ACTA ARITHMETICA XXV (1974)

Primes in intervals

by

DOUGLAS HENSLEY and IAN RICHARDS (Minneapolis, Minn.)

0. Introduction. This paper is concerned with the number of primes lying in an interval $y < n \le y + x$ of length x, and especially with the way that this number behaves when x is held fixed and y approaches infinity. In standard notation, the number of primes in (y, y + x] can be written as $\pi(y+x) - \pi(y)$. (Here and below, x and y denote integers ≥ 2 ; an "interval" is viewed as a sequence of integer points, and the "length" is just the number of these points.) It has been conjectured that no interval of length x contains more primes than the first x integers, i.e. that $\pi(y+x) - \pi(y) \le \pi(x)$, or more symmetrically:

(A)
$$\pi(x+y) \leqslant \pi(x) + \pi(y)$$
 for $x, y \geqslant 2$.

In this paper we give strong evidence against the assertion (A). More precisely, we show that (A) is incompatible with (B) the "prime k-tuples conjecture" (definition to follow), so that at least one of these conjectures must be false. (We believe that (B) is true, and (A) false.)

The "prime k-tuples conjecture" (B) is a special case of Schinzel's "Hypothesis H" (cf. [15]). An exact statement is given in Section 1. Roughly speaking, Hypothesis H asserts that k-tuples of polynomials which seemingly "could" take prime values infinitely often, actually do so. Our conjecture (B) is the monic linear case, corresponding to pairs like X, X+2 or X, X+50, triples X, X+2, X+6, etc.

EXAMPLE. The triple X, X+2, X+6 takes the prime values 5, 7, 11 or 11, 13, 17 or 17, 19, 23 when X=5 or 11 or 17. We believe, but cannot prove, that this happens infinitely often. [The k-tuples required for our work are much more complicated, and involve much larger values of k, and then the existence of even *one* prime k-tuple of the desired type is not easy to demonstrate by crude computation — more on this below.]

The inequality (A) is symmetric in x and y, and hence there is no loss of generality in assuming that $x \le y$. On the other hand, (A) can be written $\pi(y+x) - \pi(y) \le \pi(x)$. Thus it is natural to

consider the function

$$\varrho_1(x) = \max_{y \geqslant x} [\pi(y+x) - \pi(y)].$$

In words, $\varrho_1(x)$ denotes the maximum number of primes in any interval $y < n \le y + x$ of length x, beginning with a point y + 1 > x. The conjecture (A) asserts that $\varrho_1(x) \le \pi(x)$ for $x \ge 2$.

Remark. The function ϱ_1 is adequate for discussing most questions about primes in intervals, and the condition $y \geqslant x$ does not impose a vital limitation. For example, any result of the type $\varrho_1(x) \leqslant a\pi(x)$ with constant $a \geqslant 1$, $x \geqslant x_0$ implies $\pi(y+x) - \pi(y) \leqslant a\pi(x)$ for all $x, y \geqslant x_0$. The reason for requiring $y \geqslant x$ is that this makes the function ϱ_1 compatible with sieve estimates, by avoiding such exceptional configurations as the pair 2, 3 or the triple 3, 5, 7, which can occur only near the beginning of the sequence of primes. Some further remarks along these lines are given at the end of Section 1.

We review briefly the present state of knowledge concerning $\varrho_1(x)$. As noted above, the conjecture (A) is equivalent to the assertion that $\varrho_1(x) \leq \pi(x)$ for $x \geq 2$. Schinzel and Sierpiński [15] showed that this holds for $x \leq 132$, and Schinzel [14] extended it to $x \leq 146$; Selfridge and his associates have an unpublished verification running to several hundred.

However our purpose is to disprove (A), and for this we need lower bounds for $\varrho_1(x)$ which eventually become greater than $\pi(x)$. As a first attempt, we might try the relationship $\varrho_1(x) \geqslant \pi(2x) - \pi(x)$, which is obvious from the definition of ϱ_1 . The quantity $\pi(2x) - \pi(x)$ is asymptotic to $\pi(x)$, but unfortunately it is also smaller than $\pi(x)$ for all x. (For large x, this follows, as Landau [8] observed, from de la Vallée Poussin's sharp form of the Prime Number Theorem; and Rosser, Schoenfeld, and Yohe [13] have demonstrated that it holds for all $x \geqslant 2$.)

Now, rather curiously, the fact that $\pi(2x) < 2\pi(x)$, which spoils the first attempt above, also provides the key to the solution. We will use the equivalent form $2\pi(x/2) > \pi(x)$, and bound $\varrho_1(x)$ below by something which is close to $2\pi(x/2)$. More precisely, assuming the prime k-tuples conjecture, we will show that

$$\varrho_1(x) \geqslant \pi(x) + (\log 2 - \varepsilon) [x/(\log x)^2]$$
 when $x \geqslant x_0$.

Thus the true state of affairs, assuming the prime k-tuples hypothesis, is that $\varrho_1(x) < \pi(x)$ for small x, the two functions cross once or several times, and then $\varrho_1(x)$ becomes and remains greater than $\pi(x)$. Our computer experiments suggest that the crossover occurs between 10^3 and 10^5 .

Recall that $\varrho_1(x)$ is the maximum number of primes in any interval $(y, y+x], y \ge x$. By computing actual primes, Segal [16] has shown that

 $\pi(x+y) \leqslant \pi(x) + \pi(y)$ when both x and y are $\leqslant 10^5$. Our results indicate that probably $\varrho_1(10^5) > \pi(10^5)$, which means there is some y with $\pi(y+10^5) > \pi(y) + \pi(10^5)$. We suggest, however, that the values of y involved are so large that an explicit pair x, y satisfying $\pi(x+y) > \pi(x) + \pi(y)$ will never be computed. (For a further discussion of these points, cf. Section 3.)

