

Theory of arithmetic linear transformations and its application to an elementary proof of Dirichlet's theorem.

By Koichi YAMAMOTO

(Received Nov. 25, 1955)

Introduction.

A. Selberg [8] proved Dirichlet's theorem about the primes in an infinite arithmetic progression in an elementary way. His basic idea was in the introduction of a new kind of asymptotic formulas, a typical one being the so-called Selberg's asymptotic equality. His method, however, is not entirely different from those used in classical proofs since Dirichlet, and this fact is explained in the present paper by a principle, which we would call theory of arithmetic linear transformations.

This principle was, in its essence, perceived by many authors, notably by Möbius, Glaisher (Cf. [2, Chapt. XIX]), Landau, Selberg and others (Cf. [7, 10]), but seems not fully recognized.

It is observed that any of the existing proofs of Dirichlet's theorem consists of the two steps. The first, and the formal part is the derivation of the theorem from the fact that $\beta(\chi) = \sum_{n=1}^{\infty} \chi(n)/n \neq 0$ for any non-principal real character $\chi \pmod{k}$. And the second, more conceptual part is the proof of this fact.

As for the first part, the classical proofs make use of Dirichlet L -functions associated with characters $\chi \pmod{k}$ (which are generating functions of χ in the form of Dirichlet series), whereas Selberg replaces it by Selberg's asymptotic equality. In the idea of the proof, the classical method is more elementary, since it aims to generalize the well-known Mertens-Polignac formula $\sum_{p \leq x} \log p/p = \log x + O(1)$, whereas Selberg uses a more complicated sum. Here we can proceed along the classical line without resorting to L -functions.

As for the second step, the classical (Mertens-Landau [4, 5,]) method is decisively simpler, if not natural, since Selberg's method cannot avoid the use of the reciprocity law of quadratic residues. We can again give an interpretation of the former, which seems readily to be generalized to any algebraic number field.

§ 1. Arithmetic linear transformations.

1.—Let A be the totality of complex-valued arithmetic functions α , and let F be the totality of complex-valued functions f defined over the interval $(0, +\infty)$ such that $f(x)=0$ over $(0, 1)$. A is naturally imbedded in F by putting $\alpha(x)=0$ for non-integral values of x . This injection map will be denoted by $i: \alpha \rightarrow i(\alpha)$.

For $\alpha \in A$ and $f \in F$ we define $S_a f$ by

$$(1) \quad (S_a f)(x) = \sum_n \alpha(n) f(x/n).$$

The summation may be restricted to $1 \leq n \leq x$, and it is obvious that $S_a f \in F$. S_a is hence a linear transformation of F , which we shall call an *arithmetic linear transformation*. If $\beta \in A$ we have

$$S_a i(\beta) = i(\alpha * \beta),$$

where $\alpha * \beta$ is called the *convolution* of α and β :

$$(\alpha * \beta)(n) = \sum_{m|n} \alpha(m) \beta(n/m).$$

It is also obvious that

$$(2) \quad S_a f + S_b f = S_{a+\beta} f,$$

$$S_a S_b f = S_{a * \beta} f,$$

$$(3) \quad \alpha * (\beta * \gamma) = (\alpha * \beta) * \gamma.$$

Note that (3) is the special case of (2). Now A forms a commutative ring with respect to $(+, *)$, whose unit element ϵ is defined by

$$(4) \quad \epsilon(n) = \delta_{n,1} \quad (\text{Kronecker delta}).$$

The α with $\alpha(1) \neq 0$ has an inverse $\alpha^{(-1)}$.

2.—The family A forms another ring $A(+, \cdot)$ with respect to addition (+) and term-by-term multiplication (\cdot). The unit element ι is here defined by

$$(5) \quad \iota(n) = 1 \quad (\text{for any } n).$$

The inverse of ι in the sense of convolution is denoted by μ , where

$$(6) \quad \begin{aligned} \mu(n) &= (-1)^s, \quad \text{if } n \text{ is product of } s (\geq 0) \text{ distinct primes;} \\ &= 0, \quad \text{otherwise.} \end{aligned}$$

