Journal of Modern Mathematics and Statistics 5 (4): 89-95, 2011
ISSN: 1994-5388

# Pseudorandom Number Generation by Inversive Methods

M.B.O. Akinwande
Department of Mathematics, Lagos State University, Ojo-Lagos, Nigeria

**Abstract:** The Classical Linear Congruential Method for generating uniform pseudorandom numbers has some deficiencies that can render them useless for some simulation problems. This fact motivated the design and analysis of Non-linear Congruential Methods for the generation of pseudorandom numbers. Inversive Methods are an interesting and very promising approach to produce uniform pseudorandom numbers. Researchers present a critical analysis of the recent developments on the topic. The exposition concentrates on recursive inversive congruential generators and digital inversive congruential generators.

**Key words:** Discrepancy, lattice test, period length, inversive pseudorandom numbers, Digital Method, Explicit Method

## INTRODUCTION

It is well known that generating good and reliable pseudorandom numbers is crucial for various fields that depend on the computer. The success of Monte Carlo studies or any computer simulation that requires randomness depends to a large extent on a good source of random numbers. General background material on pseudorandom numbers unit interval [0, 1] can be found in the books of Gentle (2003), Knuth (2011) and Niederreiter (1992) and in the survey articles of L'Ecuyer (1994). The Classical Methods for the generation of pseudorandom numbers such as Linear Congruential Method and Shift-register Methods produce sequences of pseudorandom numbers with too much intrinsic regularity (Knuth, 2011).

This state of affairs motivated the last few years various researches on the design and analysis of Non-linear Congruential Methods for the generation of pseudorandom numbers (Eichenauer-Herrmann, 1993; L'Ecuyer, 1994). The present research therefore, concentrates exclusively with the developments in this area which include the analysis of the Inversive Method which is a particularly attractive non-linear approach. In fact, no formal definition of a sequence of uniform pseudorandom number can be given; we only have certain characteristics in mind when we talk about such a sequence (Alhakim and Akinwande, 2009):

- The sequences is generated by deterministic algorithm
- The sequences should be uniformly distributed on the unit interval [0, 1]
- It should pass relevant statistical and theoretical test for randomness

All standard methods of generating uniform pseudorandom numbers are based on congruences and they all yield periodic sequences. The desired properties of sequences of pseudorandom numbers can be summarized as follow:

- Long period length
- Good statistical properties
- Good equidistribution properties
- Little intrinsic structure (such as lattice structure)
- Reasonably fast generation

## MATERIALS AND METHODS

**General Non-linear Congruential Method:** The coarse lattice structure inherent in the Linear Congruential Method can be broken up by using Non-linear Method to generate uniform pseudorandom number. A general framework for Non-linear Methods was described by Niederreiter (1992). Let: M = p be a large modulus and generate a sequence $y_0$, $y_1$, ... of elements $Z_p$ by the 1st-order recursion $y_{n+1} \equiv f(y_n) \bmod p$ for $n \geq 0$ with initial value $y_0$ where, f is a fixed integer-valued function on $Z_p$. Since, the recursion is of 1st-order the sequence is periodic with period of $y_n \leq p$. Now, suppose f is such that the sequence $y_0$, $y_1$, ... is purely periodic with least period length p then the map $n \in F_p \mapsto y_n \in F_p$ can be represented by uniquely determined polynomial $g \epsilon F_p[x]$ with d = deg(<p). Hence, we can write $y_n = g(n) \epsilon F_p$ for $n \geq 0$ where, n is also viewed as an element of $F_p$. The pseudorandom number $x_0$, $x_1$, ... in [0, 1] are obtained by the normalization:

$$x_n = \frac{1}{p} y_n \text{ for } n \geq 0$$

We obtained a Non-linear Method if the function f can not be represented by a linear polynomial modulo p. This type of pseudorandom numbers was first proposed by Eichenauer *et al.* (1988). Inversive Methods in uniform pseudorandom number generation achieve non-linearity by employing the operation of multiplicative inversive in suitable algebraic structures such as finite fields and residue class rings of the integers. We shall concentrate on the case of the finite fields. Thus, let denote the finite field of prime-power order q by $F_q$. In the case where, q is a prime p, we identify $F_p$ with $Z_p$ as a set. For convenience, we extend the definition of multiplication inversion as follows:

$$\bar{\alpha} = \begin{cases} \alpha^{-1} & \text{if} \quad \alpha \neq 0 \\ 0 & \text{if} \quad \alpha = 0 \end{cases}$$

Where, $\alpha \epsilon F_q$. Then, the map $\alpha \mapsto \bar{\alpha}$ becomes a permutation of $F_q$.

