

SOLUTIONS OF POLYNOMIAL EQUATIONS IN SEVERAL VARIABLES MODULO A PRIME POWER

ARNAUD BODIN AND CHRISTIAN DROUIN

ABSTRACT. We explain how to obtain the set of solutions of a multivariate polynomial equation modulo a power of a prime number. These solutions are determined by a tree, called the *trunk*, which makes it possible to reconstruct all solutions. We apply these methods to determine the number of solutions, without having to enumerate them. We also illustrate these techniques by proving a simple case of Igusa's theorem: the Poincaré series associated with a polynomial in two separated variables is rational.

1. INTRODUCTION

1.1. Objectives

The main objective is to explain how to solve polynomial equations modulo an integer n :

$$(1) \quad P(x_1, \dots, x_n) \equiv 0 \pmod{n}.$$

The first step consists in applying the Chinese remainder theorem in order to reduce to the case where the modulus is a power of a prime number. Indeed, if $n = p_1^{e_1} \cdots p_r^{e_r}$, then the solutions of (1) are the solutions of

$$(2) \quad P(x_1, \dots, x_n) \equiv 0 \pmod{p_i^{e_i}} \quad \text{for all } 1 \leq i \leq r.$$

In the remainder of the paper, we will consider only one of these equations, where p is a prime number and $e \geq 1$:

$$(3) \quad P(x_1, \dots, x_n) \equiv 0 \pmod{p^e}$$

For $e = 1$, $\mathbb{Z}/p\mathbb{Z}$ is a field; in one variable, the number of solutions of (3) is bounded by the degree d of the polynomial, and in several variables by dp^{n-1} via the Schwartz–Zippel lemma. The main difficulty we will encounter is that for $e \geq 2$, $\mathbb{Z}/p^e\mathbb{Z}$ is not an integral domain, and therefore, even in one variable, the number of solutions can be much larger than the degree.

The one-variable case, based on Schmidt and Stewart [15], was studied in detail by the authors in [2]: it is explained there how to obtain and count all solutions of an equation $P(x) \equiv 0 \pmod{p^e}$ using a *trunk*, which makes it possible to compute the *solution tree*. One will also find in that article many examples in one variable, useful to understand before studying the multivariate case.

1.2. Solutions modulo p^e

It is surprising that these notions generalize without difficulty to equations in several variables, of course with some adaptations. We will thus define the notions of *trunk*, *thickness*, and *tree-top function* (with respective notations Trunk , t , φ). All these notions are defined in Section 2. This will allow us to make all solutions explicit; see Theorem 2.8.

Date: February 24, 2026.

2020 Mathematics Subject Classification. Primary 11A07; Sec. 11D45, 11S05.

Key words and phrases. Polynomial, Congruence, Tree, Poincaré series.

If one only wishes to count the solutions, without enumerating them one by one, here is a formula (Theorem 4.1), which will be proved in Section 4.

Theorem 1.1. *Let $P \in \mathbb{Z}[x_1, \dots, x_n]$. The number N_e of solutions of the equation $P(x_1, \dots, x_n) \equiv 0 \pmod{p^e}$ in $(\mathbb{Z}/p^e\mathbb{Z})^n$ is:*

$$N_e = \sum_{\substack{(\mathbf{r}, k) \in \text{Trunk}(P) \\ \varphi(\mathbf{r}, k) - t_k < e \leq \varphi(\mathbf{r}, k)}} p^{n(e-k)}.$$

1.3. The Poincaré series

Recall that N_e denotes the number of solutions of the equation $P(x_1, \dots, x_n) \equiv 0 \pmod{p^e}$. The *Poincaré series* is the generating series:

$$S(T) = \sum_{e \geq 0} N_e \frac{T^e}{p^{ne}}$$

(with $N_0 = 1$).

The celebrated theorem of Igusa [12] asserts that this series is in fact a rational fraction in T . It was originally a conjecture of Borewicz–Šafarevič [4]. Another proof was given by Denef (see for instance [7], see also the survey [14]).

A recent work [6] establishes Igusa’s theorem in a very general framework, relying on a powerful algorithmic approach. See also the thesis [5]. In the present article, we deliberately focus on the special case of two variables, and more precisely on the situation of a separated polynomial of the form $F(x) + G(y)$, for which we present an explicit computation of the rational fraction.

In the case of a univariate polynomial, the detailed study of a tree, as well as the algorithm we use, which we call the *trunk algorithm* or *thickness algorithm*, appears in Schmidt and Stewart [15], in Zúñiga-Galindo [16], in Berthomieu, Lecerf and Quintin [1], and very explicitly in Kopp, Randall, Rojas and Zhu [13], as well as in Dwivedi, Mittal and Saxena [8, 9, 10].

Computations of the Poincaré function in special cases have been treated by different methods, for example, among others, by [11] and [3].

Most of the existing studies are technical and difficult. We propose to illustrate the techniques developed here in order to give a simple proof of this result of Igusa in the special case of two separated variables.

Theorem 1.2. *Let p be a prime number. Let $P(x, y) = F(x) + G(y) \in \mathbb{Z}[x, y]$ be a separated polynomial in two variables ($n = 2$). Then the Poincaré series is a rational fraction:*

$$S(T) = \sum_{e \geq 0} N_e \frac{T^e}{p^{2e}} \in \mathbb{Q}[T].$$

Moreover, the expression as a rational fraction could be computed from the trunk; here we will do so in practice only for certain special cases. Everything concerning Poincaré series and the proof of this result is contained in Section 4 and the following sections.

In the appendix, we provide the detailed example of $P(x, y) = x^2 - y^3$ and of its solutions modulo p . One finds there the computation of the trunk, of the Poincaré series, and of the number of solutions of $x^2 - y^3 \equiv 0 \pmod{p^e}$.

2. THE TRUNK

Fix a prime integer p . Let \mathbf{Z} denote either the ring \mathbb{Z} of integers or the ring \mathbb{Z}_p of p -adic integers. Let $P(x_1, \dots, x_n)$ be a polynomial in $n \geq 1$ variables with coefficients in \mathbf{Z} . We write $\mathbf{x} = (x_1, \dots, x_n)$.

2.1. Thickness

Definition 2.1. The **thickness** of $P(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}]$ at the point $\mathbf{x}_0 \in \mathbb{Z}^n$ is the largest integer t such that there exists $Q(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}]$ satisfying:

$$P(\mathbf{x}_0 + p\mathbf{x}) = p^t Q(\mathbf{x}).$$

The polynomial $Q(\mathbf{x})$ is then called the **successor** of P at \mathbf{x}_0 .

The thickness t is positive if and only if $\mathbf{x}_0 \in \mathbb{Z}^n$ is a solution of $P(\mathbf{x}) \equiv 0 \pmod{p}$.

Throughout the remainder of the article, we shall assume that $P(\mathbf{x})$ is p -primitive (i.e., not all coefficients are divisible by p). This can be done without loss of generality: indeed, if $P(\mathbf{x})$ were not p -primitive, we would write $P(\mathbf{x}) = p^{t_0} P_0(\mathbf{x})$ where P_0 is p -primitive. Anticipating what follows, one would then assign the thickness t_0 to the vertex $(\mathbf{0}, 0)$ of the trunk, and add the value t_0 to the definition of the tree-top function in order to ensure the validity of the statements.

2.2. Solution tree

Definition 2.2. The **p -adic congruence tree** Ω_p is given by the *vertices*:

$$\Omega_p = \left\{ (\mathbf{x}, e) \mid \mathbf{x} \in (\mathbb{Z}/p^e\mathbb{Z})^n, e \geq 0 \right\}.$$

Two vertices (\mathbf{x}, e) and $(\mathbf{x}', e+1)$ are connected by an *edge* if and only if $\mathbf{x}' \equiv \mathbf{x} \pmod{p^e}$, that is, $x'_i \equiv x_i \pmod{p^e}$ for all $i = 1, \dots, n$.

In this way, we endow Ω_p with a tree structure. The root is the vertex $(\mathbf{0}, 0)$. From each vertex emanate exactly p^n outgoing edges.

Remark 2.3. We sometimes use the natural identification of $\mathbb{Z}/m\mathbb{Z}$ with $\llbracket 0, m-1 \rrbracket$. We denote by $k \% m$ the remainder of the Euclidean division of k by m .

In the one-variable case ($n = 1$), a finite path in the p -adic congruence tree Ω_p starting from the root corresponds to the p -adic expansion of an integer $N \in \mathbb{Z}$ associated with the terminal vertex:

$$N = a_0 + a_1p + \dots + a_kp^k$$

where $a_i \in \llbracket 0, p-1 \rrbracket$. The p possible values for a_i correspond to the p outgoing edges from a vertex. An infinite path in Ω_p corresponds to a p -adic integer $N \in \mathbb{Z}_p$ via its expansion:

$$N = a_0 + a_1p + \dots + a_kp^k + \dots$$

In the case of n variables, one works componentwise: a finite path in Ω_p corresponds to $(N_1, \dots, N_n) \in \mathbb{Z}^n$, and an infinite path to $(N_1, \dots, N_n) \in \mathbb{Z}_p^n$.

Definition 2.4. The **solution tree** is defined by

$$\text{Tree}(P) = \left\{ (\mathbf{x}, e) \in \Omega_p \mid P(\mathbf{x}) \equiv 0 \pmod{p^e} \right\}.$$

It is a (finite or infinite) subtree of Ω_p containing the root.

We again refer to the exposition [2] for further explanations, examples, and figures.

2.3. Trunk

The trunk is a tree of Ω_p that makes it possible to reconstruct the solution tree $\text{Tree}(P)$. It is in fact a subtree of $\text{Tree}(P)$, which may also be finite or infinite, but is simpler in the sense that it contains far fewer vertices.

Definition 2.5. The **trunk** of $P(\mathbf{x}) \in \mathbf{Z}[\mathbf{x}]$, denoted by $\text{Trunk}(P)$, is defined recursively as follows:

- *Initialization.* The root $(\mathbf{0}, 0)$ is an element of the trunk (this vertex has no thickness). The polynomial attached to this vertex is $P(\mathbf{x})$.

- *Heredity.* Suppose that (\mathbf{r}, k) is a vertex of the trunk attached to a polynomial $P_k(\mathbf{x})$. We construct the vertices of height $k + 1$ attached to this vertex. Consider the equation $P_k(\mathbf{x}) \equiv 0 \pmod{p}$. For each of its solutions $\mathbf{r}_k \in (\mathbb{Z}/p\mathbb{Z})^n$, we compute the decomposition associated with the thickness $P_k(\mathbf{r}_k + p\mathbf{x}) = p^{t_{k+1}}P_{k+1}(\mathbf{x})$. Then $(\mathbf{r} + p^k\mathbf{r}_k, k + 1)$ is a new element of the trunk. We associate to it the thickness t_{k+1} and the polynomial P_{k+1} .

Thus, a vertex of the trunk at height k is defined by an element $\mathbf{r} = \mathbf{r}_0 + p\mathbf{r}_1 + \cdots + p^{k-1}\mathbf{r}_{k-1}$, where $\mathbf{r}_i \in \llbracket 0, p - 1 \rrbracket^n$ ($1 \leq i \leq k - 1$). The outgoing edges are associated with the solutions \mathbf{r}_k of $P_k(\mathbf{x}) \equiv 0 \pmod{p}$. In what follows, we will essentially consider the trunk as a tree weighted by a thickness at each vertex.

2.4. Tree-top function

Definition 2.6. Let $(\mathbf{r}, k) \in \text{Trunk}(P)$. The **tree-top function** at this vertex is defined by:

$$\varphi(\mathbf{r}, k) = t_1 + \cdots + t_k$$

where t_1, \dots, t_k are the thicknesses of the vertices along the path connecting the vertex (\mathbf{r}, k) to the root $(\mathbf{0}, 0)$.

Lemma 2.7. *There exists a decomposition:*

$$P(\mathbf{r} + p^k\mathbf{x}) = p^{\varphi(\mathbf{r}, k)}Q(\mathbf{x})$$

where $Q(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$.

Proof. Let $\mathbf{r} = \mathbf{r}_0 + p\mathbf{r}_1 + \cdots + p^{k-1}\mathbf{r}_{k-1}$ be the p -adic decomposition of \mathbf{r} , obtained componentwise for each of the n coordinates. We have $P(\mathbf{r}_0 + p\mathbf{x}) = p^{t_1}P_1(\mathbf{x})$, $P_1(\mathbf{r}_1 + p\mathbf{x}) = p^{t_2}P_2(\mathbf{x})$, hence $P(\mathbf{r}_0 + p\mathbf{r}_1 + p^2\mathbf{x}) = p^{t_1+t_2}P_2(\mathbf{x})$, and the stated formula follows by induction. \square

2.5. From the trunk to the tree

By definition:

$$(\mathbf{x}_0, e) \in \text{Tree}(P) \iff P(\mathbf{x}_0) \equiv 0 \pmod{p^e}.$$

Here is how to compute all solutions from the trunk; this is a multivariate generalization of [2]:

Theorem 2.8.

$$P(\mathbf{x}_0) \equiv 0 \pmod{p^e} \iff \text{there exists } (\mathbf{r}, k) \in \text{Trunk}(P) \text{ such that } \begin{cases} \mathbf{x}_0 \equiv \mathbf{r} \pmod{p^k} \\ \text{and } \varphi(\mathbf{r}, k) \geq e \end{cases}$$

Moreover, for a given solution \mathbf{x}_0 , such a pair (\mathbf{r}, k) is unique if we impose the condition:

$$\varphi(\mathbf{r}, k) - t_k < e \leq \varphi(\mathbf{r}, k)$$

where t_k is the thickness of the vertex (\mathbf{r}, k) .

Let us reformulate the first part of the theorem in graph-theoretic terms. We say that the **fan** from a vertex (\mathbf{r}, k) up to height h is the set of vertices of Ω_p issued from the vertex (\mathbf{r}, k) up to height h :

$$\text{Fan}_{\leq h}(\mathbf{r}, k) = \{(\mathbf{x}, l) \in \Omega_p \mid \mathbf{x} \equiv \mathbf{r} \pmod{p^k} \text{ and } l \leq h\}.$$

In graph-theoretic terms, Theorem 2.8 becomes:

$$\text{Tree}(P) = \bigcup_{(\mathbf{r}, k) \in \text{Trunk}(P)} \text{Fan}_{\leq \varphi(\mathbf{r}, k)}(\mathbf{r}, k).$$

The uniqueness will in turn be fundamental when we want to count the number of solutions; see Theorem 4.1.

