Journal of Integer Sequences, Vol. 16 (2013),
Article 13.8.3

Iterations of Integer Polynomial Maps Modulo Primes

Alexander Borisov[1]
Department of Mathematics
University of Pittsburgh
301 Thackeray Hall
Pittsburgh, PA 15260
USA
borisov@pitt.edu

Abstract

In this elementary note we discuss some questions related to the behavior of iterations of polynomial maps with integer coefficients modulo primes. In particular, we introduce three examples of such maps that have interesting dynamical properties. Several open questions are stated and discussed.

1 Introduction

Polynomial maps with integer coefficients are among the simplest mathematical objects. If the number of polynomials equals the number of variables, then the map can be iterated. So for any ring R we get a discrete dynamical system on the set R^n, where n is the number of variables (polynomials). In spite of the simplicity of this setup, relatively little is known regarding the dynamical properties of these maps, in particular their periodic points. Generally, one expects that over a global field there are few periodic points. See the paper of Fakhruddin for some results and conjectures in this direction [8]. On the other hand, over an algebraic closure of a finite field there are usually many periodic points. Indeed, if the

[1]The research of the author was supported in part by the NSA grants H98230-08-1-0129, H98230-06-1-0034 and H98230-11-1-0148.

reduction of the map is dominant, then the periodic points are Zariski dense, by a result of the author and Sapir [3]. The dynamics over the local fields received considerable attention, in particular by Silverman and his school [5, 11]. The primary object of investigation in that context is the recurrent points, i.e., the points that lie in the limit set of their iterated images. The one-dimensional case has been especially well studied, in particular by Benedetto [1]. Independently, interesting results were obtained by Khrennikov and Nilsson [9].

Modulo primes, some special cases, most notably monomial maps and quadratic maps in one variable, were studied in great detail. The early works include those of Chassé [6], motivated by the Pollard's rho factorization algorithm. More recently, very precise results were obtained by Vasiga and Shallit [12], Chou and Shparlinski [7], and Sha [10]. This list is very incomplete, and you should consult the above mentioned papers, especially the paper of Vasiga and Shallit, for more references.

This short note is devoted to comparison of the dynamical properties of the map at a generic point (i.e., over $\mathbb{Z}$) and its reductions modulo primes p. The author and Sapir [4] obtained some very general results of this kind and used them to prove that the mapping tori of free group endomorphisms are virtually residually (finite p)-groups for all but finitely many primes p. Importantly, we used the maps over the extensions of of $\mathbb{Z}/p\mathbb{Z}$, and the corresponding extensions of the p-adic numbers. This note grew from an observation that there exist integer polynomial maps which are dominant over $\mathbb{Z}$, but "nilpotent" modulo all primes (see Example 1 below).

The paper is organized as follows. In Section 2 we introduce three particular polynomial maps and prove their properties. In Section 3 we discuss some natural open questions.

2 Examples and Theorems

The first map is the simplest. We discovered it while working with Mark Sapir [3].

Example 1. (Additive Trap) Define $F_{at}(x, y) = (u, v)$, where

$$(u, v) = (x^2y, x^2y + xy^2).$$

Theorem 2. *(a) F_{at} and its reductions modulo p for all primes p are dominant.*

(b) The only fixed point over the algebraic closure of the ground field of F_{at}, and any reduction of it modulo p, is $(0, 0)$.

(c) For every $(x, y) \in \mathbb{F}_p^2$ some multiple of the reduction of F_{at} modulo p sends it to $(0, 0)$.

Proof. (a) We need to show that for a Zariski open subset of pairs (u, v) there exists (x, y) such that $F(x, y) = (u.v)$. For $u \neq 0$, $u \neq v$, take x such that $x^3 = \frac{u^2}{v-u}$ and take $y = \frac{u}{x^2}$.

(b) Suppose $x^2y = x$ and $x^2y + xy^2 = y$. If $x = 0$, then from the second equation $y = 0$. If $x \neq 0$, then from the first equation $xy = 1$. Plugging this into the second equation, we get $x + y = y$, so $x = 0$.

(c) We will prove that modulo any prime p the p-th iteration of F_{at} sends everything to $(0,0)$. Indeed, if $x \neq 0$, then $\frac{v}{u} = \frac{y}{x} + 1$. So after no more than $p-1$ iterations, we get $y = 0$, which forces x and y to become zero at the next step and forever afterwards. $\square$

Note that these properties are in sharp contrast with the result of the author and Sapir that implies that periodic orbits of F_{at} over the algebraic closure of $\mathbb{F}_p$ are Zariski dense [3].

