REAMC Report-002(2020)
Issue 1, November 2020

Statistical Performance of Additive Congruential Random Number Generators

Part 1 - Results of Testing Some Specific Seed Values

Roy S Wikramaratna

REAMC Limited (Reservoir Engineering and Applied Mathematics Consultancy)

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

Website: https://www.reamc-limited.com

Email: rwikramaratna@gmail.com

Telephone: +44(0)7968 707062

REAMC®
Limited

Statistical Performance of Additive Congruential Random Number Generators

Part 1 - Results of Testing Some Specific Seed Values

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.

Extensive empirical testing using standard test software has demonstrated the excellent statistical performance of the ACORN generators with appropriately chosen order and modulus, over a very wide range of initialisations. In this report we present results of comprehensive testing, using the standard TestU01 package, for ACORN generators having modulus equal to 2^{120}, for all orders between 8 and 25 and a selection of larger values up to 101, and for a wide range of seed values. The main objective in this report has been to explore whether there are particular choices of seed for which the statistical performance of the resulting ACORN sequences fall below the levels that can generally be expected.

The results presented in this report have identified a relatively small number of very specific seed values that need to be avoided. Some specific seeds to be avoided include very small values (close to 1) or very large seed values (such that 2^{120} minus the seed is close to 1); also, certain values such that the seed divided by the modulus closely approximates a rational fraction of the form *a*/*n* where *n* is an odd integer and *a* is an integer less than *n*.

Given that there are 2^{119} different possible choices of odd seed, it is not computationally feasible to test all the possible choices of seed or to enumerate all the seed values that should be avoided. However, based on the results of these tests, we are able to make a very powerful conjecture (which will be proposed, discussed and tested in part 2 of this report [1]) concerning the likelihood of an ACORN generator with order at least 8, modulus 2^{120} and a randomly chosen seed value passing all the TestU01 BigCrush tests - which turns out to be an almost certain event.

1 INTRODUCTION

The Additive Congruential Random Number (ACORN) generator is a method for generating uniformly distributed pseudo-random numbers which gives rise to sequences with long period which can be proven from theoretical considerations to approximate to uniformity in any specified number of dimensions. Extensive empirical testing has previously demonstrated the excellent statistical performance of the ACORN generators with appropriately chosen parameters over a very wide range of initialisations.

This is the first part of a two-part report in which the standard TestU01 package of statistical tests for uniform distribution of sequences are applied to a range of ACORN sequences having modulus equal to 2^{120}, with different seed values and a range of different orders from 8 through 25 as well as a selection of larger orders up to 101. The results presented here in Part 1 of the report are focussed on testing ACORN sequences with a wide selection of different seeds and identifying some very specific seed values that should be avoided (most notably seeds that are very small or very close to the modulus; also cases where the seed divided by the modulus approximates very closely to certain rational fractions). Results demonstrate that making relatively minor perturbations to those seed values results in ACORN sequences that successfully pass all the TestU01 tests.

Part 2 of the report is currently in preparation [1]; it will present some significant conjectures on the very wide range of conditions (specifically relating to the choice of seed and initial values) under which ACORN sequences having modulus 120 and order 8 or larger can be expected to reliably pass all the TestU01 tests. The conjectures cover the case of sequences having all initial values equal to zero as well as the case of sequences having non-zero initial values. Results will be presented to support the conjectures for a wide range of ACORN generators having order 8, 9 or 10 and different seeds and initial values selected according to the criteria specified in the conjectures.

Section 2 of the present report provides the definition of an ACORN sequence and an overview of the existing theoretical analysis and empirical test results that have been published to date. Section 3 gives a brief overview of the standard TestU01 package of empirical tests of uniformity and randomness that has been used in this work.

The main content of the present report is included in Section 4, which details the test cases that are considered in this report and Section 5 which includes both tabulations and a discussion of the results.

2 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 $Y^m{}_0$, $m = 1,..., k$, each satisfying $0 \leq Y^m{}_0 < M$ by the equations

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

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

where by $[Y]_{\mathrm{mod}\,M}$ we mean the (integer) remainder on dividing Y by M.

The k-th order Additive Congruential Random Number (ACORN) generator is defined by Wikramaratna [2,3] 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

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

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 [2] 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 [3] through the use of the integer implementation based on equations (1) – (3). Theoretical analysis given by Wikramaratna [3] 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

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

More extensive theoretical analysis and empirical testing of the algorithm have been described in subsequent papers, including [4] and [5].

From a theoretical viewpoint [4] the ACORN generator was shown to be 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 [6]. The theoretical analysis in [5] 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 [7], have been reported in [4]. Further empirical testing was carried out in 2008 and reported by the author [5], using the Version 0.6.1 of the TestU01 package described by L'Ecuyer and Simard [8]. More recently, empirical testing has been carried out using the most current Version 1.2.3 of the TestU01 package as reported in [9] and [10]; that work has now been systematically extended to ACORN generators with much wider choices of initialisations.

