ON THE CONVERGENCE OF MEAN VALUES OVER LATTICES

WOLFGANG SCHMIDT

Introduction. Recently *C. A. Rogers* (**2**, Theorem 4) proved the following theorem which applies to many problems in geometry of numbers:

Let $f(X_1,X_2,\ldots,X_k)$ be a non-negative Borel-measurable function in the nk-dimensional space of points $(X_1,X_2,\ldots,X_k)$. Further, let Λ_0 be the fundamental lattice, Ω a linear transformation of determinant 1, F a fundamental region in the space of linear transformations of determinant 1, defined with respect to the subgroup of unimodular transformations and $\mu(\Omega)$ the invariant measure[1] *on the space of linear transformations of determinant 1 in R_n. Then, if $1 \leqslant k \leqslant n-1$,*

$$\int_F \sum_{X_j \in \Omega\Lambda_0} f(X_1,\ldots,X_k)\, d\mu(\Omega) = f(0,\ldots,0) + \int\ldots\int f(X_1,\ldots,X_k)\, dX_1\ldots dX_k \tag{1}$$
$$+ \sum_{(\nu;\mu)} \sum_{q=1}^{\infty} \sum_{D} \left(\frac{N(D,q)}{q^m}\right)^n \int\ldots\int f\Big(\sum_{i=1}^m \frac{d_{i1}}{q}X_i,\ldots,\sum_{i=1}^m \frac{d_{ik}}{q}X_i\Big)\, dX_1\ldots dX_m,$$

both sides having perhaps the value $+\infty$. The outer sum on the right side is over all divisions $(\nu;\mu) = (\nu_1,\ldots,\nu_m;\mu_1,\ldots,\mu_{k-m})$ of the numbers $1,2,\ldots,k$ into two sequences $\nu_1,\ldots,\nu_m$ and $\mu_1,\ldots,\mu_{k-m}$ with $1 \leqslant m \leqslant k-1$

$$\begin{aligned} &1 \leqslant \nu_1 < \nu_2 < \ldots < \nu_m \leqslant k, && 1 \leqslant \mu_1 < \mu_2 < \ldots < \mu_{k-m} \leqslant k \\ &\nu_i \neq \mu_j, && 1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant k-m. \end{aligned} \tag{2}$$

The inner sum is over all $m \times k$-matrices D with integral elements, having highest common factor relatively prime to q, and with

$$\begin{aligned} &d_{i\nu_j} = q\delta_{ij}, && 1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant m \\ &d_{i\mu_j} = 0 \text{ if } \mu_j < \nu_i, && 1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant k-m. \end{aligned} \tag{3}$$

Finally, $N(D,q)$ is the number of sets of integers $(a_1,a_2,\ldots,a_m)$ with $0 \leqslant a_i < q$ and

$$\sum_{i=1}^m d_{ij}a_i \equiv 0 \pmod q, \qquad 1 \leqslant i \leqslant k.$$

Received January 29, 1957.

[1] F and the invariant measure are defined in (**5**).

https://doi.org/10.4153/CJM-1958-013-2 Published online by Cambridge University Press

Rogers **(2)** wrote

$$\frac{e_1}{q}\cdots\frac{e_m}{q} \text{ instead of } \frac{N(D,q)}{q^m},$$

where $e_i = (\epsilon_i, q)$ and $\epsilon_1, \ldots, \epsilon_m$ are the elementary divisors of D. By Lemma 1 of **(2)**,

$$\frac{e_1}{q}\cdots\frac{e_m}{q} = \frac{N(D,q)}{q^m}.$$

Another proof of Rogers' theorem is given in **(4)**.

