

EVALUATION OF KLOOSTERMAN AND SALIÉ SUMS FOR ARBITRARY NUMBER FIELDS

INÉS PACHARONI

*CIEM - FaMAF, Universidad Nacional de Córdoba,
CP 5000 Córdoba, Argentina.
E-mail: pacharon@mate.uncor.edu*

1. INTRODUCTION

Let K be a number field with ring of integers \mathcal{O} . Let I be an ideal in \mathcal{O} and let φ, ψ be characters of the abelian group \mathcal{O}/I . We shall denote by $(\mathcal{O}/I)^\wedge$ the character group of \mathcal{O}/I .

We shall consider the following exponential sums: the generalized *Kloosterman sums* and the generalized *Salié sums* given respectively by

$$(1) \quad S(\varphi, \psi, I) = \sum_{x \in (\mathcal{O}/I)^*} \varphi(x)\psi(x^{-1})$$

$$(2) \quad T(\varphi, \psi, I) = \sum_{x \in (\mathcal{O}/I)^*} \left(\frac{x}{I}\right) \varphi(x)\psi(x^{-1})$$

where $\left(\frac{x}{I}\right)$ denotes the Legendre symbol in \mathcal{O} . Thus the Salié sums are *twisted Kloosterman sums*.

The main purpose of this paper is to give methods for the evaluation of these sums explicitly.

In [3], Theorem 1, we prove that $(\mathcal{O}/I)^\wedge$ is a cyclic \mathcal{O}/I -module, in others words there exist $\varphi \in (\mathcal{O}/I)^\wedge$ such that any character ψ is of the form $\psi(x) = (r\varphi)(x) = \varphi(rx)$ for some $r \in \mathcal{O}$.

In the case of Kloosterman sums the main result is given in Theorem 3.3. We evaluate sums of the form $S(r\varphi, r'\varphi, P^m)$ for P an odd prime ideal and $m \geq 2$. As usual, the case $m = 1$ resists any explicit evaluation. In Theorem 4.6 we evaluate Salié sums of the form $T(r\varphi, r'\varphi, I)$ for I an odd prime ideal and $(r', I) = 1$.

These results generalize to an arbitrary number field corresponding results on Salié sums and Kloosterman sums in the classical case, obtained by Sarnak and Salié respectively (cf. [2], §4.3, 4.6).

This generalization is based on results obtained in [3], which allow us to use the main ideas of the corresponding proofs in the classical case, as presented by Iwaniec, in [2].

Partially supported by CONICET, CONICOR and SeCYT-UNC..

We became interested in the evaluation of these sums because they are useful to study the spectrum of adjacency operators of euclidean graphs associated to finite rings of the form $(\mathcal{O}/I)^n$. In fact, the eigenvalues of these operators can be expressed in terms of Gauss sums and Kloosterman sums, when n is even, and Salié sums, when n is odd. Explicit evaluations of these eigenvalues are needed in order to decide when the algebra of all operators of $L^2((\mathcal{O}/I)^n)$ which commute with the group of all isometries of $(\mathcal{O}/I)^n$ is generated by a single adjacency operator. The knowledge of the above sums is also important to decide which of these graphs are Ramanujan graphs. Results in this direction will be the subject of a future publication.

2. PRELIMINARIES

2.1. Character groups of \mathcal{O}/I . Any character φ of \mathcal{O}/I can be seen as a homomorphism from \mathcal{O} to S^1 such that $I \subset \ker \varphi$.

We proved in [3] Theorem 1, that there exist $\varphi \in (\mathcal{O}/I)^\wedge$ such that any character ψ can be written in the form $\psi(x) = r\varphi(x)$, with $r \in \mathcal{O}$. Characters φ with this property are called generators of $(\mathcal{O}/I)^\wedge$ and they are characterized by the condition that no proper divisor of I is contained in $\ker \varphi$. Moreover, $\psi = r\varphi$ is also a generator of $(\mathcal{O}/I)^\wedge$ if and only if $(r, I) = 1$.

