in (3) we see that the first term is negligible as compared with the third. Thus, for $M \leqslant \Delta^{-1}$:

$$U_M \ll n^{701/1020+\varepsilon''}.$$

We easily see that the same result holds also for $M > \Delta^{-1}$. Hence

$$B \ll n^{701/1020+\varepsilon_1}.$$

Thus, as is shown in [1], one can obtain

$$\sum_{t=1}^{N} h(-t) = \frac{4\pi}{21\zeta(3)} N^{3/2} - \frac{2}{\pi^2} N + O(N^{701/1020+\varepsilon}).$$

References

[1] I. M. Vinogradov (И. М. Виноградов), *Улучшение остаточного члена одной асимптотической формулы,* (in Russian), Izv. Akad. Nauk SSSR, Ser. Mat., 13 (1949), pp. 97-110.

[2] — *Улучшение асимптотических формул для числа целых точек в области трех измерений,* (in Russian), ibid. 19 (1955), pp. 3-9.

Reçu par la Rédaction le 23. 3. 1960

ACTA ARITHMETICA
VI (1961)

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 $\tau(\chi)$ of a congruence character χ of an algebraic number field F is essentially the same thing as the constant factor $w(\chi)$ appearing in the functional equation of Hecke's L-function defined by the character χ. Thus interpreted, the Gauss sum $\tau(\chi)$ is very naturally decomposed into its local components $\tau_{\mathfrak{p}}(\chi)$, where $\mathfrak{p}$ means a finite or infinite place of F (see Hasse [4]). We call $\tau_{\mathfrak{p}}(\chi)$ 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

$$j_{\mathfrak{p}}(\chi,\psi) = \frac{\tau_{\mathfrak{p}}(\chi)\tau_{\mathfrak{p}}(\psi)}{\tau_{\mathfrak{p}}(\chi\psi)}$$

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 χ, ψ are divisible by a higher power of $\mathfrak{p}$, there is no so simple expression of $j_{\mathfrak{p}}(\chi,\psi)$ as ordinary Jacobi sums. We shall prove, however, the formulas (5), (12) of § 1, which show that $j_{\mathfrak{p}}(\chi,\psi)$ is in every case transformed into a *generalized Jacobi sum*.

In § 2, we deal with the explicit determination of the value of $j_{\mathfrak{p}}(\chi,\psi)$, restricting χ, ψ to quadratic characters. In general, the problem of this kind necessarily concerns a "Grössencharakter" (Weil [7]). But, if χ, ψ are quadratic, then the square of the generalized Jacobi sum $j_{\mathfrak{p}}(\chi,\psi)$ is a natural number which is easily determined and the sign of $j_{\mathfrak{p}}(\chi,\psi)$ 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 $\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)$ 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 [6].

1. Let F be an algebraic number field of finite degree. A congruence character χ of F, considered as a character of the idèle group of F, determines its $\mathfrak{p}$-component $\chi_{\mathfrak{p}}$ for every finite or infinite place $\mathfrak{p}$ of F. The $\mathfrak{p}$-component $\chi_{\mathfrak{p}}$ of χ is a character of the multiplicative group of non-zero elements of the $\mathfrak{p}$-adic number field $F_{\mathfrak{p}}$.

Assume $\mathfrak{p}$ to be finite and let $\mathfrak{f}_{\chi,\mathfrak{p}}$ be the conductor of $\chi_{\mathfrak{p}}$, $\mathfrak{d}_{\mathfrak{p}}$ the local different of $F_{\mathfrak{p}}$ and let $\varphi_{\chi,\mathfrak{p}}$ be an element of $F_{\mathfrak{p}}$ which generates the ideal $\mathfrak{f}_{\chi,\mathfrak{p}}\mathfrak{d}_{\mathfrak{p}}$. 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

$$M(s,\chi)=w(\chi)M(1-s,\bar{\chi}) \tag{1}$$

and $w(\chi)$ is decomposed into its $\mathfrak{p}$-components $w_{\mathfrak{p}}(\chi)$:

$$w(\chi)=\prod_{\mathfrak{p}} w_{\mathfrak{p}}(\chi), \tag{2}$$

where the product runs over all places of F.

For $\mathfrak{p}$ finite, we have

$$w_{\mathfrak{p}}(\chi)=\frac{\tau_{\mathfrak{p}}(\chi)}{|\tau_{\mathfrak{p}}(\chi)|}, \qquad |\tau_{\mathfrak{p}}(\chi)|=\sqrt{N\mathfrak{f}_{\chi,\mathfrak{p}}}, \tag{3}$$

where N denotes the norm. For $\mathfrak{p}$ infinite, we set always $|\tau_{\mathfrak{p}}(\chi)|=1$. The quantity $\tau_{\mathfrak{p}}(\chi)$ is the local Gauss sum of χ and its explicit form is given by

