On the Period Length of Pseudorandom Vector Sequences
Generated by Matrix Generators

By Jürgen Eichenauer-Herrmann, Holger Grothe, and Jürgen Lehn

Abstract. In Tahmi [5], Niederreiter [4], Afflerbach and Grothe [1], and Grothe [2] linear recursive congruential matrix generators for generating r-dimensional pseudorandom vectors are analyzed. In particular, conditions are established which ensure that the period length equals \( p^r - 1 \) for any nonzero starting vector in case of a prime modulus \( p \). For a modulus of the form \( p^\alpha, \alpha \geq 2 \) and \( p \) prime, this paper describes a simple method for constructing matrix generators having the maximal possible period length \( (p^r - 1) \cdot p^{\alpha-1} \) for any starting vector which is nonzero modulo \( p \).

1. Introduction and Notation. A linear recursive congruential matrix generator for generating r-dimensional pseudorandom vectors is of the form

\[
\bar{x}_{n+1} \equiv A \cdot \bar{x}_n \pmod{m}, \quad \bar{x}_{n+1} \in \mathbb{Z}_m^r, \quad n \geq 0,
\]

where the modulus \( m \) is a positive integer, \( \mathbb{Z}_m = \{0, 1, \ldots, m - 1\} \), \( \bar{x}_0 \in \mathbb{Z}_m^r \), and \( A \in \mathbb{Z}_m^{r \times r} \), i.e., \( A \) is an \( r \times r \)-matrix with elements in \( \mathbb{Z}_m \). In the sequel it is assumed that the matrix \( A \) is nonsingular modulo \( m \). Then the vector sequence \((\bar{x}_n)_{n \geq 0}\) generated by (1) is purely periodic, and the smallest positive integer \( \lambda = \lambda(A, \bar{x}_0, m) \) with \( \bar{x}_1 = \bar{x}_0 \) is called the period length of the vector sequence \((\bar{x}_n)_{n \geq 0}\).

Analogously, the matrix sequence \((A_n)_{n \geq 0}\) with \( A_n \equiv A^n \pmod{m} \), \( A_n \in \mathbb{Z}_m^{r \times r} \), is purely periodic, and the smallest positive integer \( \lambda = \lambda(A, m) \) for which \( A_\lambda \) equals the identity matrix \( I \) is called the period length of the matrix sequence \((A_n)_{n \geq 0}\).

The following two remarks are immediate consequences of these definitions.

Remark 1. The period length \( \lambda(A, \bar{x}_0, m) \) of the vector sequence \((\bar{x}_n)_{n \geq 0}\) divides the period length \( \lambda(A, m) \) of the matrix sequence \((A_n)_{n \geq 0}\) for any starting vector \( \bar{x}_0 \in \mathbb{Z}_m^r \).

Remark 2. If \( A_\nu = I \) for some positive integer \( \nu \), then the period length \( \lambda(A, m) \) of the matrix sequence \((A_n)_{n \geq 0}\) divides \( \nu \).

It is well known (cf. Tahmi [5], Niederreiter [4], and Grothe [2]) that \( \lambda(A, \bar{x}_0, p) = \lambda(A, p) = p^r - 1 \) for any starting vector \( \bar{x}_0 \in \mathbb{Z}_p^r \setminus \{0\} \) in case of a prime modulus \( m = p \) if the characteristic polynomial of the matrix \( A \) is primitive modulo \( p \). In this paper the case of a modulus \( m = p^\alpha, \alpha \geq 2 \), is considered where \( p \) is a prime number. It is shown that for \( p \geq 3 \) or \( r \geq 2 \) there exist matrix generators (1) with period length \( (p^r - 1) \cdot p^{\alpha-1} \) for any starting vector which is nonzero modulo \( p \), and a simple method is described for determining such a generator. Observe that \( (p^r - 1) \cdot p^{\alpha-1} \) is the maximal possible period length according to the following technical lemma.

Received March 1, 1988.

1980 Mathematics Subject Classification (1985 Revision). Primary 65C10; Secondary 11K45.

Key words and phrases. Pseudorandom vector sequences, matrix generator, period length.

**Lemma.** Let $A \in \mathbb{Z}_p^{r \times r}$, $\alpha \geq 1$, be a matrix which is nonsingular modulo $p$, and define matrices $A_n \in \mathbb{Z}_p^{r \times r}$ by $A_n \equiv A^n \pmod{p^{\alpha+1}}$, $n \geq 0$. Let $\lambda_\alpha = \lambda(A, p^\alpha)$ and $\lambda_{\alpha+1} = \lambda(A, p^{\alpha+1})$ denote the period lengths of the matrix sequence $(A_n)_{n \geq 0}$ modulo $p^\alpha$ and modulo $p^{\alpha+1}$, respectively. Then

$$
\lambda_{\alpha+1} = \begin{cases}
\lambda_\alpha & \text{for } A^{\lambda_\alpha} \equiv I \pmod{p^{\alpha+1}}, \\
\lambda_\alpha \cdot p & \text{for } A^{\lambda_\alpha} \not\equiv I \pmod{p^{\alpha+1}}.
\end{cases}
$$

