# About polynomials whose divided differences are integer valued on prime numbers

Jean-Luc Chabert

ICM 2012, 11-14 March, Al Ain

**Abstract**

We show here how to construct bases of the $\mathbb{Z}$-module $\mathrm{Int}^1(\mathbb{P},\mathbb{Z})$ of polynomials that are integer-valued on the prime numbers together with their finite divided difference, that is,

$$\mathrm{Int}^1(\mathbb{P},\mathbb{Z}) = \left\{ f \in \mathbb{Q}[x] \mid \forall p,q \in \mathbb{P} \;\; f(p) \in \mathbb{Z} \text{ and } \frac{f(p)-f(q)}{p-q} \in \mathbb{Z} \right\}.$$

**Keywords: Integer-valued polynomials, divided differences, prime numbers**

## 1 Motivation: polynomial approximation

A motivation for the study of polynomials which are integer-valued together with their divided differences could be polynomial aproximations.

### 1.1 Approximation in $\mathcal{C}(S,\mathbb{Q}_p)$

Weierstrass theorem [13] about the polynomial approximation of real continuous functions is well known:

**Proposition 1 (Weierstrass, 1885)** *For every compact subset $S$ of $\mathbb{R}$, the ring of polynomial functions $\mathbb{R}[x]$ is dense in the Banach space $\mathcal{C}(S,\mathbb{R})$ of continuous functions from $S$ to $\mathbb{R}$ for the uniform convergence topology.*

There is an ultrametric analog [8]:

**Proposition 2 (Dieudonné, 1944)** *For every compact subset $S$ of the field $\mathbb{Q}_p$ of $p$-adic numbers, the ring of polynomials functions $\mathbb{Q}[x]$ is dense in the Banach space $\mathcal{C}(S,\mathbb{Q}_p)$ of ultrametric continuous functions from $S$ to $\mathbb{Q}_p$ for the uniform convergence topology.*

There exists a version proved by Kaplansky in 1950 [10] where the field $\mathbb{Q}_p$ may be replaced by any local field $K$. But, for sake of simplicity, we restrict our study to the field $\mathbb{Q}_p$. In the case where $S$ is the whole ring $\mathbb{Z}_p$ of $p$-adic integers, we have explicit formulas [11]:

**Proposition 3 (Malher, 1958)** *Every $\varphi \in \mathcal{C}(\mathbb{Z}_p,\mathbb{Q}_p)$ can be expanded as a series of the form*

$$\varphi(x) = \sum_{n=0}^{\infty} c_n \, \frac{x(x-1)\cdots(x-n+1)}{n!} \;\; \textit{where } c_n \in \mathbb{Q}_p \textit{ and } v_p(c_n) \to +\infty.$$

*Moreover,*

$$\inf_{x\in\mathbb{Z}_p} v_p(\varphi(x)) = \inf_{n\geq 0} v_p(c_n).$$

One says that the *binomial polynomials* $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$ form an *orthonormal basis* of the Banach ultrametric space $\mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p)$. About theses binomial polynomials, recall that they form a basis of the $\mathbb{Z}$-module of integer-valued polynomials on $\mathbb{Z}$:

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] \mid f(\mathbb{Z}) \subseteq \mathbb{Z}\}$$

and also of the $\mathbb{Z}_p$-module of integer-valued polynomials on $\mathbb{Z}_p$:

$$\mathrm{Int}(\mathbb{Z}_p) = \{f \in \mathbb{Q}_p[x] \mid f(\mathbb{Z}_p) \subseteq \mathbb{Z}_p\}.$$

By the way, note that

$$\mathrm{Int}(\mathbb{Z}_p) = \mathbb{Q}_p[x] \cap \mathcal{C}(\mathbb{Z}_p, \mathbb{Z}_p).$$

Malher's formulas have been generalized to any subset $S$ of $\mathbb{Z}_p$ [4]. Note that

$$\mathrm{Int}(S, \mathbb{Z}_p) = \{f \in \mathbb{Q}_p[x] \mid f(S) \subseteq \mathbb{Z}_p\} = \mathbb{Q}_p[x] \cap \mathcal{C}(S, \mathbb{Z}_p).$$