2.2. Gauss sums. Our evaluations of Salié sums and Kloosterman sums involve the following *Gauss sums* associated to an integral ideal I and $\varphi \in (\mathcal{O}/I)^\wedge$:

$$(3) \quad G(\varphi, I) = \sum_{x \in \mathcal{O}/I} \varphi(x^2).$$

Hecke, in [1], considers Gauss sums in a number field K associated to an element $\omega \in K$. Let \mathfrak{d} be the different ideal of K . So there exist $\mathfrak{a}, \mathfrak{b}$ relative prime integral ideals such that $(\omega) = \frac{\mathfrak{b}}{\mathfrak{d}\mathfrak{a}}$. The Gauss sum considered by Hecke is

$$(4) \quad C(\omega) = \sum_{x \in \mathcal{O}/\mathfrak{a}} e^{2\pi i \text{Tr}(\omega x^2)}.$$

Both definitions coincide in the following way: Given $(\omega) = \frac{\mathfrak{b}}{\mathfrak{d}\mathfrak{a}}$, let $I = \mathfrak{a}$ and let $\varphi \in (\mathcal{O}/I)^\wedge$ be the character defined by $\varphi(x) = e^{2\pi i \text{Tr}(\omega x)}$. Then $C(\omega) = G(\varphi, I)$. Reciprocally, given an ideal I and an element $\omega \in \frac{1}{\mathfrak{d}I}$, we have $(\omega) = \frac{\mathfrak{b}}{\mathfrak{d}\mathfrak{a}}$. The map $\psi_\omega : x \mapsto e^{2\pi i \text{Tr}(\omega x)}$ defines a character in \mathcal{O}/I . Moreover any character in \mathcal{O}/I is of this form for some ω . Choosing ω such that $\varphi = \psi_\omega$ we have $G(\varphi, I) = C(\omega)$.

Now we describe the main properties of Gauss sums. In most of the cases we refer to [1] for the proofs.

If $I = AB$ with A, B coprime ideals then $\mathcal{O}/I \simeq \mathcal{O}/A \times \mathcal{O}/B$ (Chinese remainder theorem); correspondingly any $\varphi \in (\mathcal{O}/I)^\wedge$ is of the form $\varphi = \varphi_1 \times \varphi_2$ where $\varphi_1 \in (\mathcal{O}/A)^\wedge$ and $\varphi_2 \in (\mathcal{O}/B)^\wedge$.

Lemma 2.1. *If $I = AB$ with A, B coprime ideals and $\varphi = \varphi_1 \times \varphi_2$ then*

$$G(\varphi, I) = G(\varphi_1, A) G(\varphi_2, B).$$

In a number field an integer ideal is said to be *odd* if it is coprime with the ideal (2). We restrict ourselves to odd ideals.

For an odd prime ideal the Legendre symbol is given by (see [1] §54)

$$\left(\frac{x}{P}\right) = \begin{cases} 1 & \text{if } x \text{ is a quadratic residue mod } P. \\ -1 & \text{if } x \text{ is not a quadratic residue mod } P. \\ 0 & \text{if } (x, P) \neq 1. \end{cases}$$

The definition extends to any odd ideal I in the following way: If $I = \prod_j P_j^{a_j}$, with P_j prime ideals we define $\left(\frac{x}{I}\right) = \prod_j \left(\frac{x}{P_j}\right)^{a_j}$.

Lemma 2.2. *Let P be an odd prime ideal and let $\varphi \in (\mathcal{O}/P)^\wedge$ be non trivial. Then*

$$G(\varphi, P) = \sum_{x \in (\mathcal{O}/P)^*} \left(\frac{x}{P}\right) \varphi(x)$$

Proof. See (171) in [1].

Proposition 2.3. *Let P be an odd prime ideal, and φ a non trivial character in \mathcal{O}/P . Let $\varepsilon_P = \begin{cases} 1 & \text{if } N(P) \equiv 1 \pmod{4}, \\ i & \text{if } N(P) \equiv 3 \pmod{4}. \end{cases}$*

Then

$$G(\varphi, P) = \varepsilon_P N(P)^{\frac{1}{2}} \quad \text{or} \quad G(\varphi, P) = -\varepsilon_P N(P)^{\frac{1}{2}}.$$

Proof.

$$\begin{aligned} G(\varphi, P)^2 &= \sum_{x, y \in (\mathcal{O}/P)^*} \left(\frac{x}{P}\right) \left(\frac{y}{P}\right) \varphi(x+y) = \\ &= \sum_{t \in (\mathcal{O}/P)^*} \left(\frac{t}{P}\right) \sum_{x \in (\mathcal{O}/P)^*} \varphi(x(1+t)) \end{aligned}$$

The inner sum is equal to $N(P) - 1$ if $1+t \equiv 0 \pmod{P}$, otherwise it is equal to -1 . Thus

$$G(\varphi, P)^2 = \left(\frac{-1}{P}\right) (N(P) - 1) - \sum_{t \neq -1} \left(\frac{t}{P}\right).$$

