References

[1] B. Gordon, *On a Tauberian theorem of Landau*, Proc. Amer. Math. Soc. 9 (1958), pp. 693-696.

[2] G. H. Hardy, *Divergent series*, Oxford 1949.

[3] A. E. Ingham, *Some Tauberian theorems connected with the prime number theorem*, J. London Math. Soc. 20 (1945), pp. 171-180.

[4] — *On absolutely convergent Dirichlet series*, Studies in mathematical analysis and related topics, pp. 156-164, Stanford Univ. Press, Stanford, Calif., 1962.

[5] J. Karamata, *Sur les inversions asymptotiques de certains produits de convolution*, Bull. Acad. Serbe Sci. (N. S.) 20, Cl. Sci. Math. et Nat., n° 3 (1957), pp. 11-32.

[6] — *Sur les procédés de sommation intervenant dans la théorie des nombres*, Colloque sur la théorie des suites, tenu à Bruxelles du 18 au 20 décembre 1957, pp. 12-31.

[7] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig und Berlin 1909.

[8] — *Über einige neuere Grenzwertsätze*, Rend. Circ. Mat. Palermo 34 (1912), pp. 121-131.

[9] E. C. Titchmarsh, *The theory of the Riemann zeta-function*, Oxford 1951.

[10] A. Wintner, *Eratosthenian averages*, Baltimore 1943.

[11] — *On arithmetical summation processes*, Amer. J. Math. 79 (1957), pp. 559-574.

UNIVERSITY COLLEGE, LONDON
KING'S COLLEGE, CAMBRIDGE

Reçu par la Rédaction le 13. 1. 1964

ACTA ARITHMETICA
IX (1964)

On certain classes of positive definite quadratic forms

by

R. Brauer (Cambridge, Mass.)

To L. J. Mordell on his 75th birthday

In the theory of representations of finite groups, positive definite quadratic forms

$$Q(\mathfrak{x}) = \sum_{i,j=1}^{n} c_{ij} x_i x_j \tag{1}$$

with integral coefficients c_{ij} play a role which satisfy the following condition

(I) *The form Q can be represented by the unit form in $m > n$ variables.*

In other words, we require that there exists an $(m \times n)$-matrix D with integral coefficients such that

$$C = D'D \tag{2}$$

where the prime indicates the transposed matrix.

We are interested in obtaining estimates for integers represented by Q. We show

Theorem 1. *Let Δ be the largest elementary divisor of C. Let $\mathfrak{r}$ be a fixed row of D. Then $\mathfrak{x} = \Delta \mathfrak{r} C^{-1}$ is a row $\mathfrak{x} = (x_1, \ldots, x_n)$ with integral coefficients and*

$$Q(\mathfrak{x}) \leqslant \Delta^2. \tag{3}$$

Proof. Consider the set M of all columns $\mathfrak{t}$ of length m with coefficients in the ring Z of integers which satisfy the equation

$$D'\mathfrak{t} = 0.$$

Then M is a Z-module. Since C was non-singular, the rank of D is n and M has dimension $m-n$. Form an $m \times (m-n)$-matrix T whose columns form a Z-basis of M and set

$$W = T'T, \tag{4}$$

$$A = DC^{-1}D', \quad B = TW^{-1}T'. \tag{5}$$

It follows from (2), (4) and $D'T = 0$ that

$$AD = D, \quad AT = 0, \quad BD = 0, \quad BT = T.$$

Hence

$$(A+B)(D, T) = (D, T)$$

and since (D, T) is a non-singular $(m \times m)$-matrix, this implies that $A+B$ is the unit matrix I_m of degree m. If $\mathfrak{r}$ is the ith row of D and $\mathfrak{s}$ the ith row of T, we have

$$\mathfrak{r}C^{-1}\mathfrak{r}' + \mathfrak{s}W^{-1}\mathfrak{s}' = 1. \tag{6}$$

Since Δ is the largest elementary divisor of C, the matrix ΔC^{-1} has integral coefficients. It follows that the row $\mathfrak{x} = \Delta\mathfrak{r}C^{-1}$ has integral coefficients. By (6)

$$\mathfrak{x}\mathfrak{r}' = \Delta\mathfrak{r}C^{-1}\mathfrak{r}' \leqslant \Delta.$$

Since $\Delta\mathfrak{r} = \mathfrak{x}C$, we have $\Delta\mathfrak{r}' = C\mathfrak{x}'$,

$$\mathfrak{x}C\mathfrak{x}' \leqslant \Delta^2.$$

This proves the statement.

