Algebra and Discrete Mathematics
Number 4. **(2005).** pp. 81 – 92

RESEARCH ARTICLE

Recurrence sequences over residual rings

S. Sánchez, R. Criado, C. Vega

Communicated by V. A. Artamonov

Abstract. In this work we are carried out an algebraic study of the congruential lineal generator. The obtained results make possible several combinatorial approaches that improve significantly the period length and their behavior.

1. Introduction

In this paper we analyze algebraic structure of the linear congruential generator $x_{n+1} = (a \cdot x_n + b) \mod m$. Our goal is to analyze, for a given m, the influence of the coefficients a and b in the length of the period of generator. The period length is a decisive characteristic for the use of this generator type in many applications. First we analyze the linear congruential generator $x_{n+1} = (a \cdot x_n + b) \mod m$ when the parameter m is a prime number, showing that (in that case) we can choose the parameters a, b in such a form that the cyclic permutation is divided in disjoint cycles of the same order in such a manner that the length of the period obtained is close to the theoretical upper bound of $m!$. For more detailed exposition see [2].

Next we analyze linear congruential generator for $m = p \cdot q$, when p and q are prime numbers. We show that it is possible also in this case to divide the cyclic permutation in disjoint cycles of (possibly) different order. We determine the order of each permutation and we estimate the length of the period obtained in an certain example.

2000 Mathematics Subject Classification: *20B35, 11B50; 05A05.*
Key words and phrases: *cyclic permutation groups, linear congruences.*

2. Basic results and preliminaries

Let us recall that if F is a set with a finite number of elements, a generator of F is an algorithm that obtains a sequence of elements of F. A sequence $\{x_n\}_{n\geq 0}$ is *periodic* if there exists k such that $x_{n+k} = x_n$ for all $n \in \mathbb{N}$. For a periodic sequence, the set of numbers k satisfying the above condition constitutes a subset of $\mathbb{N}-\{0\}$. If λ is the smallest element of that subset, the subsequence $x_0, x_1, \ldots, x_{\lambda-1}$ is called a period of $\{x_n\}_{n\geq 0}$ and λ is called the *length* of that period. We say that $\{x_n\}_{n\geq 0}$ is *almost periodic* if there exists $m \in \mathbb{N}$ such that the sequence $\{x_n\}_{n\geq m}$ is periodic. In this case, the smallest number μ satisfying this condition is called the *occurrence* index to the period. We shall say that the period of the sequence $\{x_n\}_{n\geq 0}$ is the period of the sequence $\{x_n\}_{n\geq \mu}$. It is said that $\{F, f, x_0\}$ is of *maximum period* if the period length is equal to $|F|$.

In the sequel, we shall concentrate in single-step generators, that is, those that can be written as $x_{n+1} = f(x_n)$, where f is a mapping $f : F \to F$ and F is a finite set. We shall interpret a *generator* of F as an algorithm that produces the sequence $\{x_n\}_{n\geq 0}$ of elements of F and we shall denote it by $\{F, f, x_0\}$.

As the set F is finite, there are h, k, with $h < k$, such that $x_h = x_k$. Applying f, we have that $x_{h+r} = x_{k+r}$; therefore, $k - h$ is the period of the sequence $\{x_i\}_{i\geq h}$. If $x_i = x_j$ for $j > i$, as $\{x_l\}_{l\geq i}$ is periodic for $i \geq \mu$ then $j - i \equiv 0 \pmod{\lambda}$. We have the following simple result:

Proposition 1. *Let $\{F, f, x_0\}$ be a generator, where F is a finite set. The sequence $\{x_n\}_{n\geq 0}$ defined according to the rule $x_{n+1} = f(x_n)$ is almost periodic.*

In our case $F = \mathbb{Z}_m = \{0, 1, ..., m-1\}$ is a commutative ring with unit. We are interested in knowing under what conditions the affine mapping $x \longmapsto a \cdot x + b$ is of cycle length m. The mapping f is bijective if and only if a is an invertible element of $\mathbb{Z}_m$. The mapping f^k is the mapping $x \longmapsto a^k x_0 + (1 + a + a^2 + ... + a^{k-1}) \cdot b$. Using the notation $S_k(a) = (1+a+a^2+...+a^{k-1})$ we may rewrite f^k as $x \longmapsto a^k x_0 + b \cdot S_k(a)$. We now provide some properties related with $S_k(a)$.