A recent paper by Wikramaratna [11] addressed the periodicity of ACORN sequences for any specified order, modulus and any choice of seed that is relatively prime with the modulus. As an example, every ACORN generator with order at least 8, modulus 2^{120} and any choice of odd seed has a period length in excess of 2^{123}. This period is already far in excess of the maximum period that might be required in the largest conceivable computationally practicable (using hardware available in 2020) application requiring a source of uniformly distributed pseudo-random numbers; however we note that the ACORN algorithm extends naturally and very easily to even longer period lengths simply by increasing the modulus to a larger power of 2.

See also further discussion on the website http://acorn.wikramaratna.org, which includes a more comprehensive list of relevant ACORN references as well as links to downloadable versions of the references. Recent ACORN references (including this report) are available for download from the REAMC Limited website, https://www.reamc-limited.com.

3 EMPIRICAL TEST PACKAGE - TESTU01 VERSION 1.2.3

The TestU01 package has been described by L'Ecuyer and Simard [8]. They considered the application of empirical tests of uniformity and randomness to sequences generated by a wide range of algorithms and developed a comprehensive set of empirical tests that were designed to detect undesirable characteristics in such sequences. L'Ecuyer and Simard present results of applying the TestU01 tests to a large number of different sequences, identifying specific generators that pass all of the tests (collectively called the BigCrush test battery), as well as identifying many generators (including some that are widely used) that have serious deficiencies in respect of certain specific tests.

The results presented below for ACORN generators (which were not included among generators considered by L'Ecuyer and Simard) were obtained using the latest version 1.2.3 of TestU01. For each sequence that is tested the BigCrush battery of tests calculates p-values for 180 different test statistics, making use of some 2^{38} pseudo-random numbers from each sequence. We follow L'Ecuyer and Simard in defining a "failure" to be a test statistic with a p-value outside the range [10^{-10}, $1\text{-}10^{-10}$] and a "suspect" value to be a test statistic falling in one of the ranges [10^{-10}, 10^{-4}] or [$1\text{-}10^{-4}$, $1\text{-}10^{-10}$]. This is the same approach that was adopted in [9]. It is worth noting that there were a number of cases which gave rise to a test result with either p=0.9999 or p=0.0001; for the purpose of this study, this has in all cases been classed as a suspect value rather than a pass; how these cases are treated makes a small difference to the overall number of suspect values, but has no impact on the overall conclusions concerning the statistical behaviour of ACORN sequences.

4 SPECIFICATION OF CASES, M10XX, N10XX AND P10XX

There are three sets of cases that are considered in this first part of the report, respectively numbered M10*xx*, N10*xx* and P10*xx*; these cases have been selected to explore the statistical behaviour of ACORN sequences with seeds chosen to approximate some specific values that may cause difficulties in terms of statistical behaviour. All cases considered here have modulus equal to 2^{120}. The cases have order and seed values as specified in the respective tables of results, and all initial values set to zero. In each case considered here, the seed S is a 120-bit integer. Note that all seeds are chosen to be odd (so that the last digit in the binary representation of the seed is a one). Choosing an odd seed value guarantees that the period of the sequence will be at least eight times the modulus (which comes out as 2^{123} in this instance) for every ACORN generator of order 8 or more (see Wikramaratna [11]). When implementing an ACORN generator using either 64-bit or 32-bit integer arithmetic, the seed S can be represented as follows, either by two 60-bit integers, t_1 and t_2, or by four 30-bit integers s_1, s_2, s_3 and s_4.

$$S = 2^{60}t_1 + t_2 = 2^{90}s_1 + 2^{60}s_2 + 2^{30}s_3 + s_4 \qquad (6)$$

This representation is unique in the sense that it defines a one-one onto mapping between any two of S, (t_1, t_2) and (s_1, s_2, s_3, s_4). In presenting the results it will be helpful to specify the values of s_1, s_2, s_3 and s_4 using base 10 as numbers in the range zero to (2^{30}-1), and values of t_1 and t_2 using base 10 as numbers in the range zero to (2^{60}-1).

The cases M10*xx* with *xx* equal to 01 or between 03 and 09 (the case number M1002 was not used) are cases where the seed is “close to zero” in the sense that at most four out of the 120 binary digits in the binary representation of the seed are equal to 1, with all the remaining digits set to zero. Case M1005 is the only case in this series having four of the digits set equal to 1 (in this case the digits in question are 30, 60, 90 and 120; this is equivalent to setting all four values s_1, s_2, s_3 and s_4 equal to 1). Seed values that are very close to zero, or which have only a very small number of non-zero digits will (when combined with a relatively small order k and all initial values set equal to zero) give rise to a sequence that is initially monotonic increasing for a number of terms, with the length of the initial monotonic part growing larger as the magnitude of the seed reduces. The purpose of these tests is to investigate circumstances under which the use of seeds of this type might lead to more general failures in the statistical behaviour of the resulting sequences.

The cases M10*xx* with *xx* between 50 and 89 are cases where the seed is specified by first setting one digit in each block of 30 consecutive digits in the binary representation of the seed to one, with all the other digits set to zero and then if necessary resetting the final (120th) digit to one to ensure that the seed takes an odd value. In all the cases M105*x*, M106*x* and M107*x* the seed has precisely four non-zero digits, the last of which is the final digit, while in the cases M108*x* the seed has five non-zero digits, the last of which is again the final digit. We note that the earlier case M1005 also has four non-zero digits, the last of which is the final digit; it can usefully be considered again at the same time as these cases.

