Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2023, Volume 29, Number 4, 737–751
DOI: 10.7546/nntdm.2023.29.4.737-751

The 2-adic valuation of the general degree-2 polynomial in 2 variables

Shubham

School of Physical Sciences, Jawaharlal Nehru University
New Delhi, India
e-mail: Shubha76_sps@jnu.ac.in

Received: 1 February 2023 **Revised:** 14 October 2023
Accepted: 25 November 2023 **Online First:** 26 November 2023

Abstract: We define the p-adic valuation tree of a polynomial $f(x,y) \in \mathbb{Z}[x,y]$ by which we can find its p-adic valuation at any point. This work includes diverse 2-adic valuation trees of certain degree-two polynomials in two variables. Among these, the 2-adic valuation tree of x^2+y^2 is most interesting. We use the observations from these trees to study the 2-adic valuation tree of the general degree-two polynomial in 2 variables. We also study the 2-adic valuation tree of the polynomial x^2y+5.
Keywords: p-adic valuation, Valuation tree, Polynomial sequences.
2020 Mathematics Subject Classification: 11B99, 11D88, 11B83.

1 Introduction

For $n \in \mathbb{N}$, the exponent of the highest power of a prime p that divides n is called the p-adic valuation of the n. This is denoted by $\nu_p(n)$. Legendre establishes the following result about p-adic valuation of $n!$ in [11]

$$\nu_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n-s_p(n)}{p-1},$$

where $s_p(n)$ is the sum of digits of n in base p. It is observed in [6] that 2-adic valuation of central binomial coefficient is $s_2(n)$, that is

$$\nu_2(a_n) = s_2(n), \text{ where } a_n = \binom{2n}{n}.$$

It follows from here that a_n is always an even number and $a_n/2$ is odd when n is a power of 2. This expression is called a *closed form* in [6]. The definition of closed form depends on the context. This has been discussed in [4, 8].

The work presented in [6] forms part of a general project initiated by Moll and his co-authors to analyse the set

$$V_x = \{\nu_p(x_n) : n \in \mathbb{N}\},$$

for a given sequence $x = \{x_n\}$ of integers.

The 2-adic valuation of $\{n^2 - a\}$ is studied in [6]. It is shown that $n^2 - a, a \in \mathbb{Z}$ has a simple closed form when $a \not\equiv 4, 7 \mod 8$. For these two remaining cases the valuation is quite complicated. It is studied by the notion of the *valuation tree*.

Given a polynomial $f(x)$ with integer coefficients, the sequence $\{\nu_2(f(n))\}$ is described by a tree. This is called the valuation tree attached to the polynomial f. The vertices of this tree correspond to some selected subsets

$$C_{m,j} = \{2^m i + j : i \in \mathbb{N}\}, \quad 0 \leq j < 2^m$$

starting with the root node $C_{0,0} = \mathbb{N}$. The procedure to select classes is explained below in Example 1.1. Some notation for the vertices of this tree are introduced as follows:

Definition 1.1. *A residue class $C_{m,j}$ is called terminal if $\nu_2(f(2^m i + j))$ is independent of i. Otherwise, it is called non-terminal. The same terminology is given to vertices corresponding to the class $C_{m,j}$. In the tree, terminal vertices are labelled by their constant valuation and non-terminal vertices are labelled by a $*$.*

Example 1.1. Construction of valuation tree of $x^2 + 5$ is as follows: note that $\nu_2(1 + 5) = 1$ and $\nu_2(2 + 5)$ is 0. So node v_0 is non terminating. Hence it splits into two vertices and forms the first level. These vertices correspond to the residue classes $C_{1,0}$ and $C_{1,1}$. We can check that both these nodes are terminating with valuation 0 and 1. The valuation tree of $x^2 + 5$ is shown in Figure 1.

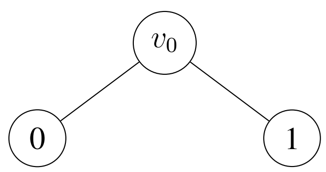

Figure 1. The valuation tree of $x^2 + 5$

The main theorem of [6] is as follows.

Theorem 1.1. *Let v be a non-terminating node at the k-th level for the valuation tree of $n^2 + 7$. Then v splits into two vertices at the $(k+1)$-level. Exactly one of them terminates, with valuation k. The second one has valuation at least $k + 1$.*

The 2-adic valuation of the Stirling numbers is discussed in [2]. The numbers $S(n,k)$ are the number of ways to partition a set of n elements into exactly k non-empty subsets where $n \in \mathbb{N}$ and $0 \le k \le n$. These are explicitly given by

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{i=k-1} (-1)^i \binom{k}{i} (k-i)^n,$$

or, by the recurrence

$$S(n,k) = S(n-1,k-1) + kS(n-1,k),$$

with initial condition $S(0,0) = 1$ and $S(n,0) = 0$ for $n > 0$.

The 2-adic valuation of $S(n,k)$ can be easily determined for $1 \le k \le 4$ and closed form expression is given as follows:

$$v_2(S(n,1)) = 0 = v_2(S(n,2)),$$

$$v_2(S(n,3)) = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{otherwise} \end{cases}$$

$$v_2(S(n,4)) = \begin{cases} 1, & \text{if } n \text{ is odd.} \\ 0, & \text{otherwise} \end{cases}$$

The important conjecture described there is that the partitions of $\mathbb{N}$ in classes of the form

$$C_{m,j}^{(k)} = \{2^m i + j : i \in \mathbb{N} \text{ and starts at the point where } 2^m i + j \ge k \}$$

leads to a clear pattern for $v_2(S(n,k))$ for $k \in \mathbb{N}$ is fixed. We recall that the parameter m is called the level of the class. The main conjecture of [2] is now stated:

Conjecture 1.1. *Let $k \in \mathbb{N}$ be fixed. Then we conjecture that*

(a) there exists a level $m_0(k)$ and an integer $\mu(k)$ such that for any $m \ge m_0(k)$, the number of non-terminal classes of level m is $\mu(k)$, independently of m;

(b) moreover, for each $m \ge m_0(k)$, each of the $\mu(k)$ non-terminal classes splits into one terminal and one non-terminal subclass. The latter generates the next level set.

