ACTA ARITHMETICA
LXXV.1 (1996)

# Distribution of lattice points on hyperbolic surfaces

by

VSEVOLOD F. LEV (Tel-Aviv)

Let two lattices $\Lambda', \Lambda'' \subset \mathbb{R}^s$ have the same number of points on each hyperbolic surface $|x_1 \dots x_s| = C$. We investigate the case when $\Lambda'$, $\Lambda''$ are sublattices of $\mathbb{Z}^s$ of the same prime index and show that then $\Lambda'$ and $\Lambda''$ must coincide up to renumbering the coordinate axes and changing their directions.

**1. Introduction.** If the opposite is not stated explicitly, we denote vectors by lower-case italic and Greek letters and their coordinates by the same letters with appropriate lower indices. This paper's aim is to prove the following result.

THEOREM 1. *Let $\Lambda'$, $\Lambda''$ be two sublattices of $\mathbb{Z}^s$ of the same prime index, having the same number of points on each surface*

$$|x_1 \dots x_s| = C.$$

*Then $\Lambda''$ may be obtained from $\Lambda'$ (and vice versa) by renumbering the coordinate axes and changing their directions.*

It would be interesting to extend this theorem to the case of $\mathbb{Z}^s$-sublattices of non-prime indices, and also to investigate the case of general $\mathbb{R}^s$-sublattices, when rotations around the bisectrices $\pm x_1 = \dots = \pm x_s$ should also be taken into account. However, this may present some unexpected difficulties, as shown already for $s = 2$ by the example of

$$\Lambda' = \{m \in \mathbb{Z}^2 \mid m_1 \equiv 0 \pmod 4\},$$
$$\Lambda'' = \{m \in \mathbb{Z}^2 \mid m_1, m_2 \equiv 0 \pmod 2\}.$$

Both these lattices are of index 4, and they evidently have the same number of points on each hyperbola $|x_1 x_2| = C$.

1991 *Mathematics Subject Classification*: Primary 11P21; Secondary 52Cxx, 11Hxx.
*Key words and phrases*: lattice, hyperbolic surface.

One may also investigate surfaces of other types, say, spheres. A special class of hyperbolas-like surfaces arises in the theory of uniform distribution, where one often encounters functions of the form

$$Z(t,\Lambda)=\sum_{m\in\Lambda}\frac{1}{(\overline{m}_1\ldots\overline{m}_s)^t},$$

where $\overline{m}_i=\max\{1,|m_i|\}$. It is natural to consider those $\Lambda'$, $\Lambda''$ for which $Z(t,\Lambda')=Z(t,\Lambda'')$ and evidently this means that on each surface of the form $\overline{x}_1\ldots\overline{x}_s=C$ there is the same number of points of $\Lambda'$ and $\Lambda''$. Using the method of this paper, one can prove that Theorem 1 remains valid also for these surfaces instead of pure hyperbolas (though the proof would require substantially greater amount of calculations).

No other results concerning this kind of problems are known to the author.

**2. Sublattices of prime index.** In this section we establish the structure of $\mathbb{Z}^s$-sublattices of prime index, and thus reduce the considered problem to an algebraic one.

In what follows $p$ will stand for a fixed prime number. For $\lambda\in\mathbb{Z}$ (or $\lambda\in\mathbb{F}_p$) define

$$\delta_p(\lambda)=\begin{cases}1 & \text{if } \lambda\equiv 0 \pmod p,\\ 0 & \text{if } \lambda\not\equiv 0 \pmod p.\end{cases}$$

LEMMA 1. *Let $a\in\mathbb{F}_p^s$ and assume $a\neq 0$. Then the set*

$$\Lambda_a=\{m\in\mathbb{Z}^s \mid \delta_p(a_1m_1+\ldots+a_sm_s)=1\}$$

*is a $\mathbb{Z}^s$-sublattice of index $p$ and moreover, every $\mathbb{Z}^s$-sublattice of index $p$ is of this form for a properly chosen $a$.*