**Lattice test:** The following definition follows Niederreiter (1992) and makes sense for any congruential generator with prime modulus.

**Definition 1:** For a given $s \geq 1$, a congruential generator $y_0$, $y_1$, ... with modulus M = p prime passes the s-dimensional lattice test if the vectors $y_n$-$y_0$, $n \geq 1$, span $F_p^s$ where, $y_n = (y_n, y_{n+1}, \ldots, y_{n+s-1}) \epsilon F_p$ for $n \geq 0$.

We observe from Niederreiter (1992) that a linear congruential generator with prime modulus passes the lattice test only for dimension s = 1 but for non-linear congruential generators, the value of d = deg(g), g being the polynomial introduced is decisive. We now state the following theorem without proof which was shown by Eichenauer *et al.* (1988).

**Theorem 1:** A non-linear congruential generator with prime modulus passes the s-dimensional lattice test if and only if $s \leq d$ = deg(g).

**Remark:** d = 1 is impossible for a non-linear congruential generator. The congruence $y_n = an+b$ (mod p) leads to the recursion $y_{n+1} \equiv y_n+a$ (mod p) which is a linear congruential generator with multiplier 1 (which is a bad choice). The degree of a permutation polynomial over $F_p$ does not divide (p-1).

Since, we only consider non-linear congruential generators with maximal period length p, g(n) is a permutation polynomial. Hence, we have that $3 \leq d \leq p-2$. Thus, it follows that any non-linear congruential generator with prime modulus and maximal period length p passes, the s-dimensional lattice test at least s = 1-3.

**Uniformity and independence:** The one-dimensional, respectively the s-dimensional discrepancy allows us to measure how well given sequences of pseudorandom numbers fulfill the two basic requirements for pseudorandom numbers, uniformity and independence. Beside discrepancy, there exist other measures for the other uniformity of pseudorandom numbers. We will only consider the (extreme) discrepancy which is the most important measure in connection with pseudorandom numbers.

**Definition 2:** The s-dimensional (extreme) discrepancy of a set $P = (x_n)_{n=0}^{N-1}$ in $[1, 0)^s$ is defined by:

$$D_N^s(x_0, x_1, \ldots, x_{N-1}) = \sup_{j \in J} \left| \frac{A(j, P)}{N} - \lambda_s(j) \right|$$

where, J is the class of all subintervals j of $[1, 0)^s$ of the form:

$$j = \prod_{i=1}^{s} [u_i, v_i), \; 0 \leq u_i < v_i \leq 1 \text{ and } A(j, P)$$

denotes the cardinality of $P \cap j$. For a 1st-order, congruential generator with modulus M and maximal period length M, we clearly have:

$$\{x_0, x_1, \ldots, x_{M-1}\} = \left\{0, \frac{1}{M}, \frac{2}{M}, \ldots, \frac{M-1}{M}\right\}$$

By the result of Niederreiter (1992), we have:

$$D_M\left(0, \frac{1}{M}, \frac{2}{M}, \ldots, \frac{M-1}{M}\right) = \frac{1}{M}$$

And so, we have:

**Theorem 2:** For any 1st-order, congruential generator with modulus M and per $(x_n)$ = M, we have:

$$D_M(x_0, x_1, \ldots, x_{M-1}) = \frac{1}{M}$$

Now, we will provide upper bounds for the s-dimensional discrepancy $(s \geq 2)$ of overlapping s-tuples $x_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$ of non-linear congruential pseudorandom numbers with primes modulus. The following theorem from Eichenauer-Herrmann and Niederreiter (1994a) is only useful if number d = deg(g) is known. We observe that it has been possible to obtain discrepancy estimates even for parts of period and the result for special types of nonlinear congruential generators can be improved considerably as illustrated in Niederreiter and Winterhof (2001).

