REAMC Report-001(2020)
Issue 1, March 2020

Periodicity of ACORN Sequences with Arbitrary Order and Modulus

Roy S Wikramaratna

REAMC Limited (Reservoir Engineering and Applied Mathematics Consultancy)

4 Nuthatch Close, Poole, Dorset BH17 7XR, United Kingdom

Website: www.reamc-limited.com

Email: rwikramaratna@gmail.com

Telephone: +44(0)7968 707062

Copyright © 2020 REAMC Limited.
Individual personal copies may be made for research and teaching purposes provided that any copies include this copyright statement.
No business, commercial or other use for gain, republication or posting/sharing copies (including on the Web) without explicit permission.

REAMC Limited

Periodicity of ACORN Sequences with Arbitrary Order and Modulus

Roy S Wikramaratna

Abstract

The Additive Congruential Random Number (ACORN) generator represents an approach to generating uniformly distributed pseudo-random numbers which is straightforward to implement for arbitrarily large order and modulus (where the modulus is a sufficiently large power of 2, typically up to 2^{120}); it has been demonstrated in previous papers to give rise to sequences with long period which, for the *k*-th order ACORN generator with modulus a power of 2, can be proven from theoretical considerations to approximate in a particular defined sense to the desired properties of uniformity in up to *k* dimensions.

In this paper we state and prove a theorem concerning the exact period length for an ACORN sequence with any given order and any integer modulus (which may either be a prime power, or a composite modulus with two or more different prime factors each raised to a possibly different power) for cases where the seed and modulus are assumed to be relatively prime.

For those cases where the modulus is a prime number or has just one single prime factor raised to an integer power, we show that this theorem is exactly equivalent to an existing, but previously unproven, conjecture concerning the periodicity. The theorem also extends the periodicity results beyond those in the conjecture, to include those cases where the modulus is composite, having two or more prime factors each of which might be raised to a different integer power.

Copyright © 2020 REAMC Limited.

1 OVERVIEW - ACORN SEQUENCES AND ACORN GENERATORS

Let k be a finite, strictly positive integer. A k-th order ACORN sequence is defined from an integer modulus M, an integer seed $Y^0{}_0$ satisfying $0 < Y^0{}_0 < M$ and an arbitrary set of k integer initial values $Y^m{}_0$, $m = 1,\ldots, k$, each satisfying $0 \leq Y^m{}_0 < M$ by the equations

$$Y^0{}_0 = Y^0{}_{n-1} \quad n \geq 1 \tag{1}$$

$$Y^m{}_n = [Y^{m-1}{}_n + Y^m{}_{n-1}]_{\mathrm{mod}M} \quad n \geq 1, m = 1, \ldots, k \tag{2}$$

where by $[Y]_{\mathrm{mod}\ M}$ we mean the (integer) remainder on dividing Y by M. Note that in this paper we will sometimes use a compressed notation where the use of square brackets around a vector or matrix means that each individual component of the relevant vector or matrix is evaluated and the result taken modulo M.

The k-th order Additive Congruential Random Number (ACORN) generator is defined by Wikramaratna [1,2] from equations (1) and (2) together with the observation that the sequence of numbers $Y^k{}_n$ can be normalised to the unit interval by dividing by M

$$X^k{}_n = Y^k{}_n/M \quad n \geq 1 \tag{3}$$

It turns out that the numbers $X^k{}_n$ defined by equations (1) - (3) approximate to being uniformly distributed on the unit interval in up to k dimensions, provided a few simple constraints on the initial parameter values are satisfied. In short the modulus M needs to be a a prime power, with powers of 2 offering the most straightforward implementation, while the seed $Y^0{}_0$ and the modulus should be chosen to be relatively prime (two numbers are said to be relatively prime if they have no prime factors in common, which means that their greatest common divisor is 1). This is the approach that we have adopted in most of our previous experiments with the ACORN generator, and it appears to work very successfully.