Schinzel has found a modification of our argument, which requires still another conjecture, but suggests that the difference $\varrho_1(x) - \pi(x)$ grows "faster than $O[x/(\log x)^2]$ ". The authors had previously believed that their method gave the maximum order of growth for $\varrho_1(x) - \pi(x)$, but this now seems extremely improbable. We return to these questions in Section 4.

So far we have given lower bounds for $\varrho_1(x)$. In the opposite direction, the strongest results to date have been obtained by Montgomery [10] and Montgomery and Vaughan [11], using the large sieve. They prove that $\varrho_1(x) \leqslant 2\pi(x)$ for all $x \geqslant 2$, and slightly more is true when x is large. It seems likely that $\varrho_1(x) \sim \pi(x)$, but this awaits further investigation. Such questions are difficult; even the relation $\varrho_1(x) \leqslant \operatorname{Const} \pi(x)$, first proved by means of the Brun sieve, is far from obvious (cf. [4]).

A note of thanks. The present paper gives an example of theoretical research which was aided by a computer, even though ultimately the computer could be dispensed with. To study the function $\varrho_1(x)$ we employ a related function $\varrho^*(x)$ (definition below), which, unlike $\varrho_1(x)$, can be calculated in a finite number of steps. (The prime k-tuples hypothesis implies $\varrho^*(x) = \varrho_1(x)$, and it is for this that we need the hypothesis.) Originally we used the computer to seek k-tuples which would give $\varrho^*(x) > \pi(x)$ and thus, on the k-tuples hypothesis, provide a counter-example to (A). Our first results, working with sequences of up to 100 000 points, were all negative (although it now appears that the number 10^5 is large enough, and our method was defective). Trying to find a better strategy, we eventually found a theoretical argument, valid for all large x.

Here a word of thanks: William Franta and Richard Franta of the computer sciences department and the computer center wrote the program for us. It was necessary to go into machine language in order to handle a sequence of 10⁵ bits without taking too much computer time and memory space. The 100000 bits were packed into around 3000 words by using 32 bits in each 60-bit word. We would probably never have come to a theoretical solution without the insight provided by the computer search.

We also wish to thank Professors Erdös, Bateman, Schinzel, Montgomery, and S. A. Burr who made numerous suggestions for improving our manuscript. Montgomery, in particular, gave us a point by point critique, which we have drawn on liberally in preparing the present version.

379

1. Principal definitions. Henceforth we will study a function $\varrho^*(x)$ which *probably* coincides with $\varrho_1(x)$; it does so, at any rate, if the prime k-tuples conjecture is true. We show (without using any conjectures) that $[\varrho^*(x) - \pi(x)] \to +\infty$ as $x \to \infty$. It is useful to consider three functions (we repeat the definition of ϱ_1).

$$\varrho(x) = \limsup_{y\to\infty} [\pi(y+x) - \pi(y)].$$

$$\varrho_1(x) = \max_{y > x} [\pi(y+x) - \pi(y)].$$

 $\varrho^*(x)$ = the maximum number of integers in any interval y < n $\leqslant y + x$ (with no restriction on y) which are relatively prime to all positive integers $\leqslant x$.

Our main result, proved in Section 2, is that

$$[\rho^*(x) - \pi(x)] \to \infty$$
 as $x \to \infty$,

and moreover

$$\varrho^*(x) - \pi(x) \geqslant (\log 2 - \varepsilon) [x/(\log x)^2]$$
 for $x \geqslant x_0$.

In this section, we will consider what that result implies about primes.

Clearly $\varrho(x) \leq \varrho_1(x) \leq \varrho^*(x)$, and we shall see below, that if the prime k-tuples conjecture is true, then $\varrho^*(x) \leq \varrho(x)$, closing the circle. The function ϱ represents the maximum value which recurs infinitely often as the number of primes in an interval of length x. Thus if $\varrho(x) = \varrho^*(x)$, then we have the corollary $(-A^*)$ in Section 2, that for all sufficiently large x, there exist infinitely many values of y, where $\pi(x+y) > \pi(x) + \pi(y)$.

There is an alternative definition of $\varrho^*(x)$, based on "sieves", which has certain advantages. Let us call a set $b_1 < b_2 < \ldots < b_k$ of integers admissible if:

(*) For each prime p, there is some congruence class (mod p) which contains none of the integers b_i .

Thus to form an admissible sequence on an interval of length x, we must eliminate one congruence class (mod 2), then one class (mod 3), one class (mod 5), etc. until the next prime exceeds the number of points which remain. Now a typical Chinese Remainder Theorem argument shows that

 $\varrho^*(x)$ is the maximum size k of any admissible k-tuple $b_1 < b_2 < \ldots < b_k$ on an interval $y < b_i \le y + x$ of length x.

Since "admissibility" is translation invariant, we can take y=0 without loss of generality. Thus the above gives an effective method for com-

puting $\varrho^*(x)$. Furthermore it shows that $\varrho^*(x)$ is a nondecreasing function of x, and that $\varrho^*(x+y) \leq \varrho^*(x) + \varrho^*(y)$ for $x, y \geq 1$.

Now the significance of $\varrho^*(x)$ is that it represents the maximum "possible" size for prime k-tuples on intervals of length x. The following conjecture asserts that this size is actually attained.

PRIME k-TUPLES CONJECTURE (the monic linear case of Schinzel's Hypothesis H; ef. [15]).

(B) Let $b_1 < b_2 < ... < b_k$ be any admissible sequence in the sense of (*) above. Then there exist infinitely many integers n > 0 for which all of the numbers $n + b_1, ..., n + b_k$ are prime.

By comparing this conjecture with the second definition of $\varrho^*(x)$ given above, we see immediately that (B) implies $\varrho(x) \geqslant \varrho^*(x)$. Since $\varrho(x) \leqslant \varrho_1(x) \leqslant \varrho^*(x)$ is trivial, we obtain $\varrho(x) = \varrho_1(x) = \varrho^*(x)$. (Recall that, loosely speaking, the function ϱ counts prime blocks which recurinfinitely often, ϱ_1 counts prime blocks which appear once, and ϱ^* measures "possible" configurations. To repeat, equality of ϱ , ϱ_1 , and ϱ^* depends on the unproved hypothesis (B).)

