PRIME NUMBERS IN ARITHMETIC PROGRESSIONS

To Professor KÔITI SAKAI on his sixtieth birthday

SABURÔ UCHIYAMA

For any positive integer q and any integer h with $(h, q)=1$, we write as usual

$$\theta(x, q, h)=\sum_{\substack{p\leq x\\ p\equiv h \pmod q}} \log p$$

and

$$\psi(x, q, h)=\sum_{\substack{n\leq x\\ n\equiv h \pmod q}} \Lambda(n),$$

where x (>1) is a real variable and $\Lambda(n)$ is the arithmetical function which is defined to be $\log p$ if n is a power of the prime p and 0 otherwise. These functions are analogues of the functions $\theta(x)$ and $\psi(x)$ introduced and studied by P. L. Čebyšev, namely, of

$$\theta(x)=\sum_{p\leq x} \log p$$

and

$$\psi(x)=\sum_{n\leq x} \Lambda(n);$$

we have in particular

$$\sum_{\substack{h=1\\ (h,q)=1}}^{q} \theta(x, q, h)=\theta(x)+O((\log q)\log x)$$

and

$$\sum_{\substack{h=1\\ (h,q)=1}}^{q} \psi(x, q, h)=\psi(x)+O((\log q) \log x),$$

where the constants implied in the symbol O are absolute.

E. Bombieri [1] proved that for any positive number A there exists a positive constant C $(=3A+23)$ such that if

$$X\leqq x^{\frac{1}{2}}(\log x)^{-C}$$

then

$$\text{(a)}\qquad \sum_{q\leq X} \sup_{y\leq x} \max_{(h,q)=1}\left|\psi(y, q, h)-\frac{y}{\phi(q)}\right|\leqq B\, x(\log x)^{-A},$$

where $B=B(A)$ denotes an unspecified positive constant depending at most on the value of the parameter A. (We shall employ similar notations such as $B=B(H)$, $c_1=c_1(H)$ and so on.)

On the other hand, improving a previous result of H. Davenport and H. Halberstam [2], P. X. Gallagher [3] gave an ingenious proof of the inequality

$$\text{(b)} \qquad \sum_{q\leq X}{}' \sum_{\substack{h=1\\(h,q)=1}}^{q} \left(\psi(x, q, h)-\frac{x}{\phi(q)}\right)^2 \leq Bx^2(\log x)^{-A+1},$$

where A is any fixed positive number, $B=B(A)>0$, and

$$X\leq x(\log x)^{-A}.$$

We know that this result of Gallagher is substantially the best possible one of the sort, in view of an investigation by H. L. Montgomery [4].

Now, our aim in the present paper is to prove the following theorems.

Theorem 1. *Let* $A>0$ *be any fixed number. Then, if*

$$X\leq x(\log x)^{-A}$$

we have

$$\sum_{q\leq X}{}' \sum_{\substack{h=1\\(h,q)=1}}^{q} \sup_{y\leq x}\left(\theta(y, q, h)-\frac{y}{\phi(q)}\right)^2 \leq B\frac{x^2}{(\log x)^{A-3}}$$

with a constant $B=B(A)>0$.

Theorem 2. *For any fixed number* $A>0$ *we have*

$$\sum_{q\leq X}{}' \sum_{\substack{h=1\\(h,q)=1}}^{q} \sup_{y\leq x}\left(\psi(y, q, h)-\frac{y}{\phi(q)}\right)^2 \leq B\frac{x^2}{(\log x)^{A-3}}$$

with a constant $B=B(A)>0$, *provided*

$$X\leq x(\log x)^{-A}.$$

We shall first prove Theorem 2 and then deduce Theorem 1 from Theorem 2. It does not seem so obvious to substitute $\theta(x, q, h)$ for $\psi(x, q, h)$ in Theorem 2 as in the inequalities (a) and (b), whereas the replacement of $\psi(x, q, h)$ by $\theta(x, q, h)$ in (a) and (b) is quite immediate, since we have

$$\psi(x, q, h)=\theta(x, q, h)+O(x^{\frac{1}{2}})$$

and

$$\psi(x)=\theta(x)+O(x^{\frac{1}{2}}),$$

the O-constants being again absolute.

