A GENERALIZATION OF MEYER'S THEOREM(1)

BY

IRVING REINER

1. **Introduction.** This paper is concerned with a generalization of the following theorem:

Every properly primitive binary quadratic form represents infinitely many primes in any preassigned arithmetic progression $Mx+N$ consistent with the generic character of the form, where M and N are relatively prime.

Dirichlet [1](2) conjectured this result in 1840, and sketched a method of proof. Weber [4] gave a complete proof for the special case where the words "in any preassigned arithmetic progression $\cdots$" are omitted, and the theorem as stated was finally proved by Meyer [3] in 1888.

The generalization consists of replacing the set of classes of properly primitive binary quadratic forms of given determinant D, which forms a group under composition, by an abelian group H whose elements we denote by θ_i. A correspondence is assumed between H and the set G of numbers $m>0$ which are prime to M and of which D is a quadratic residue. In §§2 and 3, the structures of G and H are examined, and in each case a basis is set up from which all elements may be generated. §4 then gives the specific details of the correspondence between G and H; these details parallel results about the representation of numbers by quadratic forms. Conclusions are then drawn from the correspondence which connects certain of the characters mod M set up in §2 with the group characters constructed in §3.

In §5, the basic Dirichlet series is first defined as

$$L(\chi, \tau; s) = \sum_{\theta_i \text{ in } H} \sum_{m \text{ in } G} a_m(\theta_i)\chi(\theta_i)\tau(m)m^{-s},$$

where $\tau(m)$ is a character mod M, $\chi(\theta_i)$ a group character, $a_m(\theta_i)$ is determined by the correspondence, and where the double summation extends over all elements of G and H. A few of its properties are discussed here, and in §6 sufficient conditions are found for the identity of two such series.

The series are then divided into three different types in §7. Those of the first type become infinite as $s\to 1^+$, while those of the second and third types are finite and different from 0 for $s=1$. The proof of the latter part of this statement is rather involved, and is given in §§7 and 8 after some additional conditions are imposed, without which the theorem fails to be true.

Presented to the Society, September 3, 1947; received by the editors August 6, 1947.

(1) The material of this paper comes from a thesis written under the direction of Professor Burton W. Jones.

(2) Numbers in brackets refer to the bibliography at the end of the paper.

In §9, the theorem is finally stated and its proof is completed. §10 is concerned with the additional conditions referred to in the preceding paragraph, and is devoted to proving a sufficient condition under which they hold. After a brief discussion of Meyer's results in §11, we conclude with an example showing that the new theorem is more general than the original theorem.

We shall use the following notation:

(a, b) denotes the greatest common divisor of a and b.

(a/b) denotes the Jacobi symbol $\left(\frac{a}{b}\right)$.

$\phi(n)$ is the Euler ϕ-function.

$a|b$ means a divides b.

$a\nmid b$ means a does not divide b.

2. **The set** G **and characters mod** M. Let G be a set of positive integers which is closed under multiplication, with a basis consisting of the set of all primes f satisfying

(a) $(f, M)=1$, where $M=2^s\prod_{i=1}^r p_i^{\alpha_i}$ and the p_i are distinct odd primes and where $s>3$.

(b) $(D/f)=+1$, where $D=2^\sigma\prod_{i=1}^k p_i^{\beta_i}$ with $k\leqq r$, $\sigma\leqq s$ and $\beta_i\leqq\alpha_i$ for $i=1, \cdots, k$. Let g_i be a primitive root mod p_i^2 for $i=1, \cdots, r$; then, for every m in G, there exist integers $\alpha, \beta, \gamma_1, \cdots, \gamma_r$ which are unique mod 2, 2^{s-2}, $\phi(p_1^{\alpha_1}), \cdots, \phi(p_r^{\alpha_r})$ respectively, such that

$$m \equiv (-1)^\alpha 5^\beta \pmod{2^s}, \qquad m \equiv g_i^{\gamma_i} \pmod{p_i^{\alpha_i}} \qquad (i = 1, \cdots, r). \tag{1}$$

Let $\vartheta, \eta, \rho_1, \cdots, \rho_r$ be defined by

$$\vartheta^2 = 1, \qquad \eta^{2^{s-2}} = 1, \qquad \rho_i^{\phi(p_i^{\alpha_1})} = 1 \qquad (i = 1, \cdots, r), \tag{2}$$

and set

$$\tau(\vartheta, \eta; \rho_1, \cdots, \rho_r; m) = \tau(m) = \vartheta^\alpha\eta^\beta\prod_{i=1}^r \rho_i^{\gamma_i}. \tag{3}$$

We shall call the number-theoretic function $\tau(m)$ *a character* mod M. Two characters τ and τ' are said to be the same only if their corresponding $\vartheta, \eta, \rho_1, \cdots, \rho_r$'s are the same. It may well happen that $\tau(m)=\tau'(m)$ for all m in G without τ and τ' being the same character. The set of values which $\tau(m)$ assumes for a fixed m as τ varies over the complete set of distinct characters is called the total character of m. Two numbers have the same total character if and only if they are congruent mod M. In virtue of (2), the number of distinct characters is

$$2\cdot 2^{s-2}\cdot\prod_{i=1}^r \phi(p_i^{\alpha_i}) = \phi(M).$$

We define the *principal character* τ_0 to be $\tau(1, 1; 1, \cdots, 1; m)$. By an *ambiguous character* τ_a we shall mean $\tau(\pm 1, \pm 1; \pm 1, \cdots, \pm 1; m)$, where any combination of signs is permitted. All other characters are *imaginary*. The complex conjugate of $\tau(\vartheta, \eta; \rho_1, \cdots, \rho_r; m)$ is clearly $\tau(\vartheta^{-1}, \eta^{-1}; \rho_1^{-1}, \cdots, \rho_r^{-1}; m)$.

