On Algebraic Shift Registers

MIDN 1/C Charles Celerier

November 11, 2011

Abstract

This is an Honors Project Proposal for 2011-2012 between myself and my advisor, Professor Joyner.

1 Introduction

2 The Ring of N-adic Integers

The notation used in the definition of the N-adic numbers will follow the same notation used by Borevich and Shafarevich in Chapter 1 of **Number Theory**.

In this section, the set of N-adic integers is shown to be a commutative ring with an identity.

Definition 2.1. Let N be an integer. Then the infinite integer sequence $\{x_n\}$ determines a *N-adic integer* α, or $\{x_n\} \to \alpha$, if

$$x_{i+1} \equiv x_i \pmod{N^{i+1}} \quad \forall i \geq 0. \tag{1}$$

Two sequences $\{x_n\}$ and $\{x'_n\}$ determine the same N-adic integer if

$$x_i \equiv x'_i \pmod{N^{i+1}} \quad \forall i \geq 0. \tag{2}$$

The *set of all N-adic integers* will be denoted by $\mathbb{Z}_N$.

Ordinary integers will be called *rational integers* and each rational integer x is associated with a N-adic integer, determined by the sequence $\{x,\ x,\ \ldots,\ x,\ \ldots\}$.

Example 1. Let $\{x_n\} \to \alpha \in \mathbb{Z}_3$. Then the first 5 terms of $\{x_n\}$ may look something like:

$$\begin{aligned}\{x_n\} &= \{1\ ,\ 1+2\cdot 3\ ,\ 1+2\cdot 3+1\cdot 3^2\ ,\\ &\qquad 1+2\cdot 3+1\cdot 3^2\ ,\ 1+2\cdot 3+1\cdot 3^2+1\cdot 3^4\ ,\ \ldots\}\\ &= \{1, 7, 16, 16, 97, \ldots\}\end{aligned}$$

Then equivalent sequences to $\{x_n\}$ could begin differently for the first few terms:

$$\{y_n\} = \{4, 25, 16, 178, 583, \dots\}$$
$$\{z_n\} = \{-2, -47, 232, -308, 97, \dots\}$$

The sequences for $\{y_n\}$ and $\{z_n\}$ satisfy equation (1) for the first 5 terms, so they could be N-adic integers up to this point. Also, both are equivalent to $\{x_n\}$ according to the equivalence defined in equation (2).

$$1 \equiv 4 \equiv 2 \pmod 3$$
$$7 \equiv 25 \equiv -47 \pmod{3^2}$$
$$16 \equiv 16 \equiv 232 \pmod{3^3}$$
$$16 \equiv 178 \equiv -308 \pmod{3^4}$$
$$97 \equiv 583 \equiv 97 \pmod{3^5}$$

Therefore $\{x_n\}, \{y_n\}, \{z_n\} \to \alpha$.

Because there are infinitely many sequence representations for any N-adic integer, it is useful to define a canonical sequence to be used when writing N-adic integers as sequences.

Definition 2.2. For a given N-adic integer α, a given sequence $\{a_n\}$ with the properties:

i. $\{a_n\} \to \alpha$

ii. $\{a_n\} = \{a_0,\ a_0 + a_1 \cdot N,\ \dots,\ a_0 + \dots + a_i \cdot N^i,\ \dots\} : 0 \le a_i < N \quad \forall i \ge 0$

will be called *canonical*. The number $a_0 a_1 a_2 \dots a_i \dots$ is the *digit representation* of α.

Example 2. In Example 1, the sequence $\{x_n\}$ was a canonical sequence that determined the N-adic integer α. A few more examples of canonical sequences determining 7-adic integers are given here:

$\beta = 3164\dots$, then the canonical sequence $\{b_n\} \to \beta$ is

$$\begin{aligned}\{b_n\} &= \{3,\ 3 + 1 \cdot 7,\ 3 + 1 \cdot 7 + 6 \cdot 7^2,\ 3 + 1 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^3,\ \dots\} \\ &= \{3, 10, 304, 1676, \dots\}\end{aligned}$$

$\gamma = 0164\dots$, then the canonical sequence $\{c_n\} \to \gamma$ is

$$\begin{aligned}\{c_n\} &= \{0,\ 1 \cdot 7,\ 1 \cdot 7 + 6 \cdot 7^2,\ 1 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^3,\ \dots\} \\ &= \{0, 7, 301, 1673, \dots\}\end{aligned}$$