$$\tau_{\mathfrak{p}}(\chi)=\begin{cases}\chi_{\mathfrak{p}}(\varphi_{\chi,\mathfrak{p}})^{-1}\sum\limits_{\substack{u \bmod \mathfrak{f}_{\chi,\mathfrak{p}}\\ u\not\equiv 0\,(\mathfrak{p})}}\chi_{\mathfrak{p}}(u)e_{\mathfrak{p}}\left(\dfrac{u}{\varphi_{\chi,\mathfrak{p}}}\right) & (\mathfrak{p}\text{ finite}),\\ -i & (\mathfrak{p}\text{ infinite and }\chi_{\mathfrak{p}}(-1)=-1),\\ 1 & (\text{otherwise}),\end{cases} \tag{4}$$

where $e_{\mathfrak{p}}(u)=\exp(2\pi i S_{\mathfrak{p}}u)$, $S_{\mathfrak{p}}$ denotes the local trace and the sum is extended over all prime residue classes mod $\mathfrak{f}_{\chi,\mathfrak{p}}$ in $F_{\mathfrak{p}}$. (For proof, see Hasse [4], c. f. also Dwork [1]).

Now we want to show that, for any two congruence characters χ, ψ of F, the factor set

$$\frac{\tau_{\mathfrak{p}}(\chi)\tau_{\mathfrak{p}}(\psi)}{\tau_{\mathfrak{p}}(\chi\psi)}$$

is transformed into a generalized Jacobi sum. Since we restrict ourselves to a fixed prime ideal $\mathfrak{p}$ of F in the rest of this §, we write simply χ, ψ for $\chi_{\mathfrak{p}}$, $\psi_{\mathfrak{p}}$. Therefore χ, ψ are continuous characters of the multiplicative group of non-zero elements of $F_{\mathfrak{p}}$. We write similarly $\mathfrak{f}_{\chi}$, φ_{χ}, $\mathfrak{d}$, $e(u)$ and $\tau(\chi)$ for $\mathfrak{f}_{\chi,\mathfrak{p}}$, $\varphi_{\chi,\mathfrak{p}}$, $\mathfrak{d}_{\mathfrak{p}}$, $e_{\mathfrak{p}}(u)$ and $\tau_{\mathfrak{p}}(\chi)$, respectively.

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

$$\begin{aligned}\tau(\chi)\tau(\psi)&=\chi(\varphi_{\chi})^{-1}\sum_{\substack{u \bmod \mathfrak{f}_{\chi}\\ u\not\equiv 0\,(\mathfrak{p})}}\chi(u)e\left(\frac{u}{\varphi_{\chi}}\right)\cdot\psi(\varphi_{\psi})^{-1}\sum_{\substack{v \bmod \mathfrak{f}_{\psi}\\ v\not\equiv 0\,(\mathfrak{p})}}\psi(v)e\left(\frac{v}{\varphi_{\psi}}\right)\\ &=\chi(\varphi_{\chi})^{-1}N(\lambda)^{-1}\sum_{\substack{u \bmod \mathfrak{f}_{\psi}\\ u\not\equiv 0\,(\mathfrak{p})}}\chi(u)e\left(\frac{u}{\varphi_{\chi}}\right)\cdot\psi(\varphi_{\psi})^{-1}\sum_{v}\psi(v)e\left(\frac{v}{\varphi_{\psi}}\right)\\ &=N(\lambda)^{-1}\chi(\varphi_{\chi})^{-1}\psi(\varphi_{\psi})^{-1}\sum_{u,v}\chi(u)\psi(v)e\left(\frac{\lambda u+v}{\varphi_{\psi}}\right).\end{aligned}$$

Set $\lambda u+v=t$ and $\varphi_{\chi\psi}=\varphi_{\psi}$, which is naturally legitimate. Then,

$$\begin{aligned}\tau(\chi)\tau(\psi)&=N(\lambda)^{-1}\chi(\varphi_{\chi})^{-1}\psi(\varphi_{\psi})^{-1}\sum_{\substack{t,u \bmod \mathfrak{f}_{\psi}\\ t\not\equiv 0,u\not\equiv(\mathfrak{p})}}\chi(u)\psi(t-\lambda u)e\left(\frac{t}{\varphi_{\psi}}\right)\\ &=N(\lambda)^{-1}\chi(\varphi_{\chi})^{-1}\psi(\varphi_{\psi})^{-1}\sum_{t}\left\{\sum_{u}\chi\left(\frac{u}{t}\right)\psi\left(1-\frac{\lambda u}{t}\right)\right\}\chi\psi(t)e\left(\frac{t}{\varphi_{\chi\psi}}\right)\\ &=N(\lambda)^{-1}\chi(\lambda)\sum_{\substack{s \bmod \mathfrak{f}_{\psi}\\ s\not\equiv 0\,(\mathfrak{p})}}\chi(s)\psi(1-\lambda s)\cdot\chi\psi(\varphi_{\psi})^{-1}\sum_{t}\chi\psi(t)e\left(\frac{t}{\varphi_{\chi\psi}}\right)\\ &=\tau(\chi\psi)\cdot\sum_{\substack{s \bmod \mathfrak{f}_{\chi}\\ s\not\equiv 0\,(\mathfrak{p})}}\chi(\lambda s)\psi(1-\lambda s).\end{aligned}$$

If $\mathfrak{f}_\chi = 1$, on the other hand, then $\tau(\chi) = \chi(\varphi_\chi)^{-1}$ and $\tau(\chi\psi) = \chi(\varphi_\psi)^{-1}\tau(\psi)$, whence $\tau(\chi)\tau(\psi) = \chi(\varphi_\chi)^{-1}\chi(\varphi_\psi)\tau(\chi\psi) = \chi(\lambda)\tau(\chi\psi)$.