Proof. Suppose $a_s\neq 0$, denote by $a_s'$ the inverse to $a_s$ in $\mathbb{F}_p$ and let $a_i^*=-a_ia_s'$ $(i=1,\ldots,s-1)$. Consider the matrix

$$E=\begin{pmatrix}1 & 0 & \ldots & 0 & 0\\ 0 & 1 & \ldots & 0 & 0\\ \cdot & \cdot & & \cdot & \cdot\\ \cdot & \cdot & & \cdot & \cdot\\ \cdot & \cdot & & \cdot & \cdot\\ 0 & 0 & \ldots & 1 & 0\\ a_1^* & a_2^* & \ldots & a_{s-1}^* & p\end{pmatrix}.$$

Its columns form a basis for some lattice $\Lambda$ of index $|\det E|=p$, while each column obviously belongs to $\Lambda_a$. Hence $\Lambda\subseteq\Lambda_a$, and therefore either $\Lambda_a=\Lambda$, or $\Lambda_a=\mathbb{Z}^s$. Obviously it is the first possibility that really holds, and thus $\Lambda_a=\Lambda$ is a lattice of index $p$.

Conversely, let $\Lambda \subset \mathbb{Z}^s$ be a lattice of index $p$ generated by some matrix $E$. Then $\det E = \pm p$, and, therefore, there exists a vector $a \in \mathbb{F}_p^s$, $a \neq 0$, such that $E^T a \equiv 0 \pmod p$ (more precisely, all the coordinates of $E^T a$ are divisible by $p$). Hence, each column $e$ of $E$ satisfies $a_1 e_1 + \ldots + a_s e_s \equiv 0 \pmod p$, thus $\Lambda \subseteq \Lambda_a$. But (by the already proved part of the lemma) both these lattices are of the same index $p$, so $\Lambda = \Lambda_a$. ■

Obviously, $\Lambda_a$ does not change if we multiply $a$ by a non-zero residue $\lambda \in \mathbb{F}_p$. If we permute the coordinates of $a$, the new lattice may be obtained from the original one by renumbering the coordinate axes. And if we change the signs of some of the coordinates $a_i$, this maps the lattice symmetrically relative to the hyperplanes $x_i = 0$. This shows that if

$$T_a(C) = \sum_{|m_1 \ldots m_s| = C} \delta_p(a_1 m_1 + \ldots + a_s m_s) \tag{1}$$

is the number of points of $\Lambda_a$ on the surface $|x_1 \ldots x_s| = C$, then Theorem 1 will follow from (and is actually equivalent to) the following theorem:

THEOREM 1′. *Assume $T_a(C) = T_b(C)$ for some fixed non-zero $a, b \in \mathbb{F}_p^s$ and every integer $C$. Then $b$ may be obtained from $a$ (and vice versa) by means of multiplying by a non-zero residue $\lambda \in \mathbb{F}_p$, reordering the coordinates and changing the signs of some of them.*

We write $a \sim b$ if $a$ and $b$ are related as described in this theorem.

We show now that without loss of generality we may restrict ourselves to the case when *all the coordinates of $a$, $b$ are non-zero*. This will include two steps. As the first step, we suppose $T_a(C) = T_b(C)$ for every $C$ and prove that $a$ and $b$ have the same number of non-zero coefficients. To this end, assume

$$a = (a_1, \ldots, a_{s'}, 0, \ldots, 0), \qquad b = (b_1, \ldots, b_{s''}, 0, \ldots, 0),$$

where $a_1, \ldots, a_{s'}, b_1, \ldots, b_{s''} \neq 0$, and define

$$\alpha = (a_1, \ldots, a_{s'}), \qquad \beta = (b_1, \ldots, b_{s''}).$$

If $(m_1, \ldots, m_s)$ contributes a non-zero term to the sum $T_a(1)$, then $(m_1, \ldots \ldots, m_{s'})$ contributes a non-zero term to $T_\alpha(1)$, and it is easily seen that every such $(m_1, \ldots, m_{s'})$ will be induced in this way by exactly $2^{s-s'}$ vectors (as the coordinates $m_{s'+1}, \ldots, m_s$ can be independently picked out to be $\pm 1$). The same applies to $T_b(1)$ and $T_\beta(1)$, and therefore

$$T_a(1) = 2^{s-s'} T_\alpha(1), \qquad T_b(1) = 2^{s-s''} T_\beta(1), \tag{2}$$

and for brevity we denote this common value by $T$. Furthermore, if $q$ is prime then

$$T_a(q) = 2^{s-s'} T_\alpha(q) + 2^{s-s'}(s - s') T_\alpha(1) = 2^{s-s'} T_\alpha(q) + (s - s')T, \tag{3}$$

$$(4)\quad T_b(q) = 2^{s-s''}T_\beta(q) + 2^{s-s''}(s-s'')T_\beta(1) = 2^{s-s''}T_\beta(q) + (s-s'')T.$$