This conjecture is only established for the case $k = 5$. A similar conjecture is given in [3] for the p-adic valuation of the Stirling numbers.

From the point of view of application, the 2-adic valuation tree is used to solve quadratic and cubic diophantine equations in [5]. Apart from this, some other special cases are studied in [1, 7, 12].

In this work, we discuss the set

$$V_f = \{\nu_p(f(m,n)) : m, n \in \mathbb{N}\},$$

where $f(x,y) \in \mathbb{Z}[x,y]$, by the generalized notion of the *valuation tree*. We believe that the p-adic valuation and the valuation tree of two variable polynomials have not been studied before. We define the p-adic valuation tree as follows:

Definition 1.2. *Let p be a prime number. Consider the integers $f(x, y)$ for every (x, y) in $\mathbb{Z}^2$. The p-adic valuation tree of f is a rooted, labelled p^2-ary tree defined recursively as follows:*

1. *Suppose that v_0 be a root vertex at level 0. There are p^2 edges from this root vertex to its p^2 children vertices at level 1. These vertices correspond to all possible residue classes $(i_0, j_0) \mod p$. Label the vertex corresponding to the class (i_0, j_0) with 0 if $f(i_0, j_0) \not\equiv 0 \pmod p$ and with $*$ if $f(i_0, j_0) \equiv 0 \pmod p$.*
2. *If the label of a vertex is 0, it does not have any children.*
3. *If the label of a vertex is $*$, then it has p^2 children at level 2. These vertices correspond to the residue classes $(i_0 + i_1 p, j_0 + j_1 p) \pmod{p^2}$ where $i_1, j_1 \in \{0, 1, 2, \ldots, p-1\}$ and $(i_0, j_0) \pmod p$ is the class of the parent vertex.*

This process continues recursively so that at the l^{th} level, there are p^2 children of any non-terminating vertex in the previous level $(l-1)$, each child of which corresponds to the residue classes $(i_0 + i_1 p + \cdots + i_{l-1} p^{l-1}, j_0 + j_1 p + \cdots + j_{l-1} p^{l-1}) \pmod{p^l}$.

Here $i_{l-1}, j_{l-1} \in \{0, 1, 2, \ldots, p-1\}$ and $(i_0 + i_1 p + \cdots + i_{l-2} p^{l-2}, j_0 + j_1 p + \cdots + j_{l-2} p^{l-2}) \pmod{p^{l-1}}$ is the class of the parent vertex. Label the vertex corresponding to the class (i, j) with $l-1$ if $f(i, j) \not\equiv 0 \pmod{p^l}$ and $*$ if $f(i, j) \equiv 0 \pmod{p^l}$. Thus $i = i_0 + i_1 p + \cdots + i_{l-1} p^{l-1}$, $j = j_0 + j_1 p + \cdots + j_{l-1} p^{l-1}$.

Example 1.2. Valuation tree of $x^2 + y^2 + xy + x + y + 1$ is shown in Figure 2.

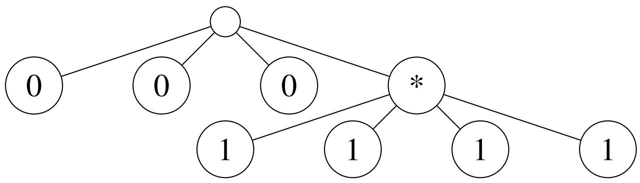

Figure 2. The valuation tree of $x^2 + y^2 + xy + x + y + 1$

So

$$\nu_2(x^2 + y^2 + xy + x + y + 1) = \begin{cases} 1, & \text{if both } x, y \text{ are odd.} \\ 0, & \text{otherwise} \end{cases}$$

We say the 2-adic valuation $\nu_2(f(x, y))$ of a polynomial $f(x, y)$ has a *closed-form* if its 2-adic valuation tree has no infinite branch. Hence the 2-adic valuation of $x^2 + y^2 + xy + x + y + 1$ admits a closed form.

2 Some examples of 2-adic valuation tree

Now we look at various diverse 2-adic valuation trees which can be described completely.

Example 2.1. The first three levels of the 2-adic valuation tree of $x^2 + y^2$ are shown in Figure 3.

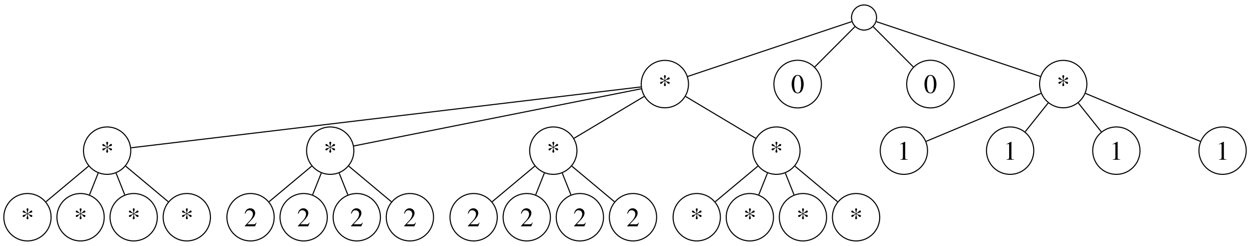

Figure 3. The first three levels of the 2-adic valuation tree of $x^2 + y^2$

By investigating the nature of the above valuation tree, we find an interesting pattern. By using Theorem 2.1 we can find the label of next k levels once the label of k-th level is given. We need some notation to state the result: Consider the binary representation of b_k and c_k,

$$b_k = (i_k i_{k-1} \cdots i_1 i_0)_2,$$
$$c_k = (j_k j_{k-1} \cdots j_1 j_0)_2$$

where $i_0, i_1, \ldots, i_{k-1}, j_0, j_1, \ldots, j_{k-1} \in \{0, 1\}$.

