Mh. Math. 86, 203—219 (1978)

Monatshefte für
Mathematik

Existence of Good Lattice Points in the Sense of Hlawka

By

Harald Niederreiter*, Kingston

(Received 8 November 1977)

Abstract

An existence theorem for good lattice points, which was so far only available for prime moduli, is established for general moduli by using a method based on exponential sums.

1. Introduction and Statement of Results

The need for good lattice points arises in a numerical integration technique for periodic functions of several variables developed by HLAWKA [2] and KOROBOV [3]. We refer to [4, Ch. 2, Sec. 5] and the survey articles [9], [10] for literature on, and a more detailed discussion of such lattice points. The method of good lattice points (or "optimal coefficients" in the terminology of KOROBOV) has gained added significance through recently established links with the multidimensional distribution behavior of linear congruential pseudo-random numbers (cf. [6], [7], [8]).

Let $s \geqslant 2$ be a given dimension and let f be a function of s variables which is periodic of period 1 in each variable. The s-dimensional unit-cube $I^s = [0,1]^s$ is then a period interval for f. The method of good lattice points is based on the approximation

$$\int_{I_s} f(\mathbf{t})\, d\mathbf{t} \approx (1/m) \sum_{n=1}^{m} f((n/m)\,\mathbf{g}), \tag{1}$$

where m is a large integer, called the *modulus*, and the lattice point $\mathbf{g} \in \mathbb{Z}^s$ is chosen so as to guarantee a small integration error, in which case it is called a *good lattice point* mod m. To make this somewhat more precise, we introduce a quantity measuring the

* Supported by United States National Science Foundation Grant MCS77-01699.

0026—9255/78/0086/0203/$ 03.40

suitability of lattice points mod m. For $m \geqslant 2$ we use the summation symbol $\sum_{h \pmod m}$ to denote a sum over the complete residue system mod m consisting of the integers h with $-m/2 < h \leqslant m/2$, whereas $\sum_{h \pmod m}^{*}$ refers to the same sum, but with $h = 0$ deleted from the range of summation. Similarly, the summation symbol $\sum_{\mathbf{h} \pmod m}$ denotes a sum over the s-fold cartesian product of the above complete residue system mod m, i. e., over the set of lattice points $\mathbf{h} = (h_1, \ldots, h_s) \in \mathbb{Z}^s$ with $-m/2 < h_j \leqslant m/2$ for $1 \leqslant j \leqslant s$, and $\sum_{\mathbf{h} \pmod m}^{*}$ designates the same sum, but with the origin deleted from the range of summation. As a distance function for lattice points relative to the origin, we use

$$r(\mathbf{h}) = r(h_1) \ldots r(h_s),$$

where $r(h) = \max(1, |h|)$ for $h \in \mathbb{Z}$. For a lattice point $\mathbf{g} \in \mathbb{Z}^s$, we define then

$$R(\mathbf{g}, m) = \sum_{\substack{\mathbf{h} \pmod m \\ \mathbf{h} \cdot \mathbf{g} \equiv 0 \pmod m}}^{*} r(\mathbf{h})^{-1}, \tag{2}$$

with $\mathbf{h} \cdot \mathbf{g}$ denoting the standard inner product of $\mathbf{h}$ and $\mathbf{g}$. This expression governs the integration error in (1) in the sense that for an integrand f with Fourier coefficients $c_{\mathbf{h}}$ satisfying $c_{\mathbf{h}} = O(r(\mathbf{h})^{-k})$ for some $k > 1$ we have

$$(1/m) \sum_{n=1}^{m} f((n/m)\,\mathbf{g}) - \int_{I^s} f(\mathbf{t})\, d\mathbf{t} = O(R(\mathbf{g}, m)^k).$$

The "goodness" of lattice points $\mathbf{g}$ mod m can therefore be described in terms of the size of $R(\mathbf{g}, m)$.

Theoretical results on the existence of lattice points $\mathbf{g}$ leading to a small value of $R(\mathbf{g}, m)$ have so far only been available for primes m (cf. [2], [10]). The sharpest result in this direction is contained in [10, Proposition 5.4] and says that for every $s \geqslant 2$ and every prime modulus m there exists a lattice point $\mathbf{g} \in \mathbb{Z}^s$ such that

$$R(\mathbf{g}, m) < (1/m)(2 + 2 \log m)^s. \tag{3}$$

The method of proving (3) breaks down for composite m. It is, however, an empirical fact that certain composite moduli perform better than prime moduli. This is particularly evident in the case $s = 2$, where it is known that optimal lattice points are obtained

by taking a Fibonacci number as a modulus. Fibonacci numbers are, of course, rarely primes. Numerical data for higher-dimensional cases suggest that lattice points which are in a sense optimal are usually obtained with a composite modulus (compare with Tables 9 and 10 in [5]).

