Malaysian Journal of Mathematical Sciences 10(S) February: 15-35 (2016)
Special Issue: The 3^{rd} International Conference on Mathematical Applications in Engineering 2014 (ICMAE'14)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Solvability and Number of Roots of Bi-Quadratic Equations over $p-$adic Fields

Saburov, M.* and Ahmad, M. A. K.

Department of Computational & Theoretical Sciences
Kulliyyah of Science, International Islamic University Malaysia

E-mail: msaburov@gmail.com
**Corresponding author*

ABSTRACT

Unlike the real number field $\mathbb{R}$, a bi-quadratic equation $x^4 + 1 = 0$ is solvable over some $p-$adic number fields $\mathbb{Q}_p$, say $p = 17, 41, \cdots$. Therefore, it is of independent interest to provide a solvability criterion for the bi-quadratic equation over $p-$adic number fields $\mathbb{Q}_p$. In this paper, we provide solvability criteria for the bi-quadratic equation $x^4 + ax^2 = b$ over domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$, where $p > 2$. Moreover, we also provide the number of roots of the bi-quadratic equation over the mentioned domains.

Keywords: Bi-quadratic equation, $p-$adic number, solvability criterion.

1. Introduction

The field $\mathbb{Q}_p$ of $p-$adic numbers which was introduced by German mathematician K. Hensel was motivated primarily by an attempt to bring the ideas and techniques of the power series into number theory. Their canonical representation is analogous to the expansion of analytic functions into power series. This is one of the manifestations of the analogy between algebraic numbers and algebraic functions.

For a fixed prime p, it is denoted the field of $p-$adic numbers by $\mathbb{Q}_p$ which is a completion of the rational numbers $\mathbb{Q}$ with respect to the non-Archimedean norm $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ given by

$$|x|_p = \begin{cases} p^{-k} & x \neq 0, \\ 0, & x = 0, \end{cases} \tag{1}$$

here, $x = p^k \frac{m}{n}$ with $r, m \in \mathbb{Z}$, $n \in \mathbb{N}$, $(m, p) = (n, p) = 1$. A number k is called *a $p-$order* of x and it is denoted by $ord_p(x) = k$.

Any $p-$adic number $x \in \mathbb{Q}_p$ can be uniquely represented in the following canonical form (Borevich and Shafarevich, 1986)

$$x = p^{ord_p(x)} \left(x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots \right)$$

where $x_0 \in \{1, 2, \cdots p-1\}$ and $x_i \in \{0, 1, 2, \cdots p-1\}$, $i \geq 1$,

We respectively denote the set of all *$p-$adic integers* and *units* of $\mathbb{Q}_p$ by

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}, \quad \mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

Any $p-$adic unit $x \in \mathbb{Z}_p^*$ has the following unique canonical form

$$x = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots$$

where $x_0 \in \{1, 2, \cdots p-1\}$ and $x_i \in \{0, 1, 2, \cdots p-1\}$, $i \in \mathbb{N}$.

Any nonzero $x \in \mathbb{Q}_p$ has a unique representation $x = \dfrac{x^*}{|x|_p}$, where $x^* \in \mathbb{Z}_p^*$.

A number $a_0 \in \mathbb{Z}$ is called *an r^{th} power residue modulo p* if the following congruent equation

$$x^r \equiv a_0 \ (mod\ p) \tag{2}$$

is solvable in $\mathbb{Z}$.

Proposition 1.1 (Rosen (2011)). *Let p be an odd prime, $a_0 \in \mathbb{Z}$, with $(a_0, p) = 1$ and $d = (r, p-1)$. The following statements hold true:*

1. *a_0 is the r^{th} power residue modulo p iff $a^{\frac{p-1}{d}} \equiv 1 \ (mod\ p)$.*
2. *If $a_0^{\frac{p-1}{d}} \equiv 1 \ (mod\ p)$ then the congruent equation (2) has d number of distinct (non-congruent) solutions in $\mathbb{Z}$.*

Throughout this paper, we always assume that $p > 2$ is an odd prime unless otherwise mentioned.

Let us consider the following quadratic equation

$$x^2 \equiv a_0 \ (mod\ p) \tag{3}$$

Due to Proposition 1.1, the congruent equation (3) is solvable iff $a_0^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ and it has two distinct non-congruent solutions in the set $\{1, 2, \cdots, p-1\}$. It is clear that one solution of the congruent equation (3) is less than $\frac{p}{2}$ and another solution is greater than $\frac{p}{2}$.

