MATHEMATICS OF COMPUTATION, VOLUME 28, NUMBER 128
OCTOBER 1974, PAGES 1117–1132

On the Distribution of Pseudo-Random Numbers Generated by the Linear Congruential Method. II

By Harald Niederreiter*

Abstract. The discrepancy of a sequence of pseudo-random numbers generated by the linear congruential method is estimated for parts of the period which are somewhat larger than the square root of the modulus. Applications to numerical integration are mentioned.

1. Introduction. Let $m \geqslant 2$ be an integer, let y_0 be an integer in the least residue system modulo m with $(y_0, m) = 1$, and let λ be an integer with $(\lambda, m) = 1$. We generate a sequence $y_0, y_1, \cdots$ of integers in the least residue system modulo m by the recursion $y_{n+1} \equiv \lambda y_n \pmod{m}$, $n = 0, 1, \cdots$. The sequence $x_0, x_1, \cdots$, defined by $x_n = y_n/m$ for $n \geqslant 0$, is then a frequently employed sequence of pseudo-random numbers in the unit interval $[0, 1]$. Its elements may also be described explicitly by $x_n = \{\lambda^n y_0/m\}$ for $n \geqslant 0$, where $\{t\}$ denotes the fractional part of the real number t. If λ belongs to the exponent $\tau = \tau(m)$ modulo m, then the sequence $x_0, x_1, \cdots$ has period τ. We note that always $\tau \leqslant \varphi(m)$, where φ is Euler's totient function.

In the first paper [7] of this series, the author has studied the distribution in $[0, 1]$ of the full period $x_0, x_1, \cdots, x_{\tau-1}$ in the case that λ is a primitive root modulo m, i.e., that $\tau = \varphi(m)$. It turned out that the full period provides an extremely good approximation to the uniform distribution in $[0, 1]$. However, in many practical situations, one will only use an initial segment of the full period, simply because the period τ is too large in most of the interesting cases. In the present paper, we therefore consider the question of the distribution of the sequence $x_0, x_1, \cdots, x_{N-1}$ with $1 \leqslant N \leqslant \tau$ in the interval $[0, 1]$. We also abandon the requirement that λ has to be a primitive root modulo m. In a sense to be made precise below, we estimate the deviation of the distribution of such a segment from the uniform distribution. We distinguish between m being a prime, a prime power, or a general modulus, since, in the special cases, somewhat better results can be

Received October 15, 1973.

AMS (MOS) subject classifications. (1970). Primary 10F40, 10K05, 65C10, 65D30; Secondary 10G05, 65C05.

Key words and phrases. Pseudo-random numbers, discrepancy, uniform distribution, trigonometric sums, numerical integration.

(*) This research was supported by NSF grant GP-36418X1.

shown. There will be an emphasis on prime power moduli, since this is the case occurring most frequently in practice. The estimates that we establish are only of interest when N is at least of the order of magnitude $m^{1/2+\epsilon}$ for some $\epsilon > 0$. In the proofs, we make use of the work of N. M. Korobov [1], [2] on special trigonometric sums and of an effective version of the Erdős-Turán inequality which was recently given by the author and W. Philipp [10]. In the last section of the paper, we mention applications of the results to numerical integrations using the points x_0, $x_1, \cdots, x_{N-1}$ as nodes.

For $1 \leqslant N \leqslant \tau$, consider the points $x_0, x_1, \cdots, x_{N-1}$ described above. Given real numbers u and v with $0 \leqslant u < v \leqslant 1$, let $A(u, v; N)$ be the number of n, $0 \leqslant n \leqslant N-1$, with $x_n \in [u, v)$. Then we define the so-called discrepancy D_N of the points $x_0, x_1, \cdots, x_{N-1}$ by

$$D_N = D_N(x_0, \cdots, x_{N-1}) = \sup_{0 \leqslant u < v \leqslant 1} |A(u, v; N)/N - (v-u)|.$$

This is the quantity which we shall estimate. For the general theory of discrepancy, see the book of L. Kuipers and the author [3, Chapter 2].

2. Lemmas on Trigonometric Sums. For real t, we write $e(t) = e^{2\pi i t}$. We consider trigonometric sums of the type

$$\sum_{n=0}^{N-1} e(rx_n) = \sum_{n=0}^{N-1} e(ry_0\lambda^n/m)$$

with a nonzero integer r and $1 \leqslant N \leqslant \tau$. The estimates given in Lemmas 2 and 3 are due to N. M. Korobov [2]. For the convenience of the reader, we include the short proofs.

LEMMA 1. *For any integers A and B with $1 \leqslant B \leqslant A$, the sum*

$$S = \sum_{c=1}^{A} \left| \sum_{y=0}^{B-1} e(cy/A) \right|$$

satisfies $S \leqslant A(1 + \log A)$.

Proof. We have

$$\left| \sum_{y=0}^{B-1} e(cy/A) \right| = B \qquad \text{for } c = A,$$

$$= \frac{|e(cB/A) - 1|}{|e(c/A) - 1|} = \frac{\sin \pi \|cB/A\|}{\sin \pi \|c/A\|} \qquad \text{for } 1 \leqslant c \leqslant A-1,$$

where $\|t\|$ denotes the distance from the real number t to the nearest integer. If $A = 1$, the lemma is trivial. For $A \geqslant 2$ we get

$$S = B + \sum_{c=1}^{A-1} \frac{\sin \pi \|cB/A\|}{\sin \pi \|c/A\|} \leqslant B + 2 \sum_{c=1}^{[A/2]} \frac{\sin \pi \|cB/A\|}{\sin \pi \|c/A\|}$$

$$\leqslant B + 2\frac{\sin \pi \|B/A\|}{\sin (\pi/A)} + 2 \sum_{c=2}^{[A/2]} (2\|c/A\|)^{-1},$$

where the last sum is taken to be zero for $A < 4$. It follows that

$$S \leqslant B + 2A\|B/A\| + A \sum_{c=2}^{[A/2]} c^{-1} \leqslant B + 2A\|B/A\| + A \log[A/2]$$

$$\leqslant A(B/A + 2\|B/A\| - \log 2 + \log A) \leqslant A(1 + \log A),$$

where the last inequality is shown by distinguishing between the cases $B/A \leqslant 1/2$ and $B/A > 1/2$.