Proof. Let (\mathbf{x}_0, e) be an element of the p -adic congruence tree Ω_p . Let $(\mathbf{r}, k) \in \text{Trunk}(P)$ denote the most recent ancestor of (\mathbf{x}_0, e) belonging to the trunk of P . The relation between \mathbf{x}_0 and \mathbf{r} is given by $\mathbf{x}_0 = \mathbf{r} + p^k \mathbf{y}_0$ (where $\mathbf{y}_0 \in \mathbb{Z}^n$).

By Lemma 2.7, since (\mathbf{r}, k) is an element of the trunk, we know that there exists a decomposition:

$$P(\mathbf{r} + p^k \mathbf{x}) = p^{\varphi(\mathbf{r}, k)} Q(\mathbf{x})$$

where $\varphi(\mathbf{r}, k)$ is the value of the tree-top function.

The assumption that $(\mathbf{r}, k) \in \text{Trunk}(P)$ is the most recent ancestor in the trunk means exactly that $Q(\mathbf{y}_0) \not\equiv 0 \pmod{p}$.

We now have all the ingredients to conclude the proof:

$$\begin{aligned} P(\mathbf{x}_0) \equiv 0 \pmod{p^e} &\iff P(\mathbf{r} + p^k \mathbf{y}_0) \equiv 0 \pmod{p^e} \\ &\iff p^{\varphi(\mathbf{r}, k)} Q(\mathbf{y}_0) \equiv 0 \pmod{p^e} \\ &\iff \varphi(\mathbf{r}, k) \geq e \end{aligned}$$

The assumption $Q(\mathbf{y}_0) \not\equiv 0 \pmod{p}$ is used in the last equivalence.

It remains to prove the uniqueness characterization. For the moment, from a vertex (\mathbf{r}, k) of the trunk, we have constructed a fan of solutions up to height $\varphi(\mathbf{r}, k)$.

But from $(\mathbf{r}^-, k-1)$ (the direct ancestor of (\mathbf{r}, k)), we construct solutions only up to height $\varphi(\mathbf{r}^-, k-1) = \varphi(\mathbf{r}, k) - t_k$. Thus the solutions whose height e satisfies $\varphi(\mathbf{r}, k) - t_k < e \leq \varphi(\mathbf{r}, k)$ are determined solely by the vertex (\mathbf{r}, k) of the trunk. \square

3. PROPERTIES OF THE THICKNESS

3.1. Computation of the thickness

Let $P(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$. Recall that the *thickness* of P at \mathbf{r} is the largest integer t such that one has a decomposition $P(\mathbf{r} + p\mathbf{x}) = p^t Q(\mathbf{x})$. We will use Taylor's formula to compute the thickness. Indeed, the Taylor expansion applied to P at \mathbf{r} gives the decomposition:

$$P(\mathbf{r} + \mathbf{x}) = \sum_{h=0}^d P_h(\mathbf{x}),$$

where d is the degree of P and $P_h(\mathbf{x})$ is a homogeneous polynomial of degree h :

$$P_h(\mathbf{x}) = \frac{1}{h!} d^h P(\mathbf{r})[\mathbf{x}, \dots, \mathbf{x}] = \frac{1}{h!} \sum_{|\mathbf{i}|=h} \partial^{\mathbf{i}} P(\mathbf{r}) \mathbf{x}^{\mathbf{i}}.$$

We use the usual conventions for multi-indices: $\mathbf{i} = (i_1, \dots, i_n)$, $|\mathbf{i}| = i_1 + \dots + i_n$, $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_n^{i_n}$, and $\partial^{\mathbf{i}} P(\mathbf{x}) = \frac{\partial^{i_1 + \dots + i_n} P}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}$.

Lemma 3.1.

$$t = \min_{|\mathbf{i}| \geq 0} \text{val}_p \left(\frac{1}{|\mathbf{i}|!} \partial^{\mathbf{i}} P(\mathbf{r}) p^{|\mathbf{i}|} \right)$$

In particular $t \leq \deg P$.

Proof. The Taylor formula applied to $P(\mathbf{r} + p\mathbf{x})$ gives:

$$P(\mathbf{r} + p\mathbf{x}) = \sum_{h=0}^d P_h(\mathbf{x}) p^h.$$

Let t denote the thickness and t' the minimum appearing in the statement. Since p^t divides $P_h(\mathbf{x}) p^h$ for all $0 \leq h \leq d$, we have $t \leq t'$. Conversely, $p^{t'}$ divides all the coefficients of all the polynomials $P_h(\mathbf{x}) p^h$, hence $p^{t'}$ divides $P(\mathbf{r} + p\mathbf{x})$, so $t \geq t'$. \square

3.2. The thickness decreases along the trunk

With the notation of the decomposition $P(\mathbf{r}_0 + p\mathbf{x}) = p^t Q(\mathbf{x})$, we define the *residual degree* of P at \mathbf{r}_0 as the integer $s = \deg \bar{Q}$, where $\bar{Q}(\mathbf{x})$ denotes the reduction modulo p of $Q(\mathbf{x})$.

We denote by $\text{mult}(\bar{P}, \mathbf{r}_0)$ the multiplicity of \mathbf{r}_0 as a root of \bar{P} in $(\mathbb{Z}/p\mathbb{Z})^n$. If $P(\mathbf{r}_0 + \mathbf{x}) = \sum_{h=0}^d P_h(\mathbf{x})$ is the decomposition into a sum of homogeneous polynomials, then this multiplicity is the smallest integer h such that $\bar{P}_h(\mathbf{x}) \not\equiv 0 \pmod{p}$.

Now consider two successive decompositions: $P(\mathbf{r}_0 + p\mathbf{x}) = p^t Q(\mathbf{x})$, followed by $Q(\mathbf{r}_1 + p\mathbf{x}) = p^{t'} R(\mathbf{x})$.

Lemma 3.2.

$$\text{mult}(\bar{P}, \mathbf{r}_0) \geq t \geq s \geq \text{mult}(\bar{Q}, \mathbf{r}_1)$$

In particular, $t \geq t'$.

An important consequence is that since $t \geq t'$, the thickness decreases as one moves upward along the trunk. Thus, along an infinite branch, the thickness eventually becomes constant.

Proof.

- Let $P(\mathbf{r}_0 + \mathbf{x}) = \sum_{h=0}^d P_h(\mathbf{x})$ be the decomposition into a sum of homogeneous polynomials. If the thickness of P at \mathbf{r}_0 is t , then p^t divides $P(\mathbf{r}_0 + p\mathbf{x})$, hence divides $p^h P_h(\mathbf{x})$ for all h . In particular, for $h < t$, p divides $P_h(\mathbf{x})$. Therefore $\text{mult}(\bar{P}, \mathbf{r}_0) \geq t$.
- Since $P(\mathbf{r}_0 + \mathbf{x}) = p^t Q(\mathbf{x})$, we have $Q(\mathbf{x}) = \sum_{h=0}^d p^{h-t} P_h(\mathbf{x})$. Thus for $h > t$, p divides $p^{h-t} P_h(\mathbf{x})$. Hence $\deg \bar{Q}(\mathbf{x}) \leq t$, so $s \leq t$.
- We always have $\text{mult}(\bar{Q}, \mathbf{r}_1) \leq \deg(\bar{Q}) = s$.
- Finally, by the very first inequality of this lemma, applied to $Q(\mathbf{x})$, we have $\text{mult}(\bar{Q}, \mathbf{r}_1) \geq t'$. Hence in particular $t \geq t'$.

□

3.3. Hensel's lemma

We have already observed that a polynomial has positive thickness at \mathbf{r}_0 if and only if $P(\mathbf{r}_0) \equiv 0 \pmod{p}$. We now study the case of thickness $t = 1$. According to Lemma 3.1, if $t = 1$ then:

- either $p \mid P(\mathbf{r}_0)$ and $p^2 \nmid P(\mathbf{r}_0)$,
- or $p \mid P(\mathbf{r}_0)$ and there exists $1 \leq i_0 \leq n$ such that $p \nmid \frac{\partial P}{\partial x_{i_0}}(\mathbf{r}_0)$.

Both cases may occur simultaneously.

Lemma 3.3. *If $t = 1$ and all partial derivatives vanish: $\frac{\partial P}{\partial x_i}(\mathbf{r}_0) \equiv 0 \pmod{p}$ for $1 \leq i \leq n$, then the trunk stops immediately after this vertex of thickness 1.*

Proof. By assumption, $P(\mathbf{r}_0 + \mathbf{x}) = c_0 + \text{terms of degree } \geq 2$, hence

$$P(\mathbf{r}_0 + p\mathbf{x}) = c_0 + p^2 R(\mathbf{x}).$$

We assumed $t = 1$, so $p \mid c_0$ and $p^2 \nmid c_0$. Thus

$$P(\mathbf{r}_0 + p\mathbf{x}) = p \left(\frac{c_0}{p} + pR(\mathbf{x}) \right).$$

Therefore the successor of P is $Q(\mathbf{x}) = \frac{c_0}{p} + pR(\mathbf{x})$. Since $\frac{c_0}{p}$ is not divisible by p , the congruence $\bar{Q}(\mathbf{x}) \equiv 0 \pmod{p}$ has no solutions, and hence the trunk stops at this point. □

In the case of thickness 1, when one of the partial derivatives does not vanish at \mathbf{r}_0 , we say that we are in the *Hensel lemma situation*. In this case as well, we obtain a complete description of the trunk.

Definition 3.4. A **Hensel tree** is an infinite tree in which each vertex admits exactly p^{n-1} outgoing edges and where all thicknesses are equal to 1.

Lemma 3.5. *If $P(\mathbf{r}_0) \equiv 0 \pmod{p}$ and there exists $1 \leq i \leq n$ such that $\frac{\partial P}{\partial x_i}(\mathbf{r}_0) \not\equiv 0 \pmod{p}$, then the part of the trunk of P issued from \mathbf{r}_0 is a Hensel tree.*

Proof. Without loss of generality, assume that $\frac{\partial P}{\partial x_1}(\mathbf{r}_0) \not\equiv 0 \pmod{p}$. Write $P(\mathbf{r}_0 + \mathbf{x}) = c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n + \cdots$. By Lemma 3.1, we know that \mathbf{r}_0 has thickness 1, which gives:

$$P(\mathbf{r}_0 + p\mathbf{x}) = p \left(\frac{c_0}{p} + c_1x_1 + c_2x_2 + \cdots + c_nx_n + pR(\mathbf{x}) \right).$$

The successor of P is therefore $Q(\mathbf{x}) = \frac{c_0}{p} + c_1x_1 + c_2x_2 + \cdots + c_nx_n + pR(\mathbf{x})$. Its reduction modulo p is $\bar{Q}(\mathbf{x}) = \frac{c_0}{p} + c_1x_1 + c_2x_2 + \cdots + c_nx_n$, with $c_1 \not\equiv 0 \pmod{p}$ by assumption. Thus, for any choice of $x_2, \dots, x_n \in \mathbb{Z}/p\mathbb{Z}$, there exists a unique $x_1 \in \mathbb{Z}/p\mathbb{Z}$ giving a solution to the linear equation $\frac{c_0}{p} + c_1x_1 + c_2x_2 + \cdots + c_nx_n \equiv 0 \pmod{p}$. Hence $\bar{Q}(\mathbf{x}) \equiv 0 \pmod{p}$ admits exactly p^{n-1} solutions.

Let \mathbf{r}_1 be such a solution. Since $\bar{Q}(\mathbf{r}_1) \equiv 0 \pmod{p}$, the thickness is at least 1. And since $\frac{\partial Q}{\partial x_1}(\mathbf{r}_0) \equiv c_1 \not\equiv 0 \pmod{p}$, we have $t = 1$ and we are again in the situation of Hensel's lemma. The conclusion then follows by induction. \square

4. THE NUMBER OF SOLUTIONS

4.1. Formula

We recall the theorem stated in the introduction. We now have all the ingredients to prove it.

Theorem 4.1. *The number of solutions to the equation $P(\mathbf{x}) \equiv 0 \pmod{p^e}$ in $(\mathbb{Z}/p^e\mathbb{Z})^n$ is:*

$$N_e = \sum_{\substack{(\mathbf{r},k) \in \text{Trunk}(P) \\ \varphi(\mathbf{r},k) - t_k < e \leq \varphi(\mathbf{r},k)}} p^{n(e-k)}.$$

Proof. Theorem 2.8 tells us that each vertex (\mathbf{r}, k) of the trunk provides, in a unique way, the solutions (\mathbf{x}_0, e) of $P(\mathbf{x}) \equiv 0 \pmod{p^e}$ if and only if (\mathbf{x}_0, e) is a successor of (\mathbf{r}, k) and $\varphi(\mathbf{r}, k) - t_k < e \leq \varphi(\mathbf{r}, k)$.

Therefore, the number of solutions arising from the fan of (\mathbf{r}, k) with height exactly e is $(p^n)^{e-k}$. This yields the desired formula. \square

4.2. Generating function

Definition 4.2. The *Poincaré series* is:

$$S(T) = \sum_{e \geq 0} N_e \frac{T^e}{p^{ne}},$$

where N_e denotes the number of solutions to the equation $P(\mathbf{x}) \equiv 0 \pmod{p^e}$ (with the convention that $N_0 = 1$). We recall that n is the number of variables.

4.3. Formula from the trunk

We will use Theorem 4.1 in order to compute the Poincaré series directly from the trunk.

Theorem 4.3.

$$S(T) = \sum_{(\mathbf{r},k) \in \text{Trunk}(P)} \frac{T^{\varphi(\mathbf{r},k) - t_k + 1}}{p^{nk}} (1 + T + T^2 + \cdots + T^{t_k - 1})$$

We define

$$\Xi_k(T) = \frac{T^{\varphi(\mathbf{r},k) - t_k + 1}}{p^{nk}} (1 + T + T^2 + \cdots + T^{t_k - 1}).$$

These functions of T are called ***xylon functions***, and the proposition will be called the ***xylon formula***:

$$S(T) = \sum_{(\mathbf{r},k) \in \text{Trunk}(P)} \Xi_k(T).$$

Remarks. By convention, the contribution of the root of the trunk is $\Xi_0(T) = 1$. On the other hand, if $t_k = 1$, then the sum $1 + T + T^2 + \dots + T^{t_k-1}$ reduces to 1.

