REAMC Report-005(2022)
Issue 1, November 2022

On the Relationship Between ACORN Generators and Pascal's Triangle

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

On the Relationship Between ACORN Generators and Pascal's Triangle

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.

This report investigates the mathematical relationship between the ACORN generators and Pascal's triangle. It turns out that if the $(k+1)$-th diagonal of Pascal's triangle is considered modulo a large integer M, then it is equivalent to a k-th order ACORN sequence with seed equal to 1 and initial values all zero; normalising this sequence to the unit interval (by dividing each term in the sequence by the modulus M) leads to a sequence that approximates to being uniformly distributed on the unit interval. The report goes on to demonstrate an augmented form of Pascal's triangle that can be shown to encapsulate all the possible ACORN generators.

Demonstration of this new relationship, between the ACORN generators and Pascal's triangle, does not lead to any significant algorithmic developments in terms of generating ACORN sequences (this is due to the inherent speed and efficiency of the existing ACORN algorithm). Having said this, Pascal's triangle has been shown over the years to possess many interesting and diverse mathematical properties, and the present work has established the existence of some novel and previously unknown mathematical properties associated both with Pascal's triangle itself and with certain generalisations thereof.

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.

In this report we investigate some relationships that exist between ACORN sequences and the diagonals of Pascal's triangle. In particular, we show that any ACORN sequence having seed equal to 1 and initial values all zero is equivalent to a corresponding diagonal of Pascal's triangle calculated modulo M and normalised to the unit interval by dividing all the resulting terms by M (where M is the modulus of the ACORN sequence). In addition, we define a modified form of Pascal's triangle (augmented by an extra row of 'initial' terms) which encapsulates all ACORN sequences, irrespective of the choice of seed and initial values, in a similar way. We note that it had never been suggested that Pascal's triangle had any relation to a potential source of pseudo-random numbers prior to the brief observation made in 2019 by Wikramaratna [1]; the current work expands on those ideas.

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 $Y^m{}_0$, $m = 1, \ldots, k$, 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.

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 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 [1] and [9]. That work has since been systematically extended to ACORN generators with much wider choices of initialisations and Wikramaratna [10,11] presented extensive results obtained with TestU01 for ACORN with orders between 8 and 15, leading to two conjectures concerning the wide range of modulus, order and initial conditions under which ACORN sequences might be relied on to pass all the tests in the TestU01 BigCrush test suite. Further testing with

even larger orders (selected values of the order between 16 and 101) is ongoing and a further report is in preparation; this is expected to be issued early in 2023 [12].

Another recent paper by Wikramaratna [13] 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 was 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. 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 those references. Recent ACORN references (including this report) are available for download from the REAMC Limited website, https://www.reamc-limited.com.

3 PASCAL'S TRIANGLE

Pascal's triangle has been widely discussed and referenced both on the web and in school and university texts; see for example the article in the online Encyclopaedia Britannica [14]. Pascal's triangle is named for Blaise Pascal, a 17th century French mathematician who studied and documented many of its properties although it is believed to have been known as early as the 11th century in both China and Persia. Pascal's triangle is known to possess many interesting mathematical properties. A few specific examples of such properties include the fact that the rows of the triangle contain the binomial coefficients, while the 'semi-diagonals' sum to give the terms of the Fibonacci sequence; further, it can be shown (by consideration of the entries in Pascal's triangle, modulo 2) that a Serpinski gasket is created if all entries containing odd numbers are shaded black and all entries containing even numbers are shaded white.

