On the Period Length of Pseudorandom Number Sequences

Amy Glen

Supervisor: Dr. Alison Wolff

November 1st, 2002

Thesis submitted for Honours in Pure Mathematics

SCHOOL OF PURE MATHEMATICS

THE UNIVERSITY OF ADELAIDE AUSTRALIA

Contents

List of Symbols

In the list below, letters that are not further qualified have the following significance:

i, j, k	non-negative integers
a, b	integers
m, n	positive integers
x	indeterminate
y	real number

Formal Symbolism	**Meaning**
$\{x_i\}$, $\{x_i\}_{i\geq 0}$	the infinite sequence $x_0, x_1, \ldots$
$\mathbb{Z}$	the set of integers
$\mathbb{Z}^+$	the set of positive integers
$\mathbb{Z}_m$	the set of reduced residues modulo m (i.e. $\{0, 1, 2, \ldots, m-1\}$)
$\mathbb{R}$	the set of real numbers
$\lfloor y \rfloor$	the greatest integer $\leq y$
$a \equiv b \pmod{m}$	a congruent to b modulo m
$a \not\equiv b \pmod{m}$	a incongruent to b modulo m
$\square$	end of proof, end of example
$gcd(a, b)$, (a, b)	greatest common divisor of a and b
$lcm(a, b)$, $[a, b]$	least common multiple of a and b
x^k	x to the k^{th} power
$\binom{a}{b}$	binomial coefficient
$\phi(n)$	Euler's ϕ-function of n: $\sum_{\substack{0\leq k<n \\ (k,n)=1}} 1$
$ord_m a$	the order of a modulo m
$\lambda(n)$	minimal universal exponent
M_n	Mersenne number $(= 2^n - 1)$
$< a >$	the cyclic group generated by a
$\sum$	summation
$\prod$	product
$\mathbb{F}_q$, $GF(q)$	the finite field with $q = p^n$ elements (p a prime, $n \in \mathbb{Z}^+$)
$\mathbb{F}_q^*$	the multiplicative group of non-zero elements of $\mathbb{F}_q$
$\mathbb{F}_q[x]$	the polynomial ring over the field $\mathbb{F}_q$
$\mathbb{Z}_2[x]$	the polynomial ring over $\mathbb{Z}_2$

Formal Symbolism	**Meaning**
$deg(f)$	degree of the polynomial f
$ord(f)$	order of the polynomial f
$\cong$	isomorphic
$\mathbf{I}$	identity matrix
$\lvert y\rvert$	absolute value of y; $\lvert y\rvert = \begin{cases} y;\ y \geq 0 \\ -y;\ y < 0 \end{cases}$
$\ln y$	natural logarithm of y: $\log_e y$
$\mu(n)$	Möbius function
$det(\mathbf{A})$, $\lvert\mathbf{A}\rvert$	determinant of square matrix $\mathbf{A}$
$\lvert S\rvert$	the number of elements in the finite set S
$max(a, b)$	maximum of a and b
$min(a, b)$	minimum of a and b
$GL(k, \mathbb{F}_q)$, $GL(k, q)$	general linear group of non-singular $k \times k$ matrices over $\mathbb{F}_q$
$Tr(\alpha)$	trace of $\alpha \in \mathbb{F}_{q^k}$
$a \mid b$	a divides b
$\left(\frac{a}{p}\right)$	Legendre symbol (p a prime, $(a, p) = 1$)
$(.a_1a_2a_3\ldots)_b$	base b expansion
$(.a_1\ldots a_{n-1}\overline{a_n\ldots a_{n+k-1}})_b$	periodic base b expansion

Abstract

'Random' numbers are useful in a wide variety of areas. For instance, they are required for computer simulations used to study phenomena in fields ranging from nuclear physics to operations research. Many users of simulation are content to remain ignorant of how such 'random' numbers are produced, merely calling standard functions to produce them. In this thesis, we will consider some of the most common recursive algorithms used to produce sequences of 'random' numbers. Such procedures are known as *pseudorandom number generators* since they produce deterministic sequences of numbers that appear to be random. The emphasis will be on the the period length of the sequences of numbers produced by such generators. Indeed, a large period length is essential for any sequence that is to be used as a source of random numbers.

Acknowledgements

I would like to express my gratitude and appreciation to Dr. Alison Wolff, whose valuable comments and helpful suggestions were of fundamental importance to the development of this thesis. I would also like to thank her for putting up with my little eccentricities, which became prominent throughout the course of the year.

A big thank-you also goes to my family for their unwavering support. This thesis was a major priority of mine and, as a consequence, they may have felt pushed away and unimportant at times. But I thank them for their understanding.

I would also like to thank my fellow Honours students - their friendship helped make it an enjoyable and fulfilling year.

Chapter 1

Introduction

1.1 Pseudorandom Numbers

Random numbers are useful in a wide variety of applications. For instance, they are required for computer simulations used to study phenomena in fields ranging from nuclear physics to operations research. With the use of random numbers, the behaviour of a system may be investigated via the construction of random samples when it would otherwise be impractical to test all possible cases. There is also extensive use of random numbers in such areas as numerical analysis for Monte Carlo and Quasi-Monte Carlo integration and, more generally, simulations methods; number theory for probabilistic primality tests; and computational statistics. In addition, random numbers are of basic importance in areas of direct practical interest such as gambling and computer games; and cryptography for generation of cryptokeys and the execution of cryptographic protocols, just to name a few.

By the phrase *random numbers*, we mean terms of a sequence of numbers in which each term is obtained by chance, independent of the other terms of the sequence, with a specified probability of lying in any given range of values. The existence of random numbers is provable from Kolmogorov's axioms for probability (see [Nev65]). However, this result does not provide a realization of a sequence of random numbers. We must therefore find procedures that generate a sequence of numbers in such a way that each number produced appears to be randomly distributed among the set of all possible numbers and statistically independent of the previously generated numbers.

Prior to 1940, users of simulation produced random numbers by physical processes such as rolling dice, spinning roulette wheels, dealing cards, or extracting random digits from tabulated data. The 1940s saw the development of machines to produce random numbers

and, in the 1950s, computers were used to generate random numbers using random noise. Nevertheless, random numbers produced by such mechanical processes were quite frequently skewed due to malfunctions in computer hardware, and it was of major concern that these random numbers could not be reproduced to check results of a computer program. Simpler methods to obtain haphazard sequences were then investigated, and various non-linear recursive schemes were considered, the earliest of which was John Von Neumann's *middle-square method*, proposed in 1946. This method generates four-digit random numbers from an initial arbitrary four-digit number. For example, we begin with a four-digit number, say 6591, then we square it to obtain 43441281 from which we extract the middle four digits 4412 as the second random number. Applying this procedure iteratively, by repeatedly squaring and taking the middle four digits as the next random number, yields a sequence of 'random' numbers. In this case, we obtain the deterministic sequence

$$6591, 4412, 4657, 6876, 2793, 8008, 1280, 6384, \ldots$$

Obviously, such a sequence of numbers cannot be considered truly random since the sequence is completely determined by the initially chosen four-digit number; whence, the terminology of *pseudorandom* (*pseudo*: false, apparent, supposed but not real – *Concise Oxford Dictionary*). On the contrary, this sequence of numbers does *appear* to be random, so it could possibly serve as a useful source of 'random' numbers for some computer simulations.

We thus formally define a *sequence of pseudorandom numbers* to be a deterministic sequence of integers which have been chosen in some methodical manner, but appear to be random; having the same relevant statistical properties as a sequence of truly random numbers. For our purposes, such a definition is sufficient, but to be more rigorous, one must specify which properties are relevant and statistical, and also more precisely define randomness. Informally, we mean that any statistical test, which aims to detect relevant departures from randomness, would not reject the null hypothesis when applied to a finite part of the given sequence (see Ripley [Rip87]). It is most convenient to view this definition in terms of *predictability* since we intuitively call something random if we cannot predict it. Knuth [Knu81] deals with the subject of randomness in substantial detail – it is quite a philosophical matter.

Unfortunately, the middle-square method has some unavoidable weaknesses, the most undesirable of which is the fact that, for many choices of the initial four-digit integer, it generates a sequence which ultimately consists of the same *small* set of numbers repeated indefinitely. As an example, the sequence obtained by applying the middle-

square method to 6300 is

$$6900, 6100, 2100, 4100, 8100, 6100, 2100, 4100, \ldots$$

Excluding the first number 6900, the sequence forever repeats the four integers 6100, 2100, 4100, 8100 so that the sequence is *ultimately periodic* with *pre-period length* 1 and *least period length* 4. (We will formally define the afore mentioned terms, relating to periodicity, in Section 1.2 of this chapter). In fact, even though the sequence of the previous example may at first strike one as being unpredictable, it also settles down to a repetition of these same four integers. We require sequences that are difficult to predict unless the process generating them is known, and so it was for this reason that the middle-square method was quickly rejected as a source of pseudorandom numbers.

In practice, many acceptable deterministic procedures exist for generating pseudorandom number sequences and, in particular, those which shall be discussed in this thesis have the property that, after possibly irregular behaviour in the beginning, they are eventually of a periodic nature (or ultimately periodic in the sense of Definition 1.2.1 to follow). For example, we saw that the middle-square method ultimately generates a sequence of length 4 which repeats itself, with this length being called the *period length* of the sequence. Such a small period length is obviously inadequate for most purposes.

In this paper, we shall concern ourselves with the question of period length; indeed, a long period is essential for any sequence that is to be used as a source of random numbers. One would certainly hope that the period of the sequence contains more terms than will ever be used in a single application. Our discussion of each type of pseudorandom number generator will focus on the period length of the sequences it produces; the main goal being to establish the conditions under which maximum possible period length is attained. It should be stressed, however, that a large period length is only one desirable property for the randomness of a sequence. The quality of pseudorandom numbers is of fundamental importance in any application requiring their use. It is therefore crucial to choose an appropriate pseudorandom number generator exhibiting not only good statistical and randomness properties, but also one which will generate sequences of large period lengths. Certainly, the period length influences the degree of randomness achievable in a sequence.

Much to the dismay of the author, the nature of such a paper restricts our attention to only a relatively small number of pseudorandom number generators as compared to the vast array of generators currently available. With much deliberation, it was thought most appropriate to simply consider the most common methods upon which other generators are based.

Each of the pseudorandom number generators examined in this thesis differ in certain

ways, but each share two common features; namely, they rely on *recurrence* to produce a sequence of pseudorandom numbers, and each exploit the concept of *congruence*. For integers a, b and $m > 0$, we say that *a is congruent to b modulo m* if m divides $a - b$, and write $a \equiv b \pmod{m}$, where m is called the *modulus*. For example, $7 \equiv 1 \pmod{6}$, $11 \equiv 2 \pmod{3}$, $-5 \equiv 7 \pmod{6}$, and $8 \equiv 338 \pmod{11}$.

Almost all pseudorandom number generators take one of the following three forms:

(1) **k^{th}-order Linear Recurrence Generator**

This type of generator produces a sequence $\{x_i\}_{i \geq 0}$ of pseudorandom numbers defined recursively by

$$x_{i+k} \equiv \sum_{j=1}^{k} a_{k-j} x_{i+k-j} + c \pmod{m}, \qquad 0 \leq x_i < m \tag{1.1}$$

where $a_0, \ldots, a_{k-1}, c$ are non-negative integers taking values in $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, with $a_0 \neq 0$ and m a positive integer. Computationally, x_{i+k} can be evaluated as

$$x_{i+k} = \sum_{j=1}^{k} a_{k-j} x_{i+k-j} + c - r_i m \qquad \text{where}$$

$$r_i = \lfloor m^{-1} \sum_{j=1}^{k} a_{k-j} x_{i+k-j} + c \rfloor.$$

When $k = 1$, such a generator is called a *linear congruential generator*, which will be described in further detail in Chapter 2. A large part of Chapter 2 will also be devoted to the case $k = 1$ and $c = 0$, which is called the *pure multiplicative congruential method*. In Chapter 3, the case of $k > 1$ and $c = 0$ requires finite field theory and matrices to establish certain results concerning period length.

(2) **Linear Recurrence Generator Modulo 2**

A sequence $\{b_i\}$ of 0s and 1s is generated by the recurrence relation

$$b_i \equiv \sum_{j=1}^{k} a_j b_{i-j} \pmod{2} \tag{1.2}$$

where $a_1, \ldots, a_{k-1} \in \mathbb{Z}_2 = \{0, 1\}$, $a_k = 1$, and each b_j takes a value in $\mathbb{Z}_2$.

This formulation is the basis for *shift register generators*, which will be discussed in Chapter 4.

(3) **Non-Linear Congruential Generator**

This type of generator takes the form

$$x_{i+1} \equiv f(x_i) \pmod{m}; \qquad 0 \leq x_{i+1} < m \tag{1.3}$$

where f is a non-linear integer-valued function of x_i. An example of such a function f is

$$f(x) = ax^{-1} + b, \qquad x \in \mathbb{Z}_m, x \neq 0,$$

where a and b are positive integers, $m = p \geq 5$ is a prime and x^{-1} is the unique positive integer less than p such that $xx^{-1} \equiv 1 \pmod{p}$, called the *multiplicative inverse of x modulo p*. Such generators are analyzed, with respect to the period length of their sequence, in Chapter 5 where we shall also discuss several other non-linear methods of special interest.

Chapter 6 will focus on the period length of sequences produced by a special type of generator, which is not of one of the above three forms. We will not yet reveal the reasons for considering this generator as this will become evident in Chapter 2.

We note that this project is more or less a survey of some common pseudorandom number generators, with regard to the period length of the sequences they produce. Consequently, we will not be reaching a particular conclusion, but rather it is hoped the reader will notice the interesting use of number theory and finite field theory for establishing periodicity properties of pseudorandom number sequences.

1.2 Preliminaries

Since we shall be dealing with the period length of sequences, it seems only proper that some formal terminology be introduced, along with an important result regarding the period length of ultimately periodic sequences.

Definition 1.2.1. *Let X be an arbitrary non-empty set, and let the sequence $\{x_i\}_{i\geq 0} = \{x_i\}$ consist of elements of X. If there exists integers $d > 0$ and $i_0 \geq 0$ such that $x_{i+d} = x_i$ for all $i \geq i_0$ then the sequence $\{x_i\}$ is said to be **ultimately periodic** and d is called a **period length** of the sequence. The smallest period length of an ultimately periodic sequence is called the **least period length** of the sequence. Moreover, an ultimately periodic sequence with least period length d is called **purely periodic** if $x_{i+d} = x_i$ for all $i \geq 0$.*

Note. If $\{x_i\}$ is ultimately periodic with least period length d, then the least non-negative integer i_0 such that $x_{i+d} = x_i$ for all $i \geq i_0$ is called the **pre-period length**. Of course, it then follows that the pre-period length of a purely periodic sequence is 0.

Lemma 1.2.1. *Every period length of an ultimately periodic sequence is divisible by its least period length.*

Proof. Let $\{x_i\}$ be an ultimately periodic sequence with an arbitrary period length d and least period length d'. Then $x_{i+d} = x_i$ for all $i \geq i_0$ and $x_{i+d'} = x_i$ for all $i \geq i'_0$, where i_0 and i'_0 are appropriate non-negative integers.

Suppose d' does not divide d. By the *Division Algorithm* (Theorem A.6), there exist positive integers q and r such that $d = qd' + r$, where $0 < r < d'$. It follows that for all $i \geq max(i_0, i'_0)$ we have

$$x_i = x_{i+d} = x_{i+qd'+r} = x_{i+qd'+d'-d'+r} = x_{i+(q-1)d'+r} = \cdots = x_{i+r},$$

so that r is a period length of the sequence $\{x_i\}$. But $0 < r < d'$; a contradiction to the definition of least period length d'. Hence, $r = 0$ and d' must divide the period length d. □

Throughout this project, the above simple result will be implicitly assumed without reference and, for convenience, we shall henceforth refer to the *least period length* as simply the *period length* of a sequence, unless otherwise stated.

In what follows, it is assumed the reader is familiar with both number theory and finite field theory. Nevertheless, for accessibility, relevant results and definitions have been provided in the appendices. Knowledge of basic matrix algebra and group theory is also expected.

"A random sequence is a vague notation ... in which each term is unpredictable to the uninitiated and whose digits pass a certain number of tests traditional with statisticians ... " –1951, D.H. Lehmer, a pioneer in computing, and especially computational number theory.

Chapter 2

First-Order Linear Recurrence Generators

2.1 Linear Congruential Method

Special cases of the following scheme, introduced by D.H. Lehmer in 1949 [Leh51], are the most commonly used pseudorandom number generators, predominantly because of the ease with which they can be implemented on a computer and the relatively fast speed at which they generate pseudorandom numbers.

The **linear congruential method** produces a sequence $\{x_i\}_{i\geq 0}$ defined recursively by

$$\boxed{x_{i+1} \equiv ax_i + c \pmod{m}, \qquad 0 \leq x_{i+1} < m} \tag{2.1}$$

where integers m (the *modulus*), a (the *multiplier*), c (the *increment*) and x_0 (the *seed*) are chosen such that $0 \leq a, c, x_0 < m$. This 'reduction modulo m' can be regarded, in a similar respect, to determining where a ball will land in a spinning roulette wheel.

As already mentioned, the special case of $c = 0$ is called the *pure multiplicative congruential method*, which was originally suggested by Lehmer, although he indicated $c \neq 0$ as a possibility. However, our discussion in Section 2.2 will show that restricting $c = 0$ reduces the maximum possible period length. In actual fact, the concept of using a non-zero increment to yield longer period lengths was due to Thomson [Tho58], and independently to Rotenburg [Rot60].

Definition 2.1.1. *A sequence* $\{x_i\}$ *produced by a linear congruential generator* (2.1)*, as defined above, is called a* ***linear congruential sequence*** *of pseudorandom numbers, which is said to be* ***determined*** *by* (x_0, a, c, m)*. From this sequence, we derive the sequence* $\{u_i\}$ *of* ***normalized*** *pseudorandom numbers, where* $u_i = x_i/m \in [0, 1)$ *for all* $i \geq 0$*.*

Remark. For computer simulations, it is often necessary to generate random numbers between 0 and 1, and so normalized pseudorandom numbers are quite important in this respect. Indeed, they are the basic ingredients for any stochastic simulation problem.

Example 2.1.1. Consider the linear congruential sequence $\{x_i\}$ determined by $(x_0, a, c, m) = (7, 3, 5, 15)$. We find that $x_1 \equiv 3 \cdot 7 + 5 \equiv 11 \pmod{15}$, so that $x_1 = 11$ and, in a similar fashion, we obtain $x_2 = 8$, $x_3 = 14$, $x_4 = 2$ and so on. Thus, this generator produces the sequence $7, 11, 8, 14, 2, 11, 8, 14, 2, 11, \ldots$ which is an ultimately periodic sequence with pre-period length 1 and (least) period length 4. □

This example provides evidence that a linear congruential sequence is not always 'random' for all choices of parameters m, a, c and x_0.

Clearly, a linear congruential sequence $\{x_i\}$ consists of at most m different terms since each x_i assumes a value in $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. If a is relatively prime to m (i.e. $(a, m) = 1$), then given x_{i+1}, congruence (2.1) can be solved uniquely for x_i since a will have a unique inverse modulo m. Therefore, the sequence $\{x_i\}$ is purely periodic, with least period length at most m, and the first term to repeat in the sequence will be x_0. However, if $(a, m) \neq 1$, the sequence $\{x_i\}$ will be ultimately periodic, but not necessarily purely periodic, as is evident in the above example. This situation is not promising enough to warrant discussion, so we will henceforth assume $(a, m) = 1$. Then the sequence $\{x_i\}$ will be purely periodic with least period length at most m. In the case that $\{x_i\}$ has period length m, we say that it has *full period length*, and $\mathbb{Z}_m = \{x_0, x_1, \ldots, x_{m-1}\}$. The above example also demonstrates that the modulus m should be an appropriately chosen large positive integer.

Of course, we can immediately disregard that case $a = 1$, for such a multiplier would mean that $x_i \equiv (x_0 + ic) \pmod{m}$, which is certainly not a randomly behaving sequence. And, considerably worse, is the case $a = 0$. Therefore, in practice, we take $a \geq 2$.

We now state the main theorem of this section, which gives necessary and sufficient conditions for a linear congruential sequence $\{x_i\}$ to attain full period length.

Theorem 2.1.1. *A linear congruential generator* (2.1) *produces a sequence* $\{x_i\}$ *of full period length* m *if and only if each of the following conditions are satisfied:*

(i) c *is relatively prime to* m*;*

(ii) $a \equiv 1 \pmod{p}$ *for each prime divisor* p *of* m*;*

(iii) $a \equiv 1 \pmod{4}$ *if* m *is a multiple of 4.*

The number-theoretical concepts used in the proof of this theorem date back at least one hundred years. Having first been proved in 1961 by Greenberger [Gre61], for the specific case of a power of two modulus, the sufficiency of conditions $(i)-(iii)$ was proved only one year later by Hull and Dobell [HD62]. In this current paper, the proof of this major result has been adapted from those of Knuth [Knu81] and Ripley [Rip87]. We shall require several lemmas; the first of which will be often referred to in this chapter as it gives a method for determining the terms of a linear congruential sequence directly from the multiplier, increment and initial seed.

Lemma 2.1.1. *Let* $\{x_i\}$ *be a linear congruential sequence determined by* (x_0, a, c, m)*. Assuming* $a \geq 2$ *then*

$$x_{i+k} \equiv a^k x_i + (a^k - 1)c/(a-1) \pmod{m} \qquad \text{for all } k \geq 0. \tag{2.2}$$

In fact, the terms of the sequence $\{x_i\}$ *are given by*

$$x_k \equiv a^k x_0 + (a^k - 1)c/(a-1) \pmod{m} \qquad \text{for all } k \geq 0. \tag{2.3}$$

Proof. We proceed by mathematical induction on k. In the case $k = 0$, it is clear that congruence (2.2) is true since $x_{i+0} \equiv a^0 x_i + (a^0 - 1)c/(a-1) \pmod{m}$. Assume (2.2) is true for the $(i+k)^{th}$ term of sequence $\{x_i\}$, and consider the $(i+k+1)^{st}$ term. We have

$$\begin{aligned}
x_{i+(k+1)} &\equiv a x_{i+k} + c \pmod{m} && \text{by (2.1)} \\
&\equiv a(a^k x_i + (a^k - 1)c/(a-1)) + c \pmod{m} && \text{by (2.2)} \\
&\equiv a^{k+1} x_i + (a(a^k - 1)/(a-1) + 1)c \pmod{m} \\
&\equiv a^{(k+1)} x_i + (a^{(k+1)} - 1)c/(a-1) \pmod{m}
\end{aligned}$$

which is the required expression for the $(i+(k+1))^{st}$ term of the sequence $\{x_i\}$. Hence, by mathematical induction, (2.2) is true for all integers $k \geq 0$.
In addition, setting $i = 0$ in (2.2) we obtain $x_k \equiv a^k x_0 + (a^k - 1)c/(a-1) \pmod{m};\ k \geq 0$ which gives congruence (2.3). □

It is deduced from this lemma that the subsequence consisting of every k^{th} term of $\{x_i\}$ is itself a linear congruential sequence with a multiplier $a^k \pmod m$ and increment $(a^k - 1)c/(a - 1) \pmod m$.

Note. By the *Fundamental Theorem of Arithmetic* (Theorem A.2), every positive integer m can be expressed as a product of powers of distinct primes; that is, $m = \prod_{j=1}^{n} p_j^{\alpha_j}$, where p_j's are distinct primes and α_j's are positive integers.

Lemma 2.1.2. *Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ be the decomposition of modulus m into prime powers where $p_1, \dots, p_n$ are distinct primes and all $\alpha_j \in \mathbb{Z}^+$. Then the least period length, d, of any linear congruential sequence $\{x_i\}$ determined by (x_0, a, c, m) is given by the least common multiple of the least period lengths, d_j, of the linear congruential sequences determined by $(x_0 \pmod{p_j^{\alpha_j}}, a \pmod{p_j^{\alpha_j}}, c \pmod{p_j^{\alpha_j}}, p_j^{\alpha_j})$, $1 \le j \le n$.*

Proof. By mathematical induction on n, it is only necessary to prove that if modulus $m = m_1 m_2$ where $(m_1, m_2) = 1$, then the period length, d, of the given sequence $\{x_i\}$ is such that $d = lcm(d_1, d_2)$, where d_1 and d_2 are the respective period lengths of the linear congruential sequences $\{y_i\}$, $\{z_i\}$ determined by $(x_0 \pmod{m_1}, a \pmod{m_1}, c \pmod{m_1}, m_1)$ and $(x_0 \pmod{m_2}, a \pmod{m_2}, c \pmod{m_2}, m_2)$.

By definition of the above three sequences, we have $y_i \equiv x_i \pmod{m_1}$ and $z_i \equiv x_i \pmod{m_2}$ for all $i \ge 0$. Hence, since $(m_1, m_2) = 1$, then

$$x_i = x_j \text{ if and only if } y_i = y_j \text{ and } z_i = z_j. \tag{2.4}$$

Note. We have made use of the elementary result: 'If $(r, s) = 1$, then $a \equiv b \pmod{rs}$ if and only if $a \equiv b \pmod r$ and $a \equiv b \pmod s$.'

Let $d' = lcm(d_1, d_2)$, and observe the following two facts:

(1) Since the sequence $\{y_i\}$ has period length d_1, then $y_j = y_0$ if and only if j is a multiple of d_1.

(2) Similarly, since the sequence $\{z_i\}$ has period length d_2, then $z_j = z_0$ if and only if j is a multiple of d_2.

Now, since the sequence $\{x_i\}$ has least period length d then d is the smallest positive integer such that $x_d = x_0$, and therefore $y_d = y_0$ and $z_d = z_0$ by (2.4). This implies that d is a multiple of both d_1 and d_2 (according to (1) and (2)), and hence d is a multiple of $d' = lcm(d_1, d_2)$ so that $d \ge d'$. Moreover, since $d' = lcm(d_1, d_2)$ is a multiple of both d_1 and d_2 then (1) and (2) imply $z_{d'} = z_0$ and $y_{d'} = y_0$. So, by (2.4), $x_{d'} = x_0$ which implies d' is a multiple of the period length d and therefore $d' \ge d$. Thus, $d = d'$, as required. □

Lemma 2.1.3. *Let p be a prime and $\alpha \in \mathbb{Z}^+$ such that $p^\alpha > 2$. If*

$$x \equiv 1 \pmod{p^\alpha},\ x \not\equiv 1 \pmod{p^{\alpha+1}} \tag{2.5}$$

$$\textit{then} \quad x^p \equiv 1 \pmod{p^{\alpha+1}},\ x^p \not\equiv 1 \pmod{p^{\alpha+2}}. \tag{2.6}$$

Proof. Suppose $x \equiv 1 \pmod{p^\alpha},\ x \not\equiv 1 \pmod{p^{\alpha+1}}$ then $x = 1 + qp^\alpha$ for some $q \in \mathbb{Z}$, where q is not a multiple of p. By the *Binomial Theorem* (Theorem A.3),

$$\begin{aligned} x^p &= (1+qp^\alpha)^p \\ &= 1 + \binom{p}{1} qp^\alpha + \ldots + \binom{p}{p-1} q^{p-1} p^{(p-1)\alpha} + q^p p^{p\alpha} \\ &= 1 + qp^{\alpha+1} \underbrace{\left(1 + \frac{1}{p}\binom{p}{2} qp^\alpha + \frac{1}{p}\binom{p}{3} q^2 p^{2\alpha} + \ldots + \frac{1}{p}\binom{p}{p} q^{p-1} p^{(p-1)\alpha}\right)}_{(*)}. \end{aligned}$$

Now, $(*) \in \mathbb{Z}$ and it is readily verified that $\binom{p}{r}$ is divisible by p for $1 < r < p$. Therefore, $\frac{1}{p}\binom{p}{r} q^{r-1} p^{(r-1)\alpha}$ is divisible by $p^{(r-1)\alpha}$ for $1 < r < p$, and the last term of $(*)$:
$\frac{1}{p}\binom{p}{p} q^{p-1} p^{(p-1)\alpha} = q^{p-1} p^{(p-1)\alpha}$ is divisible by p since $(p-1)\alpha > 1$ when $p^\alpha > 2$. Thus, p divides every term in $(*)$ except the first term. Hence, $x^p = 1 + q' p^{\alpha+1}$, where $q' = q(*) \in \mathbb{Z}$ is not divisible by p, which implies that $x^p \equiv 1 \pmod{p^{\alpha+1}}$ and $x^p \not\equiv 1 \pmod{p^{\alpha+2}}$. □

Lemma 2.1.4. *If $a \equiv 3 \pmod 4$ then $(a^{2^{\alpha-1}} - 1)/(a-1) \equiv 0 \pmod{2^\alpha}$ when $\alpha > 1$.*

Proof. Suppose $a \equiv 3 \pmod 4$ then $a = 3 + 4t$ for some $t \in \mathbb{Z}$. That is, $a = 1 + (2 + 4t)$ and so $a = 1 + 2(1 + 2t)$ which implies that $a \equiv 1 \pmod 2$.

Now, $a^2 = 9 + 24t + 16t^2 = 1 + 8(1 + 3t + 2t^2)$ and therefore $a^2 \equiv 1 \pmod 8,\ a^2 \not\equiv 1 \pmod{16}$. It follows by repeated applications of Lemma 2.1.3,

$$\begin{aligned} &a^4 \equiv 1 \pmod{16},\quad a^4 \not\equiv 1 \pmod{32} \\ &a^8 \equiv 1 \pmod{32},\ a^8 \not\equiv 1 \pmod{64}, \qquad \text{and so on.} \end{aligned}$$

In general, by mathematical induction on α, we have $a^{2^{\alpha-1}} \equiv 1 \pmod{2^{\alpha+1}}$, and hence $a^{2^{\alpha-1}} - 1 \equiv 0 \pmod{2^{\alpha+1}}$. That is, $a^{2^{\alpha-1}} - 1 = t2^{\alpha+1}$ for some odd $t \in \mathbb{Z}^+$ and therefore $(a^{2^{\alpha-1}} - 1)/2 = t2^\alpha$ so that $(a^{2^{\alpha-1}} - 1)/2 \equiv 0 \pmod{2^\alpha}$.
Thus, since $a \equiv 1 \pmod 2$, this yields the required result. □

We are now equipped with the necessary tools to prove Theorem 2.1.1.

Proof of Theorem 2.1.1. By Lemma 2.1.2, it is only necessary to consider the case of modulus $m = p^\alpha$, where p is a prime and $\alpha \in \mathbb{Z}^+$, since $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = d' = lcm(d_1, d_2, \ldots, d_n) \le d_1 d_2 \ldots d_n \le p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ holds if and only if $d_j = p_j^{\alpha_j}$ for $1 \le j \le n$.

Assume $c > 0$ since we will separately consider the case $c = 0$ in Section 2.2.

If $a = 1$ then it follows that $x_i \equiv x_0 + ic \pmod{m}$ for all $i \geq 0$, and so $x_i = x_0$ if and only if $ic \equiv 0 \pmod{m}$ – that is, if and only if $i \equiv 0 \pmod{m/k}$ where $k = (c, m)$, by Theorem A.1. Hence, $x_i = x_0$ if and only if i is a multiple of m/k. This implies m/k is the period length of sequence $\{x_i\}$, which therefore has full period length m if and only if $k = (c, m) = 1$. Furthermore, since $a = 1$ we also have $a \equiv 1 \pmod{p}$ for each prime divisor p of m, and $a \equiv 1 \pmod{4}$ if 4 divides m. Thus, the theorem holds for $a = 1$ and we therefore take $a > 1$.

Necessity

Note that the period length is m if and only if each possible residue $0, 1, 2, \ldots, (m-1)$ modulo m appears in the period, since no value occurs in the period more than once. Therefore, the period length is m if and only if the period of the sequence, with $x_0 = 0$, is of length m. So, without loss of generality, one may suppose that the period length of the sequence $\{x_i\}$ is $m = p^\alpha$ with initial seed $x_0 = 0$.

It immediately follows from Lemma 2.1.1 that the terms of the sequence $\{x_i\}$ are given by

$$x_k \equiv (a^k - 1)c/(a-1) \pmod{m} \qquad \text{for all } k \geq 1. \tag{2.7}$$

By the above note, $x_i = 1$ for some i which can occur if and only if $(a^i - 1)c/(a-1) \equiv 1 \pmod{m}$ (by (2.7)). Moreover, this congruence holds if and only if $(c, m) = 1$ since c has an inverse modulo m; namely: $(a^i - 1)/(a-1) = 1 + a + a^2 + \ldots + a^{i-1} \in \mathbb{Z}$ (by geometric series). Hence, condition (i) of the theorem has been proved both necessary and sufficient.

Now, since the period length is $m = p^\alpha$ then m is the smallest positive integer such that $x_m = x_0 = 0$, and this implies $(a^m - 1)c/(a-1) \equiv 0 \pmod{m}$. That is, since $(c, m) = 1$, then

$$(a^m - 1)/(a-1) \equiv 0 \pmod{m}, \tag{2.8}$$

by Theorem A.1.

