SOLUTIONS OF A POLYNOMIAL EQUATION MODULO A PRIME POWER

ARNAUD BODIN AND CHRISTIAN DROUIN

Abstract. How do you find the integer solutions of a polynomial equation modulo an integer?

1. Introduction

1.1. Roots of polynomials over $\mathbb{Z}/n\mathbb{Z}$

If p is a prime number, the ring $\mathbb{Z}/p\mathbb{Z}$ is actually a field. Thus, a polynomial $P(X) \in \mathbb{Z}[X]$ of degree d has at most d roots in $\mathbb{Z}/p\mathbb{Z}$. Problems arise when calculations are done modulo an arbitrary integer n. For example, what are the solutions to the equation

$$x^2 + 11 \equiv 0 \pmod{15}?$$

There are 4 solutions $\{2, 7, 8, 13\}$ even though the equation is indeed a polynomial equation of degree 2.

Even very simple equations can have surprisingly many solutions. For instance, take $P(X) = X^2$. When working modulo p^{2e} with $p > 2$, the equation

$$x^2 \equiv 0 \pmod{p^{2e}}$$

has not two but p^e distinct solutions:

$$x_i = ip^e \quad \text{for } i = 0, 1, \ldots, p^e - 1.$$

Thus, even a degree 2 polynomial can have exponentially many solutions as the modulus grows.

Finally, Shamir [10] gave the remarkable example of the polynomial $P(X) = X$, which factors in a surprising way modulo a composite number $n = pq$ with two distinct primes:

$$X \equiv (p^2 + q^2)^{-1}(pX + q)(qX + p) \pmod{pq},$$

where $p^2 + q^2$ is invertible modulo n, and $pX + q$ and $qX + p$ are irreducible over $\mathbb{Z}/n\mathbb{Z}$. Even such a simple polynomial can behave in subtle ways when the modulus is not prime.

1.2. Reduction to a prime power modulus

How should one understand these phenomena? If p is prime, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field, so a polynomial of degree d has at most d roots modulo p.
If $n = \prod_{i=1}^{l} p_i^{e_i}$ is the prime factorization, then solving $P(x) \equiv 0 \pmod{n}$ is equivalent to solving $P(x) \equiv 0 \pmod{p_i^{e_i}}$ for each $i = 1, \ldots, l$. This reduction follows from the Chinese Remainder Theorem, which also provides an efficient way to recombine the solutions modulo each prime power into solutions modulo n, using only modular inverses.
But is the problem of determining the roots of a polynomial simpler if the modulus is just a power of a prime number? In fact, no! For example, the polynomial X^2 of degree 2 already has 3 roots $\{0, 3, 6\}$ modulo 3^2. Thus, the real source of complications is already present when $n = p^e$ is a prime power.

Date: October 7, 2025.
2020 *Mathematics Subject Classification.* Primary 11A07; Sec. 11D45, 11S05.
Key words and phrases. polynomial, congruence, tree.

Let p be a prime number, $e \geqslant 0$ an integer, and $P(X) \in \mathbb{Z}[X]$. The purpose of this article is to calculate the integer solutions x of the equation $P(x) \equiv 0 \pmod{p^e}$, and to understand how these solutions evolve as e grows.

1.3. **Outline**

In this note, we explain how the solutions of the equations $P(x) \equiv 0 \pmod{p^e}$ evolve as e grows, and how they can all be represented in the form of a *tree*. Each vertex corresponds to a solution modulo p^e, and its children are the solutions of the same equation modulo p^{e+1} that reduce to it modulo p^e. The figure below represents the set of solutions to the equations $P(x) \equiv 0 \pmod{p^e}$ for $P(X) = (X^2+3)(X^2+3X+9)$, with $p = 3$, for different values of e. (This example will be revisited later, see Examples 2.2 and 3.2.)

Since this tree can have many vertices, our goal is to concentrate all this information into a much smaller subtree, the *trunk*. (In our example, this corresponds to the subtree with two edges in red, drawn with thick lines in the figure.) To each vertex of the trunk, we attach an integer called the *thickness*.

The trunk allows the complete reconstruction of the solution tree (Theorem 3.1): starting from each vertex of the trunk, we build a *fan* of solutions emerging from this vertex. In the figure below there are two fans: the first one consists of all possible children of the vertex 0 at level 1, up to level $t_1 = 3$ (t_1 being the thickness at this vertex of level 1). The second fan starts at the vertex 3 at level 2, up to level $t_1 + t_2 = 4$ (t_2 being the thickness at this vertex of level 2). Alternatively, one could simply count the number of solutions at each level p^e without enumerating them (Corollary 6.1).

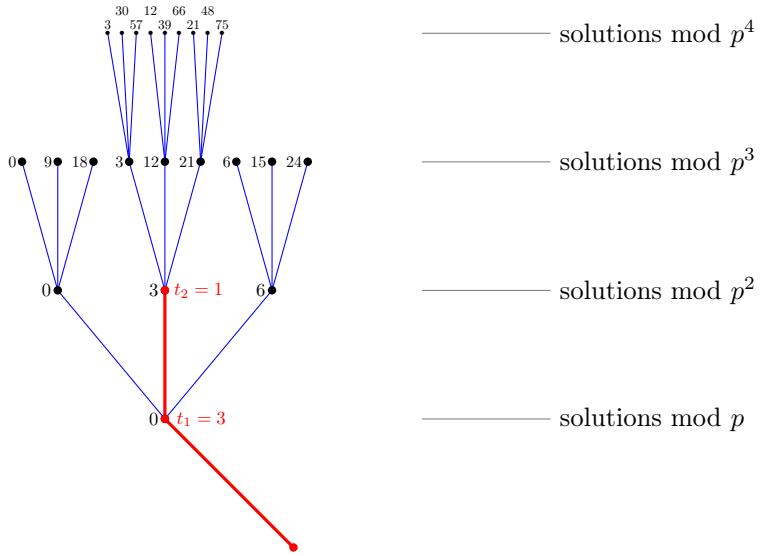

FIGURE 1. The trunk and the tree of solutions of $P(X) = (X^2+3)(X^2+3X+9)$, $p = 3$.

2. Trees and trunks

2.1. p-adic congruence tree

We fix $p \geqslant 2$ a prime number. The ***p-adic congruence tree***, denoted Ω_p, is an infinite tree whose root is the pair $(0,0)$ of level $e = 0$ and whose vertices of level e are the pairs (x, e), where the integer x is between 0 and $p^e - 1$. The edges of this tree are those connecting two vertices (x, e) and $(x', e+1)$ such that $x' \equiv x \pmod{p^e}$. Thus, we can define a partial order relation on

the vertices of this graph by: $(x,e) \lhd (x',e')$ if and only if $e \leqslant e'$ and $x' \equiv x \pmod{p^e}$. In other words, (x,e) is located on the path connecting the root to (x',e').

