International Journal of Pure and Applied Mathematics
Volume 42 No. 4 2008, 515-520

FINITE DYNAMICAL SYSTEMS ON $\mathbb{Z}_{p^n}$

René A. Hernández-Toledo
Department of Mathematics
University of Puerto Rico at Cayey
Cayey, Puerto Rico, 00736, USA
e-mail: rhernandez@cayey.upr.edu

Abstract: The dynamics of multiplication by elements of $\mathbb{Z}_{p^n}$ is studied and closed formulas are obtained for all possible cases.

AMS Subject Classification: 37B99, 05C38, 99B20, 94C99
Key Words: finite dynamical systems, cycles' formulas, Galois rings

1. Introduction

Finite dynamical systems (FDS) include a variety of types: cellular automatas, machines of finite states, logic sequential circuits, sequential dynamical systems, neuronal networks, genetic networks, etc. As consequence, they have a great amount of applications. An FDS consists of a function $f : X \longrightarrow X$, where X is a finite set. Associated with that system, there is a directed graph, $\mathcal{G}_f$, whose vertices are the elements of X and there is an arrow from the vertex x to the vertex y whenever $f(x) = y$. It is known that its connected components consist of trees (transients states) whose roots are located on a cycle (stable state or limit cycle). The dynamic of the system is the description of the transients states and the amount and length of the cycles. Usually, an state is an n–uple of elements that belong to a set V of values. The function f is the transition from some state to the next one. Initially, V was chosen to be equal to $\{0, 1\}$ provided with the natural Boolean algebra structure. Later, with the objective of having more values for the state variables, V was chosen to be a finite field. In such case, X has a natural structure of vector space and when we suppose that

Received: August 17, 2007

f is linear, we obtain the notion of linear FDS (LFDS). The dynamic structure of such systems is totally well–known over an arbitrary finite field (see [4], [5]). This article study the use of the ring of integer module a power of p, as possible values. Our motivation is twofold. In the first place, it is, mathematically, a natural extension. Secondly, most of the authors (see [2], [7]) consider, specially for genetic networks, an advantage to have a greater amount of possible values, since that would allow better discretization of variables that appear naturally like continuous (for example, variations in concentrations). Certainly, there are fields of big size, but the computacional manipulation of the arithmetic of such fields requires specialized software and relatively deep knowledge of the finite field theory. On the contrary, the arithmetic of the indicated rings is built–in in most of computer languages and its manipulation requires only a basic congruences' knowledge. We added to the previous observation, an interesting remark in [1] saying that any n–dimensional FDS over $\mathbb{Z}_p$ is equivalent to some unidimensional FDS over $\mathbb{Z}_{p^n}$.

In this article, we study the dynamic of the multiplications in $\mathbb{Z}_{p^n}$, p an odd prime. The main results are Theorems 1 and 2 of the third section. They describe the dynamic of all possible cases. In the second section, we present the notation that we will use and some previous results necessary for the theorem's proofs. For other nomenclature and conventions, we refer to [5].

2. General Considerations

We denoted by $\mathbb{Z}$ the ring of integers and by $\mathbb{Z}_m$ the ring of integers module m. From now on, we will fix a prime number p. An element x has *p–weight* $r = w_p(x)$, iff, p^r is a factor of x but p^{r+1} is not. We agree that $w_p(0) = \infty$. We will be denoted by $o_n(x)$ the order of the reduction module p^n of x in the multiplicative rings of units $\mathbb{Z}^*_{p^n}$. Finally, $hi(x)$ will denote the largest integer r such that $x^r = 1$ on $\mathbb{Z}_{p^n}$.

The following propositions relate orders among different reductions of same elements.

Proposition 2.1. *Let x be an integer, $r = hi(x)$, p an odd prime.*
(a) If $x \equiv I \pmod{p^r}$, then $x^p \equiv I \pmod{p^{r+1}}$.
(b) If $hi(x) = r > 0$, then $o_{r+1}(x) = p$ and $hi(x^p) = r + 1$.
(c) Let $o_n(x) = tp^e$ with $(t, p) = 1$ and $e \geq 0$. Then, $o_{n+1}(x) = tp^{e+1}$.
(d) $o_{r+k}(x) = tp^{k-1}$, where $t = o_{r+1}(x)$.