It is the *Möbius' function*. And *Möbius' inversion formula* may be written compactly as

$$(7) \quad S_i f = g \Leftrightarrow S_\mu g = f,$$

$$(8) \quad \iota * \alpha = \beta \Leftrightarrow \mu * \beta = \alpha,$$

the two forms corresponding to (2) and (3). The second is conveniently written as

$$(9) \quad (\mu * \beta)(n) = \prod_{p|n} \Delta_p \beta(n),$$

where Δ_p is an analogue of difference operator Δ in the theory of finite differences:

$$(10) \quad \Delta_p \alpha(n) = \alpha(n) - \alpha(n/p).$$

3.—We denote by L the arithmetic function

$$(11) \quad L(n) = \log n.$$

Then we have

$$(12) \quad L(\alpha * \beta) = L\alpha * \beta + \alpha * L\beta,$$

or the term-by-term multiplication by L yields a *derivation* of the ring $A(+, *)$. The last formula has its counterpart in F :

$$(13) \quad \log x S_a f(x) = S_{La} f(x) + S_a \log x f(x).$$

A very important family of arithmetic functions is defined by

$$(14) \quad \Lambda_m = \mu * L^m \quad (m=0, 1, 2, \dots).$$

(L^0 denotes of course ι .) $\Lambda_1 = \Lambda$ is *von Mangoldt's function*, and Λ_2 is *Selberg's function*. In a more explicit form they are given by (Cf. [10])

$$(15) \quad \begin{aligned} \Lambda(n) &= L(p), & \text{if } n \text{ is power of prime } p, \\ &= 0, & \text{otherwise;} \\ \Lambda_2(n) &= (2e-1)L^2(p), & \text{if } n=p^e \text{ and } p \text{ prime,} \\ &= 2L(p)L(q), & \text{if } n=p^e q^f \text{ where } p, q \text{ are} \\ (16) & & \text{distinct primes,} \\ &= 0, & \text{otherwise;} \end{aligned}$$

and in general if $n=p_1^{e_1} \dots p_s^{e_s}$ where p_1, \dots, p_s are distinct primes,

$$(17) \quad \Lambda_m(n) = \sum \frac{m!}{j_1! \dots j_s!} \varpi e^{j_1} \dots \varpi e^{j_s} L(p_1)^{j_1} \dots L(p_s)^{j_s},$$

summation being taken over all positive integral solutions (j_1, \dots, j_s) of $m=j_1 + \dots + j_s$, and where $\varpi e^j = e^j - (e-1)^j$, for instance $\Lambda_m(n) = 0$ if $s > m$, i. e., if n has more than m distinct prime factors.

4.— $\alpha \in A$ is termed *multiplicative* if $\alpha(mn) = \alpha(m)\alpha(n)$ for $(m, n) = 1$ and *factorable* if $\alpha(mn) = \alpha(m)\alpha(n)$ unconditionally. In either case $\alpha = 0$ (i. e., $\alpha(n) = 0$ for any n), or $\alpha(1) = 1$ and $\alpha^{(-1)}$ exists.

If α and β are multiplicative, $\alpha\beta$ and $\alpha * \beta$ are multiplicative, and if $\alpha \neq 0$ is multiplicative $\alpha^{(-1)}$ is so.

If α and β are factorable, $\alpha\beta$ is factorable.

If α is factorable, then

$$(18) \quad \alpha(\beta * \gamma) = \alpha\beta * \alpha\gamma.$$

5.—Now let $k > 1$ be an integer, and a be an integer such that $(a, k) = 1$, $0 < a < k$. For any of these $\varphi(k)$ values of a we define arithmetic functions ι_a by $\iota_a(n) = 1$ or 0 , according as $n \equiv a$, or $n \not\equiv a \pmod{k}$. These functions ι_a will form a group if we define their composition by $\iota_a \circ \iota_b = \iota_c$, for $c \equiv ab \pmod{k}$; and the characters of

this group are *characters* mod k . Denote these characters by χ, \dots . Then as is well known

$$(19) \quad \begin{aligned} \chi &= \sum_a \chi(a) \iota_a, \\ \iota_a &= \frac{1}{\varphi(k)} \sum_{\bar{x}} \overline{\chi(a)}, \end{aligned}$$

the bar indicating of course conjugate complex.

