TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 217, 1976

L-FUNCTIONS OF A QUADRATIC FORM

BY

T. CALLAHAN AND R. A. SMITH

ABSTRACT. Let Q be a positive definite integral quadratic form in n variables, with the additional property that the adjoint form $Q^\dagger$ is also integral. Using the functional equation of the Epstein zeta function, we obtain a symmetric functional equation of the L-function of Q with a primitive character ω mod q (additive or multiplicative) defined by $\Sigma\omega(Q(\mathbf{x}))Q(\mathbf{x})^{-s}$, $\mathrm{Re}(s) > n/2$, where the summation extends over all $\mathbf{x} \in Z^n$, $\mathbf{x} \neq 0$; our result does not depend upon the usual restriction that q be relatively prime to the discriminant of Q, but rather on a much milder restriction.

1. Introduction. Let $M_n(Z)$ denote the set of $n \times n$ matrices in Z and let $SL(n, Z)$ denote those matrices in $M_n(Z)$ with determinant 1. For each $A \in M_n(Z)$, denote by $A^\dagger$ the classical adjoint of A, and by M' the transpose of M, where M is any matrix. Let $X_1, \ldots, X_n$ be n independent indeterminants and set $\mathbf{X} = (X_1, \ldots, X_n)'$. For each $B \in M_n(Z)$, define

$$B[\mathbf{X}] = \mathbf{X}'B\mathbf{X}.$$

To each integral quadratic form $Q(\mathbf{X})$ we can associate a unique symmetric matrix $A \in M_n(Z)$ such that

$$Q(X) = \tfrac{1}{2}A[\mathbf{X}] = \tfrac{1}{2}\mathbf{X}'A\mathbf{X}, \tag{1}$$

where the diagonal elements of A are each divisible by 2. Define the discriminant of Q to be

$$D = D(Q) = \det A.$$

Associated with each quadratic form Q is its adjoint form $Q^\dagger$ defined by

$$Q^\dagger(\mathbf{X}) = \tfrac{1}{2}A^\dagger[\mathbf{X}]. \tag{2}$$

Note that the discriminant of $Q^\dagger$ is $\det A^\dagger = D^{n-1}$, and that for each $n > 2$, $Q^\dagger$ may or may not be integral.

For each integral positive definite quadratic form Q in n variables and for each character ω mod q (additive or multiplicative, q a positive integer), the

Received by the editors September 21, 1970.

AMS (MOS) subject classifications (1970). Primary 10H10; Secondary 10G05.

Key words and phrases. L-functions, quadratic forms, functional equation, Gaussian sums.

n-fold sum $\Sigma_{\mathbf{x}\in Z^n-0}\omega(Q(\mathbf{x}))Q(\mathbf{x})^{-s}$ $(s = \sigma + it)$ converges absolutely for $\sigma > n/2$ and uniformly in every compact subset of the half-plane $\sigma > n/2$, and so represents an analytic function of s for $\sigma > n/2$. We therefore define for $\sigma > n/2$

$$(3) \qquad L(s, \omega, Q) = \sum_{\mathbf{x}\in Z^n-0} \omega(Q(\mathbf{x}))Q(\mathbf{x})^{-s},$$

which we call the L-function of Q with the character ω defined mod q. We remark here that by an additive character ω defined mod q, we mean $\omega = e_q(p)$ for some integer p, where $\omega(n) = e_q(pn)$ for all $n \in Z$; we say that ω is primitive mod q if $(p, q) = 1$. A multiplicative character defined mod q will have its usual meaning, i.e., a Dirichlet character mod q; we shall insist that a primitive multiplicative character is nonprincipal.

It is easy to show that $L(s, \omega, Q)$ *always* has an analytic continuation into the entire s-plane and satisfies a functional equation (see the remark at the end of §5). In this paper, we shall prove that under suitable restrictions on q, ω and Q, then $L(s, \omega, Q)$ in fact satisfies a symmetric functional equation. Such results are found in the literature if D and q are relatively prime and ω^* is also primitive mod q, where ω^* is defined in (9) below when it exists. For example, Stark [8] has proved that $L(s, \omega, Q)$ satisfies a symmetric functional equation if ω is multiplicative and $(D, q) = 1$ when ω^* is primitive (cf. [1]); implicit in his paper is a similar result for ω additive. In general, however, the restriction $(D, q) = 1$ is too strong, as is indicated in [7], where a symmetric functional equation for $L(s, \omega, Q)$ with ω additive is found for $Q(X, Y) = X^2 + Y^2$ which holds for *all* q using a method of T. Estermann [3]. In the present investigation, we shall relax these restrictions. The idea of the proof is to represent $L(s, \omega, Q)$, with ω additive, as a linear combination of Epstein zeta functions for which the analytic continuation into the entire s-plane and the functional equation are well known, and then to evaluate the resulting Gaussian sums $G_Q(q, p, \mathbf{x})$ which appear (cf. (6) below). These Gaussian sums have been studied by Stark in [8] and [9] subject to the restrictions $(D, q) = 1$. In this paper, we shall study both $G_Q(q, p, \mathbf{x})$ and $L(s, \omega, Q)$ subject to the weaker restrictions

$$(4) \qquad (D_q, q) = 1 \quad \text{where} \quad D = \delta D_q \quad \text{and} \quad \delta = (D, q).$$