The cases N10*xx* and M10*xx* are closely related. The seed values in the case N10*xx* are derived from the seed values in the corresponding case M10*xx* in that they sum to 2^{120}. This means in effect that the binary representation of case N10*xx* can be obtained by changing the first 119 digits either from 0 to 1 or from 1 to 0; the final digit is left unchanged, equal to 1, and this ensures that the seed for each case N10*xx* takes an odd value, as did the seed in the corresponding cases M10*xx*.

The cases P10*xx* have seeds specified such that the seed divided by the modulus approximates a rational fraction (1/3, 1/7, …,1/2047) each having an odd divisor of the form (2^{k+2}-1) where k ranges from 0 to 9 and the value taken by k corresponds to the final digit of the case number; we note that comparable results might be expected using other odd divisors of similar magnitude; the particular seed values to be tested were selected in this way in order to keep the number of test cases to a manageable level. In the first 10 cases where *xx* is between 00 and 09 the representation is as accurate as is possible with 120 binary digits, with the final digit always rounded to 1, to ensure that the resulting seed takes an odd value. The remaining three batches of 10 cases (ie the first batch with *xx* between 10 and 19, the second batch with *xx* between 20 and 29 and the third batch with *xx* between 30 and 39) represent small perturbations on the seeds that were used in the first 10 cases - the first 29 binary digits are unchanged and then one or more of the remaining digits are modified in various different ways (with the constraint that the final digit is always left unchanged, equal to 1, so that the resulting seed again take an odd value). The perturbations to the seed have been made as described in the next paragraph.

Suppose that the seed for case P100*x* were defined by the four 30-bit integers (s_1, s_2, s_3, $s_{4)}$. The seed for case P101*x* is then defined to be (s_1, 1, 1, 1); the seed for case P102*x* is defined to be (s_1+1, s_2, s_3, s_4); finally, the seed for case P103*x* is defined to be (s_1-1, s_2, s_3, $s_{4)}$. We note that in all these cases the perturbation has a similar magnitude, and in all cases the perturbed seed takes an odd value.

5 TABULATED RESULTS

5.1 Formats for Presentation of Results

The general discussion of table formats that follows is relevant to the Tables 1 to 6 and 8 to 14; the format adopted for Table 7 will also be discussed below.

Results have been tabulated as follows.

- Each row in the table corresponds to one specific case. In some cases, namely Tables 1, 2 and 8 to14, the final two rows of each table show the average number of failures per case, averaged over the cases that were included in the table. The average number of failures in Tables 3 to 6 is treated slightly differently - rather than include averages at the foot of each table, the averages are summarised in Table 7, with averages being taken separately over the 41 cases that are included in Tables 3 and 4 and over the 41 cases that are included in Tables 5 and 6.
- The first column in each table contains the case number.
- The next four columns specify the seed value that was used for that case; the seed value is uniquely specified by the four integers s_1, s_2, s_3 and s_4 defined as in equation (6) above.
- The remaining columns summarise the results of testing, with the TestU01 BigCrush test suite being applied to ACORN sequences with modulus 2^{120}, order as shown at the top of each column (typically this covers all values between 8 and 25; three of the tables, namely Tables 8, 9 and 14, show results for larger order with selected values in the range 29 to 101), seed as specified and all initial values set to zero. In each column, the first number shown is the number of tests that gave rise to a failure; while the second number (shown in brackets) is the number of tests that gave rise to a suspect value. Cells are highlighted dark pink if the results showed one or more

failures; cells are highlighted green if results showed no failures but one or more suspect values.

5.2 Results of Testing, Cases M10xx and N10xx

Table 1 shows results for the cases M1001 to M1009 (note that the case numbers M1000 and M1002 are not used). These are all cases where the values for $s1$, $s2$, $s3$ and $s4$ (which are used to define the seed, as specified in equation (6)) are all set either to zero or 1; in practice s4 needs to be set to 1 in all these cases, because the seed is required to be an odd integer (which is required in order to ensure maximal period length). Since each of $s1$, $s2$, $s3$ and $s4$ is a 30-bit integer, this means that in these cases the seed has at least 116 zeroes and a maximum of four ones in its binary representation (including the final bit which is always equal to 1). We can make the following observations concerning the results in Table 1:

- The statistical performance is least good for case M1001, in which $s1$=$s2$=$s3$=0 and $s4$=1 (using equation (6) we see that the seed is itself equal to 1 in this case). Despite this, the resulting ACORN generator passes all the TestU01 BigCrush tests for all orders between 15 and 25, and there is just one single suspect value which occurs for order 20. For orders between 11 and 14 there is a single failure on one test; as the order is reduced further below 10 the number of failures increases to a maximum of 34 failures for order 8.
- The three cases M1003, M1006 and M1007 all have one of $s1$, $s2$, $s3$ set equal to 1 and the other two equal to zero. In each of these cases the resulting ACORN generators pass all the TestU01 BigCrush tests for all orders between 10 and 25. Some failures occur for order 8 and 9, with increased numbers of failures for order 8 compared with order 9.
- The three cases M1004, M1008 and M1009 each have two of $s1$, $s2$, $s3$ set equal to 1 and the third one equal to zero. Here the resulting ACORN generators pass all the TestU01 BigCrush tests for all orders between 9 and 25. For order 8, two of the cases give rise to some failures, while the third (M1009) still passes all the tests for order 8.
- The final case M1005 has $s1$=$s2$=$s3$=1 (and of course $s4$=1 as well).The resulting ACORN generators pass all the tests for every order between 8 and 25.
- Across all these tests there are occasional suspect values (at most 1 suspect value per case, in less than 10% of the cases). There is no discernible pattern to the suspect values nor to the particular tests on which they occur, and we conclude that they arise simply by chance because of the natural statistical variations in the sequences of pseudo-random numbers.

