# Bhargava's work on $p$-adic analytic functions

Kiran S. Kedlaya

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

2016 Fields Medal Symposium: in hono(u)r of Manjul Bhargava
The Fields Institute for Research in Mathematical Sciences
Toronto, November 1, 2016

See last slide for references.

# Contents

# Contents

# Starting point: polynomials and congruences

**Theorem (Chen, 1995; some special cases known previously)**

*For any positive integers $m, n$, the number of distinct maps $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ induced by polynomials in $\mathbb{Z}[x]$ is*

$$\prod_{k=0}^{n-1} \frac{m}{\gcd(m, k!)} = \prod_{k=0}^{\min\{n-1, m-1\}} \frac{m}{\gcd(m, k!)}.$$

To see this, represent a general polynomial $F \in \mathbb{Z}[x]$ as a (finite) sum

$$F = \sum_{k=0}^{\infty} F_k x(x-1)\cdots(x-k+1) \qquad \text{with } F_k \in \mathbb{Z}.$$

The represented function $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ depends only on $F_0, \dots, F_{n-1}$. It will suffice to verify that $f$ vanishes if and only if $F_k$ is divisible by $m/\gcd(m, k!)$ for $k = 0, \dots, n-1$.

# Starting point: polynomials and congruences

**Theorem (Chen, 1995; some special cases known previously)**

*For any positive integers $m, n$, the number of distinct maps $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ induced by polynomials in $\mathbb{Z}[x]$ is*

$$\prod_{k=0}^{n-1} \frac{m}{\gcd(m, k!)} = \prod_{k=0}^{\min\{n-1,m-1\}} \frac{m}{\gcd(m, k!)}.$$

To see this, represent a general polynomial $F \in \mathbb{Z}[x]$ as a (finite) sum

$$F = \sum_{k=0}^{\infty} F_k x(x-1)\cdots(x-k+1) \qquad \text{with } F_k \in \mathbb{Z}.$$

The represented function $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ depends only on $F_0, \dots, F_{n-1}$. It will suffice to verify that $f$ vanishes if and only if $F_k$ is divisible by $m/\gcd(m, k!)$ for $k = 0, \dots, n-1$.

# Starting point: polynomials and congruences

**Theorem (Chen, 1995; some special cases known previously)**

*For any positive integers $m, n$, the number of distinct maps $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ induced by polynomials in $\mathbb{Z}[x]$ is*

$$\prod_{k=0}^{n-1} \frac{m}{\gcd(m, k!)} = \prod_{k=0}^{\min\{n-1, m-1\}} \frac{m}{\gcd(m, k!)}.$$

To see this, represent a general polynomial $F \in \mathbb{Z}[x]$ as a (finite) sum

$$F = \sum_{k=0}^{\infty} F_k x(x-1)\cdots(x-k+1) \qquad \text{with } F_k \in \mathbb{Z}.$$

The represented function $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ depends only on $F_0, \dots, F_{n-1}$. It will suffice to verify that $f$ vanishes if and only if $F_k$ is divisible by $m/\gcd(m, k!)$ for $k = 0, \dots, n-1$.

# Polynomials and congruences (continued)

If $m/\gcd(m, k!)$ divides $F_k$ for all $k \in \{0, \dots, n-1\}$, then the evaluation of the $k$-th summand $F_k x(x-1)\cdots(x-k+1)$ at any $x \in \{0, \dots, n-1\}$ is divisible by $F_k k!$ and hence by $m$.

Otherwise, let $x$ be the *smallest* $k \in \{0, \dots, n-1\}$ for which $m/\gcd(m, k!)$ does not divide $F_k$. Then the evaluation of the $k$-th summand at $x$ is divisible by $m$ for all $k < x$; zero for all $k > x$; and not divisible by $m$ for $k = x$.

Note the analogy with an observation of Pólya (1919): every polynomial in $\mathbb{Q}[x]$ has a unique representation as

$$\sum_{k=0}^{\infty} F_k \binom{x}{k} = \sum_{k=0}^{\infty} F_k \frac{x(x-1)\cdots(x-k+1)}{k!} \qquad \text{with } F_k \in \mathbb{Q},$$

and a polynomial in $\mathbb{Q}[x]$ maps $\mathbb{Z}$ to $\mathbb{Z}$ if and only if $F_k \in \mathbb{Z}$ for all $k$.

# Polynomials and congruences (continued)

If $m/\gcd(m, k!)$ divides $F_k$ for all $k \in \{0, \dots, n-1\}$, then the evaluation of the $k$-th summand $F_k x(x-1)\cdots(x-k+1)$ at any $x \in \{0, \dots, n-1\}$ is divisible by $F_k k!$ and hence by $m$.

Otherwise, let $x$ be the *smallest* $k \in \{0, \dots, n-1\}$ for which $m/\gcd(m, k!)$ does not divide $F_k$. Then the evaluation of the $k$-th summand at $x$ is divisible by $m$ for all $k < x$; zero for all $k > x$; and not divisible by $m$ for $k = x$.

Note the analogy with an observation of Pólya (1919): every polynomial in $\mathbb{Q}[x]$ has a unique representation as

$$\sum_{k=0}^{\infty} F_k \binom{x}{k} = \sum_{k=0}^{\infty} F_k \frac{x(x-1)\cdots(x-k+1)}{k!} \qquad \text{with } F_k \in \mathbb{Q},$$

and a polynomial in $\mathbb{Q}[x]$ maps $\mathbb{Z}$ to $\mathbb{Z}$ if and only if $F_k \in \mathbb{Z}$ for all $k$.

# Polynomials and congruences (continued)

If $m/\gcd(m, k!)$ divides $F_k$ for all $k \in \{0, \dots, n-1\}$, then the evaluation of the $k$-th summand $F_k x(x-1)\cdots(x-k+1)$ at any $x \in \{0, \dots, n-1\}$ is divisible by $F_k k!$ and hence by $m$.

Otherwise, let $x$ be the *smallest* $k \in \{0, \dots, n-1\}$ for which $m/\gcd(m, k!)$ does not divide $F_k$. Then the evaluation of the $k$-th summand at $x$ is divisible by $m$ for all $k < x$; zero for all $k > x$; and not divisible by $m$ for $k = x$.

Note the analogy with an observation of Pólya (1919): every polynomial in $\mathbb{Q}[x]$ has a unique representation as

$$\sum_{k=0}^{\infty} F_k \binom{x}{k} = \sum_{k=0}^{\infty} F_k \frac{x(x-1)\cdots(x-k+1)}{k!} \qquad \text{with } F_k \in \mathbb{Q},$$

and a polynomial in $\mathbb{Q}[x]$ maps $\mathbb{Z}$ to $\mathbb{Z}$ if and only if $F_k \in \mathbb{Z}$ for all $k$.

# An undergraduate research problem

Any function $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ represented by a polynomial is *congruence-preserving*: for all $d$ dividing $m$, if $a, b \in \{0, \dots, n-1\}$ satisfy $a \equiv b \pmod{d}$, then $f(a) \equiv f(b) \pmod{d}$. Chen observed that the converse sometimes fails (e.g., for $n = m = 8$), and asked the following.