(1) If $a \not\equiv 1 \pmod{p}$ then $a^m - 1 \equiv 0 \pmod{m}$. That is, $(a^m - 1) = tm$ for some $t \in \mathbb{Z}^+$ and so $(a^{p^\alpha} - 1) = tp^\alpha$ since $m = p^\alpha$. Hence, $(a^{p^\alpha} - 1) = (tp^{\alpha-1})p^\alpha$ where $tp^{\alpha-1} \in \mathbb{Z}^+$, and so p divides $(a^{p^\alpha} - 1)$. Thus, $a^{p^\alpha} - 1 \equiv 0 \pmod{p}$ (i.e. $a^m \equiv 1 \pmod{p}$). But, by *Fermat's Little Theorem* (Theorem A.4), $a^p \equiv a \pmod{p}$ so $a^{p^\alpha} \equiv a \pmod{p}$ which implies that $a^m \equiv a \pmod{p}$. We therefore conclude that $a \equiv 1 \pmod{p}$.

(2) Now, suppose $p = 2$ so that $m = 2^\alpha$, $\alpha \geq 2$ is the period length of $\{x_i\}$. If

$a \equiv 1 \pmod 2$ but $a \not\equiv 1 \pmod 4$, $a \equiv 3 \pmod 4$) then $(a^{2^{\alpha-1}} - 1)/(a-1) \equiv 0 \pmod{2^\alpha}$, by Lemma 2.1.4; a contradiction since $(a^{2^\alpha} - 1)/(a-1) \equiv 0 \pmod{2^\alpha}$ when $m = 2^\alpha$ is the period length. Whence, $a \equiv 1 \pmod 4$.
Alternatively, using $x_i \equiv ax_{i-1} + c \pmod m$, we obtain

$$\begin{aligned} x_i &\equiv a(ax_{i-2} + c) + c \pmod m \\ &\equiv a^2 x_{i-2} + (a+1)c \pmod m. \end{aligned}$$

So since $x_0 = 0$, then x_2 (and hence $x_4, x_6, \ldots$) is a multiple of $(a+1)c \equiv 4c \pmod m$. Consequently, the sequence $\{x_{2i}\}$ consists of at most $m/4$ different values so that, in turn, $\{x_i\}$ has period length at most $m/2$; a contradiction, and hence $a \equiv 1 \pmod 4$.

Results (1) and (2) show that conditions (ii) and (iii) of the theorem are necessary.

Sufficiency

To prove sufficiency, we assume $m = p^\alpha$ and observe (from the above arguments) that conditions (ii) and (iii) of the theorem imply $a = 1 + qp^\beta$, where $p^\beta > 2$ and q is not a multiple of p whenever the period length is $m = p^\alpha$. We therefore need to show that this condition is sufficient for the period length to be $m = p^\alpha$.

By Lemma 2.1.3, $a^p \equiv 1 \pmod{p^{\beta+1}}$ and $a^p \not\equiv 1 \pmod{p^{\beta+2}}$. It follows by mathematical induction on γ, that $a^{p^\gamma} \equiv 1 \pmod{p^{\beta+\gamma}}$ and $a^{p^\gamma} \not\equiv 1 \pmod{p^{\beta+\gamma+1}}$ for all $\gamma \geq 0$. Therefore,

$$(a^{p^\gamma} - 1)/(a-1) \equiv 0 \pmod{p^\gamma}; \quad (a^{p^\gamma} - 1)/(a-1) \not\equiv 0 \pmod{p^{\gamma+1}} \tag{2.9}$$

since $a = 1 + qp^\beta$ implies $(a-1) \equiv 0 \pmod{p^\beta}$. Furthermore, congruences (2.9) imply $(a^{p^\alpha} - 1)/(a-1) \equiv 0 \pmod{p^\alpha}$.

By (2.7), the linear congruential sequence $\{x_i\}$ determined by $(0, a, c, p^\alpha)$ is such that $x_i \equiv (a^i - 1)c/(a-1) \pmod{p^\alpha}$ for all $i \geq 0$. Suppose this sequence has period length d. Then $x_k = x_0 = 0$ (i.e. $(a^k - 1)c/(a-1) \equiv 0 \pmod{p^\alpha}$) if and only if k is a multiple of d. That is, since $(c, m) = 1$, $(a^k - 1)/(a-1) \equiv 0 \pmod{p^\alpha}$ if and only if k is a multiple of d (using Theorem A.1). So, by the above, p^α is a multiple of d, which can only occur if $d = p^\gamma$ for some integer $\gamma \geq 0$, and congruences (2.9) imply $d = p^\alpha$, completing the proof. □

As an immediate consequence of Theorem 2.1.1, the next corollary is of particular importance since powers of two are the most frequently used moduli (for reasons discussed in Section 2.2).

Corollary 2.1.1. *A linear congruential generator with modulus $m = 2^\beta \geq 4$; $\beta \in \mathbb{Z}^+$, produces a sequence $\{x_i\}$ of full period length m if and only if c is odd and $a \equiv 1 \pmod 4$.* □

Let us illustrate Theorem 2.1.1 by an example.

Example 2.1.2. Consider the linear congruential generator

$$x_{i+1} \equiv 13x_i + 5 \pmod{18},$$

which has parameters $x_0 = 7$, $a = 13$, $c = 5$, $m = 18$. We have $x_1 \equiv 13 \cdot 7 + 5 \equiv 6 \pmod{18}$, $x_2 \equiv 13 \cdot 6 + 5 \equiv 11 \pmod{18}$, etc. so that the generated sequence is

$$\underbrace{7, 6, 11, 4, 3, 8, 1, 0, 5, 16, 15, 2, 13, 12, 17, 10, 9, 14}_{\text{period}}, 7, 6, 11, 4, \ldots$$

This sequence has full period length 18; thus, demonstrating Theorem 2.1.1 since
(i) $(5, 18) = 1$;
(ii) $13 \equiv 1 \pmod 2$ and $13 \equiv 1 \pmod 3$, where 2 and 3 are the prime divisors of 18. □

As pointed out by Marsaglia [Mar72], in spite of a profuse number of articles having touted specific choices of increment c ($c \neq 0$), it is a simple known fact that the choice of c and initial seed x_0 is of no great consequence, since any linear congruential sequence $\{x_i\}$ can be obtained by an affine transformation of the *fundamental sequence* $0, 1, a + 1, a^2 + a + 1, \ldots$ accordingly:

Theorem 2.1.2. *Let $\{x_i\}$ be a linear congruential sequence. If $\{y_i\}$ is the fundamental sequence $0, 1, a + 1, a^2 + a + 1, \ldots$ generated by $y_{i+1} \equiv ay_i + 1 \pmod m$, with $y_0 = 0$, then $\{x_i\}$ may be obtained from an affine transformation $x_i \equiv vy_i + \omega \pmod m$, where $v \equiv x_0(a - 1) + c \pmod m$ and $\omega \equiv x_0 \pmod m$. Moreover, the period length of the sequence $\{x_i\}$ is the period length of $\{y_i\}$ modulo m/k, where $k = (m, x_0(a - 1) + c)$.*

Proof. We prove the first part of the theorem by verification. Observe that, by geometric series, one may write $y_i \equiv (a^i - 1)/(a - 1) \pmod m$, and by Lemma 2.1.1, $x_i \equiv a^i x_0 + (a^i - 1)c/(a - 1) \pmod m$ for all $i \geq 0$. Therefore,

$$\begin{aligned} x_i &\equiv (x_0(a - 1) + c)(a^i - 1)/(a - 1) + x_0 \pmod m \\ &\equiv (x_0(a - 1) + c)y_i + x_0 \pmod m. \end{aligned}$$

Now, since $\{x_i\}$ (and hence $\{vy_i + \omega\}$) is purely periodic, with $x_0 \equiv \omega \pmod m$ the first term to repeat in the sequence, the period length of the sequence $\{x_i\} = \{vy_i + \omega\}$ is the smallest positive integer d such that $x_d \equiv vy_d + \omega \equiv \omega \pmod m$. But, by way of Theorem A.1, $vy_d \equiv 0 \pmod m$ implies $y_d \equiv 0 \pmod{m/k}$, where $k = (m, v)$. Thus, the period length of $\{y_i\}$ modulo m/k is also d. □

Since all linear congruential generators produce sequences which are affine transformations of the fundamental sequences 0, 1, $1+a$, $1+a+a^2$, ..., the structure and period length of linear congruential sequences can be derived by simply considering fundamental sequences. Marsaglia's paper [Mar72] provides an in-depth discussion of the structure of linear congruential sequences in terms of fundamental sequences.

Our next section is devoted to the most frequently implemented pure multiplicative congruential method.

2.2 Pure Multiplicative Congruential Method

The **pure multiplicative congruential method** produces a *pure multiplicative congruential sequence* $\{x_i\}_{i\geq 0}$ of pseudorandom numbers defined recursively by

$$\boxed{x_{i+1} \equiv ax_i \pmod{m}, \qquad 0 \leq x_{i+1} < m} \tag{2.10}$$

with $0 < a, x_0 < m$.

It is clear that a *pure multiplicative congruential sequence* $\{x_i\}$ has maximal period length $m-1$ since if $x_i = 0$ for some i then the sequence degenerates to zero.

Before determining the conditions on the multiplier so that $\{x_i\}$ has a period length as large as possible, we require the notion of a *primitive root modulo* m, which is defined in terms of *Euler's ϕ-function.*

Definition 2.2.1. *Let m be a positive integer.*

*(1) The function $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $\phi(m) = |\{t \in \mathbb{Z}^+ : 1 \leq t \leq m;\ (t,m) = 1\}|$ is called the **Euler ϕ-function**.*

*(2) If a is an integer relatively prime to m, then the smallest positive integer n such that $a^n \equiv 1 \pmod{m}$ is called the **order of** a **modulo** m, denoted $ord_m a$. Furthermore, if $ord_m a = \phi(m)$, then a is called a **primitive root modulo** m.*

Quite a nice little result follows from this definition, as given below. Note that for non-zero integers a and b, $a \mid b$ means a divides b so that b is an integer multiple of a.

Theorem 2.2.1. *If $(a,m) = 1$ then $a^x \equiv 1 \pmod{m}$ if and only if $ord_m a \mid x$.*

Proof. If $ord_m a \mid x$ then $x = k \cdot ord_m a$ for some $k \in \mathbb{Z}^+$, and therefore $a^x = (a^{ord_m a})^k \equiv 1^k \equiv 1 \pmod{m}$.

Conversely, suppose $a^x \equiv 1 \pmod{m}$. By the *Division Algorithm* (Theorem A.6), one may write $x = q \cdot ord_m a + r$, for some q, $r \in \mathbb{Z}$ with $0 \leq r < ord_m a$. We thus obtain $a^x = a^{q ord_m a + r} = (a^{ord_m a})^q a^r \equiv a^r \pmod{m}$, which implies $a^r \equiv 1 \pmod{m}$ since $a^x \equiv 1 \pmod{m}$; a contradiction to the definition of $ord_m a$ unless $r = 0$. Hence, $x = q \cdot ord_m a$ and so $ord_m a \mid x$. □

Note that, in general, if k is any divisor of both m and some x_i, then x_i is a multiple of k and hence $x_{i+1}, x_{i+2}, \ldots$ are all multiples of k. Consequently, the sequence could not be perceived as random, and we shall therefore assume that x_i is relatively prime to m for all i. Of course, this will be achieved by choosing a multiplier a and initial seed x_0 such that $(a, m) = (x_0, m) = 1$, which leads to purely periodic sequences with period lengths limited to at most $\phi(m)$, the number of integers between 1 and m that are relatively prime to m.

Now, let m be a positive integer with prime-power factorization $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$. By *Euler's Theorem* (Theorem A.5), if a is an integer such that $(a, m) = 1$, then $a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}$ for all $i = 1, 2, 3, \ldots, n$.

Let $U = [\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2}), \ldots, \phi(p_n^{\alpha_n})]$ (where [ ] denotes the least common multiple), then $\phi(p_i^{\alpha_i}) \mid U$ for all $i = 1, 2, \ldots, n$, and so by Theorem 2.2.1, $a^U \equiv 1 \pmod{p_i^{\alpha_i}}$ for all $i = 1, 2, \ldots, n$. Moreover, since we have $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ for all $i \neq j$, then $[p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_n^{\alpha_n}] = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = m$. Hence, by Lemma A.4, it follows that $a^U \equiv 1 \pmod{m}$, which leads to the following definition.

Definition 2.2.2. *A positive integer U such that $a^U \equiv 1 \pmod{m}$ for all integers a relatively prime to m is called a* ***universal exponent*** *of the positive integer m. The least universal exponent of m is called the* ***minimal universal exponent*** *of m, denoted $\lambda(m)$.*

It is evident from *Euler's Theorem* that Euler's ϕ-function, $\phi(m)$, is a universal exponent. In fact, the idea of such a number-theoretic function $\lambda(m)$ was first presented in an early paper (1910) by Carmichael [Car10], who originally defined it entirely in terms of Euler's ϕ-function. And, as demonstrated in [Car10, Knu81, Ros00], we have:

$$\begin{aligned} \lambda(2) = 1,\ \lambda(4) = 2,\ \lambda(2^e) = 2^{e-2} \qquad & \text{if } e \geq 3; \\ \lambda(p^\alpha) = p^{\alpha-1}(p-1), \qquad & \text{if } p > 2; \\ \lambda(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}) = [\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_n^{\alpha_n})], & \end{aligned} \tag{2.11}$$

where p is a prime, the p_i's are distinct primes, and each $\alpha_i \in \mathbb{Z}^+$.

As a consequence of Lemma 2.1.1, we can express the terms of the pure multiplicative congruential sequence $\{x_i\}$ by

$$x_i \equiv a^i x_0 \pmod{m} \qquad \text{for all } i \geq 0. \tag{2.12}$$

It follows that if d is the period length of the pure multiplicative congruential sequence $\{x_i\}$, then d is the smallest positive integer such that $x_0 \equiv a^d x_0 \pmod{m}$. Hence, having the assumed the initial seed x_0 is relatively prime to the modulus m, Theorem A.1 implies $a^d \equiv 1 \pmod{m}$. In other words, the period length of $\{x_i\}$ is the smallest positive integer d such that $a^d \equiv 1 \pmod{m}$. It therefore immediately follows that the maximum possible period length is $\lambda(m)$. Furthermore, Carmichael [Car10] showed that if m has a primitive root then $\lambda(m) = \phi(m)$.

We may now summarize the above remarks in the following theorem.

Theorem 2.2.2. *For a pure multiplicative congruential sequence $\{x_i\}$, determined by $(x_0, a, 0, m)$, the maximum possible period length is $\lambda(m)$, which is attained if:*

(i) x_0 is relatively prime to m; and

(ii) a is a primitive root modulo m. □

2.2.1 Prime Modulus

If the modulus m is a prime then $\lambda(m) = \phi(m) = m - 1$. It is therefore advantageous in practice, as well as theory, that the modulus m be a prime, so that maximal period length $m - 1$ may be attained under the condition of the following theorem (a special case of Theorem 2.2.2).

Theorem 2.2.3. *A pure multiplicative congruential sequence $\{x_i\}$ can attain a period length of $m - 1$ only if m is prime, in which case the period length divides $m - 1$, and is $m - 1$ if and only if a is a primitive root modulo m.*

In order to prove this theorem we require the following lemma, which provides a characterization of primitive roots modulo an odd prime p.

Lemma 2.2.1. *An integer a is a primitive root modulo the odd prime p if and only if $a^{\frac{(p-1)}{q}} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$.*

Proof. Suppose a is a primitive root modulo the odd prime p. Then $a^{\frac{(p-1)}{q}} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$ since $\phi(p) = p - 1$ is the smallest power of a that is congruent to 1 modulo p.

Conversely, suppose $a^{\frac{(p-1)}{q}} \not\equiv 1 \pmod{p}$ for all prime divisors q of $(p-1)$ and suppose a is not a primitive root modulo p. Then there exists $t \in \mathbb{Z}^+$ such that $a^t \equiv 1 \pmod{p}$ with $t < p-1$ and $t \mid (p-1)$. Therefore, $(p-1) = st$ for some integer $s > 1$, so $\frac{(p-1)}{s} = t$. Let q be a prime divisor of s then $\frac{(p-1)}{q} = \frac{s}{q}t$, and hence $a^{\frac{(p-1)}{q}} = a^{\frac{s}{q}t} = (a^t)^{\frac{s}{q}} \equiv 1^{\frac{s}{q}} \pmod{p} \equiv 1 \pmod{p}$ since $a^t \equiv 1 \pmod{p}$; a contradiction to the original assumption. Thus, a is a primitive root modulo p. □

Proof of Theorem 2.2.3. By (2.3) of Lemma 2.1.1, since $c = 0$, the terms of the pure multiplicative congruential sequence $\{x_i\}$ are given by:

$$x_i \equiv a^i x_0 \pmod{m} \qquad \text{for all } i \geq 0. \tag{2.13}$$

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ be the factorization of the modulus m into prime powers.
Now, $\{x_i\}$ modulo $p_j^{\alpha_j}$ has period length at most $p_j^{\alpha_j} - 1$ (since if $x_i = 0$ for some i then the sequence degenerates to 0). Hence, $\{x_i\}$ has period length at most $\prod_{j=1}^{n}(p_j^{\alpha_j} - 1) \leq (m-1)$ with equality if and only if $n = 1$. So, let us suppose $m = p^\alpha$, where p is a prime, $\alpha \in \mathbb{Z}^+$.

Firstly, consider $\alpha \geq 2$ so that m is a *power* of a prime.
By *Fermat's Little Theorem* (Theorem A.4), $a^{p-1} \equiv 1 \pmod{p}$, and by (2.13), $x_{p-1} \equiv a^{p-1}x_0 \pmod{p} \equiv x_0 \pmod{p}$. This implies that the sequence $\{x_i\}$ modulo p has period length d dividing $p-1$. Consequently, $x_{id} \equiv x_0 \pmod{p}$ so $(x_{id} - x_0)$ is a multiple of p. Hence, the sequence $\{x_{id}\}$ has period length at most $p^{\alpha-1}$, and so $\{x_i\}$ has period length at most $dp^{\alpha-1}$ which is less than $m-1$.

Now, suppose $\alpha = 1$ so that the modulus m is a prime. As above, by *Fermat's Little Theorem*, the sequence $\{x_i\}$ has period length d dividing $m-1$, which implies $m-1 = td$ for some $t \in \mathbb{Z}^+$.

Suppose a is a primitive root modulo m and let q be a prime divisor of t. Then $\frac{(m-1)}{q} = \frac{t}{q}d$ so that $\frac{(m-1)}{q}$ is an integer multiple of d. Hence, $x_{\frac{(m-1)}{q}} \equiv a^{\frac{(m-1)}{q}} x_0 \pmod{m} \equiv x_0 \pmod{m}$ so $a^{\frac{(m-1)}{q}} \equiv 1 \pmod{m}$, and therefore a is not a primitive root modulo m unless $t = 1$ so that t has no prime divisors and we have period length $m - 1 = d$.

Conversely, suppose the period length is $m-1$ and suppose a is not a primitive root modulo m. According to Lemma 2.2.1, $a^{\frac{m-1}{q}} \equiv 1 \pmod{m}$ for all prime divisors q of m. This implies $x_{\frac{(m-1)}{q}} \equiv a^{\frac{(m-1)}{q}} x_0 \pmod{m} \equiv x_0 \pmod{m}$, and hence the period length divides $\frac{(m-1)}{q}$ so is therefore less than $m-1$; a contradiction. Thus, a is a primitive root modulo m. □

2.2.2 Finding Primitive Roots

Finding a primitive root of m may prove difficult for large m, but once one is found then all others follow, provided m is a prime.

Lemma 2.2.2. *If a pure multiplicative congruential sequence $\{x_i\}$ has period length d then $\{x_{ki}\}$ has period length $d/(k,d)$.*

Proof. Suppose the sequence $\{x_i\}$ has period length d. Then $x_{ki} = x_0$ if and only if ki is a multiple of d, i.e. if and only if $ki \equiv 0 \pmod{d}$. Further, this is equivalent to $i \equiv 0 \pmod{d/(k,d)}$ (by Theorem A.1), which means i is a multiple of $d/(k,d)$. □

Theorem 2.2.4. *Let a be a primitive root modulo a prime p. Then a^k is a primitive root modulo p if and only if $(k, p-1) = 1$.*

Proof. Let a be a primitive root modulo a prime p and consider the pure multiplicative congruential sequence $\{x_i\}$ defined recursively by $x_{i+1} \equiv ax_i \pmod{p}$. This sequence $\{x_i\}$ has period length $p-1$, according to Theorem 2.2.3. Note that the sequence $\{x_{ki}\}$ corresponds to a *multiplier* $a^k \pmod{p}$ and has period length $(p-1)/(k, p-1)$, by Lemma 2.2.2. Hence, $\{x_{ki}\}$ has period length $p-1$ if and only if $(k, p-1) = 1$. Thus, by Theorem 2.2.3, a^k is a primitive root modulo p if and only if $(k, p-1) = 1$. □

This immediately suggests that once one has determined a primitive root modulo m then testing for the condition $(k, m-1) = 1$; $k = 2, 3, \ldots$ provides a method for deriving further primitive roots modulo m, when m is a prime.

It is worth noting that a positive integer $n > 1$ possesses a primitive root if and only if $n = 2, 4, p^t$, or $2p^t$, where p is an odd prime and t is a positive integer. Furthermore, if n has a primitive root then there exist a total of $\phi(\phi(n))$ incongruent primitive roots modulo n. (Consult any elementary number theory textbook). Therefore, if the modulus m is prime, then m has $\phi(\phi(m)) = \phi(m-1)$ primitive roots.

Example 2.2.1. Consider the pure multiplicative congruential generator with prime modulus $m = 13$. Clearly, $\phi(\phi(13)) = \phi(12) = 4$ since only the four integers 1, 5, 7, 11 in the set $\{1, 2, \ldots, 12\}$ are relatively prime to 12; whence, there exists a total of four primitive roots modulo 13.

Since $2^6 \equiv 12 \not\equiv 1 \pmod{13}$ and $2^4 \equiv 3 \not\equiv 1 \pmod{13}$ (that is, $2^{12/q} \not\equiv 1 \pmod{13}$ for each prime divisor q of 12), then 2 is a primitive root of 13. It therefore follows from

Theorem 2.2.4 that the four primitive roots of 13 are:

$$\begin{aligned} 2^1 &\equiv \ \ 2 \pmod{13}, \\ 2^5 &\equiv \ \ 6 \pmod{13}, \\ 2^7 &\equiv 11 \pmod{13}, \\ 2^{11} &\equiv \ 7 \pmod{13}. \end{aligned}$$

If we take the primitive root $a = 6$ as the multiplier for the generator, and initial seed $x_0 = 5$, then the sequence produced is

$$5, 4, 11, 1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1, 6, \ldots$$

which has maximal period length 12, as expected. Indeed, for any choice of initial seed $0 < x_0 < 13$, the generated sequence will attain maximal period length since it is just a shifted version of the above sequence. □

2.2.3 Choosing a Prime Modulus

Theoretically, the modulus m can be made as large as desired. However, from a practical point of view, its size is restricted – the word size of the computer accounting for the most severe limitation. If m is no greater than the word size, then code for the generator need only make use of the computer's hardware to efficiently generate $\{x_i\}$. But, if m exceeds the word size, then the generation of $\{x_i\}$ requires more elaborate software implementation. For instance, a binary computer with a word size of β bits (usually $\beta = 32$) suggests the use of a prime modulus $m < 2^\beta$, so that m is the largest prime number in 2^β. Most computers have a word size of 31-bits (if we disregard the 'sign' bit) so that, for many applications, the pure multiplicative congruential method is used with modulus m equal to the *Mersenne prime* $M_{31} = 2^{31} - 1$, enabling us to generate $2^{31} - 2$ pseudorandom numbers, provided that the multiplier a is a primitive root modulo $2^{31} - 1$.

To find a primitive root of M_{31} that can be used with good results, we first demonstrate that 7 is a primitive root modulo M_{31}.

Theorem 2.2.5. *The integer* 7 *is a primitive root modulo* $M_{31} = 2^{31} - 1$.

Proof. The prime-power factorization of $M_{31} - 1$ can be found by observing that

$$\begin{aligned} M_{31} - 1 = 2^{31} - 2 &= 2(2^{15} - 1)(2^{15} + 1) \\ &= 2(2^5 - 1)(2^{10} + 2^5 + 1)(2^5 + 1)(2^{10} - 2^5 + 1) \\ &= 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331. \end{aligned}$$

In light of Theorem 2.2.4, it suffices to show that $7^{(M_{31}-1)/q} \not\equiv 1 \pmod{M_{31}}$ for $q = 2$, 3, 7, 11, 31, 151, and 331. Now,

$$\begin{aligned}
7^{(M_{31}-1)/2} &\equiv 2{,}147{,}483{,}646 \not\equiv 1 \pmod{M_{31}},\\
7^{(M_{31}-1)/3} &\equiv 1{,}513{,}477{,}735 \not\equiv 1 \pmod{M_{31}},\\
7^{(M_{31}-1)/7} &\equiv \quad 120{,}536{,}285 \not\equiv 1 \pmod{M_{31}},\\
7^{(M_{31}-1)/11} &\equiv 1{,}969{,}212{,}174 \not\equiv 1 \pmod{M_{31}},\\
7^{(M_{31}-1)/31} &\equiv \qquad\qquad 512 \not\equiv 1 \pmod{M_{31}},\\
7^{(M_{31}-1)/151} &\equiv \quad 535{,}044{,}134 \not\equiv 1 \pmod{M_{31}},\\
7^{(M_{31}-1)/331} &\equiv 1{,}761{,}885{,}083 \not\equiv 1 \pmod{M_{31}}.
\end{aligned}$$

Thus, 7 is a primitive root of M_{31}. □

Of course, in practice, we do not wish to use 7 as a multiplier since the first few generated numbers are rather small. That is, a small multiplier has the disadvantage that if x_i is small then so is x_{i+1}, thus yielding some degree of correlation between successive pseudorandom numbers. We instead find a larger primitive root modulo M_{31} using Theorem 2.2.4. That is, we may use 7^k where $(k, M_{31} - 1) = 1$. For example, since $(13, M_{31} - 1) = 1$ then $7^{13} \equiv 252,246,292 \pmod{M_{31}}$ may be used as a multiplier to yield a maximal period length of $M_{31} - 1$.

Matlab is just one specific example of an application which has used the pure multiplicative congruential generator with modulus M_{31}.

2.2.4 Matlab

Matlab is a widely used software package in mathematics and engineering, enabling the user to perform a whole host of different mathematical operations relatively easily and conveniently. Of particular interest, in the context of this thesis, is its `rand` function, which supplies random numbers chosen from the unit interval $(0, 1)$. Prior to Matlab version 5, its `rand` function produced random numbers using the pure multiplicative congruential generator with a multiplier $7^5 = 16807$ and modulus M_{31}. Since $(5, M_{31}-1) = 1$ then 7^5 is certainly a primitive root modulo M_{31}, and so, such a generator produces sequences with maximal period length $M_{31} - 1$. This generator was chosen for use in Matlab on the basis of its recommendation in a 1988 paper by Park and Miller [PM88]. However, although it generates $M_{31} - 1$ (a little over two billion) numbers before repeating, it was believed to be a little too skimpy for today's requirements, and so a different generator was adopted for Matlab 5.0, in 1995. Known as the *subtract-with-borrow generator*, it was suggested by George Marsaglia, a professor at Florida

State University, and author of the classic article, *"Random numbers fall mainly in the planes"* [Mar68]. The main reason for its appeal is its astonishing long periods. It also possesses an interesting underlying theory, requiring results in both number theory and group theory. A more detailed account of this type of generator will follow in Chapter 6.

2.2.5 Power of Two Modulus

There is a certain degree of computational advantage using a modulus $m = 2^\beta \geq 16$ since a binary computer may then exploit its binary character by merely shifting the *binary point* of the number being multiplied (divided) by β positions to the right (left). Such a *shift* consumes less time than a multiplication or division operation, and so is preferable. However, the sequences produced by generators with a power of two modulus have considerably shorter periods than when a prime modulus is used. According to Theorem 2.2.2, for modulus $m = 2^\beta \geq 16$, a pure multiplicative congruential sequence $\{x_i\}$ may have a period length of at most $\lambda(m) = 2^{\beta-2} = m/4$.

The next theorem was first proved by Greenberger [Gre61], but a different proof is provided here; one which makes use of Corollary 2.1.1.

Theorem 2.2.6. [Gre61] *A sequence $\{x_i\}$ produced by a pure multiplicative congruential generator, with modulus $m = 2^\beta \geq 16$, attains maximal period length $m/4$ if and only if x_0 is odd and $a \equiv 3$ or $5 \pmod 8$.*

Proof. Consider a pure multiplicative congruential generator with modulus $m = 2^\beta$ such that $\{x_i\}$ is given by

$$x_{i+1} \equiv ax_i \pmod{2^\beta}, \qquad 0 < x_{i+1} < m. \tag{2.14}$$

Suppose x_0 is even. Then $x_0 = 2^r t$ for some odd $t \in \mathbb{Z}$, $r \in \mathbb{Z}^+$ and, by (2.14), $x_{i+1}2^{-r} \equiv a(x_i 2^{-r}) \pmod{2^{\beta-r}}$, which reduces to the case of an odd seed.

Suppose a is even, then $a \equiv 0 \pmod 2$ and we have $x_\beta \equiv a^\beta x_0 \equiv 0 \pmod{2^\beta}$. So now suppose a and x_0 are odd so that each x_i is odd (since $x_i \equiv a^i x_0 \pmod{2^\beta}$ where x_0, a^i are odd).

Let x_0 be the smallest value appearing in the period. Since we have $x_i \equiv ax_{i-1} \pmod{2^\beta}$ for $i \geq 1$, then

$$\begin{aligned} x_i - x_0 &\equiv ax_{i-1} - x_0 \pmod{2^\beta} \\ &\equiv a(x_{i-1} - x_0) + (a-1)x_0 \pmod{2^\beta}. \end{aligned} \tag{2.15}$$

Since x_i is odd for all $i \geq 0$ then $(x_{i-1} - x_0)$ is even, and since a is odd then $(a-1)$ is even. It therefore follows that $(x_i - x_0)$ is even, so let $(x_i - x_0) = 2y_i$. Then, by (2.15),

$$\begin{aligned} & 2y_i \equiv a2y_{i-1} + (a-1)x_0 \pmod{2^\beta} \\ \text{so} \quad & y_i \equiv ay_{i-1} + a'x_0 \pmod{2^{\beta-1}} \qquad (\text{since } (2, 2^\beta) = 2), \end{aligned} \tag{2.16}$$

where $a' = \frac{(a-1)}{2} \in \mathbb{Z}$. Either a' is even or $a - 1 \not\equiv 0 \pmod 4$ (i.e. $a \not\equiv 1 \pmod 4$). Now, by applying Corollary 2.1.1 to the linear congruential generator (2.16), we deduce that this sequence $\{y_i\}$ has period length less than $m/2$. For, if $a' = \frac{(a-1)}{2}$ is even then increment $a'x_0$ is even, and so the first condition of the corollary does not hold. Or, if $a \not\equiv 1 \pmod 4$ then the other condition does not hold.

(1) Suppose $a \equiv 1 \pmod 4$ so that $a = 1 + 4t$ for some $t \in \mathbb{Z}$ and $a' = \frac{(a-1)}{2} = 2t$. Then, by (2.16), all y_i are even. Let $z_i = \frac{y_i}{2}$. Then, by (2.16),

$$\begin{aligned} & \frac{y_i}{2} \equiv a\frac{y_{i-1}}{2} + a'\frac{x_0}{2} \pmod{2^{\beta-2}} \\ \text{so} \quad & z_i \equiv az_i + tx_0 \pmod{2^{\beta-2}}. \end{aligned} \tag{2.17}$$

Now, if t is odd then $t = 2k+1$ for some $k \in \mathbb{Z}$ so that $a = 1+4(2k+1) = 5+8k$, and hence $a \equiv 5 \pmod 8$. In this case, it follows from Corollary 2.1.1 that the linear congruential sequence $\{z_i\}$ (and hence $\{x_i\}$) has full period length $m/4 = 2^{\beta-2}$ (since the increment tx_0 is odd and $a \equiv 1 \pmod 4$). Otherwise, the period length is less than $m/4$.

(2) Now, suppose $a \equiv 3 \pmod 4$ (so that $a \not\equiv 1 \pmod 4$, $a \equiv 1 \pmod 2$) then $a = 3 + 4t$ for some $t \in \mathbb{Z}$ and we have

$$\begin{aligned} y_i &\equiv a(ay_{i-2} + a'x_0) + a'x_0 \pmod{2^{\beta-1}} \qquad \text{by (2.16)} \\ &\equiv a^2y_{i-2} + a'ax_0 + a'x_0 \pmod{2^{\beta-1}} \\ &\equiv a^2y_{i-2} + a'(a+1)x_0 \pmod{2^{\beta-1}}, \end{aligned} \tag{2.18}$$

where $a'(a+1) = \left(\frac{2+4t}{2}\right)(4+4t)^2 = 4(1+2t)(1+t)$ so $a'(a+1)$ is a multiple of 4, and hence so are all y_{2i}.