LEMMA 2. *Let $m \geqslant 2$ be an integer, let b and λ be integers relatively prime to m, and suppose λ belongs to the exponent τ modulo m. Then*

$$\left| \sum_{n=0}^{N-1} e(b\lambda^n/m) \right| \leqslant \sqrt{m}\ (1 + \log \tau)$$

holds for all N with $1 \leqslant N \leqslant \tau$.

Proof. For integers a and c, write

$$\sigma(a, c) = \sum_{n=0}^{\tau-1} e(a\lambda^n/m + cn/\tau).$$

Since $\lambda^\tau \equiv 1 \pmod m$, we have

$$\{a\lambda^{n+\tau}/m + c(n + \tau)/\tau\} = \{a\lambda^n/m + cn/\tau\},$$

so that $e(a\lambda^n/m + cn/\tau)$, as a function of n, depends only on the residue class of n modulo τ. Therefore, for any integer y, we have

$$\sigma(a, c) = \sum_{n=0}^{\tau-1} e(a\lambda^{n+y}/m + c(n + y)/\tau),$$

and consequently

$$|\sigma(a, c)| = \left| \sum_{n=0}^{\tau-1} e(a\lambda^y\lambda^n/m + cn/\tau) \right| = |\sigma(a\lambda^y, c)|.$$

Since the integers $b\lambda, b\lambda^2, \cdots, b\lambda^\tau$ are pairwise incongruent modulo m, we have

$$\tau|\sigma(b, c)|^2 = \sum_{y=1}^{\tau} |\sigma(b\lambda^y, c)|^2 \leqslant \sum_{a=1}^{m} |\sigma(a, c)|^2 = m\tau,$$

hence $|\sigma(b, c)| \leqslant \sqrt{m}$. Now

$$\sum_{n=0}^{N-1} e(b\lambda^n/m) = \frac{1}{\tau} \sum_{c=1}^{\tau} \left(\sum_{y=0}^{N-1} e(-cy/\tau) \right) \left(\sum_{n=0}^{\tau-1} e(b\lambda^n/m + cn/\tau) \right),$$

and so by Lemma 1

$$\left| \sum_{n=0}^{N-1} e(b\lambda^n/m) \right| \leqslant \sqrt{m} \cdot \frac{1}{\tau} \sum_{c=1}^{\tau} \left| \sum_{y=0}^{N-1} e(-cy/\tau) \right| \leqslant \sqrt{m}\ (1 + \log \tau).$$

We remark that for the special case $m = p$, a prime, and λ a primitive root modulo p, trigonometric sums of the above form have also been considered by L. J. Mordell [4], [5] and R. G. Stoneham [11].

LEMMA 3. *Let $m \geqslant 2$ be an integer, and let λ be an integer relatively prime to m which belongs to the exponent τ modulo m. If b is an integer with $(b, m) = d > 1$ and such that $\sum_{n=0}^{\tau-1} e(b\lambda^n/m) = 0$, then for all N with $1 \leqslant N \leqslant \tau$ we have*

$$\left| \sum_{n=0}^{N-1} e(b\lambda^n/m) \right| \leqslant \sqrt{\frac{m}{d}}(1 + \log \tau(m/d)),$$

where $\tau(m/d)$ is the exponent to which λ belongs modulo m/d.

Proof. Since $e(b\lambda^n/m)$, as a function of n, is periodic with period $\tau(m/d)$, we have

$$\sum_{n=0}^{\tau-1} e(b\lambda^n/m) = \frac{\tau}{\tau(m/d)} \sum_{n=0}^{\tau(m/d)-1} e(b\lambda^n/m),$$

and so

$$\sum_{n=0}^{\tau(m/d)-1} e(b\lambda^n/m) = 0.$$

Write $N = q\tau(m/d) + s$, $0 \leqslant s < \tau(m/d)$. Then

$$\sum_{n=0}^{N-1} e(b\lambda^n/m) = \sum_{j=0}^{q-1} \sum_{n=0}^{\tau(m/d)-1} e(b\lambda^{j\tau(m/d)+n}/m) + \sum_{n=0}^{s-1} e(b\lambda^{q\tau(m/d)+n}/m)$$

$$= q \sum_{n=0}^{\tau(m/d)-1} e(b\lambda^n/m) + \sum_{n=0}^{s-1} e(b\lambda^n/m) = \sum_{n=0}^{s-1} e\left(\frac{(b/d)\lambda^n}{m/d}\right)$$

To the last sum we can apply Lemma 2 in order to obtain the desired inequality.