Table 2 shows results for the cases N1001 to N1009 (note that the case numbers N1000 and N1002 are not used). The seed for case N100*x* is related to the corresponding seed for case M100*x* in that the two seed values sum to 2^{120}. In effect this means that the binary representation of seed value for case N100*x* can be obtained from the binary representation of the seed value for the corresponding case M100*x* by changing each of the first 119 bits (replacing zero with 1, and 1 with zero) and leaving the final bit unchanged, equal to 1. This means that in these cases the seed has at least 117 ones (including the final bit which is always equal to 1) and a maximum of three zeroes in its binary representation We can make the following observations concerning the results in Table 2:

- The pattern of failures for each of the cases N100*x* is essentially identical to the pattern of failures for the corresponding case M100*x*.
- The frequency of suspect values for the cases N100*x* is comparable to that obtained in the cases M100*x*; there is no obvious correlation between the particular cases that gave rise to suspect values between these two sets of cases.

Table 3 and 4 show results for a range of cases in which the seed has either 4 or 5 non-zero bits; thus *s*1, *s*2 and *s*3 each have one non-zero bit, while *s*4 always has its 30th bit set to one (so that the seed, defined by equation (6) takes an odd value) while its remaining 29 bits are either all zero or else have just a single non-zero bit. Table 3 includes the case M1005 (which has also been included in Table 1) where *s*1=*s*2=*s*3=*s*4=1, because it meets these criteria; also the cases M1050 to M1059 in which *s*1 takes a range of different values, while *s*2=*s*3=*s*4=1; and finally the cases M1060 to M1069 in which *s*2 takes a range of different values while *s*1=*s*3=*s*4=1. Table 4 includes the cases M1070 to M1079 in which *s*3 takes a range of different values while *s*1=*s*2=*s*4=1 and cases M1080 to M1089 in which *s*4 takes a range of different values while *s*1=*s*2=*s*3=1. We can make the following observations concerning the results in Tables 3 and 4:

- The statistical performance is good for all the cases considered for all orders between 9 and 25, with the resulting ACORN generators passing all the TestU01 BigCrush tests for all orders between 9 and 25. Some failures (between one and 3 failures on each case) occur for order 8 for the cases M1053 to M1059 and M1067 to M1069.
- Across all the tests included in Tables 3 and 4 there are occasional suspect values (there are 2 suspect values in just 2 of the cases considered, and a single suspect value in less than 10% of the cases). There is no discernible pattern either to the suspect values or to the particular tests on which they occur, and we conclude that they arise simply by chance because of the natural statistical variations in the sequences of pseudo-random numbers.

Table 5 shows results for the cases N1005, N105*x* and N106*x* (where x takes values between 0 and 9), while Table 6 shows results for the cases N107*x* and N108*x*. As before seed for case N10*xx* is related to the corresponding seed for case M10*xx* in that the two seed values sum to 2^{120}. In effect this means that the binary representation of seed value for case N10*xx* can be obtained from the binary representation of the seed value for the corresponding case M10*xx* by changing each of the first 119 bits (replacing zero with 1, and 1 with zero) and leaving the final bit unchanged, equal to 1. This means that in these cases the seed has at least 116 ones (including the final bit which is always equal to 1) and a maximum of four zeroes in its binary representation. We can make the following observations concerning the results in Tables 5 and 6:

- The statistical performance is good for all the cases considered for all orders between 9 and 25, with the resulting ACORN generators passing all the TestU01 BigCrush tests for all orders between 9 and 25. A small number of failures (between one and 3 failures on each case) occur for order 8 for the cases N1053 to N1059 and N1067 to N1069. Thus the pattern of failures for each of the cases N10*xx* is essentially identical to the pattern of failures for the corresponding case M10*xx*.
- The overall frequency of suspect values for the cases N10*xx* is comparable to that obtained in the cases M10*xx*; there is no obvious correlation between the particular cases that gave rise to suspect values in Tables 3 and 4 and those that gave rise to suspect values in Tables 5 and 6.

Table 7 summarises the average number of failures and the average number of suspect values per case (over the 41 cases in Tables 3 and 4, and over the 41 cases in Tables 5 and 6) for each value of the order between 8 and 25. The results in Table 7 illustrate the statistical similarity of the results for the two sets of cases having the designations M and N respectively; at the same time they illustrate the absence of obvious correlation between the cases giving rise to suspect values from the two sets of results.

