On some applications of Brun's method[1]).

By P. ERDÖS in Syracuse (N. Y., U. S. A.)

Denote by $P(k, l)$ the least prime in the arithmetic progression $kx+l$. Subsequently we shall always assume $0<l<k$, $(l, k)=1$. TURÁN[2]) proved that under assumption of the generalised RIEMANN hypothesis we have for every fixed positive ε

$$P(k, l)<k(\log k)^{2+\varepsilon}$$

except possible for $o(\varphi(k))$ progressions. He also remarks that it immediately follows from the prime number theorem that $P(k, l)< <(1-\varepsilon)\varphi(k)\log k$ does not hold for almost all progressions, since the number of primes not exceeding $(1-\varepsilon)\varphi(k)\log k$ is less than $\left(1-\frac{\varepsilon}{2}\right)\varphi(k)$ (almost all will mean throughout: with the exception of $o(\varphi(k))$ values of l). It seems very likely that for any constant C, $P(k, l)<C\varphi(k)\log k$ does not hold for almost all progressions. But at present I cannot even disprove the existence of infinitely many k so that $P(k, l)<\varphi(k)\log k$ holds for almost all values of l. On the other hand, I can prove the following weaker

Theorem 1. *There exists a constant $c_1>0$ and infinitely many integers k, such that*

$$P(k, l)\leqq(1+c_1)\varphi(k)\log k \tag{1}$$

does not hold for almost all l. In other words, there exists a constant c_2 and infinitely many values of k so that $P(k, l)>(1+c_1)\varphi(k)\log k$ for more than $c_2\varphi(k)$ values of l.

Further we shall prove

Theorem 2. *Let $c_3>0$ be any constant. Then for $c_4\varphi(k)$ values of l $(c_4=c_4(c_3))$*

$$P(k, l)<c_3\varphi(k)\log k. \tag{2}$$

---

[1]) Recently A. SELBERG deduced (and sharpened) some results of BRUN in a surprisingly simple way.

[2]) P. TURÁN, Über die Primzahlen der arithmetischen Progressionen,. *these Acta*, 8 (1937), p. 226—235.

Remark. It easily follows from the prime number theorem that $P(k, l) = o(\varphi(k) \log k)$ can hold only for $o(\varphi(k))$ values of l. Thus Theorem 2 is in some sense the best possible.

Next we investigate a different question. Since the integers $n!+2, \ldots, n!+n$ are all composite, it follows immediately that $\limsup (p_{n+1} - p_n) = \infty$. SIERPINSKI[3]) proved that $\limsup (\min (p_{n+1} - p_n, p_n - p_{n-1})) = \infty$, by using Dirichlet's theorem according to which every arithmetic progression whose first term and difference are relatively prime contains infinitely many primes. In other words, as SIERPINSKI puts it, there are infinitely many primes isolated from both sides. By using Brun s method we shall prove the following sharper

Theorem 3. *Let c_5 be any constant and n sufficiently large. Then there exist a constant $c_6 = c_6(c_5)$, $[c_6 \log n]$ primes $p_k < p_{k+1} < \ldots < p_{k+r} < n$, $r = [c_6 \log n]$, so that*

$$p_{k+i+1} - p_{k+i} > c_5, \qquad i = 0, 1, \ldots, r-1.$$

One final remark: In a previous paper[4]) I proved that

$$\liminf \frac{p_{n+1} - p_n}{\log n} < 1. \tag{3}$$

By the same method we can show that for any r

$$\liminf \frac{p_{n+r} - p_n}{r \log n} < \vartheta = \vartheta(r) < 1. \tag{4}$$

We do not give the details of the proof, since it is quite similar to that of (3). It can be conjectured that

$$\liminf \frac{p_{n+r} - p_n}{r \log n} < 1 - c_6 \tag{5}$$

where c_6 is a constant *independent* of r (in fact, it is very likely that the lim inf in (5) is 0).

Proof of Theorem 2. (It is more convenient to prove Theorem 2 first.) Denote $x = c_3 \varphi(k) \log k$; $p_1, p_2, \ldots$ will denote the sequence of consecutive primes. Further $A_x(k)$ denote the number of solutions of the congruence

$$p_j - p_i \equiv 0 \pmod{k}, \qquad p_i < p_j \leq x.$$

$B_z(k, l)$ denote the number of primes $p \leq z$ in the arithmetic progression $kx + l$. Clearly

$$A_x(k) = \sum_l \frac{1}{2} (B_x(k, l)(B_x(k, l) - 1). \tag{6}$$

---

[3]) W. SIERPIŃSKI, Remarque sur la répartition des nombres premiers, *Colloquium Math.*, **1** (1948), p. 193–194.

[4]) P. ERDŐS, The difference of consecutive primes, *Duke Math. Journal*, **6** (1940), p. 438–441.