Pascal's triangle is conceptually very simple and straightforward to construct, see Figure 1. It should be noted that the numberings of the rows, diagonals and anti-diagonals of the triangle that have been adopted in this report are particular to this work (by analogy with the numbering adopted in the definition of ACORN generators); in certain other contexts it may prove more convenient to adopt different numbering schemes. Calculation of the terms in Pascal's triangle proceeds as follows. The entries in diagonal 0 and anti-diagonal 1 (which correspond to the first and last entries in each row of the triangle) are all set equal to 1. Each of the remaining entries in the triangle can be calculated as the sum of the two entries to the

left and right in the preceding row of the triangle; all entries in the triangle can be calculated by working systematically downwards from row 3 of the triangle, noting that the first row contains just a single entry equal to one while the second row contains two entries, both equal to 1. The arrows within the triangle in Figure 2 show which two entries in the row above must be summed to derive each subsequent entry. Note that although Figure 1 only includes the first six rows of the triangle, the process can be repeated to generate further rows of the triangle *ad infinitum*. It is also worth noting that the entries in any given diagonal of the triangle can be calculated as long as the terms in the previous diagonal have been calculated to the same point, without needing to calculate any terms in any of the later diagonals, nor any of the later terms in the earlier rows. In this way it is possible to calculate the just the diagonals 0 to k, without calculating any of the terms in diagonal k+1 or any subsequent diagonal.

