RESEARCH STATEMENT
Andrew O’Desky

My research is in the general area of arithmetic geometry. I am particularly interested in $p$-adic analysis and the study of rational points on algebraic varieties.

In the sections below, I will first describe the results from two independent projects in $p$-adic analysis. Then I will briefly describe the results from two other recent papers that made use of techniques from the theory of rational points on varieties to prove results in other areas.

Local-global principles for functions $f : \mathbb{N} \to \mathbb{Q}$

A guiding tenet of arithmetic geometry is Hasse’s local-global principle: the idea that an integral solution to a set of polynomial equations can be obtained by piecing together solutions modulo prime powers. This principle manifests itself more generally as the idea that a global feature of a mathematical object can be checked locally. For example, a well-known theorem in complex analysis says that any entire function $f$ which is suitably bounded at infinity is a polynomial. We define a local-global principle for functions $f : \mathbb{N} \to \mathbb{Q}$ to be a collection of $p$-adic conditions which guarantee that $f$ is a polynomial function.

A beautiful theorem independently discovered by Hall and Ruzsa gives a number-theoretic local-global principle for functions [2], [8]. For $p$ a prime integer, let $\mathbb{Z}_p$ denote the ring of $p$-adic integers and let $\mathbb{Q}_p$ denote the field of $p$-adic numbers.

**Theorem** (Hall–Ruzsa [2], [8]). If $f : \mathbb{N} \to \mathbb{Z}$ extends to a Lipschitz continuous function $\hat{f}_p : \mathbb{Z}_p \to \mathbb{Z}_p$ with a Lipschitz constant $C$ satisfying $C \leq 1$ for every prime $p$, and

$$|f(n)| \ll \theta^n \text{ for some } \theta < e - 1,$$

then there exists a polynomial $q \in \mathbb{Q}[X]$ such that $f(n) = q(n)$ for all $n \in \mathbb{N}$.

Thus, the local $p$-adic Lipschitz conditions together with a growth condition at the ‘infinite prime’ is equivalent to the global condition that $f$ is a polynomial function.

The local $p$-adic Lipschitz conditions in the Hall–Ruzsa theorem can be elegantly packaged and generalized by using divided differences. The first divided difference $\delta_1 f$ is the function defined for distinct natural numbers $m$ and $n$ by

$$\delta_1 f(m, n) = \frac{f(m) - f(n)}{m - n}.$$
Higher divided differences $\delta_m f$, $m \geq 2$, are important in interpolation theory and $p$-adic analysis and are defined inductively. It is easy to see that the collection of local $p$-adic Lipschitz conditions in the Hall–Ruzsa theorem is equivalent to the condition that $\delta_1 f$ is integer-valued. In [4], I proved the generalization of their result to higher divided differences by using $p$-adic analysis and some analytic number theory.

**Theorem ([4]).** If the $m$-th divided difference $\delta_m f$ of a function $f : \mathbb{N} \to \mathbb{Q}$ is integer-valued, and

$$|f(n)| \ll \theta^n \text{ for some } \theta < e^{H_m} - 1,$$

where $H_m := 1 + \frac{1}{2} + \cdots + \frac{1}{m}$ is the $m$-th harmonic number, then there exists a polynomial $q \in \mathbb{Q}[X]$ such that $f(n) = q(n)$ for all $n \in \mathbb{N}$.

The appearance of harmonic numbers in the context of interpolation theory and $p$-adic analysis was beautiful and completely unexpected.

**The $p$-adic incomplete gamma function**

In some recent joint work with David H. Richman [5] we introduce a $p$-adic analogue of the classical incomplete gamma function. Our construction is analogous to the construction of Morita’s $p$-adic gamma function [3].

The classical incomplete gamma function is defined for $(s, u) \in \mathbb{C} \times \mathbb{R}^>0$ by the integral

$$\Gamma(s, u) = \int_u^\infty z^s e^{-z} \frac{dz}{z}$$

and then extended by analytic continuation.