Definition 1.1. *We denote by $\sqrt{a_0}$ (resp. $-\sqrt{a_0}$) the solution of quadratic congruent equation (3) which is less than $\frac{p}{2}$ (resp. greater than $\frac{p}{2}$).*

Remark 1.1. *Due to the definition, $\sqrt{a_0}$ exists if and only if $a_0^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$. Moreover, $\sqrt{a_0}$ and $-\sqrt{a_0} \in \{1, 2, \cdots, p-1\}$.*

Let us now consider the following quadratic equation over $\mathbb{Q}_p$

$$x^2 = a \tag{4}$$

where $a \in \mathbb{Q}_p$ is a nonzero $p-$adic number. Let $a = \frac{a^*}{|a|_p}$ with $a^* = a_0 + a_1 p + a_2 p^2 + \cdots$ such that

$$a_0 \in \{1, 2, \cdots, p-1\}, \quad a_i \in \{0, 1, 2, \cdots, p-1\}, \ \forall\ i \in \mathbb{N}.$$

We know that the quadratic equation (4) is solvable in $\mathbb{Q}_p$ iff $a_0^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ and $\log_p |a|_p$ is even. Moreover, it has two distinct solutions x_+ and x_- such that $x_+^* \equiv \sqrt{a_0} \ (mod\ p)$ and $x_-^* \equiv -\sqrt{a_0} \ (mod\ p)$.

Definition 1.2. *We denote the solution x_+ (resp. x_-) of the quadratic equation equation* (4) *by $\sqrt{a}$ (resp. $-\sqrt{a}$).*

Remark 1.2. *By the definition, for the given nonzero $a \in \mathbb{Q}_p$, $\sqrt{a}$ exists if and only if $a_0^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ and $\log_p |a|_p$ is even. Moreover, $\sqrt{a}$ is a solution of the quadratic equation* (4) *such that $\left(\sqrt{a}\right)^* \equiv \sqrt{a_0} \ (mod\ p)$ and $-\sqrt{a}$ is a solution of the quadratic equation* (4) *such that $\left(-\sqrt{a}\right)^* \equiv -\sqrt{a_0} \ (mod\ p)$.*

Unlike the real number field $\mathbb{R}$, the bi-quadratic equation $x^4 + 1 = 0$ is solvable over some $p-$adic number fields $\mathbb{Q}_p$ such as $p = 17, 41, \cdots$. Therefore, it is of independent interest to provide a solvability criterion of a bi-quadratic equation $x^4 + ax^2 = b$ over $p-$adic number fields $\mathbb{Q}_p$. In this paper, we provide solvability criteria and the number of roots of the bi-quadratic equations $x^4 + ax^2 = b$ over the domains $\mathbb{Z}_p^*,\ \mathbb{Z}_p \setminus \mathbb{Z}_p^*,\ \mathbb{Q}_p \setminus \mathbb{Z}_p,\ \mathbb{Q}_p$.

It is worth of mentioning that the similar problems for cubic equations were studied in refs. (see Mukhamedov and Saburov (2013), Mukhamedov et al. (2013), Mukhamedov et al. (2014), Saburov and Ahmad (2014), and Saburov and Ahmad (2015)). Applications of those results were demonstrated in refs. (see Mukhamedov and Akin (2013a) and Mukhamedov and Akin (2013b)).

2. The Main Strategies

Obviously, we can apply the substitution method for the bi-quadratic equation. However, this method is not efficient. Let us explain it in a detail. We consider the bi-quadratic equation

$$x^4 + ax^2 = b. \tag{5}$$

where $a, b \in \mathbb{Q}_p$.

If we let $y = x^2$ then we may have the following quadratic equation $y^2 + ay = b$. In its own turns, in order to get a solvability criterion for the bi-quadratic equation, we have to solve the following quadratic equations $x^2 = \frac{-a \pm \sqrt{a^2+4b}}{2}$. To check whether one of the last two quadratic equations has a root or not, we have to verify that $\log_p |\frac{-a \pm \sqrt{a^2+4b}}{2}|$ is even number and the first $p-$adic digit of the $p-$adic unit $\left(\frac{-a \pm \sqrt{a^2+4b}}{2}\right)^*$ is a quadratic residue. This is a tedious work. However, our aim is to provide a solvability criterion for the bi-quadratic equation in terms of a, b. Therefore, we suggest another approach to fulfill our aim.

