INVERSIVE PSEUDORANDOM NUMBER GENERATORS: CONCEPTS, RESULTS AND LINKS

Peter Hellekalek

Department of Mathematics
University of Salzburg
A-5020 Salzburg, Austria

ABSTRACT

Stochastic simulation requires a reliable source of randomness. *Inversive* methods are an interesting and very promising new approach to produce uniform pseudorandom numbers.

In this paper, we present evidence that these methods are an *important contribution* to our toolbox. We survey the outstanding performance of inversive pseudorandom number generators in theoretical and empirical tests, in comparison to linear generators. In addition, this paper contains tables of parameters to implement inversive congruential generators.

More empirical results as well as an implementation of inversive generators in C are available in the INTERNET from our WEB-site `http://random.mat.sbg.ac.at`.

1 INTRODUCTION

Pseudorandom number generators are essential elements in the toolbox of stochastic simulation. Their task is to simulate realizations of independent, identically $U([0,1[)$-distributed random variables. Other distributions will be obtained by transformation methods, see Devroye (1986), and the software package C-Rand, see Stadlober and Kremer (1992) and Stadlober and Niederl (1994).

There is a strong need to enlarge this toolbox by widely different pseudorandom number generators. We refer the reader to Ferrenberg and Landau (1992), L'Ecuyer (1992, 1994), Eddy (1990), and Anderson (1990) for a discussion of some of the deficiencies of traditional generators.

Pseudorandom number generators are like antibiotics. No generator will be appropriate for all tasks. Any type of generator has some unwanted side-effects. Hence, we are in need of an arsenal of pseudorandom number generators with *distinct properties.* If two strongly different generators yield the same outcome in a simulation, we will gain confidence in the results.

Many properties of inversive methods are complementary to those of linear algorithms. Inversive generators are easy to initialize. Their excellent properties remain invariant under the choice of parameters. For certain inversive types this robustness was even proved for subsequences. We may work with larger sample sizes on a given architecture. Extensive tables of parameters are available for implementation.

In our opinion, inversive methods should not be viewed as a replacement of linear methods. In view of their remarkable properties, they are *a valuable completion* of our arsenal of uniform generators.

2 INVERSIVE GENERATORS

We discuss three concepts of inversive methods, inversive congruential generators, explicit-inversive congruential generators, and combinations of these algorithms.

Inversive methods may be defined even for composite moduli. In view of their outstanding performance, we shall only consider *prime* moduli. Elaborate theoretical analysis has shown that the composite case is of little practical interest. We refer the reader to Niederreiter (1995a) for a comprehensive survey of these results.

For a given prime number p, and for $c \in \mathbf{Z}_p$, let $\overline{c} := 0$ if $c = 0$ and $\overline{c} := c^{-1}$ if $c \neq 0$. In other words, $\overline{c}$ equals the number c^{p-2} modulo p.

2.1 Inversive Congruential Generators

Inversive congruential generators ("ICG") are due to Eichenauer and Lehn (1986). We have to choose the modulus p, a multiplier a, an additive term b, and an initial value y_0. Then the congruence

$$y_{n+1} \equiv a\overline{y}_n + b \pmod{p}, \quad n \geq 0, \tag{1}$$

defines an inversive congruential generator. We denote this generator by

$$\mathrm{ICG}(p, a, b, y_0).$$

It produces a sequence $(y_n)_{n\geq 0}$ in the set $\{0, 1, \ldots, p-1\}$. Pseudorandom numbers x_n in $[0, 1[$ are obtained by the normalization $x_n := y_n/p$.

A prominent feature of the ICG with prime modulus is the absence of any lattice structure, in sharp contrast to linear congruential generators ("LCG"). In the following scatter plot, all possible points ("nonoverlapping pairs" of consecutive pseudorandom numbers) (x_{2n}, x_{2n+1}), $n \geq 0$, in a region near the point (0.5, 0.5) are shown.

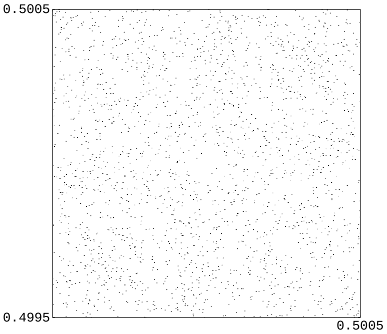

Figure 1: ICG($2^{31} - 1$, 1288490188, 1, 0)

The proper choice of the parameters a and b will be discussed in Section 3. An important feature of the ICG with respect to implementation is the "mother-son" principle, see Section 5.