Remarks. The function ϱ was introduced by Hardy and Littlewod [4]. In the same paper they conjectured both (A) and (B) (and many other results as well); we have shown that at least one of these conjectures must be false. Schinzel and Sierpiński [15] studied the function ϱ^* (which they called $\overline{\varrho}$), and computed it for $x \leq 132$. The use of ϱ_1 was suggested to us by Montgomery; he has also considered the quantity

$$\pi_1(x) = \max_{y>0} [\pi(y+x) - \pi(y)].$$

Erdös and Selfridge [3] have investigated the function $r^*(x) =$ the maximum number of integers which can be chosen from any interval $y < n \le y + x$ in such a way that these integers are relatively prime to one another.

Just as for $\varrho^*(x)$, one can define a notion of admissibility corresponding to $r^*(x)$: a set $b_1 < b_2 < \ldots < b_k$ of integers is r^* -admissible if, for each prime p, there is some congruence class (mod p) which contains at most one of the b_i . The relationships satisfied by ϱ , ϱ_1 , ϱ^* , π_1 , and r^* are (for $x \ge 2$):

(a)
$$\varrho(x) \leqslant \varrho_1(x) \leqslant \varrho^*(x) < r^*(x),$$

and

(b)
$$[r^*(x) - \varrho^*(x)] \rightarrow \infty$$
 as $x \rightarrow \infty$;

also

(c)
$$\varrho_1(x) \leqslant \pi_1(x) \leqslant r^*(x),$$

and

(d)
$$\pi_1(x) \geqslant \pi(x+1).$$

^{5 -} Acta Arithmetica XXV.4

On the prime k-tuples hypothesis we have:

(e)
$$\varrho(x) = \varrho_1(x) = \varrho^*(x) \leqslant \pi_1(x) \leqslant r^*(x).$$

Finally we can show, with or without the k-tuples hypothesis, that:

(f)
$$\pi_1(x) \leqslant \varrho^*(x) \quad \text{for} \quad x \geqslant x_0$$

(this fails when x is small).

Of these, only (b) and (f) are not obvious. To prove (f), we consider several cases. Recall that $\pi_1(x)$ is the maximum value of $\pi(y+x)-\pi(y)$ for $y \geq 0$. Then either $y \geq x$, in which case $\pi_1(x) = \varrho_1(x) \leqslant \varrho^*(x)$, or y < x. In Section 2 we will show that $\varrho^*(x) - \pi(x) \geq \operatorname{Const}[x/(\log x)^2]$ for $x \geq x_0$. So we need only consider the possibility that y < x, but $\pi(y+x) - \pi(y) > \pi(x) + \operatorname{Const}[x/(\log x)^2]$. This cannot happen, however. For the de la Vallée Poussin sharp form of the Prime Number Theorem [9] implies that if $\pi(x+y) > \pi(x) + \pi(y)$ with y < x, then y is much smaller than x; specifically $y = O[x/(\log x)^N]$ for any fixed N. And thus the trivial inequality $\pi(x+y) \leq \pi(x) + y$ would give a contradiction.

To prove (b), we let x exceed twice the product of the first n primes, and show that then $r^*(x) - \varrho^*(x)$ exceeds n. For, starting with a maximal admissible set for $\varrho^*(x)$, we can add n extra points and still have an admissible set for $r^*(x)$. To do this, adjoin a sequence b+2, b+3, b+5, ..., $b+p_n$ congruent to the first n primes, where b is picked, via the Chinese Remainder Theorem, according to the rule: If, in the original ϱ^* -admissible set, $\{j_i\}$ denotes the empty congruence class $(\text{mod } p_i)$, then let $b+p_i$ lie in $\{j_i\}$, $1 \le i \le n$. Then for each prime p (less than p_n or not) there is some congruence class (mod p) which meets the new set in at most one point; i.e. the new set is r^* -admissible.

Erdös and Selfridge [3] anticipated the results of this paper by proving that $r^*(x) - \pi(x) \geqslant [\log 2 - (1/2) - \varepsilon][x/(\log x)^2]$. Their proof is based on the same "midpoint sieve" which we use in Section 2. However their method fails for $\varrho^*(x) - \pi(x)$, since it gives a constant $[\log 2 - 2] < 0$. The true orders of $r^*(x) - \pi(x)$ and $\varrho^*(x) - \pi(x)$ remain in doubt, but probably they exceed $O[x/(\log x)^2]$ (cf. Section 4).

2. The main result. We adhere to the notations of Section 1. Furthermore, in discussing $\varrho^*(x)$, we emphasize the second (sieve theoretic) definition of it.

Theorem. $\lim_{x\to\infty} \varrho^*(x) - \pi(x) = +\infty$; the difference is $\geqslant (\log 2 - \varepsilon) \times [x/(\log x)^2]$.

If the prime k-tuples conjecture (B) in Section 1 holds, then $\varrho^*(x) = \varrho(x)$, and so we have:

COROLLARY. The hypotheses (A) and (B) are incompatible. Moreover, if we assume (B), then we obtain:

(-A*) For all sufficiently large x, there exist infinitely many y, such that $\pi(x+y) > \pi(x) + \pi(y)$.

(Our hunch is that, while "sufficiently large" for x means somewhere between 10^3 and 10^5 , the corresponding values of y are beyond all sensible bounds.)

Proof. The theorem follows from two lemmas. Of these, the first is easy, while the second requires several more lemmas before it is established. The idea is to take an interval of integer points $-x/2 < n \le x/2$ located symmetrically about the origin. Then we will construct a set of points $\{b_i\}$ by *eliminating* points as follows:

First fix an integer $N \geqslant 3$. Eliminate all multiples (positive and negative) of all primes $p \leqslant x/N\log x$ (the "hard" sieve of Eratosthenes, where the prime itself is not saved). Call what remains the residual set. (This set consists of the primes between $x/N\log x$ and x/2, and their negatives, plus the points ± 1 .) Then:

LEMMA 1. The number of points in the residual set exceeds $\pi(x)$ by an amount asymptotic to $\lceil \log 2 - 2/N \rceil [x/(\log x)^2]$.

