MATHEMATICS OF COMPUTATION
Volume 68, Number 225, January 1999, Pages 249–260
S 0025-5718(99)00996-5

# TABLES OF LINEAR CONGRUENTIAL GENERATORS OF DIFFERENT SIZES AND GOOD LATTICE STRUCTURE

PIERRE L'ECUYER

ABSTRACT. We provide sets of parameters for multiplicative linear congruential generators (MLCGs) of different sizes and good performance with respect to the spectral test. For $\ell = 8, 9, \ldots, 64, 127, 128$, we take as a modulus $m$ the largest prime smaller than $2^\ell$, and provide a list of multipliers $a$ such that the MLCG with modulus $m$ and multiplier $a$ has a good lattice structure in dimensions 2 to 32. We provide similar lists for power-of-two moduli $m = 2^\ell$, for multiplicative and non-multiplicative LCGs.

## 1. INTRODUCTION

A *multiplicative linear congruential generator* (MLCG) is defined by a recurrence of the form

$$x_n = a x_{n-1} \mod m \tag{1}$$

where $m$ and $a$ are integers called the *modulus* and the *multiplier*, respectively, and $x_n \in \mathbf{Z}_m = \{0, \ldots, m-1\}$ is the *state* at step $n$. To obtain a sequence of "random numbers" in the interval $[0, 1)$, one can define the *output* at step $n$ as

$$u_n = x_n / m. \tag{2}$$

We use the expression "the MLCG $(m, a)$" to denote a sequence that obeys (1) and (2). The properties of MLCGs have been studied extensively and are well-known; see, for example, [3, 5, 7].

If $m$ is prime, $a$ is a primitive element modulo $m$, and $x_0 \neq 0$, then the sequences $\{x_n\}$ and $\{u_n\}$ are periodic with period lengths $\rho = m - 1$, and the generator is called a *full period* MLCG.

For each integer $t \geq 1$, define

$$T_t = \{\mathbf{u}_n = (u_n, \ldots, u_{n+t-1}) \mid n \geq 0,\ x_0 \in \mathbf{Z}_m\}, \tag{3}$$

the set of all overlapping $t$-tuples of successive values of $u_n$, from all possible initial seeds. The set $T_t$ is equal to the intersection of a lattice $L_t$ with the $t$-dimensional unit cube $[0, 1)^t$ (see, e.g., [5, 9] for more details). This implies in particular that all the points of $T_t$ lie on a relatively small number of equidistant parallel hyperplanes.

Received by the editor May 9, 1997.
1991 *Mathematics Subject Classification.* Primary 65C10.
*Key words and phrases.* Random number generation, linear congruential, lattice structure, spectral test.
This work has been supported by NSERC-Canada grants ODGP0110050 and SMF0169893, and FCAR-Québec grant 93ER1654. Thanks to Raymond Couture, Peter Hellekalek, and Harald Niederreiter for useful suggestions, to Ajmal Chaumun who helped in computing the tables, and to Karl Entacher who pointed out an error in an earlier version.

Among all families of hyperplanes that cover all the points, choose the one for which the distance between the successive hyperplanes is the largest, and let $d_t$ be this distance. The set $T_t$ is more uniformly distributed over the cube if $d_t$ is smaller. In the literature, examining the $d_t$'s associated with a given generator is often called the *spectral test* [3, 5].

The minimal value of $d_t$ for a lattice in $\mathbf{R}^t$ with $m$ points per unit of volume is

$$d_t^*(m) = \gamma_t^{-1} m^{-1/t}, \tag{4}$$

where the constant $\gamma_t$ depends only on $t$ and is known for $t \le 8$ (see [5]). For $t > 8$, lower and upper bounds on $\gamma_t$ are available. An upper bound $\rho_t$ can be deduced from Rogers' bound on the density of sphere packings (see [1, p.88]). It can be written as

$$\rho_t = 2e^{R(t)/t}, \tag{5}$$

where $R(t)$ can be found in [1] for $t \le 24$. For $t \ge 25$, $R(t)$ can be approximated with $O(1/t)$ error, and approximately four decimal digits of precision for $t = 25$, by

$$R(t) = \frac{1}{2} t \lg\left(\frac{t}{4\pi e}\right) + \frac{3}{2}\lg(t) - \lg(e/\sqrt{\pi}) + \frac{5.25}{t+2.5}, \tag{6}$$

where lg is the log in base 2. A lower bound can be obtained by looking at the value of $d_t$ associated with the laminated lattice in dimension $t$. This gives $\gamma_t \ge \ell_t = 2\lambda_t^{-1/(2t)}$, where $\lambda_t$ is given in [1, p.88] for $t \le 48$. For $t \le 8$, it turns out that $\ell_t = \gamma_t$ up to at least 52 bits of precision. Table 1 gives the ratio $\ell_t/\rho_t$, of the lower bound over the upper bound, for $1 \le t \le 48$. This ratio tends to decrease with increasing $t$, but not monotonously.

In this paper, following a suggestion in [11], we chose to replace $\gamma_t$ by $\rho_t$ in the lower bound (4), for $t > 8$. This yields the lower bound

$$d_t \ge \bar{d}_t(m) = \begin{cases} \gamma_t^{-1} m^{-1/t} & \text{for } t \le 8; \\ \rho_t^{-1} m^{-1/t} & \text{for } t > 8. \end{cases} \tag{7}$$

The value of $d_t$ can be normalized to

$$S_t = \frac{\bar{d}_t(m)}{d_t},$$

which takes its values in the interval $[0, 1]$, the larger the better. Following [3, 4], for any $T \ge 2$, we define the figure of merit:

$$M_T = \min_{2 \le t \le T} S_t. \tag{8}$$

The idea is to find full-period MLCGs with the best value of $M_T$, for given $m$ and $T$.

Other authors have already performed searches of that sort. Fishman and Moore [4] found all the 414 multipliers $a$ which are primitive elements modulo $m$ and for which $M_6 \ge 0.8$, for $m = 2^{31} - 1$. They give the values of $S_1, \ldots, S_6$ for the five best. Fishman [2] obtained similar results for MLCGs with $m = 2^{32}$ and $m = 2^{48}$. Values of $S_t$, $t \le 8$, for various LCGs proposed in the literature or available in software libraries, can be found in [3, 6, 7]. Searches for good multiple recursive generators, based on similar criteria, have also been performed for a few selected prime moduli $m$ near $2^{31}$, $2^{47}$, and $2^{63}$ (see [8]).