**Problem (Gallian; University of Minnesota, Duluth; REU 1995)**

*For which pairs $(n, m)$ are all congruence-preserving functions $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ represented by a polynomial in $\mathbb{Z}[x]$?*

**Theorem (Bhargava, 1995)**

*Let $\prod_p p^{e_p}$ be the prime factorization of $m$. Then every congruence-preserving function $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ is represented by a polynomial in $\mathbb{Z}[x]$ if and only if for each $p < n/2$, either ($p = 2$ and $e_p \leq 2$) or ($p > 2$ and $e_p \leq 1$).*

# An undergraduate research problem

Any function $f : \{0, \ldots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ represented by a polynomial is *congruence-preserving*: for all $d$ dividing $m$, if $a, b \in \{0, \ldots, n-1\}$ satisfy $a \equiv b \pmod{d}$, then $f(a) \equiv f(b) \pmod{d}$. Chen observed that the converse sometimes fails (e.g., for $n = m = 8$), and asked the following.

**Problem (Gallian; University of Minnesota, Duluth; REU 1995)**

*For which pairs $(n, m)$ are all congruence-preserving functions $f : \{0, \ldots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ represented by a polynomial in $\mathbb{Z}[x]$?*

**Theorem (Bhargava, 1995)**

*Let $\prod_p p^{e_p}$ be the prime factorization of $m$. Then every congruence-preserving function $f : \{0, \ldots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ is represented by a polynomial in $\mathbb{Z}[x]$ if and only if for each $p < n/2$, either ($p = 2$ and $e_p \leq 2$) or ($p > 2$ and $e_p \leq 1$).*

# An undergraduate research problem

Any function $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ represented by a polynomial is *congruence-preserving*: for all $d$ dividing $m$, if $a, b \in \{0, \dots, n-1\}$ satisfy $a \equiv b \pmod{d}$, then $f(a) \equiv f(b) \pmod{d}$. Chen observed that the converse sometimes fails (e.g., for $n = m = 8$), and asked the following.

Problem (Gallian; University of Minnesota, Duluth; REU 1995)

*For which pairs $(n, m)$ are all congruence-preserving functions $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ represented by a polynomial in $\mathbb{Z}[x]$?*

Theorem (Bhargava, 1995)

*Let $\prod_p p^{e_p}$ be the prime factorization of $m$. Then every congruence-preserving function $f : \{0, \dots, n-1\} \to \mathbb{Z}/m\mathbb{Z}$ is represented by a polynomial in $\mathbb{Z}[x]$ if and only if for each $p < n/2$, either ($p = 2$ and $e_p \leq 2$) or ($p > 2$ and $e_p \leq 1$).*

# Contents

# Don't stop there: Bhargava's senior honors thesis

What if we replace $\{0, \ldots, n-1\}$ with some infinite[1] subset $S$ of $\mathbb{Z}$? Can we again explicitly describe the maps from $S$ into $\mathbb{Z}/m\mathbb{Z}$ represented by polynomials?

Better yet, replace $\mathbb{Z}$ and $\mathbb{Q}$ with a Dedekind domain $R$ and its fraction field $K$. Can we explicitly describe the polynomials in $K[x]$ that map some subset $S \subseteq R$ into $R$? Many special cases had been studied previously.

Bhargava discovered a simple uniform answer to this question. In the special case where $R$ is a discrete valuation ring, one gets an analogue of Pólya's result using suitably modified versions of the binomial polynomials $\binom{x}{k}$, which are easily computable in many examples.

[1] The finite case is similar, but for ease of exposition we omit it.

# Don't stop there: Bhargava's senior honors thesis

What if we replace $\{0, \ldots, n-1\}$ with some infinite[1] subset $S$ of $\mathbb{Z}$? Can we again explicitly describe the maps from $S$ into $\mathbb{Z}/m\mathbb{Z}$ represented by polynomials?

Better yet, replace $\mathbb{Z}$ and $\mathbb{Q}$ with a Dedekind domain $R$ and its fraction field $K$. Can we explicitly describe the polynomials in $K[x]$ that map some subset $S \subseteq R$ into $R$? Many special cases had been studied previously.

Bhargava discovered a simple uniform answer to this question. In the special case where $R$ is a discrete valuation ring, one gets an analogue of Pólya's result using suitably modified versions of the binomial polynomials $\binom{x}{k}$, which are easily computable in many examples.

[1] The finite case is similar, but for ease of exposition we omit it.

# Don't stop there: Bhargava's senior honors thesis

What if we replace $\{0, \ldots, n-1\}$ with some infinite[1] subset $S$ of $\mathbb{Z}$? Can we again explicitly describe the maps from $S$ into $\mathbb{Z}/m\mathbb{Z}$ represented by polynomials?

Better yet, replace $\mathbb{Z}$ and $\mathbb{Q}$ with a Dedekind domain $R$ and its fraction field $K$. Can we explicitly describe the polynomials in $K[x]$ that map some subset $S \subseteq R$ into $R$? Many special cases had been studied previously.

Bhargava discovered a simple uniform answer to this question. In the special case where $R$ is a discrete valuation ring, one gets an analogue of Pólya's result using suitably modified versions of the binomial polynomials $\binom{x}{k}$, which are easily computable in many examples.

[1] The finite case is similar, but for ease of exposition we omit it.

# The $\mathfrak{p}$-ordering construction: local version

Suppose that $R$ is a discrete valuation ring with maximal ideal $\mathfrak{p}$. Given an infinite subset $S \subseteq R$, a $\mathfrak{p}$-*ordering*[2] of $S$ is a sequence $a_0, a_1, \dots$ such that for each $k$, $a_k$ minimizes the $\mathfrak{p}$-adic valuation of

$$k!_S := (a_k - a_0) \cdots (a_k - a_{k-1}).$$

Such a sequence (which obviously exists) does the job: a polynomial in $K[x]$ maps $S$ into $R$ if and only if it has the form

$$\sum_{k=0}^{\infty} F_k \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_S} \qquad \text{with } F_k \in R.$$

As a corollary, we have the following elementary but puzzling fact.

**Lemma (Bhargava)**

*The ideal $(k!)_S$ generated by $k!_S$ is independent of all choices. (!?)*

[2] The name is slightly misleading: this sequence does not usually exhaust $S$.

# The $\mathfrak{p}$-ordering construction: local version

Suppose that $R$ is a discrete valuation ring with maximal ideal $\mathfrak{p}$. Given an infinite subset $S \subseteq R$, a $\mathfrak{p}$-*ordering*[2] of $S$ is a sequence $a_0, a_1, \dots$ such that for each $k$, $a_k$ minimizes the $\mathfrak{p}$-adic valuation of

$$k!_S := (a_k - a_0) \cdots (a_k - a_{k-1}).$$

Such a sequence (which obviously exists) does the job: a polynomial in $K[x]$ maps $S$ into $R$ if and only if it has the form

$$\sum_{k=0}^{\infty} F_k \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_S} \qquad \text{with } F_k \in R.$$

As a corollary, we have the following elementary but puzzling fact.

**Lemma (Bhargava)**

*The ideal $(k!)_S$ generated by $k!_S$ is independent of all choices. (!?)*

[2] The name is slightly misleading: this sequence does not usually exhaust $S$.

