Local relation of Gauss sums

by

T. Kubota (Nagoya, Japan)

Among many other important properties of Gauss sums it is known that the Gauss sum $\tau_1(\chi)$ of a congruence character $\chi$ of an algebraic number field $F$ is essentially the same thing as the constant factor $\psi(\chi)$ appearing in the functional equation of Hecke's $L$-function defined by the character $\chi$. Thus interpreted, the Gauss sum $\tau_1(\chi)$ is very naturally decomposed into its local components $\tau_p(\chi)$, where $\psi$ means a finite or infinite place of $F$ (see Hasse [4]). We call $\tau_p(\chi)$ a local Gauss sum. The aim of the present note is to investigate some arithmetic attributes of the local Gauss sum.

Let us first consider the factor set

$$f_p(\chi, \psi) = \frac{\tau_p(\chi)\psi_p(\psi)}{\tau_p(\psi)}$$

between local Gauss sums. It is well known that in many cases such a factor set becomes a so-called Jacobi sum (Hasse [3], Weil [7]). But, in the general case of local Gauss sums, in particular in the case where the conductors of $\chi$, $\psi$ are divisible by a higher power of $p$, there is no so simple expression of $f_p(\chi, \psi)$ as ordinary Jacobi sums. We shall prove, however, the formulas (5), (12) of § 1, which show that $f_p(\chi, \psi)$ is in every case transformed into a generalized Jacobi sum.

In § 2, we deal with the explicit determination of the value of $f_p(\chi, \psi)$, restricting $\chi$, $\psi$ to quadratic characters. In general, the problem of this kind necessarily concerns a "Grüssencharakter" (Weil [7]). But, if $\chi$, $\psi$ are quadratic, then the square of the generalized Jacobi sum $f_p(\chi, \psi)$ is a natural number which is easily determined and the sign of $f_p(\chi, \psi)$ itself is, as the formula (16) of § 2 shows, given by the quadratic norm residue symbol.

The formula (16) is equivalent to a splitting formula (17) of the quadratic norm residue symbol. For prime ideals prime to 2, the formula (16) (or equivalently (17)) is easily proved by a simple computation, and for prime ideals dividing $2$, (17) is an almost immediate consequence of
the product formula of the norm residue symbol and of the analytic
properties of L-functions.

The formula (17) is regarded as a local form of the fact that the
inverse factor such as \( \left( \frac{a}{b} \right) \left( \frac{b}{a} \right) \) of quadratic residue symbols is expressed
by a factor set between Gauss sums. (See e.g. Hecke [5], proof of
quadratic reciprocity in an arbitrary number field.)

For prime ideals dividing 2, it seems to be an interesting problem
to prove (17) by a precise determination of the value of a local Gauss
sum as in Lamprecht [5].

1. Let \( F \) be an algebraic number field of finite degree. A congruence
character \( \chi \) of \( F \), considered as a character of the idèle group of \( F \), determines
its \( p \)-component \( \chi_p \) for every finite or infinite place \( p \) of \( F \). The
\( p \)-component \( \chi_p \) of \( \chi \) is a character of the multiplicative group of non-
zero elements of the \( p \)-adic number field \( F_p \).

Assume \( p \) to be finite and let \( \mathfrak{f}_p \) be the conductor of \( \chi_p \), \( \mathfrak{p} \), the local
different of \( F_p \) and let \( \mathfrak{p}_p \) be an element of \( F_p \) which generates the ideal
\( \mathfrak{f}_p \mathfrak{p}_p \). If \( M(s, \chi) \) is the product of Hecke’s L-function \( L(s, \chi) \) by a suitable
factor including gamma and exponential functions, then we have the
well-known functional equation

\[
M(s, \chi) = \frac{w(\chi) M(1-s, \overline{\chi})}{\Gamma(s)}
\]

and \( w(\chi) \) is decomposed into its \( p \)-components \( w_p(\chi) \):

\[
w(\chi) = \prod_p w_p(\chi),
\]

where the product runs over all places of \( F \).

