Feedback Registers Based on Ramified Extensions of the 2-Adic Numbers

(Extended Abstract)

Mark Goresky [1] Andrew Klapper[2]

Abstract

A new class of feedback register, based on ramified extensions of the 2-adic numbers, is described. An algebraic framework for the analysis of these registers and the sequences they output is given. This framework parallels that of linear feedback shift registers. As one consequence of this, a method for cracking summation ciphers is given. These registers give rise to new measures of cryptologic security.

1 Introduction

Pseudorandom sequences, with a variety of statistical properties (such as high linear span, low autocorrelation and pairwise cross-correlation values, and high pairwise hamming distance) are important in many areas of communications and computing (such as cryptography, spread spectrum communications, error correcting codes, and Monte Carlo integration). Binary sequences, such as m-sequences, more general nonlinear feedback shift register sequences, and summation combiner sequences, have been widely studied by many researchers. Linear feedback shift register hardware can be used to relate certain of these sequences (such as m-sequences) to error correcting codes (such as first order Reed-Muller codes).

In this paper we describe a new type of feedback register, ramified feedback with carry shift registers (or d-FCSRs, where d is the ramification). These relatively simple devices generate binary sequences that have an algebraic structure that parallels the algebraic structure of linear feedback shift registers [3]. This algebraic structure is based on algebra over certain extensions of the 2-adic numbers. (See, for example, Koblitz's book [7] for background on 2-adic numbers). Furthermore, there is an analog for d-FCSRs of the Berlekamp-Massey algorithm. The algebraic analysis of these sequences, together with the Berlerkamp-Massey type algorithm, leads to vulnerability of certain combiners with memory, including the summation combiner [9]. These facts lead to the consideration of an analog of the linear complexity – the π-adic span. This π-adic span is a new measure of cryptologic security that must be large for any binary sequence to be secure. This work generalizes the construction in the unramified case due to Klapper and Goresky [5].

2 Feedback Shift Registers with Carry

In this section we give a detailed description of the operation of d-FCSRs. In the simplest case, $d = 1$, the contents (0 or 1) of the tapped cells of the shift register are added *as integers* to the current contents of the memory to form a sum, Σ. The parity bit ($\Sigma \pmod 2$) of Σ is fed back into the first cell, and the higher order bits ($[\Sigma/2]$) are retained for the new value of the memory. Any periodic binary sequence may be generated by such a FCSR.

---

[1]Dept. of Mathematics and College of Computer Science, Northeastern University.

[2]University of Kentucky and University of Manitoba. Project sponsored by the Natural Sciences and Engineering Research Council under Operating Grant OGP0121648 and the National Security Agency under Grant Number MDA904-91-H-0012. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon.

More generally, we fix a positive integer d, and consider an addition operation in which the carry jumps d bits. Thus if $d = 3$, then $1 + 1 = 1000$. We will refer to this operation as addition with d-fold carry. It corresponds to addition in the integers with a positive real dth root π of 2 adjoined ($\pi^d = 2$). A register is obtained by replacing the integer addition in the preceding paragraph by this addition, and allowing plus or minus ones as coefficients on the tapped cells. Such a register is called a *ramified feedback-with-carry shift register* with ramification d, or simply a d-FCSR.

More precisely, let $R = \mathbf{Z}[\pi]$ be the integers with π adjoined. We have $\pi = 2^{1/d}$ real and positive, so R is a subset of the reals and the usual absolute value makes sense in R. Fix an odd integer $q \in R$. (Here odd means that q is congruent to 1 modulo π.) Write $q + 1 = q_1\pi + q_2\pi^2 + \cdots + q_r\pi^r$ with $q_i \in \{0, \pm 1\}$. The shift register will use r stages plus some additional bits of memory. The feedback connections will be given by the coefficients $\{q_1, q_2, \ldots, q_r\}$. We write $q_0 = -1$ when convenient.

Definition 2.1 *The d-FCSR with connection integer q is the register is a feedback register with r bits of storage plus additional memory for carry. If the contents of the register at any given time are $(a_{r-1}, a_{r-2}, \ldots, a_1, a_0)$ and the memory is m, then the operation of the shift register is defined as follows:*

A1. Form the integer sum $\sigma = \sum_{k=1}^{r} q_k a_{r-k} + m$.

A2. Shift the contents one step to the right, outputting the rightmost bit a_0.