# The $\mathfrak{p}$-ordering construction: local version

Suppose that $R$ is a discrete valuation ring with maximal ideal $\mathfrak{p}$. Given an infinite subset $S \subseteq R$, a $\mathfrak{p}$-*ordering*[2] of $S$ is a sequence $a_0, a_1, \ldots$ such that for each $k$, $a_k$ minimizes the $\mathfrak{p}$-adic valuation of

$$k!_S := (a_k - a_0) \cdots (a_k - a_{k-1}).$$

Such a sequence (which obviously exists) does the job: a polynomial in $K[x]$ maps $S$ into $R$ if and only if it has the form

$$\sum_{k=0}^{\infty} F_k \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_S} \qquad \text{with } F_k \in R.$$

As a corollary, we have the following elementary but puzzling fact.

**Lemma (Bhargava)**

*The ideal $(k!)_S$ generated by $k!_S$ is independent of all choices. (!?)*

[2] The name is slightly misleading: this sequence does not usually exhaust $S$.

# The $\mathfrak{p}$-ordering construction: local version

Suppose that $R$ is a discrete valuation ring with maximal ideal $\mathfrak{p}$. Given an infinite subset $S \subseteq R$, a $\mathfrak{p}$-*ordering*[2] of $S$ is a sequence $a_0, a_1, \dots$ such that for each $k$, $a_k$ minimizes the $\mathfrak{p}$-adic valuation of

$$k!_S := (a_k - a_0) \cdots (a_k - a_{k-1}).$$

Such a sequence (which obviously exists) does the job: a polynomial in $K[x]$ maps $S$ into $R$ if and only if it has the form

$$\sum_{k=0}^{\infty} F_k \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_S} \qquad \text{with } F_k \in R.$$

As a corollary, we have the following elementary but puzzling fact.

**Lemma (Bhargava)**

*The ideal $(k!)_S$ generated by $k!_S$ is independent of all choices. (!?)*

[2] The name is slightly misleading: this sequence does not usually exhaust $S$.

# The $\mathfrak{p}$-ordering construction: global version

Now, $R$ is again a general Dedekind domain and $S \subset R$ an infinite subset.

For each maximal ideal $\mathfrak{p}$ of $R$, we may project $S$ into the localization $R_{\mathfrak{p}}$, which is a discrete valuation ring; identify the resulting ideals $(k!)_{S,\mathfrak{p}}$ with powers of $\mathfrak{p}$ in $R$. For each $k$, the ideal $(k!)_{S,\mathfrak{p}}$ is trivial for all but finitely many $\mathfrak{p}$; we may thus form the product ideal $(k!)_S = \prod_{\mathfrak{p}} (k!)_{S,\mathfrak{p}}$.

In case $(k!)_S$ is principal for all $k$, we may use the Chinese remainder theorem to compute a sequence of polynomials $P_k \in K[x]$ of degree $k$ with the property that any $F = \sum_{k=0}^{\infty} F_k P_k(x) \in K[x]$ maps $S$ into $R$ if and only if $F_k \in R$ for all $k \geq 0$.

Otherwise, no such sequence[3] $P_k$ exists. However, one can still characterize the polynomials taking $S$ into $R$ by working locally.

[3] If it did, the reciprocal of the leading coefficient of $P_k$ would generate $(k!)_S$.

# The $\mathfrak{p}$-ordering construction: global version

Now, $R$ is again a general Dedekind domain and $S \subset R$ an infinite subset.

For each maximal ideal $\mathfrak{p}$ of $R$, we may project $S$ into the localization $R_{\mathfrak{p}}$, which is a discrete valuation ring; identify the resulting ideals $(k!)_{S,\mathfrak{p}}$ with powers of $\mathfrak{p}$ in $R$. For each $k$, the ideal $(k!)_{S,\mathfrak{p}}$ is trivial for all but finitely many $\mathfrak{p}$; we may thus form the product ideal $(k!)_S = \prod_{\mathfrak{p}} (k!)_{S,\mathfrak{p}}$.

In case $(k!)_S$ is principal for all $k$, we may use the Chinese remainder theorem to compute a sequence of polynomials $P_k \in K[x]$ of degree $k$ with the property that any $F = \sum_{k=0}^{\infty} F_k P_k(x) \in K[x]$ maps $S$ into $R$ if and only if $F_k \in R$ for all $k \geq 0$.

Otherwise, no such sequence[3] $P_k$ exists. However, one can still characterize the polynomials taking $S$ into $R$ by working locally.

[3] If it did, the reciprocal of the leading coefficient of $P_k$ would generate $(k!)_S$.

# The $\mathfrak{p}$-ordering construction: global version

Now, $R$ is again a general Dedekind domain and $S \subset R$ an infinite subset.

For each maximal ideal $\mathfrak{p}$ of $R$, we may project $S$ into the localization $R_{\mathfrak{p}}$, which is a discrete valuation ring; identify the resulting ideals $(k!)_{S,\mathfrak{p}}$ with powers of $\mathfrak{p}$ in $R$. For each $k$, the ideal $(k!)_{S,\mathfrak{p}}$ is trivial for all but finitely many $\mathfrak{p}$; we may thus form the product ideal $(k!)_S = \prod_{\mathfrak{p}} (k!)_{S,\mathfrak{p}}$.

In case $(k!)_S$ is principal for all $k$, we may use the Chinese remainder theorem to compute a sequence of polynomials $P_k \in K[x]$ of degree $k$ with the property that any $F = \sum_{k=0}^{\infty} F_k P_k(x) \in K[x]$ maps $S$ into $R$ if and only if $F_k \in R$ for all $k \geq 0$.

Otherwise, no such sequence[3] $P_k$ exists. However, one can still characterize the polynomials taking $S$ into $R$ by working locally.

[3] If it did, the reciprocal of the leading coefficient of $P_k$ would generate $(k!)_S$.

# The $\mathfrak{p}$-ordering construction: global version

Now, $R$ is again a general Dedekind domain and $S \subset R$ an infinite subset.

For each maximal ideal $\mathfrak{p}$ of $R$, we may project $S$ into the localization $R_{\mathfrak{p}}$, which is a discrete valuation ring; identify the resulting ideals $(k!)_{S,\mathfrak{p}}$ with powers of $\mathfrak{p}$ in $R$. For each $k$, the ideal $(k!)_{S,\mathfrak{p}}$ is trivial for all but finitely many $\mathfrak{p}$; we may thus form the product ideal $(k!)_S = \prod_{\mathfrak{p}} (k!)_{S,\mathfrak{p}}$.

In case $(k!)_S$ is principal for all $k$, we may use the Chinese remainder theorem to compute a sequence of polynomials $P_k \in K[x]$ of degree $k$ with the property that any $F = \sum_{k=0}^{\infty} F_k P_k(x) \in K[x]$ maps $S$ into $R$ if and only if $F_k \in R$ for all $k \geq 0$.

Otherwise, no such sequence[3] $P_k$ exists. However, one can still characterize the polynomials taking $S$ into $R$ by working locally.

[3] If it did, the reciprocal of the leading coefficient of $P_k$ would generate $(k!)_S$.