Proof. To simplify the notation, we write $t = t_k$ and $\varphi = \varphi(\mathbf{r}, k)$. We reorganize the sum $S(T)$ using Theorem 4.1:

$$\begin{aligned} S(T) &= \sum_{e \geq 0} N_e \frac{T^e}{p^{ne}} \\ &= \sum_{e \geq 0} \sum_{\substack{(\mathbf{r},k) \in \text{Trunk}(P) \\ \varphi-t < e \leq \varphi}} p^{n(e-k)} \frac{T^e}{p^{ne}} \\ &= \sum_{(\mathbf{r},k) \in \text{Trunk}(P)} \sum_{\varphi-t < e \leq \varphi} \frac{T^e}{p^{nk}} \\ &= \sum_{(\mathbf{r},k) \in \text{Trunk}(P)} \frac{1}{p^{nk}} (T^{\varphi-t+1} + T^{\varphi-t+2} + \dots + T^\varphi) \\ &= \sum_{(\mathbf{r},k) \in \text{Trunk}(P)} \frac{T^{\varphi-t+1}}{p^{nk}} (1 + T + T^2 + \dots + T^{t-1}) \end{aligned}$$

□

We now give an application of the xylon formula to two particular cases.

4.4. Infinite stalk of constant thickness

Lemma 4.4. *The generating series associated with an infinite stalk of constant thickness $t = u$ issued from the root is a rational fraction:*

$$S(T) = 1 + (1 + T + T^2 + \dots + T^{u-1}) \frac{T}{p^n} \left(1 - \frac{T^u}{p^n}\right)^{-1} \in \mathbb{Q}[T]$$

Proof. By definition, at each height k there is a unique vertex whose thickness equals $t = u$. Then the tree-top function at height k equals $\varphi_k = ku$. Thus:

$$\begin{aligned} S(T) &= \sum_{k \geq 0} \Xi_k(T) \\ &= 1 + \sum_{k > 0} \frac{T^{(k-1)u+1}}{p^{nk}} (1 + T + T^2 + \dots + T^{u-1}) \\ &= 1 + (1 + T + T^2 + \dots + T^{u-1}) \sum_{k \geq 0} \frac{T^{ku+1}}{p^{nk+n}} \\ &= 1 + (1 + T + T^2 + \dots + T^{u-1}) \sum_{k \geq 0} \frac{T}{p^n} \left(\frac{T^u}{p^n}\right)^k \\ &= 1 + (1 + T + T^2 + \dots + T^{u-1}) \frac{T}{p^n} \left(1 - \frac{T^u}{p^n}\right)^{-1} \end{aligned}$$

□

4.5. The Hensel lemma case

A Hensel tree is an infinite tree in which each vertex has exactly p^{n-1} outgoing edges, all vertices having thickness 1.

Lemma 4.5. *The generating series associated with a Hensel tree is a rational fraction:*

$$S(T) = \left(1 - \frac{T}{p}\right)^{-1} \in \mathbb{Q}[T]$$

Proof. For a given height k , there are $(p^{n-1})^k$ vertices. Each vertex of height k has tree-top value $\varphi_k = k$ and its contribution to the sum is $\Xi_k(T) = \frac{T^k}{p^{nk}}$. Thus:

$$S(T) = \sum_{k>0} p^{(n-1)k} \Xi_k(T) = 1 + \sum_{k>0} p^{(n-1)k} \frac{T^k}{p^{nk}} = \sum_{k \geq 0} \left(\frac{T}{p}\right)^k = \left(1 - \frac{T}{p}\right)^{-1}$$

□

For a Hensel tree that would not be attached to the root but to a vertex of height k_0 and with tree-top value φ_0 , one would similarly show:

$$S_{k_0, \varphi_0}(T) = \frac{T^{\varphi_0}}{p^{nk_0}} \left(1 - \frac{T}{p}\right)^{-1}.$$

5. NORMALIZATION

The purpose of this section is to provide preparatory results and to reduce to the simplest possible form of the bivariate polynomials to be studied. We will consider only *non-degenerate* polynomials, that is, $\deg_x P \geq 1$ and $\deg_y P \geq 1$.

5.1. The trunk is invariant under translation

Lemma 5.1. *Let $P(x, y) \in \mathbb{Z}_p[x, y]$ and $\alpha, \beta \in \mathbb{Z}_p$. Define $Q(x, y) \in \mathbb{Z}_p[x, y]$ by $Q(x, y) = P(x - \alpha, y - \beta)$. Then the trunks of P and Q are isomorphic (i.e. there exists a bijection between these trees that preserves the thicknesses).*

Corollary 5.2. *For an infinite stalk of a trunk, one may assume after translation that it lies above the roots $(0, 0)$ at all heights.*

Proof. Isomorphism between the roots of P and Q modulo p . Let $(r, s) \in (\mathbb{Z}/p\mathbb{Z})^2$ be a root of P modulo p :

$$P(r, s) \equiv 0 \pmod{p} \iff Q(r + \alpha, s + \beta) \equiv 0 \pmod{p} \iff Q(r + \alpha_0, s + \beta_0) \equiv 0 \pmod{p}$$

where we write $\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots = \alpha_0 + p\alpha'$, and similarly for β . Thus:

$$(r, s) \text{ is a root of } P(x, y) \text{ modulo } p \iff (r', s') = (r + \alpha_0, s + \beta_0) \text{ is a root of } Q(x, y) \text{ modulo } p$$

Preservation of thicknesses. Let (r, s) be a root of thickness t for P :

$$\begin{aligned} P(r + px, s + py) &= p^t \tilde{P}(x, y) \\ \iff Q(r + \alpha + px, s + \beta + py) &= p^t \tilde{P}(x, y) \\ \iff Q(r + \alpha_0 + p(x + \alpha'), s + \beta_0 + p(y + \beta')) &= p^t \tilde{P}(x, y) \\ \iff Q(r' + pX, s' + pY) = p^t \tilde{P}(X - \alpha', Y - \beta') &\quad \text{with } X = x + \alpha', Y = y + \beta' \\ \iff Q(r' + pX, s' + pY) = p^t \tilde{Q}(X, Y) \end{aligned}$$

where we have defined $\tilde{Q}(X, Y) = \tilde{P}(X - \alpha', Y - \beta')$. Thus Q also has thickness t at the root (r', s') .

Conclusion. We have just shown that the successor $\tilde{Q}(X, Y) = \tilde{P}(X - \alpha', Y - \beta')$ is itself a translate of the successor $\tilde{P}(X, Y)$. By induction, moving up along the tree, this proves the result for all vertices. \square

5.2. Normalization

We consider a polynomial $P(x, y)$ associated with an infinite stalk of constant thickness ≥ 2 . We wish to find a simple expression for $P(x, y)$. The guiding idea is the following: if a univariate polynomial $F(x)$ admits an infinite stalk of constant thickness equal to u at the root 0 , then one can factor $F(x)$ in the form $F(x) = x^u U(x)$.

Lemma 5.3.

- (1) If $P(x, y) = F(x) + G(y)$ (with $p \nmid P(x, y)$) admits an infinite stalk whose every vertex has thickness $\geq u$ at the root $(0, 0)$, then, up to the symmetry $(x, y) \leftrightarrow (y, x)$,

$$P(x, y) = x^u U(x) + p^\alpha y^v V(y)$$

with $\alpha \geq 0$, $v \geq u$, and $U(x) \in \mathbb{Z}_p[x]$, $V(y) \in \mathbb{Z}_p[y]$.

- (2) Let $K \geq 0$. Let $U(x) = \sum_i u_i x^i$ and $V(y) = \sum_j v_j y^j$. By going sufficiently high on the stalk of the roots $(0, 0)$, which we shall call the principal stalk, one may assume that $U(x) \equiv u_0 \pmod{p^K}$ and $V(y) \equiv v_0 \pmod{p^K}$.
- (3) If moreover the stalk has constant thickness u , then $U(0) \not\equiv 0 \pmod{p}$. At a sufficiently large level along the stalk, one can also place oneself in a situation where, in addition, $V(0) \not\equiv 0 \pmod{p}$ (by modifying the parameters α , v , and the polynomial $V(y)$).

Thus, thanks to Lemma 5.1, if one had an infinite stalk whose limit vertex at infinity is $(\rho, \sigma) \in \mathbb{Z}_p^2$, then the decomposition would be:

$$P(x, y) = (x - \rho)^u U(x) + p^\alpha (y - \sigma)^v V(y).$$

Proof.

- (1) We first show that $P(0, 0) = 0$. Let c_{00} denote the constant coefficient of $P(x, y)$. Since p^u divides $P(px, py)$, it follows that p^u divides c_{00} . By iteration, p^{ku} divides the k -th iterate $P(p^k x, p^k y)$, and hence also divides c_{00} . This holds for all k , therefore $c_{00} = 0$. By hypothesis $P(x, y) = F(x) + G(y)$, and we may thus assume without loss of generality that $F(0) = 0$ and $G(0) = 0$.

If $(0, 0)$ has thickness $t \geq u$ for $P(x, y)$, then $p^u \mid F(px) + G(py)$. Since $F(0) = 0$ and $G(0) = 0$, it follows that $p^u \mid F(px)$ and $p^u \mid G(py)$. Write $F(x) = p^\beta \sum_i a_i x^i$ and $G(y) = p^\alpha \sum_i b_i y^i$, with $a_0 = 0$ and $b_0 = 0$. Since p does not divide $P(x, y)$, we may assume $\beta = 0$.

After k iterations, p^{ku} divides $F(p^k x)$, hence p^{ku} divides $F(p^k x) = \sum_i a_i p^{ki} x^i$, and similarly p^{ku} divides $G(p^k y) = p^\alpha \sum_i b_i p^{ki} y^i$. Thus p^{ku} divides $a_i p^{ki}$ and $b_i p^{\alpha+ki}$ for all $i \geq 0$. Letting k tend to infinity, we obtain $a_i = 0$ and $b_i = 0$ for $i = 0, \dots, u-1$. Thus $F(x) = x^u U(x)$ and $G(y) = p^\alpha y^v V(y)$ with $v \geq u$.

- (2) We have $F(x) = x^u U(x) = x^u (u_0 + u_1 x + u_2 x^2 + \dots)$. We compute $F(px)$ to obtain the successor: $F_1(x) = x^u (u_0 + u_1 px + u_2 p^2 x^2 + \dots)$. After m iterations, p^m divides the coefficients of x, x^2, \dots . The proof is similar for $V(y)$.
- (3) We have seen that $P(x, y) = x^u U(x) + p^\alpha y^v V(y)$, with $v \geq u$. First observe that if $U(0) \equiv 0 \pmod{p}$, then by the univariate trunk algorithm we have $U(x) = x^{u'} \tilde{U}(x)$ with $u' > u$. In the cases $v > u$ or $\alpha > 0$, this is excluded, since it would give a thickness of $P(x, y)$ at $(0, 0)$ strictly larger than u . In these cases we therefore have $U(0) \not\equiv 0 \pmod{p}$. In the remaining case we have $P(x, y) = x^u U(x) + y^u V(y)$ with $U(0) \equiv 0 \pmod{p}$. We cannot also have $V(0) \equiv 0 \pmod{p}$, since this would imply $V(y) = y^{v'} \tilde{V}(y)$ and again a thickness of $P(x, y)$ at $(0, 0)$ strictly larger than u . Thus we have $U(0) \not\equiv 0 \pmod{p}$

or $V(0) \not\equiv 0 \pmod{p}$. By possibly exchanging the variables, we may assume $U(0) \not\equiv 0 \pmod{p}$.

We now start again from $P(x, y) = x^u U(x) + p^\alpha y^v V(y)$ with $v \geq u$. Applying the one-variable thickness algorithm to $V(y)$ along the principal stalk, the thickness becomes constant (possibly zero) from some height e onward. Thus, by applying in one variable the reasoning we have just carried out, we obtain $V_e(y) = y^w W(y)$ with $W(0) \not\equiv 0 \pmod{p}$. At height e , we have $P_e(x, y) = x^u U_e(x) + p^{\alpha'} y^v V_e(y)$, hence $P_e(x, y) = x^u U_e(x) + p^{\alpha'} y^{v+w} W(y)$, with $W(0) \not\equiv 0 \pmod{p}$, which is consistent with the final conclusion of the lemma. □

5.3. Finiteness of infinite stalks

Lemma 5.4. *The number of infinite stalks issued from the root of the trunk, whose vertices all have thickness $t \geq 2$, is finite.*

As an immediate consequence, the number of stalks of constant thickness ≥ 2 (issued from any vertex of the trunk) is finite.

Proof. First note that the thickness of a vertex is bounded above by the degree of the polynomial, and hence can take only finitely many values. Let $P(x, y)$ denote the polynomial, and let $(\rho_i, \sigma_i) \in \mathbb{Z}_p^2$ be the vertices at infinity of the infinite stalks. By Lemmas 5.1 and 5.3, after normalization we have (with $t = u_i$)

$$P(x, y) = (x - \rho_i)^{u_i} U_i(x) + p^{\alpha_i} (y - \sigma_i)^{v_i} V_i(y)$$

for each i . By identification, we have $(x - \rho_i)^{u_i} U_i(x) = (x - \rho_1)^{u_1} U_1(x) + c_i$ (where c_i is a constant). Since $u_i \geq 2$, differentiation shows that ρ_i is a root of the fixed polynomial $\frac{d}{dx}(x - \rho_1)^{u_1} U_1(x)$, and hence can take only finitely many values. The same argument applies to the σ_i . Thus the set of (ρ_i, σ_i) is finite, and therefore only finitely many stalks issue from the root of the trunk. □

6. THE GENERATING FUNCTION IS RATIONAL

In this section we prove Theorem 1.2: the Poincaré series of a separated polynomial in two variables is rational. The idea is to establish this result for certain model polynomials, as we began to do at the end of Section 4. This time, starting from an arbitrary polynomial, we decompose its trunk into a finite number of pieces, each of which is either finite or isomorphic to the trunk of a model polynomial. From explicit computations for each piece, we will deduce that the Poincaré series for the polynomial under consideration is a rational function, which is precisely Igusa's result.