Let $w_i = \frac{y_{2i}}{4}$ so that (2.18) yields

$$\begin{aligned} & \frac{y_{2i}}{4} \equiv a^2\frac{y_{2i-2}}{4} + \frac{a'(a+1)}{4}x_0 \pmod{2^{\beta-3}} \\ \text{and so} \quad & w_i \equiv a^2w_{i-1} + (1+2t)(1+t)x_0 \pmod{2^{\beta-3}}. \end{aligned} \tag{2.19}$$

This linear congruential generator (2.19) has multiplier $a^2 = 16t^2+24t+9 = 4(4t^2+6t+2)+1 \equiv 1 \pmod 4$ and, if t is even, it has an odd increment $s = (1+2t)(1+t)x_0$.

Thus, it follows from Corollary 2.1.1 that the sequence $\{w_i\}$ has full period length $m/8 = 2^{\beta-3}$ if t is even (i.e. $a \equiv 3 \pmod 8$); otherwise, the period length is less than $m/8$. So if $a \equiv 7 \pmod 8$ (i.e. t is odd) then $\{y_i\}$ has period length less than $m/8$, and if $a \equiv 3 \pmod 8$ (i.e. t is even), all y_{2i} are multiples of 4 with period length $m/8$ whereas y_{2i+1} are odd. Therefore, the sequence $\{y_i\}$ (and hence $\{x_i\}$) has period length $m/4$.

By (1) and (2), the theorem is proved. □

The following exemplifies the above result.

Example 2.2.2. Consider the pure multiplicative congruential generator, with modulus $m = 2^4 = 16$, defined by

$$x_{i+1} \equiv 11x_i \pmod{32}; \qquad i \geq 0.$$

Choosing initial seed $x_0 = 21$ yields the sequence

$$\underbrace{21, 7, 13, 15, 5, 23, 29, 31}_{\text{period}}, 21, 7, 13, 15, 5, 23, 29, \ldots,$$

which has maximal period length of $8 = 32/4$. Indeed, this is not surprising since x_0 is odd and the multiplier is $11 \equiv 3 \pmod 8$.

Similarly, if we use a multiplier such as $29 \equiv 5 \pmod 8$, with an initial seed $x_0 = 15$ for example, the following sequence is obtained:

$$\underbrace{15, 11, 23, 19, 31, 27, 7, 3}_{\text{period}}, 15, 11, 23, 19, 31, 27, 7, \ldots,$$

which also has maximal period length 8, as expected. On the other hand, we see that the generator:

$$x_0 = 5, \qquad x_{i+1} \equiv 9x_i \pmod{16},$$

produces the sequence

$$\underbrace{5, 13, 21, 29}_{\text{period}}, 5, 13, 21, 29, 5, 13, 21, 29, \ldots$$

In this case, maximal period length 8 is not reached since the multiplier is $9 \equiv 1 \pmod 8 \not\equiv 3 \text{ or } 5 \pmod 8$. □

2.3 Some Remarks

Numerous theoretical results on the structural and statistical properties of linear congruential pseudorandom numbers are covered in quite some detail by Niederreiter's articles [Nie77, Nie78, Nie85]. These results indicate that, with a judicious choice of multiplier and increment, linear congruential sequences display reasonably acceptable random behaviour.

It is well known (see such articles as [Mar68, Mar70, BRW71, Bey72, Mar72]) that n-tuple vectors (points) of n consecutive terms of the normalized linear congruential pseudorandom number sequence $\{u_i\}$ form a lattice in the n-dimensional unit cube $[0,1]^n$, and the n-dimensional volume of a unit cell of the lattice is $1/m$ if $\{u_i\}$ has full period length m. However, according to Marsaglia [Mar68], this property should be regarded as defect, stemming from the simple nature of the underlying *linear* recursion, since such a coarse lattice structure implies several undesirable regularities. Unfortunately, this inherent deficiency cannot be removed by even the most prudent choice of parameters. Consequently, for simulations requiring random irregularites (such as Monte Carlo simulations), points in n-space produced by linear congruential generators are too regular, rendering linear congruential pseudorandom numbers useless. In particular, for the pure multiplicative congruential generator, this regularity was established in Marsaglia's famous paper [Mar68] by showing that all the points lie in a relatively small number of parallel hyperplanes.

Although conceptual simplicity and computing ease have allowed linear congruential generators to dominate the field of pseudorandom number generation, deficiencies such as this coarse lattice structure, prompted the development of new methods. Specifically, k^{th}-order linear recurrence generators and non-linear congruential generators, which do not exhibit this non-random behaviour, but may still yield full/maximal period length sequences. Such alternative methods will be the focus of Chapters 3 to 5.

Chapter 3

k^{th}-order Linear Recurrence Generators

3.1 The General k^{th}-order Linear Recursion Method

Our discussion now turns to a generalization of the (first-order) method of Chapter 2 to the k^{th}-order linear recursion method. The fact that this method can produce sequences of period lengths as large as $m^k - 1$, in comparison to $m - 1$, is just one major factor that accounts for the appeal of this type of generator. On occasions when it is desirable to seek a longer period, this very method suggests itself as a useful source of pseudorandom numbers.

Let k be a positive integer. The **k^{th}-order linear recursion method** generates a *k^{th}-order linear recurring sequence* $\{x_i\}_{i \geq 0}$ of pseudorandom numbers by the linear recurrence relation

$$\boxed{x_{i+k} \equiv a_{k-1}x_{i+k-1} + a_{k-2}x_{i+k-2} + \cdots + a_0 x_i \pmod{m}, \qquad \text{for } i = 0, 1, 2, \ldots} \quad (3.1)$$

where *coefficients* $a_0, \ldots, a_{k-1} \in \mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, and *modulus* m is a positive integer. Clearly, the period length of $\{x_i\}$ is at most $m^k - 1$ since there are exactly m^k distinct k-tuples consisting of elements in $\mathbb{Z}_m$ and $(0, \ldots, 0)$ is excluded. If $(0, \ldots, 0)$ were allowed, the generator would eventually produce an infinite sequence of zeros.

The sole objective of this chapter is to establish the conditions under which a k^{th}-order linear recurring sequence $\{x_i\}$ attains maximum possible period length $m^k - 1$. This is only possible if the modulus m is a prime, in which case we may use the theory of finite fields (see Appendix B for some background material). When $m = p$ is prime, we will see it is possible to find coefficients $a_1, a_2, \ldots, a_k$ such that the sequence $\{x_i\}$ has

period length $p^k - 1$. In fact, it will be established that the coefficients have the desired property if the polynomial

$$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_0$$

is a *primitive polynomial modulo p*; that is, if this polynomial has a root that is a *primitive element* of the field with p^k elements. We now proceed to show this by first generalizing (3.1) to a k^{th}-order linear recurrence generator which produces sequences in a finite field with $q = p^n$ elements.

We shall henceforth assume that the modulus $m = p$ for some prime p, so that $\mathbb{Z}_p$ is a finite field of order p (see Theorem B.1).

3.2 Linear Recurring Sequences Over $GF(q)$

Of particular importance in a variety of applications are sequences over finite fields. From a computational viewpoint, the ease with which such sequences are generated by recursive procedures is certainly an advantageous feature. Specifically, linear recurring sequences (where each term depends linearly on a fixed number of predecessors) are useful in such areas as coding theory and electrical engineering. For such applications, sequences are often generated over the finite field of order 2, but in this section we shall generalize to any finite field of order $q = p^n \geq 3$, where p is a prime and n is a positive integer. The case $q = 2$ will be dealt with in a slightly different manner when we investigate shift register generators in Chapter 4.

It is a familiar fact that for every prime p, and every positive integer n, there exists a finite field with $q = p^n$ elements. Furthermore, any two finite fields with $q = p^n$ elements are isomorphic. (See [Fra94], for example).

Definition 3.2.1. *The finite field with $q = p^n$ elements, where p is a prime and $n \in \mathbb{Z}^+$, is called the* ***Galois Field of order*** *q, denoted $GF(q)$. Any finite field with $q = p^n$ elements is isomorphic to $GF(q)$.*

Notation. In what follows, we shall denote a field by $\mathbb{F}$ and the finite field with q elements (or the *Galois Field* of order q) by $\mathbb{F}_q$, so that $GF(q) = \mathbb{F}_q$. Moreover, $\mathbb{F}_q^*$ will denote the multiplicative group $\mathbb{F}_q \backslash \{0\}$. Also, note that Definition 3.2.1 implies we can identify the finite field $\mathbb{Z}_p$ with $\mathbb{F}_p$ so that we may assume $\mathbb{F}_p \cong \{0, 1, 2, \ldots, p-1\}$, where p is a prime.

Consequently, the k^{th}-order linear recurrence generator (3.1), with modulus $m = p$, is

equivalent to

$$x_{i+k} = a_{k-1}x_{i+k-1} + a_{k-2}x_{i+k-2} + \cdots + a_0 x_i, \qquad i = 0, 1, 2, \ldots, \tag{3.2}$$

where each $x_i,\ a_j \in \mathbb{F}_p$. However, we shall further generalize to a k^{th}**-order linear recurrence generator over** $\mathbb{F}_q$ defined by

$$\boxed{x_{i+k} = a_{k-1}x_{i+k-1} + a_{k-2}x_{i+k-2} + \cdots + a_0 x_i, \quad x_i, a_j \in \mathbb{F}_q} \tag{3.3}$$

for $i = 0, 1, \ldots$ Such a generator is said to produce a k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$.

It is evident, from recursion (3.3), that for fixed coefficients $a_j \in \mathbb{F}_q$, each x_i is completely determined by the k-tuple $\mathbf{x}_i = (x_i, x_{i+1}, \ldots, x_{i+k-1})$ of terms preceding it, called the i^{th} *state vector* of the sequence. Similarly, x_{i+1} is completely determined by the k-tuple $\mathbf{x}_{i+1} = (x_{i+1}, x_{i+2}, \ldots, x_{i+k})$. Thus, each state vector has a unique successor governed by recurrence relation (3.3), and so the period length of the sequence $\{x_i\}$ is clearly equal to the period length of the succession of state vectors. Of course, if it ever happens that a state vector is the 'zero' k-tuple, then all subsequent state vectors will be zero vectors, and hence the sequence $\{x_i\}$ degenerates to zero.

Note that the terms $x_0, x_1, \ldots, x_{k-1}$, which uniquely determine the rest of the sequence $\{x_i\}_{i\geq 0}$, are referred to as the *initial values*; whence, the k-tuple $\mathbf{x}_0 = (x_0, x_1, \ldots, x_{k-1})$ is naturally called the *initial state vector* of the sequence.

3.2.1 Periodicity Properties

Theorem 3.2.1. *Every k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ is ultimately periodic with least period length d such that $d \leq q^k - 1$.*

Proof. Consider the i^{th} state vector of the sequence $\{x_i\}$; that is, the k-tuple $\mathbf{x}_i = (x_i, x_{i+1}, \ldots, x_{i+k-1})$. Each x_j of this k-tuple is an element of $\mathbb{F}_q$, which consists of q elements. Hence, excluding the zero k-tuple, there are exactly $q^k - 1$ distinct k-tuples of elements in $\mathbb{F}_q$. By considering the different possible state vectors (excluding the zero vector) of the sequence $\{x_i\}$; namely, $\mathbf{x}_n$, $0 \leq n \leq q^k - 1$, it follows that $\mathbf{x}_l = \mathbf{x}_j$ for some j and l with $0 \leq j < l \leq q^k - 1$. Now, using linear recurrence relation (3.3) and mathematical induction on i, it may be readily shown that $\mathbf{x}_{i+l-j} = \mathbf{x}_i$ for all $i \geq j$, which implies that the succession of state vectors is ultimately periodic with least period length $d \leq l - j \leq q^k - 1$. Thus, by the remarks preceding this theorem, it follows that the k^{th}-order linear recurring sequence $\{x_i\}$ must itself be ultimately periodic with least

period length $d \leq l-j \leq q^k-1$. If the zero k-tuple occurs as one of the state vectors, then all subsequent state vectors are zero vectors, and the sequence $\{x_i\}$ degenerates to zero. In this case, the sequence is ultimately periodic with least period length $d = 1 \leq q^k - 1$, completing the proof. □

Theorem 3.2.1 shows that any k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ is ultimately periodic with least period length at most $q^k - 1$. If $\{x_i\}$ has least period length equal to $q^k - 1$, we say the sequence has *maximal period length.*

It is not difficult to construct an example of a first-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ that achieves maximal period length $q - 1$. We first note that the multiplicative group $\mathbb{F}_q^*$ of non-zero elements of $\mathbb{F}_q$ is *cyclic* (see Definition B.1 and Theorem B.2), and define the concept of a *primitive element* of $\mathbb{F}_q$.

Definition 3.2.2. *A generator α of $\mathbb{F}_q^*$ is called a* ***primitive element*** *of $\mathbb{F}_q$. For such an α in $\mathbb{F}_q$, we have $\mathbb{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.*

Having now defined a primitive element of $\mathbb{F}_q$, we provide the aforementioned example.

Example 3.2.1. Suppose α is a primitive element of $\mathbb{F}_q$, and consider the first-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ satisfying $x_{i+1} = \alpha x_i$ for $i = 0, 1, 2, \ldots$, with $x_0 \neq 0$. The terms of such a sequence are clearly given by $x_n = \alpha^n x_0$ for $n = 0, 1, 2, \ldots$ Hence, we obtain the sequence

$$x_0,\ \alpha x_0,\ \alpha^2 x_0,\ \ldots,\ \alpha^{q-1} x_0,\ x_0,\ \alpha x_0, \ldots$$

with least period length $q-1$, which shows that the upper-bound for d in Theorem 3.2.1 may be attained. Later, it will be shown that for any $k \geq 1$, and in any $\mathbb{F}_q$, there exist k^{th}-order linear recurring sequences with least period length $d = q^k - 1$ (see Theorem 3.2.9 to follow). □

Note that a linear recurring sequence over $\mathbb{F}_q$ will be ultimately periodic, but not necessarily purely periodic. As evidence of this fact, the second-order linear recurring sequence $\{x_i\}_{i \geq 0}$ over $\mathbb{F}_q$ defined by $x_{i+2} = x_{i+1}$, with $x_0 \neq x_1$ (and $a_0 = 0$), is clearly ultimately periodic. Indeed, we obtain the sequence $x_0, x_1, x_1, x_1, \ldots$, where x_0 is the pre-period. It is decidedly more convenient to deal with purely periodic sequences, and so we give a sufficient condition for the pure periodicity of a linear recurring sequence.

Theorem 3.2.2. *If $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$, generated by recursion* (3.3) *with coefficient $a_0 \neq 0$, then the sequence is purely periodic.*

Proof. We know by Theorem 3.2.1 that the sequence $\{x_i\}$ is ultimately periodic, with least period length d and a pre-period length i_0, so that $x_{i+d} = x_i$ for all $i \geq i_0$.
Suppose that the sequence is not purely periodic; that is, suppose $i_0 \geq 1$. Then using recursion (3.3), with $i = i_0 - 1 + d$ and $a_0 \neq 0$, gives

$$x_{i_0-1+k+d} = a_{k-1}x_{i_0+k-2+d} + a_{k-2}x_{i_0+k-3+d} + \cdots a_1 x_{i_0+d} + a_0 x_{i_0-1+d}.$$

Therefore,

$$\begin{aligned} x_{i_0-1+d} &= a_0^{-1}(x_{i_0+d-1} - a_{k-1}x_{i_0+d+k-2} - a_{k-2}x_{i_0+d+k-3} - \cdots - a_1 x_{i_0+d}) \\ &= a_0^{-1}(x_{i_0+k-1} - a_{k-1}x_{i_0+k-2} - -a_{k-2}x_{i_0+k-3} - \cdots - a_1 x_{i_0}). \end{aligned} \tag{3.4}$$

Similarly, using (3.3) with $i = i_0 - 1$, we obtain

$$x_{i_0-1} = a_0^{-1}(x_{i_0+k-1} - a_{k-1}x_{i_0+k-2} - \cdots - a_1 x_{i_0}). \tag{3.5}$$

Hence, from equations (3.4) and (3.5), we have $x_{i_0-1+d} = x_{i_0-1}$; a contradiction to the definition of pre-period length i_0 since $i_0 - 1 < i_0$. □

Without loss of generality, we shall henceforth assume that a k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ is purely periodic by taking $a_0 \neq 0$.

3.2.2 Associated $k \times k$ Matrix

In this section, we define the *associated matrix* of a linear recurring sequence, and show how it relates to the least period length of the sequence.

A k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ has an associated $k \times k$ matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix} \tag{3.6}$$

where 0 and 1 are the respective additive and multiplicative identities of $\mathbb{F}_q$. Notice that the matrix $\mathbf{A}$ depends only on the linear recurrence relation generating the given sequence. Also note that if $k = 1$, $\mathbf{A}$ is considered to be the 1×1 matrix (a_0).

If one considers the i^{th} state vector $\mathbf{x}_i = (x_i, x_{i+1}, \ldots, x_{i+k-1})$ then

$$\begin{aligned}
\mathbf{x}_i\mathbf{A} &= (x_i, x_{i+1}, \ldots, x_{i+k-1}) \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix} \\
&= (x_{i+1}, x_{i+2}, \ldots, x_{i+k-1}, a_0x_i + a_1x_{i+1} + a_2x_{i+2} + \cdots + a_{k-1}x_{i+k-1}) \\
&= (x_{i+1}, x_{i+2}, \ldots, x_{i+k-1}, x_{i+k}) \\
&= \mathbf{x}_{i+1}.
\end{aligned}$$

Hence, $\mathbf{x}_{i+1} = \mathbf{x}_i\mathbf{A}$ for all $i \geq 0$.

Lemma 3.2.1. *Suppose $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$, with associated $k \times k$ matrix $\mathbf{A}$. Then the state vectors $\mathbf{x}_i$ are such that*

$$\mathbf{x}_i = \mathbf{x}_0\mathbf{A}^i \quad \textit{for all} \quad i = 0, 1, 2, \ldots \tag{3.7}$$

Proof. We proceed by induction on i. The result is trivially true for $i = 0$.
It has already been verified that

$$\mathbf{x}_{i+1} = \mathbf{x}_i\mathbf{A} \quad \text{for all } i \geq 0. \tag{3.8}$$

Assume the result holds for the $(i-1)^{st}$ state vector, $\mathbf{x}_{i-1}$, so that $\mathbf{x}_{i-1} = \mathbf{x}_0\mathbf{A}^{i-1}$, and consider the i^{th} state vector, $\mathbf{x}_i$. By (3.8), $\mathbf{x}_i = \mathbf{x}_{i-1}\mathbf{A}$ for all $i \geq 1$ and, using the inductive hypothesis, we have $\mathbf{x}_i = \mathbf{x}_0\mathbf{A}^{i-1}\mathbf{A} = \mathbf{x}_0\mathbf{A}^i$ for all $i \geq 0$. Thus, by mathematical induction, the lemma is proved. □

Definition 3.2.3. *The set of all non-singular $k \times k$ matrices with entries in $\mathbb{F}_q$ forms a finite group under matrix multiplication called the* ***general linear group****, denoted $GL(k, \mathbb{F}_q)$ or $GL(k, q)$.*

Observe that the associated matrix $\mathbf{A}$ from (3.6) is indeed an element of $GL(k, q)$ since it is a $k \times k$ matrix with entries in $\mathbb{F}_q$ and $det(\mathbf{A}) = (-1)^{k-1}a_0 \neq 0$, so that $\mathbf{A}$ is non-singular. The order of this matrix in $GL(k, q)$ has some significance since it relates to the least period length of the corresponding sequence.

Theorem 3.2.3. *If $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$, generated by (3.3) with coefficient $a_0 \neq 0$, then the least period length of the sequence divides the order of the associated matrix $\mathbf{A}$ in $GL(k, q)$.*

Proof. Suppose $\mathbf{A}$ has order n in $GL(k,q)$. Then n is the smallest positive integer such that $\mathbf{A}^n = \mathbf{I}$ in $GL(k,q)$ (where $\mathbf{I}$ is the $k \times k$ identity matrix over $\mathbb{F}_q$). So, by Lemma 3.2.1, $\mathbf{x}_{i+n} = \mathbf{x}_0\mathbf{A}^{i+n} = \mathbf{x}_0\mathbf{A}^i = \mathbf{x}_i$ for all $i \geq 0$. Therefore, n is a period length of the purely periodic sequence $\{x_i\}$. Hence, by Lemma 1.2.1, the least period length of the sequence divides n. □

Definition 3.2.4. *A k^{th}-order impulse response sequence over $\mathbb{F}_q$ is a k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$, which is uniquely determined by its initial state vector $\mathbf{x}_0 = (0, 0, \ldots, 0, 1)$; that is, initial values $x_0 = x_1 = \cdots = x_{k-2} = 0$, $x_{k-1} = 1$. If $k = 1$ then $x_0 = 1$.*

Such a k^{th}-order linear recurring sequence is of particular interest since, as we shall see later, it may attain maximal period length $q^k - 1$ under a specific necessary and sufficient condition.

Example 3.2.2. Consider a fourth-order linear recurring sequence $\{x_i\}_{i\geq 0}$ over $\mathbb{F}_3 \cong \mathbb{Z}_3 \cong \{-1, 0, 1\}$ defined by

$$x_{i+4} = x_{i+3} - x_{i+2} + x_i,$$

with associated 4×4 matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

of order 24 in $GL(4,3)$. With an initial state vector $x_0 = (-1, 0, 0, 1)$, the generated sequence is

$$\underbrace{-1, 0, 0, 1, 0, -1, -1, 1}_{\text{period}}, -1, 0, 0, 1, 0, \ldots$$

of least period length 8 which divides 24, as expected by Theorem 3.2.3. Furthermore, the corresponding impulse response sequence is

$$\underbrace{0, 0, 0, 1, 1, 0, -1, 0, -1, -1, -1, 0, 0, -1, 1, -1, 1, 1, 1, -1, -1, 1, 0, 1}_{\text{period}}, 0, 0, 0, 1, 1, 0, \ldots$$

of least period length 24 which is equal to the order of $\mathbf{A}$ in $GL(4,3)$; thus illustrating Theorem 3.2.4 (to follow). □

Lemma 3.2.2. *Suppose $\{x_i\}$ is a k^{th}-order impulse response sequence over $\mathbb{F}_q$ with associated matrix $\mathbf{A}$. Then two distinct state vectors $\mathbf{x}_m$ and $\mathbf{x}_n$ are equal if and only if $\mathbf{A}^m = \mathbf{A}^n$.*

Proof. If $\mathbf{A}^m = \mathbf{A}^n$ then it is immediately evident, from Lemma 3.2.1, that $\mathbf{x}_m = \mathbf{x}_n$. Conversely, suppose $\mathbf{x}_m = \mathbf{x}_n$. Then, by way of linear recursion (3.3), we find that $\mathbf{x}_{m+l} = \mathbf{x}_{n+l}$ for all $l \geq 0$. Applying Lemma 3.2.1, we obtain $\mathbf{x}_l\mathbf{A}^m = \mathbf{x}_l\mathbf{A}^n$ for all $l \geq 0$. Further, since state vectors $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{k-1}$ must actually form a basis for $\mathbb{F}_q^k$ as a k-dimensional vector space over $\mathbb{F}_q$, then it follows that $\mathbf{A}^m = \mathbf{A}^n$. □

Theorem 3.2.4. *Suppose $\{x_i\}$ is a k^{th}-order impulse response sequence over $\mathbb{F}_q$, generated by* (3.3) *with coefficient $a_0 \neq 0$. Then the least period length of the sequence is equal to the order of its associated matrix $\mathbf{A}$ in $GL(k, q)$.*

Proof. It is deduced from Theorem 3.2.3 that if this sequence $\{x_i\}$ has least period length d then d divides the order of $\mathbf{A}$ in $GL(k, q)$. Moreover, by Theorem 3.2.2, we have $\mathbf{x}_d = \mathbf{x}_0$; thus, Lemma 3.2.2 implies $\mathbf{A}^d = \mathbf{A}^0 = \mathbf{I}$, which gives the desired result. □

Hence, it is favourable to use a k^{th}-order impulse response sequence with coefficients such that the corresponding sequence $\{x_i\}$ has associated matrix $\mathbf{A}$ of order $q^k - 1$ in $GL(k, q)$. However, determining such a matrix $\mathbf{A}$ is somewhat difficult and so we require more refined conditions such that maximal period length $q^k - 1$ is attained. We must therefore delve into some further results concerning the associated $k \times k$ matrix $\mathbf{A}$. In order to do this, however, we must first define a *characteristic polynomial*, and state some related definitions and results in finite field theory pertaining to polynomials.

3.2.3 Characteristic Polynomial and Companion Matrix

Definition 3.2.5. *A k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ has* ***characteristic polynomial*** *$f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1x - a_0 \in \mathbb{F}_q[x]$. The polynomial $f^*(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \cdots - a_1x^{k-1} - a_0x^k \in \mathbb{F}_q[x]$ is called the* ***reciprocal characteristic polynomial*** *of $\{x_i\}$ and is derived from $f(x)$ by $f^*(x) = x^k f(1/x)$.*

Evidently, the characteristic polynomial of a sequence depends only on the linear recurrence relation by which it is defined.

Note. The characteristic polynomial, as defined above, is *monic* since it has leading coefficient 1.

Example 3.2.3. The characteristic polynomial corresponding to the fourth-order linear recurrence generator of Example 3.2.2 is $f(x) = x^4 - x^3 + x^2 - 1 \in \mathbb{F}_3[x]$. □

Definition 3.2.6. *The* ***companion matrix*** *of a monic polynomial* $g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{k-1}x^{k-1} + x^k \in \mathbb{F}_q[x]$ *of degree* $k \geq 1$ *is a* $k \times k$ *matrix* $\mathbf{M} \in GL(k, q)$ *with* ***characteristic polynomial*** $\varphi(\lambda) = |\lambda\mathbf{I} - \mathbf{M}| = c_0 + c_1\lambda + c_2\lambda^2 + \cdots + c_{k-1}\lambda^{k-1} + \lambda^k = g(\lambda)$.

Using *cofactor expansion*, it can be verified that the associated matrix $\mathbf{A}$, of a k^{th}-order linear recurring sequence $\{x_i\}$, given by

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix}$$

has characteristic polynomial $\varphi(\lambda) = |\lambda\mathbf{I} - \mathbf{A}| = \lambda^k - a_{k-1}\lambda^{k-1} - a_{k-2}\lambda^{k-2} - \cdots - a_1\lambda - a_0$. Thus, we have $\varphi(\lambda) = f(\lambda)$, where $f \in \mathbb{F}_q[x]$ is the characteristic polynomial of $\{x_i\}$. Hence, in view of Definition 3.2.6, the associated matrix $\mathbf{A}$ of $\{x_i\}$ is the companion matrix of f.

A well known theorem in linear algebra (the *Cayley-Hamilton Theorem*) asserts that $\mathbf{A}$ satisfies its own *characteristic equation* $\varphi(\lambda) = 0$ so that $\varphi(\mathbf{A}) = 0$, and hence $f(\mathbf{A}) = 0$, in this case. Moreover, the *minimal polynomial* of the $k \times k$ matrix $\mathbf{A}$ is defined to be the monic polynomial $m(x) \in \mathbb{F}_q[x]$ of least degree ≥ 1 for which $m(\mathbf{A}) = 0$. It is easily proved that f is the minimal polynomial of $\mathbf{A}$, as follows.

Lemma 3.2.3. *Suppose* $\{x_i\}$ *is a* k^{th}*-order linear recurring sequence over* $\mathbb{F}_q$ *with characteristic polynomial* $f \in \mathbb{F}_q[x]$ *and associated* $k \times k$ *matrix* $\mathbf{A}$*. Then* f *is the minimal polynomial of* $\mathbf{A}$*.*

Proof. Let $r_1((\mathbf{A}^t)^j)$ denote the first row of the matrix $(\mathbf{A}^t)^j$, where $\mathbf{A}^t$ is the transpose of the matrix $\mathbf{A}$. By a direct computation, it follows that

$$\begin{aligned} r_1((\mathbf{A}^t)^0) &= [1\ 0\ 0\ 0 \cdots\ 0], \\ r_1(\mathbf{A}^t) &= [0\ 1\ 0\ 0 \cdots\ 0], \\ r_1((\mathbf{A}^t)^2) &= [0\ 0\ 1\ 0 \cdots\ 0], \\ &\vdots \\ r_1((\mathbf{A}^t)^{k-1}) &= [0\ 0\ 0\ 0 \cdots\ 1]. \end{aligned}$$

Suppose $g(x) \in \mathbb{F}_q[x]$ is the minimal polynomial of $\mathbf{A}$. If $g(x) \neq f(x)$ then since $f(\mathbf{A}) = 0$, the degree of g is at most $k - 1$. If $g(\mathbf{A}) = \sum_{j=0}^{k-1} c_j\mathbf{A}^j = 0$, it follows from the

properties of the transpose of a matrix that $\sum_{j=0}^{k-1} c_j(\mathbf{A}^t)^j = 0$, and therefore $g(\mathbf{A}^t) = 0$. But the linear independence of the vectors $r_1((\mathbf{A}^t)^j)$, $j = 0, 1, \ldots, k-1$, implies that all $c_j = 0$; a contradiction. Thus, $g(x) = f(x)$. □

The next lemma naturally follows from Lemma 3.2.3, and will be used in the proof of our next result.

Lemma 3.2.4. *Suppose $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$ with characteristic polynomial $f \in \mathbb{F}_q[x]$ and associated $k \times k$ matrix $\mathbf{A}$. Then f divides a non-zero polynomial $g \in \mathbb{F}_q[x]$ if and only if $g(\mathbf{A}) = 0$.*

Proof. Suppose f divides a non-zero polynomial $g \in \mathbb{F}_q[x]$. Then $g(x) = f(x)q(x)$ for some polynomial $q \in \mathbb{F}_q[x]$, and since $f(\mathbf{A}) = 0$ then $g(\mathbf{A}) = f(\mathbf{A})q(\mathbf{A}) = 0$. Conversely, let g be a polynomial in $\mathbb{F}_q[x]$ of degree greater than f with $g(\mathbf{A}) = 0$. Suppose f does not divide g. Then, by the *Division Algorithm in* $\mathbb{F}_q[x]$ (Theorem B.3), there exist polynomials $q, r \in \mathbb{F}_q[x]$ such that $g(x) = f(x)q(x) + r(x)$ where $deg(r) < deg(f)$. Now, $g(\mathbf{A}) = f(\mathbf{A})q(\mathbf{A}) + r(\mathbf{A})$ and so $g(\mathbf{A}) = f(\mathbf{A}) = 0$ implies $r(\mathbf{A}) = 0$ with $deg(r) < deg(f)$. We therefore obtain a contradiction to the fact that f is the minimal polynomial for $\mathbf{A}$. Hence, f divides g. □

So as to establish some more results, it is necessary to define the *order* of a polynomial in $\mathbb{F}_q[x]$. It is known that for any polynomial $f \in \mathbb{F}_q[x]$ of degree $k \geq 1$, with $f(0) \neq 0$, there exists a positive integer $e \leq q^k - 1$ such that $f(x)$ divides $x^e - 1$ (see Lemma B.1). Since a non-zero constant polynomial divides $x - 1$, we include such polynomials in the following definition.

Definition 3.2.7. *Let $f \in \mathbb{F}_q[x]$ be a non-zero polynomial.*

- ◇ *If $f(0) \neq 0$, then the smallest positive integer e such that $f(x)$ divides $x^e - 1$ is called the* ***order*** *of f, denoted $ord(f)$.*
- ◇ *If $f(0) = 0$ then $f(x) = x^h g(x)$ for some uniquely determined $h \in \mathbb{Z}^+$; $g \in \mathbb{F}_q[x]$ with $g(0) \neq 0$, and we define $ord(f) = ord(g)$.*

We now give an interpretation of $ord(f)$.

Lemma 3.2.5. *Suppose $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$ with characteristic polynomial $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$. Then $ord(f)$ is equal to the order of the associated matrix $\mathbf{A}$ in $GL(k, q)$.*

Proof. By Lemma 3.2.4, $f(x)$ divides $x^e - 1$ (where e is a positive integer) if and only if $\mathbf{A}^e - \mathbf{I} = 0$. That is, $\mathbf{A}^e = \mathbf{I}$ for some $e \in \mathbb{Z}^+$ if and only if $f(x)$ divides $x^e - 1$. Hence, from the definitions of $ord(f)$ and the order of $\mathbf{A}$, the result is proved. □

The above lemma leads to the following important theorem, which relates the order of a characteristic polynomial to the period length of the corresponding linear recurring sequence.