For that purpose, we define the following polynomial with integer coefficients for $k \geq 1$,

$$S_k(x, y) = \frac{x^k - y^k}{x - y} = x^{k-1} + x^{k-2}y + ... + y^{k-1}.$$

Proposition 2. *[3]Let $k = p$ be a prime number and let $x, y \in \mathbb{Z}_k$. If $x \equiv y \pmod{k}$, then $S_k(x, y) \equiv 0 \pmod{k}$.*

Proof. Indeed, if $x \equiv y \pmod{k}$, then $S_k(x,y) = x^{k-1} + x^{k-1} + ... + x^{k-1} = kx^{k-1}$ and because $k = p$, according to Fermat's theorem $x^{k-1} \equiv 1 \pmod{k}$. Finally $S_k(x,y) = k \equiv 0 \pmod{k}$. If $y = 1$, then $x \equiv 1 \pmod{k}$ and $S_k(x) \equiv 0 \pmod{k}$. On the other hand $S_k(a) = (1+a+a^2+...+a^{k-1}) = \frac{1}{a-1}(a-1)(1+a+a^2+...+a^{k-1}) = \frac{1}{a-1}(a^k-1)$. Therefore $S_k(a) = (a-1)^{-1}(a^k-1)$ and $S_k(x) \equiv 0 \pmod{k}$, so $a^k \equiv 1 \pmod{k}$.

It is important to remark that for f to be of length cycle m, fixed points should not exist. For the sake of simplicity, let $b = 1$. Then the equation $x = a \cdot x + a$ has a unique solution if $a \neq 1 \pmod{m}$. Hence, if f is fixed-point free, then $a \equiv 1 \pmod{m}$. But, in this case, $S_k(x) \equiv 0 \pmod{k}$ and $f^m = e$, where e is the identity element.

Following this reasoning, it is not difficult to prove:

Proposition 3. *[3]If m is a prime number,$a \equiv 1 \pmod{m}$ and b is not congruent to $0 \pmod{m}$, the mapping $f_{a,b} : \mathbb{Z}_m \to \mathbb{Z}_m$ defined by $f_{a,b}(x) = \overline{a \cdot x + b}$, where $\overline{a \cdot x + b}$ is the equivalence class modulo m corresponding to the number $a \cdot x + b$, is a cyclic permutation of order m in $\mathbb{Z}_m$ (and hence a maximum length generator).*

The single-step generator that we have seen, cannot generate sequences with period longer than $|F|$. Our objective is to design a generator whose period length is close to the theoretical boundary $m!$, the order of a symmetric group with m elements. It is well known that if the order of the cyclic group $\langle f \rangle$ generated by f satisfies $|\langle f \rangle| = s$, given $x \in \mathbb{Z}_m$, we have that either x is a fixed point of certain element of $\langle f \rangle$ (in this case, we denote x by x_F), or the set $H_x^s = \{x, f(x), ..., f^{s-1}(x)\}$ contains exactly s elements. Moreover, it is also possible to find a sequence $x_1, x_2, ..., x_l \in \mathbb{Z}_m$ such that

$$\mathbb{Z}_m = H_0 \cup H_{x_1}^s \cup ... \cup H_{x_l}^s$$

where $H_0 = \{x_F\}$, $\left|H_{x_1}^s\right| = ... = \left|H_{x_l}^s\right| = s$, and $l \cdot s = m - 1$.

3. Generation of pseudo-random numbers and linear congruences

Generation based on the expression

$$x_{n+1} = (a \cdot x_n + b) \mod m, \tag{3.1}$$

depends on four parameters a, b, m and x_0. The parameters in expression (1) can be divided in two categories:

1. Parameters a, b, m, providing a maximum length generator.
2. Parameters a, b, m, which do not provide a maximum length generator.

The first case is thoroughly considered in [1]. We shall carry out here the analysis of the second option, concentrating first on the case where m is a prime number and second on the case where $m = p \cdot q$. To do so, we shall use the following well-known results that summarize part of what was mentioned in the previous section:

Theorem 1. *If $a \equiv 1 \pmod{m}$, then for any sequence produced according to (1) there exists a fixed point x_F such that*

$$x_F = (a \cdot x_F + b) \pmod{m}$$

Remark. The multiplicative group $\mathbb{Z}_m^* = \{1, 2, ..., m-1\}$ of the field $\mathbb{Z}_m$ is cyclic with generating element z. The order of element z is $m-1$. Therefore $a = z^l \neq 1$ has the order $s = \frac{m-1}{l}$, $a^s = 1$ and $1 + a + a^2 + ... + a^{k-1} = 0$ when $a \neq 1$. So $a^s x + \left(1 + a + a^2 + ... + a^{k-1}\right) b = x$, $s > 1, \forall x$. Definitely for $a \neq 1$ and for $\forall b$, $\left(1 + a + a^2 + ... + a^{k-1}\right) b = 0$, but $1 + a + a^2 + ... + a^{k-1} = 0$ so it is verified for $\forall b$.

