Construction of inversive congruential pseudorandom number generators with maximal period length

Jürgen Eichenauer-Herrmann

Fachbereich Mathematik, Technische Hochschule, Darmstadt, Germany

Received 25 March 1991
Revised 21 May 1991

Abstract


The inversive congruential method for generating uniform pseudorandom numbers is a particularly attractive alternative to linear congruential generators with their well-known inherent deficiencies like the unfavourable coarse lattice structure in higher dimensions. In the present paper the modulus in the inversive congruential method is chosen as a power of an arbitrary odd prime. The existence of inversive congruential generators with maximal period length is proved by a new constructive characterization of these generators.

Keywords: Pseudorandom numbers, inversive congruential method, prime power modulus, maximal period length.

1. Introduction

The linear congruential method for generating uniform pseudorandom numbers in the interval \([0, 1)\) shows a lot of undesirable regularities which are due to the linearity of the underlying recursion (cf. \([12,13,18,19]\)). Therefore several nonlinear congruential generators have been proposed and analysed (cf. \([1-11,14-17,19]\)). A particularly promising method is based on achieving nonlinearity by employing the operation of multiplicative inversion with respect to a given modulus. In case the modulus is a prime (cf. \([1,3,6,14,16,17]\)) or a power of two (cf. \([5,8,10,16]\)), several results on the corresponding inversive congruential sequences are available. When the modulus is a power of an arbitrary odd prime, inversive congruential sequences with maximal period length have been characterized (cf. \([11]\)) and their statistical independence properties have been analysed (cf. \([7]\)). However, the existence of inversive
congruential sequences with maximal period length could not yet be proved for moduli being a power of an arbitrary odd prime. This was the motivation for the present paper, where inversive congruential generators with maximal period length are explicitly constructed.

Let \( p \geq 3 \) be a prime, and let \( m \geq 2 \) be an integer. For integers \( a, b \) with \( a \neq 0 \pmod{p} \) a sequence \((x_n)_{n \geq 0}\) of integers with \( x_n \neq 0 \pmod{p} \) for \( n \geq 0 \) is called an inversive congruential sequence if the recursion

\[
x_{n+1} \equiv ax_n^{-1} + b \pmod{p^m}, \quad n \geq 0,
\]
is satisfied, where \( x_n^{-1} \) denotes the multiplicative inverse of \( x_n \) modulo \( p^n \). Let

\[
\lambda = \min\{n \geq 1 | x_n = x_0 \pmod{p}\}
\]
be the period length of \((x_n)_{n \geq 0}\) modulo \( p \). A method for computing the period length \( \lambda \) is described in [3]. In the present paper the existence of inversive congruential sequences with maximal period length \( \lambda p^{m-1} \) modulo \( p^m \) is proved by an explicit construction.

In the second section the main result is stated precisely. Its comprehensive proof is sketched in the third section.

2. Sequences with maximal period length

First, a characterization of inversive congruential sequences with maximal period length \( \lambda p^{m-1} \) modulo \( p^m \) is given, which can easily be deduced from [11, Theorem 12].

**Proposition 1.** (a) Suppose that \( \lambda = 1 \), i.e., \( x_0^2 - bx_0 - a = 0 \pmod{p} \), and \( m \geq 3 \). Then the inversive congruential sequence \((x_n)_{n \geq 0}\) has maximal period length \( p^{m-1} \) modulo \( p^m \) if and only if

1. \( a = 2 \pmod{3} \) and \( x_0^2 - bx_0 - a = 6 \pmod{9} \) for \( p = 3 \) or
2. \( a = -x_0^2 \pmod{p} \) and \( x_0^2 - bx_0 - a \equiv 0 \pmod{p^2} \) for \( p > 5 \).

(b) Suppose that \( \lambda \geq 2 \), i.e., \( x_0^2 - bx_0 - a \neq 0 \pmod{p} \). Then the inversive congruential sequence \((x_n)_{n \geq 0}\) has maximal period length \( \lambda p^{m-1} \) modulo \( p^m \) if and only if \( x_{\lambda} \neq x_0 \pmod{p^2} \).