Our aim in this paper is to provide a table of MLCGs with large values of $M_T$, for different sizes of $m$ and $T$. For $\ell = 8, 9, \ldots, 64$, and a few larger values of $\ell$, we

TABLE 1. Ratio between lower and upper bounds on $\gamma_t$

| $t$ | $\ell_t/\rho_t$ | $t$ | $\ell_t/\rho_t$ |
|---|---|---|---|
| 1 | 1.0000 | 25 | 0.9616 |
| 2 | 1.0000 | 26 | 0.9407 |
| 3 | 0.9855 | 27 | 0.9232 |
| 4 | 0.9878 | 28 | 0.9113 |
| 5 | 0.9759 | 29 | 0.8999 |
| 6 | 0.9807 | 30 | 0.8932 |
| 7 | 0.9843 | 31 | 0.8882 |
| 8 | 0.9985 | 32 | 0.8871 |
| 9 | 0.9665 | 33 | 0.8765 |
| 10 | 0.9512 | 34 | 0.8699 |
| 11 | 0.9405 | 35 | 0.8649 |
| 12 | 0.9401 | 36 | 0.8632 |
| 13 | 0.9373 | 37 | 0.8614 |
| 14 | 0.9424 | 38 | 0.8627 |
| 15 | 0.9487 | 39 | 0.8649 |
| 16 | 0.9612 | 40 | 0.8699 |
| 17 | 0.9512 | 41 | 0.8670 |
| 18 | 0.9487 | 42 | 0.8671 |
| 19 | 0.9481 | 43 | 0.8681 |
| 20 | 0.9534 | 44 | 0.8716 |
| 21 | 0.9572 | 45 | 0.8749 |
| 22 | 0.9660 | 46 | 0.8805 |
| 23 | 0.9758 | 47 | 0.8869 |
| 24 | 0.9900 | 48 | 0.8955 |

consider the largest prime $m < 2^\ell$, and seek full-period multipliers $a$ with the best values of $M_8$, $M_{16}$, and $M_{32}$. The values of $d_t$ were computed with the software package of [9]. Section 2 explains how this search was made and gives the results. In Section 3, we provide similar results for the case where $m$ is a power of 2. We consider MLCGs as in (1), as well as LCGs with a nonzero additive constant, whose period length is $m$.

MLCGs with large moduli $m$ and good lattice structure can be used as random number generators [3, 5, 7], e.g., for computer simulation. It is then recommended that the value of $m$ be several orders of magnitude larger than the number of output values $u_n$ that are generated, so even $m$ near $2^{64}$ is relatively small in this context, too small for certain types of simulation applications but enough for most.

MLCGs with small values of $m$ can be used for *quasi-Monte Carlo* integration [10] of a $t$-dimensional function over the hypercube $[0, 1]^t$. In that case, the function is evaluated at *each* of the points of $T_t$ and the integral is estimated by the average of those $m$ function values. The size of $m$ would depend on how much computing time we are ready to spend. For example, $m$ near $2^{20}$ gives approximately one million evaluation points. If the MLCG has a good lattice structure in dimension $t$, then it yields a so-called *good lattice rule* for numerical integration [10, Chapter 5]. As explained in [10], an upper bound on the integration error can be obtained in terms of a measure of regularity of the function and of a figure of merit for the lattice $L_t$. This figure of merit differs from the ones we consider in this paper, and its computation appears much more involved.

MLCGs with moderate values of $m$ can also be used to experiment with different types of statistical tests for random number generators. One can examine, for example, how the minimal size of $m$ required for a good LCG to pass a given type of test increases with the size of the test.

## 2. The search plan and results for prime $m$

For each prime number $m$, let $\Psi(m)$ be the set of all primitive elements modulo $m$; that is, the set of all $a$ in $\mathbf{Z}_m$ such that $a^n \not\equiv 1 \pmod{m}$ for $n = 1, \ldots, m-2$. For any $a \in \Psi(m)$, let $d_t(m,a)$, $S_t(m,a)$, and $M_T(m,a)$ be the values of $d_t$, $S_t$, and $M_T$ associated with the MLCG $(m,a)$. For different values of $m$, we searched for multipliers $a$ in $\Psi(m)$ with the largest possible values of $M_8(m,a)$, those with the largest values of $M_{16}(m,a)$, and those with the largest values of $M_{32}(m,a)$. The choice of $T = 8$, 16, and 32 is arbitrary. It gives multipliers that are good up to (roughly) small, medium, and large dimensions.

For each selected value of $\ell$, we considered the largest prime $m$ smaller than $2^\ell$. For $\ell \le 26$, the absolute best multipliers with respect to the criteria $M_8(m,a)$, $M_{16}(m,a)$, and $M_{32}(m,a)$ were found by an *exhaustive* search over $\Psi(m)$. For $\ell \ge 27$, we performed a *random* search within $\Psi(m)$ and retained the multipliers with the largest values of $M_8(m,a)$, $M_{16}(m,a)$, and $M_{32}(m,a)$ that we could find. Each random search was given a computing budget of between 10 and 20 hours of cpu time, with the search algorithm and program described in [9]. Different models of *SUN Sparcstation* computers were used. These random searches gave us plenty of good multipliers. Performing exhaustive searches for those large values of $m$ would provide only a marginal improvement over the best values of $M_T(m,a)$ found so far, and would require a huge computing budget, so we think it is not worth the trouble.

For $a \in \{1, \ldots, m-1\}$, the multiplicative inverse of $a$ modulo $m$ is the unique integer $a^* \in \{1, \ldots, m-1\}$ such that $a^* a \equiv 1 \pmod{m}$. If $a$ is replaced by $a^*$ in (1), then the same sequence is generated, but in reverse order. Therefore, $a$ and $a^*$ are equivalent in the sense that they produce the same lattice structure. So, good multipliers always come in pairs. In Table 2, each line gives a pair of multipliers of the form $(a, a^*)$. For example, 213 is the inverse of 33 modulo 251, and both multipliers have the same figures of merit.