Theorem 2.1. *Let v be a vertex at the k-th level of the valuation tree of $x^2 + y^2$. Let the pair (b_{k-1}, c_{k-1}) be associated with the vertex v. Suppose that $i_0 = i_1 = \cdots = i_{k-2} = j_0 = j_1 = \cdots = j_{k-2} = 0$. Then*

1. *the pair $(i_{k-1}, j_{k-1}) = (0, 0)$ implies all four children of vertex v will be labelled with $*$.*
2. *If $(i_{k-1}, j_{k-1}) = (1, 1)$ and if w is a vertex descending from v at l-th level, then w is labelled with $*$ whenever $l \in \{k+1, k+2, \ldots, (2k-1)\}$ and with $(2k-1)$ for $l = 2k$.*
3. *If $(i_{k-1}, j_{k-1}) = (1, 0)$ or $(0, 1)$ and if w is a vertex descending from v at l-th levels, then w is labelled with $*$ whenever $l \in \{k+1, k+2, \ldots, (2k-2)\}$ and with $2k-2$ when $l = 2k-1$.*

Proof. We are given that

$$b_k = b_{k-1} + 2^k i_k = (i_k i_{k-1} \cdots i_1 i_0)_2, \quad c_k = c_{k-1} + 2^k j_k = (j_k j_{k-1} \cdots j_1 j_0)_2$$

where $i_0, i_1, \ldots, i_{k-1}, j_0, j_1, \ldots, j_{k-1} \in \{0, 1\}$.
If $(i_{k-1}, j_{k-1}) = (0, 0)$, then

$$b_k^2 + c_k^2 \equiv b_{k-1}^2 + c_{k-1}^2 \pmod{2^{k+1}}, k > 0$$

but $b_{k-1} = c_{k-1} = 0$ so all four children of vertex v will be labelled with $*$.

Let us consider

$$b_{k+l-1}^2 + c_{k+l-1}^2 \equiv 0 \pmod{2^{k+l}}, 1 \le l \le k. \tag{1}$$

On putting the expression for b_{k+l-1} and c_{k+l-1} in the above equation we get

$$(2^{k-1} i_{k-1} + \cdots + 2^{k+l-1} i_{k+l-1})^2 + (2^{k-1} j_{k-1} + \cdots + 2^{k+l-1} j_{k+l-1})^2 \equiv 0 \pmod{2^{k+l}}, 1 \le l \le k \tag{2}$$

which implies

$$2^{2k-2}(i_{k-1} + 2i_k + \cdots + 2^{l+1} i_{k+l-1})^2 + 2^{2k-2}(j_{k-1} + 2j_k + \cdots + 2^{l+1} j_{k+l-1})^2 \equiv 0 \pmod{2^{k+l}}, 1 \le l \le k \tag{3}$$

If $(i_{k-1}, j_{k-1}) = (1, 1)$, then the least power of 2 in equation (3) is 2^{2k-1}. So vertices descending from v at $k+1, k+2, \ldots, (2k-1)$-th levels will be labelled with $*$ and at the $2k$-th level all vertices descending from v will be labelled with $2k-1$.

If $(i_{k-1}, j_{k-1}) = (1, 0)$ or $(0, 1)$, then the least power of 2 in equation (3) is 2^{2k-2}. So vertices descending from v at $k+1, k+2, \ldots, (2k-2)$-th levels will be labelled with $*$ and at the $(2k-1)$-th level all vertices descending from v will be labelled with $2k-2$. □

Example 2.2. The first few levels of the 2-adic valuation tree of $x^2 + y^2 + xy + x + y$ has also a specific pattern as shown in Figure 4.

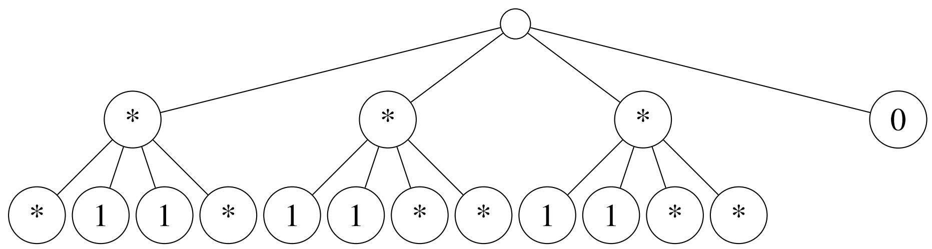

Figure 4. The first few levels of the 2-adic valuation tree of $x^2 + y^2 + xy + x + y$

We can formulate the following result for the 2-adic valuation tree of $x^2 + y^2 + xy + x + y$:

Theorem 2.2. *Let v be a vertex labelled with $*$ at the level k of the valuation tree of $x^2 + y^2 + xy + x + y$ for $k \geq 1$. Then v splits into four vertices at the level $k+1$. Exactly two of them are labelled with $*$ and two are labelled with k. The root vertex splits into three vertices with label $*$ and one vertex with label 0.*

Proof. Let the pair (b_{k-1}, c_{k-1}) be associated with the vertex v. So

$$b_k = b_{k-1} + 2^k i_k = (i_k i_{k-1} \cdots i_1 i_0)_2, \quad c_k = c_{k-1} + 2^k j_k = (j_k j_{k-1} \cdots j_1 j_0)_2$$

where $i_0, i_1, \ldots, i_{k-1}, j_0, j_1, \ldots, j_{k-1} \in \{0, 1\}$ and $(i_0, j_0) \neq (1, 1)$. We want to find (i_k, j_k) such that

$$b_k^2 + c_k^2 + b_k c_k + b_k + c_k \equiv 0 \pmod{2^{k+1}}.$$

On putting the expression of b_k and c_k in the above equation, we get

$$b_{k-1}^2 + c_{k-1}^2 + b_{k-1}c_{k-1} + b_{k-1} + c_{k-1} + 2^k(b_{k-1}j_k + c_{k-1}i_k + i_{k-1} + j_{k-1}) \equiv 0 \pmod{2^{k+1}}.$$

We know that $b_{k-1}^2 + c_{k-1}^2 + b_{k-1}c_{k-1} + b_{k-1} + c_{k-1} = a2^k, a \in \{0, 1\}$, so the above equation becomes

$$\begin{aligned} a2^k + 2^k(b_{k-1}j_k + c_{k-1}i_k + i_k + j_k) &\equiv 0 \pmod{2^{k+1}} \\ \Rightarrow a + b_{k-1}j_k + c_{k-1}i_k + i_k + j_k &\equiv 0 \pmod{2} \\ \Rightarrow i_k(j_0 + 1) + j_k(i_0 + 1) &\equiv a \pmod{2} \end{aligned} \tag{4}$$

Now if $(i_0, j_0) = (0, 0)$, then equation (2) becomes $i_k + j_k \equiv a \pmod{2}$. Hence there are two vertices labelled with k descending from v with $i_k + j_k \not\equiv a \pmod{2}$ and the other two vertices are not terminating labelled with $*$.

