JOURNAL OF NUMBER THEORY 17, 52–70 (1983)

Character Sums in Algebraic Number Fields

JÜRGEN G. HINZ

Department of Mathematics, University of Marburg, Lahnberge, 3550 Marburg, Federal Republic of Germany

Communicated by E. Hlawka

Received August 11, 1981

The Pólya–Vinogradov inequality is generalized to arbitrary algebraic number fields K of finite degree over the rationals. The proof makes use of Siegel's summation formula and requires results about Hecke's zeta-functions with Grössencharacters. One application is to the problem of estimating a least totally positive primitive root modulo a prime ideal of K, least in the sense that its norm is minimal.

1. Introduction

In 1918 Pólya [13] and Vinogradov [20] proved independently the following result about the estimation of character sums: If χ is a primitive Dirichlet character to a modulus $q > 1$, then we have for any positive integer N

$$\sum_{n=1}^{N} \chi(n) \ll q^{1/2} \log q, \qquad (1)$$

where $A \ll B$ is Vinogradov's notation for $|A| < cB$ for some constant c, and where in (1) c is absolute.

Deeper estimates of character sums were published in 1962 by Burgess [1–3]. The investigations lead, e.g., for a prime modulus p to an improved version of (1) in which the term $p^{1/2} \log p$ is replaced by $N^{1-1/(r+1)} p^{1/4r} \log p$, where r is an arbitrary positive integer. Burgess made use of (1) and Weil's result on the analog of the Riemann hypothesis for the zeta-function of an algebraic function field over a finite field.

There are many interesting applications of (1), and we mention just one. Let $m(p)$ denote the least positive primitive root mod p, where p is a prime. Using inequality (1), Vinogradov showed (see, e.g., [11]) that

$$m(p) \ll p^{(1/2)+a} \qquad \text{for fixed } a > 0. \qquad (2)$$

0022-314X/83 $3.00

This classical result can be improved by applying the deep estimates of character sums, due to Burgess. Moreover, the Pólya–Vinogradov inequality (1) is an essential ingredient in Gallagher or Vaughan's proofs of the important Bombieri–Vinogradov theorem on the average distribution of prime numbers in arithmetic progressions.

In 1918 Landau [10] generalized the Pólya–Vinogradov inequality to arbitrary algebraic number fields of finite degree n over the rationals. Let χ be a primitive nonprincipal character of the group of narrow ideal-classes modulo an ideal $\mathfrak{q}$. Then we have

$$\sum_{N\mathfrak{a}\leqslant x} \chi(\mathfrak{a}) \ll N\mathfrak{q}^{1/(n+1)}(\log N\mathfrak{q})^{n} \cdot x^{(n-1)/(n+1)},$$

where the implied constant depends only on K. It is easily seen that this estimate also holds if the summation is only over principal ideals.

Finally, a paper of Davenport and Lewis [4] should be mentioned in which the authors extend inequality (1) to finite fields. The object of the present paper is to give the following generalization of the Pólya–Vinogradov theorem:

Let K be an algebraic number field of degree $n = r_1 + 2r_2$ (in the usual notation) over the rationals with discriminant d. Z_K will denote the ring of integers in K. Let $P_1,\dots, P_{r+1}$, $r = r_1 + r_2 - 1$, be positive real numbers and $P = P_1 \cdots P_{r+1} \geqslant 1$. Consider the set $\mathfrak{N}$ of integers $\alpha \in Z_K$ subject to the conditions

$$\begin{aligned} 0 &< \alpha^{(k)} \leqslant P_k, & k &= 1,\dots, r_1, \\ 0 &< |\alpha^{(k)}|^2 \leqslant P_k, & k &= r_1 + 1,\dots, r + 1. \end{aligned} \tag{3}$$

Let $\mathfrak{q}$ be an integral ideal of K. The residue classes of integers relatively prime to $\mathfrak{q}$ form a group under multiplication, the order of which is denoted by $\Phi(\mathfrak{q})$. Let χ be a character on this group. We define primitive characters in the usual way.

THEOREM 1. *Let χ be a nonprincipal character* mod $\mathfrak{q}$, *then we have for any $a > 0$*

$$\sum_{\alpha\in\mathfrak{N}} \chi(\alpha) \ll N\mathfrak{q}^{1/2(r+2)} P^{1-(1/(r+2))+a}. \tag{4}$$

The implied $\ll$-constant depends on a and K.

Now it should be possible to extend the important work of Burgess to algebraic number fields. Result (4) is the first step in this direction. We may return to this problem in a future paper.

The proof of Theorem 1 requires results about Hecke's zeta-functions with

Grössencharacters and makes use of an identity given by Siegel in [19] for real quadratic number fields. This identity has been generalized by Grotz [7] to arbitrary algebraic number fields. For the application the following corollary of Theorem 1 can be used:

COROLLARY. *Let χ be a nonprincipal character* mod $\mathfrak{q}$. *For $a > 0$ there exists a positive number $b = b(a, r)$ such that if $N\mathfrak{q}$ is sufficiently large and P satisfies $P > N\mathfrak{q}^{(1/2)+a}$, then*

$$\left| \sum_{\alpha \in \mathfrak{R}} \chi(\alpha) \right| < P \cdot (N\mathfrak{q})^{-b}.$$

For another kind of character sums, a similar result valid only for a range of smaller values of P was found by Friedlander [5, Theorem 3.3.1]. Let $\mu_1,\ldots,\mu_n$ be an integral basis of K, so that every $\alpha \in Z_K$ is representable uniquely as $\alpha = l_1\mu_1 + \cdots + l_n\mu_n$, where $l_1,\ldots,l_n$ are rational integers. Let $\mathfrak{R}_1 = \{\alpha = l_1\mu_1 + \cdots + l_n\mu_n \in Z_K;\ |l_i| \leqslant \frac{1}{2}P^{1/n},\ i = 1,\ldots,n\}$, then Friedlander proved for large $N\mathfrak{p}$ and $N\mathfrak{p}^{(1/4)+a} \leqslant P \leqslant N\mathfrak{p}^{1/2}$

$$\left| \sum_{\alpha \in \mathfrak{R}_1} \chi(\alpha) \right| < P \cdot (N\mathfrak{p})^{-b},$$

where χ denotes a nonprincipal character with special properties modulo a prime ideal $\mathfrak{p}$ in K.

In the special case of a totally real algebraic number field K_0 the proof of Theorem 1 can be modified to give the following result which is sharper than (4) for $N\mathfrak{q} \leqslant P$:

THEOREM 2. *Let χ_0 denote the principal character* mod $\mathfrak{q}$. *For $N\mathfrak{q} \leqslant P$ and $a > 0$ we have*

$$\sum_{\alpha \in \mathfrak{R}} \chi(\alpha) = \frac{E_0(\chi)}{|\sqrt{d}|} \frac{\Phi(\mathfrak{q})}{N\mathfrak{q}} P + O\{(N\mathfrak{q})^{1-(1/2(n+1))} P^a\}, \tag{5}$$

where

$$\begin{aligned} E_0(\chi) &= 1, \qquad \text{if } \chi = \chi_0, \\ &= 0, \qquad \text{if } \chi \neq \chi_0. \end{aligned}$$

The O-constant depends on a and the field K_0.

