156. On the Existence of Prime Numbers in Arithmetic Progressions

By Zen'ichirô KOSHIBA and Saburô UCHIYAMA
Department of Mathematics, Shinshû University, Matsumoto

(Comm. by Zyoiti SUETUNA, M.J.A., Sept. 12, 1966)

The classical theorem of P. G. Lejeune Dirichlet on prime numbers in arithmetic progressions states that, if k and l are two integers with $k\geqq 1$, $(k, l)=1$, then there exist infinitely many primes $p\equiv l \pmod k$. Several elementary proofs are known of this monumental result, with or without the use of the Dirichlet characters to modulus k (cf. e.g. [3; Chap. 9, § 8], [5], [6], [7], [8]), and some of them rest upon the celebrated inequality due to A. Selberg [5]:

$$(1) \qquad \sum_{\substack{p\leqq x \\ p\equiv l \pmod k}} \log^2 p+\sum_{\substack{pq\leqq x \\ pq\equiv l \pmod k}} \log p \log q=\frac{2}{\phi(k)}x\log x+O(x)$$

as $x\to\infty$, where $\phi(k)$ is the Euler totient function.

Our main interest in the present note is to give another proof of the theorem of Dirichlet on the basis of the inequality (1) by showing that

$$(2) \qquad \sum_{\substack{p\leqq x \\ p\equiv l \pmod k}} \frac{\log p}{p}>c\log x \quad (x\to\infty)$$

with some constant $c>0$ (depending on k) implies that

$$\sum_{\substack{p\leqq x \\ p\equiv l \pmod k}} \frac{\log p}{p}\sim\frac{1}{\phi(k)}\log x \quad (x\to\infty)$$

for any l relatively prime to k.

It should be noted that we can prove the inequality (2) by an elementary argument (cf. [7, I]). As a matter of fact, a slightly weaker condition than (2) will suffice for our purpose. Indeed, one may replace, on the right-hand side of (2), $c\log x$ by $(\log\log x)^{\alpha}$, α being an arbitrary but fixed real number >1.

1. Let k be a fixed integer $\geqq 1$ and l be any integer with $(k, l)=1$.

We use partial summation to get from (1)

$$(3) \qquad \sum_{\substack{p\leqq x \\ p\equiv l \pmod k}} \frac{\log^2 p}{p}+\sum_{\substack{pq\leqq x \\ pq\equiv l \pmod k}} \frac{\log p\log q}{pq} =\frac{1}{\phi(k)}\log^2 x+O(\log x).$$

If we put $x=e^n$ and for $(h, k)=1$ $s_m(h)=\sum_{\nu=0}^{m} a_\nu(h)$ $(m=0, 1, 2, \cdots)$, where

$$a_\nu(h)=\sum_{\substack{e^\nu\leqq p<e^{\nu+1} \\ p\equiv h \pmod k}} \frac{\log p}{p}=O(1) \quad (\nu=0, 1, 2, \cdots),$$

then it follows from (3) that

$$(4)\qquad \sum_{\nu=0}^{n}\Big(\nu a_\nu(l)+\sum_{(h,k)=1} a_\nu(h)s_{n-\nu}(\bar{h}l)\Big)=\frac{1}{\phi(k)}n^2+O(n)$$

as $n\to\infty$, where $\sum_{(h,k)=1}$ indicates the summation over a complete set of residues h (mod k) prime to k and, for $(h,k)=1$, $\bar{h}$ is an integer uniquely determined (mod k) by the condition $h\bar{h}\equiv 1$ (mod k).

We define for $(h,k)=1$ and $s>0$ the functions $f_h(s)$ by

$$f_h(s)=\sum_{\nu=0}^{\infty} a_\nu(h)e^{-\nu s}:$$

the series on the right is absolutely convergent for $s>0$. Noticing that $(1-e^{-s})^{-1}=s^{-1}+O(1)$ for $s>0$, we then deduce from the relation (4) that

$$(5)\qquad \frac{d}{ds}f_l(s)-\sum_{(h,k)=1} f_h(s)f_{\bar{h}l}(s)=-\frac{2}{\phi(k)}\frac{1}{s^2}+O\Big(\frac{1}{s}\Big)$$

for $s\downarrow 0$.

Now, let χ denote a Dirichlet character to modulus k and put

$$F(s,\chi)=\sum_{(h,k)=1}\chi(h)f_h(s).$$

Since we have $\sum_{(h,k)=1}\chi(h)=\phi(k)$ $(\chi=\chi_0)$, $=0$ $(\chi\neq\chi_0)$, χ_0 being the principal character (mod k), we find from (5) that for $s\downarrow 0$

$$\frac{d}{ds}F(s,\chi)-(F(s,\chi))^2=-\frac{2e(\chi)}{s^2}+O\Big(\frac{1}{s}\Big),$$

where $e(\chi)=1$ $(\chi=\chi_0)$, $=0$ $(\chi\neq\chi_0)$.