Remark 2.1. *It is worth of mentioning that the solvability of a bi-quadratic equation is completely different from the solvability of a quadratic equation obtained by the substitution method. For example, this quadratic equation* $y^2 - 2py + p^2 = 0$ *is solvable, i.e.,* $y = p$ *is a unique solution. However, this bi-quadratic equation* $x^4 - 2px^2 + p^2 = 0$ *is not solvable because of the fact that* $\sqrt{p}$ *does not exist.*

We know that, by definition, two $p-$adic numbers are close when their difference is divisible by a high power of p. This property enables $p-$adic numbers to encode congruence information in a way that turns out to be powerful tools in the theory of polynomial equation. In fact, Hensel's lifting lemma allows us to lift a simple solution of a polynomial equation over the finite field $\mathbb{F}_p$ up to the unique solution of the same polynomial equation over the ring $\mathbb{Z}_p$ of $p-$adic integer numbers. However, that solution cannot be any more lifted up to the field $\mathbb{Q}_p$ of $p-$adic numbers. At this point, we are aiming to study the relation between solutions of the polynomial equations over $\mathbb{Q}_p$ and $\mathbb{Z}_p$. We shall show that, indeed, any solution of any bi-quadratic equation over $\mathbb{Q}_p$ (or some special sets) can be uniquely determined by a solution of another bi-quadratic equation over $\mathbb{Z}_p^*$. Consequently, in some sense, it is enough to study bi-quadratic equations over $\mathbb{Z}_p^*$.

Whenever $a, b \neq 0$, let $a = \frac{a^*}{|a|_p}$ and $b = \frac{b^*}{|b|_p}$ where $a^* \in \mathbb{Z}_p^*$, $b^* \in \mathbb{Z}_p^*$ with

$$a^* = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots, \qquad b^* = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$$

Remark 2.2. *We use the notation* $\sqrt[r]{a} - \exists$ *whenever the monomial equation* $x^r = a$ *is solvable in* $\mathbb{Q}_p$. *The solvability criterion for the last monomial equation was given in ref. Mukhamedov and Saburov (2013). Namely, for* $p > 2$, *there exists* $\sqrt[4]{a}$ *if and only if* $\log_p |a|_p$ *is divisible by 4 and* $a_0^{\frac{p-1}{d}} \equiv 1 \ (mod\ p)$, *where* $d = (p-1, 4)$, $a^* = a_0 + a_1 p + \cdots$, *and* $a = \frac{a^*}{|a|_p}$.

If $ab = 0$ then the bi-quadratic equation (5) can be easily studied.

Proposition 2.1. *Let* $ab = 0$. *The following statements hold true:*

(*i*) *Let* $a = 0 = b$. *Then* (5) *has a solution* $x_0 = 0$ *of multiplicity-4.*

(*ii*) *Let* $a \neq 0 = b$. *If* $\sqrt{-a} - \exists$ *then* (5) *has solutions* $x_\pm = \pm\sqrt{-a}$ *and* $x_0 = 0$ *of multiplicity-2. Otherwise,* (5) *has only solution* $x_0 = 0$ *of multiplicity-2.*

(*iii*) *Let $a = 0 \neq b$. The bi-quadratic equation* (5) *is solvable over $\mathbb{Q}_p$ if and only if $\sqrt[4]{b} - \exists$. In this case, if $p \equiv 1 \pmod 4$ then* (5) *has 4 distinct solutions and if $p \equiv 3 \pmod 4$ then* (5) *has 2 distinct solutions.*

The proof is straightforward.

What it follows, we always assume that $ab \neq 0$.

Let $\mathbb{A} \subset \mathbb{Z}$ be any subset. We introduce the following set

$$\frac{\mathbb{Z}_p^*}{p^{\mathbb{A}}} := \left\{x \in \mathbb{Q}_p : \log_p |x|_p \in \mathbb{A}\right\}.$$

It is easy to check that

$$\frac{\mathbb{Z}_p^*}{p^{\mathbb{A}}} = \bigcup_{i \in \mathbb{A}} \mathbb{S}_{p^i}(0),$$

where $\mathbb{S}_{p^i}(0) = \{x \in \mathbb{Q}_p : |x|_p = p^i\}$ is the sphere with the radius p^i.