We write $(\rho;\sigma) \prec (\nu;\mu)$ if

$$(\rho;\sigma) = (\rho_1, \ldots, \rho_m; \sigma_1, \ldots, \sigma_{k-m}), \; (\nu;\mu) = (\nu_1, \ldots, \nu_m; \mu_1, \ldots, \mu_{k-m})$$

and $\rho_1 = \nu_1, \rho_2 = \nu_2, \ldots, \rho_{l-1} = \nu_{l-1}, \rho_l < \nu_l$ for some $l \leqslant m$. If $m < k$ and D is a $m \times k$-matrix, then we denote by $D(\nu;\mu)$ the square submatrix with columns $\nu_1, \nu_2, \ldots, \nu_m$ and by $\det D(\nu;\mu)$ the absolute value of the determinant of $D(\nu;\mu)$.

In this paper we prove two theorems:

THEOREM 1. *Rogers' theorem remains true, if* (3) *is replaced by*

$$\begin{aligned} &D(\nu;\mu) = qI,\\ (4)\qquad &\det D(\rho;\sigma) \leqslant \det D(\nu;\mu) \textit{ for any } (\rho;\sigma) = (\rho_1, \ldots, \rho_m; \sigma_1, \ldots, \sigma_{k-m})\\ &\det D(\rho;\sigma) < \det D(\nu;\mu) \textit{ if } (\rho;\sigma) \prec (\nu;\mu). \end{aligned}$$

Theorem 1 provides better estimates for the sum in (1), since (4) permits only matrices D with $|d_{ij}| \leqslant q$. We further prove

THEOREM 2. *If $f(X_1, \ldots, X_k)$ is bounded and vanishes outside a bounded region of space, then both sides of* (1) *are finite.*

Theorem 2 is an improvement of Rogers' result, that (1) is finite, under the stated conditions, if $n \geqslant [\frac{1}{4}k^2] + 2$. Theorem 2 guarantees finiteness for all cases of Rogers' theorem, that is, for $k < n$. No results are known[2] for $n = k$ or $n < k$.

1. LEMMA 1. If $f(X_1, \ldots, X_k) \geqslant 0$, then

$$(5)\quad \sum_{X_i \in \Lambda} f(X_1, \ldots, X_k) = f(0, \ldots, 0) + \sum \begin{bmatrix} X_1, \ldots, X_k \in \Lambda \\ \dim(X_1, \ldots, X_k) = k \end{bmatrix} f(X_1, \ldots, X_k)$$

$$(6)\quad + \sum_{(\nu;\mu)} \sum_{q=1}^{\infty} \sum_{D} \sum \begin{bmatrix} Y_1, \ldots, Y_m \in \Lambda \\ \dim(Y_1, \ldots, Y_m) = m \\ \sum_{i=1}^{m} d_{ij} Y_i / q \in \Lambda \end{bmatrix} f\left(\sum_{i=1}^{m} \frac{d_{i1}}{q} Y_i, \ldots, \sum_{i=1}^{m} \frac{d_{ik}}{q} Y_i \right).$$

The sum extends over all D which satisfy (4).

[2]In **2** Theorem 5, $n \geqslant 2$ should be replaced by $n > 2$.

Lemma 1 is analogous to a formula of Rogers, where D satisfies (3).

Proof of Lemma 1. The set of points $0,0,\ldots,0$ occurs in the term $f(0,0,\ldots,0)$ and if $X_1,\ldots,X_k$ are linearly independent, then $f(X_1,\ldots,X_k)$ will occur just once in the sum

$$\sum \begin{bmatrix} X_1,\ldots,X_k \in \Lambda \\ \dim(X_1,\ldots,X_k) = k \end{bmatrix} f(X_1,\ldots,X_k).$$

If $0 < \dim(X_1,\ldots,X_k) = m < k$, then $X_1,\ldots,X_k$ span an m-dimensional space S. If $(\nu;\mu) = (\nu_1,\ldots,\nu_m;\ \mu_1,\ldots,\mu_{k-m})$, then let $d(\nu;\mu;X_1,\ldots X_k)$ be the volume of the m-dimensional parallelepiped spanned by

$$X_{\nu_1}, X_{\nu_2},\ldots, X_{\nu_m}.$$

There exists a uniquely determined $(\nu;\mu)$ so that

$$d(\rho;\sigma;X_1,\ldots,X_k) \leqslant d(\nu;\mu;X_1,\ldots,X_k) \text{ for any } (\rho;\sigma)$$

and

$$d(\rho;\sigma;X_1,\ldots,X_k) < d(\nu;\mu;X_1,\ldots,X_k) \text{ if } (\rho;\sigma) \prec (\nu;\mu).$$