Table 8 shows results for some selected orders between 29 and 101 (Cases N100*x* only). All cases show no failures for any of the orders that have been tested. The results for the corresponding Cases M100*x* have not all been calculated, and are not included in this report; however, based on the other results in Tables 1-7, it seems clear that the results for each of the Cases M100*x* will all have virtually identical characteristics to the corresponding Case N100*x*. We can therefore tentatively infer without further testing that all the initialisations that have been tested (in particular all the Cases M100*x* and N100*x*) are likely to pass all the TestU01 BigCrush tests for all orders between 25 and 101 (and, since there is no sign in Table 8 of any deterioration in statistical performance with increasing order, we have no reason to suppose that 101 represents anything close to an upper bound on the range of orders for which this will continue to be the case, or even that such an upper bound exists). Further, since the statistical performance for any given order appears to be as good or better for the cases M105*x*, M106*x*, M107*x* and M108*x* as it is for any of the cases M100x, and since the statistical performance for any given order appears to be as good or better for the cases N105*x*, N106*x*, N107*x* and N108*x* as it is for any of the cases N100*x*, we can also tentatively infer without further testing that these initialisations are also likely to pass all the TestU01 BigCrush tests for all orders between 25 and 101.

5.3 Results of Testing, Cases P10xx

Table 9 shows the results of testing for the cases P100*x* for orders between 8 and 25. The results in Table 9 are comparable to (or slightly better than) the results that were presented in Table 1 for the case M1001. We observe, despite the data being noisy and showing a small amount of fluctuation, that in general the statistical performance improves as the denominator of the rational fraction increases (ie as *x*, the final digit of the case number, increases from 0 to 9).

Tables 10, 11 and 12 show the results of testing for the three sets of cases P101*x*, P102*x* and P103*x*, in each of which a small perturbation is added to the seed value for the corresponding case P100*x*. In all cases the statistical performance is improved compared with the corresponding case in Table 9. For the cases in Table 10, 11 and 12 there are no failures for any order greater than or equal to 10, and only a couple of failures (one failure each in two of the 30 cases) for order 9.

Table 13 shows the results of testing for the cases P100*x* for some selected orders between 29 and 101. All cases show no failures for any of the orders that have been tested. Given that the statistical performance for any given order appears consistently as good or better for the cases in Tables 10, 11 and 12 compared with the corresponding cases in Table 9 we can tentatively infer without further testing (based on the results in Table 13) that all the cases P100*x*, P101*x*, P102*x* and P103*x* are likely to pass all the TestU01 BigCrush tests for all orders between 25 and 101.

In this section we have identified some specific seed values (such that the seed divided by the modulus closely approximates one of a series of specific rational fractions) that may give rise to failures in some of the TestU01 BigCrush tests. It is not possible to enumerate all of the seed values that should be avoided for these or other similar reasons, since exhaustive testing of all possible choices of seed would be too time consuming, but we can make the observation that in practice only a very small proportion of the possible seed values will fall into this category.

6 CONCLUSIONS

Results presented in this report demonstrate that for a wide range of different choices of seed, the resulting sequences will pass all of the tests in the TestU01 BigCrush test suite for modulus 2^{120} and all choices of order greater than or equal to nine and up to at least 25. Tests were also carried out for larger order, up to 101, and the results suggest that the upper bound of 25 is not necessary, and larger order sequences performed equally well.

Some specific seed values (a very small number compared with the 2^{119} different possible choices of odd seed value for an ACORN generator with modulus 2^{120}) have been identified which give rise to failures on a small number of the tests with order up to 14. It is worth noting that for every single one of the seed values tested the resulting ACORN sequences passed all the TestU01 BigCrush tests for any order of 15 or greater.

Seed values to be avoided include very small seed values (the seed value either close to 1, or having less than 4 ones and more than 116 zeroes in its binary representation) or very large seed values (such that 2^{120} minus the seed is either close to 1, or having less than 4 ones and more than 116 zeroes in its binary representation); also, seed values such that the seed divided by the modulus closely approximates a rational fraction of the form a/n where n is an odd integer and a is less than n (including, in particular, cases where a=1, which are illustrated by the test cases P100*x* that were considered above). It should be noted that making a relatively small perturbation of the seed value from one of these values that are ‘to be avoided’ appears to give a seed for which the resulting ACORN sequence will pass all the TestU01 BigCrush tests for any order of 10 or greater (and in many cases for order 9 and 8 as well).

The results presented in this report have identified some very specific seed values that need to be avoided in order to ensure that the resulting ACORN sequence will pass all the TestU01 BigCrush tests over the full range of orders considered; more extensive search would undoubtedly lead to the identification of further seed values which should similarly be avoided. It is not computationally feasible either to test all the possible choices of seed or to enumerate all of the seed values that should be avoided. However, based on the results of these tests, we are able to make a very powerful conjecture (which will be proposed, discussed and tested in Part 2 of this report [1]) concerning the likelihood of an ACORN generator with order at least 8, modulus 2^{120} and a randomly chosen seed value passing all the TestU01 BigCrush tests - which turns out to an almost certain event).