A symbol $^*$ next to a number means that this is the best value found for that figure of merit, for this modulus. For example, for $m = 251$, the multipliers 33 and 213 are those with the best value of $M_8(m,a)$, and also with the best value of $M_{32}(m,a)$ (ex-æquo with 55 and 178), among all multipliers $a$ that are primitive modulo $m$.

Table 3 reports the results of a similar search, for certain values of $\ell$, but with the additional restriction that $a(m-1) < 2^{53}$. Multipliers satisfying this constraint are more interesting from the practical viewpoint, because the generator then lends itself to a fast implementation in floating-point arithmetic on computers whose hardware supports the IEEE floating-point arithmetic standard, with at least 53 bits of precision for the mantissa (most computers do so). The results of this table are based on an exhaustive search among all multipliers $a$ that satisfy the constraint. For $\ell \le 27$, all the multipliers given in Table 2 satisfy the constraint, except for those larger than 67108883 for $m = 2^{27} - 39$.

TABLE 2. LCGs with good figures of merit

| $m$ | $a, a^*$ | $M_8(m,a)$ | $M_{16}(m,a)$ | $M_{32}(m,a)$ |
|---|---|---|---|---|
| $2^8 - 5 = 251$ | 33, 213 | 0.70617 * | 0.66083 | 0.64645 * |
| | 55, 178 | 0.66973 | 0.66973 * | 0.64645 * |
| $2^9 - 3 = 509$ | 35, 160 | 0.68202 * | 0.68202 * | 0.63233 * |
| | 110, 236 | 0.68202 * | 0.68202 * | 0.63233 * |
| | 273, 399 | 0.68202 * | 0.68202 * | 0.63233 * |
| | 349, 474 | 0.68202 * | 0.68202 * | 0.63233 * |
| $2^{10} - 3 = 1021$ | 65, 377 | 0.69069 * | 0.66317 | 0.61872 * |
| | 331, 401 | 0.67388 | 0.67388 * | 0.61872 * |
| $2^{11} - 9 = 2039$ | 995, 1498 | 0.72170 * | 0.65531 | 0.60549 |
| | 328, 603 | 0.69551 | 0.69189 * | 0.60549 |
| | 393, 799 | 0.65283 | 0.65283 | 0.65283 * |
| $2^{12} - 3 = 4093$ | 209, 3858 | 0.67296 * | 0.60649 | 0.60649 |
| | 235, 3884 | 0.67296 * | 0.60649 | 0.60649 |
| | 219, 542 | 0.66150 | 0.66150 * | 0.66150 * |
| | 3551, 3874 | 0.66150 | 0.66150 * | 0.66150 * |
| $2^{13} - 1 = 8191$ | 884, 7459 | 0.67317 * | 0.61508 | 0.61508 |
| | 1716, 5580 | 0.64854 | 0.64854 * | 0.64854 * |
| | 2685, 6083 | 0.64854 | 0.64854 * | 0.64854 * |
| $2^{14} - 3 = 16381$ | 572, 13374 | 0.71968 * | 0.59638 | 0.59638 |
| | 3007, 15809 | 0.71968 * | 0.59638 | 0.59638 |
| | 665, 3424 | 0.71116 | 0.66792 * | 0.65508 * |
| | 12957, 15716 | 0.71116 | 0.66792 * | 0.65508 * |
| $2^{15} - 19 = 32749$ | 219, 30805 | 0.71802 * | 0.56955 | 0.56955 |
| | 1944, 32530 | 0.71802 * | 0.56955 | 0.56955 |
| | 9515, 10088 | 0.69372 | 0.67356 * | 0.67356 * |
| | 22661, 23234 | 0.69372 | 0.67356 * | 0.67356 * |
| $2^{16} - 15 = 65521$ | 17364, 32236 | 0.70713 * | 0.44566 | 0.44566 |
| | 33285, 48157 | 0.70713 * | 0.44566 | 0.44566 |
| | 2469, 47104 | 0.64650 | 0.63900 * | 0.63900 * |
| $2^{17} - 1 = 131071$ | 43165, 66284 | 0.70941 * | 0.58409 | 0.58409 |
| | 29223, 119858 | 0.67169 | 0.67169 * | 0.65617 |
| | 29803, 76704 | 0.66838 | 0.66230 | 0.66230 * |
| $2^{18} - 5 = 262139$ | 92717, 166972 | 0.72539 * | 0.61601 | 0.61601 |
| | 21876, 118068 | 0.67832 | 0.67832 * | 0.67019 * |
| $2^{19} - 1 = 524287$ | 283741, 358899 | 0.72130 * | 0.59188 | 0.59188 |
| | 37698, 127574 | 0.66780 | 0.66780 * | 0.65255 |
| | 155411, 157781 | 0.69573 | 0.66646 | 0.66646 * |
| $2^{20} - 3 = 1048573$ | 380985, 444362 | 0.71709 * | 0.60387 | 0.60387 |
| | 604211, 667588 | 0.71709 * | 0.60387 | 0.60387 |
| | 100768, 463964 | 0.66055 | 0.66055 * | 0.60062 |
| | 947805, 584609 | 0.66055 | 0.66055 * | 0.60062 |
| | 22202, 246298 | 0.66738 | 0.65888 | 0.65888 * |
| | 1026371, 802275 | 0.66738 | 0.65888 | 0.65888 * |
| $2^{21} - 9 = 2097143$ | 360889, 1372180 | 0.72537 * | 0.59108 | 0.59108 |
| | 1043187, 1352851 | 0.68608 | 0.68608 * | 0.62381 |
| | 1939807, 1969917 | 0.68492 | 0.68492 | 0.67664 * |
| $2^{22} - 3 = 4194301$ | 914334, 1406151 | 0.72226 * | 0.53547 | 0.53547 |
| | 2788150, 3279967 | 0.72226 * | 0.53547 | 0.53547 |
| | 1731287, 2040406 | 0.67819 | 0.67819 * | 0.67611 * |
| | 2463014, 2153895 | 0.67819 | 0.67819 * | 0.67611 * |