Every point X_j can be expressed uniquely in the form

$$X_j = \sum_{i=1}^{m} c_{ij} X_{\nu_i} = \sum_{i=1}^{m} \frac{d_{ij}}{q} X_{\nu_i}$$

where c_{ij} are rationals and d_{ij}, $q > 0$ are integers so that the highest common factor of the d_{ij} is relatively prime to q. Clearly, $D = (d_{ij})$ and q satisfy (4).

Further, if we take

$$Y_s = X_{\nu_s}$$

then $Y_1, Y_2,\ldots, Y_m$ are linearly independent points of Λ, and the points

$$X_j = \sum_{i=1}^{m} \frac{d_{ij}}{q} Y_i$$

are points of Λ. Consequently, there is a term

$$f\Big(\sum_{i=1}^{m} \frac{d_{i1}}{q} Y_i,\ldots, \sum_{i=1}^{m} \frac{d_{ik}}{q} Y_i\Big) = f(X_1,\ldots,X_k)$$

in the sum (6), corresponding to the points $X_1,\ldots,X_k$. It is clear that $(\nu;\mu)$, q and D are uniquely determined by the points $X_1, X_2,\ldots, X_k$. So corresponding to each k-tuple of points $X_1, X_2,\ldots, X_k$ there will be just one term in the sum (6).

Conversely, it is easy to see that each term in (6) corresponds to just one term in (5). Since f is non-negative, Lemma 1 follows.

Proof of Theorem 1. We make use of the following theorem of Rogers (**2**, Theorem 3):

Let $f(X_1, \dots, X_m)$ be a Borel-measurable function which is integrable in the Lebesgue sense over the whole $X_1, \dots, X_m$-space. Then the lattice function

$$f(\Lambda) = \sum \begin{bmatrix} X_1, \dots, X_m \in \Lambda \\ \dim(X_1, \dots, X_m) = m \\ \sum_{i=1}^{m} d_{ij}/q X_i \in \Lambda \end{bmatrix} f(X_1, \dots, X_m)$$

is Borel-measurable in the space of lattices of determinant 1 *and*

$$\int_F f(\Omega\Lambda_0)\, d\mu(\Omega) = \left(\frac{N(D,q)}{q^m}\right)^n \int \dots \int f(X_1, \dots, X_m)\, dX_1 \dots dX_m.$$

A combination of this theorem and Lemma 1 gives (1), where the sum is extended over all D with (4). This proves Theorem 1.

2. Some properties of systems of linear congruences. There exist many papers on this subject (for example, **(1)**), but it seems desirable to develop the theory in a way which is most suitable for our purposes.

Let $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_m$ be integral vectors, p^t a power of a prime. We define the rank $r(p^t)$ of $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_m$ (mod p^t) to be k, if there exists a subset R of k vectors

$$\mathfrak{a}_{i_1}, \mathfrak{a}_{i_2}, \dots, \mathfrak{a}_{i_k},$$

so that each vector is (mod p^t) a linear combination of vectors of R, and if k is the least integer with this property. We say R is a basis of $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_m$ (mod p^t). If H is an integral matrix, then we define the rank $r(H, p^t)$ to be the rank $r(p^t)$ of the rows of H.

