# Calculations with Pseudo-Random Numbers*

FRANK STOCKMAL

*System Development Corporation, Santa Monica, California*

*Abstract.* Two pseudo-random number generators are considered, the multiplicative congruential method and the mixed congruential method. Some properties of the generated sequences are derived, and several algorithms are developed for the evaluation of $x_i = f(i)$ and $i = f^{-1}(x_i)$, where $x_i$ is the $i$th element of a pseudo-random number sequence.

## 1. *Introduction*

Many methods for generating pseudo-random numbers on computers by arithmetic procedures have been proposed and investigated, and some of these are currently in widespread use. All of the methods have in common the advantageous characteristic that the generated sequence of numbers can be exactly reproduced from the known initial value and generator parameters. Then with all other factors remaining (hopefully) constant, a computer run can be duplicated. However, situations may occur when we wish to take advantage of this characteristic of determinability without being prodigal with computer time. Two particular questions which can arise are: (1) what is the $i$th element of the generated sequence? (2) given a specific random number, where in the sequence did it occur? These problems may come up during the checkout of a generator or a Monte Carlo program, in the calculation of key values to be used as internal program checks, in reproducing a segment of a computer run, in examination of anomalous results, etc. Depending upon the particular generator and parameters involved, it may be possible to compute the desired function by shortcut methods, avoiding the brute-force reproduction of the sequence. This paper deals with such procedures for two types of generators, the multiplicative congruential and the mixed congruential methods.

The multiplicative congruential method is defined by the recurrence relationship

$$x_{i+1} \equiv \lambda x_i \pmod{M}, \tag{1.1}$$

where $x_0$, $\lambda$ and $M$ are integers. The mixed method takes the form

$$r_{i+1} \equiv \lambda r_i + c \pmod{M}, \tag{1.2}$$

where $r_0$, $\lambda$, $c$ and $M$ are integers. In usual practice, the choice of $r_0$ is largely arbitrary while $x_0$, $\lambda$ and $c$ are chosen prime to $M$. Selection of any of the latter parameters not prime to $M$ decreases the period of the sequence without apparent compensation. For a binary computer of word length $n$ bits, a convenient choice for $M$ is $2^n$. With this modulus, $\lambda$ for the multiplicative method has frequently been chosen [1–4] as the largest odd power of 5 satisfying $\lambda < 2^n$; common choices

* Received January, 1963.

[5–8] for the mixed method are $\lambda = 2^a \pm 1$, $a \geqq 2$. In the literature, increasing attention is being given to imposing constraints upon the parameters in order that the generated sequence satisfy certain statistical criteria. This subject is of no concern here; hence the treatment will be somewhat general. For the remainder of this paper it will be assumed that:

$$M = 2^n, \quad n \geqq 3; \tag{1.3}$$

$$3 \leqq \lambda \leqq 2^n - 3, \quad \text{and odd}; \tag{1.4}$$

$$1 \leqq c \leqq 2^n - 1, \quad \text{and odd}; \tag{1.5}$$

$$1 \leqq x_0 \leqq 2^n - 1, \quad \text{and odd}; \tag{1.6}$$

$$0 \leqq r_0 \leqq 2^n - 1. \tag{1.7}$$

## 2. *Periodicity*

*Notation.* The sequences generated by (1.1) and (1.2) will be represented by $\{x\}$ and $\{r\}$, with elements $x_i$ and $r_i$, respectively. The binary digits of a random number will be denoted by $d_k$, $0 \leqq k \leqq n-1$:

$$x_i\,, r_i = \sum_{k=0}^{n-1} d_k 2^k, \quad d_k = 0 \text{ or } 1.$$

The index of the sequence elements will be $i$. For $i \geqq 1$, in the assumed range $2^s \leqq i < 2^{s+1}$, $i$ will have the representations

$$i = \sum_{j=0}^{s} b_j 2^j, \quad b_j = 0 \text{ or } 1; \quad b_s \neq 0. \tag{2.1}$$

$$i = \sum_{j=0}^{s} e_j\,, \quad e_j = b_j 2^j. \tag{2.2}$$

The notation $x = y \pmod M$ will be used to indicate that $x$ is taken as the least non-negative residue of $y$, modulo $M$.

It will be convenient to define a function $\alpha$: for given integers $A \neq 0$ and $p$ (prime) $\geqq 2$, the function $\alpha_p(A)$ is defined to be the greatest integer $q$ such that $p^q$ divides $A$; and $\alpha_p(0) = \infty$. The following rather obvious relationships are stated without proof. For all integers $A$, $B$:

$$\alpha_p(A \cdot B) = \alpha_p(A) + \alpha_p(B); \tag{2.3}$$

$$\alpha_p(A/B) = \alpha_p(A) - \alpha_p(B), \text{ for } A/B \text{ an integer}; \tag{2.4}$$

$$\alpha_p(A) < \alpha_p(B) \Rightarrow \alpha_p(A + B) = \alpha_p(A); \tag{2.5}$$

$$\alpha_p(A) = \alpha_p(B) \Rightarrow \alpha_p(A + B) \geqq \alpha_p(A); \tag{2.6}$$

$$\alpha_2(A) = \alpha_2(B) \Rightarrow \alpha_2(A + B) \geqq 1 + \alpha_2(A); \tag{2.7}$$

$$0 < |A| < p^B \Rightarrow \alpha_p(A) < B. \tag{2.8}$$

Further mention of $\alpha$ will assume that $p = 2$. Given the assumptions (1.3) through (1.7), it can be shown that the sequences $\{x\}$ and $\{r\}$ are periodic, periodicity beginning with the starting value $x_0$ or $r_0$; and that the period $P$ is a function of $n$ and $\lambda$ only. The periods of the individual binary digits $d_k$ can be determined, as well as the sequence period. First, some identities are stated and some lemmas proved. Subsequent sections refer repeatedly to identities (2.9)–(2.11), which are derivable from (1.1) and (1.2).