We show, independently of Morita’s construction, that the restriction of incomplete gamma function to positive integers extends to a $p$-adic locally analytic function on $\mathbb{Z}_p$. Let $\sigma : \mathbb{C}_p \to \mathbb{C}$ be an isomorphism. Define $\Gamma^\sigma(n, r) := \sigma^{-1} \Gamma(n, \sigma r)$ for any $r \in \mathbb{C}_p^\times$.

**Theorem ([5]).** Let $r$ be a $p$-adic integer congruent to 1 modulo $p$. Then

$$n \mapsto \Gamma^\sigma(n, r) \quad (n \in \mathbb{N}^>0)$$

extends to a $p$-adic locally analytic function $\Gamma_{p, \sigma}(\cdot, r) : \mathbb{Z}_p \to \mathbb{C}_p$.

We note that the dependence of $\Gamma_{p, \sigma}(\cdot, r)$ on $\sigma$ is only up to multiplication by an explicitly computable constant.

The $p$-adic incomplete gamma function has applications to combinatorics. The gamma
function interpolates factorials which are the numbers of permutations on finite sets. Similarly, the incomplete gamma function interpolates the numbers of permutations without a fixed point in certain wreath products. Let $C_r \wr S_n$ denote the wreath product of the cyclic group of order $r$ with the symmetric group of degree $n$. A cyclic derangement of $[r] \times [n]$ is an element of $C_r \wr S_n$ whose action on $[r] \times [n]$ has no fixed point. A cyclic arrangement of $[r] \times [n]$ is a pair $(A, \sigma)$ consisting of a subset $A \subset [n]$ and an element $\sigma \in C_r \wr S_{|A|}$.

We prove that the incomplete gamma function interpolates the counts of cyclic derangements and arrangements by showing, for any nonzero integer $r$,

$$r^n e^{1/r} \Gamma(1 + n, 1/r) = \alpha_r(n) \text{ for all } n \in \mathbb{N},$$

where

$$\alpha_r(n) := \begin{cases} (-1)^n (# \text{ of derangements of } [-r] \times [n]) & \text{if } r < 0, \\ # \text{ of arrangements of } [r] \times [n] & \text{if } r > 0. \end{cases}$$

We also prove the following beautiful formula for $\alpha_r(n)$ in terms of the floor function:

$$\alpha_r(n) := \begin{cases} \left\lfloor e^{1/r} r^n n! + \frac{1}{2} \right\rfloor & \text{if } r < 0, \\ \left\lfloor e^{1/r} r^n n! \right\rfloor & \text{if } r > 0. \end{cases} \quad (1)$$

We prove that for any prime number $p$ and integer $r$, the function $\alpha_r$ extends uniquely to a $p$-adic locally analytic metric map on $\mathbb{Z}_p$. The function $\alpha_r(n)$ thus exhibits a surprising harmony between the $p$-adic topologies and the real topology, the latter of which is crucially used in (1) to define the ordering on $\mathbb{R}$. The existence of the $p$-adic incomplete gamma function thus explains the $p$-adic interpolation properties enjoyed by the counts of derangements and arrangements which were otherwise quite mysterious.

**Heights on moduli spaces and the classical discriminant**

The discriminant of an algebraic number field is a classical invariant with important ramifications for the structure of its ring of integers. In some recent joint work with Julian Rosen [6], we introduce a moduli space $X_G$ associated to any finite group $G$ with special relevance to the Galois module theory of algebraic number fields with Galois group $G$ (“$G$-fields”). We prove that $X_G$ is a *Fano variety*, meaning that its anticanonical class $-K_{X_G}$ is ample, and we prove a formula for the anticanonical height induced by the corresponding projective embedding. Using our formula, we explain how the discriminant of a $G$-field $L$ can be interpreted as the height of a rational point $P_{L,x} \in X_G(\mathbb{Q})$ corresponding to $L$ and a special kind of element $x$ in $L$. 

3
I will state our formula in a special case where it is particularly simple. Let $L$ be a Galois number field with Galois group $G$ and let $x$ be a self-dual\(^1\) element of $L$. Let $S$ denote the ring of integers of $L$ and let $d_L$ denote the discriminant of $L$. Define the order $T = \{ a \in L : aI \subset I \}$ where $I$ is the lattice $\sum_{g \in G} \mathbb{Z}g(x) \subset L$. Let $H$ denote the anticanonical height function on $X_G$.