In \mathcal{O}/P there exists an equal number of quadratic residues and non quadratic residues. Hence $\sum_{t \in (\mathcal{O}/P)^*} \left(\frac{t}{P}\right) = 0$ and therefore

$$G(\varphi, P)^2 = \left(\frac{-1}{P}\right) (N(P) - 1) + \left(\frac{-1}{P}\right) = \left(\frac{-1}{P}\right) N(P).$$

Moreover $\left(\frac{-1}{P}\right) \equiv (-1)^{\frac{N(P)-1}{2}} \pmod{P}$. Then $\left(\frac{-1}{P}\right) = 1$ or -1 according to $N(P) \equiv 1 \pmod{4}$ or $N(P) \equiv 3 \pmod{4}$.

Remark. We define the *sign* of the Gauss sum $G(\varphi, P)$, and denote it by s_φ , as the number 1 or -1 such that

$$G(\varphi, P) = s_\varphi \varepsilon_P N(P)^{\frac{1}{2}}.$$

We shall see in Corollary 2.6 that there exists a non trivial character φ such that $s_\varphi = 1$.

Proposition 2.4. *Let P be an odd prime ideal, $k \in \mathbb{N}$ and φ a generator of $(\mathcal{O}/P^k)^\wedge$. We have*

- i) *If $k = 2m$ then $G(\varphi, P^k) = N(P)^m$.*
- ii) *If $k = 2m + 1$, let $p \in P \setminus P^2$ and $\psi = p^{2m}\varphi \in (\mathcal{O}/P)^\wedge$. Then*

$$G(\varphi, P^k) = N(P)^m G(\psi, P).$$

Proof. Let $k \geq 2$. If s (respectively t) runs through a complete system of representatives of \mathcal{O}/P^{k-1} (respectively P^{k-1}/P^k) then $s + t$ runs through a complete system of representatives of \mathcal{O}/P^k . Thus,

$$G(\varphi, P^k) = \sum_{s \in \mathcal{O}/P^{k-1}} \varphi(s^2) \sum_{t \in P^{k-1}/P^k} \varphi(2st)$$

The map $t \mapsto \varphi(2st)$ defines a character of the group P^{k-1}/P^k . It is the trivial character if and only if $s \in P$. By the orthogonality relations in P^{k-1}/P^k we have

$$G(\varphi, P^k) = N(P) \sum_{s \in P/P^{k-1}} \varphi(s^2).$$

We fix $p \in P \setminus P^2$. The map $u \mapsto pu$ defines an isomorphism of abelian groups from \mathcal{O}/P^{k-2} onto P/P^{k-1} . Therefore

$$G(\varphi, P^k) = N(P) \sum_{u \in \mathcal{O}/P^{k-2}} \varphi(p^2 u^2) = N(P) G(p^2 \varphi, P^{k-2}).$$

By repeated application of this formula we complete the proof of the proposition.

For k odd and any character $\varphi \in (\mathcal{O}/P^k)^\wedge$ we extend the definition of s_φ given above:

$$(5) \quad s_\varphi = \frac{G(\varphi, P^k)}{\varepsilon_P N(P)^{k/2}}$$

By Propositions 2.3 and 2.4 we have $s_\varphi \in \{1, -1\}$. Moreover if $\psi = p^{k-1}\varphi$ with $p \in P \setminus P^2$ then $s_\varphi = s_\psi$.

Proposition 2.5. *Let φ be a generator of $(\mathcal{O}/I)^\wedge$ and let $r \in \mathcal{O}$ be relative prime with I . Then*

$$G(r\varphi, I) = \left(\frac{r}{I}\right) G(\varphi, I).$$

Proof. See Theorem 155 in [1].