3. **The group H and group characters.** Let H be a multiplicative abelian group with generators $\theta_1, \cdots, \theta_\nu$; let n_i be the degree of θ_i, that is, the smallest positive exponent r for which θ_i^r is the identity element θ_0. Every θ in H can then be written as

$$\theta = \prod_{i=1}^{\nu} \theta_i^{s_i}, \tag{4}$$

where s_i is uniquely determined mod n_i $(i=1, \cdots, \nu)$. The number of elements in H is $h = \prod_{i=1}^{\nu} n_i$. Let λ be defined by

$$n_1, \cdots, n_{\lambda-1} \text{ are even,} \quad n_\lambda, \cdots, n_\nu \text{ are odd.} \tag{5}$$

Define ω_i by

$$\omega_i^{n_i} = 1 \qquad (i = 1, \cdots, \nu), \tag{6}$$

and define

$$\chi(\omega_1, \cdots, \omega_\nu; \theta) = \chi(\theta) = \prod_{i=1}^{\nu} \omega_i^{s_i}. \tag{7}$$

Similar definitions hold for the $\chi(\theta)$ as held for the $\tau(m)$ above. The number of ambiguous characters χ_a is then $2^{\lambda-1}$.

Definition. An element θ in H is *ambiguous* if $\theta^2 = \theta_0$. The number of ambiguous elements is then $2^{\lambda-1}$, and these are representable as

$$\prod_{i=1}^{\lambda-1} (\theta_i^{n_i/2})^{\epsilon_i} \tag{8}$$

where each ϵ_i may be 0 or 1.

Definition. A *genus* is the aggregate of all elements

$$\prod_{i=1}^{\lambda-1} \theta_i^{2s_i+\epsilon_i} \cdot \prod_{i=\lambda}^{\nu} \theta_i^{s_i} \tag{9}$$

obtained by letting $s_1, \cdots, s_{\lambda-1}, s_\lambda, \cdots, s_\nu$ range over complete residue systems mod $n_1/2, \cdots, n_{\lambda-1}/2, n_\lambda, \cdots, n_\nu$ respectively, where $\epsilon_1, \cdots, \epsilon_{\lambda-1}$ are all fixed and are 0 or 1. The number of genera is seen to be $2^{\lambda-1}$.

4. **The correspondence between G and H.** We assume that there is a correspondence between G and H such that

(a) Every element of G corresponds to at least one element of H, and conversely.

(b) If m in G corresponds to θ in H, then θ corresponds to m, and conversely.

(c) If m_1, m_2 in G correspond to θ_1, θ_2 in H, then m_1m_2 corresponds to $\theta_1\theta_2$.

(d) If m_1, m_2 in G correspond to θ_1, θ_2 in H, and if $m_2 \equiv n^2m_1 \pmod{D}$ for some integer n, then for all χ_a, $\chi_a(\theta_1) = \chi_a(\theta_2)$.

(e) If θ_1, θ_2 in H correspond to m_1, m_2 in G, and if for all χ_a, $\chi_a(\theta_1) = \chi_a(\theta_2)$, then there exists an integer n for which $m_2 \equiv n^2m_1 \pmod{D}$.

(f) For every prime f in G, there exist two elements θ_f and θ_f^{-1} in H, whose product is θ_0, to which f corresponds. (The possibility $\theta_f = \theta_f^{-1}$ is not excluded; indeed, this relation will hold for any ambiguous θ_f.)

It is clear that the total ambiguous character of m depends only on the quadratic character of m (mod M), where by the total ambiguous character of m we mean the set of values which $\tau_a(m)$ assumes as we keep m fixed and let τ_a range over all ambiguous characters. Among these τ_a, there will be some whose value depends only on the quadratic character of m (mod D); call the set of these characters Σ. By the Σ-character of m we shall mean the set of values of $\tau_a(m)$, where m is kept fixed and τ_a ranges over all characters in Σ.

If we denote by χ_i that ambiguous character obtained by setting $\omega_i = -1$ and $\omega_j = 1$ if $j \neq i$, then these χ_i (for $i = 1, \cdots, \lambda - 1$) are $\lambda - 1$ independent characters in the sense that $\chi_1(\theta), \cdots, \chi_{\lambda-1}(\theta)$ may be any sequence of $+1$'s and -1's (depending, of course, on the choice of θ), and indeed every such sequence can be obtained by choosing θ of the proper genus. In fact, if the ϵ's are as in (9), the sequence $\chi_1(\theta), \cdots, \chi_{\lambda-1}(\theta)$ is simply $(-1)^{\epsilon_1}, \cdots, (-1)^{\epsilon_{\lambda-1}}$. Thus, to specify the values of these $\lambda - 1$ characters is equivalent to fixing a unique genus. This in turn means that the quadratic character of m (mod D) is determined, where m corresponds to some θ of the genus. Conversely, if we specify the values of

$$(10) \qquad (-1/m) \text{ and/or } (2/m), \quad \text{or} \quad (-2/m), \text{ and } (m/p_i) \qquad (i = 1, \cdots, k),$$

where the p_i are given in §2, (b), then the quadratic character of m (mod D) is uniquely determined, and so are the $\chi_a(\theta)$, where θ corresponds to m. Here, the characters in (10) other than the (m/p_i) are to be chosen according to the following scheme:

$$(11) \qquad \begin{aligned} D &\equiv 3 \pmod{4}: (-1/m), \\ D &\equiv 2 \pmod{8}: (2/m), \\ D &\equiv 6 \pmod{8}: (-2/m), \\ D &\equiv 4 \pmod{8}: (-1/m), \\ D &\equiv 0 \pmod{8}: (-1/m) \text{ and } (2/m). \end{aligned}$$

(We assume hereafter that $D \not\equiv 1 \pmod{4}$, and that D is not a perfect square.)

Suppose that there are λ_1 symbols in (10); since there is exactly one relation connecting them, namely $(D/m)=+1$, it follows that λ_1-1 of them are independent. In virtue of the relation between the symbols (10) and the $\lambda-1$ (multiplicatively) independent characters $\chi_1, \cdots, \chi_{\lambda-1}$ defined above, it follows that $\lambda_1-1=\lambda-1$, or $\lambda_1=\lambda$.