Hence in either case we have

$$(5)\qquad \frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)} = \sum_{\substack{s \bmod \mathfrak{f}_\chi \\ s \not\equiv 0\,(\mathfrak{p})}} \chi(\lambda s)\psi(1-\lambda s) \qquad (\mathfrak{f}_\chi\lambda = \mathfrak{f}_\psi,\ \lambda\in\mathfrak{p}).$$

Next we consider the case of $\mathfrak{f}_\chi = \mathfrak{f}_\psi = \mathfrak{f}$. Let $\mathfrak{f}_0$ be any divisor of $\mathfrak{f}$ and λ_0 be an integer in $F_\mathfrak{p}$ such that $\mathfrak{f}_0 = \mathfrak{f}/\lambda_0$. For any $t\in F_\mathfrak{p}$ with $t \equiv 1 \pmod{\mathfrak{f}_0}$ and for any unit $s\in F_\mathfrak{p}$, we have

$$\chi\left(\frac{st}{\lambda_0}\right)\psi\left(1-\frac{st}{\lambda_0}\right) = \chi\psi(t)\chi\left(\frac{s}{\lambda_0}\right)\psi\left(\frac{1}{t}-\frac{s}{\lambda_0}\right)$$
$$= \chi\psi(t)\chi\left(\frac{s}{\lambda_0}\right)\psi\left(1+\omega_0-\frac{s}{\lambda_0}\right) = \chi\psi(t)\chi\left(\frac{s}{\lambda_0}\right)\psi\left(\frac{\lambda_0-s+\lambda_0\omega_0}{\lambda_0}\right),$$

where ω_0 is an element in $\mathfrak{f}_0$. If λ_0 is not a unit, then $\lambda_0 - s$ is a unit and $\lambda_0\omega_0\in\mathfrak{f}$. Therefore we have $\psi(\lambda_0-s+\lambda_0\omega_0) = \psi(\lambda_0-s)$ and

$$(6)\qquad \psi\left(\frac{\lambda_0-s+\lambda_0\omega_0}{\lambda_0}\right) = \psi\left(1-\frac{s}{\lambda_0}\right).$$

If λ_0 is a unit, then (6) is of course true. Thus we have

$$(7)\qquad \chi\left(\frac{st}{\lambda_0}\right)\psi\left(1-\frac{st}{\lambda_0}\right) = \chi\psi(t)\chi\left(\frac{s}{\lambda_0}\right)\psi\left(1-\frac{s}{\lambda_0}\right).$$

Let $\mathfrak{f}_0$ be a proper divisor of $\mathfrak{f}_{\chi\psi}$, i. e., a divisor of $\mathfrak{f}_{\chi\psi}$ different from $\mathfrak{f}_{\chi\psi}$ itself, and consider the sum

$$\sum_{\substack{s \bmod \mathfrak{f} \\ s\not\equiv 0\,(\mathfrak{p})}} \chi\left(\frac{s}{\lambda_0}\right)\psi\left(1-\frac{s}{\lambda_0}\right)$$

extended over prime residue classes $\bmod\,\mathfrak{f}$. Then, since λ_0 cannot be a unit and since it gives a unit in $F_\mathfrak{p}$ such that $\chi\psi(t)\neq 1$, $t\equiv 1 \pmod{\mathfrak{f}_0}$, the above formula (7) gives

$$\sum_s \chi\left(\frac{s}{\lambda_0}\right)\psi\left(1-\frac{s}{\lambda_0}\right) = \sum_s \chi\left(\frac{st}{\lambda_0}\right)\psi\left(1-\frac{st}{\lambda_0}\right) = \chi\psi(t)\sum_s \chi\left(\frac{s}{\lambda_0}\right)\psi\left(1-\frac{s}{\lambda_0}\right).$$

This implies

$$(8)\qquad \sum_{\substack{s \bmod \mathfrak{f}_0 \\ s\not\equiv 0\,(\mathfrak{p})}} \chi\left(\frac{s}{\lambda_0}\right)\psi\left(1-\frac{s}{\lambda_0}\right) = 0.$$