For \( p \) finite, we have

\[
w_p(\chi) = \frac{\tau_p(\chi)}{|\tau_p(\chi)|}, \quad |\tau_p(\chi)| = \sqrt{N_{F_p/F}}
\]

where \( N \) denotes the norm. For \( p \) infinite, we set always \( |\tau_p(\chi)| = 1 \).

The quantity \( \tau_p(\chi) \) is the local Gauss sum of \( \chi \) and its explicit form is given by

\[
\tau_p(\chi) = \begin{cases} 
\tau_p(\chi) & (p \text{ finite and } \chi_p(-1) = 1), \\
-1 & (p \text{ infinite and } \chi_p(-1) = -1), \\
1 & (\text{otherwise}),
\end{cases}
\]

where \( \tau_p(\chi) = \exp(2\pi i \text{Tr}_F u) \), \( \text{Tr}_F \) denotes the local trace and the sum is
extended over all prime residue classes mod \( \mathfrak{f}_p \) in \( F_p \). (For proof, see
Hasse [4], e. g., also Dwork [1]).

Now we want to show that, for any two congruence characters \( \chi, \psi \)
of \( F \), the factor set

\[
\frac{\tau_p(\chi) \tau_p(\psi)}{\tau_p(\chi \psi)}
\]

is transformed into a generalized Jacobi sum. Since we restrict ourselves
to a fixed prime ideal \( p \) of \( F \) in the rest of this §, we write simply \( \chi, \psi \)
for \( \chi_p, \psi_p \). Therefore \( \chi, \psi \) are continuous characters of the multiplicative
group of non-zero elements of \( F_p \). We write similarly \( \mathfrak{f}_p, \mathfrak{p}_p, \mathfrak{f}_p \) and
\( \mathfrak{f}_p \) for \( \mathfrak{f}_p, \mathfrak{p}_p, \mathfrak{f}_p \) and \( \mathfrak{f}_p \), respectively.

Assume first that \( \mathfrak{f}_p \neq \mathfrak{f}_p \). Without any loss of generality, we may
only treat the case where \( \mathfrak{f}_p \) divides \( \mathfrak{f}_p \). There is an element \( \lambda \) in \( \mathfrak{f}_p \) such that
\( \mathfrak{f}_p \lambda = \mathfrak{f}_p \), \( \mathfrak{p}_p \lambda = \mathfrak{p}_p \) and we have \( \mathfrak{f}_p \lambda = \mathfrak{f}_p \). So, under the additional
assumption \( \mathfrak{f}_p \neq 1 \), we have

\[
\tau(\chi) \tau(\psi) = \chi(\varphi_\chi^{-1}) \sum_{\mathfrak{f}_p < u < \mathfrak{f}_p} \chi(u) \psi(u) \frac{\varphi_\psi(u)}{\varphi_\psi} \sum_{\mathfrak{f}_p < v < \mathfrak{f}_p} \psi(v) \psi(v) \frac{\varphi_{\psi}}{\varphi_{\psi}}
\]

\[
= \chi(\varphi_\chi^{-1}) \sum_{\mathfrak{f}_p < u < \mathfrak{f}_p} \chi(u) \psi(\varphi_\psi^{-1}) \sum_{\mathfrak{f}_p < v < \mathfrak{f}_p} \psi(v) \psi(v) \frac{\varphi_{\psi}}{\varphi_{\psi}}
\]

\[
= \lambda(\lambda)^{-1} \chi(\varphi_\chi^{-1}) \sum_{\mathfrak{f}_p < u < \mathfrak{f}_p} \chi(u) \psi(u) \psi(\varphi_{\psi}) \frac{\lambda u + v}{\varphi_{\psi}}
\]