Proposition 2.2. *Let p be any prime, $a, b \in \mathbb{Q}_p$ with $ab \neq 0$, and $\mathbb{A} \subset \mathbb{Z}$ be any subset. The bi-quadratic equation* (5) *is solvable in the set $\dfrac{\mathbb{Z}_p^*}{p^{\mathbb{A}}}$ iff there exists a pair $(y^*, k) \in \mathbb{Z}_p^* \times \mathbb{A}$ such that y is a solution of the following bi-quadratic equation*

$$y^4 + A_k y^2 = B_k \tag{6}$$

where $A_k = ap^{2k}$ and $B_k = bp^{4k}$. Moreover, in this case, a solution of the bi-quadratic equation (5) *has the form $x = \dfrac{y^*}{p^k}$.*

Proof. Let $x \in \mathbb{Q}_p$ and $|x|_p = p^k$. Then $x \in \dfrac{\mathbb{Z}_p^*}{p^{\mathbb{A}}}$ is a solution of the bi-quadratic equation (5) if and only if $y^* = x|x|_p \in \mathbb{Z}_p^*$ is a solution of the bi-quadratic equation (6). This completes the proof. □

Here, we list frequently used domains in this paper.

1. If $\mathbb{A}_1 = \{0\}$ then $\dfrac{\mathbb{Z}_p^*}{p^{\mathbb{A}_1}} = \mathbb{Z}_p^*$;

2. If $\mathbb{A}_2 = \mathbb{N}_-$ (all negative natural numbers) then $\dfrac{\mathbb{Z}_p^*}{p^{\mathbb{A}_2}} = \mathbb{Z}_p \setminus \mathbb{Z}_p^*$;

3. If $\mathbb{A}_3 = \mathbb{N}$ then $\dfrac{\mathbb{Z}_p^*}{p^{\mathbb{A}_3}} = \mathbb{Q}_p \setminus \mathbb{Z}_p$;

4. If $\mathbb{A}_4 = \mathbb{Z}$ then $\dfrac{\mathbb{Z}_p^*}{p^{\mathbb{A}_4}} = \mathbb{Q}_p$.

Corollary 2.1. *Let p be any prime, $a, b \in \mathbb{Q}_p$ with $ab \neq 0$, and $\mathbb{A}_i \subset \mathbb{Z}$ be a subset given as above, $i = \overline{1,4}$. The bi-quadratic equation* (5) *is solvable in the set $\dfrac{\mathbb{Z}_p^*}{p^{\mathbb{A}_i}}$ iff there exists $(y^*, k) \in \mathbb{Z}_p^* \times \mathbb{A}_i$ such that y^* is a solution of the following bi-quadratic equation*

$$y^4 + A_k y^2 = B_k$$

where $A_k = ap^{2k}$ and $B_k = bp^{4k}$.

Consequently, it is enough to study solvability of the bi-quadratic equation (5) over $\mathbb{Z}_p^*$, where $a, b \in \mathbb{Q}_p$ with $ab \neq 0$.

Proposition 2.3. *Let p be any prime and $a, b \in \mathbb{Q}_p$ with $ab \neq 0$. If the bi-quadratic equation* (5) *is solvable in $\mathbb{Z}_p^*$ then either one of the following conditions holds true:*

(i) $|a|_p = |b|_p \geq 1$;

(ii) $|b|_p < |a|_p = 1$;

(iii) $|a|_p < |b|_p = 1$.

Proof. Let $x \in \mathbb{Z}_p^*$ be a solution of (5). Since $ab \neq 0$, one can get that

$$\begin{aligned} |b|_p = |x^4 + ax^2|_p &\leq \max\{1, |a|_p\}, \\ |a|_p = |ax^2|_p = |b - x^4|_p &\leq \max\{1, |b|_p\}, \\ 1 = |x^4|_p = |b - ax^2|_p &\leq \max\{|a|_p, |b|_p\}. \end{aligned}$$

Thus, if $|a|_p \neq |b|_p$ then $\max\{|a|_p, |b|_p\} = 1$ and if $|a|_p = |b|_p$ then $|a|_p = |b|_p \geq 1$. This yields the claim. □

This proposition gives necessary conditions for solvability of the bi-quadratic equation over $\mathbb{Z}_p^*$. To get the solvability criteria, we need Hensel's lifting lemma.

Lemma 2.1 (Hensel's Lemma)**.** *Let $f(x)$ be polynomial whose coefficients are $p-$adic integers. Let θ be a $p-$adic integer such that for some $i \geq 0$ we have*

$$f(\theta) \equiv 0 \ (mod\ p^{2i+1}),$$

$$f'(\theta) \equiv 0 \ (mod\ p^{i}), \quad f'(\theta) \not\equiv 0 \ (mod\ p^{i+1}).$$

Then $f(x)$ has a unique $p-$adic integer root x_0 which satisfies $x_0 \equiv \theta \ (mod\ p^{i+1})$.

3. The Solvability Criteria

Throughout this section we always assume that $p > 2$.