2.2 Explicit Inversive Congruential Generators

Roughly speaking, the EICG is the "easy-going brother" of the ICG. It is due to Eichenauer-Herrmann (1993a). As we shall see, the EICG is easier to handle in practice, for example when producing independent substreams. The cost is a slightly smaller maximal sample size, as our empirical tests have shown, see Figure 6 in Section 4.

We choose a prime number p, a multiplier $a \in \mathbf{Z}_p$, $a \neq 0$, an additive term $b \in \mathbf{Z}_p$, and an initial value n_0 in $\mathbf{Z}_p$. Then

$$y_n \equiv \overline{a(n + n_0) + b} \pmod{p}, \quad n \geq 0, \qquad (2)$$

defines a sequence of pseudorandom numbers in $\{0, 1, \ldots, p-1\}$. As before, we put $x_n := y_n/p$, $n \geq 0$, to obtain pseudorandom numbers in $[0, 1[$. We shall denote this generator by

$$\mathrm{EICG}(p, a, b, n_0).$$

In the definition of $\mathrm{EICG}(p, a, b, n_0)$, the additive term b is superfluous. It is easy to see that the two generators $\mathrm{EICG}(p, a, b, n_0)$ and $\mathrm{EICG}(p, a, 0, m_0)$, with

$$m_0 \equiv n_0 + \overline{a}b \pmod{p},$$

produce identical output. Hence, in most of our tests, we shall put $b = 0$.

2.3 Compound generators

Eichenauer-Herrmann (1993b, 1994a) has introduced a simple technique to combine inversive generators, the *compound approach.*

Let $p_1, p_2, \ldots, p_r$ be distinct prime numbers, each $p_j \geq 5$. For each index j, $1 \leq j \leq r$, let $(y_n^{(j)})_{n\geq 0}$ be a sequence of elements of $\mathbf{Z}_{p_j}$ that is purely periodic with period length p_j. In other words,

$$\{y_n^{(j)} : \ 0 \leq n < p_j\} = \mathbf{Z}_{p_j}.$$

Let $(x_n^{(j)})_{n\geq 0}$ denote the related sequence of pseudorandom numbers in $[0, 1[$, where

$$x_n^{(j)} := \frac{y_n^{(j)}}{p_j}, \quad n \geq 0, \quad 1 \leq j \leq r.$$

A sequence $(x_n)_{n\geq 0}$ of *compound pseudorandom numbers* in $[0, 1[$ is defined by the congruence

$$x_n :\equiv x_n^{(1)} + \ldots + x_n^{(r)} \pmod{1}, \quad n \geq 0. \qquad (3)$$

It is elementary to see that the period of the sequence $(x_n)_{n\geq 0}$ equals $M := p_1 \cdot \ldots \cdot p_r$. We shall write cICG for a compound ICG and cEICG for a compound EICG.

The compound approach allows to combine ICG and EICG, provided they have full period. This method has important advantages: we may obtain very long periods easily, modular operations may be carried out with relatively small moduli, increasing the effectiveness of our computations, and the good correlation structure of the ICG and EICG is preserved. For the latter statement, see Section 3.

We present a scatter plot of a combined ICG, c(ICG(1031,55,1,0), ICG(1033,103,1,0), ICG(2027, 66,1,0)). All possible points (x_{2n}, x_{2n+1}), $n \geq 0$, have been computed. The period of this generator is $M = 2158801621$.

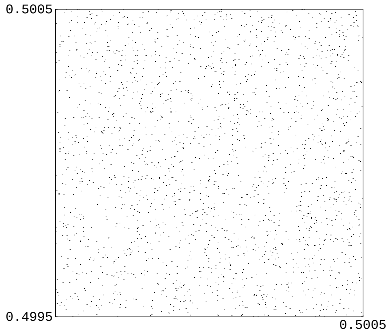

Figure 2: A Combined ICG with Three Components

3 THEORETICAL RESULTS

In the theoretical analysis of pseudorandom number generators, we study the following questions:

(Q1) What is the maximal period length of the given type of generator?

(Q2) How to choose the parameters to obtain maximal period length?

(Q3) Which algorithms let us obtain such parameters?

(Q4) What can we say about correlations between pseudorandom numbers and what results hold for the empirical distribution of samples?

(Q5) What are the regularities (i.e. lattice structures, ...) of this type of generator?