An immediate consequence of our symmetric functional equation for $L(s, \omega, Q)$ with ω additive and (4) holding is that we can write down a *symmetric* functional equation for $L(s, \omega, Q)$ with ω multiplicative, subject to (4) and ω^* being primitive when it exists. These results are the content of Theorem 3.

It is instructive to see the meaning of the restriction (4) in terms of valuations. Let ord_p denote the order valuation at the prime p. Then (4) is equivalent to

(5) $\operatorname{ord}_p q \geqslant \operatorname{ord}_p D \quad \text{or} \quad \operatorname{ord}_p q = 0, \quad \text{for all primes } p.$

Roughly speaking, these conditions mean that the form Q should not "degenerate" too much p-adically. Whether or not $L(s, \omega, Q)$ possesses a "nice" functional equation if Q is allowed to degenerate more than permitted by (5) is an open question, though the results in [7] must be kept in mind in looking into this matter.

2. **Notation.** Before we state the main results, we shall require some additional definitions to those given above. For any $t \in \mathbf{R}$ and $q \in Z$, $q \geqslant 1$, write $e(t) = e^{2\pi i t}$ and $e_q(t) = e(t/q)$. If $p \in Z$ is relatively prime to q, define $\bar{p} \in Z$ by

$$p\bar{p} \equiv 1 \bmod q.$$

For any integral quadratic form Q in n variables, $p \in Z$ and $\mathbf{a} \in Z^n$, define the Gaussian sum

(6) $$G_Q(q, p, \mathbf{a}) = \sum_{\mathbf{x} \bmod q} e_q(pQ(\mathbf{x}) + \mathbf{a} \cdot \mathbf{x}),$$

where "$\mathbf{x} \bmod q$" means that each component of $\mathbf{x} \in Z^n$ runs through a complete set of residues mod q and $\mathbf{a} \cdot \mathbf{x}$ represents the ordinary inner product of $\mathbf{a}$ and $\mathbf{x}$. Also, we define

(7) $$G_Q(q, p) = G_Q(q, p, \mathbf{0}).$$

Suppose there exists a multiplicative character χ_1 defined by

(8) $$G_Q(q, p) = \chi_1(p) G_Q(q, 1),$$

where the defining modulus of χ_1 may depend on both q and Q. (Actually, if q is odd, the existence of χ_1 is guaranteed by Theorem 1, in which case it is described explicitly.) To each character ω, we now associate a new character ω^* defined by

(9) $$\omega^* = \begin{cases} e_q(\overline{pD_q}) & \text{if } \omega = e_q(p), \\ \chi\bar{\chi}_1 & \text{if } \omega = \chi, \end{cases}$$

provided, in the second case, that χ_1 exists (cf. (8)). Note that ω^* depends on both ω and Q when it is defined.

We now introduce certain roots of unity which play a vital role in our functional equations. Since $G_Q(q, p) \neq 0$ when q, Q satisfy (4) (cf. (35), for example), we define

(10) $$\epsilon_Q(q, p) = G_Q(q, p)/|G_Q(q, p)|.$$

For any multiplicative character χ mod q, define

$$\tau(\chi) = \sum_{x \bmod q} \chi(x) e_q(x),$$

where $|\tau(\chi)| = \sqrt{q}$ if χ is primitive mod q. Therefore, if ω is a primitive character mod q, define

$$\epsilon(\omega, Q) = \begin{cases} \epsilon_Q(q, p) & \text{if } \omega = e_q(p), \\ \dfrac{\tau(\omega^*)}{\tau(\omega)} \epsilon_Q(q, 1)\chi^*(-D_q) & \text{if } \omega = \chi, \end{cases} \tag{11}$$

provided, in the second case, that χ_1 exists (cf. (8)). Note that $|\epsilon(\omega, Q)| = 1$ whenever ω^* is defined and is a primitive character mod q, which is no restriction for additive ω in view of (4) and (9).

Finally, for $\mathbf{x} \in Z^n$, define

$$E_m(\mathbf{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \equiv \mathbf{0} \bmod m, \\ 0 & \text{otherwise,} \end{cases} \tag{12}$$

where m is any positive integer.