By the Dirichlet theorem, for each $z = 1, \ldots, p-1$ there exists a prime $q_z$ with $q_z \equiv z \pmod p$, and for $z = 0$ choose $q_0 = p$. Substituting this $q_z$ into (3), (4) and summing up over all $z$ one obtains

$$(5)\qquad 2^{s-s'}\sum_{z=0}^{p-1} T_\alpha(q_z) + p(s-s')T = 2^{s-s''}\sum_{z=0}^{p-1} T_\beta(q_z) + p(s-s'')T.$$

But the sums in the latter identity may be explicitly evaluated:

$$\begin{aligned}
&\sum_{z=0}^{p-1} T_\alpha(q_z)\\
&\quad= \sum_{z=0}^{p-1}\ \sum_{\varepsilon_1,\ldots,\varepsilon_{s'}=0}^{1}\ \sum_{i=1}^{s'} \delta_p((-1)^{\varepsilon_1}a_1 + \ldots + (-1)^{\varepsilon_i}q_z a_i + \ldots + (-1)^{\varepsilon_{s'}}a_{s'})\\
&\quad= \sum_{\varepsilon_1,\ldots,\varepsilon_{s'}=0}^{1}\ \sum_{i=1}^{s'}\sum_{z=0}^{p-1} \delta_p((-1)^{\varepsilon_1}a_1 + \ldots + (-1)^{\varepsilon_i}z a_i + \ldots + (-1)^{\varepsilon_{s'}}a_{s'})\\
&\quad= 2^{s'}s',
\end{aligned}$$

and similarly,

$$\sum_{z=0}^{p-1} T_\beta(q_z) = 2^{s''}s''.$$

Hence (5) yields

$$\begin{gathered}
2^s s' + p(s-s')T = 2^s s'' + p(s-s'')T,\\
s'(2^s - pT) = s''(2^s - pT),
\end{gathered}$$

and so $s' = s''$, unless $p = 2$. But if $p = 2$, then

$$T = T_a(1) = \begin{cases} 2^s & \text{if } s' \equiv 0 \pmod 2,\\ 0 & \text{if } s' \not\equiv 0 \pmod 2,\end{cases}$$

therefore $2^s \neq pT$ and $s' = s''$ also in this case. Observe that this completely settles Theorem 1′ for $p = 2$, and in what follows we will assume $p$ to be *odd*.

Next (and this is our second step), we show that $T_\alpha(C) = T_\beta(C)$ provided $T_a(C) = T_b(C)$ (for each $C$). For $C = 1$ this follows from (2) (in view of $s' = s''$); and for $C > 1$ we have

$$T_a(C) = 2^{s-s'}T_\alpha(C) + 2^{s-s'}\sum_{d\mid C,\, d<C} k_{C/d}T_\alpha(d),$$

where $k_{C/d}$ are some combinatorial coefficients which do not depend on $a$, but only on $s-s'$ and on the system of exponents in the prime decomposition of $C/d$. A similar equality holds for $T_b(C)$, and thus the required conclusion follows by induction on $C$.

Now, if we prove Theorem $1'$ for vectors with non-zero coordinates, then $T_\alpha(C) = T_\beta(C)$ implies $\alpha \sim \beta$, and hence $a \sim b$. Thus we arrive at the final form of the theorem to be proved:

THEOREM $1''$. *Let $p$ be an odd prime, and let $a, b \in (\mathbb{F}_p^\times)^s$. Assume $T_a(C) = T_b(C)$ for all integer $C$. Then $a \sim b$.*

**3. Even Dirichlet characters.** The starting point of our proof is as follows: along with $T_a(C)$, we consider all the values $T_c(C)$ for $c \in (\mathbb{F}_p^\times)^s$, sum them up and then select $T_a(C)$ using characters of the group $(\mathbb{F}_p^\times)^s$. But characters of $(\mathbb{F}_p^\times)^s$ are closely related to the Dirichlet characters of $\mathbb{F}_p^\times$. And of all the characters of $\mathbb{F}_p^\times$, of particular interest for us will be the *even* ones (those for which $\chi(-1) = 1$). The even characters form a subgroup of index 2 in the group of *all* characters, and we denote this subgroup by $X$. Also, we denote by $G$ the multiplicative group of all squares of $\mathbb{F}_p^\times$, and by $\widehat{G}$ the dual group of characters of $G$. Most of the properties of $X$ we use will be derived from the following simple lemma.