If P is degenerate, that is, if for instance $P(x, y) = R(x)$ with $R \in \mathbb{Z}_p[X]$, then the trunk of $P(x, y)$ is easily deduced from that of $R(x)$, and the Poincaré series of $P(x, y)$ coincides with that of $R(x)$. It follows from the study of the univariate case in [2], using the same arguments as in the present paper, that the Poincaré series of $R(x)$ (and hence that of $P(x, y)$) is rational. In this case, one recovers Igusa's result. Consequently, in the sequel, we assume that $P(x, y)$ actually depends on both x and y .

6.1. Reduction of the proof of rationality to the normalized case sufficiently far along an infinite stalk.

We work under the assumptions of Theorem 1.2. The idea is to establish the result first for certain model polynomials, as we began to do at the end of Section 5. We now proceed as follows: starting from an arbitrary polynomial, we decompose its trunk into finitely many pieces, each of which is either finite or isomorphic to the trunk of a model polynomial. From explicit computations

on each piece, we then deduce that the Poincaré series associated with the polynomial under consideration is a rational function, thereby recovering Igusa's result.

If the trunk of the polynomial $P(x, y)$ is finite, then by Theorem 4.3, the Poincaré series $S(T)$ is a polynomial, which proves the desired result in this case. If the trunk is infinite, then by Lemma 5.4, there exist only finitely many (maximal) infinite stalks of constant thickness ≥ 2 .

By cutting these constant-thickness stalks high enough up and keeping only the vertices above a certain level, we may assume they are independent, meaning that no ancestor of a vertex in one stalk belongs to another stalk. Let Σ_i be such a stalk. For each such stalk Σ'_i , we denote by T_i the part of the trunk of P attached to it, that is, the set of vertices of $\text{Trunk}(P)$ having an ancestor in Σ'_i .

The main task of this section is to prove that the contribution of each T_i to the series $S(T)$ is rational. We denote by T' the trunk of P with all the T_i removed.

There may exist infinitely many stalks (infinite paths) of thickness 1. However, we saw in Section 3.3 that for a vertex of thickness 1, either it is a terminal vertex (the trunk stops there), or a Hensel tree is attached to it (which indeed produces infinitely many stalks of thickness 1). And we know that a Hensel tree contributes a rational fraction (Lemma 4.5, see also the end of Section 6.8).

Let T'' denote the tree obtained by removing from T' all Hensel trees. Such a tree is finite (otherwise, by König's lemma, it would contain an infinite stalk of thickness 1 or ≥ 2 , both of which have been removed by construction). Since T'' is finite, only finitely many Hensel trees can be attached to it, and their total contribution is therefore a rational series. (Warning: as we shall see in the case of infinite stalks of thickness ≥ 2 , infinitely many Hensel trees may be attached to such a stalk, but these stalks are by definition excluded from the tree T' .)

We therefore consider an infinite stalk of constant thickness ≥ 2 (among finitely many possible ones, see Lemma 5.4) issued from a vertex s_0 of height k_0 and with tree-top value φ_0 . We denote by $P_0(x, y)$ the polynomial attached to the root of this stalk; it is again a separated polynomial. We consider two series:

- the Poincaré series $S_1(T)$ associated with the original polynomial $P(x, y)$ and with the part of the trunk issued from the vertex s_0 ;
- the Poincaré series $S_0(T)$ associated with the polynomial $P_0(x, y)$ (that is, we now consider s_0 as the root of the trunk).

Then the xylon formula 4.3 gives the relation $S_1(T) = \frac{T^{\varphi_0}}{p^{2k_0}} S_0(T)$ (see also the remark following Lemma 4.5). It therefore suffices to prove the rationality of $S_0(T)$.

Still considering the case of an infinite stalk of constant thickness ≥ 2 , we use the results of Section 5 to reduce to a simple form of $P_0(x, y)$. More precisely, we work under the conclusions of Lemma 5.3:

$$P_0(x, y) = x^u U(x) + p^\alpha y^v V(y).$$

We may even, without loss of generality and still by Lemma 5.3, consider the polynomial sufficiently high on the stalk, and thus assume that

$$U(x) \equiv u_0 \pmod{p^m}, \quad V(y) \equiv v_0 \pmod{p^m},$$

with m an arbitrarily large integer and $u_0 \not\equiv 0 \pmod{p}$, $v_0 \not\equiv 0 \pmod{p}$. We will even see that we can further reduce to $Q_0(x, y) = u_0 x^u + p^\alpha v_0 y^v$. It is for these polynomials that we will carry out the computations of the Poincaré series.

6.2. Normalized case

Proposition 6.1. *The series $S(T)$ associated with $Q_0(x, y) = u_0 x^u + p^\alpha v_0 y^v$ is rational (where $u_0 \not\equiv 0 \pmod{p}$, $v_0 \not\equiv 0 \pmod{p}$ and $1 < u \leq v$).*

The trunk associated with $P_0(x, y) = x^u U(x) + p^\alpha y^v V(y)$ (with $\alpha \geq 0$, $1 < u \leq v$, $U(x) = u_0 + u_1 x + \dots$, $V(y) = v_0 + v_1 y + \dots \in \mathbb{Z}_p[y]$, and $u_0 \not\equiv 0 \pmod{p}$, $v_0 \not\equiv 0 \pmod{p}$, and for all $i \geq 1$, $u_i \equiv 0 \pmod{p^m}$, $v_i \equiv 0 \pmod{p^m}$ with $m = \text{val}_p(u) + 2$) is identical to that of $Q_0(x, y)$. In particular, the same sum $S(T)$ is associated with it and is therefore rational.

Moreover, the denominators of this series in $\mathbb{Q}(T)$ are among:

$$p - T, \quad p^2 - T^u, \quad p^{2u} - T^{u^2}, \quad p^{u+v} - T^{uv}.$$

The remainder of this section is devoted to the proof. Our proof is explicit: we partition the trunk into a finite number of subtrees, and for each such subtree we give the exact expression of the associated rational series. Since the formulas are tedious, we do not give the explicit expression of the final series. However, a complete example will be worked out in the Appendix.

6.3. Description of the trunk after leaving the principal stalk

We begin with the general case $P_0(x, y) = x^u U(x) + p^\alpha y^v V(y)$. The root $(0, 0)$ gives rise to an infinite stalk of constant thickness $t = u$, called the *principal stalk*. The k -th successor of P_0 is

$$P_k(x, y) = x^u U(p^k x) + p^{\alpha+k(v-u)} y^v V(p^k y),$$

which has a form similar to that of P_0 . The contribution of this stalk to the sum $S(T)$ is rational by Lemma 4.4.

6.4. The case $\alpha > 0$

We first reduce the case $\alpha > 0$ by Euclidean division to one of the two cases $0 < \alpha < u$ or $\alpha = 0$. We then treat these two situations.

The reduction modulo p of P_0 is $\bar{P}_0(x, y) = u_0 x^u$, whose roots are of the form $(0, s_0)$. We have already studied the case $s_0 = 0$ above, so we assume $s_0 \not\equiv 0 \pmod{p}$. At such a root $(0, s_0)$, we have

$$P_0(0 + px, s_0 + py) = p^u x^u U(px) + p^\alpha (s_0 + py)^v V(s_0 + py).$$

The constant term of $(s_0 + py)^v V(s_0 + py)$ is $\tilde{v}_0 = v_0 s_0^v$.

Case $\alpha \geq u$. When $\alpha \geq u$, each root $(0, s_0)$ has thickness u , and the successor of P_0 is:

$$P_1(x, y) = x^u U(px) + p^{\alpha-u} (s_0 + py)^v V(s_0 + py).$$

As long as the exponent of p is $\geq u$, we continue this process, the k -th successor being:

$$P_k(x, y) = x^u U_k(x) + p^{\alpha-ku} (s_0 + s_1 p + \dots + s_{k-1} p^{k-1} + p^k y)^v V_k(y),$$

where $U_k(x) = U(p^k x)$ and $V_k(y) = V(s_0 + s_1 p + \dots + s_{k-1} p^{k-1} + p^k y)$. We still have $U_k(x) \equiv u_0 \pmod{p^m}$ and $V_k(y) \equiv v_0 \pmod{p^m}$.

Thus we obtain $\lfloor \frac{\alpha}{u} \rfloor$ iterations, leading to a tree that splits at the first step into $p - 1$ vertices, and then splits in cascade, each vertex thereafter having p children, over a total height of $\lfloor \frac{\alpha}{u} \rfloor$, with vertices all having thickness equal to u . (For the initial vertex there is one omitted edge, since it is already counted in the stalk above $(0, 0)$.)

By Euclidean division, we are thus reduced to the case $0 < \alpha' < u$ or to the case $\alpha' = 0$, where α' is the remainder of the Euclidean division of α by u .

Case $0 < \alpha' < u$.

Let us restart from

$$P_k(x, y) = x^u U_k(x) + p^{\alpha'} (s_0 + s_1 p + \dots + s_{k-1} p^{k-1} + p^k y)^v V_k(y)$$

with $0 < \alpha' < u$. A root $(0, s_k)$ has thickness $t = \alpha'$, and the successor is:

$$P_{k+1}(x, y) = p^{u-\alpha'} x^u U_k(px) + (s_0 + s_1 p + \dots + s_k p^k + p^{k+1} y)^v V_k(s_k + py).$$

Thus $\bar{P}_{k+1}(x, y) \equiv s_0^v v_0 \equiv \tilde{v}_0 \not\equiv 0 \pmod{p}$. Hence \bar{P}_{k+1} has no root modulo p , and this branch terminates.

Writing $U(x) = u_0 + u_1x + \dots$ and $V(y) = v_0 + v_1y + \dots$, one sees, upon repeating the previous computations, that they do not depend on the coefficients u_1, u_2, \dots or v_1, v_2, \dots . Thus the trunk for P_0 is identical to that of $Q_0 = u_0x^u + p^\alpha v_0y^v$.

Summary: in the case where u does not divide α , the trunk consists of a tree that first has $p - 1$ branches, which then split into p branches, then again into p branches, and so on, for a total of $\lfloor \frac{\alpha}{u} \rfloor$ steps, always with thickness u . Then there is a final splitting into p branches, with terminal vertices of thickness $\alpha' = \alpha \% u$ (the remainder of the Euclidean division of α by u).

It remains to consider the case where u divides α . As we have seen, this situation reduces to the case $\alpha = 0$, which we now study. Beforehand, we prove a few results on valuations in the binomial expansion of Newton.

6.5. Valuations of the binomial coefficients

Lemma 6.2. *Let p be a prime number.*

- (1) *If $k \geq 1$, then $\text{val}_p(k!) \leq k - 1$.*
- (2) *If $1 \leq k \leq n$, then $\text{val}_p \binom{n}{k} \geq \text{val}_p(n) + 1 - k$.*
- (3) *If $2 \leq k \leq n$, then $\text{val}_p \left[k \binom{n}{k} \right] \geq \text{val}_p(n) + 2 - k$.*
- (4) *Let $l \geq 1$, $n \geq 1$, and let s be an integer not divisible by p . Denote by C_k the coefficient of x^k in the expansion of $(s + p^l x)^n$. Then for $k \geq 1$, one has $\text{val}_p(C_k) \geq \text{val}_p(C_1)$.*

Proof. (1) By Legendre's formula,

$$\text{val}_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \dots$$

In particular,

$$\text{val}_p(k!) \leq \text{val}_2(k!) = \sum_{j \geq 1} \left\lfloor \frac{k}{2^j} \right\rfloor < \sum_{j \geq 1} \frac{k}{2^j} = k,$$

the second inequality being strict since the terms $\lfloor \frac{k}{2^j} \rfloor$ vanish from some index onward. Thus $\text{val}_p(k!) \leq k - 1$.

- (2) The integer $\binom{n}{k}$ is the quotient of $n(n-1) \cdots (n-k+1)$ by $k!$. It follows that $\text{val}_p \binom{n}{k} \geq \text{val}_p(n) - \text{val}_p(k!)$. Thus, by the first property, $\text{val}_p \binom{n}{k} \geq \text{val}_p(n) + 1 - k$.
- (3) Since $k \binom{n}{k} = n \binom{n-1}{k-1}$, we have:

$$\begin{aligned} \text{val}_p \left[k \binom{n}{k} \right] &= \text{val}_p \left[n \binom{n-1}{k-1} \right] = \text{val}_p(n) + \text{val}_p \binom{n-1}{k-1} \\ &\geq \text{val}_p(n) + (\text{val}_p(n-1) + 1 - (k-1)) \\ &\geq \text{val}_p(n) + 2 - k, \end{aligned}$$

where we used the inequality from the previous point, applied to $\binom{n-1}{k-1}$.

- (4) We have $\text{val}_p(C_1) = \text{val}_p(ns^{n-1}p^l) = \text{val}_p(n) + l$, whereas $\text{val}_p(C_k) = \text{val}_p \left(\binom{n}{k} s^{n-k} p^{lk} \right)$. By the second point,

$$\text{val}_p(C_k) \geq (\text{val}_p(n) + 1 - k) + lk = \text{val}_p(C_1) + (k-1)(l-1) \geq \text{val}_p(C_1).$$

□

6.6. Case $\alpha = 0$

We resume the notation of Section 6.4, now with $\alpha = 0$:

$$P_k(x, y) = x^u U_k(x) + (s_0 + s_1 p + \cdots + s_{k-1} p^{k-1} + p^k y)^v V_k(y),$$

where $U_k(x) \equiv u_0 \pmod{p^m}$ and $V_k(y) \equiv v_0 \pmod{p^m}$. This formula is valid for $k = 0$, in which case we simply have $P_0(x, y) = x^u U(x) + y^v V(y)$. If P_k has no root modulo p , then the trunk ends at that vertex. Otherwise, let (r_k, s_k) be a root of P_k modulo p . Modulo p^m we have:

$$P_k(r_k + px, s_k + py) \equiv u_0(r_k + px)^u + v_0(s_0 + s_1 p + \cdots + s_k p^k + p^{k+1} y)^v \pmod{p^m}.$$

We set $r = r_k$, $s = s_0 + s_1 p + \cdots + s_k p^k$, and $l = k + 1$ in order to write more simply:

$$P_k(r_k + px, s_k + py) \equiv u_0(r + px)^u + v_0(s + p^l y)^v \pmod{p^m}.$$

Thus:

$$\begin{aligned} P_k(r_k + px, s_k + py) &\equiv u_0(r + px)^u + v_0(s + p^l y)^v \pmod{p^m} \\ &\equiv u_0 r^u + v_0 s^v \\ &\quad + u_0 u r^{u-1} p x + u_0 \binom{u}{2} r^{u-2} p^2 x^2 + \cdots \\ &\quad + v_0 v s^{v-1} p^l y + v_0 \binom{v}{2} r^{v-2} p^{2l} y^2 + \cdots \pmod{p^m}. \end{aligned}$$

Let $\beta = \text{val}_p(u_0 r^u + v_0 s^v)$ and $\gamma = \min(\text{val}_p(pu), \text{val}_p(vp^l))$. Note that by Lemma 6.2, the valuations of the coefficients of $x^2, x^3, \dots, y^2, y^3, \dots$ are greater than or equal to γ . We will see that the thickness of the root (r_k, s_k) equals $t = \min(\beta, \gamma)$. Thus, by definition of γ , this thickness is less than or equal to $u + 1$, hence strictly less than m , which justifies that all computations may be carried out modulo p^m .