$$x_i = x_0 \lambda^i \pmod{2^n} \tag{2.9}$$

$$r_i = r_0 \lambda^i + c \frac{\lambda^i - 1}{\lambda - 1} \pmod{2^n} \tag{2.10}$$

$$r_{j+k} = r_k \lambda^j + c \frac{\lambda^j - 1}{\lambda - 1} \pmod{2^n} \tag{2.11}$$

Lemma 1. *For $\lambda \equiv h \pmod 4, h = \pm 1$, let $\beta = \alpha(\lambda - h)$. Then $\alpha(\lambda^{2^z} - 1) = 1$ for $z = 0, h = -1$; and $\alpha(\lambda^{2^z} - 1) = z + \beta$ for $h = -1, \quad z \geqq 1$ and $h = 1$, $z \geqq 0$.*

Proof. The proof can be demonstrated by induction on $z$. By (2.5), $\alpha(\lambda^{2^z} - 1) > 1 \Rightarrow \alpha(\lambda^{2^z} + 1) = \alpha(2) = 1$, hence $\alpha(\lambda^{2^{z+1}} - 1) = 1 + \alpha(\lambda^{2^z} - 1)$. Details are left to the reader.

Lemma 2. *For a given positive integer $i$, let $q = \alpha(i)$. Then $\alpha(\lambda^i - 1) = \alpha(\lambda^{2^q} - 1)$ for all positive odd integers $\lambda$.*

Proof. Let $i = K2^q$, $K$ an odd integer. Then

$$\lambda^i - 1 = \lambda^{K2^q} - 1 = (\lambda^{2^q} - 1) \sum_{j=0}^{K-1} (\lambda^{2^q})^j;$$

$$\alpha(\lambda^i - 1) = \alpha(\lambda^{2^q} - 1) + \alpha\left(\sum_{j=0}^{K-1} (\lambda^{2^q})^j\right). \tag{2.12}$$

Since $\lambda$ is odd, $(\lambda^{2^q})^j$ is odd for $q \geqq 0$ and $j \geqq 0$. Since $K$ is odd, the sum in (2.12) is the sum of an odd number of odd integers, which is an odd integer. Then $\alpha(\Sigma) = 0$ and $\alpha(\lambda^i - 1) = \alpha(\lambda^{2^q} - 1)$. Q.E.D.

Theorem 1. *Given $\lambda$ and the integer $y$, $1 \leqq y \leqq n - \beta$, let $\epsilon = \alpha(\lambda^{2^{y-1}} - 1)$. The binary digit $d_\epsilon$ in the sequence $\{x\}$ has a period of $2^y$.*

Proof. Given the integers $n$, $\lambda$ and $x_0$ satisfying (1.3), (1.4) and (1.6) respectively; let $\beta$ be defined as in Lemma 1. For an integer $m$ in the range $\beta+1 \leqq m \leqq n$, let $\{x\}_m$ be the sequence of elements $x_{i,m}$ generated by

$$x_{i+1,m} = \lambda_m x_{i,m} \pmod{2^m}, \tag{2.13}$$

where $\lambda_m$ and $x_{0,m}$ are the least non-negative residues modulo $2^m$ of $\lambda$ and $x_0$ respectively. Assume the period of $\{x\}_m$ to be $P_m$ ; then $P_m$ is the least positive integer such that $x_{i+P_m,m} = x_{i,m}$, or by (2.9)

$$(x_{0,m}\lambda_m{}^i)(\lambda_m^{P_m} - 1) \equiv 0 \pmod{2^m}. \tag{2.14}$$

Since $x_{0,m}$ and $\lambda_m$ are odd, (2.14) will be satisfied if and only if $2^m$ divides $\lambda_m^{P_m} - 1$; that is, if and only if

$$\alpha(\lambda_m^{P_m} - 1) \geqq m. \tag{2.15}$$

Let $\alpha(P_m) = q$ and $P_m = K \cdot 2^q$, $K$ an odd integer. By Lemma 2, $\alpha(\lambda_m^{K2^q} - 1) = \alpha(\lambda_m^{2^q} - 1)$ for all odd positive integers $K$; then $K = 1$ for $P_m$ to be a minimum. Also, for all integers $m$ in the stated range, $\alpha(\lambda_m^{2^q} - 1) = \alpha(\lambda^{2^q} - 1)$. Then

$P_m = 2^q$, where $q$ is the least integer satisfying $\alpha(\lambda^{2^q} - 1) \geqq m$. Now for a given integer $y$, $1 \leqq y \leqq n - \beta$, let $\epsilon = \alpha(\lambda^{2^{y-1}} - 1)$. Setting aside for the moment the case of $y = 1$, the range of $\epsilon$ is given by Lemma 1: $\beta+1 \leqq \epsilon \leqq n-1$. Then we can let $m = \epsilon$ to obtain

$$\alpha(\lambda^{2^q} - 1) \geqq \alpha(\lambda^{2^{y-1}} - 1). \tag{2.16}$$

Again by Lemma 1, the function $\alpha(\lambda^{2^q} - 1)$ is strictly increasing with $q$ for fixed $\lambda$; then the least integer $q$ satisfying (2.16) is $y-1$, and $P_\epsilon = 2^{y-1}$. Using the same rationale, we can obtain $P_{\epsilon+1} = 2^y$. (An incidental result can be obtained at this point by taking $y = n-\beta+1$. Then $\epsilon = n$ and $P_n$, the period of the sequence $\{x\}$, is $2^{n-\beta}$. This result appears in [1] and [9].)