6.—Let 1 denote the unit element of the ring F , i. e., the function with constant value 1 over $[1, \infty)$ and 0 over $(0, 1)$. We define the *trace* $T(\alpha)$ of the element $\alpha \in A$ by $T(\alpha) = S_a 1$. Note that this is the function of x , though the argument x is not written explicitly. We have for instance

$$(20) \quad \begin{aligned} T(\iota) &= [x], \\ T(\alpha * \beta) &= S_a T(\beta) = S_\beta T(\alpha), \end{aligned}$$

and the *Selberg's asymptotic equality* may be written as

$$(21) \quad T(\Lambda_2) = 2x \log x + O(x),$$

of which a natural generalization is

$$(22) \quad T(\Lambda_m) = mx \log^{m-1} x + O(x \log^{m-2} x) \quad (m \geq 2),$$

whereas the case $m=1$,

$$(23) \quad T(\Lambda) \sim x$$

is essentially difficult to prove and is equivalent to the prime-number theorem, since $T(\Lambda) = \psi(x)$ is Tchebychef's function.

7.—All the above results are readily extended to the case of an arbitrary (finite) algebraic number field K , with slight modifications. We state them here merely for a future use.

First A is replaced by the totally A_K of arithmetic functions of K , i. e., functions α of integral ideals \mathfrak{a} of K . F remains the same. The definition (1) is replaced by

$$(1') \quad (S_a f)(x) = \sum_{\mathfrak{a}} \alpha(\mathfrak{a}) f(x/N\mathfrak{a}).$$

There is no injection map this time, but the convolution of α and β in A_K is defined directly by

$$(\alpha * \beta)(a) = \sum_{b|a} \alpha(b) \beta(a/b).$$

Instead of (11) we define

$$(11') \quad L(a) = \log Na.$$

Then (7), (8), (12) and (13) remain valid; and (4)–(9), (10), (15)–(18) will be valid if we replace n by α , p by \mathfrak{p} , prime ideal in K , and 1 (in (5)) by \mathfrak{o} , the unit ideal in K .

Next we must replace (20) by the formula of Dedekind, stating that

$$(20') \quad T(\iota) = gx + O(x^{1-1/n}),$$

where g is a positive constant denoting the “natural density” of ideals in K , and n is the degree of K over rational field. Then (21)–(23) will be valid, and can be proved by mere transliteration.

§ 2. Elementary proof of Dirichlet's theorem.

8.—We now return to the case of rational number field and prove some lemmas. These are more or less well known, but we present here just in the form which is ready to be generalized for any algebraic number field.

LEMMA 1. $S_\mu x = O(x)$.

PROOF. $S_\mu x = S_\mu[x] + S_\mu(x - [x]) = S_\mu T(\iota) + S_\mu O(1) = T(\mu * \iota) + O(S_\mu 1) = 1 + O([x]) = O(x)$.

LEMMA 2. $S_i \log x = x + O(\log x)$.

PROOF. $S_i \log x = \log x S_i 1 - S_L 1 = [x] \log x - \log [x]! = x \log x + O(\log x) - (x \log x - x + O(\log x)) = x + O(\log x)$.

LEMMA 3. $\psi(x) = T(\Lambda) = O(x)$.

PROOF. $T(\Lambda) = S_\mu T(L) = S_\mu \log [x]! = S_\mu(x \log x - x + O(\log x)) = S_\mu x \log x + O(x) + O(x)$. But since $S_\mu x = x \sum_{n \leq x} 1/n = x \log x + Cx + O(1)$, with Euler's constant C , we have $x = S_\mu S_i x = S_\mu x \log x + CS_\mu x + S_\mu O(1) = S_\mu x \log x + O(x) + O(x)$, i. e., $S_\mu x \log x = O(x)$.

LEMMA 4. $S_A x = x \log x + O(x)$.

PROOF. $S_A x = S_A[x] + S_A O(1) = S_A T(L) + O(S_A 1) = T(L) + O(\psi(x))$
 $= \log [x]! + O[x] = x \log x + O(x)$. This Lemma is equivalent to the
 Mertens-Polignac formula $\sum_{p \leq x} \log p/p = \log x + O(1)$.

9.—Now let k be an integer > 1 , and χ be a non-principal character mod. k , and put $\beta = \beta(\chi) = \sum_{n=1}^{\infty} \chi(n)/n$.