LEMMA 2. The residual set is an admissible set for $\varrho^*(x)$ (cf. Section 1) as soon as x is large enough.

Remark. It would be trivial that the residual set is admissible if we stopped at primes $p > 2\pi(x/2) \sim x/\log x$ (since then there would be more congruence classes (mod p) than points in the residual set). However we have an average of about N points per congruence class (N is fixed). We need to show that as the number of trials increases (i.e. as $x \to \infty$), then at least one empty class appears.

Proof of Lemma 1. The number of points remaining is (with an error of ± 2 or less) $2\pi(x/2) - 2\pi(x/N\log x)$. Now de la Vallée Poussin's sharp form of the Prime Number Theorem (cf. [9]) gives $[2\pi(x/2) - \pi(x)] \sim (\log 2)[x/(\log x)^2]$. On the other hand, $\pi(x/N\log x)$ is close to $(1/N)[x/(\log x)^2]$. This proves the lemma.

Proof of Lemma 2. As stated above, several auxiliary lemmas will be necessary. Although this is technically the hard part of the proof, it involves ingredients which have been known for a long time. The main step, Lemma 5, is essentially contained in a result of Westzynthius and Erdös ([17], [1]), that the maximum gap between primes $p_{n+1}-p_n$ is asymptotically larger than $\log p_n$. The sharpest results in the same direction are due to Rankin [12] (see the Addendum at the end of Section 4). Here we give a self-contained treatment, developing only as much precision as we need.

We begin with a lemma (to roughly the opposite effect as our theorem) about how few primes are necessary to completely eliminate a sequence

of t consecutive integers. [Later on, t will be Const·log x, the number of multiples of any prime $q > x/N \log x$ between -x and x.]

LEMMA 3 (cf. [17], [1], [12]). Let T(t) denote the minimum value of T for which the set of primes $p_i \leqslant T$ can "sieve out" an interval of length t: this means that there exist congruence classes $n \equiv j_i (\bmod p_i)$, one congruence class for each $p_i \leqslant T$, whose union contains the entire interval $1 \leqslant j \leqslant t$. Then T(t) = o(t).

Proof. The condition T = o(t) is equivalent to the assertion that the number of primes $\pi(T) = o[\pi(t)]$. This latter is what we shall prove.

We start with Mertens' Theorem (cf. [5]): $\prod_{p < x} \left(1 - \frac{1}{p}\right) \sim e^{-\gamma}/\log x$.

Let
$$C_M = \prod_{M .$$

We will show that, given a large fixed number M, we can make $\pi(T) < \pi(t/M) + C_M \pi(t)$ if t is large enough. Since M is arbitrary, this implies $\pi(T) = o[\pi(t)]$.

First apply the "hard" sieve of Eratosthenes, taking out *all* multiples of the primes in the two ranges $1 \leq p \leq M$ and $e^M \leq p \leq t/M$ (saving the middle range for later use). What remains of the original interval $1 \leq j \leq t$ is:

- (a) primes > t/M, and
- (b) integers all of whose prime factors come from the fixed middle interval M .

If t is large enough, the set (b) becomes small in comparison with (a), so that, say, (a) and (b) together have at most $\pi(t)$ elements. (This determines how large t must be; see the remark below.)

Now use the primes in the middle interval $M in an optimal way, whatever that may be. This must in any case reduce the residual set of <math>\leq \pi(t)$ elements by a multiplicative factor $\leq C_M$ (= the product of the corresponding $1 - \frac{1}{m}$).

Finally remove the remaining points (at most $C_M\pi(t)$ in number) one at a time, using another $C_M\pi(t)$ primes. In all, $\pi(t/M)+C_M\pi(t)$ primes have been used. This proves Lemma 3.

Remarks. Concerning the size of t: More careful estimates could be given, but we are satisfied to observe that there is a *fixed* number K of primes in the middle interval, and the smallest of these primes is $\geq M$. Let $t = M^u$ (where u varies); then the size of the set (b) is obviously bounded by $(u+1)^K$ (for each of the K primes, choose an exponent $0 \leq n \leq u$). As $u \to \infty$, $t = M^u \geq (u+1)^K$, and the set (a) becomes much larger than (b).

The significance of the number T(t) in Lemma 3 is that it yields a divisibility criterion for arithmetic progressions of length t. This criterion does not depend on the common difference a between the terms of the progression. (Nor, for the moment, do we need the result of Lemma 3 — only the definition of T(t).)

LEMMA 4. Define T(t) as in Lemma 3. Then, given any integer a > 0⁴ there exists an integer b such that every term in the finite arithmetic progression b+a, b+2a, ..., b+ta is divisible by some prime $p \leq T$.

Proof. Corresponding to each prime $p_i \leq T$, we have one congruence class $\{j_i\}$ (mod p_i), such that the union of the $\{j_i\}$ covers the entire interval $1 \leq j \leq t$. Now the Chinese Remainder Theorem shows that there is some translate $c+1 \leq j \leq c+t$ of our original interval, in which each number $c+j_i$ (with $1 \leq j_i \leq t$) is divisible by the corresponding prime p_i . We have only to solve the simultaneous congruences

$$c \equiv -j_i \pmod{p_i}$$
.

[If this holds for one j_i in $\{j_i\}$, then it holds for all!] Multiplying by a, the corresponding numbers ca + a, ca + 2a, ..., ca + ta remain divisible by the same primes p_i , and we have found the desired progression (b = ca).

LEMMA 5. Fix an arbitrarily large number N > 0. Then there is a number $x_0(N)$ such that: For every integer $x \ge x_0$, every integer y (unrestricted), and every integer a > 0, there exists an arithmetic progression b + a, b + 2a, ..., b + ta

- (a) whose length $t \geqslant N \log x$,
- (b) whose first term b + a lies in the interval $y < b + a \le y + x$ of length x and
 - (c) all of whose terms are divisible by some prime $p \leq (\log x)/N$.