An element generated by (1.1) or (2.13) is defined as the least non-negative residue with respect to the given modulus. It follows that $x_{i,\epsilon}$ is the least non-negative residue of $x_{i,\epsilon+1}$ (mod $2^\epsilon$) and $x_{i,\epsilon+1} = x_{i,\epsilon} + d_\epsilon 2^\epsilon$. It also follows that all digits $d_k$, $0 \leqq k \leqq \epsilon$, have the same value in $x_{i,n}$ as in $x_{i,\epsilon+1}$, hence the same period in $\{x\}$ as in $\{x\}_{\epsilon+1}$. Letting $S_\epsilon$ be the period of $d_\epsilon$ (which is the same as the period of $d_\epsilon 2^\epsilon$), then $P_{\epsilon+1}$ is the least common multiple of $P_\epsilon$ and $S_\epsilon$:

$$2^y = \text{lcm}\,(2^{y-1}, S_\epsilon). \tag{2.17}$$

Equation (2.17) has the unique solution $S_\epsilon = 2^y$, which proves the theorem for $y \neq 1$. For $y = 1$, the solution to (2.15) can be obtained by inspection. For $\lambda \equiv 1$ and $-1$ (mod 4), $\epsilon = \beta, 1$ and $\lambda_{\epsilon+1} = 2^\beta + 1, 2$ respectively; $P_{\epsilon+1} = 2$, $\lambda_\epsilon = 1$, $P_\epsilon = 1$ and $S_\epsilon = 2$. Q.E.D.

THEOREM 2. *Given $\lambda$ and the integer $y$, where $1 \leqq y \leqq n$ for $\lambda \equiv 1$ (mod 4) and $1 \leqq y \leqq n+1-\beta$ for $\lambda \equiv -1$ (mod 4); let $\epsilon = \alpha(\lambda^{2^{y-1}} - 1) - \alpha(\lambda - 1)$. Then the binary digit $d_\epsilon$ in the sequence $\{r\}$ has a period of $2^y$.*

The proof for Theorem 2 is basically the same as for Theorem 1; details are omitted. The bit characteristics which can be inferred from these theorems are displayed in Table 1.

## 3. *Determination of $x_i$*

The two algorithms described in this section can be used to determine $x_i$, given index $i \geqq 1$. The first of these uses a precomputed table and is suitable for desk calculation. The second algorithm requires no table and is convenient for use as a computer subroutine.

Assume $i$ in the range of $2^s \leqq i < 2^{s+1}$; then equation (2.9) can be put into the form

$$x_i = x_0 \prod_{j=0}^{s} (\lambda)^{e_j} \pmod{2^n}. \tag{3.1}$$

Then $x_i$ can be constructed using a table of $\lambda^{2^z}$ (mod $2^n$), $0 \leqq z \leqq n-\beta-1$, such as Table 2 in the Appendix.

TABLE 1. CHARACTERISTICS OF THE BINARY DIGITS $d_k$ IN THE SEQUENCES $\{x\}$ AND $\{r\}$

<table>
<tr><th>$\lambda$<br>($\beta \geqq 2$; $K$ odd)</th><th>Period of Sequence</th><th>$d_k$<br>$n-1 \geqq k \geqq \beta+1$</th><th>$d_\beta$</th><th>$d_k$<br>$\beta-1 \geqq k \geqq 2$</th><th>$d_1$</th><th>$d_0$</th></tr>
<tr><td>Multiplicative method<br>$\lambda = K \cdot 2^\beta + 1$</td><td>$2^{n-\beta}$</td><td colspan="2">period $= 2^{k+1-\beta}$</td><td colspan="2">*</td><td>1</td></tr>
<tr><td>Multiplicative method<br>$\lambda = K \cdot 2^\beta - 1$</td><td>$2^{n-\beta}$</td><td>period $= 2^{k+1-\beta}$</td><td>*</td><td>†</td><td>period $= 2$</td><td>1</td></tr>
<tr><td>Mixed method<br>$\lambda = K \cdot 2^\beta + 1$</td><td>$2^n$</td><td colspan="5">period $= 2^{k+1}$</td></tr>
<tr><td>Mixed method<br>$\lambda = K \cdot 2^\beta - 1$</td><td>$2^{n+1-\beta}$</td><td colspan="2">period $= 2^{k+2-\beta}$</td><td colspan="2">†</td><td>period $= 2$</td></tr>
</table>

* Digit has the same value as the corresponding digit of $x_0$.

† Digit has a constant value or a period of 2, function of the low order bits of $x_0$, or $r_0$ and $c$.

PROCEDURE A1.

(1) Partition $i$ into parts $e_j$, defined by (2.1) and (2.2), ignoring parts equal to 0 and discarding parts greater than or equal to the period of the sequence;

(2) select corresponding values of $\lambda^{e_j}$ (mod $2^n$) from table;

(3) form the product $x_0 \Pi_j \lambda^{e_j} = x_i$.

A similar procedure can be performed without the use of tables, requiring inputs of $\lambda$, $x_0$ and $i$ (and $n$).

PROCEDURE A2.

(1) Set $y' = 0$, $\Pi = x_0$, $i' = i$, $\gamma = \lambda$;

(2) if $i' = 0$: iteration is completed and $\Pi = x_i$; if $i' \neq 0$: form $y = \alpha(i')$;

(3) if $y' = y$: replace $\Pi$ by $\gamma\Pi$ (mod $2^n$), $i'$ by $i' - 2^y$, and repeat from step (2); if $y' \neq y$: replace $\gamma$ by $\gamma^2$ (mod $2^n$), $y'$ by $y' + 1$, and repeat step (3).

The latter algorithm is valid for $i \geqq 0$. For $i$ in the range $2^s \leqq i < 2^{s+1}$, the average number of multiplications required is $\approx (s/2) + 1$ for procedure A1, $(3s/2) + 1$ for A2.

## 4. *Determination of $r_i$*

The particular method best suited to computation of $r_i$ depends upon the parameters involved. No exhaustive treatment will be attempted here but a few possibilities will be mentioned. For desk calculation, it is usually advantageous to reduce $i$ to the least non-negative residue, modulo the period of the sequence.