$\delta = 5031\dots$, then the canonical sequence $\{d_n\} \to \delta$ is

$$\begin{aligned}\{d_n\} &= \{5,\ 5, 5 + 3 \cdot 7^2,\ 5 + 3 \cdot 7^2 + 1 \cdot 7^3,\ \dots\} \\ &= \{5, 5, 152, 495, \dots\}.\end{aligned}$$

Definition 2.3. Addition and multiplication in $\mathbb{Z}_N$ are done term by term. Let $\alpha, \beta \in \mathbb{Z}_N$ and $\{x_n\} \to \alpha, \{y_n\} \to \beta$. Then,

$$\{x_n\} + \{y_n\} := \{x_0 + y_0, x_1 + y_1, \dots\} \to \alpha + \beta$$
$$\{x_n\} \cdot \{y_n\} := \{x_0 \cdot y_0, x_1 \cdot y_1, \dots\} \to \alpha \cdot \beta$$

Define $\{0, 0, 0, \dots\} \to 0 \in \mathbb{Z}_N$ and $\{1, 1, 1, \dots\} \to 1 \in \mathbb{Z}_N$

Lemma 2.1. *For $\alpha \in \mathbb{Z}_N$, $\alpha + 0 = 0 + \alpha = \alpha$ and $1 \cdot \alpha = \alpha \cdot 1 = \alpha$.*

Proof. Let $\{x_n\} \to \alpha \in \mathbb{Z}_N$.

$$\begin{aligned}\{x_n\} + \{0, 0, \dots\} &= \{x_0 + 0, x_1 + 0, \dots, x_i + 0, \dots\} \\ &= \{x_0, \dots, x_i, \dots\}. \\ \{0, 0, \dots\} + \{x_n\} &= \{0 + x_0, 0 + x_1, \dots, 0 + x_i, \dots\} \\ &= \{x_0, \dots, x_i, \dots\}.\end{aligned}$$

$\{x_n\} = \{x_n\} + \{0, 0, \dots\} = \{0, 0, \dots\} + \{x_n\}$ implies $\alpha = \alpha + 0 = 0 + \alpha$. Therefore, the additive identity in $\mathbb{Z}_N$ is 0.

$$\begin{aligned}\{x_n\} \cdot \{1, 1, \dots\} &= \{x_0 \cdot 1, x_1 \cdot 1, \dots, x_i \cdot 1, \dots\} \\ &= \{x_0, \dots, x_i, \dots\}. \\ \{1, 1, \dots\} \cdot \{x_n\} &= \{1 \cdot x_0, 1 \cdot x_1, \dots, 1 \cdot x_i, \dots\} \\ &= \{x_0, \dots, x_i, \dots\}.\end{aligned}$$

$\{x_n\} = \{x_n\} \cdot \{1, 1, \dots\} = \{1, 1, \dots\} \cdot \{x_n\}$ implies $\alpha = \alpha \cdot 1 = 1 \cdot \alpha$. Therefore, the multiplicative identity in $\mathbb{Z}_N$ is 1. □

Finally, this paper defines a *ring* accroding to Fine, Gaglione, and Roesenberger and shows that $\mathbb{Z}_N$ is a *commutative ring with an identity.*

Definition 2.4. [**?**] A *ring* is a set R with two binary operations defined on it. These are usually called addition denoted by $+$, and multiplication denoted by $\cdot$ or juxtaposition, satisfying the following six axioms:

1. Addition is commutative: $a + b = b + a \ \ \forall a, b \in R$.
2. Addition is associative: $a + (b + c) = (a + b) + c \ \ \forall a, b, c \in R$.
3. There exists an additive identity, denoted by 0, such that $a+0 = a \ \forall a \in R$.
4. $\forall a \in R$ there exists an additive inverse, denoted by $-a$, such that $a + (-a) = 0$.
5. Multiplication is associative: $a(bc) = (ab)c \ \forall a, b, c \in R$

6. Multiplication is left and right distributive over addition:

$$a(b+c) = ab + ac$$
$$(b+c)a = ba + ca$$

If it is also true that

7. Multiplication is commutative: $ab = ba \quad \forall a, b \in R$, then R is a *commutative ring*.

Further if

8. There exists a multiplicative identity denoted by 1 such that $a \cdot 1 = a$ and $1 \cdot a = a \quad \forall a \in R$, then R is a *ring with an identity*.