There is an indirect way of getting information about the size of $R(\mathbf{g},m)$ for composite m, by using the number

$$\varrho(\mathbf{g},m) = \min_{\mathbf{h}} r(\mathbf{h}),$$

where the minimum is extended over all lattice points $\mathbf{h} = (h_1,\ldots,h_s) \in \mathbb{Z}^s$ with $\mathbf{h} \neq \mathbf{0}$, $\mathbf{h}\cdot\mathbf{g} \equiv 0 \pmod m$, and $-m/2 < h_j \leqslant m/2$ for $1 \leqslant j \leqslant s$. It was shown by ZAREMBA [11] that for every sufficiently large modulus m, no matter whether prime or composite, there exists a lattice point $\mathbf{g} \in \mathbb{Z}^s$ such that

$$\varrho(\mathbf{g},m) > \frac{(s-1)!\,m}{(2\log m)^{s-1}}.$$

Together with an estimate for $R(\mathbf{g},m)$ of the form $R(\mathbf{g},m) = O\left(\varrho(\mathbf{g},m)^{-1}(\log m)^s\right)$ (cf. [7, Sec. 3]), it follows that there exists a $\mathbf{g} \in \mathbb{Z}^s$ with

$$R(\mathbf{g},m) = O\left(m^{-1}(\log m)^{2s-1}\right).$$

Via a direct approach, we prove in the present paper that for any modulus $m \geqslant 2$ there is a lattice point $\mathbf{g} \in \mathbb{Z}^s$ for which $R(\mathbf{g},m)$ satisfies an estimate of the type (3). A careful treatment of constants in our method actually leads to a bound that is better than (3). The first crucial idea in our proof is to restrict the attention to lattice points whose coordinates are relatively prime to m. Secondly, rather than using elementary considerations about congruences as in the proof of (3), we employ a more powerful analytic technique based on exponential sums. Our final result reads as follows.

Theorem 1. *For every integer $m \geqslant 2$ and every dimension $s \geqslant 2$, there exists a lattice point $\mathbf{g} \in \mathbb{Z}^s$ with coordinates relatively prime to m and*

$$R(\mathbf{g},m) < (1/m)(1.4 + 2\log m)^s. \tag{4}$$

In the special case of a prime power modulus, the method simplifies somewhat and a slightly better result can be achieved as a consequence.

Theorem 2. *If m is a prime or a prime power, then for every dimension $s \geqslant 2$ there exists a lattice point $\mathbf{g} \in \mathbb{Z}^s$ with coordinates relatively prime to m and*

$$R(\mathbf{g}, m) < (1/m)(0.81 + 2\log m)^s. \tag{5}$$

These results on $R(\mathbf{g}, m)$ yield information about the discrepancy D_m of sequences of the form $(n/m)\mathbf{g}$, $n = 1, 2, \ldots, m$, considered mod 1. In fact, by [10, Théorème 6.6] we have

$$D_m \leqslant s/m + \tfrac{1}{2} R(\mathbf{g}, m)$$

for any $\mathbf{g} \in \mathbb{Z}^s$, and so Theorem 1 implies that for any $m \geqslant 2$ and every dimension $s \geqslant 2$ there exists a lattice point $\mathbf{g} \in \mathbb{Z}^s$ such that the discrepancy D_m of the above sequence satisfies $D_m = O(m^{-1}(\log m)^s)$ with an effective constant. By way of comparison, we note that the smallest known discrepancy of a sequence of m points in I^s is of the order $m^{-1}(\log m)^{s-1}$.

In Section 2 we collect some preparatory results. Section 3 contains a basic estimate for certain weighted exponential sums. Theorems 1 and 2 are proved in Section 4.

2. Auxiliary Results

For an integer $m \geqslant 2$ we set

$$L(m) = \sum_{h \pmod m}^{*} r(h)^{-1} = \sum_{h \pmod m}^{*} |h|^{-1},$$

and we extend this definition by putting $L(1) = 0$. We need a good estimate for $L(m)$, and for this purpose we distinguish between m even and m odd.

Lemma 1. *For any even integer $m \geqslant 2$ we have*

$$L(m) = 2\log m + 2\gamma - \log 4 + \varepsilon_m \quad \text{with} \quad -4/m^2 < \varepsilon_m \leqslant 0,$$

where γ is the Euler-Mascheroni constant.

Proof. From [1, p. 347] we get for any $x \geqslant 1$,

$$\sum_{1 < h < x} h^{-1} = \log x + \gamma + \theta_x \tag{6}$$

with

$$\theta_x = \int_x^{\infty} \frac{\{t\}}{t^2}\, dt - \frac{\{x\}}{x}, \tag{7}$$

where $\{x\}$ denotes the fractional part of x. For a positive integer x we obtain

$$\theta_x = \int_x^\infty \frac{\{t\}}{t^2}\,dt = \sum_{n=x}^{\infty} \int_n^{n+1} \frac{\{t\}}{t^2}\,dt\,. \tag{8}$$

Furthermore, we have

$$\int_n^{n+1} \frac{\{t\}}{t^2}\,dt = \int_n^{n+1} \frac{t-n}{t^2}\,dt = \log\left(1+\frac{1}{n}\right) - \frac{1}{n+1} \tag{9}$$

for every positive integer n. We note that

$$\log(1+t) \leqslant \frac{t^2+2t}{2t+2} \quad \text{for } t \geqslant 0 \tag{10}$$

since the function $f(t) = ((t^2+2t)/(2t+2)) - \log(1+t)$ satisfies $f(0) = 0$ and $f'(t) \geqslant 0$ for $t \geqslant 0$. By combining (9) and (10) we get

$$\int_n^{n+1} \frac{\{t\}}{t^2}\,dt \leqslant \frac{2n+1}{2n(n+1)} - \frac{1}{n+1} = \frac{1}{2n(n+1)}\,,$$

and so from (8),

$$\theta_x \leqslant \tfrac{1}{2} \sum_{n=x}^{\infty} \frac{1}{n(n+1)} = \frac{1}{2x} \quad \text{for integers } x \geqslant 1\,. \tag{11}$$