TABLE 2. LCGs with good figures of merit (continued)

| $m$ | $a, a^*$ | $M_8(m,a)$ | $M_{16}(m,a)$ | $M_{32}(m,a)$ |
|---|---|---|---|---|
| $2^{23}-15$ | 653276, 5169235 | 0.73407 * | 0.65758 | 0.61581 |
| $=8388593$ | 3219358, 7735317 | 0.73407 * | 0.65758 | 0.61581 |
| | 1706325, 6513898 | 0.67462 | 0.67462 * | 0.65778 |
| | 6682268, 1874695 | 0.67462 | 0.67462 * | 0.65778 |
| | 422527, 5515073 | 0.67530 | 0.66916 | 0.66916 * |
| | 7966066, 2873520 | 0.67530 | 0.66916 | 0.66916 * |
| $2^{24}-3$ | 6423135, 9726917 | 0.74477 * | 0.54337 | 0.54337 |
| $=16777213$ | 7050296, 10354078 | 0.74477 * | 0.54337 | 0.54337 |
| | 4408741, 6180188 | 0.66849 | 0.66849 * | 0.66543 |
| | 12368472, 10597025 | 0.66849 | 0.66849 * | 0.66543 |
| | 931724, 5637643 | 0.68149 | 0.66735 | 0.66735 * |
| | 15845489, 11139570 | 0.68149 | 0.66735 | 0.66735 * |
| $2^{25}-39$ | 25907312, 32544832 | 0.74982 * | 0.58170 | 0.58170 |
| $=33554393$ | 12836191, 5420585 | 0.69488 | 0.68447 * | 0.57247 |
| | 28133808, 20718202 | 0.69488 | 0.68447 * | 0.57247 |
| | 25612572, 1860625 | 0.67766 | 0.67105 | 0.66953 * |
| | 31693768, 7941821 | 0.67766 | 0.67105 | 0.66953 * |
| $2^{26}-5$ | 26590841, 11526618 | 0.76610 * | 0.55995 | 0.55995 |
| $=67108859$ | 19552116, 24409594 | 0.69099 | 0.69099 * | 0.64966 |
| | 66117721, 6763103 | 0.68061 | 0.67408 | 0.67062 * |
| $2^{27}-39$ | 45576512, 70391260 | 0.75874 * | 0.58717 | 0.58717 |
| $=134217689$ | 63826429, 88641177 | 0.75874 * | 0.58717 | 0.58717 |
| | 3162696, 71543207 | 0.70233 | 0.67264 * | 0.66714 * |
| $2^{28}-57$ | 246049789, 150873839 | 0.74215 * | 0.52820 | 0.52820 |
| $=268435399$ | 140853223, 102445941 | 0.70462 | 0.67353 * | 0.56023 |
| | 29908911, 166441841 | 0.67604 | 0.67353 * | 0.58183 |
| | 104122896, 111501501 | 0.66326 | 0.65808 | 0.65808 * |
| $2^{29}-3$ | 520332806, 219118189 | 0.75238 * | 0.59538 | 0.59538 |
| $=536870909$ | 530877178, 475905290 | 0.67352 | 0.67088 * | 0.66418 * |
| $2^{30}-35$ | 771645345, 599290962 | 0.74881 * | 0.60540 | 0.59895 |
| $=1073741789$ | 295397169, 1017586987 | 0.68323 | 0.67420 * | 0.52102 |
| | 921746065, 679186565 | 0.65830 | 0.65830 | 0.65830 * |
| $2^{31}-1$ | 1583458089, 1132489760 | 0.72771 * | 0.61996 | 0.61996 |
| $=2147483647$ | 784588716, 163490618 | 0.65885 | 0.65388 * | 0.65388 * |
| $2^{32}-5$ | 1588635695, 3870709308 | 0.74530 * | 0.64199 | 0.64034 |
| $=4294967291$ | 1223106847, 4223879656 | 0.69299 | 0.67551 * | 0.64034 |
| | 279470273, 1815976680 | 0.65862 | 0.65862 | 0.65862 * |
| $2^{33}-9$ | 7425194315, 8436767804 | 0.73666 * | 0.45155 | 0.45155 |
| $=8589934583$ | 2278442619, 1729516095 | 0.66244 | 0.65958 * | 0.63549 |
| | 7312638624, 205277214 | 0.65221 | 0.65221 | 0.65221 * |
| $2^{34}-41$ | 5295517759, 2447157083 | 0.73607 * | 0.42784 | 0.42784 |
| $=17179869143$ | 473186378, 6625295500 | 0.66652 | 0.66652 * | 0.65074 * |
| $2^{35}-31$ | 3124199165, 27181987157 | 0.74740 * | 0.55117 | 0.55117 |
| $=34359738337$ | 22277574834, 16353251630 | 0.68241 | 0.65471 * | 0.61272 |
| | 8094871968, 31023073077 | 0.64471 | 0.64471 | 0.64471 * |
| $2^{36}-5$ | 49865143810, 44525253482 | 0.72011 * | 0.56045 | 0.56045 |
| $=68719476731$ | 45453986995, 40162435147 | 0.66038 | 0.65905 * | 0.65665 * |
| $2^{37}-25$ | 76886758244, 31450092817 | 0.73284 * | 0.59222 | 0.55865 |
| $=137438953447$ | 2996735870, 105638438130 | 0.70849 | 0.65341 * | 0.63328 |
| | 85876534675, 116895888786 | 0.66073 | 0.65085 | 0.65085 * |

TABLE 2. LCGs with good figures of merit (continued)

