MATHEMATICS OF COMPUTATION, VOLUME 30, NUMBER 135
JULY 1976, PAGES 571–597

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

By Harald Niederreiter*

Abstract. The discrepancy of a sequence of pseudo-random numbers generated by the linear congruential method, both homogeneous and inhomogeneous, is estimated for parts of the period that are somewhat larger than the square root of the modulus. The analogous problem for an arbitrary linear congruential generator modulo a prime is also considered, the result being particularly interesting for maximal period sequences. It is shown that the discrepancy estimates in this paper are best possible apart from logarithmic factors.

1. **Introduction.** Let $m \geqslant 2$ and r be integers, let y_0 be an integer in the least residue system modulo m, and let λ be an integer relatively prime to m. We generate a sequence $y_0, y_1, \ldots$ of integers in the least residue system modulo m by the recursion $y_{n+1} \equiv \lambda y_n + r \pmod{m}$ for $n = 0, 1, \ldots$. The sequence $x_0, x_1, \ldots$, defined by $x_n = y_n/m$ for $n = 0, 1, \ldots$, is then a frequently employed sequence of pseudo-random numbers in the unit interval $[0, 1]$ and is said to be generated by the linear congruential method. In the discussion of this method, one usually distinguishes two cases: the homogeneous case $r \equiv 0 \pmod{m}$ and the inhomogeneous case $r \not\equiv 0 \pmod{m}$. In both cases, the sequence $y_0, y_1, \ldots$ is eventually periodic. From the observation that the predecessor of each y_n is uniquely determined because of the relative primality of λ and m, it follows that the sequence $y_0, y_1, \ldots$ is, in fact, purely periodic. We denote the length of the period by τ. Then the sequence $x_0, x_1, \ldots$ is purely periodic with period τ.

In the first paper [7] of this series, the author has studied the distribution in $[0, 1]$ of the full period $x_0, x_1, \ldots, x_{\tau-1}$ in the homogeneous case, under the assumption that λ is a primitive root modulo m and y_0 is relatively prime to m (see [6] for a slight improvement of the result). It turns out that the empirical distribution of the points of 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. Therefore, in the second part [8] of this series, the distribution of the points $x_0, x_1, \ldots, x_{N-1}$ with $1 \leqslant N \leqslant \tau$ in the interval $[0, 1]$ was considered. The requirement that λ be a primitive root modulo m was abandoned, but the discussion was still confined to the homogeneous case. Satisfactory results were obtained for values

Received November 8, 1974.

AMS (MOS) subject classifications (1970). Primary 10F40, 10K05, 65C10; Secondary 10A35, 10G05, 12C10, 12C25, 65C05, 65D30, 68A55.

Key words and phrases. Pseudo-random numbers, discrepancy, equidistribution test, trigonometric sums, linear recurring sequences, maximal period sequences.

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

of N somewhat larger than the square root of the modulus m. One of the objectives of the present paper is the extension of these results to the inhomogeneous case.

For sufficiently large N, one will expect the empirical distribution of the points $x_0, x_1, \ldots, x_{N-1}$ to be close to the uniform distribution in $[0, 1]$, at least for well-chosen random number generators. The deviation between the two distribution functions is measured by the so-called discrepancy. For real numbers α_1 and α_2 with $0 \leqslant \alpha_1 < \alpha_2 \leqslant 1$, let $A(\alpha_1, \alpha_2; N)$ be the number of n, $0 \leqslant n \leqslant N-1$, with $x_n \in [\alpha_1, \alpha_2)$. Then we define the discrepancy D_N of the points $x_0, x_1, \ldots, x_{N-1}$ by

$$D_N = D_N(x_0, \ldots, x_{N-1}) = \sup_{0 \leqslant \alpha_1 < \alpha_2 \leqslant 1} |A(\alpha_1, \alpha_2; N)/N - (\alpha_2 - \alpha_1)|.$$

For the general theory of discrepancy, see the book of L. Kuipers and the author [4, Chapter 2].

We shall estimate the discrepancy of $x_0, x_1, \ldots, x_{N-1}$ for $1 \leqslant N \leqslant \tau$, in both the homogeneous and the inhomogeneous case. We concentrate on the important classes of moduli, namely, primes and prime powers. For results on general moduli in the homogeneous case, see [8, Section 5]. It should be clear how to use the methods of the present paper in order to obtain slight improvements of these results as well as extensions to the inhomogeneous case. The main tools of our investigation are an inequality of the author and W. Philipp [12] and estimates of character sums involving linear recurring sequences that were established in [10]. Incidentally, these estimates are also of importance in the study of the cycle structure of linear recurring sequences in finite fields (see [11]). The possibility of obtaining the results of the present paper by means of the estimates in [10] was already announced in [9].

A brief survey of the contents of the paper follows. In Section 2, we take up the homogeneous case. This has already been dealt with in [8], but we shall show how to refine the methods of that paper in order to get various improvements. However, the resulting estimates are again only of interest when N is at least of the order of magnitude $m^{1/2+\epsilon}$ for some $\epsilon > 0$. In Section 3, the inhomogeneous case is treated on the basis of the estimates in [10]. Essentially, the remark concerning the order of magnitude of N is also valid in this case, although the situation is a bit more complicated because of the appearance of one more parameter. Since they can be treated by similar methods, we study pseudo-random numbers generated by higher-order linear recurrences in Section 4. The most interesting pseudo-random numbers of this type are based on maximal period sequences in finite fields, and their use was suggested by R. C. Tausworthe [13] and D. E. Knuth [3, p. 27], among others. In the last section, we show that the estimates of this paper are best possible apart from logarithmic factors.

It should be pointed out that the subsequent discrepancy estimates imply error estimates for quasi-Monte Carlo integrations using the points $x_0, x_1, \ldots, x_{N-1}$ as nodes (compare with [8, Section 6]). We remark also that the methods of this paper can be used to obtain results concerning the serial test for pseudo-random numbers generated by the linear congruential method. The author intends to treat this subject on another occasion.

2. The Homogeneous Case. We consider the sequence $y_0, y_1, \ldots$ of integers described in the introduction, generated by the recursion $y_{n+1} \equiv \lambda y_n \pmod{m}$ for $n = 0, 1, \ldots$. It is customary to assume in the homogeneous case that y_0 be relatively prime to m, and we shall do so in the sequel. Then the period τ of the sequence $y_0, y_1, \ldots$ is equal to the exponent to which λ belongs modulo m. The corresponding sequence $x_0, x_1, \ldots$ of pseudo-random numbers in the unit interval $[0, 1]$ may also be described explicitly by $x_n = \{\lambda^n y_0/m\}$ for $n = 0, 1, \ldots$, where $\{t\}$ denotes the fractional part of the real number t. The discrepancy of $x_0, x_1, \ldots, x_{N-1}$ with $1 \leqslant N \leqslant \tau$ was already estimated in [8]. We shall present various improvements in this section.

We first discuss the case that m is a prime. Some auxiliary results on trigonometric sums are needed. They ameliorate corresponding lemmas in [8]. Throughout this paper, we write $e(t) = e^{2\pi i t}$ for real t.

LEMMA 1. *Let m be a prime, let b and λ be integers not divisible by m, and suppose λ belongs to the exponent τ modulo m. Then,*

$$\left| \sum_{n=0}^{\tau-1} e(b\lambda^n/m)e(cn/\tau) \right| \leqslant (m-\tau)^{1/2} \tag{1}$$

for every integer c divisible by τ, and

$$\left| \sum_{n=0}^{\tau-1} e(b\lambda^n/m)e(cn/\tau) \right| \leqslant m^{1/2} \tag{2}$$

for every integer c not divisible by τ.

Proof. For integers a and c, write

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

The general term of this sum, considered as a function of n, is periodic with period τ. Therefore, for any integer y, we have

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

and so,

$$|\sigma(a, c)| = \left| \sum_{n=0}^{\tau-1} e(a\lambda^y\lambda^n/m)e(cn/\tau) \right| = |\sigma(a\lambda^y, c)|. \tag{3}$$

Since the integers $b\lambda, b\lambda^2, \ldots, b\lambda^\tau$ are pairwise incongruent modulo m and not divisible by m, it follows from (3) that

$$\begin{aligned} \tau|\sigma(b, c)|^2 &= \sum_{y=1}^{\tau} |\sigma(b\lambda^y, c)|^2 \leqslant \sum_{a=1}^{m-1} |\sigma(a, c)|^2 = \sum_{a=0}^{m-1} |\sigma(a, c)|^2 - |\sigma(0, c)|^2 \\ &= \sum_{h,j=0}^{\tau-1} e(c(h-j)/\tau) \sum_{a=0}^{m-1} e(a(\lambda^h - \lambda^j)/m) - |\sigma(0, c)|^2 \\ &= m\tau - |\sigma(0, c)|^2. \end{aligned}$$

The inequalities (1) and (2) are immediate consequences.

LEMMA 2. *For any positive integers A and B, we have*

$$\sum_{c=1}^{A-1}\left|\sum_{y=0}^{B-1} e(cy/A)\right| < \frac{2}{\pi}A\log A + \frac{2}{5}A. \tag{4}$$

Proof. The lemma is trivial for $A = 1$. For $A \geqslant 2$, we have

$$\left|\sum_{y=0}^{B-1} e(cy/A)\right| = \frac{|e(cB/A)-1|}{|e(c/A)-1|} = \frac{\sin \pi\|cB/A\|}{\sin \pi\|c/A\|} \quad \text{for } 1 \leqslant c \leqslant A-1,$$

where $\|t\|$ denotes the absolute distance from the real number t to the nearest integer. If S stands for the expression on the left-hand side of (4), then

$$\begin{aligned} S = \sum_{c=1}^{A-1}\frac{\sin \pi\|cB/A\|}{\sin \pi\|c/A\|} &\leqslant \sum_{c=1}^{A-1}(\sin \pi\|c/A\|)^{-1} \\ &\leqslant 2\sum_{c=1}^{[A/2]}(\sin(\pi c/A))^{-1}. \end{aligned}$$

Now, by the usual method of comparing sums with integrals, we obtain

$$\begin{aligned} \sum_{c=1}^{[A/2]}(\sin(\pi c/A))^{-1} &= (\sin(\pi/A))^{-1} + \sum_{c=2}^{[A/2]}(\sin(\pi c/A))^{-1} \\ &\leqslant (\sin(\pi/A))^{-1} + \int_1^{[A/2]}\frac{dx}{\sin(\pi x/A)} \\ &\leqslant (\sin(\pi/A))^{-1} + \frac{A}{\pi}\int_{\pi/A}^{\pi/2}\frac{dt}{\sin t} \\ &= (\sin(\pi/A))^{-1} + \frac{A}{\pi}\log\cot\frac{\pi}{2A} \leqslant (\sin(\pi/A))^{-1} + \frac{A}{\pi}\log\frac{2A}{\pi}. \end{aligned}$$

Now, for $A \geqslant 6$ we have $(\pi/A)^{-1}\sin(\pi/A) \geqslant (\pi/6)^{-1}\sin(\pi/6)$, hence $\sin(\pi/A) \geqslant 3/A$. This implies

$$\sum_{c=1}^{[A/2]}(\sin(\pi c/A))^{-1} \leqslant \frac{A}{\pi}\log A + \left(\frac{1}{3} - \frac{1}{\pi}\log\frac{\pi}{2}\right)A \quad \text{for } A \geqslant 6;$$

and so,

$$\sum_{c=1}^{[A/2]}(\sin(\pi c/A))^{-1} < \frac{A}{\pi}\log A + \frac{1}{5}A \quad \text{for } A \geqslant 6. \tag{5}$$

The inequality (5) is easily checked for $A = 3$, 4, and 5, so that (4) holds for $A \geqslant 3$. For $A = 2$, the inequality (4) is shown by inspection.