This estimate should be compared with a result of Lee [12], who proved for real quadratic number fields a version of Theorem 2 in which the remainder term in (5) is replaced by $O(N\mathfrak{q}^{1/2}P^a + N\mathfrak{q})$.

As an application of Theorem 1, in the form of the corollary, we extend a well-known result about the distribution of primitive roots to algebraic number fields. Consider the set $\mathfrak{S}_1 = \mathfrak{S}_1(\mathfrak{p})$ of all totally positive primitive roots modulo a prime ideal $\mathfrak{p}$ of K. Then the following result is shown:

THEOREM 3. *For $a > 0$ and $P > (N\mathfrak{p})^{(1/2)+a}$ we have*

$$\sum_{\alpha \in \mathfrak{R} \cap \mathfrak{S}_1} 1 = \frac{(2\pi)^{r_2}}{|\sqrt{d}|} \frac{\varphi(N\mathfrak{p}-1)}{N\mathfrak{p}-1} P\{1 + O((N\mathfrak{p})^{-b})\},$$

where b is a positive number depending on a and the degree n. In particular, it follows that a least primitive root $\nu \in \mathfrak{S}_1$, least in the sense that $N\nu$ is minimal, satisfies

$$N\nu \ll (N\mathfrak{p})^{(1/2)+a}. \tag{6}$$

Inequality (6) can be considered as an extension of (2) to algebraic number fields. For the smallest positive integer in the set $\{|N\gamma|$; γ a primitive root mod $\mathfrak{p}$ in $K\}$, where K is a quadratic field, estimate (6) has already been obtained by Friedlander [6].

A second application is to the problem of the distribution of quadratic nonresidues modulo a prime ideal $\mathfrak{p}$ in K. Let $\mathfrak{S}_2 = \mathfrak{S}_2(\mathfrak{p})$ denote the set of all totally positive quadratic nonresidues mod $\mathfrak{p}$. An immediate consequence of Theorem 1 shows that for $a > 0$ and $P > (N\mathfrak{p})^{(1/2)+a}$

$$\sum_{\alpha \in \mathfrak{R} \cap \mathfrak{S}_2} 1 = \frac{1}{2} \frac{(2\pi)^{r_2}}{|\sqrt{d}|} P\{1 + O((N\mathfrak{p})^{-b})\} \tag{7}$$

holds.

In this connection Friedlander's paper [5] should be mentioned. Friedlander proves in algebraic number fields remarkable upper bounds for the least positive integer in the set $\{|N\alpha|$; $\alpha \in Z_K$, α is a kth power nonresidue mod $\mathfrak{p}\}$.

2. SIEGEL'S FORMULA

Let $\mathfrak{q}$ be an integral ideal of K, $r = r_1 + r_2 - 1$, $\eta_1,\ldots,\eta_r$ the totally positive fundamental units mod $\mathfrak{q}$, i.e., with $\eta_l \equiv 1 \bmod \mathfrak{q}$ $(l = 1,\ldots,r)$, w_0 the number of roots of unity in K, $w(\mathfrak{q})$ the number of the totally positive roots of unity which are congruent to 1 mod $\mathfrak{q}$. Consider now the matrix

$$M(\mathfrak{q}) = \begin{pmatrix} \frac{1}{n} & \log|\eta_1^{(1)}| & \cdots & \log|\eta_r^{(1)}| \\ \vdots & \vdots & & \vdots \\ \frac{1}{n} & \log|\eta_1^{(r+1)}| & \cdots & \log|\eta_r^{(r+1)}| \end{pmatrix}$$

and the inverse matrix of $M(\mathfrak{q})$:

$$M(\mathfrak{q})^{-1} = \begin{pmatrix} e_1 & e_2 & \cdots & e_{r+1} \\ e_1^{(1)} & e_2^{(1)} & \cdots & e_{r+1}^{(1)} \\ \vdots & \vdots & & \vdots \\ e_1^{(r)} & e_2^{(r)} & \cdots & e_{r+1}^{(r)} \end{pmatrix}.$$

Then a Grössencharacter λ modulo $\mathfrak{q}$ for ideal numbers $\hat{\gamma}$ is defined as

$$\lambda(\hat{\gamma}) = \prod_{k=1}^{r+1} |\hat{\gamma}^{(k)}|^{2\pi i \cdot \sum_{q=1}^{r} m_q e_k^{(q)}},$$

where $m_1, \ldots, m_r$ are rational integers. These characters were introduced by Hecke in 1920. For more details on ideal numbers and Grössencharacters, see Hecke [8] and Rademacher [15].

If η is a totally positive unit mod $\mathfrak{q}$ it follows from the definition of the numbers $e_k^{(q)}$ that $\lambda(\eta\hat{\gamma}) = \lambda(\hat{\gamma})$.

Let χ be a character of the group of reduced residue classes modulo $\mathfrak{q}$. By $\mathfrak{a} = (\hat{\alpha}_0)$ we denote an integral ideal of K with $(\mathfrak{a}, \mathfrak{q}) = 1$ which will be kept fixed throughout this section. We put

$$\begin{aligned} f(\gamma) &= \chi(\gamma), && \text{if} \quad \gamma \equiv 0 \bmod \mathfrak{a}, \\ &= 0, && \text{otherwise}, \end{aligned} \tag{8}$$

and define the function

$$\Xi(s, \lambda\chi) = \sum_{\gamma \succ 0}{}^{*} \frac{\lambda(\gamma) f(\gamma)}{(N\gamma)^s}, \qquad s = \sigma + it, \quad \sigma > 1,$$

where $\sum^*$ indicates that the sum is to be taken over a set of totally positive ($\succ 0$) numbers $\gamma \in Z_K$ which are not associated mod $\mathfrak{q}$.

We are now in a position to introduce an identity given by Siegel in [19] for real quadratic number fields. This summation formula has been generalized by Grotz [7] to arbitrary algebraic number fields. We use here a simple extension of this identity.

LEMMA 1. *Let* $S(P_1,\ldots,P_{r+1}) = \sum_{\alpha\in\mathfrak{R}} f(\alpha)$ *and let*

$$E_k(m) = E_k(m_1,\ldots,m_r) = \frac{2\pi}{e_k} \sum_{q=1}^{r} m_q e_k^{(q)}, \qquad k = 1,\ldots, r+1.$$

Then we have for $\sigma > 1$ *and for positive real numbers* $Q_1,\ldots,Q_{r+1}$

$$\int_0^{Q_1} \cdots \int_0^{Q_{r+1}} S(P_1 + x_1,\ldots, P_{r+1} + x_{r+1})\, dx_1 \cdots dx_{r+1}$$

$$= \frac{w(\mathfrak{q})}{2\pi i R(\mathfrak{q})} \sum_{m_1,\ldots,m_r=-\infty}^{\infty} \int_{\sigma - i\infty}^{\sigma + i\infty} \Xi(s, \lambda\chi)$$

$$\times \prod_{k=1}^{r+1} \frac{(P_k + Q_k)^{s+1-iE_k(m)} - P_k^{s+1-iE_k(m)}}{(s - iE_k(m))(s + 1 - iE_k(m))}\, ds,$$

where $R(\mathfrak{q})$ *is the absolute value of the determinant*

$$\begin{vmatrix} \log|\eta_1^{(1)}| & \cdots & \log|\eta_r^{(1)}| \\ \vdots & & \vdots \\ \log|\eta_1^{(r)}| & \cdots & \log|\eta_r^{(r)}| \end{vmatrix}.$$

It is easy to investigate the function $\Xi(s, \lambda\chi)$ by reducing it to Hecke's well-known zeta-functions. For this purpose we divide the ideal numbers prime to $\mathfrak{q}$ into classes under the stipulation that $\hat{\alpha}$ and $\hat{\beta}$ with $(\hat{\alpha}, \mathfrak{q}) = (\hat{\beta}, \mathfrak{q}) = 1$ belong to the same class if and only if

$$\hat{\alpha} \equiv \hat{\beta} \bmod \mathfrak{q}, \frac{\hat{\alpha}}{\hat{\beta}} \text{ totally positive.}$$

These classes form a group $G(\mathfrak{q})$ of order $2^{r_1} h \Phi(\mathfrak{q})$, where h denotes the ordinary class number of K. In this context the given character χ is defined only for a subgroup of $G(\mathfrak{q})$. But according to a general property of characters of finite Abelian groups it is always possible to extend a character given on a subgroup to the total enclosing group.