We further observe that each of the symbols (10) is an ambiguous character mod M; their $2^{\lambda-1}$ products are clearly then the same as the subset Σ. However, even more significant is the fact that these $\lambda-1$ independent symbols (10) are functions of the element θ to which m corresponds (in virtue of condition (e) in this section), and hence are also ambiguous characters χ_a. The $2^{\lambda-1}$ products of these symbols must therefore be the same as the set of ambiguous characters χ_a. Thus, every $\chi_a(\theta)$ may be written as

$$\chi_a(\theta) = \delta^{(m-1)/2}\cdot\epsilon^{(m^2-1)/8}\cdot(m/Q_1), \tag{12}$$

where m corresponds to θ, $\delta=\pm 1$, $\epsilon=\pm 1$, and Q_1 is an odd divisor of D. By the quadratic reciprocity law, this can be written as

$$\chi_a(\theta) = (Q/m), \tag{13}$$

where Q is a squarefree divisor of D, where m corresponds to θ, and where Q is even only if D is even; Q may, however, be negative. In any case, Q is determined by χ_a and does not depend on θ.

We may similarly write

$$\tau_a(m) = \vartheta^{(m-1)/2}\cdot\eta^{(m^2-1)/8}\cdot(m/P_1), \tag{14}$$

where P_1 is the product of all those odd primes p_i which divide M, for which $\rho_i=-1$. As above, we then have

$$\tau_a(m) = (P/m), \tag{15}$$

where P is a squarefree divisor of M, and where P is determined by the character τ_a and does not depend on m.

5. ***L*-series.** We define

$$L(\chi, \tau; s) = \prod_{f \text{ in } G} \{1 + [\chi(\theta_f) + \chi(\theta_f^{-1})]\tau(f)f^{-s} + [\chi(\theta_f^2) + \chi(\theta_f^{-2})]\tau(f^2)f^{-2s} + \cdots\} \tag{16}$$

$$= \prod_{f \text{ in } G} \frac{1-\tau(f^2)f^{-2s}}{[1-\chi(\theta_f)\tau(f)f^{-s}][1-\chi(\theta_f^{-1})\tau(f)f^{-s}]}. \tag{17}$$

Then if we set

$$K = \prod_{f \text{ in } G} [1-\tau(f^2)f^{-2s}], \tag{18}$$

we may write

$$L = K \cdot \prod_{f \text{ in } G} \frac{1}{[1 - \chi(\theta_f)\tau(f)f^{-s}][1 - \chi(\theta_f^{-1})\tau(f)f^{-s}]}. \tag{19}$$

From (16) we have

$$L = \sum_{\theta_i \text{ in } H} \sum_{m \text{ in } G} a_m(\theta_i)\chi(\theta_i)\tau(m)m^{-s}, \tag{20}$$

where $a_m(\theta_i)$ is the number of products $\prod_{f^\alpha | m,\, f^{\alpha+1} \nmid m} (\theta_f^{\pm\alpha})$ which are the same as θ_i. Clearly

$$\sum_{\theta_i \text{ in } H} a_m(\theta_i) = 2^{\nu(m)}, \tag{21}$$

where $\nu(m)$ is the number of distinct prime factors of m. From (19) we obtain

$$\log \frac{L}{K} = \sum_{f \text{ in } G} \sum_{r=1}^{\infty} \frac{[\chi(\theta_f^r) + \chi(\theta_f^{-r})]\tau(f^r)}{rf^{rs}}, \tag{22}$$

for a properly chosen value of $\log L/K$. All of the results stated so far hold for $s > 1$.

6. **Identity of L-series.** We shall write $L(\chi', \tau'; s) \equiv L(\chi'', \tau''; s)$, and call the two L-series identical, if corresponding terms m^{-s} in (20) have equal coefficients, that is, if

$$\chi'(\theta)\tau'(m) = \chi''(\theta)\tau''(m) \tag{23}$$

for all m and their corresponding θ's. Define χ and τ by

$$\chi'' = \chi\chi', \qquad \tau'' = \tau\tau'. \tag{24}$$

Then (23) holds if and only if for all m and their corresponding θ's,

$$\chi(\theta)\tau(m) = 1. \tag{25}$$

In virtue of (3) and (7), (25) may be written as

$$\prod_{i=1}^{\nu} \omega_i^{s_i} \cdot \vartheta^{\alpha} \eta^{\beta} \prod_{i=1}^{r} \rho_i^{\gamma_i} = 1, \tag{26}$$

where the correspondence between the s_i and α, β and the γ_i is determined by the correspondence between m and θ.

Let $\theta = \theta_0$. Then for all m corresponding to θ_0,

$$\vartheta^{\alpha} \eta^{\beta} \prod_{i=1}^{r} \rho_i^{\gamma_i} = 1. \tag{27}$$

But for all primes f, conditions (c) and (f) of §4 imply that f^2 corresponds to $\theta_f \cdot \theta_f^{-1} = \theta_0$. Hence, if we choose one of the indices α, β, $\gamma_1, \cdots, \gamma_r$, say I, then we can find an m corresponding to θ_0 all of whose indices are 0, except for

I which has the value 2. Therefore

$$\vartheta^2 = 1, \qquad \eta^2 = 1, \qquad \rho_i^2 = 1 \qquad (i = 1, \cdots, r), \text{ or } \tau = \tau_a.$$

Next, set $\theta = \theta_i^2$ $(i = 1, \cdots, \nu)$. If θ_i corresponds to m, then θ_i^2 corresponds to m^2, and all indices of m can be made even. Therefore $\omega_i^2 = 1$ for $i = 1, \cdots, \nu$, or $\chi = \chi_a$. (23) thus holds if and only if

$$(28) \qquad (Q/m)(P/m) = 1 \qquad \text{for all } m \text{ in } G,$$

where P and Q are given by (15) and (13) respectively. Since m may be any integer prime to M for which $(D/m) = +1$, (28) implies either

$$(29a) \qquad P = Q$$

or

$$(29b) \qquad P = ((QD)),$$

where $((x))$ denotes the product of all prime divisors of x which occur to an odd exponent in the factorization of x.

