A GENTLE INTRODUCTION TO ARITHMETIC DYNAMICS

JIWU JANG

Abstract. We provide an introduction to the field of arithmetic dynamics. We start by defining fundamental terminology and notation from classical dynamics, including periodic points, wandering points, rational maps, power maps, Chebyshev polynomials, and Lattès maps. Together, we cover basic machinery from algebraic geometry, number theory, and p-adic analysis, including affine and projective space, ideals and varieties, and completions of $\mathbb{Q}$. Continuing the discussion, we discuss dynamics over global fields, ultimately leading to the proof of Northcott's theorem, involving Hilbert's Nullstellensatz. We then discuss pathways emerging from it, centered around the uniform boundedness conjecture.

> All the lonely objects, where do
> they all belong?
>
> *Joseph H. Silverman*

1. Introduction

As does any interesting journey start, we start with some motivation. There are types of mathematics that people like to study. Of course, there are just so many mathematical objects. What do people do with interesting objects? They prove theorems about those objects, sometimes with additional restrictions. Lots of great mathematics is done in that form, where people restrict their attention to a very small subset of objects, then prove cool properties that hold within those objects. But there are also great mathematics that aim to prove *general* properties that hold within *all* objects of that type. In that case, it makes natural sense to look at the family $\mathcal{F}$ of objects. For example, as we will introduce later, one looks at the set of all morphisms $\mathbb{P}^n \to \mathbb{P}^n$, and try to prove properties that hold as generally as possible, within those set of objects. But there is a trade-off: too much zooming out often leads to general, but pretty boring statements; these sets can be too large and unwieldy. In order to avoid this problem, we study better behaved subsets by adding restrictions. For instance, there are "too many" maps $\mathbb{P}^n \to \mathbb{P}^n$, so in dynamics, we restrict our attention to *finite* maps $\mathbb{P}^n \to \mathbb{P}^n$ of *fixed degree*.

In dynamics, we look at the *composition* of functions and their behavior. For example, consider the function $\phi(z) = z^2 + 1$ in the complex plane. Traditional complex dynamics asks the following questions: "What are the fixed points of ϕ, that is, points $z \in \mathbb{C} \cup \{\infty\}$ such that $\phi(z) = z$? How can we describe the local behavior near those fixed points? Can we classify periodic points, that is, which points $z \in \mathbb{C}$ satisfy $\phi^n(z) = \phi^{n+m}(z)$ for some $n, m \in \mathbb{N}$? Which points $z \in \mathbb{C}$ *repel* the points near them, that is, they move farther away from z as we iteratively apply ϕ? Which points *attract* other points?" These properties of the map ϕ, are often colloquially called the *dynamics* of ϕ. In order to study the dynamics of a map, we consider the orbit of α, which is the set

$$\mathcal{O}_\phi(\alpha) = \{\phi^n(\alpha) : n \geq 0\}$$

Date: December 10, 2023.

The principal goal of dynamics is to classify the points α in the set S, according to the behavior of their orbits $\mathcal{O}_\phi(\alpha)$. Within $\mathbb{C}$, this is much of what complex dynamics is devoted to, and if one wants to study in this direction, an excellent reference is [Mil06]. The topic of this paper, arithmetic dynamics, instead looks at the dynamics of mappings under an *arithmetic* setting, such as $\mathbb{Q}$, $\mathbb{Z}_p$, or $\mathbb{Q}_p$, as any number theorist would do, asking the same questions as above. However, the nonarchimedean nature of $\mathbb{Q}_p$ leads to interesting theories, worth pursuing by itself. We will reach some of the deepest conjectures and results of interest, but just as how good theories are developed, we start with the basics.

2. The Basics

First, we define some commonly used notation, and give some basic definitions. Throughout this paper, we use the standard symbols

$$\mathbb{N},\ \mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{F}_q,\ \mathbb{Z}_p,\ \mathbb{A}^N,\ \mathbb{P}^N$$

to represent the natural numbers, integers, rational numbers, real numbers, complex numbers, finite field with $q = p^k$ elements, ring of p-adic integers, N-dimensional affine space, and N-dimensional projective space, respectively. We do not count 0 as a natural number. Moreover, we utilize the notation S^* to denote the set S without zero. For instance, $\mathbb{Q}^*$ is just $\mathbb{Q} \setminus \{0\}$, and $(\mathbb{Z}/p\mathbb{Z})^*$ is the set of integers modulo p without zero. Sometimes, we may also write $(\mathbb{Z}/p\mathbb{Z})^\times$ for the same set, but this time, to signify the underlying multiplicative group structure of $(\mathbb{Z}/p\mathbb{Z})^*$. Some of the following definitions are adapted from [Sil07], a standard reference for arithmetic dynamics. In dynamics, we mostly work with projective spaces (since they have various nice properties), so let's first define it.

Definition 2.1. Given a vector space V over a field K, the *projective space* $\mathbb{P}(V)$ is the set of equivalence classes of $V^* = V \setminus \{0\}$ with equivalence under scaling, that is, $\mathbb{P}(V) = V^*/\sim$ where $\sim$ is an equivalence relation such that $x \sim y$ iff $x = \lambda y$ for some nonzero λ.

If V is a topological vector space (TVS), the quotient space $\mathbb{P}(V)$ is also a TVS, equipped with the quotient topology of the subspace topology of V^*. For example, this is certainly the case when $K = \mathbb{R}$ or $K = \mathbb{C}$.

Exercise 2.2. Prove that if $\dim V < \infty$, then $\dim \mathbb{P}(V) = \dim(V) - 1$.

Indeed, with the above result, when $V = K^{n+1}$, we may also write $\mathbb{P}(V)$ as $\mathbb{P}^n(K) = K\mathbb{P}^n = \mathbb{P}^n K$. (For example, $\mathbb{CP}^1$ denotes the complex projective line, and $\mathbb{RP}^2$ denotes the real projective plane. The complex projective line $\mathbb{CP}^1$ is also known as the Riemann sphere, since $\mathbb{P}^1(\mathbb{C}) \cong S^2$.)