Proposition 1 shows that inversive congruential sequences with maximal period length \( \lambda p^{m-1} \) can be characterized by simple explicit conditions for \( \lambda = 1 \), whereas for \( \lambda \geq 2 \) the crucial condition \( x_{\lambda} \neq x_0 \pmod{p^2} \) is only implicit. The difficulty in evaluating this condition arises from the nonlinearity of the underlying recursion. Nevertheless, in the following main result an explicit characterization is established.

**Theorem 2.** Suppose that \( \lambda \geq 2 \). Let \( \xi \) be an integer with \( x_\lambda = x_0 + p\xi \pmod{p^2} \). For integers \( \alpha, \beta \), let \((y_n)_{n \geq 0}\) be a sequence of integers with \( y_0 = x_0 \pmod{p} \) and

\[
y_{n+1} \equiv (a + p\alpha)y_n^{-1} + b + p\beta \pmod{p^m}, \quad n \geq 0.
\]

Then the inversive congruential sequence \((y_n)_{n \geq 0}\) has maximal period length \( \lambda p^{m-1} \) modulo \( p^m \) if and only if

\[
\lambda(x_0^2 - bx_0 - a)(b\alpha - 2a\beta) + \xi(a(4a + b^2) \neq 0 \pmod{p}).
\]
3. Proof of Theorem 2

(i) First, observe that the sequence \((y_n)_{n \geq 0}\) is well defined since \(y_n = x_n \mod p^n\) for \(n \geq 0\). In the following presentation the integer matrix
\[
A = \begin{pmatrix} b & a \\ 1 & 0 \end{pmatrix}
\]
plays an important role. Let \(I\) denote the unit matrix and let \((a_n)_{n \geq 0}\) be a sequence of integers with \(a_0 = 0, a_1 = 1\) and \(a_n = ba_{n-1} + aa_{n-2}\) for \(n \geq 2\). Then
\[
A^n = aq_{n-1}I + q_nA
\]
and
\[
x_n \equiv (q_{n+1}x_0 + aq_n)(q_nx_0 + aq_{n-1})^{-1} \mod p^n
\]
for \(n \geq 1\) can easily be proved by induction. Therefore one obtains
\[
x_0 + p\xi \equiv x_\lambda \equiv (q_{\lambda+1}x_0 + aq_\lambda)(q_\lambda x_0 + aq_{\lambda-1})^{-1} \mod p^2,
\]
which yields
\[
q_\lambda(x_0^2 + bx_0 - a) + p\xi(q_\lambda x_0 + aq_{\lambda-1}) = 0 \mod p^2.
\]
Now, the assumption \(\lambda \geq 2\), i.e., \(x_0^2 - bx_0 - a \not\equiv 0 \mod p\), implies that \(q_\lambda \equiv p\nu_0 \mod p^2\) and hence
\[
A^\lambda \equiv aq_{\lambda-1}I + p\nu_0A \mod p^2,
\]
where \(\nu_0\) denotes an integer with \(\nu_0 \equiv -\xi(x_0^2 - bx_0 - a)^{-1}aq_{\lambda-1} \mod p\).