**Proof.** From $A^{\lambda_\alpha} \equiv I \pmod{p^{\alpha+1}}$ it follows that $A^{\lambda_\alpha} = I + p^\alpha \cdot B$ for some matrix $B \in \mathbb{Z}_p^{r \times r}$. Therefore,

$$
A^{\lambda_\alpha} \cdot p = (I + p^\alpha \cdot B)^p = I + \binom{p}{1} \cdot p^\alpha \cdot B + \binom{p}{2} \cdot (p^\alpha \cdot B)^2 + \cdots + (p^\alpha \cdot B)^p,
$$

which yields $A^{\lambda_\alpha} \cdot p \equiv I \pmod{p^{\alpha+1}}$, i.e., $\lambda_{\alpha+1}$ divides $\lambda_\alpha \cdot p$ according to Remark 2. From $A^{\lambda_{\alpha+1}} \equiv I \pmod{p^{\alpha+1}}$ it follows that $A^{\lambda_{\alpha+1}} \equiv I \pmod{p^{\alpha}}$, i.e., $\lambda_\alpha$ divides $\lambda_{\alpha+1}$ according to Remark 2, which proves the lemma. □

The purpose of this paper is to prove the following result.

**Theorem.** Let $B \in \mathbb{Z}_p^{r \times r}$, $\alpha \geq 2$, be a matrix whose characteristic polynomial is primitive modulo $p$. Then

$$(2) \quad B^{p^\alpha-1} \equiv I + p^\alpha \cdot C \pmod{p^2}
$$

for some matrix $C \in \mathbb{Z}_p^{r \times r}$. Let $D \in \mathbb{Z}_p^{r \times r}$ denote an arbitrary matrix with $B \cdot D \equiv D \cdot B \pmod{p}$,

$$(3) \quad \det(D) \not\equiv 0 \pmod{p} \quad \text{for } p \geq 3,
$$

and

$$(4) \quad \det(D) \equiv \det(D + I) \equiv 1 \pmod{2} \quad \text{for } p = 2.
$$

Define a matrix $A \in \mathbb{Z}_p^{r \times r}$ by

$$(5) \quad A \equiv B \cdot (I + p^\alpha \cdot (C - D)) \pmod{p^\alpha}.
$$

Then the period length of the vector sequence $(\vec{x}_n)_{n \geq 0}$ generated according to (1) with matrix $A$ and modulus $m = p^\alpha$ is given by

$$
\lambda(A, \vec{x}_0, p^\alpha) = (p^\alpha - 1) \cdot p^{\alpha-1}
$$

for any starting vector $\vec{x}_0 \in \mathbb{Z}_p^r$ with $\vec{x}_0 \not\equiv \vec{0} \pmod{p}$.

**Proof.** The proof is subdivided into four parts (i) to (iv).

(i) Because of $A \equiv B \pmod{p}$ according to (5) it follows that

$$(6) \quad \lambda(A, \vec{x}_0, p) = \lambda(A, p) = p^\alpha - 1
$$

for any starting vector $\vec{x}_0 \in \mathbb{Z}_p^r \setminus \{\vec{0}\}$, since the characteristic polynomial of the matrix $B$ is primitive modulo $p$. In particular, $B^{p^\alpha-1} \equiv I \pmod{p}$ holds. Hence a matrix $C$ with (2) exists. Observe that (2) yields $B \cdot C \equiv C \cdot B \pmod{p}$, which implies that $B \cdot (C - D) \equiv (C - D) \cdot B \pmod{p}$ because of the hypothesis $B \cdot D \equiv D \cdot B \pmod{p}$. Therefore (5) and (2) yield

$$(7) \quad A^{p^\alpha-1} \equiv [B \cdot (I + p^\alpha \cdot (C - D))]^{p^\alpha-1} \equiv B^{p^\alpha-1} \cdot (I + (p^\alpha - 1) \cdot p \cdot (C - D)) \equiv (I + p \cdot C) \cdot (I - p \cdot (C - D)) \equiv I + p \cdot D \pmod{p^2}.
$$
If $p = 2$ then it follows from (7) that

$$A^{2^2 - 1} = I + 2 \cdot D + 4 \cdot E$$

for some matrix $E \in \mathbf{Z}^{r \times r}$ and hence

$$A^{(2^2 - 1)^2} = (I + 2 \cdot D + 4 \cdot E)^2 = I + 4 \cdot D + 4 \cdot D^2 + 8 \cdot F$$

for some matrix $F \in \mathbf{Z}^{r \times r}$, i.e.,

$$A^{(2^2 - 1)^2} \equiv I + 4 \cdot D \cdot (D + I) \pmod{8}.$$ 

(ii) Now it is shown by induction that in case of $p \geq 3$,

$$A^{(p^r - 1) \cdot p^\nu} \equiv I + p^{\nu + 1} \cdot D \pmod{p^{\nu + 2}}$$

for $0 \leq \nu \leq \alpha - 2$. Obviously, (7) is equivalent to (8) for $\nu = 0$. If (8) is valid for some $\nu$ with $0 \leq \nu \leq \alpha - 3$, then

