

The least primitive root in number fields

by

YONGHUI WANG (Beijing) and CLAUS BAUER (San Francisco, CA)

Dedicated to Prof. Wang Yuan on his 75th birthday

1. Introduction. Let K be an algebraic number field of degree $[K : \mathbb{Q}] = n = r_1 + 2r_2$ (in the standard notation), d its discriminant, h its class number, and $r = r_1 + r_2 - 1$ its number of fundamental units. Let \mathcal{E} , R , and ω denote respectively the group of units, the regulator, and the number of roots of unity in K .

The conjugates of a number $\alpha \in K$ are denoted by $\alpha^{(k)}$ ($k = 1, \dots, n$), and we write $\alpha \succ 0$ to indicate that α is *totally positive*, i.e. $\alpha \neq 0$ and $\alpha^{(k)} > 0$ for $1 \leq k \leq r_1$ (so $\alpha \succ 0$ means simply $\alpha \neq 0$ if K is totally imaginary). As usual, the numbers e_1, \dots, e_{r+1} are defined by

$$e_k = \begin{cases} 1 & \text{for } k = 1, \dots, r_1, \\ 2 & \text{for } k = r_1 + 1, \dots, r_1 + r_2. \end{cases}$$

Throughout, x will denote a vector

$$x = (x_1, \dots, x_{r+1}) \in \mathbb{R}_+^{r+1},$$

and

$$X := X(x) := \prod_{k=1}^{r+1} x_k^{e_k}.$$

We denote by O_K the ring of integers in K . Let \mathfrak{q} be an integral ideal of K . The reduced residue classes of integers (relatively prime to \mathfrak{q}) form a group under multiplication; its order is denoted by $\phi(\mathfrak{q})$. Let χ be a Dirichlet character of this group. Throughout this paper, we will abbreviate principal ideals (α) as α when no confusion is possible.

Next, we introduce an extended definition of the von Mangoldt function for ideals. Whereas in the original definition, the argument of the function must be an ideal, we allow ideal numbers for K as arguments as well. We

2000 *Mathematics Subject Classification*: Primary 11L40, 11R47.

The first author is supported by National Natural Science Foundation (China), Tianyuan Youth Foundation and the Morning Side center.

recall that in [3, p. 108], a *prime ideal number* is defined as an ideal number that corresponds to a prime ideal in the field K . Now, for an α that is either a principal ideal or a prime ideal number, we define

$$(1) \quad \Lambda(\alpha) = \begin{cases} \log(N\mathfrak{p}) & \text{if } \alpha = \mathfrak{p}^f, \mathfrak{p} \text{ is an prime ideal} \\ & \text{(if } \alpha \text{ is a principal ideal)} \\ & \text{or } \mathfrak{p} \text{ is a prime ideal number} \\ & \text{(if } \alpha \text{ is an ideal number),} \\ 0 & \text{otherwise.} \end{cases}$$

By using a Perron formula for algebraic number fields, we can show the following:

THEOREM 1. *Under the assumption that the Grand Riemann Hypothesis (GRH) holds in algebraic number fields, we have*

$$\sum_{\substack{\alpha \in O_K \\ \alpha > 0}} \chi(\alpha) \Lambda(\alpha) \Phi(|\alpha|x^{-1}) = g(\chi) \frac{\omega 2^{r_2 - r_1}}{hR} X + O_K(X^{1/2} \log(N\mathfrak{q})),$$

where $g(\chi) = 1$ if χ is a principal character and 0 otherwise. $\Phi(x)$ is a weight function such that

$$(2) \quad \Phi(x) := e^{-(x_1 + \dots + x_{r+1})}, \quad |\alpha|x^{-1} := (|\alpha^{(1)}|x_1^{-1}, \dots, |\alpha^{(r+1)}|x_{r+1}^{-1}).$$

Using Theorem 1 and the sieve method in [11], we consider the least primitive root modulo a prime ideal \mathfrak{q} . First, we define

$$(3) \quad I_c(x) := \{\alpha > 0 \mid |\alpha^{(k)}| \leq cx_k, k = 1, \dots, r + 1\}.$$

We will prove the following theorem:

THEOREM 2. *Assume that the Grand Riemann Hypothesis (GRH) holds in number fields. Then there exists a primitive root α modulo a prime ideal \mathfrak{q} such that*

$$\alpha \in I_c(m^6 \log^2(N\mathfrak{q})),$$

where c is an absolute constant depending only on K , $m := \omega(\phi(N\mathfrak{q}))$, and $\omega(n)$ denotes the number of distinct prime divisors of n .

For rational number fields, Burgess [1] has proved unconditionally that the least positive primitive root modulo a prime q must be less than $q^{1/4+\varepsilon}$. Assuming the GRH in rational number fields, Wang Yuan [11] improved upon this result by showing that the least primitive root must be less than $\omega^6(q - 1) \log^2 q$. For algebraic number fields, Hinz [5] first gave an unconditional bound of $\alpha \in I_c(N\mathfrak{q}^{1/2+\varepsilon})$ which he later improved [6] to $\alpha \in I_c(N\mathfrak{q}^{1/4+\varepsilon})$. The latter result generalizes Burgess’s result to algebraic number fields. Here, we intend to generalize Wang Yuan’s conditional result to algebraic number fields. For this purpose, we need to establish a Perron

formula that is more accurate than the one used by Hinz, and we will appeal to the sieve method as in [11].

2. Perron formula in number fields. The Perron formula for the rational field plays a vital role in analytic number theory, e.g. in proving the prime number theorem. For algebraic number fields, in 1936, Siegel established the so-called Siegel formula for real quadratic number fields [10]. The generalization of his results to totally real number fields and then to arbitrary algebraic number fields was achieved respectively by Schaal [9] and Grotz [2]. This work was further generalized by Rausch [8], who established general identities for weighted sums over algebraic number fields. This paper will use a simplified version of Rausch’s idea.

In this section, we will first recall some facts from the theory of Grössencharacters and Hecke’s zeta function. Then, we will prove the Perron formula.

We always assume χ to be a character mod \mathfrak{q} and set $r = r_1 + r_2 - 1 > 0$. Let \mathcal{U} be the free group of the totally positive free units which are congruent to 1 mod \mathfrak{q} , i.e. $\eta \equiv 1 \pmod{\mathfrak{q}}$ for $\eta \in \mathcal{U}$. Therefore, $\chi(\eta) = 1$ for $\eta \in \mathcal{U}$.