| $m$ | $a, a^*$ | $M_8(m,a)$ | $M_{16}(m,a)$ | $M_{32}(m,a)$ |
|---|---|---|---|---|
| $2^{38}-45$ | 17838542566, 234584904863 | 0.72311 * | 0.59289 | 0.57131 |
| | 101262352583, 258824536167 | 0.65223 | 0.65035 * | 0.60629 |
| | 24271817484, 141086538846 | 0.64022 | 0.64022 | 0.63644 * |
| $2^{39}-7$ | 61992693052, 207382937966 | 0.72606 * | 0.50283 | 0.50283 |
| | 486583348513, 247058793858 | 0.65522 | 0.64233 * | 0.62267 |
| | 541240737696, 68317042802 | 0.64118 | 0.64118 | 0.64118 * |
| $2^{40}-87$ | 1038914804222, 956569416632 | 0.73656 * | 0.56206 | 0.56206 |
| | 88718554611, 864341149053 | 0.68083 | 0.67629 * | 0.60506 |
| | 937333352873, 945467218816 | 0.69567 | 0.64693 | 0.64286 * |
| $2^{41}-21$ | 140245111714, 1888116500887 | 0.72891 * | 0.57568 | 0.57568 |
| | 416480024109, 1420814698317 | 0.65093 | 0.64692 * | 0.61035 |
| | 1319743354064, 717943173063 | 0.65422 | 0.63748 | 0.63748 * |
| $2^{42}-11$ | 2214813540776, 4365946432566 | 0.74418 * | 0.62178 | 0.62178 |
| | 2928603677866, 3015630915308 | 0.66427 | 0.66427 * | 0.62145 |
| | 92644101553, 626031856758 | 0.66812 | 0.65172 | 0.64110 * |
| $2^{43}-57$ | 4928052325348, 4541763706392 | 0.73258 * | 0.58054 | 0.58054 |
| | 4204926164974, 3434105419275 | 0.67015 | 0.65195 * | 0.62862 |
| | 3663455557440, 2399767999928 | 0.65062 | 0.63552 | 0.63552 * |
| $2^{44}-17$ | 6307617245999, 12680217534946 | 0.72095 * | 0.40161 | 0.40161 |
| | 11394954323348, 6363281811747 | 0.64726 | 0.64726 * | 0.61755 |
| | 949305806524, 12442836230635 | 0.64034 | 0.63577 | 0.63577 * |
| $2^{45}-55$ | 25933916233908, 3608903742640 | 0.74020 * | 0.48371 | 0.48371 |
| | 18586042069168, 11850386302026 | 0.66812 | 0.65288 * | 0.57775 |
| | 20827157855185, 5870357204989 | 0.65174 | 0.63771 | 0.63771 * |
| $2^{46}-21$ | 63975993200055, 63448138118203 | 0.74158 * | 0.59455 | 0.59455 |
| | 15721062042478, 56602273662768 | 0.65292 | 0.65292 * | 0.56919 |
| | 31895852118078, 30001556873103 | 0.65853 | 0.64391 | 0.63482 * |
| $2^{47}-115$ | 72624924005429, 90086464761505 | 0.73939 * | 0.61202 | 0.58428 |
| | 47912952719020, 65482710949587 | 0.66046 | 0.66046 * | 0.57075 |
| | 106090059835221, 115067325755975 | 0.63210 | 0.63210 | 0.63210 * |
| $2^{48}-59$ | 49235258628958, 253087341916107 | 0.74586 * | 0.42596 | 0.42596 |
| | 51699608632694, 8419150949545 | 0.66302 | 0.64985 * | 0.58435 |
| | 59279420901007, 163724808306782 | 0.65839 | 0.63595 | 0.63595 * |
| $2^{49}-81$ | 265609885904224, 463134250989782 | 0.73506 * | 0.53066 | 0.53066 |
| | 480567615612976, 545116409148737 | 0.65594 | 0.64246 * | 0.57269 |
| | 305898857643681, 190965926304768 | 0.66333 | 0.63788 | 0.63577 * |
| $2^{50}-27$ | 1087141320185010, 1051122009542795 | 0.72852 * | 0.52208 | 0.52208 |
| | 157252724901243, 422705992136651 | 0.63912 | 0.63912 * | 0.62044 |
| | 791038363307311, 605985299432352 | 0.64466 | 0.62837 | 0.62837 * |
| $2^{51}-129$ | 349044191547257, 2128884970512414 | 0.73054 * | 0.53683 | 0.53683 |
| | 277678575478219, 598269678776822 | 0.65501 | 0.64283 * | 0.61820 |
| | 486848186921772, 1980113709690257 | 0.67181 | 0.63497 | 0.63497 * |
| $2^{52}-47$ | 4359287924442956, 3707079847465153 | 0.72095 * | 0.48117 | 0.48117 |
| | 3622689089018661, 290414426581729 | 0.68827 | 0.64482 * | 0.60841 |
| | 711667642880185, 3319347797114578 | 0.63766 | 0.63067 | 0.63067 * |
| $2^{53}-111$ | 2082839274626558, 3141627116318043 | 0.74842 * | 0.49471 | 0.49471 |
| | 4179081713689027, 1169831480608704 | 0.64967 | 0.64102 * | 0.59333 |
| | 5667072534355537, 7982986707690649 | 0.67430 | 0.63503 | 0.63503 * |

TABLE 2. LCGs with good figures of merit (continued)