Corollary 2.6. *Let P be an odd prime ideal. Then there exists λ a generator of $(\mathcal{O}/P)^\wedge$ such that*

$$G(\lambda, P) = \varepsilon_P N(P)^{\frac{1}{2}}.$$

Proof. If φ generates $(\mathcal{O}/P)^\wedge$ and satisfies $G(\varphi, P) = -\varepsilon_P N(P)^{1/2}$, we take $\lambda = a\varphi$ for any a , a non quadratic residue mod P . Then

$$G(a\varphi, P) = \left(\frac{a}{P}\right) G(\varphi, P) = \varepsilon_P N(P)^{1/2}.$$

3. KLOOSTERMAN SUMS

Kloosterman sums have the following multiplicative property (see [3]): Let $I = P_1^{n_1} \cdots P_r^{n_r}$ and let $\varphi, \psi \in (\mathcal{O}/I)^\wedge$. We write the characters φ, ψ in the form $\varphi = \times_1^r \varphi_j$ and $\psi = \times_1^r \psi_j$ where $\varphi_j, \psi_j \in (\mathcal{O}/P_j^{n_j})^\wedge$. Then

$$S(\varphi, \psi, I) = \prod_{j=1}^r S(\varphi_j, \psi_j, P_j^{n_j}).$$

Therefore we may restrict ourself to evaluate Kloosterman sums of the form $S(\varphi, \psi, P^m)$ with P a prime ideal. In this section we shall consider the case where P is an odd prime ideal and $m \geq 2$.

Lemma 3.1. *Let P be an odd prime ideal, $m \geq 1$ and let φ be a generator of $(\mathcal{O}/P^{2m})^\wedge$. Then*

$$S(\varphi, \varphi, P^{2m}) = 2N(P)^m \operatorname{Re}(\varphi(2)).$$

Proof. (cf. [2], Lemma 4.1) If x runs through $(\mathcal{O}/P^{2m})^*$ and y runs through P^m/P^{2m} , then $x(1+y)$ runs, $N(P)^m$ times, through $(\mathcal{O}/P^{2m})^*$. Moreover in \mathcal{O}/P^{2m} the inverse of $x(1+y)$ is the element $x^{-1}(1-y)$. Hence

$$\begin{aligned} S(\varphi, \varphi, P^{2m}) &= \sum_{x \in (\mathcal{O}/P^{2m})^*} \varphi(x + x^{-1}) \\ &= N(P)^{-m} \sum_{x \in (\mathcal{O}/P^{2m})^*} \sum_{y \in P^m/P^{2m}} \varphi(x(1+y) + x^{-1}(1-y)) \\ &= N(P)^{-m} \sum_{x \in (\mathcal{O}/P^{2m})^*} \varphi(x + x^{-1}) \sum_{y \in P^m/P^{2m}} \varphi((x - x^{-1})y) \end{aligned}$$

The character φ generates $(\mathcal{O}/P^{2m})^\wedge$, then the ideals P^j with $j < 2m$ are not contained in $\ker \varphi$ (Proposition 2, in [3]). Thus by the orthogonality relations between characters in the group P^m/P^{2m} , the inner sum is zero if $x - x^{-1} \not\equiv 0 \pmod{P^m}$; otherwise it is $N(P)^m$.

If $x \in \mathcal{O}/P^{2m}$ satisfies the equations $xx^{-1} \equiv 1 \pmod{P^{2m}}$ and $x \equiv x^{-1} \pmod{P^m}$ then $x^2 \equiv 1 \pmod{P^m}$. Since P is relative prime to (2) , we have that $x \equiv 1 \pmod{P^m}$ or $x \equiv -1 \pmod{P^m}$. Thus x is of the form

$$x = 1 + t \quad \text{or} \quad x = -1 + t$$

where t is any element of P^m/P^{2m} . In this way we have

$$\begin{aligned} S(\varphi, \varphi, P^{2m}) &= \sum_{\substack{x \in (\mathcal{O}/P^{2m})^* \\ x \equiv x^{-1} \pmod{P^m}}} \varphi(x + x^{-1}) = \sum_{t \in P^m/P^{2m}} (\varphi(2) + \varphi(-2)) \\ &= 2N(P)^m \operatorname{Re}(\varphi(2)) \end{aligned}$$

Lemma 3.2. *Let P be an odd prime ideal, $m \geq 1$ and let λ be a generator of $(\mathcal{O}/P^{2m+1})^\wedge$ such that $s_\lambda = 1$. Let $\varphi = r\lambda$, with $(r, P) = 1$. Then*

$$S(\varphi, \varphi, P^{2m+1}) = 2N(P)^{m+1/2} \left(\frac{r}{P}\right) \operatorname{Re}(\varepsilon_P \varphi(2))$$

where ε_P was defined in Proposition 2.3.

Note. See (5) for the definition of s_λ .