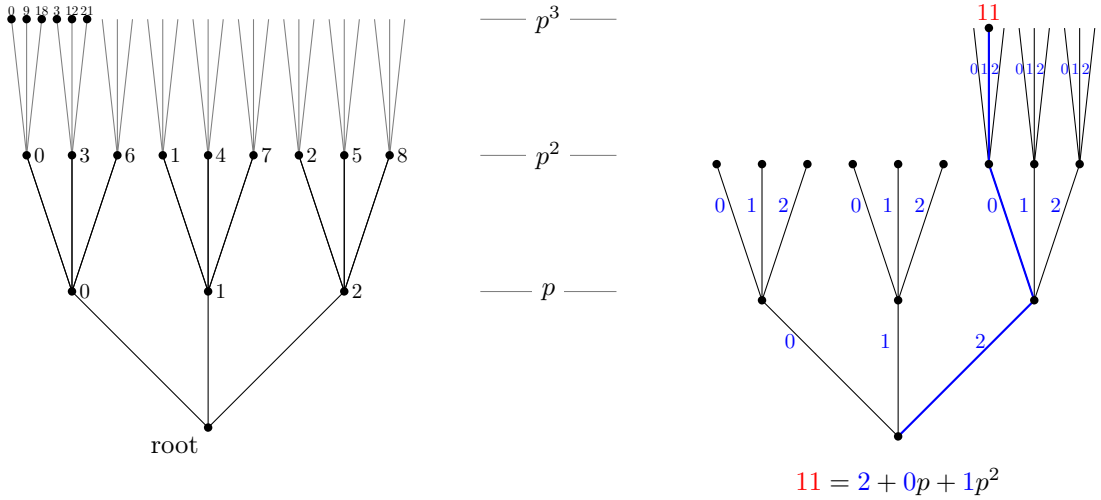

FIGURE 2. Here $p = 3$. Left: the p-adic congruence tree Ω_p, each vertex is labeled by in integer $x \in [0, p^e - 1]$. Right: the decomposition of $x = 11$ in base p, each edge is labeled by a integer $a_i \in [0, p-1]$.

For a given vertex, we can consider that each outgoing edge is indexed by an integer between 0 and $p-1$. A vertex of the tree corresponds to an integer $x \in \mathbb{Z}$, the path from the root of the tree to this vertex corresponds to its p-adic decomposition, i.e. a finite sum $x = \sum_{i \geqslant 0} a_i p^i$ with $0 \leqslant a_i \leqslant p-1$ (for each $i \geqslant 0$). The infinite paths in the tree correspond to coherent sequences of residues and naturally form a ring, which is exactly the ring of p-adic integers $\mathbb{Z}_p$.

2.2. **Solution tree**

Let $P(X) \in \mathbb{Z}[X]$ be a polynomial with integer coefficients. We denote:

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

This ***solution tree*** may be finite or infinite. Let us verify that $\mathrm{Tree}(P)$ is indeed a tree: let $(x,e) \lhd (x',e')$ with $(x',e') \in \mathrm{Tree}(P)$, then $x \equiv x' \pmod{p^e}$ hence $P(x) \equiv P(x') \equiv 0 \pmod{p^e}$ and thus we also have $(x,e) \in \mathrm{Tree}(P)$.
In particular, infinite paths in $\mathrm{Tree}(P)$ (that is, sequences (x_e, e) with $P(x_e) \equiv 0 \mod p^e$ and $x_{e+1} \equiv x_e \mod p^e$) correspond to roots in $\mathbb{Z}_p$ of the polynomial P, meaning p-adic integers α such that $P(\alpha) = 0$ in $\mathbb{Z}_p$.

2.3. **Thickness**

Let $P \in \mathbb{Z}[X]$ be a polynomial of degree d. To simplify the presentation throughout this article, we assume that p does not divide $P(X)$ in $\mathbb{Z}[X]$, in other words, the coefficients of P are not simultaneously all divisible by p. This is not a significant loss of generality; if this assumption were not verified, we would start by writing $P(X) = p^{t_0} Q(X)$ where p does not divide $Q(X)$ and then all the results would apply to $Q(X)$.

Definition 2.1. Let $r \in \mathbb{Z}$. The ***thickness*** t of P at r is the largest integer such that there exists $Q(X) \in \mathbb{Z}[X]$ such that:

$$P(r + pX) = p^t Q(X)$$

The polynomial Q is the ***successor*** of P for the root r.

Note that the definition of thickness is only meaningful for the roots of P modulo p:

$$P(r) \equiv 0 \pmod{p} \iff t \geqslant 1$$

Also note that by the maximality of t, p does not divide $Q(X)$ in $\mathbb{Z}[X]$.

2.4. **Trunk of a polynomial**

For a polynomial $P \in \mathbb{Z}[X]$, we now define its ***trunk*** and the ***thicknesses*** associated with its vertices. We will denote the trunk by $\mathrm{Trunk}(P)$. It is a subtree, maybe infinite, of the solution tree $\mathrm{Tree}(P)$.
We set $P_0 = P$. We define the structure of the trunk inductively, with each level built from the previous one. At each step, we look for roots modulo p of the current polynomial P_k. For each such root r, we consider the polynomial $P_k(r + pX)$ and factor out the highest power p^t of p (t is the thickness). We then define the successor polynomial associated with r as $P_{k+1}(X) = \frac{1}{p^t} P_k(r + pX)$.
More precisely:

- *Level* 0. We set $(r, k) = (0, 0) \in \mathrm{Trunk}(P)$. This is the only vertex of the trunk to which no thickness is associated.
- *Level* 1. For each $r_0 \in [\![0, p-1]\!]$ such that $P(r_0) \equiv 0 \pmod{p}$, we compute the decomposition $P(r_0 + pX) = p^{t_1} Q(X)$ and include in the trunk the vertex $(r_0, 1)$ associated with the thickness t_1.
- *Level* 2. For the successor Q of P at each r_0 from the previous step, we look for solutions $r_1 \in [\![0, p-1]\!]$ such that $Q(r_1) \equiv 0 \pmod{p}$; we compute the decomposition $Q(r_1+pX) = p^{t_2} R(X)$; the pair $(r_0+pr_1, 2)$ is a new element of $\mathrm{Trunk}(P)$ associated with the thickness t_2.
- *From level k to level $k+1$.* By induction, suppose that $(r_0+pr_1+p^2r_2+\cdots+p^{k-1}r_{k-1}, k) \in \mathrm{Trunk}(P)$ with the polynomial P_k obtained as a successor of r_{k-1}. We look for solutions $r_k \in [\![0, p-1]\!]$ such that $P_k(r_k) \equiv 0 \pmod{p}$; we compute the decomposition $P_k(r_k + pX) = p^{t_{k+1}} P_{k+1}(X)$; the pair $(r_0 + pr_1 + p^2 r_2 + \cdots + p^k r_k, k + 1)$ is an element of $\mathrm{Trunk}(P)$ associated with the thickness t_{k+1}.