LEMMA 5. If $\beta \neq 0$, $S_{\chi A} x = O(x)$.

PROOF. It is easy to see that $\sum_{n > x} \chi(n)/n = O(1/x)$. Thus $S_{\chi} x = x \sum_{n \leq x} \chi(n)/n = \beta x - x \sum_{n > x} \chi(n)/n = \beta x + O(1)$. Applying $S_{\chi A}$ we have $S_{\chi A} S_{\chi} x = \beta S_{\chi A} x + OS(1)$, i. e., $S_{\chi L} x = S_{\chi A * \chi} x = \beta S_{\chi A} x + OS_A(1) = \beta S_{\chi A} x + O(x)$, by using (18), (14). Since $\sum_{n \leq x} \chi(n) L(n)/n$ is bounded, $S_{\chi L} x = O(x)$, and $S_{\chi A} x = O(x)$, provided that $\beta \neq 0$.

LEMMA 6. If $\beta = 0$, $S_{\chi A} x = -x \log x + O(x)$.

PROOF. $S_{\chi} x \log x = \log x S_{\chi} x - S_{\chi L} x = (\beta x + O(1)) \log x - S_{\chi L} x = -S_{\chi L} x + O(\log x)$. Applying $S_{\chi \mu}$ we find $x \log x = S_{\chi \mu * \chi} x \log x = -S_{\chi \mu * \chi L} x + S_{\chi \mu} O(\log x) = -S_{\chi A} x + O(x)$.

LEMMA 7. There is at most one non-principal character χ mod k such that $\beta = 0$, and if there exists one such, it must be a real character.

PROOF. By (19) we have

$$(24) \quad \varphi(k) S_{\chi A} x = \sum_{\chi} \chi(a) S_{\chi A} x.$$

Here left-hand side is

$$(25) \quad \varphi(k) x \sum_{\substack{n \leq x \\ n \equiv a \pmod{k}}} \frac{\Lambda(n)}{n} \geq 0,$$

and the right-hand side is, by Lemmas 6 and 7, $= (1-u)x \log x + O(x)$, if we denote by u number of non-principal characters χ with $\beta(\chi) = 0$. This means that $u = 0$ or $u = 1$, and that if $u = 1$, the character χ with $\beta(\chi) = 0$ must be real, since $\beta(\chi) = 0$ and $\beta(\bar{\chi}) = 0$ are equivalent.

There are thus only two possibilities;

A) $u = 0$. Then by (25),

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{k}}} \Lambda(n)/n = (\varphi(k))^{-1} \log x + O(1),$$

which, after standard transformation yields

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{k}}} \log p/p = (\varphi(k))^{-1} \log x + O(1)$$

This, in particular, implies that there are infinitely many primes in the arithmetic progression $a, a+k, a+2k, \dots$.

B) $u=1$. Then denoting the exceptional character by χ we have

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{k}}} \log p/p = (1 - \chi(a))/\varphi(k) \cdot \log x + O(1),$$

which means, roughly speaking, almost all primes satisfy $\chi(p) = -1$.

Thus in order to prove Dirichlet's theorem, we have only to show that $\beta \neq 0$ for any real non-principal character, or that there are "sufficiently many" primes with $\chi(p) = 1$ for each non-principal real character. These two directions correspond to the classical (Mertens-Landau) and Selberg's proofs.

10.—In the rest of the paper χ always denotes a real non-principal character mod. k . We define $\xi = \iota * \chi$ and $\eta = \xi * \xi$. These are multiplicative, as seen from § 4, and if p is a prime, $\xi(p^e) = 1 + \chi(p) + \dots + \chi(p^e) \geq 0$, where the equality sign is valid only when $\chi(p) = -1$ and $2 \nmid e$. Thus

(26) $\xi(n) \geq 0$

and

(27) $\xi(n^2) \geq 1, \quad \xi(pn^2) \geq 1 \quad (\text{for } p \text{ with } \chi(p) = 1),$

for any integer n .