Proof. (cf. [2], Lemma 4.2) If x runs through $(\mathcal{O}/P^{2m+1})^*$ and y runs through P^{m+1}/P^{2m+1} , then $x(1+y)$ runs through $(\mathcal{O}/P^{2m+1})^*$, $N(P)^m$ times. Thus

$$S(\varphi, \varphi, P^{2m+1}) = \sum_{\substack{x \in (\mathcal{O}/P^{2m+1})^* \\ x \equiv x^{-1} \pmod{P^m}}} \varphi(x + x^{-1})$$

In \mathcal{O}/P^{2m+1} the solutions of the equations $xx^{-1} \equiv 1 \pmod{P^{2m+1}}$ and $x \equiv x^{-1} \pmod{P^{m+1}}$ are of the form $x = \pm 1 + t$ where $t \in P^{m+1}/P^{2m+1}$. We have $(1+t)^{-1} = 1 - t + t^2$ and $(-1+t)^{-1} = -1 - t - t^2$. So $x + x^{-1} = \pm(2 + t^2)$. Therefore,

$$\begin{aligned} S(\varphi, \varphi, P^{2m+1}) &= \sum_{t \in P^m/P^{2m+1}} \varphi(2 + t^2) + \varphi(-(2 + t^2)) \\ &= 2 \operatorname{Re} \left(\varphi(2) \sum_{t \in P^m/P^{2m+1}} \varphi(t^2) \right) \end{aligned}$$

Putting $t = t_1 + t_2$, with $t_1 \in P^m/P^{m+1}$ and $t_2 \in P^{m+1}/P^{2m+1}$ we have $t^2 \equiv t_1^2 \pmod{P^{2m+1}}$. Then

$$\sum_{t \in P^m/P^{2m+1}} \varphi(t^2) = N(P)^m \sum_{t_1 \in P^m/P^{m+1}} \varphi(t_1^2).$$

This sum is a Gauss sum in \mathcal{O}/P , by any isomorphism $P^m/P^{m+1} \simeq \mathcal{O}/P$, and it is equal to $\left(\frac{r}{P}\right) \varepsilon_P N(P)^{1/2}$ because $s_\lambda = 1$ and $\varphi = r\lambda$. Then

$$\begin{aligned} S(\varphi, \varphi, P^{2m+1}) &= 2N(P)^m \operatorname{Re} \left(\varphi(2) \left(\frac{r}{P}\right) \varepsilon_P N(P)^{\frac{1}{2}} \right) \\ &= 2N(P)^{m+\frac{1}{2}} \left(\frac{r}{P}\right) \operatorname{Re}(\varepsilon_P \varphi(2)). \end{aligned}$$

Theorem 3.3. *Let P be an odd prime ideal, $m \geq 2$, and let φ a generator of $(\mathcal{O}/P^m)^\wedge$ with $s_\varphi = 1$. We denote*

$$\varepsilon_{m,P} = \begin{cases} \varepsilon_P & \text{if } m \text{ is odd} \\ 1 & \text{if } m \text{ is even} \end{cases}.$$

Let $r, r' \in \mathcal{O}$ with $(rr', P) = 1$. Then

- i) $S(r\varphi, r'\varphi, P^m) = 0$ if $r \not\equiv r'\ell^2 \pmod{P^m}$, for any $\ell \in \mathcal{O}$.
- ii) $S(r\varphi, r\ell^2\varphi, P^m) = 2N(P)^{\frac{m}{2}} \left(\frac{r\ell}{P^m}\right) \operatorname{Re}(\varepsilon_{m,P}\varphi(2r\ell))$.

Proof. i) Let $k \in \mathcal{O}$. By Lemma 6 in [3] we have

$$S(\varphi, k\varphi, P^m) = \sum_{s \in (\mathcal{O}/P^{m-1})^*} \varphi(s + ks^{-1}) \sum_{t \in P^{m-1}/P^m} \varphi((1 - ks^{-2})t).$$

Hence

$$S(\varphi, k\varphi, P^m) = 0 \text{ if } \left(\frac{k}{P}\right) = -1.$$

Furthermore if $\left(\frac{k}{P}\right) = 1$ then $k \equiv \ell^2 \pmod{P^m}$ for some $\ell \in \mathcal{O}$. In fact if k is a residue quadratic mod P then $k \equiv s^2 + t \pmod{P^m}$ for some $t \in P^{m-1}$. Thus $k \equiv (s + \tilde{t})^2 \pmod{P^m}$ where $\tilde{t} \in P^{m-1}$ satisfies $2\tilde{t} \equiv t \pmod{P^{m-1}}$.