The ***tree-top function*** associates to each vertex (r, k) of $\mathrm{Trunk}(P)$ is the sum of the thicknesses encountered on the path to the root. In other words,

$$\varphi(r, k) = t_1 + t_2 + \cdots + t_k.$$

where each t_i is the thickness at level i of the vertex on the path between the root and the vertex (r, k).

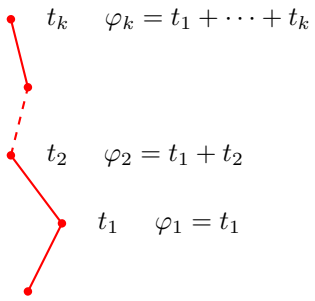

FIGURE 3. Thickness and the tree-top function φ.

2.5. **An example**

Before stating the theorem, let's go through an example to better understand these concepts. We explain the computation of the trunk illustrated in Figure 5.

Example 2.2. Let $P(X) = (X^2+3)(X^2+3X+9)$ and $p = 3$. The reduction modulo p of P is $\overline{P}(X) = X^4$. Thus for $r_0 = 0$, we have $P(r_0) \equiv 0 \pmod 3$. The decomposition of $P(r_0 + pX)$ is $P(3X) = 3^3(3X^2+1)(X^2+X+1)$. Thus the thickness associated with r_0 is $t_1 = 3$ and the successor of P at r_0 is $P_1(X) = (3X^2+1)(X^2+X+1)$. The first vertex of the trunk is thus $(r_0, 1) = (0, 1)$ associated with a thickness $t_1 = 3$.
We start again, from P_1: $\overline{P_1}(X) = X^2+X+1$ vanishes modulo 3 at $r_1 = 1$, and the decomposition of $P_1(r_1 + pX)$ is $P_1(1+3X) = 3^1(27X^2+18X+4)(3X^2+3X+1)$. Thus the second vertex of the trunk is $(r_0 + pr_1, 2) = (3, 2)$ associated with a thickness $t_2 = 1$.
The successor of P_1 at r_1 is $P_2(X) = (27X^2+18X+4)(3X^2+3X+1)$, which does not vanish modulo $p = 3$. Thus, the calculations stop here.
In summary, besides the root $(0, 0)$, the trunk is composed of vertices $(0, 1)$ (with $t_1 = 3$) and $(3, 2)$ (with $t_2 = 1$).

3. Main theorem

3.1. **From the trunk to the tree**

We recall that:

$$P(x) \equiv 0 \pmod{p^e} \iff (x, e) \in \mathrm{Tree}(P)$$

The following theorem indicates how $\mathrm{Trunk}(P)$ determines the roots $\mathrm{Tree}(P)$ of a polynomial P, via the tree-top function φ associated with the trunk. What's the benefit? The trunk is easily computed from P and its number of vertices for a fixed level e is bounded by the degree of P (see Section 7), unlike the tree $\mathrm{Tree}(P)$, which can have a number of vertices that grows exponentially with level e.

Theorem 3.1.

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

Thus, to know if x is a root of P modulo p^e, it suffices to check a combinatorial condition on x (modulo a certain p^k). Since these solutions can be numerous, one might want to simply calculate their number without explicitly listing them all; this will be done in Section 6.

Let us reformulate these results to explain how the solution tree is recovered from the trunk by adding fans. The ***fan*** of a vertex (r, k) up to level h is the set of vertices of Ω_p, issued from vertex (r, k) up to level h:

$$\mathrm{Fan}_{\leqslant h}(r,k) = \big\{(x,l) \in \Omega_p \mid (r,k) \lhd (x,l) \text{ and } l \leqslant h\big\}$$

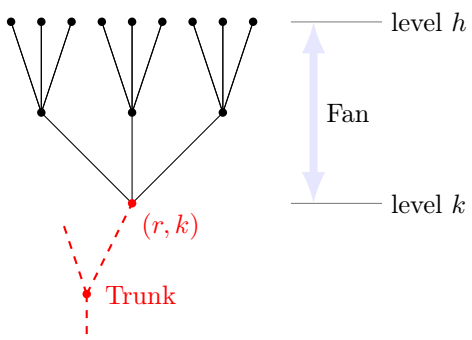

FIGURE 4. A fan.

Thus, Theorem 3.1 is reformulated as:

$$\mathrm{Tree}(P) = \bigcup_{(r,k)\in \mathrm{Trunk}(P)} \mathrm{Fan}_{\leqslant \varphi(r,k)}(r,k)$$

Since the thickness is always at least 1, we have $k \leqslant \varphi(r,k)$, and therefore the vertex (r,k) is indeed an element of $\mathrm{Fan}_{\leqslant \varphi(r,k)}(r,k)$. Moreover, if the trunk is a finite tree, then there exists $e \geqslant 0$ such that the equation $P(x) \equiv 0 \pmod{p^e}$ has no integer solutions.

3.2. **First example for the main theorem**

Let us compute the tree of Example 2.2, which is already depicted in Figure 1.

Example 3.2. Let $P(X) = (X^2+3)(X^2+3X+9)$ and $p = 3$. In the figure below on the left, we have the trunk of P, which is a tree with only 3 vertices (the computation has been done in Example 2.2). The vertex $(0,1)$ has a thickness $t_1 = 3$ (and thus a tree-top function value of $\varphi_1 = t_1 = 3$); the vertex $(3,2)$ has a thickness $t_2 = 1$ and thus a tree-top function value of $\varphi_2 = t_1 + t_2 = 4$. To obtain the solution tree, below on the right: we start from the trunk of P; to the vertex $(0,1)$ we adjoin the fan originating from this vertex that goes up to level $\varphi_1 = 3$; to the vertex $(3,2)$ we adjoin the fan originating from this vertex that goes up to level $\varphi_2 = 4$.

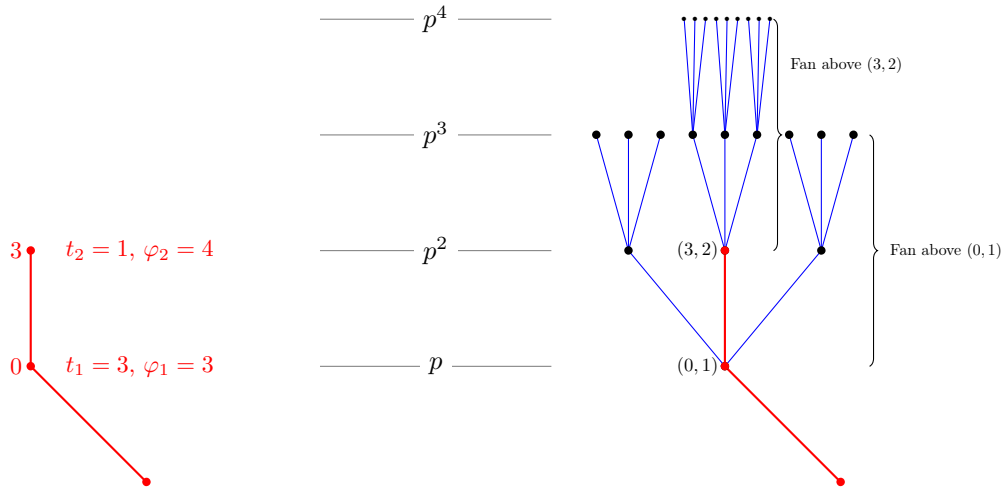

FIGURE 5. The tree from the trunk.