3. Prime Modulus. Here we consider the case that m is a prime. The notation remains the same as in the introduction.

THEOREM 1. *Let m be a prime. Then, for $1 \leqslant N \leqslant \tau$, the discrepancy D_N of the points $x_0, x_1, \cdots, x_{N-1}$ satisfies the inequality*

$$D_N \leqslant \frac{4\sqrt{m}\ (1 + \log \tau)}{\pi N} \left| \log \frac{\pi N}{\sqrt{m}(1 + \log \tau)} \right| + \frac{5\sqrt{m}\ (1 + \log \tau)}{\pi N}.$$

Proof. We use an inequality established by the author and W. Philipp [10, Corollary of Theorem 1']: for any points $z_0, \cdots, z_{N-1}$ in $[0, 1)$ with discrepancy $D_N(z_0, \cdots, z_{N-1})$ we have

$$D_N(z_0, \cdots, z_{N-1}) \leqslant \frac{4}{L} + \frac{4}{\pi} \sum_{r=1}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \left| \frac{1}{N} \sum_{n=0}^{N-1} e(rz_n) \right| \tag{1}$$

for all positive integers L. In order to apply this to the special sequence $x_0, x_1, \cdots, x_{N-1}$, we choose

$$L = \left[\frac{\pi N}{\sqrt{m}(1 + \log \tau)}\right].$$

If $L < 5$, then the theorem is trivial since we have always $D_N \leqslant 1$. Thus we assume $L \geqslant 5$ from now on. For the same reason, the case $\tau = 1$ is trivial, so that we may assume $\tau \geqslant 2$. From (1) we obtain

$$\begin{aligned} D_N &\leqslant \frac{4}{L} + \frac{4}{\pi} \sum_{r=1}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \left|\frac{1}{N} \sum_{n=0}^{N-1} e(rx_n)\right| \\ &= \frac{4}{L} + \frac{4}{\pi} \sum_{r=1}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \left|\frac{1}{N} \sum_{n=0}^{N-1} e(ry_0\lambda^n/m)\right| \end{aligned} \tag{2}$$

We note that

$$5 \leqslant L \leqslant \frac{\pi N}{\sqrt{m}(1 + \log \tau)} \leqslant \frac{\pi \tau}{\sqrt{m}(1 + \log \tau)} < \frac{\pi m}{\sqrt{m}(1 + \log 2)},$$

hence $\sqrt{m} > 5(1 + \log 2)/\pi$. It follows that

$$L < \frac{1}{5}\left(\frac{\pi}{1 + \log 2}\right)^2 m < m.$$

Therefore we have $(ry_0, m) = 1$ for all the values of r considered in (2). By applying Lemma 2, we deduce from (2) that

$$D_N \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \sum_{r=1}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \log L,$$

where we use the inequality $\Sigma_{r=1}^{L} r^{-1} \leqslant 1 + \log L$. From $L \geqslant 5$, the inequality $[t] \geqslant 5t/6$ for $t \geqslant 5$, and the special form of L it follows that

$$\begin{aligned} D_N &\leqslant \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \log \frac{\pi N}{\sqrt{m}(1 + \log \tau)} + \frac{24\sqrt{m}(1 + \log \tau)}{5\pi N} \\ &< \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \left|\log \frac{\pi N}{\sqrt{m}(1 + \log \tau)}\right| + \frac{5\sqrt{m}(1 + \log \tau)}{\pi N} \end{aligned}$$

This concludes the proof of the theorem.

We remark that the estimate in Theorem 1 is nontrivial when N is at least of the order of magnitude $m^{1/2+\epsilon}$ for some $\epsilon > 0$. In this case, D_N is then of the order of magnitude $N^{-1}\sqrt{m}(1 + \log \tau) \log m$. This gives a considerable improvement on a result of R. G. Stoneham [11].

4. Prime Power Modulus. Let $m = p^\alpha$ with a prime p and $\alpha \geqslant 2$. Let λ be relatively prime to m with $|\lambda| > 1$. Otherwise, the notation from the introduction remains operative. We determine a positive integer β as follows. First, let $\tau(p)$ be the exponent to which λ belongs modulo p. Then, if p is odd, β is the largest integer such that $p^\beta | (\lambda^{\tau(p)} - 1)$. If $p = 2$, set $\mu = 1$ if $\lambda \equiv 1 \pmod 4$ and $\mu = 2$ if $\lambda \equiv 3 \pmod 4$. Then β is taken to be the largest integer such that $2^\beta | (\lambda^\mu - 1)$.

THEOREM 2. *Let $m = p^\alpha$ with a prime p and $\alpha \geqslant 2$. Let λ be relatively prime to m with $|\lambda| > 1$ and $\alpha > \beta$, where β is defined above. Then, if $1 \leqslant N \leqslant \tau$ and*

$$p^\beta < \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{m^{3/2}(1 + \log \tau)}{\pi N}, \tag{3}$$

the discrepancy D_N of the points $x_0, x_1, \cdots, x_{N-1}$ satisfies the inequality

$$\begin{aligned} D_N \leqslant{}& \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \left| \log \frac{(p^{3/2} - 1)\pi N}{(p^{3/2} - p^{1/2})\sqrt{m}(1 + \log \tau)} \right| \\ &+ (2 + \log p) \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} + \left(1 + \frac{4}{p^{1/2}}\right) \frac{4m(1 + \log \tau)^2}{\pi^2 N^2}. \end{aligned} \tag{4}$$

Proof. As in the proof of Theorem 1, we infer from (1) that

$$D_N \leqslant \frac{4}{L} + \frac{4}{\pi} \sum_{r=1}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \left| \frac{1}{N} \sum_{n=0}^{N-1} e(r y_0 \lambda^n / m) \right| \tag{5}$$

for all positive integers L. We now choose

$$L = \left\lfloor \frac{(p^{3/2} - 1)\pi N}{(p^{3/2} - p^{1/2})\sqrt{m}(1 + \log \tau)} \right\rfloor.$$

If $L < 5$, the theorem is again trivial. So $L \geqslant 5$ from now on. Moreover, condition (3) implies that $L < p^{\alpha - \beta}$. From Lemma 2 we get

$$\left| \frac{1}{N} \sum_{n=0}^{N-1} e(r y_0 \lambda^n / m) \right| \leqslant \frac{\sqrt{m}(1 + \log \tau)}{N} \quad \text{for } (r, m) = 1. \tag{6}$$