2. In order to determine the asymptotic behaviour of the functions $F(s,\chi)$ for $s\downarrow 0$ we require the following two Lemmas.*) Let us set $y=F(s,\chi)$.

Lemma 1. *The equation*

$$\frac{dy}{ds}-y^2=-\frac{2}{s^2}+O\Big(\frac{1}{s}\Big)\qquad (s\downarrow 0)$$

implies that either

$$y=\frac{1}{s}+O(1)\qquad (s\downarrow 0)$$

or

$$y=-\frac{2}{s}+O(1)\qquad (s\downarrow 0).$$

This result is due to J. Korevaar [4].

Lemma 2. *The equation*

$$\frac{dy}{ds}-y^2=O\Big(\frac{1}{s}\Big)\qquad (s\downarrow 0)$$

implies that either

$$y=O\Big(\log\frac{1}{s}\Big)\qquad (s\downarrow 0)$$

---

*) It is possible to avoid the use of the result in Lemma 1 by directly appealing to the fact that $\sum_{p\leq x}(\log p)/p=\log x+O(1)$.

or

$$y=-\frac{1}{s}+O(1) \qquad (s \downarrow 0).$$

We postpone the proof of Lemma 2 until the end of this note.

It is not difficult to see that the second possibilities in Lemmas 1 and 2 cannot occur for any of our functions $y=F(s,\chi)$, if one observes that for $(h,k)=1$

$$f_h(s)=\frac{1}{\phi(k)}\sum_{\chi(\mathrm{mod}\, k)}\chi(\bar{h})F(s,\chi)$$

and that the assumption (2) implies that $f_1(s)>c/s$ $(s \downarrow 0)$ with some constant $c>0$. We thus obtain for $(k,l)=1$

$$f_l(s)=\frac{1}{\phi(k)}\frac{1}{s}+O\left(\log\frac{1}{s}\right) \qquad (s \downarrow 0). \tag{6}$$

This relation (6) already proves the theorem of Dirichlet mentioned at the beginning of this note. For, if there were some integers k, l with $k\geqq 1$, $(k,l)=1$, for which only a finite number of primes $p\equiv l \pmod k$ exist, then the function $f_l(s)=\sum a_\nu(l)e^{-\nu s}$ would remain bounded as $s\downarrow 0$, which, however, is impossible in view of (6).

Now, by a well-known Tauberian theorem for power series (cf. [2; Theorem 96 or 98]), we readily conclude from (6) that for $(k,l)=1$

$$s_n(l)\sim\frac{1}{\phi(k)}n \qquad (n\to\infty)$$

or

$$\sum_{\substack{p\leqq x\\ p\equiv l\ (\mathrm{mod}\ k)}}\frac{\log p}{p}\sim\frac{1}{\phi(k)}\log x \qquad (x\to\infty),$$

which was the result to be proved.

We note that a slightly more precise result than the above, i.e. the relation

$$\sum_{\substack{p\leqq x\\ p\equiv l\ (\mathrm{mod}\ k)}}\frac{\log p}{p}=\frac{1}{\phi(k)}\log x+O(1)$$

as $x\to\infty$, can in fact be obtained (cf. [3; Chap. 9, § 8]).

3. It now remains to prove Lemma 2. Consider the differential equation

$$\frac{dy}{ds}-y^2=R(s), \tag{7}$$

where $R(s)=O(s^{-1})$ $(s\downarrow 0)$. If we put

$$v=v(t)=tu(t^{-1}),\ t=s^{-1},$$

after the substitution

$$y=-\frac{1}{u}\frac{du}{ds}, \qquad u=u(s),$$

then we have

$$y=-t+tC(t) \quad \text{with} \quad C(t)=\frac{t}{v}\frac{dv}{dt},$$

and the equation (7) becomes

$$\frac{d^2v}{dt^2}+A(t)v=0, \tag{8}$$

where

$$A(t)=\frac{1}{t^4}R\left(\frac{1}{t}\right)=O\left(\frac{1}{t^3}\right) \qquad (t\to\infty).$$

By integrating twice between t_0 and t, where t_0 is a fixed positive real number, we obtain from (8)

$$\frac{dv}{dt}=c_1-\int_{t_0}^{t}A(\tau)v(\tau)d\tau \tag{9}$$

and

$$v=c_0+c_1t-\int_{t_0}^{t}(t-\tau)A(\tau)v(\tau)d\tau \tag{10}$$

with some constants c_0 and c_1.