From the tree, we read the solutions of the equation $P(x) \equiv 0 \pmod{p^e}$ for different values of e. The formula from Corollary 6.1 will allow us to count the number N_e of solutions without explicitly enumerating them.

p^e	solutions	N_e
3^1	0	1
3^2	$0, 3, 6$	3
3^3	$0, 3, 6, 9, 12, 15, 18, 21, 24$	9
3^4	$3, 12, 21, 30, 39, 48, 57, 66, 75$	9

For $e \geqslant 5$, the equation has no solutions.

3.3. **Second example**

We will consider an example in which the congruence $P(x) \equiv 0 \pmod{p^e}$ has solutions for every $e \geqslant 1$. One situation where this happens is when there is a simple root modulo p, that is $P(x_1) \equiv 0 \pmod{p}$ but $P'(x_1) \not\equiv 0 \pmod{p}$. Then Hensel's lemma (see [1] or [7]) shows that this root can be lifted indefinitely to solutions modulo $p^2, p^3, \ldots$, thereby producing an infinite branch in the solution tree whose vertices all have thickness 1 (see Lemma 4.1).

Theorem 3.3 (Hensel's Lemma)**.** *Let $P(x) \in \mathbb{Z}[x]$ and $x_1 \in \mathbb{Z}$ be such that $P(x_1) \equiv 0 \pmod{p}$ and $P'(x_1) \not\equiv 0 \pmod{p}$. Then, for every integer $e \geqslant 1$, there exists a unique integer x_e (determined modulo p^e) satisfying $P(x_e) \equiv 0 \pmod{p^e}$ and $x_e \equiv x_1 \pmod{p}$.*

The idea of the proof is a variant of Newton's method for finding roots. We proceed by induction on the exponent e. The first step is a Taylor expansion around the known root x_1:

$$P(x_1 + hp) \equiv P(x_1) + hpP'(x_1) \pmod{p^2}.$$

Since $p \mid P(x_1)$, write $P(x_1) = p \cdot C$ and let D be an inverse of $P'(x_1)$ modulo p. Then set $h_0 = -\frac{P(x_1)}{p} D = -CD$. By construction,

$$P\big(x_1 + h_0 p\big) \equiv P(x_1) + h_0 p P'(x_1) \equiv pC\big(1 - DP'(x_1)\big) \equiv 0 \pmod{p^2},$$

so $x_2 = x_1 + h_0 p$ is indeed a root modulo p^2. From there one continues inductively to lift to all higher powers of p.

Example 3.4. Let $P(X) = X(X-1)^2 + 5^2$ and consider $p = 5$.

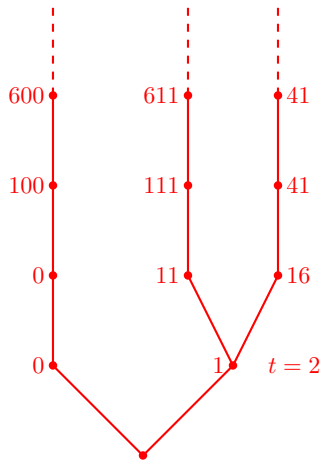

FIGURE 6. Trunk with infinite branches. All non-marked thicknesses equal 1.

The root 0 is a simple root of P modulo 5, meaning that $P'(0) \not\equiv 0 \pmod 5$. By Hensel's lemma, this root can be lifted indefinitely to solutions modulo each p^e. This results in an infinite branch of the trunk (on the left in Figure 6). At each level of this branch, the thickness is 1, so the part of the solution tree corresponding to this branch coincides with the branch itself. In summary, for each level e, there is a unique solution x satisfying $x \equiv 0 \pmod p$ and $P(x) \equiv 0 \pmod{p^e}$. The root 1 is not a simple root; it has thickness 2. After level 1, the trunk splits into two infinite branches, each of thickness 1. The solution tree can be recovered from the trunk by Theorem 3.1 (but is not pictured in Figure 6).

p^e	solution above 0	solutions above 1	N_e
5^1	0	1	2
5^2	0	$1, 6, 11, 16, 21$	6
5^3	100	$11, 16, 36, 41, 61, 66, 86, 91, 111, 116$	11
5^4	600	$41, 111, 166, 236, 291, 361, 416, 486, 541, 611$	11

For all $e \geqslant 5$, the number of solutions remains $N_e = 11$.

Remark. There may exist infinite branches with vertices of thickness greater than 1; an example will be given in Section 8. Such infinite branches correspond to multiple roots of the polynomial $P(X)$ in the ring $\mathbb{Z}_p$ of p-adic integers, and are therefore associated with multiple factors in the decomposition of $P(X)$ into irreducible factors in $\mathbb{Z}[X]$. It is also possible to detect whether a branch beginning with vertices of thickness greater than 1 will extend to infinity; see [5, Section 3].

4. Thickness

In this section, we provide further information and properties about the thickness.

4.1. Characterization by Taylor's formula

Lemma 4.1.

$$t = \min_{i \geqslant 0} \operatorname{val}_p \left(\frac{P^{(i)}(r)}{i!} p^i \right)$$

And in particular $t \leqslant d$.

We recall that $\operatorname{val}_p(x)$, the ***valuation*** at p of an integer x, is the largest exponent i such that p^i divides x. For example $\operatorname{val}_p(p^i) = i$. Also, for any $r \in \mathbb{Z}$ and $i \geqslant 0$, $\frac{P^{(i)}(r)}{i!}$ is an integer. As an application of this lemma, $t = 1$ iff r is a simple root modulo p, i.e. $P(r) \equiv 0 \pmod p$ and $P'(r) \not\equiv 0 \pmod p$.

Proof. The Taylor formula for P around the root r is written:

$$P(r+X) = P(r) + P'(r)X + \frac{P''(r)}{2!}X^2 + \cdots + \frac{P^{(i)}(r)}{i!}X^i + \cdots + \frac{P^{(d)}(r)}{d!}X^d$$

This gives:

$$P(r+pX) = P(r) + P'(r)pX + \frac{P''(r)}{2!}p^2X^2 + \cdots + \frac{P^{(i)}(r)}{i!}p^iX^i + \cdots$$

Let t be the thickness of P at r and $t' = \min_{i \geqslant 0} \operatorname{val}_p \left(\frac{P^{(i)}(r)}{i!} p^i \right)$.