The definition of $L(m)$ and (6) imply

$$L(m) = 2 \sum_{h=1}^{m/2} h^{-1} - 2/m = 2\log m + 2\gamma - \log 4 + \varepsilon_m$$

with

$$\varepsilon_m = 2\,\theta_{m/2} - 2/m\,.$$

The inequality $\varepsilon_m \leqslant 0$ follows now immediately from (11). To obtain the lower bound for ε_m, we note that for a positive integer n we have

$$\int_n^{n+1} \frac{\{t\}}{t^2}\,dt = \int_n^{n+1} \frac{t-n}{t^2}\,dt \geqslant \frac{1}{(n+1)^2} \int_n^{n+1} (t-n)\,dt = \frac{1}{2(n+1)^2}$$

by the second mean-value theorem. It follows from (8) that

$$\theta_x \geqslant \tfrac{1}{2} \sum_{n=x}^{\infty} \frac{1}{(n+1)^2} \geqslant \tfrac{1}{2} \int_x^{\infty} \frac{dt}{(t+1)^2} = \frac{1}{2(x+1)} \tag{12}$$

for integers $x \geqslant 1$, and so

$$\varepsilon_m = 2\theta_{m/2} - \frac{2}{m} \geqslant \frac{2}{m+2} - \frac{2}{m} = -\frac{4}{m(m+2)} > -\frac{4}{m^2}.$$

Lemma 2. *For any odd integer $m \geqslant 1$ we have*

$$L(m) = 2\log m + 2\gamma - \log 4 + \varepsilon_m \quad \text{with} \quad -\frac{3}{m^2} < \varepsilon_m < \frac{1}{m^2}.$$

Proof. The result is obvious for $m = 1$, so that we may assume $m \geqslant 3$. From the definition of $L(m)$ and (6) we get

$$L(m) = 2 \sum_{1 < h < m/2} h^{-1} = 2\log m + 2\gamma - \log 4 + 2\theta_{m/2},$$

and together with (7) we obtain

$$\varepsilon_m = 2\theta_{m/2} = 2\int_{m/2}^{\infty} \frac{\{t\}}{t^2}\,dt - \frac{2}{m} = 2\int_{m/2}^{(m+1)/2} \frac{\{t\}}{t^2}\,dt + 2\theta_{(m+1)/2} - \frac{2}{m}. \tag{13}$$

Now

$$\int_{m/2}^{(m+1)/2} \frac{\{t\}}{t^2}\,dt = \int_{m/2}^{(m+1)/2} \frac{t - (m-1)/2}{t^2}\,dt = \log\left(1 + \frac{1}{m}\right) - \frac{m-1}{m(m+1)},$$

and so (10) implies

$$\int_{m/2}^{(m+1)/2} \frac{\{t\}}{t^2}\,dt \leqslant \frac{3}{2m(m+1)}.$$

An application of (11) yields

$$\varepsilon_m \leqslant \frac{3}{m(m+1)} + \frac{2}{m+1} - \frac{2}{m} = \frac{1}{m(m+1)} < \frac{1}{m^2}.$$

For the lower bound, we observe that

$$\int_{m/2}^{(m+1)/2} \frac{\{t\}}{t^2}\,dt = \int_{m/2}^{(m+1)/2} \frac{t - (m-1)/2}{t^2}\,dt \geqslant$$

$$\geqslant \frac{4}{(m+1)^2} \int_{m/2}^{(m+1)/2} \left(t - \frac{m-1}{2}\right) dt = \frac{3}{2(m+1)^2}$$

by the second mean-value theorem. Together with (12) and (13) we obtain

$$\varepsilon_m \geqslant \frac{3}{(m+1)^2} + \frac{2}{m+3} - \frac{2}{m} = -\frac{3m^2+3m+6}{m(m+3)(m+1)^2} > -\frac{3}{m^2}.$$

The above results are applied to the estimation of a sum involving the Moebius function μ. The summation symbol $\sum_{d|m}$ denotes, as usual, a sum over the positive divisors d of m.

Lemma 3. *Let m be a positive integer having at least two distinct prime divisors. Then for every positive integer b we have*

$$-\frac{4.3}{b^2} < \sum_{d|m} \mu(d) L(bd) < \frac{2.7}{b^2}. \tag{14}$$

Proof. By Lemmas 1 and 2 we have

$$\sum_{d|m} \mu(d) L(bd) = \sum_{d|m} \mu(d)(2\log d + 2\log b + 2\gamma - \log 4 + \varepsilon_{bd}) =$$
$$= 2\sum_{d|m} \mu(d) \log d + \sum_{d|m} \mu(d)\, \varepsilon_{bd},$$

where we used $\sum_{d|m} \mu(d) = 0$ for $m \geqslant 2$. Under the given hypothesis on m, we also have

$$\sum_{d|m} \mu(d) \log d = 0$$

by [1, Theorem 298]. Therefore,

$$\sum_{d|m} \mu(d) L(bd) = \sum_{d|m} \mu(d)\, \varepsilon_{bd}. \tag{15}$$

If b is even, we get from Lemma 1,

$$-\frac{4}{b^2} \sum_{\substack{d|m \\ \mu(d)=1}} \frac{1}{d^2} < \sum_{d|m} \mu(d)\, \varepsilon_{bd} < \frac{4}{b^2} \sum_{\substack{d|m \\ \mu(d)=-1}} \frac{1}{d^2}. \tag{16}$$