LEMMA 3. *Suppose the conditions of Lemma* 1 *are satisfied. Then,*

$$\left|\sum_{n=0}^{N-1} e(b\lambda^n/m)\right| < m^{1/2}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{N}{\tau}(m-\tau)^{1/2} \quad \text{for } 1 \leqslant N \leqslant \tau.$$

Proof. We note that

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

for $1 \leqslant N \leqslant \tau$. Thus, by Lemmas 1 and 2,

$$\begin{aligned}\left|\sum_{n=0}^{N-1} e(b\lambda^n/m)\right| &\leqslant \frac{1}{\tau}\sum_{c=1}^{\tau}\left|\sum_{y=0}^{N-1} e(-cy/\tau)\right|\;\left|\sum_{n=0}^{\tau-1} e(b\lambda^n/m)e(cn/\tau)\right| \\ &\leqslant \frac{1}{\tau}m^{1/2}\sum_{c=1}^{\tau-1}\left|\sum_{y=0}^{N-1} e(-cy/\tau)\right| + \frac{N}{\tau}(m-\tau)^{1/2} \\ &< m^{1/2}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{N}{\tau}(m-\tau)^{1/2}.\end{aligned}$$

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

$$D_N < X\log(1 + 4/X) + X, \tag{6}$$

where

$$X = \frac{4m^{1/2}}{\pi N}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{4(m-\tau)^{1/2}}{\pi\tau}.$$

Proof. For $\tau = 1$ or 2, one sees easily that $X > 1$, so that (6) is trivial in this case. Thus $\tau \geqslant 3$ from now on. This implies, in particular, that $m \geqslant 5$. We use an inequality of the author and W. Philipp [12, Corollary of Theorem 1′]: for any points $t_0, \ldots, t_{N-1}$ in $[0, 1)$ with discrepancy $D_N(t_0, \ldots, t_{N-1})$ we have

$$D_N(t_0, \ldots, t_{N-1}) \leqslant \frac{4}{L} + \frac{4}{\pi}\sum_{b=1}^{L}\left(\frac{1}{b} - \frac{1}{L}\right)\left|\frac{1}{N}\sum_{n=0}^{N-1} e(bt_n)\right| \tag{7}$$

for all positive integers L. For the given points $x_0, x_1, \ldots, x_{N-1}$, we choose $L = [4/X] + 1$. We note that

$$m^{1/2}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + (m-\tau)^{1/2} \geqslant \sqrt{5}\left(\frac{2}{\pi}\log 3 + \frac{2}{5}\right) + 1 > \pi > \frac{\pi\tau}{m},$$

so that

$$\begin{aligned}\frac{X}{4} &= \frac{m^{1/2}}{\pi N}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{(m-\tau)^{1/2}}{\pi\tau} \\ &\geqslant \frac{m^{1/2}}{\pi\tau}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{(m-\tau)^{1/2}}{\pi\tau} > \frac{1}{m}.\end{aligned}$$

This is equivalent to $L \leqslant m$. From (7) we get

$$D_N \leqslant \frac{4}{L} + \frac{4}{\pi} \sum_{b=1}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) \left| \frac{1}{N} \sum_{n=0}^{N-1} e(by_0 \lambda^n/m) \right|.$$

For $1 \leqslant b \leqslant L - 1$, we have g.c.d.$(by_0, m) = 1$, so that we may use Lemma 3. For $b = L$, the coefficient of the trigonometric sum is zero, so that formally we may also use the upper bound in Lemma 3. We obtain

$$\begin{aligned} D_N &\leqslant \frac{4}{L} + \frac{4}{\pi N}\left(m^{1/2}\left(\frac{2}{\pi} \log \tau + \frac{2}{5}\right) + \frac{N}{\tau}(m - \tau)^{1/2}\right) \sum_{b=1}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) \\ &\leqslant \frac{4}{L} + X \log L < X + X \log\left(1 + \frac{4}{X}\right), \end{aligned}$$

and the proof of the theorem is complete.

In the case of m being a prime, there is an alternative way of estimating D_N that may sometimes yield an even better estimate than (6). This approach is based on the following general lemma that may be thought of as a crude version of the inequality (7).

LEMMA 4. *Let $m \geqslant 2$ be an integer, and let $z_0, z_1, \ldots, z_{N-1}$ be integers in the least residue system modulo m. Suppose that $|\sum_{n=0}^{N-1} e(hz_n/m)| \leqslant Y$ for $h = 1, 2, \ldots, m - 1$. Then the discrepancy of the points $z_0/m, z_1/m, \ldots, z_{N-1}/m$ satisfies*

$$D_N\left(\frac{z_0}{m}, \ldots, \frac{z_{N-1}}{m}\right) \leqslant \frac{2}{m} + \frac{Y}{N}\left(\frac{2}{\pi} \log m + \frac{2}{5}\right). \tag{8}$$

Proof. For $0 \leqslant \alpha_1 < \alpha_2 \leqslant 1$, let $A(\alpha_1, \alpha_2; N)$ be the number of n, $0 \leqslant n \leqslant N - 1$, with $z_n/m \in [\alpha_1, \alpha_2)$. For $j = 0, 1, \ldots, m - 1$, let $A(j; N)$ be the number of n, $0 \leqslant n \leqslant N - 1$, with $z_n = j$. Then, if u, v are integers with $0 \leqslant u < v \leqslant m$, we can write

$$A\left(\frac{u}{m}, \frac{v}{m}; N\right) = \sum_{j=u}^{v-1} A(j; N) = \sum_{j=u}^{v-1} \sum_{n=0}^{N-1} c_j(z_n),$$

where c_j is the characteristic function of the singleton $\{j\}$. Now

$$c_j(z) = \frac{1}{m} \sum_{h=0}^{m-1} e(h(z - j)/m) \quad \text{for } z = 0, 1, \ldots, m - 1,$$

so that

$$\begin{aligned} A\left(\frac{u}{m}, \frac{v}{m}; N\right) &= \sum_{j=u}^{v-1} \sum_{n=0}^{N-1} \frac{1}{m} \sum_{h=0}^{m-1} e(h(z_n - j)/m) \\ &= \frac{1}{m} \sum_{h=0}^{m-1} \left(\sum_{j=u}^{v-1} e(-hj/m)\right)\left(\sum_{n=0}^{N-1} e(hz_n/m)\right) \end{aligned}$$

and

$$A\left(\frac{u}{m}, \frac{v}{m}; N\right) - \frac{N(v-u)}{m} = \frac{1}{m}\sum_{h=1}^{m-1}\left(\sum_{j=u}^{v-1} e(-hj/m)\right)\left(\sum_{n=0}^{N-1} e(hz_n/m)\right).$$

Using Lemma 2, we get

$$\left|A\left(\frac{u}{m}, \frac{v}{m}; N\right) - \frac{N(v-u)}{m}\right| \leqslant \frac{1}{m}\sum_{h=1}^{m-1}\left|\sum_{j=u}^{v-1} e(-hj/m)\right|\left|\sum_{n=0}^{N-1} e(hz_n/m)\right|$$

$$(9) \qquad \leqslant \frac{Y}{m}\sum_{h=1}^{m-1}\left|\sum_{j=u}^{v-1} e(-hj/m)\right| = \frac{Y}{m}\sum_{h=1}^{m-1}\left|\sum_{j=0}^{v-u-1} e(hj/m)\right|$$

$$\leqslant Y\left(\frac{2}{\pi}\log m + \frac{2}{5}\right).$$

Now let $J = [\alpha_1, \alpha_2)$ be an arbitrary subinterval of $[0, 1)$. Then there exist subintervals $J_1 = [\beta_1^{(1)}, \beta_2^{(1)})$ and $J_2 = [\beta_1^{(2)}, \beta_2^{(2)})$ of $[0, 1)$ such that $J_1 \subseteq J \subseteq J_2$, the endpoints of J_1 and J_2 are rationals with denominator m, and $|\nu(J_i) - \nu(J)| \leqslant 2/m$ for $i = 1, 2$, where ν denotes Lebesgue measure. Then,

$$A(\beta_1^{(1)}, \beta_2^{(1)}; N) - N\nu(J_1) + N(\nu(J_1) - \nu(J)) \leqslant A(\alpha_1, \alpha_2; N) - N\nu(J)$$
$$\leqslant A(\beta_1^{(2)}, \beta_2^{(2)}; N) - N\nu(J_2) + N(\nu(J_2) - \nu(J));$$

hence,

$$|A(\alpha_1, \alpha_2; N) - N(\alpha_2 - \alpha_1)| \leqslant \max_{i=1,2} |A(\beta_1^{(i)}, \beta_2^{(i)}; N) - N\nu(J_i)|$$
$$+ N\max_{i=1,2}|\nu(J_i) - \nu(J)| \leqslant Y\left(\frac{2}{\pi}\log m + \frac{2}{5}\right) + \frac{2N}{m}$$

by (9). Now (8) follows immediately.

THEOREM 2. *Let m be a prime. Then, for $1 \leqslant N \leqslant \tau$, the discrepancy D_N of the points $x_0, x_1, \ldots, x_{N-1}$ satisfies the inequality*

$$D_N \leqslant \frac{m^{1/2}}{N}\left(\frac{2}{\pi}\log m + \frac{2}{5}\right)\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{(m-\tau)^{1/2}}{\tau}\left(\frac{2}{\pi}\log m + \frac{2}{5}\right) + \frac{2}{m}.$$

Proof. For $h = 1, 2, \ldots, m - 1$, we have

$$\sum_{n=0}^{N-1} e(hy_n/m) = \sum_{n=0}^{N-1} e(hy_0\lambda^n/m).$$

Since g.c.d.$(hy_0, m) = 1$, Lemma 3 can be applied. The result follows then from Lemma 4 with

$$Y = m^{1/2}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{N}{\tau}(m-\tau)^{1/2}.$$

We consider now the case that m is a prime power, say $m = p^\alpha$ with $\alpha \geqslant 2$ and p a prime. If λ belongs to the exponent τ modulo m and to the exponent γ modulo $p^{\alpha-1}$, then $d = \tau/\gamma$ is an integer.

LEMMA 5. *Let $m = p^{\alpha}$, p prime, $\alpha \geqslant 2$. Let b and λ be integers relatively prime to m. Suppose λ belongs to the exponent τ modulo m and to the exponent γ modulo $p^{\alpha-1}$, and set $d = \tau/\gamma$. Then,*

$$\left|\sum_{n=0}^{\tau-1} e(b\lambda^n/m)e(cn/\tau)\right| \leqslant \left(\frac{p-d}{p-1}\varphi(m)\right)^{1/2} \tag{10}$$

for every integer c divisible by d, and

$$\left|\sum_{n=0}^{\tau-1} e(b\lambda^n/m)e(cn/\tau)\right| \leqslant m^{1/2} \tag{11}$$

for every integer c not divisible by d.