If R satisfies all eight properties, then R is a *commutative ring with an identity.*

Theorem 2.1. *$\mathbb{Z}_N$ is a commutative ring with an identity.*

Proof. Let $\{x_n\}, \{y_n\}, \{z_n\}$ determine $\alpha, \beta, \gamma \in \mathbb{Z}_N$ respectively. Then

1. *Commutativity of Addition*

$$\begin{aligned}\{x_n\} + \{y_n\} &= \{x_0 + y_0, \dots, x_i + y_i, \dots\} \\ &= \{y_0 + x_0, \dots, y_i + x_i, \dots\} \\ &= \{y_n\} + \{x_n\}.\end{aligned}$$

   $\{x_n\} + \{y_n\} \to \alpha + \beta$ and $\{x_n\} + \{y_n\} = \{y_n\} + \{x_n\} \to \beta + \alpha$. Therefore, by Definition 2.1, $\alpha + \beta = \beta + \alpha$.

2. *Associativity of Addition*

$$\begin{aligned}\{x_n\} + (\{y_n\} + \{z_n\}) &= \{x_n\} + \{y_0 + z_0, \dots, y_i + z_i, \dots\} \\ &= \{x_0 + (y_0 + z_0), \dots, x_i + (y_i + z_i), \dots\} \\ &= \{(x_0 + y_0) + z_0, \dots, (x_i + y_i) + z_i, \dots\} \\ &= \{x_0 + y_0, \dots, x_i + y_i, \dots\} + \{z_n\} \\ &= (\{x_n\} + \{y_n\}) + \{z_n\}.\end{aligned}$$

   Therefore, $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$.

3. *Existence of the Additive Identity*

   By Lemma 2.1, 0 is the additive identity.

4. *Existence of Additive Inverses*

   Define $-\{x_n\} = \{p - x_0, p^2 - x_1, \dots, p^{i+1} - x_i, \dots\} \to -\alpha$. Then

$$\begin{aligned}\{x_n\} + (-\{x_n\}) &= \{x_0 + p - x_0, x_1 + p^2 - x_1, \dots, x_i + p^{i+1} - x_i, \dots\} \\ &= \{p, p^2, \dots, p^{i+1}, \dots\} \\ &\equiv \{0, 0, \dots\} \\ &= 0.\end{aligned}$$

Therefore, $\alpha + (-\alpha) = 0$.

5. *Associativity of Multiplication*

$$\begin{aligned}\{x_n\}(\{y_n\}\{z_n\}) &= \{x_n\}\{y_0z_0, \dots, y_iz_i, \dots\} \\ &= \{x_0(y_0z_0), \dots, x_i(y_iz_i), \dots\} \\ &= \{(x_0y_0)z_0, \dots, (x_iy_i)z_i, \dots\} \\ &= \{x_0y_0, \dots, x_iy_i, \dots\}\{z_n\} \\ &= (\{x_n\}\{y_n\})\{z_n\}.\end{aligned}$$

Therefore, $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.

7. *Commutativity of Multiplication*

$$\begin{aligned}\{x_n\}\{y_n\} &= \{x_0y_0, \dots, x_iy_i, \dots\} \\ &= \{y_0x_0, \dots, y_ix_i, \dots\} \\ &= \{y_n\}\{x_n\}.\end{aligned}$$

Therefore, $\alpha\beta = \beta\alpha$.

6. *Left and right distributivity of multiplication over addition*

$$\begin{aligned}\{x_n\}(\{y_n\} + \{z_n\}) &= \{x_n\}\{y_0 + z_0, \dots, y_i + z_i, \dots\} \\ &= \{x_0(y_0 + z_0), \dots, x_i(y_i + z_i), \dots\} \\ &= \{x_0y_0 + x_0z_0, \dots, x_iy_i + x_iz_i, \dots\} \\ &= \{x_n\}\{y_n\} + \{x_n\}\{z_n\}.\end{aligned}$$

By commutativity of multiplication,

$$\begin{aligned}(\{y_n\} + \{z_n\})\{x_n\} &= \{x_n\}(\{y_n\} + \{z_n\}) \\ &= \{x_n\}\{y_n\} + \{x_n\}\{z_n\} \\ &= \{y_n\}\{x_n\} + \{z_n\}\{x_n\}.\end{aligned}$$

Therefore, $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $(\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha$.