After these preliminaries, we set $\mathfrak{f}_\chi = \mathfrak{f}_\psi = \mathfrak{f}_{\chi\psi}\lambda$, $\varphi_\chi = \varphi_\psi = \varphi_{\chi\psi}\lambda$. The factor λ is an integer in $F_\mathfrak{p}$, but not necessarily an element of $\mathfrak{p}$. Then, we have

$$\tau(\chi)\tau(\psi) = \chi(\varphi_\chi)^{-1}\sum_{\substack{u \bmod \mathfrak{f}_\chi \\ u\not\equiv 0\,(\mathfrak{p})}} \chi(u)e\left(\frac{u}{\varphi_\chi}\right)\cdot\psi(\varphi_\psi)^{-1}\sum_{\substack{v \bmod \mathfrak{f}_\psi \\ v\not\equiv 0\,(\mathfrak{p})}} \psi(v)e\left(\frac{v}{\varphi_\psi}\right)$$
$$= \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\sum_{u,v}\chi(u)\psi(v)e\left(\frac{u+v}{\varphi_\chi}\right).$$

Putting $u+v = t$, we get

$$\tau(\chi)\tau(\psi) = \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\sum_{\substack{u,t \bmod \mathfrak{f}_\chi \\ u\not\equiv 0,\, t-u\not\equiv 0\,(\mathfrak{p})}} \chi(u)\psi(t-u)e\left(\frac{t}{\varphi_\chi}\right).$$

Let π be a prime element of $\mathfrak{p}$ and set $t = \pi^i t'$ ($t'\not\equiv 0 \pmod{\mathfrak{p}}$). Moreover, set $\mathfrak{f}_\chi = \mathfrak{p}^r$. Then, i running over $0, 1, \ldots, r$ and t' moving $\bmod\,\mathfrak{f}_\chi/\pi^i$ we have

$$\tau(\chi)\tau(\psi) = \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\sum_{\substack{i,u,t \\ u\not\equiv 0,\,1\not\equiv u/\pi^i t'\,(\mathfrak{p})}} \chi\left(\frac{u}{\pi^i t'}\right)\psi\left(1-\frac{u}{\pi^i t'}\right)\chi\psi(\pi^i t')e\left(\frac{t'}{\varphi_\chi\pi^{-i}}\right)$$
$$= \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\sum_i\Bigg\{\sum_{\substack{s \bmod \mathfrak{f}_\chi \\ s\not\equiv 0,\, s/\pi^i\not\equiv 1\,(\mathfrak{p})}} \chi\left(\frac{s}{\pi^i}\right)\psi\left(1-\frac{s}{\pi^i}\right)\Bigg\}\Bigg\{\chi\psi(\pi^i)\sum_{t'}\chi\psi(t')e\left(\frac{t'}{\varphi_\chi\pi^{-i}}\right)\Bigg\}.$$

If $\mathfrak{f}_\chi/\pi^i$ is a proper divisor of $\mathfrak{f}_{\chi\psi}$, then we have $i > r'$ with the exponent r' determined by $(\lambda) = \mathfrak{p}^{r'}$, and (8) shows

$$(9)\qquad \sum_s \chi\left(\frac{s}{\pi^i}\right)\psi\left(1-\frac{s}{\pi^i}\right) = 0.$$

If conversely $i < r'$, then, provided that $\mathfrak{f}_{\chi\psi} = 1$, the following relation holds for any unit γ in $F_\mathfrak{p}$ and for $\mathfrak{a}_i = \mathfrak{f}_\chi/\pi^i$:

$$\sum_{\substack{t' \bmod \mathfrak{a}_i \\ t'\equiv\gamma\,(\mathfrak{f}_{\chi\psi})}} e\left(\frac{t'}{\varphi_\chi\pi^{-i}}\right) = e\left(\frac{\gamma}{\varphi_\chi\pi^{-i}}\right)\sum_{\substack{t'' \bmod \mathfrak{a}_i \\ t''\equiv 0\,(\mathfrak{f}_{\chi\psi})}} e\left(\frac{t''}{\varphi_\chi\pi^{-i}}\right) = 0.$$

Therefore we have

$$(10)\qquad \sum_{t'}\chi\psi(t')e\left(\frac{t'}{\varphi_\chi\pi^{-i}}\right) = \sum_{\substack{\gamma \bmod \mathfrak{f}_{\chi\psi} \\ \gamma\not\equiv 0\,(\mathfrak{p})}} \chi\psi(\gamma)\sum_{\substack{t' \bmod \mathfrak{a}_i \\ t'\equiv\gamma\,(\mathfrak{f}_{\chi\psi})}} e\left(\frac{t'}{\varphi_\chi\pi^{-i}}\right) = 0$$

and it follows from (9) and (10) that

$$\tau(\chi)\tau(\psi) = \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\times$$

$$\times \sum_{\substack{s \bmod \mathfrak{f}_\chi \\ s\not\equiv 0,\, s/\pi^{r'}\not\equiv 1\,(\mathfrak{p})}} \chi\left(\frac{s}{\pi^{r'}}\right)\psi\left(1-\frac{s}{\pi^{r'}}\right)\cdot\chi\psi(\pi^{r'})\sum_{\substack{t' \bmod \mathfrak{f}_{\chi\psi} \\ t'\not\equiv 0\,(\mathfrak{p})}}\chi\psi(t')\,e\left(\frac{t'}{\varphi_\chi\pi^{-r'}}\right)$$

$$= \chi\psi(\varphi_{\chi\psi})^{-1}\chi\psi(\lambda)^{-1}\sum_s \chi\left(\frac{s}{\lambda}\right)\psi\left(1-\frac{s}{\lambda}\right)\cdot\chi\psi(\lambda)\sum_{t'}\chi\psi(t')\,e\left(\frac{t'}{\varphi_{\chi\psi}}\right)$$

$$= \tau(\chi\psi)\sum_s \chi\left(\frac{s}{\lambda}\right)\psi\left(1-\frac{s}{\lambda}\right).$$