Let R be the largest integer with $p^R \leqslant L$. We note that $0 \leqslant R \leqslant \alpha - \beta - 1$. For an integer r, $1 \leqslant r \leqslant L$, with $(r, m) = d > 1$ we have $d = p^s$ for some s with $1 \leqslant s \leqslant R$. Furthermore, $p^{\alpha - \beta}$ does not divide r. It follows then from a theorem

of N. M. Korobov [1, Theorem 2] that

$$\sum_{n=0}^{\tau-1} e(ry_0\lambda^n/m) = 0,$$

and so Lemma 3 yields

$$\left|\frac{1}{N}\sum_{n=0}^{N-1} e(ry_0\lambda^n/m)\right| \leqslant \frac{1}{N}\sqrt{\frac{m}{d}}\,(1 + \log \tau(m/d)) \leqslant \frac{1}{N}\sqrt{\frac{m}{d}}\,(1 + \log \tau). \tag{7}$$

Combining (5), (6) and (7), we arrive at the inequality

$$D_N \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \sum_{s=0}^{R} p^{-s/2} \sum_{r=1;(r,m)=p^s}^{L} \left(\frac{1}{r} - \frac{1}{L}\right). \tag{8}$$

For an integer s with $0 \leqslant s \leqslant R$ we have

$$\sum_{r=1;(r,m)=p^s}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) = \frac{1}{p^s} \sum_{r=1}^{[L/p^s]} \frac{1}{r} - \frac{1}{p^{s+1}} \sum_{r=1}^{[L/p^{s+1}]} \frac{1}{r}$$

$$- \frac{1}{L}\left(\left[\frac{L}{p^s}\right] - \left[\frac{L}{p^{s+1}}\right]\right),$$

and, using $\log (K + 1) \leqslant \sum_{r=1}^{K} r^{-1} \leqslant 1 + \log K$ for $K \geqslant 1$, we get

$$\sum_{r=1;\,(r,m)=p^s}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \leqslant \frac{1}{p^s}\left(1 + \log\left[\frac{L}{p^s}\right]\right) - \frac{1}{p^{s+1}} \log\left(\left[\frac{L}{p^{s+1}}\right] + 1\right)$$

$$- \frac{1}{L}\left(\left[\frac{L}{p^s}\right] - \left[\frac{L}{p^{s+1}}\right]\right)$$

$$= \frac{1}{p^s} \log\left[\frac{L}{p^s}\right] - \frac{1}{p^{s+1}} \log\left(\left[\frac{L}{p^{s+1}}\right] + 1\right) \tag{9}$$

$$+ \frac{1}{L}\left\{\frac{L}{p^s}\right\} + \frac{1}{L}\left[\frac{L}{p^{s+1}}\right]$$

If $R = 0$, that is, if $L < p$, then from (9) with $s = 0$ and (8) we deduce that

$$D_N \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \log L.$$

Since $L \geqslant 5$ and $[t] \geqslant 5t/6$ for $t \geqslant 5$, we arrive at

$$D_N \leqslant \frac{24(p^{3/2} - p^{1/2})\sqrt{m}(1 + \log \tau)}{5(p^{3/2} - 1)\pi N}$$

$$+ \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \log p < (2 + \log p) \frac{4\sqrt{m}(1 + \log \tau)}{\pi N},$$

so that (4) is shown in this case.

If $R = 1$, that is, if $p \leqslant L < p^2$, then from (9) with $s = 0, 1$ and from (8) we deduce that

$$D_N \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \left(\log L - \frac{1}{p} \log \frac{L}{p} + \frac{1}{p} + \frac{1}{p^{3/2}} \log \frac{L}{p} + \frac{1}{Lp^{1/2}} \right)$$

$$\leqslant \frac{4}{L} + \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \left(\frac{p-1}{p} \log L + \frac{\log p}{p} + \frac{1}{p} + \frac{\log p}{p^{3/2}} + \frac{1}{Lp^{1/2}} \right)$$

Using the special form of L, as well as $L \geqslant p$ and $[t] \geqslant (p/(p+1))t$ for $t \geqslant p$, we get

$$D_N \leqslant \frac{p-1}{p} \cdot \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \left| \log \frac{(p^{3/2} - 1)\pi N}{(p^{3/2} - p^{1/2})\sqrt{m}(1 + \log \tau)} \right|$$

$$+ \left(\frac{(p+1)(p^{3/2} - p^{1/2})}{p(p^{3/2} - 1)} + \frac{1}{p} + \frac{\log p}{p} + \frac{\log p}{p^{3/2}} \right) \frac{4\sqrt{m}(1 + \log \tau)}{\pi N}$$

$$+ \frac{(p+1)(p^{3/2} - p^{1/2})}{p^{3/2}(p^{3/2} - 1)} \cdot \frac{4m(1 + \log \tau)^2}{\pi^2 N^2}.$$

Now

$$\frac{p-1}{p} < \frac{p-1}{p} \cdot \frac{p^{3/2}}{p^{3/2} - 1} = \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1}$$

and

$$\frac{(p+1)(p^{3/2} - p^{1/2})}{p^{3/2}(p^{3/2} - 1)} < \frac{p+1}{p^{3/2}} < 1 + \frac{4}{p^{1/2}},$$

and furthermore

$$\frac{(p+1)(p^{3/2} - p^{1/2})}{p(p^{3/2} - 1)} + \frac{1}{p} + \frac{\log p}{p} + \frac{\log p}{p^{3/2}} < \frac{p+2}{p} + \log p \leqslant 2 + \log p,$$

so that (4) is also shown in this case.