Now

$$\sum_{\substack{d|m \\ \mu(d)=1}} \frac{1}{d^2} < \sum_{\substack{d=1 \\ \mu(d)=1}}^{\infty} \frac{1}{d^2} < 1.075$$

and

$$\sum_{\substack{d|m \\ \mu(d)=-1}} \frac{1}{d^2} < \sum_{\substack{d=1 \\ \mu(d)=-1}}^{\infty} \frac{1}{d^2} < \frac{\pi^2}{6} - 1,$$

and so the bounds in (14) follow from (15) and (16). If b is odd, then by (15) we can write

$$\sum_{d \mid m} \mu(d) L(b\,d) = \sum_{\substack{d \mid m \\ 2 \mid d}} \mu(d)\, \varepsilon_{bd} + \sum_{\substack{d \mid m \\ 2 \nmid d}} \mu(d)\, \varepsilon_{bd}. \tag{17}$$

Using Lemmas 1 and 2, we get

$$\sum_{d \mid m} \mu(d) L(b\,d) <$$

$$< \frac{4}{b^2} \sum_{\substack{d \mid m \\ 2 \mid d,\, \mu(d) = -1}} \frac{1}{d^2} + \frac{1}{b^2} \sum_{\substack{d \mid m \\ 2 \nmid d,\, \mu(d) = 1}} \frac{1}{d^2} + \frac{3}{b^2} \sum_{\substack{d \mid m \\ 2 \nmid d,\, \mu(d) = -1}} \frac{1}{d^2} <$$

$$< \frac{4}{b^2} \sum_{\substack{d=1 \\ 2 \mid d,\, \mu(d) = -1}}^{\infty} \frac{1}{d^2} + \frac{1}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = 1}}^{\infty} \frac{1}{d^2} + \frac{3}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = -1}}^{\infty} \frac{1}{d^2} =$$

$$= \frac{2}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = 1}}^{\infty} \frac{1}{d^2} + \frac{3}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = -1}}^{\infty} \frac{1}{d^2}.$$

Now

$$\sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = 1}}^{\infty} \frac{1}{d^2} < 1.02 \quad \text{and} \quad \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = -1}}^{\infty} \frac{1}{d^2} < 0.22, \tag{18}$$

and this leads to the upper bound in (14). Using (17) and Lemmas 1 and 2, we obtain

$$\sum_{d \mid m} \mu(d) L(b\,d) >$$

$$> -\frac{4}{b^2} \sum_{\substack{d \mid m \\ 2 \mid d,\, \mu(d) = 1}} \frac{1}{d^2} - \frac{1}{b^2} \sum_{\substack{d \mid m \\ 2 \nmid d,\, \mu(d) = -1}} \frac{1}{d^2} - \frac{3}{b^2} \sum_{\substack{d \mid m \\ 2 \nmid d,\, \mu(d) = 1}} \frac{1}{d^2} >$$

$$> -\frac{4}{b^2} \sum_{\substack{d=1 \\ 2 \mid d,\, \mu(d) = 1}}^{\infty} \frac{1}{d^2} - \frac{1}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = -1}}^{\infty} \frac{1}{d^2} - \frac{3}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = 1}}^{\infty} \frac{1}{d^2} =$$

$$= -\frac{2}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = -1}}^{\infty} \frac{1}{d^2} - \frac{3}{b^2} \sum_{\substack{d=1 \\ 2 \nmid d,\, \mu(d) = 1}}^{\infty} \frac{1}{d^2},$$

and the lower bound in (14) holds because of (18).

Lemma 4. *Let $m=p^\alpha$, p prime, $\alpha \geqslant 1$. Then for every positive integer b we have*

$$-2\log p - \frac{4}{b^2} < \sum_{d|m} \mu(d) L(bd) < 0.$$

Proof. We obtain

$$\sum_{d|m} \mu(d) L(bd) = L(b) - L(bp) < 0$$

from the increasing behavior of L. Furthermore,

$$\sum_{d|m} \mu(d) L(bd) = L(b) - L(bp) = -2\log p + \varepsilon_b - \varepsilon_{bp}$$

because of Lemmas 1 and 2, and we get the lower bound by using the information about ε_b and ε_{bp} in those results and distinguishing between the three cases (i) b even; (ii) b odd, p odd; (iii) b odd, $p=2$.

3. An Inequality for Exponential Sums

We use the results of the preceding section to establish an estimate for certain weighted exponential sums. We write φ for Euler's totient function and $e(t)=e^{2\pi i t}$ for real t.

Lemma 5. *For integers $m \geqslant 2$ and $j \not\equiv 0 \pmod m$ we have*

$$\left| \sum_{h \pmod m} \sum_{\substack{g \pmod m \\ (g,m)=1}} e\left(\frac{j}{m} hg\right) r(h)^{-1} \right| < \varphi(m) + \frac{2.7}{b} \tag{19}$$

with $b=(m,j)$. If m/b is a prime or a prime power, then we have

$$\left| \sum_{h \pmod m} \sum_{\substack{g \pmod m \\ (g,m)=1}} e\left(\frac{j}{m} hg\right) r(h)^{-1} \right| < \varphi(m). \tag{20}$$