**Theorem 3:** For a sequence of non-linear congruential pseudorandom numbers $x_0, x_1, \ldots$ with prime modulus p, we have:

$$D_p^{(s)}(x_0, x_1, \ldots, x_{p-1}) \leq 1 - (1 - \tfrac{1}{p})^s + (d-1)p^{-1/2}(\tfrac{4}{\pi^2}\log p + 1.72)^s \text{ for } 2 \leq s \leq d \tag{1}$$

$$D_N^{(s)}(x_0, x_1, \ldots, x_{N-1}) \leq 1 - (1 - \tfrac{1}{p})^s + (d-1)\tfrac{p^{1/2}}{N}(\tfrac{4}{\pi^2}\log p + 1.72)^{s+1} \text{ for } 2 \leq s \leq d-1,\ 1 \leq N < p \tag{2}$$

Where:

$$x_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$$

We observe that the degree d of the polynomial g plays an important role. If d is of magnitude $p^{1/2}$ or larger, the bounds become useless, since we always have $0 \leq D_N^{(s)} \leq 1$. The second inequality in Theorem 3 which gives a bound for the s-dimensional discrepancy for parts of the period p is only useful if N, the number of points is of higher order of magnitude than $p^{1/2}(d-1)$. Thus by Eichenauer-Herrmann (1993), the upper bound in Theorem 3(ii) is when s = 1 in general best possible up to the logarithmic factor. Researchers now consider special cases of non-linear congruential generators.

**Inversive congruential generators:** The inversive congruential generators was first proposed by Eichenauer and Lehn (1986) and is defined by the recursion:

$$y_{n+1} \equiv a\overline{y}_n + b \bmod p$$

for $n \geq 0$ where, a, b and $y_0$ are well chosen integers in $F_p$ For $c \in F_p$, $\overline{c}$ is defined as the unique solution modulo p of the congruence if $c\overline{c} \equiv 1 \bmod p$ if $c \neq 0$ and c = 0 if c = 0. Clearly, $c\overline{c} \equiv c^{p-2} \bmod p$ for $p \geq 3$. A sequence of pseudorandom numbers $x_0, x_1, \ldots$ in [0, 1) is obtained by normalization $x_n = y_n/p$.

**Period length:** The parameters a and b should be chosen in such a way that the least period length of the sequence $x_0, x_1, \ldots$ is as large as possible. Since, an inversive congruential generator is defined by a 1st-order recursion, the maximal value for the least period length is equal to the modulus p. The following theorem which was proved by Eichenauer and Lehn (1986), yields a sufficient condition for maximal period length p.

**Theorem 4:** If $a, b \in F_p$ are such that the polynomial $x^2$-bx-a is primitive over $F_p$ then the sequence $x_0, x_1, \ldots$ of inversive congruential pseudorandom numbers with modulus p satisfies per $(x_n)$ = p.

A monic irreducible polynomial over $F_p$ of degree 2 is called a primitive polynomial over $F_p$, it has a root in $F_{p2}$ that generates the cyclic group $F_{p2}^*$. Parameters $a, b \in F_p$ such that $x^2$-bx-a is primitive over $F_p$ are tabulated by Hellekalek and Entacher (1995) for some primes such as $p = 2^{31}-1$. The condition that $x^2$-bx-a is a primitive polynomial over $F_p$ is sufficient but not necessary for maximal period length p.

A polynomial $x^2$-bx-a is called an Inversive Maximal Period polynomial (IMP-polynomial) if the corresponding inversive congruential generator with parameters a and b yields a sequence with maximal period p. An algorithm to find all IMP-polynomials over a given field $F_p$ was given by Chou (1995).

**Lattice test:** Consider the following theorem which proof is based on the corresponding result for the general non-linear congruential generator discussed before and can be found by Niederreiter (1992).

**Theorem 5:** An inversive congruential generator with prime modulus p and maximal period length passes the s-dimensional lattice test for all $s \leq p+1/2$. We recall that the lattice structure of linear congruential generators is completely different. Linear congruential generators fail this test for all dimensions $s \geq 2$.

**Hyperplane structure:** The following strong non-inearity property of inversive pseudorandom numbers was shown by Eichenauer-Herrmann (1992) which stands in sharp contrast to the lattice structure of linear congruential pseudorandom numbers.