A3. Place $a_r = \sigma \pmod{\pi}$ into the leftmost cell of the shift register

A4. Replace the memory m with $(\sigma - a_r)/\pi$.

We have the following analogs of LFSR theory.

1. For any binary periodic pseudorandom sequence we may consider the smallest FCSR which generates that sequence.

   Definition 4.1 *The size of the smallest d-FCSR which generates the periodic part of an eventually periodic sequence* **a** *is the* π-adic span *of the sequence* **a**. *Here, $\pi^d = 2$.*

2. There is an analog (due to Mandelbaum [8]) of the Berlekamp-Massey algorithm, which we discuss in Section 4. For any periodic binary sequence and $d \geq 1$, this algorithm may be used to construct a d-FCSR which generates the sequence.

3. If two periodic binary sequences are added *with d-fold carry* operation, then the π-adic span of the resulting sequence is no more than the sum of the π-adic complexities of the original sequences. In §4 we use this fact and (2) above to provide a cryptologic attack on the certain combiners with memory, including "summation combiners" described in [9].

4. The number q, which we call the *connection number*, is analogous to the connection polynomial of a LFSR. The period and other properties of the binary sequence are determined from number theoretic properties of q.

5. An ℓ-sequence is a FCSR sequence with maximum possible period $T = |(R/(q))^*|$. An ℓ-sequence is analogous to an m-sequence in LFSR theory. In case $d = 1$, so $\pi = 2$, such a sequence is the cyclic shift of the sequence formed by *reversing* the period of the binary expansion of the fraction $1/q$ and have been studied since the time of Gauss ([1, 2, 6]). They have remarkable distribution and correlation properties and are generated by connection numbers q for which 2 is a *primitive root.*

Suppose that $\mathbf{a} = \{a_0, a_1, a_2, \ldots\}$ and $\mathbf{b} = \{b_0, b_1, b_2, \ldots\}$ are infinite periodic binary sequences and that the sequence $\mathbf{c}$ is obtained by adding the sequences $\mathbf{a}$ and $\mathbf{b}$ with *d-fold carry* operation. In other words,

$$\begin{aligned} c_0 &= (a_0 + b_0) \pmod{\pi}, & m_1 &= (a_0 + b_0 - c_0)/\pi \\ c_1 &= (a_1 + b_1 + m_1) \pmod{\pi}, & m_2 &= (a_1 + b_1 + m_1 - c_1)/\pi \end{aligned} \tag{1}$$

and so on. (Here, m_j is the bit carried from stage $j-1$ to stage j.)

We model this addition with carry operation by associating to the infinite binary sequence $\mathbf{a}$ the formal power series

$$\alpha = \sum_{i=0}^{\infty} a_i \pi^i \tag{2}$$

and similarly associating β to $\mathbf{b}$. These are the analogs of generating functions in LFSR theory, and there are analogs of well known facts relating rationality of generating functions to periodicity of sequences, and relating the denominator of a rational generating function to the connection polynomial of a LFSR which outputs the sequence. Such power series over π do not converge in the usual sense but can be interpreted as defining elements in the ring $\hat{R} = \mathbf{Z}[[\pi]]$ of π-adic integers. This ring consists of all formal power series $\sum_{i=0}^{\infty} s_i \pi^i$ with $s_i \in \{0, 1\}$, and can be interpretted as the completion of R with respect to the π-adic valuation. It has been studied extensively by mathematicians for many years. The main difference between the two rings $\mathbf{Z}/(2)[[x]]$ and $\hat{R}$ is that addition in $\hat{R}$ is performed by "carrying" overflow bits to higher order terms, so that $\pi^i + \pi^i = 2\pi^i = \pi^{i+d}$. It follows that the formal power series $\gamma = c_0 + c_1\pi + c_2\pi^2 + \cdots$ associated to the sum-with-d-fold-carry sequence $\mathbf{c}$ is given by addition, $\gamma = \alpha + \beta \in \hat{R}$. In the π-adic numbers, -1 is represented by $-1 = 1 + \pi^d + \pi^{2d} + \pi^{3d} + \cdots$. A π-adic number $\sum a_i \pi^i$ has a multiplicative inverse if and only if $a_0 = 1$. Also, any π-adic number α can be written

$$\alpha = \sum_{i=0}^{d-1} \alpha_i \pi^i.$$

If $\alpha \in R = \mathbf{Z}[\pi]$, then each α_i is an ordinary integer.