If $(i_0, j_0) = (1, 0)$, then equation (2) becomes $i_k \equiv a \pmod 2$. Hence there are two vertices labelled with k descending from v with $i_k \not\equiv a \pmod 2$ and the other two vertices are non-terminating labelled with $*$. Similarly for $(i_0, j_0) = (0, 1)$, equation (2) becomes $j_k \equiv a \pmod 2$. Hence there are two vertices labelled with k descending from v with $j_k \not\equiv a \pmod 2$ and the other two vertices are non-terminating labelled with $*$. □

Example 2.3. The first few levels of the 2-adic valuation tree of $xy + x + y + 1$ are shown in Figure 5.

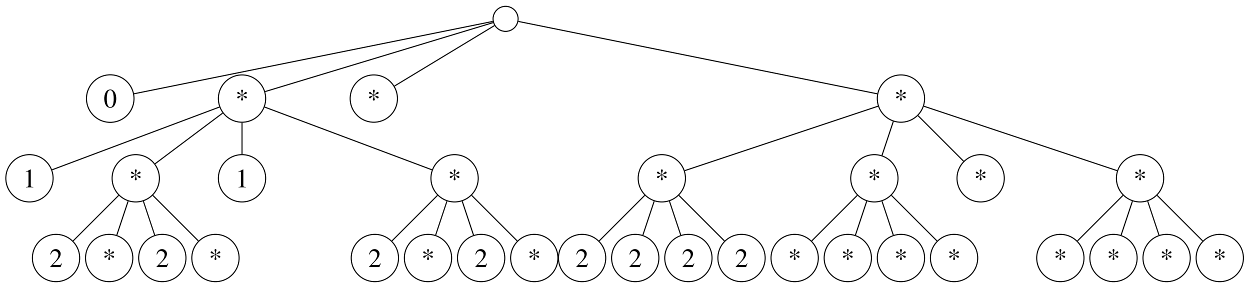

Figure 5. The first few levels of the 2-adic valuation tree of $xy + x + y + 1$

By analysing the pattern in the above tree, we can state the following result:

Theorem 2.3. *Let v be a vertex labelled with $*$ at the k-th level of the valuation tree of $xy + x + y + 1$, for $k > 0$. Then this vertex v splits into four vertices such that*

1. *If $(i_0, j_0) = (1, 1)$, then all four vertices will be labelled with $*$ or $k + 1$.*
2. *If $(i_0, j_0) = (0, 1), (1, 0)$ and $(0, 0)$, then exactly two will be labelled with $*$.*

The root vertex v_0 splits into four vertices, each labelled with $*$.

Proof. Let (b_{k-1}, c_{k-1}) be associated with the vertex v at the k-th level of the valuation tree of $xy + x + y + 1$, for $k > 0$. So

$$b_k = 2^k i_k + b_{k-1}, \quad c_k = 2^k j_k + c_{k-1}$$

where $i_0, i_1, \ldots, i_k, j_0, j_1, \ldots, j_k \in \{0, 1\}$. We want to find (i_k, j_k) such that

$$b_k c_k + b_k + c_k + 1 \equiv 0 \pmod{2^{k+1}}.$$

On putting the expression of b_k and c_k in the above equation, we get

$$b_{k-1}c_{k-1} + b_{k-1} + c_{k-1} + 1 + 2^k(b_{k-1}j_k + c_{k-1}i_k + i_{k-1} + j_{k-1}) \equiv 0 \pmod{2^{k+1}}.$$

We know that $b_{k-1}c_{k-1} + b_{k-1} + c_{k-1} + 1 = a2^k, a \in \{0, 1\}$, so the above equation becomes

$$\begin{aligned} a2^k + 2^k(b_{k-1}j_k + c_{k-1}i_k + i_k + j_k) &\equiv 0 \pmod{2^{k+1}} \\ \Rightarrow a + b_{k-1}j_k + c_{k-1}i_k + i_k + j_k &\equiv 0 \pmod 2 \\ \Rightarrow i_k(j_0 + 1) + j_k(i_0 + 1) &\equiv a \pmod 2 \end{aligned} \tag{5}$$

Now if $(i_0, j_0) = (0, 0)$, then equation (5) becomes $i_k + j_k \equiv a \pmod 2$. Hence there are two vertices labelled with k descending from v with $i_k + j_k \not\equiv a \pmod 2$ and the other two vertices are non-terminating labelled with $*$.

If $(i_0, j_0) = (1, 0)$, then equation (5) becomes $i_k \equiv a \pmod 2$. Hence there are two vertices labelled with k descending from v with $i_k \not\equiv a \pmod 2$ and the other two vertices are non-terminating labelled with $*$.

If $(i_0, j_0) = (0, 1)$ then equation (5) becomes $j_k \equiv a \pmod 2$. Hence there are two vertices labelled with k descending from v with $j_k \not\equiv a \pmod 2$ and the other two vertices are non-terminating labelled with $*$.

Similarly for $(i_0, j_0) = (1, 1)$, equation (5) becomes $0 \equiv a \pmod 2$. Hence v splits into four vertices labelled with $*$ or k depending upon whether $a \equiv 0 \pmod 2$ or $a \equiv 1 \pmod 2$. □

Remark. It may be pointed out there that the polynomials in the theorems 2.1, 2.2, 2.3 are symmetric. However, in section 4 and 5 we will see similar results for the asymmetric polynomials.