Hence \mathcal{U} has finite index $[\mathcal{E} : \mathcal{U}]$ in the units group \mathcal{E} . If we fix a basis η_1, \dots, η_r of \mathcal{U} and define

$$R(\mathcal{U}) := |\det(e_j \log |\eta_1^{(j)}|, \dots, e_j \log |\eta_r^{(j)}|)_{j=1, \dots, r}|,$$

then (see [8])

$$[\mathcal{E} : \mathcal{U}] = \omega R(\mathcal{U})/R.$$

Following Hecke’s idea [4], we now define the *Grössencharacters* λ with respect to \mathcal{U} (i.e. $\lambda(\eta) = 1$ for every $\eta \in \mathcal{U}$). For $\tau := (\tau_1, \dots, \tau_r) \in \mathbb{R}^r$ define the numbers

$$E(\tau) := (E_1(\tau), \dots, E_{r+1}(\tau))$$

by the system of equations

$$(4) \quad \sum_{j=1}^{r+1} e_j E_j(\tau) = 0, \quad \sum_{j=1}^{r+1} e_j E_j(\tau) \log |\eta_k^{(j)}| = 2\pi\tau_k \quad (k = 1, \dots, r).$$

As in [8], we define a *generalized Grössencharacter* as

$$(5) \quad \lambda_\tau(\alpha) = \prod_{j=1}^{r+1} |\alpha^{(j)}|^{ie_j E_j(\tau)} \quad (0 \neq \alpha \in K).$$

Thus, by (4) for $m := (m_1, \dots, m_r) \in \mathbb{Z}^r$ we have $\lambda_m(\eta) = 1$ for every $\eta \in \mathcal{U}$, i.e., λ_m is indeed a Grössencharacter with respect to \mathcal{U} .

Following Hecke [3, p. 108], we assign to K a system of ideal numbers $\hat{\alpha}, \hat{\beta}, \dots$. For an integral ideal α , $\hat{\alpha}$ is a specimen out of this system of ideal numbers such that $\alpha = (\hat{\alpha})$. One can deduce from the structure of this

system that if $(\hat{\alpha}) = (\hat{\beta})$ then $\hat{\alpha} = \hat{\beta}\varepsilon$ where $\varepsilon \in \mathcal{E}$. Indeed, the system of ideal numbers splits into h classes,

$$\mathfrak{R}(\hat{\alpha}) = \{\hat{\alpha}\varrho : \varrho \in K\}.$$

These classes are mutually disjoint except for the number 0. Further, we follow [4] and divide the set of ideal numbers into “narrow” classes as follows: Two ideal numbers $\hat{\alpha}$ and $\hat{\beta}$ are in the same class if and only if

$$\hat{\beta} \in \mathfrak{R}(\hat{\alpha}), \text{ and } \hat{\alpha}/\hat{\beta} \text{ is totally positive.}$$

These classes form a group \mathfrak{G} of order $2^{r_1}h$ (see [5, p. 57]). Let ψ be a character of this group. Then for $\text{Re } s > 1$, we can transform the following summation over totally positive algebraic integers into a summation over ideal integers:

$$\begin{aligned} (6) \quad \sum_{\substack{\alpha \in \mathcal{O}_K \\ \alpha > 0}} \frac{\lambda_m(\alpha)\chi(\alpha)\Lambda(\alpha)}{|N(\alpha)|^s} &= \frac{1}{2^{r_1}h} \sum_{\psi} \sum_{\hat{\alpha}} \frac{\Lambda(\hat{\alpha})\lambda_m(\hat{\alpha})\chi(\hat{\alpha})\psi(\hat{\alpha})}{|N(\hat{\alpha})|^s} \\ &=: \frac{1}{2^{r_1}h} \sum_{\psi} \sum_{\hat{\alpha}} \frac{\Lambda(\hat{\alpha})\lambda_m\chi\psi(\hat{\alpha})}{|N(\hat{\alpha})|^s}, \quad \text{say.} \end{aligned}$$

We note that on the right hand side, χ is extended to a character for all ideal integers, since 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 ambient group. We also apply our extended definition of the von Mangoldt function in (1). We now introduce Hecke’s zeta functions: First, let

$$Z(s, \lambda_m\chi\psi, \mathcal{U}) := \sum_{(\hat{\alpha})_{\mathcal{U}}} \frac{\lambda_m\chi\psi(\hat{\alpha})}{|N(\hat{\alpha})|^s} \quad (\text{Re } s > 1),$$

where $(\hat{\alpha})_{\mathcal{U}}$ means that the sum runs over a complete set of the ideal integers which are not associated with respect to \mathcal{U} . Since $\lambda_m\chi\psi(\eta) = 1$ for $\eta \in \mathcal{U}$, it is well defined.

We note that the units not associated mod \mathcal{U} form a group of order $[\mathcal{E} : \mathcal{U}] = \omega R(\mathcal{U})/R$. Obviously, $\lambda_m\chi\psi$ is a character of this group. In the next equation, we indicate by $(\varepsilon)_{\mathcal{U}}$ the fact that ε runs over this group. We find that

$$\begin{aligned} (7) \quad Z(s, \lambda_m\chi\psi, \mathcal{U}) &= \sum_{(\hat{\alpha})_{\mathcal{U}}} \frac{\lambda_m\chi\psi(\hat{\alpha})}{|N(\hat{\alpha})|^s} = \sum_{(\hat{\alpha})_{\mathcal{E}}} \sum_{(\varepsilon)_{\mathcal{U}}} \frac{\lambda_m\chi\psi(\hat{\alpha}\varepsilon)}{|N(\hat{\alpha})|^s} = \sum_{(\hat{\alpha})_{\mathcal{E}}} \frac{\lambda_m\chi\psi(\hat{\alpha})}{|N(\hat{\alpha})|^s} \sum_{(\varepsilon)_{\mathcal{U}}} \lambda_m\chi\psi(\varepsilon) \\ &= \begin{cases} \frac{\omega R(\mathcal{U})}{R} \sum_{(\hat{\alpha})_{\mathcal{E}}} \frac{\lambda_m\chi\psi(\hat{\alpha})}{|N(\hat{\alpha})|^s} & \text{if } \lambda_m\chi\psi(\varepsilon) = 1 \text{ for } \varepsilon \in \mathcal{E}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

If $\lambda_m(\varepsilon)\chi(\varepsilon)\psi(\varepsilon) = 1$ for $\varepsilon \in \mathcal{E}$, then $\lambda_m\chi\psi$ is called a Hecke Grössencharacter for ideals, and we may define $\lambda_m\chi\psi(\mathfrak{a})$ for nonzero ideals \mathfrak{a} in K by

$$\lambda_m\chi\psi(\mathfrak{a}) := \lambda_m\chi\psi(\widehat{\mathfrak{a}}) := \lambda_m(\widehat{\mathfrak{a}})\chi(\widehat{\mathfrak{a}})\psi(\widehat{\mathfrak{a}}),$$

where $\mathfrak{a} = (\widehat{\mathfrak{a}})$.