3. Statement of results. For convenience in stating our results, we introduce the following

DEFINITIONS. For each $n \geqslant 2$, the set $\mathcal{H}_n$ denotes the collection of all pairs (q, Q), where q is a positive integer and Q is an integral quadratic form in n variables, satisfying $(D(Q)_q, q) = 1$; also, $\mathcal{H}_n^+$ denotes the subset of pairs $(q, Q) \in \mathcal{H}_n$ for which Q is positive definite. Further, the set H_n denotes the set of pairs $(q, Q) \in \mathcal{H}_n$ for which the adjoint form $Q^\dagger$ is integral [cf. (2)], and finally let $H_n^+ = H_n \cap \mathcal{H}_n^+$. We shall write $Q \in \mathcal{H}_n$ instead of $(1, Q) \in \mathcal{H}_n$.

For each $Q \in \mathcal{H}_n$, let A denote the unique defining matrix of Q given in (1), and set

$$N(q, Q) = \operatorname{card}\{\mathbf{x} \bmod q : A\mathbf{x} \equiv \mathbf{0} \bmod q\}, \tag{13}$$

for any positive integer q.

If $[s_i \delta_{ij}]$, $s_i \in Z$, is the Smith Normal Form of A (cf. [5, p. 26]), it follows that $N(q, Q) = (s_1, q) \cdots (s_n, q)$ and $D(Q) = s_1 \cdots s_n$, whence $N(q, Q)$ divides $D(Q)$. Therefore, if $Q \in \mathcal{H}_n^+$, there exists a unique positive integer $R(q, Q)$ such that

$$D(Q) = N(q, Q) R(q, Q). \tag{14}$$

THEOREM 1. *Let* $(q, Q) \in H_n$ *and suppose* $p \in Z$ *is relatively prime to* q.
(i) *For any* $\mathbf{a} \in Z^n$, *then*

$$G_Q(q, p, \mathbf{a}) = E_\delta(A^\dagger \mathbf{a}) e_q(-\overline{pD_q}\delta^{-1}Q^\dagger(\mathbf{a}))G_Q(q, p),$$

where $A^\dagger$ *is the adjoint of the defining matrix* A *of* Q *and* $\delta = (D(Q), q)$, *(cf.* (2), (7) *and* (12)).

(ii) *For* q *odd, then*

$$G_Q(q, p) = \left(\frac{p}{q}\right)^n \left(\frac{p}{N(q, Q)}\right) G_Q(q, 1) \tag{15}$$

where $(p, N(q, Q)) = 1$ *and*

$$\left(\frac{p}{q}\right)$$

denotes the Jacobi symbol.

THEOREM 2. *Let* $Q \in H_n^+$ *and assume that* ω *is any primitive character* mod q, *additive or multiplicative.*

(i) *If* $\omega = e_q(p)$, *then* $L(s, e_q(p), Q)$ *is a meromorphic function of* s *having a unique singularity at* $s = n/2$ *corresponding to a simple pole with residue*

$$\operatorname*{res}_{s=n/2} L(s, e_q(p), Q) = \frac{(2\pi)^{n/2} q^{-n}}{D(Q)^{1/2}\Gamma(n/2)} G_Q(q, p).$$

(ii) *If* $\omega = \chi$, *then* $L(s, \chi, Q)$ *is an entire function of* s, *provided* χ^* *exists and is nonprincipal.*

THEOREM 3. *Let* $(q, Q) \in H_n^+$ *and assume that* ω *is a primitive character* mod q *such that* ω^* *is defined and primitive* mod q *(cf.* (9) *and Theorem* 1(ii)). *Then there exists an integral positive definite quadratic form* Q^*, *depending on* q *and* Q, *such that*

$$Z(s, \omega, Q) = \epsilon(\omega, Q) Z(n/2 - s, \overline{\omega}^*, Q^*), \tag{16}$$

where

$$Z(s, \omega, Q) = (qR(q, Q)^{1/n}/2\pi)^s \Gamma(s) L(s, \omega, Q)$$

and $\epsilon(\omega, Q)$ *is defined by* (11). *Also,* $R(q, Q)$ *is defined in* (14).

Note that the right-hand side of (16) is defined even though (q, Q^*) may not belong to H_n^+, in spite of Q^* being integral (cf. Remark 5 below).

REMARKS. 1. From the obvious identity

$$L(s, \chi, Q) = \frac{1}{\tau(\overline{\chi})} \sum_{p \bmod q} \overline{\chi}(p) L(s, e_q(p), Q) \tag{17}$$

for primitive χ, we obtain

$$Z(s, \chi, Q) = \frac{1}{\tau(\overline{\chi})} \sum_{p \bmod q} \overline{\chi}(p) Z(s, e_q(p), Q).$$

Therefore, the functional equation for $Z(s, \chi, Q)$ follows immediately from the functional equation for $Z(s, e_q(p), Q)$, which we establish in §6.