8. *Existence of a multiplicative identity*

By Lemma 2.1, 1 is the multiplicative identity.

Properties 1 through 8 from Definition 2.4 are satisfied, so $\mathbb{Z}_N$ is a commutative ring with an identity.

□

Theorem 2.2. *An N-adic integer α, which is determined by a sequence $\{x_n\}$, is a unit if and only if x_0 is relatively prime to N.*

Proof. Let α be a unit. Then there is an N-adic integer β such that $\alpha\beta = 1$. If β is determined by the sequence $\{y_n\}$, then

$$x_i y_i \equiv 1 \pmod{N^{i+1}} \ \ \forall i \geq 0. \tag{3}$$

In particular, $x_0 y_0 \equiv 1 \pmod{N}$ and hence $x_0 \not\equiv 0 \bmod N$. Thus, x_0 is relatively prime to N. Conversely, let x_0 be relatively prime to N. Then $x_0 \not\equiv 0 \pmod{N}$. From (1)

$$\begin{aligned} x_1 &\equiv x_0 \pmod{N} \\ &\vdots \\ x_{i+1} &\equiv x_i \pmod{N^i}. \end{aligned}$$

Working backward, $x_{i+1} \equiv x_i \equiv \cdots \equiv x_1 \equiv x_0 \pmod{N}$. Thus, x_i is relatively prime to $p \ \ \forall i \geq 0$, which implies x_i is relatively prime to N^{i+1}. Consequently, $\forall i \geq 0 \ \exists y_i$ such that $x_i y_i \equiv 1 \pmod{N^{i+1}}$. Since $x_{i+1} \equiv x_i \pmod{p}^i$ and $x_{i+1} y_{i+1} \equiv x_i y_i \pmod{N^i}$. Then, $y_{i+1} \equiv y_i \pmod{N^i}$. Therefore the sequence $\{y_n\}$ determines some N-adic integer β. Because $x_i y_i \equiv 1 \pmod{N^{i+1}} \ \ \forall i \geq 0$, $\alpha\beta = 1$. This means α is a unit. □

From this theorem it follows that a rational integer $a \in \mathbb{Z}_N$ is a unit if and only if a is relatively prime to N. If this condition holds, then $a^{-1} \in \mathbb{Z}_N$. Then for any rational integer $b \in \mathbb{Z}_N$, $b/a = a^{-1}b \in \mathbb{Z}_N$.

3 Constructing Sequences Determing $\frac{b}{a}$ in $\mathbb{Z}_N$

For any rational number b/a, a relatively prime to N, there exists a sequence $\{x_n\} \to b/a \in \mathbb{Z}_N$. At this point, it is worth using the digit representation for integers in $\mathbb{Z}_N$. So $\{x_n\} = \{x_0, \ x_0 + x_1 N, \ \ldots, \ x_0 + \cdots + x_i N^i, \ \ldots\}$ and $b/a = x_0 x_1 \ldots x_i \ldots$. Rather than finding $a^{-1} \pmod{N}^{i+1}$ to determine each x_i, it is not too difficult for every i to find $\sum_{k=0}^{i} x_k N^k$ such that

$$b \equiv a \sum_{k=0}^{i} x_k N^k \pmod{N^{i+1}}. \tag{4}$$

Then,

$$x_i = \frac{\sum_{k=0}^{i} x_k N^k - \sum_{k=0}^{i-1} x_k N^k}{N^k}. \tag{5}$$

Nearly all of the digits for any rational number in $\mathbb{Z}_N$ can also be found using powers of N^{-1}, which is much simpler to analyze than the brute force search for the digits mentioned above.