**Theorem 4 (Bhargava and Kedlaya, 1999)** *Let $S$ be an infinite subset of $\mathbb{Z}_p$. Let $\{a_n\}_{n\geq 0}$ be a $p$-ordering of $S$ and, for $n \geq 0$, consider the associated* generalized binomial polynomials

$$\binom{x}{n}_{\{a_k\}} = \prod_{k=0}^{n-1} \frac{x - a_k}{a_n - a_k}.$$

*Then, the sequence $\left\{\binom{x}{n}_{\{a_k\}}\right\}_{n\geq 0}$ is*

- *a basis of the $\mathbb{Z}_p$-module* $\mathrm{Int}(S, \mathbb{Z}_p)$
- *an orthonormal basis of the Banach space $\mathcal{C}(S, \mathbb{Q}_p)$*

This last assertion means that every $\varphi \in \mathcal{C}(S, \mathbb{Q}_p)$ can be expanded as a series of the form

$$\varphi = \sum_{n\geq 0} c_n \binom{x}{n}_{\{a_k\}} \quad \text{with } c_n \in \mathbb{Q}_p \text{ and } v_p(c_n) \to +\infty.$$

We will recall below what is this notion of $p$-ordering introduced by Bhargava [2].

## 1.2 Approximation in $\mathcal{C}^1(S, \mathbb{Q}_p)$

This was the state of the art at the end of the last century. In a recent paper, Bhargava [3] extends this approximation result to function of class $\mathcal{C}^r$. For sake of simplicity, we restrict our study to functions of class $\mathcal{C}^1$. What is an ultrametric function of class $\mathcal{C}^1$? To say that the function is just a continuously differentiable function is not a good choice in ultrametric analysis because with such a definition we don't have the local invertibility theorem (*cf.* Schikhof [12]). We have to consider divided differences where, following Cauchy [5], the *divided difference* of $f : S \to \mathbb{Q}_p$ is the function of two variables

$$\Phi(f) : (x, y) \in S \times S \setminus \Delta \mapsto \Phi(f)(x, y) = \frac{f(x) - f(y)}{x - y} \in \mathbb{Q}_p$$

where $\Delta = \{(x,x) \mid x \in S\}$.

**Definition** Assume that $S$ has no isolated point. A function $f : S \to \mathbb{Q}_p$ is said *of classe* $\mathcal{C}^1$ on $S$ if $\Phi(f)$ may be extended continuously to $S \times S$.

If $f$ is of classe $\mathcal{C}^1$ on $S$ then, for every $x \in S$, we have:

$$f'(x) = \lim_{(y,z)\to(x,x)} \Phi(f)(y,z)$$

and $f'$ is continuous on $S$. Note also that

$$\mathcal{C}^1(S,\mathbb{Z}_p) \cap \mathbb{Q}_p[x] = \{f \in \mathbb{Q}_p[x] \mid f(S) \subseteq \mathbb{Z}_p, \Phi(f)(S \times S) \subseteq \mathbb{Z}_p\}.$$

So that we consider the ring

$$\mathrm{Int}^1(S,\mathbb{Z}_p) = \left\{ f \in \mathbb{Q}_p[x] \mid \forall s,t \in S \quad f(s) \in \mathbb{Z}_p \text{ and } \frac{f(s)-f(t)}{s-t} \in \mathbb{Z}_p \right\}$$

formed by the polynomials which are integer-valued on $S$ together with their first divided difference. Bhargava's result [3] is then the following:

**Theorem 5 (Bhargava, 2009)** *Let $S$ be a subset of $\mathbb{Z}_p$ without any isolated point. Every basis of the $\mathbb{Z}_p$-module $\mathrm{Int}^1(S,\mathbb{Z}_p)$ is an orthonormal basis of the Banach space $\mathcal{C}^1(S,\mathbb{Q}_p)$.*

It is the reason why we are interested in bases of the ring of polynomials $\mathrm{Int}^1(S,\mathbb{Z}_p)$. From now on, we may forget all what has been said: we just need to know what is the ring $\mathrm{Int}^1(S,\mathbb{Z}_p)$.

## 2 Bases of the $\mathbb{Z}_p$-module $\mathrm{Int}^1(S,\mathbb{Z}_p)$

Let us recall first how we can construct bases of the $\mathbb{Z}_p$-module $\mathrm{Int}(S,\mathbb{Z}_p)$.