Thus, we may choose for $\chi(\theta)$ any ambiguous χ_a, and then use either (29a) or (29b) to determine a character τ_a which satisfies (25); in other words, if we start with a fixed $L(\chi', \tau'; s)$, there will be 2^λ series identical with it: $L(\chi_a\chi', \tau_a\tau'; s)$, where χ_a and τ_a are any two ambiguous characters satisfying either (29a) or (29b). Thus the $h \cdot \phi(M)$ series $L(\chi, \tau; s)$ fall into sets of 2^λ identical ones.

Nonidentical series may (and, as we shall show, sometimes do) have the same value. However, exactly 2^λ series have the value

$$(30) \qquad L_1 = L_1(\chi_0, \tau_0; s) = \sum_{\theta_i \text{ in } H} \sum_{m \text{ in } G} a_m(\theta_i) m^{-s} = \sum_{m \text{ in } G} 2^{\nu(m)} m^{-s},$$

since if $L(\chi, \tau; s) = L_1$, we would have $\chi(\theta)\tau(m) = 1$ for all m and their corresponding θ's, and the previous discussion shows that this has exactly 2^λ solutions.

7. **L-series of the first and second kinds.** We divide the $L(\chi, \tau)$ into three kinds:

First kind (L_1): any L series identical with $L(\chi_0, \tau_0)$;

Second kind (L_2): any $L(\chi_a, \tau_a)$ not identical with $L(\chi_0, \tau_0)$;

Third kind (L_3): all other L series.

No $L_3 \equiv L_2$; for $L_2(\chi', \tau') \equiv L_3(\chi'', \tau'')$ would imply that χ'/χ'' and τ'/τ'' would both be ambiguous, whence so would both χ'' and τ'', and this is impossible.

We next show that $\lim_{s \to 1+} (s-1)L_1(s)$ exists and is not 0. We have

$$L_1 = \sum_m 2^{\nu(m)} m^{-s},$$

where $\sum_m$ extends over all $m>0$ for which $(m, M)=1$ and $(D/m)=1$. Set

$$M_1 = \sum_{m>0,(m,2D)=1,(D/m)=1} 2^{\nu(m)} m^{-s}.$$

Then

$$M_1 = L_1 \cdot \prod_{f|M, f|2D, (D/f)=1} [1 + 2f^{-s} + 2f^{-2s} + \cdots].$$

It therefore suffices to show that $\lim_{s\to 1+} (s-1)M_1$ exists and is not 0. This, however, follows from Dirichlet [2; paragraphs 89 and 96]. Thus

$$\lim_{s\to 1+} (s-1)L_1(s) = A \neq 0. \tag{31}$$

Next, we have

$$L_2 = \sum_{\theta_i \text{ in } H} \sum_{m \text{ in } G} a_m(\theta_i)(Q/m)(P/m)m^{-s} = \sum_{m \text{ in } G} 2^{\nu(m)}(PQ/m)m^{-s}, \tag{32}$$

where P and Q are given by (15) and (13) respectively, and neither (29a) nor (29b) holds. We shall prove that $L_2(s)$ exists and is not 0 for $s=1$, by use of the result of Dirichlet [2; paragraph 101] that $\sum_{n,(n,2D)=1} (D/n)n^{-s}$ exists and is not 0 for $s=1$, provided that D is not a perfect square.

Now, from (32) we obtain

$$\begin{aligned} L_2 &= \prod_{f \text{ in } G} \frac{1 + (PQ/f)f^{-s}}{1 - (PQ/f)f^{-s}} \\ &= \prod_{f \text{ in } G} \frac{1 + (PQM^2/f)f^{-s}}{1 - (PQM^2/f)f^{-s}}, \end{aligned} \tag{33}$$

where in each case $\prod_{f \text{ in } G}$ extends over all positive primes f such that $f\nmid M$ and $(D/f)=1$. Set $PQM^2 = D\cdot D_1$; then D_1 is not a square because neither (29a) nor (29b) holds. Then

$$L_2 = \prod_{f,(f,2DD_1)=1,(D/f)=1} \frac{1 + (DD_1/f)f^{-s}}{1 - (DD_1/f)f^{-s}} = \prod_p \frac{1 + (DD_1/p)p^{-s}}{1 - (D_1/p)p^{-s}},$$

where $\prod_p$ extends over all primes $p>0$ such that $p\nmid 2DD_1$. Therefore

$$\begin{aligned} L_2 &= \prod_p (1 - p^{-2s}) \cdot \prod_p \frac{1}{1 - (DD_1/p)p^{-s}} \cdot \prod_p \frac{1}{1 - (D_1/p)p^{-s}} \\ &= \frac{\sum_n (DD_1/n)n^{-s} \cdot \sum_n (D_1/n)n^{-s}}{\sum_n n^{-2s}}, \end{aligned} \tag{34}$$

where in each case $\sum_n$ extends over all postive n for which $(n, 2DD_1)=1$.

The denominator of the right-hand side of (34) is positive for $s>1/2$; the first factor in the numerator of the right-hand side of (34), by Dirichlet's theorem quoted above, is finite and not 0 for $s=1$. We need only prove the same for the second factor $\sum_n (D_1/n)n^{-s}$. Now clearly

$$\sum_{n,q} (D_1/nq)(nq)^{-s} = \sum_{n'} (D_1/n')(n')^{-s}, \tag{35}$$

where q ranges over all divisors of D which are prime to $2D_1$ and n' ranges over all numbers prime to $2D_1$. However, the left-hand side of (35) is

$$\sum_n (D_1/n)n^{-s} \cdot \sum_q (D_1/q)q^{-s},$$

the second factor of which is merely

$$\prod_r [1 + (D_1/r)r^{-s} + (D_1/r^2)r^{-2s} + \cdots] = \prod_r \frac{1}{1-(D_1/r)r^{-s}},$$

where $\prod_r$ ranges over all primes $r>0$ for which $r \mid D$ and $r\nmid 2D_1$. Therefore

$$\sum_n (D_1/n)n^{-s} = \prod_r [1 - (D_1/r)r^{-s}] \cdot \sum_{n'} (D_1/n')(n')^{-s}. \tag{36}$$

Since both factors on the right exist and are not 0 for $s=1$, the same is true for the left-hand side. This completes the proof that $L_2(1)$ exists and is not 0.