We present a solvability criterion of the bi-quadratic equation over $\mathbb{A}$

$$x^4 + ax^2 = b \tag{7}$$

where

$$\mathbb{A} \in \left\{\mathbb{Z}_p^*, \ \ \mathbb{Z}_p \setminus \mathbb{Z}_p^*, \ \ \mathbb{Q}_p \setminus \mathbb{Z}_p, \ \ \mathbb{Q}_p\right\}.$$

Let $a, b \in \mathbb{Q}_p$ with $ab \neq 0$ and $D = a^2 + 4b$.

We then have that $a = \dfrac{a^*}{|a|_p}$, $b = \dfrac{b^*}{|b|_p}$ and $D = \dfrac{D^*}{|D|_p}$ whenever $D \neq 0$, where

$$\begin{aligned} a^* &= a_0 + a_1 p + a_2 p^2 + \cdots \\ b^* &= b_0 + b_1 p + b_2 p^2 + \cdots \\ D^* &= d_0 + d_1 p + d_2 p^2 + \cdots \end{aligned}$$

where $a_0, b_0, d_0 \in \{1, 2, \cdots p-1\}$ and $a_i, b_i, d_i \in \{0, 1, 2, \cdots p-1\}$ for any $i \in \mathbb{N}$.

Throughout this paper, the notation $(a \vee b) - \exists$ means that there exists either a or b, the notation $(a \barwedge b) - \exists$ means that there exists only a or b, and the notation $(a \doublebarwedge b) - \exists$ means that there exists both a and b. In this case, it is clear that $\{(a \vee b) - \exists\} = \{(a \barwedge b) - \exists\} \bigcup \{(a \doublebarwedge b) - \exists\}$.

3.1 The Solvability Criterion over $\mathbb{Z}_p^*$

Theorem 3.1. *The bi-quadratic equation* (7) *is solvable in $\mathbb{Z}_p^*$ if and only if either one of the following conditions holds true:*

1. $|a|_p < |b|_p = 1, \quad \sqrt[4]{b} - \exists;$
2. $|b|_p < |a|_p = 1, \quad \sqrt{-a} - \exists;$
3. $|a|_p = |b|_p > 1, \quad \sqrt{ab} - \exists;$
4. $|a|_p = |b|_p = 1 \neq |D|_p, \quad \left(\sqrt{D} \ \bar{\wedge} \sqrt{-2a}\right) - \exists;$
5. $|a|_p = |b|_p = 1 = |D|_p, \quad \sqrt{D} - \exists, \quad \left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \vee \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$

Proof. Due to Proposition 2.3, if the bi-quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ then either one of the following conditions must be satisfied: $|a|_p = |b|_p \geq 1$ or $|b|_p < |a|_p = 1$ or $|a|_p < |b|_p = 1$. We shall study case by case.

1. Let $|a|_p < |b|_p = 1$. In this case, we want to show that the bi-quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{b}$ or equivalently $b_0^{\frac{p-1}{(4,p-1)}} \equiv 1 \ (mod\ p)$.

Only if part. Let $x \in \mathbb{Z}_p^*$ be a solution of the bi-quadratic equation (7). Since $|a|_p < 1$, it yields that $x^4 \equiv b \ (mod\ p)$ or $x_0^4 \equiv b_0 \ (mod\ p)$. This means that b_0 is the forth power residue modulo p, i.e., $b_0^{\frac{p-1}{(4,p-1)}} \equiv 1 \ (mod\ p)$.

If part. Let $b_0^{\frac{p-1}{(4,p-1)}} \equiv 1 \ (mod\ p)$. Then there exists $\bar{x} \in \{1, 2, \cdots p-1\}$ such that $\bar{x}^4 \equiv b_0 \ (mod\ p)$. Let us consider the following bi-quadratic function $f_{a,b}(x) = x^4 + ax^2 - b$. It is clear that

$$\begin{aligned} f_{a,b}(\bar{x}) &= \bar{x}^4 + a\bar{x}^2 - b \equiv \bar{x}^4 - b \equiv \bar{x}^4 - b_0 \equiv 0 \ (mod\ p), \\ f'_{a,b}(\bar{x}) &= 4\bar{x}^3 + 2a\bar{x} \equiv 4\bar{x}^3 \not\equiv 0 \ (mod\ p). \end{aligned}$$

Then due to Hensel's Lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b}(x) = 0$ and $x \equiv \bar{x} \ (mod\ p)$. Since $\bar{x} \not\equiv 0 \ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

2. Let $|b|_p < |a|_p = 1$. We show that the bi-quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{-a}$ or equivalently $(-a_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.