# Global $\mathfrak{p}$-orderings

Even when the ideals $(k!)_S$ are principal, we may not be able to force $P_k$ to have the form of a generalized binomial coefficient

$$P_k = \frac{(x - a_0) \cdots (x - a_{k-1})}{(a_k - a_0) \cdots (a_k - a_{k-1})}$$

for some sequence $a_0, a_1, \ldots$. This only works if $a_0, a_1, \ldots$ is a $\mathfrak{p}$-ordering for all $\mathfrak{p}$ at once (or for short, a *global* $\mathfrak{p}$*-ordering*).

Global $\mathfrak{p}$-orderings exist in a few natural examples, but not in any great generality even when $R$ is a principal ideal domain.

**Theorem (Wood, 2003; from the Duluth REU)**

*Let $R$ be the ring of integers in an imaginary quadratic field and take $S = R$. Then there exists no global $\mathfrak{p}$-ordering.*

# Global $\mathfrak{p}$-orderings

Even when the ideals $(k!)_S$ are principal, we may not be able to force $P_k$ to have the form of a generalized binomial coefficient

$$P_k = \frac{(x - a_0) \cdots (x - a_{k-1})}{(a_k - a_0) \cdots (a_k - a_{k-1})}$$

for some sequence $a_0, a_1, \dots$. This only works if $a_0, a_1, \dots$ is a $\mathfrak{p}$-ordering for all $\mathfrak{p}$ at once (or for short, a *global* $\mathfrak{p}$*-ordering*).

Global $\mathfrak{p}$-orderings exist in a few natural examples, but not in any great generality even when $R$ is a principal ideal domain.

**Theorem (Wood, 2003; from the Duluth REU)**

*Let $R$ be the ring of integers in an imaginary quadratic field and take $S = R$. Then there exists no global $\mathfrak{p}$-ordering.*

# Global $\mathfrak{p}$-orderings

Even when the ideals $(k!)_S$ are principal, we may not be able to force $P_k$ to have the form of a generalized binomial coefficient

$$P_k = \frac{(x - a_0) \cdots (x - a_{k-1})}{(a_k - a_0) \cdots (a_k - a_{k-1})}$$

for some sequence $a_0, a_1, \ldots$. This only works if $a_0, a_1, \ldots$ is a $\mathfrak{p}$-ordering for all $\mathfrak{p}$ at once (or for short, a *global* $\mathfrak{p}$*-ordering*).

Global $\mathfrak{p}$-orderings exist in a few natural examples, but not in any great generality even when $R$ is a principal ideal domain.

Theorem (Wood, 2003; from the Duluth REU)

*Let $R$ be the ring of integers in an imaginary quadratic field and take $S = R$. Then there exists no global $\mathfrak{p}$-ordering.*

# Examples

## Example

Take $S = R = \mathbb{Z}$. Then $0, 1, \ldots$ is a global $\mathfrak{p}$-ordering for which $k!_S = k!$.

## Example

Take $S = R = \mathbb{F}_q[t]$. Write $\mathbb{F}_q = \{0 = c_0, \ldots, c_{q-1}\}$. Write $k$ in base $q$ as $\cdots k_2 k_1 k_0$; setting $a_k = c_{k_0} + c_{k_1} t + c_{k_2} t^2 + \cdots$ gives a global $\mathfrak{p}$-ordering. Here $k!_S$ reproduces the *Carlitz factorials*.

## Example

Let $S$ be the set of primes in $\mathbb{Z}$. There is no global $\mathfrak{p}$-ordering, but

$$(k!)_S = \prod_p (p)^{e_{p,k}}, \qquad e_{p,k} = \sum_{j=0}^{\infty} \left\lfloor \frac{k-1}{(p-1)p^j} \right\rfloor \qquad (k > 0).$$

(Hint: compute a local $p$-ordering starting with $p$ itself.)

# Examples

### Example

Take $S = R = \mathbb{Z}$. Then $0, 1, \dots$ is a global $\mathfrak{p}$-ordering for which $k!_S = k!$.

### Example

Take $S = R = \mathbb{F}_q[t]$. Write $\mathbb{F}_q = \{0 = c_0, \dots, c_{q-1}\}$. Write $k$ in base $q$ as $\cdots k_2 k_1 k_0$; setting $a_k = c_{k_0} + c_{k_1} t + c_{k_2} t^2 + \cdots$ gives a global $\mathfrak{p}$-ordering. Here $k!_S$ reproduces the *Carlitz factorials*.

### Example

Let $S$ be the set of primes in $\mathbb{Z}$. There is no global $\mathfrak{p}$-ordering, but

$$(k!)_S = \prod_p (p)^{e_{p,k}}, \qquad e_{p,k} = \sum_{j=0}^{\infty} \left\lfloor \frac{k-1}{(p-1)p^j} \right\rfloor \qquad (k > 0).$$

(Hint: compute a local $p$-ordering starting with $p$ itself.)

# Examples

## Example

Take $S = R = \mathbb{Z}$. Then $0, 1, \dots$ is a global $\mathfrak{p}$-ordering for which $k!_S = k!$.

## Example

Take $S = R = \mathbb{F}_q[t]$. Write $\mathbb{F}_q = \{0 = c_0, \dots, c_{q-1}\}$. Write $k$ in base $q$ as $\cdots k_2 k_1 k_0$; setting $a_k = c_{k_0} + c_{k_1} t + c_{k_2} t^2 + \cdots$ gives a global $\mathfrak{p}$-ordering. Here $k!_S$ reproduces the *Carlitz factorials*.

## Example

Let $S$ be the set of primes in $\mathbb{Z}$. There is no global $\mathfrak{p}$-ordering, but

$$(k!)_S = \prod_p (p)^{e_{p,k}}, \qquad e_{p,k} = \sum_{j=0}^{\infty} \left\lfloor \frac{k-1}{(p-1)p^j} \right\rfloor \qquad (k > 0).$$

(Hint: compute a local $p$-ordering starting with $p$ itself.)

# Contents

# Uniform approximation by polynomials

And now for something completely different.

**Theorem (Stone–Weierstrass approximation theorem, 1937)**

*Let $S$ be a compact subset of $\mathbb{R}^n$. Then every continuous function from $S$ to $\mathbb{R}$ can be uniformly approximated by polynomials.*

Does this have a nonarchimedean analogue? Here is one with $n = 1$.

**Theorem (Mahler, 1958)**

*Every continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ has a unique representation as $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}$ for some $f_k \in \mathbb{Q}_p$ with $\lim_{k\to\infty} f_k = 0$.*

It is easy to generalize this to functions $\mathbb{Z}_p^n \to \mathbb{Q}_p$. But what if the domain is an arbitrary compact (= closed and bounded) subset? Or $\mathbb{Q}_p$ is replaced by another local field (i.e., a complete discretely valued field with *finite* residue field)?

# Uniform approximation by polynomials

And now for something completely different.

**Theorem (Stone–Weierstrass approximation theorem, 1937)**

*Let $S$ be a compact subset of $\mathbb{R}^n$. Then every continuous function from $S$ to $\mathbb{R}$ can be uniformly approximated by polynomials.*

Does this have a nonarchimedean analogue? Here is one with $n = 1$.