LEMMA 8. $T(\xi) = \beta x + O(\sqrt{x}),$

$$T(\xi) \geq [\sqrt{x}].$$

PROOF. $T(\xi) = \sum_{n \leq x} \xi(n) = \sum_{n \leq x} \sum_{m|n} \chi(m) = \sum_{mn \leq x} \chi(n) = Z_1 + Z_2,$ where Z_1
 $= \sum_{\substack{mn \leq x \\ n \leq \sqrt{x}}} \chi(n) = \sum_{n \leq \sqrt{x}} \chi(n) \sum_{\substack{m \leq x/n \\ n | m}} 1 = \sum_{n \leq \sqrt{x}} \chi(n) \left(\frac{x}{n} + O(1) \right) = \beta x + O(\sqrt{x}) +$

$+O(\sqrt{x}) = \beta x + O(\sqrt{x})$, and $Z_2 = \sum_{\substack{mn \leq x \\ n > \sqrt{x}}} \chi(n) = \sum_{m < \sqrt{x}} \sum_{\substack{\sqrt{x} < n \leq x \\ m}} \chi(n) = \sum_{m < \sqrt{x}} O(1) = O(\sqrt{x})$. This is the first relation. Next it follows from (26), (27) that $T(\xi) = \sum_{n \leq x} \xi(n) \geq \sum_{n^2 \leq x} \xi(n^2) \geq \sum_{n^2 \leq x} 1 = [\sqrt{x}]$.

LEMMA 9. $T(\eta) = \beta(S_\xi x + O(x)) + O(\sqrt{x})$,
 $T(\eta) \geq \frac{1}{4} \sqrt{x} \log x \quad (x \geq 4)$.

PROOF. $T(\eta) = S_\xi T(\xi) = S_\xi(\beta x + O(\sqrt{x})) = \beta S_\xi x + S_\xi O(\sqrt{x})$. As $\xi(n) \geq 0$ and $\sqrt{x}/n \geq 0$ we see that $S_\xi O(\sqrt{x}) = O(S_\xi \sqrt{x})$, and it is sufficient to prove that $S_\xi \sqrt{x} = \beta x + O(\sqrt{x})$, or that

$$(28) \quad \sum_{n \leq x} \frac{\xi(n)}{\sqrt{n}} = \beta \sqrt{x} + O(1).$$

This is just the relation which Mertens [4] and Landau [5] adopted. The relation (28) is proved quite in the same way as the previous Lemma if we use auxiliary evaluations $\sum_{n \leq x} 1/\sqrt{n} = 2\sqrt{x} + B + O(1/\sqrt{x})$ and $\sum_{x < n < y} \chi(n)/\sqrt{n} = O(1/\sqrt{x})$. The second part of the Lemma is simple. In fact $T(\eta) = S_\xi T(\xi) \geq S_\xi[\sqrt{x}] = \frac{1}{2} \sqrt{x} \sum_{n \leq x} \xi(n)/\sqrt{n} \geq \frac{1}{2} \sqrt{x} \sum_{n^2 \leq x} \xi(n^2)/\sqrt{n^2} \geq \frac{1}{4} \sqrt{x} \log x$.

Now Lemma 9 assures that $\beta > 0$, completing a proof of Dirichlet's theorem.

11.—On the other hand Selberg [8] proved that

$$(29) \quad \sum_{x(p)=1} \log p/p > \frac{1}{9} \log x,$$

which is seen equivalent to $\beta \neq 0$. (29) is again equivalent to a weaker one

$$(30) \quad \sum_{x(p)=1} \log p/p = \infty.$$

In proving (29) Selberg used the reciprocity law of quadratic residues, which gives an integer D such that $\chi(p) = (D|p)$ with Legendre symbol, and he showed (29) through an evaluation of the product

$$P = \prod_{\substack{0 < |u| < \sqrt{x} \\ 0 < |v| < \sqrt{x|D|}}} |u^2 - Dv^2|.$$