Proof. We note that

$$S := \sum_{h \pmod m} \sum_{\substack{g \pmod m \\ (g,m)=1}} e\left(\frac{j}{m} hg\right) r(h)^{-1} =$$

$$= \varphi(m) + \sum_{h \pmod m}^{*} |h|^{-1} \sum_{\substack{g \pmod m \\ (g,m)=1}} e\left(\frac{j}{m} hg\right) =$$

$$= \varphi(m) + \sum_{h \pmod m}^{*} |h|^{-1} \sum_{g \pmod m} e\left(\frac{j}{m} hg\right) \sum_{d \mid (g,m)} \mu(d) =$$

$$= \varphi(m) + \sum_{d \mid m} \mu(d) \sum_{h \pmod m}^{*} |h|^{-1} \sum_{a \pmod{m/d}} e\left(\frac{j}{m} had\right).$$

The inner sum is equal to 0 if $jh \not\equiv 0 \pmod{(m/d)}$ and equal to m/d otherwise. Therefore,

$$S = \varphi(m) + m \sum_{d \mid m} \frac{\mu(d)}{d} \sum_{\substack{h \pmod m \\ (m/d) \mid jh}}^{*} |h|^{-1}.$$

Now $jh \equiv 0 \pmod{(m/d)}$ iff $h \equiv 0 \pmod{(m/c_d d)}$, where $c_d = (m/d, j)$. It follows that

$$\sum_{\substack{h \pmod m \\ (m/d) \mid jh}}^{*} |h|^{-1} = \sum_{k \pmod{c_d d}}^{*} \frac{c_d d}{m \mid k \mid} = \frac{c_d d}{m} L(c_d d),$$

and so

$$S = \varphi(m) + \sum_{d \mid m} \mu(d) c_d L(c_d d). \tag{21}$$

Let the notation for the canonical factorizations of m and $b = (m, j)$ be arranged in such a way that we can write

$$m = p_1^{\alpha_1} \dots p_t^{\alpha_t},$$

$$b = p_1^{\beta_1} \dots p_u^{\beta_u} p_{u+1}^{\alpha_{u+1}} \dots p_t^{\alpha_t},$$

where $\alpha_i \geqslant 1$ for $1 \leqslant i \leqslant t$ and $0 \leqslant \beta_i \leqslant \alpha_i - 1$ for $1 \leqslant i \leqslant u$. We have $u \geqslant 1$ by the hypothesis on j, but we may have $u = t$. Let

$$b_1 = p_1^{\beta_1} \dots p_u^{\beta_u}, \; b_2 = p_{u+1}^{\alpha_{u+1}} \dots p_t^{\alpha_t},$$

where $b_2 = 1$ if $u = t$, so that $b = b_1 b_2$ in all cases. Because of the factor $\mu(d)$ in the sum in (21), it suffices to consider squarefree divisors d of m. Any such divisor can be uniquely represented in the form $d = d_1 d_2$ with $d_1 \mid p_1 \dots p_u$, $d_2 \mid p_{u+1} \dots p_t$, where the latter product is 1 if $u = t$. We get then

$$c_d = \left(\frac{m}{d}, j\right) = \left(\frac{p_1^{\alpha_1} \dots p_u^{\alpha_u}}{d_1} \cdot \frac{b_2}{d_2}, j\right) = b_1 \frac{b_2}{d_2} = \frac{b}{d_2},$$

and so

$$\sum_{d|m} \mu(d)\, c_d\, L(c_d d) = \sum_{d_1|p_1\ldots p_u} \sum_{d_2|p_{u+1}\ldots p_t} \mu(d_1 d_2)\, \frac{b}{d_2}\, L(b\, d_1) =$$

$$= b \left(\sum_{d_1|p_1\ldots p_u} \mu(d_1)\, L(b\, d_1) \right) \left(\sum_{d_2|p_{u+1}\ldots p_t} \frac{\mu(d_2)}{d_2} \right) =$$

$$= b\, \frac{\varphi(b_2)}{b_2} \sum_{d_1|p_1\ldots p_u} \mu(d_1)\, L(b\, d_1)\,.$$

Altogether, we have

$$S = \varphi(m) + b_1 \varphi(b_2) \sum_{d_1|p_1\ldots p_u} \mu(d_1)\, L(b\, d_1)\,. \tag{22}$$

If $u \geqslant 2$, we can use Lemma 3 to obtain

$$\varphi(m) - b_1 \varphi(b_2)\, \frac{4.3}{b^2} < S < \varphi(m) + b_1 \varphi(b_2) \frac{2.7}{b^2}\,,$$

hence

$$\varphi(m) - \frac{4.3}{b} < S < \varphi(m) + \frac{2.7}{b}\,,$$

which implies (19). If $u = 1$, i. e., if m/b is a prime or a prime power, then

$$S > \varphi(m) - b_1 \varphi(b_2) \left(2 \log p_1 + \frac{4}{b^2} \right)$$

follows from Lemma 4 and (22). To obtain $S > -\varphi(m)$, it suffices then to show that

$$b_1 \varphi(b_2) \left(\log p_1 + \frac{2}{b^2} \right) < \varphi(m)\,,$$

which, after multiplication by $b_2/\varphi(b_2)$, becomes

$$b \log p_1 + \frac{2}{b} < \frac{\varphi(m)\, b_2}{\varphi(b_2)} = m \left(1 - \frac{1}{p_1} \right). \tag{23}$$

If $b\, m \geqslant 14$, then

$$\frac{2}{b} < m \left(1 - \frac{1 + \log 2}{2} \right) \leqslant m \left(1 - \frac{1 + \log p_1}{p_1} \right),$$

and since $b \leqslant m/p_1$, (23) is established. In the finitely many remaining cases with $b\, m < 14$, the inequality $S > -\varphi(m)$ can be checked by inspection. The estimate $S < \varphi(m)$ follows from Lemma 4 and (22).