We also deal with affine spaces, which are Euclidean spaces without a fixed origin (that has "forgotten" its origin). To be precise, they are defined as follows.

Definition 2.3. Given a vector space V over a field K, whose underlying set is A, the *affine space* $\mathbb{A}(V)$ is the pair (A, V), that is, a set A together with a vector space V, and a transitive and free action of the additive group of V on the set A.

The elements of the affine space $\mathbb{A}(V)$ are called *points*, and the vector space V is said to be *associated* to the affine space. As with projective spaces, if $V = K^n$, we equivalently write $\mathbb{A}(V)$ as $\mathbb{A}^n(K) = K\mathbb{A}^n = \mathbb{A}^n K$.

Remark 2.4. *Note that affine spaces are contained in projective spaces. For instance, one may obtain an affine place from a projective plane by removing a single line; conversely, any affine plane has an extension to a projective plane, namely by adding a line at infinity.*

Now, we move on to rational functions, which are the main objects of interest in both classical and arithmetic dynamics.

Definition 2.5. A *rational function* $\phi(z) \in \mathbb{C}(z)$ is a quotient of polynomials

$$\phi(z) = \frac{F(z)}{G(z)} = \frac{a_0 + a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

with no common factors; the *degree* of ϕ, denoted by $\deg \phi$, is $\max\{\deg F, \deg G\}$.

Definition 2.6. A *rational map of degree* d between projective spaces is a map $\phi : \mathbb{P}^N \to \mathbb{P}^M$ such that

$$\phi(P) = [f_0(P), \ldots, f_M(P)]$$

where $f_0, \ldots, f_M \in \bar{K}[X_0, \ldots, X_N]$ are fully reduced homogeneous polynomials of degree d.

Note that ϕ is defined at P if at least one of the values $f_0(P), \ldots, f_M(P)$ is nonzero, since 0 doesn't make sense in projective space.

Definition 2.7. A *rational morphism* ϕ is a rational map that is defined at every point of $\mathbb{P}^N(\bar{K})$, that is, a rational map with $\phi^{-1}(0) = \{0\}$. If the polynomials $f_0, \ldots, f_N$ have coefficients in K, we say that ϕ *is defined over* K.

Note that a rational function of degree d naturally induces a rational map of the complex projective line $\mathbb{P}^1(\mathbb{C})$, which is just the evaluation map.

Remark 2.8. *In dynamics, we generally consider maps with* $\deg \phi \geq 2$*, since degree one maps are just Möbius transformations* $\phi(z) = \frac{az+b}{cz+d} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{C})$*, i.e., automorphisms of* $\mathbb{P}^1$*, whose behaviors are very well-studied. They can be further classified into four types with respect to the trace* $\operatorname{tr} \phi = a + d$ *(given that we rescale the numerator and the denominator so that* $\det \phi = ad - bc = 1$*): parabolic, elliptic, hyperbolic, and loxodromic. Conversely, the behaviors of maps* ϕ *with* $\deg \phi \geq 2$ *are very rich, which is why we are mostly interested in the* $\deg \phi \geq 2$ *case.*

Two very important properties of rational maps are that they are continuous and open, that is, they preserve open sets.

Exercise 2.9. Prove that a rational map is continuous and open, with a rigorous $\varepsilon - \delta$ argument. (Recall that a function $f : X \to Y$ is an *open map* if it maps open sets to open sets, that is, for all U open, $f(U)$ is also open. Conversely, a function is *continuous* if the preimage of an open set is open, that is, for all V open, $f^{-1}(V)$ is also open.)

In order to study the arithmetic properties of points in projective space, we must have a good notion of "size" for the points, so that we can measure the arithmetical complexity of a point via its size. Similar to how we defined the degree of a rational function as the maximum of the degrees of the numerator and the denominator, provided that both the numerator and the denominator are fully reduced, we define the size (called the "height") of a point as follows:

Definition 2.10. The *height* of a point $P \in \mathbb{P}^N(K)$, denoted as $H(P)$, is defined as

$$H(P) := \max_{i \in [\![0,N]\!]} |x_i|$$

where $P = [x_0, x_1, \ldots, x_N]$ is homogenized with $\gcd_{i \in [\![0,N]\!]}(x_i) = 1$ and $x_i \in \mathbb{Z}$, that is, fully reduced with no common factors.

In algebraic geometry and dynamics, we typically work with commutative rings, so all rings R are assumed to be commutative unless specified otherwise.

Definition 2.11. For a ring R, a subset $I \subset R$ is called an *ideal* of R if it is an additive subgroup of R that "absorbs" multiplication by the elements of R, that is, for every $r \in R$ and every $x \in I$, we have $rx = xr \in I$.

Note that an ideal does not necessarily have to be generated by a single element. Now, it is helpful to talk about various types of ideals that have properties analogous to numbers.

Definition 2.12. For a ring R, an ideal $P \subsetneq R$ is *prime* if $ab \in P$ implies $a \in P$ or $b \in P$.

Note that this definition is an extension of the typical Euclid's lemma: p is prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$. This has an ideal analogue: $ab \in (p)$ implies $a \in (p)$ or $b \in (p)$. Indeed, from this, one can immediately see that all ideals of prime numbers are prime ideals, specifically principal prime ideals. A *principal ideal* is simply an ideal generated by a single element.

What about the notion of irreducibility? It is a slightly broader notion that captures prime ideals, but there are other types of ideals that are irreducible but not prime.

Definition 2.13. For a ring R, an ideal $I \subsetneq R$ is *irreducible* if $\nexists J, K \supsetneq I$ such that $I = J \cap K$, that is, it cannot be written as the intersection of two strictly larger ideals.