The original implementation proposed in [1] used real arithmetic modulo one, calculating the $X^k{}_n$ directly. This implementation suffered from a number of conceptual and practical limitations (in particular, the sequences generated with any specific initialisation could not be guaranteed reproducible on different hardware or with different compilers, although the statistical properties of the sequences were unaffected). These limitations could be overcome [2] through the use of the integer implementation based on equations (1) – (3). Theoretical analysis given by Wikramaratna [2] has shown that the numbers $Y^m{}_n$ are of the form

$$Y^m{}_n = \left[\sum_{i=0}^{m} Y^i{}_0 Z^{m-i}{}_n\right]_{\mathrm{mod}M} \tag{4}$$

where for any integer values of a (non-negative) and b (positive) we define $Z^a{}_b$ by

Copyright © 2020 REAMC Limited.

$$Z^{a}{}_{b} = \frac{(a+b-1)!}{a!(b-1)!} \qquad (5)$$

More extensive theoretical analysis and empirical testing of the algorithm have been described in subsequent papers, including [3] and [4].

From a theoretical viewpoint, it turned out [3] that the ACORN generator was a very particular special case of a multiple recursive generator; when this formulation was written in a specified matrix form, it led in turn to the discovery of some special matrices (called centro-invertible matrices) which have some interesting and unusual properties [5]. The theoretical analysis in [4] led to a proof that a k-th order ACORN generator with modulus 2^{30p} approximates to being k-distributed in a particular sense that was defined in the paper.

Empirical tests carried out previously by the author, making use of the Diehard statistical test suite, Marsaglia [6], have been reported in [3]. Further empirical testing was carried out in 2008 and reported by the author [4], using the Version 0.6.1 of the TestU01 package described by L'Ecuyer and Simard [7]. More recently, further empirical testing has been carried out using the most current Version 1.2.3 of the TestU01 package as reported in [8]; that work has continued and will be reported in more detail in Wikramaratna [9].

Further discussion of ACORN sequences is available at the ACORN website http://acorn.wikramaratna.org/index.html. Included on that website there is a page http://acorn.wikramaratna.org/references.html with a more comprehensive list of relevant ACORN references as well as links, pointing either to downloadable versions of the references, or to other sites where those references can be accessed and downloaded.

2 EXISTING CONJECTURE ON PERIODICITY

A periodic sequence is one in which the values taken by terms in the sequence eventually begin to repeat themselves; in broad terms the period length is the shortest interval over which the sequence recurs. About a decade ago Wikramaratna [3] proposed the following conjecture concerning the period length of ACORN sequences with prime power modulus:

CONJECTURE 1. Let $X^{k}{}_{n}$ be a k-th order ACORN sequence, defined by equations (1)-(3), with modulus equal to a prime power, say $M = q^{t}$, where q is a prime and t is a positive integer and suppose that the seed and modulus are chosen to be relatively prime. Then the sequence $X^{k}{}_{n}$, $k = 1, \ldots, n$ will have a period length equal to $q^{i}M = q^{i+t}$, where i is the largest integer such that $q^{i} \leq k$. □

Copyright © 2020 REAMC Limited.

The conjecture was based on the results of numerical experiments that were undertaken with a wide range of choices of modulus, seed and initial value; until now there has been no published proof.

The following sections of the present paper are devoted to the development of some relevant background, followed by the statement and proof of a theorem concerning the periodicity of ACORN sequences having arbitrary modulus, where the seed is chosen such that it is relatively prime with the modulus. For those cases where the modulus is either a prime number or a prime raised to an integer power, the theorem is exactly equivalent to the corresponding cases in the conjecture – thus the proof of the theorem is also a proof of the conjecture. The theorem also extends the result to the general case where the modulus has two or more distinct prime factors, each raised to a (possibly different) integer power.