Proof. For integers a and c, write

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

By the same arguments as in the proof of Lemma 1, we obtain

$$\tau|\sigma(b, c)|^2 = \sum_{y=1}^{\tau} |\sigma(b\lambda^y, c)|^2 \leqslant \sum_{a=0}^{m-1}{}^{*}|\sigma(a, c)|^2, \tag{12}$$

where the asterisk signalizes that we only sum over those a with g.c.d.$(a, m) = 1$. Furthermore,

$$\sum_{a=0}^{m-1}{}^{*}|\sigma(a, c)|^2 = \sum_{h,j=0}^{\tau-1} e(c(h-j)/\tau) \sum_{a=0}^{m-1}{}^{*}e(a(\lambda^h - \lambda^j)/m). \tag{13}$$

Now, for an integer t, the sum $\Sigma_{a=0}^{*m-1} e(at/m)$ is a Ramanujan sum which, according to [2, p. 238], has the value

$$\sum_{a=0}^{m-1}{}^{*} e(at/m) = \frac{\mu(m/t')\varphi(m)}{\varphi(m/t')},$$

where $t' = \text{g.c.d.}(t, m)$ and μ is the Moebius function. It follows that in (13) we only get a contribution from those ordered pairs (h, j) for which $\lambda^h \equiv \lambda^j \pmod{p^{\alpha-1}}$, or, equivalently, $h \equiv j \pmod{\gamma}$. In detail, we have

$$\sum_{a=0}^{m-1}{}^{*}|\sigma(a, c)|^2 = \varphi(m)\tau + \frac{\mu(p)\varphi(m)}{\varphi(p)} \sum_{\substack{h,j=0\\ h\neq j, h\equiv j \,(\mathrm{mod}\ \gamma)}}^{\tau-1} e(c(h-j)/\tau).$$

Now,

$$\sum_{\substack{h,j=0\\ h\neq j, h\equiv j \,(\mathrm{mod}\ \gamma)}}^{\tau-1} e(c(h-j)/\tau) = \sum_{\substack{h,j=0\\ h\equiv j \,(\mathrm{mod}\ \gamma)}}^{\tau-1} e(c(h-j)/\tau) - \tau$$

$$= \frac{1}{\gamma}\sum_{h,j=0}^{\tau-1} e(c(h-j)/\tau) \sum_{s=0}^{\gamma-1} e(s(h-j)/\gamma) - \tau = \frac{1}{\gamma}\sum_{s=0}^{\gamma-1}\left|\sum_{j=0}^{\tau-1} e\left(\frac{c+sd}{\tau}j\right)\right|^2 - \tau.$$

If $d|c$, then there is a unique s, $0 \leqslant s \leqslant \gamma - 1$, such that $c + sd \equiv 0 \pmod{\tau}$; if $d \nmid c$, we always have $c + sd \not\equiv 0 \pmod{\tau}$. Therefore,

$$\sum_{\substack{h,j=0\\ h\neq j, h\equiv j \ (\mathrm{mod}\ \gamma)}}^{\tau-1} e(c(h-j)/\tau) = \begin{cases}(d-1)\tau & \text{if } d|c,\\ -\tau & \text{if } d\nmid c.\end{cases}$$

It follows that

$$\sum_{a=0}^{m-1}{}^{*}|\sigma(a,c)|^2 = \begin{cases}\varphi(m)\tau - \dfrac{d-1}{p-1}\varphi(m)\tau & \text{if } d|c,\\ m\tau & \text{if } d\nmid c.\end{cases}$$

By combining this with (12), we arrive at the inequalities (10) and (11).

Since $\lambda^{\gamma} \equiv 1 \pmod{p^{\alpha-1}}$ implies $\lambda^{\gamma p} \equiv 1 \pmod{p^{\alpha}}$, the value of d in Lemma 5 can only be 1 or p. If $d = 1$, then we have (10) for all integers c, and the sum occurring in (14) below can be estimated as in Lemma 3. If $d = p$, one obtains the following result.

LEMMA 6. *Suppose the conditions of Lemma 5 hold with $d = p$. Then,*

$$\left|\sum_{n=0}^{N-1} e(b\lambda^n/m)\right| < m^{1/2}\left(\frac{2(p-1)}{\pi p}\log\tau + \frac{3}{4}\right) \quad \textit{for } 1 \leqslant N \leqslant \tau. \tag{14}$$

Proof. As in the proof of Lemma 3, we have

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

It follows from Lemma 5 that

$$\left|\sum_{n=0}^{N-1} e(b\lambda^n/m)\right| \leqslant \frac{m^{1/2}}{\tau}\sum_{c=1;\,p\nmid c}^{\tau-1}\left|\sum_{y=0}^{N-1} e(cy/\tau)\right|. \tag{15}$$

If $\tau = p$, then

$$\sum_{c=1;\,p\nmid c}^{\tau-1}\left|\sum_{y=0}^{N-1} e(cy/\tau)\right| = \sum_{c=1}^{p-1}\left|\sum_{y=0}^{N-1} e(cy/p)\right| < \frac{2}{\pi}\, p\log p + \frac{2}{5}\, p$$

by Lemma 2. Together with (15), the inequality (14) follows easily. Thus, $\tau \geqslant 2p$ from now on. As in the proof of Lemma 2, we get

$$\sum_{c=1;\,p\nmid c}^{\tau-1}\left|\sum_{y=0}^{N-1} e(cy/\tau)\right| = \sum_{c=1;\,p\nmid c}^{\tau-1}\frac{\sin\pi\|cN/\tau\|}{\sin\pi\|c/\tau\|} \leqslant \sum_{c=1;\,p\nmid c}^{\tau-1}(\sin\pi\|c/\tau\|)^{-1}$$

$$\leqslant 2\sum_{c=1;\,p\nmid c}^{[\tau/2]}(\sin(\pi c/\tau))^{-1};$$

and so,

$$\sum_{c=1;\,p\nmid c}^{\tau-1}\left|\sum_{y=0}^{N-1} e(cy/\tau)\right| \leqslant 2\sum_{c=1}^{[\tau/2]}(\sin(\pi c/\tau))^{-1} - 2\sum_{c=1;\,p|c}^{[\tau/2]}(\sin(\pi c/\tau))^{-1}. \tag{16}$$

Now,

$$\sum_{c=1;\,p|c}^{[\tau/2]} (\sin(\pi c/\tau))^{-1} = \sum_{c=1}^{[\tau/2p]} (\sin(\pi pc/\tau))^{-1} = (\sin(\pi p[\tau/2p]/\tau))^{-1}$$

$$\tag{17} + \sum_{c=1}^{[\tau/2p]-1} (\sin(\pi pc/\tau))^{-1} \geqslant 1 + \int_1^{[\tau/2p]} \frac{dx}{\sin(\pi px/\tau)}$$

$$= 1 + \frac{\tau}{\pi p}\int_{\pi p/\tau}^{\pi p[\tau/2p]/\tau} \frac{dt}{\sin t} = 1 + \frac{\tau}{\pi p}\log\tan\frac{\pi p[\tau/2p]}{2\tau}$$

$$+ \frac{\tau}{\pi p}\log\cot\frac{\pi p}{2\tau}.$$

Since $f(x) = x^{-1} - \cot x$ is increasing for $0 < x \leqslant \pi/4$, we have

$$x^{-1} - \cot x \leqslant f(\pi/4) = \frac{4}{\pi} - 1 \quad \text{for } 0 < x \leqslant \pi/4;$$

and consequently,

$$\tag{18} \log\cot\frac{\pi p}{2\tau} \geqslant \log\left(\frac{2\tau}{\pi p} + 1 - \frac{4}{\pi}\right) \geqslant \log\frac{2\tau}{\pi p} - \left(\frac{4}{\pi} - 1\right)\left(\frac{2\tau}{\pi p} + 1 - \frac{4}{\pi}\right)^{-1}$$

by the mean-value theorem. Furthermore, $[\tau/2p] \geqslant \tau/2p - 1/2$, and so, by the mean-value theorem again,

$$\tag{19} \begin{aligned} \log\tan\frac{\pi p[\tau/2p]}{2\tau} &\geqslant \log\tan\left(\frac{\pi}{4} - \frac{\pi p}{4\tau}\right) \geqslant -\frac{\pi p}{4\tau}\cdot\frac{2}{\sin(\pi/2 - \pi p/2\tau)} \\ &= -\frac{\pi p}{2\tau}\left(\cos\frac{\pi p}{2\tau}\right)^{-1} \geqslant -\frac{\pi p}{2\tau}\left(\cos\frac{\pi}{4}\right)^{-1} = -\frac{\pi p}{\tau\sqrt{2}}. \end{aligned}$$

By combining (17), (18), and (19), we obtain

$$\sum_{c=1;\,p|c}^{[\tau/2]} (\sin(\pi c/\tau))^{-1} \geqslant \frac{\tau}{\pi p}\log\frac{2\tau}{\pi p} + 1 - \frac{1}{\sqrt{2}} - \frac{\tau}{\pi p}\left(\frac{4}{\pi} - 1\right)\left(\frac{2\tau}{\pi p} + 1 - \frac{4}{\pi}\right)^{-1},$$

and it is easily checked that this implies

$$\tag{20} \sum_{c=1;\,p|c}^{[\tau/2]} (\sin(\pi c/\tau))^{-1} > \frac{\tau}{\pi p}\log\frac{2\tau}{\pi p}.$$

By an inequality in the proof of Lemma 2, we have

$$\sum_{c=1}^{[\tau/2]} (\sin(\pi c/\tau))^{-1} \leqslant \frac{\tau}{\pi}\log\tau + \left(\frac{1}{3} - \frac{1}{\pi}\log\frac{\pi}{2}\right)\tau \quad \text{for } \tau \geqslant 6.$$

Then, using (16) and (20),

$$\sum_{c=1;\,p\nmid c}^{\tau-1} \left|\sum_{y=0}^{N-1} e(cy/\tau)\right| < \frac{2\tau}{\pi}\log\tau + \left(\frac{2}{3} - \frac{2}{\pi}\log\frac{\pi}{2}\right)\tau - \frac{2\tau}{\pi p}\log\frac{2\tau}{\pi p}$$

$$= \frac{2(p-1)}{\pi p}\tau\log\tau + \left(\frac{2}{3} - \frac{2}{\pi}\log\frac{\pi}{2} + \frac{2}{\pi p}\log\frac{\pi p}{2}\right)\tau$$

for $\tau \geqslant 6$. Since $g(x) = x^{-1} \log x$ is decreasing for $x > e$, we have

$$\frac{2}{\pi p} \log \frac{\pi p}{2} \leqslant \frac{\log \pi}{\pi};$$

and so,

$$\sum_{c=1;p\nmid c}^{\tau-1} \left| \sum_{y=0}^{N-1} e(cy/\tau) \right| < \frac{2(p-1)}{\pi p} \tau \log \tau + \frac{3}{4}\tau, \tag{21}$$

at least for $\tau \geqslant 6$. In the only exceptional case, namely $\tau = 4$ and $p = 2$, one checks (21) directly on the basis of (16). The desired inequality (14) follows now from (15) and (21).