Proof. (a) $x \equiv I \pmod{p^n}$ implies that $x = I + p^r y$ for some $y \in B$. Thus,

$$x^p = (I + p^r y)^p = I + \sum_{k=1}^{p-1} \binom{p}{k} (p^r)^k y^k + (p^r)^p y^p.$$

Now, for $1 \leq k \leq p-1$, we have that $w_p(\binom{p}{k})(p^r)^k) \geq 1 + rk \geq 1 + r$ and $w_p((p^r)^p) = rp \geq 2r \geq r + 1$. Hence, all terms inside the summatory are divisible by p^{r+1}, therefore $x^p \equiv I \pmod{p^{r+1}}$.

(b) By the previous result, we have that $x^p \equiv I \pmod{p^{r+1}}$, so $o_{r+1}(x)$ must divide p. But, $o_{r+1}(x) = 1$ contradicts the maximality of r, so $o_{r+1}(x) = p$. $hi(x) = r$ implies that $x = 1 + p^r u$ with $(u, p) = 1$. Hence

$$x^p = (1 + p^r u)^p = 1 + p^{r+1} u + \sum_{j=2}^{p-1} \binom{p}{j} (p^r)^j u^j + (p^r)^p u^p.$$

Now $w_p(\binom{p}{j} p^{rj}) = 1 + rj \geq 1 + 2r \geq r + 2$ and $w_p(p^{rp}) \geq pr \geq 3r \geq r + 2$. Hence, $x^p = 1 + p^{r+1} u \neq 1 \pmod{p^{r+2}}$.

(c) Let $y = x^t$, then $o_n(y) = p^e$, that is, $y^{p^e} \equiv I \pmod{p^n}$, and e is the largest integer with such property. Therefore, $o_{n+1}(y) = p^{e+1}$. Therefore, $x^{tp^{e+1}} \equiv I \pmod{p^{n+1}}$. This implies that $o_{n+1}(x) = sp^{e+1}$ with $s|t$. As $x^{sp^{e+1}} \equiv I \pmod{p^{n+1}}$ implies that $x^{sp^{e+1}} \equiv I \pmod{p^n}$, we have that $o_n(x) = tp^e | sp^{e+1}$, and since $(t, p) = 1$, we must have that $t|s$. So, $s = t$.

(d) If $r = 0$ the result follows from part c), else it follows form part b) with $t = p$ and induction. □

3. Dynamics on $\mathbb{Z}_{p^n}$

3.1. Notations, Conventions and Other Previous Facts

From now on p will denote an odd prime number, $\mathbb{Z}_{p^n}^*$ will be the group of units of $\mathbb{Z}_{p^n}$. We choose a fixed set of representatives for $\mathbb{Z}_{p^n}$ consisting of all integers from 0 up to $p^n - 1$. Therefore, as sets we have that $\mathbb{Z}_p \subset \mathbb{Z}_{p^2} \subset \cdots \subset \mathbb{Z}_{p^n} \subset \cdots \subset \mathbb{Z}$. It is known, see for example [6], that $|\mathbb{Z}_{p^n}^*| = p^{n-1}(p-1)$.

3.2. Dynamics of Multiplication by Units

The objective of this section is to prove the following theorem.

Theorem 1. *Let a be an unit of $\mathbb{Z}_{p^n}$ with $hi(a) = r$, $n > r$, then the graph of $L_{a,n} : x \mapsto ax$ is given by*

$$\mathcal{L}_{a,n} = 1 + (p^r - 1)C_1 + s\sum i = r + 1^n C_{tp^{i-r-1}},$$

where C_m denotes a cycle of length m, 1 stands for the cycle $0 \leftrightarrow 0$, t is the order of a in $\mathbb{Z}_{p^r}$ and $s = (p^r)(p-1)/t$.