Let ψ be a character of $G(1)$. The unit element of this group is the class of all totally positive algebraic numbers of the field K. Hence we have

$$\Xi(s, \lambda\chi) = \frac{1}{2^{r_1} h} \sum_{\psi} \sum_{\hat{\gamma}}{}^{*} \frac{\lambda(\hat{\gamma}) f(\hat{\gamma})\, \psi(\hat{\gamma})}{|N\hat{\gamma}|^s}, \qquad \sigma > 1,$$

where $\sum^*$ means again that out of each set of ideal numbers associated $\bmod\, \mathfrak{q}$ we have only to take one representative.

If we select only nonassociated numbers in the ordinary sense, we must consider units ε which are not associated mod $\mathfrak{q}$

$$\Xi(s, \lambda\chi) = \frac{1}{2^{r_1}h} \sum_{\psi} \sum_{\substack{(\hat{\gamma}) \\ \hat{\alpha}_0/\hat{\gamma}}} \frac{\lambda(\hat{\gamma})\,\chi(\hat{\gamma})\,\psi(\hat{\gamma})}{|N\hat{\gamma}|^s} \sum_{\varepsilon}{}^{*}\, \lambda(\varepsilon)\,\chi(\varepsilon)\,\psi(\varepsilon).$$

The units not associated mod $\mathfrak{q}$ form a group of order $w_0R(\mathfrak{q})/w(\mathfrak{q})R$, where R is the regulator of K. Obviously $\lambda\chi\psi$ is a character of this group of units. We see that

$$\begin{aligned} &\sum_{\varepsilon}{}^{*}\, \lambda(\varepsilon)\,\chi(\varepsilon)\,\psi(\varepsilon) \\ &\qquad = \frac{w_0R(\mathfrak{q})}{w(\mathfrak{q})R}, \qquad \text{if } \lambda(\varepsilon)\,\chi(\varepsilon)\,\psi(\varepsilon) = 1 \text{ for all units } \varepsilon, \\ &\qquad = 0, \qquad\qquad\quad \text{otherwise.} \end{aligned}$$

If $\lambda(\varepsilon)\,\chi(\varepsilon)\,\psi(\varepsilon) = 1$ for every unit ε of K, then $\lambda\chi\psi$ is called a Grössencharacter for ideals modulo $\mathfrak{q}$ and the abbreviated symbol $\lambda\chi\psi(\hat{\gamma})$ is used. In fact this character has the same value for all $\hat{\gamma}$ representing the same ideal. Therefore, we can introduce Hecke's zeta-function

$$\zeta(s, \lambda\chi\psi) = \sum_{(\hat{\gamma})} \frac{\lambda\chi\psi(\hat{\gamma})}{|N\hat{\gamma}|^s}, \qquad \operatorname{Re} s > 1,$$

where the sum runs over a set of nonassociated ideal numbers. Using (8), we obtain

$$\Xi(s, \lambda\chi) = \frac{1}{2^{r_1}h}\,\frac{w_0R(\mathfrak{q})}{w(\mathfrak{q})R} \sum_{\psi} \lambda\chi\psi(\hat{\alpha}_0)(N\mathfrak{a})^{-s}\zeta(s, \lambda\chi\psi).$$

In these circumstances Lemma 1 can be brought into the form

$$\begin{aligned} &\int_0^{Q_1} \cdots \int_0^{Q_{r+1}} S(P_1 + x_1, \ldots, P_{r+1} + x_{r+1})\, dx_1 \cdots dx_{r+1} \\ &\quad = \frac{1}{2\pi i}\,\frac{w_0}{2^{r_1}hR} \sum_{\psi} \sum_{m_1, \ldots, m_r = -\infty}^{\infty}{}' \lambda\chi\psi(\hat{\alpha}_0) \\ &\quad \times \int_{\sigma - i\infty}^{\sigma + i\infty} (N\mathfrak{a})^{-s}\zeta(s, \lambda\chi\psi) \\ &\quad \times \prod_{k=1}^{r+1} \frac{(P_k + Q_k)^{s+1-iE_k(m)} - P_k^{s+1-iE_k(m)}}{(s - iE_k(m))(s + 1 - iE_k(m))}\, ds, \end{aligned} \tag{9}$$

where the dash indicates that the sum runs only over such numbers $m_1, \ldots, m_r$ which determine a Grössencharacter for ideals.

For the estimate of $\zeta(s, \lambda\chi\psi)$ we shall make use of the following application of a Phragmén–Lindelöf theorem:

LEMMA 2. *Let $\lambda\chi\psi$ be a primitive Grössencharacter for ideals modulo* $\mathfrak{q}$, $\mathfrak{q} \neq (1)$. *Then we have for $-\delta \leqslant \sigma = \operatorname{Re} s \leqslant 1 + \delta$, $0 < \delta \leqslant \frac{1}{2}$*

$$\zeta(s, \lambda\chi\psi) \ll N\mathfrak{q}^{(1+\delta-\sigma)/2} \prod_{k=1}^{r+1} |1 + s - iE_k(m)|^{e_k(1+\delta-\sigma)/2}, \tag{10}$$

the $\ll$-constant depending on δ and the field K. Estimate (10) *is also true for* $\mathfrak{q} = (1)$ *if $\lambda \neq 1$ or if $\lambda = 1$ but* $|\operatorname{Im} s| \geqslant t_0 > 0$.

Proof. The calculations which lead to (10) are given in [16, Sect. 8].