We recall the definition of the number β introduced in [8, Section 4]. Let λ be relatively prime to m with $|\lambda| > 1$, and 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 $\delta = 1$ if $\lambda \equiv 1 \pmod 4$ and $\delta = 2$ if $\lambda \equiv 3 \pmod 4$. Then β is the largest integer such that $2^\beta | (\lambda^\delta - 1)$. The significance of β stems from the fact that $\tau(p^{h+1}) = p\tau(p^h)$ as soon as $h \geqslant \beta$, where $\tau(p^h)$ is the exponent to which λ belongs modulo p^h.

THEOREM 3. *Let $m = p^\alpha$, p prime, $\alpha \geqslant 2$. 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*

$$p^\beta < \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{m^{3/2}}{\pi N} \left(\frac{2(p-1)}{\pi p} \log \tau + \frac{3}{4} \right), \tag{22}$$

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

$$D_N < \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} X \log \left(1 + \frac{4(p^{3/2} - 1)}{p^{3/2} - p^{1/2}} \cdot \frac{1}{X} \right) + \left(\frac{p^{3/2}}{p^{3/2} - 1} + \frac{\log p}{p} \right) X,$$

where

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

Proof. Because of (7), we have

$$D_N \leqslant \frac{4}{L} + \frac{4}{\pi} \sum_{b=1}^{L} \left(\frac{1}{b} - \frac{1}{L} \right) \left| \frac{1}{N} \sum_{n=0}^{N-1} e(by_0 \lambda^n / m) \right| \tag{23}$$

for all positive integers L. We choose now

$$L = \left[\frac{4(p^{3/2} - 1)}{p^{3/2} - p^{1/2}} \cdot \frac{1}{X} \right] + 1.$$

It follows then from (22) that $L \leqslant p^{\alpha - \beta}$.

For $1 \leqslant b \leqslant L - 1$, we have g.c.d.$(by_0, m) =$ g.c.d.$(b, m) = p^s$ with $0 \leqslant s \leqslant \alpha - \beta - 1$. If $s > 0$, then

$$\sum_{n=0}^{\tau-1} e(by_0 \lambda^n / m) = \sum_{n=0}^{\tau-1} e\left(\frac{(b/p^s) y_0 \lambda^n}{p^{\alpha - s}} \right) = \frac{\tau}{\tau(p^{\alpha-s})} \sum_{n=0}^{\tau(p^{\alpha-s})-1} e\left(\frac{(b/p^s) y_0 \lambda^n}{p^{\alpha-s}} \right). \tag{24}$$

Since $s \leqslant \alpha - \beta - 1$, we have $\tau(p^{\alpha-s}) = p\tau(p^{\alpha-s-1})$ by the remark preceding Theorem 3. Therefore, the last sum in (24) is equal to zero by (10), and so

$$\sum_{n=0}^{\tau-1} e(by_0\lambda^n/m) = 0.$$

It follows then by the same argument as in [8, Lemma 3] and by Lemma 6 that

$$\begin{aligned}\left|\sum_{n=0}^{N-1} e(by_0\lambda^n/m)\right| &< p^{(\alpha-s)/2}\left(\frac{2(p-1)}{\pi p}\log \tau(p^{\alpha-s}) + \frac{3}{4}\right)\\ &\leqslant (m/p^s)^{1/2}\left(\frac{2(p-1)}{\pi p}\log \tau + \frac{3}{4}\right) \quad \text{for } 1 \leqslant N \leqslant \tau.\end{aligned}$$

The above inequality is also satisfied in the case $s = 0$, for then the requirements of Lemma 6 are met because of $\tau = p\tau(p^{\alpha-1})$. For $b = L$, the coefficient of the corresponding trigonometric sum in (23) is zero. Let R be the largest integer with $p^R \leqslant L$. Then,

$$\begin{aligned}D_N &\leqslant \frac{4}{L} + \frac{4m^{1/2}}{\pi N}\left(\frac{2(p-1)}{\pi p}\log \tau + \frac{3}{4}\right)\sum_{s=0}^{R} p^{-s/2} \sum_{\substack{b=1\\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right)\\ &= \frac{4}{L} + X\sum_{s=0}^{R} p^{-s/2} \sum_{\substack{b=1\\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right).\end{aligned} \tag{25}$$

To estimate the double sum in (25), we distinguish several cases depending on the value of R. If $R = 0$, then $L < p$, and so by [8, Eq. (9)] with $s = 0$,

$$\begin{aligned}\sum_{s=0}^{R} p^{-s/2} \sum_{\substack{b=1\\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) &\leqslant \log L < \frac{p-1}{p}\log L + \frac{\log p}{p}\\ &\leqslant \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1}\log L + \frac{\log p}{p}.\end{aligned}$$

If $R = 1$, then $p \leqslant L < p^2$, and so from [8, Eq. (9)] with $s = 0, 1$, we get

$$\begin{aligned}&\sum_{s=0}^{R} p^{-s/2} \sum_{\substack{b=1\\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right)\\ &\leqslant \log L - \frac{1}{p}\log\left(\left[\frac{L}{p}\right] + 1\right) + \frac{1}{L}\left[\frac{L}{p}\right] + \frac{1}{p^{3/2}}\log\left[\frac{L}{p}\right] + \frac{1}{Lp^{1/2}}\left\{\frac{L}{p}\right\}\\ &\leqslant \log L - \frac{1}{p}\log\frac{L}{p} + \frac{1}{L}\left(\left[\frac{L}{p}\right] + \left\{\frac{L}{p}\right\}\right) + \frac{1}{p^{3/2}}\log\frac{L}{p}\\ &= \left(\frac{p-1}{p} + \frac{1}{p^{3/2}}\right)\log L + \frac{1+\log p}{p} - \frac{\log p}{p^{3/2}}.\end{aligned}$$

Since $\log p > \frac{1}{2} \log L$, the last expression is less than

$$\left(\frac{p-1}{p} + \frac{1}{2p^{3/2}}\right)\log L + \frac{1+\log p}{p}.$$

It is straightforward to check that

$$\frac{p-1}{p} + \frac{1}{2p^{3/2}} < \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1};$$

and so we obtain

$$\sum_{s=0}^{R} p^{-s/2} \sum_{\substack{b=1 \\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) < \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}\log L + \frac{1+\log p}{p}.$$

Finally, let $R \geqslant 2$. Then, from [8, Eq. (9)] we get

$$\sum_{\substack{b=1 \\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) \leqslant \frac{1}{p^s}\log\frac{L}{p^s} - \frac{1}{p^{s+1}}\log\frac{L}{p^{s+1}} + \frac{1}{L}\left\{\frac{L}{p^s}\right\} + \frac{1}{L}\left[\frac{L}{p^{s+1}}\right] \quad \text{for } 0 \leqslant s < R,$$

and

$$\sum_{\substack{b=1 \\ \text{g.c.d.}(b,m)=p^R}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) \leqslant \frac{\log p}{p^R} + \frac{1}{L}\left\{\frac{L}{p^R}\right\}.$$

It follows that

$$\text{(26)} \quad \begin{aligned} \sum_{s=0}^{R} p^{-s/2} \sum_{\substack{b=1 \\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) &\leqslant \sum_{s=0}^{R-1} p^{-3s/2}\left(\log\frac{L}{p^s} - \frac{1}{p}\log\frac{L}{p^{s+1}}\right) \\ &+ p^{-3R/2}\log p + \frac{1}{L}\left(\sum_{s=0}^{R-1} p^{-s/2}\left(\left\{\frac{L}{p^s}\right\} + \left[\frac{L}{p^{s+1}}\right]\right) + p^{-R/2}\left\{\frac{L}{p^R}\right\}\right). \end{aligned}$$

Now

$$\sum_{s=0}^{R-1} p^{-s/2}\left(\left\{\frac{L}{p^s}\right\} + \left[\frac{L}{p^{s+1}}\right]\right) + p^{-R/2}\left\{\frac{L}{p^R}\right\} = \sum_{s=1}^{R} p^{-s/2}\left\{\frac{L}{p^s}\right\} + \sum_{s=0}^{R-1} p^{-s/2}\left[\frac{L}{p^{s+1}}\right]$$

$$\text{(27)} = \sum_{s=0}^{R-1} p^{-(s+1)/2}\left\{\frac{L}{p^{s+1}}\right\} + \sum_{s=0}^{R-1} p^{-s/2}\left[\frac{L}{p^{s+1}}\right] \leqslant \sum_{s=0}^{R-1} p^{-s/2}\left(\left\{\frac{L}{p^{s+1}}\right\} + \left[\frac{L}{p^{s+1}}\right]\right)$$

$$= \frac{L}{p}\sum_{s=0}^{R-1} p^{-3s/2} < \frac{p^{1/2}}{p^{3/2}-1} L.$$

Furthermore,

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

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

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

$$\leqslant \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}\log L + \frac{\log p}{p} - p^{-3R/2}\left(\frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}\log L - \log p\right).$$

However, since $\log L \geqslant 2\log p$, the last expression in parentheses is easily shown to be positive. By combining this with (26) and (27), we obtain

$$(28)\qquad \sum_{s=0}^{R} p^{-s/2} \sum_{\substack{b=1 \\ \text{g.c.d.}(b,m)=p^s}}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) < \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}\log L + \frac{\log p}{p} + \frac{p^{1/2}}{p^{3/2}-1}.$$

By comparing this with the results in the earlier cases $R = 0$ and $R = 1$, we see that (28) holds in all cases. Thus, together with (25),

$$D_N < \frac{4}{L} + \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}X\log L + \left(\frac{\log p}{p} + \frac{p^{1/2}}{p^{3/2}-1}\right)X.$$

Using the special form of L, we obtain

$$D_N < \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}X + \frac{p^{3/2}-p^{1/2}}{p^{3/2}-1}X\log\left(1 + \frac{4(p^{3/2}-1)}{p^{3/2}-p^{1/2}}\cdot\frac{1}{X}\right)$$
$$+ \left(\frac{\log p}{p} + \frac{p^{1/2}}{p^{3/2}-1}\right)X,$$

which proves the theorem.

A condition which implies (22), and which is easier to check, is the following one:

$$(29)\qquad p^\beta < (0.24)m^{1/2}\left(\frac{2(p-1)}{\pi p}\log\tau + \frac{3}{4}\right).$$

That (29) is a sufficient condition for (22) is shown as in [8, Eq. (12)]. In practical cases, m and τ are large, so that (29) can be satisfied by choosing a λ with $\beta \leqslant \alpha/2$.

We note that on the basis of Lemma 2 one can also improve somewhat on the results in [8, Theorems 3 and 4].