In view of (30) we may use somewhat simpler product than P ,

$$(31) \quad R = \prod_{\sqrt{|D|} < u < \sqrt{x}} (u^2 - D).$$

Indeed if (30) is false, then $\beta = 0$ and we have $T(\xi) = O(\sqrt{x})$ by Lemma 8. We see from (27) that $T(\xi) \geq \sum_{\substack{\chi(p)=1 \\ p \leq \sqrt{x}}} [\sqrt{x/p}] \geq \sum_{\substack{\chi(p)=1 \\ p \leq \sqrt{x}}} [\sqrt{x/p}]$
 $= \sum_{\substack{\chi(p)=1 \\ p \leq \sqrt{x}}} (\sqrt{x}/\sqrt{p} + O(1)) = \sqrt{x} \left(\sum_{\substack{\chi(p)=1 \\ p \leq \sqrt{x}}} 1/\sqrt{p} + O(1) \right)$ and hence that

$$(32) \quad \sum_{\chi(p)=1} 1/\sqrt{p} < \infty.$$

Now if p divide R , then $(D|p) = \chi(p) = 1$, and the order of R with respect to p is given, for $p \leq \sqrt{x}$, by an analogue of Legendre's formula [2, p. 262]:

$$2[\sqrt{x/p}] + [\sqrt{x/p^2}] + \dots + O(1) = 2\sqrt{x/p} + O(\sqrt{x/p^2}) + O(1),$$

whereas if $p > \sqrt{x}$ and $p|R$ then the order of R with respect to p is 1 or 2. Since it is evident that $\log R = \sqrt{x} \log x + O(\sqrt{x})$, we have

$$\begin{aligned} \sqrt{x} \log x + O(\sqrt{x}) &\leq 2\sqrt{x} \sum_{\substack{\chi(p)=1 \\ p \leq \sqrt{x}}} \log p/p + O(\sqrt{x}) \sum_{\substack{\chi(p)=1 \\ p \leq \sqrt{x}}} \log p/p^2 + \\ &+ O\psi(\sqrt{x}) + 2 \sum_{\substack{p|R \\ p > \sqrt{x}}} \log p = O(\sqrt{x}) + O(\sqrt{x}) + O(\sqrt{x}) + 2 \sum_{\substack{p|R \\ p > \sqrt{x}}} \log p, \\ 2 \sum_{\substack{\chi(p)=1 \\ \sqrt{x} < p \leq x}} \log p &\geq 2 \sum_{\substack{p|R \\ p > \sqrt{x}}} \log p \geq \sqrt{x} \log x + O(\sqrt{x}). \end{aligned}$$

On the other hand, considering (32), we can take x sufficiently large and assume

$$\sum_{\substack{\chi(p)=1 \\ p > \sqrt{x}}} 1/\sqrt{p} < \frac{1}{4}.$$

Then, we would have

$$\begin{aligned} \sqrt{x} \log x + O(\sqrt{x}) &< 2 \sum_{\substack{\chi(p)=1 \\ \sqrt{x} < p \leq x}} \log p = 2 \sum_{\substack{\chi(p)=1 \\ \sqrt{x} < p \leq x}} \sqrt{p} \log p / \sqrt{p} \\ &\leq 2\sqrt{x} \log x \sum_{\substack{\chi(p)=1 \\ p > \sqrt{x}}} 1/\sqrt{p} < \frac{1}{2} \sqrt{x} \log x, \end{aligned}$$

which is a contradiction. This completes again a proof of Dirichlet's theorem.

Kyushu University.

References

- [1] P. G. Ayoub: On Selberg's lemma for algebraic fields, *Canad. Journ. Math.*, 7 (1955), 138-143.
- [2] L. E. Dickson: *History of the theory of numbers*, I, Washington 1919.
- [3] G. H. Hardy and E. M. Wright: *An introduction to the theory of numbers*, Oxford 1938.
- [4] F. Mertens: Über Multiplikation und Nichtverschwinden Dirichletscher Reihen, *Journ. für Math.*, 117 (1897), 169-184.
- [5] E. Landau: Beiträge zur analytischen Zahlentheorie, *Rend. Circ. Mat. Palermo*, 26 (1908), 297.
- [6] E. Landau: *Vorlesungen über Zahlentheorie*, Berlin 1927.
- [7] J. Popken: On convolutions in number theory, *Indagationes Mathematicae*, 17 (1955), 10-15.
- [8] A. Selberg: An elementary proof of Dirichlet's theorem about primes in an arithmetical progression, *Ann. Math.*, 50 (1949), 297-304.
- [9] A. Selberg: An elementary proof of the prime-number theorem, *ibid.*, 305-313.
- [10] H. N. Shapiro: On a theorem of Selberg and generalizations, *Ann. Math.*, 51 (1950), 485-497.