For $R \geqslant 2$ we proceed as follows. By first simplifying (9) somewhat, we get

$$(10)\qquad \sum_{r=1;(r,m)=p^s}^{L}\left(\frac{1}{r}-\frac{1}{L}\right)\leqslant \frac{1}{p^s}\log\frac{L}{p^s}-\frac{1}{p^{s+1}}\log\frac{L}{p^{s+1}}+\frac{1}{L}+\frac{1}{p^{s+1}}$$

for $0\leqslant s\leqslant R-1$ and

$$\sum_{r=1;\ (r,m)=p^s}^{L}\left(\frac{1}{r}-\frac{1}{L}\right)\leqslant \frac{1}{p^s}\log\frac{L}{p^s}+\frac{1}{L}\quad\text{for}\quad s=R.$$

Using these inequalities, we have

$$\begin{aligned}
&\sum_{s=0}^{R}p^{-s/2}\sum_{r=1;\ (r,m)=p^s}^{L}\left(\frac{1}{r}-\frac{1}{L}\right)\\
&\quad\leqslant\sum_{s=0}^{R-1}p^{-3s/2}\left(\log\frac{L}{p^s}-\frac{1}{p}\log\frac{L}{p^{s+1}}+\frac{p^s}{L}+\frac{1}{p}\right)\\
&\qquad+p^{-R/2}\left(\frac{1}{p^R}\log\frac{L}{p^R}+\frac{1}{L}\right)\\
&\quad\leqslant\sum_{s=0}^{R-1}p^{-3s/2}\left(\frac{p-1}{p}\log L-s\log p+\frac{s+1}{p}\log p+\frac{p^s}{L}+\frac{1}{p}\right)\\
&\qquad+p^{-R/2}\left(\frac{\log p}{p^R}+\frac{1}{L}\right)\\
&\quad=\left(\frac{p-1}{p}\log L+\frac{1}{p}\right)\sum_{s=0}^{R-1}p^{-3s/2}+\frac{1}{L}\sum_{s=0}^{R}p^{-s/2}\\
&\qquad+(\log p)\sum_{s=0}^{R-1}\left(\frac{s+1}{p}-s\right)p^{-3s/2}+\frac{\log p}{p^{3R/2}}\\
&\quad\leqslant\left(\frac{p-1}{p}\log L+\frac{1}{p}\right)\left(\frac{p^{3/2}}{p^{3/2}-1}-\frac{p^{3/2}}{(p^{3/2}-1)p^{3R/2}}\right)+\frac{1}{L}\cdot\frac{p^{1/2}}{p^{1/2}-1}\\
&\qquad+\frac{\log p}{p}+\frac{\log p}{p^{3R/2}}\\
&\quad\leqslant\frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}\log L+\frac{1}{L}\cdot\frac{p^{1/2}}{p^{1/2}-1}+\frac{p^{1/2}}{p^{3/2}-1}+\frac{\log p}{p}\\
&\qquad+p^{-3R/2}\left(\log p-\frac{p-1}{p}\log L\right)
\end{aligned}$$

Since $L \geqslant p^2$, we get therefore

$$\sum_{s=0}^{R} p^{-s/2} \sum_{r=1;\ (r,m)=p^s}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \leqslant \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \log L$$

$$+ \frac{1}{L} \cdot \frac{p^{1/2}}{p^{1/2} - 1} + \frac{p^{1/2}}{p^{3/2} - 1} + \frac{\log p}{p} \tag{11}$$

Using (8), (11), the special form of L, and $[t] \geqslant (p^2/(p^2+1))t$ for $t \geqslant p^2$, we arrive at

$$D_N \leqslant \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \left| \log \frac{(p^{3/2} - 1)\pi N}{(p^{3/2} - p^{1/2})\sqrt{m}(1 + \log \tau)} \right|$$

$$+ \left(\frac{(p^2 + 1)(p^{3/2} - p^{1/2})}{p^2(p^{3/2} - 1)} + \frac{p^{1/2}}{p^{3/2} - 1} + \frac{\log p}{p} \right) \frac{4\sqrt{m}(1 + \log \tau)}{\pi N}$$

$$+ \frac{(p^2 + 1)(p^{3/2} - p^{1/2})p^{1/2}}{p^2(p^{3/2} - 1)(p^{1/2} - 1)} \cdot \frac{4m(1 + \log \tau)^2}{\pi^2 N^2}.$$

Now

$$\frac{(p^2 + 1)(p^{3/2} - p^{1/2})}{p^2(p^{3/2} - 1)} + \frac{p^{1/2}}{p^{3/2} - 1} + \frac{\log p}{p} = \frac{p^3 + p - 1}{p^3 - p^{3/2}} + \frac{\log p}{p} \leqslant 2 + \log p$$

and

$$\frac{(p^2 + 1)(p^{3/2} - p^{1/2})p^{1/2}}{p^2(p^{3/2} - 1)(p^{1/2} - 1)} = \frac{(p^2 + 1)(p^{1/2} + 1)}{p(p^{3/2} - 1)}$$

$$= 1 + \frac{p^2 + p + p^{1/2} + 1}{p^{5/2} - p} \leqslant 1 + \frac{4}{p^{1/2}}.$$

This concludes the proof of the theorem.

A condition which implies (3), and which is easier to check, is the following one:

$$p^\beta \leqslant (0.24)m^{1/2}(1 + \log \tau). \tag{12}$$

For if (12) holds, then

$$p^\beta \leqslant (0.24)m^{1/2}(1 + \log \tau) < \frac{\sqrt{2}}{2\sqrt{2} - 1} \cdot \frac{m^{1/2}(1 + \log \tau)}{\pi}$$

$$\leqslant \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{m^{3/2}(1 + \log \tau)}{\pi m},$$

since the function $f(t) = (t^{3/2} - t^{1/2})/(t^{3/2} - 1)$ is increasing for $t \geqslant 2$. But $m > \tau \geqslant N$ implies then (3). In practical cases, m and τ are large, so that (12) can be satisfied by choosing a λ with $\beta \leqslant \alpha/2$. We remark also that if β is large, then τ is rather small, since the two numbers are related by the identity $\tau = \tau(p^\alpha) = p^{\alpha-\beta}\tau(p^\beta) = p^{\alpha-\beta}\tau(p)$ (see [1, Lemma 1]).