3 The algebraic meaning of an infinite branch of the valuation tree

In the last section, we have seen examples of valuation trees with infinite branches. But what is the algebraic meaning of such a phenomenon? From the definition of the valuation tree we can deduce the following results:

Lemma 3.1. *Let* $i_0, j_0, i_1, j_1, \ldots, i_n, j_n \in \{0, 1, 2, \ldots, p-1\}$ *satisfying*

$$f(i_0, j_0) \equiv 0 \pmod p$$
$$f(i_0 + i_1 p, j_0 + j_1 p) \equiv 0 \pmod{p^2}$$
$$f(i_0 + i_1 p + i_2 p^2, j_0 + j_1 p + j_2 p^2) \equiv 0 \pmod{p^3}$$
$$\cdots$$
$$f(i_0 + i_1 p + \cdots + i_{n-1} p^{n-1}, j_0 + j_1 p + \cdots + j_{n-1} p^{n-1}) \equiv 0 \pmod{p^n} \text{ and}$$
$$f(i_0 + i_1 p + \cdots + i_n p^n, j_0 + j_1 p + \cdots + j_n p^n) \not\equiv 0 \pmod{p^{n+1}}.$$

Then any $(i, j) = (i_0 + i_1 p + \cdots + i_n p^n, j_0 + j_1 p + \cdots + j_n p^n) \pmod{p^{n+1}}$*, satisfies*

$$\nu_p(f(i, j)) = n.$$

Theorem 3.1. *The* p*-adic valuation* $\nu_p(f(x, y))$ *admits a closed-form if the equation* $f(x, y) = 0$ *has no solution in* $\mathbb{Q}_p \times \mathbb{Q}_p$.

Proof. Let the sequence of indices generated to come an infinite branch of the tree at n-th level be $(a_n, b_n) = (i_0 + i_1 p + \cdots + i_{n-1} p^{n-1}, j_0 + j_1 p + \cdots + j_{n-1} p^{n-1})$ where $i_0, j_0, i_1, j_1, \ldots, i_{n-1}, j_{n-1} \in \{0, 1, 2, \ldots, p-1\}$ such that

$$f(i_0, j_0) \equiv 0 \pmod p$$
$$f(i_0 + i_1 p, j_0 + j_1 p) \equiv 0 \pmod{p^2}$$
$$f(i_0 + i_1 p + i_2 p^2, j_0 + j_1 p + j_2 p^2) \equiv 0 \pmod{p^3}$$
$$\cdots$$
$$f(i_0 + i_1 p + \cdots + i_{n-1} p^{n-1}, j_0 + j_1 p + \cdots + j_{n-1} p^{n-1}) \equiv 0 \pmod{p^n} \text{ and}$$
$$f(i_0 + i_1 p + \cdots + i_n p^n, j_0 + j_1 p + \cdots + j_n p^n) \not\equiv 0 \pmod{p^{n+1}}.$$

Now a_n and b_n satisfy: $0 \le a_n, b_n \le p^n$ and $a_n \equiv a_{n+1} \pmod{p^n}$, $b_n \equiv b_{n+1} \pmod{p^n}$. Hence sequences $\{a_n\}$ and $\{b_n\}$ are convergent to some element in the field $\mathbb{Q}_p$. Let $\{(a_n, b_n)\}$ converges to (x, y) for $x, y \in \mathbb{Q}_p$. Since the polynomial $f(x, y)$ is continuous so $f(a_n, b_n)$ converges to $f(x, y)$. Now by Lemma 3.1, we know that $v_p(f(a_n, b_n))$ tends to ∞ as n tends to ∞ so $f(a_n, b_n)$ tends to 0 when n tends to ∞. Hence $f(x, y) = 0$. So any infinite branch in the tree associated to polynomial $f(x, y)$ corresponds to a root of $f(x, y) = 0$ in $\mathbb{Q}_p \times \mathbb{Q}_p$. A valuation tree having an infinite branch cannot have a closed-form. □

Since the polynomials in examples 2.1, 2.2 and 2.3 have zeros in $\mathbb{Q}_p \times \mathbb{Q}_p$, they do not admit closed-form for 2-adic valuation.

Further, consider the sequence of the valuations $V_p(f) = \{\nu_p(f(n, m) : 0 \le m \le n, n \in \mathbb{N}\}$ for a prime p and a polynomial $f(x, y) \in \mathbb{Z}[x, y]$. We say $V_p(f)$ is periodic with a period α if $V_p(f(n, m)) = V_p(f(n + \alpha, m + \alpha))$. We prove that:

Theorem 3.2. *Let p be a prime and $f \in \mathbb{Z}[x, y]$. Then $V_p(f)$ is either periodic or unbounded. Moreover, $V_p(f)$ is periodic if and only if f has no zeros in $\mathbb{Z}_p^2$. In the periodic case, the minimal period is a power of p.*

Proof. Assume that f has no zeros in $\mathbb{Z}_p^2$. If $V_p(f)$ is not bounded there exists a sequence $(n_j, m_j) \to \infty$ such that $V_p(f) \to \infty$. The compactness of $\mathbb{Z}_p^2$ gives a subsequence converging to $(n_\infty, m_\infty) \in \mathbb{Z}_p^2$. Then $f(n_\infty, m_\infty)$ is divisible by arbitrary large powers of p, thus $f(n_\infty, m_\infty) = 0$. This contradiction shows $V_p(f)$ is bounded. In order to $V_p(f)$ is periodic, define

$$d = \sup\{k : p^k \text{ divides } f(m, n) \text{ for some } (m, n) \in \mathbb{Z}^2\}. \tag{6}$$

Then $d \ge 0$ and

$$f(n + p^{d+1}, m + p^{d+1}) = f(n, m) + (f_x + f_y)p^{d+1} + O(p^{d+2}). \tag{7}$$

Since $\nu_p(f(n, m) \le d$, it follows that

$$\nu_p(f(n + p^{d+1}, m + p^{d+1})) = \nu_p(f(n, m)), \tag{8}$$

proving that $\nu_p(f(n, m))$ is periodic and minimal period is a divisor of p^{d+1}.
On the other hand, if $f(x, y)$ has a zero $\alpha(y)$ in$\mathbb{Z}_p[y]$,

$$f(x, y) = (x - \alpha) f_1(x, y) \text{ for some } f_1(x, y) \in \mathbb{Z}_p[x, y]. \tag{9}$$

Then $v_p(f) \ge v_p(x - \alpha)$, and $V_p(f)$ is unbounded. □

4 The 2-adic valuation tree of the general polynomial $ax^2 + by^2 + cxy + dx + ey + g$

We are ready to find the 2-adic valuation tree of the general degree-two polynomial $f(x, y) \in \mathbb{Z}[x, y]$. First we generalize Example 2.1 to the case $ax^2 + by^2$. Consider the binary representation of b_k and c_k:

$$b_k = (i_k i_{k-1} \cdots i_1 i_0)_2, \quad c_k = (j_k j_{k-1} \cdots j_1 j_0)_2,$$

where $i_0, i_1, \ldots, i_k, j_0, j_1, \ldots, j_k \in \{0, 1\}$.