Set \( \lambda u + v = t \) and \( \varphi_\psi = \varphi_\psi \), which is naturally legitimate. Then,

\[
\tau(\chi) \tau(\psi) = \lambda(\lambda)^{-1} \chi(\varphi_\chi^{-1}) \sum_{\mathfrak{f}_p < u < \mathfrak{f}_p} \chi(u) \psi(t - \lambda u) \frac{t}{\varphi_{\psi}}
\]

\[
= \lambda(\lambda)^{-1} \chi(\varphi_\chi^{-1}) \sum_{\mathfrak{f}_p < u < \mathfrak{f}_p} \chi(u) \psi(t - \lambda u) \psi(\varphi_{\psi}) \frac{t}{\varphi_{\psi}}
\]

\[
= \lambda(\lambda)^{-1} \chi(\lambda) \sum_{\mathfrak{f}_p < u < \mathfrak{f}_p} \chi(u) \psi(t - \lambda u) \psi(\varphi_{\psi}) \frac{t}{\varphi_{\psi}}
\]

\[
= \tau(\chi) \sum_{\mathfrak{f}_p < u < \mathfrak{f}_p} \chi(u) \psi(t - \lambda u).
\]
If \( f = 1 \) on the other hand, then \( \tau(x) = x(\phi_x)^{-1} \) and \( \tau(y) = x(\phi_y)^{-1} \), whence \( \tau(x) \tau(y) = x(\phi_x)^{-1} x(\phi_y)^{-1} \), \( \tau(x) \tau(y) = x(\lambda) \tau(y) \).

Hence in either case we have

\[
\tau(x) \tau(y) = \sum_{\substack{u \equiv \phi_x \pmod{\lambda_x} \\ u \neq 1 \pmod{\lambda_x}}} x(\phi_x)^{-1} x(1 - \frac{s}{\lambda_x}) \cdot \sum_{\substack{v \equiv \phi_y \pmod{\lambda_y} \\ v \neq 1 \pmod{\lambda_y}}} y(\phi_y)^{-1} y(1 - \frac{t}{\lambda_y}) (f \wedge \lambda = f \wedge \lambda + v) x \cdot y.
\]

Next we consider the case of \( f = f' \neq 1 \). Let \( f = f' \). Let \( f \neq f' \). Let \( f' \) be any divisor of \( f \) and \( \lambda' \) be an integer in \( F_0 \) such that \( f' = |\lambda'| \). For any \( \lambda \in \mathbb{Z}_+ \) with \( t = 1 \pmod{\lambda} \) and for any unit \( * \neq \lambda' \), we have

\[
\sum_{\substack{\phi_x \equiv \phi_y \pmod{\lambda} \\ \phi_y \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]

where \( c \) is a divisor of \( f' \). If \( \lambda' \) is not a unit, then \( \lambda' - s \) is a unit and \( \lambda' - t \) is a unit. Therefore we have \( y(\lambda' - s, \lambda') = y(\lambda' - s, \lambda') \) and

\[
\psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right) = \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right).
\]

If \( \lambda' \) is a unit, then (6) is of course true. Thus we have

\[
\sum_{\substack{\phi_x \equiv \phi_y \pmod{\lambda} \\ \phi_y \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right). \tag{7}
\]

Let \( f \neq f' \) be a divisor of \( f_\psi \), i.e., a divisor of \( f_\psi \) different from \( f_\psi \) itself, and consider the sum

\[
\sum_{\substack{\phi_x \equiv \phi_y \pmod{\lambda} \\ \phi_y \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]

extended over prime residue classes \( \mod{f} \). Then, since \( \lambda' \) cannot be a unit and since it gives a unit in \( F_0 \) such that \( \psi(t) \neq 1 \), \( t = 1 \pmod{\lambda} \), the above formula (7) gives

\[
\sum_{\substack{\phi_x \equiv \phi_y \pmod{\lambda} \\ \phi_y \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right) = \psi(t) \sum_{\substack{\phi_x \equiv \phi_y \pmod{\lambda} \\ \phi_y \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi \left( 1 - \frac{s}{\lambda} \right).
\]