By means of this lemma we are now in a position to investigate the right-hand side of (9). We deduce the following result:

LEMMA 3. *Let χ be a primitive character* mod $\mathfrak{q}$. *For positive real numbers $Q_1, \ldots, Q_{r+1}$ and for $0 < a \leqslant \frac{1}{2}$ we have*

$$\begin{aligned} J &:= \int_0^{Q_1} \cdots \int_0^{Q_{r+1}} S(P_1 + x_1, \ldots, P_{r+1} + x_{r+1})\, dx_1 \cdots dx_{r+1} \\ &= E_0(\mathfrak{q}) \frac{\pi^{r_2}}{2^{r_1}|\sqrt{d}|} \frac{1}{N\mathfrak{a}} \prod_{k=1}^{r+1} \{(P_k + Q_k)^2 - P_k^2\} \\ &\quad + O\left\{ N\mathfrak{q}^{1/2} \cdot \prod_{k=1}^{r+1} (P_k + Q_k)^{1+a} \right\}, \end{aligned}$$

where $E_0(\mathfrak{q}) = 1$ if $\mathfrak{q} = (1)$ *and* $E_0(\mathfrak{q}) = 0$ *if* $\mathfrak{q} \neq (1)$. *The constant implied by the O-notation depends on a and K.*

Proof. It is easily seen that $\lambda\chi\psi$ is a primitive Grössencharacter mod $\mathfrak{q}$. Now the path of integration in (9) is shifted to the left up to the abscissa $\sigma = a$, $0 < a \leqslant \frac{1}{2}$. Considering for $\mathfrak{q} = (1)$ and $\lambda = 1$ the simple pole of the integrand at $s = 1$ with the residue [9, Satz LXI]

$$\frac{1}{N\mathfrak{a}} \frac{2^{r_1+r_2}\pi^{r_2}hR}{w_0|\sqrt{d}|} \prod_{k=1}^{r+1} \frac{(P_k + Q_k)^2 - P_k^2}{2}$$

we find that

$$J = \frac{E_0(\mathfrak{q})}{N\mathfrak{a}} \frac{\pi^{r_2}}{2^{r_1}|\sqrt{d}|} \prod_{k=1}^{r+1} \{(P_k+Q_k)^2 - P_k^2\}$$
$$+ \frac{1}{2\pi i} \frac{w_0}{2^{r_1} hR} \sum_{\psi} \sum_{m_1,\dots,m_r=-\infty}^{\infty}{}' \lambda\chi\psi(\hat{\alpha}_0)$$
$$\times \int_{a-i\infty}^{a+i\infty} (N\mathfrak{a})^{-s} \zeta(s, \lambda\chi\psi)$$
$$\times \prod_{k=1}^{r+1} \frac{(P_k+Q_k)^{s+1-iE_k(m)} - P_k^{s+1-iE_k(m)}}{(s-iE_k(m))(s+1-iE_k(m))} \, ds.$$

Now, the infinite sums over $m_1,\dots, m_r$ have to be estimated. For this purpose we introduce a formula for $E_k(m)$ [15, p. 347] valid only if $m_1, \dots, m_r$ determine a Grössencharacter for ideals

$$E_k(m) = E_k'(m') := \frac{2\pi}{e_k} \sum_{q=1}^{r} f_k^{(q)}(m_q' + z_q), \quad z_q \in \mathbb{Q}, \; k = 1,\dots, r+1,$$

where

$$\begin{pmatrix} e_1 & e_2 & \cdots & e_{r+1} \\ f_1^{(1)} & f_2^{(1)} & \cdots & f_{r+1}^{(1)} \\ \vdots & \vdots & & \vdots \\ f_1^{(r)} & f_2^{(r)} & \cdots & f_{r+1}^{(r)} \end{pmatrix}$$
$$= \begin{pmatrix} \frac{1}{n} & \log|\varepsilon_1^{(1)}| & \cdots & \log|\varepsilon_r^{(1)}| \\ \vdots & \vdots & & \vdots \\ \frac{1}{n} & \log|\varepsilon_1^{(r+1)}| & \cdots & \log|\varepsilon_r^{(r+1)}| \end{pmatrix}^{-1}.$$

The numbers $\varepsilon_1,\dots, \varepsilon_r$ denote the totally positive fundamental units mod (1).

Changing the variables of summation from $m_1,\dots, m_r$ to $m_1',\dots, m_r'$, we find that Lemma 2 leads at once to

$$\sum_{m_1,\dots,m_r=-\infty}^{\infty}{}' \lambda\chi\psi(\hat{\alpha}_0) \int_{a-i\infty}^{a+i\infty} (N\mathfrak{a})^{-s} \zeta(s, \lambda\chi\psi)$$
$$\times \prod_{k=1}^{r+1} \frac{(P_k+Q_k)^{s+1-iE_k(m)} - P_k^{s+1-iE_k(m)}}{(s-iE_k(m))(s+1-iE_k(m))} \, ds$$

$$\ll N\mathrm{q}^{1/2} \prod_{k=1}^{r+1} (P_k+Q_k)^{1+a}$$

$$\times \left(1 + \sum_{\substack{m'_1,\ldots,m'_r=-\infty \\ \lambda \neq 1}}^{\infty} \int_{-\infty}^{\infty} \prod_{k=1}^{r+1} |a+it-iE'_k(m')|^{-1-a/2}\, dt\right). \tag{11}$$

To complete the proof of Lemma 3 it only remains to obtain an appropriate estimate for the term in parentheses on the right of (11). Putting $u=t-E'_{r+1}(m')$, the sums over $m'_1,\ldots, m'_r$ are less than

$$\sum_{m'_1,\ldots,m'_r=-\infty}^{\infty} \int_{-\infty}^{\infty} \prod_{k=1}^{r} |a+iu-i(E'_k(m')-E'_{r+1}(m'))|^{-1-(a/2)}$$
$$\times \frac{du}{|a+iu|^{1+(a/2)}}.$$

This expression can be estimated if one observes that the determinant does not vanish

$$\begin{vmatrix} \dfrac{f_1^{(1)}}{e_1}-\dfrac{f_{r+1}^{(1)}}{e_{r+1}} & \cdots & \dfrac{f_1^{(r)}}{e_1}-\dfrac{f_{r+1}^{(r)}}{e_{r+1}} \\ \vdots & & \vdots \\ \dfrac{f_r^{(1)}}{e_r}-\dfrac{f_{r+1}^{(1)}}{e_{r+1}} & \cdots & \dfrac{f_r^{(r)}}{e_r}-\dfrac{f_{r+1}^{(r)}}{e_{r+1}} \end{vmatrix} = \pm\frac{1}{R(1)}.$$

Thus, the vectors

$$2\pi\left(\frac{f_1^{(1)}}{e_1}-\frac{f_{r+1}^{(1)}}{e_{r+1}},\ldots,\frac{f_r^{(1)}}{e_r}-\frac{f_{r+1}^{(1)}}{e_{r+1}}\right),\ldots,\ 2\pi\left(\frac{f_1^{(r)}}{e_1}-\frac{f_{r+1}^{(r)}}{e_{r+1}},\ldots,\frac{f_r^{(r)}}{e_r}-\frac{f_{r+1}^{(r)}}{e_{r+1}}\right)$$

generate an r-dimensional lattice, depending only on the field K. In view of

$$u-(E'_k(m')-E'_{r+1}(m'))$$
$$=u-2\pi\sum_{q=1}^{r}\left(\frac{f_k^{(q)}}{e_k}-\frac{f_{r+1}^{(q)}}{e_{r+1}}\right)(m'_q+z_q), \qquad k=1,\ldots,r,$$

we have

$$\sum_{m'_1,\ldots,m'_r=-\infty}^{\infty} \int_{-\infty}^{\infty} \prod_{k=1}^{r} |a+iu-i(E'_k(m')-E'_{r+1}(m'))|^{-1-(a/2)}$$
$$\times \frac{du}{|a+iu|^{1+(a/2)}}$$
$$\ll \sum_{l_1,\ldots,l_r=0}^{\infty} \prod_{k=1}^{r} |a+il_k|^{-1-(a/2)} \int_{-\infty}^{\infty} \frac{du}{|a+iu|^{1+(a/2)}} \ll 1$$

and this completes the proof of Lemma 3.