4. Proof of Theorems 1 and 2

Let G be the set of lattice points $\mathbf{g}=(g_1,\ldots,g_s)\in\mathbb{Z}^s$ for which each $g_j, 1\leqslant j\leqslant s$, is relatively prime to m and satisfies $-m/2<g_j\leqslant m/2$. The cardinality of G is $\varphi(m)^s$. To prove the two theorems, it will suffice to show that

$$M:=\frac{1}{\varphi(m)^s}\sum_{\mathbf{g}\in G}R(\mathbf{g},m)<\frac{1}{m}(C+2\log m)^s, \tag{24}$$

where $C=1.4$ for Theorem 1 and $C=0.81$ for Theorem 2. Now

$$M=\frac{1}{\varphi(m)^s}\sum_{\mathbf{g}\in G}\sum_{\substack{\mathbf{h}\,(\mathrm{mod}\,m)\\ \mathbf{h}\cdot\mathbf{g}\equiv 0\,(\mathrm{mod}\,m)}}^{*} r(\mathbf{h})^{-1}=$$

$$=\frac{1}{\varphi(m)^s}\sum_{\mathbf{h}\,(\mathrm{mod}\,m)}^{*}N(\mathbf{h})\,r(\mathbf{h})^{-1}=\frac{1}{\varphi(m)^s}\sum_{\mathbf{h}\,(\mathrm{mod}\,m)}N(\mathbf{h})\,r(\mathbf{h})^{-1}-1,$$

where $N(\mathbf{h})$ is the number of lattice points $\mathbf{g}\in G$ with $\mathbf{h}\cdot\mathbf{g}\equiv 0\,(\mathrm{mod}\,m)$. Since

$$N(\mathbf{h})=\sum_{\mathbf{g}\in G}\frac{1}{m}\sum_{j=0}^{m-1}e\left(\frac{j}{m}\mathbf{h}\cdot\mathbf{g}\right),$$

we can write

$$\sum_{\mathbf{h}\,(\mathrm{mod}\,m)}N(\mathbf{h})\,r(\mathbf{h})^{-1}=\frac{1}{m}\sum_{j=0}^{m-1}\sum_{\mathbf{h}\,(\mathrm{mod}\,m)}\sum_{\mathbf{g}\in G}e\left(\frac{j}{m}\mathbf{h}\cdot\mathbf{g}\right)r(\mathbf{h})^{-1}=$$

$$=\frac{1}{m}\sum_{j=0}^{m-1}\sum_{h_1\,(\mathrm{mod}\,m)}\cdots\sum_{h_s\,(\mathrm{mod}\,m)}$$

$$\sum_{\substack{g_1\,(\mathrm{mod}\,m)\\ (g_1,m)=1}}\cdots\sum_{\substack{g_s\,(\mathrm{mod}\,m)\\ (g_s,m)=1}}\frac{e\left((j/m)\,h_1g_1\right)\ldots e\left((j/m)\,h_sg_s\right)}{r(h_1)\ldots r(h_s)}=$$

$$=\frac{1}{m}\sum_{j=0}^{m-1}\left(\sum_{h\,(\mathrm{mod}\,m)}\sum_{\substack{g\,(\mathrm{mod}\,m)\\ (g,m)=1}}e\left(\frac{j}{m}hg\right)r(h)^{-1}\right)^s,$$

and so

$$M = \frac{1}{m} \sum_{j=0}^{m-1} \left(\frac{1}{\varphi(m)} \sum_{h \,(\mathrm{mod}\, m)} \sum_{\substack{g \,(\mathrm{mod}\, m) \\ (g,m)=1}} e\left(\frac{j}{m} hg\right) r(h)^{-1} \right)^s - 1 .$$

The contribution from $j=0$ to the above sum is $(1+L(m))^s$, so that

$$M = \frac{1}{m} (1+L(m))^s + \tag{25}$$
$$+ \frac{1}{m} \sum_{j=1}^{m-1} \left(\frac{1}{\varphi(m)} \sum_{h \,(\mathrm{mod}\, m)} \sum_{\substack{g \,(\mathrm{mod}\, m) \\ (g,m)=1}} e\left(\frac{j}{m} hg\right) r(h)^{-1} \right)^s - 1 .$$

If m is a prime or a prime power, we can apply (20) to obtain

$$M < \frac{1}{m} (1+L(m))^s + \frac{m-1}{m} - 1 < \frac{1}{m} (1+L(m))^s .$$

Furthermore, Lemmas 1 and 2 easily yield the inequality

$$L(m) < 2 \log m - 0.19 \quad \text{for} \quad m \geqslant 2 ,$$

and so (24) is shown with $C = 0.81$. Thus, Theorem 2 is established.

