Revista de la
Unión Matemática Argentina
Volumen 40, Números 3 y 4, 1997.

PROPERTIES OF KLOOSTERMAN SUMS ON NUMBER FIELDS OF CLASS NUMBER ONE

INES PACHARONI

ABSTRACT. We study Kloosterman sums on number fields of class number one. In particular, we extend to Kloosterman sums over such fields, a decomposition formula due to Selberg in the classical case.

1. INTRODUCTION

Let F be a number field with ring of integers $\mathcal{O}$. If I is an ideal in $\mathcal{O}$, and ψ, φ are unitary characters of the finite abelian group $\mathcal{O}/I$, one defines the generalized Kloosterman sum (see [BM], §5) as

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

This includes in particular sums of the form

$$S(r,r',c) = \sum_{a\in(\mathcal{O}/(c))^*} e^{2\pi i \mathrm{Tr}(\frac{ra+r'a^{-1}}{c})} \tag{1}$$

where $c \in \mathcal{O}, c \neq 0$, $\mathrm{Tr} = \mathrm{Tr}_{F|\mathbb{Q}}$, $r, r' \in F\backslash\{0\}$ satisfy $\mathrm{Tr}(rx), \mathrm{Tr}(r'x) \in \mathbb{Z}, \forall x \in \mathcal{O}$. So $S(r,r',c) = S[\varphi_{r/c}, \varphi_{r'/c}, (c)]$, where $\varphi_q(y) = e^{2\pi i \mathrm{Tr}(qy)}$. In the case $F = \mathbb{Q}$, $r, r', c \in \mathbb{Z}$, equation (1) defines a classical Kloosterman sum (see [HW]).

The purpose of this note is to study these sums and extend many properties, satisfied by classical Kloosterman sums, to the context of number fields of class number one. As a main result we will extend to this case the following identity:

Theorem. *If $r, r' \in \mathcal{O}', c \in \mathcal{O}$ and δ is a generator of the different ideal of $\mathcal{O}$, then*

$$S(r,r',c) = \sum_{(d)|(r\delta,r'\delta,c)} |N(d)|\; S\left(\tfrac{1}{\delta}, \tfrac{\delta r r'}{d^2}, \tfrac{c}{d}\right).$$

In the case of classical Kloosterman sums (i.e. $F = \mathbb{Q}$) this identity was stated (without proof) by Selberg ([Se]). Kuznetsov ([K]) gives a proof which uses his

Partially supported by CONICET and by grants from SeCYT-UNC and CONICOR .

sum formula and the multiplicative properties of the Hecke operators. Also, R. Matthes ([Ma]) gives an elementary proof of this theorem.

The restriction to number fields of class number one, is essential in the proof of the main theorem, because only in this situation, we may reduce the proof to the case in which c is a power of a prime in $\mathcal{O}$. On the other hand, the identity in the theorem makes sense in any number field, but it does not hold as stated, if $\mathcal{O}$ is not principal ideal domain. (For example, in $\mathbb{Q}[\sqrt{-5}]$, with $r = r' = 0$ and $c = 2 - \sqrt{-5}$.) However, there is a possible attempt of generalization of the theorem to arbitrary number fields, if we sum over the ideals dividing the ideal $(r\delta, r'\delta, c)$ (not only principal ideals), and we take suitables characters. The general case is quite more complicated, and it will be the subject of a future publication.

2. Preliminaries

Since we are assuming that the class number of F is one, any $c \in \mathcal{O}$ decomposes uniquely (up to order and unit factors) as a product of irreducible elements in $\mathcal{O}$.

Notation. We shall recall some standard notation. Let $c, d \in \mathcal{O}$ we shall denote $N(c)$ the norm of c. Then $N((c)) = |N(c)|$. As usual, the greatest common divisor of c and d will be denoted by (c, d). If I is a fractionary ideal of F, we write $c \equiv d \pmod{I}$ if $c - d \in I$.