8. **L-series of the third kind.** To prove a similar result for $L_3(s)$, we begin by summing (22) over all $\phi(M)$ characters τ, and use the result

$$\sum_\tau \tau(a) = \begin{cases} \phi(M) & \text{if } a \equiv 1 \pmod{M}, \\ 0 & \text{otherwise.} \end{cases} \tag{37}$$

(We sketch a proof of this result:

If $a\equiv 1 \pmod{M}$, the result is clear; if $a \not\equiv 1 \pmod{M}$, then there exists a character τ' for which $\tau'(a)\neq 1$. But as τ ranges over all characters, so does $\tau\tau'$. Hence $\sum_\tau \tau(a) = \sum_\tau \tau\tau'(a) = \tau'(a)\cdot\sum_\tau \tau(a)$, whence $\sum_\tau \tau(a)=0$.) We then obtain

$$\begin{aligned} \phi(M)\Big\{ &\sum_{f,f\equiv 1 (\mathrm{mod}\, M)} [\chi(\theta_f) + \chi(\theta_f^{-1})]f^{-s} \\ &+ \frac{1}{2} \sum_{f,f^2\equiv 1(\mathrm{mod}\, M)} [\chi(\theta_f^2) + \chi(\theta_f^{-2})]f^{-2s} + \cdots \Big\} = \sum_\tau \log \frac{L}{K}. \end{aligned} \tag{38}$$

Now, from (18) it is clear that $K=K(\tau; s)$ exists and is not 0 for $s>1/2$, and is indeed continuous in that range. If $\tau=\tau_a$, K is real and positive; if τ is imaginary, K may also be imaginary. However, if $\bar{z}$ denotes the complex conjugate of z, we have $K(\bar{\tau}; s)=\overline{K}(\tau; s)$. Similarly $L(\chi, \bar{\tau}; s)=\overline{L}(\chi, \bar{\tau}; s)$. The terms on the right-hand side of (38) may thus be grouped in pairs of conjugates

$$\log \frac{L}{K} + \log \frac{\overline{L}}{\overline{K}} = \log \frac{L\overline{L}}{K\overline{K}} \cdot$$

Suppose now that $\chi = \chi_a$. If $f \equiv 1 \pmod{M}$, then θ_f is in the same genus as θ_0, whence $\chi_a(\theta_f^{\pm 1}) = 1$. (38) then becomes

$$(39) \qquad 2\phi(M) \left\{ \sum_{f, f \equiv 1 (\mathrm{mod}\, M)} f^{-s} + \frac{1}{2} \sum_{f, f^2 \equiv 1 (\mathrm{mod}\, M)} f^{-2s} + \cdots \right\} = \sum_{\tau} \log \frac{L}{K} \cdot$$

Since for each χ there are two characters τ for which two L series are identical, and in particular for each χ_a there are two τ_a for which $L = L_1$, it follows that on the right-hand side of (39) each L occurs in two terms corresponding to the same χ but having two different τ's. Keeping only one of these in each case, we have

$$(40) \qquad \phi(M) \left\{ \sum_{f, f \equiv 1 (\mathrm{mod}\, M)} f^{-s} + \cdots \right\} = \sum_{\tau}{}' \log \frac{L}{K} \cdot$$

Suppose now that we know that $L_2(s)$ and $L_3(s)$ are finite and continuous for $s \geqq 1$, with finite and continuous derivatives for $s \geqq 1$. If we set

$$(41) \qquad L(s) = f_1(s) + i f_2(s),$$

where $f_1(s)$ and $f_2(s)$ are real functions of s, we have for L_2 and L_3

$$(42) \qquad \begin{gathered} L(s) = L(1) + (s-1)\left[f_1'(\vartheta_1(s-1)) + i f_2'(\vartheta_2(s-1))\right], \\ 0 < \vartheta_1 < 1,\ 0 < \vartheta_2 < 1, \end{gathered}$$

where $f_i(s)$ and $f_i'(s)$ $(i = 1, 2)$, are continuous for $s \geqq 1$.

We may deduce from this that $L_3(1) \neq 0$. If this is not the case, (42) implies

$$(43) \qquad L_3(s) \cdot \overline{L}_3(s) = O((s-1)^2) \text{ as } s \to 1+.$$

We assume to begin with that $L_3(\chi_a, \tau; 1) = 0$, where χ_a is some particular ambiguous character. On the right side of (40) there occurs a corresponding term $\log (s-1)$, so that as $s \to 1^+$ the right side cannot become positively unbounded. By Dirichlet [2; paragraph 137], however, the left side of (40) becomes positively infinite as $s \to 1^+$. Therefore $L_3(\chi_a, \tau; 1) \neq 0$.

Next, suppose that $L_3(\chi, \tau; 1) = 0$ for some imaginary χ. Summing (38) over all characters χ and using the result

$$(44) \qquad \sum_{\chi} \chi(\theta) = \begin{cases} h & \text{if } \theta = \theta_0, \\ 0 & \text{otherwise}, \end{cases}$$

we obtain

$$2h\phi(M)\left\{\sum_{f,f\equiv 1(\text{mod } M),f\leftrightarrow\theta_0} f^{-s}+\frac{1}{2}\sum_{f,f^2\equiv 1(\text{mod } M),f^2\leftrightarrow\theta_0} f^{-2s}+\cdots\right\} \tag{45}$$
$$= \sum_{\chi,\tau} \log\frac{L}{K},$$

where $f\leftrightarrow\theta_0$ means that f corresponds to θ_0, and so on. On the right-hand side of (45), log L_1 occurs exactly 2^λ times. However, for each $L_3(\chi, \tau; 1)$ which is 0 there are 2^λ such $L_3(\chi\chi_a, \tau\tau_a)$ (including the original $L_3(\chi, \tau)$), where χ_a and τ_a are related by (29a) or (29b). Now $L_3(\chi, \tau)=0$ implies $L_3(\bar{\chi}, \tau)=0$; if this $L_3(\bar{\chi}, \tau)$ is not included in the above 2^λ L_3's, there are at least $2^\lambda+1$ terms on the right-hand side of (45) each of which contributes the term log $(s-1)$; this is enough to counterbalance the contribution of $-2^\lambda \log(s-1)$ from the $2^\lambda \log L_1$ terms. As a result, the right-hand side of (45) becomes negatively infinite as $s\to 1+$, while the left-hand side of (45) is non-negative. We thus have a contradiction in this case.