3 MATRIX FORMS OF ACORN EQUATIONS

It should be observed that there is more than one way in which the ACORN equations (1) – (3) can be represented in matrix form. The form that will be adopted in this paper is particularly well suited to the analysis of periodicity and specifically to the proof of the theorem below. However, we note that it is different from the form of the equations that was adopted in [3] and [5], where the ACORN generator was viewed as a special case of a multiple recursive generator - this required a matrix of size k by k (rather than k+1 by k+1 as in equation (7) of this paper) and different structure and leads to a matrix with different properties. In particular we note that in [3] the resulting matrix turned out to be centro-invertible (which means [5] that its inverse can be found simply by reversing the order of both the rows and columns of the matrix, equivalent to rotating all elements of the matrix through 180º about the mid-point of the matrix). It will be clear from an inspection of equation (7) below that this is not the case with the alternative matrix form of the equations that is considered in this paper.

For any given value of k, define $\mathbf{L}_k$ to be the (k+1) by (k+1) lower triangular matrix with all entries equal to 1 both on the diagonal and in the lower triangle, while all entries in the upper triangle are equal to zero. Let $\mathbf{y}_n$ be the (k+1) vector with i-th component equal to $[Y^{i-1}{}_n]$. Equations (1) and (2) for a k-th order ACORN generator can then be rewritten in matrix form as follows

$$\begin{aligned}\mathbf{y}_n &= ([Y^0{}_n]_{\mathrm{mod}M}, [Y^1{}_n]_{\mathrm{mod}} \ , \ldots, [Y^k{}_n]_{\mathrm{mod}M})^T \\ &= [\mathbf{L}_k \mathbf{y}_{n-1}]_{\mathrm{mod}M} = [(\mathbf{L}_k)^n \mathbf{y}_0]_{\mathrm{mod}M} \end{aligned} \quad (6)$$

Copyright © 2020 REAMC Limited.

We observe that, for each k, the matrix $\mathbf{L}_k$ is an invertible matrix with determinant equal to 1; its inverse is the (k+1) by (k+1) lower triangular matrix with all entries equal to 1 on the diagonal, equal to -1 on the lower "off-diagonal" with unit offset, while all remaining entries in the lower triangle and all entries in the upper triangle are zero. For example, for k=3

$$\mathbf{L}_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad (\mathbf{L}_3)^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{pmatrix} \tag{7}$$

If we write

$$[(\mathbf{L}_k)^n]_{\mathrm{mod}M} = \left(L^n_{k(p,q)}\right) \tag{8}$$

where on the right hand side of this equation the terms $L^n_{k(p,q)}$ represent the individual components of the matrix (modulo M), the indices k and n identify the matrix which is being considered and the power to which it is raised and the subscript terms (p, q) are respectively the row and column indices, each running from 1 to (k+1); then, comparing terms between equations (4), (6) and (8), we obtain

$$\begin{aligned} L^n_{k(p,q)} &= 0 && \text{if } p < q \\ L^n_{k(p,q)} &= \left[Z^{n-1}{}_{p-q+1}\right]_{\mathrm{mod}M} = [Z^{p-q}{}_n]_{\mathrm{mod}M} \\ &= \left[\tfrac{(n+p-q-1)!}{(p-q)!(n-1)!}\right]_{\mathrm{mod}M} && \text{if } p \geq q \end{aligned} \tag{9}$$

where the meaning of $Z^a{}_b$ is as defined previously in equation (5). It should be noted that the right hand side of equation (9) is a function of (p-q), so that each matrix $(\mathbf{L}_k)^n$ is a lower triangular matrix with constant values along the diagonal (equal to 1) and with a (possibly different) constant value along each lower off-diagonal with fixed offset.

4 PERIOD LENGTH FOR ACORN SEQUENCES

THEOREM 1. Let $X^k{}_n$ be a k -th order ACORN sequence, defined by equations (1) and (2), and then normalised to the unit interval as in equation (3), with modulus

$$M = \prod_{r=1}^{s} (q_r)^{t_r} \tag{10}$$

where each q_r is a prime (ordered such that $q_r < q_{r+1}$), each t_r is a positive integer and suppose that the seed and modulus are chosen to be relatively prime. Then the sequence $X^k{}_n$, k = 1,…, n will have a period length equal to

$$P = \prod_{r=1}^{s} (q_r)^{i_r} M \tag{11}$$

Copyright © 2020 REAMC Limited.

where for each r, i_r is the largest integer such that

$$(q_r)^{i_r} \leq k \tag{12}$$

Proof

The proof is in two parts.