If Theorem 2 is not true, then for a suitable sequence k_i of integers $B_x(k_i, l) = 0$ for all but $o(\varphi(k_i))$ values of l. Let $k_1 < k_2 < \dots$ be such a sequence. The number of integers l with $B_x(k_i, l) \neq 0$ we denote by $\varepsilon_i \varphi(k_i)$, where $\lim \varepsilon_i = 0$. We have by the theorem of CHEBISHEF ($\pi(z)$ denotes the number of primes not exceeding z)

$$c_7 \varphi(k_i) > \sum_l B_x(k_i, l) = \pi(x) - \nu(k_i) > c_8 \varphi(k_i), \tag{7}$$

where $\nu(k_i)$ denotes the number of prime factors of k_i ($\nu(k) < c \log k$). Further from (6) and (7)

$$A_x(k_i) = \sum_l \frac{1}{2} B_x(k_i, l)\,(B_x(k_i, l) - 1) \geqq -\pi(x) + \frac{1}{2} \sum_l (B_x(k_i, l))^2$$

and applying Schwarz's inequality

$$A_x(k_i) > -\pi(x) + \frac{1}{2} \frac{\left(\sum_l B_x(k_i, l)\right)^2}{\sum\limits_{B_x(k_i, l) \geqq 1} 1} > -c_7 \varphi(k_i) + \frac{(\pi(x) - \nu(k_i))^2}{2\varepsilon_i \varphi(k_i)} >$$
$$> -c_7 \varphi(k_i) + \frac{c_8^2}{2\varepsilon_i} \varphi(k_i) > \frac{c_9}{\varepsilon_i} \varphi(k_i). \tag{8}$$

Now we shall prove that for every k

$$A_x(k) < c_{10} \varphi(k) \tag{9}$$

which contradicts (8), and this contradiction completes the proof of Theorem 2.

Denote by $C_x(r)$ the number of solutions of

$$p_j - p_i = kr, \qquad 1 < p_i < p_j \leqq x.$$

Clearly

$$A_x(k) = \sum C_x(r), \quad 1 \leqq r \leqq \frac{c_3 \varphi(k) \log k}{k}. \tag{10}$$

Denote by $C'_x(r)$ the number of primes $p \leqq x$ so that $p_i + kr$ is also a prime. Evidently

$$C_x(r) \leqq C'_x(r). \tag{11}$$

We obtain by a result of SCHNIRELMANN[5]) that

$$C'_x(r) < c_{11} \frac{x}{(\log x)^2} \prod_{p \mid kr} \left(1 + \frac{1}{p}\right) < c_{12} \frac{\varphi(k)}{\log k} \prod_{p \mid kr} \left(1 + \frac{1}{p}\right). \tag{12}$$

Thus from (10), (11) and (12)

$$A_x(k) \leqq \sum_{1 \leqq r \leqq \frac{x}{k}} C'_x(r) < c_{12} \frac{\varphi(k)}{\log k} \sum_{1 \leqq r \leqq \frac{x}{k}} \prod_{p \mid kr} \left(1 + \frac{1}{p}\right) \leqq$$
$$\leqq c_{12} \frac{\varphi(k)}{\log k} \prod_{p \mid k} \left(1 + \frac{1}{p}\right) \sum_{1 \leqq r \leqq \frac{x}{k}} \prod_{p \mid r} \left(1 + \frac{1}{p}\right).$$

---

[5]) E. LANDAU, Die Goldbachsche Vermutung und der Schnirelmannsche Satz, *Göttinger Nachrichten*, 1930, p. 255—276.

Now $\varphi(k) \prod_{p|k} \left(1+\frac{1}{p}\right) = k \prod_{p|k} \left(1-\frac{1}{p^2}\right) < k$ Thus

$$A_x(k) < c_{12} \frac{k}{\log k} \sum_{1 \leq r \leq \frac{x}{k}} \prod_{p|r} \left(1+\frac{1}{p}\right) < c_{13} \frac{k}{\log k} \sum_{d=1}^{\infty} \frac{x}{kd^2} < c_8 \varphi(k),$$

which proves (9) and completes the proof of Theorem 2.