On the other hand, suppose that $L_3(\bar{\chi}, \tau)$ is included in the 2^λ L_3's previously mentioned; then for some χ_a we have $\bar{\chi}=\chi\chi_a$, whence $\chi^4=\chi_a^2=1$ for all θ. We shall now show that in this case there is another L_3 which is 0 and which is not included in any of the previous 2^λ L_3's. This will then establish the result that $L_3(\chi, \tau; 1)\neq 0$.

Since $\chi^4(\theta)=1$ for all θ, and since χ is imaginary, at least one of the roots $\omega_1, \cdots, \omega_{\lambda-1}$ must be $\pm i$, and also $\omega_\lambda=\cdots=\omega_\nu=i$. Suppose then that

$$\begin{array}{lll} \omega_1, \cdots, \omega_R & \text{are all } \pm i & (R\geqq 1), \\ \omega_{R+1}, \cdots, \omega_{\lambda-1} & \text{are all } \pm 1, & \\ \omega_\lambda, \cdots, \omega_\nu & \text{are all } \quad 1. & \end{array}$$

This implies that $n_1, \cdots, n_R$ are all multiples of 4. In the series $L(\chi, \tau)$, the sum of those terms for which $\chi(\theta_i)=\pm i$ has the value 0, since the terms occur pairwise with opposite signs corresponding to inverse elements θ_i and θ_i^{-1} [using the fact that $a_m(\theta_i)=a_m(\theta_i^{-1})$]. Next, consider the remaining terms, that is, those for which $\chi(\theta)=\pm 1$. Since $\chi(\theta)=(\pm i)^{s_1}\cdots(\pm i)^{s_R}(\pm 1)^{s_{R+1}}\cdots(\pm 1)^{s_{\lambda-1}}=\pm 1$, we have $2\mid(s_1+\cdots+s_R)$. Let (P''/m) be that ambiguous character χ_a' obtained by letting $\omega_1=\cdots=\omega_R=-1$, $\omega_{R+1}=\cdots=\omega_\nu=1$. Then for all those θ's for which $\chi(\theta)=\pm 1$ we have $(P''/m)=1$, where θ corresponds to m, and where P'' is neither $((D))$ nor 1. Hence $L(\chi, \tau)$ has the same value as $L(\chi\chi_a', \tau)$, which is not one of the 2^λ series $L(\chi\chi_a, \tau\tau_a)$ mentioned above, since if it were $\chi_a=\chi_a'$, $\tau_a=\tau_0$, and then neither (29a) nor (29b) could hold. This completes the proof that $L_3(\chi, \tau; 1)\neq 0$.

9. **Completion of proof and statement of theorem.** In the proof that neither $L_2(1)$ nor $L_3(1)$ is 0, we needed the fact that $L_2(s)$, $L_2'(s)$, $L_3(s)$ and $L_3'(s)$ are all finite and continuous for $s\geqq 1$. We shall postpone the discussion of this to §10, and for the present follow the main line of the argument.

Let $(N, M)=1$. Multiplying (22) by $\tau^{-1}(N)$ and summing over all characters τ gives (from (37))

$$\phi(M)\left\{\sum_{f,f\equiv N(\bmod M)}[\chi(\theta_f)+\chi(\theta_f^{-1})]f^{-s}\right.$$
(46)
$$\left.+\frac{1}{2}\sum_{f,f^2\equiv N(\bmod M)}[\chi(\theta_f^2)+\chi(\theta_f^{-2})]f^{-2s}+\cdots\right\}=\sum_{\tau}\tau^{-1}(N)\log\frac{L}{K}.$$

If we now multiply (46) by $\chi(\theta_j)$ and sum over χ, we obtain

$$eh\left\{\sum_{f,f\equiv N(\bmod M),f\leftrightarrow\theta_j}f^{-s}+\frac{1}{2}\sum_{f,f^2\equiv N(\bmod M),f^2\leftrightarrow\theta_j}f^{-2s}+\cdots\right\}$$
(47)
$$=\sum_{\chi}\sum_{\tau}\chi(\theta_j)\tau^{-1}(N)\log\frac{L}{K},$$

where $e=2$ or 1 according as θ_j is ambiguous or not. On the right-hand side of (47), the term $\log L_1$ occurs exactly 2^λ times, namely twice for each

$$\chi_a(\theta)=(Q/m),\qquad m\leftrightarrow\theta, \tag{48}$$

in combination with τ_a given by

$$\tau_a(m)=(Q/m)\quad\text{or}\quad\tau_a(m)=(QD/m), \tag{49}$$

as can be seen from (29a) and (29b). The coefficient of $\log L_1$ on the right-hand side of (47) is therefore

$$\sum\chi_a(\theta_j)\tau_a(N), \tag{50}$$

since $\tau_a^{-1}(N)=\tau_a(N)$, and this in turn is

$$\sum_{Q}(Q/m_j)[(Q/N)+(QD/N)],\qquad m_j\leftrightarrow\theta_j, \tag{51}$$

and this is equal to

$$[1+(D/N)]\sum_{Q}(Q/Nm_j), \tag{52}$$

where $\sum_Q$ is such as to make (Q/Nm_j) range over all ambiguous characters τ_a in Σ. This sum will be 0 except when N and m_j have the same Σ-character, in which case it will be positive. Thus, the right-hand side of (47) becomes positively infinite as $s\rightarrow 1+$ when the correspondent of N is in the genus of θ_j. This leads to the theorem:

If N is prime to M and corresponds to an element of the same genus as θ_j, then there are infinitely may primes f which correspond to θ_j for which $f\equiv N$ (mod M), *provided that conditions* (a)–(f) *of* §4 *hold, and that $L_i(s)$ and $L_i'(s)$* ($i=2, 3$) (*see* §7) *are continuous for $s\geqq 1$.*

We shall discuss this latter condition in the next section.