Theorem 3.1. *Let $u_0, q, N \in \mathbb{Z}$, where q is relatively prime to N, $|u_0| < q$, and $q = -q_0 + \sum_{i=1}^{r} q_i N^i$ for $0 \leq q_i < N$. Define $\alpha = u_0/q \in \mathbb{Z}_N$ such that $\alpha = \sum_{i=0}^{\infty} a_i N^i$ for $0 \leq a_i < N$. Also, define $u_k \in \mathbb{Z}$ such that $u_k/q =$*

$\sum_{i=k}^{\infty} a_i N^{i-k} \in \mathbb{Z}_N$ *and* $\gamma \equiv N^{-1} \pmod{q}$. *Then, there exist* u_k *for every* $k \geq 0$ *such that*

$$a_k \equiv q^{-1} u_k \pmod{N}. \tag{6}$$

If $-q < u_0 < 0$, *then* $u_k \in \{-q, \ldots, -1\}$ *for* $k \geq 0$. *Otherwise, for* $k > \lfloor \log_N(q) \rfloor = r$, $u_k \in \{-q, \ldots, -1\}$

Let $\omega \in \{-q, \ldots, -1\}$ *such that* $\omega \equiv \gamma^k u_0 \pmod{q}$. *Then for* $k > \lfloor \log_N(q) \rfloor = r$, *or if* $-q < u_0 < 0$, *then* $k \geq 0$,

$$a_k \equiv q^{-1} \omega \pmod{N}. \tag{7}$$

Proof. Write u_0/q in terms of u_k.

$$\begin{aligned} \frac{u_0}{q} &= a_0 + N\frac{u_1}{q} = a_0 + a_1 N + N^2 \frac{u_2}{q} = \ldots \\ &= \sum_{i=0}^{k-1} a_i N^i + N^k \frac{u_k}{q} \quad \forall k \geq 1. \end{aligned} \tag{8}$$

Rewrite (8) to be

$$p^k u_k = u_0 - q\left(\sum_{i=0}^{k-1} a_i p^i\right) \quad \forall k \geq 1 \tag{9}$$

Then $|u_0| < q$ and $0 \leq a_i < p$ from the assumptions and equation (9). These imply for all $k \geq 1$, $|u_0| = |q\sum_{i=0}^{k-1} a_i p^i + p^k u_k| < q$. Then,

$$\begin{aligned} -q - q\sum_{i=0}^{k-1} a_i p^i < p^k u_k < q - q\sum_{i=0}^{k-1} a_i p^i \\ \Rightarrow -q\left(\frac{1 + \sum_{i=0}^{k-1} a_i p^i}{p^k}\right) < u_k < q\left(\frac{1 - \sum_{i=0}^{k-1} a_i p^i}{p^k}\right). \end{aligned}$$

u_k may only greater than zero when $\frac{1-\sum_{i=0}^{k-1} a_i p^i}{p^k}$ greater than zero. This only occurs when the sequence $[a_0, \ldots, a_j] = [0, \ldots, 0]$ for $j \geq 0$. Such a sequence occurs if and only if $u_0 \geq 0$ and $u_0 \equiv 0 \pmod{p)^i}$ for $0 \leq i \leq j$, $j \geq 0$. This is clear from the construction of p-adic sequences for rational numbers. Therefore u_k may only be greater than zero if $u_0 \geq 0$ and $u_0 \equiv 0 \pmod{p)^i}$ for $0 \leq i \leq j$, $j \geq 0$. The lower bound is greater than $-q$. This clear because $\frac{1+\sum_{i=0}^{k-1} a_i p^i}{p^k} \leq 1$. Therefore,

$$-q < u_k < 0 \; for \; -q < u_0 < 0.$$

If $0 \geq u_0 < q$, then the upper bound remains unchanged.

$$-q < u_k < q\left(\frac{1 - \sum_{i=0}^{k-1} a_i p^i}{p^k}\right) \text{ for } 0 \leq u_0 < q$$

There is still work to be done on the upper bound.

$$\begin{aligned} 0 \leq \sum_{i=0}^{k-1} a_i p^i < p^k \ for\ k \geq 1 \\ \Rightarrow -q(\sum_{i=0}^{k-1} a_i p^i) \leq 0 \\ \Rightarrow u_0 - q(\sum_{i=0}^{k-1} a_i p^i) < q \\ \Rightarrow p^k u_k < q \\ \Rightarrow u_k < \frac{q}{p^k}. \end{aligned}$$