Exercise 2.14. Prove that all prime ideals are irreducible, and provide a counterexample for the reverse implication, that is, find an irreducible ideal that is not prime.

Remark 2.15. *Indeed, this notion is in correspondence with the spirit of the distinction between irreducible numbers and prime numbers when discussing non-UFDs such as* $\mathbb{Z}[\sqrt{-5}]$. *In a UFD, all irreducibles are prime, so the notion of prime and irreducible coincide. (The other implication, that is, all primes are irreducible, only requires* R *to be an integral domain.)*

Next, we provide some machinery needed to state the Nullstellensatz, which means, in German, "the zero-locus theorem." First, we need the definition of the *radical* of an ideal.

Definition 2.16. In a ring R, the *radical* of an ideal I, denoted by $\operatorname{rad}(I)$ or $\sqrt{I}$, is defined as

$$\sqrt{I} = \{r \in R : r^n \in I \text{ for some } n \in \mathbb{N}\}$$

Indeed, in algebraic geometry, it is much more convenient to deal with homogeneous polynomials, and in the same virtue, homogeneous ideals, since they can be scaled, and work more naturally in a projective setting.

Definition 2.17. For a ring R, an ideal $I \subset K[X_0, \dots, X_N]$ is *homogeneous* if I is generated by homogeneous polynomials.

Moreover, we define the concept of an *algebraic variety.* As usual, we have the affine case and the projective case; as such, we have affine varieties as well as projective varieties. First, the affine case:

Definition 2.18. For a field K and $S \subset \bar{K}[x_1, \dots, x_n]$ (we consider the algebraic closure $\bar{K}$ to capture all zeros of the polynomial), define the *zero-locus* $Z(S)$ to be the set of points in $\mathbb{A}^N$ on which the functions in S simultaneously vanish, that is,

$$Z(S) = \left\{x \in \mathbb{A}^N : f(x) = 0 \text{ for all } f \in S\right\}$$

A subset $V \subset \mathbb{A}^N$ is called an *affine algebraic set* if $V = Z(S)$ for some S. If the ideal generated by elements of S is prime, then V is called an *affine variety.* In that case, we write $V = V(I)$ for the ideal $I = (S)$ generated by elements of S.

Analogously, we define a projective variety as follows:

Definition 2.19. For a field K and $S \subset \bar{K}[X_0, X_1, \dots, X_n]$, define the *zero-locus* $Z(S)$ to be the set of points in $\mathbb{P}^N$ on which the functions in S simultaneously vanish, that is,

$$Z(S) = \left\{x \in \mathbb{P}^N : f(x) = 0 \text{ for all } f \in S\right\}$$

A subset $V \subset \mathbb{P}^N$ is called a *projective algebraic set* if $V = Z(S)$ for some S. If the ideal generated by elements of S is prime, then V is called a *projective variety.* In that case, we write $V = V(I)$ for the ideal $I = (S)$ generated by elements of S.

In dynamics, there are several common maps that arise from the study of commuting rational functions. What are commuting rational functions? We say f commutes with g if $f = \Theta^{-1} \circ g \circ \Theta$ for some "nice" map Θ (for an actual, rigorous definition, read [Mil04]). Usually, we take the domain to be a quotient of the complex plane by a lattice Λ, that is, $\mathbb{C}/\Lambda$, with some points on the boundary, which are called the *exceptional points.* The goal of studying commuting rational functions is to, well, study which rational functions commute, and it is known that commuting rational functions can be classified into the following trichotomy: power maps, Chebyshev polynomials, and Lattès maps. The criterion for classification of these maps is by the rank of the lattice Λ; the first two maps have $\operatorname{rank}\Lambda = 1$, and the second one has $\operatorname{rank}\Lambda = 2$.

First, the d^{th} power map is just a function $\phi(z) = z^d$ with $d \in \mathbb{N}$. Note that $\phi^n(z) = z^{d^n}$. Moreover, ϕ^n and ϕ^m commute. In some sense, power maps show behavior that is relatively trivial to analyze, compared to generic rational functions.

Next, we have Chebyshev polynomials, which could be seen as the first nontrivial examples of commuting rational functions (depending on the perspective, the behavior or construction of Chebyshev polynomials could be trivial as well, only leaving Lattès maps as having interesting, nontrivial properties). Actually, there are two kinds of Chebyshev polynomials: Chebyshev polynomials of the first kind (denoted as T_n), and Chebyshev polynomials of the second kind (denoted as U_n). They are closely related, as both arise from the trigonometric multiple angles construction. Intuitively, when one expands $\sin(n\theta)$, one obtains an expression of the form $\sin\theta \cdot f(\cos\theta)$ where f is a polynomial, and Chebyshev polynomials of the second kind are exactly derived from such. In this paper, we only consider Chebyshev polynomials of the first kind, that is, the unique polynomial satisfying $T_n(\frac{z+z^{-1}}{2}) = \frac{z^n+z^{-n}}{2}$. Noting that $\cos z = \frac{e^{iz}+e^{-iz}}{2}$, we see that $T_n(\cos\theta) = \cos n\theta$. Such a trigonometric interpretation directly implies that Chebyshev polynomials commute, that is, $T_n(T_m(z)) = T_m(T_n(z))$. Sometimes, in dynamics, one rather considers the closely related polynomial $C_n(z) = 2T_n(\frac{x}{2})$ for convenient reasons, since $C_n(z + z^{-1}) = z^n + z^{-n}$. The polynomials C_n are called the *Vieta-Lucas* polynomials [Hor02].