THEOREM 2. *Let Q be a quadratic form which satisfies condition* (I) *and let Δ be the largest elementary divisor of Q. There exists a form Q^* equivalent to Q such that the coefficients g_{ij} of the matrix (g_{ij}) of Q^* satisfy the conditions*

$$|g_{ij}| \leqslant (\tfrac{3}{2})^{i+j-2}\Delta^2. \tag{7}$$

The proof can be obtained in a fairly obvious manner from Theorem 1. Choosing n linearly independent rows of D, we obtain n linearly independent rows $\mathfrak{x}_1, \mathfrak{x}_2, \ldots, \mathfrak{x}_n$ with coefficients in $\boldsymbol{Z}$ such that

$$Q(\mathfrak{x}_i) \leqslant \Delta^2 \quad \text{for} \quad i = 1, 2, \ldots, n. \tag{8}$$

Let N be the $\boldsymbol{Z}$-module of all rows of length n with coefficients in $\boldsymbol{Z}$. We claim that we can find a $\boldsymbol{Z}$-basis $\mathfrak{y}_1, \mathfrak{y}_2, \ldots, \mathfrak{y}_n$ of N such that

$$\mathfrak{x}_i = \sum_{j \leqslant i} a_{ij}\mathfrak{y}_j \quad (1 \leqslant i \leqslant n) \tag{9}$$

with coefficients $a_{ij} \in \boldsymbol{Z}$ which satisfy

$$|a_{ij}| \leqslant \tfrac{1}{2}a_{ii} \quad \text{for} \quad j < i. \tag{10}$$

We take $a_{11}\mathfrak{y}_1 = \mathfrak{x}_1$ where $a_{11} > 0$ is the greatest common divisor of the n coefficients of $\mathfrak{x}_1$. Then $\mathfrak{y}_1$ can be taken as the first element of a basis of N. Suppose that we have already found $h-1$ elements $\mathfrak{y}_1, \ldots, \mathfrak{y}_{h-1}$ of a basis B of N such that (9) and (10) hold for $i < h$. If $h \leqslant n$, let the coordinates of $\mathfrak{x}_h$ with regard to the basis B be given by $(\xi_1, \xi_2, \ldots, \xi_n)$.

Then $\xi_h, \xi_{h+1}, \ldots, \xi_n$ cannot all vanish. Let $a_{hh} > 0$ denote the greatest common divisor of these $n-h+1$ integers. For $j < h$, determine a_{hj} as the absolute least residue of the division of ξ_j by a_{hh},

$$\xi_j \equiv a_{hj} \pmod{a_{hh}}; \quad |a_{hj}| \leqslant \tfrac{1}{2}|a_{hh}|.$$

Then

$$\mathfrak{y}_h = \frac{1}{a_{hh}}\Big(\mathfrak{x}_h - \sum_{j<h} a_{hj}\mathfrak{y}_j\Big)$$

belongs to N. Moreover, the greatest common divisor of the last $n-h+1$ coordinates with regard to the basis B is 1. Hence $\mathfrak{y}_1, \ldots, \mathfrak{y}_h$ form part of a $\boldsymbol{Z}$-basis of N. Clearly, (9) and (10) hold for $i = h$.

Applying this for $h = 2, 3, \ldots, n$, we obtain a $\boldsymbol{Z}$-basis $\mathfrak{y}_1, \ldots, \mathfrak{y}_n$ with the required properties.