**Theorem** ([6]). Suppose $G$ has odd order and that $T$ is Gorenstein. Then

$$H(P_{L,x}) = [S : T] \cdot \sqrt{|d_L|}.$$ 

This formula is the first instance of a direct connection between heights on an algebraic variety and discriminants of number fields. I expect that this formula will soon lead to new results about the distribution of $G$-fields.

**Rational points on curves and complex dynamics**

Another thread of my research has focused on rational points on algebraic curves, i.e. algebraic varieties of dimension one. This research from my thesis shows how tools from the arithmetic geometry of curves can be wielded to prove results in the mathematical area of dynamics.

Consider an orbit $O_f(P)$ of a rational function $f$:

$$O_f(P) := \{ P, f(P), f(f(P)), \ldots \}, \quad P \in \mathbb{P}^1(\mathbb{C}).$$

When do two rational functions $f$ and $g$ have orbits $O_f(P)$ and $O_g(Q)$ with infinite intersection? For example, if $a$ and $b$ are integers greater than one, then $f = X^a$ and $g = X^b$ have orbits with infinite intersection if and only if $a$ and $b$ have a common divisor. In [1], one of the main results was to show that two *polynomials* have orbits with infinite intersection if and only if they have a common iterate.

In [7], Michael Zieve and I gave a definitive answer to the above question for a very large class of *rational functions*. Our results were the first to prove something about the orbit intersections of rational functions which were not polynomials. One of our main results is easy to grasp in non-technical terms. Let us write $f^m$ for the $m$th iterate of $f$. The key idea is to look at the algebraic curves defined by the equations $f^m(X) = g^n(Y)$ for large iterates. In general, this defines a *reducible* algebraic curve. We say a pair $(f, g)$ of

---

\(^1\)An element $x$ of a $G$-extension is called *self-dual* if its set of $G$-conjugates form an orthonormal basis for the bilinear form defined by the trace pairing $x \otimes y \mapsto \text{tr}(xy)$. 
nonconstant rational functions is \textit{eventually stable} if the number of irreducible components of the curve $f^m(X) = g^n(Y)$ is bounded independently of $m$ and $n$. Recall the degree of a rational function is defined to be the larger of the degrees of its numerator and denominator when expressed in reduced terms. For example, $X^3(X - 1)^{-2}$ has degree 3.

Let $f$ and $g$ be complex rational functions of degree at least two. The following theorem is the main result of [7].

\textbf{Theorem ([7])}. If $(f, g)$ is eventually stable then for any $P, Q \in \mathbb{P}^1(\mathbb{C})$ the intersection of the orbits $\mathcal{O}_f(P), \mathcal{O}_g(Q)$ is finite.

It is important to recognize that the condition of being eventually stable is generically satisfied and so ‘most’ pairs of rational functions are eventually stable.

To get a better sense for this condition, it helps to consider a concrete application. The simplest case of eventual stability concerns rational functions $f$ and $g$ with \textit{coprime degree}. It is easy to show that if the degrees of $f$ and $g$ are coprime then the pair $(f, g)$ is eventually stable. Our result now implies that for rational functions $f$ and $g$ of degree at least two,

$$f \text{ and } g \text{ have coprime degree } \implies \mathcal{O}_f(P) \cap \mathcal{O}_g(Q) \text{ is finite for any } P, Q \in \mathbb{P}^1(\mathbb{C}).$$

For example, $X^3(X - 1)^{-2}$ and $(X^2 + 1)(X + 1)^{-1}$ form an eventually stable pair because their degrees are coprime. Our result implies that any two orbits of these rational functions have finite intersection.

Our result is a decisive step towards understanding how far an orbit of a rational function determines the rational function itself. In [7], we advanced the conjecture that a single orbit determines a rational function up to iterates. More precisely, if $f$ and $g$ are rational functions of degree greater than one, we have conjectured that $f$ and $g$ have orbits with infinite intersection if and only if $f$ and $g$ have a common iterate. Future investigation of eventually \textit{unstable} pairs may pave the way for a complete understanding of the intersection of orbits of rational functions, which is an important question in the study of dynamical systems.

\textbf{References}