Thus if $m \geq 5$ is a prime number, then $m-1$ is composed, so the period formed by the previous $m-1$ numbers is divided into l subgroups of s elements each, so that

$$l \cdot s = m - 1 = \phi(m)$$

where $\phi(m)$ is the Euler ϕ-function, which counts the number of integers in $\{1, ..., n\}$ that are relatively prime to n. The number of possible values of s is

$$\tau(\phi(m)) - 1$$

where $\tau(p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_n + 1)$ for $(m-1) = p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$. The number of subsets l *is*

$$l = \frac{m-1}{s}$$

Now, for a given value of s, the valid values of parameter a are the solutions of the following equation:

$$a^s \equiv 1 \pmod{m} \tag{3.2}$$

The number of solutions of this equation is $\phi(s)$, so that, if s=$\phi(m)$, we have the Euler theorem.

Remark. As we have seen $\mathbb{Z}_m^*$ is a cyclic permutation divided into l disjoint cosets consisting of s elements, $z \in \mathbb{Z}_m^*$ and we can express this in the form

$$\mathbb{Z}_m^* = \langle z \rangle x_0 \cup \langle z \rangle x_1 \cup ... \cup \langle z \rangle x_{l-1} \tag{3.3}$$

where x_i is a generating element of each coset

$$\begin{gathered} x_0 = \min \langle z \rangle \\ x_1 = \min \mathbb{Z}_m^* \setminus \langle z \rangle \\ x_2 = \min \mathbb{Z}_m^* \setminus \{\langle z \rangle x_0 \cup \langle z \rangle x_1\} \\ ..... \end{gathered}$$

4. Combinatorial approach

In a computer applications the choice of a modulo m is restricted by computer word size. For a generator of maximum period, the only way to increase the period length is to increase the value of the parameter m, which is bounded, or to use a combination of generators.

In our case, the following procedures can be followed in order to achieve a large period length. As we have l subsets we can form one of the $l!$ permutation of the numbers of the set $\{0, 1, ..., l-1\}$ as $\{i_0, i_1, ..., i_{l-1}\}$. So we have in this way a permutation of the subsets $\{H_{i_0}, H_{i_1}, ..., H_{i_{l-1}}\}$ or a permutation of the seeds $\{x0_{i_0}, x0_{i_1}, ..., x0_{i_{l-1}}\}$. Next we can follow the following basic procedure for the case $m = p$:

- First Step. Start with one permutation obtaining a list of subsets

  $$\{H_{i_0}, H_{i_1}, ..., H_{i_{l-1}}\}$$

  or a permutation of the seeds $\{x0_{i_0}, x0_{i_1}, ..., x0_{i_{l-1}}\}$.

- Second Step. Of each subset H_{i_j}, in the list of permutation

  $$\{H_{i_0}, H_{i_1}, ..., H_{i_{l-1}}\},$$

  choose the first element x_1, or the last element x_{s-1}, or one at random x_j until all subsets in the list of permutation $\{H_{i_0}, H_{i_1}, ..., H_{i_{l-1}}\}$ are examining.

- Third Step.The obtained element is sent to the output.

- Fourth step. The next permutation (list of subsets) is generated [1].

- The steps 3,4 are continued until all of the possible permutation are examined.

- Fifth step. Repeat the Second Step choosing the second element x_2, or the element x_{s-2}, or one at random $x_k \neq x_j$ until all subsets in the list of permutation are examined.

- Sixth step. 3,4 are continued until all of the possible permutation are examined.

- ..... and so forth .

The complexity of the presented algorithm doesn't turn out to be very superior to the complexity of the algorithm LCG, since differs only in necessity of generating the next permutation in the step 4 and needs to evaluate the formula (4.1), slightly more complex then (3.1).

$$x_j = \left(a^j \cdot x0_{i_j} + \frac{a^j - 1}{a - 1} \cdot b\right) \mod m \tag{4.1}$$

When j is chosen at random the procedure is more complex then the algorithm LCG. It is necessary to generate an integer number uniformly distributed between 1 and $s-1$. This can be obtaining using the relationship (3.1). In the successive steps it is necessary to try that the distribution law is verified, in other words it is necessary to generate an integer number uniformly distributed between 1 and $s-2$, $s-3$, ... and so on.