Theorem 3.2.5. *Suppose $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$ with characteristic polynomial $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$. Then the least period length of the sequence divides $ord(f)$, and the least period length of the corresponding impulse response sequence is equal to $ord(f)$. Furthermore, both sequences are a purely periodic.*

Proof. Due to Lemma 3.2.5, this result is basically a restatement of Theorems 3.2.3 and 3.2.4. It follows from Theorem 3.2.2 that both sequences are indeed purely periodic since $f(0) \neq 0$ implies that the coefficient $a_0 \neq 0$. □

Example 3.2.4. As we have seen, the characteristic polynomial of Example 3.2.2 is the *reducible* characteristic polynomial $f(x) = x^4 - x^3 + x^2 - 1 = (x^2 + x + 1)(x - 1)^2 \in \mathbb{F}_3[x]$. It can be easily verified that $f(x)$ divides $x^{24} - 1$ and no polynomial $x^e - 1$ with $0 < e < 24$, so that $ord(f) = 24$, which is the order of the associated matrix $\mathbf{A}$ in $GL(4, 3)$ (see Example 3.2.2). With an initial state vector $(-1, 0, 0, 1)$, we saw that the corresponding sequence is purely periodic of least period length 8, which certainly divides $ord(f)$. Also, the corresponding impulse response sequence was seen to be purely periodic with least period length $24 = ord(f)$, as expected. □

Lidl and Niederreiter [LN97] determined a polynomial identity in terms of a linear recurring sequence and its characteristic polynomial. We now provide this result, and ask that the reader excuse the unfortunate notation with x_i a term of the sequence and x the indeterminate of a polynomial.

Theorem 3.2.6. *Suppose $\{x_i\}$ is a purely periodic k^{th}-order linear recurring sequence over $\mathbb{F}_q$ with least period length d and characteristic polynomial $f \in \mathbb{F}_q[x]$. Then the polynomial identity*

$$f(x)g(x) = (1 - x^d)h(x) \tag{3.9}$$

holds where

$$g(x) = x_0 x^{d-1} + x_1 x^{d-2} + \cdots + x_{d-2}x + x_{d-1} \in \mathbb{F}_q[x],$$
$$h(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} a_{i+j+1} x_i x^j \in \mathbb{F}_q[x],$$

and we set $a_k = -1$.

Proof. This proof follows that of Lidl and Niederreiter [LN97]. We simply compare coefficients on both sides of identity (3.9).

For $0 \leq l \leq k+d-1$, suppose c_l and d_l are the coefficients of x^l on the respective left-hand and right-hand sides of (3.9). Setting $a_k = -1$, the characteristic polynomial of the given sequence may be written as $f(x) = -\sum_{j=0}^{k} a_j x^j \in \mathbb{F}_q[x]$. It then follows, by multiplication of polynomials in $\mathbb{F}_q[x]$, that the coefficient of x^l on the left-hand side of (3.9) is given by

$$c_l = -\sum_{\substack{0 \leq i \leq k,\ 0 \leq j \leq d-1 \\ i+j=l}} a_i x_{d-1-j} \qquad \text{for } 0 \leq l \leq k+d-1. \tag{3.10}$$

Also observe that the given purely periodic sequence $\{x_i\}$ in $\mathbb{F}_q$ satisfies the linear recurrence relation

$$x_{i+k} = a_{k-1}x_{i+k-1} + a_{k-2}x_{i+k-2} + \cdots + a_0 x_i \qquad \text{for } i = 0, 1, 2, \ldots,$$

which can alternatively be written as

$$\sum_{j=0}^{k} a_j x_{i+j} = 0 \qquad \text{for all } i \geq 0. \tag{3.11}$$

We may now distinguish four different cases.

(1) If $k \leq l \leq d$, then by (3.10) and (3.11),

$$c_l = -\sum_{j=0}^{k} a_j x_{d-1-l+j} = 0 = d_l.$$

(2) If $l \leq d-1$ and $l < k$, then it follows from (3.10), (3.11), and the periodicity of the given sequence, that

$$\begin{aligned} c_l &= -\sum_{j=0}^{l} a_j x_{d-1-l+j} = \sum_{j=l+1}^{k} a_j x_{d-1-l+j} \\ &= \sum_{j=l+1}^{k} a_j x_{j-l-1} = \sum_{j=0}^{k-1-l} a_{j+l+1} x_j = d_l. \end{aligned}$$

(3) If $l \geq d$ and $l \geq k$, then the following is derived from (3.10):

$$c_l = -\sum_{j=l-d+1}^{k} a_j x_{d-1-l+j} = -\sum_{j=0}^{k-1-l+d} a_{j+l-d+1} x_j = d_l.$$

(4) If $d \leq l < k$, then again using (3.10) and the periodicity of the given sequence, we find

$$\begin{aligned} c_l &= -\sum_{j=l-d+1}^{l} a_j x_{d-1-l+j} = -\sum_{j=0}^{d-1} a_{j+l-d+1} x_j \\ &= \sum_{j=d}^{k-1-l+d} a_{j+l-d+1} x_j - \sum_{j=0}^{k-1-l+d} a_{j+l-d+1} x_j \\ &= \sum_{j=0}^{k-1-l} a_{j+l+1} x_{j+d} - \sum_{j=0}^{k-1-l+d} a_{j+l-d+1} x_j \\ &= \sum_{j=0}^{k-1-l} a_{j+l+1} x_j - \sum_{j=0}^{k-1-l+d} a_{j+l-d+1} x_j = d_l. \end{aligned}$$

Thus, it has been verified that the polynomial identity (3.9) holds. □

Our next theorem shows that in order for a linear recurring sequence to achieve a least period length *equal* to $ord(f)$, it is sufficient that its characteristic polynomial $f \in \mathbb{F}_q[x]$ be *irreducible*.

Theorem 3.2.7. *Suppose $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$ with non-zero initial state vector and irreducible characteristic polynomial $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$. Then the sequence is purely periodic with least period length equal to $ord(f)$.*

Proof. By Theorem 3.2.5, $\{x_i\}$ is purely periodic and its least period length d divides $ord(f)$. Further, one deduces from identity (3.9) of Theorem 3.2.6, that $f(x)$ divides $(x^d - 1)h(x) \in \mathbb{F}_q[x]$ since $f(x)s(x) = (1 - x^d)h(x)$, where $s(x)$ (and hence $h(x)$) is a non-zero polynomial in $\mathbb{F}_q[x]$. Thus, $deg(h) < deg(f)$ and so, by the irreducibility of f, $f(x)$ must divide $x^d - 1$. Hence, by Definition 3.2.8, $d \geq ord(f)$. But, $d \leq ord(f)$ since d divides $ord(f)$, and therefore $d = ord(f)$. □

Example 3.2.5. Consider the fourth-order linear recurring sequence $\{x_i\}_{i\geq 0}$ over $\mathbb{F}_3 \cong \mathbb{Z}_3 \cong \{-1, 0, 1\}$ defined by

$$x_{i+4} = x_{i+2} + x_i.$$

The associated 4×4 matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \in GL(4, 3)$$

has order 16, and the corresponding characteristic polynomial $f(x) = x^4 - x^2 - 1 \in \mathbb{F}_3[x]$ is irreducible over $\mathbb{F}_3$ with $ord(f) = 16$, as expected by Lemma 3.2.5. If we take $\mathbf{x}_0 = (1, 0, 1, 1)$ as the initial state vector, we arrive at the purely periodic sequence

$$\underbrace{1, 0, 1, 1, -1, 1, 0, -1, -1, 0, -1, -1, 1, -1, 0, 1}_{\text{period}}, 1, 0, 1, 1, -1, \ldots$$

of least period length $16 = ord(f)$, which demonstrates Theorem 3.2.7. □

3.2.4 Criterion For Maximal Period Length

Finally, after proving a whole host of results, we are now in the position to establish the chief result of this chapter, which gives a sufficient (but not necessary) condition for a k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_q$ to achieve maximal period length $q^k - 1$. However, we must first define the notion of a *primitive polynomial over* $\mathbb{F}_q$.

Definition 3.2.8. *A polynomial $f \in \mathbb{F}_q[x]$ of degree $k \geq 1$ is called a* ***primitive polynomial over*** $\mathbb{F}_q$ *if it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^k}$.*

The reader is referred to Theorem B.4 and Definition B.4 of Appendix B for the existence and definition of a minimal polynomial.

In light of Definition 3.2.8, we may consider a primitive polynomial of degree $k \geq 1$ over $\mathbb{F}_q$ to be a monic irreducible polynomial over $\mathbb{F}_q$ with a root $\alpha \in \mathbb{F}_{q^k}$ that generates the multiplicative group $\mathbb{F}_{q^k}^*$. We may further characterize a primitive polynomial via the next theorem.

Theorem 3.2.8. *A polynomial $f \in \mathbb{F}_q[x]$ of degree $k \geq 1$ is a primitive polynomial over $\mathbb{F}_q$ if and only if f is monic, $f(0) \neq 0$ and $ord(f) = q^k - 1$.*

Proof. The proof of this theorem requires the use of several results in finite field theory which will detract from the focus of this paper, so it is for this reason the proof is omitted. See [LN97]. □

Theorem 3.2.9. *Let $\{x_i\}$ be a k^{th}-order linear recurring sequence over $\mathbb{F}_q$ with non-zero initial state vector. If $\{x_i\}$ has a primitive characteristic polynomial $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$, then $\{x_i\}$ is purely periodic and attains maximal period length $q^k - 1$.*

Proof. Let $\{x_i\}$ be a k^{th}-order linear recurring sequence over $\mathbb{F}_q$ with non-zero initial state vector. Suppose the sequence $\{x_i\}$ has characteristic polynomial $f \in \mathbb{F}_q[x]$, which is a primitive polynomial over $\mathbb{F}_q$. Then, by the note following Definition 3.2.8, f is

certainly irreducible over $\mathbb{F}_q$, and Theorem 3.2.8 implies that $ord(f) = q^k - 1$ so that, by Theorem 3.2.7, the sequence $\{x_i\}$ is purely periodic with least period length equal to $q^k - 1$. □

Corollary 3.2.1. *Let $\{x_i\}$ be a k^{th}-order impulse response sequence over $\mathbb{F}_q$. Then $\{x_i\}$ is purely periodic and attains maximal period length $q^k - 1$ if and only if its characteristic polynomial $f \in \mathbb{F}_q[x]$, with $f(0) \neq 0$, is a primitive polynomial over $\mathbb{F}_q$.*

Proof. One may prove sufficiency as for Theorem 3.2.9.
To prove necessity, suppose $\{x_i\}$ has period length $q^k - 1$. Then, since $\{x_i\}$ has characteristic polynomial $f \in \mathbb{F}_q[x]$ of degree $k \geq 1$ (with $f(0) \neq 0$), it immediately follows from Theorem 3.2.5 that $q^k - 1 = ord(f)$. Therefore, Theorem 3.2.8 implies f is a primitive polynomial over $\mathbb{F}_q$. In addition, since $f(0) \neq 0$ implies $a_0 \neq 0$ then $\{x_i\}$ is purely periodic, according to Theorem 3.2.2. □

The two preceding results may be proved more readily for the case $q = 2$, as we will see in the analogous result – Theorem 4.1.3 of Chapter 4. In this particular situation, the use of a *generating function* will allow us to arrive at the desired result much sooner.

The next example illustrates both of the above theorems.

Example 3.2.6. Consider a third-order linear recurring sequence $\{x_i\}_{i\geq 0}$ over $\mathbb{F}_3 \cong \mathbb{Z}_3 \cong \{-1, 0, 1\}$ defined by

$$x_{i+3} = x_{i+1} - x_i.$$

If $\mathbf{x}_0 = (1, 1, 1)$ is taken as the initial state vector, then we obtain the purely periodic sequence

$$\underbrace{1, 1, 1, 0, 0, -1, 0, -1, 1, -1, -1, 1, 0, -1, -1, -1, 0, 0, 1, 0, 1, -1, 1, 1, -1, 0}_{\text{period}}, 1, 1, 1, 0, \ldots$$

with maximal period length $26 = 3^3 - 1$. Indeed, the corresponding characteristic polynomial $f(x) = x^3 - x + 1$ is primitive over $\mathbb{F}_3$. Moreover, the corresponding impulse response sequence is

$$\underbrace{0, 0, 1, 0, 1, -1, 1, 1, -1, 0, 1, 1, 1, 0, 0, -1, 0, -1, 1, -1, -1, 1, 0, -1, -1, -1}_{\text{period}}, 0, 0, 1, 0, 1, \ldots$$

of least period length 26, as it should be.
Note that the associated 3×3 matrix is given by

$$\mathbf{A} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \in GL(3, 3).$$

It is left to the reader to check that 26 is the smallest positive integer such that $\mathbf{A}^{26} \equiv \mathbf{I} \pmod 3$ so that $\mathbf{A}$ has order 26 in $GL(3,3)$. According to Lemma 3.2.5, this means that $ord(f) = 26 = 3^3 - 1$, which is certainly the case since f is primitive over $\mathbb{F}_3$. □

Of course, we would like to have k as large as possible (so that the period length is large), but its size is limited by two factors. Firstly, the initial state vector is a k-tuple (excluding the k-tuple $(0, \ldots, 0)$), which requires k memory locations in a computer – a limitation if a computer has only a small memory capacity. In light of Theorem 3.2.9, one would also like the characteristic polynomial of the generator to be a primitive polynomial over $\mathbb{F}_q$. So the second restriction arises when one attempts to determine a primitive polynomial (of degree k) over $\mathbb{F}_q$.

3.2.5 The Number of Primitive Polynomials

Definition 3.2.9. *The function $\mu : \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^r & \text{if } n = p_1 p_2 \ldots p_r, \text{ where the } p_i \text{ are distinct primes}; \\ 0 & \text{if } n \text{ has a squared factor} \end{cases}$$

is called the ***Möbius Function****.*

The number of monic irreducible polynomials of degree k over $\mathbb{F}_q$ is given by

$$\boxed{\psi_q(k) = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) q^d} \tag{3.12}$$

where this sum is over all positive divisors d of k.

Clearly, not every monic irreducible polynomial in $\mathbb{F}_q[x]$ is necessarily a primitive polynomial over $\mathbb{F}_q$. In fact, the number of primitive polynomials of degree k over $\mathbb{F}_q$ is

$$\boxed{\lambda_q(k) = \frac{\phi(q^k - 1)}{k}.} \tag{3.13}$$

For proofs of the above two results, a recommended reference is [LN97].

We now return to our original (and most practical) k^{th}-order linear recurrence generator defined by

$$x_{i+k} \equiv a_{k-1} x_{i+k-1} + a_{k-2} x_{i+k-2} + \cdots + a_0 x_i \pmod p, \quad \text{for } i = 0, 1, 2, \ldots \tag{3.14}$$

where $a_0, a_2, \ldots, a_{k-1} \in \mathbb{Z}_p$, and p is a prime. It has been determined that such a generator produces sequences of maximal period length $p^k - 1$ if the polynomial $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \cdots - a_1 x - a_0$ is a primitive polynomial modulo p. Of course, the mere fact that suitable coefficients $a_0, a_2, \ldots a_{k-1}$ exist giving a period length of $p^k - 1$ is not enough for practical purposes; we must be able to find them. Since p is usually chosen to be some large prime, it is infeasible to simply try all p^k possibilities. Fortunately, it follows from (3.13) that there are $\phi(p^k - 1)/k$ suitable choices of $(a_0, a_2, \ldots, a_{k-1})$, so there is a reasonably good chance of finding one after a few random tries. On the other hand, there exist efficient methods for testing the primitivity of polynomials over $\mathbb{F}_p$, as discussed by Alanen and Knuth [AK64].

3.2.6 Representation of the terms of the sequence $\{x_i\}$

Suppose the characteristic polynomial of a k^{th}-order linear recurring sequence $\{x_i\}$ is irreducible over $\mathbb{F}_q$. The following definition and theorem are stated mainly for interest, and the fact that they give a representation of the elements of the sequence $\{x_i\}$ in terms of a *trace* function; we will, however, make use of them in Section 5.3 of Chapter 5.

Definition 3.2.10. *For $k \geq 1$, the **trace** of an element $\alpha \in \mathbb{F}_{q^k}$ is defined as*

$$Tr(\alpha) = \sum_{j=0}^{k-1} \alpha^{q^j} = \alpha + \alpha^q + \cdots + \alpha^{q^{k-1}}.$$

Theorem 3.2.10. *Suppose $\{x_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{F}_q$, with an irreducible characteristic polynomial $f \in \mathbb{F}_q[x]$ having a root $\alpha \in \mathbb{F}_{q^k}$. Then there exists a uniquely determined $\theta \in \mathbb{F}_{q^k}$ such that:*

$$x_i = Tr(\theta\alpha^i) \qquad \text{for } \ i = 0, 1, \ldots$$

If the sequence has non-zero initial state vector then $\theta \neq 0$.

Proof. See [Nie92] - the proof requires properties of the trace function. □

Our approach to k^{th}-order linear recurring sequences has employed only matrix algebra, polynomial algebra and the theory of finite fields. However, even more remarkable results can be established via the use of algebraic properties of formal power series. This leads to a computation-oriented way of introducing the minimal polynomial of a linear recurring sequence, which is of crucial importance since the order of the minimal polynomial gives the least period length of the sequence. Nevertheless, for practical purposes, it suffices to

use a maximal period length sequence. For a viewpoint based on formal power series and minimal polynomials see [LN97]. Alternatively, Zieler [Zie59] provides a very detailed account of all the basic results on minimal polynomials and an in-depth investigation of linear recurring sequences in general. Unfortunately, a project of this nature does not permit us to go any further than we have already.

We end this chapter by taking a very brief look at the closely related *digital k-step method*.

3.3 Digital k-step Method

This particular method was first proposed by Tausworthe [Tau65]. It works by transforming a *maximal period length* k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_p$ into a sequence of *digital k-step pseudorandom numbers* $\{y_i\}$ defined by

$$y_i = \sum_{j=1}^{n} x_{ni+j-1} p^{-j}; \qquad \text{for } i = 0, 1, \ldots \tag{3.15}$$

where n is chosen such that $2 \leq n \leq k$. Equivalently, it may be viewed that the sequence $\{y_i\}$ is obtained by partitioning the sequence $\{x_i\}$ into consecutive blocks of length n and interpreting each y_i of the sequence as the base p expansion of a number in $[0, 1)$.

As a consequence of the next theorem, a sequence $\{y_i\}$ of digital k-step pseudorandom numbers is purely periodic and attains maximal period length $p^k - 1$ if and only if n $(2 \leq n \leq k)$ is chosen such that $(n, p^k - 1) = 1$.

Theorem 3.3.1. *A sequence $\{y_i\}$ of digital k-step pseudorandom numbers, generated by* (3.15)*, is purely periodic with period length* $\frac{p^k-1}{(n,p^k-1)}$.

Proof. [Nie92]
Let $d = p^k - 1$ and $t = (n, p^k - 1)$. A sequence of digital k-step pseudorandom numbers $\{y_i\}$ is defined from a maximal period length k^{th}-order linear recurring sequence $\{x_i\}$ over $\mathbb{F}_p$; that is, the period length of $\{x_i\}$ is $d = p^k - 1$. Using this fact, together with (3.15), we find $y_{i+(d/t)} = y_i$ for all $i \geq 0$, and therefore the sequence $\{y_i\}$ is purely periodic with period length d' a divisor of d/t, so that $d' \leq d/t$. Now, since we have $y_{i+d'} = y_i$ for all $i \geq 0$, it can be derived from (3.15) that $x_{ni+j-1+nd'} = x_{ni+j-1}$ for all $i \geq 0$; $1 \leq j \leq n$. Consequently, $x_{i+nd'} = x_i$ for all $i \geq 0$; and thus, d divides nd' which means d/t divides d', so that $d' \geq d/t$. Hence, $d' = d/t = \frac{p^k-1}{(n,p^k-1)}$ is the period length of $\{y_i\}$. □

Chapter 4

Linear Recurrence Generators Modulo 2

4.1 Shift Register Generators

Linear recurrence generators modulo 2 are special cases of the k^{th}-order linear recurrence generators discussed in the previous chapter. This particular type of generator, often called a *shift register generator*, was originally derived from the idea of a physical device known as a feedback shift register, which we will first explore in order to gain an understanding for the motivation behind such generators.

4.1.1 Feedback Shift Registers

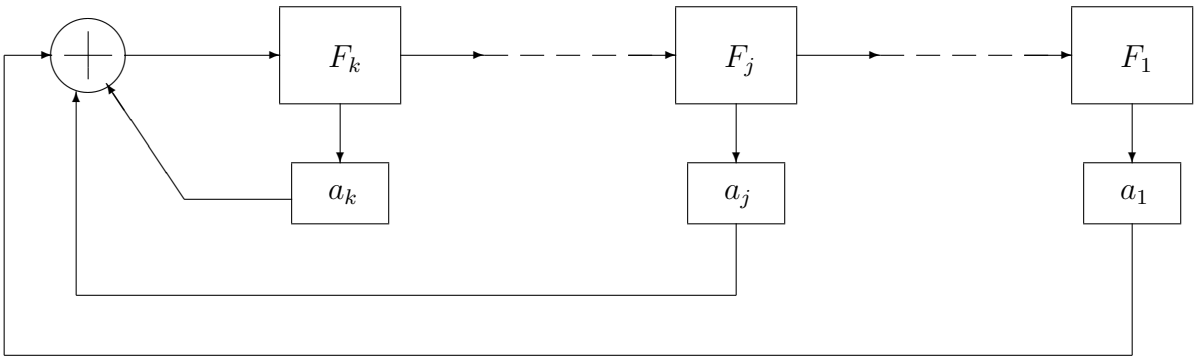


Figure 4.1: Feedback Shift Register

A *feedback shift register* is an arrangement of k binary storage devices (tubes) $F_1, F_2, \ldots, F_k$ in a row; switches; and a modulo 2 *adder* (see Figure 4.1). The switches

are represented by the boxes labelled $a_1, a_2, \ldots, a_k$. A tube F_i is either 'on' ($a_i = 1$) or 'off' ($a_i = 0$). If $a_i = 1$, we say the corresponding switch is closed and the contents of F_i is 'fed back' into the modulo 2 adder. If $a_i = 0$, the switch is open and no such feedback occurs. The contents of each tube is *shifted* to the next, in time with a clock pulse. That is, at each pulse, the contents of tube F_i is shifted to F_{i-1} ($i = 2, 3 \ldots, k$), and the new value stored in F_k is $a_1b_1 + a_2b_2 + \cdots + a_kb_k \pmod 2$, where b_i is the value stored in tube F_i prior to the clock pulse. If no new signal is introduced into tube F_k during this process, then at the completion of k shifts (or even sooner), all the tubes will be 'off', and the feedback shift register will forever remain in this state.

We shall henceforth refer to a feedback shift register as simply a *shift register*.

4.1.2 Shift Register Sequences

Consider the succession of states of the first tube, F_k, of a k-tube shift register. Suppose, at the i^{th} clock pulse of the shift register, tube F_k has a history given by successive values $b_1, b_2, \ldots, b_i$. Then, by the feedback arrangement,

$$b_i \equiv a_1b_{i-1} + a_2b_{i-2} + \cdots + a_kb_{i-k} \pmod 2. \tag{4.1}$$

Therefore, tube F_k can be thought of as satisfying the above linear recurrence relation (4.1). Furthermore, it should be observed that the history of the second tube, F_{k-1}, is the history of the first tube F_k, except for a delay of one state. Similarly for the other tubes – so that, in general, the history of a particular tube F_i is the history of the tube F_{i-1} ($i = 2, 3 \ldots, k$), but with a delay of one state. Hence, each tube of the shift register satisfies the same linear recurrence relation (4.1) as the first tube.

Accordingly, a **shift register generator** produces a sequence $\{b_i\}_{i\geq 0}$ satisfying the linear recursion

$$\boxed{b_i \equiv (a_1b_{i-1} + \cdots + a_kb_{i-k}) \pmod 2, \qquad \text{for } i = 0, 1, 2, \ldots} \tag{4.2}$$

where *feedback coefficients* $a_1, \ldots, a_k \in \mathbb{Z}_2 = \{0, 1\}$. Without loss of generality, it is assumed the shift register is actually making use of its k tubes, and so we take $a_k \neq 0$. In keeping with previous terminology, the sequence $\{b_i\}$ is a k^{th}-order linear recurring sequence over $\mathbb{Z}_2$ (or $\mathbb{F}_2$), but we shall call it a *k^{th}-order shift register sequence*. In this case, each b_i is determined by the k-tuple $\mathbf{b}_i = (b_{i-1}, \ldots, b_{i-k})$, which is known as the *i^{th} state vector* of the shift register sequence $\{b_i\}$. Naturally, the initial values $b_{-1}, b_{-2}, \ldots, b_{-k}$ form the initial state vector $\mathbf{b}_0$.

It is not difficult to show that the succession of states of a shift register is purely periodic.

Theorem 4.1.1. *The succession of states of a k-tube shift register is purely periodic with period length* $d \leq 2^k - 1$.

Proof. First observe that each state of the shift register is completely determined by the previous state. Hence, if it ever happens that a state is the same as some earlier state, then the following states will be the same; thus, pure periodicity is established for the states of the shift register.

Since each of the k tubes of the shift register are either 'on' or 'off', there are only 2^k different possible states. Therefore, a repetition must occur somewhere among the first $2^k + 1$ states, and so there is pure periodicity with period $d \leq 2^k$. But, if the state 'all zeros' (i.e. all tubes 'off') ever occurs, the subsequent states of the shift register will also have all tubes 'off', and the period is $d = 1$. Thus, a long period cannot include this state, and therefore $d \leq 2^k - 1$. □

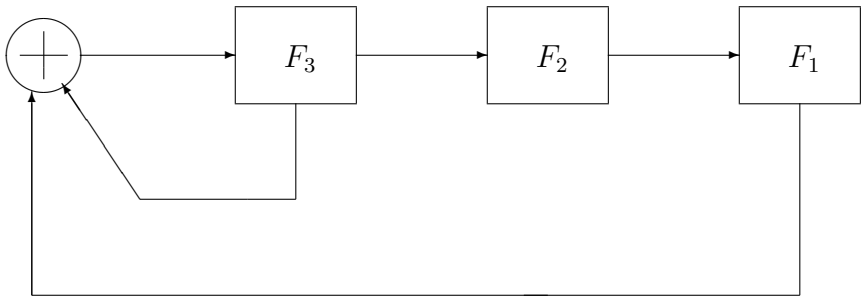
An immediate corollary to Theorem 4.1.1 provides an upper-bound for the period length of a k^{th}-order shift register sequence, and is analogous to Theorem 3.2.1 of Chapter 3, although any such sequence is *purely* periodic in this case.

Corollary 4.1.1. *A* k^{th}*-order shift register sequence* $\{b_i\}$ *is purely periodic with period length at most* $2^k - 1$.

Proof. A particular state of a k tube shift register can be represented by a state vector of the corresponding shift register sequence. It is therefore deduced, from Theorem 4.1.1, that the succession of state vectors is purely periodic. Moreover, it is clear that the period length of the sequence $\{b_i\}$ is equal to the period length of the succession of state vectors since each b_i is uniquely determined by the i^{th} state vector. Thus, the result follows from Theorem 4.1.1. □

Note. Theorem 4.1.1 holds no matter what we take as the initial state of the shift register.

Example 4.1.1. Consider the three tube shift register as in the diagram below.



The corresponding third-order shift register sequence $\{b_i\}$ is defined by

$$b_i \equiv b_{i-1} + b_{i-3} \pmod 2; \qquad \text{for } i = 0, 1 \ldots \tag{4.3}$$

If the initial state vector is $\mathbf{b}_0 = (b_{-1}, b_{-2}, b_{-3}) = (1, 1, 1)$ then the terms of the sequence $\{b_i\}$ are

$$\begin{aligned}
b_0 &= b_{-1} + b_{-3} = 1 + 1 \equiv 0 \pmod 2,\\
b_1 &= b_0 + b_{-2} = 0 + 1 \equiv 1 \pmod 2,\\
b_2 &= b_1 + b_{-1} = 1 + 1 \equiv 0 \pmod 2,\\
b_3 &= b_2 + b_0 = 0 + 0 \equiv 0 \pmod 2,\\
b_4 &= b_3 + b_1 = 0 + 1 \equiv 1 \pmod 2,\\
b_5 &= b_4 + b_2 = 1 + 0 \equiv 1 \pmod 2,\\
b_6 &= b_5 + b_3 = 1 + 0 \equiv 1 \pmod 2,\\
b_7 &= b_6 + b_4 = 1 + 1 \equiv 0 \pmod 2,\\
b_8 &= b_7 + b_5 = 0 + 1 \equiv 1 \pmod 2\ ,\ \text{etc}\ldots
\end{aligned}$$

That is, the corresponding sequence $\{b_i\}$ is

$$\underbrace{0, 1, 0, 0, 1, 1, 1}_{\text{period}}, 0, 1, 0, 0, 1, 1, 1, 0, 1, \ldots$$

Therefore, one sees that $\{b_i\}$ is purely periodic with period length $7 = 2^3 - 1$, which is the longest period length possible, by Corollary 4.1.1.

Moreover, the succession of states (or state vectors) is

$$\begin{aligned}
&\mathbf{b}_0 = (1, 1, 1), \quad &&\mathbf{b}_2 = (1, 0, 1), \quad &&\mathbf{b}_4 = (0, 0, 1), \quad &&\mathbf{b}_6 = (1, 1, 0),\\
&\mathbf{b}_1 = (0, 1, 1), \quad &&\mathbf{b}_3 = (0, 1, 0), \quad &&\mathbf{b}_5 = (1, 0, 0), \quad &&\mathbf{b}_7 = (1, 1, 1),\ \text{etc}\ldots
\end{aligned}$$

The eighth state is the same as the initial state, and so the period length of the succession of states is also $7 = 2^3 - 1$, which is expected (by the proof of Corollary 4.1.1). Certainly, all possible states have occurred, except the zero state (0, 0, 0).

□

4.1.3 Generating Functions

There are two basic methods used for the study of shift register sequences. If only a single tube is considered, the *method of generating functions* yields quick results. If, however, the entire shift register is thought to satisfy recurrence relation (4.2) then the

matrix method (as described later) is more appropriate, and is most frequently presented in the literature.

In this section, we will use a generating function to derive the characteristic polynomial of a shift register sequence, and establish some results analogous to those given in Chapter 3.

Suppose the k^{th}-order shift register sequence $\{b_i\}$ corresponds to the history of the first tube, F_k. Then we associate it with the *generating function*

$$G(x) = \sum_{i=0}^{\infty} b_i x^i \tag{4.4}$$

where x is an indeterminate. Despite the name, we do not consider $G(x)$ to be a function, but rather a formal object, with the basic idea being that $G(x)$ represents the terms of the sequence $\{b_i\}$ in the correct order and so should, in some way, reflect the properties of the sequence.

Since $\{b_i\}$ satisfies the recurrence relation $b_i \equiv (a_1 b_{i-1} + \cdots + a_k b_{i-k}) \pmod 2$, then

$$\begin{aligned} G(x) &= \sum_{i=0}^{\infty} \sum_{j=1}^{k} a_j b_{i-j} x^i \\ &= \sum_{j=1}^{k} a_j x^j \sum_{i=0}^{\infty} b_{i-j} x^{i-j} \\ &= \sum_{j=1}^{k} a_j x^j (b_{-j} x^{-j} + \cdots + b_{-1} x^{-1} + \sum_{i=0}^{\infty} b_i x^i). \end{aligned}$$

Thus,

$$G(x) = \sum_{j=1}^{k} a_j x^j (b_{-j} x^{-j} + \cdots + b_{-1} x^{-1} + G(x))$$

and

$$G(x) - \sum_{j=1}^{k} a_j x^j G(x) = \sum_{j=1}^{k} a_j x^j (b_{-j} x^{-j} + \cdots + b_{-1} x^{-1}).$$

That is,

$$G(x) = \frac{\sum_{j=1}^{k} a_j x^j (b_{-j} x^{-j} + \cdots + b_{-1} x^{-1})}{1 - \sum_{j=1}^{k} a_j x^j}. \tag{4.5}$$

So $G(x)$ is expressed entirely in terms of the initial state vector $\mathbf{b}_0 = (b_{-1}, \ldots, b_{-k})$ and the feedback coefficients $a_1, \ldots, a_k$, with the denominator of (4.5) independent of the initial state vector.

Now, with $b_{-1} = b_{-2} = \cdots = b_{1-k} = 0,\ b_{-k} = 1$ (so that $\mathbf{b}_0 = (0, 0, \ldots, 0, 1)$) expression (4.5) becomes

$$G(x) = \frac{a_k}{1 - \sum_{j=1}^{k} a_j x^j}. \tag{4.6}$$

Consider the polynomial

$$\begin{aligned} f(x) = 1 - \sum_{j=1}^{k} a_j x^j &= 1 - a_1 x - a_2 x^2 - \cdots - a_{k-1} x^{k-1} - a_k x^k \\ &\equiv 1 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} + a_k x^k \pmod 2. \end{aligned}$$

Since we have assumed a_k is non-zero (i.e. $a_k = 1$), the polynomial f has degree k. Now, the **characteristic polynomial** of the k^{th}-order shift register sequence $\{b_i\}$ is defined to be the k^{th} degree polynomial

$$f(x) = x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + 1 \in \mathbb{Z}_2[x]. \tag{4.7}$$

Example 4.1.2. The third-order shift register sequence $\{b_i\}$ defined by

$$b_i \equiv b_{i-1} + b_{i-3} \pmod 2, \tag{4.8}$$

as in Example 4.1.1, has characteristic polynomial $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ of degree 3.

□

Using the concept of a generating function, we now proceed to establish the analogous result to Theorem 3.2.5.