Remarks. Lemma 5 is merely an extension of the Westzynthius-Erdös-Rankin result ([17], [1], [12]) that $p_{n+1}-p_n$ sometimes exceeds "any constant" times $\log p_n$ (to obtain this last, set $a=1,\ y=x$). For our purposes, it is essential that the difference a can go to infinity with x. The condition $p \leq (\log x)/N$ means that the numbers in our sequence are not only composite, but have rather small factors. For most applications this is unimportant, and the crucial point involves getting the first term b+a to fall between y and y+x.

Proof of Lemma 5. We combine Lemma 4, which tells us how to build such a progression (but gives us no control over b), with Lemma 3 which bounds T(t). First build the progression $b+a,\ldots,b+ta$ according to Lemma 4. Then all the numbers in this progression are divisible by some prime $p \leq T(t)$. By Lemma 3, T(t) = o(t). Thus, since N is fixed, we can satisfy (a) $t \geq N\log x$ and (c) $p \leq (\log x)/N$ as soon as t and x are large enough.

385

However (c) implies (b). For clearly we can vary the first term b+a by any multiple of

$$\prod_{p\leqslant (\log x)/N} p.$$

Thus we have to estimate this product. But the Prime Number Theorem for $\psi(x)$ (cf. [9]) gives $\sum_{p\leqslant u}\log p\sim u$, whence the product $\prod_{p\leqslant u}p$ lies between $e^{(1-\epsilon)u}$ and $e^{(1+\epsilon)u}$. Consequently the product over $p\leqslant (\log x)/N$ is "exponentially asymptotic" to $x^{1/N}$, and is in any case much smaller than x. Hence we can vary b+a to hit any interval of length x, and Lemma 5 is proved.

Proof of Lemma 2, completed. Recall that we started with the interval $-x/2 < n \le x/2$, and sieved out all multiples of the primes $p \le x/N\log x$. We have to show that the residual set is admissible: which means, for any prime $q > x/N\log x$, there is at least one congruence class (mod q) already empty, so no further sieving is necessary. Now each congruence class (mod q) is an arithmetic progression whose intersection with the interval $-x/2 < n \le x/2$ contains at most $N\log x$ points!!! Hence the desired result can be read out of Lemma 5.

For the details: Expand the original interval threefold, arriving at $-3x/2 < n \le 3x/2$. Replace the N in Lemma 5 by 3N, set $a = q > x/N\log x$, $t = [3N\log x]$, and let the first term b+q in the arithmetic progression b+q, b+2q, ..., b+tq lie between -3x/2 and -x/2. The last term b+tq > 3x/2. Thus b determines a congruence class (mod q) which, in the interval $-x/2 < n \le x/2$, hits no member of the residual set (since it hits only multiples of the relatively small primes $p \le (\log x)/N$, whereas primes up to $x/N\log x$ have been sieved out). This proves Lemma 2, and completes the proof of our theorem.

3. Numerical questions. It would be interesting to know the smallest value of $x \ge 2$ for which $\varrho^*(x) > \pi(x)$, and also the smallest value of x+y (with $x \le y$) for which $\pi(x+y) > \pi(x) + \pi(y)$. Let us call these smallest values x_0 and x_1+y_1 respectively. Of course x_0 and x_1 need not coincide (clearly $x_0 \le x_1$, but the minimal y for x_0 may be much larger than y_1).

[By the way, we are here supposing that (A) is false (as would follow if (B) were known to be true), so that the number $x_1 + y_1$ does exist.]

Let us begin with x_0 , the first value of x for which $\varrho^*(x) > \pi(x)$ (and thus, on the prime k-tuples conjecture, the smallest value of x such that there exists some y with $\pi(x+y) > \pi(x) + \pi(y)$). Preliminary computer experiments indicate that probably $x_0 \leq 10^5$. The authors, together with Warren Stenberg, plan to write a more thorough computer program to establish rigorous upper bounds for x_0 . The results of this calculation

may be ready by the time this paper comes to press (in which case we will signal the outcome by a brief "added in proof" attached to the present paper). Here we wish to thank Stefan A. Burr who gave us valuable advice about writing this program. We again acknowledge our debt to William Franta and Richard Franta who wrote the original version.

To bound x_0 above we must bound $\varrho^*(x)$ below, and vice-versa. Obtaining lower bounds for $\varrho^*(x)$ is relatively easy, since any example of an admissible set on (0, x] furnishes one. Finding sharp upper bounds is harder, because $\varrho^*(x)$ denotes the maximum over a large set of possibilities. (It is like trying to determine the optimal strategy in a game of chess.) As noted in § 0, Schinzel [14] has proved that $\varrho^*(x) \leq \pi(x)$ for $x \leq 146$, and Selfridge and his associates have an unpublished verification for $x \leq 500$. Thus $x_0 > 500$. Our computer experiments suggest that x_0 is considerably larger, perhaps $> 10^4$, but that is more problematical.

It should be remarked that although $\varrho^*(x) < \pi(x)$ for small x, and we have shown that $\varrho^*(x) > \pi(x)$ when x is large, the difference $\varrho^*(x) - \pi(x)$ is not monotone. Thus the two functions $\varrho^*(x)$ and $\pi(x)$ may cross several times. The problem of determining rigorously the *last* crossing point (i.e. the largest value of x for which $\varrho^*(x) = \pi(x)$) is very difficult. Our theoretical proof in Section 2 would give a numerical value absurdedly large; on the other hand, computer experiments might determine the last crossing point (which we believe to be $< 10^5$), but would provide no hint of a rigorous proof.