Theorem 4.1. *Let v be a vertex at the k-th level of the valuation tree of $ax^2 + by^2$ where $a = 2^n\alpha$, $b = 2^m\beta$, α and β are odd. Let $\gamma = \min(m, n)$. Let the pair (b_{k-1}, c_{k-1}), in the above notation be associated with vertex v. Further suppose that $i_0 = i_1 = \cdots = i_{k-2} = j_0 = j_1 = \cdots = j_{k-2} = 0$. Then*

1. *the pair $(i_{k-1}, j_{k-1}) = (0, 0)$ implies all four children of vertex v are labelled with $*$.*
2. *If $(i_{k-1}, j_{k-1}) = (1, 1)$ and if w is a vertex descending from v at l-th level, then w is labelled with $*$ whenever $l \in \{k+1, k+2, \ldots, (2k+\gamma-1)\}$ and with $(2k+\gamma-1)$ for $l = 2k+\gamma$.*
3. *If $(i_{k-1}, j_{k-1}) = (1, 0)$ or $(0, 1)$ and if w is a vertex descending from v at l-th levels, then w is labelled with $*$ whenever $l \in \{k+1, k+2, \ldots, (2k+\gamma-2)\}$ and with $2k+\gamma-2$ when $l = 2k+\gamma-1$.*

Proof. We are given that

$$b_k = b_{k-1} + 2^k i_k = (i_k i_{k-1} \cdots i_1 i_0)_2, \quad c_k = c_{k-1} + 2^k j_k = (j_k j_{k-1} \cdots j_1 j_0)_2,$$

where $i_0, i_1, \ldots, i_{k-1}, j_0, j_1, \ldots, j_{k-1} \in \{0, 1\}$. When $(i_{k-1}, j_{k-1}) = (0, 0)$ then

$$ab_k^2 + bc_k^2 \pmod{2^{k+1}} \equiv ab_{k-1}^2 + bc_{k-1}^2 \pmod{2^{k+1}}, k > 0.$$

But $b_{k-1} = c_{k-1} = 0$ so all four children of the vertex v will be labelled with $*$. Let us consider

$$ab_{k+l-1}^2 + bc_{k+l-1}^2 \equiv 0 \pmod{2^{k+l}}, 1 \le l \le k \tag{10}$$

On putting the expression for b_{k+l-1}, c_{k+l-1}, a and b in the above equation we get

$$2^{2k+\gamma-2}(\alpha(i_{k-1} + 2i_k + \cdots + 2^{l+1} i_{k+l-1})^2 + \beta(j_{k-1} + 2j_k + \cdots + 2^{l+1} j_{k+l-1})^2) \equiv 0 \pmod{2^{k+l}}, 1 \le l \le k. \tag{11}$$

If $(i_{k-1}, j_{k-1}) = (1, 1)$, then the least power of 2 in equation (11) is $2^{2k+\gamma-1}$. So vertices descending from v at $k+1, k+2, \ldots, (2k+\gamma-1)$-th levels will be labelled with $*$ and at the $(2k+\gamma)$-th level all vertices descending from v will be labelled with $2k+\gamma-1$.

If $(i_{k-1}, j_{k-1}) = (1, 0)$ or $(0, 1)$, then the least power of 2 in equation (11) is $2^{2k+\gamma-2}$. The vertices descending from v at $k+1, k+2, \ldots, (2k+\gamma-2)$-th levels will be labelled with $*$ and at the $(2k+\gamma-1)$-th level all vertices descending from v will be labelled with $2k+\gamma-2$. □

Let $f(x, y) = ax^2 + by^2 + cxy + dx + ey + g$, for $a, b, c, d, g \in \mathbb{Z}$. The following theorem describes the valuation tree of $f(x, y)$:

Theorem 4.2. *Let v be a vertex at the k-th level of the valuation tree of $f(x,y)$ labelled with $*$ for $k>1$. Then v splits into four vertices such that either all are non-terminating or two of them are non-terminating.*

Proof. We are given that $f(x,y) = ax^2+by^2+cxy+dx+ey+g$. Let (b_{k-1},c_{k-1}) be associated with the vertex v at the k-th level of the valuation tree. So we have $f(b_{k-1},c_{k-1}) \equiv 0 \pmod{2^k}$, where $b_k = (i_k i_{k-1}\cdots i_1 i_0)_2$, $c_k = (j_k j_{k-1}\cdots j_1 j_0)_2$. Here $i_0, i_1, \ldots, i_k, j_0, j_1, \ldots, j_k \in \{0,1\}$ and $(b_0,c_0) = (i_0,j_0)$. We want to find (i_k,j_k) such that $f(b_k,c_k) \equiv 0 \pmod{2^{k+1}}$.

On putting the expression for (b_k,c_k) in the above equation we get

$$a(b_{k-1}+2^k i_k)^2 + b(c_{k-1}+2^k j_k)^2 + c(b_{k-1}+2^k i_k)(c_{k-1}+2^k j_k) + d(b_{k-1}+2^k i_k) + e(c_{k-1}+2^k j_k) + g \equiv 0 \pmod{2^{k+1}}, k>0.$$

But we know that $f(b_{k-1},c_{k-1}) \equiv 0 \pmod{2^k}$. So $f(b_{k-1},c_{k-1}) = \alpha 2^k, \alpha \in \{0,1\}$. Hence we want to find (i_k,j_k) such that $\alpha 2^k + 2^k[i_k(cc_{k-1}+d) + j_k(cb_{k-1}+e)] \equiv 0 \pmod{2^{k+1}}$, that is $\alpha + i_k(cj_0+d) + j_k(ci_0+e) \equiv 0 \pmod 2$.