Hence, under the assumtpion $\mathfrak{f}_{\chi\psi}\neq 1$, we have

$$\text{(11)}\qquad \frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)} = \sum_{\substack{s \bmod \mathfrak{f}_\chi \\ s\not\equiv 0,\, s/\lambda\not\equiv 1\,(\mathfrak{p})}} \chi\left(\frac{s}{\lambda}\right)\psi\left(1-\frac{s}{\lambda}\right)\qquad (\mathfrak{f}_\chi = \mathfrak{f}_\psi = \lambda\mathfrak{f}_{\chi\psi}),$$

where the sum is extended over all prime residue classes mod. $\mathfrak{f}_\chi$ with the additional condition $s/\lambda\not\equiv 1 \pmod{\mathfrak{p}}$, which may be omitted unless λ is a unit.

If we again use (7), the right hand side of (11) turns out

$$\text{(12)}\qquad \frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)} = N(\lambda)\sum_{\substack{s \bmod \mathfrak{f}_{\chi\psi} \\ s\not\equiv 0,\, s/\lambda\not\equiv 1\,(\mathfrak{p})}} \chi\left(\frac{s}{\lambda}\right)\psi\left(1-\frac{s}{\lambda}\right)\qquad (\mathfrak{f}_\chi = \mathfrak{f}_\psi = \lambda\mathfrak{f}_{\chi\psi}).$$

The formula (12) is proved whenever $\mathfrak{f}_{\chi\psi}\neq 1$. But, as the matter of fact, (12) is also valid even if $\mathfrak{f}_{\chi\psi} = 1$.

To show this, assume first $\mathfrak{f}_\chi = \mathfrak{f}_\psi \neq 1$, $\mathfrak{f}_{\chi\psi} = 1$. Then it follows from $\chi\psi(t') = 1$ that

$$\tau(\chi)\tau(\psi) = \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\times$$

$$\times\sum_i\Bigg\{\sum_{\substack{s \bmod \mathfrak{f}_\chi \\ s\not\equiv 0,\, s/\pi^i\not\equiv 1\,(\mathfrak{p})}}\chi\left(\frac{s}{\pi^i}\right)\psi\left(1-\frac{s}{\pi^i}\right)\Bigg\}\Bigg\{\chi\psi(\pi^i)\sum_{\substack{t' \bmod \mathfrak{f}_\chi/\pi^i \\ t'\not\equiv 0\,(\mathfrak{p})}} e\left(\frac{t'}{\varphi_\chi\pi^{-i}}\right)\Bigg\}.$$

Since

$$\sum_{\substack{t' \bmod \mathfrak{f}_\chi/\pi^i \\ t'\not\equiv 0\,(\mathfrak{p})}} e\left(\frac{t'}{\varphi_\chi\pi^{-i}}\right) = \begin{cases} 0 & \text{for}\quad i < r-1, \\ -1 & \text{for}\quad i = r-1, \\ 1 & \text{for}\quad i = r, \end{cases}$$

we have

$$\tau(\chi)\tau(\psi) = \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\Bigg\{-\chi\psi(\pi^{r-1})\sum_s \chi\left(\frac{s}{\pi^{r-1}}\right)\psi\left(1-\frac{s}{\pi^{r-1}}\right) +$$

$$+\chi\psi(\pi^r)\sum_s\chi\left(\frac{s}{\pi^r}\right)\psi\left(1-\frac{s}{\pi^r}\right)\Bigg\}$$

$$= \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\Big\{-\sum_s\chi(s)\psi(\pi^{r-1}-s)+\sum_s\chi(s)\psi(\pi^r-s)\Big\}$$

$$= \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\Bigg\{-\sum_s\psi\left(\frac{\pi^{r-1}}{s}-1\right)+\sum_s\psi\left(\frac{\pi^r}{s}-1\right)\Bigg\}$$

$$= \chi(\varphi_\chi)^{-1}\psi(\varphi_\psi)^{-1}\psi(-1)\Bigg(-\sum_{\substack{s' \bmod \mathfrak{f}_\chi \\ s'\not\equiv 0,\, s'\pi^{r-1}\not\equiv 1\,(\mathfrak{p})}}\psi(1-s'\pi^{r-1})+\sum_{\substack{s' \bmod \mathfrak{f}_\chi \\ s\not\equiv 0\,(\mathfrak{p})}}\psi(1)\Bigg)$$

$$= \chi\psi(\varphi_\chi)^{-1}\psi(-1)\left(\frac{N\mathfrak{p}^r-N\mathfrak{p}^{r-1}}{N\mathfrak{p}-1}+N\mathfrak{p}^r-N\mathfrak{p}^{r-1}\right)$$

$$= N(\lambda)\chi\psi(\lambda)^{-1}\psi(-1)\chi\psi(\mathfrak{d})^{-1} = \tau(\chi\psi)N(\lambda)\chi\left(\frac{1}{\lambda}\right)\psi\left(1-\frac{1}{\lambda}\right).$$