Different ideal. The ideal $\mathcal{O}' = \{q \in F \mid \mathrm{Tr}(qx) \in \mathbb{Z}, \forall x \in \mathcal{O}\}$ is a fractionary ideal of F, which coincides with the inverse of the different $\mathcal{D}_{F/\mathbb{Q}}$. The different is an integral ideal, hence there exists $\delta \in \mathcal{O}$ such that $\mathcal{D}_{F/\mathbb{Q}} = \delta\mathcal{O}$. Thus $\mathcal{O}' = \frac{1}{\delta}\mathcal{O}$, therefore any $r \in \mathcal{O}'$ can be written uniquely $r = \frac{r_1}{\delta}$, with $r_1 \in \mathcal{O}$.

Remark 2.1. We note that if $c \in \mathcal{O}, c \neq 0$, and $r, r' \in \mathcal{O}'$, then $\delta r r' \in \mathcal{O}'$. Moreover, $c | r\delta$ if and only if $\frac{r}{c} \in \mathcal{O}'$.

Characters of $\mathcal{O}/(c)$. The characters of $\mathcal{O}/(c)$ form a finite group, isomorphic to $\mathcal{O}/(c)$, hence of order $|N(c)|$.

If $c \in \mathcal{O}, r \in \mathcal{O}'$ $\varphi_{r/c} : x \mapsto e^{2\pi i \mathrm{Tr}(\frac{rx}{c})}$, defines a character on the abelian group $\mathcal{O}/(c)$, which depends on the class of r mod $c\mathcal{O}'$. We note that $\varphi_{r/c}$ is the trivial character if and only if $r \in c\mathcal{O}'$. It is easy to prove that all characters of $\mathcal{O}/(c)$ are of this form.

Remark 2.2. If c and δ are prime to each other, any character of $\mathcal{O}/(c)$ has the form $\varphi_{r/c}$, with $r \in \mathcal{O}$.

By the orthogonality relations we have

$$\sum_{x \in \mathcal{O}/(c)} e^{2\pi i Tr(\frac{r}{c}x)} = \begin{cases} |N(c)| & \text{if } r \in c\mathcal{O}' \\ 0 & \text{if } r \notin c\mathcal{O}' \end{cases}.$$

3. Properties of Kloosterman Sums

Basic properties. In this subsection we list several elementary properties of Kloosterman sums. We will leave their verification to the reader.

Lemma 1. *Let $r, r' \in \mathcal{O}'$, $c, u \in \mathcal{O}$, $c \neq 0$, u a unit. Then*

(i) $S(r, r', c) = S(r', r, c)$.
(ii) *If ϕ denotes the Euler function of F, $c \in \mathcal{O}$, and $r, r' \in c\mathcal{O}'$, then* $S(r, r', c) = S(0, 0, c) = \phi(c)$.
(iii) *If $r - r_1 \in c\mathcal{O}'$, then $S(r, r', c) = S(r_1, r', c)$.*
(iv) $S(r, r', c) = S(ru, r'u, cu)$.

Remark 3.1. Property (iii) says that the definition of $S(r, r', c)$ depends on the class of $r \pmod{c\mathcal{O}'}$. $S(r, r', c)$ is not well defined as a function of the ideal generated by c, for example, in $F = \mathbb{Q}[i]$, we have $S(1, 1, 3) = 5$ and $S(1, 1, 3i) = S(1, 2, 3) = 2$ (see §6).

Remark 3.2. If δ and c are prime to each other, then all Kloosterman sums are of the form $S(r, r', c)$ with $r, r' \in \mathcal{O}$. Moreover $S(\frac{1}{\delta}, \delta r r', c) = S(1, r r', c)$.

Notation. We shall denote $e(x) := e^{2\pi i \mathrm{Tr}(x)}$.