If $\lambda_m\chi\psi$ is a Hecke Grössencharacter, we can define a Hecke zeta function as follows:

$$\zeta(s, \lambda_m\chi\psi) := \sum_{(\widehat{\mathfrak{a}})_{\mathcal{E}}} \frac{\lambda_m\chi\psi(\widehat{\mathfrak{a}})}{|N(\widehat{\mathfrak{a}})|^s} = \prod_{(\widehat{\mathfrak{q}})_{\mathcal{E}}} \left(1 - \frac{\lambda_m\chi\psi(\widehat{\mathfrak{q}})}{|N(\widehat{\mathfrak{q}})|^s}\right)^{-1} \quad (\text{Re } s > 1),$$

where $(\widehat{\mathfrak{q}})_{\mathcal{E}}$ runs over prime ideal numbers mod \mathcal{E} . Therefore, we deduce from (7) that

$$Z(s, \lambda_m\chi\psi, \mathcal{U}) = \frac{\omega R(\mathcal{U})}{R} \zeta(s, \lambda_m\chi\psi),$$

if $\lambda_m\chi\psi$ is a Hecke Grössencharacter. We note that for $\text{Re } s > 1$,

$$\log \zeta(s, \lambda_m\chi\psi) = \log \prod_{(\widehat{\mathfrak{q}})_{\mathcal{E}}} \left(1 - \frac{\lambda_m\chi\psi(\widehat{\mathfrak{q}})}{|N(\widehat{\mathfrak{q}})|^s}\right)^{-1} = \sum_{(\widehat{\mathfrak{q}})_{\mathcal{E}}} \sum_{n=1}^{\infty} \frac{\lambda_m\chi\psi(\widehat{\mathfrak{q}}^n)}{n|N(\widehat{\mathfrak{q}}^n)|^s},$$

and obtain

$$\frac{\zeta'(s, \lambda_m\chi\psi)}{\zeta(s, \lambda_m\chi\psi)} = - \sum_{(\widehat{\mathfrak{a}})_{\mathcal{E}}} \frac{\lambda_m\chi\psi(\widehat{\mathfrak{a}})A(\widehat{\mathfrak{a}})}{|N(\widehat{\mathfrak{a}})|^s},$$

where $A(\widehat{\mathfrak{a}})$ is the von Mangoldt function defined in (1). Arguing as in (6) and (7), we find:

$$\begin{aligned} (8) \quad \sum_{\substack{(\alpha)_{\mathcal{U}} \\ \alpha > 0}} \frac{\lambda_m\chi(\alpha)A(\alpha)}{|N(\alpha)|^s} &= \frac{1}{2^{r_1}h} \sum_{\psi} \sum_{(\widehat{\mathfrak{a}})_{\mathcal{U}}} \frac{\lambda_m\chi\psi(\widehat{\mathfrak{a}})A(\widehat{\mathfrak{a}})}{|N(\widehat{\mathfrak{a}})|^s} \\ &= \frac{1}{2^{r_1}h} \sum_{\psi} \sum_{(\widehat{\mathfrak{a}})_{\mathcal{E}}} \frac{\lambda_m\chi\psi(\widehat{\mathfrak{a}})A(\widehat{\mathfrak{a}})}{|N(\widehat{\mathfrak{a}})|^s} \sum_{(\varepsilon)_{\mathcal{U}}} \lambda_m\chi\psi(\varepsilon) \\ &= - \frac{\omega R(\mathcal{U})}{2^{r_1}hR} \sum_{\psi} \frac{\zeta'(s, \lambda_m\chi\psi)}{\zeta(s, \lambda_m\chi\psi)}, \end{aligned}$$

where \sum_{ψ} runs over $\lambda_m\chi\psi$ that are Hecke Grössencharacters, i.e. $\lambda_m\chi\psi(\varepsilon) = 1$ for all $\varepsilon \in \mathcal{E}$.

We will now begin with the preparations for the proof of the Perron formula which will allow us to estimate the sum $\sum_{\alpha} \chi(\alpha)A(\alpha)\Phi(|\alpha|x^{-1})$ via Hecke's zeta functions. Our result can be regarded as a simplified case of the theorem of Rausch [8, Theorems 2.1 and 2.2], the difference being that we do not apply a complicated smoothing integral operator as in [8, Theorems

2.1 and 2.2], since our weight function Φ is already sufficiently smooth. This simplifies our application in this paper.

We now define the $(r + 1)$ -dimensional Mellin transform of $\Phi(u) = e^{-(u_1 + \dots + u_{r+1})}$ as

$$\Psi(s) := 2^{r^2} \int_{\mathbb{R}_+^{r+1}} \Phi(u) \prod_{k=1}^{r+1} u_k^{e_k s_k - 1} du = 2^{r^2} \prod_{k=1}^{r+1} \Gamma(e_k s_k)$$

for $s = (s_1, \dots, s_{r+1}) \in \mathbb{C}^{r+1}$.

We first consider the special case of

$$\sum_{\eta \in \mathcal{U}} \lambda(\eta) \Phi(|\eta| x^{-1}),$$

where λ is a generalized Grössencharacter defined as

$$\lambda(\alpha) := \prod_{k=1}^{r+1} |\alpha^{(k)}|^{ie_k b_k}.$$

LEMMA 1. *We have*

$$(9) \quad \sum_{\eta \in \mathcal{U}} \lambda(\eta) \Phi(|\eta| x^{-1}) = \frac{1}{2\pi i R(\mathcal{U})} \sum_m \int_{2-i\infty}^{2+i\infty} \Psi(s + ib - iE(m)) \prod_{k=1}^{r+1} x_k^{e_k(s + ib_k - iE_k(m))} ds,$$

where m runs through \mathbb{Z}^r , and we use the abbreviation

$$s + ib - iE(m) := (s + ib_1 - iE_1(m), \dots, s + ib_{r+1} - iE_{r+1}(m)).$$

Proof. This is a special case of [8, Theorem 2.1]. Since

$$\Psi(s) = 2^{r^2} \prod_{k=1}^{r+1} \Gamma(e_k s_k),$$

and $\Gamma(\sigma + it)$ is of exponential decay in $|t|$, the sum and integrals on the right converge absolutely. Thus, there is no need to apply the smoothing operator as in [8, Theorem 2.1]. Hence, by the same argument of applying Poisson summation as in [8, Theorem 2.1], the lemma is proved. ■

Therefore we get the Perron formula for number fields as follows.

THEOREM 3. *Set $s - iE(m) := (s - E_1(m), \dots, s - E_{r+1}(m))$. Then*

$$(10) \quad \sum_{\alpha > 0} A\chi(\alpha) \Phi(|\alpha| x^{-1}) = -\frac{\omega 2^{r^2 - r_1}}{hR} \sum_{\psi} \sum_{m \in \mathbb{Z}^r} \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)}$$

$$\begin{aligned} & \times \prod_{k=1}^{r+1} (\Gamma(e_k(s - iE_k(m))) x_k^{e_k(s - iE_k(m))}) ds \\ & =: -\frac{\omega 2^{r_2 - r_1}}{hR} \sum_{\psi} \sum_{m \in \mathbb{Z}^r} \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} Y(s - iE(m)) ds, \end{aligned}$$

where m runs over \mathbb{Z}^r and ψ runs over characters of \mathfrak{S} (see (6)) such that $\lambda_m \chi \psi$ is a Hecke Grössencharacter, and

$$Y(s) := \prod_{k=1}^{r+1} Y_k(s_k) := \prod_{k=1}^{r+1} (\Gamma(e_k s_k) x_k^{e_k s_k})$$

for $s = (s_1, \dots, s_{r+1}) \in \mathbb{C}^{r+1}$.