(i) In the first part it is proved that, provided the seed and modulus are relatively prime, then a necessary and sufficient condition for the period to be N is that $[(\mathbf{L}_k)^N]_{\mathrm{mod}M}=\mathbf{I}$ (where $\mathbf{I}$ is the k+1 by k+1 identity matrix) and $[(\mathbf{L}_k)^N]_{\mathrm{mod}M}\neq\mathbf{I}$ for any $n<N$.

The sufficiency of this condition is obvious: from equation (6) we obtain

$$\mathbf{y}_{N+r} = [(\mathbf{L}_k)^N]_{\mathrm{mod}M}\mathbf{y}_r = \mathbf{I}\mathbf{y}_r = \mathbf{y}_r \tag{13}$$

This holds for all r and N is the smallest value for which it holds, which is the definition of the period length.

Necessity is also clear. Suppose (assumption A) that $[(\mathbf{L}_k)^N]_{\mathrm{mod}M}\neq\mathbf{I}$; we know from (9) that $L^N_{k(1,1)} = 1$ and there must be at least one other non-zero element in the first column of $[(\mathbf{L}_k)^N]_{\mathrm{mod}M}$ (if not, this would contradict assumption A - since each lower off-diagonal has constant values). Suppose that the second non-zero element is in row t, so that $L^N_{k(t,1)}$ is the second non-zero element in the first column of the matrix. From an inspection of equation (9) it can be seen that in this case the t-th row of the matrix can have only two non-zero elements; thus if we write ${Y^{t-1}}_0$ for the t-th element of the vector $\mathbf{y}_0$ then in this case the t-th row of the matrix equation (6) reduces to

$$L^N_{k(t,1)}{Y^0}_0 + L^N_{k(t,t)}{Y^{t-1}}_0 = {Y^{t-1}}_0 \tag{14}$$

and since the terms on the diagonal are all equal to 1, this in turn requires

$$L^N_{k(t,1)}{Y^0}_0 = \left(1 - L^N_{k(t,t)}\right){Y^{t-1}}_0 = 0 \tag{15}$$

Remembering that this equation must be satisfied modulo M, and that the seed ${Y^0}_0$ and the modulus are relatively prime, this equation can only be satisfied if $L^N_{k(t,1)}$is divisible by M and therefore equal to zero modulo M. This contradicts assumption A, proving that the condition $[(\mathbf{L}_k)^N]_{\mathrm{mod}M}=\mathbf{I}$ is necessary.

This completes the first part of the proof.

(ii) In the second part of the proof we will use mathematical induction on the order k of the generator, together with the result of the first part of the proof, to prove the theorem.

Copyright © 2020 REAMC Limited.

Consider first the cases where p-q=1 (when k=1 this means that p=2 and q=1)

$$Z^1{}_n = n \tag{16}$$

Choosing n=M gives the smallest solution with equation (16) equal to zero modulo M. Hence the period for a first-order ACORN sequence must be equal to M, provided that the seed and the modulus are relatively prime. This proves the theorem for k=1.

Now suppose that the theorem holds for all k less than or equal to K. Suppose that the period length for the K-th order sequence is n_KM. Then the theorem will be proved if we can show that (a) n_{K+1} is equal to Pn_K whenever K+1 is a power of a prime P which is a factor of M; (b) n_{K+1} is equal to n_K whenever K+1 is a power of a prime P which is not a factor of M; (c) n_{K+1} is equal to n_K whenever K+1 is a composite number, ie has two or more different prime factors which may each be raised to any integer power greater than or equal to 1. We will consider each of these cases separately in the relevant paragraphs below.

We know that (K+1) can be written in the form (K+1)=ab where all the prime factors of a are also prime factors of M and where b and M are relatively prime (and where we allow the possibility that either a or b may be equal to 1; we observe that a and b cannot both be 1 by the induction hypothesis).