Only if part. Let $x \in \mathbb{Z}_p^*$ be a solution of the bi-quadratic equation (7). Since $|b|_p < 1$, it yields $x_0^2(x_0^2 + a_0) \equiv 0 \ (mod\ p)$. We have that $x_0^2 \equiv -a_0 \ (mod\ p)$. So, $-a_0$ is the quadratic residue modulo p, i.e, $(-a_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.

If part. Let $(-a_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$, so there exist $\bar{x}^2 \equiv -a_0 \ (mod\ p)$ where $(\bar{x}, p) = 1$. We consider the following bi-quadratic function $f_{a,b}(x) = x^4 + ax^2 - b$. It is clear that

$$\begin{aligned} f_{a,b}(\bar{x}) &= \bar{x}^4 + a\bar{x}^2 - b \equiv \bar{x}^2(\bar{x}^2 + a) \equiv {a_0}^2 - {a_0}^2 \equiv 0 \ (mod\ p), \\ f'_{a,b}(\bar{x}) &= 4\bar{x}^3 + 2a\bar{x} \equiv 2\bar{x}^3 + 2\bar{x}(\bar{x}^2 + a) \equiv 2\bar{x}^3 \not\equiv 0 \ (mod\ p). \end{aligned}$$

Then due to Hensel's Lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b}(x) = 0$ and $x \equiv \bar{x} \ (mod\ p)$. Since $\bar{x} \not\equiv 0 \ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

3. Let $|a|_p = |b|_p > 1$. We show that the bi-quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{ab}$ or equivalently $(a_0b_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ (because of $|ab|_p = |a|_p^2$). Since $|a|_p = |b|_p = p^k$ for some $k \in \mathbb{N}$, the solvability of the following two bi-quadratic equations are equivalent

$$x^4 + ax^2 = b, \qquad p^k x^4 + a^* x^2 = b^*. \tag{8}$$

Moreover, any solution of the first bi-quadratic equation is a solution of the second one and vise versa. On the other hand, the second bi-quadratic equation is suitable to apply Hensel's lemma. Therefore, we study the second bi-quadratic equation instead of the first one.

Only if part. Let $x \in \mathbb{Z}_p^*$ be a solution of the bi-quadratic equation $p^k x^4 + a^* x^2 = b^*$. We then have that

$$\begin{aligned} p^k x^4 + a^* x^2 &\equiv b^* \ (mod\ p) \\ a_0 x_0^2 &\equiv b_0 \ (mod\ p) \\ (a_0 x_0)^2 &\equiv a_0 b_0 \ (mod\ p). \end{aligned}$$

This means that a_0b_0 is a quadratic residue modulo p or $(a_0b_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\, p)$.

If part. Let $(a_0b_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\, p)$. Then there exists $(a_0\bar{x})^2 \equiv a_0b_0 \ (mod\, p)$ where $(\bar{x}, p) = 1$. We consider the following bi-quadratic function $g_{a,b}(x) = p^k x^4 + a^* x^2 - b^*$. We get that

$$\begin{aligned} g_{a,b}(\bar{x}) &= p^k\bar{x}^4 + a^*\bar{x}^2 - b^* \equiv a_0\bar{x}^2 - b_0 \equiv 0 \ (mod\ p), \\ g'_{a,b}(\bar{x}) &= 4p^k\bar{x}^3 + 2a^*\bar{x} \equiv 2a_0\bar{x} \not\equiv 0 \ (mod\ p). \end{aligned}$$

Then due to Hensel's Lemma, there exists $x \in \mathbb{Z}_p$ such that $g_{a,b}(x) = 0$ and $x \equiv \bar{x} \ (mod\ p)$. Since $\bar{x} \not\equiv 0 \ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$. This shows that the bi-quadratic equation (7) is also solvable in $\mathbb{Z}_p^*$.

Now let us consider the bi-quadratic equation (7) in the form of

$$(2x^2 + a)^2 = D. \tag{9}$$

It is clear that if $|a|_p = |b|_p = 1$ then $|D|_p = |a^2 + 4b|_p \leq 1$.

4. We consider the case $|a|_p = |b|_p = 1 \neq |D|_p$.

Let $D = 0$. We have that $2x^2 + a = 0$. The last equation is solvable over $\mathbb{Q}_p$ if and only if there exists $\sqrt{-2a}$. Since $|a|_p = 1$, we have that $\log_p |-2a|_p = 0$ is even. In this case, it can be easily checked that the solution x of the bi-quadratic equation (7) is in $\mathbb{Z}_p^*$. Therefore, if $|a|_p = |b|_p = 1$ and $D = 0$ then the bi-quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if $(-2a_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.