3. Proof of Theorem 1

If $\mathfrak{a} \geqslant \frac{1}{2}$ or $P^2 \leqslant N\mathfrak{q}$ the statement is true in view of the trivial estimate

$$\sideset{}{'}\sum_{\alpha \in \mathfrak{R}} \chi(\alpha) \ll \sideset{}{'}\sum_{\alpha \in \mathfrak{R}} 1 \ll P, \tag{12}$$

so that we may assume that $0 < \mathfrak{a} \leqslant \frac{1}{2}$ and $N\mathfrak{q} \leqslant P^2$. It is convenient to assume for the computations that

$$c_1 P^{1/(r+1)} \leqslant P_k \leqslant c_2 P^{1/(r+1)}, \qquad k = 1,\dots, r+1, \tag{13}$$

where the positive constants c_1, c_2 depend on the field K only. If the P_k do not satisfy inequalities (13) one can restore (13) by multiplying the P_k by a suitably chosen totally positive unit $\varepsilon \in K$ (cf. [18, Hilfssatz 6]):

Let $y_1,\dots, y_{r+1}$ be real numbers determined by the simultaneous equations

$$\begin{aligned} &y_1 \log |\rho_1^{(k)}| + \cdots + y_r \log |\rho_r^{(k)}| \\ &\quad = \frac{1}{e_k} \log(P_k P^{-1/(r+1)}), \qquad k = 1,\dots, r+1, \end{aligned}$$

where $\rho_1,\dots, \rho_r$ are fundamental units of K. Setting

$$\varepsilon = \rho_1^{-2m_1} \cdots \rho_r^{-2m_r}, \qquad m_i = \left[\frac{y_i}{2}\right], \qquad i = 1,\dots, r,$$

we obtain

$$P^{1/(r+1)} \ll |\varepsilon^{(k)}|^{e_k} P_k \ll P^{1/(r+1)}, \qquad k = 1,\dots, r+1.$$

Let χ be first a primitive nonprincipal character mod $\mathfrak{q}$. We observe that Lemma 3 gives an estimate for

$$\int_0^{Q_1} \cdots \int_0^{Q_{r+1}} \Bigg(\sum_{\substack{\alpha \succ 0 \\ 0 < |\alpha^{(k)}|^{e_k} \leqslant P_k + x_k}} f(\alpha) \Bigg)\, dx_1 \cdots dx_{r+1},$$

where the index k always takes on the values $1,\dots, r+1$. From this result we deduce an upper bound for the sum $\sum_{\alpha \in \mathfrak{R}, \alpha \equiv 0 \bmod \mathfrak{a}} \chi(\alpha)$. We begin with the remark that

$$\Bigg| \sum_{\substack{\alpha > 0 \\ 0 < |\alpha^{(k)}|^{e_k} \leqslant P_k + x_k}} f(\alpha) - \sum_{\substack{\alpha > 0 \\ 0 < |\alpha^{(k)}|^{e_k} \leqslant P_k}} f(\alpha) \Bigg|$$

$$\leqslant \sum_{\substack{\alpha > 0 \\ 0 < |\alpha^{(k)}|^{e_k} \leqslant P_k + x_k}} 1 - \sum_{\substack{\alpha > 0 \\ 0 < |\alpha^{(k)}|^{e_k} \leqslant P_k}} 1$$

$$= \frac{(2\pi)^{r_2}}{|\sqrt{d}|} \left\{ \prod_{k=1}^{r+1} (P_k + x_k) - \prod_{k=1}^{r+1} P_k \right\} + O \left\{ \prod_{k=1}^{r+1} (P_k + x_k)^{1 - (1/(r+2)) + a} \right\},$$

using at the last step a result of Grotz [7, Korollar 3]. If we now combine this inequality with Lemma 3 we see that

$$\sum_{\substack{\alpha \in \mathfrak{N} \\ \alpha \equiv 0 \bmod \mathfrak{a}}} \chi(\alpha) \ll \prod_{k=1}^{r+1} (P_k + Q_k) - P + \prod_{k=1}^{r+1} (P_k + Q_k)^{1 - (1/(r+2)) + a}$$

$$+ \frac{N\mathfrak{q}^{1/2}}{Q_1 \cdots Q_{r+1}} \prod_{k=1}^{r+1} (P_k + Q_k)^{1+a}$$

$$= P \prod_{k=1}^{r+1} \left(1 + \frac{Q_k}{P_k}\right) - P + \prod_{k=1}^{r+1} (P_k + Q_k)^{1 - (1/(r+2)) + a}$$

$$+ N\mathfrak{q}^{1/2} \prod_{k=1}^{r+1} (P_k + Q_k)^a \prod_{k=1}^{r+1} \left(1 + \frac{P_k}{Q_k}\right). \tag{14}$$

Taking

$$Q_k = N\mathfrak{q}^{1/2(r+2)} \cdot P_k^{1/(r+2)}, \qquad k = 1, \ldots, r+1,$$

we find, by (13), that

$$\frac{Q_k}{P_k} \ll N\mathfrak{q}^{1/2(r+2)} \cdot P^{-1/(r+2)} \leqslant 1, \qquad k = 1, \ldots, r+1,$$

holds for $N\mathfrak{q} \leqslant P^2$. Accordingly (14), with the above choice of the parameters, leads to the estimate

$$\sum_{\substack{\alpha \in \mathfrak{N} \\ \alpha \equiv 0 \bmod \mathfrak{a}}} \chi(\alpha) \ll N\mathfrak{q}^{1/2(r+2)} P^{1 - (1/(r+2)) + a}. \tag{15}$$

The special case $\mathfrak{a} = (1)$ gives the stated result (4) for a primitive nonprincipal character.

Finally, we remark that (4) holds for any nonprincipal character χ, whether primitive or not. Suppose χ is imprimitive and is induced by the primitive character $\chi_1 \bmod \mathfrak{q}_1$, $\mathfrak{q}_1/\mathfrak{q}$. Then we have

$$\sum_{\alpha \in \mathfrak{N}} \chi(\alpha) = \sum_{\substack{\alpha \in \mathfrak{N} \\ (\alpha, \mathfrak{q}) = 1}} \chi_1(\alpha) = \sum_{\substack{\mathfrak{a}/\mathfrak{q} \\ (\mathfrak{a}, \mathfrak{q}_1) = 1}} \mu(\mathfrak{a}) \sum_{\substack{\alpha \in \mathfrak{N} \\ \alpha \equiv 0 \bmod \mathfrak{a}}} \chi_1(\alpha).$$

The result now follows from (15) and the estimate

$$\sum_{\mathfrak{a}/\mathfrak{c}} 1 \ll_\delta (N\mathfrak{c})^\delta, \qquad \delta > 0.$$

Proof of Corollary. From Theorem 1, we have for any positive number a_1,

$$\sum_{\alpha \in \mathfrak{R}} \chi(\alpha) \ll N\mathfrak{q}^{1/2(r+2)} P^{1-(1/(r+2))+a_1}.$$

We now choose

$$a_1 = \frac{a}{(r+2)(2+4a)}.$$

Then $P > N\mathfrak{q}^{(1/2)+a}$ implies that for all sufficiently large $N\mathfrak{q}$

$$\left| \sum_{\alpha \in \mathfrak{R}} \chi(\alpha) \right| \leqslant c(a_1, K)\, PN\mathfrak{q}^{-(a/(r+2))+a_1(1+2a)/2} < P(N\mathfrak{q})^{-b},$$

where $b = a/2(r+2)$.