Proof of Theorem 1. Let $N_i = \{x \in \mathbb{Z}_{p^n} : w_p(x) = n - i\}$, $i = 1, 2, \ldots, n$ and let $N_0 = \{0\}$. Note that $\mathbb{Z}_{p^n}$ is the disjoint union of the N_i's. Hence, $\mathcal{L}_a, n$ will be the sum of the graphs determined over each of the N_i's. Let us remark that $x \in N_i$, iff, there is a y with $x = p^{n-i}y$, $(y, p) = 1$. By the selected representation for the elements of $\mathbb{Z}_{p^n}$ we have that y belongs to $\mathbb{Z}^*_{p^i}$, that is, $N_i = p^{n-1}\mathbb{Z}^*_{p^i}$. As $a(p^{n-i}y) = p^{n-i}(ay)$, we have that the dynamic of the restriction of $L_{a,n}$ over N_i coincides with the dynamics of $L_{a,i}$ over $\mathbb{Z}^*_{p^i}$. For $1 \leq i \leq r$ we have that $L_{a,i} = id$, therefore its graph consists only of 1–cycles. Adding over all such cycles for $i = 1$ up to r, we have that

$$\sum_i^r \mathcal{L}_{a,n} = \sum_{i=1}^r p^{i-1}(p-1)C_1 = (p^r - 1)C_1. \tag{1}$$

Let us see now $L_{a,n}\big|_{N_i}$ for $i > r$. It follows from the previous work that $o_{p^i}(a) = tp^{i-r-1}$. Moreover, as $\mathbb{Z}^*_{p^i}$ is a group, the order of a is the order of the cyclic group generated by a and the other orbits are the cosets of such cyclic group. Hence the have the same amount of elements. Hence, the number of such cycles will be

$$\frac{p^{i-1}(p-1)}{tp^{i-r-1}} = \frac{p^r(p-1)}{t}. \tag{2}$$

Let us call s such number. Thus, $\mathcal{L}_{a,n}\big|_{N_i}$ is given by $sC_{tp^{i-r-1}}$. This finish the proof of the formula. □

Example 3.1. Let $p = 7$ and $a = 4$. Then, $r = hi(4) = 0$ and $t = o_1(3) = 3$. Thus, $s = 1 * 6/3 = 2$. So, $\mathcal{L}_{4,1} = 1 + 2C_3$, $\mathcal{L}_{4,2} = 1 + 2C_3 + 2C_{21}$, $\mathcal{L}_{4,3} = 1 + 2C_3 + 2C_{21} + 2C_{147}$, etc.

Example 3.2. Let $p = 3$ and $a = 7$. Then, $r = hi(7) = 1$, $o_2(7) = 3$. Thus $s = 3 * 2/3 = 2$. So, $\mathcal{L}_{7,1} = 1 + 2C_1$, $\mathcal{L}_{7,2} = 1 + +2C_1 + 2C_3$, $\mathcal{L}_{7,3} = 1 + 2C_1 + 2C_3 + 2C_9$, etc.

3.3. Dynamics of Multiplication by a Non–Unit Element

By using the p–ary expansion, we can consider $\mathbb{Z}_{p^n}$ as vector space over $\mathbb{Z}_p$ with basis $\{1, p, \ldots, p^{n_1}\}$. Let $0 < r < n$, and let L_{p^r} be the multiplication by p^r on $\mathbb{Z}_{p^n}$. The effect of such map over some element x is shifting its coordinates r positions to the right and filling the initial positions with 0's.

$$(a_0, a_1, \ldots, \ldots) \mapsto (\underbrace{0, 0, \ldots, 0}_{r}, a_0, a_1, \ldots).$$

We shall, first, show that L_{p^r} splits $\mathbb{Z}_{p^n}$ into exactly r subspaces that are L_{p^r} invariants. Let $0 \leq i < r$ and consider the subspace $< p^i >$ spanned by p^i and its iterated images by L_{p^r}: $p^i, p^{i+r}, p^{i+2r}, \ldots$. Since $L_{p^r}(p^{i+kr}) = p^{i+(k+1)r}$, we get by induction that $L^k_{p^r}(p^i) = p^{i+kr}$, therefore