From now on, we may assume that m has at least two distinct prime divisors, so that, in particular, $m \geqslant 6$. We apply (19) in (25) and note that each proper divisor b of m appears exactly $\varphi(m/b)$ times among the greatest common divisors (m,j), $1 \leqslant j \leqslant m-1$. This yields

$$M < \frac{1}{m} (1+L(m))^s + \frac{1}{m} \sum_{\substack{b \mid m \\ b<m}} \varphi\left(\frac{m}{b}\right) \left(1 + \frac{2.7}{\varphi(m) b}\right)^s - 1 =$$
$$= \frac{1}{m} (1+L(m))^s + \frac{1}{m} \sum_{\substack{b \mid m \\ b<m}} \varphi\left(\frac{m}{b}\right) - 1 +$$
$$+ \frac{1}{m} \sum_{\substack{b \mid m \\ b<m}} \varphi\left(\frac{m}{b}\right) \sum_{k=1}^{s} \binom{s}{k} \left(\frac{2.7}{\varphi(m) b}\right)^k .$$

Since

$$\sum_{\substack{b \mid m \\ b<m}} \varphi\left(\frac{m}{b}\right) = m - 1 ,$$

it follows that

$$M < \frac{1}{m} \sum_{k=1}^{s} \binom{s}{k} L(m)^k + \frac{1}{m} \sum_{k=1}^{s} \binom{s}{k} \left(\frac{2.7}{\varphi(m)} \right)^k \sum_{b \mid m} \varphi\left(\frac{m}{b}\right) b^{-k}.$$

By using a simple change of variable in the last sum and setting

$$F_k(m) = \frac{1}{\varphi(m)^k m^k} \sum_{b \mid m} \varphi(b) b^k \quad \text{for } k \geqslant 1,$$

we get

$$M < \frac{1}{m} \sum_{k=1}^{s} \binom{s}{k} L(m)^k + \frac{1}{m} \sum_{k=1}^{s} \binom{s}{k} (2.7)^k F_k(m). \tag{26}$$

The treatment of F_k is based on the fact that it is a multiplicative arithmetic function. For a prime p and $\alpha \geqslant 1$, a straightforward calculation shows that

$$F_1(p^\alpha) = 1 + \frac{1 + p^{1-2\alpha}}{p^2 - 1} \leqslant 1 + \frac{1 + p^{-1}}{p^2 - 1} = 1 + \frac{1}{p(p-1)},$$

and so

$$F_1(m) \leqslant \prod_{p \mid m} \left(1 + \frac{1}{p(p-1)} \right) < \prod_{p} \left(1 + \frac{1}{p(p-1)} \right) < 2. \tag{27}$$

For $k \geqslant 2$ we set

$$H_k(m) = \varphi(m)^{k-1} F_k(m), \tag{28}$$

and then another calculation yields

$$H_k(p^\alpha) = 1 + \frac{p - 1 + p^{(k+1)(1-\alpha)} - p^{1-\alpha-\alpha k}}{(p^{k+1} - 1)(p-1)} <$$

$$< 1 + \frac{p}{(p^{k+1} - 1)(p-1)} \leqslant 1 + \frac{p}{(p^3 - 1)(p-1)}$$

and

$$H_k(m) \leqslant$$

$$\leqslant \prod_{p \mid m} \left(1 + \frac{p}{(p^3 - 1)(p-1)} \right) < \prod_{p} \left(1 + \frac{p}{(p^3 - 1)(p-1)} \right) < 1.4.$$

Together with (28) we get

$$F_k(m) < \frac{1.4}{\varphi(m)^{k-1}} \quad \text{for } k \geqslant 2,$$

and combining this with (26) and (27), we obtain

$$M < \frac{1}{m} \sum_{k=1}^{s} \binom{s}{k} L(m)^k + \frac{1}{m} \left((5.4)\, s + \sum_{k=2}^{s} \binom{s}{k} (2.7)^k \frac{1.4}{\varphi(m)^{k-1}} \right) =$$

$$= \frac{1}{m} \sum_{k=1}^{s} \binom{s}{k} L(m)^k + \frac{1}{m} \left((5.4)\, s + (3.78) \sum_{k=2}^{s} \binom{s}{k} \left(\frac{2.7}{\varphi(m)} \right)^{k-1} \right). \tag{29}$$

We consider first the case $s = 2$. We claim that

$$2L(m) + L(m)^2 + 10.8 + \frac{(3.78)\,(2.7)}{\varphi(m)} < (1.6 + L(m))^2 \text{ for } m \geqslant 46, \tag{30}$$

or, equivalently, that

$$8.24 + \frac{10.206}{\varphi(m)} < (1.2)\, L(m) \quad \text{for } m \geqslant 46.$$

Since $\varphi(m) \geqslant 16$ for $m \geqslant 46$, we have

$$(1.2)\, L(m) \geqslant (1.2)\, L(46) > 8.91 > 8.24 + \frac{10.206}{\varphi(m)} \quad \text{for } m \geqslant 46,$$

and so (30) is shown. It follows then from (29) with $s = 2$ that

$$M < \frac{1}{m} (1.6 + L(m))^2 \quad \text{for } m \geqslant 46.$$

Since Lemmas 1 and 2 imply

$$L(m) < 2 \log m - 0.2 \text{ for } m \geqslant 6, \tag{31}$$

we have thus established (24) with $C = 1.4$ for $s = 2$ and $m \geqslant 46$. For the remaining moduli m in the case $s = 2$, Theorem 1 can be shown by explicit construction of a suitable lattice point. Thus, we take $\mathbf{g} = (1, -1)$ for $m = 6, 10, 12, 14, 15$; $\mathbf{g} = (1,3)$ for $m = 20$; $\mathbf{g} = (1,4)$ for $m = 21$; $\mathbf{g} = (1,5)$ for $m = 18, 22, 28, 33, 34, 42$; $\mathbf{g} = (1, 7)$ for $m = 24, 26, 30, 36, 38, 39, 40, 44, 45$; and $\mathbf{g} = (1,8)$ for $m = 35$.

