, and the numbers $m + 2^{s_j} \cdot p_{i_j}$ are clearly distinct for $j=1, 2, \dots, r$. Thus I' contains at least $r + \frac{k^2}{r} > 2k$ distinct multiples of the p 's which completes the proof.

Now we prove the more difficult statement that there is an I of length $(3-\epsilon)p_1$ which contains no more than $2k$ distinct multiples of the p 's. First we prove a

Lemma.- For every k and arbitrary large N there are k^2 primes

$$N < q_0 < q_1 < \dots < q_{k^2-1} < N + (\log N)^{k+3}$$

satisfying for every $1 \leq i \leq k-1$, $1 \leq j \leq k-1$

$$q_i - q_0 = q_{i+tk} - q_{tk}.$$

In others words there are k sets of k primes whose internal structure is the same. Probably very much more is true: there is an $f(k)$ and infinitely many primes p so that all the numbers $p + t f(k)$, $0 \leq t < k^2$, are primes - in fact consecutive primes. Needless to say it is quite hopeless at present to prove this conjecture and fortunately we do not need it.

The proof of the Lemma is by a simple counting argument. It followq from the prime number theorem (or a more elementary theorem) that for every large x there is an interval of length $L > (4k \log x)^{k+2}$ between $\frac{x}{2}$ and x which contains more than $\frac{L}{2 \log x}$ primes. Denote these primes by

$$y < r_1 < r_2 < \dots < r_w < y+L, \quad w > \frac{L}{2 \log x}.$$

Consider the $\left[\frac{w-1}{k} \right]$ intervals $[r_{(u-1)k+1}, r_{uk+1}]$, $uk+1 < w$. We only retain those intervals which are shorter than $4k \log x$. Clearly there are at least

$L(4k \log x)^{-1}$ such intervals. The number of patterns for the k primes $r_{(u-1)k+1}, r_{(u-1)k+2}, \dots, r_{uk}$ in these intervals is clearly less than $(4k \log x)^{k+1}$. Thus for sufficiently large x there are more than k k -tuples of primes giving the same pattern, which completes the proof of our Lemma. Now using the Chinese remainder theorem we are ready to complete the proof of our theorem. Put

$$\alpha_i = \prod_{j=0}^{k-1} q_{ik+j}, \quad \beta_j = \prod_{i=0}^{k-1} q_{ik+j}, \quad 1 \leq i, j \leq k-1.$$

Clearly

$$\prod_{i=0}^{k-1} \alpha_i = \prod_{j=0}^{k-1} \beta_j = \prod_{\ell=0}^{k^2-1} q_{\ell}.$$

Now we determine $x \pmod{\prod_{\ell=0}^{k^2-1} q_{\ell}}$ as follows :

$$x+q_j \equiv 0 \pmod{\beta_j}, \quad x+q_0 \equiv q_{jk} \pmod{\alpha_j}, \quad 0 \leq j \leq k-1.$$

A simple argument shows that the interval $\{x-q_0+1, x+2q_0-1\}$ of length $3q_0-2 > (3-\epsilon) \prod_{\ell=0}^{k^2-1} q_{\ell}$ contains only $2k$ multiples of the q 's namely the unique multiples of $\alpha_0, \alpha_1, \dots, \alpha_{k-1}; \beta_0, \beta_1, \dots, \beta_{k-1}$.

Let now again $p_1 > p_2 > \dots > p_{k^2}$, and I an interval of length $\geq 3p_1$. Unfortunately here so to speak "all hell breaks loose" and we completely lose control over the distinct multiples of the p 's. It is quite possible that in this case I contains more than $c k^2$ distinct multiples of the p 's. I can only prove the following much weaker theorem.

Let $p_1 > \dots > p_{k^2}$, and I an interval of length $\geq 3p_1$. Then I contains at least $6^{1/2} k$ distinct multiples of the p 's.

Clearly the interval I contains at least $3k^2$ multiples of the p 's, counted by multiplicity. Let r be the largest integer so that there is an m in I which is the multiple of r p 's say $m \equiv 0 \pmod{p_{\ell_1}, \dots, p_{\ell_r}}$.