Greenberger [5] suggests that a choice of $\lambda$ approximately equal to, but less than $2^{n/2}$ is good in several respects. If we choose the common form $\lambda = 2^a + 1$

and restrict $a$ to the range $n/3 \leqq a < n/2$, then $r_i$ is expressible as

$$r_i = \sum_{k=0}^{2} 2^{ak} \left[ r_0 \binom{i}{k} + c \binom{i}{k+1} \right] \pmod{2^n},$$

which requires little computation. For $\lambda = 2^a - 1$ and $n/3 \leqq a < n/2$,

$$r_i = \xi + (-1)^i \left( r_0 - \frac{c}{2} \right) \sum_{k=0}^{2} \binom{i}{k} (-2^a)^k \pmod{2^n},$$

where $\xi = (c/4)(2^{2a}i + 1)$ for $i$ even; $\xi = (c/2)[2^a + 1 - 2^{2a-1}(i - 1)]$ for $i$ odd.

In seeking a general method applicable for any $\lambda$, $c$ and $r_0$, analogous to algorithm A1, we encounter an obstacle not present in the multiplicative generator. The counterpart of equation (3.1) is the following, obtained from (2.10):

$$r_i = r_0 + [r_0(\lambda - 1) + c] \left\{ \frac{-1 + \prod_{j=0}^{s} \lambda^{e_j}}{\lambda - 1} \right\} \pmod{2^n}. \tag{4.1}$$

As it stands, this formulation requires that most of the computation be carried out modulo $2^n(\lambda - 1)$, which can be highly undesirable. However, the last equation can be modified to allow the computation to be performed modulo $2^n$, at the expense of additional operations. The expression in braces of (4.1) can be expanded:

$$\frac{-1 + \prod_{j=0}^{s} \lambda^{e_j}}{\lambda - 1} = \frac{(\lambda^{e_0} - 1) \prod_{j=1}^{s} \lambda^{e_j}}{\lambda - 1} + \frac{-1 + \prod_{j=1}^{s} \lambda^{e_j}}{\lambda - 1}.$$

Continuing the expansion in this manner, we can obtain

$$r_i = r_0 + [r_0(\lambda - 1) + c] \sum_{k=0}^{s} \frac{\lambda^{e_k} - 1}{\lambda - 1} \prod_{j=k+1}^{s} \lambda^{e_j} \pmod{2^n},$$

where $\prod_{j=s+1}^{s} \lambda^{e_j}$ is defined equal to 1. The factor $(\lambda^{e_k} - 1)/(\lambda - 1)$ can be generated modulo $2^n$ (see final section, *Table Construction*) and $r_i$ can be calculated by means of tables of $\lambda^{2^z} \pmod{2^n}$ and $(\lambda^{2^z} - 1)/(\lambda - 1) \pmod{2^n}$, $0 \leqq z \leqq n - 1$, such as Tables 2 and 3.

Procedure A3.

(1) Partition $i$ into parts $e_j$, defined by (2.1) and (2.2), ignoring parts equal to 0 and discarding parts greater than or equal to the period of the sequence; select any $e_j$; set $i' = i - e_j$; set $\Sigma = (\lambda^{e_j} - 1)/(\lambda - 1) \pmod{2^n}$ (from table);
(2) if $i' = 0$, proceed to step (4); if $i' \neq 0$, proceed to step (3);
(3) select any remaining $e_j$ and obtain $\lambda^{e_j} \pmod{2^n}$ and $(\lambda^{e_j} - 1)/(\lambda - 1) \pmod{2^n}$ from tables; replace $\Sigma$ by $(\lambda^{e_j} - 1)/(\lambda - 1) + \lambda^{e_j}\Sigma \pmod{2^n}$, replace $i'$ by $i' - e_j$, and repeat from step (2);
(4) form $r_0 + [r_0(\lambda - 1) + c]\Sigma \pmod{2^n} = r_i$.

At the expense of additional multiplications, the procedure can be performed without tables.

PROCEDURE A4.

*Explanatory Note.* A4 operates upon an argument $i$, using parameters $\lambda$, $c$ and $r_0$ (and $n$). The algorithm variables have the following meaning: at the point of re-entry of step (2) from step (3), $e_y$ is the most recently determined $e_j$, $\delta \equiv \lambda^{2^y} \pmod{2^n}$, $\gamma = (\lambda^{2^y} - 1)/(\lambda - 1) \pmod{2^n}$, $\Sigma = [1/(\lambda - 1)][-1 + \Pi_{j=0}^{y} \lambda^{e_j}] \pmod{2^n}$, and $i' = i - \Sigma_{j=0}^{y} e_j$.

(1) Set $\Sigma = 0$, $\delta = \lambda$, $\gamma = 1$, $i' = i$, $y' = 0$;
(2) if $i' = 0$, proceed to step (4); if $i' \neq 0$, form $y = \alpha(i')$;
(3) if $y' = y$, replace $\Sigma$ by $\gamma + \delta\Sigma \pmod{2^n}$, $i'$ by $i' - 2^y$, and repeat from step (2); if $y' \neq y$, replace $\gamma$ by $\gamma(\delta + 1) \pmod{2^n}$, $\delta$ by $\delta^2 \pmod{2^n}$, $y'$ by $y' + 1$, and repeat step (3);
(4) form $r_0 + [r_0(\lambda - 1) + c]\,\Sigma \pmod{2^n} = r_i$.

This algorithm is valid for $i \geqq 0$. For $i$ in the range $2^s \leqq i < 2^{s+1}$, A3 requires an average of approximately $s+1$ table references and $s/2 + 2$ multiplications; A4, an average of approximately $5s/2 + 3$ multiplications.

## 5. *Determination of Index, Multiplicative Generator*

The algorithm for determination of $i$, given $x_i$, is based upon the recognizability of $\alpha(i)$ through inspection of the bits of $x_i - x_0$. The least nonzero $e_j$ component of $i$ can be determined by application of Theorem 3.