We investigate the set $H(u, v; r_1, r_2, \dots, r_t; p)$ of matrices H which have u rows, v columns and $r(H, p^j) = r_j$ $(1 \leqslant j \leqslant t)$. If

$$H \in H(u, v;\, r_1, r_2, \dots, r_t; p),$$

then there exist bases R_j of all rows (mod p^j), consisting of r_j rows. R_j has (mod p^{j-1}) rank $s_{j-1} \leqslant r_{j-1}$ and a basis S_{j-1} (mod p^{j-1}) consisting of s_{j-1} rows. ($s_{j-1} \leqslant r_{j-1}$ follows from the fact that if vectors $\mathfrak{b}_1, \dots, \mathfrak{b}_h$ are linearly dependent on $\mathfrak{c}_1, \dots, \mathfrak{c}_s$ (mod p^t), then there is a subset of s vectors

$$\mathfrak{b}_{i_1}, \dots, \mathfrak{b}_{i_s},$$

so that $\mathfrak{b}_1, \dots, \mathfrak{b}_h$ are linearly dependent on

$$\mathfrak{b}_{i_1}, \dots, \mathfrak{b}_{i_s} \pmod{p^t}.$$

This fact can be verified similarly to the corresponding proofs in vector-algebra.) Each row is a linear combination of rows of R_j (mod p^j), hence a fortiori (mod p^{j-1}). Consequently, S_{j-1} is a basis R_{j-1} (mod p^{j-1}) of all rows of H and we have $s_{j-1} = r_{j-1}$, $R_{j-1} \subseteq R_j$. If therefore $H \in H$ $(u, v;$ $r_1, \dots, r_t; p)$, then there exists a sequence of bases R_j (mod p^j), each consisting of r_j rows and with $R_1 \subseteq R_2 \subseteq \dots \subseteq R_t$.

We define $G(u,v;r_1,r_2,\ldots,r_t;p)$ to be the subset of those $H \in H(u,v;r_1,r_2,\ldots,r_t;p)$ which have a sequence of bases $R_1 \subseteq \ldots \subseteq R_t$ so that R_j consists of the first r_j rows

$$\mathfrak{h}_1,\mathfrak{h}_2,\ldots,\mathfrak{h}_{r_j}$$

of $H\,(1 \leqslant j \leqslant t)$. If $N_H(u,v;r_1,\ldots,r_t;p)$ is the number of $H \in H(u,v;r_1,\ldots,r_t;p)$ (mod p^t) and $N_G(u,v;r_1,\ldots,r_t;p)$ is the number of $H \in G(u,v;r_1,\ldots,r_t;p)$ (mod p^t), then

$$N_H(u,v;r_1,\ldots,r_t;p) \leqslant u!\,N_G(u,v;r_1,\ldots,r_t;p). \tag{7}$$

LEMMA 2. *If $H \in G(u,v;r_1,\ldots,r_t;p)$ has the rows $\mathfrak{h}_1,\mathfrak{h}_2,\ldots,\mathfrak{h}_u$, and if*

$$\mathfrak{h} \equiv \sum_{i=1}^{r_j} \mathfrak{h}_i c_i \pmod{p^j} \tag{8}$$

then there exist d_i $(1 \leqslant i \leqslant r_j)$, so that

$$\mathfrak{h} \equiv \sum_{i=1}^{r_j} \mathfrak{h}_i d_i \pmod{p^j} \qquad 0 \leqslant d_i < p^{j-e} \text{ if } i > r_e, \tag{9}$$

where $1 \leqslant e < j \leqslant t+1$; we write $r_0 = 0$, $r_{t+1} = u$.

Proof of Lemma 2. The lemma is true if

$$c_{r_1+1} = c_{r_1+2} = \ldots = c_{r_j} = 0.$$

Using induction on f, we assume it to be true for

$$c_{r_f+1} = c_{r_f+2} = \ldots = c_{r_j} = 0 \tag{10}$$

and prove it for

$$c_{r_{f+1}+1} = c_{r_{f+1}+2} = \ldots = c_{r_j} = 0. \tag{11}$$

If (11) holds, then

$$\mathfrak{h} \equiv \sum_{i=1}^{r_{f+1}} \mathfrak{h}_i c_i \pmod{p^j}.$$

If $r_f < i \leqslant r_{f+1}$, then

$$\mathfrak{h}_i \equiv \sum_{l=1}^{r_f} w_{li}\mathfrak{h}_l + p^f \mathfrak{g}_i \pmod{p^j}.$$