This implies

\[
\sum_{\substack{\phi_x \equiv \phi_y \pmod{\lambda} \\ \phi_y \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi \left( 1 - \frac{s}{\lambda} \right) = 0. \tag{8}
\]

After these preliminaries, we set \( \epsilon = \epsilon = f_\psi \), \( \epsilon = \epsilon = f_\psi \), and then, \( \epsilon \) not necessarily an element of \( p \). Then, we have

\[
\tau(x) \tau(y) = x(\phi_x)^{-1} \sum_{\substack{\epsilon \equiv \phi_x \pmod{\lambda} \\ \epsilon \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi(\epsilon)^{-1} \psi(\epsilon') \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]

where \( \epsilon' \) is a divisor of \( f_\psi \). Let \( \epsilon' \neq f_\psi \). Putting \( u + v = t \), we get

\[
\tau(x) \tau(y) = x(\phi_x)^{-1} \psi(\phi_y)^{-1} \sum_{\substack{\epsilon \equiv \phi_x \pmod{\lambda} \\ \epsilon \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi(\epsilon)^{-1} \psi(\epsilon') \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]

where \( \epsilon' \) is a divisor of \( f_\psi \). Let \( \epsilon' \neq f_\psi \). Putting \( u + v = t \), we get

\[
\tau(x) \tau(y) = x(\phi_x)^{-1} \psi(\phi_y)^{-1} \sum_{\substack{\epsilon \equiv \phi_x \pmod{\lambda} \\ \epsilon \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi(\epsilon)^{-1} \psi(\epsilon') \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]

where \( \epsilon' \) is a divisor of \( f_\psi \). Let \( \epsilon' \neq f_\psi \). Putting \( u + v = t \), we get

\[
\tau(x) \tau(y) = x(\phi_x)^{-1} \psi(\phi_y)^{-1} \sum_{\substack{\epsilon \equiv \phi_x \pmod{\lambda} \\ \epsilon \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi(\epsilon)^{-1} \psi(\epsilon') \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]

where \( \epsilon' \) is a divisor of \( f_\psi \). Let \( \epsilon' \neq f_\psi \). Putting \( u + v = t \), we get

\[
\tau(x) \tau(y) = x(\phi_x)^{-1} \psi(\phi_y)^{-1} \sum_{\substack{\epsilon \equiv \phi_x \pmod{\lambda} \\ \epsilon \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi(\epsilon)^{-1} \psi(\epsilon') \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]

where \( \epsilon' \) is a divisor of \( f_\psi \). Let \( \epsilon' \neq f_\psi \). Putting \( u + v = t \), we get

\[
\tau(x) \tau(y) = x(\phi_x)^{-1} \psi(\phi_y)^{-1} \sum_{\substack{\epsilon \equiv \phi_x \pmod{\lambda} \\ \epsilon \neq 1 \pmod{\lambda}}} x(\phi_x)^{-1} y(\phi_y)^{-1} \psi(\epsilon)^{-1} \psi(\epsilon') \psi \left( 1 - \frac{s}{\lambda} \right) \psi \left( 1 - \frac{t}{\lambda} \right)
\]
and it follows from (9) and (10) that
\[
\tau(x) \tau(x) = x(p^{-r-1} \psi(p^{-r-1}) \times \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \psi(\sigma) \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) )
\]

\[
= x(p^{-r-1} \psi(x^{-r-1}) \times \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \psi(\sigma) \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) )
\]

\[
= \tau(x) \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda})
\]

Hence, under the assumption \( f \neq 1 \), we have
\[
(\tau(x) \tau(x)) = \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \quad (f_\lambda = f_\psi = \lambda f_\nu)
\]

where the sum is extended over all prime residue classes mod.\( f_\lambda \) with the additional condition \( \sigma/\lambda \equiv 1 \mod{p} \), which may be omitted unless \( \lambda \) is a unit.