**Theorem (Mahler, 1958)**

*Every continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ has a unique representation as $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}$ for some $f_k \in \mathbb{Q}_p$ with $\lim_{k\to\infty} f_k = 0$.*

It is easy to generalize this to functions $\mathbb{Z}_p^n \to \mathbb{Q}_p$. But what if the domain is an arbitrary compact (= closed and bounded) subset? Or $\mathbb{Q}_p$ is replaced by another local field (i.e., a complete discretely valued field with *finite* residue field)?

# Uniform approximation by polynomials

And now for something completely different.

**Theorem (Stone–Weierstrass approximation theorem, 1937)**

*Let $S$ be a compact subset of $\mathbb{R}^n$. Then every continuous function from $S$ to $\mathbb{R}$ can be uniformly approximated by polynomials.*

Does this have a nonarchimedean analogue? Here is one with $n = 1$.

**Theorem (Mahler, 1958)**

*Every continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ has a unique representation as $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}$ for some $f_k \in \mathbb{Q}_p$ with $\lim_{k\to\infty} f_k = 0$.*

It is easy to generalize this to functions $\mathbb{Z}_p^n \to \mathbb{Q}_p$. But what if the domain is an arbitrary compact (= closed and bounded) subset? Or $\mathbb{Q}_p$ is replaced by another local field (i.e., a complete discretely valued field with *finite* residue field)?

# Uniform approximation by polynomials

And now for something completely different.

Theorem (Stone–Weierstrass approximation theorem, 1937)

*Let $S$ be a compact subset of $\mathbb{R}^n$. Then every continuous function from $S$ to $\mathbb{R}$ can be uniformly approximated by polynomials.*

Does this have a nonarchimedean analogue? Here is one with $n = 1$.

Theorem (Mahler, 1958)

*Every continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ has a unique representation as $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}$ for some $f_k \in \mathbb{Q}_p$ with $\lim_{k\to\infty} f_k = 0$.*

It is easy to generalize this to functions $\mathbb{Z}_p^n \to \mathbb{Q}_p$. But what if the domain is an arbitrary compact (= closed and bounded) subset? Or $\mathbb{Q}_p$ is replaced by another local field (i.e., a complete discretely valued field with *finite* residue field)?

# An explicit nonarchimedean Stone-Weierstrass theorem

Let $K$ be a local field whose valuation ring $R$ has maximal ideal $\mathfrak{p}$.

**Theorem (Bhargava-K, 1997; generalizes Amice, 1967)**

*Let $S \subseteq R$ be an infinite compact subset. Choose a $\mathfrak{p}$-ordering $a_0, a_1, \dots$ of $S$ and define*

$$\binom{x}{k}_S := \frac{(x-a_0)\cdots(x-a_{k-1})}{(a_k-a_0)\cdots(a_k-a_{k-1})} \qquad (k=0,1,\dots).$$

*Then every continuous function $f: S \to K$ has a unique representation as $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_S$ for some $f_k \in K$ with $\lim_{k\to\infty} f_k = 0$.*

**Corollary (just now!)**

*Let $S$ be a compact subset of $K^n$ for some positive integer $n$. Then every continuous function from $S$ to $K$ can be uniformly approximated by polynomials. (Hint: identify $K^n$ with an extension of $K$.)*

# An explicit nonarchimedean Stone-Weierstrass theorem

Let $K$ be a local field whose valuation ring $R$ has maximal ideal $\mathfrak{p}$.

**Theorem (Bhargava-K, 1997; generalizes Amice, 1967)**

*Let $S \subseteq R$ be an infinite compact subset. Choose a $\mathfrak{p}$-ordering $a_0, a_1, \ldots$ of $S$ and define*

$$\binom{x}{k}_S := \frac{(x - a_0) \cdots (x - a_{k-1})}{(a_k - a_0) \cdots (a_k - a_{k-1})} \qquad (k = 0, 1, \ldots).$$

*Then every continuous function $f : S \to K$ has a unique representation as $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_S$ for some $f_k \in K$ with $\lim_{k\to\infty} f_k = 0$.*

**Corollary (just now!)**

*Let $S$ be a compact subset of $K^n$ for some positive integer $n$. Then every continuous function from $S$ to $K$ can be uniformly approximated by polynomials. (Hint: identify $K^n$ with an extension of $K$.)*

# A lemma from the proof

The previous theorem does not depend on the choice of the $\mathfrak{p}$-ordering; but restricting the $\mathfrak{p}$-ordering provides useful extra precision.

We say that a $\mathfrak{p}$-ordering $a_0, a_1, \ldots$ of $S$ is *proper* if for all $m, k \geq 0$, $a_k$ is chosen[4] in a new residue class modulo $\mathfrak{p}^m$ only if no other option exists. For example, for $S \subseteq \mathbb{Z}$ and $p > 2$, $0, 1, p, 2p, p^2 + 1, \ldots$ cannot be proper.

**Lemma**

*Choose a proper $\mathfrak{p}$-ordering $a_0, a_1, \ldots$ of $S$. If $a_k$ is in a new residue class modulo $\mathfrak{p}^m$ and $x, y \in S$ satisfy $x \equiv y \pmod{\mathfrak{p}^m}$, then*

$$\binom{x}{k}_S \equiv \binom{y}{k}_S \pmod{\mathfrak{p}}.$$

This generalizes a classical lemma of Lucas on binomial coefficients.

[4] Why can this be achieved for all $m$ at once? If $a_k$ is *too* congruent to some previous $a_i$, then $(a_k - a_0) \cdots (a_k - a_{k-1})$ will have no chance to achieve its minimum valuation.

# A lemma from the proof

The previous theorem does not depend on the choice of the $\mathfrak{p}$-ordering; but restricting the $\mathfrak{p}$-ordering provides useful extra precision.

We say that a $\mathfrak{p}$-ordering $a_0, a_1, \ldots$ of $S$ is *proper* if for all $m, k \geq 0$, $a_k$ is chosen[4] in a new residue class modulo $\mathfrak{p}^m$ only if no other option exists. For example, for $S \subseteq \mathbb{Z}$ and $p > 2$, $0, 1, p, 2p, p^2 + 1, \ldots$ cannot be proper.

**Lemma**

*Choose a proper $\mathfrak{p}$-ordering $a_0, a_1, \ldots$ of $S$. If $a_k$ is in a new residue class modulo $\mathfrak{p}^m$ and $x, y \in S$ satisfy $x \equiv y \pmod{\mathfrak{p}^m}$, then*

$$\binom{x}{k}_S \equiv \binom{y}{k}_S \pmod{\mathfrak{p}}.$$

This generalizes a classical lemma of Lucas on binomial coefficients.

[4] Why can this be achieved for all $m$ at once? If $a_k$ is *too* congruent to some previous $a_i$, then $(a_k - a_0) \cdots (a_k - a_{k-1})$ will have no chance to achieve its minimum valuation.

# A lemma from the proof

The previous theorem does not depend on the choice of the $\mathfrak{p}$-ordering; but restricting the $\mathfrak{p}$-ordering provides useful extra precision.

We say that a $\mathfrak{p}$-ordering $a_0, a_1, \dots$ of $S$ is *proper* if for all $m, k \geq 0$, $a_k$ is chosen[4] in a new residue class modulo $\mathfrak{p}^m$ only if no other option exists. For example, for $S \subseteq \mathbb{Z}$ and $p > 2$, $0, 1, p, 2p, p^2 + 1, \dots$ cannot be proper.