The answers for the ICG are as follows. We consider ICG(p, a, b, y_0), with p a prime. As for (Q1), Eichenauer and Lehn (1986) have shown that the maximal period length is p. In the same paper, the have provided an answer to question (Q2): if $x^2 - bx - a$ is a primitive polynomial over the finite field $\mathbf{Z}_p$, then ICG(p, a, b, y_0) has maximal period length. Flahive and Niederreiter (1992) have extended this result considerably. They have shown that IMP-polynomials induce maximal period length. This approach has allowed Chou (1994) to obtain a very effective algorithm for IMP-polynomials, thereby replying to (Q3). Our tables in Section 5 have been computed with an implementation of this algorithm.

Question (Q4) is the most difficult to answer. It is a generally accepted approach to study the empirical distribution of *overlapping* s-tuples

$$\mathbf{x}_n := (x_n, x_{n+1}, \ldots, x_{n+s-1}), \quad n \geq 0,$$

or *nonoverlapping* s-tuples

$$\mathbf{x}_n := (x_{ns}, x_{ns+1}, \ldots, x_{ns+s-1}), \quad n \geq 0,$$

in the s-dimensional unit cube $[0,1[^s$, either with tools from number theory and statistics, in other words, with *discrepancy*, or with geometrical test quantities like the *spectral test*. The behavior of the points $\mathbf{x}_n$ is used as an indicator of correlations within the sequence $(x_n)_{n\geq 0}$ of pseudorandom numbers.

Uniform pseudorandom numbers x_n, $n \geq 0$, should simulate realizations of independent, identically $U([0,1[)$-distributed random variables. Hence the points $\mathbf{x}_n$ should be approximately $U([0,1[^s)$-distributed. For a given sample $\mathcal{P} = (\mathbf{x}_n)_{n=0}^{N-1}$ in $[0,1[^s$, there are several concepts to assess its empirical distribution. From the statistical point of view, it is natural to compare the empirical distribution function of the points $\mathbf{x}_n$, $0 \leq n < N$, to the target distribution, which is uniform distribution on $[0,1[^s$, by means of a classical goodness-of-fit test, the *two-sided Kolmogorov-Smirnov* test statistic ("KS-test"). In number theory, this test quantity is called the *star discrepancy*. Niederreiter has developed an impressive technique to obtain discrepancy estimates. It has allowed to determine the order of magnitude of discrepancy for most types of pseudorandom number generators. Usually, these results hold for the whole period of a generator only and not for smaller samples, as they are relevant in practice. We refer to the monograph Niederreiter (1992) and the comprehensive survey Niederreiter (1995a).

The ICG excels in this respect. The discrepancy of full period sets $\mathcal{P}$ is of the same order of magnitude as the law of the iterated logarithm for the discrepancy suggests, see Niederreiter (1992) and Eichenauer-Hermann (1994b). An average-case analysis of the discrepancy of samples has been carried out by Eichenauer-Herrmann and Emmerich (1994, 1995), with interesting results. It has to be noted that *the only condition* on the parameters a and b is that they must imply maximal period length. Once this requirement is met, ICG(p, a, b, y_0) will have those excellent correlation properties. This fact stands in sharp contrast to the sensibility of the LCG concerning the choice of parameters.

The *spectral test* of Coveyou and MacPherson (1967) is a completely different approach. In its original form, it is a figure of merit derived from certain exponential sums. In practice, this numerical quantity can only be computed if the set $\mathcal{P}$ in $[0,1[^s$ has a lattice structure. In this special case there exists a nice geometric interpretation, see Knuth (1981) and Ripley (1987).

The spectral test does not apply to the ICG, nor the EICG, see the discussion of (Q5) below.

Concerning (Q5), the ICG differs strongly from linear methods in its geometrical structure. As Marsaglia (1968) has noted for the LCG, "random numbers fall mainly in the planes". Eichenauer-

Herrmann (1991) has shown that ICG "avoid" the planes. Further, ICG pass the *lattice test* in dimensions that are out of reach for the LCG, see Niederreiter (1992, 1995a).

The simple definition of the EICG allows even stronger results. Questions (Q1), (Q2), and (Q3) are easy to answer. The maximal period of EICG(p, a, b, n_0) is p. It will be obtained if we choose $a \in \mathbf{Z}_p \setminus \{0\}$. As for (Q4), EICG behave like ICG with respect to discrepancy. Again, the spectral test is useless, due to the absence of any lattice structure.