2. The decisive step in establishing (16) for $(q, Q) \in H_n^+$ and ω additive is the explicit evaluation of $G_Q(q, p, \mathbf{a})$ given in Theorem 1(i).

3. In his paper, Stark does not assume that $Q^\dagger$ is integral. In the present paper, however, not only does this assumption simplify to some extent the proof of Theorem 1, it is essential. Indeed, the form Q defined by $X_1^2 + X_2^2 + X_3^2 + X_2X_3$, whose discriminant is 6, does not belong to H_3 since $Q^\dagger$ is not integral, and furthermore Theorem 1(i) is easily seen to be false with $q = 2$ and $\mathbf{a} = (1, 0, 0)'$.

4. Q^* is defined explicitly in (31) and (32) in terms of the Smith Normal Form of $A^\dagger$. If $\delta = 1$, then $Q^* = Q^\dagger$, so that (16) is essentially Stark's result in [8] for ω multiplicative. For $n = 2$ and $Q(X, Y) = aX^2 + 2bXY + cY^2$ with $(a, b) = 1$, say, then

$$Q^*(X, Y) = \delta((1 + Ds^2)/a)X^2 + 2sDXY + aD_qY^2,$$

where $s \in Z$ is defined by $bs \equiv 1 \bmod a$. This is a fairly direct consequence of (29), since the congruence conditions on the sum are easily seen to be equivalent to the single congruence condition $ax + by \equiv 0 \bmod \delta$. Observe that Q^* is an integral form with $D(Q^*) = D(Q)$.

5. The statement of Theorem 3 contains a defect, namely, our functional equation cannot be iterated except in special instances, since $(q, Q) \in H_n^+$ does not necessarily imply that $(q, Q^*) \in H_n^+$. However, if $\delta = 1$ or $n = 2$, this defect does not arise in view of earlier remarks.

4. **Proof of Theorem 1.** For each $\gamma \in Z^n$, the automorphism of the group of residue classes mod q defined by $\mathbf{x} \longrightarrow \mathbf{x} + \bar{p}\gamma$ transforms $G_Q(q, p, \mathbf{a})$ defined by (6) into

$$G_Q(q, p, \mathbf{a}) = e_q(\bar{p}Q(\gamma) + \bar{p}\mathbf{a} \cdot \gamma)G_Q(q, p, A\gamma + \mathbf{a}) \tag{18}$$

where A is the defining matrix of Q. In order to evaluate $G_Q(q, p, \mathbf{a})$, the following result is found to be useful. The proof is an easy consequence of the well-known matrix identity $AA^\dagger = DI_n$, $D = \det A$.

LEMMA 1. *$A\mathbf{X} + \mathbf{a} \equiv \mathbf{0} \bmod q$ is solvable in Z^n iff $A^\dagger\mathbf{a} \equiv \mathbf{0} \bmod \delta$, $\delta = (D, q)$. If the congruence is solvable, then $-\overline{D_q}\delta^{-1}A^\dagger\mathbf{a}$ is a solution.*

To evaluate $G_Q(q, p, \mathbf{a})$, we distinguish two cases.

Case 1. *$A\mathbf{X} + \mathbf{a} \equiv \mathbf{0} \bmod q$ is solvable.* By Lemma 1, $A^\dagger\mathbf{a} \equiv \mathbf{0} \bmod \delta$. Therefore, $D\mathbf{a}'A^\dagger\mathbf{a} = 2Q(A^\dagger\mathbf{a}) \equiv 0 \bmod 2\delta^2$, which may be rewritten as $\mathbf{a}'A^\dagger\mathbf{a} \equiv 0 \bmod 2\delta$ when δ is even, since $(D_q, q) = 1$ implies $(D_q, 2\delta) = 1$; for δ odd, this is trivial. Hence, $A^\dagger\mathbf{a} \equiv \mathbf{0} \bmod \delta$ implies $Q^\dagger(\mathbf{a}) \equiv 0 \bmod \delta$, noting that $Q^\dagger$

is an integral form since $Q \in H_n$. Using the solution of $A\mathbf{X} + \mathbf{a} \equiv \mathbf{0} \bmod q$ given in Lemma 1, then (18) becomes

$$G_Q(q, p, \mathbf{a}) = e_q(-\overline{pD_q}\delta^{-1}Q^\dagger(\mathbf{a}))G_Q(q, p, \mathbf{0}),$$

where $\delta^{-1}Q^\dagger(\mathbf{a}) \in Z$. Furthermore, it is easy to verify that this result is independent of which solution of $A\mathbf{X} + \mathbf{a} \equiv \mathbf{0} \bmod q$ is chosen.

