ON AN ELEMENTARY PROBLEM IN NUMBER THEORY

Paul Erdős

(received October 26, 1957)

A question which Chalk and L. Moser asked me several years ago led me to the following problem: Let 0 < \( x \leq y \). Estimate the smallest \( f(x) \) so that there should exist integers \( u \) and \( v \) satisfying

\[
0 \leq u, v < f(x), \text{ and } (x+u, y+v) \equiv 1. \tag{1}
\]

I am going to prove that for every \( \epsilon > 0 \) there exist arbitrarily large values of \( x \) satisfying

\[
f(x) > (1-\epsilon)(\log x/\log\log x)^{1/2}, \tag{2}
\]

but that for a certain \( c > 0 \) and all \( x \)

\[
f(x) < c \log x/\log\log x. \tag{3}
\]

A sharp estimation of \( f(x) \) seems to be a difficult problem. It is clear that \( f(p) = 2 \) for all primes \( p \).

I can prove that \( f(x) \to \infty \) and \( f(x)/\log\log x \to 0 \) if we neglect a sequence of integers of density 0, but I will not give the proof here.

First we prove (2). Let \( p_1 < p_2 < \ldots \) be the sequence of consecutive primes. Let \( k > 0 \) be an arbitrary integer. Put \( (1 \leq i \leq k) \)

\[
A_i = \prod p_j, \quad (i-1)k < j \leq ik,
\]

and

\[
B_i = \prod p_j, \quad j \equiv 1 \pmod{k}, \quad 0 < j \leq k^2.
\]

Clearly

\[
\prod_{i=1}^{i=k} A_i = \prod_{i=1}^{i=k} B_i = \prod_{j=1}^{j=k} p_j.
\]

Thus the system of congruences \((1 \leq i \leq k)\)

\[
(A_1 \equiv A_2 \pmod{k}, B_1 \equiv B_2 \pmod{k} = 1, (A_1, B_2) \neq 1.
\]

Thus the system of congruences \((1 \leq i \leq k)\)

\[ x + 1 - 1 \equiv 0 \pmod{A_1}, \quad 0 < x < \prod_{j=1}^{K_2} P_j; \]
\[ y + 1 - 1 \equiv 0 \pmod{B_1}, \quad \prod_{j=1}^{K_2} P_j < y < 2 \prod_{j=1}^{K_2} P_j \]

has a unique solution in integers \( x \) and \( y \). Clearly, if \( 0 \leq i_1, i_2 < k \), then
\[
(x + i_1, y + i_2) = P(i_1 - 1)k + i_2 > 1.
\]

Thus \( f(x) \geq k \). From the prime number theorem we have
\[ p_n = (1 + o(1))n \log n. \]
Thus
\[ x < \prod_{j=1}^{K_2} P_j < \exp(2(1+\varepsilon)k^2 \log k), \]
hence (2) follows.

To prove (3) let \( n \) be such that for all \( 0 \leq u, v < n \),
\[ (x + u, y + v) > 1. \]
We first remark that if \( p \leq n \), then
the number of pairs \( 0 \leq u, v < n \), for which
\[ (x + u, y + v) \equiv 0 \pmod{p}, \]
is less than
\[
(n/p + 1)^2 \leq n^2/p^2 + 3n/p.
\]
Thus the number of pairs \( 0 \leq u, v < n \), for which
\[ (x + u, y + v) \]
has a prime factor not exceeding \( n \), is less than
\[
\frac{n^2}{2} \sum_{p \leq n} \frac{1}{p^2} + 3n \sum_{p \leq n} \frac{1}{p} = (1 + o(1)) \frac{n^2}{2} \sum_{p \leq n} \frac{1}{p^2} < 3n^2/4
\]
for sufficiently large \( n \).
\[
(\frac{n^2}{2})^{1/p^2} < 1/4 + \sum_{k=1}^{\infty} 1/k(k+1) = 3/4.
\]
Thus for at least \( n^2/4 \) pairs \( 0 \leq u, v < n \),
\[ (x + u, y + v) \]
must have a prime factor greater than \( n \).
But if \( p > n \) then there is at most one \( 0 \leq u, v < n \)
with \( (x + u, y + v) \equiv 0 \pmod{p} \). Thus \( \prod_{i=0}^{n-1} (x+1) \)
must have at least \( n^2/4 \) distinct prime factors greater than \( n \).
Hence \( n < x \)
\[
(2x)^n > \prod_{i=0}^{n-1} (x+1) > n^{n^2/4};
\]
thus \( \log 2x > n/4 \log n \), or \( n < c \log x/\log\log x \),
which proves (3). By a slightly more careful computa-
tation it is easy to show that for sufficiently large $x$, $f(x) < (\pi^2/12 + \varepsilon)\log x/\log\log x$, and by a little more sophisticated but still elementary reasoning I can show that $f(x) < (1/2 + \varepsilon)\log x/\log\log x$. Any further improvement of the estimation of $f(x)$ from above or below seems difficult.