Lemma 2. *Let $r, r' \in \mathcal{O}'$, $c, u \in \mathcal{O}$, $c \neq 0$, u a unit. Then*

(i) *If $s \in \mathcal{O}$ is coprime to c, then $S(rs, r', c) = S(r, sr', c)$.*
(ii) $S(r, r', uc) = S(r, r'u^{-2}, c) = S(ru^{-1}, r'u^{-1}, c)$.
(iii) *If $(r\delta, c) = 1$ then $S(r, r', c) = S(\frac{1}{\delta}, \delta r r', c)$.*

Proof. (i) $S(rs, r', c) = \sum_{x \in (\mathcal{O}/(c))^*} e(\frac{rsx + r'x^{-1}}{c})$. If $(s, c) = 1$, and $\{x\}$ is a system of representatives of $(\mathcal{O}/(c))^*$, so is $\{sx\}$, hence $S(rs, r', c) = \sum e(\frac{rx + r'sx^{-1}}{c}) = S(r, sr', c)$.

(ii) and (iii) are direct consequences of (i) and Lemma 1 (iv). □

Remarks 3.3. We note that (iii) does not depend on the choice of the generator of the ideal $\mathcal{D}_{F/\mathbb{Q}}$. Also, as a particular case of Kloosterman sums, we have the (generalized) **Ramanujan sums** $S(r, 0, c)$. These sums depend on the ideal (c) and not on c.

Multiplicativity. For fixed $r, r' \in \mathcal{O}'$, Kloosterman sums are not multiplicative, but have a similar important property.

Lemma 3. *Let $r_1, r_2 \in \mathcal{O}'$ and $a, b \in \mathcal{O}$ with $(a, b) = 1$. Then*

$$S(r, r_1, a) S(r, r_2, b) = S(r, r_1 b^2 + r_2 a^2, ab).$$

Proof.

$$S(r, r_1, a) S(r, r_2, b) = \sum_{x \in (\mathcal{O}/(a))^*} \sum_{y \in (\mathcal{O}/(b))^*} e((rx + r_1 x^{-1})/a + (ry + r_2 y^{-1}/b))$$

$$= \sum_{x,y} e((r(bx + ay) + r_1 bx^{-1} + r_2 ay^{-1})/ab)$$

If x (resp. y) runs through a coprime system of representatives of $\mathcal{O}/(a)$ (resp. $\mathcal{O}/(b)$), then $z = bx + ay$ runs through a coprime system of representatives of $\mathcal{O}/(ab)$.

Let z^{-1} be the inverse of z (mod $ab\mathcal{O}$). That is, $zz^{-1} = (bx + ay)z^{-1} \equiv 1$ (mod $ab\mathcal{O}$), hence $b^2z^{-1} \equiv bx^{-1}$ (mod $ab\mathcal{O}$).

Similarly $a^2z^{-1} \equiv ay^{-1}$ (mod $ab\mathcal{O}$), hence $r_1bx^{-1}+r_2ay^{-1} - (r_1b^2+r_2a^2)z^{-1} \in ab\mathcal{O}'$ and the lemma follows easily. □

Corollary 1. *Let $r, r' \in \mathcal{O}', a, b \in \mathcal{O}$. If $(a,b) = 1$, then there exist $r_1, r_2 \in \mathcal{O}'$ such that $r' \equiv r_1b^2 + r_2a^2$ (mod $ab\,\mathcal{O}'$) and $S(r,r',ab) = S(r,r_1,a)S(r,r_2,b)$.*

Proof. Since $(a,b) = 1$, there exist $\tilde{r}_1, \tilde{r}_2 \in \mathcal{O}$ such that $r'\delta \equiv \tilde{r}_1b^2$ (mod $a\mathcal{O}$) and $r'\delta \equiv \tilde{r}_2a^2$ (mod $b\mathcal{O}$), hence $\tilde{r}_1b^2 + \tilde{r}_2a^2 \equiv r'\delta$ (mod $ab\mathcal{O}$) . Put $r_1 = \tilde{r}_1/\delta$ and $r_2 = \tilde{r}_2/\delta$, then $r_1, r_2 \in \mathcal{O}'$ and $r' \equiv r_1b^2 + r_2a^2$ (mod $ab\,\mathcal{O}'$) □

Local properties. In this subsection we consider the Kloosterman sums $S(r,r',p^m)$, where p is a prime element in $\mathcal{O}$, and $r, r' \in \mathcal{O}'$.