If we again use (7), the right hand side of (11) turns out
\[
(\tau(x) \tau(x)) = \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \quad (f_\lambda = f_\psi = \lambda f_\nu).
\]

The formula (12) is proved whenever \( f_\psi \neq 1 \). But, as the matter of fact, (12) is also valid even if \( f_\psi = 1 \).

To show this, assume first \( f_\psi = 1 \) or \( f_\psi = 1 \). Then it follows from \( \psi(\tau) = 1 \) that
\[
\tau(x) \tau(x) = x(p^{-r-1} \psi(p^{-r-1}) \times \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \psi(\sigma) \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) )
\]

Since
\[
\sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \psi(\sigma) = 0 \quad \text{for } \lambda < r - 1,
\]
\[
= -1 \quad \text{for } \lambda = r - 1,
\]
\[
= 1 \quad \text{for } \lambda = r,
\]

we have
\[
\tau(x) \tau(x) = x(p^{-r-1} \psi(p^{-r-1}) \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \psi(\sigma) \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda})
\]

\[
= x(p^{-r-1} \psi(p^{-r-1}) \times \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \psi(\sigma)
\]

\[
= x(p^{-r-1} \psi(p^{-r-1}) \times \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda})
\]

So, in this case, (12) is also true. If next \( f_\lambda = f_\psi = f_\nu = 1 \), then \( \tau(x) \tau(x) = x(p^{-r-1} \psi(p^{-r-1}) = \tau(x) \psi(p^{-r-1}) \). Thus, (12) holds in every case without exception.

We call the sum in (5) or (12) a generalized Jacobi sum.

It must be noted that, if \( f_\lambda = f_\psi = f_\nu = 1 \) and \( N f_\psi = 2 \), then the sum in (13) is nonsense. It is convenient to regard such a sum always to be 1, although it plays no essential role.

2. Let \( I, I \) be congruence characters of \( \mathbb{F} \). We denote by \( j_\lambda(I, I) \) the generalized Jacobi sum of \( I, I \) of \( I, I \). In a explicit form, we have
\[
j_\lambda(I, I) = \sum_{\lambda \equiv \lambda \mod{1, \mu} \neq (1)} \lambda \left( \frac{s}{\lambda} \right) \psi(1 - \frac{s}{\lambda}) \quad (f_\psi = f_\nu = \lambda f_\psi).
\]

As for the case where the relation \( f_\psi = f_\nu = \lambda f_\psi \) holds, we may define \( j_\lambda(I, I) \) by setting \( j_\lambda(I, I) = j_\lambda(I, I) \). It follows from (5) and (12) that
\[
j_\lambda(I, I) = \psi(n) j_\lambda(I, I) \quad (f_\psi = f_\nu = \lambda f_\psi).
\]
Therefore (3) yields

\[ |j_F(x, \psi)| = \nu \min (N_{l_1, \psi}, N_{l_2, \psi}, N_{l_3, \psi}) \]

for any two congruence characters \( \chi_1, \chi_2 \).

Assume now that \( F \) contains all the \( m \)-th roots of unity. Then a non-zero element \( \alpha \in F \) determines a congruence character \( \chi_\alpha \) of \( F \) whose \( p \)-component is given by the norm residue symbol

\[ \chi_\alpha_p = \left( \frac{\alpha}{p} \right)_m. \]

For such characters \( \chi_1, \chi_2 \), we set

\[ j_F(\alpha, \beta) = j_F(\chi_1, \chi_2). \]

For the sake of convenience, we write furthermore \( \chi(a), \chi(a), \psi(a), \psi(a), \psi(a), \psi(a), \psi(a), \psi(a) \), respectively.