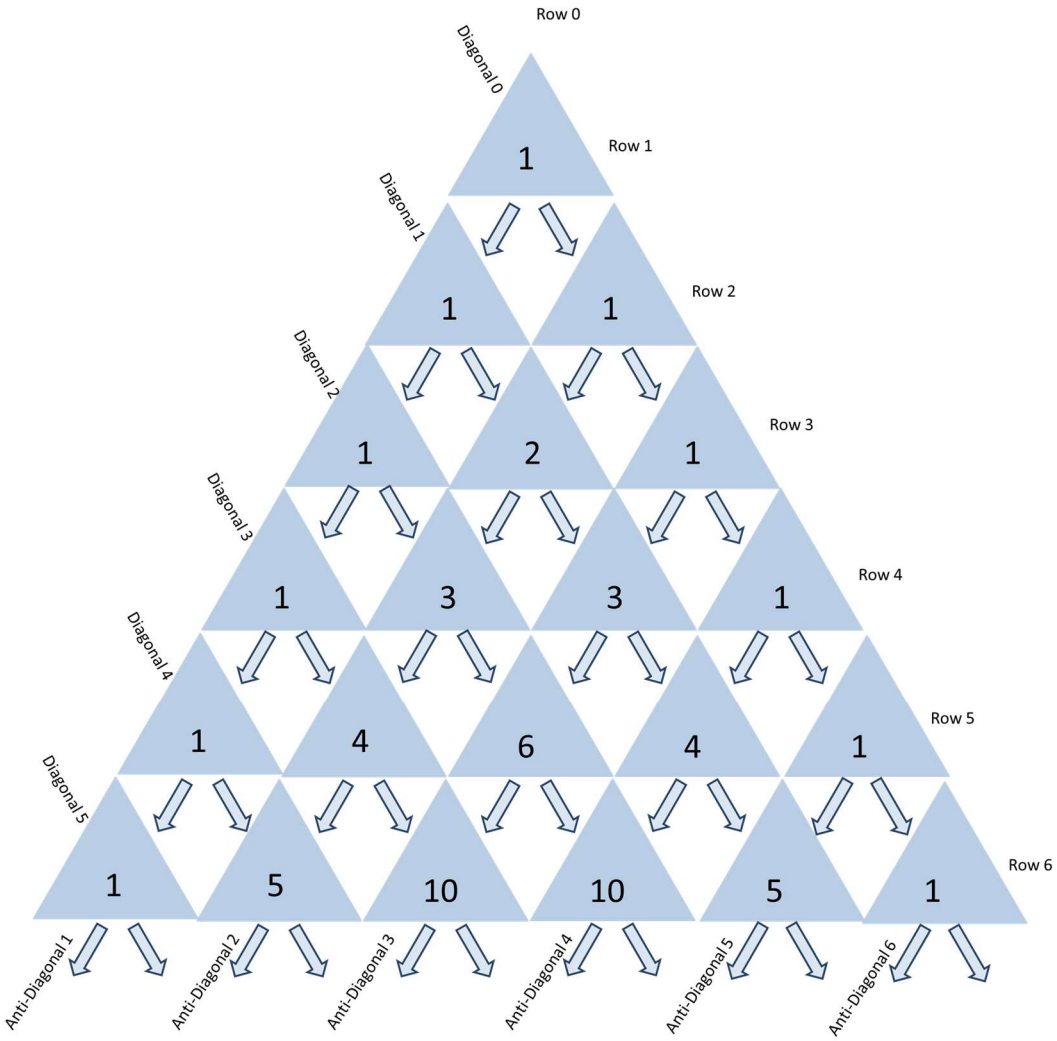

Figure 1 Rows 1 to 6 of Pascal's Triangle

Another way of generating the entire triangle is afforded by augmenting the triangle as in Figure 2 through inclusion of anti-diagonal 0, which consists of a single 1 at the top followed by a string of zeroes (shown in the circles on the left side of Figure 2). Entries in diagonal 0 of the triangle can be obtained by noting that the first entry is equal to the top entry of anti-diagonal 0 (equal to 1) and all subsequent entries can be obtained by copying the previous entry (illustrated by the single arrow joining successive entries in diagonal 1). All other entries in the triangle can be obtained by summing the two entries to the left and right in the previous row, noting that entries in anti-diagonal 1 are calculated by summing the previous entry in anti-diagonal 1 and the corresponding entry from anti-diagonal 0 (which is not strictly part of the Pascal triangle). We observe that the result in this case corresponds exactly to Pascal's triangle.

Figure 2 shows the first six rows of the triangle, augmented by the numbers in circles which are labelled "Anti-Diagonal 0". As discussed, the augmentation is not itself part of the triangle; the augmentation, together with the numbering that we have adopted for the diagonals and anti-diagonals (in which the diagonals of the triangle are numbered from zero, while the anti-diagonals of the triangle are numbered from 1) will be useful in establishing the analogy with the ACORN sequences.

It will also be of interest in this work to consider Pascal's triangle modulo an integer M; this triangle is calculated in an entirely analogous way, but all the additions are carried out modulo M. It is worth noting that the upper part of the triangle is unchanged until the first row containing one or more values that are greater than or equal to M. Thus, the first six rows of the triangle (as shown in Figure 2) would remain unchanged for any choice of M greater than or equal to 11. By contrast, a choice of $M = 8$ would change the two entries that are equal to 10 (in row 6) to the value of 10 modulo 8 which is equal to 2; all other entries in the first six rows would be unchanged. The values of M that will be of particular interest to us in this work will be much larger, specifically large integer powers of 2 (for example, we will refer to and make use of some existing empirical results concerning the uniformity of ACORN sequences having modulus $M=2^{120}$, after normalisation to the unit interval).