Finally, Lattès maps are defined as follows: the map $f = \Theta^{-1} \circ L \circ \Theta$ is said to be a *Lattès map*, if $\operatorname{rank}\Lambda = 2$ (whence the quotient $\mathcal{T} = \mathbb{C}/\Lambda$ is a torus), L is an affine automorphism of the torus, and $\Theta : \mathcal{T} \to \hat{\mathbb{C}}$ is holomorphic. These maps exhibit the most interesting behaviors, and there is extensive literature on the behavior of Lattès maps alone; they are crucial to the theory of commuting rational functions. For deeper reference on Lattès maps and their rather varied behavior, consult [Mil04], which provides an excellent exposition to Lattès maps and their dynamical behavior.

Now, the time has come for us to define a dynamical system, which is the central object of study in dynamics.

Definition 2.20. A *dynamical system* consists of a set S and a function $\phi : S \to S$, where we consider the iteration of ϕ:

$$\phi^n = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_{n \text{ times}} = n^{\text{th}} \text{ iterate of } \phi$$

for $n \in \mathbb{N}$ with ϕ^0 being the identity map on S.

Indeed, as previously noted, we look at the orbit of points.

Definition 2.21. For a given point $\alpha \in S$, the *orbit* of α is the set

$$\mathcal{O}_\phi(\alpha) = \{\phi^n(\alpha) : n \geq 0\}$$

We call a point α to be *periodic* if $\phi^n(\alpha) = \alpha$ for some $n \geq 1$. Moreover, the smallest such n is called the *exact period* of α. We also call a point α to be *preperiodic* if some iterate $\phi^m(\alpha)$ is periodic. Indeed, the set of periodic points of ϕ in S are denoted by

$$\mathrm{Per}(\phi, S) = \{\alpha \in S : \phi^n(\alpha) = \alpha \text{ for some } n \geq 1\}$$

and the set of preperiodic points of ϕ in S are denoted by

$$\mathrm{PrePer}(\phi, S) = \left\{\alpha \in S : \phi^{m+n}(\alpha) = \phi^m(\alpha) \text{ for some } n \geq 1, m \geq 0\right\}$$

which is the set of $\alpha \in S$ such that $\mathcal{O}_\phi(\alpha)$ is finite. For convenience, if the base set S is fixed, we just write $\mathrm{Per}(\phi)$ and $\mathrm{PrePer}(\phi)$.

Indeed, it makes sense to look at points of period n and exact period n:

Definition 2.22. The set of periodic points of ϕ with period n are denoted by

$$\mathrm{Per}_n(\phi) = \left\{\alpha \in \mathbb{P}^1(\mathbb{C}) : \phi^n(\alpha) = \alpha\right\}$$

Moreover, the set of periodic points of ϕ with exact period n are denoted by

$$\mathrm{Per}_n^{**}(\phi) = \{\alpha \in \mathrm{Per}_n(\phi) : \alpha \text{ has exact period } n\}$$

The reason for this weird $\mathrm{Per}_n^{**}(\phi)$ notation is that we also have $\mathrm{Per}_n^*(\phi)$, which is the set of points with *formal period n*. The consideration for formal periods comes from Galois theory, more specifically, the theory of cyclotomic polynomials, where the roots of a cyclotomic polynomial are said to be algebraically indistinguisable. Indeed, it makes sense to consider the following dynamic analogue of a cyclotomic polynomial:

$$\Phi_n^*(z) = \prod_{m|n} (\phi^m(z) - z)^{\mu(n/m)}$$

where μ is the Möbius function. The product makes sense because we are essentially performing PIE to quotient out all the smaller factors, and only leave the highest factor. Then, the roots of $\Phi_n^*(z)$ are said to have *formal period n*. The roots of $\Phi_n^*(z)$ behave in many ways as if they have exact period n, although their actual period is smaller than n.

Exercise 2.23. Prove that $\Phi_n^*(z)$ is well-defined, that is, $\phi^m(z) - z \mid \phi^n(z) - z$ whenever $m \mid n$ and $\Phi_n^*(z)$ is a polynomial.

Exercise 2.24. Prove that

$$\text{exact period } n \implies \text{formal period } n \implies \text{period } n$$

and that the reverse implication does not hold, that is, find a counterexample for each reverse implication.

In the spirit of discussing heights of points, we need the notion of an absolute value, which assists in the notion of how "large" a point is. This naturally leads to the discussion of local height functions and p-adic analysis on primes of bad reduction.

Definition 2.25. An *absolute value* on a field K is a map $|\cdot| : K \to \mathbb{R}$ with the following properties:

- $|\alpha| \geq 0$, and $|\alpha| = 0$ if and only if $\alpha = 0$.
- $|\alpha\beta| = |\alpha| \cdot |\beta|$ for all $\alpha, \beta \in K$.
- $|\alpha + \beta| \leq |\alpha| + |\beta|$ for all $\alpha, \beta \in K$ (triangle inequality).

In a p-adic setting, we have the *ultrametric* property, which allows us to give much stronger bounds for absolute values. This consequently admits various "rigid" theorems that are impossible in regular metrics such as in Euclidean space. But first, what is a p-adic number?

Definition 2.26. An absolute value is *nonarchimedean* (or *ultrametric*) if $|x + y| \leq \max\{|x|, |y|\}$ (strong triangle inequality), and called *archimedean* otherwise.

A *metric* on K is defined by a distance function $d : K \times K \to \mathbb{R}_{\geq 0}$. Note that an absolute value induces a metric defined by $d(x, y) = |x - y|$ for all $x, y \in K$.

Definition 2.27. A set on which a metric is defined is called a *metric space.* A set with a metric induced by a nonarchimedean absolute value is called an *ultrametric space.*

Now, we state some properties of absolute values, left as an exercise to the reader.

Exercise 2.28. Let K be an ultrametric space, and let $x, y \in K$. Show that if $|x| \neq |y|$, then $|x + y| = \max\{|x|, |y|\}$.

Exercise 2.29. Prove that if $x \in \mathbb{Q}$, we have $x = p^{v_p(x)} \frac{a}{b}$, where $p \nmid a, b$.