First case: $\beta < \gamma$. Note that $\beta > 0$, since by definition (r_k, s_k) is a root of P_k modulo p . Assume now that $0 < \beta < \gamma$. We prove that in this case the vertex (r_k, s_k) has thickness β and has no successor in the trunk (i.e. the trunk terminates there). Since $0 < \beta < \gamma$, the thickness of the root (r_k, s_k) equals β . Thus:

$$P_{k+1}(x, y) = \frac{1}{p^\beta} P_k(r_k + px, s_k + py) = \frac{u_0 r^u + v_0 s^v}{p^\beta} + pR(x, y).$$

Indeed, all coefficients of $u_0 u r^{u-1} p x + \cdots + v_0 v s^{v-1} p^l y + \cdots$ are divisible by p^γ , hence by $p^{\beta+1}$. Thus the reduction modulo p of P_{k+1} is reduced to a constant polynomial:

$$\bar{P}_{k+1}(x, y) \equiv \frac{u_0 r^u + v_0 s^v}{p^\beta} \pmod{p}.$$

By definition of β , this constant is nonzero modulo p . Hence P_{k+1} has no roots modulo p , and therefore the trunk stops here.

Second case: $\beta \geq \gamma$. We prove that in this case, a Hensel tree arises from each of the possible roots (r_{k+1}, s_{k+1}) succeeding (r_k, s_k) .

Since $\beta \geq \gamma$, the thickness of the root (r_k, s_k) now equals γ . Thus the successor of P_k at (r_k, s_k) can be written as:

$$\begin{aligned} P_{k+1}(x, y) &\equiv \frac{1}{p^\gamma} (u_0 r^u + v_0 s^v) \\ &\quad + \frac{1}{p^\gamma} (u_0 u r^{u-1} p) x + \frac{1}{p^\gamma} (u_0 \binom{u}{2} r^{u-2} p^2) x^2 + \cdots \\ &\quad + \frac{1}{p^\gamma} (v_0 v s^{v-1} p^l) y + \frac{1}{p^\gamma} (v_0 \binom{v}{2} s^{v-2} p^{2l}) y^2 + \cdots \pmod{p^{m-\gamma}}. \end{aligned}$$

We write this as:

$$\begin{aligned} P_{k+1}(x, y) &= \frac{1}{p^\gamma}(u_0r^u + v_0s^v) \\ &\quad + c_1x + c_2x^2 + \cdots \\ &\quad + d_1y + d_2y^2 + \cdots. \end{aligned}$$

Recall that $\gamma = \min(\text{val}_p(pu), \text{val}_p(vp^l))$. Assume $\gamma = \text{val}_p(vp^l)$; then $d_1 \not\equiv 0 \pmod{p}$. Let us compute $\frac{\partial P_{k+1}}{\partial y}(x, y)$. The constant coefficient of this partial derivative is d_1 . The coefficient of y^{j-1} in this partial derivative is:

$$jd_j = jv_0 \binom{v}{j} r^{v-j} p^{jl}.$$

By Lemma 6.2:

$$\begin{aligned} \text{val}_p(jd_j) &= \text{val}_p\left(j \binom{v}{j}\right) + jl \\ &\geq (\text{val}_p(v) + 2 - j) + jl \\ &\geq (\text{val}_p(v) + l) + 1 + (j - 1)(l - 1) \\ &> \gamma. \end{aligned}$$

Thus $\frac{\partial P_{k+1}}{\partial y}(x, y) = d_1 + pR(y)$. Let (r_{k+1}, s_{k+1}) be a solution of $P_{k+1}(x, y) \equiv 0 \pmod{p}$. Still modulo p , we have $\frac{\partial P_{k+1}}{\partial y}(x, y) \equiv d_1 \not\equiv 0 \pmod{p}$, in particular at $(x, y) = (r_{k+1}, s_{k+1})$. Therefore the thickness of (r_{k+1}, s_{k+1}) is exactly $t = 1$, and we are in the situation of Hensel's lemma.

If $\gamma = \text{val}_p(pu)$, then $c_1 \not\equiv 0 \pmod{p}$. A very similar computation (taking $l = 1$) gives $\frac{\partial P_{k+1}}{\partial x}(x, y) \equiv c_1 \not\equiv 0 \pmod{p}$, and we are again in the situation of Hensel's lemma.

6.7. General structure of the outgoing branches

To prove the rationality of the sum $S(T)$, the trunk must have a particular structure. We will see that when one moves up along the principal stalk, that is, above the roots $(0, 0)$, the branches attached to it form patterns that are roughly periodic, above a certain height.

We set $A_0(x, y) = P_0(x, y) = x^u U(x) + p^\alpha y^v V(y)$. Let $k > 0$ be a multiple of u ; we denote by $B_0(x, y) = P_k(x, y)$ the k -th successor of P_0 along the stalk $(0, 0)$:

$$B_0(x, y) = P_k(x, y) = x^u U(p^k x) + p^{\alpha+k(v-u)} y^v V(p^k y).$$

In this subsection, we assume that $v - u > 0$, so that the quantity $\alpha + k(v - u)$ becomes arbitrarily large as $k \rightarrow \infty$. We will see later that the case $v = u$ is much simpler.

The polynomial B_0 is similar to A_0 , where the exponent $\alpha_k = \alpha + k(v - u)$ changes, but the exponents u and v , and the constant coefficients u_0 and v_0 , do not. Now, the computations in the previous paragraphs depend mainly on these data α_k, u, v, u_0, v_0 . We must now show that, above a certain height, the outgoing branch from the principal stalk for A_0 (at height 0) is similar to the outgoing branch for B_0 (at height k). According to the computations in the previous paragraphs, the branch leaving a height k begins with branches of thickness $t = u$, of length $\lfloor \frac{\alpha_k}{u} \rfloor$, which therefore becomes longer and longer as k grows. Note that since we choose here k to be a multiple of u , we have

$$\left\lfloor \frac{\alpha_k}{u} \right\rfloor = \left\lfloor \frac{\alpha}{u} \right\rfloor + \frac{k}{u}(v - u).$$

We now show that apart from this difference in branch length, what is attached afterwards is identical at height 0 and at height k .

If α is not a multiple of u , then at the end of the stalk for A_0 a vertex of thickness $\alpha\%u$ is attached (see Section 6.4). In this case α_k is also not a multiple of u , and since $\alpha_k\%u = \alpha\%u$, at the end of the stalk for B_0 a vertex of thickness $\alpha\%u$ is also attached.

Now consider the case where α , and hence also α_k , are multiples of u . This corresponds to the situation of Section 6.6, whose notation we reuse. We denote by A_i and B_i the respective successors of A_0 and B_0 along their outgoing branch, corresponding to the same choices of the roots s_0, s_1, \dots, s_{i-1} for both polynomials. Let A_m and B_n be the successors corresponding to the exponent $\alpha' = 0$ (with $m = \lfloor \frac{\alpha}{u} \rfloor < n = \lfloor \frac{\alpha_k}{u} \rfloor$), that is, to the last vertex of thickness u on the stalk.

For the subsequent reasoning, it will suffice to study the highest part of the stalk. Consequently, we assume that α is sufficiently large so that the inequality $\text{val}_p(vp^{m+1}) \geq \text{val}_p(pu)$ holds, where $m = \lfloor \frac{\alpha}{u} \rfloor$. We therefore obtain $\gamma(A_m) = \text{val}_p(pu) = \text{val}_p(u) + 1$. Moreover, since $n > m$, we also have $\text{val}_p(vp^{n+1}) \geq \text{val}_p(pu)$, and hence $\gamma(B_m) = \text{val}_p(u) + 1$. Therefore $\gamma(B_n) = \gamma(A_m)$, which we simply denote by γ . Next, note that the roots of A_m modulo p and those of B_n modulo p are the solutions of the same equation $u_0x^u + v_0s_0^v \equiv 0 \pmod{p}$. Choose (ρ, σ) to be such a root. In the “ $\alpha' = 0$ ” situation, the point is to compare the value of β with γ . Let

$$C = u_0\rho^u + v_0(s_0 + s_1p + \dots + s_{m-1}p^{m-1} + \sigma p^m)^v,$$

so that $\beta(A_m) = \text{val}_p(C)$. Also let

$$C' = u_0\rho^u + v_0(s_0 + s_1p + \dots + s_{m-1}p^{m-1} + \dots + s_{n-1}p^{n-1} + \sigma p^n)^v,$$

so that $\beta(B_n) = \text{val}_p(C')$. If we move sufficiently high on the principal stalk so that $m = \lfloor \frac{\alpha}{u} \rfloor \geq \text{val}_p(u) + 1 = \gamma$, then we have the equivalences:

$$\beta(A_m) \geq \gamma \iff C \equiv 0 \pmod{p^{\text{val}_p(u)+1}} \iff C' \equiv 0 \pmod{p^{\text{val}_p(u)+1}} \iff \beta(B_n) \geq \gamma.$$

Thus, if $\beta(A_m) \geq \gamma$, then we also have $\beta(B_n) \geq \gamma$, and we attach a Hensel tree in both cases. If $\beta(A_m) < \gamma$, then we also have $\beta(B_n) < \gamma$, and the trunk stops at the end of the stalk of thickness β in both cases.

Finally, in the case $\beta < \gamma$, after γ vertices after leaving the principal stalk, the value of β is constant. Indeed, let

$$C_k = u_0\rho^u + v_0(s_0 + s_1p + \dots + s_kp^k)^v.$$

Since we assume $\beta < \gamma$, for $k \geq \gamma$ we have

$$\beta_k = \text{val}_p(C_k) = \text{val}_p(C_\gamma).$$

6.8. Decomposition of the Poincaré series

We have already seen two simple cases where the series is rational: (i) the case of an infinite stalk of constant thickness u (Lemma 4.4), which produces a denominator $p^2 - T^u$, and (ii) the case of a Hensel tree issued from the origin (Lemma 4.5), which produces a denominator $p - T$.

A. Series for the principal stalk and a particular case

The vertices of this principal stalk, of constant thickness u , yield the rational series (Lemma 4.4):

$$S_A(T) = 1 + A(T) \frac{T}{p^2} \left(1 - \frac{T^u}{p^2}\right)^{-1}$$

where we set:

$$A(T) = 1 + T + T^2 + \dots + T^{u-1}.$$

We now consider the trunks encountered in this section. We will prove rationality by using periodicity. We have seen that the exponent α defining P_0 (or Q_0) becomes, for the k -th successor

P_k along the principal stalk, $\alpha_k = \alpha + k(v - u)$. Modulo u , this exponent is therefore periodic with period (at most) u .

For any set E of vertices, we define $\text{Poinc}(E)$ as the series of the values $\Xi_s(T)$ of the xylon function for all the elements s of E . In this language $S_A(T) = \text{Poinc}(\text{PrincStalk})$.

We define the **starred trunk** Trunk_k^* as the set of vertices whose most recent ancestor on the principal trunk at height k , i.e. the set of branches leaving the principal trunk is at height k . Formally this is the set of the vertices (r, s, j) of the trunk such that $(0, 0, k) \triangleleft (r_{k+1}, s_{k+1}, k+1) \triangleleft (r, s, j)$ where $(r_{k+1}, s_{k+1}) \neq (0, 0)$.

The Poincaré series of the whole trunk is:

$$S(T) = S_A(T) + \sum_{k=0}^{+\infty} \text{Poinc}(\text{Trunk}_k^*).$$

In this expression, none of the starred trunks Trunk^* can contain infinitely many (maximal) Hensel trees, nor an infinite stalk of thickness ≥ 2 (because we have build independent infinite constant stalks in paragraph 6.1). It follows that each series $\text{Poinc}(\text{Trunk}^*)$ is either a polynomial or a rational function whose only possible non-constant denominator is $p - T$.

The case $v = u$, that is $P_0(x, y) = x^u U(x) + p^\alpha y^u V(y)$, is a special situation for which the general method used when $v > u$ is not relevant. We therefore state a specific proposition for this case.

Proposition 6.3. *In the case $P_0(x, y) = x^u U(x) + p^\alpha y^u V(y)$, the Poincaré series of the polynomial is a rational function.*

Proof. In this case, each successive transform $P_k(x, y)$ of $P_0(x, y)$ has the form $P_k(x, y) = x^u U(p^k x) + p^\alpha y^u V(p^k y)$, which is essentially stable. It follows that all the starred trunks Trunk_k^* are isomorphic to one another. Ignoring their initial level, they therefore have the same Poincaré series, say $H(T)$, which is a rational function by the previous remark.

From the earlier relation we obtain $\text{Poinc}(\text{Trunk}_k^*) = \frac{T^{ku}}{p^{2k}} H(T)$. Using this identity, we deduce

$$S(T) = S_A(T) + \sum_{k=0}^{+\infty} \frac{T^{ku}}{p^{2k}} H(T) = S_A(T) + \left(1 - \frac{T^u}{p^2}\right)^{-1} H(T),$$

which proves the proposition and, in particular, Proposition 6.1 in this case. \square

From now on, we assume that $v > u$. In this case, in the formula above $S(T) = S_A(T) + \sum_{k=0}^{+\infty} \text{Poinc}(\text{Trunk}_k^*)$, we decompose the second summand as

$$\sum_{k=0}^{u-1} \sum_{l \geq 0} \text{Poinc}(\text{Trunk}_{k+lu}^*).$$

To prove the rationality of $S(T)$, it is sufficient to prove the rationality of each series

$$\sum_{l \geq 0} \text{Poinc}(\text{Trunk}_{k_0+lu}^*)$$

for $k_0 = 0, \dots, u - 1$.