On solving (9) for $\mathfrak{y}_i$, we have formulas

$$\mathfrak{y}_i = \sum_{k \leqslant i} b_{ik}\mathfrak{x}_k \quad (1 \leqslant i \leqslant n) \tag{11}$$

with rational coefficients b_{ik}. Here

$$b_{ii} = \frac{1}{a_{ii}} \leqslant 1, \quad |b_{ik}| \leqslant \frac{1}{2}\Big(\frac{3}{2}\Big)^{i-k-1} \quad \text{for} \quad k < i. \tag{12}$$

Indeed, it follows from (9) and (11) that

$$a_{ii}\mathfrak{y}_i = \mathfrak{x}_i - \sum_{j<i} a_{ij} \sum_{k \leqslant j} b_{jk}\mathfrak{x}_k.$$

Hence $b_{ii} = a_{ii}^{-1}$ and, for $k < i$

$$a_{ii}b_{ik} = -\sum_j a_{ij}b_{jk}$$

with j ranging over $k, k+1, \ldots, i-1$. Since $|a_{ij}| \leqslant \frac{1}{2}a_{ii}$ by (10), we obtain the second inequality (12) easily by induction.

Let $Q(\mathfrak{x}, \mathfrak{z})$ denote the bilinear form belonging to Q, $\mathfrak{x}, \mathfrak{z} \in N$. Then (8) implies

$$|Q(\mathfrak{x}_j, \mathfrak{x}_k)| \leqslant \Delta^2.$$

It now follows from (11) that

$$Q(\mathfrak{y}_i) \leqslant \sum_{j,k \leqslant i} |b_{ij}b_{ik}|\Delta^2 = \Delta^2\Big(\sum_{j \leqslant i} |b_{ij}|\Big)^2$$

and now (12) yields

$$Q(\mathfrak{y}_i) \leqslant \Delta^2(\tfrac{3}{2})^{2i-2}.$$

Then

$$|Q(\mathfrak{y}_i, \mathfrak{y}_j)| \leqslant \left(Q(\mathfrak{y}_i)Q(\mathfrak{y}_j)\right)^{1/2} \leqslant \Delta^2 (\tfrac{3}{2})^{i+j-2}.$$

Since $\mathfrak{y}_1, \ldots, \mathfrak{y}_n$ was a basis of N, the theorem is proved.

We can apply the same method to the quadratic form Q^* whose matrix is the inverse matrix C^{-1}. If $\mathfrak{x}_1, \ldots, \mathfrak{x}_n$ are n linearly independent rows of D, then (6) shows that

$$Q^*(\mathfrak{x}_i) \leqslant 1 \qquad (i = 1, 2, \ldots, n).$$

In fact, if $\mathfrak{s}_i$ is the row of T corresponding to the row $\mathfrak{x}_i$ of D and if

$$\mu = \min_{i=1,2,\ldots,n} (\mathfrak{s}_i W^{-1} \mathfrak{s}_i') \tag{13}$$

then

$$Q^*(\mathfrak{x}_i) \leqslant 1 - \mu \qquad (i = 1, 2, \ldots, n).$$

We now have

THEOREM 3. *If Q^* is the quadratic form whose matrix is the inverse of the matrix C of Q in Theorem 2, then Q^* is equivalent to a form whose matrix g_{ij}^* satisfies the conditions*

$$|g_{ij}^*| \leqslant (\tfrac{3}{2})^{i+j-2}. \tag{14}$$

If μ is defined by (13), *we may replace* (14) *by*

$$|g_{ij}^*| \leqslant (1-\mu)(\tfrac{3}{2})^{i+j-2}. \tag{14*}$$

Let S be the quadratic form with the matrix W in (4). Then S is determined by D up to equivalence. As shown by (4), S satisfies again our condition (I); the number of variables in S is $m-n$. In order to have complete symmetry between Q and S, we impose on D a further condition

(II) *The n-th determinant divisor of D is 1. This means that Q is represented properly by the unit form in m variables.*

This condition is satisfied for the quadratic forms occurring in group theory.