10. **Sufficiency conditions.** We shall now prove that $L_i(s)$ and $L_i'(s)$ $(i=2, 3)$ are finite and continuous for $s\geqq 1$, provided that our correspondence established in §4 satisfies certain conditions. If we define

$$R(m_0, \theta; s) = \sum_{m, m\equiv m_0 \,(\mathrm{mod}\, M)} a_m(\theta)m^{-s}, \tag{53}$$

we see that $R(m_0, \theta)=0$ unless m_0 corresponds to an element in the genus of θ. Furthermore, by use of (20), we obtain

$$L(\chi, \tau) = \sum_{m_0} \tau(m_0) \sum_{\theta_i} \chi(\theta_i)R(m_0, \theta_i), \tag{54}$$

where $\sum_{m_0}$ ranges over a reduced residue system mod M and $\sum_{\theta_i}$ ranges over all elements of H. We now impose the conditions:

$$R(m_0, \theta_i; s) = A_1/(s-1) + B_1(m_0, \theta_i; s), \tag{A}$$

if m_0 corresponds to any element in the genus of θ_i, where A_1 is a constant $(\neq 0)$ independent of m_0 and θ_i, and $B_1(m_0, \theta_i; s)$ is continuous for $s\geqq 1$.

$$R'(m_0, \theta_i; s) = A_2/(s-1)^2 + B_2(m_0, \theta_i; s), \tag{B}$$

if m_0 corresponds to any element in the genus of θ_i, where A_2 is a constant $(\neq 0)$ independent of m_0 and θ_i, and $B_2(m_0, \theta_i; s)$ is continuous for $s\geqq 1$.

To prove that $L_i(s)$ and $L_i'(s)$ $(i=2, 3)$ are finite and continuous for $s\geqq 1$, in virtue of (54) and (A) and (B) it suffices to show that

$$P(\chi, \tau) = \sum_{m_0, \theta_i} \tau(m_0)\chi(\theta_i) \tag{55}$$

is 0 provided that τ and χ do not satisfy (25) for all m and their corresponding θ's. We may write

$$P(\chi, \tau) = \sum_{\theta} \chi(\theta) \left\{ \sum_{m_0} \tau(m_0) \right\}, \tag{56}$$

where $\sum_{m_0}$ extends over all m_0 which correspond to elements in the genus of θ, and then $\sum_\theta$ extends over all θ. Further, the choice of the reduced residue system mod M to which the m_0 belong has no effect on the value of $P(\chi, \tau)$ because two numbers congruent mod M correspond to θ's of the same genus.

Let f be any prime in G; then, as m_0 ranges over those elements of a reduced residue system mod M which correspond to elements in the genus of θ, so does f^2m_0, because $f^2m_0\equiv f^2m_0'$ (mod M) holds if and only if $m_0\equiv m_0'$ (mod M), and f^2m_0 and m_0 correspond to elements in the same genus. Hence

$$P(\chi, \tau) = \sum_{\theta} \chi(\theta) \left\{ \sum_{m_0} \tau(f^2m_0) \right\} = \tau(f^2)P(\chi, \tau). \tag{57}$$

Hence $P=0$ unless $\tau(f^2)=1$ for each f in G; this in turn is true if and only if τ is an ambiguous character. But in virtue of (13) and (15), every ambiguous character τ_a is also an ambiguous character χ_a. Hence

$$P(\chi, \tau) = \sum_{\theta} \chi(\theta) \sum_{m_0} \chi_a(\theta), \tag{58}$$

where m_0 corresponds to elements in the same genus as θ. Now it is clear that the same number of elements in a reduced residue system correspond to each genus, since if m_0 corresponds to a genus containing θ, so do all of the numbers $m_0 n^2$ obtained by letting n range over all numbers prime to M which give incongruent values of n^2, and conversely. The number of m_0 corresponding to elements in a given genus is thus $\phi(M)$ divided by $2^{\lambda-1}$. Call their quotient q. Then

$$P(\chi, \tau) = q \sum_{\theta} \chi(\theta)\chi_a(\theta) = q \sum_{\theta} \chi\chi_a(\theta). \tag{59}$$

Therefore $P(\chi, \tau)=0$ unless $\chi\chi_a=\chi_0$, that is, unless either (29a) or (29b) holds. This completes the proof that $L_i(s)$ and $L_i'(s)$ $(i=2, 3)$ are finite and continuous for $s \geqq 1$.

11. **Meyer's theorem.** A. Meyer [3] proved this theorem for the special case where H is the set of classes of properly primitive binary quadratic forms of determinant D, which forms a group under the operation of composition. In that case, it is known from the theory of quadratic forms that all of the conditions (a)–(f) of §4 hold, where the θ_i are the classes of forms of determinant D, and m corresponds to those classes θ which represent m. The crucial (and most difficult) part of the proof is to show the correctness of (A) and (B). Meyer proved this (or results equivalent to this) by using some theorems of H. Weber [4] who considered the simpler problem of representation of primes by quadratic forms (without considering the arithmetic progressions in which they lie). Weber's results were established by use of ϑ-function identities; simpler proofs for equivalent results are to be found (for suitably restricted values of D) in Landau, *Neuere Fortschritte der additiven Zahlentheorie*, pp. 87–90.

12. **An example.** We conclude with an example to show that this theorem is more general than the original theorem. We shall use the result of Dirichlet [2; p. 359] that $\sum_f f^{-s}-(1/\phi(M))\ln(1/(s-1))$ is analytic for $s>1/2$, where $\sum_f$ extends over all primes $f\equiv N \pmod{M}$, and where $(N, M)=1$.

Set $D=-20$, $M=-80$. G has a basis consisting of all primes $f\equiv 1$, 3, 7 or 9 (mod 20). Let H be the group $\{\theta, \theta_0\}$ with $\theta^2=\theta_0$. Since there are four reduced (nonequivalent) forms of determinant -20, this means that we are not working with quadratic forms in this case.