Exercise 2.30. Prove that for all $x, y \in \mathbb{Q}$, $v_p(xy) = v_p(x) + v_p(y)$.

Exercise 2.31. Prove that for all $x, y \in \mathbb{Q}$, $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

Definition 2.32. The *p-adic valuation* on $\mathbb{Q}$ is defined by a function $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$. Let $x \in \mathbb{Q}^*$. If $x \in \mathbb{Z}$, let $v_p(x)$ be the unique positive integer satisfying $x = p^{v_p(x)} x'$ where $p \nmid x'$ and $x' \in \mathbb{Z}$. Now, for $x \in \mathbb{Q}^*$, writing $x = \frac{a}{b}$ where $a, b \in \mathbb{Z}$, define $v_p(x) = v_p(a) - v_p(b)$. Finally, $v_p(0) = +\infty$.

Exercise 2.33. Prove that v_p is well-defined, that is, $v_p(x)$ stays the same regardless of the representation of $x = \frac{a}{b}$ with respect to a and b.

Definition 2.34. The *p-adic absolute value* $| \cdot |_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ is defined as

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

The p-adic absolute value induces the p-adic metric, denoted by d_p.

Exercise 2.35. Prove that the p-adic absolute value is a nonarchimedean absolute value on $\mathbb{Q}$.

Definition 2.36. Two absolute values $| \cdot |_1$ and $| \cdot |_2$ on K are said to be *equivalent*, if there is a constant $c > 0$ such that $|x|_2 = |x|_1^c$ for all $x \in K$.

Now, the following theorem of Ostrowski provides a clean classification of absolute values on $\mathbb{Q}$.

Theorem 2.37 (Ostrowski)**.** *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to either the standard absolute value $| \cdot |_\infty$ or one of the p-adic absolute values $| \cdot |_p$.*

Proof. For a proof of Ostrowski's theorem, see pages 56-59 of [Gou20]. □

Moreover, it is known that Ostrowski's theorem admits a natural extension to number fields, whose detailed study can be found in [Con07]. In order to understand the statement (not mentioning the proof), one needs to know a fair amount of algebraic number theory, so although the statement of the theorem is provided below, it is advised to the interested readers to consult an algebraic number theory textbook, such as [IR90].

Definition 2.38. For a number field K, we denote the ring of integers of K as $\mathcal{O}_K$, which is the ring of all algebraic integers contained in K.

Definition 2.39. For a number field K, a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ admits a $\mathfrak{p}$-adic valuation $v_{\mathfrak{p}}$ on K: for $x \in \mathcal{O}_K$, define $v_{\mathfrak{p}}(x) = n$, where n is the greatest integer such that $x \in \mathfrak{p}^n$, defining $\mathfrak{p}^0 = \mathcal{O}_K$. Then, for all $\alpha \in K$, writing $\alpha = \frac{a}{b}$ where $a, b \in \mathcal{O}_K$, define $v_{\mathfrak{p}}(\alpha) = v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b)$.

Theorem 2.40 (Ostrowski for number fields)**.** *Every nontrivial absolute value on K is equivalent to a $\mathfrak{p}$-adic, real, or complex absolute value, for some prime ideal $\mathfrak{p} \subset \mathcal{O}_K$.*

Thus, it makes sense to partition the set of absolute values M_K of a field K into M_K^0 and M_K^∞ and say that $v \in M_K^0$ must be of the form $v = v_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ whereas $v \in M_K^\infty$ must be a real or complex absolute value, where M_K^0 is the set of nonarchimedean valuations, and M_K^∞ is the set of archimedean valuations. This will be helpful later on when we consider all valuations simultaneously to calculate the global height.

Now, we can talk about completions of $\mathbb{Q}$, which will lead to the construction of $\mathbb{Q}_p$ from which $\mathbb{Z}_p$ can also be obtained. First, we will state a theorem on general completions of fields without proof, whose proof can be found in [Sto15]. The general idea is to consider all elements generated by limits of Cauchy sequences, just as how one would construct $\mathbb{R}$ from $\mathbb{Q}$ (instead of using Dedekind cuts).

Theorem 2.41. *Let K be a field with an absolute value $|\cdot|$. Then, there is a complete field $\bar{K}$ with an absolute value $|\cdot|'$ that extends from K, and $\bar{K}$ is unique up to isomorphism.*

With this, we define the field of p-adic numbers as the completion of $\mathbb{Q}$ with respect to the p-adic metric, denoted as $\mathbb{Q}_p$. By Ostrowski's theorem, we know that the only two completions of $\mathbb{Q}$ are $\mathbb{Q}_p$ and $\mathbb{R}$, up to isomorphism. Now, from $\mathbb{Q}_p$, one can define $\mathbb{Z}_p$ as the ring of integers of $\mathbb{Q}_p$, that is, $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. Note that $|x|_p \leq 1$ if and only if $v_p(x) \geq 0$, so this makes sense with the usual intuition of p-adic integers obtained via Hensel's lemma, that is, a number taken mod p, p^2, p^3, and so on, giving a p-ary number written from right to left.

Going back to dynamics, p-adic valuations will provide a useful ground for studying the local behavior of rational maps over a number field $K/\mathbb{Q}$. Now, with these notation and definitions, we are set to discuss some of the most important results in arithmetic dynamics.

3. Dynamics over Global Fields

Naturally, we want to know if the set of preperiodic points has bounded height, that is, with respect to the morphism ϕ, or the height will rather explode. A famous result of Northcott [Nor50] tells us that the set of preperiodic points indeed has bounded height.