Therefore,

$$\mathfrak{h} \equiv \sum_{i=1}^{r_f} \mathfrak{h}_i c_i + \sum_{i=r_f+1}^{r_{f+1}} \Big(\sum_{l=1}^{r_f} w_{li}\mathfrak{h}_l + p^f\mathfrak{g}_i\Big)c_i \pmod{p^j}.$$

If we take $d_i \equiv c_i \pmod{p^{j-f}}$, $0 \leqslant d_i < p^{j-f}$ $(r_f + 1 \leqslant i \leqslant r_{f+1})$, then

$$\mathfrak{h} \equiv \mathfrak{h}' + \sum_{i=r_f+1}^{r_{f+1}} \mathfrak{h}_i d_i \pmod{p^j} \tag{12}$$

where $\mathfrak{h}'$ can be written in the form (8) with (10), whence by induction in the form (9). Therefore and by (12) we proved Lemma 2 for all h with (8) and (11).

LEMMA 3.

(13) $$N_H(u,v;r_1,\ldots,r_t;p) \leqslant u!p^{(u+v)(r_1+\ldots+r_t)-r_1^2-r_2^2-\ldots-r_t^2}.$$

Proof of Lemma 3. Because of (7) it suffices to prove

$$N_G(u,v;r_1,\ldots,r_t;p) \leqslant p^{(u+v)(r_1+\ldots+r_t)-r_1^2-\ldots-r_t^2}.$$

If $\mathfrak{h}_1,\ldots,\mathfrak{h}_u$ are the rows of $H \in G(u,v;r_1,\ldots,r_t;p)$ and if $r_j < s \leqslant r_{j+1}$, then $\mathfrak{h}_s$ can be written in the form (8), hence by Lemma 2 in the form (9). There are

$$(p^j)^{r_1}(p^{j-1})^{(r_2-r_1)}(p^{j-2})^{(r_3-r_2)}\ldots p^{(r_j-r_{j-1})} = p^{r_1+r_2+\ldots+r_j}$$

possibilities for the coefficients d. If therefore $\mathfrak{h}_1,\ldots,\mathfrak{h}_{s-1}$ are given, we have $p^{r_1+\ldots+r_j}$ possibilities for $\mathfrak{h}_s$ (mod p^j), times $p^{(t-j)v}$ possibilities if we fix $\mathfrak{h}_s$ (mod p^t). This gives $p^{r_1+\ldots+r_j+(t-j)v}$ possibilities. Hence,

$$\begin{aligned} N_G(u,v;r_1,\ldots,r_t;p) &\leqslant p^{tvr_1}\cdot p^{[r_1+(t-1)v](r_2-r_1)}\cdot \\ &\quad p^{[r_1+r_2+(t-2)v](r_3-r_2)}\ldots p^{[r_1+\ldots+r_t](u-r_t)} \\ &= p^{(u+v)(r_1+\ldots+r_t)-r_1^2-\ldots-r_t^2}. \end{aligned}$$

LEMMA 4. *If* $Z_H(u,v;r_1,\ldots,r_t;p)$ *is the maximal number of solutions* (mod p^t) *of an equation*

(14) $$\mathfrak{h}_1x_1+\ldots+\mathfrak{h}_ux_u \equiv 0 \pmod{p^t},$$

where $\mathfrak{h}_1,\mathfrak{h}_2,\ldots,\mathfrak{h}_u$ *are the rows of a matrix* $H \in H(u,v;r_1,\ldots,r_t;p)$, *then*