Lemma 4. *In the above notation we have*

(i) *If $r, r' \in p\mathcal{O}'$, then $S(r,r',p) = |N(p)| - 1$.*
(ii) *If $r \notin p\mathcal{O}'$, $r' \in p\mathcal{O}'$, then $S(r,r',p) = -1$.*
(iii) *If $r \notin p\mathcal{O}'$, then $S(r,r',p) = S(\frac{1}{\delta}, \delta rr', p)$.*

Proof. If $r' \in p\,\mathcal{O}'$, $S(r,r',p) = S(r,0,p) = \sum e(\frac{rx}{p})$ where the sum is over $(\mathcal{O}/(p))^*$. Thus, (i) and (ii) follow from the ortogonality relations. Part (iii) is a consequence of Lemma 2 (iii). □

Lemma 5. *Let p be a prime in $\mathcal{O}$, $r, r' \in \mathcal{O}'$ and $m, n \in \mathbb{N}, m > n$. Then*

$$S(r,r',p^m) =$$
$$= \sum_{s\in(\mathcal{O}/p^{m-n})^*} e\left(\frac{rs + r's^{-1}}{p^m}\right) \sum_{t\in\mathcal{O}/(p^n)} e\left(\frac{rt + r'\,(\sum_{j=1}^m (-1)^{j+1}\bar{s}^j t^{j-1})}{p^n}\right)$$

Proof. If s (resp. t) runs through a system of representatives of $\mathcal{O}/(p^{m-n})$ (resp. $(p^{m-n})/(p^m)$), then $s+t$ runs through a system of representatives of $\mathcal{O}/(p^m)$ and $s+t \in (\mathcal{O}/(p^m))^*$ if and only if $s \in (\mathcal{O}/(p^{m-n}))^*$. Furthermore, if $(s,p) = 1$ and $s\bar{s} \equiv 1\,(p^m)$, thus

$$(s+t)^{-1} \equiv \sum_{j=1}^{m} (-1)^{j+1}\bar{s}^j t^{j-1} \quad (\text{mod } p^m\mathcal{O}).$$

Moreover $(p^{m-n})/(p^m) \cong \mathcal{O}/(p^n)$.Then $S(r,r',p^m) = \sum_s \sum_t e(\frac{r(s+t)+r'(s+t)^{-1}}{p^m}) = \sum_s e(\frac{rs+r'\bar{s}^1}{p^m}) \sum_t e(\frac{rt+r'\,(\sum_{j=1}^m (-1)^{j+1}\bar{s}^j t^{j-1})}{p^n})$. □

Corollary 2. *Let p be a prime in $\mathcal{O}$, $m \geq 2$, $r, r' \in \mathcal{O}'$ such that $r \notin p\mathcal{O}'$, and $r' \in p\mathcal{O}'$, then $S(r, r', p^m) = 0$.*

Proof. Applying the previous lemma with $n = 1$, we have

$$S(r, r', p^m) = \sum_{s \in (\mathcal{O}/(p^{m-1}))^*} e\left(\frac{rs + r's^{-1}}{p^m}\right) \sum_{k \in \mathcal{O}/(p)} e\left(\frac{r}{p}k\right) e\left(\frac{-r'}{p}s^{-2}k\right).$$

By the orthogonality relations, we have that each inner sum is equal to zero. $\square$

Corollary 3. *If $r, r' \in p\mathcal{O}'$, and $m \geq 2$, then $S(r, r', p^m) = |N(p)| S(\frac{r}{p}, \frac{r'}{p}, p^{m-1})$.*

Proof. For any $t, s \in \mathcal{O}$, $e(\frac{rt + r'(-s^{-2}t)}{p}) = 1$, since $\frac{r}{p}, \frac{r'}{p} \in \mathcal{O}'$. Then, by Lemma 5 with $n = 1$, $S(r, r', p^m) = \sum_{s \in (\mathcal{O}/p^{m-1})^*} e(\frac{rs + r's^{-1}}{p^m})|N(p)|$, and the corollary follows. $\square$

4. Proof of the main theorem

Remark 4.1. The theorem can be seen as a generalization of the property stated in Lemma 2, (iii).