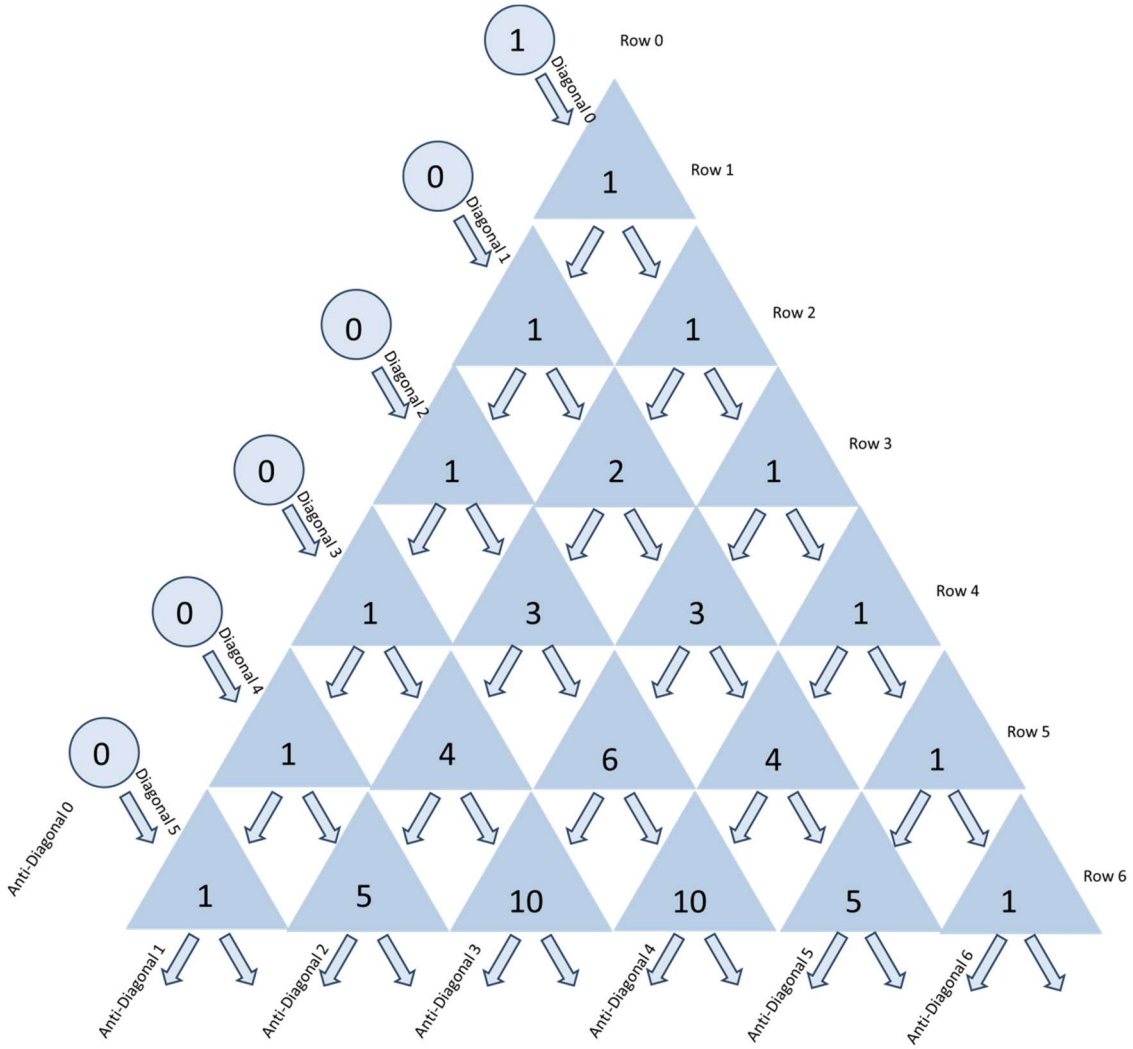

Figure 2 Rows 1 to 6 of Pascal's Triangle (augmented on the left by cells labelled as "Anti-Diagonal 0" which includes the row labelled as "Row 0"; as discussed in text, inclusion of this augmentation helps to illustrate the analogies with ACORN sequences while still preserving the structure of the triangle unchanged)

We can further generalise Pascal's triangle modulo M by permitting the choice of different values for the initialisation of the anti-diagonal zero. In the generalised case the uppermost entry of the anti-diagonal 0 can take any non-zero positive integer value less than M, while all other values on the anti-diagonal 0 can be either zero or positive integers strictly less than M. This is illustrated in Figure 3. The entries in Pascal's triangle would usually be referenced by the row number and the position in the row; however, it will prove more convenient for our purpose to label the entries P^i_j with a superscript i to denote the diagonal number and a subscript j to denote the row number. The arrows within the triangle again show which two entries must be summed modulo M to derive each subsequent entry; although the figure only shows the first six rows of the triangle, the process can be repeated to generate further terms of the triangle *ad infinitum*.

We will now proceed to demonstrate the direct analogy that exists between any k-th order ACORN sequence and the k-th diagonal of a corresponding generalised Pascal's triangle modulo M.