**Theorem 6:** Let $s \geq 2$ then for every inversive congruential generator:

$$y_{n+1} \equiv a\overline{y}_n + b \bmod p$$

with prime modulus p and maximal period length p any hyperplane in $F_p^s$ contains at most s of the points $y_n = (y_n, y_{n+1}, \ldots, y_{n+s-1})$ with $0 \leq n \leq p-1$ and $y_n \ldots y_{n+s-2} \neq 0$. Observe that the condition $y_n, \ldots, y_{n+s-2} \neq 0$ eliminates exactly (s-1) of the points $y_n$ with $0 \leq n \leq p-1$ (these are the points on the boundary of $[0, 1)^s$ while the remaining (p-s+1) points avoid the planes.

**Independence:** The discrepancy bound for the general class of non-linear congruential generators does not provide a bound for the discrepancy of inversive congruential pseudorandom numbers, since we have $d = \deg(g) \geq p+1/2$ in case of the inversive congruential generator. The following upper and lower bounds for the discrepancy of inversive congruential pseudorandom numbers are due to Niederreiter (1992).

**Theorem 7:** For inversive congruential pseudorandom numbers $x_0, x_1, \ldots$ with prime modulus and maximal length, we have:

$$D_p^{(s)}(x_0, x_1, \ldots, x_{p-1}) \leq 1-\left(1-\tfrac{1}{p}\right)^s + \left(\tfrac{2s-2}{p^{1/2}}+\tfrac{s-1}{p}\right)\left(\tfrac{4}{\pi^2}\log\ p+1.72\right)^s$$

for $s \geq 2$ where, $x_n = (x_n, x_{n+1}, \ldots, x_{n+s-1})$, $n \geq 0$. The inequality gives a bound of the discrepancy of the points $x_0, x_1, \ldots, x_{p-1}$. For the discrepancy of parts of the period, i.e., $D_N^{(s)}(x_0, x_1, \ldots, x_{N-1})$ with $N<p$, there are no theoretical results available. The next theorem shows that the order of magnitude of the bound in theorem 7, $p^{1/2}(\log p)^s$ is in general, best possible up to the logarithmic factor. The total number of primitive polynomials $x^2$-bx-a over $F_p$ is $(\phi(p^2-1))/2$ where, $\phi$ is Euler's totient function.

**Theorem 8:** Let $p \geq 5$ be a prime and let $0<t<1$. Then, there are more than $A_p(t)\phi(p^2-1)/2$ primitive polynomials $x^2$-bx-a over $F_p$, such that for the corresponding inversive congruential pseudorandom numbers with modulus p, we have:

$$D_p^{(s)}(x_0, x_1, \ldots, x_{p-1}) > \frac{t}{2\pi+4}p^{-1/2}$$

for $s \geq 2$ where, $A_p(t)$ satisfy:

$$\lim_{p\to\infty} A_p(t) = \frac{1-t^2}{4-t^2} > 0 \ \text{ for all } \ t$$

**Recursive inversive pseudorandom numbers:** We choose a large prime modulus p and use the Recursive Non-linear Method with the special function $f(z)=a\bar{z}+b$ for all $z \in F_p$ where $a, b \in F_p$ are fixed parameters with $a \neq 0$. The resulting pseudorandom numbers $x_0, x_1, \ldots$ are called recursive (congruential) pseudorandom numbers which were introduced by Eichenauer and Lehn (1986). Thus, we have $per(x_n) \leq p$.

We observe that every primitive polynomial over $F_p$ is an IMP polynomial over $F_p$. Hence for every prime p, there exist $a, b \in F_p$ such that we can have $per(x_n) = p$. The s-dimensional serial test for recursive inversive pseudorandom number was first investigated by Niederreiter (1989). And, it was shown that if $per(x_n) = p$ then the discrepancy $D_p^{(s)}$ of overlapping s-tuples for the full period satisfies:

$$D_p^{(s)} = O(p^{-1/2}(\log\ p)^s)$$

For $1 \leq s<p$, the same bound holds for non-overlapping s-tuples as well. This upper bound is in general best possible up to the logarithm factor. Since in practice, we never exhaust the full period of a sequence of pseudorandom number, it is more important to have discrepancy bounds for parts of the period.