(15) $$Z_H(u,v;r_1,\ldots,r_t;p) \leqslant p^{tu-r_1-\ldots-r_t}.$$

Proof of Lemma 4. It is enough to prove (15) for $H \in G(u,v;r_1,\ldots,r_t;p)$. First we choose

$$x_{r_t+1},\ldots,x_u$$

arbitrarily. This gives $p^{t(u-r_t)}$ possibilities (mod p^t). The number of solutions of (14) with fixed

$$x_{r_t+1},\ldots,x_u$$

is at most equal to the number of solutions of the homogeneous equation

(16) $$\mathfrak{h}_1x_1+\ldots+\mathfrak{h}_{r_t}x_{r_t} \equiv 0 \pmod{p^t}.$$

Since $h_1,\ldots,h_{r_t}$ have rank r_t (mod p^t), all x_j have to be multiples of p, that is, $x_j = py_j$ $(1 \leqslant j \leqslant r_t)$. Hence we have the new system

(17) $$\mathfrak{h}_1y_1+\ldots+\mathfrak{h}_{r_t}y_{r_t} \equiv \mathfrak{o} \pmod{p^{t-1}}.$$

System (17) is similar to (14), we only substituted r_t for v, $t-1$ for t. By repeated application of this argument we see that

$$Z_H(u,v;r_1,\ldots,r_t;p) \leqslant p^{t(u-r_t)+(t-1)(r_t-r_{t-1})+\ldots+(r_2-r_1)} = p^{tu-r_1-\ldots-r_t}.$$

If

$$q = \prod_{i=1}^{l} p_i^{c_i},$$

then we define the set of matrices

$$H\begin{pmatrix} & r_{11},r_{12},\ldots,r_{1c_1} & \\ & r_{21},r_{22},\ldots,r_{2c_2} & \\ u,v; & \ldots & ;q \\ & r_{l1},r_{l2},\ldots,r_{lc_l} & \end{pmatrix} = H(u,v;\rho;q) = \bigcap_{i=1}^{l} H(u,v;r_{i1},\ldots,r_{ic_i};p_i).$$

Let $N_H(u,v;\rho;q)$ be the number of $H \in H(u,v;\rho;q)$ (mod q) and $Z_H(u,v;\rho;q)$ the maximal number of solutions (mod q) of

$$(18) \qquad \mathfrak{h}_1 x_1 + \ldots + \mathfrak{h}_u x_u \equiv 0 \pmod{q}$$

where $\mathfrak{h}_1,\mathfrak{h}_2,\ldots,\mathfrak{h}_u$ are rows of an $H \in H(u,v;\rho;q)$.

We observe

$$(19) \qquad N_H(u,v;\rho;q) = \prod_{i=1}^{l} N_H(u,v;r_{i1},\ldots,r_{ic_i};p_i)$$

and

$$(20) \qquad Z_H(u,v;\rho;q) = \prod_{i=1}^{l} Z_H(u,v;r_{i1},\ldots,r_{ic_i};p_i).$$

3. Proof of Theorem 2. If $f(X_1,\ldots,X_k)$ is a non-negative Borel-measurable function, then (1) holds. We are going to show that if, in addition, f is bounded and vanishes outside a bounded region of space, then both sides of (1) are finite.

There is only a finite number of divisions $(\nu;\mu)$. Hence it suffices to prove the convergence of the sum for a given $(\nu;\mu)$. Finally we observe that, under the stated conditions, the integrals

$$(21) \qquad \int\ldots\int f\Big(\sum_{i=1}^{m} \frac{d_{i1}}{q} X_i,\ldots,\sum_{i=1}^{m} \frac{d_{ik}}{q} X_i\Big)dX_1\ldots dX_m$$

are less than a fixed constant. Therefore it remains to show the convergence of

$$\sum_{q=1}^{\infty} \sum_{D} \left(\frac{N(D,q)}{q^m}\right)^n$$

where $(\nu;\mu) = (\nu_1,\ldots,\nu_m;\ \mu_1,\ldots,\mu_{k-m})$ is given and D runs through all matrices satisfying (4). D has m rows, k columns.