| $m$ | $a, a^*$ | $M_8(m,a)$ | $M_{16}(m,a)$ | $M_{32}(m,a)$ |
|---|---|---|---|---|
| $2^{54}-33$ | 9131148267933071, 17639054895509756 | 0.71956 * | 0.59136 | 0.59136 |
| | 3819217137918427, 6822546395505148 | 0.67456 | 0.65646 * | 0.60358 |
| | 11676603717543485, 13197393252146039 | 0.66189 | 0.63663 | 0.63250 * |
| $2^{55}-55$ | 33266544676670489, 11719476530693442 | 0.73046 * | 0.61066 | 0.55598 |
| | 19708881949174686, 32182684885571630 | 0.65421 | 0.65091 * | 0.61035 |
| | 32075972421209701, 15995561023396933 | 0.62948 | 0.62948 | 0.62948 * |
| $2^{56}-5$ | 4595551687825993, 6128514294048584 | 0.72026 * | 0.57724 | 0.57724 |
| | 26093644409268278, 69294271672288492 | 0.67840 | 0.66318 * | 0.58207 |
| | 4595551687828611, 2389916809994467 | 0.64778 | 0.64243 | 0.62784 * |
| $2^{57}-13$ | 75953708294752990, 66352637866891714 | 0.72732 * | 0.57473 | 0.56026 |
| | 95424006161758065, 2274812368615087 | 0.64856 | 0.64856 * | 0.59464 |
| | 133686472073660397, 113079751547221130 | 0.64588 | 0.62957 | 0.62957 * |
| $2^{58}-27$ | 101565695086122187, 56502943171806276 | 0.77453 * | 0.55885 | 0.55885 |
| | 163847936876980536, 256462492811829427 | 0.68047 | 0.66531 * | 0.54314 |
| | 206638310974457555, 28146528635210647 | 0.64632 | 0.63406 | 0.63406 * |
| $2^{59}-55$ | 346764851511064641, 287514719519235431 | 0.71819 * | 0.54325 | 0.54325 |
| | 124795884580648576, 526457461907464601 | 0.64928 | 0.64760 * | 0.62279 |
| | 573223409952553925, 81222304453481810 | 0.64258 | 0.63111 | 0.63111 * |
| $2^{60}-93$ | 561860773102413563, 79300725740259852 | 0.72541 * | 0.50786 | 0.50786 |
| | 439138238526007932, 998922549734761568 | 0.66098 | 0.65258 * | 0.60350 |
| | 734022639675925522, 67273627956685463 | 0.66024 | 0.62375 | 0.62375 * |
| $2^{61}-1$ | 1351750484049952003, 2078173049752560138 | 0.71028 * | 0.54999 | 0.54276 |
| | 1070922063159934167, 212694642947925581 | 0.63769 | 0.63769 * | 0.56108 |
| | 1267205010812451270, 1283839219676404755 | 0.63648 | 0.62092 | 0.62092 * |
| $2^{62}-57$ | 2774243619903564593, 1983373718104285921 | 0.72982 * | 0.61073 | 0.59560 |
| | 431334713195186118, 1159739479727509578 | 0.64966 | 0.64180 * | 0.59560 |
| | 2192641879660214934, 2674546532986414750 | 0.62431 | 0.62374 | 0.62374 * |
| $2^{63}-25$ | 4645906587823291368, 60091810420728157 | 0.73855 * | 0.50741 | 0.50741 |
| | 2551091334535185398, 9006541669060512547 | 0.65169 | 0.64418 * | 0.58261 |
| | 4373305567859904186, 6458928179451363983 | 0.62582 | 0.62582 | 0.62497 * |
| $2^{64}-59$ | 13891176665706064842, 9044836419713972268 | 0.74105 * | 0.36297 | 0.36297 |
| | 2227057010910366687, 17412224886468018797 | 0.68377 | 0.64579 * | 0.52405 |
| | 18263440312458789471, 811465980874026894 | 0.63276 | 0.62970 | 0.62970 * |
| $2^{127}-1$ | 82461096547334812307256211668490605096, 33541844155669201573045277354985961133 | 0.74702 * | 0.50027 | 0.50027 |
| | 11378330613449548425753788132509481 5818, 549754870954195569833520341422926719 | 0.63462 | 0.62590 * | 0.56105 |
| | 29590761937684265566924671478132826269, 11248885089597022078606294279796866 5210 | 0.68766 | 0.62059 | 0.61214 * |
| $2^{128}-159$ | 24326737456428468704266740392335053 9132, 27020879817483204922701172229972746 8712 | 0.74262 * | 0.56865 | 0.50100 |
| | 55401819577318168010061270369451294976, 16932721170062974039116472397285204 6130 | 0.64466 | 0.64466 * | 0.51726 |
| | 11968281120219477730553883247824104 0430, 19780143067665547712361282937147708 8259 | 0.64289 | 0.62396 | 0.62396 * |

TABLE 3. LCGs with good figures of merit and $a(m-1) < 2^{53}$

| $m$ | $a$ | $M_8(m,a)$ | $M_{16}(m,a)$ | $M_{32}(m,a)$ |
|---|---|---|---|---|
| $2^{28} - 57 = 268435399$ | 31792125 | 0.75519 * | 0.62442 | 0.61882 |
| | 28932291 | 0.68564 | 0.67353 * | 0.64453 |
| | 18225409 | 0.68003 | 0.66230 | 0.66230 * |
| $2^{29} - 3 = 536870909$ | 16538103 | 0.75238 * | 0.59538 | 0.59538 |
| | 3893367 | 0.69582 | 0.67168 * | 0.62950 |
| | 4723776 | 0.68494 | 0.66667 | 0.66418 * |
| | 5993731 | 0.67352 | 0.67088 | 0.66418 * |
| $2^{30} - 35 = 1073741789$ | 5122456 | 0.73967 * | 0.59108 | 0.59108 |
| | 4367618 | 0.70100 | 0.67634 * | 0.59583 |
| | 6453531 | 0.66184 | 0.65253 | 0.65253 * |
| $2^{31} - 1 = 2147483647$ | 1389796 | 0.72332 * | 0.58994 | 0.57735 |
| | 950975 | 0.67392 | 0.66519 * | 0.60858 |
| | 3467255 | 0.66306 | 0.65379 | 0.65379 * |
| $2^{32} - 5 = 4294967291$ | 657618 | 0.72484 * | 0.47308 | 0.47308 |
| | 93167 | 0.65996 | 0.65996 * | 0.62613 |
| | 1345659 | 0.65121 | 0.65121 | 0.65121 * |
| $2^{33} - 9 = 8589934583$ | 340416 | 0.74831 * | 0.54269 | 0.54269 |
| | 885918 | 0.66495 | 0.66295 * | 0.65151 |
| | 530399 | 0.67694 | 0.65619 | 0.65438 * |
| $2^{34} - 41 = 17179869143$ | 102311 | 0.72236 * | 0.53661 | 0.53661 |
| | 151586 | 0.65895 | 0.65355 * | 0.56180 |
| | 97779 | 0.67327 | 0.64581 | 0.64581 * |
| $2^{35} - 31 = 34359738337$ | 200105 | 0.70888 * | 0.59919 | 0.59919 |
| | 258524 | 0.64888 | 0.64749 * | 0.60094 |
| | 185852 | 0.65064 | 0.64725 | 0.64725 * |

## 3. Power-of-two moduli

We now report a computer search for the case where $m = 2^e$ for some positive integer $e$. In this case, the maximal period of the MLCG (1) is $2^{e-2} = m/4$, attained (in particular) if $a \mod 8 = 5$. The period length can be increased to $m$ if (1) is replaced by

$$x_n = (ax_{n-1} + c) \mod m, \tag{9}$$

where $c > 0$ is odd, and $a \mod 8 = 5$ (see, e.g., [3, 5]). Redefine $\Psi(m) = \{a \in \mathbf{Z}_m : a \mod 8 = 5\}$. In the case where $c$ is odd, $T_t$, $d_t(a,m)$, $d_t^*(m)$, etc., are defined as before. For the MLCG case ($c = 0$), redefine

$$\begin{aligned} T_t &= \{\mathbf{u}_n = (u_n, \ldots, u_{n+t-1}) \mid n \geq 0,\ x_0 \in \mathbf{Z}_m \text{ and } x_0 \bmod 4 = 1\} \\ &= \{(u_n, \ldots, u_{n+t-1}) \mid n \geq 0,\ x_0 = 1\}. \end{aligned}$$

This set has cardinality $m/4$ and is the intersection of a shifted lattice $L_t$ with $[0,1)^t$ ([5]). In this case, the lower bound on $d_t$ becomes $d_t^*(m) = \gamma_t^{-1}(m/4)^{-1/t}$.