4. Proof of Theorem 2

We shall devote this section to the proof of Theorem 2. Here we are concerned with the case of a totally real algebraic number field of degree $n = r+1$ and discriminant d. Let χ be a primitive character mod $\mathfrak{q}$. Then Lemma 3 yields, for $0 < a \leqslant 1$,

$$\begin{aligned} &\int_0^{Q_1} \cdots \int_0^{Q_n} \Biggl(\sum_{\substack{0 < \alpha^{(k)} \leqslant P_k + x_k \\ k=1,\ldots,n}} f(\alpha) \Biggr) dx_1 \cdots dx_n \\ &\quad = \frac{E_0(\mathfrak{q})}{N\mathfrak{a}} \frac{1}{2^n |\sqrt{d}|} \prod_{k=1}^{n} \{(P_k + Q_k)^2 - P_k^2\} \\ &\qquad + O\Biggl(N\mathfrak{q}^{1/2} \cdot \prod_{k=1}^{n} (P_k + Q_k)^{1+(a/2)} \Biggr). \end{aligned} \tag{16}$$

We shall need to make use of the following simple result:

Lemma 4. *With the above notation we obtain the identity*

$$\sum_{0 < \alpha^{(k)} \leqslant P_k + x_k} f(\alpha) = \sum_{P_k < \alpha^{(k)} \leqslant P_k + x_k} f(\alpha) + \sum_{m=1}^{n} \sum_{1 \leqslant j_1 < \cdots < j_m \leqslant n} \sum_{\alpha}{}_{*} f(\alpha),$$

where the index k always takes on the values $1,\ldots,n$. *The star at the sign of summation indicates that the sum runs over* $\alpha \in Z_K$ *subject to the conditions* $0 < \alpha^{(j_l)} \leqslant P_{j_l}$, $l = 1,\ldots,m$, $P_k < \alpha^{(k)} \leqslant P_k + x_k$, $k \neq j_1,\ldots,j_m$.

Proof. The identity can be easily derived by induction on $n \geqslant 1$. The proof is therefore omitted.

Proof of Theorem 2. We may assume immediately that $0 < a \leqslant 1$, since otherwise the theorem holds trivially in view of (12). The remarks about the P_k we made in (13) apply here also. Let χ be first a primitive character mod $\mathfrak{q}$. Suppose now that

$$\sum_{\substack{0<\alpha^{(k)}\leqslant P_k \\ \alpha\equiv 0 \bmod \mathfrak{a}}} \chi(\alpha) = \frac{E_0(\mathfrak{q})}{N\mathfrak{a}\,|\sqrt{d}\,|} P + O(N(\mathfrak{a}\mathfrak{q})^{q-(n/l)} P^{(n/l)+(a/2)}) \tag{17}$$

has already been proved for $N(\mathfrak{a}\mathfrak{q}) \leqslant P$, $\frac{1}{2} \leqslant q \leqslant 1$, $l \geqslant n$. We pause to study the sum

$$\sum_{u_k<\alpha^{(k)}\leqslant y_k+u_k} f(\alpha),$$

where $y_1,\ldots,y_n$ are positive, $u_1,\ldots,u_n$ arbitrary real numbers. We can choose a basis $\mu_1,\ldots,\mu_n$ of the ideal $\mathfrak{a}\mathfrak{q}$ (see, e.g., [14]) such that

$$|\mu_j^{(k)}| \ll N(\mathfrak{a}\mathfrak{q})^{1/n}, \qquad j,k = 1,\ldots,n. \tag{18}$$

Let $z_1,\ldots,z_n$ be real numbers determined by the simultaneous equations

$$z_1\mu_1^{(k)} + \cdots + z_n\mu_n^{(k)} = u_k, \qquad k = 1,\ldots,n.$$

Setting $\beta_1 = [z_1]\mu_1 + \cdots + [z_n]\mu_n$, we obtain

$$\beta_1 \in \mathfrak{a}\mathfrak{q}, \qquad |u_k - \beta_1^{(k)}| \leqslant \sum_{j=1}^{n} |\mu_j^{(k)}|, \qquad k = 1,\ldots,n. \tag{19}$$

It is easily seen—the problem can be interpreted as a lattice point problem in an n-dimensional space—that there exists a $\beta_2 \in \mathfrak{a}\mathfrak{q}$ such that

$$2\sum_{j=1}^{n} |\mu_j^{(k)}| \leqslant \beta_2^{(k)} \leqslant 3\sum_{j=1}^{n} |\mu_j^{(k)}|, \qquad k = 1,\ldots,n. \tag{20}$$

Since $f(\alpha) = f(\beta)$ if $\alpha \equiv \beta \bmod \mathfrak{a}\mathfrak{q}$, we have

$$\sum_{u_k<\alpha^{(k)}\leqslant y_k+u_k} f(\alpha) = \sum_{v_k<\beta^{(k)}\leqslant y_k+v_k} f(\beta),$$

where $v_k = \beta_2^{(k)} + u_k - \beta_1^{(k)}$, $k = 1,\ldots,n$.

Using (18)–(20), we find that $v = v_1 \cdots v_n$ satisfy the inequalities

$$v \geqslant \prod_{k=1}^{n} \sum_{j=1}^{n} |\mu_j^{(k)}| \geqslant |N\mu_1| \geqslant N(\mathfrak{aq}),$$

$$0 < v_k \leqslant 4 \sum_{j=1}^{n} |\mu_j^{(k)}| \leqslant cN(\mathfrak{aq})^{1/n}, \qquad k = 1,\dots, n.$$

Therefore we may apply (17) to obtain

$$\begin{aligned}
&\sum_{u_k < \alpha^{(k)} \leqslant y_k + u_k} f(\alpha) \\
&\quad= \sum_{v_k < \beta^{(k)} \leqslant y_k + v_k} f(\beta) \\
&\quad= \sum_{0 < \beta^{(k)} \leqslant y_k + v_k} f(\beta) + \sum_{m=1}^{n} (-1)^m \sum_{1 \leqslant j_1 < \cdots < j_m \leqslant n} \sum_{\substack{0 < \beta^{(j_l)} \leqslant v_{j_l} \\ 0 < \beta^{(k)} \leqslant y_k + v_k \\ k \neq j_1, \dots, j_m}} f(\beta) \\
&\quad= \frac{E_0(\mathfrak{q})}{N\mathfrak{a}\,|\sqrt{d}|} \left\{ \prod_{k=1}^{n} (y_k + v_k) + \prod_{k=1}^{n} (y_k + v_k - v_k) - \prod_{k=1}^{n} (y_k + v_k) \right\} \\
&\qquad + O\left\{ N(\mathfrak{aq})^{q-(n/l)} \cdot \prod_{k=1}^{n} (y_k + v_k)^{(n/l)+(a/2)} \right\} \\
&\quad= \frac{E_0(\mathfrak{q})}{N\mathfrak{a} \cdot |\sqrt{d}|} \prod_{k=1}^{n} y_k + O\left\{ N(\mathfrak{aq})^{q-(n/l)} \right. \\
&\qquad \left. \cdot \prod_{k=1}^{n} (y_k + cN(\mathfrak{aq})^{1/n})^{(n/l)+(a/2)} \right\}. \qquad (21)
\end{aligned}$$

We are now in a position to show that if (17) holds for l, then it also holds for $l+1$ in place of l.