Case 2. $A\mathbf{X} + \mathbf{a} \equiv \mathbf{0} \bmod q$ *is not solvable.* We shall prove that $G_Q(q, p, \mathbf{a}) = 0$. To verify this, replace γ in (18) by $q_1 A^\dagger \gamma$, where q_1 is defined by $q = \delta q_1$, so that

$$G_Q(q, p, \mathbf{a}) = e_q(\bar{p}q_1 A^\dagger \mathbf{a} \cdot \gamma)G_Q(q, p, \mathbf{a}). \tag{19}$$

If $A^\dagger \mathbf{a} \cdot \gamma \equiv 0 \bmod \delta$ for all $\gamma \in Z^n$, then we would have $A^\dagger \mathbf{a} \equiv \mathbf{0} \bmod \delta$, contrary to Lemma 1. Therefore, there exists $\gamma \in Z^n$ so that $\bar{p}q_1 A^\dagger \mathbf{a} \cdot \gamma \not\equiv 0 \bmod q$, from which the result follows by (19). This completes the proof of (i).

To prove (15), we employ a variation of a technique used by Stark [8]. By Jones [4, p. 65, Theorem 25], we know that for each odd prime l, and for each positive integer e, there exists $E \in SL(n, Z)$ such that $EAE' \equiv 2K \bmod l^e$, where $K \in M_n(Z)$ is a diagonal matrix. By the Chinese Remainder Theorem and the fact that q is odd, there exists $E \in M_n(Z)$ with $\det E \equiv 1 \bmod q$ such that $EAE' \equiv 2C \bmod q$, where $C = [c_i\delta_{ij}] \in M_n(Z)$ is a diagonal matrix. Therefore, the automorphism of the group of residue classes mod q defined by $\mathbf{x} \longrightarrow E\mathbf{x}$ transforms $G_Q(q, p)$ into

$$G_Q(q, p) = \sum_{\mathbf{x} \bmod q} e_q(p(c_1x_1^2 + \cdots + c_nx_n^2)) = \prod_{j=1}^{n} G(q, pc_j), \tag{20}$$

where $G(q, h)$ is the ordinary Gaussian sum defined by

$$G(q, h) = \sum_{x \bmod q} e_q(hx^2).$$

It is well known that

$$G(q, ph) = \left(\frac{p}{r}\right)G(q, h) \quad \text{and} \quad |(G(q, h)| = \sqrt{dq},$$

where $(p, q) = 1$, $(q, h) = d$, $q = dr$ and

$$\left(\frac{p}{r}\right)$$

is the Jacobi symbol. Therefore, (20) implies

$$G_Q(q, p) = \prod_{j=1}^{n}\left(\frac{p}{q_j}\right) \cdot G_Q(q, 1) \tag{21}$$

and

$$|G_Q(q, p)|^2 = t_1 \cdots t_n q^n, \tag{22}$$

where $t_j = (c_j, q)$ and $q = t_j q_j$, $j = 1, \ldots, n$. In order to obtain an invariant interpretation of the product $t_1 \cdots t_n$, we evaluate $|G_Q(q, p)|$ in another way, which is given by

LEMMA 2. *Let $Q \in H_n$ and $p, q \in Z$ be relatively prime, $q \geqslant 1$. If $G_Q(q, p) \neq 0$, then*

$$|G_Q(q, p)|^2 = q^n N(q, Q), \tag{23}$$

where $N(q, Q)$ is defined by (13).

We shall complete the proof of Theorem 1(ii) before proving Lemma 2. By (20) and the results immediately following it, it is clear that $G_Q(q, p) \neq 0$, so that on comparing (22) and (23), we have $t_1 \cdots t_n = N(q, Q)$. Since $(p, q) = 1$ and t_j divides q for each $j = 1, \ldots, n$, then $(p, N(q, Q)) = 1$. Therefore, (15) follows immediately from (21), as required.

We now prove Lemma 2. By the definition of $G_Q(q, p)$, we clearly have

$$|G_Q(q, p)|^2 = \sum_{\mathbf{x} \bmod q} \sum_{\mathbf{y} \bmod q} e_q(p[Q(\mathbf{y}) - Q(\mathbf{x})]);$$

applying the automorphism $\mathbf{y} \longrightarrow \mathbf{y} + \mathbf{x}$ to the inner sum transforms the sum into

$$\sum_{\mathbf{x},\mathbf{y} \bmod q} e_q(p[Q(\mathbf{y}) + \mathbf{x} \cdot A\mathbf{y}]).$$

By appealing to the obvious identity

$$\sum_{\mathbf{x} \bmod q} e_q(\mathbf{a} \cdot \mathbf{x}) = q^n E_q(\mathbf{a}),$$

$\mathbf{a} \in Z^n$ (cf. (12)), it follows that

$$|G_Q(q, p)|^2 = q^n \psi, \tag{24}$$

where

$$\psi = \sum_{\mathbf{x} \bmod q; A\mathbf{x} \equiv 0 \bmod q} e_q(pQ(\mathbf{x})).$$

Now consider

$$\psi^2 = |\psi|^2 = \sum_{\mathbf{x},\mathbf{y} \bmod q; A\mathbf{x} \equiv A\mathbf{y} \equiv 0 \bmod q} e_q(p[Q(\mathbf{y}) - Q(\mathbf{x})]).$$

The same argument used above (i.e., $\mathbf{y} \longrightarrow \mathbf{y} + \mathbf{x}$) transforms this sum into $\psi^2 = N(q, Q)\psi$. Since $G_Q(q, Q) \neq 0$ by hypothesis, $\psi \neq 0$, whence $\psi = N(q, Q)$, as required.

