# Intrinsic Relations in the Structure of Linear Congruential Generators modulo $2^\beta$

Ora E. Percus and J. K. Percus
Ultracomputer Research Laboratory
Courant Institute of Mathematical Sciences, New York University
251 Mercer Street, New York, NY 10012

Ultracomputer Note #172
January, 1991

This work was supported in part by Applied Mathematical Sciences Program of the U. S. Department of Energy under Contract DE-FG02-88ER25052 and in part under contract DARPA F49620-87-C-0065.

**Abstract**

We show two different general relationships that exist among terms of the linear congruential generator

$$x_{i+1} = ax_i + b \bmod 2^\beta$$

that are separated by powers of two. These two relationships are not equivalent except in one special case which turns out to be Marsaglia's result.

## 1. Introduction.

One of the most successful classes of pseudo random number generators is the so called linear congruential generator (lcg) which is uniquely determined by selecting $\beta$, $a$, $b$ and $x_0$, and for every $i \geq 0$ is defined by

$$x_{i+1} \equiv ax_i + b \mod 2^\beta \tag{1.1}$$

If we choose

$$a = 1 + A2^\alpha$$

$A$ odd, $1 < \alpha$ integer, $b$ odd, then the sequence (1.1) has a period $2^\beta$ (i.e. $(x_0, x_1, \ldots, x_{2^\beta - 1})$ is a permutation of $(0, 1, \ldots, 2^\beta - 1)$ ). In addition one should require that the multiplicative constant $a$ at least pass low order spectral tests (see [1]).

Marsaglia in [2] has proved that although the period of the sequence (1.1) is $2^\beta$, the effective period is $2^{\beta-\alpha}$ i.e. the sequence starts with a block

$$B = \{x_0, x_1, \ldots, x_{2^{\beta-\alpha}-1}\}$$

and follows by $2^\alpha - 1$ translates of that block

$$\{B + C\} \ , \ \{B + 2C\} \ , \ \ldots \ , \ \{B + (2^\alpha - 1)C\}$$

where

$$x_{n+2^{\beta-\alpha}} - x_n = C \ . \tag{1.2}$$

It may appear that for $\alpha << \beta$ there are very few ($2^\alpha$) blocks and the length of each block ($2^{\beta-\alpha}$) is large. Does this mean that we can use our lcg safely for the first $2^{\beta-\alpha}$ values?

Unfortunately the answer is No! In §2 we'll show that for a special case of our previous theorem (concerning general relationships between terms separated by powers of two, see [3]), even for small $\alpha$, there are repeats of certain combinations of $x$'s in blocks of size

$\beta - \alpha s$ for every integer $s$. A special case of this theorem with the aid of an additional lemma will produce Marsaglia's result.

The repeats of a different combination of $x$'s in blocks of size $\beta - \alpha s$ for every $s$ will be demonstrated in §3 (Theorem 2). Marsaglia's result will be an immediate consequence for $s = 1$.

**2. A general relationship among terms separated by powers of two as applied to blocks of size $\beta - \alpha s$.**

In [3] we have shown that every linear congruential generator that uses a power of 2 as modulus introduces correlations among elements separated sequentially by powers of two. In particular we proved the following:

**Theorem 1.** *Let*

$$x_{i+1} \equiv a x_i + b \bmod 2^\beta$$

$$a = 1 + A2^\alpha \ , \quad A \text{ odd integer, } \alpha > 1$$

*Then for every $k$ the linear relation*

$$\sum_{j=0}^{\ell} c_j x_{n+j2^k} \equiv 0 \bmod 2^\beta$$

*holds, where*

$$C_j = (-1)^j \binom{\ell}{j}$$

$$\ell \text{ is the smallest integer } \geq \begin{cases} \frac{\beta+\alpha}{k+\alpha} & \text{if} \quad b \text{ is odd;} \\ \frac{\beta}{k+\alpha} & \text{if} \quad b = 0 \ . \end{cases}$$

Using this theorem for $k = \beta - \alpha$ and $b$ odd, we get

$$\ell = 1 + \left[\frac{\beta + \alpha}{\beta}\right] = 2$$

Hence

$$x_{n+2\cdot 2^{\beta-\alpha}} - 2x_{n+2^{\beta-\alpha}} + x_n = 0 \mod 2^\beta$$