Example 3. (Multiplicative Trap) Suppose $n \geq 2$ is a natural number. Define $F_{mt(n)}(x,y) = (u,v)$, where

$$(u,v) = (x^2y(x-y), nxy^2(x-y)).$$

Theorem 4. *(a) $F_{mt(n)}$ and its reductions modulo p for all primes $p \nmid n$ are dominant.*

(b) The only fixed point over the algebraic closure of the ground field of $F_{mt(n)}$, and its reductions modulo $p \nmid n-1$, is $(0,0)$. For $p|n-1$, the fixed points of the reduction of $F_{mt(n)}$ are $(0,0)$ and such (x,y) that $xy(x-y) = 1$.

(c) The following two statements are equivalent:

1. *Either $p|n$ or n is a multiplicative generator modulo p.*
2. *For every $(x,y) \in \mathbb{F}_p^2$, some multiple of the reduction of $F_{mt(n)}$ modulo p sends it to $(0,0)$.*

Proof. (a) For generic u and v, take x so that $x^4 = \frac{n^2u^3}{v(nu-v)}$ and $y = \frac{v}{nu}x$. One can check that $F_{mt(n)}(x,y) = (u,v)$.

(b) Suppose $F_{mt(n)}(x,y) = (x,y)$. If $x = 0$, then $y = 0$ and vice versa. If x and y are non-zero, then from the first equation we get $xy(x-y) = 1$, after which from the second equation we get $n = 1$. If $p \nmid n-1$, this is impossible; if $p|n-1$, it is true, which implies the result.

(c) For $p|n$ two iterations are enough to send everything to $(0,0)$. Modulo any prime $p \nmid n$, if $x \neq 0$ and $\frac{y}{x} \neq 1$, then $\frac{u}{v} = n\frac{y}{x}$. If n is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$, then iterations of this map eventually send everything to $(0,0)$. Otherwise, if $\frac{y}{x}$ is not a power of n, then no iteration will send (x,y) to $(0,0)$. $\square$

Example 5. (Power Trap) Suppose $n \geq 2$ is a natural number. Define $F_{pt(n)}(x,y) = (u,v)$, where

$$(u,v) = (x^{n+1}y(x-y), xy^{n+1}(x-y)).$$

Theorem 6. *(a) $F_{pt(n)}$ and its reductions modulo p for all primes p are dominant.*

(b) For a prime p the following two statements are equivalent.

1. *$(p-1)|n^k$ for some k.*
2. *For every $(x,y) \in \mathbb{F}_p^2$, some multiple of the reduction of $F_{pt(n)}$ modulo p sends it to $(0,0)$.*

Proof. (a) For generic u and v, take t such that $t^n = \frac{v}{u}$. Then take x such that $x^{n+3} = \frac{u}{t-t^2}$ and $y = tx$. One can check that $F_{pt(n)}(x, y) = (u, v)$.

(b) Modulo any prime p if $x \neq 0$ and $\frac{y}{x} \neq 1$, then $\frac{u}{v} = (\frac{y}{x})^n$. If $(p-1)|n^k$ for some k, then $k+1$ iterations of this map send everything to $(0, 0)$. For general p a high enough iteration of $F_{pt(n)}$ sends to $(0, 0)$ all pairs (x, y) such that at least one of the coordinates is zero or the order of $\frac{y}{x}$ in $(\mathbb{Z}/p\mathbb{Z})^*$ divides n^k for some k. □

These examples inspire the following definition.

Definition 7. Suppose F is an integer polynomial map. Then its *nilpotency locus* $\mathrm{Nil}(F)$ is the set of all primes p such that some iteration of F is constant on $\mathbb{Z}/p\mathbb{Z}$. We denote by $\mathcal{NIL}$ the set of all subsets of the set of primes that can be realized as a nilpotency locus for some integer polynomial map F.

Theorem 8. *Suppose $S_1 \in \mathcal{NIL}$ and $S_2 \in \mathcal{NIL}$. Then $S_1 \cap S_2 \in \mathcal{NIL}$.*

Proof. Suppose $S_1 = \mathrm{Nil}(F_1)$ and $S_2 = \mathrm{Nil}(F_2)$, where F_1 has n variables and F_2 has m variables. Consider the direct sum of F_1 and F_2, which is the polynomial map on $(n+m)$ variables defined as follows:

$$(F_1 \oplus F_2)(x_1, ..., x_n; x_{n+1}, ..., x_{n+m}) = (F_1(x_1, ..., x_n); F_2(x_{n+1}, ..., x_{n+m}))$$

Clearly, $\mathrm{Nil}(F_1 \oplus F_2) = S_1 \cap S_2$. □

The definition of the nilpotency locus admits an interesting variation.