As in the proof of Theorem 1 we take as our starting point identity (16). For the sum on the left of (16) we use Lemma 4, and we obtain for $N(\mathfrak{aq}) \leqslant P$, in conjunction with (21),

$$\begin{aligned}
&\sum_{\substack{0 < \alpha^{(k)} \leqslant P_k \\ \alpha \equiv 0 \bmod \mathfrak{a}}} \chi(\alpha) = \frac{E_0(\mathfrak{q})}{N\mathfrak{a} \cdot |\sqrt{d}|} \\
&\quad \times \left\{ \prod_{k=1}^{n} \left(P_k + \frac{Q_k}{2}\right) - \prod_{k=1}^{n} \frac{Q_k}{2} - \sum_{m=1}^{n-1} \sum_{1 \leqslant j_1 < \cdots < j_m \leqslant n} P_{j_1} \cdots P_{j_m} \prod_{\substack{k=1 \\ k \neq j_i}}^{n} \frac{Q_k}{2} \right\} \\
&\quad + O\left\{ N\mathfrak{q}^{1/2} \prod_{k=1}^{n} \left(1 + \frac{P_k}{Q_k}\right) \prod_{k=1}^{n} (P_k + Q_k)^{a/2} \right\}
\end{aligned}$$

$$+ O\left\{N(\mathfrak{aq})^{q-(n/l)} \prod_{k=1}^{n} (Q_k + cN(\mathfrak{aq})^{1/n})^{(n/l)+a/2}\right\}$$
$$+ O\left\{N(\mathfrak{aq})^{q-(n/l)} \sum_{m=1}^{n-1} \sum_{1\leqslant j_1<\cdots<j_m\leqslant n} (P_{j_1}\cdots P_{j_m})^{(n/l)+(a/2)}\right.$$
$$\left.\times \prod_{\substack{k=1\\ k\neq j_i}}^{n} (Q_k + cN(\mathfrak{aq})^{1/n})^{(n/l)+(a/2)}\right\}.$$

We now choose

$$Q_k = N(\mathfrak{aq})^{1/(l+1)} P_k P^{-1/(l+1)}, \qquad k = 1,\ldots, n.$$

Since $N(\mathfrak{aq}) \leqslant P$, we have then

$$\sum_{\substack{0<\alpha^{(k)}\leqslant P_k\\ \alpha\equiv 0 \bmod \mathfrak{a}}} \chi(\alpha) = \frac{E_0(\mathfrak{q})}{N\mathfrak{a}\cdot|\sqrt{d}|} P + O\{N(\mathfrak{aq})^{(1/2)-(n/(l+1))} P^{(n/(l+1))+(a/2)}\}$$
$$+ O\left\{N(\mathfrak{aq})^{q-(n/l)} P^{a/2} \prod_{k=1}^{n} Q_k^{n/l}\right\}$$
$$+ O\left\{N(\mathfrak{aq})^{q-(n/l)} P^{(n/l)+(a/2)} \sum_{m=1}^{n-1} \left(\frac{N(\mathfrak{aq})}{P}\right)^{((n-m)/(l+1))(n/l)}\right\}$$
$$= \frac{E_0(\mathfrak{q})}{N\mathfrak{a}\cdot|\sqrt{d}|} P + O\{N(\mathfrak{aq})^{q-(n/(l+1))} P^{(n/(l+1))+(a/2)}\}.$$

Finally, we note by reference to (15) and the estimate (cf. [17])

$$\sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \bmod \mathfrak{a}}} 1 = \frac{(2\pi)^{r_2}}{N\mathfrak{a}\,|\sqrt{d}|} P + O\left(\left(\frac{P}{N\mathfrak{a}}\right)^{1-(1/n)} + 1\right) \tag{22}$$

that (17) is true if we take

$$l = n+1, \qquad q = 1 - \frac{1}{2(n+1)}.$$

To complete the proof of Theorem 2 for a primitive character $\chi \bmod \mathfrak{q}$ we can use induction with respect to $l \geqslant n+1$. We arrive at

$$\sum_{\substack{0<\alpha^{(k)}\leqslant P_k\\ \alpha\equiv 0 \bmod \mathfrak{a}}} \chi(\alpha) = \frac{E_0(\mathfrak{q})}{N\mathfrak{a}\,|\sqrt{d}|} P + O\{N(\mathfrak{aq})^{1-(1/2(n+1))} P^{a}\}, \tag{23}$$

provided that $N(\mathfrak{aq}) \leqslant P$.

It only remains to deal with the case when the given‘ character is imprimitive. Each character χ mod $\mathfrak{q}$ is induced by a primitive character χ_1 to a modulus $\mathfrak{q}_1$ which divides $\mathfrak{q}$. We have

$$\chi(\alpha)=\chi_1(\alpha) \qquad \text{whenever } (\alpha, \mathfrak{q})=1.$$

Hence,

$$\sum_{\alpha\in\mathfrak{R}} \chi(\alpha)= \sum_{\substack{\alpha\in\mathfrak{R}\\ (\alpha,\mathfrak{q})=1}} \chi_1(\alpha)= \sum_{\substack{\mathfrak{a}/\mathfrak{q}\\ (\mathfrak{a},\mathfrak{q}_1)=1}} \mu(\mathfrak{a}) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \bmod \mathfrak{a}}} \chi_1(\alpha),$$

and accordingly for $N\mathfrak{q}\leqslant P$, by (23),

$$\sum_{\alpha\in\mathfrak{R}} \chi(\alpha)=\frac{E_0(\mathfrak{q}_1)}{|\sqrt{d}|} P \sum_{\mathfrak{a}/\mathfrak{q}} \frac{\mu(\mathfrak{a})}{N\mathfrak{a}} + O\left\{P^{a/2} \sum_{\mathfrak{a}/\frac{\mathfrak{q}}{\mathfrak{q}_1}} N(\mathfrak{a}\mathfrak{q}_1)^{1-(1/2(n+1))}\right\}$$

$$=\frac{E_0(\chi)}{|\sqrt{d}|}\frac{\Phi(\mathfrak{q})}{N\mathfrak{q}} P + O\{(N\mathfrak{q})^{1-(1/2(n+1))}P^{a}\}.$$

5. Applications

Our first application of Theorem 1, in the form of the corollary, is to the problem of investigating the distribution of primitive roots in an algebraic number field. We follow the argument used by Burgess in [1, Sect. 6].

Let $\mathfrak{S}_1=\mathfrak{S}_1(\mathfrak{p})$ denote the set of all totally positive primitive roots modulo a prime ideal $\mathfrak{p}$ of K. To prove Theorem 3 the following result will be required:

Lemma 5. *Let*

$$g(\alpha)=\frac{\varphi(N\mathfrak{p}-1)}{N\mathfrak{p}-1}\left\{1+\sum_{\substack{m/N\mathfrak{p}-1\\ m>1}} \frac{\mu(m)}{\varphi(m)} \sum_{\chi_{(m)}} \chi_{(m)}(\alpha)\right\},$$

the inner sum being over all characters $\chi_{(m)}$ mod $\mathfrak{p}$ *of order m. Then for* $\alpha\not\equiv 0 \bmod \mathfrak{p}$

$$\begin{aligned} g(\alpha)&=1, &&\textit{if } \alpha \textit{ is a primitive root} \bmod \mathfrak{p},\\ &=0, &&\textit{otherwise.}\end{aligned}$$

Proof. The lemma is a simple extension of [1, Lemma 5] to algebraic number fields.