### 2.1 Bases of $\mathrm{Int}(S,\mathbb{Z}_p)$

**Definition** [2] A *p-ordering* of $S$ is a sequence $\{a_n\}_{n\geq 0}$ of elements of $S$ where $a_0$ may be chosen arbitrarily and, for $n \geq 1$, $a_n$ is chosen in such a way that

$$v_p\left(\prod_{k=0}^{n-1}(a_n - a_k)\right) = \inf_{x\in S} v_p\left(\prod_{k=0}^{n-1}(x - a_k)\right)$$

where $v_p$ denotes the $p$-adic valuation on $\mathbb{Q}_p$.

Recall that, with this definition of a $p$-ordering, Bhargava and Kedlaya's theorem (Theorem 4) says that, if $\{a_n\}$ is a $p$-ordering of $S$, then, the associated sequence of polynomials $\left\{\binom{x}{n}_{\{a_k\}}\right\}$ is a basis of $\mathbb{Z}_p$-module $\mathrm{Int}(S,\mathbb{Z}_p)$.

### 2.2 Bases of $\mathrm{Int}^1(S,\mathbb{Z}_p)$

For the study of polynomials which are integer-valued with their divided differences, Bhargava introduced a generalized notion of $p$-ordering. Let us recall the notion which is useful for the case of the first divided difference.

**Definition** A 1-*removed p-ordering* of $S$ is a sequence $\{a_n\}_{n\geq 0}$ of elements of $S$ where $a_0, a_1$ are chosen arbitrarily and, for $n \geq 2$, the element $a_n$ is chosen in such a way that, for some index $i_n$, we have:

$$v_p\left(\prod_{0\leq k<n,\, k\neq i_n}(a_n - a_k)\right) = \inf_{x\in S,\, 0\leq j<n} v_p\left(\prod_{0\leq k<n,\, k\neq j}(x - a_k)\right).$$

**Theorem 6 (Bhargava, 2009)** *If $\{a_n\}_{n\in\mathbb{N}}$ is a* 1*-removed p-ordering of $S$, then the associated sequence of* generalized binomial polynomials*:*

$$\binom{x}{n}^1_{\{a_k\}} = \frac{(x-a_0)\dots(x-a_{i_n})\dots(x-a_{n-1})}{(a_n-a_0)\dots\widehat{(a_n-a_{i_n})}\dots(a_n-a_{n-1})}$$

*is a basis of the $\mathbb{Z}_p$-module* $\mathrm{Int}^1(S,\mathbb{Z}_p)$.

In fact we are not interested in the exact value of the denominator of the leading term of the polynomial $\binom{x}{n}^1_{\{a_k\}}$, but in its valuation that we denote by $w^1_S(n)$.

**Corollary 7** *The integer*

$$w^1_S(n) = v\left(\prod_{0\leq k\leq n-1,\, k\neq i_n}(a_n - a_k)\right)$$

*does not depend on the choice of the* 1*-removed p-ordering of $S$.*

## 3 Explicit formulas for $w^1_S(n)$

In 2010, Keith Johnson [9] gave an explicit formula for $w^1_{\mathbb{Z}_p}(n)$. In 2011, S. Evrard, Y. Fares, and myself [7], we gave explicit formulas in the case where $S$ is a *regular subset* of $\mathbb{Z}_p$ in Amice's sense, that is when, for every $k$, each class of $S$ modulo $p^k$ contains the same number of classes of $S$ modulo $p^{k+1}$.

**Proposition 8** *Let $S$ be a regular subset of $\mathbb{Z}_p$ and, for every $k$, let $q_k$ denotes the number of classes of $S$ mod $p^k$. Then*

$$w^1_S(n) = \sum_{k=1}^{\infty}\left\lfloor\frac{n}{q_k}\right\rfloor - t \quad \textit{where } q_t \leq n < q_{t+1}$$

Let us recall the corresponding formula for the ring $\mathrm{Int}(S,\mathbb{Z}_p)$:

$$w_S(n) = \sum_{k=1}^{\infty}\left\lfloor\frac{n}{q_k}\right\rfloor.$$

Moreover [7],

**Proposition 9** *If $S$ is a regular subset of $\mathbb{Z}_p$, then every strong p-ordering of $S$ is a* 1*-removed p-ordering of $S$.*

Note that strong $p$-orderings of regular subsets may be easily described.