Remark 4.2. The right hand side of the identity in the theorem is well defined, that is, it does not depend on the choice of the generator of (d). Indeed, if $u \in \mathcal{O}$ is a unit, by Lemma 2 (ii), $S(\frac{1}{\delta}, \frac{\delta r r'}{d^2 u^2}, \frac{c}{du}) = S(\frac{1}{\delta}, \frac{\delta r r'}{d^2}, \frac{c}{d})$.

We shall first give the statement and proof in the case when c is a power of a prime.

Proposition. *Let $r, r', \in \mathcal{O}'$, and p prime in $\mathcal{O}$. If $(r\delta, r'\delta, p^m) = p^n$, then*

$$S(r, r', p^m) = \sum_{j=0}^{n} |N(p)|^j \, S(\tfrac{1}{\delta}, \tfrac{\delta r r'}{p^{2j}}, p^{m-j}) \tag{2}$$

Proof. (i) If $n = m$, we have $\frac{r}{p^m}, \frac{r'}{p^m} \in \mathcal{O}'$, then $S(r, r', p^m) = \phi(p^m) = |N(p)|^m - |N(p)|^{m-1}$. It follows from Corollary 2 that the summands with $m - j \geq 2$ equal zero, since $\frac{\delta r r'}{p^{2j}} \in p\,\mathcal{O}'$. Hence the expression in the right hand side reduces to $|N(p)|^m S(\frac{1}{\delta}, \frac{\delta r r'}{p^{2m}}, 1) + |N(p)|^{m-1} S(\frac{1}{\delta}, \frac{\delta r r'}{p^{2m-2}}, p) = |N(p)|^m - |N(p)|^{m-1}$.

(ii) If $n = 0$, then $(r\delta, p) = 1$ or $(r'\delta, p) = 1$. Hence by Lemma 2 (iii), $S(r, r', p^m) = S(\frac{1}{\delta}, \delta r r', p^m)$, and this coincides with the expression in the right hand side of (2).

(iii) If $1 \leq n < m$, by Corollary 2 all summands with $j < n$, are zero. Hence

$$\sum_{j=0}^{n} |N(p)|^j S(\tfrac{1}{\delta}, \tfrac{\delta r r'}{p^{2j}}, p^{m-j}) = |N(p)|^n S(\tfrac{1}{\delta}, \tfrac{\delta r r'}{p^{2n}}, p^{m-n}). \tag{3}$$

On the other hand, by Corollary 3, we have

$$S(r, r', p^m) = |N(p)|^n S(\frac{r}{p^n}, \frac{r'}{p^n}, p^{m-n}). \tag{4}$$

Since $(\frac{r}{p^n}\delta, \frac{r'}{p^n}\delta, p^{m-n}) = 1$, expressions (3) and (4) coincide by Lema 2 (iii). $\square$

We now give the proof of the main theorem in the general case. Since we are assuming that the class number of F is one, any $c \in \mathcal{O}$ decomposes uniquely (up to order and unit factors) as a product of prime elements in $\mathcal{O}$. If c is a power of a prime in $\mathcal{O}$, the identity in the theorem has been already proved. By induction on the number of distinct primes in the factorization of c, we may assume that the theorem holds for coprime integers $a, b \in \mathcal{O}$, and prove the result for $c = ab$.