(ii) Let \(\nu_1, \nu_2\) be integers with
\[
\nu_1 \equiv \lambda(4a + b^2)^{-1}(2\alpha + b_\beta)q_{\lambda-1} \mod p
\]
and
\[
\nu_2 \equiv \lambda(4a + b^2)^{-1}(2a_\beta - b\alpha)q_{\lambda-1} \mod p.
\]
Note that \(4a + b^2 \not\equiv 0 \mod p\) follows from part (ii) of the Theorem in [3]. Furthermore, let
\[
B = \begin{pmatrix} \beta_1 & \beta_2 \\ \beta_3 & \beta_4 \end{pmatrix}
\]
be an integer matrix with
\[
(4a + b^2)B = (2\alpha + b_\beta)A + (2a_\beta - b\alpha)I \mod p.
\]
Then, according to (i), one obtains
\[
(A + pB)^\lambda = A^\lambda + p\lambda A^{\lambda-1}B = aq_{\lambda-1}I + p(\nu_0A + \lambda aq_{\lambda-1}A^{-1}B)
\]
\[
= aq_{\lambda-1}I + p\left(\nu_0A + \nu_1I + \nu_2A^{-1}\right)
\]
\[
= aq_{\lambda-1}I + p\begin{pmatrix} b\nu_0 + a\nu_1 & a(\nu_0 + \nu_2) \\ \nu_0 + \nu_2 & a\nu_1 - b\nu_2 \end{pmatrix} \mod p^2.
\]
(iii) Subsequently, let \((z_n)_{n \geq 0}\) be a sequence of integers with 
\[
z_0 := (1 - p\beta_3)y_0 - p\beta_4 \pmod{p^2}
\]
and 
\[
z_{n+1} \equiv ((b + p\beta_1)z_n + a + p\beta_2)((1 + p\beta_3)z_n + p\beta_4)^{-1} \pmod{p^2}, \quad n \geq 0.
\]
Note that the sequence \((z_n)_{n \geq 0}\) is well defined since 
\(z_n \equiv x_n \pmod{p}\) for \(n \geq 0\). Furthermore, let 
\(\gamma_1^{(n)}, \ldots, \gamma_4^{(n)}\) be integers with 
\[
(A + pB)^n = \begin{pmatrix}
\gamma_1^{(n)} & \gamma_2^{(n)} \\
\gamma_3^{(n)} & \gamma_4^{(n)}
\end{pmatrix},
\]
for \(n \geq 0\). Then 
\[
z_n \equiv (\gamma_1^{(n)}z_0 + \gamma_2^{(n)})(\gamma_3^{(n)}z_0 + \gamma_4^{(n)})^{-1} \pmod{p^2}
\]
for \(n \geq 0\) can easily be proved by induction. Hence, it follows from (ii) that 
\[
z_\lambda = ((aq_{\lambda - 1} + p(bv_0 + au_1))z_0 + pa(v_0 + v_2)) \\
\cdot (p(v_0 + v_2)z_0 + aq_{\lambda - 1} + p(au_1 - bv_2))^{-1} \\
\equiv (aq_{\lambda - 1}z_0 + p[(bv_0 + au_1)z_0 + a(v_0 + v_2)]) \\
\cdot ((aq_{\lambda - 1})^{-1} - p(aq_{\lambda - 1})^{-2}[(v_0 + v_2)z_0 + av_1 - bv_2]) \\
\equiv z_0 - p(aq_{\lambda - 1})^{-1}(v_0 + v_2)(z_0^2 - bz_0 - a) \\
\equiv z_0 + pa^{-1}(4a + b^2)^{-1}\lambda(x_0^2 - bx_0 - a)(b\alpha - 2a\beta) + \xi a(4a + b^2) \pmod{p^2}.
\]
(iv) Finally, a short calculation and an induction argument show that 
\[
y_n \equiv (1 + p\beta_3)z_n + p\beta_4 \pmod{p^2}, \quad n \geq 0,
\]
where the relations \(\alpha \equiv \beta_2 + a\beta_3 - b\beta_4 \pmod{p}\) and \(\beta \equiv \beta_1 + \beta_4 \pmod{p}\) are used. Therefore 
\(y_\lambda \equiv y_0 \pmod{p^2}\) if and only if 
\(z_\lambda \equiv z_0 \pmod{p^2}\), i.e., according to (iii), if and only if 
\[
\lambda(x_0^2 - bx_0 - a)(b\alpha - 2a\beta) + \xi a(4a + b^2) \equiv 0 \pmod{p}.
\]
Hence, the desired result follows from Proposition 1(b).

References