The simplest way to demonstrate the analogy is as follows. Consider a k-th order ACORN generator having modulus M, seed $Y^0{}_0$ satisfying $0 < Y^0{}_0 < M$ and k integer initial values $Y^m{}_0$, $m = 1, ..., k$, each satisfying $0 \le Y^m{}_0 < M$. Equations (1) and (2) can then be represented by the diagonals 0 to k of a generalised Pascal triangle modulo M, as shown in Figure 3, if we set $P^m{}_0 = Y^m{}_0$ for $m = 0,..., k$; we note that the $P^m{}_0$ with $m>k$ can be set arbitrarily to zero (or any other positive value less than M) as they have no impact on any of the first k diagonals of the triangle. It now follows that if the entries in the k-th diagonal are normalised to the unit interval (by dividing each value by the modulus M) the result is precisely the sequence generated by the corresponding k-th order ACORN generator, as defined in equation (3).

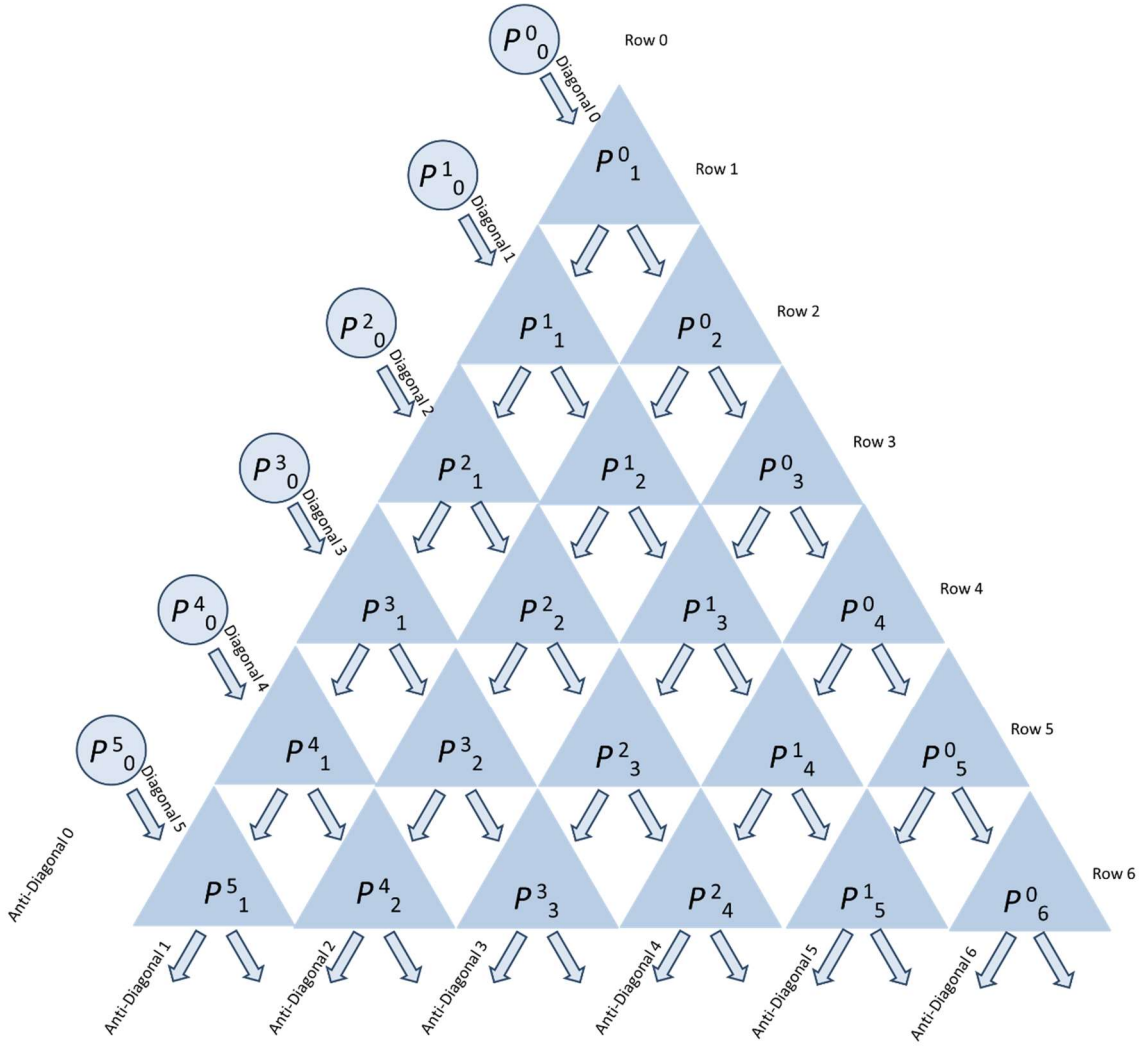

Figure 3 Rows 0 to 6 of generalised Pascal's triangle, modulo *M*

4 DISCUSSION AND CONCLUSIONS

The first suggestion that Pascal's triangle may have had any mathematical relationship to a potential source of pseudo-random numbers was a brief passing observation made in 2019 by Wikramaratna [1]. In the current work, we have demonstrated a one-to-one correspondence that exists between the ACORN sequences and the diagonals of what we have called a generalised Pascal's triangle modulo M. Existing results obtained for ACORN sequences can therefore be applied directly to the diagonals of a generalised Pascal's triangle modulo M with an appropriately chosen initialisation of the anti-diagonal 0.

For any appropriate choice of M, the resulting sequence (normalised to the unit interval by dividing each of the terms by M) can therefore be shown to be periodic and to approximate to uniformly distributed on the unit interval. It should be noted that the period length for these sequences can be calculated by direct analogy with the existing results for ACORN sequences, see Wikramaratna [13].

In particular, for modulus $M = 2^{120}$ and if the seed Y^0_0 is an odd integer, chosen randomly and lying between 0 and M, together with an arbitrary set of initial values, then any resulting ACORN generator of order eight or more satisfies all the conditions for the conjectures in the references [10, 11], and so the same conjectures can also be applied to the diagonals of the generalised Pascal's triangle with the analogous initialisation and normalisation. In summary, the conjectures state that any ACORN sequence satisfying these conditions will almost certainly pass all the tests in the TestU01 BigCrush test suite.