Now, the aim of this \( \S \) is to determine explicitly the value of \( j_F(\alpha, \beta) \), provided that \( m = 2 \). The result is as follows:

\[ j_F(\alpha, \beta) = \left( \frac{\alpha \beta}{p} \right) \nu \min (N_{l_1, \psi}, N_{l_2, \psi}, N_{l_3, \psi}), \]

where we write \( \left( \frac{\alpha \beta}{p} \right)_m \) for \( \left( \frac{\alpha \beta}{p} \right)_m \).

Since it follows from (3), (16), and (15) that (16) is equivalent with

\[ \left( \frac{\alpha \beta}{p} \right) = \psi(a) \psi(\beta) \quad (a, \beta \equiv 0, \beta \equiv 0), \]

it suffices to prove the latter relation.

If \( p \) is infinite, then (16) is clear from the definition. If \( p \) is finite and does not divide 2, then, instead of (17), (16) is proved directly by the defining formula (15) of the generalized Jacobi sum. Namely, since in this case

\[ \nu \min (N_{l_1, \psi}, N_{l_2, \psi}, N_{l_3, \psi}) = 1, \]

we have simply to show

\[ j_F(\alpha, \beta) = \left( \frac{\alpha \beta}{p} \right). \]

If the exponents of \( p \) in \( \alpha, \beta \) are both even, then \( \left( \frac{\alpha \beta}{p} \right) = 1 \) and by the formula of (13), we have \( j_F(\alpha, \beta) = 1 \). (Put \( \lambda = 1 \) and let \( s \) be any unit \( \psi(1) \).) For the exponent of \( p \) in \( \alpha \) is even and that of \( \beta \) is odd, then

\[ \left( \frac{\alpha \beta}{p} \right) = \left( \frac{\alpha}{p} \right) \left( \frac{\beta}{p} \right) \]

and by the upper formula of (13) we have \( j_F(\alpha, \beta) = \left( \frac{\alpha}{p} \right) \left( \frac{\beta}{p} \right) \). where \( \pi \) is a prime element of \( p \). (Set \( \lambda = \pi \) and \( s = 1 \).)

If finally the exponents of \( p \) in \( \alpha \) and \( \beta \) are both odd, again the lower formula of (13) shows

\[ j_F(\alpha, \beta) = \left( \frac{\alpha}{p} \right) \left( \frac{\beta}{p} \right) \left( \frac{\alpha \beta}{p} \right) \left( \frac{1}{p} \right) = \left( \frac{\beta}{p} \right) \left( \frac{1}{p} \right) = \left( \frac{\alpha \beta}{p} \right). \]

(Set \( \lambda = \pi, s = 1 \).

It remains therefore to prove (17) in the case where \( p \) divides 2. Let \( l_1, \ldots, l_\ell \) be all the prime divisors of 2 in \( F \) and \( l \) be any one of them. Then, for non-zero \( \alpha, \beta \epsilon F \), it follows from the approximation theorem of valuation that there exists \( \alpha^* F \) such that \( a^* F \) is a square in \( F \) and \( \alpha^* \) itself is a square in every \( F_{l_i} \) for which \( l_i \neq 1 \). We choose similarly \( \alpha^* \) for \( \beta^* \).

Then, as direct consequences of (3) and (4), we have

\[ \psi(\alpha) = \psi(\beta) = \psi(\alpha^* \beta^*) = 1 \quad (l_i \neq 1), \]

\[ \psi(\alpha^*) = \psi(\beta^*) = \psi(\alpha^* \beta^*) = \psi(\alpha^* \beta^*), \]

\[ \left( \frac{\alpha^* \beta^*}{l_i} \right) = \left( \frac{\alpha}{l_i} \right) \left( \frac{\beta}{l_i} \right) = \left( \frac{\alpha \beta}{l_i} \right) = 1 \quad (l_i \neq 1). \]

On the other hand, since \( \chi_1, \chi_2, \chi_\alpha \) are all quadratic, the general theory of Hecke’s \( L \)-function shows that \( \psi(\alpha) = \psi(\beta) = \psi(\alpha^2) = 1 \). (See, e.g. Hasse [2].)