So, in this case, (12) is also true. If next $\mathfrak{f}_\chi = \mathfrak{f}_\psi = \mathfrak{f}_{\chi\psi} = 1$, then $\tau(\chi)\tau(\psi) = \chi(\mathfrak{d})^{-1}\psi(\mathfrak{d})^{-1} = \chi\psi(\mathfrak{d})^{-1} = \tau(\chi\psi)$. 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 $\mathfrak{f}_\chi = \mathfrak{f}_\psi = \mathfrak{f}_{\chi\psi} = 1$ and $N\mathfrak{p} = 2$, then the sum in (12) is nonsence. It is convenient to regard such a sum always to be 1, although it plays no essential role.

2. Let χ, ψ be congruence characters of F. We denote by $j_\mathfrak{p}(\chi,\psi)$ the generalized Jacobi sum of $\mathfrak{p}$-components $\chi_\mathfrak{p}$, $\psi_\mathfrak{p}$ of χ,ψ. In a explicit form, we have

$$\text{(13)}\qquad j_\mathfrak{p}(\chi,\psi) = \begin{cases} \displaystyle\sum_{\substack{s \bmod \mathfrak{f}_{\chi,\mathfrak{p}} \\ s\not\equiv 0\,(\mathfrak{p})}}\chi_\mathfrak{p}(\lambda s)\psi_\mathfrak{p}(1-\lambda s) & (\mathfrak{f}_{\chi,\mathfrak{p}}\lambda = \mathfrak{f}_{\psi,\mathfrak{p}},\ \lambda\in\mathfrak{p}), \\ \displaystyle\sum_{\substack{s \bmod \mathfrak{f}_{\chi\psi,\mathfrak{p}} \\ s\not\equiv 0,\, s/\lambda\not\equiv 1\,(\mathfrak{p})}}\chi_\mathfrak{p}\left(\frac{s}{\lambda}\right)\psi_\mathfrak{p}\left(1-\frac{s}{\lambda}\right) & (\mathfrak{f}_{\chi,\mathfrak{p}} = \mathfrak{f}_{\psi,\mathfrak{p}} = \lambda\mathfrak{f}_{\chi\psi,\mathfrak{p}}). \end{cases}$$

As for the case where the relation $\mathfrak{f}_{\chi,\mathfrak{p}} = \mathfrak{f}_{\psi,\mathfrak{p}}\lambda$ $(\lambda\in\mathfrak{p})$ holds, we may define $j_\mathfrak{p}(\chi,\psi)$ by setting $j_\mathfrak{p}(\chi,\psi) = j_\mathfrak{p}(\psi,\chi)$. It follows from (5) and (12) that

$$\text{(14)}\qquad \frac{\tau_\mathfrak{p}(\chi)\tau_\mathfrak{p}(\psi)}{\tau_\mathfrak{p}(\chi\psi)} = \begin{cases} j_\mathfrak{p}(\chi,\psi) & (\mathfrak{f}_{\chi,\mathfrak{p}}|\mathfrak{f}_{\psi,\mathfrak{p}},\ \mathfrak{f}_{\chi,\mathfrak{p}}\neq\mathfrak{f}_{\psi,\mathfrak{p}}) \\ N(\lambda)j_\mathfrak{p}(\chi,\psi) & (\mathfrak{f}_{\chi,\mathfrak{p}} = \mathfrak{f}_{\psi,\mathfrak{p}} = \lambda\mathfrak{f}_{\chi\psi,\mathfrak{p}}). \end{cases}$$

Therefore (3) yields

$$|j_{\mathfrak{p}}(\chi,\psi)| = \sqrt{\min(N\mathfrak{f}_{\chi,\mathfrak{p}}, N\mathfrak{f}_{\psi,\mathfrak{p}}, N\mathfrak{f}_{\chi\psi,\mathfrak{p}})} \tag{15}$$

for any two congruence characters χ, ψ.