Proof. Using Lemma 1 with $b_k = 0$ and noting that $\chi \psi(\eta) = 1$ for $\eta \in \mathcal{U}$, and $\Lambda(\hat{\alpha}\varepsilon) = \Lambda(\hat{\alpha})$ for $\varepsilon \in \mathcal{E}$, we see that

$$\begin{aligned} \sum_{\substack{\alpha > 0 \\ (\alpha)_{\mathcal{U}}} } \chi(\alpha) \Lambda(\alpha) \Phi(|\alpha|x^{-1}) &= \sum_{\substack{(\alpha)_{\mathcal{U}} \\ \alpha > 0}} \chi(\alpha) \Lambda(\alpha) \sum_{\eta \in \mathcal{U}} \Phi(|\eta|(|\alpha|x^{-1})) \\ &= \frac{1}{2\pi i R(\mathcal{U})} \sum_{\substack{(\alpha)_{\mathcal{U}} \\ \alpha > 0}} \chi(\alpha) \Lambda(\alpha) \sum_{m \in \mathbb{Z}^r} \int_{2-i\infty}^{2+i\infty} \Psi(s - iE(m)) \\ &\quad \times \prod_{k=1}^{r+1} (|\alpha^{(k)}|^{-1} x_k)^{e_k(s - iE_k(m))} ds. \end{aligned}$$

Note that $N(\alpha) = \prod_{k=1}^{r+1} (\alpha^{(k)})^{e_k}$ and $\lambda_m(\alpha) = \prod_{k=1}^{r+1} |\alpha^{(k)}|^{ie_k E_k(m)}$, hence the above is

$$\begin{aligned} &= \frac{1}{2\pi i R(\mathcal{U})} \sum_{m \in \mathbb{Z}^r} \int_{2-i\infty}^{2+i\infty} \Psi(s - iE(m)) \\ &\quad \times \left(\sum_{\substack{(\alpha)_{\mathcal{U}} \\ \alpha > 0}} \frac{\Lambda(\alpha) \chi(\alpha) \lambda_m(\alpha)}{|N(\alpha)|^s} \right) \prod_{k=1}^{r+1} x_k^{e_k(s - iE_k(m))} ds \\ &= -\frac{\omega}{2^{r_1} hR} \sum_{\psi} \sum_{m \in \mathbb{Z}^r} \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \Psi(s - iE(m)) \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} \prod_{k=1}^{r+1} x_k^{e_k(s - iE_k(m))} ds. \end{aligned}$$

The last equality follows from (8) and (5), as each expression $\lambda_m \chi \psi$ is a Hecke Grössencharacter while m runs over \mathbb{Z}^r and ψ runs over characters of \mathfrak{S} (see (6)). Hence, we get the desired Perron formula. ■

We assume that for a given $\chi \psi$, $\lambda_m \chi \psi$ is a Hecke Grössencharacter, i.e. $\lambda_m \chi \psi(\varepsilon) = 1$ for all $\varepsilon \in \mathcal{E}$. We let $E(m) = (E_1(m), \dots, E_{r+1}(m))$ as in (4)

and let $\varepsilon_1, \dots, \varepsilon_r$ be a basis of the subgroup of \mathcal{E} that contains all torsion-free elements of \mathcal{E} . We derive from (4) and (5) a system of equations

$$\sum_{j=1}^{r+1} e_j E_j(m) = 0, \quad \sum_{j=1}^{r+1} e_j E_j(m) \log |\varepsilon_k^{(j)}| = 2\pi m'_k + i \log \chi\psi(\varepsilon_k) \quad (k=1, \dots, r).$$

Since $|\chi\psi| = 1$, $i \log \chi\psi$ is real. Then we get

$$(11) \quad E_j(m) = E'_j \left(\left(m'_k + \frac{i}{2\pi} \log \chi\psi(\varepsilon_k) \right)_{k=1, \dots, r} \right),$$

where $E'(\tau)$ denotes the solution of

$$(12) \quad \sum_{j=1}^{r+1} e_j E'_j(\tau) = 0, \quad \sum_{j=1}^{r+1} e_j E'_j(\tau) \log |\varepsilon_k^{(j)}| = 2\pi\tau_k \quad (k=1, \dots, r).$$

We will use this relation to show in Lemma 6 that the summation over m which runs over \mathbb{Z}^r with $\lambda_m \chi\psi$ being Hecke Grössencharacter does not depend on \mathcal{U} .

3. Estimate for Hecke’s zeta functions. In this section, we will derive several estimates for Hecke’s zeta functions. If χ is a nonprincipal character modulo \mathfrak{q} ($\mathfrak{q} \neq (1)$), ψ is a character of the “narrow” class group \mathfrak{S} in (6), and λ_m is the generalized Grössencharacter (5) such that $\lambda_m \chi\psi(\varepsilon) = 1$ for $\varepsilon \in E$, then $\lambda_m \chi\psi$ is a nonprincipal Hecke Grössencharacter. And if χ is a primitive character mod q , then $\lambda_m \chi\psi$ is also a primitive Hecke Grössencharacter (see [4]). We note that if χ is not primitive, then it is induced by a primitive character $\chi^* \bmod \mathfrak{f}$, where $\mathfrak{f} | \mathfrak{q}$. In this case,

$$(13) \quad \begin{aligned} \zeta(s, \lambda_m \chi\psi) &= \zeta(s, \lambda_m \chi^* \psi) \prod_{\mathfrak{p} | \mathfrak{q}} (1 - \lambda_m \chi^* \psi(\mathfrak{p}) N\mathfrak{p}^{-s}) \\ &= \zeta(s, \lambda_m \chi^* \psi) \left(\sum_{\mathfrak{a} | \mathfrak{q}} \mu(\mathfrak{a}) \lambda_m \chi^* \psi(\mathfrak{a}) N\mathfrak{a}^{-s} \right). \end{aligned}$$

Hence, we can reduce our investigations to the case that $\lambda_m \chi\psi$ is primitive modulo \mathfrak{f} , where $\mathfrak{f} | \mathfrak{q}$. For primitive $\lambda_m \chi\psi$, Hecke (see [4, p. 35]) obtained the following functional equation for $\zeta(s, \lambda_m \chi\psi)$: Let

$$\xi(s, \lambda_m \chi\psi) := \zeta(s, \lambda_m \chi\psi) \prod_{k=1}^{r_1} \Gamma\left(\frac{1}{2}(s + a_k + iE_k(m))\right) \prod_{k=r_1+1}^{r_1+r_2} \Gamma(s + iE_k(m)),$$

where a_1, \dots, a_{r_1} are determined by the sign character induced by $\chi\psi$ (see

[4, p. 20]). Then

$$\begin{aligned} \xi(s, \overline{\lambda_m \chi \psi}) &= \zeta(s, \overline{\lambda_m \chi \psi}) \\ &\times \prod_{k=1}^{r_1} \Gamma\left(\frac{1}{2}(s + a_k - iE_k(m))\right) \prod_{k=r_1+1}^{r_1+r_2} \Gamma(s - iE_k(m)), \end{aligned}$$

and we have the functional equation

$$\xi(s, \lambda_m \chi \psi) = W(\lambda_m \chi \psi) A^{1-2s} \xi(1 - s, \overline{\lambda_m \chi \psi}),$$

where $|W(\lambda_m \chi \psi)| = 1$, $A = \sqrt{|d|N(\mathfrak{f})/\pi^n} 2^{-r_2}$.