Now we come to the second problem mentioned at the beginning of this section: namely the smallest number x_1+y_1 for which $\pi(x_1+y_1) > \pi(x_1)+\pi(y_1)$. We suspect, even assuming the k-tuples hypothesis (B) is eventually proved constructively, that the value of x_1+y_1 will never be found; and moreover that no pair x, y satisfying $\pi(x+y) > \pi(x) + \pi(y)$ will ever be computed. (Of course an effective upper bound for x_1+y_1 may be given, but we believe that particular values x, y satisfying the above "reverse inequality" are very rare, and the size of y (assuming $x \leq y$) well beyond computer range.)

To justify these speculations, we make the following remarks. Consider an admissible k-tuple on an interval of length x for which $k = \varrho^*(x)$ exceeds $\pi(x)$. Then x must be fairly large, at least > 500 by Selfridge's calculations, and probably x > 1000. By definition, $k > \pi(x)$, but k is probably only slightly larger, so we may write, after the Prime Number Theorem, $k \sim x/\log x$.

Here we will invoke a famous conjecture, due to Hardy and Little-wood [4] and Stäckel, about the asymptotic distribution of prime k-tuples. Very crudely, their conjecture is that the number of such k-tuples between 0 and y, belonging to one particular pattern (like X, X+2, X+6),

is asymptotic to $\text{Const} \cdot [y/(\log y)^k]$. (The constant depends on the pattern being considered.)

Now, while y grows faster than any power of $\log y$ as $y\to\infty$, the size of y needed to make $y/(\log y)^k>1$ is not negligible when k is large; in fact $y>k^k$. There are, however, two compensating effects. The first is that the constant in the Hardy-Littlewood formula increases with k. But an examination of their formula shows that $\operatorname{Const} \leqslant (\log k)^k$, and the equation $(\log k)^k [y/(\log y)^k] = 1$ has the exact solution $y=k^k$ (clearly small values of y, such as y<2k, are absurd for our problem).

The second and more important effect is that we must consider, not one particular k-tuple as in the Hardy-Littlewood formula, but rather the set of all admissible k-tuples on an interval of length x. But it is easy to show that the number of such k-tuples is much smaller than k^k . For the number of all k-tuples (admissible or not) on an interval of length x is just the binomial coefficient $\binom{x}{k}$. And remembering that $k \sim x/\log x$, whence $x \sim k\log k$, we have by Stirling's formula that $\binom{x}{k}$ is roughly of the order $(k\log k)^k/k!$ which we replace by $e^k(\log k)^k$. This is negligible compared to k^k for k > 100 (a very conservative lower bound). Furthermore the number of admissible k-tuples must be small compared to the number of all k-tuples.

4. A result of Schinzel. Schinzel has found an extension of our argument, which requires another hypothesis (C), but shows that probably the difference $\varrho^*(x) - \pi(x)$ grows faster than $O[x/(\log x)^2]$. (We proved in Section 2, without any hypothesis, that

$$\varrho^*(x) - \pi(x) \geqslant (\log 2 - \varepsilon) \lceil x/(\log x)^2 \rceil$$

and the assumption (B) would give $\varrho^*(x) = \varrho_1(x)$.) Schinzel's result casts some doubt, in the authors' minds at least, as to whether $\varrho^*(x) \sim \pi(x)$ (cf. the end of Section 0). We observe that the arguments used so far (by the authors and by Schinzel) to give lower bounds for $\varrho^*(x)$ have involved modifications of the standard sieve of Eratosthenes. The question remains, whether there is any radically different sieve which does better. A proof that $\varrho^*(x) \leqslant (1+\varepsilon)\pi(x)$ as $x\to\infty$ would provide a kind of negative answer.

Notation. From now on, p will represent a particular prime (which is held fixed throughout the argument), and an arbitrary prime (say any prime $\leq x$) will be denoted by P.

In Section 2, we constructed an admissible set on an interval (-x/2, x/2] of length x by eliminating all multiples of the primes $P \leq x/N \log x$, where N was a fixed large number. Our advantage over the standard "hard" sieve of Eratosthenes was obtained by moving the origin to the

center of the interval. Schinzel instead takes the usual interval (0, x], but alters the sieve by switching congruence classes (mod 2), i.e. eliminating the odd numbers and keeping the even ones. This produces a gain of $[2\log 2 - \varepsilon][x/(\log x)^2]$, twice the value obtained by us. Moreover, carrying out the same process with an arbitrary prime p (i.e. eliminating the class $n \equiv 1 \pmod{p}$ instead of $n \equiv 0 \pmod{p}$) gives an advantage of

$$[(\log p) p/(p-1)^2][x/(\log x)^2].$$

These advantages combine linearly (ignoring second order effects) when the process is applied to a *finite* set of primes p_1, \ldots, p_m . And since the series $\sum (\log p)/p$ diverges, the sum of the advantages can be made larger than any fixed constant times $[x/(\log x)^2]$. However, to make the argument work, one has to stop sieving after the last prime $P \leq x/N(\log x)(\log\log x)^m$, where m is the number of the p_i . We do not know whether this process yields admissible sets (but we suspect that it does). So we make the hypothesis:

(C) Fix a number N > 0, an integer m, and m distinct primes p_1, \ldots, p_m . Apply the "hard" sieve of Eratosthenes to the interval (0, x], eliminating all multiples of the primes $P \leq x/N(\log x)(\log \log x)^m$, except: for the distinguished primes p_1, \ldots, p_m , we eliminate the congruence classes $n \equiv 1 \pmod{p_i}$ instead of the classes $n \equiv 0 \pmod{p_i}$. Then the residual set is admissible as soon as x is sufficiently large.

Remarks. If we stopped at $P \leq x/N\log x$, this would be Lemma 2 in Section 2. For the case m=1, (C) can "almost" be deduced from a result of Rankin [12]. This result and a sieve theoretic hypothesis (D) which would imply (C), are discussed in the Addendum at the end of this section. (Although (D) is easier to state, we have chosen (C) because it may hold even if (D) fails.)

The idea behind the following theorem was communicated to us by Schinzel.