These constructions may be made using ramified extensions of the p-adic numbers $\mathbf{Z}_p$ (for any prime p) and all our results remain valid essentially without change. However, for the most part, we will restrict attention to the case $p = 2$ because this is probably the most important case from the point of view of applications.

If $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ is an eventually periodic sequence, then the associated π-adic number is a quotient of elements of R, a so-called R-rational. If $\mathbf{a}$ is strictly periodic of period T, then the associated R-rational number α is easily found. Set $\alpha = \sum_{i=0}^{\infty} a_i \pi^i$. Then

$$\alpha = -\frac{(\sum_{i=0}^{T-1} a_i \pi^i)}{(\pi^T - 1)}. \tag{3}$$

Theorem 2.2 *There is a one to one correspondence between R-rational numbers $\alpha = p/q$ (where $q \equiv 1 \pmod{\pi}$) and eventually periodic binary sequences $\mathbf{a}$. If $d = 1$, then α is strictly periodic if and only if*

$0 \le -p < q$. If p and q are relatively prime in R, and q is odd, then the eventual period of the bit sequence for the π-adic expansion of $\alpha = p/q$ is $T = ord_q(\pi)$.

This partially explains how to generate any periodic binary sequence using a FCSR: express the corresponding π-adic number as a fraction p/q, then write $q = -1 + q_1\pi + q_2\pi^2 + \cdots + q_r\pi^r$, with $q_i \in \{0, \pm 1\}$ (every element of R which is congruent to one modulo π can be so written). The coefficients $q_1, q_2, \ldots, q_r$ specify the multipliers on the taps of the FCSR. The numerator p determines the initial loading of the shift register in a way that is described later in this paper. The π-adic span of the sequence $\mathbf{a}$ is therefore one less than the number of bits in the smallest such expansion of q. (The memory requires at most an additional $2\lceil d \cdot \log_2(t/(\pi - 1))\rceil$ bits, where t is the maximum of the number of 1s and the number of -1s in the expansion of q.)

3 Analysis of FCSRs

According to the preceding sections, there are four different ways to view an infinite, eventually periodic binary sequence: (1) As a binary sequence $\mathbf{a}$; (2) As an element α of the 2-adic integers Z_2; (3) As a rational number p/q; (4) As the output stream of a FCSR. We have already identified representations (1) and (2) by associating the binary sequence $\mathbf{a}$ with the coefficients in the formal power series expression for α. The translation between representations (2) and (3) was explained in Theorem 2.2. In this section we show how to translate between representations (3) and (4).

Suppose we fix a FCSR with connection number $q = -1 + q_1\pi + q_2\pi^2 + \cdots + q_r\pi^r$ and some initial loading of the memory and the register. The register will generate an infinite, eventually periodic sequence $\mathbf{a} = a_0, a_1, a_2, \ldots$ of bits. Let α be the associated π-adic number, which we call the *π-adic value* of the FCSR (with its initial loading and initial memory).

Let us consider the transition from one state of the shift register to the next. Suppose that, for some given state, the value of the memory is mem $= m_{n-1}$ and that the contents of the register is given by the r bits $a_{n-1}, a_{n-2}, \ldots, a_{n-r}$ (with a_{n-1} the leftmost bit and a_{n-r} the rightmost bit, and where the register shifts towards the right). The next state is determined by calculating ([A1]) $\sigma_n = m_{n-1} + \sum_{i=1}^{r} q_i a_{n-i}$, writing the new contents of the leftmost cell as $a_n = \sigma_n (\mathrm{mod}\ \pi)$, and writing the new memory contents as $m_n = (\sigma_n - a_n)/\pi$ (see [A3] and [A4]). (The remaining bits are shifted once to the right.) These equations may be combined into the expression $\sigma_n = \pi m_n + a_n$. It follows that

$$a_n = \sum_{i=1}^{r} q_i a_{n-i} + (m_{n-1} - \pi m_n) \tag{4}$$

provided $n \ge r$. Suppose the initial loading of the register consists of memory mem $= m_{r-1}$ and with register bit values $a_{r-1}, a_{r-2}, \ldots, a_1, a_0$. Now substitute (4) into the expression (2) for α to obtain,

$$\begin{aligned} \alpha &= a_0 + a_1\pi + \cdots + a_{r-1}\pi^{r-1} + \sum_{n=r}^{\infty} a_n\pi^n \\ &= \sum_{i=0}^{r-1} a_i\pi^i + \sum_{n=r}^{\infty}\Big(\sum_{i=1}^{r} q_i a_{n-i}\Big)\pi^n + \sum_{n=r}^{\infty}(m_{n-1} - \pi m_n)\pi^n. \end{aligned} \tag{5}$$