There have been several occasions to announce without detailed proofs our results presented in this paper. For an application of Theorem 1 we should like to refer to [6].

Proof of Theorem 2.

We define for each residue character χ (mod q)

$$S(\chi)=\sum_{n\leq x}\Lambda(n)\chi(n).$$

Then we have for $(h, q)=1$

$$\psi(x, q, h)=\frac{1}{\phi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}\overline{\chi}(h)S(\chi),$$

where $\phi(q)$ is the Euler totient function.

In Theorem 2, as well as in Theorem 1, we may clearly assume that $x=N$ and $y=n$ are integer valued variables, thus replacing sup with max.

Assuming further that $N\geqq 2$, taking a positive integer L which is uniquely determined by

$$2^{L-1}<N\leqq 2^L,$$

and setting

$$c_n=\begin{cases}1 & \text{for}\quad 1\leqq n\leqq N\\ 0 & \text{for}\quad N<n\leqq 2^L\end{cases},$$

we define for $1\leqq n\leqq 2^L$

$$S(n,\chi)=\sum_{m\leq n}c_m\Lambda(m)\chi(m).$$

For integers k, l with $1\leqq k\leqq 2^l$, $0\leqq l\leqq L$, we put

$$S_{k,l}(\chi)=\sum_{m=(k-1)2^{L-l}+1}^{k2^{L-l}}c_m\Lambda(m)\chi(m)$$

and write for $(q, h)=1$

$$T_l(q, h)=\max_{1\leq k\leq 2^l}\left|\frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}\overline{\chi}(h)S_{k,l}(\chi)\right|.$$

If we put

$$\Delta(N, q, h)=\max_{n\leq N}\left|\psi(n, q, h)-\frac{S(n, \chi_0)}{\phi(q)}\right|,$$

where χ_0 is the principal character to the modulus q, then we have, on taking account of the dyadic development of an integer n, $1\leqq n\leqq N$,

$$\Delta(N, q, h)\leqq\sum_{l=0}^{L} T_l(q, h),$$

so that

$$(\Delta(N, q, h))^2\leqq(L+1)\sum_{l=0}^{L}(T_l(q, h))^2$$

by Cauchy-Bunjakovskiĭ's inequality. Hence, putting

$$Q=N(\log N)^{-A},$$

we get

$$(1)\qquad \sum_{q\leqq Q}\sum_{(h,q)=1}(\Delta(N, q, h))^2\leqq(L+1)\sum_{l=0}^{L}\sum_{q\leqq Q}\sum_{(h,q)=1}(T_l(q, h))^2.$$

We need the following lemma, for a proof of which we refer to [5; IV. Satz 7.2 combined with Satz 8.2]:

Lemma. *If* χ *is a non-principal character* (mod q), *then there holds the inequality*

$$|S(n, \chi)|\leqq Bn\exp(-c_1(\log n)^{1/2})$$

uniformy for $q\leqq(\log n)^H$, *where* $H>0$ *is any fixed number,* $B=B(H)>0$ *and* $c_1=c_1(H)>0$.