3. The Inhomogeneous Case. We consider now the sequence $y_0, y_1, \ldots$ of integers described in Section 1, generated by the recursion $y_{n+1} \equiv \lambda y_n + r \pmod m$

for $n = 0, 1, \ldots$, where λ is relatively prime to m and $r \not\equiv 0 \pmod m$; the last condition is, however, never used in the proofs. To rule out the trivial case that $y_0, y_1, \ldots$ is a constant sequence, we assume $\lambda y_0 + r \not\equiv y_0 \pmod m$. We shall also require that $\lambda \not\equiv 1 \pmod m$, in order to discard another uninteresting case. In some of the lemmas, these restrictions are not necessary. In the inhomogeneous case, the initial value y_0 need not be relatively prime to m. One shows easily by induction that

$$y_n \equiv \lambda^n y_0 + \frac{\lambda^n - 1}{\lambda - 1} r \pmod m \quad \text{for } n = 0, 1, \ldots. \tag{30}$$

Let τ again be the period of the sequence $y_0, y_1, \ldots$. We shall estimate the discrepancy D_N of the pseudo-random numbers $x_0 = y_0/m$, $x_1 = y_1/m, \ldots, x_{N-1} = y_{N-1}/m$ for $1 \leqslant N \leqslant \tau$.

In the case that m is prime, the period τ can be described in the same way as in the homogeneous case. Because of (30), we have $y_n \equiv y_0 \pmod m$ if and only if

$$\frac{\lambda^n - 1}{\lambda - 1}((\lambda - 1)y_0 + r) \equiv 0 \pmod m,$$

which, by virtue of $\lambda \not\equiv 1 \pmod m$ and $(\lambda - 1)y_0 + r \not\equiv 0 \pmod m$, is equivalent to $\lambda^n \equiv 1 \pmod m$. Therefore, τ is equal to the exponent to which λ belongs modulo m.

LEMMA 7. *Let $m_1 \geqslant 2$ and r be integers, let b and λ be relatively prime to m_1, let λ belong to the exponent μ_1 modulo m_1, and let $z_0, z_1, \ldots$ be a sequence of integers with $z_{n+1} = \lambda z_n + r$ $(n = 0, 1, \ldots)$ having period τ_1 modulo m_1. Then,*

$$\left|\sum_{n=0}^{N-1} e(bz_n/m_1)\right| < \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2}\left(\frac{2}{\pi}\log \tau_1 + \frac{2}{5} + \frac{N}{\tau_1}\right) \quad \textit{for } 1 \leqslant N \leqslant \tau_1.$$

Proof. Since λ is relatively prime to m_1, the sequence $z_0, z_1, \ldots$ is purely periodic modulo m_1 with period τ_1. By [10, Theorem 1] (compare also with [10, Theorem 4]), we have

$$\left|\sum_{n=0}^{\tau_1 - 1} e(bz_n/m_1)e(cn/\tau_1)\right| \leqslant \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2} \tag{31}$$

for all integers c. Then, as in the proof of Lemma 3,

$$\begin{aligned}
\left|\sum_{n=0}^{N-1} e(bz_n/m_1)\right| &\leqslant \frac{1}{\tau_1}\sum_{c=1}^{\tau_1}\left|\sum_{y=0}^{N-1} e(-cy/\tau_1)\right| \left|\sum_{n=0}^{\tau_1-1} e(bz_n/m_1)e(cn/\tau_1)\right| \\
&\leqslant \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2} \frac{1}{\tau_1}\sum_{c=1}^{\tau_1}\left|\sum_{y=0}^{N-1} e(cy/\tau_1)\right| = \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2} \frac{1}{\tau_1}\sum_{c=1}^{\tau_1-1}\left|\sum_{y=0}^{N-1} e(cy/\tau_1)\right| \\
&\quad + \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2} \frac{N}{\tau_1} < \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2}\left(\frac{2}{\pi}\log \tau_1 + \frac{2}{5} + \frac{N}{\tau_1}\right),
\end{aligned}$$

where we have applied Lemma 2 in the last step.

THEOREM 4. *Let m be a prime, and let $\lambda \not\equiv 1 \pmod m$, g.c.d.$(\lambda, m) = 1$, and $\lambda y_0 + r \not\equiv y_0 \pmod m$. Then, for $1 \leqslant N \leqslant \tau$, the discrepancy D_N of the points x_0,*

$x_1, \ldots, x_{N-1}$ *satisfies the inequality* $D_N < X \log(1 + 4/X) + X$, *where*

$$X = \frac{4m^{1/2}}{\pi N}\left(\frac{2}{\pi} \log \tau + \frac{2}{5} + \frac{N}{\tau}\right).$$

Proof. By (7), we have

$$D_N \leqslant \frac{4}{L} + \frac{4}{\pi} \sum_{b=1}^{L}\left(\frac{1}{b} - \frac{1}{L}\right)\left|\frac{1}{N}\sum_{n=0}^{N-1} e(by_n/m)\right|$$

for all positive integers L. We choose now $L = [4/X] + 1$. We note that

$$\frac{X}{4} = \frac{m^{1/2}}{\pi N}\left(\frac{2}{\pi} \log \tau + \frac{2}{5}\right) + \frac{m^{1/2}}{\pi \tau} \geqslant \frac{7m^{1/2}}{5\pi\tau} \geqslant \frac{7m^{1/2}}{5\pi(m-1)} > \frac{1}{m},$$

and so $L \leqslant m$. We apply now Lemma 7 with $m_1 = m$ and with the sequence $z_0, z_1, \ldots$ determined by $z_0 = y_0$. We have $z_n \equiv y_n \pmod m$ for $n = 0, 1, \ldots$ and $\tau_1 = \mu_1 = \tau$, therefore, by using the estimate in Lemma 7 formally in case $b = L = m$, we get

$$\begin{aligned} D_N &\leqslant \frac{4}{L} + \frac{4m^{1/2}}{\pi N}\left(\frac{2}{\pi} \log \tau + \frac{2}{5} + \frac{N}{\tau}\right)\sum_{b=1}^{L}\left(\frac{1}{b} - \frac{1}{L}\right) \\ &< X + X \log L \leqslant X + X \log(1 + 4/X), \end{aligned}$$

and the proof is complete.

THEOREM 5. *Suppose the conditions of Theorem* 4 *hold. Then, for* $1 \leqslant N \leqslant \tau$, *the discrepancy* D_N *of the points* $x_0, x_1, \ldots, x_{N-1}$ *satisfies the inequality*

$$D_N \leqslant \frac{m^{1/2}}{N}\left(\frac{2}{\pi} \log \tau + \frac{2}{5} + \frac{N}{\tau}\right)\left(\frac{2}{\pi} \log m + \frac{2}{5}\right) + \frac{2}{m}.$$

Proof. This is an immediate consequence of Lemmas 4 and 7, with the latter lemma applied in the same way as in the proof of Theorem 4.

Now let m be a prime power, say $m = p^\alpha$ with p prime and $\alpha \geqslant 2$. There are various ways of characterizing the period τ of $y_0, y_1, \ldots$ in this case. See [1], [3, Chapter 3], and [5]. For our purposes, the following characterization is convenient.

LEMMA 8. *Let* $m = p^\alpha$, *p prime*, $\alpha \geqslant 1$, *let* $\lambda \neq 1$ *be relatively prime to m and let r be an integer. Let* $z_0, z_1, \ldots$ *be a sequence of integers with* $z_{n+1} = \lambda z_n + r$ $(n = 0, 1, \ldots)$ *such that* $(\lambda - 1)z_0 + r \neq 0$. *Let* ρ *be the largest integer such that* $p^\rho | (\lambda - 1)$ *and* ω *the largest integer such that* $p^\omega | ((\lambda - 1)z_0 + r)$. *We assume* $\alpha - \omega + \rho \geqslant 0$. *Then* $z_0, z_1, \ldots$ *is purely periodic modulo m, and its period modulo m is equal to the exponent to which* λ *belongs modulo* $p^{\alpha-\omega+\rho}$. *This holds trivially for* $\alpha = 0$ *as well.*

Proof. Since λ is relatively prime to m, the sequence $z_0, z_1, \ldots$ is purely periodic modulo m. In analogy with (30), we have

$$z_n - z_0 = \frac{\lambda^n - 1}{\lambda - 1}((\lambda - 1)z_0 + r) \quad \text{for } n = 0, 1, \ldots .$$

But the number on the right-hand side is divisible by $m = p^\alpha$, $\alpha \geqslant 1$, if and only if $\lambda^n \equiv 1 \pmod{p^{\alpha-\omega+\rho}}$, and the assertion follows.

The exceptional cases in Lemma 8 are trivial. If $\alpha - \omega + \rho < 0$, then $\omega > \alpha$, and the period is 1. If $(\lambda - 1)z_0 + r = 0$, then the period is also 1, and if $\lambda = 1$, then the period is m/r', where $r' = \text{g.c.d.}(r, m)$. Since the given sequence $y_0, y_1, \ldots$ is identical modulo m with a sequence $z_0, z_1, \ldots$ from Lemma 8, this result yields the desired information about the period τ. The conditions of Lemma 8 will be satisfied if we assume $\lambda \not\equiv 1 \pmod{m}$, $\text{g.c.d.}(\lambda, m) = 1$, and $\lambda y_0 + r \not\equiv y_0 \pmod{m}$. The subsequent lemma generalizes (10) in the case $d = p$.

LEMMA 9. *Let $m_1 = p^\sigma$, p prime, $\sigma \geqslant 1$, and let $z_0, z_1, \ldots$ be a sequence of integers with $z_{n+1} = \lambda z_n + r$ $(n = 0, 1, \ldots)$ which is purely periodic modulo m_1 with period τ_1 and purely periodic modulo $m_2 = p^{\sigma-1}$ with period $\tau_2 = \tau_1/p$. Then,*

$$\sum_{n=0}^{\tau_1-1} e(bz_n/m_1)e(cn/\tau_1) = 0$$

for all integers b relatively prime to m_1 and all integers c divisible by p.

Proof. We have

$$\sum_{\substack{b=1\\ \text{g.c.d.}(b,m_1)=1}}^{m_1} \left|\sum_{n=0}^{\tau_1-1} e(bz_n/m_1)e(cn/\tau_1)\right|^2$$

$$= \sum_{b=1}^{m_1} \left|\sum_{n=0}^{\tau_1-1} e(bz_n/m_1)e(cn/\tau_1)\right|^2 - \sum_{b=1;p|b}^{m_1} \left|\sum_{n=0}^{\tau_1-1} e(bz_n/m_1)e(cn/\tau_1)\right|^2$$

$$= \sum_{b=1}^{m_1} \sum_{h,j=0}^{\tau_1-1} e(b(z_h - z_j)/m_1)e(c(h-j)/\tau_1) - \sum_{b=1}^{m_2} \left|\sum_{n=0}^{\tau_1-1} e(bz_n/m_2)e((c/p)n/\tau_2)\right|^2$$

$$= \sum_{h,j=0}^{\tau_1-1} e(c(h-j)/\tau_1) \sum_{b=1}^{m_1} e(b(z_h - z_j)/m_1) - p^2 \sum_{b=1}^{m_2} \left|\sum_{n=0}^{\tau_2-1} e(bz_n/m_2)e(cn/\tau_1)\right|^2$$

$$= m_1\tau_1 - p^2 \sum_{h,j=0}^{\tau_2-1} e(c(h-j)/\tau_1) \sum_{b=1}^{m_2} e(b(z_h - z_j)/m_2)$$

$$= m_1\tau_1 - p^2 m_2 \tau_2 = 0,$$

which proves the result.