There is a truly remarkable difference between the EICG and any other type of pseudorandom number generator, namely *excellent splitting properties*. As a consequence, the EICG qualifies as one of the most promising candidates for parallelization. Due to Eichenauer-Herrmann (1993a), Niederreiter (1994), and Eichenauer-Herrmann and Niederreiter (1994), a thorough theoretical assessment of the behavior of substreams and of general types of s-tuples $\mathbf{x}_n$ is known. These results ensure against *long-range correlations*, in sharp contrast to the LCG. We refer to De Matteis and Pagnutti (1990) for the latter.

Niederreiter (1994) has shown that the explicit-inversive method yields optimal behavior under the lattice test. There are no regularities with respect to hyperplanes. As with the ICG, explicit-inversive pseudorandom numbers avoid the hyperplanes. This replies to (Q5).

The compound approach preserves the excellent properties of the ICG and EICG. The answers to (Q1), (Q2), and (Q3) follow directly from the above results for the components. Compound inversive generators have the same outstanding correlation properties as single inversive generators, see the survey of Eichenauer-Herrmann and Emmerich (1995). This answers (Q4). Question (Q5) is still open, but there is some empirical evidence. All scatterplots show the same nonlinear structures as single ICG and EICG.

3.1 An Important Remark

The theoretical assessment of pseudorandom number generators is sometimes viewed as being "esoteric". This fact is partly due to the abstract language in which the results are presented.

Theoretical tests of a certain pseudorandom number generator cannot guarantee that samples from this generator will pass a given statistical test. In the first type of tests we are forced to consider very large samples, usually the full period of the generator. This limitation is due to the mathematical methods involved. In empirical tests, we consider much smaller samples, as they appear in the practice of simulation. Alas, from the behavior of very large samples we cannot reason on the performance of small samples. The missing mathematical link between theoretical and empirical tests has not yet been found. Nevertheless, almost three decades of practical experience have shown that certain theoretical measures, such as discrepancy or the spectral test, are *reliable indicators*. If a generator performs well with respect to these tests, its samples will pass a large class of stringent empirical tests.

Theoretical test quantities like discrepancy or the spectral test cannot be computed for samples as they appear in practice. Either the computational complexity is prohibitive, as in the case of discrepancy, or the test is not defined, as it happens to be the case for the spectral test. There is a *definite lack of test quantities* that are relevant in theory as well as in numerical practice.

4 EMPIRICAL RESULTS

As the performance in theoretical tests is *no guarantee*, but *only an indicator* of what we may expect in practice, empirical testing of pseudorandom number generators is an absolute necessity. A *popular misconception* is to equate testing pseudorandom numbers with testing "randomness". The latter term is undefined in statistics. No random number generator is "more random" than any other. We propose to forget about the misleading term "randomness" and to concentrate upon the original purpose of pseudorandom number generation. The objective is to get reliable results in stochastic simulation. No pseudorandom number generator is appropriate for all tasks. As a consequence, we shall try to identify statistical tests that are similar to our simulation problem. If a generator passes these tests, we may expect "good" simulation results from it. For our notion of "goodness", see Wegenkittl (1995). Certain statistical tests have proven their relevance for a large number of problems encountered in practice.

As a first example of such a test, we would like to check if the bits in the binary representation of pseudorandom numbers x_n, $n \geq 0$, simulate realizations of independent random variables, equidistributed on the set $\{0, 1\}$. The following test design is due to Leeb (1995), who has also contributed Figures 3 and 4. From the binary representation of every coordinate of the nonoverlapping s-tuple $(x_{ns}, x_{ns+1}, \ldots, x_{ns+s-1})$, we take a block of l digits that starts at the k-th digit. We perform this operation on $N = 6 \cdot 2^{sl}$ s-tuples. This procedure will yield a quantity $t_1(s, k, l)$ that simulates the upper tail probability T_1 of a χ^2-distributed random variable. T_1 is an equidistributed random variable on $[0,1[$. In a second step, we compute the value of $t_1(s,k,l)$ for 64 distinct consecutive samples of size N. We compare the empirical distribution of these 64 numbers to the distribution of T_1 by means of a two-sided Kolmogorov-Smirnov test statistic. We denote its value by $t_2(s,k,l)$. The distribution of the KS-statistic is known. To a level of significance of 0.01, there corresponds the critical region $[1.63,\infty[$. The following figures illustrate the results for the Ansi-C generator, see Figure 3, and ICG$(2^{31}-1,1,1,0)$, see Figure 4. The parameters are $s=4$, $k=1,5,9,\ldots,21$ and $l=1,2,\ldots,5$. Large values of t_2 have been truncated to keep the graphics in scale. The ICG is clearly superior, the LCG performs poorly.