It is not difficult to show that $v(t)=O(t)$ $(t\to\infty)$ and the limit $\lim\limits_{t\to\infty}\frac{dv}{dt}=c$ exists (cf. [1; Chap. 6, Theorem 5 and its proof]). We have, therefore,

$$\begin{aligned}\frac{dv}{dt}&=c_1-\int_{t_0}^{\infty}A(\tau)v(\tau)d\tau+\int_{t}^{\infty}A(\tau)v(\tau)d\tau\\ &=c+O(t^{-1}) \qquad (t\to\infty),\end{aligned} \tag{11}$$

and, using (11) in (10),

$$\begin{aligned}v&=c_0+c_1t-t\int_{t_0}^{t}A(\tau)v(\tau)d\tau+\int_{t_0}^{t}\tau A(\tau)v(\tau)d\tau\\ &=c_0+ct+t\int_{t}^{\infty}A(\tau)v(\tau)d\tau+\int_{t_0}^{t}\tau A(\tau)v(\tau)d\tau\\ &=ct+O(\log t) \qquad (t\to\infty).\end{aligned} \tag{12}$$

If $c\neq 0$ then we have

$$C(t)=\frac{t}{v}\frac{dv}{dt}=\frac{ct+O(1)}{ct+O(\log t)}=1+O\left(\frac{\log t}{t}\right) \qquad (t\to\infty),$$

so that $y=O(\log t)$ $(t\to\infty)$ or

$$y=O\left(\log\frac{1}{s}\right) \qquad (s\downarrow 0).$$

If $c=0$ then it follows from (12) that $v=O(\log t)$ $(t\to\infty)$ and the integral

$$\int_{t_0}^{\infty}\tau A(\tau)v(\tau)d\tau=c'$$

converges. Hence we have

$$v=c_0+t\int_t^\infty A(\tau)v(\tau)d\tau+c'-\int_t^\infty \tau A(\tau)v(\tau)d\tau$$
$$=c_0+c'+O\left(\frac{\log t}{t}\right) \qquad (t\to\infty),$$

which yields via (10)

$$v=c_0+c'+O\left(\frac{1}{t}\right) \qquad (t\to\infty).$$

Noticing that

$$v-t\frac{dv}{dt}=c_0+\int_{t_0}^t \tau A(\tau)v(\tau)d\tau$$
$$=c_0+c'+O(t^{-1}) \qquad (t\to\infty),$$

we obtain

$$t\frac{dv}{dt}=O\left(\frac{1}{t}\right) \qquad (t\to\infty).$$

Thus, if $c=0$ and $c_0+c'\neq 0$, then

$$C(t)=\frac{O(t^{-1})}{c_0+c'+O(t^{-1})}=O\left(\frac{1}{t}\right) \qquad (t\to\infty),$$

so that $y=-t+O(1)$ $(t\to\infty)$ or

$$y=-\frac{1}{s}+O(1) \qquad (s\downarrow 0).$$

If $c=0$ and $c_0+c'=0$, then $v=v(t)=0$ for all $t>0$. For, since there are constants $A>0$ and $K>0$ such that we have, for $t\geqq t_0$, $|A(t)|\leqq At^{-3}$, and $|v(t)|\leqq Kt^{-1}$, we see from (10) with $c=c_0+c'=0$, i.e. from the relation

$$v(t)=t\int_t^\infty A(\tau)v(\tau)d\tau-\int_t^\infty \tau A(\tau)v(\tau)d\tau,$$

that

$$|v(t)|\leqq KA\left(\frac{1}{3}+\frac{1}{2}\right)\frac{1}{t^2} \qquad (t\geqq t_0).$$

Thus we have, by induction,

$$|v(t)|\leqq KA^m\prod_{j=1}^m\left(\frac{1}{j+2}+\frac{1}{j+1}\right)\frac{1}{t^{m+1}} \qquad (t\geqq t_0)$$

for every integral $m\geqq 0$. Since

$$\prod_{j=1}^m\left(\frac{1}{j+2}+\frac{1}{j+1}\right)\leqq\frac{2^m}{(m+1)!} \qquad (m\geqq 0)$$

and $t_0>0$ is arbitrary, this proves the assertion.

Our proof of Lemma 2 is now complete.

References

[1] R. Bellman: Stability Theory of Differential Equations. New York-Toronto-London (1953).
[2] G. H. Hardy: Divergent Series. London (1956).

[3] L.-K. Hua: Introduction to Number Theory (in Chinese). Peking (1964).
[4] J. Korevaar: Notes on differential equations. I. Analogue of a nonlinear Tauberian theorem of Erdös. Bull. Amer. Math. Soc., **62**, 42 (1956).
[5] A. Selberg: An elementary proof of Dirichlet's theorem about primes in an arithmetic progression. Ann. of Math., **50**, 297-304 (1949).
[6] ——: An elementary proof of the prime-number theorem for arithmetic progressions. Canadian J. of Math., **2**, 66-78 (1950).
[7] H. N. Shapiro: On primes in arithmetic progressions (I), (II). Ann. of Math., **52**, 217-230, 231-243 (1950).
[8] H. Zassenhaus: Über die Existenz von Primzahlen in arithmetischen Progressionen. Comment. Math. Helvetici, **22**, 232-259 (1949).