$$< p^i >= \{\sum_k \alpha_k p^{i+kr}\}.$$

Let h be the least positive integer such that $p^{i+hr} = 0$ in $\mathbb{Z}_{p^n}$, then $i+hr \geq n$, so $h \geq (n-i)/r$, thus $h = \lceil (n-1)/r \rceil$. Since $p^{i+(h-1)r} \neq 0$, we have that a basis for $< p^i >$ is given by $1, p^i, \ldots p^{i+(h-1)r}$, thus the dimension of $< p^i >$ is precisely h. Since $L^h_{p^r} = 0$, L^h is a nilpotent linear map whose kernel consists of the elements $\alpha p^{i+(h-1)r}$, with $0 \leq \alpha < p$, hence it have dimension 1. From our previous work in [5], it follows that the graph of L_{p^r} restricted to $< p^i >$ is a tree of height h where each node has ramification p, that is each node has p ancestors. We shall denote such tree by $FT(p, h)$. Thus, with respect to L_{p^r}, we have the following decomposition of $\mathbb{Z}_{p^n}$,

$$\mathbb{Z}_{p^n} =< p^0 = 1 > \oplus < p^1 > \oplus \ldots \oplus < p^{r-1} > .$$

Putting, $h_i = \lceil (n-i)/r \rceil$, then we have, see [5], that the graph of L_{p^r} is given by:

$$\mathcal{L}_{p^r} = FT(p, h_1) \times FT(p, h_2) \times \cdots \times FT(p, h_{r-1}).$$

Example 3.3. Let us suppose that $n = 7$, and $r = 3$. Then $h_0 = \lceil 7/3 \rceil = 3$, $h_1 = \lceil 6/3 \rceil = 2$, and $h_2 = \lceil 5/2 \rceil = 2$. Thus.

$$\mathcal{L}_{p^7} = FT(p, 3) \times FT(p, 2) \times FT(p, 2).$$

Let a be a unit of $\mathbb{Z}_{p^n}$ and let us consider multiplication by ap^r. Since $ap^r x = ap^r a^{-1} ax$, we have that $L_{ap^r}(x) = (L_a \circ L_{p^r} \circ L_{a^{-1}})(ax)$. Now as $L_a \circ L_{p^r} \circ L_{a^{-1}}$ is conjugate to L_{p^r} by a bijective map, both maps have the same dynamic, and since $L_{p^r}(ap^i) = ap^{i+r}$, we see that $< ap^i >=< p^i >$, we get that the dynamic of L_{ap^r} and L_{p^r} are the same. Thus, we have proved the following

theorem.

Theorem 2. *Let p be a prime number, n a natural number, a any integer with $(a,p)=1$, and r such that $0<r<n-1$. Let L_{ap^r} denotes the map obtained by multiplication by ap^r on $\mathbb{Z}_{p^n}$. Then, the graph, $\mathcal{L}_{ap^r}$ corresponding to the map is given by*

$$\mathcal{L}_{ap^r} = FT(p,h_1)\times FT(p,h_2)\times\cdots\times FT(p,h_{r-1}),$$

where $h_i=\lceil (n-1)/r\rceil$.

References

[1] D. Bollman, O. Colón-Reyes, E. Orozco, Fixed points in discrete models for regulatory genetic networks, In: *EURASIP Journal on Bioinformatics and System Biology* (2007).

[2] A. Brazma, T. Schlitt, Reverse engineering of gene regulatory networks: a finite state linear model (2003); Preprint available at: htpp://genomebiology.com/2003/4/6/P5.

[3] O. Colón-Reyes, R. Laubenbacher, B. Pareigis, Boolean monomial dynamics systems, *Annals of Combinatorics*, **8**, No. 4 (2004), 425-439.

[4] B. Elspas, The theory of autonomous linear sequential networks, *IRE Transactions on Circuit Theory,* **6**, No. 1 (1959), 45-60.

[5] R.A. Hernández-Toledo, Linear finite dynamical systems, *Communications in Algebra*, **33**, No. 9 (2005), 210-218.

[6] M. Steinberger, *Algebra*, PWS Publishing Company, Boston (1994).

[7] R. Laubenbacher, B. Stigler, A computational algebra approach to the reverse-engineering of gene regulatory networks, *J. Theor. Biol.*, **229** (2004), 523-537.