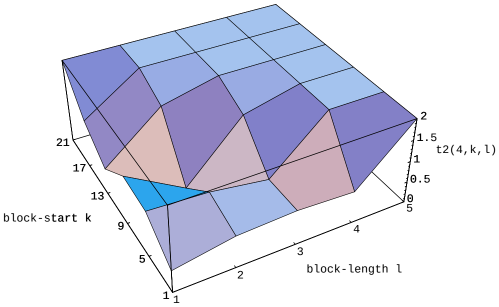

Figure 3: Ansi-C

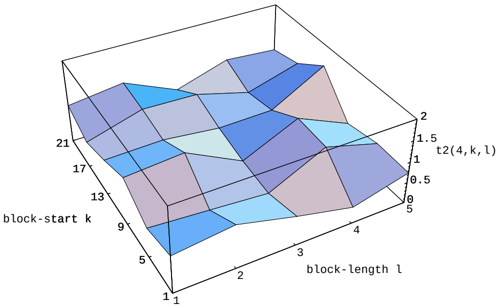

Figure 4: ICG$(2^{31}-1,1,1,0)$

Many models in stochastic simulation have the form

$$Y := \sum_{n=0}^{N-1} g(X_n, X_{n+1}, \ldots, X_{n+M-1}), \qquad (4)$$

where $g : [0,1[^M \to \mathbf{R}$ is some given function and the X_n are independent, identically $U([0,1[)$-distributed random variables. As the M-tuples overlap, the usual χ^2-test cannot be applied. This approach leads to the important *overlapping M-tuple test* of Marsaglia (1985).

The M-tuple test is a stringent test. Wegenkittl (1995) gave a detailed proof of the distribution of this random variable that is missing in Marsaglia's paper. The following test design and Figures 5 and 6 stem from Wegenkittl (1995). It is an application of the M-tuple test. From every component of an overlapping 5-tuple $(x_n, x_{n+1}, \ldots, x_{n+4})$ of pseudorandom numbers $x_n \in [0,1[$, we take the first four bits in its binary representation. Then, for a given sample size N, we compute 32 values of the –theoretically equidistributed– upper tail probability of the M-tuple test. In the following figures, the sample size ranges between 2^{18} and 2^{26}. In Figure 5, we plot the 32 values of this test statistic. The resulting patterns should be irregular. If, for a given sample size N, the corresponding box is either totally white or black, the generator has failed miserably. For example, the Fishman and Moore LCG begins to break down from $N=2^{21}$ onwards. In Figure 6, we show the result of a two-sided KS-test applied to these 32 values. Values of the KS-test statistic greater than the critical value 1.59 that corresponds to the significance level of 1% are shown in dark grey. We compare the following PRN generators:

EICG$(2^{31}-1,1,0,0)$, short "EICG1"
EICG$(2^{31}-1,7,0,0)$, short "EICG7"
ICG$(2^{31}-1,1,1,0)$, short "ICG"
LCG$(2^{31}-1,950706376,0,1)$, short "FISH"
LCG$(2^{31},1103515245,12345,12345)$, short "ANSIC"
LCG$(2^{31}-1,16807,0,1)$, short "MINSTND"
LCG$(2^{31},65539,0,1)$ short "RANDU"

"FISH" was recommended by Fishman and Moore (1986) because of its excellent lattice structure. "ANSIC" is the Ansi-C system generator. The call `rand(0)` is equivalent to our initialization. "MINSTND" is the "minimal standard" generator of Park and Miller (1988) , where "RANDU" is also discussed. The latter is an unlucky product of IBM.