We need, also, to evaluate $a^j \mod m$.We can use the "power algorithm" or "binary method". This algorithm computes $a^j \mod m$, using $O\left((\lg j)(\lg m)^2\right)$ bit operations.

The statistical properties of the sequences that is generated by the algorithm as well as other statistical aspects are shown in [2].

Therefore, it is possible to produce a series whose generation depends on:

1. The order in which we go through the subsets. The number of possible variations is $l!$, hence the period length will be $l! \cdot m$.

2. The choice of seed x_0 in each subset. The number of combinations for the choice of initial value is s^l, hence the period length will be $l! \cdot m \cdot s^l$.

3. The choice of subset can be random, as well as the choice of the number of elements in the chosen subset. This process is carried out so that the uniform law of distribution of x in the interval between 0 and $m-1$ holds; in other words, each value x in the interval between 0 and $m-1$ should appear only once. In consequence, the period length will be $l! \cdot m \cdot (s!)^l$.

In this way, for the chosen parameters a, b, m we can generate not only one serie2 (as in the generator of complete period case) but many different series. Therefore, it is possible to come closer to the theoretically possible upper bound of $m!$ elements.

Following the generation procedures above and if we take initially $m = 655339$, its closest prime number is 655337, so taking $m = 655337$, we have that $m - 1 = 655336 = (2^3) \cdot (11)^2 \cdot 677$. If, for instance, $l = 2 \cdot 11 = 22$, we determine $s = \frac{655337-1}{22} = 29778$. The period length for each generation from 1 to 3 will be:

1. $22! \cdot 6.55336 \cdot 10^5 \approx 10^{21} \cdot 6.55336 \cdot 10^5 \approx 10^{26}$;
2. $22! \cdot 6.55336 \cdot 10^5 \cdot (29778)^{22} \approx 10^{21} \cdot 6.55336 \cdot 10^5 \cdot 10^{98} \approx 10^{124}$;
3. $48! \cdot 6.55336 \cdot 10^5 \cdot (29778!)^{22} \approx 10^{21} \cdot 6.55336 \cdot 10^5 \cdot 10^{2.647.414} \approx 10^{2.646.441}$.

To see the degree of approximation, we can apply Stirling's formula to approximate the value 655337!,

$$\ln(m!) \approx \left(m + \frac{1}{2}\right) \cdot \ln(m) - m + \ln(\sqrt{2\pi})$$

from where

$$6.55336! \approx 10^{3.527.102}$$

5. Linear congruences and pseudorandom-numbers generation for a composite module

We have analyzed a linear congruential generator $x_{n+1} = (a \cdot x_n + b) \mod m$ when the parameter m is a prime number, showing that (in that case) we can choose the parameters a, b in such a form that the cyclic permutation is divided in disjoint cycles of the same order in such a manner that the length of the period obtained is close to the theoretical upper bound of $m!$.

In this chapter we analyze the linear congruential generator for $m = m_1 \cdot m_2$, when m_1 and m_2 are prime numbers. We show that it is possible also in this case to divide the cyclic permutation in disjoint cycles of (possibly) different order. We determine the order of each permutation and we estimate the length of the period obtained in an specific example.

In order to do that, we recall that a pseudo-random numbers generator based in a recursive relation

$$x_{n+1} = (a \cdot x_n + b) \mod m \tag{5.1}$$

makes an ordered arrangement of the different elements of an specific set. If we consider the following affine function:

$$\begin{array}{rccc} f_{a,b}: & \mathbb{Z}_m & \to & \mathbb{Z}_m \\ & x & \mapsto & a \cdot x + b \end{array} \tag{5.2}$$

we have that when the parameter a has an inverse (modulo m) this function is a bijection. Moreover, the set of invertible functions of this form constitutes a twice transitive group with respect to the operation:

$$* : f_{a,b} * f_{c,d} = f_{ac,ad+b} \tag{5.3}$$

At this moment it is important to recall the following theorem:

Theorem. *(Chinese Remainder Theorem) If m_1 and m_2 are positive integers such that $gcd(m_1, m_2) = 1$ then the groups $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ and $\mathbb{Z}_{m_1 m_2}$ are isomorphic.*

In our context one could say: If m_1 and m_2 are two prime numbers, then the function

$$\begin{array}{ccc} \mathbb{Z}_{m_1 m_2} & \longrightarrow & \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \\ & & \\ \overline{x_{m_1 m_2}} & \longrightarrow & (\overline{x_{m_1}}, \overline{x_{m_2}}) \end{array} \tag{5.4}$$

is an isomorphism of groups (in fact an isomorphism of rings), so we have that $\mathbb{Z}_{m_1 m_2} \backsimeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$.