This equation gives

$$\alpha = \frac{m_{r-1}\pi^r - \sum_{i=0}^{r-1}\sum_{j=0}^{r-i-1} q_i\pi^i a_j\pi^j}{1 - \sum_{i=1}^{r} q_i\pi^i}. \tag{6}$$

Thus we have proven

Theorem 3.1 *The output,* **a**, *of a d-FCSR with connection integer q, initial memory value m_{r-1}, and initial loading $a_{r-1}, a_{r-2}, \ldots, a_1, a_0$, is the bit sequence of the π-adic representation of a rational number (eq. (6)) $\alpha = -p/q$ with denominator q.*

Initial Loading of a FCSR

Now let us show how to construct a FCSR which generates the bit sequence for a given rational p/q. For this purpose we fix an odd connection integer $q = \sum_{i=0}^{r} q_i \pi^i$ with $q_0 = -1$ and $q_i \in \{0, \pm 1\}$ for $i > 0$. Fix $p \in R$. An initial loading of the FCSR is defined as follows:

B1. Set $m_{-1} = p$.

B2. For each $i = 0, 1, \ldots, r-1$ compute the following numbers:

$$\sigma_i = \sum_{k=0}^{i-1} q_{i-k} a_k + m_{i-1} \in \mathbf{Z} \tag{7}$$

$$a_i = \sigma_i \pmod{\pi} \in R/(\pi) \tag{8}$$

$$m_i = \frac{\sigma_i - a_i}{\pi}. \tag{9}$$

Proposition 3.2 *If we use the initial loading $(a_{r-1}, a_{r-2}, \ldots, a_1, a_0)$, and initial memory $m_{r-1} \in R$, then the resulting d-FCSR outputs the π-adic expansion of p/q.*

If p is relatively prime to q, then the period of the sequence is $T = \mathrm{ord}_q(2)$. However if p and q have a common factor then the period may be smaller but at least it will divide $\mathrm{ord}_q(2)$.

Fact 3.3 *Adding b to the initial memory changes the π-adic value of the shift register by $-b\pi^r/q$.*

Let t be the maximum of the number of q_i equal to 1 and the number of q_i equal to -1, $i = 0, \ldots, r$. If m is the initial memory value, we can write $m = m^{(1)} - m^{(2)}$, where the expansion of each $m^{(i)}$ has all nonnegative coefficients. If for each i we have $m^{(i)} \leq t/(\pi - 1)$, then the same will be true for all later values of the memory. We will therefore need at most $2\lceil d \cdot \log_2(t/(\pi - 1))\rceil$ bits of memory. Moreover, if we initialize a FCSR with $m^{(i)} > t/(\pi - 1)$, then the memory will decrease so that after at most $d \cdot \log_2(m^{(i)} - t)$ steps, $m^{(i)}$ will be at most t. In particular, if the expansion of p/q is strictly periodic, then there is an initial loading of the register with each $m^{(i)} \leq t/(\pi - 1)$. By Fact 3.3, there is a unique initial memory for a given p/q. Therefore, if p/q is periodic, the initial memory derived by (C1) and (C2) satisfies this bound and the register requires at most $2\lceil d \cdot \log_2(t/(\pi - 1))\rceil$ bits of memory throughout it the execution of the register.

If $d = 1$, then it can be shown that p/q is strictly periodic if and only if $0 \leq -p < q$, and the expansion of p has all nonnegative coefficients. In this case it turns out that $m^{(2)} = 0$. The memory is always nonnegative and requires only $\lceil log_2(t) \rceil$ bits.

If we let $x = \sum_{i=0}^{r-1} a_i \pi^i$, then the double sum occurring in equation (6) is the portion of the binary expansion for the product

$$q \cdot x = \sum_{i=0}^{r} q_i 2^i \sum_{j=0}^{r-1} a_j 2^j$$

which is obtained by removing all terms involving powers of π^r or higher. Therefore, the numerator p is congruent to $q \cdot x$ modulo π^r. It is possible to invert this and to give a formula for the initial loading in terms of the fraction $\alpha = p/q$ (whether or not p and q are relatively prime).

