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

By Harald Niederreiter

Abstract. The discrepancy of sequences of pseudo-random numbers generated by the linear congruential method is estimated, thereby improving a result of Jagerman. Applications to numerical integration are mentioned.

Let \( m \) be a modulus with primitive root \( \lambda \), and let \( y_0 \) be an integer in the least residue system modulo \( m \) with \( \gcd(y_0, m) = 1 \). We generate a sequence \( y_0, y_1, \ldots \) of integers in the least residue system modulo \( m \) by \( y_{j+1} \equiv \lambda y_j \pmod{m} \) for \( j \geq 0 \). The sequence \( x_0, x_1, \ldots \), defined by \( x_j = y_j/m \) for \( j \geq 0 \), is then a frequently employed sequence of pseudo-random numbers in the unit interval \([0, 1]\). Its elements \( x_j \) may also be described explicitly by \( x_j = \lfloor \lambda^j y_0/m \rfloor \) for \( j \geq 0 \), where \( \lfloor x \rfloor \) denotes the fractional part of the real number \( x \). The sequence \( x_0, x_1, \ldots \) has period \( Q = \varphi(m) \), where \( \varphi \) is Euler's totient function.

For a real number \( a \) with \( 0 \leq a \leq 1 \), let \( A(a) \) be the number of elements of the sequence \( x_0, x_1, \ldots, x_{Q-1} \) lying in the interval \([0, a]\). We define the discrepancy \( D = \sup_{0 \leq a \leq 1} |A(a)/Q - a| \) which measures the deviation from the uniform distribution. Jagerman [2] has shown that \( D \leq (4/\pi) ((3 \log m)/Q)^{1/2} \). His method is based on an estimate of the discrepancy in terms of certain trigonometric sums. In the present note, we shall show that a much simpler method yields a considerably sharper estimate for \( D \) (see Theorem 2). We prove also some related results.

For \( \alpha \) from above and a positive integer \( k \), let \( A^{(k)}(\alpha) \) be the number of rationals \( i/k, 1 \leq i \leq k, \gcd(i, k) = 1 \), lying in the interval \([0, \alpha]\).

Theorem 1. For any positive integer \( k \), we have

\[
D^{(k)} = \sup_{0 \leq a \leq 1} \left| \frac{A^{(k)}(\alpha)}{\varphi(k)} - \alpha \right| = O(k^{-\epsilon}) \quad \text{for every } \epsilon > 0.
\]

Proof. For an arbitrary positive integer \( r \), we consider the sequence of rationals \( 1/r, 2/r, \ldots, r/r \). There are exactly \( \lfloor r \alpha \rfloor \) elements of this sequence in the interval \([0, \alpha]\). We now count these elements by a second method. We write the rationals \( j/r, 1 \leq j \leq r \), in reduced form and then count, for each positive divisor \( d \) of \( r \), the resulting rationals with denominator \( d \) lying in \([0, \alpha]\). We thereby arrive at the identity

\[
(1) \quad \lfloor r \alpha \rfloor = \sum_{d \mid r} A^{(d)}(\alpha) \quad \text{for all } r \geq 1 \text{ and all } \alpha, 0 \leq \alpha \leq 1.
\]

Applying the Moebius inversion formula to (1), we obtain

Received January 6, 1972.

AMS 1970 subject classifications. Primary 65C10, 10F40; Secondary 65D30.

Key words and phrases. Pseudo-random numbers, discrepancy, numerical integration.

Copyright © 1972, American Mathematical Society
\[ A^{(k)}(\alpha) = \sum_{d | k} \mu(d) \left[ \frac{k}{d} \alpha \right] \text{ for all } k \geq 1 \text{ and all } \alpha, 0 \leq \alpha \leq 1. \]

Consequently, we have, for all \( \alpha \) with \( 0 \leq \alpha \leq 1 \),
\[
\left| \frac{A^{(k)}(\alpha)}{\phi(k)} - \alpha \right| = \left| \frac{1}{\phi(k)} \sum_{d | k} \mu(d) \frac{k}{d} \alpha - \frac{1}{\phi(k)} \sum_{d | k} \mu(d) \left[ \frac{k}{d} \alpha \right] - \alpha \right|,
\]
\[
= \left| \frac{1}{\phi(k)} \sum_{d | k} \mu(d) \left[ \frac{k}{d} \alpha \right] \right|.
\]

Therefore, \( D^{(k)} \leq \left( 1/\phi(k) \right) \sum_{d | k} |\mu(d)| = g(k) \). Now, \( g(k) \) is a multiplicative number-theoretic function. To prove that \( \lim_{k \to \infty} g(k)k^{-1-\epsilon} = 0 \), it will therefore suffice to show that \( \lim_{p \to \infty} g(p)p^{-1-\epsilon} = 0 \), where \( p' \) runs through all prime powers. But \( g(p)p^{-1-\epsilon} = 2p^{-\epsilon}(1 - 1/p)^{-1} \leq 4p^{-\epsilon} \), and we are done.

Let us now return to the sequence \( x_0, x_1, \ldots, x_{Q-1} \). Since there is a primitive root modulo \( m \), we must have \( m = 2, 4, p^s \), or \( 2p^s \), where \( p \) is an odd prime and \( s \geq 1 \). For \( m = 2 \) and \( 4 \), we readily get \( D = \frac{1}{2} \) and \( D = \frac{1}{4} \), respectively. For the remaining cases, we have the following estimates.