REMARK. For $(q, Q) \in H_n$, it is easy to see that $A\mathbf{x} \equiv \mathbf{0} \bmod q$ implies $D\mathbf{x}'A\mathbf{x} = 2Q^{\dagger}(A\mathbf{x}) \equiv 0 \pmod{q^2}$ from which $\mathbf{x}'A\mathbf{x} \equiv 0 \bmod q$. Therefore, for q odd, (23) follows from (24) directly. However, for q even, this argument does not work. The proof of (23) given above has been designed to avoid these difficulties.

5. **Proof of Theorem 2.** Before beginning the proof of this theorem, we shall require the following information regarding the Epstein zeta function.

For each $Q \in H_n^+$ and $\mathbf{u}, \mathbf{v} \in \mathbf{R}^n$, the associated Epstein zeta function is defined as

$$\zeta(s, \mathbf{u}, \mathbf{v}, Q) = \sum_{\mathbf{x} \in Z^n, \mathbf{x}+\mathbf{v} \neq \mathbf{0}} e(\mathbf{x} \cdot \mathbf{u}) Q(\mathbf{x}+\mathbf{v})^{-s}, \tag{25}$$

which is an analytic function of s for $\sigma > n/2$ and has the following additional properties due to Epstein [2] (for a convenient version, see Siegel [6, p. 69]).

LEMMA 3. *$\zeta(s, \mathbf{u}, \mathbf{v}, Q)$ has an analytic continuation into the entire s-plane, which is an entire function of s if $\mathbf{u} \notin Z^n$. If $\mathbf{u} \in Z^n$, then $\zeta(s, \mathbf{u}, \mathbf{v}, Q)$ is meromorphic in the entire s-plane possessing a unique singularity at $s = n/2$ corresponding to a simple pole with residue $(2\pi)^{n/2}/D(Q)^{1/2}\Gamma(n/2)$. In either case, $\zeta(s, \mathbf{u}, \mathbf{v}, Q)$ satisfies the following symmetric functional equation*:

$$\left(\frac{D(Q)^{1/n}}{2\pi}\right)^{s} \Gamma(s)\zeta(s, \mathbf{u}, \mathbf{v}, Q) = e(-\mathbf{u}\cdot\mathbf{v})\left(\frac{D(Q^{\dagger})^{1/n}}{2\pi}\right)^{s'} \Gamma(s')\zeta(s', \mathbf{v}, -\mathbf{u}, Q^{\dagger})$$

where $s' = n/2 - s$ for fixed n.

REMARK. Lemma 3 is true in a much wider context, though the above is sufficient for the present needs (cf. [6]).

We now prove Theorem 2. By definition of $L(s, e_q(p), Q)$, we may partition Z^n into residue classes mod q so that

$$L(s, e_q(p), Q) = \sum_{\mathbf{d} \bmod q} e_q(pQ(\mathbf{d})) \sum_{\mathbf{x} \in Z^n - 0; \mathbf{x} \equiv \mathbf{d} \bmod q} Q(\mathbf{x})^{-s},$$

which by (25) can be rewritten as

$$L(s, e_q(p), Q) = q^{-2s} \sum_{\mathbf{d} \bmod q} e_q(pQ(\mathbf{d}))\zeta(s, \mathbf{0}, q^{-1}\mathbf{d}, Q). \tag{26}$$

By Lemma 3, it is clear that $L(s, e_q(p), Q)$ has an analytic continuation into the entire s-plane, and further that it is meromorphic in the entire s-plane with a unique singularity occurring at $s = n/2$ corresponding to a simple pole with residue as given in Theorem 2. To prove (ii), apply (i) to (17), which shows that $L(s, \chi, Q)$ has in fact a removable singularity at $s = n/2$ when χ^* is defined and nonprincipal mod q.

REMARK. In view of the functional equation for the Epstein zeta function, it is clear from (26) that a functional equation for $L(s, e_q(p), Q)$ can be written down. It turns out that the functional equation for $\zeta(s, \mathbf{u}, \mathbf{v}, Q)$, together with the condition $(q, Q) \in H_n^+$, forces the functional equation of $L(s, e_q(p), Q)$ to be symmetric. This is the content of the next section.