**Lemma**

*Choose a proper $\mathfrak{p}$-ordering $a_0, a_1, \dots$ of $S$. If $a_k$ is in a new residue class modulo $\mathfrak{p}^m$ and $x, y \in S$ satisfy $x \equiv y \pmod{\mathfrak{p}^m}$, then*

$$\binom{x}{k}_S \equiv \binom{y}{k}_S \pmod{\mathfrak{p}}.$$

This generalizes a classical lemma of Lucas on binomial coefficients.

[4] Why can this be achieved for all $m$ at once? If $a_k$ is *too* congruent to some previous $a_i$, then $(a_k - a_0) \cdots (a_k - a_{k-1})$ will have no chance to achieve its minimum valuation.

# A lemma from the proof

The previous theorem does not depend on the choice of the $\mathfrak{p}$-ordering; but restricting the $\mathfrak{p}$-ordering provides useful extra precision.

We say that a $\mathfrak{p}$-ordering $a_0, a_1, \dots$ of $S$ is *proper* if for all $m, k \geq 0$, $a_k$ is chosen[4] in a new residue class modulo $\mathfrak{p}^m$ only if no other option exists. For example, for $S \subseteq \mathbb{Z}$ and $p > 2$, $0, 1, p, 2p, p^2 + 1, \dots$ cannot be proper.

**Lemma**

*Choose a proper $\mathfrak{p}$-ordering $a_0, a_1, \dots$ of $S$. If $a_k$ is in a new residue class modulo $\mathfrak{p}^m$ and $x, y \in S$ satisfy $x \equiv y \pmod{\mathfrak{p}^m}$, then*

$$\binom{x}{k}_S \equiv \binom{y}{k}_S \pmod{\mathfrak{p}}.$$

This generalizes a classical lemma of Lucas on binomial coefficients.

[4]Why can this be achieved for all $m$ at once? If $a_k$ is *too* congruent to some previous $a_i$, then $(a_k - a_0) \cdots (a_k - a_{k-1})$ will have no chance to achieve its minimum valuation.

# Contents

# Beyond continuous functions

In $p$-adic analysis, it is common to consider functions on local fields which are not merely continuous, but obey some stronger differentiability conditions. For instance, in the representation theory of $p$-adic groups, it is common to form such a function space, then interpret a suitable topological dual space as a *space of distributions*.

Bhargava showed that our theorem on continuous functions could be modified to handle continuously differentiable functions and locally analytic functions. For this, however, one must replace $\mathfrak{p}$-orderings by slightly modified concepts which are also related to certain integrality conditions on polynomials. (Most of this work was done before 2000, but only published in 2009.)

# Beyond continuous functions

In *p*-adic analysis, it is common to consider functions on local fields which are not merely continuous, but obey some stronger differentiability conditions. For instance, in the representation theory of *p*-adic groups, it is common to form such a function space, then interpret a suitable topological dual space as a *space of distributions*.

Bhargava showed that our theorem on continuous functions could be modified to handle continuously differentiable functions and locally analytic functions. For this, however, one must replace $\mathfrak{p}$-orderings by slightly modified concepts which are also related to certain integrality conditions on polynomials. (Most of this work was done before 2000, but only published in 2009.)

# Divided differences

Again, let $R$ be a Dedekind domain with fraction field $K$. (On this slide, we only use that $R$ is a domain.)

For $F \in K[x]$, define the *difference quotient* of $F$ as

$$\Phi F(x, y) = \frac{F(x) - F(y)}{x - y} \in K[x, y].$$

More generally, for $r > 0$, define the *r-th difference quotient* as

$$\Phi^r F(x_0, \dots, x_r) = \frac{\Phi^{r-1} F(x_0, \dots, x_{r-1}) - \Phi^{r-1} F(x_0, \dots, x_{r-2}, x_r)}{x_{r-1} - x_r}.$$

One shows that $F \in R[x]$ if and only if $\Phi^r F(R^{r+1}) \subseteq R$ for all $r \geq 0$. (Hint: do the case $F(x) = cx^k$ for each $k$.)

# Divided differences

Again, let $R$ be a Dedekind domain with fraction field $K$. (On this slide, we only use that $R$ is a domain.)

For $F \in K[x]$, define the *difference quotient* of $F$ as

$$\Phi F(x, y) = \frac{F(x) - F(y)}{x - y} \in K[x, y].$$

More generally, for $r > 0$, define the *r-th difference quotient* as

$$\Phi^r F(x_0, \dots, x_r) = \frac{\Phi^{r-1} F(x_0, \dots, x_{r-1}) - \Phi^{r-1} F(x_0, \dots, x_{r-2}, x_r)}{x_{r-1} - x_r}.$$

One shows that $F \in R[x]$ if and only if $\Phi^r F(R^{r+1}) \subseteq R$ for all $r \geq 0$. (Hint: do the case $F(x) = cx^k$ for each $k$.)

# Divided differences

Again, let $R$ be a Dedekind domain with fraction field $K$. (On this slide, we only use that $R$ is a domain.)

For $F \in K[x]$, define the *difference quotient* of $F$ as

$$\Phi F(x,y) = \frac{F(x) - F(y)}{x - y} \in K[x,y].$$

More generally, for $r > 0$, define the *$r$-th difference quotient* as

$$\Phi^r F(x_0,\dots,x_r) = \frac{\Phi^{r-1}F(x_0,\dots,x_{r-1}) - \Phi^{r-1}F(x_0,\dots,x_{r-2},x_r)}{x_{r-1} - x_r}.$$

One shows that $F \in R[x]$ if and only if $\Phi^r F(R^{r+1}) \subseteq R$ for all $r \geq 0$. (Hint: do the case $F(x) = cx^k$ for each $k$.)

# Divided differences and $\mathfrak{p}$-orderings

Switch back to the local case: $R$ is a DVR with maximal ideal $\mathfrak{p}$.

Let $S \subseteq R$ be an infinite subset and let $r$ be a nonnegative integer. An *$r$-removed $\mathfrak{p}$-ordering* is a sequence $a_0, a_1, \ldots \in S$ in which $a_k$ is chosen to minimize the valuation of the ideal generated by $(a_k - a_{i_0}) \cdots (a_k - a_{i_{k-r-1}})$ for all $(k-r)$-element subsets $\{i_0, \ldots, i_{k-r-1}\} \subseteq \{0, \ldots, k-1\}$. Denote this ideal by $(k!)_{S,r}$.

**Theorem (Bhargava, 2009)**

*For $F \in K[x]$, we have $\Phi^k F(S^{k+1}) \subseteq R$ for $k = 0, \ldots, r$ if and only if $F = \sum_{k=0}^{\infty} F_k (x - a_0) \cdots (x - a_{k-1})$ with $F_k (k!)_{S,r} \subseteq R$ for all $k \geq 0$.*

Again, it follows that $(k!)_{S,r}$ is independent of all choices.

# Divided differences and $\mathfrak{p}$-orderings

Switch back to the local case: $R$ is a DVR with maximal ideal $\mathfrak{p}$.