THEOREM. If the hypothesis (C) holds, then the difference $\varrho^*(x) - \pi(x)$ grows faster than any constant multiple of $[x/(\log x)^2]$ as $x \to \infty$. And if (C) merely holds for the case $m = 1, p_1 = 2$, then

$$\varrho^*(x) - \pi(x) \geqslant [2\log 2 - \varepsilon][x/(\log x)]^2.$$

Proof. Since the proof in Section 2 was worked out in detail, and the ideas involved here are similar (but more complicated), we will only give a sketch. Let us first examine the case (m=1) of a single prime p. We apply the standard "hard" sieve of Eratosthenes, eliminating from (0, x] all multiples of the primes $P \leq x/N(\log x)(\log \log x)$, except that for

the prime p we eliminate the class $n \equiv 1 \pmod{p}$ and leave $n \equiv 0 \pmod{p}$ alone. What remains is:

the primes $P>x/N(\log x)(\log\log x)$ with $P\not\equiv 1(\bmod p),$ and

all numbers of the form $p^a P$ with $a \ge 1$ and prime $P > x/N(\log x)(\log \log x)$ (here it doesn't matter whether $P \equiv 1 \pmod{y}$).

To estimate the size of this set, we use the de la Vallée Poussin sharp form of the Prime Number Theorem for Arithmetic Progressions (cf. [9]). The series below is cut off at $M = [N^{1/2} \log \log x]$. For simplicity, we let $X = 1/\log x$, and ignore any "second order effects" which are smaller than $X \cdot \pi(x)$. Thus \cong means "to within $o(X) \cdot \pi(x) = o[x/(\log x)^2]$ ". Now the size of our residual set is:

$$\cong \pi(x)\left(\frac{p-2}{p-1}\right) + \sum_{a=1}^{M} \pi(x/p^a).$$

Since $\pi(x/c) \cong (1/c)\pi(x) + [(\log c)/c]\pi(x) \cdot X$, the above becomes

$$\cong \pi(x) \left(\frac{p-2}{p-1} + \sum_{a=1}^{M} \frac{1}{p^a} + \sum_{a=1}^{M} \frac{\log(p^a)}{p^a} \cdot X \right).$$

Summing these series (setting $M=\infty$ for the moment), we obtain $\pi(x) \times (1+[(\log p)p/(p-1)^2]X)$. (For the second series, use the formula $\sum_{a=1}^{\infty}az^a=z/(1-z)^2$.)

Now we must consider the errors in our reckoning. They have three sources. The first, and by far the largest, comes from the primes $P \leq x/N(\log x)(\log\log x)$ eliminated by the "hard" sieve. The number of such primes is like $x/N(\log x)^2(\log\log x)$ (less by a power of $\log x$ than the above), and each one of them must be counted $M \sim N^{1/2}\log\log x$ times. The product is $\varepsilon[x/(\log x)^2]$ with $\varepsilon = N^{-1/2}$. The second error comes from truncating the series at M. This gives $\pi(x)\sum_{a=M}^{\infty}(1/p^a)$ which is like $\pi(x)p^{-M} = \pi(x)(\log x)^{-\text{Const}}$ with a large value of the constant. The third error involves the round-off in approximating $\pi(x/c)$ by $(1/c)\pi(x) + [(\log c)/c]\pi(x) \cdot X$. This is less by a power of $(1/\log x)$ than the last term considered, and since our series involves only $M = \text{Const} \cdot \log\log x$ terms, the effect is less than $\pi(x)(\log x)^{-2+\varepsilon}$, while our principal term is $\pi(x)(\log x)^{-1}$. Thus the case m=1 is proved.

The main difficulties in treating the general case are algebraic; they involve keeping track of the congruence classes (mod Q), where Q=

 $= p_1 \dots p_m$. (The error estimates go as before, except that now m-fold sums are involved, giving altogether $\operatorname{Const}(\log\log x)^m$ terms.) We shall therefore ignore the errors, and concentrate on the algebraic aspects. Among the various possible approaches, the following has the advantage of displaying the relationships involved in a visual form.

To avoid the use of subscripts, suppose there are three primes p_i , which we label p, q, r. Set Q = pqr, and recall that $X = 1/\log x$. Second order terms like X^2 , X^3 , ... will be discarded.

Consider a particular congruence class $b \pmod{Q}$. The number of points in the residual set lying in this class is: none if $b \equiv 1 \pmod{p_i}$ for some $p_i = p$, q, r; otherwise, an amount which varies depending on which of the primes p, q, r divide b. Thus it emerges that the count should be made, not over congruence classes $b \pmod{Q}$, but rather over subsets of $\{p, q, r\}$, corresponding to the p_i which divide b. To fix the ideas, consider the subset $\{p, q\}$. Then the effect of all the congruence classes $b \pmod{Q}$ for which p|b, q|b, but $r \nmid b$ is:

$$\begin{split} &\cong \left(\frac{r-2}{r-1}\right) \Bigl(\sum_{a,b\geqslant 1} \pi(x/p^a q^b)\Bigr) \\ &\cong \pi(x) \Bigl(\frac{r-2}{r-1}\Bigr) \Bigl(\sum_{a,b\geqslant 1} \frac{1}{p^a q^b} + \frac{\log(p^a q^b)}{p^a q^b} \cdot X\Bigr). \end{split}$$

The factor (r-2)/(r-1) takes care of the requirement that $b\not\equiv 1 \pmod r$; and the sum of $\pi(x/p^aq^b)$ with $a,b\geqslant 1$ takes account of the fact that both p and q divide b. Remember that (pq) corresponds to the subset $\{p,q\}$, i.e. to all the congruence classes $b \pmod Q$ which are divisible by p and q but not r. Thus the total number of points in the residual set is equal to a sum, taken over the eight subsets of $\{p,q,r\}$, of terms like (pq). To evaluate this sum, consider the following product:

$$(**) \qquad \pi(x) \left(\frac{p-2}{p-1} + \sum_{a=1}^{\infty} \frac{1}{p^a} + \sum_{a=1}^{\infty} \frac{\log(p^a)}{p^a} \cdot X \right) \times \\ \times \left(\frac{q-2}{q-1} + \sum_{a=1}^{\infty} \frac{1}{q^a} + \sum_{a=1}^{\infty} \frac{\log(q^a)}{q^a} \cdot X \right) \times \\ \times \left(\frac{r-2}{r-1} + \sum_{a=1}^{\infty} \frac{1}{r^a} + \sum_{a=1}^{\infty} \frac{\log(r^a)}{r^a} \cdot X \right).$$