It follows from the manner in which T was constructed that the $(m-n)$-th determinant divisor of T is 1. Hence S always satisfies the condition analogous to (II). If D satisfies (II), the columns of D form a basis for the $\boldsymbol{Z}$-module of columns with integral coefficients which are orthogonal to the columns of T. Hence the relationship between the classes of Q and of S is reciprocal. We shall speak of dual classes. We show:

THEOREM 4. *If the conditions* (I) *and* (II) *are satisfied, the form Q and a form S in the dual class have the same elementary divisors different from* 1.

Proof. Let p be a fixed prime and let R_p denote the ring of local integers for p. If we replace $\boldsymbol{Z}$ by R_p, the elementary divisors of, say, C are simply the powers of p which divide the elementary divisors of C in the original sense. It will therefore suffice to prove the theorem in the case that $\boldsymbol{Z}$ is replaced by R_p.

If the rows of D are taken in suitable order, it follows from (II) that there exists an $(n \times n)$-matrix V of determinant 1 with coefficients in R_p such that

$$DV = \begin{pmatrix} I_n \\ A \end{pmatrix}$$

where I_n denotes the unit matrix of degree n and where A is an $(m-n) \times n$-matrix. In R_p, Q is equivalent to the form with the matrix

$$C_1 = V'CV = (DV)'(DV) = I_n + A'A. \tag{15}$$

On the other hand, if we work in R_p, we may take

$$T = \begin{pmatrix} -A' \\ I_{m-n} \end{pmatrix}.$$

Then (4) yields

$$W = I_{m-n} + AA'. \tag{16}$$

Let s be a positive integer. The number k of elementary divisors of C_1 in R_p which are divisible by p^s can be interpreted as the maximal number of columns $\mathfrak{x}_1, \ldots, \mathfrak{x}_k$ with coefficients in R_p which are linearly independent mod p and which satisfy

$$C_1 \mathfrak{x}_j \equiv 0 \pmod{p^s} \tag{17}$$

$(j = 1, 2, \ldots, k)$. Set $\mathfrak{y}_j = A\mathfrak{x}_j$. On account of (15), (17) can be written as $\mathfrak{x}_j + A'\mathfrak{y}_j \equiv 0 \pmod{p^s}$. If we multiply with A and use (16), we find

$$W\mathfrak{y}_j \equiv 0 \pmod{p^s}. \tag{18}$$

Suppose that we have a congruence

$$\sum_j \alpha_j \mathfrak{y}_j \equiv 0 \pmod{p}$$

with coefficients $\alpha_j \in R_p$. Multiply with A'. Since $s \geqslant 1$, it follows from (15) and (17) that

$$A'\mathfrak{y}_j = A'A\mathfrak{x}_j = (C_1 - I_n)\mathfrak{x}_j \equiv -\mathfrak{x}_j \pmod{p}$$

and we obtain $\sum \alpha_j \mathfrak{x}_j \equiv 0 \pmod{p}$. Now, $\mathfrak{x}_1, \ldots, \mathfrak{x}_k$ were linearly independent (mod p). It follows that all α_j are divisible by p. Hence $\mathfrak{y}_1, \ldots, \mathfrak{y}_k$ are linearly independent (mod p). Now (18) shows that W has at least

k elementary divisors in R_p which are divisible by p^s. By reasons of symmetry, C_1 and W have the same number of elementary divisors which are divisible by p^s. Since this holds for every $s > 0$, the theorem now is evident.

We discuss briefly the application to the group theoretical case. Let G be a finite group, p a given prime and consider a p-block of given defect d. Since the following results are trivial for defect 0, we assume $d > 0$. Let D be the matrix of decomposition numbers of B and let C be the Cartan matrix. Then our assumptions (I) and (II) are satisfied and (2) holds. We suppose here that an arbitrary basic set φ_B for the block B is used (cf. [1]). Actually, the greatest elementary divisor Δ of C is p^d and it appears only once, [2]. The number n of rows of C is the number of irreducible modular characters in B and then

$$n < p^{2d} \tag{19}$$

cf. [3].