**Discrepancy bound:** The process made in the theory of certain exponential sums makes it possible to find nontrivial discrepancy bounds for individual sequences of these pseudorandom number for parts of the period since the introduction of recursive inversive pseudorandom number in 1986. The method for bounding $D_N^{(s)}$ for parts of the period is sufficiently general that it permits the treatment of sequence $x_0, x_1, \ldots$ of recursive inversive pseudorandom number for which $t = per(x_n)$ is arbitrary. The problem was solved by Niederreiter and Shparlinski (2001) for the dimension $s = 1$ and by Gutierrez *et al.* (2000) for $s \geq 2$. The results were stated without proof in the following theorem:

**Theorem 9:** For overlapping s-tuples of the recursive inversive pseudorandom number, we have:

$$D_N^{(s)} = O(N^{-1/2}p^{1/4}(\log\ p)^s) \ \text{ for } \ 1 \leq N \leq t$$

A similar result to the theorem 9 for recursive inversive pseudorandom number with prime power moduli was established by Niederreiter and Shparlinski (2000b). Their method can also be applied to the general non-linear generators described before. For instance, they proved a non-trivial discrepancy bound in the case where the case where the modulus M is a prime. In fact, this bound can be extended from 1st-order recursions to recursions of arbitrary order $m \geq 1$. In general setting, the modulus is a large prime p and the generating recursion has the form:

$$y_{n+m} \equiv f(y_n, \ldots, y_{n+m-1}) \mod p$$

for $n \geq 1$ where, f is a polynomial over $F_p$ in m variables and $y_0, y_1, \ldots, y_{m-1} \in F_p$ are initial values. A non-trivial discrepancy bound for this case was obtained by Gutierrez and Gomez-Perez (2001).

**Digital inversive pseudorandom numbers:** Let p be a prime and suppose $F_q$ is a finite of order $q = p^k$ for some integer $k \geq 1$. The preferred choice $p = 2$. For fixed parameters $\alpha, \beta \in F_q$ with $\alpha \neq 0$, we generate the sequence $\gamma_0, \gamma_1, \ldots$ of elements of $F_q$ by the recursion:

$$\gamma_{n+1} = \alpha\bar{\gamma} + \beta$$

for $n \geq 0$ with initial value $\gamma_0$. If $\{\lambda_0, \ldots, \lambda_k\}$ is an ordered basis of the vector space $F_q$ over $F_p$ then we have the unique representation:

$$\gamma_n = \sum_{j=1}^{k} c_n^{(j)} \lambda_j \text{ for } n \ge 0$$

with all $c^{(j)}_n \epsilon F_p$. Now, a sequence $x_0$, $x_1$, ... of digital inversive pseudorandom numbers is defined by:

$$x_n = \sum_{j=1}^{k} c_n^{(j)} p^{-j} \text{ for } n \ge 0$$

These pseudorandom numbers were introduced by Eichenauer-Herrmann and Niederreiter (1994b). The speedup in the generation algorithm of digital inversive pseudorandom number results from the fact that whereas multiplicative inversion in $F_q$ requires in general O(log q) field operations in the case $q = 2^k$, we need only O(log log q) field operations due to a specialized inversion algorithm for this case. Obviously if $per(\gamma_n) = t$ then $per(x_n) = t$ and we clearly have $t \le q$. The criterion for having $t = q$ is completely analogous to that for maximum possible period length in the Recursive Inversive Method stated. Particularly, we can always achieve $t = q$ in the Digital Inversive Method. The s-dimensional serial test digital inversive pseudorandom number was first studied by Eichenauer-Herrmann and Niederreiter (1994a, b). It was shown that if $t = q$ then the discrepancy $D_q^{(s)}$ of overlapping s-tuples for the full period satisfies $D_q^{(s)} = O(q^{1/2}(\log\ q)^s)$ and this upper bound is in general best possible up to the logarithmic factor. Niederreiter and Shparlinski (2000a) obtained the 1st non-trivial discrepancy bound for the general case $1 \le N \le t \le q$. The resulting discrepancy bound is completely similar to that in theorem 9.