For $s \geqslant 3$ it is clear from (29) and (31) that (24) with $C = 1.4$ will hold for $m \geqslant 6$ if we can show that

$$\sum_{k=1}^{s} \binom{s}{k} L(m)^k + (5.4)\, s + (3.78) \sum_{k=2}^{s} \binom{s}{k} \left(\frac{2.7}{\varphi(m)} \right)^{k-1} <$$

$$< (1.6 + L(m))^s \text{ for } m \geqslant 6.$$

Since $\varphi(m) \geqslant 2$ for $m \geqslant 6$, it suffices to prove that

$$\sum_{k=1}^{s} \binom{s}{k} L(m)^k + (5.4)\, s + (3.78) \sum_{k=2}^{s} \binom{s}{k} (1.35)^{k-1} < (1.6 + L(m))^s,$$

or, equivalently,

$$(5.4)\, s + (2.8) \sum_{k=2}^{s} \binom{s}{k} (1.35)^k < \\ < (1.6)^s + \sum_{k=1}^{s-1} \binom{s}{k} \left((1.6)^{s-k} - 1\right) L(m)^k \quad \text{for } m \geqslant 6. \tag{32}$$

We note that

$$(5.2)\, s = s\,(1.56)\, L(6) \leqslant s \left((1.6)^{s-1} - 1\right) L(m) \text{ for } m \geqslant 6. \tag{33}$$

Next we claim that for $m \geqslant 6$ we have

$$(0.2)\, s + (2.8)\,(1.35)^s + (2.8)\, s\,(1.35)^{s-1} < (1.6)^s + (0.6)\, s\, L(m)^{s-1}. \tag{34}$$

To verify (34), we observe that

$$(0.2)\, s + (2.8)\,(1.35)^s + (2.8)\, s\,(1.35)^{s-1} = \\ = (1.35)^s \left(\frac{0.2}{(1.35)^s} s + 2.8 + \frac{2.8}{1.35} s \right) < \tag{35}$$

$$< (1.35)^s \left(\frac{0.2}{(1.35)^3} s + 2.8 + (2.08)\, s \right) < (1.35)^s \left(2.8 + (2.17)\, s\right).$$

Furthermore, we have

$$2.8 < (1.18)^3 + 3 \left((0.18)\,(2.45)^3 - 2.17\right) \leqslant (1.18)^s + \\ + s \left((0.18)\,(2.45)^s - 2.17\right),$$

and so

$$2.8 + (2.17)\, s < (1.18)^s + (0.18)\, s\,(2.45)^s.$$

Multiplication by $(1.35)^s$ yields

$$(1.35)^s \left(2.8 + (2.17)\, s\right) < (1.6)^s + (0.18)\, s\, (\tfrac{10}{3})^s = (1.6)^s + (0.6)\, s\, (\tfrac{10}{3})^{s-1} \\ \leqslant (1.6)^s + (0.6)\, s\, L(m)^{s-1}$$

since $\frac{10}{3} = L(6) \leqslant L(m)$. In combination with (35), we get then (34). For $2 \leqslant k \leqslant s-2$ and $m \geqslant 6$ we have

$$(2.8)\,(1.35)^k < (1.56)\, (\tfrac{10}{3})^k \leqslant \left((1.6)^{s-k} - 1\right) L(m)^k,$$

and so

$$(2.8)\quad \binom{s}{k}(1.35)^k < \binom{s}{k}\left((1.6)^{s-k}-1\right)L(m)^k \quad \text{for } 2 \leqslant k \leqslant s-2,\ m \geqslant 6\,. \tag{36}$$

By adding up the inequalities (33), (34), and (36), we obtain (32), and the proof of Theorem 1 is complete.

References

[1] HARDY, G. H., and E. M. WRIGHT: An Introduction to the Theory of Numbers, 4th ed. Oxford: Clarendon Press. 1960.

[2] HLAWKA, E.: Zur angenäherten Berechnung mehrfacher Integrale. Mh. Math. **66**, 140—151 (1962).

[3] KOROBOV, N. M.: The approximate computation of multiple integrals. Dokl. Akad. Nauk SSSR **124**, 1207—1210 (1959). (Russian.)

[4] KUIPERS, L., and H. NIEDERREITER: Uniform Distribution of Sequences. New York: Wiley-Interscience. 1974.

[5] MAISONNEUVE, D.: Recherche et utilisation des „bons treillis". Programmation et résultats numériques. Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.), pp. 121—201. New York: Academic Press. 1972.

[6] NIEDERREITER, H.: Statistical independence of linear congruential pseudo-random numbers. Bull. Amer. Math. Soc. **82**, 927—929 (1976).

[7] NIEDERREITER, H.: Pseudo-random numbers and optimal coefficients. Advances Math. **26**, 99—181 (1977).

[8] NIEDERREITER, H.: The serial test for linear congruential pseudo-random numbers. Bull. Amer. Math. Soc. **84**, 273—274 (1978).

[9] NIEDERREITER, H.: Quasi-Monte Carlo methods and pseudo-random numbers. Bull. Amer. Math. Soc. (To appear.)

[10] ZAREMBA, S. K.: La méthode des „bons treillis" pour le calcul des intégrales multiples. Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.), pp. 39—119. New York: Academic Press. 1972.

[11] ZAREMBA, S. K.: Good lattice points modulo composite numbers. Mh. Math. **78**, 446—460 (1974).

Prof. Dr. H. NIEDERREITER
Chair in Pure Mathematics
University of the West Indies
Kingston 7, Jamaica