But we have already established that each series $\text{Poinc}(\text{Trunk}_{k_0+lu}^*)$ is either a polynomial or a rational function whose only possible denominator is $p - T$.

Consequently, in order to prove rationality, it suffices to show that there exists an integer L such that $\sum_{l \geq L} \text{Poinc}(\text{Trunk}_{k_0+lu}^*)$ is rational. In other words, to prove rationality, we may assume that we are at a sufficiently large level along the principal stalk.

We choose L any integer such that $\alpha + Lu(v - u) \geq \gamma u$, and set $a = \alpha + Lu(v - u)$. We will prove the rationality of the Poincaré series for the polynomial \tilde{P}_0 with this exponent a (instead of the original P_0 of exponent α) using the fact that $a \geq \gamma u$ (see parts D and E below). To this end, we decompose the vertices into two sets: on one hand, the set of the interior vertices of all

the starred trunks, with thickness u ; on the other hand the terminal vertices of all these starred trunks. In the case $a\%u \neq 0$, these vertices have thickness $a\%u$; in the other case $a\%u = 0$, these terminal vertices may be either simple, or belonging to a Hensel tree.

B. Series for all interior vertices

Consider an interior vertex of an outgoing branch (among the $p - 1$ possible ones) of a starred trunk $\text{Trunk}^*(P_{lu})$. It is characterized by the integer l and another integer m which is the distance between the vertex and the departure vertex of this starred trunk. The height of this general vertex is $k = lu + m$, its thickness is $t = u$, and the value of the tree-top function is $\varphi = (lu + m)u$.

Thus, the contribution of this vertex is:

$$\Xi_{l,m}(T) = \frac{T^{\varphi-t+1}}{p^{2k}}(1 + T + \cdots + T^{u-1}) = \frac{T^{(lu+m)u-u+1}}{p^{2(lu+m)}}(1 + T + \cdots + T^{u-1}).$$

At this height $k = lu + m$ there are p^{m-1} vertices. The index m ranges from 1 to $\lfloor \frac{a+lu(v-u)}{u} \rfloor = \lfloor \frac{a}{u} \rfloor + l(v-u)$. By the xylon formula (Theorem 4.3), the Poincaré series is the sum of the $\Xi_{l,m}(T)$:

$$\begin{aligned} S(T) &= \sum_{l \geq 0} \sum_{m=1}^{l(v-u) + \lfloor \frac{a}{u} \rfloor} p^{m-1} \Xi_{l,m}(T) \\ &= (1 + T + \cdots + T^{u-1}) \sum_{l \geq 0} \sum_{m=1}^{l(v-u) + \lfloor \frac{a}{u} \rfloor} \frac{T^{mu-u+1}}{p^{m+1}} \frac{T^{lu^2}}{p^{2lu}} \\ &= A(T) \sum_{l \geq 1} \sum_{m=1}^{l(v-u)} \xi_{l,m} + A(T) \sum_{l \geq 0} \sum_{m=l(v-u)+1}^{l(v-u) + \lfloor \frac{a}{u} \rfloor} \xi_{l,m}, \end{aligned}$$

where we have set $A(T) = 1 + T + \cdots + T^{u-1}$ and $\xi_{l,m} = \frac{T^{mu-u+1}}{p^{m+1}} \frac{T^{lu^2}}{p^{2lu}}$.

In the first summand, we write the Euclidean division $m = q(v-u) + r$, with here $1 \leq r \leq v-u$, and then interchange the sums:

$$\begin{aligned} S_1(T) &= A(T) \sum_{l \geq 1} \sum_{0 \leq q \leq l-1} \sum_{1 \leq r \leq v-u} \xi_{l,m} \\ &= A(T) \sum_{q \geq 0} \sum_{l \geq q+1} \sum_{1 \leq r \leq v-u} \xi_{l,m} \\ &= A(T) \frac{T}{p^2} \sum_{q \geq 0} \frac{T^{qu(v-u)}}{p^{q(v-u)}} \sum_{l \geq q+1} \frac{T^{lu^2}}{p^{2lu}} \sum_{1 \leq r \leq v-u} \frac{T^{(r-1)u}}{p^{r-1}} \\ &= A(T) B(T) \frac{T}{p^2} \sum_{q \geq 0} \frac{T^{qu(v-u)}}{p^{q(v-u)}} \sum_{l \geq q+1} \frac{T^{lu^2}}{p^{2lu}}. \end{aligned}$$

Here we have set

$$B(T) = 1 + \frac{T^u}{p} + \left(\frac{T^u}{p}\right)^2 + \cdots + \left(\frac{T^u}{p}\right)^{v-u-1}.$$

Thus:

$$\begin{aligned}
S_1(T) &= A(T)B(T) \frac{T}{p^2} \sum_{q \geq 0} \frac{T^{qu(v-u)}}{p^{q(v-u)}} \frac{T^{(q+1)u^2}}{p^{2(q+1)u}} \sum_{l \geq 0} \left(\frac{T^{u^2}}{p^{2u}} \right)^l \\
&= A(T)B(T) \frac{T}{p^2} \left(1 - \frac{T^{u^2}}{p^{2u}} \right)^{-1} \sum_{q \geq 0} \frac{T^{u^2}}{p^{2u}} \left(\frac{T^{uv}}{p^{u+v}} \right)^q \\
&= A(T)B(T)C(T) \left(1 - \frac{T^{u^2}}{p^{2u}} \right)^{-1} \left(1 - \frac{T^{uv}}{p^{u+v}} \right)^{-1},
\end{aligned}$$

where we have set

$$C(T) = \frac{T^{u^2+1}}{p^{2u+2}}.$$

The second is, with $m = k + l(v - u)$:

$$\begin{aligned}
S_2(T) &= A(T) \sum_{l \geq 0} \sum_{m=l(v-u)+1}^{l(v-u)+\lfloor \frac{a}{u} \rfloor} \xi_{l,m} \\
&= A(T) \sum_{l \geq 0} \sum_{k=1}^{\lfloor \frac{a}{u} \rfloor} \frac{T^{(k+l(v-u))u-u+1}}{p^{k+l(v-u)+1}} \frac{T^{lu^2}}{p^{2lu}} \\
&= A(T) \left(\sum_{k=1}^{\lfloor \frac{a}{u} \rfloor} \frac{T^{uk-u+1}}{p^{k+1}} \right) \sum_{l \geq 0} \frac{T^{luv}}{p^{l(u+v)}} \\
&= A(T)D(T) \left(1 - \frac{T^{uv}}{p^{u+v}} \right)^{-1},
\end{aligned}$$

with the polynomial $D(T) = \sum_{k=1}^{\lfloor \frac{a}{u} \rfloor} \frac{T^{uk-u+1}}{p^{k+1}}$.

Conclusion: $S(T) = S_1(T) + S_2(T) \in \mathbb{Q}(T)$, with denominators $p^{2u} - T^{u^2}$ and $p^{u+v} - T^{uv}$. We have computed the series for a single outgoing branch; for all $p - 1$ outgoing branches, the associated series is $(p - 1)S(T) \in \mathbb{Q}(T)$.

C. Series for terminal vertices, case u does not divide a

We now compute the series associated with the vertices in the case $a \% u \neq 0$. Thus, we count the contribution of a terminal vertex of thickness $a_0 = a \% u$ on each outgoing branch of the starred trunk.

A terminal vertex is characterized by a single integer l : its height is $k = lu + l(v - u) + \lfloor \frac{a}{u} \rfloor + 1 = lv + \lfloor \frac{a}{u} \rfloor + 1$, its thickness is $t = a_0 = a \% u$, and the value of the tree-top function is $\varphi = (lv + \lfloor \frac{a}{u} \rfloor)u + a_0$. For this vertex:

$$\Xi_l(T) = \frac{T^{lv + \lfloor \frac{a}{u} \rfloor u + 1}}{p^{2(lv + \lfloor \frac{a}{u} \rfloor + 1)}} (1 + T + \dots + T^{a_0 - 1}).$$

All the $p^{l(v-u)+\lfloor \frac{a}{u} \rfloor}$ terminal vertices (for one branch issued from the principal trunk among the $p-1$ possible ones) give rise to the following series, which is indeed rational:

$$\begin{aligned}
S(T) &= \sum_{l \geq 0} p^{l(v-u)+\lfloor \frac{a}{u} \rfloor} \Xi_l(T) \\
&= (1 + T + \cdots + T^{a_0-1}) \sum_{l \geq 0} \frac{T^{luv+\lfloor \frac{a}{u} \rfloor u+1}}{p^{2(lv+\lfloor \frac{a}{u} \rfloor+1)-(l(v-u)+\lfloor \frac{a}{u} \rfloor)}} \\
&= (1 + T + \cdots + T^{a_0-1}) \frac{T^{\lfloor \frac{a}{u} \rfloor u+1}}{p^{\lfloor \frac{a}{u} \rfloor+2}} \sum_{l \geq 0} \left(\frac{T^{uv}}{p^{u+v}} \right)^l \\
&= (1 + T + \cdots + T^{a_0-1}) \frac{T^{\lfloor \frac{a}{u} \rfloor u+1}}{p^{\lfloor \frac{a}{u} \rfloor+2}} \left(1 - \frac{T^{uv}}{p^{u+v}} \right)^{-1}.
\end{aligned}$$

The denominator is $p^{u+v} - T^{uv}$.

D. Series for the case u divides a , with terminal vertex

Here we use the notations of Section 6.6 and the results of Section 6.4. With these notations, we consider the case $0 < \beta < \gamma$ (if $\beta = 0$ there is no terminal vertex). We have a computation very similar to the previous case. We have seen that γ vertices after leaving the principal stalk, the value of β becomes constant. We thus group the terminal vertices of thickness β into packets of $p^{l(v-u)+\lfloor \frac{a}{u} \rfloor - \gamma}$ terminal vertices (here we use that $\lfloor \frac{a}{u} \rfloor \geq \gamma$).

$$\begin{aligned}
S(T) &= \sum_{l \geq 0} p^{l(v-u)+\lfloor \frac{a}{u} \rfloor - \gamma} \Xi_l(T) \\
&= (1 + T + \cdots + T^{\beta-1}) \sum_{l \geq 0} \frac{T^{luv+\lfloor \frac{a}{u} \rfloor u+1}}{p^{2(lv+\lfloor \frac{a}{u} \rfloor+1)-l(v-u)-\lfloor \frac{a}{u} \rfloor + \gamma}} \\
&= (1 + T + \cdots + T^{\beta-1}) \frac{T^{\lfloor \frac{a}{u} \rfloor u+1}}{p^{\lfloor \frac{a}{u} \rfloor + \gamma + 2}} \sum_{l \geq 0} \left(\frac{T^{uv}}{p^{u+v}} \right)^l \\
&= (1 + T + \cdots + T^{\beta-1}) \frac{T^{\lfloor \frac{a}{u} \rfloor u+1}}{p^{\lfloor \frac{a}{u} \rfloor + \gamma + 2}} \left(1 - \frac{T^{uv}}{p^{u+v}} \right)^{-1}.
\end{aligned}$$

E. Series for the case u divides a , with Hensel trees

This occurs only when u divides a . First, recall the generalization of Lemma 4.5 for a Hensel tree not attached to the root but to a vertex of height k and with tree-top value φ (with n variables):

$$S_{k,\varphi}(T) = \frac{T^\varphi}{p^{nk}} \left(1 - \frac{T}{p} \right)^{-1}.$$

Again we use the notations of Section 6.6 and the results of Section 6.4. The vertices where the Hensel trees are attached have height $k = lu + l(v-u) + \lfloor \frac{a}{u} \rfloor + 1 = lv + \lfloor \frac{a}{u} \rfloor + 1$ at a vertex where the thickness is $t = \gamma$, and tree-top value $\varphi = (lv + \lfloor \frac{a}{u} \rfloor)u + \gamma$. We have seen that, γ vertices after leaving the principal stalk, the value of β becomes constant. There are $p^{l(v-u)+\lfloor \frac{a}{u} \rfloor - \gamma}$ such vertices (for one branch issued from the principal trunk, here we use that $\lfloor \frac{a}{u} \rfloor \geq \gamma$), so the total

contribution of these Hensel trees is:

$$\begin{aligned}
S(T) &= \sum_{l \geq 0} p^{l(v-u) + \lfloor \frac{a}{u} \rfloor - \gamma} \frac{T^{lv + \lfloor \frac{a}{u} \rfloor u + \gamma}}{p^{2(lv + \lfloor \frac{a}{u} \rfloor + 1)}} \left(1 - \frac{T}{p}\right)^{-1} \\
&= \left(1 - \frac{T}{p}\right)^{-1} \frac{T^{\lfloor \frac{a}{u} \rfloor u + \gamma}}{p^{\lfloor \frac{a}{u} \rfloor + \gamma + 2}} \sum_{l \geq 0} \left(\frac{T^{uv}}{p^{u+v}}\right)^l \\
&= \left(1 - \frac{T}{p}\right)^{-1} \frac{T^{\lfloor \frac{a}{u} \rfloor u + \gamma}}{p^{\lfloor \frac{a}{u} \rfloor + \gamma + 2}} \left(1 - \frac{T^{uv}}{p^{u+v}}\right)^{-1}.
\end{aligned}$$

This is once again a rational fraction with denominators $p - T$ and $p^{u+v} - T^{uv}$.