6. Linear congruences over $\mathbb{Z}_{m_1 m_2}$

We denote by $\{F, f, x_0\}$ a generic single-step generator, that is, a generator that can be written as $x_{n+1} = f(x_n)$, where f is a mapping $f : F \to F$ and F is a finite set, as a consequence of Chinese Remainder theorem we can combine two generators $\{F, f, x_0\}$ and $\{G, g, y_0\}$ obtaining the cartesian product generator $\{F \times G, f \times g, (x_0, y_0)\}$.

Lemma. [3] *If m is the product of two distinct prime numbers $m = m_1 \cdot m_2$, the generator $G : z_{i+1} = (a \cdot z_i + b) \mod m$ is the cartesian product of $G_1 : x_{i+1} = (a \cdot x_i + b) \mod m_1$ and $G_2 : y_{i+1} = (a \cdot y_i + b) \mod m_2$. Moreover, the length of G is equal to the least common multiple of the lengths of G_1 and G_2.*

Now, if we consider the functions f_1, f_2 and f defined by $f_1(x) = a \cdot x + b \mod m_1$,$f_2(y) = a \cdot y + b \mod m_2$ and $f(z) = a \cdot z + b \mod m$, the following diagram show us how these functions are relating:

$$\begin{array}{ccc} & f & \\ \mathbb{Z}_m & \to & \mathbb{Z}_m \\ \downarrow & & \downarrow \\ & f_1 \times f_2 & \\ \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} & \to & \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \end{array} \tag{6.1}$$

In this diagram the upright arrows represent the Chinese isomorphism. Let us consider the generator $G_1 : x_{i+1} = (a \cdot x_i + b) \mod m_1$. Following the underlying ideas of previous lemma, the decomposition into independent cycles of G_1 is

$$m_1 - 1 = l_1 \cdot s_1$$
$$m_1 - 1 = \varphi(m_1)$$
$$l_1 = \tfrac{m_1-1}{s_1} = \tfrac{\varphi(m_1)}{s_1}$$

and the same for generator G_2:

$$m_2 - 1 = l_2 \cdot s_2$$
$$m_2 - 1 = \varphi(m_2)$$
$$l_2 = \tfrac{m_2-1}{s_2} = \tfrac{\varphi(\ m_2)}{s_2}$$

On the other hand, we have that

$$m_1 \cdot m_2 - 1 = \varphi(m_1) + \varphi(m_2) + \varphi(m_1 \cdot m_2)$$

where $\varphi(m)$ is the Euler ϕ-function. Therefore,

$$m_1 \cdot m_2 - 1 = \varphi(m_1) + \varphi(m_2) + \varphi(m_1 \cdot m_2) = s_1 \cdot l_1 + s_2 \cdot l_2 + s_3 \cdot l_3.$$
$$G : z_{i+1} = (a \cdot z_i + b) \mod (m_1 \cdot m_2),\ \varphi(m_1 \cdot m_2) = l_3 \cdot s_3.$$

hence

$$(m_1 \cdot m_2) = s_3 \cdot l_3,\ \varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2) = s_3 \cdot l_3$$

and

$$(l_1 \cdot s_1) \cdot (l_2 \cdot s_2) = (l_3 \cdot s_3)$$

so, we can obtain

$$G : z_{i+1} = (a \cdot z_i + b) \mod (m_1 \cdot m_2\ )$$
$$\varphi(m_1 \cdot m_2) = l_3 \cdot s_3$$

Thus $ord(s_3) = (a_1, a_2)$, $a_1, a_2 \neq 1$, when $\langle z_1 \rangle = \mathbb{Z}^*_{m_1}$, $\langle z_2 \rangle = \mathbb{Z}^*_{m_2}$, $(a_1, a_2) = \left(z_1^{l_1}, z_2^{l_2}\right)$, and $(m_1 - 1) \cdot (m_1 - 1) = l_3 \cdot s_3$.

Therefor the condicion for $s_3 = s_1 \cdot s_2$ is that $gcd(s_1, s_2) = 1$.