**Theorem 2.** If \( m = p^s \), then \( D \leq \frac{1}{Q} \). If \( m = 2p^s \), then \( D \leq \frac{2}{Q} \).

**Proof.** We note that the sequence \( x_0, x_1, \ldots, x_{Q-1} \) runs, in some order, through all the rationals \( i/Q \) with \( 1 \leq i \leq m \) and \( \gcd(i, m) = 1 \). Therefore, \( A(\alpha) = A^{(m)}(\alpha) \), and we can apply (2). For \( m = p^s \), we get, for all \( \alpha \) with \( 0 \leq \alpha \leq 1 \),
\[
\left| \frac{A(\alpha)}{Q} - \alpha \right| = \frac{1}{Q} \left\{ \max_{1 \leq \alpha \leq 1} \left\{ \frac{m}{p^s} \alpha \right\} \right\} < \frac{1}{Q}.
\]
For \( m = 2p^s \), we get, for all \( \alpha \) with \( 0 \leq \alpha \leq 1 \),
\[
\left| \frac{A(\alpha)}{Q} - \alpha \right| = \frac{1}{Q} \left\{ \max_{1 \leq \alpha \leq 1} \left\{ \frac{m}{2} \alpha \right\} - \left\{ \frac{m}{2p} \alpha \right\} + \left\{ \frac{m}{2p} \alpha \right\} \right\} < \frac{2}{Q}.
\]

It is well known (see for instance [4]) that the discrepancy \( D \) of any sequence in \([0, 1]\) with \( Q \) elements must satisfy \( D \geq \frac{1}{2Q} \). Therefore, no substantial improvement of Theorem 2 is possible. We refer to [1] for results on the distribution of pseudorandom numbers in the case \( m = 2^s \) with \( s \geq 3 \) (of course, \( \lambda \) is then not a primitive root any more).

Theorem 2 implies two error estimates for numerical integration based on the sequence \( x_0, x_1, \ldots, x_{Q-1} \). First, we apply Koksma's inequality [3] which states that, for any sequence \( a_0, a_1, \ldots, a_{Q-1} \) in \([0, 1]\) with discrepancy \( D_N \) and any integrand \( f \) with bounded variation \( V(f) \) on \([0, 1]\), one has
\[
\left| \frac{1}{N} \sum_{i=0}^{N-1} f(a_i) - \int_0^1 f(x) \, dx \right| \leq V(f)D_N.
\]
The notion of discrepancy is usually defined in terms of the counting functions relative to the half-open intervals \([0, \alpha) \), \( 0 < \alpha \leq 1 \). But it is easily seen that this is identical with our concept of discrepancy in which we used the counting functions relative to the closed intervals \([0, \alpha] \), \( 0 \leq \alpha \leq 1 \).

**Corollary 1.** Let \( f \) be a function with bounded variation \( V(f) \) in \([0, 1] \). Then
\[
\left| \frac{1}{Q} \sum_{i=0}^{Q-1} f(x_i) - \int_0^1 f(x) \, dx \right| \leq \frac{c}{Q} V(f),
\]
where \( c = \frac{1}{2} \) for \( m = 2 \) and \( 4 \), \( c = 1 \) for \( m = p^s \), and \( c = 2 \) for \( m = 2p^s \).
Finally, we apply an inequality given by the present author in [4]: If $a_0, a_1, \ldots, a_{N-1}$ is a sequence in $[0, 1]$ with discrepancy $D_N$ and $f$ is continuous in $[0, 1]$ with modulus of continuity $\omega$, then

$$\left| \frac{1}{N} \sum_{i=0}^{N-1} f(a_i) - \int_0^1 f(x) \, dx \right| \leq \omega(D_N).$$

For the convenience of the reader, we include the short proof. We may assume without loss of generality that $0 \leq a_0 \leq a_1 \leq \cdots \leq a_{N-1} \leq 1$. We know then from [5, Eq. (4)], [6, Theorem 1] that $D_N$ is also given by

$$D_N = \max_{i=0, \ldots, N-1} \max_{j=0, \ldots, N-1} \left| a_i - \frac{i}{N} \right| \left| a_i - \frac{i+1}{N} \right|.$$ 

Now,

$$\int_0^1 f(x) \, dx = \sum_{i=0}^{N-1} \frac{1}{N} \int_{i/N}^{(i+1)/N} f(x) \, dx = \sum_{i=0}^{N-1} \frac{1}{N} f(\xi_i) \text{ with } \frac{i}{N} < \xi_i < \frac{i+1}{N} \text{ for } 0 \leq i \leq N-1.$$

Therefore,

$$\frac{1}{N} \sum_{i=0}^{N-1} f(a_i) - \int_0^1 f(x) \, dx = \frac{1}{N} \sum_{i=0}^{N-1} (f(a_i) - f(\xi_i)).$$

But $|a_i - \xi_i| < \max(|a_i - i/N|, |a_i - (i+1)/N|) \leq D_N$ for $0 \leq i \leq N-1$, hence $|f(a_i) - f(\xi_i)| \leq \omega(D_N)$ for $0 \leq i \leq N-1$, and we are done.

Using the fact that $\omega$ is a nondecreasing function, we arrive at the following consequence.

**Corollary 2.** Let $f$ be a continuous function in $[0, 1]$ with modulus of continuity $\omega$. Then

$$\left| \frac{1}{Q} \sum_{i=0}^{Q-1} f(\xi_i) - \int_0^1 f(x) \, dx \right| \leq \omega \left( \frac{c}{Q} \right),$$

where $c$ has the same meaning as in Corollary 1.