Theorem 3.1 (Northcott's theorem)**.** *Let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over a number field K. Then, the set of preperiodic points* $\mathrm{PrePer}(\phi) \subset \mathbb{P}^N(\bar{K})$ *is a set of bounded height.*

Note that we look at the algebraic closure $\bar{K}$ instead of K for $\mathrm{PrePer}(\phi)$, since preperiodic points are solutions of $\phi^n(z) = \phi^m(z)$, whose solutions are all contained in $\bar{K}$ by definition of algebraic closure. This makes things much nicer, just as how $\mathbb{C}$ has elegantly beautiful theorems regarding zeros of univariate polynomials, compared to the toil and pathology of $\mathbb{R}$, for $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

In order to prove Northcott's theorem, we first need some preliminary results, some of which are cited without proof, since it suffices to only know the statement for our purposes.

Theorem 3.2 (Hilbert's Nullstellensatz)**.** *Let I and J be homogeneous ideals properly contained in $\bar{K}[X_0, \ldots, X_N]$, then*

$$V(I) = V(J) \iff \sqrt{I} = \sqrt{J}$$

Recall that $V(I)$ is the set of points that are killed by polynomials in I, and $\sqrt{I}$ is the ideal that contains all ideals whose k^{th} power is I for some $k \in \mathbb{N}$.

Proof. First, note that one direction is relatively trivial, that is, the $\sqrt{I} = \sqrt{J} \implies V(I) = V(J)$ direction, since for some point $P \in V(I)$ and $f \in J$, we have $f^n \in I$ for some $n \in \mathbb{N}$, so $f^n(P) = 0$, thus $f(P) = 0$, implying $P \in V(J)$. This implies that $V(I) \subset V(J)$, and vice versa. The other direction typically needs some techniques, and although there are some proofs that avoid it, this is beyond the scope of this paper, so we leave it to the interested reader to look up the proof. For reference, some often cited proofs are in [Art98] and [AM69]. □

For ease of notation, we define the following shorthand notations.

Definition 3.3. For $P = [x_0, x_1, \ldots, x_N] \in \mathbb{P}^N(K)$ and any absolute value $v \in M_K$, write the *absolute value of a point* to be

$$|P|_v = \max_i |x_i|_v$$

More generally, define *the absolute value of a polynomial*

$$f(X_0, \ldots, X_N) = \sum_{i_0, \ldots, i_N} a_{i_0 \ldots i_N} X_0^{i_0} \ldots X_N^{i_N}$$

to be

$$|f|_v = \max_{i_0, \ldots, i_N} |a_{i_0 \ldots i_N}|_v$$

Further, if $\phi = [f_0, \ldots, f_M]$ is a collection of polynomials, let $|\phi|_v = \max_j |f_j|_v$.

Note that the height of a point $P \in \mathbb{P}^N(K)$ can be written in the form

$$H(P) = \left(\prod_{v \in M_K} |P|_v^{n_v} \right)^{1/[K:\mathbb{Q}]}$$

We define the height of a polynomial f or a collection of polynomials ϕ similarly,

$$H(f) = \left(\prod_{v \in M_K} |f|_v^{n_v} \right)^{1/[K:\mathbb{Q}]}$$

and also

$$H(\phi) = \left(\prod_{v \in M_K} |\phi|_v^{n_v} \right)^{1/[K:\mathbb{Q}]}$$

Following the notation of [Sil07], we define $\delta_v(m)$ as follows, which lets us write a uniform version of the triangle inequality as

$$|x_1 + \cdots + x_m|_v \leq \delta_v(m) \max\{|x_1|_v, \ldots, |x_m|_v\}$$

Definition 3.4. For any absolute value $v \in M_K$ and any number m, we set

$$\delta_v(m) = \begin{cases} m & \text{if } v \in M_K^\infty \text{ (i.e., if } v \text{ is archimedean),} \\ 1 & \text{if } v \in M_K^0 \text{ (i.e., if } v \text{ is nonarchimedean).} \end{cases}$$

With these definitions, we state a lemma that will almost immediately imply Northcott's theorem:

Lemma 3.5. *Let $\phi : \mathbb{P}^N(\bar{K}) \to \mathbb{P}^M(\bar{K})$ be a morphism of degree d. Then, there exist constants $C_1 = C_1(\phi)$ and $C_2 = C_2(\phi)$ with $C_1, C_2 > 0$, such that*

$$C_1 \leq \frac{H(\phi(P))}{H(P)^d} \leq C_2$$

for all $P \in \mathbb{P}^N(\bar{K})$, or equivalently, $H(\phi(P)) = \Theta(H(P)^d)$, using asymptotic notation.

Intuitively, this means that a morphism of degree d raises the height to the d^{th} power.

Proof. Let $P = [x_0, \dots, x_N] \in \mathbb{P}^N(K)$ be a rational point, and $f \in K[X_0, \dots, X_N]$ a homogeneous polynomial of degree d. Then, for any $v \in M_K$ we can estimate

$$\begin{aligned} |f(P)|_v &= \left| \sum_{\substack{i_0,\dots,i_N \geq 0 \\ i_0+\dots+i_N=d}} a_{i_0\dots i_N} x_0^{i_0} \dots x_N^{i_N} \right|_v \\ &\leq \delta_v(\#\text{ of terms}) \max_{i_0,\dots,i_N} \left| a_{i_0\dots i_N} x_0^{i_0} \dots x_N^{i_N} \right|_v \end{aligned}$$

The number of terms in the sum is equal to at most the number of monomials of degree d in $N+1$ variables, which is, by stars and bars, $\binom{N+d}{d}$. Continuing with the computation, we find that

$$\begin{aligned} |f(P)|_v &\leq \delta_v \left(\binom{N+d}{d} \right) \max_{i_0,\dots,i_N} |a_{i_0\dots i_N}|_v \max_{i_0,\dots,i_N} \max_{j \in [\![0,N]\!]} |x_j|_v^{i_0+\dots+i_N} \\ &= \delta_v \left(\binom{N+d}{d} \right) |f|_v |P|_v^d \end{aligned}$$