THEOREM 3. *If $x_i = x_0$, then $i \equiv 0 \pmod P$, where $P$ is the period of the sequence $\{x\}$; if $x_i \neq x_0$, and $\alpha(x_i - x_0) = w$, then $\alpha(i) = y$, where $y$ is the solution of $\alpha(\lambda^{2^y} - 1) = w$.*

PROOF. The sequence $\{x\}$ has been shown to be periodic, periodicity beginning with the initial element $x_0$. The period $P$ is the least positive integer such that

$$x_{j+P} = x_j, \quad \text{for all } j \geqq 0; \tag{5.1}$$

which implies that $x_{j+k} \neq x_j$ for $1 \leqq k \leqq P-1$. Repeated application of (5.1) yields $x_{j+KP} = x_j$, for $K, j \geqq 0$. Given the integer $i \not\equiv 0 \pmod P$, let $k$ be the least non-negative residue of $i \pmod P$. Then $1 \leqq k \leqq P-1$ and $x_i = x_k \neq x_0$; or $i \not\equiv 0 \pmod P \Rightarrow x_i \neq x_0$, which proves the first part of the theorem.

Now assume that $x_i \neq x_0$, and $\alpha(x_i - x_0) = w$. From (2.9),

$$x_i - x_0 \equiv x_0(\lambda^i - 1) \pmod{2^n},$$

$$\alpha[x_i - x_0 + 2^n K] = \alpha[x_0(\lambda^i - 1)], \tag{5.2}$$

where $K$ is an integer. Since $0 < x_i$, $x_0 < 2^n$, then $0 < |x_i - x_0| < 2^n$ and $\alpha(x_i - x_0) < n$, by (2.8). Also $\alpha(2^n K) \geqq n$; then by (2.5) the left-hand member of (5.2) is $\alpha(x_i - x_0) = w$. Let $\alpha(i) = y$. By Lemma 2, the right-hand member of (5.2) is $\alpha(\lambda^{2^y} - 1)$, $x_0$ being odd; or $\alpha(\lambda^{2^y} - 1) = w$. Q.E.D.

For a given $\lambda$ and $w$, the solution of $\alpha(\lambda^{2^y} - 1) = w$ in $y$ is given by Lemma 1:

$$y = w - \beta \qquad \text{for } \lambda \equiv 1 \pmod 4; \tag{5.3}$$

$$y = 0 \qquad \text{if } w = 1 \tag{5.4}$$

$$y = w - \beta \text{ if } w \neq 1 \quad \text{for } \lambda \equiv -1 \pmod 4. \tag{5.5}$$

Having determined the least nonzero $e_j$ to be $e_y$, the next larger $e_j$ is determinable by removing the factor of $\lambda^{2^y}$ from the product $x_i = x_0 \Pi_{j=y}^{s} \lambda^{e_j} \pmod{2^n}$. This can be effected by multiplying $x_i$ by the appropriate integer $Q_y$, defined by $Q_y\lambda^{2^y} \equiv 1 \pmod{2^n}$. For $\beta < n$, which is satisfied by (1.4), Lemma 1 implies that $\alpha(\lambda^{2^{n-\beta}} - 1) = n$, and $\lambda^{2^{n-\beta}} \equiv 1 \pmod{2^n}$. Then $Q_y \equiv \lambda^{K-2^y} \pmod{2^n}$, where $K$ is any integral multiple of $2^{n-\beta}$, $\geqq 2^y$. For convenience, $Q_y$ will be expressed as

$$Q_y = \lambda^{2^n-2^y} \pmod{2^n}. \tag{5.6}$$

After multiplication by $Q_y$, the process can be repeated to determine the next larger $e_j$; the iteration continues until the entire composition of $i$ is known. The algorithm can take the form of A5, utilizing a table of $\lambda^{2^n-2^z} \pmod{2^n}$, $0 \leqq z \leqq n-\beta-1$ (such as Table 4); or A6, with no table required.

PROCEDURE A5.

(1) Set $\Sigma = 0$, $\gamma = x_i$;
(2) if $\gamma = x_0$, iteration is completed and $\Sigma = i$; if $\gamma \neq x_0$, determine $w = \alpha(\gamma - x_0)$, determine $y$ by means of one of the relationships (5.3)–(5.5);
(3) obtain $Q_y$ from table; replace $\gamma$ by $\gamma Q_y \pmod{2^n}$, $\Sigma$ by $2^y + \Sigma$; repeat from step (2).

PROCEDURE A6.

*Explanatory Note.* A6 operates upon any argument $x_i$ generated by (1.1) with $M = 2^n$, employing parameters $\lambda$ and $x_0$ (and $n$). Step (1) is a subalgorithm which solves the congruence $\lambda Q_0 \equiv 1 \pmod{2^n}$ for $Q_0$. The algorithm variables denote the following: at the point of re-entry of step (5) from step (6), $e_y$ is the most recently determined nonzero $e_j$, $Q = \lambda^{2^n-2^y} \pmod{2^n}$, $\Sigma = \Sigma_{j=0}^{y} e_j$, and $\gamma = x_0 \Pi_{j=y+1}^{s} \lambda^{e_j} \pmod{2^n}$.

(1) Compute $Q_0$ as follows:
  (1.1) set $A = 1$, $B = \lambda - 1$;
  (1.2) form $u = \alpha(B)$; replace $A$ by $A + 2^u$, $B$ by $B + \lambda \cdot 2^u \pmod{2^n}$;
  (1.3) if $B \equiv 0 \pmod{2^n}$, proceed to step (2); if $B \not\equiv 0$, repeat from step (1.2);
(2) set $Q = A$, $y' = 0$; if $\lambda \equiv 3 \pmod 4$, compute $\beta = \alpha(\lambda + 1)$ and proceed to step (3); if $\lambda \equiv 1 \pmod 4$, compute $\beta = \alpha(\lambda - 1)$, proceed to step (4);
(3) if $x_i - x_0 \equiv 2 \pmod 4$, set $\Sigma = 1$, $\gamma \equiv Qx_i \pmod{2^n}$, go to step (5); if $x_i - x_0 \not\equiv 2 \pmod 4$, go to step (4);
(4) set $\Sigma = 0, \gamma = x_i$;
(5) if $\gamma = x_0$, iteration is completed and $\Sigma = i$; if $\gamma \neq x_0$, form $y = \alpha(\gamma - x_0) - \beta$, replace $\Sigma$ by $2^y + \Sigma$;
(6) if $y' = y$, replace $\gamma$ by $\gamma Q \pmod{2^n}$ and repeat from step (5); if $y' \neq y$, replace $Q$ by $Q^2 \pmod{2^n}$, $y'$ by $y' + 1$, and repeat step (6).