By Corollary 1, there exist $r_1, r_2 \in \mathcal{O}'$ such that $r_1 b^2 + r_2 a^2 \equiv r' \pmod{c\mathcal{O}'}$ and $S(r, r', c) = S(r, r_1, a) S(r, r_2, b)$. We denote $M_1 = (r\delta, r_1\delta, a)$, $M_2 = (r\delta, r_2\delta, b)$. Hence

$$S(r, r', c) = \sum_{(d_1)|M_1} |N(d_1)| S(\tfrac{1}{\delta}, \tfrac{\delta r r_1}{d_1^2}, \tfrac{a}{d_1}) \sum_{(d_2)|M_2} |N(d_2)| S(\tfrac{1}{\delta}, \tfrac{\delta r r_2}{d_2^2}, \tfrac{b}{d_2})$$

and by the multiplicativity of Kloosterman sums we have

$$= \sum_{(d_1)|M_1} \sum_{(d_2)|M_2} |N(d_1 d_2)| S(\tfrac{1}{\delta}, \tfrac{\delta r r_1}{d_1^2}\tfrac{b^2}{d_2^2} + \tfrac{\delta r r_2}{d_2^2}\tfrac{a^2}{d_1^2}, \tfrac{ab}{d_1 d_2}).$$

It is easy to see that $\frac{\delta r r_1}{d_1^2}\frac{b^2}{d_2^2} + \frac{\delta r r_2}{d_2^2}\frac{a^2}{d_1^2} \equiv \frac{\delta r r'}{(d_1 d_2)^2} \pmod{\frac{c}{d_1 d_2}\mathcal{O}'}$.

Furthermore, any divisor of $(r\delta, r'\delta, c)$ is of the form $d_1 d_2$, with d_1 a divisor of M_1 and d_2 a divisor of M_2, hence

$$\begin{aligned} S(r, r', c) &= \sum_{(d_1)|M_1} \sum_{(d_2)|M_2} |N(d_1 d_2)| S(\tfrac{1}{\delta}, \tfrac{\delta r r'}{(d_1 d_2)^2}, \tfrac{c}{d_1 d_2}) \\ &= \sum_{(d)|(r, r', c)} |N(d)| S(\tfrac{1}{\delta}, \tfrac{\delta r r'}{d^2}, \tfrac{c}{d}) \end{aligned}$$

$\square$

5. Some consequences

In this section we will apply the above results to prove other useful properties of Kloosterman sums in our context.

Corollary 4. *Let $r, r' \in \mathcal{O}$, and $(\delta, c) = 1$, then*

$$S(r, r', c) = \sum_{(d)|(r,r',c)} \left|N(d)\right| \, S(1, \tfrac{rr'}{d^2}, \tfrac{c}{d}).$$

Proof. The identity follows from the theorem and Lemma 2 (i).

On any number field F the *Moebius function* is defined as follows. If I is an ideal in $\mathcal{O}$, and $I = \mathcal{P}_1^{r_1} \cdots \mathcal{P}_k^{r_k}$ its factorization into prime ideals, let

$$\mu(I) = \begin{cases} 0 & \text{if } \exists j \, : r_j \geq 2 \\ (-1)^k & \text{if } r_1 = \cdots = r_k = 1. \end{cases}$$

Proposition. $S(\frac{1}{\delta}, 0, c) = \mu(c)$.

Proof. By the multiplicativity of Kloosterman sums, if $c = ab$ with $(a, b) = 1$, then $S(\frac{1}{\delta}, 0, c) = S(\frac{1}{\delta}, 0, a) S(\frac{1}{\delta}, 0, b)$.

We have proved that $S(\frac{1}{\delta}, 0, p) = -1$ and $S(\frac{1}{\delta}, 0, p^j) = 0$, if $j \geq 2$.

If $(c) = (p_1 \cdots p_k)$ where the p_j are distint primes in $\mathcal{O}$, then

$$S(\tfrac{1}{\delta}, 0, c) = \prod_j S(\tfrac{1}{\delta}, 0, p_j) = (-1)^k.$$

□

As a consequence we obtain some generalizations of useful identities which hold for classical Kloosterman sums.