Theorem 4.1.2. *If a k^{th}-order shift register sequence $\{b_i\}$ has initial state state vector $(0, 0, \ldots, 0, 1)$, so that $b_{-1} = b_{-2} = \cdots = b_{1-k} = 0,\ b_{-k} = 1$, then the period length of $\{b_i\}$ is equal to $ord(f)$, where $f(x) \in \mathbb{Z}_2[x]$ is the characteristic polynomial of the sequence.*

Proof. [Gol67]
With the given initial state vector, we have the expression

$$G(x) = \frac{1}{f(x)} = \sum_{i=0}^{\infty} b_i x^i. \tag{4.9}$$

Corollary 4.1.1 shows that the sequence $\{b_i\}$ is purely periodic with period length at most $2^k - 1$.

(*i*) Suppose $\{b_i\}$ has period length d, then

$$\begin{aligned}\frac{1}{f(x)} =&(b_0 + b_1x + \cdots + b_{d-1}x^{d-1}) + x^d(b_0 + b_1x + \cdots + b_{d-1}x^{d-1}) \\ & x^{2d}(b_0 + b_1x + \cdots + b_{d-1}x^{d-1}) + \cdots \\ =&(b_0 + b_1x + \cdots + b_{d-1}x^{d-1})(1 + x^d + x^{2d} + x^{3d} + \cdots) \\ =&(b_0 + b_1x + \cdots + b_{d-1}x^{d-1})/(1 - x^d).\end{aligned}$$

Thus, $f(x)(b_0 + b_1x + \cdots + b_{d-1}x^{d-1}) = 1 - x^d$, which implies that $f(x)$ divides $1 - x^d$.

(*ii*) Conversely, suppose $f(x)$ divides $1 - x^d$ and let the quotient be

$$\beta_0 + \beta_1x + \cdots + \beta_{d-1}x^{d-1}.$$

Then

$$\begin{aligned}\frac{1}{f(x)} &= \frac{\beta_0 + \beta_1x + \cdots + \beta_{d-1}x^{d-1}}{1 - x^d} \\ &= (\beta_0 + \beta_1x + \cdots + \beta_{d-1}x^{d-1})(1 + x^d + x^{2d} + \cdots) \\ &= (\beta_0 + \beta_1x + \cdots + \beta_{d-1}x^{d-1}) + x^d(\beta_0 + \beta_1x + \cdots + \beta_{d-1}x^{d-1}) + \cdots \\ &= G(x) = \sum_{i=0}^{\infty} b_ix^i.\end{aligned}$$

Equating coefficients of 'like powers' of x gives $\{b_i\} = \{\beta_i\}$, so that sequence $\{b_i\}$ has period length d, or some factor of d.

Thus, the smallest positive integer d for which $f(x)$ divides $1 - x^d$ is the period length of $\{b_i\}$. That is, the period length of $\{b_i\}$ is $ord(f)$, by Definition 3.2.7. □

The shift register sequence $\{b_i\}$ with initial state vector, as given in the preceding theorem, is called an *impulse response sequence*, previously defined in Section 3.2 of Chapter 3.

Remark. Recall expression (4.5): $G(x) = g(x)/f(x)$ where $g(x)$ has degree less than $deg(f) = k$. The proof of Theorem 4.1.2 still works if $g(x)$ has no factors in common with $f(x)$ so that the period length of the corresponding sequence is $ord(f)$. (See Golomb [Gol67]).

Corollary 4.1.2. *Suppose $\{b_i\}$ is a k^{th}-order shift register sequence with non-zero initial state vector and irreducible characteristic polynomial $f(x) \in \mathbb{Z}_2[x]$. Then the period length of the sequence is equal to $ord(f)$.*

Proof. By expression (4.5), we have $G(x) = g(x)/f(x)$, where $g(x)$ has degree less than $deg(f) = k$. If $f(x)$ is irreducible over $\mathbb{Z}_2$ then it can have no factors in common with $g(x)$ (a polynomial of lower degree) unless $g(x) = 0$, which corresponds to initial state vector $(0, \ldots, 0)$. Consequently, if $f(x)$ is irreducible over $\mathbb{Z}_2$, then the period length of the shift register sequence does *not* depend on the initial state vector, excepting the 'zero' initial state vector. Furthermore, by the above remark, since $g(x)$ has no factors in common with $f(x)$ then the proof of Theorem 4.1.2 still works, and so the period length of the sequence is equal to $ord(f)$. □

Example 4.1.3. As shown in the previous example, the third-order shift register sequence $\{b_i\}$ of Example 4.1.1 has characteristic polynomial $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ of degree 3. If f is not irreducible over $\mathbb{Z}_2$ then f must have at least one linear factor of the form $(x - a)$ for some $a \in \mathbb{Z}_2$, which implies a would be a zero of f. But, $f(0) = 0 + 0 + 1 = 1$ and $f(1) = 1 + 1 + 1 = 1$ in $\mathbb{Z}_2$. So f has no zeros in $\mathbb{Z}_2$, and hence no linear factors in $\mathbb{Z}_2[x]$, which shows that f is irreducible over $\mathbb{Z}_2$.

Now, consider the polynomial $g_e(x) = x^e - 1 = x^e + 1 \in \mathbb{Z}_2[x]$, where e is a positive integer. By long division of polynomials, we find that $f(x)$ does not divide $g_e(x)$ for $e = 0, 1, \ldots, 6$. However, $f(x)$ divides $g_7(x)$ since long division yields

$$x^7 - 1 = (x^3 + x + 1)(x^4 + x^2 + x + 1).$$

That is, $g_7(x)/f(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. Therefore, $e = 7$ is the smallest positive integer such that $f(x)$ divides $x^e - 1$, and thus, $ord(f) = 7$.

This sequence has an irreducible characteristic polynomial $f \in \mathbb{Z}_2[x]$. Hence, by Corollary 4.1.2, the sequence $\{b_i\}$ must have period length equal to $ord(f)$. Indeed, it was found in Example 4.1.1 that the period length of the sequence is in fact $d = 7 = ord(f)$. Moreover, since f is a monic (irreducible) polynomial over $\mathbb{Z}_2$ of degree 3, with $f(0) \neq 0$ and $ord(f) = 7 = 2^3 - 1$, then by Theorem 3.2.8, f is a primitive polynomial over $\mathbb{Z}_2$. □

The next result naturally follows from Theorem B.5 and Corollary 4.1.2.

Lemma 4.1.1. *If a k^{th}-order shift register sequence $\{b_i\}$ has an irreducible characteristic polynomial $f \in \mathbb{Z}_2[x]$ of degree $k > 1$, then the period length of the sequence divides $2^k - 1$.*

Proof. Since $\{b_i\}$ has irreducible characteristic polynomial $f \in \mathbb{Z}_2[x]$ then, by Corollary 4.1.2, the period length of the sequence is equal to $ord(f)$. Furthermore, according the Theorem B.5 of Appendix B, $ord(f)$ divides $2^k - 1$. □

Example 4.1.4. The sixth-order shift register sequence $\{b_i\}_{i \geq 0}$ defined by

$$b_i \equiv b_{i-3} + b_{i-6} \pmod 2,$$

with initial state vector $(b_{-1}, \ldots, b_{-6}) = (0, 0, 0, 1, 1, 1)$, is the string of binary digits

$$\underbrace{1, 1, 1, 1, 1, 1, 0, 0, 0}_{\text{period}}, 1, 1, 1, \ldots\ldots$$

of period length 9. The corresponding characteristic polynomial $f(x) = x^6 + x^3 + 1$ is irreducible over $\mathbb{Z}_2$ with $ord(f) = 9$, as expected by Corollary 4.1.2. In particular, this example demonstrates Lemma 4.1.1 since 9 divides $2^6 - 1 = 63$. □

We now prove an analogous result to the main theorem (Theorem 3.2.9) of Chapter 3. Notice that we have arrived at this result with comparatively little effort.

Theorem 4.1.3. *Let $\{b_i\}$ be a k^{th}-order shift register sequence with non-zero initial state vector. Then $\{b_i\}$ is purely periodic and attains maximal period length $2^k - 1$ if and only if its characteristic polynomial $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + 1 \in \mathbb{Z}_2[x]$ is a primitive polynomial over $\mathbb{Z}_2$.*

Proof. Let $\{b_i\}$ be a k^{th}-order shift register sequence with non-zero initial state vector. By Corollary 4.1.1, $\{b_i\}$ is purely periodic.

Suppose the sequence $\{b_i\}$ has maximal period length $2^k - 1$. Since $\{b_i\}$ runs through $2^k - 1$ terms before it repeats, then every possible binary sequence, consisting of 1's and 0's, of length k (except k consecutive zeros) will appear in $\{b_i\}$. In particular, somewhere within the sequence $\{b_i\}$ there will be a 1 followed by $k - 1$ zeros. If we begin here, then Theorem 4.1.2 applies, and hence, the period length of $\{b_i\}$ is $ord(f)$. Since the sequence has period length $2^k - 1$, we have $ord(f) = 2^k - 1$. In addition, $f \in \mathbb{Z}_2[x]$ is monic and of degree $k \geq 1$ with $f(0) \neq 0$ so that, by Theorem 3.2.8, the characteristic polynomial f is a primitive polynomial over $\mathbb{Z}_2$.

Conversely, suppose the characteristic polynomial $f \in \mathbb{Z}_2[x]$ of the sequence $\{b_i\}$ is a primitive polynomial over $\mathbb{Z}_2$. Then, by Theorem 3.2.8, $ord(f) = 2^k - 1$. From the note following Definition 3.2.8, f is certainly irreducible of $\mathbb{Z}_2$, and by Lemma 4.1.1, the period length of the sequence is a factor of $2^k - 1$. But, in this case, $ord(f) = 2^k - 1$; thus, by Corollary 4.1.2, the period length of the sequence $\{b_i\}$ is $2^k - 1$. □

Example 4.1.3 illustrates the above result.

4.1.4 Matrix Theory

From our discussion thus far, we can represent each state of a k-tube shift register by a k-dimensional vector, so that the shift register can be thought of as a linear transformation,

which changes each state into the next. It is well known that a linear transformation, on k-dimensional vectors, is most conveniently represented by a $k \times k$ matrix.

Example 4.1.5. Referring to Example 4.1.1, the given 3-tube shift register is mathematically *equivalent* to the matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

In particular, we see that

$$\mathbf{b}_0\mathbf{A} = (1\ 1\ 1)\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (0\ 1\ 1) = \mathbf{b}_1, \quad \mathbf{b}_1\mathbf{A} = (0\ 1\ 1)\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = (1\ 0\ 1) = \mathbf{b}_2,$$

and so on.

In general, a k^{th}-order shift register sequence $\{b_i\}$ has associated $k \times k$ matrix

$$\mathbf{A} = \begin{pmatrix} a_1 & 1 & 0 & \cdots & 0 \\ a_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k-1} & 0 & 0 & \cdots & 1 \\ a_k & 0 & 0 & \cdots & 0 \end{pmatrix} \tag{4.10}$$

called a **shift register matrix**.

If one considers the i^{th} state vector $\mathbf{b}_i = (b_{i-1}, b_{i-2}, \ldots, b_{i-k})$ then

$$\begin{aligned} \mathbf{b}_i\mathbf{A} &= (b_{i-1}, b_{i-2}, \ldots, b_{i-k}) \begin{pmatrix} a_1 & 1 & 0 & \cdots & 0 \\ a_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{k-1} & 0 & 0 & \cdots & 1 \\ a_k & 0 & 0 & \cdots & 0 \end{pmatrix} \\ &= (a_1 b_{i-1} + a_2 b_{i-2} + \cdots + a_k b_{i-k}, b_{i-1}, b_{i-2}, \ldots, b_{i-k+1}) \\ &= (b_i, b_{i-1}, \ldots, b_{i-k+1}) = \mathbf{b}_{i+1}. \end{aligned}$$

Clearly, $\mathbf{b}_{i+1} = \mathbf{b}_i\mathbf{A}$ for all $i \geq 0$, as was also established in Chapter 3 although the associated matrix was of a different form. Therefore, it has been verified that $\mathbf{A}$ is indeed the matrix associated with the k^{th}-order shift register sequence $\{b_i\}$.

The *characteristic polynomial* of the matrix $\mathbf{A}$ is

$$\begin{aligned}\varphi(\lambda) = |\mathbf{A} - \lambda\mathbf{I}| &= \begin{vmatrix} a_1 - \lambda & 1 & 0 & \cdots & 0 \\ a_2 & -\lambda & 1 & \cdots & 0 \\ a_3 & 0 & -\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_k & 0 & 0 & \cdots & -\lambda \end{vmatrix} \\ &= (-\lambda)^{k-1}(a_1 - \lambda) - a_2(-\lambda)^{k-2} + a_3(-\lambda)^{k-3} - \cdots + (-1)^k a_k \\ &= -(-\lambda)^k \left[1 - \frac{a_1}{\lambda} - \frac{a_2}{\lambda^2} - \frac{a_3}{\lambda^3} - \cdots - \frac{a_k}{\lambda^k}\right],\end{aligned}$$

and if we substitute $\lambda = 1/x$, then

$$\begin{aligned}\varphi(\lambda) = \varphi(1/x) &= \frac{(-1)^{k+1}}{x^k}[1 - (a_1 x + a_2 x^2 + \cdots + a_k x^k)] \\ &\equiv \frac{1}{x^k}(a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + 1) \pmod 2 \\ &\equiv \frac{f(x)}{x^k} \pmod 2.\end{aligned}$$

Thus, except for a factor of $1/x^k$ modulo 2, the characteristic polynomial $\varphi(\lambda) = |\mathbf{A} - \lambda\mathbf{I}|$ (with $\lambda = 1/x$) of $\mathbf{A}$ is the characteristic polynomial $f(x) \in \mathbb{Z}_2[x]$ of the sequence $\{b_i\}$. In fact, we have

$$f(x) = x^k \varphi(1/x) \in \mathbb{Z}_2[x], \tag{4.11}$$

so that $\phi(x) \in \mathbb{Z}_2[x]$ is the reciprocal characteristic polynomial of $\{b_i\}$.

One may easily prove, by mathematical induction, that the state vectors $\mathbf{b}_i$ of a k^{th}-order shift register sequence $\{b_i\}$ are such that

$$\mathbf{b}_i = \mathbf{b}_0\mathbf{A}^i \quad \text{for all} \quad i = 0, 1, 2, \ldots \tag{4.12}$$

The next theorem relates to the period length of the succession of state vectors, and hence of the sequence $\{b_i\}$. A nice proof was given by Marsaglia [MT85], and has been adapted here.

Theorem 4.1.4. *Suppose $\{b_i\}$ is a k^{th}-order shift register sequence with associated $k \times k$ shift register matrix $\mathbf{A}$ and non-zero initial state vector $\mathbf{b}_0$. Then the sequence $\mathbf{b}_0$, $\mathbf{b}_0\mathbf{A}$, $\mathbf{b}_0\mathbf{A}^2$, $\mathbf{b}_0\mathbf{A}^3, \ldots$ has maximal period length $2^k - 1$ if and only if the matrix $\mathbf{A}$ has order $2^k - 1$ in $GL(k, 2)$.*

Proof. Suppose the sequence $\mathbf{b}_0$, $\mathbf{b}_0\mathbf{A}$, $\mathbf{b}_0\mathbf{A}^2$, $\mathbf{b}_0\mathbf{A}^3, \ldots$ has maximal period length $d = 2^k - 1$ for some non-zero initial state vector $\mathbf{b}_0$. Then $\mathbf{A}$ has order at most

d in $GL(k,2)$ and, since there are $d = 2^k - 1$ non-zero binary k-tuples, the set $\{\mathbf{b}_0, \mathbf{b}_0\mathbf{A}, \mathbf{b}_0\mathbf{A}^2, \ldots \mathbf{b}_0\mathbf{A}^{d-1}\}$ consists of all of these binary $1 \times k$ vectors. Therefore, $\mathbf{b}\mathbf{A}^d = \mathbf{b}$ for every binary k-tuple $\mathbf{b}$ and thus, the null space of $\mathbf{A}^d - \mathbf{I}$ has dimension k, which implies $\mathbf{A}^d = \mathbf{I}$ so that the order of $\mathbf{A}$ in $GL(k,2)$ is at least d. Consequently, the $k \times k$ matrix $\mathbf{A}$ has order $d = 2^k - 1$ in $GL(k,2)$.

Conversely, suppose the matrix $\mathbf{A}$ has order $d = 2^k - 1$ in $GL(k,2)$. If S is the set of distinct powers of $\mathbf{A}$ then $S = \{\mathbf{I}, \mathbf{A}, \mathbf{A}^2, \ldots, \mathbf{A}^{d-1}\}$. Let $g \in \mathbb{Z}_2[x]$ be the minimal polynomial of $\mathbf{A}$ with $deg(g) = n$. Since $\mathbf{A}$ satisfies its own characteristic equation then $n \leq k$. Consider the set of all polynomials in $\mathbf{A}$ of degree less than n, given by

$$P = \{p(\mathbf{A}) \mid p(x) \in \mathbb{Z}_2[x] \ , \ deg(p) < n\}.$$

That is, $P = \{c_0 + c_1\mathbf{A} + \cdots + c_{n-1}\mathbf{A}^{n-1} \mid c_i \in \mathbb{Z}_2\}$ so that one clearly sees that $|P| = 2^n$. Now, by means of the *Division Algorithm for* $\mathbb{Z}_2[x]$ (Theorem B.3), there exist polynomials $q(x), r(x) \in \mathbb{Z}_2[x]$ such that $x^e = q(x)g(x) + r(x)$ with $deg(r) < n$. Hence, for every positive integer e, $\mathbf{A}^e = q(\mathbf{A})g(\mathbf{A}) + r(\mathbf{A}) = r(\mathbf{A})$ with $deg(r) < n$, so that every element of S is expressible as an element of P.
It follows that S is a subset of $P\backslash\{0\}$, and therefore $|S| \leq |P\backslash\{0\}|$, which implies $2^k - 1 \leq 2^n - 1$. However, $2^n - 1 \leq 2^k - 1$ since $n \leq k$. Thus, $k = n$ and so $S = P\backslash\{0\}$. Further, since the elements of S are non-singular then so to are the elements of $P\backslash\{0\}$.

Consider any non-zero initial state vector $\mathbf{b}_0$. Then to have $\mathbf{b}_0\mathbf{A}^j = \mathbf{b}_0$ we require $\mathbf{A}^j - \mathbf{I} = \mathbf{A}^j + \mathbf{I}$ to be singular. By the *Division Algorithm for* $\mathbb{Z}_2[x]$, every matrix $\mathbf{A}^j + \mathbf{I}$ is in P, with the only singular matrix in P being the zero matrix. Hence, $\mathbf{A}^j + \mathbf{I} = \mathbf{0}$ for $j < 2^k - 1$; a contradiction to the supposition that $\mathbf{A}$ has order $2^k - 1$ in $GL(k,2)$. □

Corollary 4.1.3. *A k^{th}-order shift register sequence $\{b_i\}$ has maximal period length $2^k - 1$ if and only if the associated $k \times k$ shift register matrix A has order $2^k - 1$ in $GL(k,2)$.*

□

The following example nicely illustrates some of the main results of this chapter.

Example 4.1.6. Consider the sixth-order shift register generator

$$x_i \equiv x_{i-2} + x_{i-4} + x_{i-5} + x_{i-6} \pmod 2 \qquad \text{for } i = 0, 1, 2, \ldots$$

The corresponding characteristic polynomial $f(x) = x^6 + x^4 + x^2 + x + 1 \in \mathbb{Z}_2[x]$ is irreducible. Further, $f(x)$ divides $x^{21} - 1$ and no polynomial $x^e - 1$ with $0 < e < 21$, so $ord(f) = 21$. If we take $(1, 1, 0, 0, 0, 0)$ as the initial state vector, we arrive at the

sequence of binary digits

$$\underbrace{1,1,0,1,1,0,1,0,1,0,1,1,1,0,1,0,0,0,0,1,1}_{\text{period}},1,1,0,1,1$$

of least period length $21 = ord(f)$, as it should be. The associated shift register matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in GL(6,2)$$

has order 21, as expected. Also, we see that $ord(f) = 21$ divides $2^6 - 1 = 63$. □

The final small section of this chapter is devoted to Mersenne prime period lengths.

4.2 Mersenne Prime Period Lengths

Recall that $M_n = 2^n - 1$ is called a *Mersenne number* or *Mersenne prime* according to whether or not it is prime. Observe the following immediate corollary to Lemma 4.1.1.

Lemma 4.2.1. *If $M_k = 2^k - 1$ is a Mersenne prime, every irreducible characteristic polynomial of degree k in $\mathbb{Z}_2[x]$ corresponds to a shift register sequence of maximal period length.* □

Indeed, in this situation, the only factor of $2^k - 1$ is itself.

Explicit formulas for the number of irreducible (and also primitive) polynomials over $\mathbb{F}_q$ were given in Section 3.2.5 of Chapter 3. For the case $q = 2$, the number of irreducible polynomials of degree k in $\mathbb{Z}_2[x]$ is

$$\psi_2(k) = \frac{1}{k} \sum_{d|k} \mu\left(\frac{k}{d}\right) 2^d,$$

and the number of primitive polynomials of degree k over $\mathbb{Z}_2$ is

$$\lambda_2(k) = \frac{\phi(2^k - 1)}{k}.$$

Consider any positive integer $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, where p_i's are distinct primes and α_i's are non-negative integers. In terms of this prime-power factorization of n, we may define

the Euler ϕ-function as

$$\phi(n) = \begin{cases} 1 & \text{if } n = 1, \\ n \prod_{i=1}^{r} (1 - 1/p_i) & \text{if } n > 1. \end{cases} \tag{4.13}$$

It is also worthwhile noting that Euler's ϕ-function is a *multiplicative* function since $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$.

Example 4.2.1. Consider (monic) irreducible polynomials of degree 8 over $\mathbb{F}_2 \cong \mathbb{Z}_2$. The positive divisors of 8 are $d = 1, 2, 4, 8$ so that $8/d = 8, 4, 2, 1$ and $\mu\left(\frac{6}{d}\right) = 0, 0, -1, 1$. Therefore, the number of monic irreducible polynomials of degree 8 in $\mathbb{F}_2[x]$ is

$$\psi_2(8) = \frac{1}{8} \sum_{d|8} \mu\left(\frac{8}{d}\right) 2^d = \frac{0 + 0 - 16 + 256}{8} = 30.$$

Furthermore, the number of primitive polynomials of degree 8 in $\mathbb{F}_2[x]$ is

$$\lambda_2(8) = \frac{\phi(255)}{8} = \frac{\phi(3 \cdot 5 \cdot 17)}{8} = \frac{2 \cdot 4 \cdot 16}{8} = 16.$$

Hence, just over half the irreducible polynomials of degree 8 in $\mathbb{Z}_2[x]$ are primitive. □

However, if $2^k - 1$ is prime then $\psi_2(k) = \lambda_2(k) = (2^k - 2)/k$ so that every irreducible polynomial of degree k is in fact a primitive polynomial in $\mathbb{Z}_2[x]$. It is therefore beneficial, in the practical sense, to choose a reasonably large value of k such that $2^k - 1$ is prime. Of course, if we have a prime $p > 2$ then $p^k - 1$ is always even, and hence not a prime (excluding the trivial case: $3^1 - 1$ is prime). Thus, for primes $p > 2$, the number of primitive polynomial of degree k in $\mathbb{F}_p[x]$ will always be less than the number of irreducible polynomials of degree k over $\mathbb{F}_p$, with the exception of the above trivial case. Consequently, determining a maximal period length shift register generator presents no special problem in comparison to a linear recurrence generator modulo p. We simply choose k such that M_k is prime so that every irreducible polynomial over $\mathbb{Z}_2$ is a primitive polynomial. Then taking any such polynomial as the characteristic polynomial for the shift register generator will yield maximal period length sequences.

Chapter 5

Non-Linear Congruential Pseudorandom Numbers

The well known coarse lattice structure of linear congruential pseudorandom numbers (as discussed in Section 2.3) leads to undesirable effects on the results in some stochastic simulations. This state of affairs provided the motivation for studying non-linear congruential generators, which do not display such regularity.

In this chapter, we will discuss several non-linear congruential pseudorandom number generators and, in each case, establish the conditions required for maximal period length sequences. It is hoped the reader will notice the connections with previous chapters, and also the predominance of number theory.

5.1 The General Non-Linear Congruential Method

For a positive integer m, the general **first-order congruential generator** is defined by an arbitrary first-order recursion

$$\boxed{x_{i+1} \equiv f(x_i) \pmod{m}; \qquad 0 \leq x_{i+1} < m} \tag{5.1}$$

where f is a function $f : \mathbb{Z}_m \longrightarrow \mathbb{Z}$. It is usual, in practice, to choose a function f and initial seed x_0 such that the sequence $\{x_i\}$ is purely periodic with a long period length. Once again, it is obvious that the maximum possible period length is m. Full period length m can always be attained by initially taking a purely periodic sequence $\{x_i\}$ with period length m and $\{x_0, x_1, \ldots, x_{m-1}\} = \mathbb{Z}_m$, and then defining the corresponding function $f(x_i) = x_{i+1}$ for $i = 0, 1, 2, \ldots, m-1$. Nevertheless, for practical purposes,

this is pointless since we require use of a function f that is computable without prior knowledge of the sequence $\{x_i\}$.

Among the first-order congruential methods, we can distinguish between the linear congruential method and *non-linear congruential methods*, with the latter being all the remaining methods. And, as for the linear congruential method, the most convenient moduli for non-linear congruential methods are primes and powers of two. Therefore, we shall let the modulus $m = p$, for some prime p, so that we may have $\mathbb{Z}_m \cong \mathbb{F}_p$, the finite field of order p.

Consider a sequence $\{x_i\}$ over $\mathbb{F}_p$ with period length p. Then the map

$$\begin{aligned} \mathbb{F}_p &\to \mathbb{F}_p \\ i &\mapsto x_i, \end{aligned}$$

like any map of a finite field onto itself, can be represented by a uniquely determined polynomial $g \in \mathbb{F}_p[x]$ with $deg(g) < p$. That is, we have the map

$$g : \mathbb{F}_p \to \mathbb{F}_p \text{ defined by } g(i) = x_i \qquad \text{for } i = 0, 1, \ldots \tag{5.2}$$

where each i is considered an element of $\mathbb{F}_p$.

Definition 5.1.1. *A polynomial $g \in \mathbb{F}_p[x]$ is said to be a* ***permutation polynomial over*** $\mathbb{F}_p$ *if* $\{g(0), g(1), \ldots, g(p-1)\} = \mathbb{F}_p$.

Theorem 5.1.1. *The sequence $\{x_i\}$, given by* (5.2)*, has period length p if and only if g is a permutation polynomial over $\mathbb{F}_p$.*

Proof. Suppose the given sequence $\{x_i\}$ has period length p. Then $\{x_0, x_1, \ldots, x_{p-1}\} = \mathbb{F}_p$ and, by the map (5.2), we have $\{g(0), g(1), \ldots, g(p-1)\} = \mathbb{F}_p$. Hence, g is a permutation polynomial over $\mathbb{F}_p$.

Conversely, suppose the given sequence $\{x_i\}$ is given by the map (5.2) where g is a permutation polynomial over $\mathbb{F}_p$. Then, by Definition 5.1.1, $\{g(0), g(1), \ldots, g(p-1)\} = \mathbb{F}_p$ so that $\{x_0, x_1, \ldots, x_{p-1}\} = \mathbb{F}_p$. Thus, $\{x_i\}$ has period length p. □

Note. Such a sequence $\{x_i\}$ can also be generated by recursion (5.1) with a suitable function f.

If g is a permutation polynomial in $\mathbb{F}_p[x]$ then $deg(g) \geq 1$. Furthermore, if $deg(g) = 1$, the sequence $\{x_i\}$ can be generated by (5.1) with the function f being a monic linear polynomial, which corresponds to a linear congruential generator with multiplier $a = 1$ and prime modulus p; certainly not a good generator, as seen in Chapter 2. On the

contrary, if $deg(g) > 1$, then $deg(g)$ cannot divide $p-1$, by Theorem B.6. Thus, $3 \leq deg(g) \leq p-2$ which implies $p \geq 5$. In particular, if $deg(g) > 1$ we refer to the generator as a (first-order) *non-linear congruential generator modulo p*, which produces a *non-linear congruential sequence* $\{x_i\}$ of pseudorandom numbers.

These pseudorandom numbers were first suggested by Eichenauer, Grothe, and Lehn [EGL88]. However, the earliest first-order non-linear congruential method, that has received a fair amount of attention since its inception, is the *quadratic congruential method* proposed by Donald E. Knuth in 1969 (see [Knu81]).

5.2 Quadratic Congruential Method

A **quadratic congruential generator** produces a *quadratic congruential sequence* $\{x_i\}_{i\geq 0}$ by the recursion

$$\boxed{x_{i+1} \equiv ax_i^2 + bx_i + c \pmod{m}; \qquad 0 \leq x_{i+1} < m} \tag{5.3}$$

where $a, b, c, x_0 \in \mathbb{Z}_m$. That is, this method uses (5.1) with function f as the quadratic polynomial $f(x) = ax^2 + bx + c$. As usual, the corresponding sequence $\{u_i\}$ of quadratic congruential pseudorandom numbers in $[0, 1)$, can be obtained by the normalization $u_i = x_i/m$; $i \geq 0$.

We now proceed to establish a result that gives the conditions under which a quadratic congruential sequence attains full period length. The reader should note that this theorem may be viewed as a generalization of Theorem 2.1.1, and the restrictions are not much more severe than for the linear congruential method.

Note. The integer sequence $\{x_i\}$, defined by

$$x_0 = 0, \; x_{i+1} = ax_i^2 + bx_i + c \qquad \text{for } i = 0, 1, \ldots \tag{5.4}$$

has period length m (when the terms of the sequence are reduced modulo m) only if its period length is d (when the terms of the sequence are reduced modulo d), for any divisor d of m.

Theorem 5.2.1. [Knu81] *A quadratic congruential sequence* $\{x_i\}$ *attains full period length* m *if and only if each of the following conditions are satisfied:*

(i) c *is relatively prime to* m*;*

(ii) $a, b - 1 \equiv 0 \pmod{p}$ *for each odd prime divisor* p *of* m*;*

(iii) a *is even and* $b \equiv a + 1 \pmod{4}$ *if* $4 \mid m$*, or* $b \equiv a + 1 \pmod{2}$ *if* $2 \mid m$*;*

(iv) either $a \equiv 0 \pmod 9$, *or* $b \equiv 1 \pmod 9$ *and* $ac \equiv 6 \pmod 9$ *if* $9 \mid m$.

Proof. As in the proof of Theorem 2.1.1, we may assume that modulus $m = p^\alpha$, where p is a prime and $\alpha \in \mathbb{Z}^+$. Also, without loss of generality, we will take initial seed $x_0 = 0$.

Necessity

Suppose the sequence $\{x_i\}$ has full period length $m = p^\alpha$. It follows that the sequence $\{x_i\}$ modulo p^β has period length p^β for $1 \leq \beta \leq \alpha$; otherwise, some residues modulo p^β would not appear in the sequence.

Suppose c is a multiple of p. Then each x_i is a multiple of p, and hence not all residues modulo p^α occur in the sequence; a contradiction to the fact that the sequence $\{x_i\}$ has period length $m = p^\alpha$. Therefore, c is not a multiple of p, and hence $(c, m) = (c, p^\alpha) = 1$.

If $p \leq 3$, it is trivial to establish the necessity of conditions (iii) and (iv), so assume $p \geq 5$.

Now, consider condition (ii) and suppose $a \not\equiv 0 \pmod p$. Then, for all x, $ax^2 + bx + c \equiv a(x + b')^2 + c' \pmod{p^\alpha}$ for some integers b', c'. At the points x and $-x - 2b'$, this quadratic assumes the same value and consequently cannot yield all values modulo p^α; a contradiction. Thus, $a \equiv 0 \pmod p$. Also, if $b \not\equiv 1 \pmod p$ then we would have $ax^2 + bx + c \equiv x \pmod p$ for some x, and so not all residues modulo p are assumed; a contradiction, since the sequence $\{x_i\}$ modulo p has period length p. Hence, $b \equiv 1 \pmod p$, and the necessity of the conditions has been proved.

Sufficiency

Assume conditions (i) to (iv) hold.

Note that by using Theorem 2.1.1 and considering some trivial cases, one may assume that $m = p^\alpha$ where $\alpha \geq 2$.

It can be proved that the sequence $\{x_i\}$ of integers, defined by (5.4) in the note preceding this theorem, satisfies the congruence

$$x_{i+p^\beta} \equiv x_i + kp^\beta \pmod{p^{\beta+1}} \qquad \text{for } i = 0, 1, 2, \ldots \tag{5.5}$$

for some integer $k \not\equiv 0 \pmod p$ and for all $\beta \geq 1$. The above relation implies that the period length of $\{x_i\}$ modulo p^α divides p^α, but does not divide $p^{\alpha-1}$. Thus, upon proving (5.5), we will have shown that the sequence $\{x_i\}$ modulo p^α has period length p^α.

Now, we shall prove relation (5.5) by induction on β. Let $\beta = 1$. It is easily checked:

- ◇ If $p = 2$, $x_{i+p} \equiv x_i + pc \pmod{p^2}$ for all i;
- ◇ If $p = 3$, either $x_{i+p} \equiv x_i + pc \pmod{p^2}$ or $x_{i+p} \equiv x_i - pc \pmod{p^2}$ for all i.