Let $S \subseteq R$ be an infinite subset and let $r$ be a nonnegative integer. An *$r$-removed $\mathfrak{p}$-ordering* is a sequence $a_0, a_1, \ldots \in S$ in which $a_k$ is chosen to minimize the valuation of the ideal generated by $(a_k - a_{i_0}) \cdots (a_k - a_{i_{k-r-1}})$ for all $(k-r)$-element subsets $\{i_0, \ldots, i_{k-r-1}\} \subseteq \{0, \ldots, k-1\}$. Denote this ideal by $(k!)_{S,r}$.

**Theorem (Bhargava, 2009)**

*For $F \in K[x]$, we have $\Phi^k F(S^{k+1}) \subseteq R$ for $k = 0, \ldots, r$ if and only if $F = \sum_{k=0}^{\infty} F_k (x - a_0) \cdots (x - a_{k-1})$ with $F_k (k!)_{S,r} \subseteq R$ for all $k \geq 0$.*

Again, it follows that $(k!)_{S,r}$ is independent of all choices.

# Divided differences and $\mathfrak{p}$-orderings

Switch back to the local case: $R$ is a DVR with maximal ideal $\mathfrak{p}$.

Let $S \subseteq R$ be an infinite subset and let $r$ be a nonnegative integer. An *$r$-removed $\mathfrak{p}$-ordering* is a sequence $a_0, a_1, \ldots \in S$ in which $a_k$ is chosen to minimize the valuation of the ideal generated by $(a_k - a_{i_0}) \cdots (a_k - a_{i_{k-r-1}})$ for all $(k-r)$-element subsets $\{i_0, \ldots, i_{k-r-1}\} \subseteq \{0, \ldots, k-1\}$. Denote this ideal by $(k!)_{S,r}$.

**Theorem (Bhargava, 2009)**

*For $F \in K[x]$, we have $\Phi^k F(S^{k+1}) \subseteq R$ for $k = 0, \ldots, r$ if and only if $F = \sum_{k=0}^{\infty} F_k (x - a_0) \cdots (x - a_{k-1})$ with $F_k (k!)_{S,r} \subseteq R$ for all $k \geq 0$.*

Again, it follows that $(k!)_{S,r}$ is independent of all choices.

# Divided differences and $\mathfrak{p}$-orderings

Switch back to the local case: $R$ is a DVR with maximal ideal $\mathfrak{p}$.

Let $S \subseteq R$ be an infinite subset and let $r$ be a nonnegative integer. An *$r$-removed $\mathfrak{p}$-ordering* is a sequence $a_0, a_1, \ldots \in S$ in which $a_k$ is chosen to minimize the valuation of the ideal generated by $(a_k - a_{i_0}) \cdots (a_k - a_{i_{k-r-1}})$ for all $(k-r)$-element subsets $\{i_0, \ldots, i_{k-r-1}\} \subseteq \{0, \ldots, k-1\}$. Denote this ideal by $(k!)_{S,r}$.

**Theorem (Bhargava, 2009)**

*For $F \in K[x]$, we have $\Phi^k F(S^{k+1}) \subseteq R$ for $k = 0, \ldots, r$ if and only if $F = \sum_{k=0}^{\infty} F_k (x - a_0) \cdots (x - a_{k-1})$ with $F_k (k!)_{S,r} \subseteq R$ for all $k \geq 0$.*

Again, it follows that $(k!)_{S,r}$ is independent of all choices.

# Continuously differentiable functions of order $r$

Let $K$ be a local field with valuation ring $R$. Let $S \subseteq R$ be an infinite compact subset. We say that $f : S \to K$ is *continuously differentiable of order $r$* if for $k = 0, \dots, r$, the difference quotient $\Phi^k f$ extends to a continuous function on $S^k$ (i.e., over the *big diagonal*).

**Theorem (Bhargava, 2009)**

*Let $k!_{S,r}$ be any generator of $(k!)_{S,r}$ and define*

$$\binom{x}{k}_{S,r} := \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_{S,r}} \qquad (k = 0, 1, \dots).$$

*Then $f : S \to K$ is continuously differentiable of order $r$ if and only if $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_{S,r}$ for some $f_k \in K$ with $\lim_{k \to \infty} f_k = 0$.*

Again, for the proof it is convenient to reduce to considering $\mathfrak{p}$-orderings which are *proper* in a suitably modified sense.

# Continuously differentiable functions of order $r$

Let $K$ be a local field with valuation ring $R$. Let $S \subseteq R$ be an infinite compact subset. We say that $f : S \to K$ is *continuously differentiable of order r* if for $k = 0, \dots, r$, the difference quotient $\Phi^k f$ extends to a continuous function on $S^k$ (i.e., over the *big diagonal*).

**Theorem (Bhargava, 2009)**

*Let $k!_{S,r}$ be any generator of $(k!)_{S,r}$ and define*

$$\binom{x}{k}_{S,r} := \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_{S,r}} \qquad (k = 0, 1, \dots).$$

*Then $f : S \to K$ is continuously differentiable of order $r$ if and only if $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_{S,r}$ for some $f_k \in K$ with $\lim_{k\to\infty} f_k = 0$.*

Again, for the proof it is convenient to reduce to considering $\mathfrak{p}$-orderings which are *proper* in a suitably modified sense.

# Continuously differentiable functions of order $r$

Let $K$ be a local field with valuation ring $R$. Let $S \subseteq R$ be an infinite compact subset. We say that $f : S \to K$ is *continuously differentiable of order $r$* if for $k = 0, \dots, r$, the difference quotient $\Phi^k f$ extends to a continuous function on $S^k$ (i.e., over the *big diagonal*).

**Theorem (Bhargava, 2009)**

*Let $k!_{S,r}$ be any generator of $(k!)_{S,r}$ and define*

$$\binom{x}{k}_{S,r} := \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_{S,r}} \qquad (k = 0, 1, \dots).$$

*Then $f : S \to K$ is continuously differentiable of order $r$ if and only if $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_{S,r}$ for some $f_k \in K$ with $\lim_{k \to \infty} f_k = 0$.*

Again, for the proof it is convenient to reduce to considering $\mathfrak{p}$-orderings which are *proper* in a suitably modified sense.

# Polynomials with modulus

Let $R$ be a domain with fraction field $K$, let $\mathfrak{m}$ be an ideal of $R$, and let $S$ be a subset of $R$. We say that $f \in K[x]$ is *$R$-valued on $S$ of modulus* $\mathfrak{m}$ if

$$f(mx + a) \in R[x] \text{ for all } m \in \mathfrak{m}, a \in S.$$

Now take $R$ to be a discrete valuation ring and $\mathfrak{m} = \mathfrak{p}^h$. A *$\mathfrak{p}$-ordering of order $h$* is a sequence $a_0, a_1, \ldots \in S$ in which $a_k$ is chosen to minimize the valuation of the ideal $\prod_{i=0}^{k-1}(\mathfrak{p}^h, a_k - a_i)$. (That is, the valuation of each factor in the product is truncated down to $h$.) Denote this ideal by $(k!)_{S,h}$.