Now we have

$$\sum_{(h,q)=1}(T_l(q, h))^2\leqq\sum_{(h,q)=1}\sum_{k=1}^{2^l}\left|\frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}\overline{\chi}(h)S_{k,l}(\chi)\right|^2$$

$$=\sum_{k=1}^{2^l}\frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}|S_{k,l}(\chi)|^2$$

and so

$$(2)\qquad \sum_{q\leqq Q}\sum_{(h,q)=1}(T_l(q, h))^2\leqq\sum_{k=1}^{2^l}\sum_{q\leqq Q}\frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}|S_{k,l}(\chi)|^2.$$

Since each non-principal character χ (mod q) is equivalent to a primitive character χ^* to a modulus d with $d|q, d>1$, and $\chi(n)=\chi^*(n)$ unless $(n, q)\neq 1$, it follows that

$$S_{k,l}(\chi)=S_{k,l}(\chi^*)+R_{k,l}(\chi),$$

where

$$|R_{k,l}(\chi)|\leq \sum_{\substack{(k-1)2^{L-l}<p^\nu\leq k2^{L-l}\\ p|q}} \log p = R_{k,l}, \text{ say. Hence, noticing that}$$

$$\sum_{\chi\neq\chi_0}|S_{k,l}(\chi)|^2\leq 2\sum_{\substack{d|q\\ d>1}}\sum_{\chi \pmod d}^{*}|S_{k,l}(\chi)|^2+2\phi(q)R_{k,l}^2,$$

where $\sum_\chi^*$ indicates that the sum is taken over primitive characters χ only, and using

$$\sum_{\substack{q\leq Q\\ d|q}}\frac{1}{\phi(q)}\leq B\frac{1+\log(Q/d)}{\phi(d)},$$

we find

$$\sum_{k=1}^{2^l}\sum_{q\leq Q}\frac{1}{\phi(q)}\sum_{\chi\neq\chi_0}|S_{k,l}(\chi)|^2$$

(3) $$\leq B\sum_{k=1}^{2^l}\sum_{1<d\leq Q}a(d)\sum_{\chi (\mathrm{mod}\ d)}^{*}|S_{k,l}(\chi)|^2+R,$$

where

$$a(d)=\frac{1+\log(Q/d)}{\phi(d)}$$

and

$$R\leq 2\sum_{k=1}^{2^l}\sum_{q\leq Q}R_{k,l}^2\leq 2\sum_{q\leq Q}\Big(\sum_{k=1}^{2^l}R_{k,l}\Big)^2$$

$$\leq 2\sum_{q\leq Q}\Big(\sum_{\substack{p^\nu\leq N\\ p|q}}\log p\Big)^2$$

$$\leq BQ(\log Q)^2(\log N)^2\leq B\frac{N^2}{(\log N)^A}.$$

Put

$$D=(\log N)^{A+1}$$

and

$$E=\exp(c_2(\log N)^{1/2})$$

with

$$c_2=c_1(A+2)/2>0.$$

For the terms with $1<d\leqq D$ in the first member on the right-hand side of (3) we argue in the following way. If $2^l\leqq E$, then we have uniformly in $1\leqq k\leqq 2^l$

$$\log k2^{L-l}=\log N+O((\log N)^{1/2})$$

so that

$$(\log k2^{L-l})^{1/2}>\frac{1}{2}(\log N)^{1/2}$$

and

$$(\log k2^{L-l})^{A+2}>(\log N)^{A+1}$$

for $N>n_1(A)$. Hence, applying the lemma with $H=A+2$, we find for $N>n_2(A)$

$$\sum_{k=1}^{2^l}\sum_{1<d\leqq D} a(d)\sum_{\chi}{}^{*}|S_{k,2}(\chi)|^2$$
$$\leqq\sum_{k=1}^{2^l}\sum_{d\leqq D}\left(1+\log\frac{Q}{d}\right)Bk^2 2^{2L-2l}\exp(-c_1(\log N)^{1/2})$$
$$\leqq BN^2DE\exp(-c_1(\log N)^{1/2})\leqq B\frac{N^2}{(\log N)^A}.$$