Therefore $S(r\varphi, r'\varphi, P^m) = S(\varphi, rr'\varphi, P^m) = 0$ if $rr' \not\equiv k^2 \pmod{P^m}$ or equivalently if $r \not\equiv r'\ell^2 \pmod{P^m}$, for any $\ell \in \mathcal{O}$.

ii) We have $S(r\varphi, r\ell^2\varphi, P^m) = S(r\ell\varphi, r\ell\varphi, P^m)$. Hence the statement follows from Lemmas 3.1 and 3.2.

4. SALIÉ SUMS

In this section we study some basic properties of Salié sums and we also give an explicit evaluation of $T(r\varphi, r'\varphi, I)$ for $(2r', I) = 1$.

Lemma 4.1. *Let I be an ideal and $r \in \mathcal{O}$ coprime with I . Let φ, ψ be characters in \mathcal{O}/I . Then we have:*

- i) $T(\varphi, \psi, I) = T(\psi, \varphi, I)$.
- ii) $T(r\varphi, \psi, I) = \left(\frac{r}{I}\right) T(\varphi, r\psi, I)$.
- iii) $\overline{T(\varphi, \psi, I)} = \left(\frac{-1}{I}\right) T(\varphi, \psi, I)$.

Proof. i) If we change the variable x by $y = x^{-1}$ we have $\left(\frac{x}{I}\right) = \left(\frac{y}{I}\right)$ and then

$$T(\varphi, \psi, I) = \sum_{x \in (\mathcal{O}/I)^*} \left(\frac{x}{I}\right) \varphi(x) \psi(x^{-1}) = \sum_{y \in (\mathcal{O}/I)^*} \left(\frac{y}{I}\right) \varphi(y^{-1}) \psi(y).$$

ii) As r is coprime with I we put $y = rx$. So,

$$T(r\varphi, \psi, I) = \sum_{x \in (\mathcal{O}/I)^*} \left(\frac{x}{I}\right) \varphi(rx) \psi(x^{-1}) = \sum_{y \in (\mathcal{O}/I)^*} \left(\frac{r}{I}\right) \left(\frac{y}{I}\right) \varphi(y) \psi(ry^{-1}).$$

iii) $\overline{T(\varphi, \psi, I)} = T(-\varphi, -\psi, I) = \left(\frac{-1}{I}\right) T(\varphi, \psi, I)$.

The following lemma establishes the multiplicative property of the Salié sums.

Lemma 4.2. *Let $I = P_1^{n_1} \cdots P_r^{n_r}$ an ideal in \mathcal{O} , $\varphi, \psi \in (\mathcal{O}/I)^\wedge$, $\varphi = \times_1^r \varphi_j$, and $\psi = \times_1^r \psi_j$ with $\varphi_j, \psi_j \in (\mathcal{O}/P^{n_j})^\wedge$. Then*

$$T(\varphi, \psi, I) = \prod_{j=1}^r T(\varphi_j, \psi_j, P^{n_j}).$$

Proof. If $d = (d_1, \dots, d_r) \in \mathcal{O}/I$ then

$$\left(\frac{d}{I}\right) = \left(\frac{d_1}{P_1^{n_1}}\right) \cdots \left(\frac{d_r}{P_r^{n_r}}\right).$$

Now the proof follows in the same way as for Kloosterman sums. (Lemma 4, in [3]).

We denote by Φ the Euler phi function and by 1 the trivial character.

Proposition 4.3. *Let $I = P_1^{r_1} \cdots P_k^{r_k}$. Then*

$$T(1, 1, I) = \begin{cases} \Phi(I) & \text{if } r_i \equiv (2) \text{ for all } i, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. $f(I) = T(1, 1, I)$ is a multiplicative function. So we need only consider the following cases.

Case $I = P$. In a finite field there exists an equal number of quadratic residues and non quadratic residues. Thus $\sum_{t \in (\mathcal{O}/P)^*} \left(\frac{t}{P}\right) = 0$.

Case $I = P^{2k+1}$. By definition we have $\left(\frac{x}{P^{2k+1}}\right) = \left(\frac{x}{P}\right)^{2k+1} = \left(\frac{x}{P}\right)$. Then

$$\begin{aligned} f(I) &= \sum_{d \in \mathcal{O}/P^{2k+1}} \left(\frac{d}{P}\right) = \sum_{s \in \mathcal{O}/P} \sum_{t \in P/P^{2k+1}} \left(\frac{s+t}{P}\right) = \sum_{s \in \mathcal{O}/P} \sum_{t \in P/P^{2k+1}} \left(\frac{s}{P}\right) \\ &= N(P)^{2k} \sum_{s \in \mathcal{O}/P} \left(\frac{s}{P}\right) = N(P)^{2k} f(P) = 0. \end{aligned}$$

Case $I = P^{2k}$. As $\left(\frac{x}{P^{2k}}\right) = \left(\frac{x}{P}\right)^{2k} = 1$, then $f(P^{2k}) = \Phi(P^{2k})$.