Claim. If $p \geq 5$ then $x_{i+p} \equiv x_i + pc \pmod{p^2}$ for all i.

Proof of Claim. Since $a \equiv 0 \pmod{p}$ and $b \equiv 1 \pmod{p}$ then $a = ps$ and $b = 1 + pt$ for some integers s, t. It follows that if $x_i \equiv ci + py_i \pmod{p^2}$ then
$y_{i+1} \equiv i^2c^2s + ict + y_i \pmod{p}$, using (5.4); whence, $y_i \equiv \binom{i}{3}2c^2s + \binom{i}{2}(c^2s + ct) \pmod{p}$. Therefore, $y_p \equiv 0 \pmod{p}$ since both binomial coefficients $\binom{p}{3}$ and $\binom{p}{2}$ are divisible by p. Thus, the claim is proved and so relation (5.5) holds for $\beta = 1$.

Consider $\beta \geq 2$ and let

$$x_{i+p^\beta} \equiv x_i + kp^\beta + z_i p^{\beta+1} \pmod{p^{\beta+2}}.$$

Then, applying (5.4) with $a = ps$ and $b = 1 + pt$, gives

$$z_{i+1} \equiv 2skic + tk + z_i \pmod{p}.$$

It is then deduced that $z_{i+p} \equiv z_i \pmod{p}$, and therefore

$$x_{i+np^\beta} \equiv x_i + n(kp^\beta + z_i p^{\beta+1}) \pmod{p^{\beta+2}} \qquad \text{for all integers } n \geq 1.$$

Setting $n = p$, we then obtain

$$x_{i+p^{\beta+1}} \equiv x_i + kp^{\beta+1} + z_i p^{\beta+2} \equiv x_i + kp^{\beta+1} \pmod{p^{\beta+2}},$$

and the result is proved. □

For the most commonly used moduli – namely, powers of two – Theorem 5.2.1 naturally implies the next result.

Corollary 5.2.1. *A quadratic congruential sequence $\{x_i\}$, generated by (5.3) with modulus $m = 2^\beta \geq 4$, has full period length $m = 2^\alpha$ if and only if c is odd,*
$b \equiv a + 1 \pmod{4}$, and a is even.

□

Example 5.2.1. Consider the quadratic congruential generator with modulus $m = 36 = 2^2 \cdot 3^2$, and parameters $a = 12$, $b = 25$, $c = 11$. Clearly, the conditions of Theorem 5.2.1 are satisfied since $(c, m) = (11, 36) = 1$; $a = 12$ where $12 \equiv 0$ modulo 2 and 3; $b = 25$ where $25 \equiv 1$ modulo 2 and 3; $a = 12$ is even and $b \equiv a + 1 \equiv 13 \pmod{4}$; and, $ac = 132 \equiv 6 \pmod{9}$. Therefore, any sequence produced by this generator must have full period length. Indeed, with initial seed $x_0 = 13$, we obtain the sequence

$$13, 24, 35, 34, 9, 20, 19, 30, 5, 4, 15, 26, 25, 0, 11, 10, 21, 32, 31, 6, 17, 16, 27, 2, 1, 12, 23, 22,$$
$$33, 8, 7, 18, 29, 28, 3, 14, 13, 24 \ldots,$$

which has full period length 36. □

5.2.1 Compound Quadratic Congruential Method

We now consider the quadratic congruential method with odd composite modulus $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, where the $p_j \geq 3$ are distinct primes and the $\alpha_j \geq 2$ are integers for $1 \leq j \leq k$. The corresponding quadratic congruential sequence $\{x_i\}_{i \geq 0}$ is defined by

$$x_{i+1} \equiv a x_i^2 + b x_i + c \pmod{m}; \qquad 0 \leq x_{i+1} < m \tag{5.6}$$

where $a, b, c, x_0 \in \mathbb{Z}_m$. A sequence $\{u_i\}$ of pseudorandom numbers in $[0, 1)$ is obtained by $u_i = x_i/m$, $i \geq 0$. Clearly, the period length of $\{x_i\}$ is equal to the period length of $\{u_i\}$, and it follows from Theorem 5.2.1 that such sequences are purely periodic with full period length m if and only if $c \not\equiv 0 \pmod{p_j}$, $a \equiv 0 \pmod{p_j}$, $b \equiv 1 \pmod{p_j}$ for all $1 \leq j \leq k$ and $ac \equiv 6 \pmod{9}$ if $p_j = 3$ for some j.

In this case, we consider k quadratic congruential generators with respective moduli $q_j = p_j^{\alpha_j}$, $1 \leq j \leq k$, where the $p_j \geq 3$ are distinct primes and the $\alpha_j \geq 2$ are integers. We require the corresponding quadratic congruential sequences $\{x_i^{(j)}\}$ to have full period length $q_j = p_j^{\alpha_j}$ for each $j = 1, 2, \dots, k$, and so the parameters $a_j, b_j, c_j \in \mathbb{Z}_{q_j}$ must be chosen in accordance with the conditions of Theorem 5.2.1. We thus obtain k sequences $\{u_i^{(j)}\}$, $j = 1, 2 \dots, k$ of quadratic congruential pseudorandom numbers in $[0, 1)$ with full period lengths $q_1, \dots, q_k$ respectively.

The **compound quadratic congruential method** generates a sequence $\{y_i\}_{i \geq 0}$ of pseudorandom numbers in $[0, 1)$ by the relation

$$\boxed{y_i \equiv u_i^{(1)} + \cdots + u_i^{(k)} \pmod{1}, \qquad i \geq 0.} \tag{5.7}$$

Such a generator was introduced in 1996 by Strandt [Str97].

By applying the *Chinese Remainder Theorem* (Theorem A.7), we find that the sequence $\{y_i\}$ is purely periodic with full period length $m = q_1 \cdots q_k$. When compared to the ordinary quadratic congruential method, this compound approach clearly yields larger period lengths and is much easier to implement on a computer since exact integer calculations need only be performed with respect to smaller moduli $q_1, \dots, q_k$. Nevertheless, it is more convenient to consider the ordinary generator for certain aspects of theoretical analysis, and fortunately, under specific conditions, there is a one-to-one correspondence between sequences produced by the two generators.

Theorem 5.2.2. [Str97] *Consider a quadratic congruential generator with modulus $m = q_1 \cdots q_k$ (where $q_j = p_j^{\alpha_j}$, p_j are distinct primes and $\alpha_j \geq 2$ are integers) and parameters $a, b, c, x_0 \in \mathbb{Z}_m$ are such that the sequence $\{x_i\}$ has full period length m. Let $a_j, b_j, c_j \in \mathbb{Z}_{q_j}$ be parameters of the corresponding compound quadratic congruential generator with*

initial seeds $x_0^{(j)}$ *for* $1 \leq j \leq k$. *Then the corresponding sequences* $\{u_i\}$ *and* $\{y_i\}$ *are equal if and only if each of the following conditions are satisfied:*

(i) $a \equiv n_j a_j + r_j \frac{q_j}{2} \pmod{q_j}$;

(ii) $b \equiv b_j + r_j \frac{q_j}{2} \pmod{q_j}$;

(iii) $c \equiv m_j c_j \pmod{q_j}$;

(iv) $x_0 \equiv m_j x_0^{(j)} \pmod{q_j}$

where $m_j = m/q_j$, $n_j \equiv m_j^{-1} \pmod{q_j}$, $r_j = 0$ *if* q_j *is odd, and* $r_j \in \{0, 1\}$ *if* q_j *is even, for* $1 \leq j \leq k$.

Proof. First observe that $u_i = y_i$ for all $i \geq 0$ if and only if $x_i = my_i$ for all $i \geq 0$. By the *Chinese Remainder Theorem*, we may then assert that $x_i = my_i$ for all $i \geq 0$ if and only if $x_i \equiv m_j x_i^{(j)} \pmod{q_j}$ for all $1 \leq j \leq k$ and $i \geq 0$. By definition, both sequences $\{x_i\}$, $\{x_i^{(j)}\}$ have full period length and satisfy

$$\begin{aligned} x_{i+1} &\equiv a x_i^2 + b x_i + c \pmod{q_j} \\ m_j x_{i+1}^{(j)} &\equiv n_j a_j (m_j x_i^{(j)})^2 + b_j (m_j x_i^{(j)}) + m_j c_j \pmod{q_j} \end{aligned}$$

for all $i \geq 0$, and therefore $x_i \equiv m_j x_i^{(j)} \pmod{q_j}$ if and only if

(1) $x_0 \equiv m_j x_0^{(j)} \pmod{q_j}$; and

(2) the maps $f_j, g_j \colon \mathbb{Z}_{q_j} \to \mathbb{Z}_{q_j}$ defined by

$$\begin{aligned} f_j(x) &\equiv a x^2 + b x + c \pmod{q_j}, \\ g_j(x) &\equiv n_j a_j x^2 + b_j x + m_j c \pmod{q_j} \end{aligned} \qquad \text{are the same.}$$

Furthermore, (1) and (2) hold if and only if

$$2a \equiv 2 n_j a_j \pmod{q_j}, \tag{5.8}$$

$$a + b \equiv n_j a_j + b_j \pmod{q_j}, \tag{5.9}$$

$$c \equiv m_j c_j \pmod{q_j}. \tag{5.10}$$

Now, using Theorem A.1, (5.8) implies $a \equiv n_j a_j + r_j \frac{q_j}{2} \pmod{q_j}$ where $r_j = 0$ if q_j is odd and $r_j \in \{0, 1\}$ if q_j is even. Combined with (5.9), it follows that $b \equiv b_j + r_j \frac{q_j}{2} \pmod{q_j}$, where r_j is defined with respect to q_j, as above. Hence, from expressions (5.8)–(5.10) we obtain conditions *(i)*–*(iii)* of the theorem.

Thus, it has been determined that $u_i = y_i$ for all $i \geq 0$ if and only if *(i)*–*(iv)* of the theorem hold, as required. □

In order to demonstrate the above theorem, we provide an example.

Example 5.2.2. Recall the quadratic congruential generator of Example 5.2.1 with $a = 12$, $b = 25$, $c = 11$, $x_0 = 13$, and modulus $m = 36 = 2^2 \cdot 3^2$.
Consider the full period length quadratic congruential generators:

$$x_{i+1}^{(1)} \equiv 2(x_i^{(1)})^2 + 3x_i^{(1)} + 3 \pmod 4, \tag{5.11}$$

$$x_{i+1}^{(2)} \equiv 3(x_i^{(2)})^2 + 7x_i^{(2)} + 5 \pmod 9, \tag{5.12}$$

where (5.11) has parameters $a_1 = 2$, $b_1 = c_1 = 3$, $q_1 = 4$, $x_0^{(1)} = 1$; and (5.12) has parameters $a_2 = 3$, $b_1 = 7$, $c_1 = 5$, $q_2 = 9$, $x_0^{(2)} = 1$.

Now, $m_1 = 36/q_1 = 9$, $m_2 = 36/q_2 = 4$, and therefore $n_1 \equiv 5 \pmod 4$ and $n_2 \equiv 7 \pmod 9$. Checking the conditions of Theorem 5.2.2:

(i) $n_1 a_1 + q_1/2 = 20 \equiv 0 \pmod 4$ and $n_2 a_2 = 21 \equiv 3 \pmod 9$, and so $a = 12$ satisfies condition (i) of the theorem;

(ii) $b_1 + q_1/2 = 3 + 2 \equiv 1 \pmod 4$ and $b_2 = 7 \equiv 7 \pmod 9$, and so $b = 25$ satisfies condition (ii) of the theorem;

(iii) $m_1 c_1 = 27 \equiv 3 \pmod 4$ and $m_2 c_2 = 20 \equiv 2 \pmod 9$, and so $c = 11$ satisfies condition (iii) of the theorem; and

(iv) $m_1 x_0^{(1)} = 9 \equiv 1 \pmod 4$ and $m_2 x_0^{(2)} = 4 \equiv 4 \pmod 9$, and so $x_0 = 13$ satisfies condition (iv) of the theorem.

Thus, the normalized sequence $\{u_i\}_{i\geq 0} = \{x_i/36\}_{i\geq 0}$ and the compound quadratic quadratic congruential sequence $\{y_i\}$ must be equal. To verify this, we find that $\{u_i\}$ is the sequence

$$0.3611, 0.6667, 0.9722, 0.9444, 0.2500, 0.5556, 0.5278, 0.8333, 0.1389, 0.1111, 0.4167,$$
$$0.7222, 0.6944, 0, 0.3056, 0.2778, 0.5833, 0.8889, 0.8611, 0.1667, 0.4722, 0.4444, 0.7500,$$
$$0.5833, 0.3333, 0.6389, 0.6111, 0.9167, 0.2222, 0.1944, 0.5000, 0.8056, 0.7778, 0.0833,$$
$$0.3889, 0.3611, 0.6667, \ldots$$

The corresponding compound quadratic congruential sequence $\{y_i\}$ is given by $y_i = u_i^{(1)} + u_i^{(2)}$ for all $i \geq 0$, where $u_i^{(j)} = x_i^{(j)}/q_j$ for $j = 1, 2$. We find that $\{u_i^{(1)}\}$ is the sequence

$$0.2500, 0, 0.7500, 0.5000, 0.2500, 0, \ldots$$

and $\{u_i^{(2)}\}$ is the sequence

$$0.1111, 0.6667, 0.2222, 0.4444, 0, 0.5556, 0.7778, 0.3333, 0.8889, 0.1111, 0.6667, \ldots$$

Termwise addition of the above two sequences yields $\{y_i\}$, which is identical to $\{u_i\}$. □

5.3 Inversive Congruential Generators With Prime Modulus

Another type of non-linear congruential method, which has received a great deal of attention in recent times, is the *inversive congruential method*. Proposed in a 1986 paper by Eichenauer and Lehn [EL86], this method is based on multiplicative inversion in modular arithmetic. Yet again, it is most convenient to use powers of 2 or primes as the moduli. We will first consider the case of a prime modulus $m = p \geq 5$.

Eichenauer and Lehn's **inversive congruential generator with prime modulus** p produces an *inversive congruential sequence* $\{x_i\}_{i\geq 0}$ of pseudorandom numbers by implementation of the recursion

$$\boxed{x_{i+1} \equiv ax_i^{-1} + b \pmod{p}; \qquad 0 \leq x_{i+1} < p} \tag{5.13}$$

where we choose parameters $a, b, x_0 \in \mathbb{Z}_p$, $a \neq 0$. The corresponding normalized sequence $\{u_i\}$ of pseudorandom numbers in [0,1) is such that $u_i = x_i/p$, $i \geq 0$.

Notation. For for a non-zero $x \in \mathbb{Z}_p$, the inverse of x modulo p, denoted x^{-1}, is such that $xx^{-1} \equiv 1 \pmod{p}$, and we define $x^{-1} = 0$ if $x = 0$.

Note that since p is a prime then $(x, p) = 1$ for all non-zero elements $x \in \mathbb{Z}_p$. Therefore, the inverse of x modulo p exists, and is unique, for each element $x \neq 0$ in $\mathbb{Z}_p$. The inverse x^{-1} is easily computed using a fast and efficient method such as the well known extended Euclidean algorithm.

Clearly, an inversive congruential sequence $\{x_i\}$ consists of at most p different terms. Since $a \neq 0$ and $(a, p) = 1$ then a has a unique inverse modulo p; whence, if x_{i+1} is given, congruence (5.13) can be solved uniquely for x_i. Consequently, the sequence $\{x_i\}$ is purely periodic with period length $d \leq p$.

Understandably, as with all non-linear generators, this technique is somewhat slower than the linear congruential method. According to Eichenauer and Lehn [EL86], the calculation of a pseudorandom number by the inversive generator (5.13) requires an average of approximately $12 \cdot \ln 2/\pi^2 \cdot \ln p + 1$ times more time than the generation of a pseudorandom number by the linear congruential method. This suggests that the use of inversive congruential generator (5.13) should be limited to situations when lattices need to be avoided. However, depending on the type of simulation problem, the time needed to generate a pseudorandom number is negligible in comparison to the time taken to carry out a much greater number of other calculations required in solving the problem.

As in Chapter 3, we shall identify the field $\mathbb{Z}_p$ with $\mathbb{F}_p$ so that $\mathbb{F}_p \cong \mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ and then recursion (5.13) is *equivalent* to

$$\boxed{x_{i+1} = ax_i^{-1} + b, \qquad a \neq 0, b, x_i \in \mathbb{F}_p,\ i \geq 0} \tag{5.14}$$

which defines an *inversive sequence* $\{x_i\}$ *over* $\mathbb{F}_p$.

We again find a connection between primitive polynomials and full/maximal period length sequences, as the following theorem shows.

Theorem 5.3.1. *Consider an inversive sequence* $\{x_i\}$ *over* $\mathbb{F}_p$*, generated by* (5.14) *with parameters* $a, b \in \mathbb{F}_p$*,* $a \neq 0$*. If* $x^2 - bx - a$ *is a primitive polynomial over* $\mathbb{F}_p$ *then* $\{x_i\}$ *has full period length* p*.*

Proof. [Nie92] Let $\{x_i\}$ be an inversive sequence over $\mathbb{F}_p$, generated by (5.14) with parameters $a, b \in \mathbb{F}_p$, $a \neq 0$, such that $x^2 - bx - a$ is a primitive polynomial over $\mathbb{F}_p$.
Consider the sequence $\{y_i\}$ defined by the second-order linear recurrence relation

$$y_{i+2} = by_{i+1} + ay_i\ ; \qquad i = 0, 1, \ldots$$

where $a, b \in \mathbb{F}_p$, $a \neq 0$ and initial values $y_0 = 0, y_1 = 1$. By our discussion in Chapter 3, the corresponding characteristic polynomial is $f(x) = x^2 - bx - a \in \mathbb{F}_p[x]$ with $f(0) \neq 0$ (since $a \neq 0$), which is a primitive polynomial over $\mathbb{F}_p$, by assumption. Hence, by Theorem 3.2.9, the sequence $\{y_i\}$ is purely periodic and attains maximal period length $d = p^2 - 1$.
Let $\alpha \in \mathbb{F}_{p^2}$ be a root of f. Then, by Theorem 3.2.10, there exists a uniquely determined $\theta \in \mathbb{F}_{p^2}$, $\theta \neq 0$ such that

$$y_i = Tr(\theta\alpha^i) = \theta\alpha^i + \theta^p\alpha^{pi} \qquad \text{for } i = 0, 1, \ldots \tag{5.15}$$

Since $y_0 = 0$, then it follows from (5.15) that $0 = \theta + \theta^p$ and so $\theta^{p-1} = -1$.
Now, suppose $y_n = 0$ for some integer n with $1 \leq n \leq p$. Then (5.15) gives
$0 = \theta\alpha^n + \theta\alpha^{pn}$ so that $\alpha^{(p-1)n} = -\theta^{1-p} = 1$. Again, using (5.15) we obtain $y_{i+(p-1)n} = \theta\alpha^{i+(p-1)n} + \theta^p\alpha^{pi+p((p-1)n)} = \theta\alpha^i + \theta^p\alpha^{pi}$. Thus, $y_{i+(p-1)n} = y_i$ for all $i \geq 0$. Therefore, the sequence $\{y_i\}$ has period length $d = p^2 - 1 \leq (p-1)n \leq (p-1)p < p^2 - 1$; a contradiction. Hence, $y_i \neq 0$ for $1 \leq i \leq p$.

Suppose the initial seed is $x_0 = 0$. Then, by mathematical induction on i, it is easily proved that $x_i = y_{i+1}y_i^{-1}$, for $0 \leq i \leq p$, if we use the fact that $y_i \neq 0$ for $1 \leq i \leq p$. Hence, $x_i \neq 0$ for $1 \leq i \leq p-1$, and so $\{x_i\}$ has period length at least p. This obviously implies that the sequence $\{x_i\}$ must have period length p and, in particular, $\{x_0, x_1, \ldots, x_{p-1}\} = \mathbb{Z}_p \cong \mathbb{F}_p$. Also, for an arbitrary initial seed x_0, the corresponding sequence $\{x_i\}$ is just a shifted version of the sequence with initial seed $x_0 = 0$; thus, the sequence will still have period length p. □

Example 5.3.1. Consider the inversive congruential generator $x_{i+1} \equiv 2x_i^{-1}+3 \pmod 7$. The polynomial $x^2-3x-2 \equiv x^2+4x+5 \pmod 7$ is a primitive polynomial over $\mathbb{F}_7$, and therefore any sequence produced by this generator must have full period length. Indeed, with an initial seed $x_0 = 1$ for example, we obtain the sequence

$$1, 5, 2, 4, 0, 3, 6, 1, 5, \ldots$$

which has full period length 7.

Note that the converse of Theorem 5.3.1 does not hold. For instance, the generator $x_{i+1} \equiv x_i^{-1} + 3 \pmod 7$ yields sequences with full period length 7. As an example, with initial seed $x_0 = 5$, this generator produces the full period length sequence

$$5, 6, 2, 0, 3, 1, 4, 5, 6, \ldots$$

However, the polynomial $f(x) = x^2 - 3x - 1 \equiv x^2 + 4x + 6 \pmod 7$ is not a primitive polynomial over $\mathbb{F}_7$ since $ord(f) = 16 \neq 7^2 - 1$. Worthy of note is the fact that $f(x)$ is an irreducible polynomial in $\mathbb{F}_7[x]$. □

The following lemma and theorem were proved in 1986 by Eichenauer and Lehn [EL86], and stated in articles [EHT90, Hub94]. The proofs, however, will not be given in the present paper as they require several other results, which are interesting in their own right, but not relevant to our focus. For convenience, we shall denote the period length of an inversive congruential sequence $\{x_i\}$, with initial seed x_0, by

$$\nu(x_0) = min\{k \in \mathbb{Z}^+ |\ x_k = x_0\}.$$

Also, we need first define the concept of a *quadratic residue modulo p.*

Definition 5.3.1. *Let a be an integer and p a prime such that* $a \not\equiv 0 \pmod p$. *We say that a is a* ***quadratic residue modulo*** *p if there exists an integer q such that* $q^2 \equiv a \pmod p$. *If there does not exist such an integer q then a is called a* ***quadratic non-residue modulo*** *p.*

We may now state the aforementioned lemma and theorem.

Lemma 5.3.1. [EL86] *Let* $\{x_i\}$ *be an inversive congruential sequence generated by* (5.13). *Assume* $x_0 \neq x_1$ *and* $x_i \geq 1$ *for all* $i \geq 0$. *Then* $\nu(x_0) = \nu(0) + 1$.

□

Theorem 5.3.2. [EL86] *Let* $\{x_i\}$ *be an inversive congruential sequence generated by* (5.13)*. Then*

(i) $\nu(0) = p - 1$ *if* $4a + b^2 \equiv 0 \pmod{p}$*;*

(ii) $\nu(0) + 1$ *divides* $p - 1$ *if* $4a + b^2 \not\equiv 0 \pmod{p}$ *is a quadratic residue modulo* p*;*

(iii) $\nu(0) + 1$ *divides* $p + 1$ *if* $4a + b^2 \not\equiv 0 \pmod{p}$ *is quadratic non-residue modulo* p*.* □

The above two results will prove useful in the next section where we consider a composite modulus.

5.4 Inversive Congruential Generators With Composite Modulus

The inversive congruential method can also be implemented with a composite modulus m, but the sequences produced by such a generator have period lengths bounded above by $\phi(m)$, in comparison to m when m is a prime.

Let m be composite and let R_m be the set defined by $R_m = \{x \in \mathbb{Z}_m : (x, m) = 1\}$. Then, for each $x \in R_m$, there exists a unique inverse $x^{-1} \in R_m$ such that $xx^{-1} \equiv 1 \pmod{m}$. Note that R_m is a *reduced residue system* (mod m) and evidently contains $\phi(m)$ elements. In fact, R_m is a multiplicative group.

Now, the **inversive congruential generator with composite modulus** m generates an inversive congruential sequence $\{x_i\}_{i\geq 0}$, with elements in R_m, by the recursion

$$\boxed{x_{i+1} \equiv ax_i^{-1} + b \pmod{m}; \qquad x_{i+1} \in R_m} \tag{5.16}$$

where we choose initial seed $x_0 \in R_m$ and parameters $a \in R_m$, $b \in \mathbb{Z}_m$ in such a way that we have each x_i in R_m.

Since we have $a \in R_m$, so that $(a, m) = 1$, then a has a unique inversive modulo m; thus, the sequence $\{x_i\}$ is purely periodic with period length $d \leq |R_m| = \phi(m)$ (because all $x_i \in R_m$).

5.4.1 Huber's Generator

In 1994, Huber [Hub94] generalized Eichenauer and Lehn's [EL86] inversive congruential generator (5.13) for arbitrary composite moduli. Huber suggested an alternative for

composite modulus m, which does not necessarily restrict all x_i to the set $R_m \cup \{0\}$, leading to considerably greater period lengths.

Huber's inversive generator produces a sequence $\{y_i\}_{i\geq 0}$ of pseudorandom numbers defined by

$$\boxed{y_{i+1} \equiv a y_i^{\phi(m)-1} + b \pmod{m}; \qquad 0 \leq y_{i+1} < m} \tag{5.17}$$

where $a \in R_m$ and $b, y_0 \in \mathbb{Z}_m$. As $y^{\phi(m)} \equiv 1 \pmod{m}$ for each $y \in R_m$ (by *Euler's Theorem*), then if each $y_i \in R_m \cup \{0\}$, Huber's generator (5.17) reduces to the ordinary generator (5.16). On the contrary, if $y_i \neq 0$ and $y_i \notin R_m$ (i.e. $(y_i, m) \neq 1$), then recursion (5.17) still remains well defined. We therefore have a generator that produces a purely periodic sequence $\{y_i\}$ with least period length d bounded above by m in contrast to $\phi(m)$ for the ordinary generator (5.16). Furthermore, for appropriately chosen values of a, b, m, x_0, Huber's generator may produce sequences of pseudorandom numbers with longer periods than inversive congruential generator (5.16).

Example 5.4.1. Consider Huber's generator (5.17) with modulus $m = 21$ and parameters $a = 1$, $b = 4$. We find that, for any initial seed $y_0 \in \mathbb{Z}_m$, this generator produces a sequence $\{y_i\}$ of pseudorandom numbers with least period length $m = 21$, which cannot be attained using generator (5.16). □

In order to state a condition on a, b, m such that a sequence $\{y_i\}$, generated by (5.17), has full period length m, we first define an IMP polynomial.

Definition 5.4.1. *A polynomial of the form $f(x) = x^2 - bx - a$ is called an **inversive maximal period (IMP) polynomial** if the least period length of the sequence $\{x_i\}_{i\geq 0}$ defined by $x_{i+1} \equiv a x_i^{p-2} + b \pmod{p}$ equals p for prime p.*

Note that the recursion of Definition 5.4.1 is simply Huber's generator (5.17) with prime modulus p since $\phi(p) = p - 1$.

Let u_1, u_2 be the two zeros of $f(x)$, then $u_{1,2} = (b \pm D)/2$ where $D = \sqrt{b^2 + 4a}$. It was shown by Flahive and Niederreiter [FN92] that the period length of a sequence $\{x_i\}$, generated by (5.13) with initial seed $x_0 = 0$, is $n - 1$ where n is the order of $\xi = u_1/u_2$ in the multiplicative group $\mathbb{F}_{p^2}^*$. In addition, $f(x)$ is an IMP polynomial if and only if ξ has order $p + 1$. Flahive and Niederreiter [FN92] also showed that all primitive polynomials over $\mathbb{F}_p$ are IMP polynomials, but not conversely.

Example 5.4.2. Consider the generator $x_{i+1} \equiv a x_i^{p-2} + b \pmod{p}$ with parameters $a = 1$ and $b = 4$ (as in Example 5.4.1), and $p = 7$. For any choice of initial seed $x_0 \in \mathbb{Z}_p$, we obtain a sequence with full period length 7, as shown in the table below.

x_0	$x_{i+1} \equiv x^5 + 4 \pmod 7$
0	0, 4, 6, 3, 2, 1, 5, 0, 4, ...
1	1, 5, 0, 4, 6, 3, 2, 1, 5, ...
2	2, 1, 5, 0, 4, 6, 3, 2, 1, ...
3	3, 2, 1, 5, 0, 4, 6, 3, 2, ...
4	4, 6, 3, 2, 1, 5, 0, 4, 6, ...
5	5, 0, 4, 6, 3, 2, 1, 5, 0, ...
6	6, 3, 2, 1, 5, 0, 4, 6, 3, ...

Therefore, the polynomial $f(x) = x^2 - 4x - 1 \equiv x^2 + 3x + 6 \pmod 7$ is an IMP polynomial. But $x^2 + 3x + 6$ is not a primitive polynomial over $\mathbb{F}_7$. □

Theorem 5.4.1. [Hub94] *Let $p_1, \ldots, p_k$ be distinct primes. Then a sequence $\{y_i\}$ produced by Huber's generator* (5.17) *with modulus $m = \prod_{j=1}^{k} p_j$ has full period length m if and only if the polynomials $(x^2 - bx - a)$ modulo p_j are IMP polynomials over the fields $\mathbb{F}_{p_j}$ for $1 \leq j \leq k$.*

Proof. This result is immediately evident since the period length d modulo m is the least common multiple of the period lengths, p_j, of the sequences modulo p_j generated by (5.17). That is, $d = \prod_{j=1}^{k} p_j = m$. Explicitly, the polynomials $(x^2 - bx - a)$ modulo p_j are IMP polynomials over the fields $\mathbb{F}_{p_j}$ if and only if the sequences $\{x_i^{(j)}\}$ generated by $x_{i+1} \equiv a x_i^{p_j - 2} + b \pmod{p_j}$ have full period lengths p_j, $1 \leq j \leq k$. This is equivalent to $\{y_i\}$ having period length $d = lcm(p_1, \ldots, p_k) = \prod_{j=1}^{k} p_j = m$. □

In view of Theorem 5.4.1, for any given modulus $m = \prod_{j=1}^{k} p_j$, we can quite easily find values of a, b such that Huber's generator (5.17) produces a sequence $\{y_i\}$ of full period length m. One need only determine an IMP (or primitive) polynomial over each of the fields $\mathbb{F}_{p_j}$, $1 \leq j \leq k$. Then, from the coefficients of these polynomials, a and b can be computed using the *Chinese Remainder Theorem* (Theorem A.7). A specific example clearly outlines this method.

Example 5.4.3. Consider Huber's generator with modulus $m = 2^{14} - 1 = 16383 = 3 \cdot 43 \cdot 127$. Fast methods for determining primitive polynomials over finite fields are given in [Rab80, LN97]. We shall take the first primitive polynomials in lexicographic order. That is, $x^2 + x + 2 \in \mathbb{F}_3[x]$, $x^2 + x + 3 \in \mathbb{F}_{43}[x]$, and $x^2 + x + 3 \in \mathbb{F}_{127}[x]$. Then, equating these polynomials to $x^2 - bx - a$, we have

$$\begin{aligned}
(x^2 - bx - a) &\equiv x^2 + x + 2 \pmod 3, \\
(x^2 - bx - a) &\equiv x^2 + x + 3 \pmod{43}, \\
(x^2 - bx - a) &\equiv x^2 + x + 3 \pmod{127}.
\end{aligned}$$

Hence, $b = -1$ and to solve for a we apply the *Chinese Remainder Theorem* (see proof in Appendix A) to the system of congruences

$$\begin{aligned} -a &\equiv 2 \pmod 3, \\ -a &\equiv 3 \pmod{43}, \\ -a &\equiv 3 \pmod{127}. \end{aligned}$$

Now, $n_1 = 5461$, $n_2 = 381$, $n_3 = 129$ and solving for x_i in each of the following

$$\begin{aligned} n_1 x_1 &\equiv 2 \pmod 3, \\ n_2 x_2 &\equiv 3 \pmod{43}, \\ n_3 x_3 &\equiv 3 \pmod{127}, \end{aligned}$$

yields $x_1 = 2$, $x_2 = 21$ and $x_3 = 65$ so that $-a = n_1 x_1 + n_2 x_2 + n_3 x_3 = 27308 \equiv -5458 \pmod{16383}$. Therefore, $a = 5458$.
Also, note that $\phi(m) = \phi(3 \cdot 43 \cdot 127) = 16383(1 - 1/3)(1 - 1/43)(1 - 1/127) = 10584$. Thus, by Theorem 5.4.1, the sequence $\{y_i\}$, generated by

$$y_{i+1} \equiv 5458 y_i^{10583} - 1 \pmod{16383},$$

attains full period length $m = 16383$.

□

5.4.2 Inversive Generators With Modulus Divisible By A Square

Now, let the modulus $m = \prod p_j^{\alpha_j}$ with at least one $\alpha_j \geq 2$. We shall only be concerned with purely periodic sequences, and so the period length of Huber's generator (5.17) is still the least common multiple of the period lengths of the sequences modulo $p_j^{\alpha_j}$. Let ν be the period length of the sequence $\{x_i\}$ generated by $x_{i+1} \equiv a x^{\phi(p^\alpha)-1} + b \pmod p$. For the case $\nu > 1$, the main theorem of Eichenauer-Herrmann and Topuzoğlu's paper [EHT90] reads as follows:

Theorem 5.4.2. [EHT90] *Let $\alpha \geq 2$, $\nu \geq 2$, and p be a prime. Then the period length of the inversive congruential generator* (5.16) *with modulus p^α equals $\nu p^{\alpha-1}$ if and only if $x_\nu \not\equiv x_0 \pmod{p^2}$.* □

Using results proved by Eichenauer and Lehn [EL86], Huber [Hub94] showed that $\nu \leq (p+1)/2$.