Each p_{ℓ_j} , $j=1, \dots, r$ has at least two other multiples in I (namely $m \pm p_{\ell_j}$ or $m+p_{\ell_j}, m+2p_{\ell_j}$ or $m-p_{\ell_j}, m-2p_{\ell_j}$). These $2r+1$ multiples of the p 's are clearly all distinct. Thus I contains at least

$$\min\left(\frac{3k^2}{r}, 2r+1\right) > 6^{1/2} k$$

distinct multiples of the p 's, which completes our proof of our theorem.

I am sure that this result is not best possible. Perhaps the following related pro-

blem is also interesting : Determine the smallest $f(u)$ so that if $p_1 > \dots > p_u$ are primes, every interval of length $f(u)p_1$ contains an integer divisible by precisely one of the p 's . Clearly many related questions can be asked.

Denote by I_n the interval $(\frac{n}{3}, \frac{n}{2})$ and by $f(x,n)$ the number of integers m , $x < m < x+n$ which have at least one prime factor in I_n . An old conjecture of mine states

$$(28) \quad f(x,n) > cn/\log n .$$

It seems ridiculous that I have not been able to make any progress with (28) and I am not sure if I am just being silly and overlook an obvious point or whether (28) is really difficult or at least requires a clever idea. It is easy to see that the number of integers having at least two prime factors in $\{x,x+n\}$ is at most

$$\frac{1}{2} (\pi(\frac{n}{2}) - \pi(\frac{n}{3})) = (1+o(1)) \frac{n}{12 \log n}$$

and that equality is possible here, also $f(x,n) \leq 2(\pi(\frac{n}{2}) - \pi(\frac{n}{3}))$ for suitable values of x and equality is again possible, but I would only prove

$f(x,n) > c \left(\frac{n}{\log n}\right)^{1/2}$. It is not difficult to show that there is an absolute constant C so that if $n \rightarrow \infty$ then for almost all x

$$f(x,n) = (C+o(1)) \frac{n}{\log n}$$

and with a little more trouble one could obtain results on the distribution function of the error $f(x,n) - C \frac{n}{\log n}$. None of this seems to help with (28) .

To finish the paper let me just state a few older problem. Denote by p_1, p_2, \dots the sequence of primes. Prachar and I [14] conjectured that the number of indices k for which for every $i < k < j$

$$(29) \quad p_i/i < p_k/k < p_j/j$$

is finite.

(29) seems very plausible and it probably holds for many other sequences e.g. for the primes $p \equiv a \pmod{b}$ or for the set of integers not divisible by a set of primes $\sum 1/p_i = \infty$ where the complementary set q_i also satisfies $\sum 1/q_i = \infty$. In fact (29) should hold if $a_k/k \rightarrow \infty$ but not too fast and a_k is not too regular. These rather vague statements of course do not really help and it must be left open whether any non-trivial statement related to (29) can be made and proved.

More than 25 years ago I made the following (foolish) conjecture.

Let $a_1 < a_2 < \dots < a_k \leq n$, $\prod_{i=1}^k 1/a_i \leq 1$. Is it then true that the number of

integers not exceeding n which are not divisible by any of the a_i 's is $> cn$. This was disproved by Schinzel and Szekeres [15] and more recently Ruzsa and Tenenbaum proved that the number of these integers is $> c_1 \frac{n}{\log n}$, but can be less than $c_2 n / \log n$.

Let $p_1 < p_2 < \dots < n$ be a sequence of primes for which $\sum 1/p_i \leq 1$. Then it is easy to see that there are cn integers no one of which is a multiple of any of the p_i 's $\leq n$. It will perhaps not be difficult to determine the smallest possible value of c .

One of the most interesting unconventional problems of primes is due to Ostman: Prove that one can not find two sequences $a_1 < a_2 < \dots$, $b_1 < b_2 < \dots$ of at least two elements so that all but a finite number of primes are of the form $a_i + b_j$ and only a finite number of composite numbers are of the form $a_i + b_j$, in other words the symmetric difference of the primes and the integers of the form $a_i + b_j$ must be infinite. This striking conjecture is still open. Hornfeck [16] proved it in the case that one of the sequence $a_1 < a_2 < \dots$ or $b_1 < b_2 < \dots$ is finite.