LEMMA 10. *Suppose the conditions of Lemma 9 are satisfied, and that λ is relatively prime to m_1 and belongs to the exponent μ_1 modulo m_1. Then, for all integers b relatively prime to m_1 we have*

$$\left|\sum_{n=0}^{N-1} e(bz_n/m_1)\right| < \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2} \left(\frac{2(p-1)}{\pi p} \log \tau_1 + \frac{3}{4}\right) \quad \textit{for } 1 \leqslant N \leqslant \tau_1.$$

Proof. As in the proof of Lemma 3, we have

$$\left|\sum_{n=0}^{N-1} e(bz_n/m_1)\right| \leqslant \frac{1}{\tau_1} \sum_{c=1}^{\tau_1} \left|\sum_{y=0}^{N-1} e(-cy/\tau_1)\right| \left|\sum_{n=0}^{\tau_1-1} e(bz_n/m_1)e(cn/\tau_1)\right|.$$

Because of Lemma 9, this reduces to

$$\left|\sum_{n=0}^{N-1} e(bz_n/m_1)\right| \leqslant \frac{1}{\tau_1} \sum_{c=1;p\nmid c}^{\tau_1 - 1} \left|\sum_{y=0}^{N-1} e(cy/\tau_1)\right| \left|\sum_{n=0}^{\tau_1 - 1} e(bz_n/m_1)e(cn/\tau_1)\right|.$$

By applying (31), we get

$$\left|\sum_{n=0}^{N-1} e(bz_n/m_1)\right| \leqslant \left(\frac{m_1\tau_1}{\mu_1}\right)^{1/2} \frac{1}{\tau_1} \sum_{c=1;p\nmid c}^{\tau_1 - 1} \left|\sum_{y=0}^{N-1} e(cy/\tau_1)\right|.$$

The sum on the right-hand side was estimated in the proof of Lemma 6, and this implies already the desired inequality.

For λ relatively prime to m and $|\lambda| > 1$, we define the positive integer β in the same way as in the paragraph preceding Theorem 3, and we denote by μ the exponent to which λ belongs modulo m. We define the number ρ as in Lemma 8, and we let ω be the largest integer such that $p^\omega | ((\lambda - 1)y_0 + r)$. We note that $0 \leqslant \rho < \alpha$ and $0 \leqslant \omega < \alpha$ under the conditions of the subsequent theorem.

THEOREM 6. *Let $m = p^\alpha$, p prime, $\alpha \geqslant 2$, let λ be relatively prime to m with $|\lambda| > 1$, $\lambda \not\equiv 1 \pmod m$, and $\lambda y_0 + r \not\equiv y_0 \pmod m$, and let $\alpha - \omega + \rho > \beta$. Then, if $1 \leqslant N \leqslant \tau$ and*

$$p^{\beta+\omega-\rho} < \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} \cdot \frac{m^{3/2}\tau^{1/2}}{\pi N \mu^{1/2}}\left(\frac{2(p-1)}{\pi p} \log \tau + \frac{3}{4}\right), \tag{32}$$

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

$$D_N < \frac{p^{3/2} - p^{1/2}}{p^{3/2} - 1} X \log\left(1 + \frac{4(p^{3/2} - 1)}{p^{3/2} - p^{1/2}} \cdot \frac{1}{X}\right) + \left(\frac{p^{3/2}}{p^{3/2} - 1} + \frac{\log p}{p}\right) X,$$

where

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

Proof. Let $z_0, z_1, \ldots$ be the sequence of integers determined by $z_0 = y_0$ and $z_{n+1} = \lambda z_n + r$ for $n = 0, 1, \ldots$. Then $z_n \equiv y_n \pmod m$ for $n = 0, 1, \ldots$, and from (7) we get

$$D_N \leqslant \frac{4}{L} + \frac{4}{\pi} \sum_{b=1}^{L} \left(\frac{1}{b} - \frac{1}{L}\right) \left|\frac{1}{N} \sum_{n=0}^{N-1} e(bz_n/m)\right| \tag{33}$$

for all positive integers L. We choose now

$$L = \left[\frac{4(p^{3/2} - 1)}{p^{3/2} - p^{1/2}} \cdot \frac{1}{X}\right] + 1.$$

It follows from (32) that $L \leqslant p^{\alpha-\beta-\omega+\rho}$.

The sequence $z_0, z_1, \ldots$ is purely periodic modulo m and, by Lemma 8, its period τ modulo m is equal to the exponent to which λ belongs modulo $p^{\alpha-\omega+\rho}$. Since $\alpha - \omega + \rho > \beta$, it follows from Lemma 8 and the remark preceding Theorem 3 that the conditions of Lemma 10 are satisfied for $m_1 = m$. Therefore, for $1 \leqslant N \leqslant \tau$,

$$(34)\qquad \left|\sum_{n=0}^{N-1} e(bz_n/m)\right| < \left(\frac{m\tau}{\mu}\right)^{1/2}\left(\frac{2(p-1)}{\pi p}\log\tau + \frac{3}{4}\right) \quad \text{if g.c.d.}(b, m) = 1.$$

If b with $1 \leqslant b \leqslant L - 1$ is not relatively prime to m, then g.c.d.$(b, m) = p^s$ with $0 < s \leqslant \alpha - \beta - \omega + \rho - 1$. Since we always have $\beta \geqslant \rho$, this implies $s \leqslant \alpha - 1$. For $1 \leqslant N \leqslant \tau$, we write

$$(35)\qquad \sum_{n=0}^{N-1} e(bz_n/m) = \sum_{n=0}^{N-1} e(b'z_n/m'),$$

where $b' = b/p^s$, $m' = p^{\alpha-s}$, and g.c.d.$(b', m') = 1$. According to Lemma 8, the period τ' modulo m' of the sequence $z_0, z_1, \ldots$ is equal to the exponent to which λ belongs modulo $p^{\alpha-s-\omega+\rho}$. Since $\alpha - s - \omega + \rho > \beta$, it follows from Lemma 8 and the remark preceding Theorem 3 that the conditions of Lemma 9 are satisfied for $m_1 = m'$. Therefore,

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

Using the division algorithm, we write $N = q\tau' + N'$ with $0 \leqslant N' < \tau'$. Then,

$$\sum_{n=0}^{N-1} e(b'z_n/m') = \sum_{n=0}^{N'-1} e(b'z_n/m').$$

Since the conditions of Lemma 10 are also satisfied for $m_1 = m'$, we can apply this lemma to the last sum. Together with (35), we obtain

$$\left|\sum_{n=0}^{N-1} e(bz_n/m)\right| < \left(\frac{m'\tau'}{\mu'}\right)^{1/2}\left(\frac{2(p-1)}{\pi p}\log\tau' + \frac{3}{4}\right),$$

where μ' is the exponent to which λ belongs modulo m'. From the above descriptions of τ and τ' as exponents to which λ belongs, from $\alpha - s - \omega + \rho > \beta$, and from the remark preceding Theorem 3, we infer $\tau = p^s\tau'$. Furthermore, since for $h \geqslant 1$ the exponent to which λ belongs modulo p^{h+1} is either equal to or p times the exponent to which λ belongs modulo p^h, we have $\mu \leqslant p^s\mu'$. Therefore, $\tau'/\mu' \leqslant \tau/\mu$. We can combine these results with (34) to obtain

$$(36)\qquad \left|\sum_{n=0}^{N-1} e(bz_n/m)\right| < \left(\frac{m\tau}{p^s\mu}\right)^{1/2}\left(\frac{2(p-1)}{\pi p}\log\tau + \frac{3}{4}\right)$$

$$\text{for } 1 \leqslant b \leqslant L - 1 \text{ and } 1 \leqslant N \leqslant \tau,$$

where $p^s =$ g.c.d.(b, m). On the basis of (33) and (36), we proceed now in complete analogy with the part of the proof of Theorem 3 starting from (25), and we arrive at the desired inequality.

If the condition (32) is not satisfied, one can employ the method of [8, Theorem 3], in combination with the improvements in the present paper, to obtain a discrepancy estimate for this case as well, which will, however, be weaker than the estimate in Theorem 6. This suggests that the parameters of a good congruential random number generator should satisfy (32) with $N = \tau$. In a special case that is considered frequently (see [1]), namely, when $m = 2^\alpha$ with $\alpha \geqslant 3$, $\lambda \equiv 5 \pmod 8$, and r odd, we have $\beta = \rho = 2$, $\omega = 0$, $\tau = m$, and $\mu = 2^{\alpha-2}$, and so it is easily checked that (32) is valid. In general, for a given prime power m one should choose λ, r, and y_0 in such a way that β and ω are small. Then (32) will be satisfied and, due to $\rho \leqslant \beta$ and Lemma 8, the factor $(\tau/\mu)^{1/2}$ in the discrepancy estimate will be close to 1.

4. Maximal Period Sequences. We discuss now the equidistribution test for a class of random number generators suggested by various authors (see [1, Section 7], [3, p. 27], [13]).

Let $k \geqslant 1$ be an integer and let p be a prime. We note that the finite field F_{p^k} of p^k elements is an extension field of $F_p = \mathbf{Z}/p\mathbf{Z}$, and that the multiplicative group $F^*_{p^k}$ of F_{p^k} is cyclic. A polynomial $f(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_0 \in \mathbf{Z}[x]$ is called a primitive polynomial modulo p if the polynomial $\bar{f}(x) \in F_p[x]$ canonically associated with $f(x)$ is the minimal polynomial over F_p of a generator of $F^*_{p^k}$. With such a primitive polynomial modulo p, we can associate the kth order homogeneous linear congruential recurrence

$$(37) \qquad y_{n+k} \equiv a_{k-1}y_{n+k-1} + \cdots + a_0 y_n \pmod p \quad \text{for } n = 0, 1, \ldots .$$

Any sequence $y_0, y_1, \ldots$ of integers in the least residue system modulo p satisfying (37) with $(y_0, \ldots, y_{k-1}) \neq (0, \ldots, 0)$ is called a maximal period sequence modulo p. The reason behind this terminology is the fact that the length of the period of a maximal period sequence modulo p is equal to $p^k - 1$, the largest possible period length of any kth order homogeneous linear recurring sequence in $\mathbf{Z}/p\mathbf{Z}$. A maximal period sequence modulo p is easily seen to be purely periodic. If $k = 1$ and a_0 is a primitive root modulo p, we get a case that was already discussed in Section 2.

For a maximal period sequence $y_0, y_1, \ldots$ modulo p, the associated sequence $x_0, x_1, \ldots$ of pseudo-random numbers in $[0, 1]$ is given by $x_n = y_n/p$ for $n = 0, 1, \ldots$. In practice, p will of course be a large prime.