6. **Proof of Theorem 3 for $\omega = e_q(p)$, $(p, q) = 1$.** By multiplying both sides of (26) by $(D(Q)^{1/n}/2\pi)^s\Gamma(s)$ and applying the functional equation of $\zeta(s, \mathbf{0}, q^{-1}\mathbf{d}, Q)$ given in Lemma 3 we obtain

$$\left(\frac{D(Q)^{1/n}}{2\pi}\right)^s \Gamma(s)L(s, e_q(p), Q) = q^{-2s}\left(\frac{D(Q^\dagger)^{1/n}}{2\pi}\right)^{s'} \Gamma(s')W(s', e_q(p), Q) \tag{27}$$

where $s' = n/2 - s$ and

$$W(s', e_q(p), Q) = \sum_{\mathbf{d} \bmod q} e_q(pQ(\mathbf{d}))\zeta(s', q^{-1}\mathbf{d}, \mathbf{0}, Q^\dagger). \tag{28}$$

Inserting the definition of $\zeta(s', q^{-1}\mathbf{d}, \mathbf{0}, Q^\dagger)$ into (28) for $\sigma < 0$ and changing the order of summation, we find that

$$\begin{aligned} W(s', e_q(p), Q) &= \sum_{\mathbf{x}\in Z^n - 0} G_Q(q, p, \mathbf{x})Q^\dagger(\mathbf{x})^{-s'} \\ &= G_Q(q, p) \sum_{\mathbf{x}\in Z^n - 0; A^\dagger\mathbf{x}\equiv 0 \bmod \delta} e_q(-\overline{pD_q}\delta^{-1}Q^\dagger(\mathbf{x}))Q^\dagger(\mathbf{x})^{-s'} \end{aligned} \tag{29}$$

by Theorem 1.

Let $S = [s_i\delta_{ij}]$ denote the Smith Normal Form of $A^\dagger$, $s_i \in Z$ (cf. [5, p. 26]). Then there exists $U, V \in SL(n, Z)$ such that $A^\dagger = U^{-1}SV^{-1}$. Substituting this into (29) and applying the automorphism $\mathbf{x} \longrightarrow V\mathbf{x}$ of Z^n, we obtain

$$\begin{aligned} &W(s', e_q(p), Q) \\ &\quad = G_Q(q, p) \sum_{\mathbf{x}\in Z^n - 0; S\mathbf{x}\equiv 0 \bmod \delta} e_q(-\overline{pD_q}\delta^{-1}Q^\dagger(V\mathbf{x}))Q^\dagger(V\mathbf{x})^{-s'}. \end{aligned} \tag{30}$$

As S is diagonal, the restriction on the sum in (30) is easily dealt with. For each $i = 1, \ldots, n$, define b_i by

$$\delta = b_i(\delta, s_i) \quad \text{and put} \quad B = \begin{bmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_n \end{bmatrix}.$$

Define a quadratic form Q^* by

$$Q^*(\mathrm{X}) = \tfrac{1}{2}A^*[\mathrm{X}], \tag{31}$$

where A^* is the symmetric positive definite matrix defined by

$$A^* = \delta^{-1} B V' A^\dagger V B. \tag{32}$$

Since $SB \in \delta M_n(Z)$, $A^\dagger(VB\mathbf{x}) = U^{-1}SB\mathbf{x} \equiv \mathbf{0} \pmod{\delta}$ for all $\mathbf{x} \in Z^n$. Therefore, the argument at the beginning of the proof of Theorem 1(i), Case 1, shows that $\delta Q^*(\mathbf{x}) = Q^\dagger(VB\mathbf{x}) \equiv 0 \bmod \delta$, for all $\mathbf{x} \in Z^n$. Therefore, Q^* is an integral quadratic form belonging to H_n^+, so that (30) may be rewritten as

$$W(s', e_q(p), Q) = \delta^{-s'} G_Q(q, p) L(s', e_q(-pD_q), Q^*).$$

Consequently, (27) can now be written as

$$\left(\frac{qD(Q)^{1/n}}{2\pi}\right)^s \Gamma(s) L(s, e_q(p), Q) = q^{-n/2} G_Q(q, p) \left(\frac{qD(Q^\dagger)^{1/n}}{2\pi\delta}\right)^{s'} \Gamma(s') L(s', e_q(-\overline{pD_q}), Q^*). \tag{33}$$