It can be remarked that to every $x$ and $n$ there exists a $y$ so that $(x+i,y+i) > 1$ for $0 \leq i \leq n$. To see this it suffices to put $y = x + n!$. On the other hand one can show by using Brun's method that there exists a constant $c$ so that, for some $0 \leq i < (\log y)^c$, $(x+i,y+i) = 1$. To see this observe that every common factor of $x+i$ and $y+i$ must divide $y-x$. Thus if $i$ is chosen so that $(x+i,y-x) = 1$, then $(x+i,y+i) = 1$. Now it follows from Brun's method that there exists a constant $c$ so that, for every $n$, $(\log n)^c$ consecutive integers always contain an integer relatively prime to $n$. Putting $n = y-x$ we obtain our result.

By similar methods as used in the proof of (3) we can prove the following

THEOREM. Let $g(x)(\log x/\log\log x)^{-1} \to \infty$, $0 < x < y$. Then the number of pairs $0 \leq u,v < g(x)$ satisfying $(x+u,y+v) = 1$ equals $(1+o(1))(6/x^2)g^2(x)$.

To outline the proof of our theorem we split the pairs $u,v$ satisfying

\begin{equation}
0 \leq u,v < g(x), \quad (x+u,y+v) > 1
\end{equation}

into three classes. In the first class are those for which $(x+u,y+v)$ has a prime factor not exceeding $p_k$, where $k$ tends to infinity sufficiently slowly. In the second class are those for which $(x+u,y+v)$ has a prime factor in the interval $(p_k,g(x))$, and in the third class are those where all prime factors are
greater than \( g(x) \).

As can be easily seen by a simple sieve process, the number of pairs in the first class is

\[
(5) \quad (1+o(1))(1-\pi^2/6)g^2(x).
\]

As in the proof of (3) we show that the number of pairs in the second class is less than

\[
(6) \quad (1+o(1))g^2(x)\sum_{p \leq x_1} \frac{1}{p^2} = o(g^2(x)).
\]

Denote by \( t \) the number of pairs in the third class. As in the proof of (3) we have

\[
(7) \quad (2x)^{g(x)} > \prod_{i=0}^{g(x)-1} (x+1) > g(x)t,
\]

or

\[
t < g(x)\log 2x/\log g(x) = o(g^2(x))
\]

since \( g(x)(\log x/\log\log x)^{-1} \rightarrow \infty \). (5), (6) and (7) imply that the number of pairs \( u \) and \( v \) satisfying (4) is of the form \( (1+o(1))(\pi^2/6)(g^2(x)) \), which proves the theorem.

We can show by methods used in the proof of (2) in our theorem that we cannot have \( g(x) \) less than \( c(\log x/\log\log x)^{1/2} \), i.e., \( g(x)(\log x/\log\log x)^{-1/2} \rightarrow \infty \) is necessary for the truth of our theorem. An exact estimation of \( g(x) \) seems difficult.

University of Toronto

* L. Moser informs me that he independently obtained this result and its generalization to an m-dimensional lattice.