For $i$ in the range $2^s \leqq i < 2^{s+1}$, A5 requires an average $\approx(s/2) + 1$ multiplications, a maximum of $s+1$, and a like number of table references. Exclusive of the computation of $Q_0$, A6 requires an average $\approx(3s/2) + 1$ multiplications, a maximum of $2s+1$.

## 6. *Determination of Index, Mixed Generator*

As in the multiplicative method, the procedure for determination of the index $i$ for the mixed method is based upon the relationship of $\alpha(i)$ and $\alpha(r_i - r_0)$.

THEOREM 4. *If $r_i = r_0$, then $i \equiv 0 \pmod P$, where $P$ is the period of the sequence $\{r\}$. If $r_i \neq r_0$ and $\alpha(r_i - r_0) = w$, then $\alpha(i) = y$, where $y$ is the solution of $\alpha(\lambda^{2^y} - 1) = w + \alpha(\lambda - 1)$.*

PROOF. The proof of the first part of Theorem 4 is identical to the proof for the first part of Theorem 3. Now take $r_i \neq r_0$, and let $\alpha(r_i - r_0) = w$. From (2.10),

$$r_i - r_0 \equiv r_0(\lambda^i - 1) + \frac{c(\lambda^i - 1)}{\lambda - 1} \pmod{2^n}$$

$$\alpha[r_i - r_0 + K2^n] = \alpha\left[r_0(\lambda^i - 1) + \frac{c(\lambda^i - 1)}{\lambda - 1}\right], \tag{6.1}$$

where $K$ is an integer. Since $0 \leqq r_i,\ r_0 < 2^n$ and $r_i \neq r_0$, then $0 < |r_i - r_0| < 2^n$ and $\alpha(r_i - r_0) < n$, by (2.8). Also, $\alpha(K \cdot 2^n) \geqq n$; then by (2.5), $\alpha(r_i - r_0 + K \cdot 2^n) = \alpha(r_i - r_0) = w$. With $\lambda$ and $c$ odd, $\alpha(c) = 0$, $\alpha(\lambda - 1) \geqq 1$, and

$$\alpha\left\{\frac{c(\lambda^i - 1)}{\lambda - 1}\right\} = \alpha(c) + \alpha(\lambda^i - 1) - \alpha(\lambda - 1) < \alpha(\lambda^i - 1);$$

whereas $\alpha[r_0(\lambda^i - 1)] \geqq \alpha(\lambda^i - 1)$. By (2.5), equation (6.1) becomes $w = \alpha(\lambda^i - 1) - \alpha(\lambda - 1)$. Let $\alpha(i) = y$. By Lemma 2, $\alpha(\lambda^i - 1) = \alpha(\lambda^{2^y} - 1)$ and

$$\alpha(\lambda^{2^y} - 1) = w + \alpha(\lambda - 1). \qquad \text{Q.E.D.} \tag{6.2}$$

The solution in $y$ to (6.2) is given by Lemma 1 as:

$$y = w \qquad \text{for } \lambda \equiv 1 \pmod 4; \tag{6.3}$$

$$y = 0 \qquad \text{if } w = 0 \tag{6.4}$$

$$y = w - \beta + 1 \text{ if } w \geqq 1 \quad \text{for } \lambda \equiv -1 \pmod 4. \tag{6.5}$$

Having determined the least nonzero $e_j = 2^y$, the next larger $e_j$ is determinable in the same fashion after $i$ is depressed by $2^y$, as follows. Let $i' = i - 2^y$, and apply identity (2.11):

$$r_i = r_{(i'+2^y)} = \lambda^{2^y} r_{i'} + \frac{c(\lambda^{2^y} - 1)}{\lambda - 1} \pmod{2^n}$$

$$r_{i'} = Q_y\left\{r_i - \frac{c(\lambda^{2^y} - 1)}{\lambda - 1}\right\} \pmod{2^n},$$

where $Q_y$ is defined by (5.6). Using preconstructed tables of $(\lambda^{2^z} - 1)/(\lambda - 1) \pmod{2^n}$ and $\lambda^{2^n - 2^z} \pmod{2^n}$, $0 \leqq z \leqq n - 1$ (such as Tables 3 and 4), $r_{i'}$ can be calculated and the next larger $e_j$ determined, the process being repeated until the entire composition of $i$ is revealed. The procedure can be stated as A7 or A8, the latter generating the required table values.

PROCEDURE A7.

(1) Set $\Sigma = 0$, $\gamma = r_i$;
(2) if $\gamma = r_0$, iteration is completed and $\Sigma = i$; if $\gamma \neq r_0$, determine $w = \alpha(\gamma - r_0)$; determine $y$ by one of the relationships (6.3)–(6.5); replace $\Sigma$ by $2^y + \Sigma$;

(3) obtain values of $\lambda^{2^n-2^y}$ (mod $2^n$) and $(\lambda^{2^y} - 1)/(\lambda - 1)$ (mod $2^n$) from tables; replace $\gamma$ by $(\lambda^{2^n-2^y})[\gamma - c(\lambda^{2^y} - 1)/(\lambda - 1)]$ (mod $2^n$); repeat from step (2).

PROCEDURE A8.