REFERENCES

- [1] Jérémy Berthomieu, Grégoire Lecerf, and Guillaume Quintin. Polynomial root finding over local rings and application to error correcting codes. *Appl. Algebra Engrg. Comm. Comput.*, 24(6):413–443, 2013.
- [2] Arnaud Bodin and Christian Drouin. Solutions of a polynomial equation modulo a prime power. *The American Mathematical Monthly*, 2026. To appear (2026). Preprint available at <https://arxiv.org/abs/2510.07168>.
- [3] Dirk Bollaerts. On the Poincaré series associated to the p -adic points on a curve. *Acta Arith.*, 51(1):9–30, 1988.
- [4] A. I. Borevich and I. R. Shafarevich. *Number theory*, volume Vol. 20 of *Pure and Applied Mathematics*. Academic Press, New York-London, 1966. Translated from the Russian by Newcomb Greenleaf.
- [5] Sayak Chakrabarti. Multivariate polynomials modulo prime powers: their roots, zeta-function and applications. Master’s thesis, Department of Computer Science and Engineering, IIT Kanpur, Kanpur, India, 2022.
- [6] Sayak Chakrabarti and Nitin Saxena. An effective description of the roots of bivariate polynomials modulo p^k and the related Igusa’s local zeta function. In *Proceedings of the International Symposium on Symbolic & Algebraic Computation (ISSAC 2023)*, pages 135–144. ACM, New York, 2023.
- [7] Jan Denef. Report on Igusa’s local zeta function. Number 201-203, pages Exp. No. 741, 359–386. 1991. Séminaire Bourbaki, Vol. 1990/91.
- [8] Ashish Dwivedi, Rajat Mittal, and Nitin Saxena. Counting basic-irreducible factors mod p^k in deterministic poly-time and p -adic applications. In *34th Computational Complexity Conference*, volume 137 of *LIPICs. Leibniz Int. Proc. Inform.*, pages Art. No. 15, 29. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2019.
- [9] Ashish Dwivedi, Rajat Mittal, and Nitin Saxena. Efficiently factoring polynomials modulo p^4 . In *ISSAC’19—Proceedings of the 2019 ACM International Symposium on Symbolic and Algebraic Computation*, pages 139–146. ACM, New York, 2019.
- [10] Ashish Dwivedi and Nitin Saxena. Computing Igusa’s local zeta function of univariates in deterministic polynomial-time. In *ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 of *Open Book Ser.*, pages 197–214. Math. Sci. Publ., Berkeley, CA, 2020.
- [11] David R. Hayes and Michael D. Nutt. Reflective functions on p -adic fields. *Acta Arith.*, 40(3):229–248, 1981/82.
- [12] Jun-ichi Igusa. Complex powers and asymptotic expansions. I. Functions of certain types. *J. Reine Angew. Math.*, 268/269:110–130, 1974.
- [13] Leann Kopp, Natalie Randall, J. Maurice Rojas, and Yuyu Zhu. Randomized polynomial-time root counting in prime power rings. *Math. Comp.*, 89(321):373–385, 2020.
- [14] Naud Potemans and Willem Veys. Introduction to p -adic Igusa zeta functions. In *p -adic analysis, arithmetic and singularities*, volume 778 of *Contemp. Math.*, pages 71–102. Amer. Math. Soc., 2022.
- [15] Wolfgang M. Schmidt and C. L. Stewart. Congruences, trees, and p -adic integers. *Trans. Amer. Math. Soc.*, 349(2):605–639, 1997.
- [16] W. A. Zuniga-Galindo. Computing Igusa’s local zeta functions of univariate polynomials, and linear feedback shift registers. *J. Integer Seq.*, 6(3):Article 03.3.6, 18, 2003.

APPENDIX A. EXAMPLE $P(x, y) = x^2 - y^3$

The goal of this appendix is to illustrate the results of the previous sections with the example $P(x, y) = x^2 - y^3$, where $p > 2$ is a prime number. In particular, we compute the trunk of P , its Poincaré series, and the first values N_e for the number of solutions of $x^2 - y^3 \equiv 0 \pmod{p^e}$. We recover the same results as those obtained by Denef's formula [14].

We follow step by step the method of Section 6, which will allow us to make the series $S(T)$ completely explicit.

A.1. Preliminaries

Let us make the following remarks, which we will need later:

- For every prime p , the congruence $x^2 - y^3 \equiv 0 \pmod{p}$ has p solutions. They are obtained via the parametrization (t^3, t^2) for $t \in \llbracket 0, p-1 \rrbracket$.
- It is known that there are $\frac{p-1}{2}$ elements $y \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ that are squares modulo p .
- Finally, y^3 is a square modulo p if and only if y is. A proof using the Legendre symbol is: $\left(\frac{y^3}{p}\right) = +1 \iff \left(\frac{y}{p}\right)^3 = +1 \iff \left(\frac{y}{p}\right) = +1$.

As in Section 6, we compute the trunk (see the figures on the following pages) and we partition this trunk with an explicit computation of the series associated with each piece.

A.2. Principal stalk

Above $(0, 0)$, there is an infinite stalk whose vertices have thickness $t = 2$. We denote by $P_k(x, y) = x^2 - p^k y^3$ the k -th successor of P for the root $(0, 0)$.

Let us compute the Poincaré series $S_A(T)$ associated with this stalk via the xylon formula 4.3. The vertices are indexed by their height $k \geq 0$. For $k > 0$ the tree-top value is $\varphi = 2k$, and the thickness is $t = 2$. We also refer to Lemma 4.4. Thus:

$$\begin{aligned} S_A(T) &= 1 + \sum_{k>0} \Xi_k(T) = 1 + \sum_{k>0} \frac{T^{2k-1}}{p^{2k}} (1+T) \\ &= 1 + (1+T) \frac{T}{p^2} \sum_{k \geq 0} \left(\frac{T^2}{p^2}\right)^k \\ &= 1 + (1+T) \frac{T}{p^2} \left(1 - \frac{T^2}{p^2}\right)^{-1} \\ &= \frac{p^2 + T}{p^2 - T^2} \end{aligned}$$

A.3. Other branches from the root

We now consider the nonzero roots of $P(x, y) \equiv 0 \pmod{p}$. We have seen that there are $p-1$ nonzero solutions (r_i, s_i) (their exact values depend on p , but not their number). These branches must be studied separately since, in the language of Section 6, they are not “sufficiently high on the trunk”. For such a nonzero root (r, s) , we have:

$$P(r + px, s + py) = (r + px)^2 - (s + py)^3 = r^2 - s^3 + 2rpx - 3s^2py + \dots$$

We know that $p \mid r^2 - s^3$. For $p > 2$, we have $p^2 \nmid 2rp$, hence the thickness is $t = 1$. The successor is

$$Q_1(x, y) = \frac{r^2 - s^3}{p} + 2rx - 3s^2y + \dots$$

Since the coefficient of x is nonzero modulo p , we are in the situation of Hensel's lemma. Conclusion: to each of the $p-1$ nonzero roots of \bar{P} , we associate an outgoing branch from the root, which is in fact a Hensel tree.

Each of these trees is attached at height $k_0 = 1$ and with tree-top value $\varphi_0 = 1$. We apply $p - 1$ times the shifted version of Lemma 4.5:

$$S_B(T) = (p - 1) \frac{T^{\varphi_0}}{p^{2k_0}} \left(1 - \frac{T}{p}\right)^{-1} = \frac{(p - 1)T}{p(p - T)}.$$

Remark: the notation for the series $S_B(T), S_C(T), \dots$ is slightly different here from that of Section 6.

A.4. Branches from an odd height

See Figure 3. We start with height 1 and $P_1(x, y) = x^2 - py^3$: the nonzero roots of $\bar{P}_1(x, y) \equiv x^2 \pmod{p}$ are the $(0, s)$ with $s \in \llbracket 1, p - 1 \rrbracket$. For one of these roots, we have $P_1(0 + px, s + py) = pQ_1(x, y)$ with $Q_1(x, y) = px^2 - (s + py)^3$. Thus each root has thickness $t = 1$. But then $\bar{Q}_1(x, y) \equiv s \not\equiv 0 \pmod{p}$, and the trunk stops there. Conclusion: the branches (other than the principal stalk) issued from the vertex of height 1 consist of $p - 1$ terminal vertices of thickness 1.

More generally, for a vertex of height $k = 2l + 1$, the polynomial is $P_k(x, y) = x^2 - p^k y^3$. We always exclude the root $(0, 0)$. The structure of the outgoing branches is as follows:

- $p - 1$ outgoing branches from the vertex of height k (there would be p in total if we added the branch of the principal stalk), which lead to $p - 1$ vertices of thickness 2.
- From each of these vertices are attached p vertices of thickness $t = 2$, to which are attached p vertices of thickness $t = 2$, and so on, up to height $k + l$.
- From each of the vertices of height $k + l$ are attached p vertices of thickness $t = 1$, and the trunk stops there.

We call the *partial trunk* the sub-trunk consisting of the vertices of thickness 2, and we then study the contribution of the terminal vertices (of thickness 1).

We compute the contribution of the partial trunk (odd case) for each of the $p - 1$ outgoing branches. A vertex on such a branch is indexed by (l, m) , where $2l + 1$ is the height of the attachment point on the principal stalk and m is the distance from this attachment point (with $1 \leq m \leq l$). Thus the height of the vertex is $k = (2l + 1) + m$, and $\varphi = 2k$ with $t = 2$. For a

fixed index m there are p^{m-1} vertices.

$$\begin{aligned}
\tilde{S}_C(T) &= \sum_{l>0} \sum_{m=1}^l p^{m-1} \Xi_{l,m}(T) = \sum_{l>0} \sum_{m=1}^l p^{m-1} \frac{T^{\varphi-t+1}}{p^{2k}} (1+T) \\
&= (1+T) \sum_{l \geq 1} \sum_{m=1}^l \frac{T^{4l}}{p^{4l}} \frac{T^{2m+1}}{p^{m+3}} \\
&= (1+T) \sum_{m \geq 1} \sum_{l \geq m} \frac{T^{4l}}{p^{4l}} \frac{T^{2m+1}}{p^{m+3}} \\
&= (1+T) \sum_{m \geq 1} \frac{T^{2m+1}}{p^{m+3}} \frac{T^{4m}}{p^{4m}} \sum_{l \geq 0} \frac{T^{4l}}{p^{4l}} \\
&= (1+T) \sum_{m \geq 1} \frac{T^{6m+1}}{p^{5m+3}} \left(1 - \frac{T^4}{p^4}\right)^{-1} \\
&= (1+T) \frac{T^7}{p^8} \left(1 - \frac{T^6}{p^5}\right)^{-1} \left(1 - \frac{T^4}{p^4}\right)^{-1} \\
&= \frac{p(1+T)T^7}{(p^4 - T^4)(p^5 - T^6)}.
\end{aligned}$$

Summing over the $p-1$ branches gives:

$$S_C(T) = (p-1)\tilde{S}_C(T) = \frac{p(p-1)(1+T)T^7}{(p^4 - T^4)(p^5 - T^6)}.$$

It remains to compute the contribution of the terminal vertices. There are p^l of them, at height $k = 3l + 2$, with $\varphi = 6l + 3$ and $t = 1$.

$$\begin{aligned}
\tilde{S}_D(T) &= \sum_{l \geq 0} p^l \Xi_l(T) = \sum_{l \geq 0} p^l \frac{T^{\varphi-t+1}}{p^{2k}} (1) \\
&= \sum_{l \geq 0} \frac{T^{6l+3}}{p^{5l+4}} = \frac{T^3}{p^4} \left(1 - \frac{T^6}{p^5}\right)^{-1}.
\end{aligned}$$

Summing over the $p-1$ branches gives:

$$S_D(T) = (p-1)\tilde{S}_D(T) = \frac{p(p-1)T^3}{p^5 - T^6}.$$

A.5. Branches from an even height

See Figure 4. We consider a vertex of the principal stalk of height $k = 2l$ with $l > 0$.

Let us start with height 2 and $P_2(x, y) = x^2 - p^2y^3$. The roots modulo p , other than $(0, 0)$, are the $(0, s)$ with $s \in \llbracket 1, p-1 \rrbracket$. Each root $(0, s)$ has thickness $t = 2$ and has successor $Q_1(x, y) = x^2 - (s + py)^3$.

We now focus on $Q_1(x, y)$, with s fixed. Since $\overline{Q_1}(x, y) \equiv x^2 - s^3 \pmod{p}$, we discuss according to whether s^3 is a square modulo p :

- if s is not a square modulo p , then neither is s^3 , and thus $\overline{Q_1}(x, y) \equiv 0 \pmod{p}$ has no solutions. The trunk stops there. This happens for $\frac{p-1}{2}$ nonzero values of s that are not squares.
- if $s \neq 0$ is a square modulo p , then s^3 is also a square. In this case $\overline{Q_1}(x, y) \equiv 0 \pmod{p}$ has $2p$ solutions (r'_1, s') and (r'_2, s') , with two possible values for the first coordinate ($r'_2 = -r'_1$) and $s' \in \llbracket 0, p-1 \rrbracket$ arbitrary. Fix such a solution (r', s') . Then

$$Q_1(r' + px, s' + py) = r'^2 - s^3 + 2pr'x + \dots$$

This is therefore a vertex of thickness $t = 1$, and indeed a Hensel configuration. Conclusion in this case: from the principal stalk there branch off $\frac{p-1}{2}$ vertices of thickness $t = 2$. To each of these vertices are attached $2p$ Hensel trees.

Conclusion: there are $p - 1$ outgoing branches from the vertex of height 2: half lead to terminal vertices of thickness 2; the other half lead to vertices of thickness 2 to which, for each such vertex, $2p$ Hensel trees are attached.

Remark: for this example there are no vertices of Case D of Section 6. Indeed we assumed $u = 2$ and $p > 2$, hence $\text{val}_p(pu) = 1$. Thus for $\gamma = \text{val}_p(pu)$, there is no β satisfying $0 < \beta < \gamma$.

More generally, for a vertex of the principal stalk of height $k = 2l$ (with $l > 0$), the polynomial is $P_k(x, y) = x^2 - p^k y^3$, and we exclude the root $(0, 0)$ from the discussion. We denote by $(0, s)$ with $s \in \llbracket 1, p-1 \rrbracket$ the roots of \overline{P}_k . The structure of the outgoing branches is as follows:

- $p - 1$ outgoing branches from the vertex of height k (there would be p in total if we counted the branch of the principal stalk), which lead to $p - 1$ vertices of thickness 2.
- From each of these vertices are attached p vertices with $t = 2$, to which are attached p vertices with $t = 2$, and so on, up to height $k + l$.
- For the end of the partial trunk:
 - for half of these vertices of height $k + l$, the partial trunk stops there: these are the vertices arising from a branch where s is not a square modulo p ,
 - for the other half, to each of these vertices of height $k + l$ are attached $2p$ Hensel trees: these are the vertices arising from a branch where s is a square modulo p .