Using the functional equation, the Phragmén–Lindelöf principle, and the relation (13), the following lemma is shown in [5, Lemma 2] for all $\lambda_m \chi \psi$:

LEMMA 2. *Let $0 < \eta \leq 1/2$, then for $-\eta \leq \sigma \leq 1 + \eta$, where $s = \sigma + it$, we have*

$$\begin{aligned} \zeta(s, \lambda_m \chi \psi) &\ll_{\eta, K} \left(N\mathfrak{q}(1 + |t|)^n \prod_{k=1}^{r+1} (1 + |E_k(m)|)^{e_k} \right)^{(1+\eta-\sigma)/2} \\ &= (N\mathfrak{q}|E(m)|(1 + |t|)^n)^{(1+\eta-\sigma)/2}, \end{aligned}$$

where $|E(m)| := \prod_{k=1}^{r+1} (1 + |E_k(m)|)^{e_k}$.

Applying Lemma 2 of Moroz [7, p. 54], and in particular taking the order of $\zeta(s, \lambda_m \chi \psi)$ in his lemma, one obtains:

LEMMA 3 ([7, p. 55, Proposition 2]). *If $\rho = \sigma + i\gamma$ are the nontrivial zeros of $\zeta(s, \lambda_m \chi \psi)$, then the number of zeros such that $l \leq \gamma \leq l + 1$ is $O(\log(N\mathfrak{q}|E(m)|(|l + 1)^n))$.*

For the entire function $\xi(s, \lambda_m \chi \psi)$, we write the Weierstrass product

$$g(\lambda_m \chi \psi) s(s - 1) \xi(s, \lambda_m \chi \psi) = \exp(A + Bs) \prod_{\rho} \exp\left(\frac{s}{\rho}\right) \left(1 - \frac{s}{\rho}\right)$$

where ρ runs over all nontrivial zeros of $\zeta(s, \lambda_m \chi \psi)$. Using this presentation, we follow the argument in [7, p. 55, Lemma 3] to obtain

$$\begin{aligned} (14) \quad &\frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} \\ &= \sum_{\rho} \frac{1}{s - \rho} - g(\lambda_m \chi \psi) \left(\frac{1}{s} + \frac{1}{s - 1}\right) + O(\log(N\mathfrak{q}|E(m)|(|t| + 2)^n)) \\ &= \sum_{|t-\gamma| < 1} \frac{1}{s - \rho} - g(\lambda_m \chi \psi) \left(\frac{1}{s} + \frac{1}{s - 1}\right) + O(\log(N\mathfrak{q}|E(m)|(|t| + 2)^n)), \end{aligned}$$

with $-1/4 < \text{Re } s \leq 2$. Now, $g(\lambda_m \chi \psi) = 1$ if $\lambda_m \chi \psi$ is principal and 0 otherwise. The last equality above is deduced using Lemma 3.

Hence, the residue of the Hecke zeta function is:

$$(15) \quad \begin{aligned} \operatorname{Res} \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} \Big|_{s=\varrho} &= 1 && \text{if } \varrho \text{ is a zero of } \zeta(s, \lambda_m \chi \psi), \\ \operatorname{Res} \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} \Big|_{s=0,1} &= -1 && \text{if } \lambda_m \chi \psi \text{ is principal.} \end{aligned}$$

Using again Lemma 3, we obtain:

LEMMA 4. *For all $l \in \mathbb{Z}$, $|l| \geq 2$, there exists $T_l \in (l, l + 1)$ such that*

$$\frac{\zeta'(\sigma + iT_l, \lambda_m \chi \psi)}{\zeta(\sigma + iT_l, \lambda_m \chi \psi)} \ll \log^2(N\mathfrak{q}|E(m)|(|T_l| + 1)^n).$$

Proof. By Lemma 3, for each $\lambda_m \chi \psi$ there exists a positive constant c and $T_l \in (l, l + 1)$ such that there is no zero of $\zeta(s, \lambda_m \chi \psi)$ in the region

$$|\operatorname{Im} s - T_l| \leq c \log^{-1}(N\mathfrak{q}|E(m)|(|T_l| + 1)^n).$$

Then we get the lemma by applying (14) and Lemma 3. ■

Furthermore, if we assume GRH, i.e. all the nontrivial zeros of $\zeta(s, \lambda_m \chi \psi)$ have the form $\varrho = 1/2 + i\gamma$, then by (14) and Lemma 3 we have:

LEMMA 5. *Assuming the GRH, we have*

$$\frac{\zeta'}{\zeta} \left(\frac{1}{3} + it, \lambda_m \chi \psi \right) \ll \log(N\mathfrak{q}|E(m)|(|t| + 1)^n).$$

4. Estimate for character sums and proof of Theorem 1. We suppose $r > 0$; then $R \neq 0$. Define $E_k(m)$ as in (4) for a general Grössen-character λ_m with respect to \mathcal{U} , and set

$$W_k(m) := E_k(m) - E_{r+1}(m) \quad (k = 1, \dots, r).$$

This is an r -dimensional lattice, and by Rausch [8, Lemma 4.4], for any fixed $w = (w_1, \dots, w_r) \in \mathbb{R}^r$,

$$(16) \quad \#\{m \in \mathbb{Z}^r : w_k \leq W_k(m) \leq w_k + 1, k = 1, \dots, r\} \ll R(\mathcal{U}).$$

We will show in the following similar lemma that the distribution of $E_k(m)$ such that all $\lambda_m \chi \psi$ are Hecke Grössencharacters for fixed $\chi \psi$ no longer depends on \mathcal{U} :

LEMMA 6. *Let $E_k(m)$ be as in (4) such that $\lambda_m \chi \psi$ are Hecke Grössencharacters for fixed $\chi \psi$. Then*

$$\#\{m \in \mathbb{Z}^r, l \in \mathbb{Z} : w_k \leq l - E_k(m) \leq w_k + 1, k = 1, \dots, r + 1\} \ll R.$$

Proof. By (11), if $\lambda_m \chi \psi$ are Hecke Grössencharacters for fixed $\chi \psi$, then there exist $m' \in \mathbb{Z}^r$ and fixed $z \in \mathbb{R}^r$ such that

$$E_k(m) = E'_k(m' + z), \quad W_k(m) = W'_k(m' + z),$$

where $m' + z := (m'_1 + z_1, \dots, m'_r + z_r)$, and $E'(\tau)$ is defined as in (12) with respect to \mathcal{E} . Since $R, R(\mathcal{U}) \neq 0$ the correspondence $m \mapsto m'$ defined by (11) is then injective.