Lemma 4.4. *Let $0 < n \leq m$ and $\varphi, \psi \in (\mathcal{O}/P^m)^\wedge$. Then*

$$T(\varphi, \psi, P^m) = \sum_{s \in (\mathcal{O}/P^n)^*} \left(\frac{s}{P}\right)^m \varphi(s) \psi(s^{-1}) \sum_{t \in P^n/P^m} \varphi(t) \psi\left(\sum_{j=2}^m (-1)^{j+1} s^{-j} t^{j-1}\right).$$

Proof. See the proof of Lemma 6 in [3].

Given $\varphi \in (\mathcal{O}/P^m)^\wedge$ we set $N_\varphi = \min\{n \geq 0 : P^n \subseteq \ker \varphi\}$, that is P_φ^N is the largest power of P on which φ is trivial.

Corollary 4.5. *Let $\varphi, \psi \in (\mathcal{O}/P^m)^\wedge$, $r_1, r_2 \in \mathcal{O}$.*

- i) If $N_\varphi \neq N_\psi$ and $\max\{N_\varphi, N_\psi\} \geq 2$, then $T(\varphi, \psi, P^m) = 0$.
- ii) If $N > 0$ is such that $N \equiv m \pmod{2}$ and $N_\varphi, N_\psi \leq N < m$, then $T(\varphi, \psi, P^m) = N(P)^{m-N} T(\varphi, \psi, P^N)$.
- iii) If $\left(\frac{r_1}{P}\right) \neq \left(\frac{r_2}{P}\right)$ then $T(r_1\varphi, r_2\varphi, P^m) = 0$.

Proof. Parts i) and ii) follow from Lema 4.4 with the same proof as in the case of Kloosterman sums (Lemma 7 in [3]). We need the condition $N \equiv m \pmod{2}$ in order to have $\left(\frac{s}{P}\right)^m = \left(\frac{s}{P}\right)^N$.

iii) We take $n = m - 1$ in Lemma 4.4. Then

$$T(r_1\varphi, r_2\varphi, P^m) = \sum_{s \in (\mathcal{O}/P^{m-1})^*} \left(\frac{s}{P}\right)^m \varphi(r_1s + r_2s^{-1}) \sum_{t \in P^{m-1}/P^m} \varphi((r_1 - r_2s^{-2})t)$$

The inner sum is zero unless $r_1 - r_2s^{-2} \in P$.

Theorem 4.6. *Let I be an odd ideal, and φ a generator of $(\mathcal{O}/I)^\wedge$. Let $r, r' \in \mathcal{O}$, r' coprime with I . Then*

$$T(r\varphi, r'\varphi, I) = \left(\frac{r'}{I}\right) G(\varphi, I) \sum_{y^2 \equiv rr' \pmod{I}} \varphi(2y).$$

Proof. (cf. [2], Lemma 4.9) We define the following functions in \mathcal{O}/I :

$$F(x) = \sum_{d \in (\mathcal{O}/I)^*} \left(\frac{d}{I}\right) \varphi(r\bar{d} + r'dx^2), \quad \hat{F}(y) = \sum_{x \in \mathcal{O}/I} F(x)\varphi(-xy)$$

where \bar{d} denotes the inverse of d module I . Then

$$\begin{aligned} \hat{F}(y) &= \sum_{x \in \mathcal{O}/I} \sum_{d \in (\mathcal{O}/I)^*} \left(\frac{d}{I}\right) \varphi(r\bar{d} + r'dx^2)\varphi(-xy) \\ &= \sum_{d \in (\mathcal{O}/I)^*} \left(\frac{d}{I}\right) \varphi(r\bar{d}) \sum_{x \in \mathcal{O}/I} \varphi(r'dx^2 - xy) \\ &= \sum_{d \in (\mathcal{O}/I)^*} \left(\frac{d}{I}\right) \varphi(r\bar{d}) \sum_{x \in \mathcal{O}/I} \varphi(r'd(x - \overline{2r'\bar{d}}y)^2) \varphi(-\overline{4r'\bar{d}}y^2) \end{aligned}$$