Let T be a positive integer. We can write

$$Z^{K+1}{}_{Tn_KM} = \frac{(Tn_KM+K)!}{(K+1)!(Tn_KM-1)!} = \frac{(Tn_KM)(Tn_KM+1)\ldots(Tn_KM+K)}{(K+1)!}$$

$$= \frac{(Tn_KM)}{(K+1)} Z^K{}_{n_KM+1} = \frac{(Tn_KM)}{a} \frac{Z^K{}_{n_KM+1}}{b} \tag{17}$$

This equation holds for any integer value of T, and clearly still holds if both sides are evaluated modulo M. We now consider three options depending on the value of K+1.

(a) Suppose K+1 is a power of a prime, and the prime (which we shall call P) is a factor of M.

By assumption, this requires b=1. By the induction hypothesis, we know that $\left[Z^K{}_{n_KM+1}\right]_{\mathrm{mod}M} = [Z^K{}_1]_{\mathrm{mod}M} = 1$ and so in this case equation (17), when evaluated modulo M, reduces to

$$\left[Z^{K+1}{}_{Tn_KM}\right]_{\mathrm{mod}M} = \left[\frac{(Tn_KM)}{a}\right]_{\mathrm{mod}M} \tag{18}$$

By the induction hypothesis when K+1 is a prime power, n_K is divisible by a/P, but not by a (since K+1=a=P^t for some integer t, the largest power of P less than or equal

Copyright © 2020 REAMC Limited.

to K must be $P^{t-1} = a/P$). Hence T=P is the smallest value of T such that equation (18) is equal to zero. We have shown that in this case n_{K+1}=Pn_K, as required for the theorem.

(b) Suppose K+1 is a power of a prime (which we shall call P), but the prime is not a factor of the modulus M.

In this case a=1 and b has just a single prime factor raised to some power. Suppose we put a=1 and also set T=1 in equation (17)

$$Z^{K+1}{}_{n_K M} = \frac{(n_K M)}{(K+1)} Z^{K}{}_{n_K M+1}$$

$$= n_K M \left(\frac{Z^{K}{}_{n_K M+1}}{b} \right) \qquad (19)$$

The left hand side of equation (19) is a binomial coefficient and hence by a standard result in Number Theory (for example, see Hardy and Wright [10], Theorem 73) it must be an integer. We know by its definition that b does not have any factors in common with either M or n_K, so therefore it follows that the final term in brackets on the right hand side of equation (19) must also be an integer. Hence it follows that

$$\left[Z^{K+1}{}_{n_K M} \right]_{\mathrm{mod} M} = \left[n_K M \frac{(Z^{K}{}_{n_K M+1})}{b} \right]_{\mathrm{mod} M} = 0 \qquad (20)$$

Therefore we have shown that in this case n_{K+1} must be equal to n_K, as required for the theorem.

(c) Suppose finally that K+1 is composite, so that it is not a prime power. Setting T=1 in equation (17), then

$$Z^{K+1}{}_{n_K M} = \frac{(n_K M)}{a} \frac{Z^{K}{}_{n_K M+1}}{b} \qquad (21)$$

We note that it is possible in (21) that either a or b may be equal to 1; however if a=1 then b must be composite and if b=1 then a must be composite (since otherwise K+1 would have only a single prime factor, contradicting the assumption that it is not a prime power). By the induction hypothesis, since K+1 is not a prime power, n_K must clearly be divisible by a. On the other hand, neither n_K nor M can be divisible by b, so by an analogous argument to that used in part (b) above, we require the final term in brackets on the right hand side of equation (21) to be an integer. Hence it follows that

$$\left[Z^{K+1}{}_{n_K M} \right]_{\mathrm{mod} M} = \left[\frac{n_K M}{a} \frac{(Z^{K}{}_{n_K M+1})}{b} \right]_{\mathrm{mod} M} = 0 \qquad (22)$$

Copyright © 2020 REAMC Limited.