If (3) does not hold, then D_N can still be estimated, although in a weaker form only.

THEOREM 3. *Let the conditions of Theorem 2 hold, with* (3) *being replaced by*

$$p^\beta \geqslant \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{m^{3/2}(1 + \log \tau)}{\pi N} \tag{13}$$

Then the discrepancy D_N *of the points* $x_0, x_1, \cdots, x_{N-1}$ *satisfies the inequality*

$$D_N \leqslant \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \log \frac{(\pi + 1)m}{p^\beta} + \left(\frac{p^{3/2}(m + p^\beta)}{(p^{3/2} - 1)m} + \frac{\log p}{p}\right) \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} + \left(1 + \log(\pi + 1) + \frac{p^\beta}{m}\right) \frac{4p^\beta}{m}$$

Proof. We start from (5) and choose

$$L = \left[\frac{(p^{3/2} - 1)(\pi + 1)mN}{(p^{3/2} - p^{1/2})m^{3/2}(1 + \log \tau) + (p^{3/2} - 1)p^\beta N}\right]$$

Condition (13) implies that

$$(p^{3/2} - 1)(\pi + 1)mN \geqslant (p^{3/2} - p^{1/2})m^{3/2}p^{\alpha-\beta}(1 + \log \tau) + (p^{3/2} - 1)mN,$$

and so $L \geqslant p^{\alpha-\beta}$. Using (6) and (7), we have

$$D_N \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \sum_{s=0}^{\alpha-\beta-1} p^{-s/2} \sum_{r=1;\,(r,m)=p^s}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \left|\frac{1}{N} \sum_{n=0}^{N-1} e(ry_0\lambda^n/m)\right| + \frac{4}{\pi} \sum_{r=1;\,p^{\alpha-\beta}\mid r}^{L} \left(\frac{1}{r} - \frac{1}{L}\right) \left|\frac{1}{N} \sum_{n=0}^{N-1} e(ry_0\lambda^n/m)\right|$$

With (10) and the trivial estimate

$$\left|\frac{1}{N} \sum_{n=0}^{N-1} e(ry_0\lambda^n/m)\right| \leqslant 1$$

we get

$$D_N \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1+\log\tau)}{\pi N} \sum_{s=0}^{\alpha-\beta-1} p^{-s/2}\left(\frac{1}{p^s}\log\frac{L}{p^s} - \frac{1}{p^{s+1}}\log\frac{L}{p^{s+1}} + \frac{1}{L} + \frac{1}{p^{s+1}}\right)$$
$$+ \frac{4}{\pi} \sum_{r=1;p^{\alpha-\beta}\mid r}^{L} \left(\frac{1}{r} - \frac{1}{L}\right)$$

Now

$$\sum_{s=0}^{\alpha-\beta-1} p^{-s/2}\left(\frac{1}{p^s}\log\frac{L}{p^s} - \frac{1}{p^{s+1}}\log\frac{L}{p^{s+1}} + \frac{1}{L} + \frac{1}{p^{s+1}}\right)$$
$$= \left(\frac{p-1}{p}\log L + \frac{1}{p}\right)\sum_{s=0}^{\alpha-\beta-1} p^{-3s/2}$$
$$+ \frac{1}{L}\sum_{s=0}^{\alpha-\beta-1} p^{-s/2} + (\log p)\sum_{s=0}^{\alpha-\beta-1}\left(\frac{s+1}{p} - s\right)p^{-3s/2} \leqslant \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}\log L$$
$$+ \frac{1}{L}\cdot\frac{p^{1/2}}{p^{1/2}-1} + \frac{p^{1/2}}{p^{3/2}-1} + \frac{\log p}{p}$$

and

$$\sum_{r=1;p^{\alpha-\beta}\mid r}^{L}\left(\frac{1}{r} - \frac{1}{L}\right) = \frac{1}{p^{\alpha-\beta}}\sum_{r=1}^{[L/p^{\alpha-\beta}]}\frac{1}{r} - \frac{1}{L}\left[\frac{L}{p^{\alpha-\beta}}\right]$$
$$\leqslant \frac{1}{p^{\alpha-\beta}}\cdot\left(1 + \log\left[\frac{L}{p^{\alpha-\beta}}\right]\right) - \frac{1}{L}\left[\frac{L}{p^{\alpha-\beta}}\right]$$
$$\leqslant \frac{1}{p^{\alpha-\beta}}\log\frac{L}{p^{\alpha-\beta}} + \frac{1}{L} = \frac{p^\beta}{m}\log L + \frac{1}{L} - \frac{p^\beta}{m}\log\frac{m}{p^\beta},$$

so that

$$D_N \leqslant 4\left(\frac{(p^{3/2}-p^{1/2})\sqrt{m}(1+\log\tau)}{(p^{3/2}-1)\pi N} + \frac{p^\beta}{\pi m}\right)\log L + \frac{4}{L}\left(1 + \frac{1}{\pi}\right)$$
$$+ \left(\frac{p^{1/2}}{p^{3/2}-1} + \frac{\log p}{p}\right)\frac{4\sqrt{m}(1+\log\tau)}{\pi N} - \frac{4p^\beta}{\pi m}\log\frac{m}{p^\beta}.$$