Since p^t divides the polynomial $P(r+pX)$, then p^t divides all the coefficients $\frac{P^{(i)}(r)}{i!}p^i$ of $P(r+pX)$, thus $t \leqslant t'$. Conversely, by Taylor's formula, $p^{t'}$ divides all the coefficients of $P(r+pX)$, hence $t' \leqslant t$. □

Lemma 4.2. *The thickness t of P at r is less than or equal to the multiplicity* $\operatorname{mult}(r)$ *of the root r as a root of the polynomial $\overline{P} \in \mathbb{Z}/p\mathbb{Z}[X]$.*

We will also prove in Lemma 4.6 that the thickness can only decrease as we ascend the tree.

Proof. To simplify the proof, and without loss of generality, we can assume $r = 0$. Let us write $P(X) = \sum_{0 \leqslant i \leqslant d} a_i X^i$. Then p^t divides $P(pX)$, so p^t divides the $a_i p^i$ (for $0 \leqslant i \leqslant d$). Thus p divides a_i for $i < t$, so after reduction modulo p, $\overline{P}(X) = \overline{a_t} X^t + \cdots + \overline{a_d} X^d$ factors through X^t. Thus the multiplicity of $r = 0$ as a root of $\overline{P}$ is greater than or equal to t. □

4.2. **Residual degree**

Definition 4.3. Let $P \in \mathbb{Z}[X]$ of thickness t at $r \in \mathbb{Z}$, associated with the decomposition $P(r + pX) = p^t Q(X)$. The ***residual degree*** of P at r, denoted s, is the degree of the reduction of Q in $\mathbb{Z}/p\mathbb{Z}[X]$. In other words, $s = \deg \overline{Q}$.

Lemma 4.4. *The residual degree s is at most t, and is the largest integer $i \geqslant 0$ such that*

$$\operatorname{val}_p\left(\frac{P^{(i)}(r)}{i!} p^i\right) = t.$$

Example 4.5. Let $P(X) = X^3 + pX^2 + pX$. The thickness of the root $r = 0$ is $t = 2$ because $P(pX) = p^2 Q(X)$ where $Q(X) = pX^3 + pX^2 + X$. The residual degree is $s = 1$ because the reduction of Q modulo p is of degree 1.

Proof. To simplify the writing of the proof, we can again assume without loss of generality that $r = 0$ and write $P(pX) = p^t Q(X)$. Let $P(X) = \sum_{0 \leqslant i \leqslant d} a_i X^i$. By Taylor's formula, $a_i = \frac{P^{(i)}(r)}{i!}$. By hypothesis p^t divides $P(pX)$, so $p^t \mid a_i p^i$ for all $0 \leqslant i \leqslant d$. Thus:

$$\begin{aligned}
\deg \overline{Q} = s &\iff p^{t+1} \nmid a_s p^s \text{ and } p^{t+1} \mid a_i p^i \text{ for all } i > s \\
&\iff \operatorname{val}_p(a_s p^s) = t \text{ and } \operatorname{val}_p(a_i p^i) > t \text{ for all } i > s \\
&\iff s \text{ is the largest integer such that } \operatorname{val}_p(a_i p^i) = t
\end{aligned}$$

Finally $t \geqslant s$ because:

$$t = \min_{0 \leqslant i \leqslant d} \left[\operatorname{val}_p\left(\frac{P^{(i)}(r)}{i!}\right) + i \right] = \operatorname{val}_p\left(\frac{P^{(s)}(r)}{s!}\right) + s$$

□

4.3. **Node rule**

Lemma 4.6 (Node rule)**.** *Let $(r, k) \in \operatorname{Trunk}(P)$ with thickness t and residual degree s. Let $(r_i, k+1) \in \operatorname{Trunk}(P)$ of thickness t_i be the children of (r, k), $i = 1, \ldots, l$. Then:*

$$t_1 + t_2 + \cdots + t_l \leqslant s \leqslant t$$

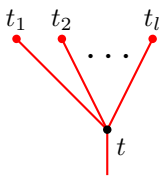

FIGURE 7. The node rule: $t_1 + t_2 + \cdots + t_l \leqslant t$.

Proof. Let $P(r + pX) = p^t Q(X)$. Let $r_i = r + \rho_i p^k$, $i = 1, \ldots, l$ where ρ_i are the roots of Q modulo p. Consider the decomposition of the reduction of Q modulo p according to its roots:

$$\overline{Q}(X) = (X - \rho_1)^{\mu_1} \cdots (X - \rho_l)^{\mu_l} I(X) \in \mathbb{Z}/p\mathbb{Z}[X]$$

where $I(X)$ has no roots modulo p. By Lemma 4.2, the thickness is less than or equal to the multiplicity: $t_i \leqslant \mu_i$. Thus, remembering that $\deg \overline{Q}$ is by definition the residual degree s and that $s \leqslant t$ (Lemma 4.4):

$$\sum_{1 \leqslant i \leqslant l} t_i \leqslant \sum_{1 \leqslant i \leqslant l} \mu_i \leqslant \deg \overline{Q} = s \leqslant t$$

□

5. Construction of the solution tree from the trunk

Now that we have defined the trunk and explained its main properties, it is time to prove Theorem 3.1 which explains how to compute the tree $\mathrm{Tree}(P)$ of solutions $P(x) \equiv 0 \pmod{p^e}$ from the trunk $\mathrm{Trunk}(P)$, via the formula:

$$P(x) \equiv 0 \pmod{p^e} \iff \text{there exists } (r,k) \in \mathrm{Trunk}(P) \text{ such that } x \equiv r \pmod{p^k} \text{ and } \varphi(r,k) \geqslant e$$

5.1. Tree-top function

For $(r,k) \in \mathrm{Trunk}(P)$, let $t_1, \dots, t_k$ be the thicknesses associated with the path from the root to the vertex (r,k). Let $\varphi = \varphi(r,k) = t_1 + \cdots + t_k$ be the value of the tree-top function at this vertex.

Lemma 5.1. *There exists a decomposition*

$$P(r + p^k X) = p^{\varphi} Q(X)$$

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

Proof. Let $r = r_0 + r_1 p + r_2 p^2 + \cdots + r_{k-1} p^{k-1}$ be the p-adic expansion of r. Then $P(r_0 + pX) = p^{t_1} P_1(X)$ where P_1 denotes the successor of P for the root r_0, hence

$$P(r_0 + r_1 p + p^2 X) = P\big(r_0 + p(r_1 + pX)\big) = p^{t_1} P_1(r_1 + pX) = p^{t_1+t_2} P_2(X)$$

where P_2 is the successor of P_1 for the root r_1. By induction, $P(r + p^k X) = p^{t_1+\cdots+t_k} P_k(X)$ with $P_k(X) \in \mathbb{Z}[X]$. □

5.2. Proof of Theorem 3.1

Let $(x,e) \in \Omega_p$. We want to know if $P(x) \equiv 0 \pmod{p^e}$, that is if $(x,e) \in \mathrm{Tree}(P)$. Let $(r,k) \in \mathrm{Trunk}(P)$ be the most recent ancestor of (x,e) belonging to the trunk of P. We have $x = r + p^k y$ (where $y \in \mathbb{Z}$).