Table 1 Summary of results obtained for Cases M1000 to M1009, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
M1000	Not used																					
M1001	0	0	0	1	34 (1)	21 (6)	5 (0)	1 (0)	1 (0)	1 (0)	1 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1002	Not used																					
M1003	0	0	1	1	22 (2)	5 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)
M1004	0	1	1	1	4 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1005	1	1	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1006	0	1	0	1	4 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (1)
M1007	1	0	0	1	5 (0)	1 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)
M1008	1	0	1	1	3 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1009	1	1	0	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (1)	0 (0)
Average failures - Cases M1001, M1003-M1009					9.00	3.38	0.63	0.13	0.13	0.13	0.13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average suspect values - Cases M1001, M1003-M1009					0.38	0.75	0.13	0.00	0.00	0.13	0.00	0.13	0.00	0.00	0.13	0.00	0.13	0.13	0.25	0.13	0.13	0.13

Table 2 Summary of results obtained for Cases N1000 to N1009, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
N1000	Not used																					
N1001	1073741823	1073741823	1073741823	1073741823	34 (1)	21 (5)	5 (0)	1 (0)	1 (0)	1 (0)	1 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1002	Not used																					
N1003	1073741823	1073741823	1073741822	1073741823	22 (2)	5 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1004	1073741823	1073741822	1073741822	1073741823	4 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1005	1073741822	1073741822	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1006	1073741823	1073741822	1073741823	1073741823	4 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1007	1073741822	1073741823	1073741823	1073741823	5 (0)	1 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)
N1008	1073741822	1073741823	1073741822	1073741823	3 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1009	1073741822	1073741822	1073741823	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
Average failures - Cases N1001, N1003-N1009					9.00	3.38	0.63	0.13	0.13	0.13	0.13	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average suspect values - Cases N1001, N1003-N1009					0.38	0.63	0.00	0.00	0.00	0.00	0.00	0.13	0.00	0.00	0.13	0.00	0.13	0.00	0.13	0.00	0.00	0.00

Table 3 Summary of results obtained for Cases M1005 and M1050 to M1069, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
M1005	1	1	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1050	2	1	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1051	4	1	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1052	8	1	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
M1053	32	1	1	1	1 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1054	1024	1	1	1	1 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)
M1055	1048576	1	1	1	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1056	33554432	1	1	1	3 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1057	134217728	1	1	1	3 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1058	268435456	1	1	1	3 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1059	536870912	1	1	1	3 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)
M1060	1	2	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1061	1	4	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1062	1	8	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1063	1	32	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1064	1	1024	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1065	1	1048576	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
M1066	1	33554432	1	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1067	1	134217728	1	1	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)
M1068	1	268435456	1	1	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1069	1	536870912	1	1	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)

Table 4 Summary of results obtained for Cases M1070 to M1089, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
M1070	1	1	2	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)
M1071	1	1	4	1	0 (0)	0 (0)	0 (0)	0 (2)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1072	1	1	8	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)
M1073	1	1	32	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1074	1	1	1024	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1075	1	1	1048576	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1076	1	1	33554432	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1077	1	1	134217728	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1078	1	1	268435456	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)
M1079	1	1	536870912	1	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1080	1	1	1	3	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (1)	0 (0)	0 (0)	0 (0)
M1081	1	1	1	5	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1082	1	1	1	9	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
M1083	1	1	1	33	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
M1084	1	1	1	1025	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1085	1	1	1	1048577	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)
M1086	1	1	1	33554433	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1087	1	1	1	134217729	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
M1088	1	1	1	268435457	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)
M1089	1	1	1	536870913	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (2)	0 (0)	0 (0)

Table 5 Summary of results obtained for Cases N1005 and N1050 to N1069, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
N1005	1073741822	1073741822	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1050	1073741821	1073741822	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1051	1073741819	1073741822	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1052	1073741815	1073741822	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
N1053	1073741791	1073741822	1073741822	1073741823	1 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1054	1073740799	1073741822	1073741822	1073741823	1 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (1)	0 (0)	0 (0)	0 (0)
N1055	1072693247	1073741822	1073741822	1073741823	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1056	1040187391	1073741822	1073741822	1073741823	3 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1057	939524095	1073741822	1073741822	1073741823	3 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
N1058	805306367	1073741822	1073741822	1073741823	3 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1059	536870911	1073741822	1073741822	1073741823	3 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1060	1073741822	1073741821	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1061	1073741822	1073741819	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1062	1073741822	1073741815	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1063	1073741822	1073741791	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1064	1073741822	1073740799	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1065	1073741822	1072693247	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
N1066	1073741822	1040187391	1073741822	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)
N1067	1073741822	939524095	1073741822	1073741823	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1068	1073741822	805306367	1073741822	1073741823	2 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1069	1073741822	536870911	1073741822	1073741823	2 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)

Table 6 Summary of results obtained for Cases N1070 to N1089, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
N1070	1073741822	1073741822	1073741821	1073741823	0 (1)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1071	1073741822	1073741822	1073741819	1073741823	0 (0)	0 (0)	0 (0)	0 (2)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1072	1073741822	1073741822	1073741815	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)
N1073	1073741822	1073741822	1073741791	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1074	1073741822	1073741822	1073740799	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1075	1073741822	1073741822	1072693247	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1076	1073741822	1073741822	1040187391	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1077	1073741822	1073741822	939524095	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1078	1073741822	1073741822	805306367	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)
N1079	1073741822	1073741822	536870911	1073741823	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1080	1073741822	1073741822	1073741822	1073741821	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)
N1081	1073741822	1073741822	1073741822	1073741819	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1082	1073741822	1073741822	1073741822	1073741815	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
N1083	1073741822	1073741822	1073741822	1073741791	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)
N1084	1073741822	1073741822	1073741822	1073740799	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1085	1073741822	1073741822	1073741822	1072693247	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)
N1086	1073741822	1073741822	1073741822	1040187391	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1087	1073741822	1073741822	1073741822	939524095	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1088	1073741822	1073741822	1073741822	805306367	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)
N1089	1073741822	1073741822	1073741822	536870911	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (1)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (0)	0 (2)	0 (0)	0 (0)