Therefore we have shown that in this case n_{K+1} must be equal to n_K, as required for the theorem.

Given that the induction hypothesis holds for K, the combination of the cases (a), (b) and (c) above proves the induction hypothesis holds for K+1; we have already shown that it holds for K=1 and hence it must hold for all K; this completes the proof of the Theorem. □

For the special case where the modulus is equal to the product of the first s prime numbers greater than 1 there is a simpler way of writing the period length, specified in the theorem by equations (11) and (12). This is given by the following Corollary 1, where we define L_k to be the least common multiple of the first k integers (the use of curly brackets to denote the least common multiplier follows the notation adopted by Hardy and Wright [10])

$$L_k = \{1,2,\dots,k\} \tag{23}$$

Corollary 1. Let ${X^k}_n$ be a k-th order ACORN sequence, as in Theorem 1, and suppose that the modulus M is equal to the product of the first s prime numbers greater than 1, ie p_1=2, p_2=3, … p_s.

$$M = \prod_{i=1}^{s} p_i \tag{24}$$

Let L_k be the least common multiple of the first k integers, as defined by equation (23). Then for any $p_s \le k < p_{s+1}$ (where p_{s+1} is the (s+1)-th prime number greater than 1) the sequence ${X^k}_n$ will have period length equal to

$$P = ML_k \tag{25}$$

Proof

The conditions of the Corollary 1 satisfy the conditions of Theorem 1 with the added restriction that the primes q_r, r=1,…,s defined in the theorem are required to be the first s prime numbers greater than 1, thus q_r=p_r for each r. The Corollary will be proven provided it can be established that

$$L_k = \prod_{r=1}^{s} (p_r)^{i_r} \tag{26}$$

where for each r, i_r is the largest integer such that

$$(p_r)^{i_r} \le k \tag{27}$$

This follows immediately from the definition of the least common multiple of k integers as the smallest number that is divisible by each of those k integers: first, L_k must be divisible by each of the terms in the product on the right hand side of equation (26), since by equation

Copyright © 2020 REAMC Limited.

(27) each such term is an integer less than or equal to k; secondly, every integer less than or equal to k can be written as a product of powers of the p_r, with the power of p_r being less than or equal to the corresponding i_r (since otherwise this would require the integer in question to be greater than k). □

5 PRACTICAL IMPLICATIONS OF PERIODICITY RESULTS

In existing implementations of the ACORN random number generator it was convenient to select a modulus 2^{30p} for a small integer value of p giving a sequence with period length in each case being a small multiple of the modulus. In practice p=1 gives rise to sequences that are too short for use in some practical applications, so p=2 was the preferred choice in early implementations; larger values of p have also been considered and in recent and ongoing work [8,9] a choice of p=4 appears to give a very good approximation to uniformity for an extremely wide choice of initialisations while also providing a good balance between period length and speed of execution. These choices of modulus also give rise to a particularly simple implementation of the ACORN algorithm in any high-level programming language (see [3] for an example of an implementation in Fortran for the case p=2, which generalises easily to arbitrary p). The results obtained in Theorem 1 can be applied to derive the exact period length for ACORN random number generators (of any given order k) with modulus equal to 2^{30p} for any integer value of p and having an odd value for the seed, as shown in Table 1 for some example cases.

Table 1 Period length for ACORN generators of order up to 63 and for modulus 2^{60} (p=2) or 2^{120} (p=4), calculated using Theorem 2 assuming an odd seed value.

	Modulus $M=2^{60}$	Modulus $M=2^{120}$
Order k=1	2^{60}	2^{120}
Order k=2,3	2^{61}	2^{121}
Order k=4,5,6,7	2^{62}	2^{122}
Order k=8,9,10,…,15	2^{63}	2^{123}
Order k=16,17,18,…,31	2^{64}	2^{124}
Order k=32,33,34,…,63	2^{65}	2^{125}

Copyright © 2020 REAMC Limited.