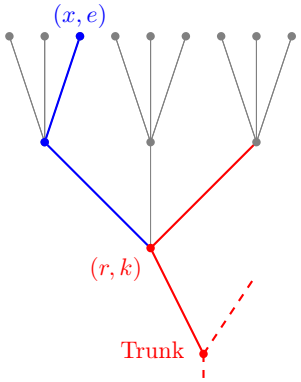

Figure 8. The most recent ancestor of (x,e).

Using the notations of Lemma 5.1, we have:

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

where $\varphi(r,k)$ is the value of the tree-top function. But additionally, we know that $Q(y) \not\equiv 0 \pmod{p}$ because otherwise (r,k) would not be the most recent ancestor of (x,e) belonging to the trunk.
Thus:

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

where for the last equivalence we used that $Q(y) \not\equiv 0 \pmod{p}$.
Moreover, for a given solution x, such a pair (r,k) is unique if we impose the condition:

$$\varphi(r,k) - t_k < e \leqslant \varphi(r,k)$$

where t_k is the thickness of the vertex (r,k). This means that a vertex (r,k) of the trunk corresponds uniquely to roots whose level is strictly greater than $\varphi(r,k) - t_k$ but less than or equal to $\varphi(r,k)$.

6. Number of solutions

We will extract from Theorem 3.1 a formula that allows us to directly compute the number of solutions from the trunk.

6.1. **Formula**

Corollary 6.1. *The number of solutions of the equation $P(x) \equiv 0 \pmod{p^e}$ in $\mathbb{Z}/p^e\mathbb{Z}$ is:*

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

Proof. We have seen that the fan originating from the vertex (r,k) of the trunk produces solutions up to the height $\varphi(r,k)$. Let $(r^-, k-1)$ be the direct predecessor of (r,k) (that is, the vertex of the trunk adjacent to (r,k) on the side of the root). By denoting t as the thickness of (r,k) and $\varphi(r,k)$ as the tree-top function, we obtain: $\varphi(r^-, k-1) = \varphi(r,k) - t$. Thus, the vertex $(r^-, k-1)$ produces solutions up to the height $\varphi(r,k) - t$. Therefore the solutions x, whose height e satisfies $\varphi(r,k) - t < e \leqslant \varphi(r,k)$, are uniquely associated with the single element (r,k) of the trunk.
How many solutions does such a vertex (r,k) of the trunk produce? The fan originating from (r,k) has: 1 vertex at level k, p vertices at level $k+1$, p^2 vertices at level $k+2$, and so on. Thus, for a given level e, we associate p^{e-k} solutions. The condition $\varphi(r,k) - t < e \leqslant \varphi(r,k)$ ensures that this level e is reached by this vertex (r,k) but not by any other vertices of the trunk. □

6.2. **Example**

The formula from Corollary 6.1 allows us to count the number N_e of solutions without explicitly enumerating them. We return to our favorite example, whose trunk was computed in Example 2.2 and whose solutions were computed in Example 3.2.

Example 6.2. Let $P(X) = (X^2+3)(X^2+3X+9)$ and $p = 3$. The vertex $(0,1)$ at level $k = 1$ of the trunk satisfies $\varphi_1 = 3$ and $t_1 = 3$. It contributes to the solutions modulo p^e for levels e satisfying $\varphi_1 - t_1 < e \leqslant \varphi_1$, that is, $e = 1, 2, 3$. Thus, $N_e = p^{e-k} = p^{e-1} = 3^{e-1}$ for $e = 1, 2, 3$.
The vertex $(3,2)$ at level $k = 2$ of the trunk satisfies $\varphi_2 = 4$ and $t_2 = 1$. It contributes to the solutions modulo p^e for levels e satisfying $\varphi_2 - t_2 < e \leqslant \varphi_2$, which means only at level $e = 4$, and thus $N_4 = p^{4-2} = 9$. For $e \geqslant 5$, we have $N_e = 0$.

7. Structure of solutions

7.1. **Algorithmic aspects**

This is a well-studied aspect (see references in Section 9.2). Here we will just explain that expressing the set of solutions in a compact form is easy, meaning it is done in polynomial complexity (depending on the degree of the polynomial and the level e; the prime p being fixed), even though the number of these solutions can exponentially depend on these data.
The main reason this is possible is that the trunk is considerably simpler than the tree, even though by Theorem 3.1 they are combinatorially equivalent data. Indeed, the number of vertices of $\mathrm{Trunk}(P)$ located at a fixed level is bounded by d (the degree of P). The proof for level $k = 1$ is simply that the number of roots of P on the field $\mathbb{Z}/p\mathbb{Z}$ is less than d. This remains true for any level by induction thanks to the node rule (Lemma 4.6).

Let's outline the algorithm for computing the trunk and the set of solutions of the equation $P(x) \equiv 0 \pmod{p^e}$.
Data. p a prime number; $P \in \mathbb{Z}[X]$ of degree d; $e \geqslant 0$ an integer.
Goal. Compute all solutions $P(x) \equiv 0 \pmod{p^e}$ for $x \in \mathbb{Z}/p^e\mathbb{Z}$.
Step a. Find solutions modulo p: solve $P(x) \equiv 0 \pmod{p}$ by exhaustive search on $0 \leqslant x \leqslant p-1$. The polynomial P of degree d on the field $\mathbb{Z}/p\mathbb{Z}$ has at most d roots (and at most p distinct roots). Each solution gives a vertex of the trunk.
Step b. Compute the thickness and decomposition $P(r + pX) = p^t Q(X)$ for each root r from the previous step. This is done through a sequence of elementary operations: (i) translation $P(X) \to P(a + X)$; (ii) substitution $P(X) \to P(pX)$; (iii) coefficient valuation. Associate the thickness with the corresponding vertex of the trunk.
Iteration. Each successor of Q from the previous step, once reduced modulo p, has a degree equal to the residual degree (thus less than or equal to d, see Lemma 4.4), and additionally, by the node rule (Lemma 4.6), the total number of vertices for a given level is bounded by d. Thus each step **a** or **b** is repeated at most $d \cdot e$ times.

The algorithms for calculating the trunk, the solution tree, and the formula for the number of solutions have been implemented via the computer algebra system *Sage* [11].

7.2. **Degrees**

Let $P \in \mathbb{Z}[X]$.