From the special form of L it is easily seen that $L \leqslant (\pi+1)p^{\alpha-\beta}$. Therefore

$$D_N \leqslant \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1} \cdot \frac{4\sqrt{m}(1+\log \tau)}{\pi N} \log \frac{(\pi+1)m}{p^{\beta}} + \frac{4}{L}\left(1+\frac{1}{\pi}\right)$$

$$+\left(\frac{p^{1/2}}{p^{3/2}-1}+\frac{\log p}{p}\right)\frac{4\sqrt{m}(1+\log \tau)}{\pi N} + \frac{4p^{\beta}}{\pi m} \log (\pi+1).$$

Using again the special form of L, as well as $L \geqslant p^{\alpha-\beta}$ and $[t] \geqslant (p^{\alpha-\beta}/(p^{\alpha-\beta}+1))t$ for $t \geqslant p^{\alpha-\beta}$, we obtain

$$D_N \leqslant \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1} \cdot \frac{4\sqrt{m}(1+\log \tau)}{\pi N} \log \frac{(\pi+1)m}{p^{\beta}}$$

$$+\left(\frac{(p^{\alpha-\beta}+1)(p^{3/2}-p^{1/2})}{p^{\alpha-\beta}(p^{3/2}-1)}+\frac{p^{1/2}}{p^{3/2}-1}+\frac{\log p}{p}\right)\frac{4\sqrt{m}(1+\log \tau)}{\pi N}$$

$$+\left(\frac{p^{\alpha-\beta}+1}{p^{\beta}}+\log (\pi+1)\right)\frac{4p^{\beta}}{\pi m},$$

and the proof of the theorem is complete.

In the remaining case, namely when $\beta \geqslant \alpha$, the sequence $x_0, x_1, \cdots, x_{N-1}$ shows a bad distribution behavior. For then we have $\tau = \tau(m) = \tau(p) \leqslant p-1$; also, as for any N points in $[0, 1)$, we have $D_N \geqslant 1/N$ (see [3, Chapter 2]), and so $D_N \geqslant 1/(p-1)$ for $1 \leqslant N \leqslant \tau$. Another negative result in this case can be derived as follows. Let $m = p^2$ with an odd prime p, let g be a primitive root modulo p^2, and set $\lambda = g^p$. Then we have of course $\tau = \tau(m) = \tau(p) = p-1$ and $\beta = \alpha$. As N. M. Korobov [1, p. 643] has shown, there exists a y_0 relatively prime to m such that

$$\left|\sum_{n=0}^{\tau-1} e(x_n)\right| = \left|\sum_{n=0}^{\tau-1} e(y_0\lambda^n/m)\right| \geqslant \sqrt{p-1},$$

and so

$$\left|\frac{1}{\tau}\sum_{n=0}^{\tau-1} e(x_n)\right| \geqslant p^{-1/2} = m^{-1/4}.$$

As for any τ points in $[0, 1)$, we have

$$\left|\frac{1}{\tau}\sum_{n=0}^{\tau-1} e(x_n)\right| \leqslant 4\,D_{\tau}$$

by [3, Chapter 2], and so $D_\tau \geqslant \frac{1}{4} m^{-1/4}$.

5. General Modulus. Let $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the canonical factorization of m and suppose that $s \geqslant 2$. Let λ be relatively prime to m with $|\lambda| > 1$. Otherwise, the notation from the introduction remains operative. For $m_0 = p_1 \cdots p_s$, let $\tau(m_0)$ be the exponent to which λ belongs modulo m_0. We set $\mu = 2$ if $m \equiv 0 \pmod 2$, $\tau(m_0) \equiv 1 \pmod 2$, and $\lambda \equiv 3 \pmod 4$, and $\mu = 1$ otherwise. Let

$$\lambda^{\mu\tau(m_0)} - 1 = u_0 p_1^{\beta_1} \cdots p_s^{\beta_s} \quad \text{with } (u_0, m_0) = 1. \tag{14}$$

Then we have the following result.

THEOREM 4. *Let $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the canonical factorization of m and suppose $s \geqslant 2$. Let λ be relatively prime to m with $|\lambda| > 1$ and $\alpha_\nu > \beta_\nu$ for $1 \leqslant \nu \leqslant s$, where the β_ν are defined according to* (14). *Then, if $1 \leqslant N \leqslant \tau$ and*

$$p_1^{\beta_1} \cdots p_s^{\beta_s} < \frac{m^{3/2}(1 + \log \tau)}{\pi N}, \tag{15}$$

the discrepancy D_N of the points $x_0, x_1, \cdots, x_{N-1}$ satisfies

$$D_N \leqslant \frac{4\sqrt{m}(1 + \log \tau)}{\pi N} \left| \log \frac{\pi N}{\sqrt{m}(1 + \log \tau)} \right| + \frac{5\sqrt{m}(1 + \log \tau)}{\pi N}.$$

Proof. We use (5) with $L = [\pi N/\sqrt{m}(1 + \log \tau)]$. For the same reason as in the proof of Theorem 1, the theorem is trivial if $L < 5$. Thus $L \geqslant 5$ from now on. Furthermore, condition (15) implies that $L < p_1^{\alpha_1 - \beta_1} \cdots p_s^{\alpha_s - \beta_s}$. In order to estimate

$$\left| \frac{1}{N} \sum_{n=0}^{N-1} e(r y_0 \lambda^n / m) \right|$$

for $1 \leqslant r \leqslant L$, we use Lemma 2 in case $(r, m) = 1$. Now consider $(r, m) > 1$. Since $r < p_1^{\alpha_1 - \beta_1} \cdots p_s^{\alpha_s - \beta_s}$, it follows that there exists ν, $1 \leqslant \nu \leqslant s$, such that $p_\nu^{\alpha_\nu - \beta_\nu}$ does not divide r. Then by a result of N. M. Korobov [1, Theorem 2] we have

$$\sum_{n=0}^{\tau-1} e(r y_0 \lambda^n / m) = 0,$$

so that Lemma 3 is applicable. Altogether, we have then

$$\left| \frac{1}{N} \sum_{n=0}^{N-1} e(r y_0 \lambda^n / m) \right| \leqslant \frac{\sqrt{m}(1 + \log \tau)}{N} \quad \text{for } 1 \leqslant r \leqslant L, \tag{16}$$

and thus

$$D_N \leqslant \frac{4}{L} + \frac{4\sqrt{m}(1+\log \tau)}{\pi N} \sum_{r=1}^{L} \left(\frac{1}{r} - \frac{1}{L}\right).$$