**Theorem (Bhargava, 2009)**

*For $F \in K[x]$, $F$ is $R$-valued on $S$ of modulus $\mathfrak{p}^h$ if and only if $F = \sum_{k=0}^{\infty} F_k(x - a_0)\cdots(x - a_{k-1})$ with $F_k(k!)_{S,h} \subseteq R$ for all $k \geq 0$.*

# Polynomials with modulus

Let $R$ be a domain with fraction field $K$, let $\mathfrak{m}$ be an ideal of $R$, and let $S$ be a subset of $R$. We say that $f \in K[x]$ is *$R$-valued on $S$ of modulus* $\mathfrak{m}$ if

$$f(mx + a) \in R[x] \text{ for all } m \in \mathfrak{m}, a \in S.$$

Now take $R$ to be a discrete valuation ring and $\mathfrak{m} = \mathfrak{p}^h$. A $\mathfrak{p}$*-ordering of order* $h$ is a sequence $a_0, a_1, \ldots \in S$ in which $a_k$ is chosen to minimize the valuation of the ideal $\prod_{i=0}^{k-1}(\mathfrak{p}^h, a_k - a_i)$. (That is, the valuation of each factor in the product is truncated down to $h$.) Denote this ideal by $(k!)_{S,h}$.

**Theorem (Bhargava, 2009)**

*For $F \in K[x]$, $F$ is $R$-valued on $S$ of modulus $\mathfrak{p}^h$ if and only if $F = \sum_{k=0}^{\infty} F_k(x - a_0) \cdots (x - a_{k-1})$ with $F_k(k!)_{S,h} \subseteq R$ for all $k \geq 0$.*

# Polynomials with modulus

Let $R$ be a domain with fraction field $K$, let $\mathfrak{m}$ be an ideal of $R$, and let $S$ be a subset of $R$. We say that $f \in K[x]$ is *$R$-valued on $S$ of modulus* $\mathfrak{m}$ if

$$f(mx + a) \in R[x] \text{ for all } m \in \mathfrak{m}, a \in S.$$

Now take $R$ to be a discrete valuation ring and $\mathfrak{m} = \mathfrak{p}^h$. A *$\mathfrak{p}$-ordering of order $h$* is a sequence $a_0, a_1, \ldots \in S$ in which $a_k$ is chosen to minimize the valuation of the ideal $\prod_{i=0}^{k-1}(\mathfrak{p}^h, a_k - a_i)$. (That is, the valuation of each factor in the product is truncated down to $h$.) Denote this ideal by $(k!)_{S,h}$.

Theorem (Bhargava, 2009)

*For $F \in K[x]$, $F$ is $R$-valued on $S$ of modulus $\mathfrak{p}^h$ if and only if $F = \sum_{k=0}^{\infty} F_k(x - a_0) \cdots (x - a_{k-1})$ with $F_k(k!)_{S,h} \subseteq R$ for all $k \geq 0$.*

# Locally analytic functions

Let $K$ be a local field with valuation ring $R$. Let $S \subseteq R$ be an infinite compact subset. We say that $f : S \to K$ is *locally analytic of order $h$* if for each $a \in S$, the restriction of $f$ to $S \cap (a + \mathfrak{p}^h)$ extends to some analytic function on $a + \mathfrak{p}^h$ (i.e., a function given by a convergent[5] power series).

**Theorem (Bhargava, 2009)**

*Let $k!_{S,h}$ be any generator of $(k!)_{S,h}$ and define*

$$\binom{x}{k}_{S,h} := \frac{(x-a_0)\cdots(x-a_{k-1})}{k!_{S,h}} \qquad (k = 0, 1, \dots).$$

*Then $f : S \to K$ is locally analytic of order $h$ if and only if $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_{S,h}$ for some $f_k \in K$ with $\lim_{k\to\infty} f_k = 0$.*

This extends a result of Amice (for sufficiently "regular" $S$).

[5] Meaning convergence on the ball over a completed algebraic closure of $K$.

# Locally analytic functions

Let $K$ be a local field with valuation ring $R$. Let $S \subseteq R$ be an infinite compact subset. We say that $f : S \to K$ is *locally analytic of order $h$* if for each $a \in S$, the restriction of $f$ to $S \cap (a + \mathfrak{p}^h)$ extends to some analytic function on $a + \mathfrak{p}^h$ (i.e., a function given by a convergent[5] power series).

**Theorem (Bhargava, 2009)**

*Let $k!_{S,h}$ be any generator of $(k!)_{S,h}$ and define*

$$\binom{x}{k}_{S,h} := \frac{(x - a_0)\cdots(x - a_{k-1})}{k!_{S,h}} \qquad (k = 0, 1, \dots).$$

*Then $f : S \to K$ is locally analytic of order $h$ if and only if $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_{S,h}$ for some $f_k \in K$ with $\lim_{k\to\infty} f_k = 0$.*

This extends a result of Amice (for sufficiently “regular” $S$).

[5] Meaning convergence on the ball over a completed algebraic closure of $K$.

# Locally analytic functions

Let $K$ be a local field with valuation ring $R$. Let $S \subseteq R$ be an infinite compact subset. We say that $f : S \to K$ is *locally analytic of order $h$* if for each $a \in S$, the restriction of $f$ to $S \cap (a + \mathfrak{p}^h)$ extends to some analytic function on $a + \mathfrak{p}^h$ (i.e., a function given by a convergent[5] power series).

**Theorem (Bhargava, 2009)**

*Let $k!_{S,h}$ be any generator of $(k!)_{S,h}$ and define*

$$\binom{x}{k}_{S,h} := \frac{(x - a_0) \cdots (x - a_{k-1})}{k!_{S,h}} \qquad (k = 0, 1, \dots).$$

*Then $f : S \to K$ is locally analytic of order $h$ if and only if $f(x) = \sum_{k=0}^{\infty} f_k \binom{x}{k}_{S,h}$ for some $f_k \in K$ with $\lim_{k\to\infty} f_k = 0$.*

This extends a result of Amice (for sufficiently "regular" $S$).

[5] Meaning convergence on the ball over a completed algebraic closure of $K$.

# Contents

# Conclusions

There is a robust link between integrality properties of polynomials and topological/analytic properties of functions on local fields. The strategy of $\mathfrak{p}$-orderings provides an approach to dealing with both in surprising generality.

Are there more results to be found in this direction? For example, can one extend to some noncommutative rings, such as Iwasawa algebras (completed group algebras of $p$-adic Lie groups)?

# Conclusions

There is a robust link between integrality properties of polynomials and topological/analytic properties of functions on local fields. The strategy of $\mathfrak{p}$-orderings provides an approach to dealing with both in surprising generality.

Are there more results to be found in this direction? For example, can one extend to some noncommutative rings, such as Iwasawa algebras (completed group algebras of $p$-adic Lie groups)?

# References


Z. Chen, On polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$, *Discrete Math.* **137** (1995), 137–145.

M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly* **107** (2000), 783–799.

M. Bhargava and K.S. Kedlaya, Continuous functions on compact subsets of local fields, *Acta Arith.* **91** (1999), 191–198.

M. Wood, *P*-orderings: a metric viewpoint and the non-existence of simultaneous orderings, *J. Num. Theory* **99** (2003), 36–56.

M. Bhargava, On *P*-orderings, rings of integer-valued polynomials, and ultrametric analysis, *J. Amer. Math. Soc.* **22** (2009), 963–993.

P.-J. Cahen, J.-L. Chabert, and K.S. Kedlaya, Bhargava's early work: *P*-orderings and generalized factorials, *Amer. Math. Monthly*, to appear.