It follows from the prime k -tuple conjecture that there are two infinite sequences $a_1 < a_2 < \dots$, $b_1 < b_2 < \dots$ so that all the sums $a_i + b_j$ are primes. It seems certain that at least one of these sequences must tend to infinity at least exponentially. By the way it seems certain that if there are only a finite number of composite numbers among the $a_i + b_j$ then there are only $(\frac{x}{\log x})$ primes $p < x$ of the form $a_i + b_j$ which would be much stronger than Ostmans conjecture. Since the analog of the prime k -tuple conjecture clearly holds for the squarefree numbers it is easy to see that there are infinite sequences $a_1 < a_2 < \dots$, $b_1 < b_2 < \dots$ so that all the integers $a_i + b_j$ are squarefree. Perhaps it is true that if all but a finite number of the $a_i + b_j$ are squarefree and both sequences a_i and b_j are infinite then the number of squarefree integers of the form $a_i + b_j$ is $\sigma(x)$, or even slightly stronger $A(x) B(x) = \sigma(x)$ where $A(x) = \sum_{a_i < x} 1$, $B(x) = \sum_{b_j < x} 1$.

Pomerance once asked: Is there a subsequence of the primes $p_{i_1} < p_{i_2} < \dots$ whose second difference $p_{i_r} - 2p_{i_{r+1}} + p_{i_{r+2}}$ is bounded from above (or bounded in absolute value). Probably such a sequence does not exist, not even if the primes are replaced by the squarefree numbers, but I do not see how to attack these questions.

About 30 years ago, Ricci and I [17] proved that the set of limit points of $(p_{k+1} - p_k) / \log k$ is of positive Lebesgue measure. Unfortunately ∞ is the only limit point of this set known to us. Can one prove that this set has a finite limit point ≥ 1 ?

Perhaps the following somewhat vague conjecture is not hopeless : Let $H(x)/\log x \rightarrow \infty$ smoothly but $H(x) < L(x)$ (see (8)) . Is it then true that the set of limit points of $(p_{k+1} - p_k) / H(k)$ have positive measure ? Is there for every C an index k for which

$$C \log x < p_k - p_{k-1} < p_{k+1} - p_k, p_k < x ?$$

Finally I state a somewhat unconventional problem which was considered by Pomerance and myself. Straus and I once conjectured that if $k > k_0$ then there always is an i for which

$$(30) \quad p_k^2 < p_{k+i} p_{k-i} .$$

Pomerance [18] disproved this, in fact he disproved this for much more general sequences. We tried unsuccessfully to prove that in fact for almost k (30) in fact holds. It would suffice to show that for almost all k there is an i for which

$$(31) \quad 2p_k > p_{k+i} + p_{k-i}, p_{k+i} < p_k + p_k^{1/2}$$

but we could not prove (31). Is it true that the number of distinct integers of the form $p_{n+i} + p_{n-i}$, $i = 1, 2, \dots$ is $> cn/\log n^2$? It easily follows from the sharper form of the prime number theorem that the number of solutions of

$A = p_{n+i} + p_{n-i}$ in i is bounded if $n \rightarrow \infty$, but we can show this only for the A 's in the neighborhood of $2p_n$.

Pomerance and I further considered the following problems : Is it true that for $n > n_0$ there always is an i for which $2p_n = p_{n+i} + p_{n-i}$? The answer is almost certainly affirmative. Is it true that there is a c so that infinitely many i and every $i < n$

$$p_{n+i} + p_{n-i} - 2p_n > -c ?$$

Put

$$M(n) = \max_i p_{n+i} p_{n-i} .$$

Is it true that there is an $\alpha > 0$ so that for infinitely many n

$$(32) \quad M_n > p_{n+i} p_{n-i} + n^\alpha ,$$

and if the answer is affirmative try to determine the largest α for which (32) holds for infinitely many n .