*Explanatory Note.* A8 operates upon any argument $r_i$ generated by (1.2) with $M = 2^n$, using parameters $\lambda$, $c$ and $r_0$ (and $n$). Step (1) solves the congruence $\lambda Q_0 \equiv 1$ (mod $2^n$) for $Q_0$. The internal variables denote the following: at the point of re-entry of step (5) from step (6), $e_y$ is the most recently determined nonzero $e_j$, $Q = \lambda^{2^n-2^y}$ (mod $2^n$), $\Sigma = \Sigma_{j=0}^{y} e_j$, $T = (\lambda^{2^y} - 1)(\lambda - 1)$ (mod $2^n$), and $\gamma = r_{i'}$, where $i' = i - \Sigma_{y=0}\, e_j$. The difference between (6.3) and (6.5) is compensated for by $\Delta$.

(1) Compute $Q_0$ as follows:
 (1.1) set $A = 1$, $B = \lambda - 1$;
 (1.2) form $u = \alpha(B)$; replace $A$ by $A + 2^u$, $B$ by $B + \lambda \cdot 2^u$ (mod $2^n$);
 (1.3) if $B \equiv 0$ (mod $2^n$), go to step (2); if $B \not\equiv 0$ (mod $2^n$), repeat from step (1.2);
(2) set $Q = A$, $T = 1$, $y' = 0$; if $\lambda \equiv 3$ (mod 4), compute $\Delta = \alpha(\lambda + 1) - 1$, go to step (3); if $\lambda \equiv 1$ (mod 4), set $\Delta = 0$, to to step (4);
(3) if $r_i - r_0 \equiv 0$ (mod 2), go to step (4); if $r_i - r_0 \equiv 1$ (mod 2), set $\Sigma = 1$, $\gamma \equiv Q(r_i - c)$ (mod $2^n$), go to step (5);
(4) set $\Sigma = 0$, $\gamma = r_i$;
(5) if $\gamma = r_0$, iteration is completed and $\Sigma = i$; if $\gamma \neq r_0$, compute $y = \alpha(\gamma - r_0) - \Delta$, replace $\Sigma$ by $2^y + \Sigma$;
(6) if $y' = y$, replace $\gamma$ by $Q(\gamma - cT)$ (mod $2^n$) and repeat from step (5); if $y' \neq y$, replace $Q$ by $Q^2$ (mod $2^n$), $T$ by $T[T(\lambda - 1) + 2]$ (mod $2^n$), $y'$ by $y' + 1$, and repeat step (6).

For $i$ in the range $2^s \leqq i < 2^{s+1}$, A7 involves a maximum of $2s+2$ table references and $2s+2$ multiplications; the average for each being $\approx s+2$. Exclusive of the computation of $Q_0$, the average number of multiplications required by A8 is $\approx 4s+2$; the maximum, $5s+2$. Of course, procedures A5 through A8 can only produce a number which is representative of a residue class modulo $P$, the period of the sequence; the number being the least non-negative residue of $i$ (mod $P$).

## 7. *Table Construction*

The required tables can be generated recursively as follows. Let $z$ be the argument and $f_2$, $f_3$ and $f_4$ the functions of Tables 2, 3 and 4 respectively. For Table 2, $f_2(z) = \lambda^{2^z}$ (mod $2^n$), $0 \leqq z \leqq n - 1$; then $f_2(0) = \lambda$ and $f_2(z + 1) = [f_2(z)]^2$ (mod $2^n$).

For Table 3, $f_3(z) = (\lambda^{2^z} - 1)/(\lambda - 1)$ (mod $2^n$), $0 \leqq z \leqq n - 1$. $f_3(0) = 1$ and $f_3(z + 1) = [f_3(z)][2 + (\lambda - 1)f_3(z)]$ (mod $2^n$). An alternative is to use Table 2 to reduce the amount of computation: $f_3(z + 1) = [1 + f_2(z)][f_3(z)]$ (mod $2^n$).

For Table 4, $f_4(z) = \lambda^{2^n-2^z}$ (mod $2^n$), $0 \leqq z \leqq n-1$. Generation can be performed with decreasing $z$, using Table 2: $f_4(z) = 1$ for $n-\beta \leqq z \leqq n-1$ and $f_4(z) = [f_4(z + 1)][f_2(z)]$ (mod $2^n$) for $0 \leqq z \leqq n-\beta-1$. Generating with increasing $z$, $f_4(z + 1) = [f_4(z)]^2$ (mod $2^n$), and $f_4(0)$ is the solution of $\lambda f_4(0) \equiv 1$ (mod $2^n$). $f_4(0)$ can be computed from $f_4(0) = \Pi_{z=0}^{n-\beta-1} f_2(z)$ (mod $2^n$), or by the algorithm which comprises step (1) of procedures A6 and A8.

## APPENDIX

Tables are based on $\lambda = 2^7 + 1$, $n = 35$. Argument is given in decimal form, function in octal form.

### TABLE 2

| $z$ | $\lambda^{2^z} \pmod{2^{35}}$ | | | |
|---|---|---|---|---|
| 0 | 000 | 000 | 000 | 201 |
| 1 | 000 | 000 | 040 | 401 |
| 2 | 002 | 040 | 301 | 001 |
| 3 | 214 | 701 | 602 | 001 |
| 4 | 100 | 607 | 404 | 001 |
| 5 | 075 | 437 | 010 | 001 |
| 6 | 153 | 176 | 020 | 001 |
| 7 | 226 | 774 | 040 | 001 |
| 8 | 057 | 770 | 100 | 001 |
| 9 | 147 | 760 | 200 | 001 |
| 10 | 357 | 740 | 400 | 001 |
| 11 | 137 | 701 | 000 | 001 |
| 12 | 277 | 602 | 000 | 001 |
| 13 | 177 | 404 | 000 | 001 |
| 14 | 377 | 010 | 000 | 001 |
| 15 | 376 | 020 | 000 | 001 |
| 16 | 374 | 040 | 000 | 001 |
| 17 | 370 | 100 | 000 | 001 |
| 18 | 360 | 200 | 000 | 001 |
| 19 | 340 | 400 | 000 | 001 |
| 20 | 301 | 000 | 000 | 001 |
| 21 | 202 | 000 | 000 | 001 |
| 22 | 004 | 000 | 000 | 001 |
| 23 | 010 | 000 | 000 | 001 |
| 24 | 020 | 000 | 000 | 001 |
| 25 | 040 | 000 | 000 | 001 |
| 26 | 100 | 000 | 000 | 001 |
| 27 | 200 | 000 | 000 | 001 |
| 28 | 000 | 000 | 000 | 001 |