Applying this for $f_0, f_1, \dots, f_N$ and taking the maximum again, we get

$$|\phi(P)|_v \leq \delta_v \left(\binom{N+d}{d} \right) |\phi|_v |P|_v^d$$

Now, raising this to the ${n_v}^{\text{th}}$ power, then multiply over all valuations $v \in M_K$, we get

$$\prod_{v \in M_K} |\phi(P)|_v^{n_v} \leq \prod_{v \in M_K} \delta_v^{n_v} \left(\binom{N+d}{d} \right) \prod_{v \in M_K} |\phi|_v^{n_v} |P|_v^{d \cdot n_v}$$

Taking the $[K:\mathbb{Q}]^{\text{th}}$ root, we obtain

$$H(\phi(P)) \leq \binom{N+d}{d} H(\phi) H(P)^d$$

recalling

$$\prod_{v \in M_K} \delta_v(a)^{n_v} = \prod_{v \in M_K^\infty} a^{n_v} = a^{\sum_{v \in M_K^\infty} n_v} = a^{[K:\mathbb{Q}]}$$

This gives the desired constant upper bound for $\frac{H(\phi(P))}{H(P)^d}$. For the lower bound, take ϕ be a morphism, then we may write $\phi = [f_0, \dots, f_M]$ for homogeneous polynomials $f_0, \dots, f_M$ which do not have any common zeros in $\mathbb{P}^N(\bar{K})$, as we can clear all common factors. This implies that the ideals $(f_0, \dots, f_M)$ and $(X_0, \dots, X_N)$ in $\bar{K}[X_0, \dots, X_N]$ have the same algebraic set, that is, the empty set. Now, by the Nullstellensatz, those two ideals have the same radical, that is, $X_0, X_1, \dots, X_N \in \sqrt{(f_0, f_1, \dots, f_M)}$, thus $\exists e = \max_i e_i$ such that $X_i^{e_i} \in (f_0, \dots, f_M)$, implying $X_i^e \in (f_0, \dots, f_M)$. By this, we know that there are homogeneous polynomials $g_{ij} \in \bar{K}[X_0, \dots, X_N]$ such that $X_i^e = \sum_{j \in [\![0,M]\!]} g_{ij} f_j$ for each $i \in [\![0, N]\!]$. Note that $\deg g_{ij} = e - d$ since $\deg f_j = d$ for all j. Evaluating this at $P = [x_0, \dots, x_N] \in \mathbb{P}^N(K)$, we have

$$x_i = g_{i0}(P) f_0(P) + g_{i1}(P) f_1(P) + \dots + g_{iM}(P) f_M(P)$$

for all $0 \leq i \leq N$. Now, estimating v-adic absolute values, we have

$$\begin{aligned}
|P|_v^e &= \max_{0\leq i\leq N} |x_i|_v^e \\
&= \max_{0\leq i\leq N} \left| \sum_{j\in[\![0,M]\!]} g_{ij}(P)f_j(P) \right|_v \\
&\leq \delta_v(M+1) \max_{(i,j)\in[\![0,N]\!]\times[\![0,M]\!]} |g_{ij}(P)f_j(P)|_v \\
&\leq \delta_v(M+1) \max_{(i,j)\in[\![0,N]\!]\times[\![0,M]\!]} \left\{ \delta_v\left(\binom{N+e-d}{e-d}\right) |g_{ij}|_v\, |P|_v^{e-d}\, |f_j(P)|_v \right\} \\
&\leq \delta_v\left((M+1)\binom{N+e-d}{e-d}\right)\left(\max_{(i,j)\in[\![0,N]\!]\times[\![0,M]\!]} |g_{ij}|_v\right) |P|_v^{e-d}|\phi(P)|_v
\end{aligned}$$

With this, we have some constant $C = C(M,N,d,e) = (M+1)\binom{N+e-d}{e-d}$, and letting $|g|_v = \max_{i,j}|g_{ij}|_v$, we get

$$|P|_v^d \leq \delta_v(C)|g|_v|\phi(P)|_v$$

and as done before, we take the $n_v{}^{\text{th}}$ power, then multiply over all valuations $v \in M_K$, and finally take the $[K:\mathbb{Q}]^{\text{th}}$ root, which gives $H(P)^d \leq CH(g)H(\phi(P))$, where $H(g)$ is a constant with respect to P. Indeed, this gives the desired constant lower bound for $\frac{H(\phi(P))}{H(P)^d}$, and we are done. □

Lemma 3.5 tells us that a morphism ϕ of degree d basically sends the height $H(P)$ to approximately the d^{th} power, which tells us that H acts like a multiplicative function. Regarding notation, it is often easier to work with additive functions instead, since otherwise we have to write power towers all the time; nobody likes to do that. This prompts the following definition:

Definition 3.6. The *logarithmic height*, with respect to K, is the function $h_K : \mathbb{P}^N(K) \to \mathbb{R}$ such that $h_K(P) = \log H_K(P)$. Analogously, the *absolute logarithmic height* is the function $h : \mathbb{P}^N(\bar{Q}) \to \mathbb{R}$ where $h(P) = \log H(P)$.

Using this notation, Lemma 3.5 is just $h(\phi(P)) = dh(P) + O(1)$. Now, we are ready to prove Northcott's theorem.