Theorem 5.4.3. [Hub94] *Let p be a prime and $\alpha \geq 2$. Then the period length of inversive congruential generator* (5.16) *with modulus p^α is at most $\frac{p+1}{2}p^{\alpha-1}$ if $p \geq 3$, or $2^{\alpha-1}$ if $p = 2$.*

Proof. In view of Theorem 5.4.2, for $p \geq 3$, the upper-bound for ν is an immediate consequence of Lemma 5.3.1 and Theorem 5.3.2. The case $p = 2$ is treated in the next section of this chapter. □

Corollary 5.4.1. [Hub94] *The period lengths of the sequences produced by Huber's generator* (5.17) *for modulus $m = p^\alpha$, $\alpha \geq 2$, are at most $\frac{p+1}{2}p^{\alpha-1}$ if $p \geq 3$, or $2^{\alpha-1}$ if $p = 2$.*

Consider inversive generator (5.16) with prime-power modulus $m = p^\alpha$, $\alpha \geq 2$. We now treat the problem of determining a and b such that this generator yields sequences with maximal period length $(p+1)p^{\alpha-1}/2$.

By setting $\nu(0)+\nu(x_0) = p$, with $\nu(x_0) = (p+1)/2$, it is first deduced from Lemma 5.3.1 and Theorem 5.3.2 that $4a + b^2$ must be a quadratic non-residue modulo p. Moreover, $\xi = u_1/u_2$ (where $u_{1,2} = (b \pm \sqrt{4a+b^2})/2$) must have order $(p+1)/2$ modulo p since we have $\nu(0) = (p+1)/2 - 1$. Let r be a quadratic non-residue of p, then we can write

$$\xi \equiv x + \sqrt{r}y \equiv \underbrace{\frac{b+\sqrt{4a+b^2}}{b-\sqrt{4a+b^2}}}_{(*)} \equiv \underbrace{\frac{b+\sqrt{r}\frac{\sqrt{r(4a+b^2)}}{r}}{b-\sqrt{r}\frac{\sqrt{r(4a+b^2)}}{r}}}_{(**)} \pmod{p}, \tag{5.18}$$

where it should be noted that $\sqrt{r(4a+b^2)}$ is an element of $\mathbb{F}_p$.

Now, using $(**)$, we obtain the relation

$$x^2 - ry^2 \equiv 1 \pmod{p}, \tag{5.19}$$

and by comparing integer and surd parts of $x + \sqrt{r}y$ with $(*)$, we find that

$$b^2 \equiv -2a(x+1) \pmod{p}, \tag{5.20}$$

where (5.19) is simply *Pell's equation* modulo p.

Thus, to determine the required a and b we proceed as follows. First we find a quadratic non-residue r modulo p and a solution (x, y) to Pell's equation (5.19), which leads to $\xi = x + \sqrt{r}y$ of order $(p+1)/2$ modulo p. We then select an a such that equation (5.20) can be solved for b (i.e. $-2a(x+1)$ must be a quadratic residue of p). Finally, we check whether the period length of inversive generator (5.16) with modulus p equals $(p+1)/2$, and if $x_{(p+1)/2} \not\equiv x_0 \pmod{p^2}$. An example clearly illustrates this method.

Example 5.4.4. Let us determine parameters a and b such that, for the prime $p = 17$, the period length of the sequences produced by inversive generator (5.16) with modulus $m = p^\alpha$, $\alpha \geq 2$ equals $(p+1)p^{\alpha-1}/2$.

Since $\left(\frac{3}{17}\right) \equiv 3^8 \equiv 16 \equiv -1 \pmod{17}$ then $r = 3$ is a quadratic non-residue of 17. Here, we have used the *Legendre symbol* and *Euler's Criterion*. (See Appendix A – Definition A.1 and Theorem A.8 for clarification). An obvious solution of Pell's equation $x^2 - 3y^2 \equiv 1 \pmod{17}$ is $(x, y) = (2, 1)$. Now, $x + \sqrt{r}y = 2 + \sqrt{3}$ has order $18 = p + 1$. Hence, since we require ξ to have order $(p+1)/2 = 9$ then we set $\xi \equiv (2+\sqrt{3})^2 \equiv 7+4\sqrt{3} \pmod{17}$. Therefore, we take $x = 7$ in equation (5.20) so that $b^2 \equiv a \pmod{17}$. Setting $a = 1$ we obtain $b = \pm 1$, which both give the desired generator for $x_0 = 3$.

To verify this for $a = b = 1$, we consider the period length of the inversive generator with prime modulus $p = 17$. For $x_0 = 3$, this generator yields the sequence

$$3, 7, 6, 4, 14, 12, 11, 15, 9, 3, 7, \ldots,$$

which has period length $(p + 1)/2 = 9$, as does any sequence it produces. We see that $x_9 = 9 \not\equiv 3 \pmod{289}$; that is, $x_{(p+1)/2} \not\equiv x_0 \pmod{p^2}$. Thus, one concludes that, for any $\alpha \geq 2$, the inversive generator defined by

$$x_{i+1} \equiv x_i^{-1} + 1 \pmod{17^\alpha}; \qquad x_{i+1} \in R_{17^\alpha}, \tag{5.21}$$

with $x_0 = 3$, produce a sequence $\{x_i\}$ with maximal period length $(p + 1)p^{\alpha-1}/2 = 9 \cdot 17^{\alpha-1}$.

For example, if we take $\alpha = 2$, then generator (5.21) gives the sequence

$$3, 194, 74, 208, 133, 114, 181, 100, 264, 105, 279, 261, 259, 184, 12, 266, 202, 94,$$
$$207, 75, 159, 21, 235, \ldots, 96, 287, 145, 3, 194, 74, \ldots$$

with maximal period length
$9 \cdot 17^{\alpha-1} = 153$. □

Note that solutions of Pell's equation $x^2 - ry^2 = 1$ may be derived by considering the *convergents* of the simple *continued fraction* expansion of $\sqrt{r}$. Most elementary number theory textbooks deal with this topic, and the reader is referred to [Ros00] which discusses the problem in quite some detail.

In summary of this section, we have seen a generalization of Eichenauer and Lehn's inversive congruential generator (5.13) to arbitrary composite modulus m. It has been established that the maximal period length of the purely periodic generators (5.17), with

modulus $m = \prod_{j=1}^{k} p_j^{\alpha_j}$, equals

$$lcm(\nu_1, \nu_2, \ldots, \nu_k) \text{ where } \nu_j = \begin{cases} p_j & \text{if } \alpha_j = 1, \\ \frac{p_j+1}{2} p_j^{\alpha_j - 1} & \text{if } \alpha_j \geq 2, \text{and } p_j \geq 3, \\ 2^{\alpha_j - 1} & \text{if } \alpha_j \geq 2, \text{and } p_j = 2. \end{cases}$$

Also, a simple method involving Pell's equation has been given to determine parameters a and b for maximal period length. Note that we have not actually proven that $\nu_j = 2^{\alpha_j - 1}$ if $\alpha_j \geq 2$ and $p_j = 2$; this is treated in the next section, which is the last of this chapter.

5.5 Inversive Congruential Generators With Power of Two Modulus

In practice, as always, the most commonly used composite modulus is a power of 2 with this type of inversive congruential generator first being introduced by Eichenauer, Lehn and Topuzoğlu [ELT88]. It is also studied in quite substantial detail in the articles [Nie89, ELNT90].

Suppose inversive congruential generator (5.13) has modulus $m = 2^\beta \geq 8$. By our discussion in Section 5.4, we must have both $a \equiv 1 \pmod 2$ and $x_0 \equiv 1 \pmod 2$ so that $(a, 2^\beta) = (x_0, 2^\beta) = 1$ and $a, x_0 \in R_{2^\beta}$. Then $x_i \in R_{2^\beta}$ for all i if and only if $b \equiv 0 \pmod 2$.

We may now consider the **inversive congruential generator with power of two modulus** $m = 2^\beta$, which generates a sequence $\{x_i\}_{i \geq 0}$ by the recursion

$$\boxed{x_{i+1} \equiv a x_i^{-1} + b \pmod{2^\beta}; \qquad x_{i+1} \in R_{2^\beta}} \tag{5.22}$$

where $\beta \geq 3$, and parameters $a, b, x_0 \in \mathbb{Z}_{2^\beta} = \{0, 1, \ldots, 2^\beta - 1\}$ are chosen such that $a \equiv 1 \pmod 2$, $b \equiv 0 \pmod 2$, and $x_0 \equiv 1 \pmod 2$ so that each $x_i \in R_{2^\beta}$.

Since $x_i \in R_{2^\beta}$ for all i, each x_i has a unique inverse x_i^{-1} modulo 2^β, and therefore, the corresponding inversive congruential sequence $\{x_i\}$ is purely periodic with period length not exceeding $\phi(2^\beta) = 2^{\beta-1}$.

The next theorem establishes conditions on a and b such that an inversive congruential sequence $\{x_i\}$ modulo $m = 2^\beta \geq 8$ has maximal period length $m/2 = 2^{\beta-1}$. First we prove the following lemma, which will be required in the proof the theorem.

Lemma 5.5.1. *Let* $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 4s+1 & 4t+2 \end{pmatrix}$ *for some integers* $s, t \geq 0$. *Then*

$$\mathbf{A}^{2^{n-2}} \equiv \begin{pmatrix} 2^{n-1}s + 2^{n-2} + 1 & 2^{n-1}t + 3 \cdot 2^{n-2} \\ 2^{n-1}t + 3 \cdot 2^{n-2} & 2^{n-1}s + 3 \cdot 2^{n-2} + 1 \end{pmatrix} \pmod{2^n} \tag{5.23}$$

for all integers $n \geq 4$.

Proof. By computation, one finds that

$$\mathbf{A}^4 = \begin{pmatrix} 16w + 8s + 5 & 16x + 8t + 12 \\ 16y + 8t + 12 & 16z + 8s + 13 \end{pmatrix} \text{ for some integers } w, x, y, z \geq 0, \text{ and hence}$$

$$\mathbf{A}^4 = \mathbf{A}^{2^{4-2}} \equiv \begin{pmatrix} 2^{4-1}s + 2^{4-2} + 1 & 2^{4-1}t + 3 \cdot 2^{4-2} \\ 2^{4-1}t + 3 \cdot 2^{4-2} & 2^{4-1}s + 3 \cdot 2^{4-2} + 1 \end{pmatrix} \pmod{2^4}.$$

It then follows, by mathematical induction on n, that

$$\mathbf{A}^{2^{n-2}} = \begin{pmatrix} 2^n w' + 2^{n-1}s + 2^{n-2} + 1 & 2^n x' + 2^{n-1}t + 3 \cdot 2^{n-2} \\ 2^n y' + 2^{n-1}t + 3 \cdot 2^{n-2} & 2^n z' + 2^{n-1}s + 3 \cdot 2^{n-2} + 1 \end{pmatrix}$$

for some integers $w', x', y', z' \geq 0$, so that we have

$$\mathbf{A}^{2^{n-2}} \equiv \begin{pmatrix} 2^{n-1}s + 2^{n-2} + 1 & 2^{n-1}t + 3 \cdot 2^{n-2} \\ 2^{n-1}t + 3 \cdot 2^{n-2} & 2^{n-1}s + 3 \cdot 2^{n-2} + 1 \end{pmatrix} \pmod{2^n}$$

for all integers $n \geq 4$. □

Note. It is useful to note that Lemma 5.5.1 implies

$$\mathbf{A}^{2^{n-2}} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2^{n-1}(s+t) + 2^n + 1 \\ 2^{n-1}(s+t+1) + 2^n + 1 \end{pmatrix} \equiv \begin{pmatrix} 2^{n-1}(s+t) + 1 \\ 2^{n-1}(s+t+1) + 1 \end{pmatrix} \pmod{2^n} \tag{5.24}$$

for all integers $n \geq 4$.

Theorem 5.5.1. [ELT88] *The inversive congruential generator, with modulus* $m = 2^\beta \geq 8$, *produces a sequence* $\{x_i\}$ *with maximal period length* $m/2 = 2^{\beta-1}$ *if and only if* $a \equiv 1 \pmod 4$ *and* $b \equiv 2 \pmod 4$.

Proof. (Adapted from [ELT88]).
Suppose the inversive congruential generator (5.22) generates a sequence $\{x_i\}$ with maximal period length $m/2 = 2^{\beta-1}$ where $\beta \geq 3$. Without loss of generality, we may take initial seed $x_0 = 1$ since we must have $\{x_0, x_1, \ldots, x_{(m/2)-1}\} = R_{2^\beta}$.

Now, if we take $\beta = 2$, then the sequence $\{x_i\}$ modulo $2^2 = 4$ has least period length 2, and therefore $x_2 \equiv x_0 \equiv 1 \pmod 4$. Also, if we take $\beta = 3$, then $\{x_i\}$ modulo $2^3 = 8$

has least period length 4 so that $x_2 \not\equiv x_0 \pmod 8$; that is, $x_2 \not\equiv 1 \pmod 8$, and hence $x_2 \equiv 5 \pmod 8$.

For all $x \in R_8 = \{1, 3, 5, 7\}$, $x^{-1} \equiv x \pmod 8$. Consequently, from generator (5.22) with $\beta = 3$, we obtain

$$x_2 \equiv a(a+b) + b \equiv (a+1)b + 1 \pmod 8 \tag{5.25}$$

since $a \in R_8$. Thus, $(a+1)b \equiv 4 \pmod 8$ since $x_2 \equiv 5 \pmod 8$, and this implies that $(a+1)b = 4+8k$ for some integer k, so that $(a+1)b = 2(2+4k)$ or $ab+b = (1+4k)2+2$. Hence, $a = 1+4k$ and $b = 2+4k$, and therefore $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$.

Conversely, suppose that $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$, and consider the sequence $\{x_i\}$ obtained from inversive congruential generator (5.22). Again, let us assume that $x_0 = 1$.

For modulus $m = 2^3 = 8$, it is immediately evident from the above reasoning, and using (5.25), that the sequence $\{x_i\}$ has maximal period length $m/2 = 4$. Therefore, consider generator (5.22) with modulus $m = 2^\beta \geq 16$.

Observe that since $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$ then $a + b \equiv 3 \pmod 4$, and so $a + b = 3 + 4k = 1 + 2(1 + 2k)$ for some integer k; thus, $a + b \equiv 1 \pmod 2$.
Consider the second-order linear recurring sequence $\{y_i\}_{i\geq 0}$ defined by

$$y_0 = y_1 = 1, \qquad y_{i+2} \equiv by_{i+1} + ay_i \pmod{2^\beta}; \qquad 0 \leq y_i < 2^\beta. \tag{5.26}$$

Since $a + b \equiv 1 \pmod 2$ then it follows that $y_i \equiv 1 \pmod 2$ for all $i \geq 0$, by strong mathematical induction on i. That is, each $y_i \in R_{2^\beta}$, and so has a unique inverse y_i^{-1} modulo 2^β.

It is now deduced from (5.26) that

$$\begin{aligned} &y_{i+2}y_{i+1}^{-1} \equiv by_{i+1}y_{i+1}^{-1} + ay_iy_{i+1}^{-1} \equiv ay_iy_{i+1}^{-1} + b \pmod{2^\beta}, \qquad \text{and hence} \\ &y_{i+2}y_{i+1}^{-1} \equiv a(y_{i+1}y_i^{-1})^{-1} + b \pmod{2^\beta}; \qquad i \geq 1. \end{aligned} \tag{5.27}$$

Using (5.27) and (5.22), it can easily be proved by mathematical induction on i that since $x_0 = y_0 = y_1 = 1$ then

$$x_i \equiv y_{i+1}y_i^{-1} \pmod{2^\beta} \qquad \text{for all } i \geq 0. \tag{5.28}$$

Now, recursion (5.26) can be written in matrix form as

$$\begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} \equiv \mathbf{A} \begin{pmatrix} y_{i-1} \\ y_i \end{pmatrix} \pmod{2^\beta} \qquad \text{for all } i \geq 0,$$

where the matrix $\mathbf{A} = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 4s+1 & 4t+2 \end{pmatrix}$ for some integers $s, t \geq 0$, since $a \equiv 1 \pmod 4$ and $b \equiv 2 \pmod 4$. Therefore,

$$\begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} \equiv \mathbf{A}^i \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{2^\beta} \qquad \text{for all } i \geq 0. \tag{5.29}$$

If we set $n = \beta + 2$ in (5.24) then

$$\mathbf{A}^{2^\beta} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \mathbf{A}^m \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2^{\beta+1}(s+t)+1 \\ 2^{\beta+1}(s+t+1)+1 \end{pmatrix} \pmod{2^{\beta+2}} \equiv \begin{pmatrix} 1 \\ 1 \end{pmatrix} \pmod{2^\beta}.$$

Consequently, (5.29) yields

$$\begin{pmatrix} y_{i+m} \\ y_{i+m+1} \end{pmatrix} \equiv \mathbf{A}^{i+m} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \mathbf{A}^i \mathbf{A}^m \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \mathbf{A}^i \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} y_i \\ y_{i+1} \end{pmatrix} \pmod{2^\beta} \qquad i \geq 0,$$

and therefore $y_{i+m} = y_i$ for all $i \geq 0$. Moreover, it follows from (5.28) that $x_{i+m} = x_i$ for all $i \geq 0$. Hence, the period length, d, of the sequence $\{x_i\}$ must divide $m = 2^\beta$. Since it was previously shown that $d \leq m/2$, then to prove $d = m/2$ we need only show that $d > m/4$.

Suppose sequence $\{x_i\}$ has period length $d \leq m/4$ then $x_{m/4} = x_0 = 1$, and so we have $y_{(m/4)+1} = y_{m/4}$, by (5.28). However, if we consider (5.24) with $n = \beta$ then

$$\mathbf{A}^{2^{\beta-2}} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \mathbf{A}^{m/4} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2^{\beta-1}(s+t)+1 \\ 2^{\beta-1}(s+t+1)+1 \end{pmatrix} \pmod{2^\beta}.$$

Using (5.29), we find that

$$\begin{pmatrix} y_{m/4} \\ y_{(m/4)+1} \end{pmatrix} \equiv \mathbf{A}^{m/4} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 2^{\beta-1}(s+t)+1 \\ 2^{\beta-1}(s+t+1)+1 \end{pmatrix} \pmod{2^\beta},$$

which implies that $y_{(m/4)+1} \equiv y_{m/4} + 2^{\beta-1} \pmod{2^\beta}$; a contradiction, and therefore $d > m/4$.

Thus, if the sequence $\{x_i\}$ has initial seed $x_0 = 1$, then it has maximal period length $d = m/2 = 2^{\beta-1}$ so that $\{x_0, x_1, \ldots, x_{(m/2)-1}\} = R_m$. For an arbitrary initial seed $x_0 \in R_m$, the corresponding sequence $\{x_i\}$ will just be a shifted version of the sequence with initial seed $x_0 = 1$, and so will also have period length equal to $m/2 = 2^{\beta-1}$. □

A similar inversive congruential generator to (5.22), with modulus $m = 2^\beta \geq 8$, was proposed by Kato, Wu and Yanagihara [KWY96] in 1996. This particular method generates a sequence $\{x_i\}_{i \geq 0}$ by the recursion

$$\boxed{x_{i+1} \equiv a x_i^{-1} + b + c x_i \pmod{2^\beta}; \qquad x_{i+1} \in R_{2^\beta}} \tag{5.30}$$

where parameters $a, b, c \in \mathbb{Z}_{2^\beta} = \{0, 1, \ldots, 2^\beta - 1\}$ and $x_0 \in R_{2^\beta}$ are chosen such that $x_i \in R_{2^\beta}$ implies $x_{i+1} \in R_{2^\beta}$ so that $x_i \in R_{2^\beta}$ for all i.

The following result is analogous to that of Theorem 5.5.1 and its proof is extremely similar, although quite lengthy since sufficiency must be proved by separately considering the two possibilities for parameter c – either even or odd. The proof is therefore omitted.

Theorem 5.5.2. [KWY96] *The inversive congruential generator* (5.30)*, with modulus* $m = 2^\beta \geq 8$*, produces a sequence* $\{x_i\}$ *with maximal period length* $m/2 = 2^{\beta-1}$ *if and only if* $a + c \equiv 1 \pmod 4$ *and* $b \equiv 2 \pmod 4$. □

We end this chapter with a simple example which illustrates Theorem 5.5.1.

Example 5.5.1. Consider the inversive congruential generator (5.22) with modulus $m = 2^4$ and parameters $a = 13 \equiv 1 \pmod 4$, $b = 10 \equiv 2 \pmod 4$. Any choice of initial seed $x_0 \in R_{16}$ yields a sequence $\{x_i\}$ with maximal period length $m/2 = 8$. For example, with $x_0 = 9$, we obtain the sequence

$$9, 15, 13, 11, 1, 7, 5, 3, 9, 15, \ldots$$

with maximal period length 8. On the other hand, the generator $x_{i+1} \equiv 11x_i^{-1} + 10 \pmod{16}$ does not produce a maximal period length sequence for any choice of $x_0 \in R_{16}$, as expected by Theorem 5.5.1 since $a = 11 \not\equiv 1 \pmod 4$. This generator only produces sequences with period lengths at most $m/4 = 4$, as shown in the table below.

x_0	$x_{i+1} \equiv 11x_i^{-1} + 10 \pmod{16}$	Period Length
1	1, 5, 9, 13, 1, 5, ...	4
3	3, 3, 3, 3, 3, 3, ...	1
5	5, 9, 13, 1, 5, 9, ...	4
7	7, 7, 7, 7, 7, 7, ...	1
9	9, 13, 1, 5, 9, 13, ...	4
11	11, 11, 11, 11, 11, 11 ...	1
13	13, 1, 5, 9, 13, 1, ...	4
15	15, 15, 15, 15, 15, 15, ...	1

Chapter 6

A Special Type of Pseudorandom Number Generator

Having now considered some of the most common types of pseudorandom number generators, our final chapter will focus on a special type of generator. Currently adopted in Matlab for its `rand` function, it is known as the *subtract-with-borrow generator*, and was first proposed by Marsaglia and Zaman [MZ91] in 1991, along with the closely related *add-with-carry generator*. As already mentioned in Chapter 2, prior to Matlab version 5.0, a specific pure multiplicative congruential generator was used for random number generation. However, on the advice of George Marsaglia in 1995, this new kind of generator was chosen for Matlab 5.0 on the basis that a period length on the order of 2^{32} is far too short for modern needs. The main reason for its appeal is its ability to generate sequences with immensely long periods, given an initial set of r (typically from 20 to 50) seed values. It also possesses an interesting underlying theory, requiring results in both number theory and group theory.

In this chapter, we will examine two general forms of the subtract-with-borrow generator and, in each case, establish the conditions under which maximal period length sequences are produced. We will introduce such generators in Section 6.1, and then provide an analysis of the period lengths of subtract-with-sequences in Section 6.2. Section 6.3 will give a brief description of the specific subtract-with-borrow generator used in Matlab.

6.1 The Subtract-With-Borrow Generator

It is most convenient to introduce the subtract-with-borrow generator by considering a simple generator of the form

$$x_i \equiv x_{i-2} - x_{i-1} \pmod{10}; \qquad 0 \leq x_0 < 10, \tag{6.1}$$

which has a specified initial seed vector $(x_1, x_2) \in \mathbb{Z}_{10}^2$. Suppose we choose $(0, 1)$ as the seed vector, then the generated sequence is

$$0, 1, 9, 2, 7, 5, 2, 3, 9, 4, 5, 9, \ldots$$

Consider the set X of 1×2 vectors $\mathbf{x} = (x_1, x_2)$ with elements in $\mathbb{Z}_{10}$; namely, the set $X = \mathbb{Z}_{10}^2$. We can view this generator as a second-order congruential generator with iterating function $f : \mathbb{Z}_{10}^2 \longrightarrow \mathbb{Z}_{10}^2$ defined by $f(x_1, x_2) = (x_2, x_1 + x_2 \pmod{10})$. Given an initial seed vector $\mathbf{x} \in \mathbb{Z}_{10}^2$, the generated sequence is

$$\mathbf{x}, f(\mathbf{x})f^2(\mathbf{x}), f^3(\mathbf{x}), \ldots,$$

where $f^2(\mathbf{x}) = f(f(\mathbf{x}))$, $f^3(\mathbf{x}) = f(f(f(\mathbf{x})))$, and so on. Since f has an inverse, for any initial seed vector $\mathbf{x} \in \mathbb{Z}_{10}^2$, this sequence is purely periodic. According to Marsaglia [Mar92], depending on the initial seed vector, this generator produces sequences having either the longest period of 60 terms or smaller period lengths 1, 3, 4, 12 and 20. Each period length is the least common multiple of the period lengths for moduli 2 and 5 (*cf.* Lemma 2.1.2).

Now, the subtract-with-borrow version of this generator is defined as follows. We assign two initial values, such as 0 and 1, and an initial 'borrow bit', say 0. Then each new digit is the difference of the previous two digits *minus the borrow bit*. According to whether the difference is positive or negative, the next borrow bit is set to 0 or 1 respectively, and the result is taken modulo 10. For example, using a superscript to indicate the borrow bit, the above sequence of digits becomes

$$0, 1^0, 9^1, 1^1, 7^0, 4^1, 2^0, 2^0, 0^0, 2^0, 8^1, 3^1, 4^0, 1^1, 2^0, 9^1, 2^1, 6^0, \ldots$$

For this particular generator, we now let X be the set of all 1×3 vectors $\mathbf{x} = (x_1, x_2, c)$, with $x_1, x_2 \in \mathbb{Z}_{10}$ and $c \in \{0, 1\}$, so that $X = \{(x_1, x_2, c) : \ x_1, x_2 \in \mathbb{Z}_{10}, c \in \mathbb{Z}_2\}$. Our iterating function f is now

$$f(x_1, x_2, c) = \begin{cases} (x_2, x_1 - x_2 - c, 0) & \text{if } x_1 - x_2 - c \geq 0, \\ (x_2, x_1 - x_2 - c + 10, 1) & \text{if } x_1 - x_2 - c < 0, \end{cases}$$

which gives a precise description of the generator, informally defined by $x_i \equiv x_{i-2} - x_{i-1} - c \pmod{10}$. Of course, a different generator could be formed by

$x_i \equiv x_{i-1} - x_{i-2} - c \pmod{10}$ since the order of subtraction matters. More generally, the informal rules for the subtract-with-borrow methods are $x_i \equiv x_{i-r} - x_{i-s} - c \pmod{b}$ and $x_i \equiv x_{i-s} - x_{i-r} - c \pmod{b}$, for some *base* b and *lags* r, s. To formally define these generators, and subsequently establish their period lengths, it is henceforth assumed that $r > s$, and we define the finite set X of $1 \times (r+1)$ vectors $\mathbf{x} = (x_1, x_2, \ldots, x_r, c)$, where $x_1, x_2, \ldots, x_r \in \mathbb{Z}_b$ for some *base* b, and $c \in \{0, 1\}$. Then the corresponding iterating function for $x_i \equiv x_{i-r} - x_{i-s} - c \pmod{b}$ is given by

$$f(x_1, \ldots, x_r, c) = \begin{cases} (x_2, \ldots, x_r, x_1 - x_{r+1-s} - c, 0) & \text{if } x_1 - x_{r+1-s} - c \geq 0, \\ (x_2, \ldots, x_r, x_1 - x_{r+1-s} - c + b, 1) & \text{if } x_1 - x_{r+1-s} - c < 0. \end{cases}$$

Or, for the case $x_i \equiv x_{i-s} - x_{i-r} - c \pmod{b}$,

$$f(x_1, \ldots, x_r, c) = \begin{cases} (x_2, \ldots, x_r, x_{r+1-s} - x_1 - c, 0) & \text{if } x_{r+1-s} - x_1 - c \geq 0, \\ (x_2, \ldots, x_r, x_{r+1-s} - x_1 - c + b, 1) & \text{if } x_{r+1-s} - x_1 - c < 0. \end{cases}$$

In either case, the generated sequence will be purely periodic for appropriately chosen base b, lags r and s, and initial seed vector $\mathbf{x}$. As we shall see, sequences produced by such generators may have a maximal period length of $b^r - b^s - 2$ or $b^r - b^s$ respectively.

6.2 Period Lengths of the Generator

In order to establish the period lengths of subtract-with-borrow sequences, we require the use of some basic results in number theory specifically relating to the *base b expansion* of a proper fraction, rather than the conventional base 10 (decimal expansion).

6.2.1 Some Number Theory

Theorem 6.2.1. *Let γ be a real number with $0 \leq \gamma < 1$, and let b be a positive integer, $b > 1$. Then γ can be uniquely written as*

$$\gamma = \sum_{j=1}^{\infty} a_j / b_j,$$

where the coefficients a_j are integers, and $0 \leq a_j \leq b - 1$ for $j = 1, 2, \ldots$, with the restriction that for every positive integer N there exists an integer n with $n \geq N$ and $a_n \neq b - 1$.

Proof. See Rosen [Ros00]. □

The unique expansion of a real number in the form $\gamma = \sum_{j=1}^{\infty} a_j/b_j$ is called the *base b expansion* of this number and is denoted by $(.a_1a_2a_3\ldots)_b$. In this context, a base b expansion $(.a_1a_2a_3\ldots)_b$ is said to be *periodic* if there exist positive integers N and k such that $a_{n+k} = a_n$ for $n \geq N$. For example, the decimal expansions $1/6 = (.16666\ldots) = (.1\bar{6})_{10}$ and $1/7 = (.14285714285714\ldots)_{10} = (.\overline{142857})_{10}$ are both periodic, having respective pre-period lengths 1 and 0, and least period lengths 1 and 6.

Consider a positive integer m and the multiplicative group of $\phi(m)$ reduced residues modulo m relatively prime to m; that is, $R_m = \{x \in \mathbb{Z}_m : (x, m) = 1\}$. For an element n in R_m, we wish to determine the base b expansion of n/m. According to the following theorem, such an expansion will be purely periodic with least period length the order of b in R_m (assuming b is in R_m).

Theorem 6.2.2. *Suppose b is a positive integer. Then a periodic base b expansion represents a rational number. Conversely, the base b expansion of a rational number either terminates or is periodic. Further, if $0 < \alpha < 1$, $\alpha = n/m$, where n and m are relatively prime positive integers, and $m = TU$ where every prime factor of T divides b and $(U, b) = 1$, then the period length of the base b expansion of α is $ord_U b$, and the pre-period length is N, where N is the smallest non-negative integer such that $T \mid b^N$.*

Proof. See Rosen [Ros00]. □

Example 6.2.1. Suppose we wish to determine the period and pre-period lengths of the base 10 expansion of $\alpha = 5/52$. Since $52 = 2^2 \cdot 13 = TU$, it is deduced from Theorem 6.2.2 that the pre-period length is 2 and the period length is $ord_{13}10 = 6$. As $5/52 = (.09\overline{615384})_{10}$, we see that these lengths are correct. For the base 5 expansion of α, one determines that $T = 1$, $U = 52$ so that the pre-period length is 0 and the least period length is $ord_{52}5 = 4$. Certainly, we compute $5/52 = (.\overline{0220})_5$. This illustrates that if the base is relatively prime to the denominator then $T = 1$, and therefore the expansion is purely periodic.

Of particular relevance to this chapter is the case $\alpha = n/p$, where p is a prime, $1 \leq n < p$, and the base b is a primitive root of p. For such a rational number α, the base b expansion has pre-period length 0 and period length $ord_p b = \phi(p) = p - 1$. Hence, α has a purely periodic base b expansion with maximum possible period length $p - 1$. If b is not a primitive root of p, it follows from Theorem 2.2.1 and *Euler's Theorem* (Theorem A.5) that the period length must divide $\phi(p) = p - 1$. □

The cyclic subgroup generated by b, $\langle b \rangle = \{b^j \mid j = 0, 1, 2, \ldots\}$, partitions R_m into cosets. That is, two elements n and k of R_m are in the same coset if $n = kb^j$ for some

j. Consequently, if these two elements n and k belong to the same coset then n/m and k/m will have the same base b expansion (with period length the order of b), except that the digits in their periods will be cyclic permutations of one another. We demonstrate with an example.