Finally I would like to remark that (17) leads to interesting and deep problems for other sequences e.g. let $q_1 < q_2 < \dots$ be the sequence of consecutive squarefree numbers. Is it true that for every α

$$(33) \quad \sum_{q_n < x} (q_{n+1} - q_n)^\alpha < c_\alpha x ?$$

I proved (33) for every $\alpha \leq 2$ and Hooley [16] proved it for every $\alpha \leq 3$ (Hooley just informed me that he can prove it for every $\alpha \leq 3+\epsilon$ for some small positive ϵ . If (33) holds for every α then for every $\epsilon > 0$ and $n > n_0(\epsilon)$, $q_{n+1}-q_n < q_n^\epsilon$. Thus (33) if true is probably very deep. I could not disprove the following much stronger conjecture

$$(34) \quad \sum_{q_n < x} \exp C(q_{n+1} - q_n) < \alpha_C x .$$

(34) if true is completely beyond our reach, but perhaps (34) can be disproved.

Recently Heath-Brown (by using and further developing the method of Claudia Spiro) proved that the number of solutions of $d(n) = d(n+1)$, $n < x$, is greater than $c x(\log x)^{-?}$. The problem on $d(n) = d(n+1)$ is in fact a joint problem of mine with L. Missky (see P. Erdős and L. Missky, On the distribution of values of the divisor function $d(n)$, Proc. London Math. Soc. 3(1952),257-271).

*
* *

REFERENCES.

- [1] P. Erdős, Some remarks on Euler's ϕ -function, Acta Arith. 4 (1958) , 10-19.
- [2] For a more detailed proof of these statements see a forthcoming paper of Pomerance, Sárközy and myself.
- [3] H. Cramer, On the order of magnitude of the difference between consecutive prime numbers, Acta Arith. 2 (1937) , 23-46.
- [4] R.A. Rankin, The difference between consecutive prime numbers, J. London Math. Soc. 13 (1938) , 242-247.
- [5] See P.D.T. A. Elliott, Probabilistic Number Theory , Springer Verlag 1980, Vol. 1, p. 254.
- [6] P. Erdős, On the integers relatively prime to n and on a number theoretic function considered by Jacobstahl, Math. Scand. 10 (1962) , 163-170.
- [7] Iwaniec, On the problem of Jacobstahl, Demonstratio Mathematica 11 (1978), 1-7.
- [8] C. Hooley, On the differences of consecutive numbers relatively prime to n , I, II and III , Acta Arith. 8 (1963/6) ; Publ. Math. Debrecen 12 (1969) , 39-49; Math. Zeitschrift 90 (1965) , 355-369.
- [9] P. Erdős , Problem 237 in Elemente der Mathematik 10 (1955).
- [10] P. Erdős and T. Selfridge, Complete prime subsets of consecutive integers, Proc. Manitoba Conf. 1971, 1-14.
- [11] Hensley and I. Richards, Primes in intervals, Acta Arithmetica 25 (1973), 375-391, see also P. Erdős and I. Richards, Density functions for prime and relatively prime numbers, Monatshefte Math. 83 (1977) , 99-112.
- [12] R.I. Evans, On blocks of consecutive integers, Amer. Math. Monthly 76 (1969), 48-49.

- [13] P. Erdős, Problems and results in combinatorial analysis and combinatorial number theory, Proceedings of the Ninth Southeastern Conference on Combinatorics Graph Theory and Computing 1978, 29-40.-
See also a related problem of Suranyi and myself : P. Erdős and J. Suranyi, Remarks on a problem of a mathematical competition (in Hungarian) Math. Lapok, X (1959), 39-47.
- [14] P. Erdős and K. Prachar, Sätze und Probleme über $p_{h/k}$. Abhandlungen Math.Sem. Hamburg, 25 (1961-62), 251-256.
- [15] A. Schinzel and Szekeres, Sur un problème de Paul Erdős, Acta Sci. Math. Szeged 20 (1959), 221-229.
- [16] C. Hooley, On the distribution of squarefree numbers, Canada J. Math. 25 (1973), 1216-1223.
- [17] 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), 93-106. Liège and Paris. My paper appeared in the lectures notes of a conference held in 1955 at Lake Como, Italy, this paper has not been reviewed and is not easily accessible.
- [18] C. Pomeranie, The prime number graph, Math. Comp. 33 (1979), 399-408.

*

* *

P. ERDÖS
Mathematical Institute of the
Hungarian Academy of Sciences
BUDAPEST 1395, PF 428