Since $(y_n, y_{n+1}, \ldots, y_{n+k-1})$, $n = 0, 1, \ldots, p^k - 2$, runs through all k-tuples $\neq (0, \ldots, 0)$ of elements in the least residue system modulo p, it follows that in a full period of $y_0, y_1, \ldots$ each integer q, $1 \leqslant q \leqslant p - 1$, occurs exactly p^{k-1} times and 0 occurs exactly $p^{k-1} - 1$ times. Therefore, a full period of $x_0, x_1, \ldots$ has an extremely even distribution in $[0, 1]$. The following result shows that sufficiently long segments of a full period of $x_0, x_1, \ldots$ also perform well under the equidistribution test.

THEOREM 7. *For a prime p and* $k \geqslant 1$, *let* $y_0, y_1, \ldots$ *be a maximal period sequence modulo p satisfying* (37). *Then, for* $1 \leqslant N \leqslant p^k - 1$, *the discrepancy* D_N *of the associated pseudo-random numbers* $x_0, x_1, \ldots, x_{N-1}$ *satisfies the inequality*

$$(38)\quad D_N < \frac{2}{p} + \frac{p^{k/2}}{N}\left(\frac{2}{\pi}\log(p^k - 1) + \frac{2}{5}\right)\left(\frac{2}{\pi}\log p + \frac{2}{5}\right) + \frac{1}{p^k - 1}\left(\frac{2}{\pi}\log p + \frac{2}{5}\right).$$

Proof. We set $\tau = p^k - 1$. For g.c.d.$(b, p) = 1$ and any integer c, we have

$$\left|\sum_{n=0}^{\tau-1} e(by_n/p)e(cn/\tau)\right| \leqslant p^{k/2}$$

by [10, Theorem 1] (compare also with [10, Theorem 4]), since, in the notation of these theorems, we have $\tau = \mu$ for a maximal period sequence modulo p. For $c = 0$, we can obtain a sharper estimate by using the information concerning the number of occurrences of elements in the full period of $y_0, y_1, \ldots$. This yields immediately $\Sigma_{n=0}^{\tau-1} e(by_n/p) = -1$. Using these facts and the method in Lemma 3, we get for $1 \leqslant N \leqslant \tau$ and g.c.d.$(b, p) = 1$,

$$(39)\quad \begin{aligned} \left|\sum_{n=0}^{N-1} e(by_n/p)\right| &\leqslant \frac{1}{\tau}\sum_{c=1}^{\tau}\left|\sum_{y=0}^{N-1} e(-cy/\tau)\right|\left|\sum_{n=0}^{\tau-1} e(by_n/p)e(cn/\tau)\right| \\ &\leqslant \frac{1}{\tau}p^{k/2}\sum_{c=1}^{\tau-1}\left|\sum_{y=0}^{N-1} e(-cy/\tau)\right| + \frac{N}{\tau} < p^{k/2}\left(\frac{2}{\pi}\log\tau + \frac{2}{5}\right) + \frac{N}{\tau}. \end{aligned}$$

The inequality (38) follows now from Lemma 4.

An alternative discrepancy estimate can, of course, be obtained on the basis of (7) and (39). However, the inequality (38) is, in general, better than what could be achieved by this method. If N is somewhat larger than $p^{k/2}$, say $N \geqslant p^{(k+3)/2}$, then $2/p$ becomes the main term in (38), and this cannot be improved upon by the alternative method. Only under special circumstances, e.g., if k is small and N is very close to $p^{k/2}$, we get a slightly better result. The proof proceeds in complete analogy with earlier proofs involving this method.

We establish now a discrepancy estimate for pseudo-random numbers based on an arbitrary linear congruential generator. Let p be a prime, and let $y_0, y_1, \ldots$ be a sequence of integers in the least residue system modulo p satisfying the kth order linear congruential recurrence

$$y_{n+k} \equiv a_{k-1}y_{n+k-1} + \cdots + a_0y_n + a \pmod p \quad \text{for } n = 0, 1, \ldots,$$

where $a, a_0, \ldots, a_{k-1}$ are integers with a_0 not divisible by p. There is no condition on the initial values $y_0, \ldots, y_{k-1}$. The sequence $y_0, y_1, \ldots$ is purely periodic (see [11] for a general result to this effect); let τ be its period. We also associate with the sequence a number μ defined as follows (compare with [10, Lemma 3]). Let $b_0, b_1, \ldots$ be the sequence of integers in the least residue system modulo p determined by $b_0 = b_1 = \cdots = b_{k-2} = 0, b_{k-1} = 1$ ($b_0 = 1$ if $k = 1$) and

$$(40)\quad b_{n+k} \equiv a_{k-1}b_{n+k-1} + \cdots + a_0b_n \pmod p \quad \text{for } n = 0, 1, \ldots.$$

Then μ is taken to be the period of $b_0, b_1, \ldots$. The number μ may also be described as the maximal period of any sequence in the least residue system modulo p

satisfying the homogeneous linear congruential recurrence (40) (see [10, Lemma 2]).

If $y_0, y_1, \ldots$ is the sequence introduced above, let $x_0 = y_0/p, x_1 = y_1/p, \ldots$ be the associated sequence of pseudo-random numbers in $[0, 1]$.

THEOREM 8. *Let $x_0, x_1, \ldots$ be the sequence of pseudo-random numbers associated with the kth order linear recurring sequence $y_0, y_1, \ldots$ modulo the prime p. Let τ and μ be the numbers described above. Then, for $1 \leqslant N \leqslant \tau$, the discrepancy D_N of the points $x_0, x_1, \ldots, x_{N-1}$ satisfies the inequality*

$$D_N < \frac{2}{p} + \frac{p^{k/2}}{N}(\tau/\mu)^{1/2}\left(\frac{2}{\pi}\log\tau + \frac{2}{5} + \frac{N}{\tau}\right)\left(\frac{2}{\pi}\log p + \frac{2}{5}\right).$$

Proof. For g.c.d.$(b, p) = 1$ and any integer c, we have

$$\left|\sum_{n=0}^{\tau-1} e(by_n/p)e(cn/\tau)\right| \leqslant p^{k/2}(\tau/\mu)^{1/2}$$

according to [10, Theorem 1] (compare also with [10, Theorem 4]). Then, for $1 \leqslant N \leqslant \tau$ and g.c.d.$(b, p) = 1$, we get by the method of Lemma 3,

$$\begin{aligned}\left|\sum_{n=0}^{N-1} e(by_n/p)\right| &\leqslant \frac{1}{\tau}\sum_{c=1}^{\tau}\left|\sum_{y=0}^{N-1} e(-cy/\tau)\right|\left|\sum_{n=0}^{\tau-1} e(by_n/p)e(cn/\tau)\right| \\ &\leqslant \frac{1}{\tau}p^{k/2}(\tau/\mu)^{1/2}\left(\sum_{c=1}^{\tau-1}\left|\sum_{y=0}^{N-1} e(-cy/\tau)\right| + N\right) \\ &< p^{k/2}(\tau/\mu)^{1/2}\left(\frac{2}{\pi}\log\tau + \frac{2}{5} + \frac{N}{\tau}\right).\end{aligned}$$

The desired inequality follows now from Lemma 4.

The remarks following Theorem 7 are, mutatis mutandis, also applicable in the present situation. Theorem 8 suggests that those sequences $y_0, y_1, \ldots$ with a period considerably larger than $p^{k/2}$ seem to be useful as random number generators. This condition is, of course, satisfied for maximal period sequences modulo p.

5. **Lower Bounds.** In this section, we shall discuss the effectiveness of the discrepancy estimates established in this paper. It will turn out that the estimates are best possible apart from logarithmic factors. The results of this section are based on the following lemma.

LEMMA 11. *For any points $t_0, \ldots, t_{N-1}$ in $[0, 1)$ with discrepancy D_N, we have*

$$\left|\sum_{n=0}^{N-1} e(t_n)\right| \leqslant 4ND_N.$$

Proof. See [4, Chapter 2, Corollary 5.1].

The following theorem should be compared with the results in Theorem 1 and 4.

THEOREM 9. *Let m be a prime, let r be an integer, and let λ with* g.c.d.$(\lambda, m) = 1$

belong to an exponent μ modulo m with $\mu \geqslant (m-1)/2$ (e.g., λ a primitive root modulo m). Then there exists a sequence $y_0, y_1, \ldots$ in the least residue system modulo m with g.c.d.$(y_0, m) = 1$ *and $y_{n+1} \equiv \lambda y_n + r \pmod m$ for $n = 0, 1, \ldots$ such that the associated sequence $x_0, x_1, \ldots$ of pseudo-random numbers in $[0, 1]$ satisfies*

$$D_N(x_0, \ldots, x_{N-1}) > m^{1/2}/8N \tag{41}$$

for some integer N with $1 \leqslant N \leqslant \mu$.

Proof. The case $m = 2$ being trivial, we assume that m is an odd prime, and we set $N = (m-1)/2$. Then, with empty sums being interpreted as zero,

$$S = \sum_{b=1}^{m-1} \left| \sum_{n=0}^{N-1} e((b\lambda^n + (\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)r)/m) \right|^2$$

$$= \sum_{b=1}^{m-1} \sum_{h,j=0}^{N-1} e(b(\lambda^h - \lambda^j)/m)$$

$$\cdot\, e((\lambda^{h-1} + \lambda^{h-2} + \cdots + 1 - \lambda^{j-1} - \lambda^{j-2} - \cdots - 1)r/m)$$

$$= \sum_{h,j=0}^{N-1} e((\lambda^{h-1} + \lambda^{h-2} + \cdots + 1 - \lambda^{j-1} - \lambda^{j-2} - \cdots - 1)r/m)$$

$$\cdot \sum_{b=1}^{m-1} e(b(\lambda^h - \lambda^j)/m).$$

The inner sum is $m-1$ for $h = j$; for $h \neq j$, we have $\lambda^h - \lambda^j \not\equiv 0 \pmod m$, and so, the inner sum is -1. Therefore,

$$S = \frac{(m-1)^2}{2}$$

$$- \sum_{h,j=0;h\neq j}^{N-1} e((\lambda^{h-1} + \lambda^{h-2} + \cdots + 1 - \lambda^{j-1} - \lambda^{j-2} - \cdots - 1)r/m).$$

The sum occurring here is real and contains $N(N-1)$ terms. Therefore,

$$S \geqslant \frac{(m-1)^2}{2} - \frac{(m-1)(m-3)}{4} = \frac{m^2-1}{4}.$$

Recalling the definition of S, it follows that there exists an integer b_0, $1 \leqslant b_0 \leqslant m - 1$, with

$$\left| \sum_{n=0}^{N-1} e((b_0\lambda^n + (\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)r)/m) \right|^2 \geqslant \frac{m+1}{4} > \frac{m}{4}. \tag{42}$$

Now let $y_0, y_1, \ldots$ be the sequence in the least residue system modulo m determined by $y_0 = b_0$ and $y_{n+1} \equiv \lambda y_n + r \pmod m$ for $n = 0, 1, \ldots$. Then one shows by induction that $y_n \equiv b_0\lambda^n + (\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)r \pmod m$ for $n = 0, 1, \ldots$, and so (41) follows from (42) and Lemma 11.

We note that the number μ in Theorem 9 is also the period of $x_0, x_1, \ldots$ if $\lambda \not\equiv 1 \pmod{m}$ (which holds for $m \geqslant 5$) and $(\lambda - 1)y_0 + r \not\equiv 0 \pmod{m}$. The following theorem should be compared with the results in Theorem 3 and 6.