LEMMA 2. *The mapping $\widehat{G} \to X$ defined by*

$$\chi \ \mapsto \ (n \mapsto \chi(n^2)) \qquad (n \in \mathbb{F}_p^\times)$$

*establishes an isomorphism $\widehat{G} \cong X$.*

Proof. The above mapping is obviously an injective homomorphism, and $|\widehat{G}| = |G| = (p-1)/2 = |X|$. ∎

COROLLARY 1.

(i) *$X$ is cyclic.*

(ii) *For $\lambda \in \mathbb{F}_p^\times$,*

$$\sum_{\chi \in X} \chi(\lambda) = \begin{cases} (p-1)/2 & \text{if } \lambda = \pm 1, \\ 0 & \text{if } \lambda \neq \pm 1. \end{cases}$$

(iii) *Each complex multiplicative function on $X$ (that is, each character of $X$) is of the form $\chi \mapsto \chi(\lambda)$ for some fixed $\lambda \in \mathbb{F}_p^\times$ (and even $\lambda \in G$).*

Proof.

(i) $X \cong \widehat{G} \cong G$, and $G$ is cyclic.

(ii) follows from the orthogonality relation for group $G$.

(iii) follows from the canonical homomorphism between $G$ and $\widehat{\widehat{G}}$ (the group of characters of $\widehat{G}$). ∎

By $\chi_0$ we denote the principal character of $\mathbb{F}_p^\times$, and by $\overline{\chi}$ the character conjugate to $\chi$.

Lemma 3. *Let $X_0 \subseteq X$ be a set of even characters such that $\chi_0 \in X_0$, and if $\chi \in X_0$ then necessarily $\overline{\chi} \in X_0$. Let also $f : X_0 \to \mathbb{C}$ be a complex function on $X_0$ such that $\chi_1 \ldots \chi_r = \chi_0$ implies $f(\chi_1) \ldots f(\chi_r) = 1$ for every $r \geq 1$ and $\chi_1, \ldots, \chi_r \in X_0$. Then $f$ can be extended to a multiplicative function on all $X$.*

Proof. First, observe that $f$ can be extended to the subgroup $\widetilde{X}_0 \subseteq X$ generated by $X_0$: if $\chi = \chi_1 \ldots \chi_r$ $(\chi_1, \ldots, \chi_r \in X_0)$, we put $f(\chi) = f(\chi_1) \ldots f(\chi_r)$, and it is easily verified that this correctly defines $f$ as a multiplicative function on $\widetilde{X}_0$.

Next, if $\chi$ is a generating element of $X$, then all elements of $\widetilde{X}_0$ are powers of $\chi$, and we choose $\nu$ to be the smallest positive integer with $\chi^\nu$ in $\widetilde{X}_0$. Now, we choose the value of $f(\chi)$ to satisfy $f^\nu(\chi) = f(\chi^\nu)$, and then we define $f(\chi^n) = f^n(\chi)$ for every integer $n$. ∎

**4. Proof of Theorem 1″.** We start with fulfilling the plan outlined in the previous section: by (1), we have

$$T_a(C) = (p-1)^{-s} \sum_c \sum_{m_1 \ldots m_s = \pm C} \delta_p(c_1 m_1 + \ldots + c_s m_s) \times \sum_\chi \chi_1(c_1' a_1) \ldots \chi_s(c_s' a_s),$$

where $c = (c_1, \ldots, c_s)$ runs over all elements of $(\mathbb{F}_p^\times)^s$; next, $\chi$ runs over all collections $(\chi_1, \ldots, \chi_s)$ of Dirichlet characters; finally, $c_i'$ $(i = 1, \ldots, s)$ stands for the inverse of $c_i$ in $\mathbb{F}_p^\times$. For our purposes, it is sufficient to consider only those $C$ for which $C \not\equiv 0 \pmod p$. Then $c_i m_i$ runs over $\mathbb{F}_p^\times$ together with $c_i$, and using multiplicativity of characters we get