The last identity follows by completing the square. The inner sum can be written in terms of Gauss sums:

$$\sum_{x \in \mathcal{O}/I} \varphi(r'd(x - \overline{2r'\bar{d}}y)^2) = G(r'd\varphi, I) = \left(\frac{r'd}{I}\right) G(\varphi, I).$$

Hence

$$\hat{F}(y) = \left(\frac{r'}{I}\right) G(\varphi, I) \sum_{d \in (\mathcal{O}/I)^*} \varphi(r\bar{d})\varphi(-\overline{4r'\bar{d}}y^2).$$

Using that $(2r', I) = 1$ we change the variable $d' = \overline{4r'd}$.

$$\begin{aligned}\hat{F}(y) &= \left(\frac{r'}{I}\right)G(\varphi, I) \sum_{d \in (\mathcal{O}/I)^*} \varphi((4rr' - y^2)d) \\ &= \left(\frac{r'}{I}\right)G(\varphi, I) S[4rr' - y^2, 0, I]\end{aligned}$$

where $S[a, b, I]$ denotes the Kloosterman sum $S(a\varphi, b\varphi, I)$.

By the decomposition formula for Kloosterman sums, given in [3] (Corollary 3), we have

$$S(n\varphi, 1, I) = N(I) \sum_{\substack{J|I \\ J \subseteq \ker n\varphi}} N(J)^{-1} \mu(J),$$

where μ denotes the Möbius function.

If $J \subseteq \ker n\varphi$ then $(n)J \subseteq \ker \varphi$. So, $(n)J \subseteq I$ since φ generates $(\mathcal{O}/I)^\wedge$. Hence if $I = JJ'$ then J' divides to (n) . Therefore

$$S[(4rr' - y^2), 0, I] = \sum_{J|(4rr' - y^2, I)} N(J) \mu\left(\frac{I}{J}\right).$$

We have

$$\begin{aligned}F(x) &= N(I)^{-1} \sum_{y \in \mathcal{O}/I} \hat{F}(y) \varphi(xy) \\ &= N(I)^{-1} \sum_{y \in \mathcal{O}/I} \left(\frac{r'}{I}\right)G(\varphi, I) \sum_{J|(4rr' - y^2, I)} N(J) \mu\left(\frac{I}{J}\right) \varphi(xy) \\ &= N(I)^{-1} \left(\frac{r'}{I}\right)G(\varphi, I) \sum_{J|I} N(J) \mu\left(\frac{I}{J}\right) \sum_{\substack{y \in \mathcal{O}/I \\ y^2 \equiv 4rr'(J)}} \varphi(xy).\end{aligned}$$

If s (resp. t) runs through a system of representatives of \mathcal{O}/J (resp. J/I), then $y = s+t$ runs through a system mod I . We have $(s+t)^2 \equiv s^2 \pmod{J}$. Thus

$$\sum_{\substack{y \in \mathcal{O}/I \\ y^2 \equiv 4rr'(J)}} \varphi(xy) = \sum_{\substack{s \in \mathcal{O}/J \\ s^2 \equiv 4rr'(J)}} \sum_{t \in J/I} \varphi(xs) \varphi(xt).$$

If $(x, I) = 1$ then $x\varphi$ defines a non trivial character of the group J/I , unless $J = I$. Hence $\sum_{t \in J/I} \varphi(xt) = 0$. Therefore for any x coprime to I we have

$$F(x) = \left(\frac{r'}{I}\right)G(\varphi, I) \sum_{\substack{y \in \mathcal{O}/I \\ y^2 \equiv 4rr'(I)}} \varphi(xy).$$

We evaluate in $x = 1$ and we obtain

$$T(r\varphi, r'\varphi, I) = \left(\frac{r'}{I}\right)G(\varphi, I) \sum_{\substack{y \in \mathcal{O}/I \\ y^2 \equiv rr'(J)}} \varphi(2y).$$

The theorem is now proved.

REFERENCES

- [1] E. Hecke: *Lectures on the Theory of Algebraic Numbers*; Springer Verlag, GTM, Vol 77, 1981.
- [2] H. Iwaniec: *Topics in Classical Automorphic forms* ; Grad. Study in Math., Vol 17. Am. Math. Soc.,1997.
- [3] I. Pacharoni: *Kloosterman sums on number fields*; Commun. in Alg.26 (8), 1998, 2653-2667.