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

$$\chi_{\alpha,\mathfrak{p}} = \left(\frac{*,\alpha}{\mathfrak{p}}\right)_m.$$

For such characters χ_α, χ_β, we set

$$j_{\mathfrak{p}}(\alpha,\beta) = j_{\mathfrak{p}}(\chi_\alpha,\chi_\beta).$$

For the sake of convenience, we write furthermore $\mathfrak{f}_{\alpha,\mathfrak{p}}$, $\tau(\alpha)$, $\tau_{\mathfrak{p}}(\alpha)$, $w(\alpha)$, and $w_{\mathfrak{p}}(\alpha)$ for $\mathfrak{f}_{\chi_\alpha,\mathfrak{p}}$, $\tau(\chi_\alpha)$, $\tau_{\mathfrak{p}}(\chi_\alpha)$, $w(\chi_\alpha)$, and $w_{\mathfrak{p}}(\chi_\alpha)$, respectively.

Now, the aim of this § is to determine explicitly the value of $j_{\mathfrak{p}}(\alpha,\beta)$, provided that $m=2$. The result is as follows:

$$j_{\mathfrak{p}}(\alpha,\beta) = \left(\frac{\alpha,\beta}{\mathfrak{p}}\right)\sqrt{\min(N\mathfrak{f}_{\alpha,\mathfrak{p}}, N\mathfrak{f}_{\beta,\mathfrak{p}}, N\mathfrak{f}_{\alpha\beta,\mathfrak{p}})}, \tag{16}$$

where we write $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)$ for $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)_2$.

Since it follows from (3), (14), and (15) that (16) is equivalent with

$$\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = \frac{w_{\mathfrak{p}}(\alpha)w_{\mathfrak{p}}(\beta)}{w_{\mathfrak{p}}(\alpha\beta)} \quad (\alpha,\beta\in F,\ \alpha\neq 0,\ \beta\neq 0), \tag{17}$$

it suffices to prove the latter relation.

If $\mathfrak{p}$ is infinite, then (16) is clear from the definition. If $\mathfrak{p}$ is finite and does not divide 2, then, instead of (17), (16) is proved directly by the defining formula (13) of the generalized Jacobi sum. Namely, since in this case

$$\min(N\mathfrak{f}_{\alpha,\mathfrak{p}}, N\mathfrak{f}_{\beta,\mathfrak{p}}, N\mathfrak{f}_{\alpha\beta,\mathfrak{p}}) = 1,$$

we have simply to show

$$j_{\mathfrak{p}}(\alpha,\beta) = \left(\frac{\alpha,\beta}{\mathfrak{p}}\right). \tag{18}$$

If the exponents of $\mathfrak{p}$ in α,β are both even, then $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right)=1$ and by the formula of (13), we have $j_{\mathfrak{p}}(\alpha,\beta)=1$. (Put $\lambda=1$ and let s be any unit $\not\equiv 1\ (\mathfrak{p})$.) If the exponent of $\mathfrak{p}$ in α is even and that of β is odd, then $\left(\frac{\alpha,\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)$ and by the upper formula of (13) we have $j_{\mathfrak{p}}(\alpha,\beta) = \left(\frac{\pi,\alpha}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)$, where π is a prime element of $\mathfrak{p}$. (Set $\lambda=\pi$ and $s=1$.) If finally the exponents of $\mathfrak{p}$ in α and β are both odd, again the lower formula of (13) shows

$$j_{\mathfrak{p}}(\alpha,\beta) = \left(\frac{1/\pi,\alpha}{\mathfrak{p}}\right)\left(\frac{1-1/\pi,\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha\beta}{\mathfrak{p}}\right)\left(\frac{-1}{\mathfrak{p}}\right) = \left(\frac{\alpha,\beta}{\mathfrak{p}}\right).$$

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

It remains therefore to prove (17) in the case where $\mathfrak{p}$ divides 2. Let $\mathfrak{l}_1,\ldots,\mathfrak{l}_t$ be all the prime divisors of 2 in F and $\mathfrak{l}$ be any one of them. Then, for non-zero $\alpha,\beta\in F$, it follows from the approximation theorem of valuation that there exists $\alpha^*\in F$ such that α/α^* is a square in $F_{\mathfrak{l}}$ and α^* itself is a square in every $F_{\mathfrak{l}_i}$ with $\mathfrak{l}_i\neq\mathfrak{l}$. We choose similary a β^* for β. Then, as direct consequences of (3) and (4), we have

$$w_{\mathfrak{l}_i}(\alpha^*) = w_{\mathfrak{l}_i}(\beta^*) = w_{\mathfrak{l}_i}(\alpha^*\beta^*) = 1 \quad (\mathfrak{l}_i\neq\mathfrak{l}),$$

$$w_{\mathfrak{l}}(\alpha^*) = w_{\mathfrak{l}}(\alpha), \quad w_{\mathfrak{l}}(\beta^*) = w_{\mathfrak{l}}(\beta), \quad w_{\mathfrak{l}}(\alpha^*\beta^*) = w_{\mathfrak{l}}(\alpha\beta),$$

$$\left(\frac{\alpha^*,\beta^*}{\mathfrak{l}}\right) = \left(\frac{\alpha,\beta}{\mathfrak{l}}\right), \quad \left(\frac{\alpha^*,\beta^*}{\mathfrak{l}_i}\right) = 1 \quad (\mathfrak{l}_i\neq\mathfrak{l}).$$

On the other hand, since $\chi_\alpha, \chi_\beta, \chi_{\alpha\beta}$ are all quadratic, the general theory of Hecke's L-function shows that $w(\alpha)=w(\beta)=w(\alpha\beta)=1$. (See, e. g. Hasse [2].)

