# Number Theory and Dynamical Systems

Joseph H. Silverman

Brown University

MAA Invited Paper Session on the Beauty and Power of Number Theory
AMS–MAA Joint Math Meeting, Boston, 2012

Thursday January 5, 10:30–11:00am

## What Is Dynamics?

A **(Discrete) Dynamical System** is simply a map

$$\phi : S \longrightarrow S$$

from a set to itself. Dynamics is the study of the behavior of the points in $S$ under iteration of the map $\phi$.
We write

$$\phi^n = \underbrace{\phi \circ \phi \circ \phi \cdots \phi}_{n \text{ iterations}}$$

for the $n^{\text{th}}$ iterate of $\phi$ and

$$\mathcal{O}_\phi(\alpha) = \{\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \dots\}$$

for the **(forward) orbit of** $\alpha \in S$.

A primary goal in the study of dynamics is to classify the points of $S$ according to the behavior of their orbits.

# A Finite Field Example of a Dynamical System

Consider the iterates of the polynomial map $\phi$

$$\phi(z) = z^2 - 1$$

acting on the set of integers

$$\{0, 1, 2, \ldots, 10\} \text{ modulo } 11.$$

So for example

$$\phi(3) = 8 \quad \text{and} \quad \phi^2(3) = \phi(8) = 63 = 8 \text{ modulo } 11.$$

We can describe this dynamical system by drawing an arrow connecting each point to its image. Thus

$$\begin{tikzcd} 1 \arrow[r] & 0 \arrow[r, shift left] & 10 \arrow[l, shift left] \end{tikzcd} \qquad \begin{tikzcd} 5 \arrow[dr] & & & \\ & 2 \arrow[r] & 3 \arrow[r] & 8 \arrow[loop right] \\ 6 \arrow[ur] & 9 \arrow[ur] & & \end{tikzcd} \qquad \begin{tikzcd} 7 \arrow[r] & 4 \arrow[loop right] \end{tikzcd}$$

## Polynomials and Rational Maps

Classical dynamical systems studies how the iterates of polynomial maps such as

$$\phi(z) = z^2 + c$$

act on the real numbers $\mathbb{R}$ or the complex numbers $\mathbb{C}$.

More generally, people often study the dynamics of ratios of polynomials, although now we have to allow $\infty$ as a possible value.

A *rational function* is a ratio of polynomials

$$\phi(z) = \frac{F(z)}{G(z)} = \frac{a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0}{b_e z^e + b_{e-1} z^{e-1} + \cdots + b_1 z + b_0}$$

The *degree of* $\phi$ is the larger of $d$ and $e$. From now on, we will assume that $\boxed{\deg(\phi) \geq 2}$.

## Some Dynamical Terminology

A point $\alpha$ is called **periodic** if

$$\phi^n(\alpha) = \alpha \quad \text{for some } n \geq 1.$$

The smallest such $n$ is called the **period of** $\alpha$.

If $\phi(\alpha) = \alpha$, then $\alpha$ is a **fixed point**.

A point $\alpha$ is **preperiodic** if some iterate $\phi^i(\alpha)$ is periodic, or equivalently, if its orbit $\mathcal{O}_\phi(\alpha)$ is finite.

A **wandering point** is a point whose orbit is infinite.

---

## An Example: The Map $\phi(z) = z^2$

- 2 and $\frac{1}{2}$ are *wandering points*.
- 0 and 1 are *fixed points*.
- $-1$ is a *preperiodic* point that is not periodic.
- $\frac{-1+\sqrt{-3}}{2}$ is a periodic point of period 2.

# A Number Theorist's View of Periodic Points

## Periodic Points and Number Theory

For a dynamicist, the periodic points of $\phi$ are the (complex) numbers satisfying an equation

$$\phi^n(z) = z \quad \text{for some } n = 1, 2, 3, \ldots.$$

A number theorist asks:

**What sorts of numbers may appear as periodic points?**

For example:

**Question.** Is it possible for a periodic point to be a rational number?

The answer is obviously

**Yes.**

We've seen several examples. This leads to the...