$$\begin{aligned} T_a(C) &= (p-1)^{-s} \sum_\chi \chi_1(a_1) \ldots \chi_s(a_s) \sum_{m_1 \ldots m_s = \pm C} \chi_1(m_1) \ldots \chi_s(m_s) \\ &\quad \times \sum_c \overline{\chi}_1(c_1 m_1) \ldots \overline{\chi}_s(c_s m_s) \delta_p(c_1 m_1 + \ldots + c_s m_s) \\ &= (p-1)^{-s} \sum_\chi \sigma(\chi)\ \chi_1(a_1) \ldots \chi_s(a_s) \sum_{m_1 \ldots m_s = \pm C} \chi_1(m_1) \ldots \chi_s(m_s), \end{aligned}$$

where

$$\sigma(\chi) = \sum_c \overline{\chi}_1(c_1) \ldots \overline{\chi}_s(c_s) \delta_p(c_1 + \ldots + c_s).$$

Consider the latter sum. If $\lambda \in \mathbb{F}_p^\times$ is fixed, then $\lambda c$ runs over $(\mathbb{F}_p^\times)^s$ together with $c$, hence

$$\begin{aligned} \sigma(\chi) &= \sum_c \overline{\chi}_1(\lambda c_1) \ldots \overline{\chi}_s(\lambda c_s) \delta_p(\lambda(c_1 + \ldots + c_s)) \\ &= \overline{\chi_1 \cdots \chi_s}(\lambda) \sigma(\chi), \end{aligned}$$

and so $\sigma(\chi) = 0$ if the product $\chi_1 \ldots \chi_s$ is not the principal character $\chi_0$. On the other hand, for $\chi_1 \ldots \chi_s = \chi_0$ and at least one $\chi_i$ distinct from $\chi_0$, we use a well-known representation of $\delta_p$ with complex exponents to obtain

$$\begin{aligned}\sigma(\chi) &= \frac{1}{p}\sum_{z=0}^{p-1}\sum_{c_1,\ldots,c_s=1}^{p-1}\overline{\chi}_1(c_1)\ldots\overline{\chi}_s(c_s)e^{2\pi i(c_1+\ldots+c_s)z/p}\\ &= \frac{1}{p}\sum_{z=1}^{p-1}(\chi_1\ldots\chi_s)(z)\sum_{c_1,\ldots,c_s=1}^{p-1}\overline{\chi}_1(zc_1)\ldots\overline{\chi}_s(zc_s)e^{2\pi i(zc_1+\ldots+zc_s)/p}\\ &= \frac{1}{p}\sum_{z=1}^{p-1}\Big(\sum_{c_1=1}^{p-1}\overline{\chi}_1(c_1)e^{2\pi ic_1/p}\Big)\ldots\Big(\sum_{c_s=1}^{p-1}\overline{\chi}_s(c_s)e^{2\pi ic_s/p}\Big)\\ &= \frac{p-1}{p}\,\tau(\overline{\chi}_1)\ldots\tau(\overline{\chi}_s),\end{aligned}$$

where the Gaussian sums $\tau(\overline{\chi}_i)$ are known to be non-zero. Also, if $\chi_1 = \ldots = \chi_s = \chi_0$ then obviously $\sigma(\chi) \neq 0$. We see that $\sigma(\chi)$ is not 0 if and only if $\chi_1 \ldots \chi_s = \chi_0$, and thus

$$T_a(C) = (p-1)^{-s}\sum_{\chi}{}^{*}\sigma(\chi)\chi_1(a_1)\ldots\chi_s(a_s)\sum_{m_1\ldots m_s=\pm C}\chi_1(m_1)\ldots\chi_s(m_s),$$

where the sum marked by an asterisk extends over all collections of Dirichlet characters with product $\chi_0$. As to the inner sum, it may be written as

$$\sum_{\substack{m_1\ldots m_s=C\\ m_1,\ldots,m_s\geq 1}}(\chi_1(m_1)+\chi_1(-m_1))\ldots(\chi_s(m_s)+\chi_s(-m_s)),$$