The proof is then concluded in the same way as in Theorem 1.

Replacing (16) by the sharper estimate

$$\left| \frac{1}{N} \sum_{n=0}^{N-1} e(ry_0\lambda^n/m) \right| \leqslant \sqrt{\frac{m}{d}} \cdot \frac{1+\log \tau}{N}$$

would, in this case, only result in an insignificant improvement of the upper bound for D_N. If condition (15) is not satisfied, one proceeds as in Theorem 3 to obtain an estimate for D_N. Since in most practical applications of the linear congruential method one works with a prime power modulus, the discussion of this exceptional case is not of sufficient interest to be carried out in detail for the general modulus m.

6. Application to Numerical Integration. The discrepancy estimates established in the preceding sections imply error estimates for numerical integrations performed by a quasi-Monte Carlo method with nodes $x_0, x_1, \cdots, x_{N-1}$. For a general discussion of the relation between the theory of discrepancy and numerical integration, see [3, Chapter 2], [6], and [9].

Suppose $x_0, x_1, \cdots, x_{N-1}$ is a sequence of pseudo-random numbers generated by the linear congruential method with $1 \leqslant N \leqslant \tau$, and let K be an upper bound for the discrepancy D_N of the sequence. By an inequality of Koksma mentioned in [7], we arrive at the following result: for any function f with bounded variation $V(f)$ on [0, 1] we have

$$\left| \frac{1}{N} \sum_{n=0}^{N-1} f(x_n) - \int_0^1 f(t)dt \right| \leqslant V(f)K. \tag{17}$$

For a continuous integrand f which is not of bounded variation, we may employ an inequality due to the author which is based on [8, Theorem 1] and shown in [6], [7]. We obtain then the following estimate: if f is continuous on [0, 1] with modulus of continuity

$$\omega(h) = \sup_{u,v\in[0,1];|u-v|\leqslant h} |f(u) - f(v)| \quad \text{for } h \geqslant 0,$$

then

$$\left| \frac{1}{N} \sum_{n=0}^{N-1} f(x_n) - \int_0^1 f(t)dt \right| \leqslant \omega(K). \tag{18}$$

Using the upper bounds K from the theorems of the present paper in (17) and (18), we arrive at nontrivial error estimates for the considered type of numerical integration problem.

Added in Proof. In my forthcoming paper "Some new exponential sums with applications to pseudo-random numbers," *Colloquium on Number Theory* (Debrecen, 1974), North-Holland Publishing Co., Amsterdam, it will be shown that the estimates in Theorems 1 and 2 are best possible apart from the logarithmic factors. The methods of that paper also allow the treatment of pseudo-random numbers generated by inhomogeneous linear congruences.

School of Mathematics
Institute for Advanced Study
Princeton, New Jersey 08540

1. N. M. KOROBOV, "Trigonometric sums with exponential functions and the distribution of signs in repeating decimals," *Mat. Zametki,* v. 8, 1970, pp. 641–652, = *Math. Notes*, v. 8, 1970, pp. 831–837. MR 43 #6165.

2. N. M. KOROBOV, "On the distribution of digits in periodic fractions," *Mat. Sb.*, v. 89 (131), 1972, pp. 654–670 = *Math. USSR Sb.*, v. 18, 1972, pp. 659–676.

3. L. KUIPERS & H. NIEDERREITER, *Uniform Distribution of Sequences,* Wiley, New York, 1974.

4. L. J. MORDELL, "On the exponential sum $\Sigma_{x=1}^{X} \exp(2\pi i(ax + bg^x)/h)$," *Mathematika,* v. 19, 1972, pp. 84–87.

5. L. J. MORDELL, "A new type of exponential series," *Quart. J. Math.* (2), v. 23, 1972, pp. 373–374.

6. H. NIEDERREITER, "Methods for estimating discrepancy," *Applications of Number Theory to Numerical Analysis* (edited by S. K. Zaremba), Academic Press, New York, 1972, pp. 203–236.

7. H. NIEDERREITER, "On the distribution of pseudo-random numbers generated by the linear congruential method," *Math. Comp.*, v. 26, 1972, pp. 793–795.

8. H. NIEDERREITER, "Discrepancy and convex programming," *Ann. Mat. Pura Appl.* (4), v. 93, 1972, pp. 89–97.

9. H. NIEDERREITER, "Application of diophantine approximations to numerical integration," *Diophantine Approximation and Its Applications* (edited by C. F. Osgood), Academic Press, New York, 1973, pp. 129–199.

10. H. NIEDERREITER & W. PHILIPP, "Berry-Esseen bounds and a theorem of Erdös and Turán on uniform distribution mod 1," *Duke Math. J.,* v. 40, 1973, pp. 633–649.

11. R. G. STONEHAM, "On the uniform ϵ-distribution of residues within the periods of rational fractions with applications to normal numbers," *Acta Arith.*, v. 22, 1973, pp. 371–389.