**Example** Let $S = \mathbb{Z} \setminus p\mathbb{Z}$ be the set formed by the integers that are not divisible by $p$. Then, $q_k = (p-1)p^{k-1}$, and the previous formula leads to

$$w^1_{\mathbb{Z}\setminus p\mathbb{Z}}(n) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{(p-1)p^{k-1}} \right\rfloor - t \quad \text{for } p^{t-1} \leq \frac{n}{p-1} < p^t.$$

Moreover, we know that the natural increasing sequence of integers that are not divisible by $p$ is a strong $p$-ordering of $S$. We then may describe the first terms of a basis of $\mathrm{Int}^1(\mathbb{Z} \setminus p\mathbb{Z}, \mathbb{Z}_p)$ for every prime $p$. We give here the first terms when $p$ is equal to 2 and to 3.

$$p = 2: \quad 1, X-1, \frac{(X-1)(X-3)}{2}, \frac{(X-1)(X-3)(X-5)}{4}$$
$$\frac{(X-1)(X-3)(X-5)(X-7)}{16}, \frac{(X-1)(X-3)(X-5)(X-7)(X-9)}{32}, \dots$$
$$p = 3: \quad 1, X-1, (X-1)(X-2), (X-1)(X-2)(X-4),$$
$$\frac{(X-1)(X-2)(X-4)(X-5)}{3}, \frac{(X-1)(X-2)(X-4)(X-5)(X-7)}{3}, \dots$$

## 4 Globalization : bases of the $\mathbb{Z}$-module $\mathrm{Int}^1(\mathbb{P}, \mathbb{Z})$

For every subset $S$ of $\mathbb{Z}$ and every prime number $p$, one has:

$$\mathrm{Int}^1(S, \mathbb{Z})_p = \mathrm{Int}^1(S, \mathbb{Z}_{(p)}).$$

This equality says that integer-valued polynomials and divided differences behave well with respect to localization. Thus, we may globalize the previous results by means of the chinese remainder theorem. Let us show how we can do this in the case where $S = \mathbb{P}$ is the set formed by the prime numbers, that is, for the ring:

$$\mathrm{Int}^1(\mathbb{P}, \mathbb{Z}) = \left\{ f \in \mathbb{Q}[x] \mid \forall p, q \in \mathbb{P} \;\; f(p) \in \mathbb{Z} \text{ and } \frac{f(p) - f(q)}{p - q} \in \mathbb{Z} \right\}.$$

First, note that $\mathbb{P}$ is not a regular subset of $\mathbb{Z}$. This is not a surprise, but thanks to Dirichlet's theorem on primes in arithmetic progressions, we know that, for every prime $p$, the polynomial closure of $\mathbb{P}$ in $\mathbb{Z}_p$ is $X_p = \{p\} \cup (\mathbb{Z}_p \setminus p\mathbb{Z}_p)$ (*cf.* [6], this implies in particular that

$$\mathrm{Int}(\mathbb{P}, \mathbb{Z}_p) = \mathrm{Int}(X_p, \mathbb{Z}_p).$$

which means that a polynomial is integer-valued on the primes if and only if it is integer-valued on the set $X_p$. Moreover, we may verify that, things work well also with respect to divided differences, that is, that we also have the following equality:

$$\mathrm{Int}^1(\mathbb{P}, \mathbb{Z}_p) = \mathrm{Int}^1(X_p, \mathbb{Z}_p),$$

that is,

$$\forall f \in \mathrm{Int}^1(\mathbb{P}, \mathbb{Z}_p) \;\; \forall x, y \in X_p \quad \frac{f(x) - f(y)}{x - y} \in \mathbb{Z}_p.$$

And, now we have to consider a subset $X_p$ of $\mathbb{Z}_p$ which is quite a regular subset. We may easily check that the action of the singular element $p$ on the function $w_{X_p}$ is just a shift:

$$w^1_{X_p}(n) = w^1_{\mathbb{Z}\setminus p\mathbb{Z}}(n-1).$$

Then, putting all the previous results together, we may globalize and construct a basis of the $\mathbb{Z}$-module $\mathrm{Int}^1(\mathbb{P}, \mathbb{Z})$. Here are the first terms:

**Proposition 10** *The $\mathbb{Z}$-module*

$$\mathrm{Int}^1(\mathbb{P},\mathbb{Z}) = \left\{ f \in \mathbb{Q}[x] \mid \forall p,q \in \mathbb{P} \;\; f(p) \in \mathbb{Z} \text{ and } \frac{f(p)-f(q)}{p-q} \in \mathbb{Z} \right\}$$

*admits a basis whose first terms are the following*

$$1\ ,\ X-1,\ (X-1)(X-2)\ ,\ \frac{1}{2}(X-1)(X-2)(X-3)\ ,$$

$$\frac{1}{4}(X-1)(X-2)(X-3)(X-5)\ ,\ \frac{1}{48}(X-1)(X-2)(X-3)(X-5)(X-7),\ldots$$

Let us look at the sequence of denominators, that is, the denominators of the polynomials of $\mathrm{Int}^1(\mathbb{P},\mathbb{Z})$.

**Proposition 11** *If $\frac{1}{d(n)}$ denotes a generator of the ideal formed by the leading coefficients of the polynomials that are integer-valued on $\mathbb{P}$ together with their first divided difference, then*

$$d(n) = \prod_{p\in\mathbb{P}} p^{w^1_{\mathbb{Z}\setminus p\mathbb{Z}}(n-1)}.$$

*The first terms of this sequence are the following:*

$$1, 1, 1, 2, 4, 48, 96, 1152, 2304, 276480, \ldots$$

This sequence does not yet appear on *The On-Line Encyclopedia of Integer Sequences*. Let us recall that, fifteen years ago, the similar sequence for the polynomials of the ring $\mathrm{Int}(\mathbb{P},\mathbb{Z})$ was not on this Encyclopedia of Integer Sequences, but it turns out that it appears in many combinatorial questions. In particular, it is the Minkowski sequence $M_n$ where $M_n$ denotes the least common multiple of the orders of finite subgroups of $GL_n(\mathbb{Q})$.

## References


[1] Y. Amice, Interpolation $p$-adique, *Bull. Soc. Math. France* **92** (1964), 117–180.

[2] M. Bhargava, $P$-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. reine angew. Math.* **490** (1997), 101–127.

[3] M. Bhargava, On $P$-orderings, Integer-Valued Polynomials, and Ultrametric Analysis, *J. Amer. Math. Soc.* **22** (2009), 963–993.

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

[5] L.-A. Cauchy, Sur les fonctions interpolaires, *Comptes rendus de l'Académie des Sciences* **XI** (16 novembre 1840), 775–789.

[6] J.-L. Chabert, S. Chapman, and W. Smith, A Basis for the Ring of Polynomials Integer-Valued on Prime Numbers, in *Factorization in integral domains*, 271-284, Lecture Notes in Pure and Appl. Math., **189**, Dekker, New York, 1997.

[7] J.-L. Chabert, S. Evrard, and Y. Fares, Regular Subsets of valued Fields and Bhargava's $v$-orderings, preprint.

[8] J. Dieudonné, Sur les fonctions continues p-adiques, *Bull. Sci. Math.*, 2ème série. **68** (1944), 79–95.

[9] K. Johnson, Computing $r$-removed $P$-orderings and $P$-orderings of order $h$, *Actes des rencontres du C.I.R.M.* **2** n°2 (2010), 33–40.

[10] I. Kaplansky, The Weierstrass theorem in fields with valuations, *Proc. Amer. Math. Soc.* **1** (1950), 356–357.

[11] K. Mahler, An Interpolation Series for Continuous Functions of a $p$-adic Variable, *J. reine angew. Math.* **199** (1958), 23–34 and **208** (1961), 70–72.

[12] W. Schikhof, *Ultrametric Calculus, An introduction to p-adic Analysis*, Cambridge University Press, 1984.

[13] K. Weierstrass, Über die analytische Darstellbarkeit sogennanter willkurlicher Functionen reeller Argumente, *Sitzungsberichte der Konigl. Preuss. Akad. Wissenschaften Berlin* (1885), 633–639.

J.-L. Chabert
LAMFA UMR 7352
University of Picardie
80039 Amiens, France
jean-luc.chabert@u-picardie.fr