If

$$w_k < l - E_k(m) < w_k + 1, \quad k = 1, \dots, r + 1,$$

then

$$w_{r+1} - w_k - 1 \leq W'_k(m' + z) \leq w_{r+1} - w_k + 1.$$

By the injectivity of $m \mapsto m'$, it suffices to prove that the number of the m' satisfying the above inequality is at most R . This can be done by the same argument as in Rausch [8, Lemma 4.4] with the added fixed z . And for a fixed m , there exists at most one l satisfying our assumption. The assertion follows. ■

Now, we will use the Perron formula (10) to prove Theorem 1. Assuming the General Riemann Hypothesis for Hecke zeta functions, we denote by \sum_{ϱ} the fact that $\varrho := \varrho^{(m)} := 1/2 + i\gamma^{(m)}$ runs over the nontrivial zeros of $\zeta(s, \lambda_m \chi \psi)$. We first assume that χ is nonprincipal; then $\lambda_m \chi \psi$ can only run over nonprincipal Hecke Grössencharacters, and $\zeta'(s, \lambda_m \chi \psi) / \zeta(s, \lambda_m \chi \psi)$ has its all poles at $\varrho^{(m)}$ s with residue 1 by (14). From Cauchy's theorem and Lemmas 4 and 5, we obtain

$$\begin{aligned} S &:= \sum_{m \in \mathbb{Z}^r} \int_{2-i\infty}^{2+i\infty} \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} \prod_{k=1}^{r+1} Y_k(s - iE_k(m)) ds \\ &= \sum_{m \in \mathbb{Z}^r} \sum_{\gamma^{(m)}} \prod_{k=1}^{r+1} Y_k\left(\frac{1}{2} + i(\gamma^{(m)} - E_k(m))\right) \\ &\quad + \sum_{m \in \mathbb{Z}^r} \int_{1/3-i\infty}^{1/3+i\infty} \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} \prod_{k=1}^{r+1} Y_k(s - iE_k(m)) ds \\ &\ll \sum_{m \in \mathbb{Z}^r} \sum_{\gamma^{(m)}} \left| \prod_{k=1}^{r+1} \left\{ \Gamma\left(e_k\left(\frac{1}{2} + i(\gamma^{(m)} - E_k(m))\right)\right) x_k^{e_k(1/2 + i(\gamma^{(m)} - E_k(m)))} \right\} \right| \\ &\quad + X^{1/3} \sum_{m \in \mathbb{Z}^r} \log(N\mathfrak{q}|E(m)|) \int_{-\infty}^{\infty} \prod_{k=1}^{r+1} e^{-\pi|t - E_k(m)|/2} dt. \end{aligned}$$

By the well known estimate $\Gamma(\sigma + it) \ll |t|^{\sigma-1/2} e^{-\pi|t|/2}$,

$$\begin{aligned} S &\ll X^{1/2} \left(\sum_{m \in \mathbb{Z}^r} \sum_{\gamma^{(m)}} \prod_{k=1}^{r+1} |\gamma^{(m)} - E_k(m)|^{e_{k-1}/2} e^{-\pi|\gamma^{(m)} - E_k(m)|/2} \right) \\ &\quad + X^{1/3} \sum_{m \in \mathbb{Z}^r} \log(N\mathfrak{q}|E(m)|) \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-\pi|l - E_k(m)|/2} \end{aligned}$$

$$\begin{aligned} &\ll X^{1/2} \sum_{m \in \mathbb{Z}^r} \sum_{\gamma^{(m)}} \prod_{k=1}^{r+1} e^{-|\gamma^{(m)} - E_k(m)|/2} \\ &\quad + X^{1/3} \sum_{m \in \mathbb{Z}^r} \log(N\mathfrak{q}|E(m)|) \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-\pi|l - E_k(m)|/2} \\ &=: X^{1/2} S_1 + X^{1/3} S_2. \end{aligned}$$

We use Lemma 3 to estimate S_1 as follows:

$$\begin{aligned} S_1 &= \sum_{m \in \mathbb{Z}^r} \sum_{\gamma^{(m)}} \prod_{k=1}^{r+1} e^{-|\gamma^{(m)} - E_k(m)|/2} \\ &\ll \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \sum_{l < \gamma^{(m)} \leq l+1} \prod_{k=1}^{r+1} e^{-|\gamma^{(m)} - E_k(m)|/2} \\ &\ll \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-|l - E_k(m)|/2} \sum_{l < \gamma^{(m)} \leq l+1} 1 \\ &\ll \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-|l - E_k(m)|/2} \log(N\mathfrak{q}|E(m)|(|l| + 1)^n) \\ &\ll \log N\mathfrak{q} \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-|l - E_k(m)|/2} \\ &\quad + \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-|l - E_k(m)|/2} \log(|l| + 1)^n \\ &\quad + \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-|l - E_k(m)|/2} \log(|E(m)|) \\ &=: S_{11} \log(N\mathfrak{q}) + S_{12} + S_{13}. \end{aligned}$$

For S_{11} , by Lemma 6, we have

$$\begin{aligned} S_{11} &= \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-|l - E_k(m)|/2} \\ &\ll \sum_{w \in \mathbb{Z}^{r+1}} \prod_{k=1}^{r+1} e^{-|w_k|/2} \sum_{\substack{m \in \mathbb{Z}^r \\ l \in \mathbb{Z} \\ w_k \leq l - E_k(m) \leq w_k + 1}} 1 \\ &\ll R \sum_{w \in \mathbb{Z}^{r+1}} \prod_{k=1}^{r+1} e^{-|w_k|/2} \ll R. \end{aligned}$$