THEOREM 10. *Let $m = p^\alpha$, p prime, $\alpha \geqslant 2$; let r be an integer; and let λ with* g.c.d.$(\lambda, m) = 1$ *belong to the largest possible exponent μ modulo m (i.e., $\mu = \varphi(m)$ if p is odd or $m = 4$, and $\mu = 2^{\alpha-2}$ if $m = 2^\alpha$ with $\alpha \geqslant 3$). Then there exists a sequence $y_0, y_1, \ldots$ in the least residue system modulo m with* g.c.d.$(y_0, m) = 1$ *and $y_{n+1} \equiv \lambda y_n + r \pmod{m}$ for $n = 0, 1, \ldots$ such that, for some integer N with $1 \leqslant N \leqslant \mu$, the associated pseudo-random numbers $x_0, \ldots, x_{N-1}$ in $[0, 1]$ satisfy*

$$D_N(x_0, \ldots, x_{N-1}) \geqslant \frac{(p^2 - 1)^{1/2} m^{1/2}}{8pN} \quad \textit{if } p \textit{ is odd} \tag{43}$$

and

$$D_N(x_0, \ldots, x_{N-1}) \geqslant \frac{m^{1/2}}{8\sqrt{2N}} \quad \textit{if } p = 2. \tag{44}$$

Proof. For $m = 4$ and $m = 8$, this is shown by choosing $N = 1$. Thus, we may assume that p is odd or that $m = 2^\alpha$ with $\alpha \geqslant 4$. We set $N = q\mu/p$, where $q = 1$ if $p = 2$ and $q = (p - 1)/2$ if p is odd. We use asterisks to denote summations restricted to be over integers relatively prime to m. Then, with empty sums being interpreted as zero,

$$S = \sum_{b=0}^{m-1}{}^{*} \left| \sum_{n=0}^{N-1} e((b\lambda^n + (\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)r)/m) \right|^2$$

$$= \sum_{b=0}^{m-1}{}^{*} \sum_{h,j=0}^{N-1} e(b(\lambda^h - \lambda^j)/m)$$

$$\cdot e((\lambda^{h-1} + \lambda^{h-2} + \cdots + 1 - \lambda^{j-1} - \lambda^{j-2} - \cdots - 1)r/m)$$

$$= \sum_{h,j=0}^{N-1} e((\lambda^{h-1} + \lambda^{h-2} + \cdots + 1 - \lambda^{j-1} - \lambda^{j-2} - \cdots - 1)r/m)$$

$$\sum_{b=0}^{m-1}{}^{*} e(b(\lambda^h - \lambda^j)/m)$$

$$= N\varphi(m) + \sum_{\substack{h,j=0\\ h\neq j}}^{N-1} e((\lambda^{h-1} + \lambda^{h-2} + \cdots + 1 - \lambda^{j-1} - \lambda^{j-2} - \cdots - 1)r/m)$$

$$\cdot \sum_{b=0}^{m-1}{}^{*} e(b(\lambda^h - \lambda^j)/m)$$

$$\geqslant N\varphi(m) - \sum_{\substack{h,j=0\\ h\neq j}}^{N-1} \left| \sum_{b=0}^{m-1}{}^{*} e(b(\lambda^h - \lambda^j)/m) \right|.$$

The inner sum in the last expression is a Ramanujan sum with $\lambda^h - \lambda^j \not\equiv 0 \pmod{m}$. By the formula for Ramanujan sums mentioned in the proof of Lemma 5, only those sums with $\lambda^h \equiv \lambda^j \pmod{p^{\alpha-1}}$ will be nonzero, the value being $-m/p$ in this case.

Since λ belongs to the exponent μ/p modulo $p^{\alpha-1}$, the congruence $\lambda^h \equiv \lambda^j \pmod{p^{\alpha-1}}$ is equivalent to $h \equiv j \pmod{\mu/p}$. It follows that

$$S \geqslant N\varphi(m) - 2mT/p, \tag{45}$$

where T is the number of ordered pairs (h, j) with $0 \leqslant h < j \leqslant N - 1$ and $h \equiv j \pmod{\mu/p}$. For each s, $1 \leqslant s \leqslant q - 1$, we have $j - h = s\mu/p$ for the ordered pairs $(0, s\mu/p), (1, s\mu/p + 1), \ldots, (N - 1 - s\mu/p, N - 1)$. Therefore,

$$T = \sum_{s=1}^{q-1} \left(N - \frac{s\mu}{p}\right) = \frac{\mu}{p} \sum_{s=1}^{q-1} (q - s) = \frac{\mu}{p} \cdot \frac{q(q-1)}{2}.$$

Together with (45), we get

$$S \geqslant \frac{\mu}{p}\left(q\varphi(m) - \frac{m}{p}\, q(q-1)\right). \tag{46}$$

Now let $p = 2$. Then $S \geqslant \varphi(m)\mu/2$, and the definition of S implies that there exists a b_0 in the least residue system modulo m with g.c.d.$(b_0, m) = 1$ and

$$\left|\sum_{n=0}^{N-1} e((b_0\lambda^n + (\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)r)/m)\right|^2 \geqslant \frac{\mu}{2} = \frac{m}{8}. \tag{47}$$

Now let $y_0, y_1, \ldots$ be the sequence in the least residue system modulo m determined by $y_0 = b_0$ and $y_{n+1} \equiv \lambda y_n + r \pmod{m}$ for $n = 0, 1, \ldots$. Then one shows by induction that $y_n \equiv b_0\lambda^n + (\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)r \pmod{m}$ for $n = 0, 1, \ldots$, and so (44) follows from (47) and Lemma 11.

If p is odd, we use $q = (p-1)/2$ and $\mu = \varphi(m)$ to deduce from (46) that

$$\begin{aligned} S &\geqslant \frac{\varphi(m)}{p}\left(\frac{p-1}{2}\,\varphi(m) - \frac{m(p-1)(p-3)}{4p}\right) \\ &= \varphi(m)\frac{m}{4p^2}(2(p-1)^2 - (p-1)(p-3)) \\ &= \varphi(m)(p^2 - 1)m/4p^2. \end{aligned}$$

By the definition of S, there exists a b_0 in the least residue system modulo m with g.c.d.$(b_0, m) = 1$ and

$$\left|\sum_{n=0}^{N-1} e((b_0\lambda^n + (\lambda^{n-1} + \lambda^{n-2} + \cdots + 1)r)/m)\right|^2 \geqslant \frac{(p^2-1)m}{4p^2}$$

The proof is now completed in the same way as in the case $p = 2$.

If p is odd, then for the number λ from Theorem 10 we have $\rho = 0$ in Lemma 8, so that according to this lemma the number μ from Theorem 10 is equal to the period of $x_0, x_1, \ldots$ if and only if $(\lambda - 1)y_0 + r$ is not divisible by p. If $p = 2$, then $\rho = 1$ or 2, and according to Lemma 8 the number $N = \mu/2$ used in the proof of Theorem 10 for $m \geqslant 16$ is less than or equal to the period of $x_0, x_1, \ldots$ if and only if $\omega \leqslant \rho + 1$, where ω is the largest integer with $2^\omega | ((\lambda - 1)y_0 + r)$.

If one drops the condition g.c.d.$(y_0, m) = 1$ in Theorems 9 and 10, one gets analogous results by going through exactly the same method (which, in fact, becomes simpler if no restriction on y_0 is imposed). The resulting statements are, however, only of interest in the inhomogeneous case. Obviously, the method in the proof of Theorems 9 and 10 yields also results for any prescribed value of N with $1 \leqslant N \leqslant \mu$.

Finally, we shall discuss the inequality (38) in Theorem 7. Since $x_0, x_1, \ldots, x_{N-1}$ are rationals with denominator p, we clearly must have $D_N \geqslant 1/p$ (this remark applies also to Theorem 8), which shows that the main term $2/p$ in (38) is correct up to a constant. Furthermore, we have shown in [10, Theorem 5] that for every primitive polynomial modulo p of degree k there exists a corresponding maximal period sequence $y_0, y_1, \ldots$ modulo p and an integer N with $1 \leqslant N \leqslant p^k - 1$ such that

$$\left|\sum_{n=0}^{N-1} e(y_n/p)\right| > \frac{1}{2} p^{k/2}.$$

It follows then from Lemma 11 that for the associated pseudo-random numbers $x_0, x_1, \ldots, x_{N-1}$ we have

$$D_N > p^{k/2}/8N.$$

This shows that for small values of k the second term on the right-hand side of (38) is needed, at least up to logarithmic factors.

Added in Proof. The techniques in this paper can be extended to obtain results on the statistical independence of successive terms of sequences of linear congruential pseudo-random numbers. This is carried out in the author's paper "Pseudo-random numbers and optimal coefficients" to appear in *Advances in Math.*

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

1. U. DIETER, "Statistical interdependence of pseudo-random numbers generated by the linear congruential method," *Applications of Number Theory to Numerical Analysis* (Proc. Sympos., Univ. Montreal, Montreal, Que., 1971), Academic Press, New York, 1972, pp. 287–317. MR 50 #6105.

2. G. H. HARDY & E. M. WRIGHT, *An Introduction to the Theory of Numbers*, 4th ed., Clarendon Press, Oxford, 1960.

3. D. E. KNUTH, *The Art of Computer Programming.* Vol. 2: *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969. MR 44 #3531.

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

5. G. MARSAGLIA, "The structure of linear congruential sequences," *Applications of Number Theory to Numerical Analysis* (edited by S. K. Zaremba), Academic Press, New York, 1972, pp. 249–285.

6. H. G. MEIJER & H. NIEDERREITER, "Equirépartition et théorie des nombres premiers," *Colloque sur la répartition modulo un* (Marseille, 1974), Lecture Notes in Math., Vol. 475, Springer-Verlag, Berlin-Heidelberg-New York, 1975, pp. 104–112.

7. H. NIEDERREITER, "On the distribution of pseudo-random numbers generated by the linear congruential method," *Math. Comp.*, v. 26, 1972, pp. 793–795. MR 48 #5321.

8. H. NIEDERREITER, "On the distribution of pseudo-random numbers generated by the linear congruential method. II," *Math. Comp.*, v. 28, 1974, pp. 1117–1132.

9. H. NIEDERREITER, "Résultats nouveaux dans la théorie quantitative de l'équirépartition," *Colloque sur la répartition modulo un* (Marseille, 1974), Lecture Notes in Math., Vol. 475, Springer-Verlag, Berlin-Heidelberg-New York, 1975, pp. 132–154.

10. H. NIEDERREITER, "Some new exponential sums with applications to pseudo-random numbers," *Colloquium on Number Theory* (Debrecen, 1974), North-Holland, Amsterdam. (To appear.)

11. H. NIEDERREITER, "On the cycle structure of linear recurring sequences," *Math. Scand.*, v. 37. (To appear.)

12. 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. MR 49 #2642.

13. R. C. TAUSWORTHE, "Random numbers generated by linear recurrence modulo two," *Math. Comp.*, v. 19, 1965, pp. 201–209. MR 32 #1878.