For $k > \lfloor \log_p(q) \rfloor = r$, $|q/p^k| < 1$. Therefore, $-q < u_k < 0$ for $0 \leq u_0 < q$ and $k > r$. Further lowering the upperbound, if $u_k = 0$, then $u_0/q = \sum_{i=0}^{k-1} a_i p^i + 0$. This implies u_0/q is a rational integer, which is not true. Noting finally that u_k must be an integer. If $|u_0| < q$ and $u_0 < 0$, or $|u_0| < q$, $u_0 \geq 0$, and $k > \lfloor \log_p(q) \rfloor = r$, then

$$u_k \in \{-q, \ldots, -1\}.$$

It has now been shown for certain restrictions u_k belongs to a specific set of representatives for the residue classes of $\mathbb{Z}/(q)$. Define $\gamma \equiv p^{-1} \pmod{q}$. Reducing (9) modulo q shows that

$$u_k \equiv \gamma u_{k-1} \pmod{q}. \tag{10}$$

Since this is true for all k greater than or equal to 1, it is clear that

$$u_k \equiv \gamma^k u_0 \pmod{q}. \tag{11}$$

Reducing (9) modulo p shows that

$$a_k \equiv q^{-1} u_k \pmod{p}. \tag{12}$$

Define $\omega \equiv \gamma^k u_0 \pmod{q}$, and $\rho \equiv q^{-1} \bmod p$. Finally, if $|u_0| < q$ and $u_0 < 0$, or $|u_0| < q$, $u_0 \geq 0$, and $k > \lfloor \log_p(q) \rfloor = r$, then

$$a_k \equiv \rho\omega \pmod{p}. \tag{13}$$

□

Corollary 3.1. *Let $0 \leq u_0 < q$. Define j to be the greatest integer such that $u_0 \equiv 0 \pmod{p}^j$. Then the following are true:*

i. $j \leq \lfloor \log_p q \rfloor = r$

ii. $[a_0, \ldots, a_{j-1}] = [0, \ldots, 0]$

iii. $u_k > 0$ *for* $k = j$

iv. $u_k \not\equiv 0 \pmod{p}$

The results of this corollary are straightforward.

Theorem 3.1 shows that for $-q < u_0 < 0$, there is a sequence of numerators $\{u_k\}$ directly related to the sequence of digits $\{a_k\}$ for $u_0/q \in \{z_n\}$. This is provides a more powerful tool for the analysis of the sequences generated by AFSRs. The results shown here fill in the gaps of the incorrect proof shown in Theorem 10 of Klapper and Xu's paper.

4 Feedback with Carry Shift Registers

A description of algebraic feedback shift registers specific to $\mathbb{Z}_p$ is defined here. The definition of the register follows the one given in Andrew Klapper's book.

Definition 4.1. Let $q_0, q_1, \ldots, q_m \in \mathbb{Z}/(p)$ for $p \in \mathbb{Z}$ and assume that $q_0 \not\equiv 0 \pmod{p}$. An *algebraic feedback shift register* (or *AFSR*) over ($\mathbb{Z}$,p,S) of length m with *multipliers* or *taps* $q_0, q_1, \ldots, q_m$ is a discrete state machine whose states are collections

$$(a_0, a_1, \ldots, a_{m-1}; z) \text{ where } a_i \in S \text{ and } z \in \mathbb{Z}$$

consisting of cell contents a_i and memory z. The state changes according to the following rules:

1. Compute
$$\sigma = \sum_{i=1}^{m} q_i a_{m-i} + z.$$
2. Find $a_m \in S$ such that $-q_0 a_m \equiv \sigma \pmod{p}$. That is $a_m \equiv -q_0^{-1}\sigma \pmod{p}$.
3. Replace $(a_0, \ldots, a_{m-1})$ by $(a_1, \ldots, a_m)$ and replace z by $\sigma(\mathrm{div}p) = (\sigma + q_0 a_m)/p$.

5 Xu's Rational Approximation Algorithm

In Andrew Klapper's book, he roughly describes Xu's rational approximation algorithm for π-adic sequences in any ring R. A description of Xu's Algorithm is presented here in the context of the ring $\mathbb{Z}_p$, where p does not have to be prime.

The rational approximation problem is presented here: Given the eventually periodic digit representation of $fracab \in \mathbb{Z}_p$, find a and b.

If there are no constraints on a and b, then the entire sequence must be known to solve the problem. Specifically, a single algebraic feedback shift register can not produce all $fracab \in \mathbb{Z}_p$.

References