Table 7 Summary of average failures and average suspect values for cases M1005, M1050 - M1089 (shown in Tables 3 & 4) and for cases N1005, N1050 - N1089 (shown in Tables 5 & 6)

	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Average failures - Cases M1005, M1050-M1089	0.54	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Average suspect values - Cases M1005, M1050-M1089	0.05	0.02	0.05	0.07	0.05	0.02	0.02	0.05	0.05	0	0.05	0	0.1	0.12	0.05	0.15	0	0.1
Average failures - Cases N1005, N1050-N1089	0.54	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Average suspect values - Cases N1005, N1050-N1089	0.05	0	0.05	0.07	0.05	0	0	0	0.05	0.02	0.05	0.02	0.02	0.07	0.07	0.1	0	0.12

Table 8 Summary of results obtained for Cases N1000 to N1009, for ACORN generators with modulus 2^{120} and selected orders between 29 and 101

Case	Seed	Seed	Seed	Seed	Order	...	Order	...	Order	...	Order	...	Order	...	Order	...	Order
	s1	s2	s3	s4	29	...	39	...	49	...	59	...	69	...	99	...	101
N1000	Not used																
N1001	1073741823	1073741823	1073741823	1073741823	0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)
N1002	Not used																
N1003	1073741823	1073741823	1073741822	1073741823	0 (0)		0 (0)		0 (1)		0 (0)		0 (0)		0 (0)		0 (0)
N1004	1073741823	1073741822	1073741822	1073741823	0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)
N1005	1073741822	1073741822	1073741822	1073741823	0 (0)		0 (1)		0 (0)		0 (0)		0 (0)		0 (0)		0 (1)
N1006	1073741823	1073741822	1073741823	1073741823	0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)
N1007	1073741822	1073741823	1073741823	1073741823	0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)
N1008	1073741822	1073741823	1073741822	1073741823	0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)		0 (0)
N1009	1073741822	1073741822	1073741823	1073741823	0 (0)		0 (0)		0 (0)		0 (0)		0 (1)		0 (0)		0 (0)
Average failures - Cases N1001, N1003-N1009					0.00		0.00		0.00		0.00		0.00		0.00		0.00
Average suspect values - Cases N1001, N1003-N1009					0.00		0.13		0.13		0.00		0.13		0.00		0.13

Table 9 Summary of results obtained for Cases P1000 to P1009, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
P1000	357913941	357913941	357913941	357913941	28(1)	14(3)	1(2)	1(0)	0(1)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1001	153391689	153391689	153391689	153391689	31(3)	13(2)	3(0)	1(0)	1(0)	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1002	71582788	286331153	71582788	286331153	27(1)	9(0)	1(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1003	34636833	34636833	34636833	34636833	27(2)	3(3)	1(2)	1(0)	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1004	17043521	17043521	17043521	17043521	21(4)	2(1)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(1)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)
P1005	8454660	33818640	135274560	541098243	13(10)	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)
P1006	4210752	269488144	67372036	16843009	10(8)	2(2)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)
P1007	2101256	16810048	134480385	2101257	9(2)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1008	1049601	1049601	1049601	1049601	5(2)	1(0)	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1009	524544	134283296	16785412	2098177	1(3)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
Average failures - Cases P1000-P1009					17.20	4.50	0.70	0.30	0.20	0.10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average suspect values - Cases P1000-P1009					3.60	1.10	0.50	0.10	0.20	0.20	0.00	0.00	0.10	0.00	0.00	0.10	0.00	0.10	0.00	0.00	0.20	0.00

Table 10 Summary of results obtained for Cases P1010 to P1019, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
P1010	357913941	1	1	1	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1011	153391689	1	1	1	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1012	71582788	1	1	1	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1013	34636833	1	1	1	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1014	17043521	1	1	1	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)
P1015	8454660	1	1	1	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1016	4210752	1	1	1	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1017	2101256	1	1	1	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1018	1049601	1	1	1	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)
P1019	524544	1	1	1	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)
Average failures - Cases P1010-P1019					0.20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average suspect values - Cases P1010-P1019					0.00	0.00	0.10	0.00	0.00	0.10	0.00	0.00	0.00	0.10	0.00	0.10	0.00	0.00	0.10	0.10	0.00	0.10