As demonstrated by the Theorem, choosing a composite modulus can give rise to sequences with longer period length for similar magnitude of the modulus. However it should be noted that in general, despite the increase in period length, the resulting sequences are more constrained by the requirement of no common factors between the seed and modulus and also do not have the same uniformity properties as do sequences with modulus a power of 2. For example, choosing the modulus equal to a product of different prime factors (each raised to the power 1) leads to ACORN sequences that consistently fail on a few of the standard tests of uniformity that are included in [7] (this remains the case irrespective of how few or how many different prime factors are included in the product) and such choices of composite modulus should therefore be avoided for uniform pseudo-random number generation.

The results obtained in Theorem 1 for composite modulus and also the special case in Corollary 1 are therefore primarily of interest as a mathematical generalisation of the earlier Conjecture and are not being proposed or recommended as an alternative route for uniform pseudo random number generation. ACORN sequences with modulus a sufficiently large power of 2 remain the preferred choice in ACORN random number generators.

6 CONCLUSIONS

ACORN sequences with modulus a sufficiently large power of 2 have been demonstrated in previous papers to be a reliable source of uniformly distributed pseudo-random numbers which perform well on the standard tests for uniformity.

The main result in this paper is a Theorem which allows the period length to be calculated for any ACORN sequence having arbitrary modulus, provided only that the seed and modulus are relatively prime. For modulus a power of 2 and an odd value for the seed, the Theorem can be applied to determine the period length of the resulting ACORN sequence.

It is worth noting that in those special cases where the modulus is either prime or equal to a prime number raised to an integer power, this Theorem reduces precisely to a previously unproven Conjecture which was originally proposed (in 2008) by Wikramaratna [3].

The Theorem goes further, extending the result to composite modulus; however it should be noted that in general, despite the increase in period length, ACORN sequences with composite modulus may not pass all of the standard tests for uniformity and using a composite modulus is therefore not considered appropriate for a source of uniformly distributed pseudo random numbers.

Copyright © 2020 REAMC Limited.

REFERENCES

1 R.S. Wikramaratna, ACORN - A New Method for Generating Sequences of Uniformly Distributed Pseudo-random Numbers, *J. Comput. Phys.*, **83**, pp16-31, 1989.

2 R.S. Wikramaratna, Theoretical Background for the ACORN Random Number Generator, Report AEA-APS-0244, AEA Technology, Winfrith, Dorset, UK, 1992.

3 R.S. Wikramaratna, The Additive Congruential Random Number Generator – A Special Case of a Multiple Recursive Generator, *J. Comput. and Appl. Mathematics*, **261**, pp371–387, 2008. [doi: 10.1016/j.cam.2007.05.018].

4 R.S. Wikramaratna, Theoretical and Empirical Convergence Results for Additive Congruential Random Number Generators, *J. Comput. Appl. Math.*, **233**, pp2302-2311, 2010. [doi: 10.1016/j.cam.2009.10.015].

5 R.S. Wikramaratna, The Centro-invertible Matrix: A New Type of Matrix Arising in Pseudo-random Number Generation, *Linear Algebra and Its Applications*, **434**, pp144-151, 2011. [doi: 10.1016/j.laa.2010.08.011].

6 G. Marsaglia, The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness, Florida State University, Florida, USA, 1995. (http://stat.fsu.edu/pub/diehard).

7 P. L'Ecuyer and R. Simard, TestU01: A C Library for Empirical Testing of Random Number Generators, *ACM Transactions on Mathematical Software*, **33**, 4, Article 22, 2007.

8 R.S. Wikramaratna, Statistical Testing of Additive Congruential Random Number (ACORN) Generators, Meeting on 'Numerical algorithms for high-performance computational science', April 2019, The Royal Society, London, UK. [Link for download is available at http://acorn.wikramaratna.org/references.html].

9 R.S. Wikramaratna, Statistical Performance of Additive Congruential Random Number Generators, REAMC Report-002, 2020 (in preparation). REAMC Limited, UK.

10 G. H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, 5th Edition, Oxford University Press, 426pp, 1979 (reprinted 1989).

Copyright © 2020 REAMC Limited.