Hence we have

\[ 1 = \psi(\alpha^*) \psi(\beta^*) = \prod l_i \psi(\alpha^*) \psi(\alpha^* \beta^*) = \prod l_i \left( \frac{\alpha^* \beta^*}{l_i} \right) \prod l_i \left( \frac{\alpha^* \beta^*}{l_i} \right) \psi(\alpha^* \beta^*). \]

Therefore, because of the product formula of the norm residue symbol, we have

\[ \psi(\alpha) \psi(\beta) = \psi(\alpha^* \beta^*). \]

This means

\[ \left( \frac{\alpha^* \beta^*}{l_i} \right) = \psi(\alpha) \psi(\beta) \psi(\alpha^* \beta^*). \]

Thus the formula (16) is completely proved and at the same time the splitting formula (17) of the norm residue symbol is verified.
We add here a numerical example of the splitting formula in the simplest case where $F = \mathbb{Q}$ is rational number field and $p = 2$. Let $\mathbb{C}_p^*$ be the multiplicative group of non-zero elements of the 2-adic number field $\mathbb{Q}_2$. Then, for every representative of $\mathbb{C}_2^*/\mathbb{C}_2^*$, the value of $w_2(a)$ is given by

$$a = 1, 5, -1, -5, 2, 10, -2, -10$$

$$w_2(a) = 1, i, i, i, -1, i, -i.$$

This gives, for example,

$$\left(\frac{10, -2}{2}\right) = -\frac{1}{i} = -1.$$

References


MATHEMATICAL INSTITUTE
NAKOGA UNIVERSITY

Royé par la Rédaction le 6. 4. 1960

---

On the existence of primes in short arithmetical progressions

by

E. Fogels (Riga)

Introduction. In 1944 Linnik (see [4]) proved the existence of an absolute constant $c > 0$ such that the smallest prime in any arithmetical progression $kn + l$, $(k, l) = 1$, $0 < k, l, 2, \ldots$ does not exceed $k^c$. In 1954 Rodosskii (see [6]) gave a shorter proof in which a fundamental lemma of Linnik was replaced by a weaker result (see further (10)).

Introducing a new parameter in Rodosskii's proof in 1955 I proved (see (2)) the existence of an absolute constant $c > 0$ such that there is at least one prime $p \equiv l (\mod k)$, $(k, l) = 1$, in the interval

$$\{x, x + 2\} \quad \text{for all } x \geq 1,$$

and I proved that there are other absolute constants $c_1, c_2, c_3 > 0$ such that

$$\pi(x; k, l) > xk^{-c_1}$$

for all $x \in (k^c, k^{c_2})$, if $(k, l) = 1$ and $\pi(x; k, l)$ denotes the number of primes $p \equiv l (\mod k)$ not exceeding $x$.

The estimates (1) and (2) are of some importance for $x < \exp k^2$, $c_1$ denoting (throughout this paper) an arbitrarily small positive constant. In this case the uncertainty about the existence or nonexistence of the real exceptional zero of Dirichlet's function $L(s, \chi)$ with a real character $\chi$ modulo $k$ is the reason why the existing estimates of $\pi(x; k, l)$ and estimates of the difference of consecutive primes $\equiv l (\mod k)$ fail to give us any positive information. For $x \geq \exp k^2$ and $k > k_0(c_1)$ according to Tchudakoff ([3]) there is at least one prime $\equiv l (\mod k)$ in the interval

$$\{x, x(1 + x^{-c_1})\},$$

and $\pi(x; k, l) > c_3(k)\log x$, where $q(k)$ is Euler's function denoting the number of natural numbers $l \leq k$ with $(l, k) = 1$.

(1) For these results see, for example, K. Fuchs [5], I X Satz 2.2, IV Satz 8.2; IX Satz 3.2, I X Satz 4.2. (Roman numbers denoting the chapters, A the appendix).