**Theorem 10:** For overlapping s-tuples of digital inversive pseudorandom number we have $D_N^{(s)} = O(\min(N^{-1}q^{1/2}\log\ q,\ N^{-1/2}q^{1/4})\ (\log\ q)^s$ for $1 \le N \le t$. We now describe briefly a new variant of the Digital Inversive Method which was introduced independently by Levin (2000) and Niederreiter and Winterhof (2000). Suppose $q = p^k$ and let $\{\lambda_1, ..., \lambda_k\}$ be an ordered basis of the vector space $F_q$ over $F_p$ then we define $\xi_n \epsilon F_q$, $n \ge 0$ by:

$$\xi_n = \sum_{j=1}^{k} \mathbf{n}_j \lambda_j$$

if

$$\mathbf{n} \equiv \sum_{j=1}^{k} \mathbf{n}_j p^{j-1} \textbf{ mod q}$$

with $0 \le n_j < p$ for $1 \le j \le k$. For a given $\alpha, \beta \epsilon F_q$ with $\alpha \ne 0$ we generate a sequence $\eta_0$, $\eta_1$, ... of elements of $F_q$ by the explicit formula:

$$\eta_n = \overline{\alpha \xi_n + \beta} \text{ for } n \ge 0$$

We have the unique representation:

$$\eta_n = \sum_{j=1}^{k} d_n^{(j)} \lambda_j \text{ for } n \ge 0$$

with all $d_n^{(j)} \epsilon F_p$. Finally, we derive explicit inversive pseudorandom numbers by putting:

$$x_n = \sum_{j=1}^{k} d_n^{(j)} p^{-j} \text{ for } n \ge 0$$

Obviously, $per(x_n) = q$. In the special case $k = 1$, we get the explicit inversive (congruential) pseudorandom numbers. With an appropriate definition of successive elements, the following discrepancy bounds were shown by Niederreiter and Winterhof (2000).

**Theorem 11:** For digital explicit inversive pseudorandom number we have with a proper definition of the serial test, $D_N^{(s)} = O(\min(N^{-1}q^{1/2}\ \log\ q,\ N^{-1/2}q^{1/4})\ (\log\ q)^s$ for $1 \le N < q$ and $D_q^{(s)} = O(q^{-1/2}(\log\ q)^s)$. Digital explicit inversive pseudorandom number can also be used for Parallelized Simulation Methods as was demonstrated by Niederreiter and Winterhof (2001). In order to generate t parallel streams of pseudorandom numbers with $1 \le t \le q$, one chooses for each $i = 1, ..., t$ parameters $\alpha_i$ and $\beta_i$ in the roles $\alpha$ and $\beta$, respectively in such a way that the elements $\alpha_1^{-1}\beta_1, ..., \alpha_r^{-1}\beta_r$ of $F_q$ are distinct. Then, the generated parallel streams simulate t independent uniformly distributed random variables.

## RESULTS AND DISCUSSION

Firstly, inversive congruential pseudorandom number are vastly superior with respect to lattice structure in comparison to the Linear Congruential Method where a laborious calculations are needed to find multipliers that yield a nearly optimal lattice structure even for a modest range of dimension. Also, inversive congruential pseudorandom number show a better behavior under the serial test thus it display more irregularity in their distribution and so model truly random numbers more closely than linear congruential pseudorandom number. The Digital Inversive Method for pseudorandom number generation has several attractive properties. First of all, there exists a handy criterion for the maximum possible period length $q = p^k$ namely that $x^2$-$\beta$x-$\alpha$ is an IMP polynomial over $F_q$. The property that $x^2$-βx-α is a primitive polynomial over $F_q$ provides a sufficient condition for the maximum period length q. Any digital inversive sequence with maximum period length show nice statistical independence properties in the sense of asymptotic discrepancy since, there exist digital inversive sequences with a discrepancy $D_q^{(s)}$ of an order of magnitude at least $q^{-1/2}$. Digital inverse pseudorandom numbers have the usual merit of inversive pseudorandom numbers, namely that once the maximum possible period length is achieved then they satisfy the upper discrepancy bounds irrespective of the specific choice of the parameters α and β in the recursion 1. The most convenient practical implementation of the Digital Inversive Method arises if we choose p = 2 and a sufficiently large integer k such that an acceptable maximum period length $q = 2^k$ is attained. This choice has the additional advantage that allows a fast implementation of the necessary arithmetic. One step of the recursion 1 requires then only O(log log q) multiplications in $F_q$, one addition in $F_q$ and some cyclic shifts of coordinate vectors. This should be contrasted with the cost of one step in the Recursive Inversive Congruential Method with prime modulus which in the present setup corresponds to the choice where p is a large prime and k = 1. In the latter method, the number of required multiplications in $F_q$ in one step of the recursion is O(log p).