## Periodic Points and Number Theory

**Question.** How many periodic points can be rational numbers?

This is a more interesting question. There are always infinitely many complex periodic points, and in many cases there are infinitely many real periodic points.

**But among the infinitely many periodic points, how many of them can be rational numbers?**

The answer is given by a famous theorem:

**Theorem.** (Northcott 1949) A rational function $\phi(z) \in \mathbb{Q}(z)$ has only finitely many periodic points that are rational numbers.

## Proof (Skecth) of Northcott's Theorem

**Proof.** Every math talk should have one proof, so I'll sketch the (fairly elementary) proof of Northcott's result. An important tool in the proof is the **height** of a rational number $p/q$:

$$H\left(\frac{p}{q}\right) = \max\bigl\{|p|, |q|\bigr\}.$$

Notice that for any constant $B$, there are only finitely many rational numbers $\alpha \in \mathbb{Q}$ with height $H(\alpha) \le B$.

**Lemma.** If $\phi(z)$ has degree $d$, then there is a constant $C = C_\phi > 0$ so that for all rational numbers $\beta \in \mathbb{Q}$,

$$H\bigl(\phi(\beta)\bigr) \ge C \cdot H(\beta)^d.$$

This is intuitively reasonable if you write out $\phi(z)$ as a ratio of polynomials. The tricky part is making sure there's not too much cancellation.

## Proof (Sketch) of Northcott's Theorem

Suppose that $\alpha$ is periodic, say $\phi^n(\alpha) = \alpha$. We apply the lemma repeatedly:

$$\begin{aligned}
H\bigl(\phi(\alpha)\bigr) & & &\ge C \cdot H(\alpha)^d \\
H\bigl(\phi^2(\alpha)\bigr) &\ge C \cdot H\bigl(\phi(\alpha)\bigr)^d & &\ge C^{1+d} \cdot H(\alpha)^{d^2} \\
H\bigl(\phi^3(\alpha)\bigr) &\ge C \cdot H\bigl(\phi^2(\alpha)\bigr)^d & &\ge C^{1+d+d^2} \cdot H(\alpha)^{d^3} \\
&\vdots & &\vdots \\
H\bigl(\phi^n(\alpha)\bigr) &\ge C \cdot H\bigl(\phi^{n-1}(\alpha)\bigr)^d & &\ge C^{1+d+\cdots+d^{n-1}} \cdot H(\alpha)^{d^n}
\end{aligned}$$

But $\phi^n(\alpha) = \alpha$, so we get

$$H(\alpha) = H\bigl(\phi^n(\alpha)\bigr) \ge C^{(d^n-1)/(d-1)} H(\alpha)^{d^n}.$$

Then a little bit of algebra yields

$$H(\alpha) \le C^{-1/(d-1)}.$$

This proves that the rational periodic points have bounded height, hence there are only finitely many of them. QED

## Rational Periodic Points

All right, we now know that $\phi(z)$ has only finitely many rational periodic points. This raises the question:

**How many rational periodic points can $\phi(z)$ have?**

If we don't restrict the degree of $\phi$, then we can get as many as we want. Simply take $\phi$ to have large degree and set

$$\phi(0) = 1, \quad \phi(1) = 2, \quad \phi(2) = 3, \quad \ldots, \quad \phi(n-1) = 0.$$

This leads to a system of $n$ linear equations for the coefficients of $\phi$ in the coefficients of $\phi$, so if $\deg(\phi) > n$, we can solve for the coefficients of $\phi$.

## A Uniformity Conjecture

Hence in order to pose an interesting question, we should restrict attention to rational functions of a fixed degree.

**Uniform Boundedness Conjecture for Rational Periodic Points.** (Morton–Silverman) Fix an integer $d \geq 2$. Then there is a constant $P(d)$ so that every rational function $\phi(z) \in \mathbb{Q}(z)$ of degree $d$ has at most $P(d)$ rational periodic points.

## Rational Periodic Points of $\phi_c(z) = z^2 + c$

Even for very simple families of polynomials such as

$$\phi_c(z) = z^2 + c,$$

very little is known about the possible periods of rational periodic points.