In [1], we noted that there exists a number $\gamma(p^d)$ depending only on p and d and not on G with the following property. If a suitable basic set φ_B for the block B is chosen, the coefficients of C lie below $\gamma(p^d)$ in absolute value. As a consequence of Theorem 2 and (19), we have

COROLLARY 1. *The function $\gamma(p^d)$ for finite groups can be chosen as*

$$\gamma(p^d) = (\tfrac{9}{4})^{p^{2d-1}} p^{2d}.$$

The principal p-block B_0 is of special interest, i.e. the block which contains the principal character $\chi_1 = 1$. The defect d here is the exponent of the maximal power of p which divides the group order. It is natural to subject the basic set φ_B in the case $B = B_0$ to the condition that $1 \in \varphi_B$. We have noted in [1] that there exists an expression $\gamma_0(p^d)$ depending only on p and d with the following property. There exists a basic set with $1 \in \varphi_B$ for which the Cartan invariants are at most equal to $\gamma_0(p^d)$. We can use Corollary 1 to discuss $\gamma_0(p^d)$, but it is perhaps easier to apply Theorem 3.

If a row $\mathfrak{s}$ of T was equal to 0, the corresponding irreducible character χ would vanish for all p-singular elements of G. In particular, $\chi(\sigma) = 0$ for all elements $\sigma \neq 1$ of a p-Sylow group P of G. This implies that the degree $\chi(1)$ of χ is divisible by the order of P and then χ is of defect 0. This case could be excluded. It follows that μ in (13) is not 0. Then

$$\mu \geqslant p^{-d}. \tag{20}$$

We first take φ_B as the set of modular irreducible characters $\varphi_1 = 1$, $\varphi_2, \ldots, \varphi_n$ in $B = B_0$. If the first row $\mathfrak{r}_1$ of D corresponds to the principal character of G, then

$$\mathfrak{r}_1 = (1, 0, \ldots, 0).$$

Now Theorem 3 shows that we can find a basis $\mathfrak{y}_1 = \mathfrak{r}_1, \mathfrak{y}_2, \ldots, \mathfrak{y}_n$ of N such that

$$|Q^*(\mathfrak{y}_i, \mathfrak{y}_j)| \leqslant (1-p^{-d})(\tfrac{3}{2})^{i+j-2}. \tag{21}$$

Let $V = (v_{ij})$ be the matrix whose rows contain the coordinates of $\mathfrak{y}_1, \ldots, \mathfrak{y}_n$ with regard to the original basis of N (corresponding to $\varphi_1, \varphi_2, \ldots, \varphi_n$). Introduce a basic set $\psi_1, \ldots, \psi_n$ of B by setting

$$\psi_i = \sum_{j=1}^{n} v_{ij}\varphi_j \qquad (i = 1, 2, \ldots, n).$$

Then $\psi_1 = \varphi_1 = 1$. If $\tilde{C}$ is the Cartan matrix belonging to this new basic set, the coefficient in the ith row, jth column of $\tilde{C}^{-1}$ is $Q^*(\mathfrak{y}_i, \mathfrak{y}_j)$. Applying Hadamard's theorem on determinants and using (14*), we can give an estimate for the minors of degree $n-1$ of $\tilde{C}^{-1}$. An easy computation shows that each coefficient $\tilde{c}_{ij}$ of $\tilde{C}$ is at most equal to

$$c = (1-p^{-d})^{n-1}(\tfrac{3}{2})^{3n(n-1)/2}(\tfrac{4}{5})^{(n-1)/2} \det C \tag{22}$$

in absolute value. Since p^d was the largest elementary divisor of C and since it occurs only once, we have

$$\det C \leqslant p^{d+(n-1)(d-1)}. \tag{23}$$

On combining (22), (23), and (19), we obtain explicit values for $\gamma_0(p^d)$. For instance, we can say

COROLLARY 2. *The function $\gamma_0(p^d)$ for finite groups can be chosen as*

$$\gamma_0(p^d) = (\tfrac{3}{2})^{3p^{4d}/2} p^{dp^{2d}}. \tag{24}$$

We conclude the paper with the following remark.