and this vanishes if at least one of the characters $\chi_i$ is odd. But otherwise $\chi_i(m_i) + \chi_i(-m_i) = 2\chi_i(m_i)$ and therefore

$$T_a(C) = 2^s(p-1)^{-s}\sum_{\chi}{}^{**}\sigma(\chi)\chi_1(a_1)\ldots\chi_s(a_s)\sum_{m_1\ldots m_s=C}\chi_1(m_1)\ldots\chi_s(m_s),$$

where the sum marked by two asterisks extends over all collections of *even* Dirichlet characters with product $\chi_0$, and the $m_i$ here and in all subsequent sums take only positive values. Group now together those collections $\chi$ which differ only by a permutation. If $\chi'$ and $\chi''$ are two such collections then obviously $\sigma(\chi') = \sigma(\chi'')$, and also

$$\sum_{m_1\ldots m_s=C}\chi_1'(m_1)\ldots\chi_s'(m_s) = \sum_{m_1\ldots m_s=C}\chi_1''(m_1)\ldots\chi_s''(m_s)$$

for each $C$, hence

$$T_a(C) = 2^s(p-1)^{-s}\sum_{\varphi}^{***}\sigma(\varphi)\Big(\sum_{\chi\in P(\varphi)}\chi_1(a_1)\dots\chi_s(a_s)\Big)\times\sum_{m_1\dots m_s=C}\varphi_1(m_1)\dots\varphi_s(m_s),$$

where $\varphi$ runs over all *ordered* collections of even characters with product $\chi_0$, and $\chi$ runs over the set $P(\varphi)$ of all collections which may be obtained by a permutation of $\varphi$.

A similar equality holds, of course, for $T_b(C)$, and thus

$$\sum_{\varphi}^{***}u(\varphi)\sum_{m_1\dots m_s=C}\varphi_1(m_1)\dots\varphi_s(m_s)=0, \tag{6}$$

where we set

$$u(\varphi)=\sigma(\varphi)\Big(\sum_{\chi\in P(\varphi)}\chi_1(a_1)\dots\chi_s(a_s)-\sum_{\chi\in P(\varphi)}\chi_1(b_1)\dots\chi_s(b_s)\Big).$$

The next step is to show that the inner sums in (6), considered as functions of $C$, are linearly independent, and so $u(\varphi)=0$.

We first derive from (6) that for every $r\ge 1$ and every system of residues $n_1,\dots,n_r\in\mathbb{F}_p^\times$ we have

$$\sum_{\varphi}^{***}u(\varphi)\sum_{i_1,\dots,i_r=1}^{s}{}'\,\varphi_{i_1}(n_1)\dots\varphi_{i_r}(n_r)=0; \tag{7}$$

here and below the indices of the dashed sums ($\sum'$) run over pairwise distinct values; for example, in the latter sum $(i_1,\dots,i_r)$ runs over all $r$-element subsets of the set $\{1,\dots,s\}$.

To obtain (7) we use induction on $r$. For $r=1$ the result follows immediately if in (6) we choose $C=q_1$, where $q_1\equiv n_1 \pmod p$ is prime. For $r\ge 2$ we choose pairwise distinct primes $q_i$ with $q_i\equiv n_i \pmod p$ $(i=1,\dots,r)$ and let $C=q_1\dots q_r$. Next, let $\Omega$ run over all partitions of the set $\{1,\dots,r\}$. Denote by $\sum^{(\Omega)}$ the sum over all those $i_1,\dots,i_r$ for which $i_\nu=i_\mu$ if and only if $\nu$ and $\mu$ fall into the same class of the partition $\Omega$. We have

$$\begin{aligned}\sum_{\varphi}^{***}u(\varphi)\sum_{m_1\dots m_s=C}\varphi_1(m_1)\dots\varphi_s(m_s) &= \sum_{\varphi}^{***}u(\varphi)\sum_{i_1,\dots,i_r=1}^{s}\varphi_{i_1}(q_1)\dots\varphi_{i_r}(q_r)\\ &= \sum_{\Omega}\sum_{\varphi}^{***}u(\varphi)\sum_{i_1,\dots,i_r=1}^{s}{}^{(\Omega)}\varphi_{i_1}(n_1)\dots\varphi_{i_r}(n_r).\end{aligned} \tag{8}$$