## CONCLUSION

Consequently for comparable maximum period lengths the Digital Inversive Method with p = 2 allows a significantly faster generation of the pseudorandom numbers than the Inversive Congruential Method with prime modulus. The Inversive Congruential Method allows a wide choice of parameters, all of which lead to guaranteed and comparable structural and statistical properties. This feature can be of great practical value in various parallelized simulation techniques in which many parallel streams of pseudorandom numbers are needed but in case of Linear Congruential Method with prime modulus p, just choosing any primitive root a modulo p is certainly not enough.

## REFERENCES

Alhakim, A. and M. Akinwande, 2009. A multiple stream generator based on de Bruijn digraph homomorphisms. J. Stat. Comput. Simul., 79: 1371-1380.

Chou, W.S., 1995. On inversive maximal period polynomials over finite fields. Appl. Algebra Eng. Commun. Comput., 6: 245-250.

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

Eichenauer, J., H. Grothe and J. Lehn, 1988. Marsaglia's lattice test and non-linear congruential pseudo random numbers generators. Metrika, 35: 241-350.

Eichenauer-Herrmann, J., 1992. Inversive congruential pseudorandom numbers: A tutorial. Int. Stat. Rev., 60: 167-176.

Eichenauer-Herrmann, J., 1993. Equidistribution properties of nonlinear congruential pseudorandom numbers. Metrika, 40: 333-338.

Eichenauer-Herrmann, J. and H. Niederreiter, 1994a. On the statistical independence of nonlinear congruential pseudorandom numbers. ACM Trans. Model. Comput. Simul., 4: 89-95.

Eichenauer-Herrmann, J. and H. Niederreiter, 1994b. Digital inversive pseudorandom numbers. ACM Trans. Model. Comput. Simul., 4: 339-349.

Gentle, J.E., 2003. Random Number Generation and Monte Carlo Methods. 2nd Edn., Springer-Verlag, New York, ISBN-10: 0387001786, pp: 264.

Gutierrez, J., H. Niederreiter and I.E. Shparlinski, 2000. On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period. Monatsh. Math., 129: 31-36.

Gutierrez, J. and D. Gomez-Perez, 2001. Iterations of multivariate polynomials and discrepancy of pseudorandom numbers. Applied Algebra Algebraic Algorithms Error-Correcting Codes, 2227: 192-199.

Hellekalek, P. and K. Entacher, 1995. Tables of IMP-Polynomials. Version 1.0, Research Institute for Software Technology, University of Salzburg.

Knuth, D.E., 2011. The Art of Computer Programming. 3rd Edn., Addison-Wesley, Boston.

L'Ecuyer, P., 1994. Uniform random number generations. Ann. Oper. Res., 53: 77-120.

Levin, M.B., 2000. Explicit digital inversive pseudorandom numbers. Math. Slovaca, 50: 581-598.

Niederreiter, H., 1989. The serial test for congruential pseudorandom numbers generated by inversions. Math. Comp., 55: 277-287.

Niederreiter, H., 1992. Random Number Generation and Quasi-Monte Carlo Methods. SIAM, Philadelphia, ISBN: 9780898712957, Pages: 241.

Niederreiter, H. and A. Winterhof, 2000. Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. Acta Arith., 93: 387-399.

Niederreiter, H. and I.E. Shparlinski, 2000a. Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. Acta Arith., 92: 89-98.

Niederreiter, H. and I.E. Shparlinski, 2000b. On the distribution of pseudorandom numbers and vectors generated by inversive methods. Appl. Algebra Eng. Commun. Comput., 10: 189-202.

Niederreiter, H. and A. Winterhof, 2001. On a new class of inversive pseudorandom numbers for parallelized simulation methods. Periodica Math. Hungarica, 42: 77-87.

Niederreiter, H. and I.E. Shparlinski, 2001. On the distribution of inversive congruential pseudorandom numbers in parts of the period. Math. Comput., 70: 1569-1574.