Now we evaluate this product two ways. First, each term is like 1+ $+[(\log p)p/(p-1)^2] \cdot X$, and hence the product of these terms (ignoring

391

the powers X^2, X^3, \ldots) gives

$$\pi(x) \left(1 + \sum_{i=1}^{3} \left[(\log p_i) p_i / (p_i - 1)^2 \right] \cdot X \right).$$

On the other hand, it is easy to read down the product (**) and identify all the terms which appear in (pq), and to find the logical rule whereby every product in (**) (ignoring X^2 , X^3 , etc.) corresponds to a particular subset of the set $\{p,q,r\}$. Thus the sum of all the (eight) terms like (pq), which represents the number of points in the residual set, can be replaced by the product (**) which we have evaluated in the preceding paragraph.

Addendum. We consider a hypothesis (D) concerning sieves which would imply (C). Recall the definition of T(t) in Lemma 3, Section 2: T(t) represents the least value of T for which the primes $p \leq T$ are sufficient to "sieve out," all the points in an interval of length t. We proved in Section 2 that T(t) = o(t); this is a weak form of Rankin's theorem [12] that

$$T(t) = O([t/\log t][(\log_2 t)^2/\log_3 t]),$$

where $\log_2 t$ means $\log \log t$, etc. Our hypothesis is:

(D)
$$T(t) = o[t/(\log t)^m].$$

We note that for m=1, (D) is only slightly stronger than Rankin's result. To see why (D) implies (C), it is easier to ask instead what any result about T(t) would imply both for the problem of admissible sets, and also for the question of gaps between primes.

Let t(T) be the "inverse function" of T(t), i.e. $t(T_0)$ denotes the smallest value t_0 for which $T(t_0) \ge T_0$. Now the method used in Lemma 5, Section 2 shows that:

LEMMA 5*. From an interval of length x, sieve out (in an arbitrary manner) one congruence class (mod P) for every prime $P \leq x/t [(\log x)/2]$. Then the residual set is admissible as soon as x is sufficiently large. Similarly there exist infinitely many pairs of consecutive primes with a gap

$$p_{n+1} - p_n > t[(\log p_n)/2].$$

[The constant 2 can be replaced by $1+\varepsilon$ if desired.]

Since T(t) = o(t), the inverse function t(T) grows faster than T. The inverse of $T(t) = t/\log t$ is approximately $t(T) = T\log T$, and similarly for other combinations of \log , $\log\log$, etc. Thus, by this method, the hypothesis (D) is just strong enough to yield (C). (Of course there is no reason to believe that this method is best possible.) Combining Lemma 5*

with Rankin's estimate for T(t) gives Rankin's famous theorem [12]:

$$p_{n+1} - p_n > \text{Const}(\log p_n)(\log_2 p_n)(\log_4 p_n)/(\log_3 p_n)^2$$

for infinitely many n.

Added in proof. The authors, in collaboration with Warren Stenberg, have recently shown that $\varrho^*(x) > \pi(x)$ for x = 20000 (cf. the paragraph beginning at the bottom of p. 384).

References

- [1] P. Erdös, On the difference of consecutive primes, Quarterly J. Math. (Oxford) 6 (1935), pp. 124-128.
- [2] Some unsolved problems, Michigan Math. J. 4 (1957), pp. 291-300.
- [3] and J. L. Selfridge, Complete prime subsets of consecutive integers, Proceedings of the Manitoba Conference on Numerical Mathematics, University of Manitoba, Winnipeg 1971, pp. 1-14.
- [4] G. H. Hardy and J. E. Littlewood, Some problems of 'partitio numerorum'.

 III. On the expression of a number as a sum of primes, Acta Math. 44 (1923),
 pp. 1-70.
- [5] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford 1938.
- [6] D. Hensley, An asymptotic inequality concerning primes in contours for the case of quadratic number fields, to appear.
- [7] and I. Richards, On the incompatibility of two conjectures concerning primes,
 A. M. S. Symposia in Pure Math. 24(1973), pp. 123-127.
- [8] E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen, Leipzig 1909.
- [9] Vorlesungen über Zahlentheorie, vol. 2, Leipzig 1927.
- [10] H. L. Montgomery, Topics in Multiplicative Number Theory, Lecture Notes in Mathematics, vol. 227, New York 1971.
- [11] and R. C. Vaughan, to appear.
- [12] R. A. Rankin, The difference between consecutive prime numbers, Proc. Edinburgh Math. Soc. 13 (1962-1963), pp. 331-332.
- [13] J. B. Rosser, L. Schoenfeld, and J. M. Yohe, Rigorous computation and zeros of the Riemann zeta-function, Information Processing 68, Amsterdam 1969.
- [14] A. Schinzel, Remarks on the paper 'Sur certains hypothèses concernant les nombres premiers', Acta Arith. 7 (1961), pp. 1-8.
- [15] et W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, Acta Arith. 4 (1958), pp. 185-208.
- [16] S. L. Segal, $On \ \pi(x+y) < \pi(x) + \pi(y)$, Trans. Amer. Math. Soc. 104 (3) (1962), pp. 523-527.
- [17] E. Westzynthius, Über die Verteilung der Zahlen, die zu den n ersten Primzahlen teilerfremd sind, Comm. Phys. Math. Helsingfors (5) 25 (1931), pp. 1-37.

UNIVERSITY OF MINNESOTA Minneapolis, Minnesota

Received on 3, 5, 1973