The functional equation in (33) for our L-functions clearly lacks symmetry in its present form. However, in the special case in which $\delta = 1$, we can readily deduce (16) from (33) as follows. First we note that we may essentially take $Q^* = Q^\dagger$ in view of (29), in which case $N(q, Q) = 1$ since $\delta = 1$. Using (10) and (23), we obtain (16). The general case is more subtle and appears to essentially depend on our tentative functional equation (33) and the residue of our L-functions at $s = n/2$. First note that the functional equation of the Epstein zeta function of Lemma 3 immediately implies that

$$\zeta(0, \mathbf{u}, \mathbf{v}, Q) = \begin{cases} -e(-\mathbf{u} \cdot \mathbf{v}) & \text{if} \quad \mathbf{v} \in Z^n, \\ 0 & \text{otherwise.} \end{cases}$$

Combining this with (26), we find that $L(0, e_q(p), Q) = -1$. Multiplying both sides of (33) by s and letting $s \longrightarrow 0$, we find that Theorem 2(i) implies

$$G_Q(q, p) G_{Q^*}(q, -\overline{pD_q}) = q^n (\delta^n D(Q^*)/D(Q^\dagger))^{1/2}.$$

By (32), we find

$$\delta^n D(Q^*) = D(Q^\dagger) \det(B)^2, \tag{34}$$

so that

$$G_Q(q, p) G_{Q^*}(q, -\overline{pD_q}) = q^n \det B. \tag{35}$$

Taking absolute values of (35), and applying Lemma 2, as we may since the right-hand side of (35) is nonzero, we obtain

$$N(q, Q) N(q, Q^*) = \det(B)^2,$$

whence (34) becomes

$$\delta^n D(Q^*) = D(Q^\dagger)N(q, Q)N(q, Q^*). \tag{36}$$

Combining this result with (14), our tentative functional equation (33) can now be rewritten as

$$Z(s, e_q(p), Q) = q^{-n/2}N(q, Q)^{-1/2}G_Q(q, p)Z(s', e_q(-\overline{pD_q}), Q^*),$$

as claimed, in view of (10) and (23).

7. Some final observations. (35) may be interpreted as a kind of reciprocity law for our Gaussian sums $G_Q(q, p)$, which may be described equivalently by $\epsilon_{Q^*}(q, \overline{pD_q}) = \epsilon_Q(q, p)$.

It is worth noting that Stark [8, p. 43, Lemma 10] has introduced another type of reciprocity law for these Gaussian sums, namely,

$$G_Q(q, 1) = q^{n/2}D(Q)^{1/2-n}e_8(n)G_{Q^\dagger}(D, -q) \tag{37}$$

which holds for all $Q \in H_n^+$; the proof of this is a consequence of the analytic properties of the theta function of Q. In fact Stark introduced (37) precisely so that he could obtain the results in Theorem 1(ii) for arbitrary q, subject to his restriction that $(q, D(Q)) = 1$. Furthermore (37) can be used to extend Theorem 1(ii) to include the case of even q, provided $(q, Q) \in H_n$, but at the expense of considerable complications (cf. [8]).

From (37), one can deduce

$$D(Q^\dagger)N(q, Q) = \delta^n N(D_q, Q^\dagger),$$

so that on combining this with (36), we obtain the following interpretation of $R(q, Q^*)$, which can also be verified directly:

$$R(q, Q^*) = N(D_q, Q^\dagger).$$

ACKNOWLEDGEMENT. We wish to express our gratitude to the referee for several very helpful suggestions which have served to clarify an earlier version of this paper, and in particular, for helping to clarify the role of the prime two.

REFERENCES

1. S. Chowla and R. A. Smith, *On certain functional equations*, Norske Vid. Selsk. Forh. (Trondheim) 40 (1967), 43–47 (1968). MR 38 #2101.

2. P. Epstein, *Zur Theorie allgemeine Zeta funktionen.* I, II, Math. Ann. 56 (1903), 615–644; ibid. 63 (1907), 205–216.

3. T. Estermann, *On the representations of a number as a sum of two products*, Proc. London Math. Soc. (2) 31 (1930), 123–133.

4. B. W. Jones, *The arithmetic theory of quadratic forms*, Carus Monograph Series, no. 10, Math. Assoc. Amer.; distributed by Wiley, New York, 1950. MR 12, 244.

5. M. Newman, *Integral matrices,* Academic Press, New York, 1972.

6. C. L. Siegel, *Lectures on advanced analytic number theory,* Tata Institute of Fundamental Research Lectures on Math., no. 23, Tata Institute of Fundamental Research, Bombay, 1965. MR 41 #6760.

7. R. A. Smith, *The circle problem in an arithmetic progression,* Canad. Math. Bull. 11 (1968), 175–184. MR 38 #1064.

8. H. M. Stark, *L-functions and character sums for quadratic forms.* I, Acta Arith. 14 (1967/68), 35–50. MR 37 #2707.

9. ———, *L-functions and character sums for quadratic forms.* II, Acta. Arith. 15 (1968/69), 307–317. MR 39 #4101.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, TORONTO, ONTARIO, CANADA M5S 1A1