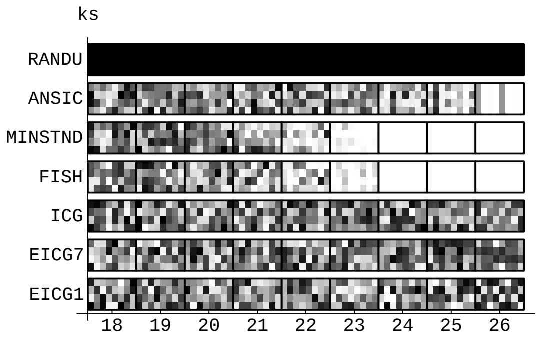

Figure 5: The Distribution of the Upper Tail Probabilities of the M-Tuple Test Statistic

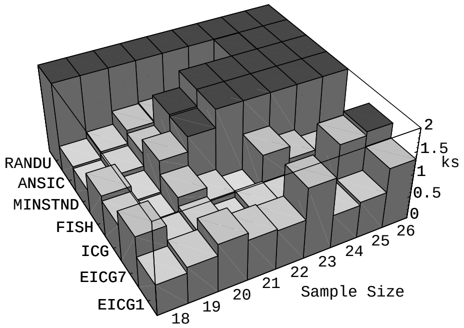

Figure 6: The Values of the KS-Test Statistic

Our third example is the *run test*. Since Knuth (1981), the run test has proven to be a very reliable test to detect correlations within a sample $(x_n)_{n=0}^{N-1}$ of pseudorandom numbers. We refer to Fishman and Moore (1982) for empirical results concerning LCGs.

Entacher (1995a, 1995b) has studied the *runs up statistic*. For a given sample of size N, 100 values of this asymptotically χ^2-distributed quantity have been generated. In a second step, a two-sided KS-test was applied to these values to check the goodness-of-fit. The following figures show the results for the minimal standard generator and for EICG$(2^{31}-1, 1, 0, 0)$. The two horizontal lines represent the critical values of the KS test statistic that correspond to the significance levels 0.05 and 0.01. The sample size ranges from 2^{12} to 2^{21}. We have considered the *subsequence* $(x_{77n})_{n\geq 0}$. Similar results hold for other LCG and EICG, see Entacher (1995b). Apparently, large samples of the LCG have an increasing tendency to fall into the critical region.

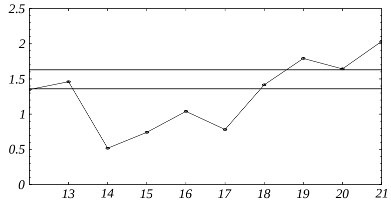

Figure 7: Run Test for MINSTD

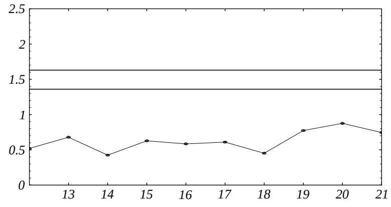

Figure 8: Run Test for EICG1

As a final remark in this section, we would like to draw the reader's attention to the fact that all our tests are *two-level tests* in the sense of L'Ecuyer (1992) and that we have *varied* the sample size. This careful test design is not as common in the published literature on pseudorandom number generation as one would wish.

5 TABLES OF PARAMETERS

If we want to implement ICG or cICG, we shall need pairs a, b of parameters such that ICG(p, a, b) will have period p. As we have pointed out in Section 3, the polynomial $x^2 - bx - a$ will have to be an IMP polynomial.

We would have to apply Chou's algorithm every time we need a different ICG, even if the modulus p remains constant. This is the common situation with pseudorandom number generators. For example, in the case of the LCG, we would have to carry out complex computations with the spectral test to determine new parameters. This is a task for specialists. Again, inversive methods are different. There is a new approach that allows us to implement many "descendants" from one single ICG with maximal period.

For every "mother" ICG$(p, a, 1)$ with period p, every "son" ICG(p, ac^2, c) will have maximal period p, provided we choose $c \neq 0$ in $\mathbf{Z}_p$, see Eichenauer-Herrmann and Emmerich (1994). As we have seen in Section 3, all these ICG will have the same excellent theoretical properties. Hundreds of empirical tests provide strong evidence that this extraordinary fact is also true for the performance of ICG in empirical tests.

We present four tables of mother ICG for small prime moduli p. These parameters allow the implementation of compound ICG with three components on 32-bit architectures. The last two tables exhibit families of ICG, one mother and five sons each, where each son has a multiplier ac^2 below 2^{16}. Such multipliers are preferable on 32-bit processors for reasons of computational efficiency of the modular inversion involved.