If $2^l>E$, then we have evidently

$$|S_{k,l}(\chi)|\leqq 2^{L-l}\log N$$

for all χ and all $1\leqq k\leqq 2^l$. Hence

$$\sum_{k=1}^{2^l}\sum_{1<d\leqq D} a(d)\sum_{\chi}{}^{*}|S_{k,l}(\chi)|^2$$
$$\leqq\sum_{k=1}^{2^l}\sum_{d\leqq D}\left(1+\log\frac{Q}{d}\right)2^{2L-2l}(\log N)^2$$
$$\leqq BN^2DE^{-1}(\log N)^2\leqq B\frac{N^2}{(\log N)^A}$$

for $N>n_3(A)$. It follows that for $N>n_4(A)=\max\ (n_2(A),\ n_3(A))$ we have in either case

$$\sum_{k=1}^{2^l}\sum_{1<d\leqq D} a(d)\sum_{\chi}{}^{*}|S_{k,l}(\chi)|^2\leqq B\frac{N^2}{(\log N)^A}\tag{4}$$

uniformly in $0\leqq l\leqq L$, which is also valid for $2\leqq N\leqq n_4(A)$ by a suitable replacement of B if necessary.

In order to treat the terms with $D<d\leqq Q$ in the first member on the right-hand side of (3), we follow the argument of P. X. Gallagher [3]. Thus, putting

$$b(t)=\frac{1+\log(Q/t)}{t},$$

we have

$$\sum_{D<d\leqq Q} a(d) \sum_{\chi}^{*} |S_{k,l}(\chi)|^2$$
$$\leqq Bb(D)(D^2+2^{L-l})+\int_D^Q b(t)t\,dt\, Z_{k,l}$$
$$\leqq BQZ_{k,l},$$

where B is uniform in l and where

$$Z_{k,l}=\sum_{m=(k-1)2^{L-l}+1}^{k2^{L-l}} c_m(\Lambda(m))^2.$$

Since

$$\sum_{k=1}^{2^l} Z_{k,l}=\sum_{n\leqq N}(\Lambda(n))^2\leqq B\,N\log N,$$

we obtain

$$\sum_{k=1}^{2^l}\sum_{D<d\leqq Q} a(d) \sum_{\chi}^{*} |S_{k,l}(\chi)|^2\leqq B\frac{N^2}{(\log N)^{A-1}} \tag{5}$$

which holds uniformly in l.

It now follows from (1), (2), (3), (4) and (5) that

$$\sum_{q\leqq Q}\sum_{(h,q)=1}(\Delta(N,q,h))^2\leqq B\frac{N^2}{(\log N)^{A-3}},$$

and this proves Theorem 2, since we have

$$S(n,\chi_0)=n+O(n\exp(-c_3(\log n)^{1/2}))+O((\log q)\log n)$$

for all $n\geqq 1$, where χ_0 is the principal character to the modulus q.

Proof of Theorem 1.

If we write

$$\psi(x,q,h)=\theta(x,q,h)+\rho(x,q,h),$$

then $\rho(x,q,h)\geqq 0$ and

$$\sup_{y\leq x}\left(\theta(y, q, h)-\frac{y}{\phi(q)}\right)^2$$
$$\leqq 2\sup_{y\leq x}\left(\psi(y, q, h)-\frac{y}{\phi(q)}\right)^2+2\sup_{y\leq x}(\rho(y, q, h))^2.$$

Thus, it will suffice to show

$$\sum_{q\leq x(\log x)^{-A}}\ \sum_{(h,q)=1}\ \sup_{y\leq x}(\rho(y, q, h))^2\leqq B\frac{x^2}{(\log x)^{A-2}}\ . \tag{6}$$

Again, we shall assume that $x=N$ and $y=n$ are integer valued variables and that $N\geqq 2$. As before, we put

$$c_n=\begin{cases}1 & \text{for}\quad 1\leqq n\leqq N\\ 0 & \text{for}\quad N<n\leqq 2^L\end{cases},$$

where $2^{L-1}<N\leqq 2^L$. Setting

$$a_n=\begin{cases}1 & \text{if } n \text{ is a prime}\\ 0 & \text{otherwise}\end{cases},$$