Proof of Theorem 1 (in one or two places we will suppress some of the details of the proof). Let n be any large integer. We shall prove that between n and $2n$ there exists always an integer k which satisfies the conditions of Theorem 1. Let δ be a small but fixed number (independent of n). Put $y = \delta n \log n$. As in the proof of Theorem 2, $A_y(m)$ denote the number of solutions of the congruence

$$p_j - p_i \equiv 0 \pmod{m}, \quad p_i < p_j \leq y.$$

First we are going to estimate from below

$$A = \sum_{n}^{2n} A_y(m). \tag{13}$$

Denote by $D_y(r)$ the number of solutions of

$$p_j - p_i = rm, \quad p_i < p_j \leq y, \quad n \leq m \leq 2n.$$

Clearly

$$A \geq \sum D_y(r), \quad 1 \leq r \leq \frac{y}{4n} \quad \left(\text{or } r \leq \frac{\delta}{4} \log n\right). \tag{14}$$

First we estimate $D_y(r)$. Let $p_i < \frac{y}{2}$ be an arbitrary prime. It immediately follows by a simple calculation from the results of PAGE[6]) on the primes in an arithmetic progression that the number of primes of the form

$$p_i + rm, \ n \leq m \leq 2n$$

is greater than $c_{14} \frac{n}{\log n}$, also these primes are all $\leq y$. Thus from $\pi(y) > c_{15} \frac{y}{\log y} > c_{16} \delta n$ we obtain

$$D_y(r) > c_{17} \delta \frac{n^2}{\log n} \tag{15}$$

and from (14) and (15) $\left(r \leq \frac{\delta}{4} \log n\right)$

$$A > c_{18} \delta^2 n^2. \tag{16}$$

---

[6]) A. PAGE, The number of primes in an arithmetic progression, *Proceedings London Math. Society*, (2) 39 (1935), p. 116–141.

On the other hand as in the proof of (9) we obtain for $n \leq m \leq 2n$

$$(17) \qquad A_\nu(m) < c_{19}\left(\frac{\delta m}{\varphi(m)}\right)^2 \varphi(m) = c_{19}\delta^2 \frac{m^2}{\varphi(m)} = c_{20}\delta^2 n \frac{m}{\varphi(m)};$$

we obtain (17) by putting $\delta n \log n = c_{20} \frac{\delta m}{\varphi(m)} \varphi(m)$, and use the same method we used in proving (9).

Hence from (17)

$$(18) \qquad \sum{}' A_\nu(m) < c_{20}\delta^2 n \sum{}' \frac{m}{\varphi(m)}$$

where the dash indicates that the summation is extended over the m satisfying $n \leq m \leq 2n$, $\frac{m}{\varphi(m)} > \frac{1}{4\delta}$. Now

$$(19) \qquad \sum_{m=1}^{u}\left(\frac{m}{\varphi(m)}\right)^2 = \sum_{m=1}^{u} \prod_{p \mid m}\left(1+\frac{1}{p}+\ldots\right)^2 <$$

$$< \sum_{m=1}^{u} \prod_{p \mid m}\left(1+\frac{5}{p}\right) < u \sum_{d=1}^{\infty} \frac{5^{\nu(d)}}{d^2} < c_{21} u.$$

Thus we have from (19) by a simple argument (putting $2n = u$)

$$(20) \qquad \sum{}' \frac{m}{\varphi(m)} < c_{22}\delta m.$$

Hence from (18) and (20) $(m \leq 2n)$

$$(21) \qquad \sum{}' A_\nu(m) < c_{23}\delta^3 n^2.$$

Thus from (16) and (21), if δ is sufficiently small,

$$(22) \qquad A - \sum{}' A_\nu(m) > \frac{c_{18}}{2}\delta^2 n^2.$$

From (22) we obtain that there exists an m_0, $n \leq m_0 \leq 2n$, $\frac{\varphi(m_0)}{m_0} \leq \frac{1}{4\delta}$ for which

$$(23) \qquad A_\nu(m_0) > \frac{c_{18}}{2}\delta^2 m.$$

Now we show that m_0 satisfies the conditions of Theorem 1. In other words we shall show that

$$(24) \qquad P(m_0, l) \leq (1+c_1)\varphi(m_0)\log m_0$$

does not hold for $c_2\varphi(m_0)$ values of l, where c_1 and c_2 are suitable constants $(c_2 = c_2(c_1))$.

We shall prove that (24) is true for $c_1 = c_2 = \delta^{20}$. Put

$$z = (1+\delta^{20})\varphi(m_0)\log m_0.$$

We have from the prime number theorem

$$(25) \qquad \pi(z) < (1+2\delta^{20})\varphi(m_0).$$

Thus to prove our assertion it will clearly suffice to show that there are at least $3\delta^{20}\varphi(m_0)$ progressions m_0d+l each of which contain more than one prime not exceeding z (i. e. it immediately follows from (25) that there are at least $\delta^{20}\varphi(m_0)$ progressions m_0d+l for which $P(m_0, l)>z$).