The contribution of the partial trunk (even case) for the $p - 1$ outgoing branches is very similar to the odd case. A vertex of the partial trunk is indexed by (l, m) with height $k = 2l + m$, $\varphi = 2k$, $t = 2$. For a fixed index m , there are p^{m-1} vertices.

$$\begin{aligned}
S_E(T) &= (p-1) \sum_{l>0} \sum_{m=1}^l p^{m-1} \Xi_{l,m}(T) \\
&= \dots \\
&= (p-1)(1+T) \frac{T^5}{p^6} \left(1 - \frac{T^4}{p^4}\right)^{-1} \left(1 - \frac{T^6}{p^5}\right)^{-1} \\
&= \frac{p^3(p-1)(1+T)T^5}{(p^4 - T^4)(p^5 - T^6)}.
\end{aligned}$$

It remains to compute the contribution of the Hensel trees, for the $\frac{p-1}{2}$ outgoing branches associated with an s that is a square modulo p (for the other branches the trunk is limited to the partial trunk).

For the height $k = 2l$ of the attachment vertex, there are thus $\frac{p-1}{2}$ outgoing branches. For each of these branches, there are p^{l-1} vertices at the end of the partial trunk, and at each such vertex $2p$ Hensel trees are attached. These Hensel trees are attached at height $k_0 = 3l + 1$ with tree-top

value $\varphi_0 = 6l + 1$. Thus:

$$\begin{aligned}
 S_F(T) &= \frac{p-1}{2} \sum_{l>0} p^{l-1} (2p) \frac{T^{\varphi_0}}{p^{2k_0}} \left(1 - \frac{T}{p}\right)^{-1} \\
 &= (p-1) \left(1 - \frac{T}{p}\right)^{-1} \sum_{l>0} \frac{T^{6l+1}}{p^{5l+2}} \\
 &= (p-1) \left(1 - \frac{T}{p}\right)^{-1} \frac{T^7}{p^7} \left(1 - \frac{T^6}{p^5}\right)^{-1} \\
 &= \frac{(p-1)T^7}{p(p-T)(p^5-T^6)}.
 \end{aligned}$$

A.6. The trunk of $x^2 - y^3$

Before drawing the trunk, let us first recall the trunk of a Hensel tree. In what follows, we will symbolize such a Hensel tree by the notation $\textcircled{\mathbf{H}}$.

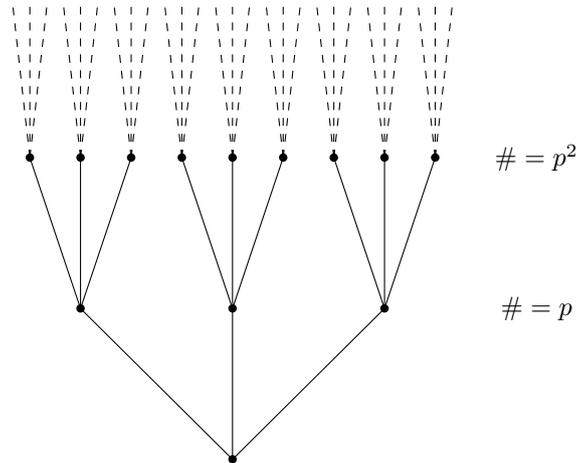


FIGURE 1. A Hensel tree for $n = 2$ variables, drawn here for $p = 3$. From each vertex there are p outgoing branches. All vertices have thickness 1.

We now depict the trunk of $P_0(x, y) = x^2 - y^3$ up to height 3. For a terminal vertex of the trunk (that is, one having no successor), we sometimes add the symbol \emptyset above the vertex in order to clarify the diagram.

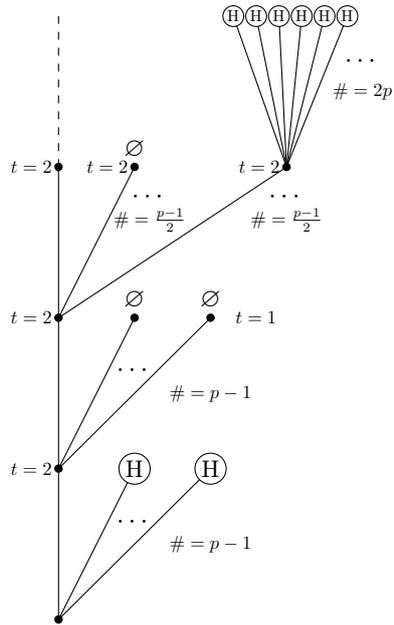


FIGURE 2. The trunk up to height 3. The drawing is for $p = 3$. The dotted parts and the numbers of branches correspond to the cases $p > 3$.

To obtain the complete trunk, one must understand the branches attached to the principal stalk. We start by representing the branches attached to a vertex of odd height.

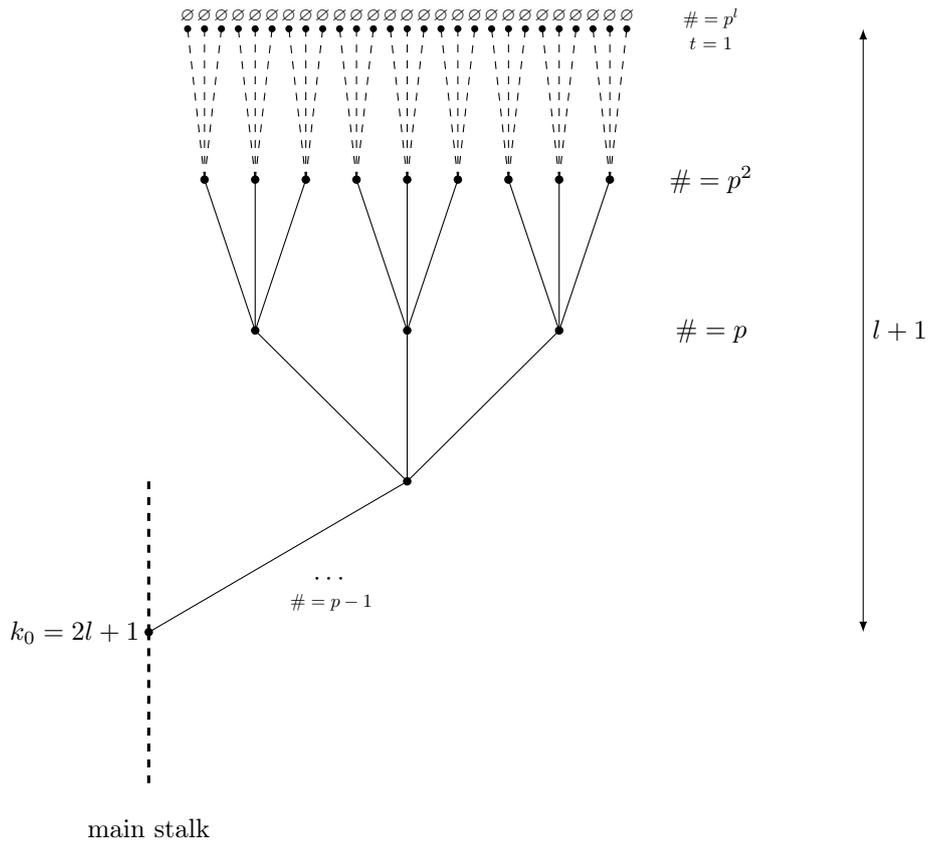


FIGURE 3. A branch attached to a vertex of odd height $2l + 1$ of the principal stalk. There are $p - 1$ such outgoing branches from this vertex. The branches are finite and stop at height $3l + 2$. All vertices have thickness 2, except the terminal vertices, which have thickness 1.

The branches attached to a vertex of even height split into two cases, according to whether the corresponding integer is a square modulo p or not.

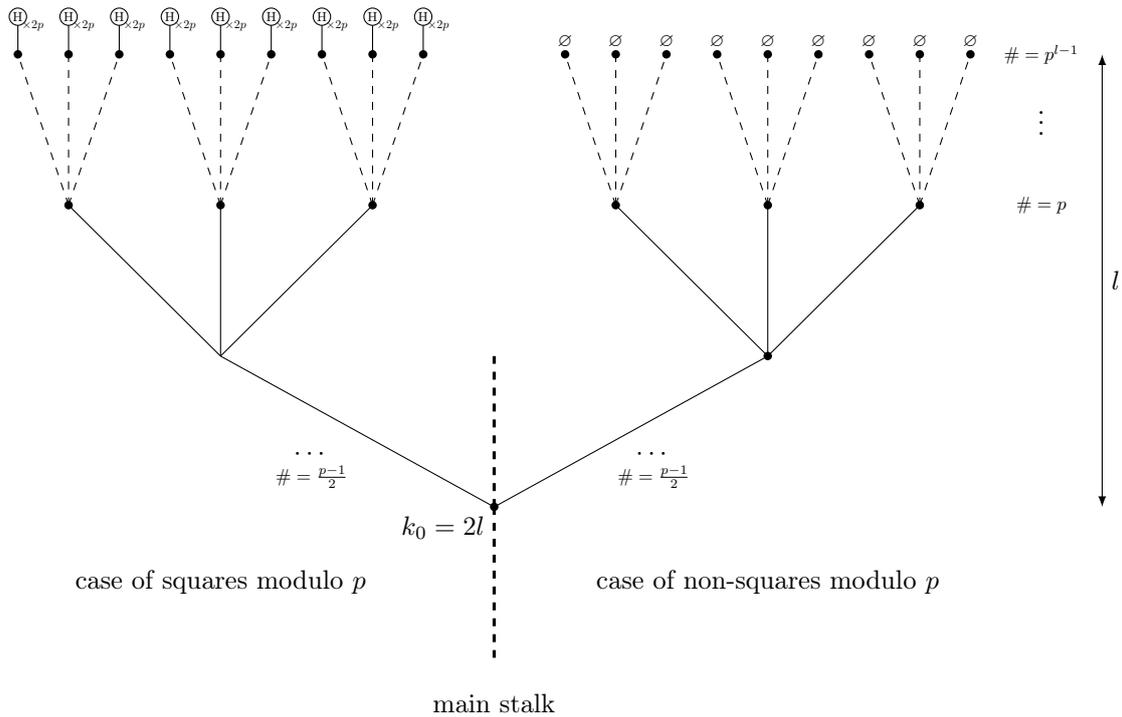


FIGURE 4. Two branches attached to a vertex of even height $2l$ (with $l > 0$) of the principal stalk. On the right, there are $\frac{p-1}{2}$ finite outgoing branches up to height $3l$, corresponding to integers that are not squares modulo p ; all their vertices have thickness 2. On the left, there are also $\frac{p-1}{2}$ outgoing branches corresponding to nonzero integers that are squares modulo p ; the vertices up to height $3l$ have thickness 2, and on each of the p^{l-1} vertices at height $3l$ are attached $2p$ Hensel trees.

A.7. The Poincaré series of $x^2 - y^3$

The Poincaré series $S(T)$ of $P(x, y) = x^2 - y^3$ for $p > 2$ is the sum of the Poincaré series computed for each part of the trunk:

$$S(T) = S_A(T) + S_B(T) + S_C(T) + S_D(T) + S_E(T) + S_F(T).$$

After computation, we finally obtain a rather simple fraction:

$$S(T) = \frac{p^6 + (p^4 - p^3)T^2 - T^6}{(p - T)(p^5 - T^6)}.$$

This formula is also valid for $p = 2$. It is indeed the same formula as the one obtained in [14].

If we expand this fraction as a power series, we obtain:

$$\begin{aligned} S(T) = & 1 + \frac{1}{p}T + \left(\frac{2}{p^2} - \frac{1}{p^3}\right)T^2 + \left(\frac{2}{p^3} - \frac{1}{p^4}\right)T^3 + \left(\frac{2}{p^4} - \frac{1}{p^5}\right)T^4 \\ & + \left(\frac{1}{p^5} - \frac{1}{p^6}\right)T^5 + \left(\frac{1}{p^5} + \frac{1}{p^6} - \frac{1}{p^7}\right)T^6 + \left(\frac{1}{p^6} + \frac{1}{p^7} - \frac{1}{p^8}\right)T^7 + \dots \end{aligned}$$

A.8. The number of solutions

By identifying the coefficients of $S(T)$ with those in the definition $S(T) = \sum_{e \geq 0} \frac{N_e}{p^{2e}} T^e$, we obtain the number of solutions of

$$x^2 - y^3 \equiv 0 \pmod{p^e}.$$

We thus find:

$$\begin{array}{ll}
 N_1 = p & N_5 = p^{10} \left(\frac{1}{p^5} - \frac{1}{p^6} \right) \\
 N_2 = p^4 \left(\frac{2}{p^2} - \frac{1}{p^3} \right) & N_6 = p^{12} \left(\frac{1}{p^5} + \frac{1}{p^6} - \frac{1}{p^7} \right) \\
 N_3 = p^6 \left(\frac{2}{p^3} - \frac{1}{p^4} \right) & N_7 = p^{14} \left(\frac{1}{p^6} + \frac{1}{p^7} - \frac{1}{p^8} \right) \\
 N_4 = p^8 \left(\frac{2}{p^4} - \frac{1}{p^5} \right) & \dots
 \end{array}$$

For example, for $p = 5$, we obtain:

$$\begin{array}{ll}
 N_1 = 5 & N_5 = 5625 \\
 N_2 = 45 & N_6 = 90\,625 \\
 N_3 = 225 & N_7 = 453\,125 \\
 N_4 = 1125 & \dots
 \end{array}$$

These are values N_e that can be checked by computer by enumerating all solutions when e is small. For larger e , the Poincaré series allows one to compute N_e efficiently. For example, still for $p = 5$ and for $e = 10$, among the $p^{2e} = 95\,367\,431\,640\,625$ possible pairs (x, y) , the number of solutions of

$$x^2 - y^3 \equiv 0 \pmod{5^{10}}$$

is

$$N_{10} = 95\,703\,125.$$

Email address: arnaud.bodin@univ-lille.fr

Email address: christian.drouin@wanadoo.fr

UNIVERSITÉ DE LILLE, CNRS, LABORATOIRE PAUL PAINLEVÉ, 59000 LILLE, FRANCE

SEIGNOSSE, FRANCE