we put for integers k, l with $1\leqq k\leqq 2^l$, $0\leqq l\leqq L$,

$$\rho_{k,l}(q, h)=\sum_{m=(k-1)2^{L-l}+1}^{k2^{L-l}} c_m(1-a_m)\Lambda(m)$$

and define

$$\sigma_l(q, h)=\max_{1\leq k\leq 2^l}\rho_{k,l}(q, h).$$

(Note that $c_m(1-a_m)\Lambda(m)\geqq 0$ for all m, $1\leqq m\leqq 2^L$.) Then we have

$$\delta(N, q, h)\overset{\text{def}}{=}\max_{n\leq N}\rho(n, q, h)\leqq\sum_{l=0}^{L}\sigma_l(q, h).$$

and the inequality of Cauchy-Bunjakovskiĭ gives

$$\begin{aligned}(\delta(N, q, h))^2&\leqq(L+1)\sum_{l=0}^{L}(\sigma_l(q, h))^2\\ &\leqq(L+1)\sum_{l=0}^{L}\sum_{k=1}^{2^l}(\rho_{k,l}(q, h))^2\\ &\leqq(L+1)\sum_{l=0}^{L}\left(\sum_{k=1}^{2^l}\rho_{k,l}(q, h)\right)^2\\ &=(L+1)^2(\rho(N, q, h))^2,\end{aligned}$$

whence

$$\sum_{(h,q)=1}(\delta(N,q,h))^2 \leqq (L+1)^2 \sum_{(h,q)=1}(\rho(N,q,h))^2$$
$$\leqq (L+1)^2\Big(\sum_{(h,q)=1}\rho(N,q,h)\Big)^2.$$

Since

$$L+1 \leqq B\log N$$

and since we have

$$\sum_{(h,q)=1}\rho(N,q,h) = O(N^{1/2})+O((\log q)\log N)$$

uniformly in q, we obtain

$$\sum_{q\leqq N(\log N)^{-A}}\ \sum_{(h,q)=1}(\delta(N,q,h))^2 \leqq B\frac{N^2}{(\log N)^{A-2}}$$

which is equivalent to the desired result (6).

Acknowledgement (added in proof, June 12, 1972).

In [6] the author proved that if $p(k,\ l)$ denotes the least prime number in the arithmetic progression $l \pmod k$, $(l,\ k)=1$, $0\leqq l<k$, and if A is an arbitrary real number with $A>3$, then for almost all (i. e. all but possibly a sequence of zero density) integers k we have

$$p(k,\ l)<\phi(k)(\log k)^A$$

for nearly $\phi(k)$ values of l with $(l,\ k)=1$, $1\leqq l<k$. The proof depended essentially on Theorem 1 of the present note. It has been brought to the author's attention that the above result on $p(k,l)$ had already been obtained, even with $A>1$ instead of $A>3$, by P. D. T. A. Elliott and H. Halberstam: The least prime in an arithmetic progression (Studies in Pure Mathematics Presented to Richard Rado. Edited by L. Mirsky. Academic Press, London and New York, 1971; pp. 59—61). The writer regrets that he had been unaware of this result of Elliott and Halberstam; the present paper will, however, not entirely lose its interest and meaning, as it seems to contain something new.

REFERENCES

[1] E. BOMBIERI: On the large sieve. Mathematika, **12**, 201—225 (1965).

[2] H. DAVENPORT and H. HALBERSTAM: Primes in arithmetic progressions. Michigan Math. J., **13**, 485—489 (1966).

[3] P. X. GALLAGHER: The large sieve. Mathematika, **14**, 14—20 (1967).
[4] H. L. MONTGOMERY: Primes in arithmetic progressions. Michigan Math. J., **17**, 33—39 (1970).
[5] K. PRACHAR: Primzahlverteilung. Springer-Verl., Berlin-Göttingen-Heidelberg, 1957.
[6] S. UCHIYAMA: An application of the large sieve. Proc. Japan Acad., **48**, 67—69 (1972).

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received April 6, 1972)