Let $0 < |D|_p < 1$. Let $y = 2x^2 + a$. The bi-quadratic equation (9) can be reduced to the quadratic equation $y^2 = D$. The last quadratic equation is solvable in $\mathbb{Q}_p$ iff $\log_p |D|_p$ is even and $d_0^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ or equivalently there exists $\sqrt{D}$.

If we let $\log_p |D|_p = -2k$ and $d_0^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ where $k > 0$ then we may have the following quadratic equation

$$x^2 = \frac{-a \pm \sqrt{D}}{2} = \frac{-a \pm p^k\sqrt{D^*}}{2}. \tag{10}$$

The last quadratic equation (10) is solvable over $\mathbb{Q}_p$ iff $\log_p \left|\frac{-a\pm\sqrt{D}}{2}\right|_p$ is even and $\left[2(-a_0 \pm p^k\sqrt{d_0})\right]^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.

Let us find the value of $\left|\frac{-a\pm\sqrt{D}}{2}\right|_p$ where $D = a^2 + 4b$. We know that

$$\left|D - a^2\right|_p = \left|\sqrt{D} - a\right|_p \left|\sqrt{D} + a\right|_p = |4b|_p = 1$$

Since $\left|\sqrt{D} \pm a\right|_p \leq 1$, due to the previous equality, we have that $\left|\sqrt{D} \pm a\right|_p = 1$. Therefore, $\log_p \left|\frac{-a\pm\sqrt{D}}{2}\right|_p = 0$ is always even.

Since $k > 0$, we have that $\left[2(-a_0 \pm p^k\sqrt{d_0})\right]^{\frac{p-1}{2}} \equiv (-2a_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$. This is equivalent to say that there exists $\sqrt{-2a}$. In this case, we can easily checked that the solution x of the bi-quadratic equation (7) is in $\mathbb{Z}_p^*$. Therefore, if $|a|_p = |b|_p = 1 \neq |D|_p$ and there exists $\sqrt{D}$ then the bi-quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{-2a}$.

5. We consider the case $|a|_p = |b|_p = 1 = |D|_p$.

Then we have that $\left[2(\sqrt{d_0}-a_0)\right]^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ or $\left[2(-\sqrt{d_0}-a_0)\right]^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$. We can easily checked that the solution x of the bi-quadratic equation (7) is in $\mathbb{Z}_p^*$. Therefore, if $|a|_p = |b|_p = 1 = |D|_p$ and there exists $\sqrt{D}$ then the bi-quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if $\left[2(\sqrt{d_0}-a_0)\right]^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ or $\left[2(-\sqrt{d_0}-a_0)\right]^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ (this is equivalently to say that there exists $\sqrt{\frac{-a+\sqrt{D}}{2}}$ or $\sqrt{\frac{-a-\sqrt{D}}{2}}$). This completes the proof. □

3.2 The Solvability Criterion over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$

Theorem 3.2. *The bi-quadratic equation* (7) *is solvable in* $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ *if and only if either one of the following conditions holds true:*

1. $|a|_p^2 < |b|_p < 1, \quad \sqrt[4]{b} - \exists;$
2. $|b|_p < |a|_p^2 < 1, \quad \sqrt{-a} - \exists;$
3. $|a|_p^2 > |b|_p, \ |a|_p > |b|_p, \quad \sqrt{ab} - \exists;$
4. $|D|_p < |a|_p^2 = |b|_p < 1, \quad \left(\sqrt{D} \ \bar{\wedge} \ \sqrt{-2a}\right) - \exists;$
5. $|D|_p = |a|_p^2 = |b|_p < 1, \quad \sqrt{D} - \exists, \quad \left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \vee \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$

Proof. Let $x \in \mathbb{Q}_p$ be a nonzero $p-$adic number and $|x|_p = p^k$ where $k \in \mathbb{Z}$. Due to Corollary 2.1, x is a solution of the bi-quadratic equation (7) in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ if and only if $y = p^k x$ is a solution of the following bi-quadratic equation

$$y^4 + A_k y^2 = B_k \tag{11}$$

in $\mathbb{Z}_p^*$ for some $k \in \mathbb{N}_-$ where $A_k = ap^{2k}$, $B_k = bp^{4k}$.