We have by the definition of m_0, $\varphi(m_0)\geqq 4\delta m_0$. Thus $y\leqq z$. Hence by (23)

$$A_z(m_0 > \frac{c_{18}}{2}\delta^2 n. \tag{26}$$

Next we prove

$$L=\sum\binom{B_z(m_0, l)}{4} < c_{24}\frac{n}{\delta^5}. \tag{27}$$

Suppose that (27) is already proved. Then we prove Theorem 1 as follows: We have by (6) and (26)

$$\frac{1}{2}B_z(m_0, l)\,(B_z(m_0, l)-1)=A_z(m_0)>\frac{c_{18}}{2}\delta^2 n. \tag{28}$$

Thus if there would be less than $3\delta^{20}\varphi(m_0)$ values of l with $B_z(m_0, l)>1$ (in fact with $B_z(m_0, l)\geqq 4$), we would obtain from (28) by a simple calculation, using Schwarz's inequality as in (8) and using $\varphi(m_0)>$ $>4\delta m_0\geqq 4\delta n$,

$$\sum\binom{B_z(m_0, l)}{4}>c_{25}\left(\frac{1}{\delta^{\frac{20-2}{2}}}\right)^4\delta^{20}\varphi(m_0)>c_{26}\frac{n}{\delta^{15}} \tag{29}$$

which for sufficiently small δ contradicts (27) and thus completes the proof of Theorem 1.

Now we only have to prove (27). Denote by $F_z(r_1, r_2, r_3)$ the number of primes p_i so that

$$p_i+r_1m_0,\ p_i+r_2m_0,\ p_i+r_3m_0$$

are all primes not exceeding z. Clearly

$$\sum_{r_1, r_2, r_3} F_z(r_1, r_2, r_3)=\sum\binom{B_z(m_0, l)}{4}. \tag{30}$$

Further

$$F_z(r_1, r_2, r_3)\leqq F'_z(r_1, r_2, r_3) \tag{31}$$

where $F'_z(r_1, r_2, r_3)$ denotes the number of primes $p_i\leqq z$ so that

$$p_i+r_1m_0,\ p_i+r_2m_0,\ p_i+r_3m_0$$

are also primes. We obtain by Brun's method[7]) that

$$F'_z(r_1, r_2, r_3)>c_{27}\frac{z}{(\log z)^4}\prod_{p\mid m_0r_1r_2r_3(r_2-r_1)(r_3-r_1)(r_3-r_2)}\left(1+\frac{4}{p}\right), \tag{32}$$

[7]) P. Erdős, On the easier Waring problem for powers of primes, *Proceedings Cambridge Philosophical Society*, **33** (1937), p. 6—12, lemma 2, p. 8.

Hence by the definition of z and m_0 $\left(\prod_{p \mid m_0}\left(1+\frac{4}{p}\right) < \frac{c_{28}}{\delta^4}\right)$

$$F_z'(r_1, r_2, r_3) < c_{29} \frac{n}{(\log n)^3} \frac{1}{\delta^5} \prod\nolimits_1 \left(1+\frac{4}{p}\right) \tag{33}$$

where in $\prod_1$, p runs through the divisors of $r_1 r_2 r_3 (r_2 - r_1)(r_3 - r_1)(r_3 - r_2)$. From (33) we evidently have

$$L \leqq \sum_{r_i \leqq \frac{z}{m_0}} F_z'(r_1, r_2, r_3) < \frac{c_{29}}{\delta^5} \frac{n}{(\log n)^3} \sum_{r_i \leqq \frac{z}{m_0}} \prod\nolimits_1 \left(1+\frac{4}{p}\right). \tag{34}$$

Now by a simple argument we obtain from lemma 1 of my paper "On the easier Waring's problem for powers of primes"[8]) that

$$\sum_{r_i \leqq \frac{z}{m_0}} \prod\nolimits_1 \left(1+\frac{4}{p}\right) < c_{30} (\log n)^3. \tag{35}$$

Thus finally from (33), (34) and (35) we obtain (27), which completes the proof of Theorem 1.

Our proof of Theorem 1 very strongly used the special properties of the primes. Perhaps the following question would be of some interest: Let $q_1, q_2, \ldots$ be a sequence of integers so that the number of q's, not exceeding n, equals $\frac{n}{\log n} + o\left(\frac{n}{\log n}\right)$. Let $(k, l) = 1$ and $P(k, l)$ denote the least q in the arithmetic progression $kx + l$. Is it true that there exists an infinite sequence of integers k_i so that

$$P(k_i, l) < (1 + c_1)\,\varphi(k_i) \log k_i$$

does not hold for $c_2 \varphi(k_i)$ values of l? Perhaps some assumption like $(q_i, q_j) = 1$ might be necessary.

Proof of Theorem 3. It follows from the result of SCHNIRELMANN[5]) that the number of solutions of

$$p_{m+1} - p_m \leqq c_5, \; p_m \leqq n$$

is less than $c_{31} \frac{n}{(\log n)^2}$. Thus since $\pi(n) > c_{32} \frac{n}{\log n}$, we immediately obtain Theorem 3.

(Recevied January 12, 1949.)

[8]) L. c. [7]).