We establish the correspondence

$$f_1, f_9 \leftrightarrow \theta_0, \qquad f_3, f_7 \leftrightarrow \theta,$$

where $f_j \equiv j \pmod{20}$. Define

$$R_1 = R(1, \theta_0), \qquad R_9 = R(9, \theta_0), \qquad R_3 = R(3, \theta), \qquad R_7 = R(7, \theta). \tag{60}$$

We shall prove that (A) and (B) hold, simply by proving (A) and showing that the function $B_1(s)$ is analytic for $s>1/2$. All other conditions of our hypothesis are automatically satisfied in this case.

If $m\leftrightarrow\theta_i$, then $a_m(\theta_i)=2^{\nu(m)}$. Since we are working here with m (mod 20), we shall restrict ourselves (in this section) to those characters τ whose value does not depend on the exponent β in (1), that is, those for which η in (2) is 1. Then we have the following table:

m (mod 20)	α	γ
1	0	0
9	0	2
3	1	3
7	1	1

For any character for which $\eta=1$, we have by setting $\chi=\chi_0$ in (17)

$$\sum_{m_0\leftrightarrow\theta_i}\tau(m_0)R(m_0,\theta_i)=\prod_{f,(-20/f)=1}\frac{1-\tau(f^2)f^{-2s}}{(1-\tau(f)f^{-s})^2},\tag{61}$$

or

$$\tau(1)R_1+\tau(9)R_9+\tau(3)R_3+\tau(7)R_7=\prod_{f,(-20/f)=1}\frac{1+\tau(f)f^{-s}}{1-\tau(f)f^{-s}}.\tag{62}$$

We shall choose four characters for τ, thus getting from (62) four equations from which we may find the R_j. Let $\tau=\tau_0,\tau_1,\tau_2,\tau_3$ successively, given by:

	ϑ	η	ρ
τ_0	1	1	1
τ_1	1	1	-1
τ_2	1	1	i
τ_3	1	1	$-i$

Let $P_i=\prod_{f_i}(1+f_i^{-s})/(1-f_i^{-s})$ $(i=1, 9, 3, 7)$. We then obtain from (62):

$$
\begin{aligned}
R_1 + R_9 + R_3 + R_7 &= P_1P_9P_3P_7 = \xi_1,\\
R_1 + R_9 - R_3 - R_7 &= P_1P_9P_3^{-1}P_7^{-1} = \xi_2,\\
R_1 - R_9 - iR_3 + iR_7 &= P_1P_9^{-1}\prod_{f_3}\frac{1 - if_3^{-s}}{1 + if_3^{-s}}\prod_{f_7}\frac{1 + if_7^{-s}}{1 - if_7^{-s}} = \xi_3,\\
R_1 - R_9 + iR_3 - iR_7 &= P_1P_9^{-1}\prod_{f_3}\frac{1 + if_3^{-s}}{1 - if_3^{-s}}\prod_{f_7}\frac{1 - if_7^{-s}}{1 + if_7^{-s}} = \xi_4.
\end{aligned}
\tag{63}
$$

Thence

$$
\begin{aligned}
R_1 &= (\xi_1 + \xi_2 + \xi_3 + \xi_4)/4, \quad & R_9 &= (\xi_1 + \xi_2 - \xi_3 - \xi_4)/4,\\
R_3 &= (\xi_1 - \xi_2 + i\xi_3 - i\xi_4)/4, \quad & R_7 &= (\xi_1 - \xi_2 - i\xi_3 + i\xi_4)/4.
\end{aligned}
\tag{64}
$$

Now

$$
\begin{aligned}
\ln P_j &= \sum_{f_j}\ln\left(1 + \frac{2f_j^{-s}}{1 - f_j^{-s}}\right)\\
&= \sum_{f_j}\left\{+\frac{2f_j^{-s}}{1 - f_j^{-s}} - \frac{1}{2}\left(\frac{2f_j^{-s}}{1 - f_j^{-s}}\right)^2 + \cdots\right\}\\
&= +\sum_{f_j}\left\{+2f_j^{-s}(1 + f_j^{-s} + \cdots) - \cdots\right\}\\
&= +2\sum_{f_j} f_j^{-s} + \sum_{f_j} O(f_j^{-2s}).
\end{aligned}
\tag{65}
$$

By Dirichlet's result, it then follows that

$$
\ln P_j - \frac{1}{4}\ln\left(\frac{1}{s - 1}\right)
\tag{66}
$$

is analytic for $s > 1/2$. Thus $\xi_1 = b/(s-1)$, where b is analytic for $s > 1/2$; similarly, ξ_2 itself is analytic for $s > 1/2$. In order to prove (A), it thus suffices to prove the analyticity of

$$
Z = \prod_{f_3}\frac{1 - if_3^{-s}}{1 + if_3^{-s}}\cdot\prod_{f_7}\frac{1 + if_7^{-s}}{1 - if_7^{-s}}
\tag{67}
$$

for $s > 1/2$. Now

$$
\begin{aligned}
Z &= \exp\left\{\sum_{f_3}\ln\left(1 - \frac{2if_3^{-s}}{1 + if_3^{-s}}\right) - \sum_{f_7}\ln\left(1 - \frac{2if_7^{-s}}{1 + if_7^{-s}}\right)\right\}\\
&= \exp\left\{2i\sum f_3^{-s} - 2i\sum f_7^{-s} + \text{remainder}\right\},
\end{aligned}
\tag{68}
$$

where the remainder is analytic for $s > 1/2$. The result then follows from Dirichlet's result quoted above.

BIBLIOGRAPHY

1. G. L. Dirichlet, C. R. Acad. Sci. Paris vol. 10 (1840) p. 285.
2. ———, *Vorlesungen über Zahlentheorie*, 4th ed., 1894.
3. A. Meyer, *Ueber einen Satz von Dirichlet*, Journal für Mathematik vol. 103 (1888) p. 98.
4. H. Weber, *Quadratische Formen und Primzahlen*, Math. Ann. vol. 20 (1882) p. 301.

CORNELL UNIVERSITY,
ITHACA, N. Y.