For S_{12} , we see that

$$\begin{aligned}
 S_{12} &= \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^{r+1} e^{-|l-E_k(m)|/2} \log(|l| + 1) \\
 &\ll \sum_{m \in \mathbb{Z}^r} \sum_{|l| \geq |E_{r+1}(m)|} e^{-(|l|-|E_{r+1}(m)|)/2} \log(|l| + 1) \prod_{k=1}^r e^{-(|l-E_k(m)|)/2} \\
 &\quad + \sum_{m \in \mathbb{Z}^r} \sum_{|l| < |E_{r+1}(m)|} e^{(|l|-|E_{r+1}(m)|)/2} \log(|E_{r+1}(m)| + 1) \prod_{k=1}^r e^{-(|l-E_k(m)|)/2} \\
 &\ll \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^r e^{-(|l-E_k(m)|)/2} (e^{-|l|/3+|E_{r+1}(m)|/2} + e^{|l|/2-|E_{r+1}(m)|/3}) \\
 &\ll \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \prod_{k=1}^r e^{-(|l-E_k(m)|)/2} \left(\sum_{u=0}^1 e^{(-1)^u l/3+E_{r+1}(m)/2} \right. \\
 &\quad \left. + \sum_{u=0}^1 e^{|l|/2+(-1)^u E_{r+1}(m)/3} \right) \\
 &\ll \sum_{u=0}^1 \sum_{m \in \mathbb{Z}^r} \sum_{l \in \mathbb{Z}} \left(e^{(-1)^u l/3+E_{r+1}(m)/2} \prod_{k=1}^r e^{-(|l-E_k(m)|)/2} \right. \\
 &\quad \left. + e^{|l|/2+(-1)^u E_{r+1}(m)/3} \prod_{k=1}^r e^{-(|l-E_k(m)|)/2} \right) \ll R.
 \end{aligned}$$

The last inequality is achieved by the same argument applied to S_{11} . Similarly, we obtain $S_{13} \ll R$, $S_2 \ll R \log(N\mathfrak{q})$. Thus,

$$(17) \quad S \ll X^{1/2} R \log(N\mathfrak{q}).$$

Applying the Perron formula (10) and (17), we obtain for a nonprincipal character χ :

$$\begin{aligned}
 &\sum_{\alpha > 0} \chi(\alpha) A(\alpha) \Phi(|\alpha|x^{-1}) \\
 &\ll \frac{\omega 2^{r_2}}{R} \max_{\psi} \sum_{m \in \mathbb{Z}^r} \int_{2-i\infty}^{2+i\infty} \frac{\zeta'(s, \lambda_m \chi \psi)}{\zeta(s, \lambda_m \chi \psi)} \prod_{k=1}^{r+1} Y_k(s - iE_k(m)) ds \\
 &\ll_K X^{1/2} \log(N\mathfrak{q}).
 \end{aligned}$$

If $\lambda_m \chi \psi$ is principal, then $\zeta'(s, \lambda_m \chi \psi) / \zeta(s, \lambda_m \chi \psi)$ has poles at $s = 0, 1$ with residue -1 by (14) and (15). When $\lambda_m \chi \psi$ is principal, it can be easily seen that the means χ, λ_m, ψ are all principal. Using again the Perron

formula (10) and Cauchy’s theorem, we obtain

$$\begin{aligned} &\sum_{\alpha \succ 0} \chi(\alpha) \Lambda(\alpha) \Phi(|\alpha|x^{-1}) \\ &= -\frac{\omega 2^{r_2-r_1}}{hR} \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{\zeta'(s, 1)}{\zeta(s, 1)} \prod_{k=1}^{r+1} Y_k(s) ds \\ &\quad - \frac{\omega 2^{r_2-r_1}}{hR} \sum_{\psi} \sum_{m \in \mathbb{Z}^r}^* \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{\zeta'(s, \lambda_m \chi^\psi)}{\zeta(s, \lambda_m \chi^\psi)} \prod_{k=1}^{r+1} Y_k(s - iE_k(m)) ds, \end{aligned}$$

where $\sum_{m \in \mathbb{Z}^r}^*$ denotes that $\lambda_m \chi^\psi$ runs over nonprincipal Hecke Grössen-characters.

Arguing as above, we find that

$$\sum_{\alpha \succ 0} \chi(\alpha) \Lambda(\alpha) \Phi(|\alpha|x^{-1}) = \frac{\omega 2^{r_2-r_1}}{hR} X + O_K(X^{1/2} \log(N\mathfrak{q}))$$

for a principal character χ . This proves Theorem 1.

5. The least primitive root. For $(\alpha, q) = 1$, denote by $\text{ind } \alpha$ the index modulo \mathfrak{q} with respect to a fixed primitive root g , i.e. $\alpha \equiv g^{\text{ind } \alpha} \pmod{\mathfrak{q}}$. If $d \mid \phi(N\mathfrak{q})$, then

$$\begin{aligned} G_d(x) &:= \sum_{\substack{\text{ind } \alpha \equiv 0 \pmod{d} \\ \alpha \succ 0}} \Lambda(\alpha) \Phi(|\alpha|x^{-1}) = \frac{1}{d} \sum_{\alpha \succ 0} \Lambda(\alpha) \Phi(|\alpha|x^{-1}) \sum_{\chi_d} \chi_d(\alpha) \\ &= \frac{1}{d} \sum_{\substack{\alpha \succ 0 \\ (\alpha, \mathfrak{q})=1}} \Lambda(\alpha) \Phi(|\alpha|x^{-1}) + \frac{1}{d} \sum_{\chi_d}^* \sum_{\alpha \succ 0} \chi_d(\alpha) \Lambda(\alpha) \Phi(|\alpha|x^{-1}), \end{aligned}$$

where $\sum_{\chi_d}^*$ means that χ_d runs over all nonprincipal characters modulo \mathfrak{q} that satisfy $\chi_d^d = \chi_0$. By Theorem 1, we have

$$(18) \quad G_d(x) = \frac{1}{d} \sum_{\alpha \succ 0} \Lambda(\alpha) \Phi(|\alpha|x^{-1}) + O(X^{1/2} \log(N\mathfrak{q})).$$

Let $I_c(x) := \{\alpha \succ 0 \mid |\alpha^{(k)}| \leq cx_k\}$ as in (3). One can assume for the convenience of computation that

$$c'_0 x^{e_k/n} \leq x_k \leq c'_1 x^{e_k/n}, \quad k = 1, \dots, r + 1,$$

where the positive constants c'_0, c'_1 depend on the field K only. This assumption can be justified by multiplying a suitably chosen totally positive unit $\varepsilon \in K$ (see proof in [5, p. 62, (13)]). If $\alpha \notin I_c(x)$, then there exists k such that $|\alpha^{(k)}| > cx_k$. For convenience, we assume that $k = 1$. Taking

$x' = (2x_1, x_2, \dots, x_{r+1})$, we apply partial summation with respect to $|\alpha^{(1)}|$:

$$(19) \quad \sum_{\substack{|\alpha^{(1)}| > cx_1 \\ \alpha > 0}} \Lambda(\alpha)\Phi(|\alpha|x^{-1}) = \sum_{\substack{|\alpha^{(1)}| > cx_1 \\ \alpha > 0}} \Lambda(\alpha)\Phi(|\alpha|(x')^{-1})e^{-|\alpha^{(1)}|x_1^{-1}/2} \leq C'_1 X e^{-c/2},$$

where C'_1 is an absolute constant only depending on K that is derived from the inequality

$$(20) \quad C_0 X \leq \sum_{\alpha > 0} \Lambda(\alpha)\Phi(|\alpha|x^{-1}) \leq C_1 X,$$

which follows from Theorem 1. Hence,

$$(21) \quad \sum_{\substack{\alpha \notin I_{c_0}(x) \\ \alpha > 0}} \Lambda(\alpha)\Phi(|\alpha|x^{-1}) \leq C_2 X e^{-c_0/2}$$

with $C_2 = nC_1$ depending only on K as well.