Proof of Theorem 3. We have by Lemma 5

$$\sum_{\alpha\in\mathfrak{R}\cap\mathfrak{S}_1} 1 = \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\not\equiv 0 \bmod \mathfrak{p}}} g(\alpha)$$

$$= \frac{\varphi(N\mathfrak{p}-1)}{N\mathfrak{p}-1}\left\{\sum_{\alpha\in\mathfrak{R}} 1 - \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \bmod \mathfrak{p}}} 1\right.$$

$$\left. + \sum_{\substack{m/N\mathfrak{p}-1\\ m>1}} \frac{\mu(m)}{\varphi(m)} \sum_{\chi_{(m)}} \sum_{\alpha\in\mathfrak{R}} \chi_{(m)}(\alpha)\right\}.$$

If we now suppose that $P > N\mathfrak{p}^{(1/2)+a}$, we obtain by the corollary and (22)

$$\sum_{\alpha\in\mathfrak{R}\cap\mathfrak{S}_1} 1 = \frac{\varphi(N\mathfrak{p}-1)}{N\mathfrak{p}-1}\left\{\frac{(2\pi)^{r_2}}{|\sqrt{d}|}P + O\left(P^{1-(1/n)} + \frac{P}{N\mathfrak{p}}\right)\right.$$

$$\left. + O\left(\sum_{\substack{m/N\mathfrak{p}-1\\ m>1}} \frac{1}{\varphi(m)} \sum_{\chi_{(m)}} P(N\mathfrak{p})^{-2b_1}\right)\right\}$$

$$= \frac{(2\pi)^{r_2}}{|\sqrt{d}|}\frac{\varphi(N\mathfrak{p}-1)}{N\mathfrak{p}-1} P\{1 + O((N\mathfrak{p})^{-b})\},$$

where $b = \min(1/2n, a/4(n+1))$.

We have made use of the fact that there are exactly $\varphi(m)$ characters $\chi_{(m)}$ of order m. This proves Theorem 3.

We add yet another application of Theorem 1 concerning the distribution of quadratic nonresidues modulo a prime ideal $\mathfrak{p}$ in K. Let $\mathfrak{S}_2 = \mathfrak{S}_2(\mathfrak{p})$ denote the set of all totally positive quadratic nonresidues mod $\mathfrak{p}$. It is easily verified that the Legendre symbol $(\alpha/\mathfrak{p})$ defines a character mod $\mathfrak{p}$. The values of α for which $(\alpha/\mathfrak{p}) = -1$ are precisely those for which there exist no solutions of $x^2 \equiv \alpha$ mod $\mathfrak{p}$. We have

$$\sum_{\alpha\in\mathfrak{R}} \left(\frac{\alpha}{\mathfrak{p}}\right) = \sum_{\substack{\alpha\in\mathfrak{R}\\ (\alpha,\mathfrak{p})=1}} 1 - 2\sum_{\alpha\in\mathfrak{R}\cap\mathfrak{S}_2} 1.$$

Suppose that $P > N\mathfrak{p}^{(1/2)+a}$, then the corollary yields

$$\sum_{\alpha\in\mathfrak{R}} \left(\frac{\alpha}{\mathfrak{p}}\right) \ll P(N\mathfrak{p})^{-b_1}.$$

Thus we obtain, using (22),

$$\sum_{\alpha\in\mathfrak{R}\cap\mathfrak{S}_2} 1 = \frac{1}{2}\frac{(2\pi)^{r_2}}{|\sqrt{d}|} P\{1 + O((N\mathfrak{p})^{-b})\}$$

for some positive b depending on a and n. This is statement (7) given in the introduction.

Remark. It is possible to deduce the bound

$$N\mu \ll (N\mathfrak{p})^{(1/2\sqrt{e})+a},$$

where $\mu \in \mathfrak{S}_2$ denotes a least totally positive quadratic nonresidue modulo a prime ideal $\mathfrak{p}$ of K, least in the sense that $N\mu$ is minimal.

REFERENCES

1. D. A. BURGESS, On character sums and primitive roots, *Proc. London Math. Soc. (3)* **12** (1962), 179–192.
2. D. A. BURGESS, On character sums and L-series, *Proc. London Math. Soc. (3)* **12** (1962), 193–206.
3. D. A. BURGESS, On character sums and L-series II, *ibid.*, **13** (1963), 524–536.
4. H. DAVENPORT AND D. J. LEWIS, Character sums and primitive roots in finite fields, *Rend. Circ. Mat. Palermo (2)* **12** (1963), 129–136.
5. J. B. FRIEDLANDER, On the least k-th power non-residue in an algebraic number field, *Proc. London Math. Soc. (3)* **26** (1973), 19–34.
6. J. B. FRIEDLANDER, On characters and polynomials, *Acta Arith.* **XXV** (1973), 34–37.
7. W. GROTZ, Einige Anwendungen der Siegelschen Summenformel, *Acta Arith.* **38** (1980), 69–95.
8. E. HECKE, Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen (Zweite Mitteilung), *Math. Z.* **6** (1920), 11–51.
9. E. LANDAU, Über Ideale und Primideale in Idealklassen, *Math. Z.* **2** (1918), 52–154.
10. E. LANDAU, "Verallgemeinerung eines Pólyaschen Satzes auf algebraische Zahlkörper", pp. 478–488, Göttinger Nachrichten, 1918.
11. E. LANDAU, "Vorlesungen über Zahlentheorie," Band 2, Teil VII, Kap. 14, Chelsea, New York.
12. K.-CH. LEE, "Über Summen von Restklassencharakteren im reell-quadratischen Zahlkörper," Dissertation, Marburg, 1973.
13. G. PÓLYA, "Über die Verteilung der quadratischen Reste und Nichtreste," pp. 21–29, Göttinger Nachrichten, 1918.
14. H. RADEMACHER, "Über die Anwendung der Viggo Brunschen Methode auf die Theorie der algebraischen Zahlkörper," pp. 211–218, Berliner Akad. der Wissenschaften, Sitzungsberichte, Berlin, 1923.
15. H. RADEMACHER, Zur additiven Primzahltheorie algebraischer Zahlkörper III, *Math. Z.* **27** (1928), 321–426.
16. H. RADEMACHER, On the Phragmén–Lindelöf theorem and some applications, *Math. Z.* **72** (1959), 192–204.
17. G. J. RIEGER, Verallgemeinerung der Siebmethode von A. Selberg auf algebraische Zahlkörper III, *J. Reine Angew. Math.* **208** (1961), 79–90.
18. C. L. SIEGEL, Additive Theorie der Zahlkörper II, *Math. Ann.* **88** (1923), 184–210.
19. C. L. SIEGEL, Mittelwerte arithmetischer Funktionen in Zahlkörpern, *Trans. Amer. Math. Soc.* **39** (1936), 219–224.
20. VINOGRADŌV, Sur la distribution des résidus et des non-résidus des puissances, *J. Phys.-Math. Soc. Univ. Perm.* **1** (1918), 94–96.