Corollary 5. *If $c \in \mathcal{O}$, $r \in \mathcal{O}'$, then*

$$\phi(c) = \sum_{(d)|(c)} |N(d)| \mu(\tfrac{c}{d})$$

$$S(r, 0, c) = \sum_{(d)|(r\delta,c)} |N(d)| \mu(\tfrac{c}{d})$$

6. An example: $F = \mathbb{Q}[i]$

In this section we consider Kloosterman sums over the ring of Gaussian integers. Let $F=\mathbb{Q}[i]$, $\mathcal{O}=\mathbb{Z}[i]$. The different ideal is generated by 2, hence any element in $\mathcal{O}'$ is of the form $\frac{r_1+ir_2}{2}$ with $r_i \in \mathbb{Z}$.

(i) We choose $c=1+i$; this is a prime in $\mathcal{O}$, with norm 2. A set of representatives of $\mathcal{O}/(1+i)$ is $\{0,1\}$, thus

$$S(r,r',1+i)=e^{2\pi i \mathrm{Tr}(\frac{r+r'}{1+i})}=S(r+r',\,0\,,1+i).$$

Let $r=\frac{r_1+ir_2}{2}\in\mathcal{O}'$, then $\mathrm{Tr}(\frac{r}{1+i})=(r_1+r_2)/2$ and $S(r,0,1+i)=(-1)^{r_1+r_2}$. Thus

$$S(\tfrac{1}{2},0,1+i)=-1, \quad S(0,0,1+i)=1.$$

(ii) We now let $c=2$. A set of representatives of $\mathcal{O}/(2)$ is $\{0,1,i,1+i\}$. The units in this ring are $\{1,i\}$, and $1.1\equiv 1 \pmod 2$, $i.i\equiv 1 \pmod 2$.

All Kloosterman sums associated with 2, are of the form $S(r,0,2)$, with $r\in\mathcal{O}'$, since $S(r,r',2)=e(\frac{r+r'}{2})+e(\frac{ri+r'i}{2})=S(r+r',0,2)$.

If $r=\frac{r_1+ir_2}{2}\in\mathcal{O}'$, then $S(r,0,2)=(-1)^{r_1}+(-1)^{r_2}$. Therefore

$$S(r,0,2)=\begin{cases} 2 & \text{if } r_1\equiv r_2\equiv 0 \pmod 2\\ -2 & \text{if } r_1\equiv r_2\equiv 1 \pmod 2\\ 0 & \text{if } r_1\not\equiv r_2 \pmod 2\end{cases}$$

Since, $S(r,r',c)$ depends on the class of r (mod $c\mathcal{O}'$), (see Lemma 1) all possible values of Kloosterman sums are

$$S(\tfrac{1}{2},0,2)=0, \quad S(\tfrac{i}{2},0,2)=0, \quad S(0,0,2)=2, \quad S(\tfrac{1+i}{2},0,2)=-2.$$

(iii) 3 is prime in $\mathcal{O}$, with $N(3)=9$, $\mathcal{O}/3\mathcal{O}$ is a field with 9 elements, and a set of representatives of this field is

$$R=\{0,\,1,\,2,\,i,\,2i,\,1+i,\,1+2i,\,2+i,\,2+2i\},$$

all non zero elements are invertible and

$$1.1\equiv 1 \quad (3), \quad 2.2\equiv 1 \quad (3), \quad i.\,2i\equiv 1 \quad (3)$$

$$(1+i).\,(2+i)\equiv 1 \quad (3), \quad (1+2i).\,(2+2i)\equiv 1 \quad (3).$$

Remark. Since 3 is coprime with 2 and $\mathcal{D}_{F/\mathbb{Q}}=2\mathcal{O}$, all Kloosterman sums associated with 3, are of the form $S(r,r',3)$ with $r,r'\in\mathcal{O}$, and they depend on the class of r (mod $3\mathcal{O}$).