Let

$$P := \prod_{p|\phi(N\mathfrak{q})} p, \quad P_1 = \prod_{\substack{p|\phi(N\mathfrak{q}) \\ p < c_1 m \log 4m}} p \quad (c_1 \geq 2),$$

where $m = \omega(\phi(N\mathfrak{q}))$. It is easily seen that α is a primitive root modulo \mathfrak{q} if $(\text{ind } \alpha, P) = 1$. We consider the summation over primitive roots as follows:

$$(22) \quad \begin{aligned} N(x) &:= \sum_{\substack{(\text{ind } \alpha, P)=1 \\ \alpha > 0}} \Lambda(\alpha)\Phi(|\alpha|x^{-1}) \\ &\geq \sum_{\substack{(\text{ind } \alpha, P_1)=1 \\ \alpha > 0}} \Lambda(\alpha)\Phi(|\alpha|x^{-1}) - \sum_{\substack{p|\phi(N\mathfrak{q}) \\ p > c_1 m \log 4m}} G_p(x) \\ &= M(x) - \sum_{\substack{p|\phi(N\mathfrak{q}) \\ p > c_1 m \log 4m}} \frac{1}{p} \sum_{\alpha > 0} \Lambda(\alpha)\Phi(|\alpha|x^{-1}) + O(mX^{1/2} \log(N\mathfrak{q})) \\ &= M(x) - H(x) \left(\sum_{\substack{p|\phi(N\mathfrak{q}) \\ p > c_1 m \log 4m}} \frac{1}{p} \right) + O(mX^{1/2} \log(N\mathfrak{q})), \end{aligned}$$

where

$$M(x) := \sum_{\substack{(\text{ind } \alpha, P_1)=1 \\ \alpha > 0}} \Lambda(\alpha)\Phi(|\alpha|x^{-1}), \quad H(x) := \sum_{\alpha > 0} \Lambda(\alpha)\Phi(|\alpha|x^{-1}).$$

We now quote a lemma from [11, Lemma 4] that is based on the sieve method:

LEMMA 7. *Let Γ be an index set, and $L : \Gamma \rightarrow \mathbb{Z}$ and $W : \Gamma \rightarrow \mathbb{R}^+$ be such that*

$$S_d := \sum_{\substack{\gamma \in \Gamma \\ L(\gamma) \equiv 0 \pmod{d}}} W(\gamma)$$

exists for any d and satisfies

$$S_d = \frac{M}{d} + O(N).$$

Let p_1, \dots, p_r be distinct primes with $Q = p_1 \cdots p_r$. Then

$$T := \sum_{\substack{\gamma \in \Gamma \\ (L(\gamma), Q) = 1}} W(\gamma) \geq C'_3 M \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) + O(p_r^{2.99} N),$$

with an absolute positive constant C'_3 .

Applying Lemma 7 with $T = M(x)$ and $Q = P_1$, from (18) we obtain

$$\begin{aligned} M(x) &\geq C'_3 \prod_{p|P_1} \left(1 - \frac{1}{p}\right) H(x) + O((c_1 m)^{2.991} X^{1/2} \log(N\mathfrak{q})) \\ &\geq \frac{C_3}{\log(c_1 m)} H(x) + O((c_1 m)^{2.991} X^{1/2} \log(N\mathfrak{q})), \end{aligned}$$

where C_3 is an absolute constant.

Taking c_1 sufficiently large, from (20) and (22) we obtain

$$\begin{aligned} N(x) &\geq \frac{C_3 C_0}{\log c_1 \log 4m} X - \frac{C_1}{c_1 \log 4m} X + O((c_1 m)^{2.991} X^{1/2} \log(N\mathfrak{q})) \\ &\geq \frac{C_4}{\log c_1 \log 4m} X + O((c_1 m)^{2.991} X^{1/2} \log(N\mathfrak{q})), \end{aligned}$$

with an absolute positive constant C_4 .

Finally, we split $N(x)$ into two sums:

$$N(x) = \sum_{\substack{\alpha \in I_{c_0}(x) \\ \alpha > 0}} A(\alpha) \Phi(|\alpha|x^{-1}) + \sum_{\substack{\alpha \notin I_{c_0}(x) \\ \alpha > 0}} A(\alpha) \Phi(|\alpha|x^{-1}) := \sum_1 + \sum_2.$$

By (21), $\sum_2 \leq C_2 X e^{-c_0/2}$. Taking $c_0 = c_2 \log 4m$ with a sufficiently large $c_2 = c_2(c_1)$, we have

$$\sum_1 \geq \frac{C}{\log c_1 \log 4m} X + O((c_1 m)^{2.991} X^{1/2} \log(N\mathfrak{q}))$$

with an absolute constant C . Hence, there exists a constant c such that if $X = cm^{5.99} \log^2(N\mathfrak{q})$, then $\sum_1 > 0$. This proves Theorem 2.

Acknowledgements. The first author expresses his gratitude to Professor Wang Yuan for proposing him the problem and steady encouragement.

References

- [1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), 179–192.
- [2] W. Grotz, *Einige Anwendungen der Siegelschen Summenformel*, Acta Arith. 38 (1980), 69–95.
- [3] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Grad. Texts in Math. 77, Springer, New York, 1981.
- [4] —, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen (II)*, Math. Z. 6 (1920), 11–51.
- [5] J. G. Hinz, *Character sums in algebraic number fields*, J. Number Theory 17 (1983), 52–70.
- [6] —, *Character sums and primitive roots in algebraic number fields*, Monatsh. Math. 95 (1983), 275–286.
- [7] B. Z. Moroz, *Analytic Arithmetic in Algebraic Number Fields*, Lecture Notes in Math. 1205, Springer, Berlin, 1986.
- [8] U. Rausch, *A summation formula in algebraic number fields and applications I*, J. Number Theory 36 (1990), 46–79.
- [9] W. Schaal, *On the expression of a number as the sum of two squares in totally real algebraic number fields*, Proc. Amer. Math. Soc. 16 (1965), 529–537.
- [10] C. L. Siegel, *Mittelwerte arithmetischer Funktionen in Zahlkörpern*, Trans. Amer. Math. Soc. 39 (1936), 219–224.
- [11] Y. Wang, *On the least primitive root of a prime*, Acta Math. Sinica 9 (1959), 432–441 (in Chinese); English version: Sci. Sinica 10 (1961), 1–14.

Department of Mathematics
Capital Normal University
Beijing 100037, P.R. China
E-mail: yhwang@mail.cnu.edu.cn
arith_wsun@sohu.com

Dolby Laboratories
San Francisco, CA, U.S.A.
E-mail: cb@dolby.com

Received on 15.12.2003
and in revised form on 6.4.2004

(4681)