Hence we have

$$1 = \frac{w(\alpha^*)w(\beta^*)}{w(\alpha^*\beta^*)} = \prod_{\mathfrak{p}}\frac{w_{\mathfrak{p}}(\alpha^*)w_{\mathfrak{p}}(\beta^*)}{w_{\mathfrak{p}}(\alpha^*\beta^*)} = \prod_{\mathfrak{p}\nmid 2}\left(\frac{\alpha^*,\beta^*}{\mathfrak{p}}\right)\prod_{\mathfrak{p}_\infty}\left(\frac{\alpha^*,\beta^*}{\mathfrak{p}_\infty}\right)\frac{w_{\mathfrak{l}}(\alpha^*)w_{\mathfrak{l}}(\beta^*)}{w_{\mathfrak{l}}(\alpha^*\beta^*)}.$$

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

$$\left(\frac{\alpha^*,\beta^*}{\mathfrak{l}}\right) = \frac{w_{\mathfrak{l}}(\alpha^*)w_{\mathfrak{l}}(\beta^*)}{w_{\mathfrak{l}}(\alpha^*\beta^*)}.$$

This means

$$\left(\frac{\alpha,\beta}{\mathfrak{l}}\right) = \frac{w_{\mathfrak{l}}(\alpha)w_{\mathfrak{l}}(\beta)}{w_{\mathfrak{l}}(\alpha\beta)}.$$

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 $F = \Omega$ is rational number field and $\mathfrak{p} = 2$. Let Ω_2^* be the multiplicative group of non-zero elements of the 2-adic number field Ω_2. Then, for every representative of Ω_2^*/Ω_2^{*2}, the value of $w_2(\alpha)$ is given by

$$\begin{array}{lcccccccc} \alpha & = 1, & 5, & -1, & -5, & 2, & 10, & -2, & -10 \\ w_2(\alpha) & = 1, & 1, & i, & i, & 1, & -1, & i, & -i. \end{array}$$

This gives, for example,

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

References

[1] B. Dwork, *On the Artin root number*, Amer. J. Math. 78 (1956), pp. 444-472.

[2] H. Hasse, Bericht I (1926), Ia (1927), II (1930), Jahresbericht der D. M. V.

[3] — *Vorlesungen über Zahlentheorie*, Berlin 1950.

[4] — *Artinsche Führer, Artinsche L-Funktionen und Gaußsche Summen über endlich-algebraischen Zahlkörpern*, Acta Salmanticensia, Universidad de Salamanca (1954).

[5] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig 1923.

[6] E. Lamprecht, *Allgemeine Theorie der Gaussschen Summen in endlichen kommutativen Ringen*, Math. Nachr. *9* (1953), pp. 149-196.

[7] A. Weil, *Jacobi sums as "Grössencharactere"*, Trans. Amer. Math. Soc. *72* (1952), pp. 487-495.

MATHEMATICAL INSTITUTE
NAGOYA UNIVERSITY

Reçu par la Rédaction le 6. 4. 1960

ACTA ARITHMETICA
VI (1961)

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 $ku+l$, $(k, l) = 1$, $u = 0, 1, 2, \ldots$ does not exceed k^c. In 1954 Rodosskiĭ (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 Rodosskiĭ's proof in 1955 I proved (see [2]) the existence of an absolute constant $c > 0$ such that there is at least one prime $p \equiv l \,(\mathrm{mod}\, k)$, $(k, l) = 1$, in the interval

$$(1) \qquad (x, xk^c) \quad \text{for all} \quad x \geqslant 1$$

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

$$(2) \qquad \pi(x; k, l) > xk^{-c_1} \quad \text{for all} \quad x \in (k^{c_2}, k^{k^2}),$$

if $(k, l) = 1$ and $\pi(x; k, l)$ denotes the number of primes $p \equiv l \,(\mathrm{mod}\, k)$ not exceeding x.

The estimates (1) and (2) are of some importance for $x < \exp k^{\varepsilon_1}$, ε_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 χ modulo k is the reason why the existing estimates of $\pi(x; k, l)$ and estimates of the difference of consecutive primes $\equiv l \,(\mathrm{mod}\, k)$ fail to give us any positive information. For $x \geqslant \exp k^{\varepsilon_1}$ and $k > k_0(\varepsilon_1)$ according to Tchudakoff ([3]) there is at least one prime $\equiv l \,(\mathrm{mod}\, k)$ in the interval

$$(3) \qquad (x, x(1+x^{-1/4})),$$

and $\pi(x; k, l) > c_3(\varepsilon_1)x/\varphi(k)\log x$, where $\varphi(k)$ is Euler's function denoting the number of natural numbers $l \leqslant k$ with $(l, k) = 1$ (1).

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