Now, if $\Omega$ is the partition into $r$ one-element sets, then the inner sum in the latter equality equals

$$\sum_{i_1,\ldots,i_r=1}^{s}{}' \; \varphi_{i_1}(n_1)\ldots\varphi_{i_t}(n_r);$$

and if $\Omega = \{S_1, \ldots, S_t\}$, where $S_1 \cup \ldots \cup S_t = \{1, \ldots, r\}$, $t < r$, then this inner sum equals

$$\sum_{j_1,\ldots,j_t=1}^{s}{}' \; \varphi_{j_1}(N_1)\ldots\varphi_{j_s}(N_t),$$

where $N_\nu = \prod_{i\in S_\nu} n_i$. Since by the induction hypothesis

$$\sum_{\varphi}{}^{***} u(\varphi) \sum_{j_1,\ldots,j_t=1}^{s}{}' \; \varphi_{j_1}(N_1)\ldots\varphi_{j_t}(N_t) = 0,$$

(7) follows from (8) and (6).

Specifically, for $r = s$, (7) yields

$$\sum_{\varphi}{}^{***} u(\varphi) \sum_{i_1,\ldots,i_s=1}^{s}{}' \; \varphi_{i_1}(n_1)\ldots\varphi_{i_s}(n_s) = 0, \tag{9}$$

where $(i_1, \ldots, i_s)$ runs over all permutations of $\{1, \ldots, s\}$.

Let $\chi$ be a fixed collection of even characters with $\chi_1 \ldots \chi_s = \chi_0$. Multiplying (9) by $\overline{\chi}_1(n_1)\ldots\overline{\chi}_s(n_s)$ and summing up over all $n \in (\mathbb{F}_p^\times)^s$ we obtain

$$\sum_{\varphi}{}^{***} u(\varphi) \sum_{i_1,\ldots,i_s=1}^{s}{}' \Big(\sum_{n_1=1}^{p-1} (\overline{\chi}_1\varphi_{i_1})(n_1)\Big)\ldots\Big(\sum_{n_s=1}^{p-1} (\overline{\chi}_s\varphi_{i_s})(n_s)\Big) = 0,$$

thus $u(\chi) = 0$ by the orthogonality relation, since there exists precisely one $\varphi$ and precisely one permutation $(i_1, \ldots, i_s)$ with $\chi_1 = \varphi_{i_1}, \ldots, \chi_s = \varphi_{i_s}$. This shows that

$$\sum_{\chi\in P(\varphi)} \chi_1(a_1)\ldots\chi_s(a_s) = \sum_{\chi\in P(\varphi)} \chi_1(b_1)\ldots\chi_s(b_s), \tag{10}$$

provided that the $\varphi_i$ are even and $\varphi_1 \ldots \varphi_s = \chi_0$.

Furthermore, it follows from (10) that

$$\sum_{i_1,\ldots,i_s=1}^{s}{}' \; \varphi_{i_1}(a_1)\ldots\varphi_{i_s}(a_s) = \sum_{i_1,\ldots,i_s=1}^{s}{}' \; \varphi_{i_1}(b_1)\ldots\varphi_{i_s}(b_s). \tag{11}$$

Indeed, if $\{\varphi_1, \ldots, \varphi_s\}$ break into $t$ groups with $l_1, \ldots, l_t$ coinciding characters in each group and distinct characters in distinct groups, then (11) is obtained from (10) by multiplying by $l_1! \ldots l_t!$. Next, (11) may be rewritten as

$$\sum_{i_1,\ldots,i_s=1}^{s}{}' \varphi_1(a_{i_1})\ldots\varphi_s(a_{i_s}) = \sum_{i_1,\ldots,i_s=1}^{s}{}' \varphi_1(b_{i_1})\ldots\varphi_s(b_{i_s}). \tag{12}$$

If now $1 \le r \le s$ and $\varphi_i$ are even with $\varphi_1\ldots\varphi_r = \chi_0$, we define $\varphi_{r+1} = \ldots = \varphi_s = \chi_0$ and get

$$\sum_{i_1,\ldots,i_r=1}^{s}{}' \varphi_1(a_{i_1})\ldots\varphi_r(a_{i_r}) = \sum_{i_1,\ldots,i_r=1}^{s}{}' \varphi_1(b_{i_1})\ldots\varphi_r(b_{i_r}). \tag{13}$$