### TABLE 3

| $z$ | $\frac{\lambda^{2^z} - 1}{\lambda - 1} \pmod{2^{35}}$ | | | |
|---|---|---|---|---|
| 0 | 000 | 000 | 000 | 001 |
| 1 | 000 | 000 | 000 | 202 |
| 2 | 000 | 010 | 201 | 404 |
| 3 | 161 | 063 | 407 | 010 |
| 4 | 074 | 403 | 036 | 020 |
| 5 | 162 | 366 | 174 | 040 |
| 6 | 114 | 654 | 770 | 100 |
| 7 | 111 | 133 | 760 | 200 |
| 8 | 320 | 277 | 740 | 400 |
| 9 | 230 | 637 | 701 | 000 |
| 10 | 021 | 677 | 602 | 000 |
| 11 | 244 | 577 | 404 | 000 |
| 12 | 115 | 377 | 010 | 000 |
| 13 | 252 | 776 | 020 | 000 |
| 14 | 225 | 774 | 040 | 000 |
| 15 | 053 | 770 | 100 | 000 |
| 16 | 127 | 760 | 200 | 000 |
| 17 | 257 | 740 | 400 | 000 |
| 18 | 137 | 701 | 000 | 000 |
| 19 | 277 | 602 | 000 | 000 |
| 20 | 177 | 404 | 000 | 000 |
| 21 | 377 | 010 | 000 | 000 |
| 22 | 376 | 010 | 000 | 000 |
| 23 | 374 | 040 | 000 | 000 |
| 24 | 370 | 100 | 000 | 000 |
| 25 | 360 | 200 | 000 | 000 |
| 26 | 340 | 400 | 000 | 000 |
| 27 | 301 | 000 | 000 | 000 |
| 28 | 202 | 000 | 000 | 000 |
| 29 | 004 | 000 | 000 | 000 |
| 30 | 010 | 000 | 000 | 000 |
| 31 | 020 | 000 | 000 | 000 |
| 32 | 040 | 000 | 000 | 000 |
| 33 | 100 | 000 | 000 | 000 |
| 34 | 200 | 000 | 000 | 000 |

### TABLE 4

| $z$ | $\lambda^{2^{35}-2^z} \pmod{2^{35}}$ | | | |
|---|---|---|---|---|
| 0 | 001 | 770 | 037 | 601 |
| 1 | 011 | 740 | 137 | 401 |
| 2 | 105 | 540 | 477 | 001 |
| 3 | 222 | 102 | 176 | 001 |
| 4 | 073 | 210 | 374 | 001 |
| 5 | 262 | 440 | 770 | 001 |
| 6 | 125 | 201 | 760 | 001 |
| 7 | 153 | 003 | 740 | 001 |
| 8 | 330 | 007 | 700 | 001 |
| 9 | 270 | 017 | 600 | 001 |
| 10 | 220 | 037 | 400 | 001 |
| 11 | 240 | 077 | 000 | 001 |
| 12 | 100 | 176 | 000 | 001 |
| 13 | 200 | 374 | 000 | 001 |
| 14 | 000 | 770 | 000 | 001 |
| 15 | 001 | 760 | 000 | 001 |
| 16 | 003 | 740 | 000 | 001 |
| 17 | 007 | 700 | 000 | 001 |
| 18 | 017 | 600 | 000 | 001 |
| 19 | 037 | 400 | 000 | 001 |
| 20 | 077 | 000 | 000 | 001 |
| 21 | 176 | 000 | 000 | 001 |
| 22 | 374 | 000 | 000 | 001 |
| 23 | 370 | 000 | 000 | 001 |
| 24 | 360 | 000 | 000 | 001 |
| 25 | 340 | 000 | 000 | 001 |
| 26 | 300 | 000 | 000 | 001 |
| 27 | 200 | 000 | 000 | 001 |
| 28 | 000 | 000 | 000 | 001 |

## REFERENCES

1. BARNETT, V. Behavior of pseudo-random sequences generated on computers by the multiplicative congruential method. *Math. Comput. 16* (1962), 63–69.
2. HILDEBRANDT, P. Notes on the generation and testing of random numbers on the AN/FSQ-7. Document SP-35, System Develop. Corp., Santa Monica, Calif., Sept. 1958.
3. JUNCOSA, M. Random number generation on the BRL high-speed computing machines. Report No. 855, Ballistics Res. Lab., Aberdeen Proving Ground, Md., 1953.
4. TAUSSKY, O. AND TODD, J. Generation and testing of pseudo-random numbers. In *Symposium on Monte Carlo Methods*, H. A. Meyer (Ed.), Wiley, New York, 1956, 15–28.
5. GREENBERGER, M. Notes on a new pseudo-random number generator. *J. ACM 8* (1961), 163–167.
6. KUEHN, H. A 48-bit pseudo-random number generator. *Comm. ACM 4* (1961), 350–352.
7. PEACH, P. Bias in pseudo-random numbers. *J. Amer. Stat. Assoc. 56* (1961), 610–618.
8. ROTENBERG, A. A new pseudo-random number generator. *J. ACM 7* (1960), 75–77.
9. BOFINGER, E., AND BOFINGER, V. J. On a periodic property of pseudo-random sequences. *J. ACM 5* (1958), 261–265.