Example 6.2.2. Let modulus $m = 41$, base $b = 10$ so that $R_{41} = \mathbb{Z}_{41}^*$, the multiplicative group of non-zero reduced residues of 41. The cyclic subgroup generated by 10 is $\langle 10\rangle = \{1, 10, 18, 16, 37\}$, and hence $ord_{41}10 = 5$. For successive elements n in $\langle 10\rangle$, one sees that the decimal expansions of $n/41$ are purely periodic (with period length 5) and consist of a common set of five digits, each a cyclic permutation of the preceding one:

$$1/41 = 0.024390243\ldots, \quad 10/41 = 0.243902439\ldots, \quad 18/41 = 0.43902439\ldots,$$
$$16/41 = 0.390243902\ldots, \quad 37/41 = 0.902439024\ldots$$

Now, choosing an element, say 11, not in the coset $\langle 10\rangle$, then 11 is in the coset $11\langle 10\rangle = \{11, 28, 34, 12, 38\}$. Again, the decimal expansions of n/m, where $n \in 11\langle 10\rangle$, have the same digits in their periods of length 5, each shifted by one place due to successive multiplications by 10:

$$11/41 = 0.268292682\ldots, \quad 28/41 = 0.682926829\ldots, \quad 34/41 = 0.829268292\ldots,$$
$$12/41 = 0.292682926\ldots, \quad 38/41 = 0.926829268\ldots$$

□

Our interest lies in choosing primes m such that b is a primitive modulo m, in which case $\phi(m) = m - 1$ is the period length of the base b expansion of every proper fraction of the form n/m, for $1 \leq n < m$.

6.2.2 Period Length of a Subtract-With-Borrow Sequence

We now provide two fundamental results for determining the period length of subtract-with-borrow sequences. It will become clear that the sequence of digits produced by a subtract-with-borrow generator, taken in the reverse order, is the same as the sequence of digits of the base b expansion of a proper fraction $n/(b^r - b^2 \pm 1)$, where the choice of $\pm$ depends on the type of generator.

Theorem 6.2.3. [MZ91] *The period length of a subtract-with-borrow sequence generated by means of the relation* $x_i \equiv x_{i-r} - x_{i-s} - c \pmod{b}$ *is the period length of the base* b *expansion of* n/m *for some* n, $1 \leq n < m$, *and* $m = b^r - b^s - 1$.

Proof. Rather than give a tiresome general proof, we consider a specific case $r = 5$, $s = 3$ and modulus $b = 10$ so that our generator has the form $x_i \equiv x_{i-5} - x_{i-3} - c \pmod{10}$. Initializing with seed vector $\mathbf{x} = (5, 9, 7, 7, 7, 0)$ yields the sequence

$$5, 9, 7, 7, 7, 8, 1, 0, 9, 5, 8, 2, 4, 0, 3, \ldots$$

Let I be the integer whose digits are the first fifteen of the above sequence in the reverse order, so that $I = 304285901877795$. Now, shift I to the left by s positions by multiplying by b^s, and then add $b^s I$ to I to obtain:

$$\begin{aligned} I &= \quad 30428\mathbf{5901877795} \\ b^s I &= \underline{30428\mathbf{5901877795}000} \\ I + b^s I &= 304\mathbf{590187779}672795 \end{aligned}$$

As a direct consequence of the rule for forming the sequence, there is substring of digits (indicated in boldface) which is common to each of the three levels. Consider this boldface string as an integer $S = 590187779$. Since S appears in each of the three levels of the sum, we can construct a simple linear equation for S:

$$30428b^{10} + bS + 30428b^{13} + b^4 S + 5000 = b^6 S + 672795.$$

However, disregarding the leading three digits, and the last digit, of each level leads to a much simpler equation for S:

$$30428b^9 + S + 28b^{12} + b^3 S + 500 = b^5 S + 67279.$$

Simplifying the above expression gives

$$\begin{aligned} 58428b^9 - 64779 = (b^5 - b^3 - 1)S, \qquad &\text{and so} \\ S = \frac{58428b^9 - 64779}{(b^5 - b^3 - 1)}&. \end{aligned}$$

Thus,

$$S = 10^9 \frac{58428}{98999} - \frac{66779}{98999},$$

where $m = b^5 - b^3 - 1 = 98999$.

Since S is an integer, it follows that the fractional part of $10^9(58428/98999)$ must cancel that of $66779/98999$, so that S is the integer part of $10^9(58428/98999)$. That is, $S = \lfloor 10^9(58428/98999) \rfloor = 590187779$. We see that S consists of the first nine digits of the decimal expansion of $58428/98999$:

$$\frac{58428}{10^5 - 10^3 - 1} = 0.590187779\ldots$$

Such an argument may be applied to the reversed digits in an arbitrary long finite string formed by $x_i \equiv x_{i-r} - x_{i-s} - c \pmod{b}$. Then the period length of the subtract-with-borrow sequence will be the period length of the base b expansion of the proper fraction of the form n/m, where $m = b^r - b^s - 1$. The value of n is dependent on the length of the string used to form I, and is of no great significance. What should be noticed, however, is that the linear equation for S will always result in the solution $S = b^t \frac{n}{m} - \alpha$, for some t, $m = b^r - b^s - 1$ and $0 < \alpha < 1$. Consequently, the solution for S is the leading t digits in the base b expansion of a proper fraction n/m for some n. □

Theorem 6.2.4. [MZ91] *The period length of a subtract-with-borrow sequence generated by means of the relation* $x_i \equiv x_{i-s} - x_{i-r} - c \pmod{b}$ *is the period length of the base* b *expansion of* n/m *for some* n, $1 \leq n < m$, *and* $m = b^r - b^s + 1$.

Proof. A similar derivation to the proof of Theorem 6.2.3 holds. In this case, we add I to $b^r I$, which leads to a common string S for which a solution is of the form $S = b^t \frac{n}{m} - \alpha$, for some t and $m = b^r - b^s + 1$ with $0 < \alpha < 1$. Whence, the digits of the integer S are obtained from the first t digits of the base b expansion of the proper fraction n/m.

To illustrate this, consider the particular case $r = 5$, $s = 3$ and modulus $b = 10$ so that our generator has the form $x_i \equiv x_{i-3} - x_{i-5} - c \pmod{10}$. Initializing with seed vector $\mathbf{x} = (2, 6, 4, 7, 9, 0)$, we obtain the sequence

$$2, 6, 4, 7, 9, 2, 1, 5, 5, 1, 2, 4, 6, 6, 2, 4, 2, 6, 7, 9, 1, 5, 3, 4, \ldots$$

Now, let I be the integer whose digits are the first twenty of the above sequence in the reverse order, so that $I = 97624266421551297462$. Multiplying I by b^r, and adding to I, gives

$$\begin{aligned} I &= 976\mathbf{24266421551297}462 \\ b^r I &= \underline{976\mathbf{24266421551297}46200000} \\ I + b^r I &= 97625\mathbf{24266421551297}97462 \end{aligned}$$

As expected, a common string $S = 242664215512974$ appears in each of the three levels of the sum, leading to a simple linear equation for the integer S:

$$976b^{17} + b^2 S + 62 + 976b^{22} + b^7 S + 6200000 = 97625b^{20} S + b^5 S + 97462.$$

Simplifying:

$$b^2(b^5 - b^3 + 1)S = (97625000 - 97600000 - 976)b^{17} - 6102600, \qquad \text{and so}$$
$$(b^5 - b^3 + 1)S = 24024b^{15} - 61026.$$

Therefore,

$$S = 10^{15}\frac{24024}{99001} - \frac{61026}{99001},$$

where $m = b^5 - b^3 + 1 = 99001$.

Hence, as S is an integer, it is the first 15 digits of the decimal expansion of $24024/99001 = 0.242664215512974\ldots$ And, as before, we may apply the same argument to the reversed string of an arbitrary length sequence obtained from $x_i \equiv x_{i-s} - x_{i-r} - c \pmod{b}$ with r initial values. Then the period length of the subtract-with-borrow sequence will be the period length of the base b expansion of the proper fraction of the form n/m for some n, where $m = b^r - b^s + 1$. □

It has thus been determined that a subtract-with-borrow sequence, generated by

$$x_i \equiv x_{i-r} - x_{i-s} - c \pmod{b}, \tag{6.2}$$

has a period length equal to that of the base b expansion of a proper fraction of the form n/m, where $m = b^r - b^s - 1$. Therefore, when n is relatively prime to m, the period length will be the order of b in R_m. Of course, this is ensured if m is prime, in which case the period length is $ord_m b$, and hence a factor of $\phi(m) = m - 1 = b^r - b^s - 2$ (see Theorem 2.2.1). Indeed, maximal period length $b^r - b^s - 2$ will be attained if $m = b^r - b^s - 1$ is prime and b is a primitive root of m.

Similarly, the period length of a subtract-with-borrow sequence, generated by

$$x_i \equiv x_{i-s} - x_{i-r} - c \pmod{b}, \tag{6.3}$$

is the period length of the base b expansion of a proper fraction of the form n/m, where $m = b^r - b^s + 1$. Therefore, if m is prime, it is deduced that the period length is $ord_m b$, and so a factor of $\phi(m) = b^r - b^s$, and will equal $b^r - b^s$ if m has b as primitive root.

Of course, this means that choosing lags r, s such that $m = b^r - b^s \pm 1$ is an extremely large prime is of significant practical interest. However, finding $ord_m b$ requires the factorization of $\phi(m)$ which, in the case of generator (6.2), is $b^r - b^s - 2$. Factoring such a number is infeasible when b is close to 2^{32} and r is from 20 to 50 (see [MZ91]). Much more promising is the subtract-with-borrow generator (6.3) since there is some hope of factoring $\phi(m) = b^r - b^s$ (for large b and r), and hence determining $ord_m b$, which gives the period length of the corresponding subtract-with-borrow sequence.

Example 6.2.3. Consider the subtract-with-borrow generator informally defined by $x_i = x_{i-1} - x_{i-2} - c \pmod{6}$, so that $b = 6$ and lags $r = 2$, $s = 2$. Then $m = 6^2 - 6 + 1 = 31$ is prime, and so the period length of the corresponding sequence will be $ord_{31} 6 = 6$.

Indeed, with an initial seed vector $\mathbf{x} = (5, 3, 0)$, we compute the purely periodic sequence

$$5, 3, 4, 0, 2, 1, 5, 3, 4, \ldots$$

of period length 6. □

Any seed vector of r digits and initial borrow c will produce a sequence that is ultimately periodic, although it may not be purely periodic. Clearly, the pre-period length will be at most r. A seed vector is said to be *periodic* if it results in a purely periodic sequence, in which case the seed vector $\mathbf{x}$ is the first vector to be repeated in the sequence $\mathbf{x}$, $f(\mathbf{x})$, $f^2(\mathbf{x})$, ... It should be emphasized that whatever the seed vector, except for the two trivial seed vectors $(0, 0, \ldots, 0)$ and $(b-1, \ldots, b-1, 1)$, subtract-with-borrow sequences become periodic after a few iterations of the iterating function f, and the period lengths are still the order of the base b for the appropriate modulus $m = b^r - b^s \pm 1$. The question of exactly which seed vectors produce purely periodic sequences is an interesting challenge that Marsaglia and Zaman [MZ91] undertook to solve. They found the following rules for the formation of periodic seed vectors of the form $(x_1, x_2, \ldots x_r, c)$ for each method. Below, a succession of symbols such as $x_r \cdots x_{s+1}$ means the integer for which that is the base b representation.

(1) $\boxed{x_i \equiv x_{i-s} - x_{i-r} - c \pmod{b}; m = b^r - b^s + 1.}$

$$c = 0 \text{ and } x_r \cdots x_{s+1} < x_{r-s} \cdots x_1,$$
$$c = 1 \text{ and } x_r \cdots x_{s+1} > x_{r-s} \cdots x_1.$$

(2) $\boxed{x_i \equiv x_{i-r} - x_{i-s} - c \pmod{b}; m = b^r - b^s - 1.}$

$$c = 0 \text{ and } x_r \cdots x_{s+1} + x_{r-s} \cdots x_1 < b^{r-s} - 1,$$
$$c = 1 \text{ and } x_r \cdots x_{s+1} + x_{r-s} \cdots x_1 > b^{r-s} - 1.$$

As we saw in the previous example, choosing an initial seed vector $\mathbf{x} = (5, 3, 0)$ results in $x_i = x_{i-1} - x_{i-2} - c \pmod 6$ producing a purely periodic sequence. Certainly, we have $c = 0$ and $x_2 < x_1$ so that (1) is satisfied.

The extremely long periods of these generators, their small memory requirements, and simple computer operations (only subtraction), combined with their excellent performance on tests of randomness (see [MZ91]), make subtract-with-borrow generators exceptional sources of pseudorandom numbers.

We end this thesis by briefly considering the specific subtract-with-borrow generator currently used in Matlab.

6.3 Matlab's Subtract-With-Borrow Generator

Matlab uses a subtract-with-borrow generator informally defined by

$$x_i = x_{i+20} - x_{i+5} - c, \tag{6.4}$$

where the three indices i, $i+20$, $i+5$ are all interpreted modulo 32 (corresponding to the word length of a computer). This is a slight variation on that which has been discussed since the terms of the sequences produced are in the interval $[0, 1)$, as required for most computer simulations. If the computed x_i is positive, the borrow bit c is set to zero for the next iteration. But, if the computed x_i would be negative, it is made positive by adding 1, and then setting c equal to 2^{-53}, ready for the next step. To produce sequences of integers, this generator would use a base $b = 2^{53}$.

Marsaglia has shown that any subtract-with-borrow sequence generated by (6.4) has an extremely huge period of almost 2^{1430} terms, but we will not enter into the details here since it beyond the scope of this thesis. A more in-depth discussion requires technical computer terms, and other related jargon. However, we will point out that with some additional "bit fiddling" the period length has been increased to 2^{1492}. Such a huge period length is certainly very extravagant since, at a generation speed of one million per second, it will take more than 10^{435} years before the period length is exhausted.

Appendix A

Theorems in Number Theory

Number theory accounts for most of the mathematics behind pseudorandom number generators and so can be considered, in a sense, to be the *mathematics* of pseudorandom number generation. Here, a small collection of relevant number-theoretic results is provided, most of which are referred to in the text – particularly in chapters 2 and 5. Where appropriate, the following theorems/lemmas are accompanied by a proof, while others are just stated since proving them may require further results or definitions that are not necessary for our purposes. The reader may wish to consult a sound elementary number theory textbook such as [Ros00].

Lemma A.1. *If a divides bc and $(a, b) = 1$ then a divides c.*

Proof. If a divides bc then $bc = ak$ for some $k \in \mathbb{Z}$. Also, since $(a, b) = 1$ then there exists integers m, n such that $ma + nb = 1$. Therefore,

$$amc + bnc = c$$
$$amc + nak = c$$
$$a(mc + nk) = c$$

where $mc + nk \in \mathbb{Z}$. Hence, a divides c. □

Theorem A.1. *If $ka \equiv kb \pmod{m}$ and $(k, m) = d$ then $a \equiv b \pmod{m/d}$.*

Proof. If $ka \equiv kb \pmod{m}$ then m divides $k(a - b)$, and therefore $\frac{m}{d}$ divides $\frac{k}{d}(a - b)$. Further, $(\frac{m}{d}, \frac{k}{d}) = 1$ since $(k, m) = d$, and so $\frac{m}{d}$ divides $a - b$ by Lemma A.1. Thus, $a \equiv b \pmod{m/d}$. □

Theorem A.2 (Fundamental Theorem of Arithmetic). *The decomposition of a natural number n as a product of primes exists and is unique (up to the order of the factors).*

□

Theorem A.3 (Binomial Theorem). *Let x and y be variable, and n be any positive integer. Then*

$$(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i.$$

Theorem A.4 (Fermat's Little Theorem). *If a is a natural number, and p a prime, then $a^p \equiv a \pmod{p}$. In particular, if $(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. (*Euler's Proof of 1736*).
We prove by mathematical induction on the natural number a. For $a = 1$, the result is trivially true since $1^p \equiv 1 \pmod{p}$.
Assume the result is true for $a = k$ and consider $a = k + 1$. By the *Binomial Theorem*,

$$a^p = (k+1)^p = k^p + \binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k + 1.$$

Now, p divides each of the binomial coefficients in the above expression. Therefore, using the inductive hypothesis that $k^p \equiv k \pmod{p}$, it follows that

$$\begin{aligned}(k+1)^p &\equiv k^p + 1 \pmod{p} \\ &\equiv k + 1 \pmod{p}.\end{aligned}$$

Thus, by the principle of mathematical induction, the result is proved. In addition, if $(a,p) = 1$, then from Theorem A.1 we obtain $a^{p-1} \equiv 1 \pmod{p}$. □

The following theorem is a generalization of *Fermat's Little Theorem.*

Theorem A.5 (Euler's Theorem). *For any positive integer m such that $(a,m) = 1$, $a^{\phi(m)} \equiv 1 \pmod{m}$.*

□

Theorem A.6 (Division Algorithm). *Given integers a, b with $b > 0$, there exist unique integers q, r such that $a = bq + r$ with $0 \leq r < b$.*

□

Lemma A.2. *For integers a and b, the equation $ax + by = n$ has integer solutions in x and y if and only if (a,b) divides n.*

□

Lemma A.3. *If $a, b,$ and c are integers then $[a,b] \mid c$ if and only if $a \mid c$ and $b \mid c$.*

Proof. Let $a = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$, and $c = p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k}$ where p_i's are distinct primes and $\alpha_i, \beta_i, \gamma_i$ are non-negative integers, some of which may be zero. Then, for an integer to be divisible by both a and b, it is necessary that in the factorization of this integer, each p_i occurs with a power at least as large as α_i and β_i. Hence, $[a,b]$ (i.e. $lcm(a,b)$), the smallest positive integer divisible by both a and b, is:

$$[a,b] = p_1^{max(\alpha_1,\beta_1)}p_2^{max(\alpha_2,\beta_2)}\cdots p_k^{max(\alpha_k,\beta_k)}.$$

If $a \mid c$ and $b \mid c$ then $max(\alpha_i, \beta_i) \leq \gamma_i$ for all $i = 1, \ldots, k$. Hence, $[a,b] \mid c$.
Conversely, if $[a,b] \mid c$ then since $a \mid [a,b]$ we have $a \mid c$, by the transitivity of $\mid$.
Similarly, $b \mid c$. □

Lemma A.4. *If $a, b, m_1, m_2, \ldots, m_k$ are integers, with each m_i positive, such that $a \equiv b \pmod{m_i}$ for all $i = 1, 2, \ldots, k$ then $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$, where $[m_1, m_2, \ldots, m_k] = lcm(m_1, m_2, \ldots, m_k)$.*

Proof. Since $a \equiv b \pmod{m_i}$ for all $i = 1, 2, \ldots, k$ then $m_i \mid (a - b)$ for all $i = 1, 2, \ldots, k$. It therefore follows from Lemma A.3 that $[m_1, m_2, \ldots, m_k] \mid (a - b)$, which yields the desired result. □

Theorem A.7 (Chinese Remainder Theorem). *Let $m_1, m_2 \ldots, m_k$ be pairwise relatively prime positive integers. Then the system of congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution for x modulo $M = m_1 m_2 \cdots m_k$.

Proof. Let $n_i = M/m_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$ so that m_j divides n_i if and only if $i \neq j$ and $(m_i, n_i) = 1$ for all i, since $(m_i, m_j) = 1$ whenever $i \neq j$.
Consider the congruence

$$n_i x_i \equiv a_i \pmod{m_i}; \qquad i = 1, \ldots, k. \tag{6.5}$$

This is equivalent to the equation $n_i x_i + m_i y_i = a_i$, which has integer solutions for x_i and y_i if and only if (m_i, n_i) divides a_i, by Lemma A.2. Hence, since $(m_i, n_i) = 1$ (and therefore divides a_i) then there exists a solution to congruence (6.5), and this solution is unique modulo m_i.
Now, consider the sum $x = n_1 x_1 + n_2 x_2 + \cdots + n_k x_k$. Since m_i divides $n_j x_j$ for all $i \neq j$ then $n_j x_j \equiv 0 \pmod{m_i}$ for all $i \neq j$, and so $x \equiv n_i x_i \pmod{m_i}$. Therefore, $x \equiv a_i \pmod{m_i}$ for all $i = 1, \ldots, k$. That is, x is a simultaneous solution of the given system of k congruences.

We now prove uniqueness of this solution x modulo M.
Suppose x and y are two simultaneous solutions of the system of k congruences. Then $x \equiv y \pmod{m_i}$ for all $i = 1, \ldots, k$ and since $(m_i, m_j) = 1$ for all $i \neq j$ then $[m_1, \ldots, m_k] = m_1 \cdots m_k = M$. Hence, by Lemma A.4, we have $x \equiv y \pmod{M}$. □

A *quadratic residue* of a prime p was defined in Definition 5.3.1. There is a special notation associated with quadratic residues, as described in the following definition.

Definition A.1. *Let p be an odd prime and $(a,p)=1$. The* ***Legendre symbol*** $\left(\frac{a}{p}\right)$ *is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue of } p. \end{cases}$$

Theorem A.8 (Euler's Criterion). *If p is an odd prime and $(a,p)=1$ then*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

□

Appendix B

Definitions & Theorems in Finite Field Theory

In addition to number theory, the theory of finite fields is certainly another major area of mathematics used in the study of pseudorandom number generation. Specifically, k^{th}-order linear recurrence and non-linear generators rely on certain aspects of finite field theory. Below, we present some auxiliary definitions and results, to those already given in the body of this thesis. For readers unfamiliar with finite fields, it is hoped that what follows is useful in their understanding. A solid reference for most of this material is [LN97], while a more compact discussion of finite fields can be found in [Fra94].

Notation. Denote a field by $\mathbb{F}$ and the finite field with q elements (or the *Galois Field* of order q) by $\mathbb{F}_q$, so that $GF(q) = \mathbb{F}_q$.

Theorem B.1. *$\mathbb{Z}_p$ is a field if and only if p is a prime.*

□

Definition B.1. *A multiplicative group G is said to be **cyclic** if there is an element $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$. We write $G = \langle a \rangle$ and a is called a **generator for** G.*

Theorem B.2. *The multiplicative group $\mathbb{F}_q^*$ of non-zero elements of $\mathbb{F}_q$ is cyclic.*

□

Theorem B.3. (Division Algorithm for $\mathbb{F}_q[x]$). *Let f and g be two polynomials in $\mathbb{F}_q[x]$ with $deg(f) = m$ and $deg(g) = n > 0$. Then there exist unique polynomials q, $r \in \mathbb{F}_q[x]$ such that $f(x) = g(x)q(x) + r(x)$ with $0 \leq deg(r) < n$.*

□

Note. If $r(x) = 0$ then the polynomial $g(x)$ *divides* $f(x)$.

Definition B.2. *Let $\mathbb{F} \supseteq \mathbb{F}_q$ and $\alpha \in \mathbb{F}$. Then α is **algebraic over** $\mathbb{F}_q$ if α is a zero of a non-zero polynomial $f \in \mathbb{F}_q[x]$. Otherwise, α is **transcendental over** $\mathbb{F}_q$.*

Definition B.3. *A non-constant polynomial $f \in \mathbb{F}[x]$ is **irreducible over** $\mathbb{F}$ (or an **irreducible polynomial in** $\mathbb{F}[x]$) if $f(x)$ cannot be expressed as a product of two polynomials in $\mathbb{F}[x]$ both of lower degree than the degree of f.*

Theorem B.4. *Let $\mathbb{F} \supseteq \mathbb{F}_q$ and $\alpha \in \mathbb{F}$ be algebraic over $\mathbb{F}_q$. Then there exists a unique monic irreducible polynomial $g \in \mathbb{F}_q$ of minimal degree ≥ 1, having α as a zero. If $f(\alpha) = 0$ for some non-zero polynomial $f \in \mathbb{F}_q[x]$ then $g(x)$ divides $f(x)$.*

□

Definition B.4. *Let $\mathbb{F} \supseteq \mathbb{F}_q$ and $\alpha \in \mathbb{F}$ be algebraic over $\mathbb{F}_q$. Then the unique monic irreducible polynomial $g \in \mathbb{F}_q[x]$ (of least degree ≥ 1), having α as a zero, is called the* ***minimal polynomial of*** *α* ***over*** *$\mathbb{F}_q$, denoted $min(\alpha, \mathbb{F}_q)$.*

Lemma B.1. *Let f be a polynomial in $\mathbb{F}_q[x]$ of degree $k \geq 1$ with $f(0) \neq 0$. Then there exists a positive integer $e \leq q^k - 1$ such that $f(x)$ divides $x^e - 1$.*

Proof. See [LN97]. □

Theorem B.5. *If $f \in \mathbb{F}_q[x]$ is an irreducible polynomial over $\mathbb{F}_q$ of degree $k > 1$, then $ord(f)$ divides $q^k - 1$.*

□

Theorem B.6. *If $k > 1$ is a divisor of $p - 1$, for some prime p, then there is no permutation polynomial over $\mathbb{F}_p$ of degree k.*

□

Bibliography

[AK64] J.D. Alanen and D.E. Knuth. Tables of finite fields. *Sankhyā(A)*, 26:305–328, 1964.

[AR94] Howard Anton and Chris Rorres. *Elementary Linear Algebra: Applications Version*. John Wiley & Sons, New York, seventh edition, 1994.

[Ash67] Robert Ash. *Information Theory*. John Wiley & Sons, New York, 1967.

[Bey72] W.A. Beyer. Lattice structure and reduced bases of random vectors generated by linear recurrences. In S. K. Zaremba, editor, *Applications of Number Theory to Numerical Analysis*, pages 361–370. Academic Press, New York, 1972.

[BRW71] W.A. Beyer, R.B. Roof, and D. Williamson. The lattice structure of multiplicative pseudo-random vectors. *Mathematics of Computation*, 25:345–363, 1971.

[Car10] R.D. Carmichael. Note on a new number theory function. *Bulletin of the American Mathematical Society*, 16:232–238, February 1910.

[Die72] U. Dieter. Statistical interdependence of pseudo-random numbers generated by the linear congruential method. In S.K. Zaremba, editor, *Applications of Number Theory to Numerical Analysis*, pages 287–317. Academic Press, New York, 1972.

[EGL88] J. Eichenauer, H. Grothe, and J. Lehn. Marsaglia's lattice test and non-linear congruential pseudo random number generators. *Metrika*, 35:241–250, 88.

[EGLT87] J. Eichenauer, H. Grothe, J. Lehn, and A. Topuzoğlu. A multiple recursive non-linear congruential pseudo random number generator. *Manuscripta Mathematica*, 59:331–346, 87.

[EH91] J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers avoid the planes. *Mathematics of Computation*, 56(193):297–301, 1991.

[EH92a] J. Eichenauer-Herrmann. Construction of inversive congruential pseudorandom number generators with maximal period length. *Journal of Computational and Applied Mathematics*, 40:345–349, 1992.

[EH92b] J. Eichenauer-Herrmann. Inversive congruential pseudorandom numbers: a tutorial. *International Statistical Review*, 60(2):167–176, 1992.

[EHT90] J. Eichenauer-Herrmann and A. Topuzoğlu. On the period length of congruential pseudorandom number sequences generated by inversions. *Journal of Computational and Applied Mathematics*, 31:87–96, 1990.

[EL86] J*ü*rgen Eichenauer and J*ü*rgen Lehn. A non-linear congruential pseudorandom number generator. *Statistische Hefte*, 27:315–326, 1986.

[EL87] J. Eichenauer and J. Lehn. On the structure of quadratic congruential sequences. *Manuscripta Mathematica*, 58:129–140, 1987.

[ELNT90] J. Eichenauer, J. Lehn, H. Niederreiter, and A. Topuzoğlu. On the lattice structure of a nonlinear generator with modulus 2^{α}. *Journal of Computational and Applied Mathematics*, 31(1):81–85, 1990.

[ELT88] J. Eichenauer, J. Lehn, and A. Topuzoğlu. A nonlinear congruential pseudorandom number generator with power of two modulus. *Mathematics of Computation*, 51(184):757–759, 1988.

[FM68] Jay P. Fillmore and Morris L. Marx. Linear recursive sequences. *SIAM Review*, 10(3):342–353, 1968.

[FN92] M. Flahive and H. Niederreiter. On inversive congruential generators for pseudorandom numbers. In G.L. Mullen and P.J. Shiue, editors, *Finite Fields, Coding Theory, and Advances in Communications and Computing*, pages 75–80. Dekker, New York, 1992.

[Fra94] John B. Fraleigh. *A First Course in Abstract Algebra*. Addison-Wesley, Reading, Massachusetts, fifth edition, 1994.

[Ful76] A.T. Fuller. The period of pseudo-random numbers generated by Lehmer's congruential method. *Computer Journal*, 19(2):173–177, 1976.

[Gol67] Solomon W. Golomb. *Shift Register Sequences*. Holden-Day, San Franciscom, California, 1967.

[Gre61] Martin Greenberger. Notes on a new pseudo-random number generator. *Journal of the Association for Computing Machinery*, 8:163–167, 1961.

[HD62] T.E. Hull and A.R. Dobell. Random number generators. *SIAM Review*, 4(3):230–254, 1962.

[Hub94] Klaus Huber. On the period length of generalized inversive pseudorandom number generator. *Appl. Algebra Engrg. Comm. Comput.*, 5(5):255–260, 1994.

[Knu81] Donald E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley, Reading, Massachusetts, second edition, 1981.

[KWY96] Takashi Kato, Li-Ming Wu, and Niro Yanagihara. On a non-linear congruential pseudorandom number generator. *Mathematics of Computation*, 65(213):227–233, 1996.

[Lag90] J. C. Lagarias. Pseudorandom number generators in cryptography and number theory. In Carl Pomerance, editor, *Proceedings of Symposia in Applied Mathematics*, volume 42, pages 115–143, 1990.

[Lag93] Jeffrey C. Lagarias. Pseudorandom numbers. *Statistical Science*, 8(1):31–39, 1993.

[Leh51] D.H. Lehmer. Mathematical methods in large-scale computing units. In *Proceedings of the Second Symposium on Large-Scale Digital Calculating Machinery*, pages 141–146, Cambridge, MA, 1951. Harvard University Press.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite Fields, Encyclopedia of Mathematics and its Applications*, volume 20. Cambridge University Press, New York, NY, 1997.

[Mar68] George Marsaglia. Random numbers fall mainly in the planes. *Proceedings of the National Academy of Sciences*, 61(1):25–28, 1968.

[Mar70] George Marsaglia. Regularities in congruential random number generators. *Numerical Mathematics*, 16:8–10, 1970.

[Mar72] George Marsaglia. The structure of linear congruential sequences. In S. K. Zaremba, editor, *Applications of Number Theory to Numerical Analysis*, pages 249–285. Academic Press, New York, 1972.

[Mar85] George Marsaglia. A current view of random number generators. In L. Billard, editor, *Computer Science and Statistics: Proceedings of the Sixteenth Symposium on the Interface*, pages 3–10, 1985.

[Mar92] George Marsaglia. The mathematics of random number generators. In Stefan A. Burr, editor, *Proceedings of Symposia in Applied Mathematics*, volume 46, pages 73–90, 1992.

[MS00] Michael Mascagni and Ashok Srinivasan. Sprng: A scalable library for pseudorandom number generation. *ACM Transactions on Mathematical Software*, 26(3):436–461, 2000.

[MT85] George Marsaglia and Liang-Huei Tsay. Matrices and the structure of random number sequences. *Linear Algebra and its Applications*, 67:147–156, 1985.

[MZ91] George Marsaglia and Arif Zaman. A new class of random number generators. *The Annals of Applied Probability*, 1(3):462–480, 1991.

[Nev65] J. Neveu. *Mathematical Foundations of the Calculus of Probabilities*. Holden-Day, San Fransisco, 1965.

[Nie77] H. Niederreiter. Pseudo-random numbers and optimal coefficients. *Advances in Mathematics*, 26:99–181, 1977.

[Nie78] H. Niederreiter. Quasi-monte carlo methods and pseudo-random numbers. *Bulletin of the American Mathematical Society*, 84:957–1041, 1978.

[Nie85] H. Niederreiter. The serial test for congruential pseudo-random numbers generated by the linear congruential method. *Numerical Mathematics*, 46:51–68, 1985.

[Nie88] Harald Niederreiter. Statistical independence of nonlinear congruential pseudorandom numbers. *Monatshefte für Mathematik*, 106:149–159, 1988.

[Nie89] H. Niederreiter. The serial test for congruential pseudo-random numbers generated by inversions. *Mathematics of Computation*, 52:135–144, 1989.

[Nie92] Harald Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*. SIAM, Philadelphia, 1992.

[PM88] Stephen K. Park and Keith W. Miller. Random number generators: Good ones are hard to find. *Communications of the ACM*, 31(10):1192–1201, 1988.

[Rab80] M.O. Rabin. Probabilistic algorithms in finite fields. *SIAM Journal of Computing*, 9:273–280, 1980.

[Rip87] Brian D. Ripley. *Stochastic Simulation*. John Wiley & Sons, New York, 1987.

[Ros00] Kenneth H. Rosen. *Elementary Number Theory*. Addison-Wesley, Reading, Massachusetts, fourth edition, 2000.

[Rot60] A. Rotenberg. A new pseudo-random number generator. *Journal of the Association of Computing Machinery*, 7:75–77, 1960.

[Str97] Sibylle Strandt. Quadratic congruential generators with odd composite modulus. In *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, Lecture Notes in Statistics*, volume 127, pages 415–426. Springer-Verlag, New York, 1997.

[Tau65] Robert C. Tausworthe. Random numbers generated by linear recurrence modulo two. *Mathematics of Computation*, 19:201–209, 1965.

[Tho58] W.E. Thomson. A modified congruence method of generating pseudo-random numbers. *Computer Journal*, 1:83, 86, 1958.

[Zie59] Neal Zierler. Linear recurring sequences. *Journal of SIAM*, 7(1):31–48, 1959.