Consequently, we have obtained the following decomposition of the cyclic permutation associated to generator G:

l_1 – groups of s_1 elements
l_2 – groups of s_2 elements
$$l_3 = l_1 \cdot l_2$$
$$s_3 = s_1 \cdot s_2$$
l_3 – groups of s_3 elements

For example, if we want a generator with m of the order $6 \cdot 10^5$, we can choose $m = 644773$, so

$$m = m_1 \cdot m_2 = 797 \cdot 809, m_1 - 1 = 796 = (2)^2 \cdot 199$$
$$m_2 - 1 = 808 = (2)^3 \cdot 101$$

If, for example, $l_1 = 2^2$, $l_2 = 2^2$, we have that $s = \frac{797-1}{2^2} = 199$ and $s_2 = \frac{809-1}{2^2} = 202$. Then, for the composite module generator $m = m_1 \cdot m_2 = 797 \cdot 809$, we have the following decomposition:

$$l_3 = l_1 \cdot l_2 = 2^2 \cdot 2^2 = 2^4 = 16$$

groups of $s_3 = s_1 \cdot s_2 = 199 \cdot 202 = 40198$ elements, $l_3 = l_1 = 4$ groups of $s_4 = s_1 = 199$ elements, and $l_4 = l_2 = 4$ groups of $s_5 = s_2 = 202$ elements. The lenghts of each period are the following:

1. $[(4!) \cdot 199] \cdot [(4!) \cdot 202] \cdot [(16!) \cdot 40198] \approx 10^{27}$
2. $\left[(4!) \cdot 4 \cdot 199^4\right] \cdot \left[(4!) \cdot 4 \cdot 202^4\right] \cdot \left[(16!) \cdot 16 \cdot 40198^{16}\right] \approx 10^{110}$
3. $\left[(4!) \cdot 4 \cdot (199!)^4\right] \cdot \left[(4!) \cdot 4 \cdot (202!)^4\right] \cdot \left[(16!) \cdot 16 \cdot (40198!)^{16}\right] \approx 10^{2.685.022}$

To see the degree of approximation, we can apply Stirling's formula to approximate the value $644773!$, $\ln(m!) \approx \left(m + \frac{1}{2}\right) \cdot \ln(m!) - m + \ln\left(\sqrt{2 \cdot \pi}\right)$, from where $644773! \approx 10^{3.465.730}$.

We can resume the results of this example in the following table:

$G1$		$G2$		$G3$	
a=797		a=797		a=797	
b=73		b=73		b=73	
m=797		m=809		m=644773	
$l_1 = 4$		$l_2 = 4$		$l_3 = 16$	
$x_F = 199$		$x_F = 455$		$x_F = 413045$	
$x_0\,[i]$	s_1	$x_0\,[i]$	s_2	$x_0\,[i]$	$s_3\,[i]$
4	199	2	202	2	40198
6	199	4	202	3	40198
11	199	5	202	4	40198
40	199	7	202	5	40198
				6	40198
				7	40198
				8	40198
				11	40198
				12	40198
				15	40198
				18	40198
				26	40198
				32	40198
				37	40198
				49	40198
				174	202
				385	199
				971	202
				1194	199
				1768	202
				3621	199
				5239	199
				7347	202

References

[1] D. Knuth, *The Art of Computing Programming*, Vol.2, Addison-Wesley, 1997.

[2] S. Sanchez, R. Criado and C. Vega, *A generator of pseudo-random numbers sequences with maximum period*, Proc. ICMMSE (2003), World Scientific Publishing Co. Pte. Ltd., 561-566 (2003).

[3] P.Naudin, C.Quitte, *Algoritmique Algebrique*, Masson, Paris, Milan, Barcelona, Bonn, 1992

Contact information

S. Sánchez
Dpto. de Matemáticas y Fisica Aplicadas y CC. de la Naturaleza, Universidad Rey Juan Carlos, E-28933 Móstoles, Madrid, Spain
E-Mail: sergio.sanchez@urjc.es

R. Criado
Dpto. de Matemáticas y Fisica Aplicadas y CC. de la Naturaleza, Universidad Rey Juan Carlos, E-28933 Móstoles, Madrid, Spain
E-Mail: regino.criado@urjc.es

C. Vega
Dpto.de Matemática Aplicada a las Tecnologias de la Información, Universidad Politécnica de Madrid, E-28040, Madrid, Spain
E-Mail: cvega@mat.upm.es

Received by the editors: 17.05.2005
and final form in 17.10.2005.