LCGs with power-of-two moduli have a major drawback: The $(r+1)$th most significant bit has period length at most $2^{-r}$ times that of the most significant bit. The low order bits thus have rather short period lengths, and for this reason, many authors recommend avoiding these generators for simulation. However, if $e$ is very large and only the most significant bits are used (e.g., if $e = 128$ and the 53 most significant bits of each $x_n$ are used to construct a floating-point number between 0 and 1), this drawback becomes much less important. Also, in the case where the entire set of points $T_t$ is used for quasi-Monte Carlo integration, this

periodicity issue is no longer relevant. The major reason for considering power-of-two moduli is that it makes (1) and (9) easy to implement on a computer and yields fast generators.

TABLE 4. LCGs with good figures of merit, for $m = 2^e$ and $c$ odd

| $m$ | $a$ | $M_8(m,a)$ | $M_{16}(m,a)$ | $M_{32}(m,a)$ |
|---|---|---|---|---|
| $2^{30}$ | 438293613 | 0.75107 * | 0.58300 | 0.58300 |
| | 523592853 | 0.70068 | 0.67686 * | 0.64694 |
| * | 0.64694 | | | |
| | 116646453 | 0.67718 | 0.67420 | 0.67107 * |
| $2^{31}$ | 37769685 | 0.75896 * | 0.51494 | 0.51494 |
| | 26757677 | 0.68312 | 0.68289 * | 0.62474 |
| | 20501397 | 0.67787 | 0.67787 | 0.66548 * |
| $2^{32}$ | 2891336453 | 0.75466 * | 0.56806 | 0.56806 |
| | 29943829 | 0.67429 | 0.67105 * | 0.58062 |
| | 32310901 | 0.65630 | 0.65336 | 0.65336 * |
| $2^{33}$ | 3766383685 | 0.75029 * | 0.56952 | 0.56952 |
| | 32684613 | 0.68055 | 0.67255 * | 0.62595 |
| | 5080384621 | 0.66619 | 0.66604 | 0.66604 * |
| $2^{34}$ | 52765661 | 0.74421 * | 0.54362 | 0.54362 |
| | 50004141 | 0.68442 | 0.67057 * | 0.65570 |
| | 67037349 | 0.69761 | 0.66579 | 0.66579 * |
| $2^{35}$ | 22475205 | 0.74676 * | 0.59182 | 0.59182 |
| | 15319397 | 0.67472 | 0.66933 * | 0.60508 |
| | 15550228621 | 0.65734 | 0.65552 | 0.65552 * |
| $2^{36}$ | 12132445 | 0.75179 * | 0.51869 | 0.51869 |
| | 8572309 | 0.66450 | 0.66389 * | 0.63361 |
| | 33690453 | 0.68461 | 0.65808 | 0.65760 * |
| $2^{40}$ | 330169576829 | 0.75723 * | 0.46879 | 0.46879 |
| | 42595477 | 0.67959 | 0.66436 * | 0.60251 |
| | 33261733 | 0.65941 | 0.65477 | 0.65477 * |
| $2^{48}$ | 181465474592829 | 0.75812 * | 0.54668 | 0.54668 |
| | 77596615844045 | 0.67653 | 0.66906 * | 0.61130 |
| | 10430376854301 | 0.66530 | 0.64759 | 0.64759 * |
| $2^{60}$ | 454339144066433781 | 0.75956 * | 0.57465 | 0.55002 |
| | 21828622668691829 | 0.65844 | 0.65566 * | 0.63458 |
| | 395904651965728677 | 0.63944 | 0.63944 | 0.63944 * |
| $2^{63}$ | 9219741426499971445 | 0.73715 * | 0.54235 | 0.54235 |
| | 2806196910506780709 | 0.69668 | 0.66519 * | 0.60754 |
| | 3249286849523012805 | 0.64507 | 0.63523 | 0.63523 * |
| $2^{64}$ | 2862933555777941757 | 0.75673 * | 0.55283 | 0.54445 |
| | 3202034522624059733 | 0.66164 | 0.66041 * | 0.60256 |
| | 3935559000370003845 | 0.67938 | 0.63763 | 0.63763 * |
| $2^{96}$ | 75564983892026345434470042133 | 0.74760 * | 0.61264 | 0.55571 |
| | 41898663544932533964435923957 | 0.64460 | 0.64460 * | 0.59583 |
| | 22104684854187731770179339485 | 0.65329 | 0.63558 | 0.63287 * |
| $2^{128}$ | 47026247687942121848144207491837418733 | 0.74763 * | 0.53649 | 0.53649 |
| | 52583122484843402430317208685168068605 | 0.70223 | 0.65994 * | 0.56182 |
| | 47026247687942121848144207491837523525 | 0.64332 | 0.63077 | 0.62853 * |