If $D \in H(m,k;\rho;q)$,

$$q = \prod_{i=1}^{l} p_i^{c_i},$$

then, by definition of $N(D,q)$, $N(D,q) \leqslant Z_H(m,k;\rho;q)$. How many matrices D in $H(m,k;\rho;q)$ satisfy (4)? Since the columns

$$d_{\nu_1},d_{\nu_2},\ldots,d_{\nu_m}$$

are fixed and $\equiv 0 \pmod{q}$, there are $\leqslant N_H(m,k-m;\rho;q)$ possibilities modulo q and because of $|d_{ij}| \leqslant q$ at most $3^{m(k-m)}N_H(m,k-m;\rho;q)$ possibilities.

Consequently, by (19) and (20),

$$\sum_D \left(\frac{N(D,q)}{q^m}\right)^n \leqslant 3^{m(k-m)} \prod_{i=1}^{l} \left(\frac{Z_H(m,k;r_{i1},\ldots,r_{ic_i};p_i)}{p_i^{c_i m}}\right)^n N_H(m,k-m;r_{i1},\ldots,r_{ic_i};p_i).$$

The summation is taken over all $D \in H(m,k;\rho;q)$ which satisfies (4).

By summation over all q,ρ, we obtain

$$\sum_{q=1}^{\infty} \sum_D \left(\frac{N(D,q)}{q^m}\right)^n \leqslant 3^{m(k-m)} \prod_p \left[1 + \sum_{1\leqslant r_1\leqslant \ldots \leqslant r_c \leqslant m} \left(\frac{Z_H(m,k;r_1,\ldots,r_c;p)}{p^{cm}}\right)^n N_H(m,k-m;r_1,\ldots,r_c;p)\right]. \tag{22}$$

The sum on the right hand side of (22) is over all sequences $1 \leqslant r_1 \leqslant r_2 \leqslant \ldots \leqslant r_c \leqslant m$ with arbitrary c. We have $r_1 \geqslant 1$, because $r_1 = 0$ would imply that all elements of D are multiples of p, and p, D were not relatively prime. It is a consequence of (13) and (15) that

$$\begin{aligned}(23)\qquad &\left(\frac{Z_H(m,k;r_1,\ldots,r_c;p)}{p^{cm}}\right)^n N_H(m,k-m;r_1,\ldots,r_c;p)\\ &\leqslant \left(\frac{p^{cm-r_1-\ldots-r_c}}{p^{cm}}\right)^n (k-m)!p^{k(r_1+\ldots+r_c)-r_1^2-\ldots-r_c^2}\\ &= (k-m)!p^{-(n-k)(r_1+\ldots+r_c)-r_1^2-\ldots-r_c^2}.\end{aligned}$$

We have

$$\begin{aligned}(24)\qquad &\sum_{1\leqslant r_1\leqslant \ldots \leqslant r_c\leqslant m} p^{-(n-k)(r_1+\ldots+r_c)-r_1^2-\ldots-r_c^2} = \prod_{l=1}^{m}\left(\sum_{t=0}^{\infty} p^{-[(n-k)l+l^2]t}\right)\\ &-1 < \prod_{l=1}^{m}(1+2p^{-(n-k)l-l^2}) - 1 < Cp^{-(n-k+1)}\end{aligned}$$

where C is a constant. Finally, the product

$$\prod_p \left(1 + \frac{C(k-m)\,(k-m)!}{p^{n-k+1}}\right)$$

is convergent. This fact, together with (22), (23) and (24), yields Theorem 2.

By estimates for the integrals (21), provided by **(3)**, it would be posible to find good bounds for (1).

References

1. A. T. Butson and B. M. Stewart, *Systems of linear congruences*, Can. J. Math., *7* (1955), 358–368.
2. C. A. Rogers, *Mean values over the space of lattices*, Acta Math., *94* (1955), 249–287.
3. ———, *A single integral inequality*, to appear in the Journal of the London Math. Soc.
4. W. Schmidt, *Mittelwerte über Gitter*, Monatshefte f. Math., *61* (1957), 000–000.
5. C. L. Siegel, *A mean value theorem in geometry of numbers*, Annals of Math., *46* (1945), 340–347.

Montana State University