Table 1: $p = 1031$

n	a_n	b_n
1	849	1
2	345	1
3	55	1
4	116	1
5	441	1

Table 2: $p = 1033$

n	a_n	b_n
1	413	1
2	878	1
3	595	1
4	522	1
5	818	1

Table 3: $p = 1039$

n	a_n	b_n
1	173	1
2	481	1
3	769	1
4	1028	1
5	136	1

Table 4: $p = 2027$

n	a_n	b_n
1	579	1
2	1877	1
3	390	1
4	837	1
5	1048	1

Table 5: $p = 2147483053$

a	b	ac^2	c
858993221	1	22211	11926380
		579	24456079
		11972	62187060
		21714	94901263
		4594	44183289

Table 6: $p = 2147483647$

a	b	ac^2	c
1288490188	1	9102	36884165
		14288	758634
		21916	71499791
		28933	59217914
		31152	48897674

6 CONCLUSIONS

The results of our assessment of inversive pseudorandom number generators with prime moduli can be summarized as follows:

(i) the choice of parameters is simple, even trivial in the case of the EICG,

(ii) initialization is trivial,

(iii) the excellent theoretical and empirical properties of inversive methods remain stable under the variation of parameters, provided we have maximal period length,

(iv) the outstanding theoretical properties remain invariant under the compound approach,

(v) the EICG has remarkable splitting properties which have been tested extensively for disjoint substreams, with excellent numerical results,

(vi) hundreds of empirical results imply that we may work with considerably larger samples than in the case of LCG, and

(vii) the modular inversion involved causes acceptable slow-downs when generating pseudorandom numbers: the time factor is less than 3.0 in comparison to the LCG, provided the simple guideline concerning the multipliers is respected (see Section 5).

ACKNOWLEDGMENTS

The author is indebted to his co-workers in the pLab group, Karl Entacher, Hannes Leeb and Stefan Wegenkittl for contributing the figures in Section 4. Chou's algorithm has been implemented by Entacher with the assistance of Andreas Weingartner. All computations have been made with the pLab system. For a description of the latter, we refer to Leeb (1994).

This research has been supported by the Austrian Science Foundation, project no. P9285 and by the Austrian Ministry of Science, Research and the Arts, project CEI-PACT, WP5.1.2.1.2.

REFERENCES

Anderson, S. L. 1990. Random number generators on vector supercomputers and other advanced architectures. *SIAM Rev.* 32:221-251.

Chou, W.-S. 1994. On inversive maximal period polynomials over finite fields. *Algebra Engrg. Comm. Comput.* to appear.

Coveyou, R. R. and R. D. MacPherson. 1967. Fourier analysis of uniform random number generators. *Journal of the ACM* 14:100–119.

De Matteis, A. and S. Pagnutti. 1990. Long-range correlations in linear and non-linear random number generators. *Parallel Computing* 14: 207–210.

Devroye, L. 1986. *Non-Uniform Random Variate Generation*. Springer-Verlag: New York.

Eddy, W. F. 1990. Random number generators for parallel processors. *J. Comput. Appl. Math.* 31:63–71.

Eichenauer, J. and J. Lehn. 1986. A non-linear congruential pseudo random number generator. *Statist. Papers* 27:315–326.

Eichenauer-Hermann, J. 1991. Inversive congruential pseudorandom numbers avoid the planes. *Math. Comp.* 56:297–301.

Eichenauer-Herrmann, J. 1993a. Statistical independence of a new class of inversive congruential pseudorandom numbers. *Math. Comp.* 60:375–384.

Eichenauer-Herrmann, J. 1993b. Explicit inversive congruential pseudorandom numbers: The compound approach. *Computing* 51:175–182.

Eichenauer-Herrmann, J. 1994a. Compound nonlinear congruential pseudorandom numbers. *Monatsh. Math* 117:213–222.

Eichenauer-Herrmann, J. 1994b. Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers. *Math. Comp* 62:783–786.

Eichenauer-Herrmann, J. and F. Emmerich. 1994. Compound inversive congruential numbers: an average-case analysis. *Math. Comp.* To appear.

Eichenauer-Herrmann, J. and F. Emmerich. 1995. A review of compound methods for pseudorandom number generation. In *Proceedings of the 1st*

Salzburg Minisymposium on Pseudorandom Number Generation and Quasi-Monte Carlo Methods, Salzburg, Nov. 18, 1994, ed. Hellekalek, P., G. Larcher, and P. Zinterhof, 5–15. Vienna: ACPC – Austrian Center for Parallel Computation, Technical Report Series, University of Vienna.

Eichenauer-Herrmann, J. and H. Niederreiter. 1994. Bounds for exponential sums and their applications to pseudorandom numbers. *Acta Arith.* 67:269–281.

Entacher, K. 1995a. Selected random number generators in the run test. *Preprint*, Dept. of Mathematics, University of Salzburg, Austria.