THEOREM 5. *If the form Q satisfies the assumption* (I) *and if Q represents a form Q_0 of determinant 1 in n_0 variables with $1 \leqslant n_0 \leqslant n$, then Q_0 is equivalent with the unit form in n_0 variables. Moreover, n_0 rows of the matrix T vanish.*

Proof. If Q_0 has the matrix C_0, there exists an $(n \times n_0)$-matrix V with integral coefficients such that $V'CV = C_0$. If we set $D_0 = DV$, we have $D_0'D_0 = C_0$. If d_λ ranges over the minors of degree n_0 of D_0, it follows that

$$1 = \det C_0 = \sum d_\lambda^2. \tag{25}$$

Consequently, one of the d_λ is ± 1 while all others vanish. If we replace Q_0 by a suitable equivalent form, we may assume that I_{n_0} appears as a submatrix of D_0. Then (25) shows that the other $m-n_0$ rows of D_0

vanish. Hence $C_0 = I_{n_0}$. Since the columns of D_0 are orthogonal to the columns of T, it follows that n_0 rows of T vanish and the proof is complete.

We have already remarked that, in the case of quadratic forms Q associated with p-blocks of positive defect of finite groups, no row of the matrix T can vanish. Hence Q cannot represent a form Q_0 of determinant 1. In particular, Q cannot represent the number 1.

References

[1] R. Brauer, *On blocks of representations of finite groups*, Proc. Nat. Acad. Sci. 47 (1961), pp. 1888-1890.

[2] — *Zur Darstellungstheorie der Gruppen endlicher Ordnung I*, Math. Zeitschr. 63 (1956), pp. 25-46.

[3] — and W. Feit, *On the number of irreducible characters of finite groups in a given block*, Proc. Nat. Acad. Sci. 45 (1959), pp. 361-365.

HARVARD UNIVERSITY

Reçu par la Rédaction le 17. 1. 1964

ACTA ARITHMETICA
IX (1964)

On Epstein's zeta function

by

P. T. Bateman (Urbana, Ill.) and E. Grosswald (Philadelphia, Pa.)*

Dedicated to Professor L. J. Mordell on the occasion of his seventy-fifth birthday

§ 1. Introduction and statement of results. The purpose of this paper is to give detailed proofs of two theorems on the Epstein zeta function which were announced without proof by S. Chowla and A. Selberg about fifteen years ago [1]. The two results which they announced are our Theorem 1 and a slightly weaker form of our Theorem 3. Our Theorem 2 was not stated explicitly by Chowla and Selberg in their paper, but they did indicate that they were in possession of a result of the same nature as our Theorem 2, that is, one giving a good approximation to the Epstein zeta function in the critical strip, particularly on or near the real line.

Throughout this paper a, b, and c will denote real numbers with $a > 0$ and $d = b^2 - 4ac < 0$, so that $am^2 + bmn + cn^2$ is a positive definite quadratic form. The Epstein zeta function associated with this form is given by

$$Z(s) = \tfrac{1}{2} {\sum}' (am^2 + bmn + cn^2)^{-s} \qquad (\mathrm{Re}\, s > 1), \tag{1}$$

where the stroke on the sign of summation indicates that the summation is to be extended over all pairs (m, n) of integers other than the pair $(0, 0)$. It will be convenient to define a positive number k by putting

$$k^2 = \frac{|d|}{4a^2} = \frac{4ac - b^2}{4a^2} = \frac{c}{a} - \left(\frac{b}{2a}\right)^2.$$

As usual ζ will denote the Riemann zeta function. We shall also require the Bessel function defined for arbitrary ν and $|\arg z| < \pi/2$ by

$$K_\nu(z) = \tfrac{1}{2} \int_0^\infty e^{-z(u+u^{-1})/2} u^{\nu-1}\, du = \tfrac{1}{2} \int_{-\infty}^{\infty} e^{-z\cosh t} e^{\nu t}\, dt = \int_0^\infty e^{-z\cosh t} \cosh \nu t\, dt. \tag{2}$$

* This work was supported by the U. S. Office of Naval Research and by the National Science Foundation.