TABLE 5. LCGs with Good Figures of Merit, for $m = 2^e$ and $c = 0$

| $m$ | $a, a^*$ | $M_8(m,a)$ | $M_{16}(m,a)$ | $M_{32}(m,a)$ |
|---|---|---|---|---|
| $2^{30}$ | 177911525, 17372909 | 0.74878 * | 0.53850 | 0.53850 |
| | 156051869, 52274357 | 0.69501 | 0.67940 * | 0.64413 |
| | 143133861, 233896749 | 0.69305 | 0.66791 | 0.66791 * |
| $2^{31}$ | 594156893, 452271861 | 0.75913 * | 0.50244 | 0.50244 |
| | 558177141, 413965533 | 0.68978 | 0.68749 * | 0.59450 |
| | 602169653, 448899357 | 0.67295 | 0.67116 | 0.67116 * |
| $2^{32}$ | 741103597, 887987685 | 0.75652 * | 0.53707 | 0.53707 |
| | 1597334677, 851723965 | 0.70068 | 0.67686 * | 0.64694 |
| | 747796405, 204209821 | 0.66893 | 0.66001 | 0.66001 * |
| $2^{33}$ | 2185253333, 173170557 | 0.75896 * | 0.49707 | 0.49707 |
| | 2174241325, 1406965157 | 0.68312 | 0.68289 * | 0.62250 |
| | 2167985045, 1720311741 | 0.67787 | 0.67787 | 0.66548 * |
| $2^{34}$ | 11481271045, 3694381517 | 0.75466 * | 0.56806 | 0.56806 |
| | 4324911125, 1620027197 | 0.67429 | 0.67105 * | 0.58062 |
| | 4327278197, 3586136541 | 0.65630 | 0.65336 | 0.65336 * |
| $2^{35}$ | 8670442045, 2200188181 | 0.75818 * | 0.51264 | 0.51264 |
| | 8622619205, 6073108621 | 0.68055 | 0.67255 * | 0.60467 |
| | 22260253805, 7113024869 | 0.66619 | 0.66604 | 0.66604 * |
| $2^{36}$ | 4092856269, 14224997637 | 0.75662 * | 0.50169 | 0.50169 |
| | 17229873325, 856580901 | 0.68442 | 0.67057 * | 0.65570 |
| | 17246906533, 12512050989 | 0.69761 | 0.66579 | 0.66579 * |
| $2^{48}$ | 49402601338917, 5567195800493 | 0.75801 * | 0.58062 | 0.58062 |
| | 70189847242853, 69036053825901 | 0.67618 | 0.66857 * | 0.61586 |
| | 21749276838573, 66473811011877 | 0.65702 | 0.64692 | 0.64692 * |
| $2^{60}$ | 276137484736346373, 96397229732113357 | 0.75277 * | 0.48916 | 0.48916 |
| | 150878991426218621, 243765350249586389 | 0.65527 | 0.65510 * | 0.59498 |
| | 271413322654087621, 111008605039107341 | 0.64851 | 0.64851 | 0.64435 * |
| $2^{63}$ | 3512401965023503517, 1447878736930374069 | 0.74926 * | 0.50092 | 0.50092 |
| | 2444805353187672469, 2079243811257762237 | 0.70937 | 0.66091 * | 0.61403 |
| | 1987591058829310733, 1702126216606895045 | 0.64490 | 0.64060 | 0.63994 * |
| $2^{64}$ | 1181783497276652981, 4292484099903637661 | 0.76039 * | 0.42672 | 0.42672 |
| | 7664345821815920749, 1865811235122147685 | 0.67778 | 0.66115 * | 0.54884 |
| | 2685821657736338717, 1803442709493370165 | 0.65961 | 0.63932 | 0.63932 * |
| $2^{128}$ | 250962815189121053421918519178387186629, 556405932620443024807664603523176778 69 | 0.76598 * | 0.55122 | 0.55122 |
| | 237666349757432700979722719899276540 85, 678363655378117076092741683238875617 41 | 0.65708 | 0.65708 * | 0.55662 |
| | 925637045628041860716555878983736061 09, 421954698262383224668211395552858351 25 | 0.63462 | 0.63462 | 0.63405 * |

Table 4 gives the results of the search, for selected powers of two, for the case $c > 0$, $c$ odd. Table 5 gives similar results for $c = 0$. Note that for $c = 0$ and $m = 2^e$, the multiplier $a^* = a^{m/4-1} \mod m$ is the inverse of $a$ modulo $m$, so it produces the same sequence as $a$, but in reverse order, and it has the same values of $d_t$. Table 5 gives the pairs $(a, a^*)$.

## REFERENCES

[1] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Grundlehren der Mathematischen Wissenschaften 290, Springer-Verlag, New York, 1988. MR **89a:**11067

[2] G. S. Fishman, *Multiplicative congruential random number generators with modulus* $2^\beta$*: An exhaustive analysis for* $\beta = 32$ *and a partial analysis for* $\beta = 48$, Mathematics of Computation **54** (1990), no. 189, 331–344. MR **91e:**65012

[3] ———, *Monte Carlo: Concepts, algorithms, and applications*, Springer Series in Operations Research, Springer-Verlag, New York, 1996. MR **97g:**65019

[4] G. S. Fishman and L. S. Moore III, *An exhaustive analysis of multiplicative congruential random number generators with modulus* $2^{31} - 1$, SIAM Journal on Scientific and Statistical Computing **7** (1986), no. 1, 24–45, 1058. MR **87g:**65010

[5] D. E. Knuth, *The art of computer programming, volume 2: Seminumerical algorithms*, second ed., Addison-Wesley, Reading, Mass., 1981. MR **83i:**68003

[6] P. L'Ecuyer, *Efficient and portable combined random number generators*, Communications of the ACM **31** (1988), no. 6, 742–749 and 774. See also the correspondence in the same journal, **32** (1989), no. 8, 1019–1024. MR **89d:**65005

[7] ———, *Random number generation*, Handbook on Simulation (Jerry Banks, ed.), Wiley, 1998, To appear.

[8] P. L'Ecuyer, F. Blouin, and R. Couture, *A search for good multiple recursive random number generators*, ACM Transactions on Modeling and Computer Simulation **3** (1993), no. 2, 87–98.

[9] P. L'Ecuyer and R. Couture, *An implementation of the lattice and spectral tests for multiple recursive linear random number generators*, INFORMS Journal on Computing **9** (1997), no. 2, 206–217. CMP 98:03

[10] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, SIAM CBMS-NSF Regional Conference Series in Applied Mathematics, vol. 63, SIAM, Philadelphia, 1992. MR **93k:**65008

[11] M. Sakamoto and S. Morito, *Combination of multiplicative congruential random number generators with safe prime modulus*, Proceedings of the 1995 Winter Simulation Conference, IEEE Press, 1995, pp. 309–315.

Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal, H3C 3J7, Canada

*E-mail address*: lecuyer@iro.umontreal.ca