$$A^{(p^r - 1) \cdot p^\nu} = I + p^{\nu + 1} \cdot D + p^{\nu + 2} \cdot E_{\nu}$$

for some matrix $E_{\nu} \in \mathbf{Z}^{r \times r}$ and hence

$$A^{(p^r - 1) \cdot p^{\nu + 1}} = (I + p^{\nu + 1} \cdot (D + p \cdot E_{\nu}))^p = I + p^{\nu + 2} \cdot (D + p \cdot E_{\nu}) + p^{\nu + 3} \cdot F_{\nu}$$

for some matrix $F_{\nu} \in \mathbf{Z}^{r \times r}$ because of $p \geq 3$, which yields

$$A^{(p^r - 1) \cdot p^{\nu + 1}} \equiv I + p^{\nu + 2} \cdot D \pmod{p^{\nu + 3}}.$$ 

Therefore (8) holds for $0 \leq \nu \leq \alpha - 2$. It can be similarly proved that in case of $p = 2$,

$$A^{(2^2 - 1) \cdot 2^\nu} \equiv I + 2^{\nu + 1} \cdot D \cdot (D + I) \pmod{2^{\nu + 2}}$$

for $1 \leq \nu \leq \alpha - 2$.

(iii) Because of (3), (4), (6), (7), (8) and (9) it follows from the lemma that

$$\lambda(A, p^{\nu + 1}) = (p^r - 1) \cdot p^\nu$$

for $0 \leq \nu \leq \alpha - 1$. Note that if $\bar{x}_0 \not\equiv \bar{0} \pmod{p}$, then

$$D \cdot \bar{x}_0 \not\equiv \bar{0} \pmod{p} \quad \text{for } p \geq 3$$

and

$$D \cdot (D + I) \cdot \bar{x}_0 \not\equiv \bar{0} \pmod{p} \quad \text{for } p = 2$$

because of (3) and (4), respectively. Therefore (7), (8) and (9) show that

$$A^{(p^r - 1) \cdot p^\nu} \cdot \bar{x}_0 \not\equiv \bar{x}_0 \pmod{p^{\nu + 2}}$$

for $\bar{x}_0 \not\equiv \bar{0} \pmod{p}$ and $0 \leq \nu \leq \alpha - 2$.

(iv) Now it is proved by induction that

$$\lambda(A, \bar{x}_0, p^{\nu + 1}) = (p^r - 1) \cdot p^\nu$$

for any starting vector $\bar{x}_0 \in \mathbf{Z}^r_p$ with $\bar{x}_0 \not\equiv \bar{0} \pmod{p}$ and $0 \leq \nu \leq \alpha - 1$. Obviously, (6) is equivalent to (12) for $\nu = 0$. Now assume that (12) is valid for some $\nu$ with $0 \leq \nu \leq \alpha - 2$. Then

$$\lambda(A, \bar{x}_0, p^{\nu + 2}) = \mu \cdot (p^r - 1) \cdot p^\nu$$
for some integer $\mu \geq 1$. Since
\[ \lambda(A, \bar{x}_0, p^{\nu+2}) \neq (p^r - 1) \cdot p^\nu \]
according to (11), it follows that $\mu > 1$. Remark 1 and (10) imply that $\lambda(A, \bar{x}_0, p^{\nu+2})$ divides $(p^r - 1) \cdot p^{\nu+1}$ and hence $\mu = p$, which proves the theorem. \( \square \)

Observe that there exist primitive polynomials of degree $r$ over the Galois field $GF(p)$ for every positive integer $r$ and every prime number $p$. Such a polynomial, and hence a matrix $B \in \mathbb{Z}_{p^r}^{n \times r}$ which satisfies the hypothesis of the theorem, can be determined without any effort if $p$ and $r$ are small integers (see, e.g., Knuth [3, p. 28]).

Since the characteristic polynomial of the matrix $B$ is primitive modulo $p$, it follows that $\det(B) \not\equiv 0 \pmod{p}$ and that $B \cdot \bar{x}_0 \not\equiv \bar{x}_0 \pmod{2}$ for $p = 2$, $r \geq 2$, and $\bar{x}_0 \not\equiv \bar{0} \pmod{2}$. Hence $\det(B + I) \equiv 1 \pmod{2}$ for $p = 2$ and $r \geq 2$. Therefore, the matrix $D \in \mathbb{Z}_{p^r}^{n \times r}$, with $D \equiv B \pmod{p^{2-1}}$ satisfies the hypothesis of the theorem if $p \geq 3$ or $r \geq 2$.

Acknowledgment. The authors are indebted to Professor H. Niederreiter for valuable hints given in a discussion on the topic of this paper. They also would like to thank the Deutsche Forschungsgemeinschaft for financial support.