- We denote d as the degree of P in $\mathbb{Z}[X]$.
- We denote d_p as the degree in $\mathbb{Z}/p\mathbb{Z}[X]$ of the reduction of P modulo p.
- We denote d_{Trunk} as the number of leaves of the trunk $\mathrm{Trunk}(P)$; each infinite branch of the tree counts as a leaf, in addition to the finite leaves.

These quantities allow for a rough estimate of the complexity of the trunk of P.

Lemma 7.1.

$$d_{\mathrm{Trunk}} \leqslant d_p \leqslant d$$

Proof. The second inequality is obvious. Let's justify the first. By the node rule, Lemma 4.6, we prove by induction on $K \geqslant 1$ that $d_p \geqslant \sum_{(r,k)\in X(\mathrm{Trunk}_{\leqslant K}(P))} t(r,k)$, where $X(\mathrm{Trunk}_{\leqslant K}(P))$ denotes the set of leaves of the trunk $\mathrm{Trunk}(P)$ truncated at level K. For $(r,k) \in \mathrm{Trunk}(P)$, $t(r,k) \geqslant 1$, so $d_p \geqslant d_{\mathrm{Trunk}}$. □

7.3. **Solutions**

Theorem 3.1 provides a combinatorial characterization of the solutions of equation $P(x) \equiv 0 \pmod{p^e}$. Now, we will provide a more arithmetic description of these solutions.

For $x \in \mathbb{Z}$, let $|x|_p = p^{-\operatorname{val}_p(x)}$ denote the p-adic absolute value and $B(r, p^{-k})$ the associated closed ball: $B(r, p^{-k}) = \{x \in \mathbb{Z} \mid \exists n \in \mathbb{Z}, x = r + np^k\}$. In other words, $x \in B(r, p^{-k})$ if and only if p^k divides $x - r$.
The set of descendants of (r, k) in the p-adic congruence tree Ω, which is an infinite fan stemming from (r, k), is thus also the set of (x, e) where $x \in B(r, p^{-k})$ (and $e \geqslant k$). We will consider $B(r, p^{-k}) \cap [\![0, p^e - 1]\!]$ which is the intersection of the fan issued from (r, k) with the level p^e.
Fix $e \geqslant 1$, we denote by $\mathcal{S}_e$, the set of solutions x, with $0 \leqslant x \leqslant p^e - 1$, of the equation $P(x) \equiv 0 \pmod{p^e}$. In other words, $\mathcal{S}_e$ corresponds exactly to the set of vertices of the Tree(P) having exactly level e.

Proposition 7.2. *The set of solutions $\mathcal{S}_e$ is the union of at most d_{Trunk} disjoint subsets $B(r_i, p^{-k_i}) \cap [\![0, p^e - 1]\!]$.*

This proposition appears in [2, Proposition 1] and [5, Proposition 3].

Proof. According to Theorem 3.1:

$$\mathcal{S}_e = \bigcup_{\substack{(r,k)\in \text{Trunk}(P) \\ \varphi(r,k)-t_k<e\leqslant\varphi(r,k)}} B(r, p^{-k}) \cap [\![0, p^e - 1]\!]$$

In particular all the solutions x in a ball $B(r, p^{-k}) \cap [\![0, p^e - 1]\!]$ are associated with the same element (r, k) of the trunk.
The discussion in Section 6.1 proves that this element (r, k) is unique, i.e. the balls $B(r_i, p^{-k_i}) \cap [\![0, p^e - 1]\!]$ are disjoint. In other words, for a path of the trunk from the root to a leaf (possibly in the form of an infinite branch) there is at most one element (r, k) in the former decomposition of $\mathcal{S}_e$. It implies the bound on the number of balls. □

8. Case of degree two polynomials

Let $p > 2$ be a prime number. Consider the case of a polynomial of degree 2:

$$P(X) = aX^2 + bX + c \in \mathbb{Z}[X]$$

with $p \nmid a$. All the configurations begin above the root with a base consisting of a stem of ℓ vertices, each with a thickness of 2 (possibly $\ell = 0$). Above this base, there are 4 possible types.

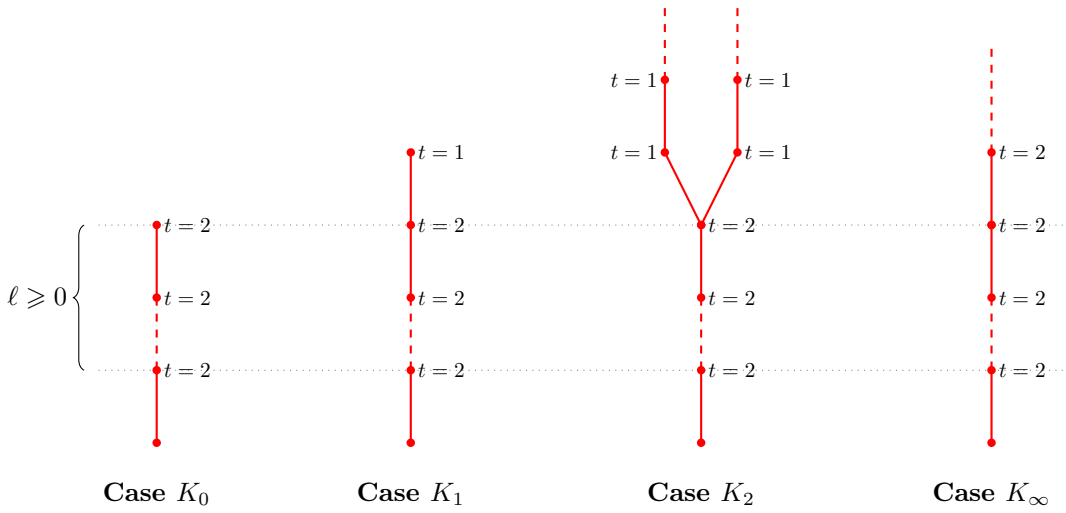

Figure 9. Possible trunks.

Base.

Since P is a polynomial of degree 2, the thickness is at most 2, and this is only possible for a single root; the same holds for its successors. What can happen after a stem with thicknesses only 2?

Cases K_0 and K_∞. This base stem of thickness 2 can be infinite; this is the case, for example, for $P(X) = X^2$. The trunk can also stop just after the last vertex of thickness 2 in the base. This is, for example, the case for $P(X) = (X-1)^2 + p^{2\ell}$ with $p = 3$.

Case K_2. In the remaining cases each vertex just after the base has a thickness of 1. Let us then consider the polynomial Q associated with the last vertex of thickness 2. Suppose it has two simple roots modulo p (that is $Q(x_i) \equiv 0 \pmod p$ and $Q'(x_i) \not\equiv 0 \pmod p$, $i = 1, 2$). Hensel's lemma then allows these two simple roots to be "lifted" indefinitely: for any $e \geqslant 1$, there exists $\tilde{x_i} \in \mathbb{Z}$ $(i = 1, 2)$ such that $\tilde{x_i} \equiv x_i \pmod p$ and $Q(\tilde{x_i}) \equiv 0 \pmod{p^e}$. This is then the K_2 situation.