Entacher, K. 1995b. Selected random number generators in the run test II: subsequence behavior. *Article in preparation*, Dept. of Mathematics, University of Salzburg, Austria.

Ferrenberg, A. M. and D. P. Landau. 1992. Monte Carlo simulations: hidden errors from "good" random number generators. *Phys. Rev. Lett* 69:3382–3384.

Fishman, G. S. and L. S. Moore. 1982. A statistical evaluation of multiplicative congruential random number generators with modulus $2^{31} - 1$. *J. Amer. Statist. Assoc.* 77:129–136.

Fishman, G. S. and L. S. Moore III. 1986. An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$. *SIAM J. Sci. and Statist. Comput.* 7:24–45. Erratum, ibid. 7:1058.

Flahive, M. and H. Niederreiter. 1992. In *Finite Fields, Coding Theory, and Advances in Communications and Computing*, ed. G. L. Mullen and P. J.-S. Shiue, 75–80. New York: Dekker.

Knuth, D.E. 1981. *The Art of Computer Programming, Vol. 2.* Addison-Wesley, Reading, Mass.

L'Ecuyer, P. 1992. Testing uniform random number generators. In *Proceedings of the 1992 Winter Simulation Conference (Arlington, Va., 1992)*, ed. J.J. Swain et al., 305–313. IEEE Press.

L'Ecuyer, P. 1994. Uniform random number generation. *Annals of Operations Research* 53: 77–120.

Leeb, H. 1994. Leeb, H., pLab- a system for testing random numbers. In *Proceedings of the International Workshop Parallel Numerics '94, Smolenice, Sept. 19-21*, ed. Vajteršic, M. and P. Zinterhof, 89–99. Bratislava: Slovak Academy of Sciences, Institute for Informatics.

Leeb, H. 1995. On the digit test. In *Proceedings of the 1st Salzburg Minisymposium on Pseudorandom Number Generation and Quasi-Monte Carlo Methods, Salzburg, Nov 18, 1994*, ed. Hellekalek, P., G. Larcher, and P. Zinterhof, 109–121. Vienna: ACPC – Austrian Center for Parallel Computation, Technical Report Series, University of Vienna.

Marsaglia, G. 1968. Random numbers fall mainly in the planes. *Proceedings of the National Academy of Sciences of the United States of America* 60:25–28.

Marsaglia, G. 1985. A Current View of Random Number Generation. In *Computer Science and Statistics, Proceedings of the Sixteenth Symposium on the Interface, Atlanta, march 1984.*, ed. Brillard, L., 3–10. Elsevier Science Publ. (North-Holland).

Niederreiter, H. 1992. *Random number generation and quasi-Monte Carlo methods.* Philadelphia: SIAM.

Niederreiter, H. 1994. On a new class of pseudorandom numbers for simulation methods. *J. Comp. Appl. Math.* 56:159–167.

Niederreiter, H. 1995a. New developments in uniform pseudorandom number and vector generation. In *Monte Carlo and quasi-Monte Carlo methods in scientific computing*, ed. H. Niederreiter and P.J.-S. Shiue. Berlin: Springer-Verlag, to appear.

Niederreiter, H. 1995b. Some linear and nonlinear methods for pseudorandom number generation. *In this volume.*

Park, S. K. and K. W. Miller. 1988. Random number generators: good ones are hard to find. *Comm. ACM* 31: 1192-1201.

Ripley, B. D. 1987. *Stochastic Simulation.* New York: John Wiley & Sons.

Stadlober, E. and R. Kremer. 1992. Sampling from discrete and continuous distributions with C-Rand. In *Simulation and Optimization*, ed. G. Pflug and U. Dieter. Lecture Notes in Economics and Math. Systems, Vol. 374, 154–162. Berlin: Springer–Verlag.

Stadlober, E. and F. Niederl. 1994. C-Rand: A package for generating nonuniform random variates. In: *Compstat '94, Software Descriptions*, 63–64.

Wegenkittl, S. 1995. Empirical testing of pseudorandom number generators. Master's thesis in preparation, Dept. of Mathematics, University of Salzburg, Austria.

AUTHOR BIOGRAPHY

PETER HELLEKALEK is an Assistant Professor in the Department of Mathematics at the University of Salzburg, Austria. He is leading the pLab group, a team of young mathematicians working on the theory and practice of random number generation. His research interests are random number generation, metric number theory and ergodic theory.