Definition 9. Suppose F is an integer polynomial map. Then its *zero nilpotency locus* $\mathrm{Nil}_0(F)$ is the set of all primes p such that some iteration of F is the constant 0 on $\mathbb{Z}/p\mathbb{Z}$. We denote by $\mathcal{NIL}_0$ the set of all subsets of the set of primes that can be realized as a nilpotency locus for some integer polynomial map F.

It is unclear if $\mathcal{NIL}_0 = \mathcal{NIL}$. In fact, it is possible that neither $\mathcal{NIL}_0 \subseteq \mathcal{NIL}$ nor $\mathcal{NIL} \subseteq \mathcal{NIL}_0$. A construction similar to the theorem above shows that $\mathcal{NIL}_0$ is also closed under finite intersections.

3 Open Questions and Conjectures

Obviously, with more variables one can create more complicated maps. However, it is unclear how much can be actually "programmed" using integer polynomial maps. The following question is very natural in this regard.

Question 10. Does there exist an integer polynomial map with two different fixed points such that modulo every prime its sufficiently high iteration will send any initial point to one of the fixed points, depending on whether or not the initial first coordinate is zero?

Another interesting question is related to the notion of the nilpotency locus.

Question 11. Which subsets of the set of all primes can be realized as a nilpotency locus of some F?

Note that the nilpotency locus of $F_{mt(n)}$ is the set of all primes p for which n is a generator modulo p, which is a very tricky arithmetic condition. The nilpotency locus of $F_{pt(2)}$ is the set of the Fermat primes, so we don't even know if it is finite or infinite. Definitely, not all subsets of the set of all primes are in $\mathcal{NIL}$, because there are uncountably many of them and only countably many integer polynomial maps.

It would also be very interesting to study "random" polynomial maps, and their dynamical properties on the finite sets of points over $\mathbb{F}_p$. The following quantities are of particular interest: the size of the intersection of the images of all iterations, the length of the longest cycle, the length of the shortest cycle, the number of cycles, and the distribution of lengths of the cycles. At this time, it is absolutely unclear what to expect in general, so one should do some computer experiments to formulate any conjectures in this direction. Some results of this kind are contained in a very recent paper by Benedetto, Ghioca, Hutz, Kurlberg, Scanlon, and Tucker [2].

4 Acknowledgments

We thank Mark Sapir for helpful suggestions and encouragement. We thank Jeffrey Shallit for many references and comments that greatly improved the paper.

References

[1] R. L. Benedetto, Components and periodic points in non-Archimedean dynamics, *Proc. London Math. Soc. (3)* **84** (2002), 231–256.

[2] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, and T. J. Tucker, Periods of rational maps modulo primes, *Math. Ann.* **355** (2013), 637–660.

[3] A. Borisov and M. Sapir, Polynomial maps over finite fields and residual finiteness of mapping tori of group endomorphisms, *Invent. Math.* **160** (2005), 341–356.

[4] A. Borisov and M. Sapir, Polynomial maps over p-adics and residual properties of mapping tori of group endomorphisms, *Int. Math. Res. Notices*, (2009), 3002–3015.

[5] G. Call and J. Silverman, Canonical heights on varieties with morphisms, *Compositio Math.* **89** (1993), 163–205.

[6] G. Chassé, Combinatorial cycles of a polynomial map over a commutative field, *Discrete Math.* **61** (1986), 21–26.

[7] W.-S. Chou and I. Shparlinski, On the cycle structure of repeated exponentiation modulo a prime, *J. Number Theory* **107** (2004), 345–356.

[8] N. Fakhruddin, Questions on self maps of algebraic varieties, *J. Ramanujan Math. Soc.* **18** (2003), 109–122.

[9] A. Khrennikov and M. Nilsson, On the number of cycles of p-adic dynamical systems, *J. Number Theory* **90** (2001), 255–264.

[10] M. Sha, On the cycle structure of repeated exponentiation modulo a prime power, *Fibonacci Quart.* **49** (2011), 340–347.

[11] J. Silverman, *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, vol. 241, Springer, 2007.

[12] T. Vasiga and J. Shallit, On the iteration of certain quadratic maps over GF(p). *Discrete Math.* **277** (2004), 219–240.

2010 *Mathematics Subject Classification*: Primary 37P05; Secondary 37P25, 37P35, 11A07.
Keywords: polynomial map, reduction, iteration.

Received May 4 2013; revised version received August 4 2013; September 1 2013. Published in *Journal of Integer Sequences*, October 12 2013.

Return to Journal of Integer Sequences home page.