Example 8.1. This is the case for $P(X) = (X-1)(X-2) + p$ with, for example, $p = 5$. For $e = 1$, the solutions of $P(x) \equiv 0 \pmod{p^e}$ are $\{1, 2\}$. For $e = 2$, it's $\{6, 22\}$, and for $e = 3$, it's $\{31, 97\}\ldots$ In this example the base is empty.

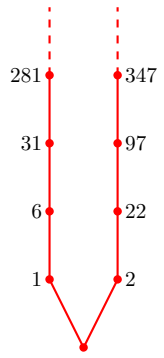

FIGURE 10. The trunk (and the tree) of $P(X) = (X-1)(X-2) + 5$.

More broadly, the polynomial $P(X) = (X - p^\ell)(X - 2p^\ell) + p^{2\ell+1}$ has a trunk, as in the case K_2, with a base of ℓ vertices and thickness 2.

Case K_1. Let us resume the discussion started in the previous case. It is possible for Q to have a double root of thickness 1, as in the case of $Q(X) = (X - x_0)^2 + p$. We then have $Q(x_0 + pX) = p\big(pX^2 + 1\big)$, which indeed gives a thickness of 1, but the successor of Q is $pX^2 + 1$, which has no root modulo p. Thus, the trunk ends here in the K_1 configuration. This is, for example, the case for $P(X) = (X-1)^2 + p^{2\ell+1}$ with $p = 3$.

Example 8.2. Let $P(X) = (X-1)^2 + p^5$ with $p = 3$. Here are the solutions of the equation $P(x) \equiv 0 \pmod{p^e}$ for different values of e:

p^e	solutions
3^1	1
3^2	$1, 4, 7$
3^3	$1, 10, 19$
3^4	$1, 10, 19, 28, 37, 46, 55, 64, 73$
3^5	$1, 28, 55, 82, 109, 136, 163, 190, 217$

For $e \geqslant 6$, the equation has no solutions.

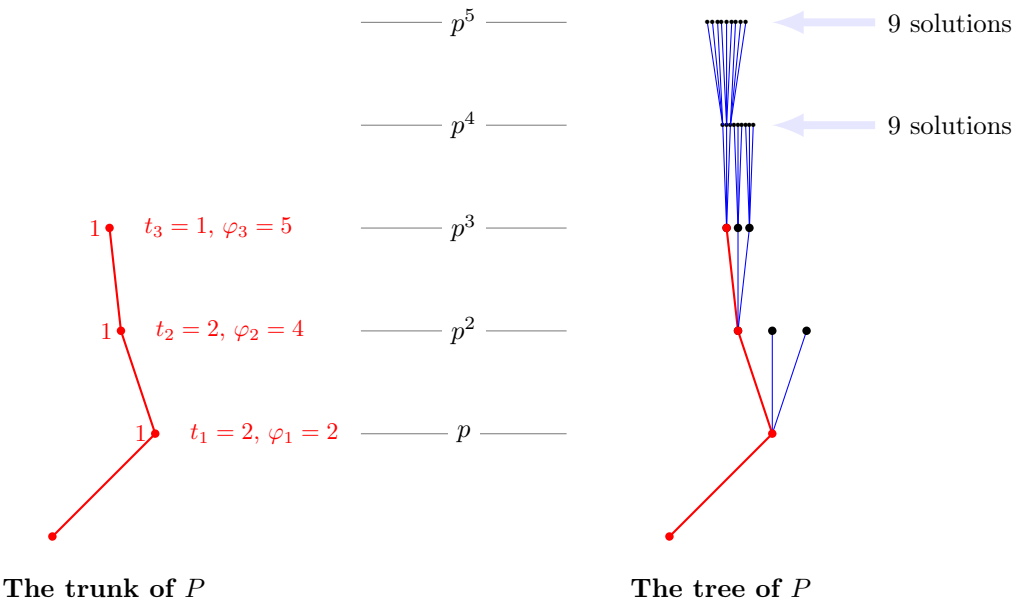

FIGURE 11. The trunk and the tree of $P(X) = (X-1)^2 + 3^5$.

9. PERSPECTIVES AND REFERENCES

9.1. **Perspectives**

Let us conclude by discussing the *Poincaré series*:

$$S(u) = \sum_{e \geqslant 0} N_e \frac{u^e}{p^e},$$

where N_e denotes the number of solutions to the equation $P(x) \equiv 0 \pmod{p^e}$ (with the convention that $N_0 = 1$). The series $S(u)$ serves as the natural generating function associated with the number of solutions. In fact, it is a rational function in u:

Theorem 9.1 (Igusa)**.**

$$S(u) \in \mathbb{Q}(u)$$

We leave it to the reader to prove this result by relying on the structure of the trunk and Corollary 6.1. For polynomials in several variables, an analogous result, due to Igusa, remains valid. This area of research is still very active today [8].

9.2. **References**

Our problem is masterfully addressed by Schmidt and Stewart in 1997, in the article [9] which utilizes graph studies and contains, either explicitly or implicitly, all the notions and results of the present article as well as numerous additional results. It seems that this article did not receive the widespread attention it deserved.

Fortunately, given its importance, the problem and the solution have resurfaced multiple times, especially when it comes to finding algorithmic solutions to polynomial problems. Thus, the explicit construction of the central notion of the present article, that of the "trunk", is given by Zúñiga-Galindo [12] for a calculation of Igusa's zeta function. The same construction is found in the article by Berthomieu, Lecerf, and Quintin [2] for determining the roots of polynomials in local rings. These same objects and results are taken up by Dwivedi, Mittal, and Saxena [3], [4], [5], for example, for factorization problems. Finally, Kopp, Randall, Rojas, and Zhu [6] define, draw, and use the trunk to count the number of solutions without explicitly detailing them.

Regarding the more elementary notion of the tree of solutions modulo p^e of a polynomial, classic references are [1] or [7].

Acknowledgments. We thank the referees and the editors for their helpful comments and suggestions.

References

[1] Tom M. Apostol. *Introduction to analytic number theory.* Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An introduction to the theory of numbers.* John Wiley & Sons, Inc., New York, fifth edition, 1991.

[8] 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.

[9] Wolfgang M. Schmidt and C. L. Stewart. Congruences, trees, and p-adic integers. *Trans. Amer. Math. Soc.*, 349(2):605–639, 1997.

[10] Adi Shamir. On the generation of multivariate polynomials which are hard to factor. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '93, page 796–804, New York, NY, USA, 1993. Association for Computing Machinery.

[11] W. A. Stein et al. *Sage Mathematics Software.* The Sage Development Team. `http://www.sagemath.org`.

[12] 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.

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