The following Table 1 gives the all possible cases for (i_k,j_k) when $\alpha \equiv 0 \pmod 2$.

Serial no.	(i_k,j_k)	c	d	e	(i_0,j_0)	Label
1	(0,0)	-	-	-	-	$*$
2	(1,0)	odd	odd	-	(0,0),(1,0)	k
3	(1,0)	odd	odd	-	(0,1),(1,1)	$*$
4	(1,0)	odd	even	-	(0,0),(1,0)	$*$
5	(1,0)	odd	even	-	(1,1),(0,1)	k
6	(1,0)	even	odd	-	-	k
7	(1,0)	even	even	-	-	$*$
8	(0,1)	odd	-	odd	(0,0),(0,1)	k
9	(0,1)	odd	-	odd	(1,0),(1,1)	$*$
10	(0,1)	odd	-	even	(0,0),(1,0)	$*$
11	(0,1)	odd	-	even	(1,1),(0,1)	k
12	(0,1)	even	-	odd	-	k
13	(0,1)	even	-	even	-	$*$
14	(1,1)	odd	odd	even	(0,0),(1,1)	k
15	(1,1)	odd	odd	even	(1,0),(0,1)	$*$
16	(1,1)	odd	odd	odd	(0,0),(1,1)	$*$
17	(1,1)	odd	odd	odd	(1,0),(0,1)	k
18	(1,1)	odd	even	even	(0,0),(1,1)	$*$
19	(1,1)	odd	even	even	(1,0),(0,1)	k
20	(1,1)	odd	even	odd	(0,0),(1,1)	k
21	(1,1)	odd	even	odd	(1,0),(0,1)	$*$
22	(1,1)	even	odd	even	-	k
23	(1,1)	even	odd	odd	-	$*$
24	(1,1)	even	even	even	-	$*$
25	(1,1)	even	even	odd	-	k

Table 1. All possible cases for (i_k,j_k) when $\alpha \equiv 0 \pmod 2$.

Hence the theorem is proved for $\alpha \equiv 0 \pmod 2$. For the case $\alpha \equiv 1 \pmod 2$, we can find the appropriate label by interchanging the $*$ and k in the last column of Table 1. Hence the theorem is proved in this case as well. □

Remark. If the label of k-th level is given then Theorem 4.2 describes only about the label of the $(k+1)$-th level of the valuation tree but Theorem 4.1 describes the label of the next k levels of the valuation tree of given $f(x, y)$.

To construct the whole tree one starts with the root vertex and recursively apply the following algorithm to every non-terminal vertex:

Algorithm 1. To find the label of the children of given non-terminating vertex v at k-th level, $k > 1$:

1 : Find α modulo 2 such that $f(b_{k-1}, c_{k-1}) = 2^k\alpha$.

2 : Use Table 1, $(i_0, j_0), \alpha$ to find the label of the children of given vertex where (i_0, j_0) is corresponding to the parent vertex of the given non-terminating vertex v.

For example, consider $f(x, y) = 2x^2 + y^2 + xy + x + y + 1, k = 2$ and the non-terminating vertex corresponds to $(0, 1)$. To find the label of the 4 children of this vertex corresponding to $(0, 1)$, we find α modulo 2 such that $f(b_1, c_1) = 4\alpha$. Here $f(b_1, c_1) = f(1, 0) = 4$. Hence $\alpha \equiv 1 \pmod 2$. By using Table 1, $(i_0, j_0) = (1, 0)$ and α we find the first two levels of the 2-adic valuation tree of $f(x, y) = 2x^2 + y^2 + xy + x + y + 1$ shown in Figure 6.

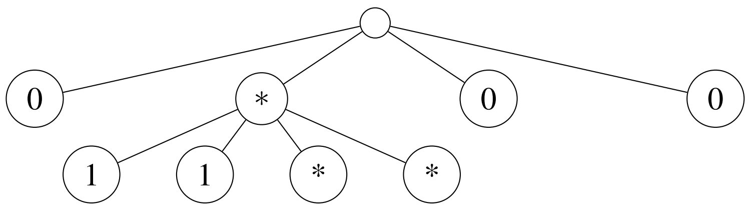

Figure 6. The first two levels of the 2-adic valuation tree of $f(x, y) = 2x^2 + y^2 + xy + x + y + 1$

5 One example of the 2-adic valuation tree of degree-3 polynomial in two variables

To study the 2-adic valuation tree of the higher degree polynomials effectively we need some advanced techniques. One of the technique, we would like to highlight is the generalized Hensel's lemma [9, 10]. We study the 2-adic valuation tree of the polynomial $x^2y + 5$ shown in Figure 7. We prove the following theorem:

Theorem 5.1. *Let v be a vertex labelled with $*$ at the level k of the valuation tree of $x^2y + 5$ for $k \geq 1$. Then v splits into four vertices at the level $k + 1$. Exactly two of them are labelled with $*$ and two are labelled with k. The root vertex splits into three vertices with label 0 and one vertex with label $*$.*

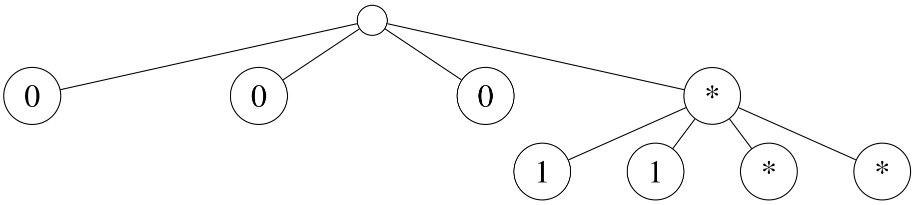

Figure 7. The first two levels of the p-adic valuation tree of x^2y+5

Proof. We are given that $f(x,y) = x^2y+5$. Let (b_{k-1}, c_{k-1}) be associated with the vertex v at the k-th level of the valuation tree. So we have

$$f(b_{k-1}, c_{k-1}) \equiv 0 \pmod{2^k},$$

where $b_k = (i_k i_{k-1} \cdots i_1 i_0)_2$, $c_k = (j_k j_{k-1} \cdots j_1 j_0)_2$. Here $i_0, i_1, \ldots, i_k$, $j_0, j_1, \ldots, j_k \in \{0,1\}$ and $(b_0, c_0) = (i_0, j_0) = (1,1)$.