Theorem 3.4 *Suppose a FCSR with r stages and connection integer q generates a sequence given by the π-adic expansion of the number $\alpha = p/q$. Let $T = ord_q(\pi)$ and set $s = (\pi^T - 1)/q \pmod{\pi^r}$. Then the initial loading is the binary expansion ofthe number $x = p \cdot s \pmod{\pi^r}$.*

Despite Fact (3.3), we do not know a similar simple formula for determining the initial memory value directly from the rational number $\alpha = p/q$.

Exponential Representation of FCSR Sequences

One of the most powerful techniques for the analysis of shift register sequences is its exponential representation using trace functions and primitive elements of finite fields. There is a similar representation for periodic sequences obtained from d-FCSRs. To describe this we need a lemma.

Lemma 3.5 *If $q \in R$ is odd, then $S = \{p : p/q$ has a strictly periodic π-adic expansion$\}$ is a complete set of residues modulo q. That is, every $p' \in R$ is congruent modulo q to precisely one $p \in S$.*

Theorem 3.6 *Suppose a periodic sequence $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ is generated by a FCSR with connection integer q. Let $\gamma = \pi^{-1} \in \mathbb{Z}/(q)$ be the inverse of 2 in the cyclic group of integers modulo q. Then there exists $A \in \mathbb{Z}/(q)$ such that for all $i = 0, 1, 2, \ldots$ we have,*

$$a_i = A\gamma^i \pmod{q} \pmod{\pi}$$

Here the notation (mod q)(mod 2) means that first the number $A\gamma^i$ should be reduced mod q to give a number in S, and then that number should be reduced mod π to give an element of $R/(\pi) = \{0, 1\}$. (Notice that there is no homomorphism $R/(q) \to R/(2)$ if q is odd, so the notation (mod q)(mod 2) needs a precise definition.)

It is desirable to generate pseudorandom sequences with large periods using simple shift register hardware. In the case of linear feedback shift registers, the subject of maximal period sequences has been studied for many years. The simplest way to obtain sequences of maximal length is to use a primitive connection polynomial (and the resulting sequences are called m-sequences.) One may ask the same question for FCSR sequences. By Theorem 3.6, the maximum period for a FCSR with connection integer q is $T = |R/(q) - \{0\}|$ (note that $R/(q)$ is always finite). Accordingly, we make the following definition.

Definition 3.7 *An ℓ-sequence is a periodic sequence of period $T = |R/(q) - \{0\}|$ obtained from a d-FCSR with connection integer q.*

By Theorem 3.6 an ℓ-sequence is generated whenever q is chosen so that $ord_q(\pi) = |R/(q) - \{0\}|$. The search for primes q such that π is a primitive root, is related to a large body of contemporary number theory. It is believed that there are infinitely many primes q with this property [4].

4 Cracking d-Fold Summation Ciphers

As mentioned in the introduction, our analysis has important consequences for the summation cipher [9]. In this cipher, two m-sequences $\mathbf{a}_1$ and $\mathbf{a}_2$ are combined using "addition with carry". The resulting sequence is used as a pseudo-one-time-pad. These sequences have generated great interest since they appear to be resistant to certain types of cryptologic attack. If the constituent sequences $\mathbf{a}_i$ have period T_i then the resulting sequence has linear span which is close to the product T_1T_2, assuming the constituent sequences were chosen appropriately. In practice, many m-sequences, $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$ are added with carry operation and the resulting linear span approaches the product $T_1 \cdot T_2 \cdots T_k$.

However, we observe that the addition with carry operation corresponds to adding the sequences as if they were 2-adic integers. This leads us to be able to synthesize a FCSR that generates the resulting sequence when only a relatively small number of bits are known. To properly describe this weakness, we need an analogue of linear span for FCSRs.

Let $\mathbf{a} = \{a_0, a_1, \ldots\}$ be a binary, eventually period sequence.

Definition 4.1 *The π-adic span of $\mathbf{a}$ is the number of stages r in the smallest d-FCSR whose output coincides with the periodic part of the sequence $\mathbf{a}$.*

If $\alpha = \sum_{i=0}^{\infty} a_i \pi^i = p/q$ is the corresponding rational number, reduced to lowest terms, with $q = \sum_{i=0}^{r} q_i \pi^i$, then the π-adic span is r since, by Theorem 3.1, q is the connection integer of the desired FCSR.