This implies

$$x_{n+d\,2^{\beta-\alpha}} = x_n + d\,\Delta x_n \mod 2^\beta \tag{2.1}$$

where

$$\Delta x_n = x_{n+2^{\beta-\alpha}} - x_n \mod 2^\beta$$

To show that $\Delta x_n$ is a constant (mod $2^\beta$) independent of $n$, we'll apply the following:

**Lemma.** *Let* $a = 1 + A2^{\alpha}$, $A$ *odd*, $\alpha > 1$. *Then for every* $k$ *integer*

$$a^{2^k} - 1 = A'2^{\alpha+k} \ , \quad A' \text{ odd.} \tag{2.2}$$

This lemma is easily proved using mathematical induction.

Now from (1.1) we get

$$x_n = a^n x_0 + b\frac{a^n - 1}{a - 1} \bmod 2^{\beta} \tag{2.3}$$

(2.2) and (2.3) imply $\Delta x_n = C$. Thus we obtain $x_{n+d2^{\beta-\alpha}} = x_n + dc$ which is Marsaglia's result.

## 3. Intrinsic Structure in lcg.

Another intrinsic structure of the lcg can be seen from the following:

**Theorem 2.** *Let*

$$x_{i+1} \equiv ax_i + b \ mod\ 2^\beta$$

*b odd integer,* $a = 1 + A2^\alpha$, *A odd integer,* $\alpha > 1$. *Then for every integer s satisfying* $\alpha s < \beta$, *and every n, the relation*

$$\sum_{j=0}^{s} \binom{s}{j} (-1)^j x_{n+j+2^{\beta-\alpha s}} \equiv \sum_{j=0}^{s} \binom{s}{j} (-1)^j x_{n+j} \ mod\ 2^\beta \tag{3.1}$$

*is satisfied.*

To prove the above we use (2.3). This leads to the sum:

$$\sum_{j=0}^{s} \binom{s}{j} (-1)^j\, x_{n+j} = (-1)^s a^n (a-1)^{s-1} \left[x_0(a-1) + b\right] \bmod 2^\beta \tag{3.2}$$

Similarly

$$\sum_{j=0}^{s} (-1)^j \binom{s}{j} \left(x_{n+j+2^{\beta-\alpha}} - x_{n+j}\right)$$
$$= (-1)^s (a-1)^{s-1} \left(x_0(a-1) + b\right) a^n \left(a^{2^{\beta-\alpha s}} - 1\right) \bmod 2^\beta$$

Using our lemma

$$(a-1)^{s-1} \left(a^{2^{\beta-\alpha s}} - 1\right) = (a-1)^{s-1} A'\, 2^{\alpha+\beta-\alpha s}$$
$$= (A2^\alpha)^{s-1}\, A'\, 2^{\beta-\alpha(s-1)} = A^{s-1} A' 2^\beta = 0 \bmod 2^\beta$$

which proves (3.1).

Note that for $s = 1$ we get from (3.1)

$$x_{n+2^{\beta-\alpha}} - x_n = x_{n+1+2^{\beta-\alpha}} - x_{n+1} = \text{ const.}$$

which is Marsaglia's result.

Note also that if $k = \beta - \alpha s$ and $b$ is odd then Theorem 1 implies the relationship

$$\sum_{j=0}^{\ell} c_j x_{n+j2^{\beta-\alpha s}} = 0 \tag{3.3}$$

where

$$\ell = 1 + [\frac{\beta + \alpha}{\beta - \alpha(s-1)}]$$

$$c_j = (-1)^j \binom{\ell}{j} .$$

Except for the case $s = 1$ the relations (3.1) and (3.3) are not equivalent.

**References**


[1] Knuth, D. E., "The Art of Computer Programming", Vol. 2, Seminumerical Algorithms, 2nd ed., Addison-Wesley, Reading, MA, 1981.

[2] Marsaglia, G. in "Application of Number Theory to Numerical Analysis", S. K. Zaremba ed., Academic Press, 1972 (p. 249).

[3] Percus, O. E. & Percus, J. K., "Long Range Correlation in Linear Congruential Generators", J. Comp. Phys., 1988 (p. 267).