We want to find (i_k, j_k) such that $f(b_k, c_k) \equiv 0 \pmod{2^{k+1}}$.

On putting the expression for (b_k, c_k) in the above equation we get

$$b_{k-1}^2 c_{k-1} + 2^k j_k b_{k-1}^2 + 5 \equiv 0 \pmod{2^{k+1}}. \tag{12}$$

We are given that $f(b_{k-2}, c_{k-2}) \equiv 0 \pmod{2^{k-1}}$. So $b_{k-2}^2 c_{k-2} + 5 = 2^{k-1}a$, where $a \in \{0,1\}$. Hence equation (12) becomes

$$2^k(b_{k-1}^2 j_k + a) \equiv 0 \pmod{2^{k+1}} \tag{13}$$

Now observe that $b_{k-1} \equiv 1 \pmod 2$. So Equation (13) becomes

$$2^k(j_k + a) \equiv 0 \pmod{2^{k+1}}$$

which implies

$$j_k \equiv a \pmod 2.$$

Therefore there are two vertices labelled with k descending from v with $j_k \not\equiv a \pmod 2$ and the other two vertices are non-terminating labelled with $*$. □

We can prove Theorem 5.1 by using the generalized Hensel's lemma [9].

Alternative proof. Let $f(x,y) = (x^2y+5, x+1)$ and $a = (1,1)$. So

$$f(1,1) = (6,6) \text{ and } J_f(x,y) = \begin{vmatrix} 2xy & x^2 \\ 1 & 0 \end{vmatrix} = -x^2$$
$$\Rightarrow ||f(1,1)||_2 = \frac{1}{2}, |J_f(1,1)|_2 = 1$$
$$\Rightarrow ||f(1,1)||_2^2 < |J_f(1,1)|_2,$$

where $J_f(x,y) = \begin{vmatrix} \partial f_1/\partial x & \partial f_1/\partial y \\ \partial f_2/\partial x & \partial f_2/\partial y \end{vmatrix}$ is the Jacobian of $f(x,y) = (f_1, f_2)$ and $||f(x,y)||_2 := \max\{|f_1|_2, |f_2|_2\}$. So by the generalized Hensel's lemma [9] there is a unique solution to $f(x,y) =$

$(0,0)$ in $\mathbb{Z}_2^2$ such that $||(x,y)-(1,1)||_2 < 1$. The vector $\begin{pmatrix} x \\ y \end{pmatrix}$ is the limit of sequence $\alpha_n = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$ where $\alpha_1 = a = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and for $n \geq 1$,

$$\alpha_{n+1} = \begin{pmatrix} x_n \\ y_n \end{pmatrix} - \begin{bmatrix} 2x_n y_n & x_n^2 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} x_n^2 y_n + 5 \\ x_n + 1 \end{bmatrix}. \tag{14}$$

Let the pair (b_{k-1}, c_{k-1}) be associated with vertex v. So

$$f(b_{k-1}, c_{k-1}) \equiv 0 \pmod{2^k}.$$

From the above equation, we get $(b_{k-1}, c_{k-1}) = (-1,-5) \pmod{2^k}$.
Now using the above expression in Equation (14) we get

$$\alpha_{k+1} = (b_k, c_k) = (-1,-5) \pmod{2^{k+1}}.$$

Hence $f(b_k, c_k) \equiv 0 \pmod{2^{k+1}}$. Similarly, on replacing $x+1$ by $y+5$ in $f(x,y)$ we get

$$(b_k, c_k) = (1,-5) \pmod{2^{k+1}}$$

and

$$f(b_k, c_k) \equiv 0 \pmod{2^{k+1}}.$$

Hence by definition, we found two nodes of the valuation tree of x^2y+5 labelled with $*$. □

References

[1] Amdeberhan, T., De Angelis, V., & Moll, V. H. (2013). *Complementary Bell numbers: Arithmetical properties and Wilf's conjecture. Advances in Combinatorics*, 23–56, Springer.

[2] Amdeberhan, T., Manna, D., & Moll, V. H. (2008). The 2-adic valuation of Stirling numbers. *Experimental Mathematics*, 17, 69–82.

[3] Berribeztia, A., Medina, L., Moll, A., Moll, V., & Noble, L. (2010). The p-adic valuation of Stirling numbers. *Journal for Algebra and Number Theory Academia*, 1, 1–30.

[4] Borwein, J. M., & Crandall, R. (2013). Closed forms: what they are and why we care. *Notices of The American Mathematical Society*, 60, 50–65.

[5] Brucal–Hallare, M., Goedhart, E. G., Riley, R. M., Sharma, V., & Thompson, B. (2021). *Solving quadratic and cubic Diophantine equations using* 2*-adic valuation trees*. Available online at: `https://doi.org/10.48550/arXiv.2105.03352`.

[6] Byrnes, A., Fink, J., Lavigne, G., Nogues, I., Rajasekaran, S., Yuan, A., Almodovar, L., Guan, X., Kesarwani, A., Medina, L., Rowland, E., & Moll, V. H. (2019). A closed-form solution might be given by a tree. Valuations of quadratic polynomials. *Scientia, Series A: Mathematical Sciences*, 29 11–28.

[7] Caicedo, J. B., Moll, V. H., Ramírez, J. L., & Villamizar, D. (2019). Extensions of set partitions and permutations. *Electronic Journal of Combinatorics*, 26(2), Article Number P2.20.

[8] Chow, T. Y. (1999). What is a closed-form number? *American Mathematical Monthly*, 106(5), 440–448.

[9] Conrad, K. *A multivariable Hensel's lemma*. Available online at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf`.

[10] Gouvêa, F. Q. (2020). *p-adic Numbers: An Introduction* (Universitext). (3rd ed.). Springer.

[11] Legendre, A. M. (1830). *Théorie des Nombres*. Firmin Didot Frères, Paris.

[12] Sun, X., & Moll, V. H. (2010). A binary tree representation for the 2-adic valuation of a sequence arising from a rational integral. *Integers*, 10(2), 211–222.