Theorem 4.2 *Suppose $\mathbf{a}$ and $\mathbf{b}$ are periodic binary sequences with π-adic span r and s respectively. Let $\mathbf{c}$ denote the binary sequence obtained by adding the sequences $\mathbf{a}$ and $\mathbf{b}$ with d-fold carry (see [9] for the $d = 1$ case). Then the π-adic span of $\mathbf{c}$ is less than or equal to $r + s$.*

We return to the situation in which two m-sequences, $\mathbf{a}_1$ and $\mathbf{a}_2$, of period T_1 and T_2, respectively, are combined using addition with carry. If $d = 1$, this is precicesly the situation of a summation combiner, but for larger d, this corresponds to a different combiner with memory (requiring d bits of memory). The preceding theorem shows that the π-adic span of the resulting sequence is bounded by $T_1 + T_2$ and it may be much smaller if the π-adic span of the constituent sequences is small. More generally, if many m-sequences, $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k$, where $\mathbf{a}_i$ has period T_i, are added with carry, the π-adic span of the resulting sequence is no more than the sum $T_1 + T_2 + \cdots + T_k$. It follows that Mandelbaum's variant of the Berlekamp-Massey algorithm [8] (which we refer to as the MBM algorithm), as described in detail in the next subsection, can be used to synthesize a FCSR that generates the sequence when only a relatively few bits are known. This throws considerable doubt on the security of these stream ciphers.

One is thus led to the rather interesting problems of identifying the π-adic span of an m-sequence and of identifying the linear span of an ℓ-sequence. Although we do not know the answer to these questions, when $d = 1$ the following result gives a sufficient condition for an m-sequence to have maximal 2-adic span.

Theorem 4.3 *Suppose $\mathbf{a}$ is a periodic sequence with period $T = 2^N - 1$. Suppose that $2^T - 1$ is prime. Then the 2-adic span of $\mathbf{a}$ is equal to the period T.*

More generally, the 2-adic span of any periodic sequence of period T is greater than or equal to the smallest prime divisor of $2^T - 1$.

The Berlekamp-Massey algorithm for synthesizing linear feedback shift registers has been modified by Mandelbaum for use with binary expansions of positive real numbers less than one [8]. Essentially the same algorithm works in the setting of π-adic numbers. If r is the π-adic span of $\mathbf{a}$, there is experimental evidence that the MBM algorithm converges in $O(r)$ steps to a d-FCSR that generates $\mathbf{a}$. As with Mandelbaum's algorithm for rational approximation to real numbers, whether this actually holds is an open question.

5 Conclusions

Feedback-with-carry shift register sequences are entirely parallel to linear feedback shift register sequences. However, techniques of number theory rather than Galois theory appear to be needed for their analysis. For $d = 1$, maximal length d-FCSR sequences have appeared in a diverse array of circumstances over the last twenty-five years, and it has often been observed that their behavior is similar to that of m-sequences. The use of the π-adic numbers provides a framework in which these similarities can be formalized and studied systematically. One consequence is that the summation cipher, when analyzed from this point of view, no longer appears to be secure. Perhaps the most important cryptographic result of these observations is that we have a new measure of security that must be considered whenever we design stream ciphers. The sequences we use must have large π-adic span, at least for small values of d.

References

[1] L. Blum, M. Blum, and M. Shub, A simple unpredictable pseudo-random number generator, *Siam J. Comput.* vol. 15, pp. 364-383 (1986).

[2] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801; reprinted in English translation by Yale Univ. Press, New Haven, CT. 1966.

[3] S. Golomb *Shift Register Sequences.* Aegean Park Press, Laguna Hills CA, 1982.

[4] C. Hooley, On Artin's conjecture. *J. Reine Angew. Math.* vol. 22, 1967 pp. 209-220.

[5] A. Klapper and M. Goresky, Feedback Shift Registers, Combiners with Memory, and Arithmetic Codes, *Univ. of Kentucky, Dept. of Comp. Sci. Tech. Rep. No. 239-93.* Presented at *1993 Cambridge Workshop on Algorithms.*

[6] D. Knuth, *The Art of Computer Programming, Vol 2. Seminumerical Algorithms.* Addison-Wesley, Reading MA, 1981.

[7] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta Functions.* Graduate Texts in Mathematics Vol. 58, Springer Verlag, N.Y. 1984.

[8] D. Mandelbaum, An approach to an arithmetic analog of Berlekamp's algorithm. *IEEE Trans. Info. Theory,* vol. IT-30, 1984 pp. 758-762.

[9] R. Rueppel *Analysis and Design of Stream Ciphers.* Springer Verlag, New York, 1986.