This means that a generalised Pascal's triangle of this form might in principle be used as the basis for a pseudo-random number generator that approximates to uniformly distributed on the unit interval. Having said this, it should be noted that any such generator is exactly equivalent to a corresponding ACORN generator, and that the existing computational algorithm developed for the ACORN generators is much more efficient than trying to first calculate the terms of a generalised Pascal's triangle modulo M. In consequence, the relationship that has been discovered between ACORN sequences and the generalised Pascal's triangle has turned out to be primarily of theoretical interest rather than possessing any particular computational significance.

REFERENCES

NOTE. 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 with a more comprehensive list of relevant ACORN references as well as links, pointing to downloadable versions, or to other sites where those references can be accessed and downloaded (see http://acorn.wikramaratna.org/references.html). 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 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]

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, 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]

10 R.S. Wikramaratna, Statistical Performance of Additive Congruential Random Number Generators Part 2 - Conjectures Concerning Seed Values Chosen Uniformly at Random, REAMC Report-003, Issue 2, August 2021, REAMC Limited, UK. *Note that this report was originally published as Issue 1 in January 2021; Issue 2 is unchanged apart from a few minor typographic corrections.* [Link for download is available at https://www.reamc-limited.com]

11 R.S. Wikramaratna, Two Conjectures on Statistical Performance of ACORN Generators: Evidence for Orders 11 - 15, REAMC Report-004, August 2021, REAMC Limited, UK. [Link for download is available at https://www.reamc-limited.com]

12 R.S. Wikramaratna, A Conjecture on Statistical Performance of ACORN Generators: Evidence for Selected Orders 16 - 101, REAMC Report-006, In preparation, to be published early 2023, REAMC Limited, UK. [Link for download will be made available at https://www.reamc-limited.com]

13 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]

14 Enclyclopaedia Britannica online edition, article on Pascal's Triangle, accessed 2022 [see the link https://www.britannica.com/science/Pascals-triangle]