We prove that the latter equality remains valid if we extend the summation over *all* collections $i_1,\ldots,i_r$, probably with coinciding $i_\nu$ and even with $r > s$. Using the above introduced notation, write

$$\sum_{i_1,\ldots,i_r=1}^{s} \varphi_1(a_{i_1})\ldots\varphi_r(a_{i_r}) = \sum_{\Omega}\sum_{i_1,\ldots,i_r=1}^{s}{}^{(\Omega)}\varphi_1(a_{i_1})\ldots\varphi_r(a_{i_r}).$$

For a fixed $\Omega = \{S_1,\ldots,S_t\}$ the inner sum on the right-hand side equals

$$\sum_{j_1,\ldots,j_t=1}^{s}{}' \Phi_1(a_{j_1})\ldots\Phi_t(a_{j_t}),$$

where $\Phi_\nu = \prod_{i\in S_\nu}\varphi_i$, and by (13) this does not change if we replace $a$ by $b$ (if $t > s$ we can not use (13) but then this last sum obviously equals 0).

Our next observation is that

$$\sum_{i_1,\ldots,i_r=1}^{s} \varphi_1(a_{i_1})\ldots\varphi_r(a_{i_r}) = \prod_{j=1}^{r}(\varphi_j(a_1)+\ldots+\varphi_j(a_s))$$

and hence we have proved that

$$\prod_{j=1}^{r}(\varphi_j(a_1)+\ldots+\varphi_j(a_s)) = \prod_{j=1}^{r}(\varphi_j(b_1)+\ldots+\varphi_j(b_s)) \tag{14}$$

as soon as $\varphi_1,\ldots,\varphi_r$ are even characters with $\varphi_1\ldots\varphi_r = \chi_0$.

We now use Lemma 3. For $X_0$ we choose the set of all characters $\varphi$ satisfying $\varphi(b_1)+\ldots+\varphi(b_s) \ne 0$, and define $f : X_0 \to \mathbb{C}$ by

$$f(\varphi) = \frac{\varphi(a_1)+\ldots+\varphi(a_s)}{\varphi(b_1)+\ldots+\varphi(b_s)}.$$

Then (14) guarantees that the conditions of Lemma 3 are satisfied, and using also Corollary 1(iii) we conclude that there exists $\lambda \in \mathbb{F}_p^\times$ such that

$$\varphi(a_1)+\ldots+\varphi(a_s) = (\varphi(b_1)+\ldots+\varphi(b_s))\,\varphi(\lambda) \tag{15}$$

for every $\varphi \in X_0$. But if in (14) we choose $r = 2$ and $\varphi_1 = \varphi$, $\varphi_2 = \overline{\varphi}$, where $\varphi$ is even but $\varphi(b_1)+\ldots+\varphi(b_s) = 0$, we see that also $\varphi(a_1)+\ldots+\varphi(a_s) = 0$

and thus (15) holds for all even $\varphi$, regardless of whether $\varphi \in X_0$ or not. By multiplicativity of $\varphi$, we can write (15) in the form

$$\sum_{i=1}^{s} \varphi(a_i) = \sum_{i=1}^{s} \varphi(\lambda b_i). \tag{16}$$

Multiplying (16) by $\overline{\varphi}(n)$ for $n \in \mathbb{F}_p^\times$ and summing up over all even characters $\varphi$, we obtain

$$\sum_{i=1}^{s} \Big(\sum_{\varphi} \varphi(a_i n')\Big) = \sum_{i=1}^{s} \Big(\sum_{\varphi} \varphi(\lambda b_i n')\Big),$$

thus using Corollary 1(ii) we conclude that $a$ and $\lambda b$ have the same number of coordinates equal to $\pm n$. And this shows that $a$ may be obtained from $b$ by multiplication by $\lambda$, reordering the coordinates and changing signs of some of them.

This completes the proof.

**Acknowledgments.** I am grateful to Prof. N. M. Korobov who drew my attention to this problem and suggested the use of the Dirichlet theorem for solving it.

School of Mathematical Sciences
Tel-Aviv University
69978 Tel-Aviv, Israel
E-mail: seva@math.tau.ac.il

*Received on 21.2.1995*
*and in revised form on 26.10.1995* (2745)