We can write down some examples:

$$\begin{array}{ll} \phi(z) = z^2 & \text{has } 1 \text{ as a point of period } 1, \\ \phi(z) = z^2 - 1 & \text{has } -1 \text{ as a point of period } 2, \\ \phi(z) = z^2 - \frac{29}{16} & \text{has } -\frac{1}{4} \text{ as a point of period } 3. \end{array}$$

**Can $\phi(z) = z^2 + c$ have a rational point of period 4?**

## Rational Periodic Points of $\phi_c(z) = z^2 + c$

**Theorem.**
(a) (Morton) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 4.
(b) (Flynn, Poonen, Schaefer) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 5.
(c) (Stoll 2008) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 6 (provided that the Birch–Swinnerton-Dyer conjecture is true).

And that is the current state of our knowledge! No one knows if $\phi_c(z)$ can have rational periodic points of period 7 or greater. (Poonen has conjectured it cannot.)

# Integer Points in Orbits

## Integers and Wandering Points

At its most fundamental level, number theory is the study of the set of integers

$$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots.$$

The orbit of a rational number $\alpha$ consists of rational numbers, so it is natural to ask how often those rational numbers can be integers.

**Question.** Is it possible for an orbit $\mathcal{O}_\phi(\alpha)$ to contain infinitely many integers?

The obvious answer is **Yes**, of course it can. For example, take $\phi(z) = z^2 + 1$ and $\alpha = 1$.

More generally, if $\phi(z)$ is any polynomial with integer coefficients and if we start with an integer point, then the entire orbit consists of integers.

**Are there any other possibilities?**

## Rational Functions with Polynomial Iterate

Here is an example of a nonpolynomial with an orbit containing infinitely many integer points. Let

$$\phi(z) = \frac{1}{z^2} \quad \text{and let} \quad \alpha \in \mathbb{Z}.$$

Then

$$\mathcal{O}_\phi(\alpha) = \left\{ \alpha, \frac{1}{\alpha^2}, \alpha^4, \frac{1}{\alpha^8}, \alpha^{16}, \frac{1}{\alpha^{32}}, \alpha^{64}, \ldots \right\}.$$

Thus half the points in the orbit are integers.

This is not an unexpected phenomenon, since $\phi^2(z) = z^2$ is a polynomial. And in principle, the same thing happens if any higher iterate of $\phi$ is a polynomial, but surprisingly:

**Theorem.** If some iterate $\phi^n(z)$ is a polynomial, then already $\phi^2(z)$ is a polynomial.

## Integer Points in Orbits

Here is an example of a rational map of degree 2 with quite a few integer points in an orbit. Let

$$\phi(z) = \frac{221z^2 + 2637z - 5150}{433z^2 - 603z - 1030}.$$

Then the orbit of 0 contains (at least) 7 integer points:

$$0 \to 5 \to 2 \to -2 \to -5 \to -1 \\ \to -1261 \to \frac{58014389}{114880291} \to \cdots.$$

However, if we rule out the examples coming from polynomials, then:

**Theorem.** (JS) Assume that $\phi^2(z)$ is not a polynomial. Then

$$\mathcal{O}_\phi(\alpha) \cap \mathbb{Z} \text{ is finite.}$$

## Integer-Like Points in Wandering Orbits

There is a stronger, and more striking, description of the extent to which orbiting points fail to be integral.

Start with some $\alpha \in \mathbb{Q}$ and write the points in its orbit as fractions,

$$\phi^n(\alpha) = \frac{A_n}{B_n} \in \mathbb{Q} \qquad \text{for } n = 0, 1, 2, 3 \ldots.$$

Notice that $\phi^n(\alpha)$ is an integer if and only if $|B_n| = 1$. So the previous theorem says that $|B_n| \geq 2$ for most $n$.