Table 11 Summary of results obtained for Cases P1020 to P1029, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
P1020	357913942	357913941	357913941	357913941	4(1)	1(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1021	153391690	153391689	153391689	153391689	3(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1022	71582789	286331153	71582788	286331153	3(1)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)
P1023	34636834	34636833	34636833	34636833	1(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1024	17043522	17043521	17043521	17043521	2(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1025	8454661	33818640	135274560	541098243	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)
P1026	4210753	269488144	67372036	16843009	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1027	2101257	16810048	134480385	2101257	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)
P1028	1049602	1049601	1049601	1049601	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1029	524545	134283296	16785412	2098177	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(1)	0(0)	0(1)	0(0)
Average failures - Cases P1020-P1029					1.30	0.10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average suspect values - Cases P1020-P1029					0.30	0.20	0.00	0.00	0.00	0.20	0.00	0.10	0.00	0.20	0.10	0.10	0.10	0.10	0.10	0.00	0.20	0.00

Table 12 Summary of results obtained for Cases P1030 to P1039, for ACORN generators with modulus 2^{120} and all orders between 8 and 25

Case	Seed	Seed	Seed	Seed	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order	Order
	s1	s2	s3	s4	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
P1030	357913940	357913941	357913941	357913941	4(0)	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1031	153391688	153391689	153391689	153391689	3(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(1)	0(0)	0(0)	0(0)
P1032	71582787	286331153	71582788	286331153	3(1)	1(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1033	34636832	34636833	34636833	34636833	1(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)
P1034	17043520	17043521	17043521	17043521	2(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1035	8454659	33818640	135274560	541098243	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1036	4210751	269488144	67372036	16843009	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)
P1037	2101255	16810048	134480385	2101257	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
P1038	1049600	1049601	1049601	1049601	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(1)	0(0)	0(0)	0(0)
P1039	524543	134283296	16785412	2098177	0(1)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)	0(0)
Average failures - Cases P1030-P1039					1.30	0.20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average suspect values - Cases P1030-P1039					0.30	0.00	0.00	0.00	0.00	0.10	0.10	0.00	0.10	0.00	0.00	0.00	0.10	0.00	0.40	0.00	0.00	0.00

Table 13 Summary of results obtained for Cases N1000 to N1009, for ACORN generators with modulus 2^{120} and selected orders between 29 and 101

Case	Seed	Seed	Seed	Seed	Order	...	Order	...	Order	...	Order	...	Order	...	Order	...	Order
	s1	s2	s3	s4	29	...	39	...	49	...	59	...	69	...	99	...	101
P1000	357913941	357913941	357913941	357913941	0(0)		0(0)		0(0)		0(0)		0(0)		0(0)		0(0)
P1001	153391689	153391689	153391689	153391689	0(0)		0(0)		0(0)		0(0)		0(0)		0(0)		0(0)
P1002	71582788	286331153	71582788	286331153	0(0)		0(0)		0(0)		0(0)		0(0)		0(1)		0(0)
P1003	34636833	34636833	34636833	34636833	0(0)		0(0)		0(0)		0(0)		0(0)		0(0)		0(0)
P1004	17043521	17043521	17043521	17043521	0(0)		0(0)		0(0)		0(0)		0(0)		0(0)		0(0)
P1005	8454660	33818640	135274560	541098243	0(0)		0(1)		0(0)		0(0)		0(0)		0(0)		0(0)
P1006	4210752	269488144	67372036	16843009	0(0)		0(0)		0(0)		0(0)		0(0)		0(0)		0(0)
P1007	2101256	16810048	134480385	2101257	0(0)		0(0)		0(0)		0(0)		0(0)		0(0)		0(0)
P1008	1049601	1049601	1049601	1049601	0(0)		0(0)		0(0)		0(0)		0(0)		0(1)		0(0)
P1009	524544	134283296	16785412	2098177	0(0)		0(0)		0(0)		0(0)		0(0)		0(0)		0(0)
Average failures - Cases P1000-P1009					0.00		0.00		0.00		0.00		0.00		0.00		0.00
Average suspect values - Cases P1000-P1009					0.00		0.10		0.00		0.00		0.00		0.20		0.00

REFERENCES

NOTE. For further discussion of ACORN sequences see the ACORN website http://acorn.wikramaratna.org, which includes a more comprehensive list of relevant ACORN references as well as links to downloadable versions of those references.). Recent ACORN references (including REAMC Limited reports, papers and presentations) are available for download from the publications page of the REAMC Limited website, https://www.reamc-limited.com.

1 R.S. Wikramaratna, Statistical Performance of Additive Congruential Random Number Generators Part 2 - Conjectures Concerning Seed Values Selected Uniformly at Random, REAMC Report-003, In preparation 2020. REAMC Limited, UK. [Link for download will be made available at https://www.reamc-limited.com]

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

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

4 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].

5 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].

6 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].

7 G. Marsaglia, The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness, Florida State University, Florida, USA, 1995. (originally made available from http://stat.fsu.edu/pub/diehard ; since November 2019 has been available from https://github.com/jeffThompson/DiehardCDROM)

8 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.

9 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 https://www.reamc-limited.com]

10 R.S. Wikramaratna, The Additive Congruential Random Number (ACORN) Generator - pseudo-random sequences that are well distributed in k dimensions, University of Oxford Numerical Analysis Group Internal Seminar, June 2019. [Link for download is available at https://www.reamc-limited.com]

11 R.S. Wikramaratna, Periodicity of ACORN Sequences with Arbitrary Order and Modulus, REAMC Report-001, March 2020. REAMC Limited, UK. [Link for download is available at https://www.reamc-limited.com]