Proof of Theorem 3.1. From Lemma 3.5, we know that $h(\phi(P)) \geq dh(P) - C$ for some constant $C = C(\phi)$ and all points $P \in \mathbb{P}^N(\bar{K})$. Inductively applying this to P, $\phi(P)$, $\phi^2(P)$, …, $\phi^{n-1}(P)$ gives

$$h(\phi^n(P)) \geq d^n h(P) - C(1 + d + d^2 + \cdots + d^{n-1}) \geq d^n h(P) - d^n C$$

and thus $h(\phi^n(P)) \geq d^n(h(P) - C)$. Since $P \in \text{PrePer}(\phi)$, we know that $\exists n, k$ with $n \geq 0$ and $k \geq 1$ such that $\phi^n(P) = \phi^{n+k}(P)$. Hence, from $h(\phi^n(P)) \geq d^n(h(P) - C)$, substituting $\phi^n(P)$ in place of P, we get

$$h(\phi^n(P)) = h(\phi^{n+k}(P)) \geq d^k(h(\phi^n(P)) - C)$$

thus

$$h(\phi^n(P)) \leq \frac{d^k}{d^k-1}C \leq 2C$$

Now, from the original equation

$$h(P) \leq \frac{h(\phi^n(P)) + d^n C}{d^n}$$

combining this with the previous equation, we get

$$h(P) \leq \frac{2C + d^n C}{d^n} \leq 3C$$

Thus, for some $C = C(\phi)$, we know that $h(P)$ is bounded, and so is $H(P)$, as desired. □

Now, with the following lemma, the set of preperiodic points is finite, and further, the set of preperiodic points of all finite field extensions of bounded degree is finite as well.

Lemma 3.7. *Let $K/\mathbb{Q}$ be a number field, and fix constants B and D. Then, the set of points*

$$\left\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \leq B \quad \textit{and} \quad [\mathbb{Q}(P) : \mathbb{Q}] \leq D\right\}$$

is finite.

Proof. The proof of this lemma needs Galois theory, which is beyond the scope of this paper. For reference, consult the proof of Theorem 3.7 of [Sil07]. Essentially, one looks at the height $H(P)$ for each individual point $P \in \mathbb{P}^N$, views at each coordinate x_i of P, and gives an upper bound for $H(x_i)$ with respect to B, that is, one gets $H(x_i) \leq B^N$. This means that it remains to prove that the set

$$\{\alpha \in \bar{\mathbb{Q}} : H(\alpha) \leq B \quad \text{and} \quad [Q(\alpha) : Q] = d\}$$

is finite. For this, one considers all Galois conjugates of α, all of which have the same height because they are algebraically indistinguishable (see Theorem 3.6 of [Sil07]), looking at the minimal polynomial of α with coefficients in $\mathbb{Q}$, written as $F_\alpha(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Q}[X]$. Then, one uses the uniformized version of the triangle inequality to get a bound on $|a_k|_v$, after which the usual lifting to the ${n_v}^{\text{th}}$ power, multiplying over all valuations, and taking the d^{th} root gives a bound on $H([1, a_1, \ldots, a_d])$. Finally, since there are only finitely many $\mathbb{Q}$-rational points in projective space with bounded height, the set of $F_\alpha(X)$ is finite, thus the set of α is also finite, which finishes. □

Indeed, it is possible to give explicit bounds for $\left|\text{PrePer}\left(\phi, \mathbb{P}^N(K)\right)\right|$ in terms of ϕ, and there are several results on this, especially when $N = 1$. The above method of proving Northcott's theorem was, in a sense, global, but a local method of using primes of (sufficiently) good reduction would work equally well in proving Northcott's theorem.

Let's take a brief moment to sum up what we have until now. Theorem 3.1 tells us that the height of preperiodic points is bounded by a constant that is solely dependent on the morphism ϕ. Can we do any better? Is there a universal upper bound that works for any morphism of fixed degree, or even bounded degree? The following conjecture, still open at the time of writing this paper, asks this question.

Conjecture 3.8 (Uniform boundedness conjecture)**.** *Fix a number field $K/\mathbb{Q}$ with $[K : \mathbb{Q}] \leq D$, and consider all finite morphisms $\phi : \mathbb{P}^N \to \mathbb{P}^N$ defined over K with $\deg \phi = d$ for some fixed d. Then, there is a universal constant $C = C(d, N, D)$ such that*

$$\left|\text{PrePer}\left(\phi, \mathbb{P}^N(K)\right)\right| \leq C$$

Indeed, even the simplest case, that is, $(d, N, D) = (2, 1, 1)$, is not known; for more special cases, such as the quadratic $\phi(z) = z^2 + c$, consult [Sil07]. This conjecture is of critical importance, because it would mean that the global structure of preperiodic points is systematically limited by the mere choice of degrees of the morphism ϕ itself, the space $\mathbb{P}^N$, and the finite field extension $[K : \mathbb{Q}]$. Some further questions that may arise from this conjecture would be on the analysis of global structure of the set of preperiodic points, given (d, N, D), and linking that set of preperiodic points back to its geometry. The ramifications of the proof or disproof of this conjecture (or even a partial one) would be truly manifold.

References

[AM69] Michael Francis Atiyah and I. G. MacDonald, *Introduction to commutative algebra.*, Addison-Wesley-Longman, 1969.

[Art98] Michael Artin, *Algebra*, Birkhäuser, 1998.

[Con07] Keith Conrad, *Ostrowski for number fields*, 2007.

[Gou20] Fernando Q. Gouvêa, *The p-adic numbers*, pp. 53–71, Springer International Publishing, Cham, 2020.

[Hor02] AF Horadam, *Vieta polynomials*, Fibonacci Quarterly **40** (2002), no. 3, 223–232.

[IR90] Kenneth Ireland and Michael Rosen, *Algebraic number theory*, pp. 172–187, Springer New York, New York, NY, 1990.

[Mil04] John W. Milnor, *On lattès maps.*

[Mil06] John Milnor, *Dynamics in one complex variable. (am-160): Third edition. (am-160)*, Princeton University Press, 2006.

[Nor50] D. G. Northcott, *Periodic points on an algebraic variety*, Annals of Mathematics **51** (1950), no. 1, 167–177.

[Sil07] Joseph H. Silverman, *The arithmetic of dynamical systems*, Springer New York, New York, NY, 2007.

[Sto15] Michael Stoll, *p-adic analysis in arithmetic geometry.*

Euler Circle, Mountain View, CA 94040
Email address: cliid@ohs.stanford.edu