**Theorem.** (JS) Assume that $\phi^2(z)$ is not a polynomial and that $1/\phi^2(z^{-1})$ is not a polynomial. Let $\alpha \in \mathbb{Q}$ be a point having infinite orbit. Then

$$\lim_{n\to\infty} \frac{\text{Number of digits in } A_n}{\text{Number of digits in } B_n} = 1.$$

## Integer-Like Points — An Example

We take the function

$$\phi(z) = \frac{z^2-1}{z} = z - \frac{1}{z} \qquad \text{and initial point } \alpha = 2.$$

$$\begin{aligned}
\phi(2) &= \frac{3}{2} \\
\phi^2(2) &= \frac{5}{6} \\
\phi^3(2) &= -\frac{11}{30} \\
\phi^4(2) &= \frac{779}{330} \\
\phi^5(2) &= \frac{497941}{257070} \\
\phi^6(2) &= \frac{181860254581}{128005692870} \\
\phi^7(2) &= \frac{16687694789137362648661}{23279147893155496537470} \\
\phi^8(2) &= -\frac{263439569256003706800705587722279993788907979}{388475314992168993748220639081347493631827670}
\end{aligned}$$

The numbers get very large. One can show that $A_n$ and $B_n$ have approximately $0.174 \cdot 2^n$ digits!

# Putting Number Theory and Dynamics into Context

## Arithmetic Dynamics

Arithmetic Dynamics refers to the study of number theoretic properties of dynamical systems inspired by classical theorems and conjectures in Arithmetic Geometry and the theory of Diophantine Equations.

- The Dynamical Uniform Boundedness Conjecture is inspired by boundedness theorems of Mazur, Kamienny, and Merel for torsion points on elliptic curves.
- Studying integer-like points in orbits is inspired by Siegel's theorem on integer-like points on affine curves, and its generalization to abelian varieties by Faltings.
- There is much current research on dynamical analogues of the Mordell–Lang conjecture (proven by Faltings) that attempt to describe when an orbit in $\mathbb{P}^N$ can be Zariski dense on a proper subvariety.
- There are dynamical modular curves and dynamical moduli spaces analogous to classical elliptic modular and moduli spaces of abelian varieties.

## $p$-adic Dynamics

A fundmental tool in number theory is reduction modulo $m$, which by the Chinese Remainder Theorem often reduces to working modulo prime powers. Fitting the prime powers together leads to the field of $p$-adic numbers $\mathbb{Q}_p$ with its strange absolute value $\|\cdot\|_p$ satisfying

$$\|\alpha+\beta\|_p \le \max\bigl\{\|\alpha\|_p,\ \|\beta\|_p\bigr\}.$$

***p*-adic** (or **Non-Archimedean**) **Dynamics** is the study of dynamical systems working with the field $\mathbb{Q}_p$, or its completed algebraic closure $\mathbb{C}_p$.

Many of the theorems and conjectures in $p$-adic dynamics are inspired by classical results in real and complex dynamics. However, there are some interesting differences. I will give two examples.

## $p$-adic Dynamics versus Complex Dynamics

The **Fatou set** $\mathcal{F}(\phi)$ of a map is the set of points where iteration is "well-behaved," while the **Julia set** $\mathcal{J}(\phi)$ is the set of points where iteration is "chaotic."

Classical results say that over $\mathbb{C}$, we always have $\mathcal{J}(\phi) \neq \emptyset$, but that it is possible to have $\mathcal{F}(\phi) = \emptyset$.

In the non-archimedean setting of $\mathbb{C}_p$, the results are reversed. We always have $\mathcal{F}(\phi) \neq \emptyset$, but it often happens that $\mathcal{J}(\phi) = \emptyset$!

A famous result of Sullivan says that the connected components of $\mathcal{F}(\phi)$ are all preperiodic, they never wander, but ...

Benedetto has shown that over $\mathbb{C}_p$, it is possible for $\mathcal{F}(\phi)$ to have wandering domains! The existence of wandering domains over $\mathbb{Q}_p$ is still an open problem.

I thank you for your attention
and
the organizers for inviting me to speak.

# Number Theory and Dynamical Systems

Joseph H. Silverman

Brown University

MAA Invited Paper Session on the Beauty and Power of Number Theory
AMS–MAA Joint Math Meeting, Boston, 2012

Thursday January 5, 10:30–11:00am