For example if $r \notin 3\mathcal{O}$, 3 is coprime with $2r$, and $S(\frac{1}{2}, 2r, 3) = S(2, 2r, 3) = S(1, 4r, 3) = S(1, r, 3)$.

It is not difficult to evaluate these sums. If $r, r' \in 3\mathcal{O}$, then $S(r, r', 3) = S(0, 0, 3) = 8 = N(3) - 1$. In this case $(r, r', 3) = (3)$ and

$$S(r, r', 3) = S(1, 0, 3) + 9S(1, \tfrac{rr'}{3^2}, 1).$$

If $r \notin 3\mathcal{O}$ and $r' \in 3\mathcal{O}$, $S(r, r', 3) = \sum_{x \in R - \{0\}} e^{2\pi i \mathrm{Tr}(rx)/3} = S(1, 0, 3)$, thus we have

$$S(1, 0, 3) = 2 + 3\, e^{2\pi i 2/3} + 3\, e^{2\pi i 4/3} = -1.$$

If $r, r' \notin 3\mathcal{O}$, we have $S(r, r', 3) = S(1, rr', 3)$, since 3 is coprime with r. The Kloosterman sums of the form $S(1, r, 3)$ take the values

$$\begin{array}{lll} S(1,0,3) = -1, & S(1,1,3) = 5, & S(1,2,3) = 2, \\ S(1,i,3) = -1, & S(1,2i,3) = -1, & S(1,1+i,3) = -4, \\ S(1,1+2i,3) = -4, & S(1,2+i,3) = 2, & S(1,2+2i,3) = 2 \end{array}$$

To conclude we will verify the main theorem, with $c = 2$. Let $r = \frac{r_1 + i r_2}{2} \in \mathcal{O}'$, we have

$$S(r, 0, 2) = \sum_{(d) | (2r, 2)} N(d)\, S(\tfrac{1}{2}, 0, \tfrac{2}{d})$$

2 it is not prime in $\mathcal{O}$, and the decomposition into primes ideals is $2 = (1 + i)^2$.

If $(2r, 2) = 2$ i.e. $r \in \mathcal{O}$, we have

$$S(\tfrac{1}{2}, 0, 2) + N(1 + i)\, S(\tfrac{1}{2}, 0, 1 + i) + N(2) S(\tfrac{1}{2}, 0, 1) = 2(-1) + 4 = 2 = S(r, 0, 2).$$

If $(2r, 2) = (1 + i)$, that is $r_1 \equiv r_2 \equiv 1 \pmod 2$, the theorem gives

$$N(1)\, S(\tfrac{1}{2}, 0, 2) + N(1 + i) S(\tfrac{1}{2}, 0, 1 + i) = -2 = S(r, 0, 2).$$

If $(2r, 2) = 1$, i.e. $r_1 \not\equiv r_2 \pmod 2$, then $N(1) S(\frac{1}{2}, 0, 2) = 0 = S(r, 0, 2)$

Acknowledgement. I would like to thank my advisor Professor Roberto Miatello for introducing me into this area, and for useful comments which improved the first version of this paper.

References

[BM] R. Bruggeman and R. Miatello, *Estimates of Kloosterman sums for groups of real rank one*, Duke Mathematical Journal **80** (1995).

[K] N. Kuznetsov, *Petersson's conjecture for cups forms of weight zero and Linnik's conjecture. Sums of Kloosterman sums*; English transl. in Mat. Sbornik **39** (1981), no. 3.

[Ma] R. Matthes, *An elementary proof of a formula of Kuznetsov for Kloosterman sums*, Results in Mathematics **18** (1990).

[Se] A. Selberg, *Uber die Fourierkoeffizienten elliptischer Modulformen negativer Dimension*, Neuvieme Congres Math. Scandinaves, Helsingfors (1938), 320–322; reprinted in: Collected papers **1**. **3**.

[HW] Hardy and Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford. Reprint, 1989.

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

Recibido en Diciembre de 1996