It is clear that $A_k^* = a^*$, $B_k^* = b^*$ and $|A_k|_p = p^{-2k}|a|_p$, $|B_k|_p = p^{-4k}|b|_p$. Let $D = a^2 + 4b$ and $D_k = A_k^2 + 4B_k$. Then $D_k = p^{4k}D$ and $D_k^* = D^*$, $|D_k|_p = p^{-4k}|D|_p$ whenever $D_k \neq 0$ (or equivalently $D \neq 0$). We know that, due to Theorem 3.1, the bi-quadratic equation (11) is solvable in $\mathbb{Z}_p^*$ if and only if either one of the following conditions holds true:

I. $|A_k|_p < |B_k|_p = 1, \ \sqrt[4]{B_k} - \exists;$

II. $|B_k|_p < |A_k|_p = 1$, $\sqrt{-A_k} - \exists$;

III. $|A_k|_p = |B_k|_p > 1$, $\sqrt{A_k B_k} - \exists$;

IV. $|A_k|_p = |B_k|_p = 1 \neq |D_k|_p$, $\sqrt{D_k} - \exists$, $\sqrt{-2A_k} - \exists$;

V. $|A_k|_p = |B_k|_p = 1 = |D_k|_p$, $\sqrt{D_k} - \exists$, $\left(\sqrt{\frac{-A_k+\sqrt{D_k}}{2}} \vee \sqrt{\frac{-A_k-\sqrt{D_k}}{2}}\right) - \exists$

We want to describe all $p-$adic numbers $a, b \in \mathbb{Q}_p$ for which at least one of the conditions I–V should be satisfied for some $k \in \mathbb{N}_-$.

1. Let us consider the condition I: $|A_k|_p < |B_k|_p = 1$ and $\sqrt[4]{B_k} - \exists$ (or equivalently $b_0^{\frac{p-1}{(4,p-1)}} \equiv 1 \ (mod\ p)$).

We have that $\log_p p^{-4k}|b|_p = 0$. Hence, we obtain that $4k = \log_p |b|_p$. It is clear that $k \in \mathbb{N}_-$ if and only if $\log_p |b|_p$ is divisible by 4 and $|b|_p < 1$. Moreover, one has that $|A_k|_p = p^{-2k}|a|_p < 1$, where $k = \frac{1}{4}\log_p |b|_p$, if and only if $|a|_p^2 < |b|_p$. Therefore, if $|a|_p^2 < |b|_p < 1$, $4 \mid \log_p |b|_p$ and $b_0^{\frac{p-1}{(4,p-1)}} \equiv 1 \ (mod\ p)$ (or equivalently $|a|_p^2 < |b|_p < 1$ and $\sqrt[4]{b} - \exists$) then the condition I is satisfied with $k = \frac{1}{4}\log_p |b|_p \in \mathbb{N}_-$.

2. Let us consider the condition II: $|B_k|_p < |A_k|_p = 1$ and $\sqrt{-A_k} - \exists$ (or equivalently $(-a_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$).

We have that $|A_k|_p = 1$ if and only if $2k = \log_p |a|_p$. It is clear that $k \in \mathbb{N}_-$ if and only if $\log_p |a|_p$ is even and $|a|_p < 1$. Besides that, we have that $|B_k|_p < 1$, where $k = \frac{1}{2}\log_p |a|_p$, if only if $|b|_p < |a|_p^2$. Hence, if $|b|_p < |a|_p^2 < 1$, $2 \mid \log_p |a|_p$ and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ (or equivalently $|b|_p < |a|_p^2 < 1$ and $\sqrt{-a} - \exists$) then the condition II is satisfied with $k = \frac{1}{2}\log_p |a|_p \in \mathbb{N}_-$.

3. Let us consider the condition III: $|A_k|_p = |B_k|_p > 1$ and $\sqrt{A_k B_k} - \exists$; (or equivalently $(a_0 b_0)^{\frac{p-1}{2}} \equiv 1 (mod\ p)$).

We have that $\log_p \left(p^{-4k}|b|_p\right) = \log_p \left(p^{-2k}|a|_p\right) > 0$. Hence, we obtain that $2k = \log_p |b|_p - \log_p |a|_p$. It is clear that $k \in \mathbb{N}_-$ if and only if $\log_p \frac{|b|_p}{|a|_p}$ (equivalently $\log_p |ab|_p$) is even and $|b|_p < |a|_p$. Moreover, one has that $\log_p(p^{-2k}|a|_p) > 0$, where $k = \frac{1}{2}\log_p \frac{|b|_p}{|a|_p}$, if and only if $|a|_p^2 > |b|_p$. Therefore, if $|a|_p^2 > |b|_p$, $|a|_p > |b|_p$, and $\sqrt{ab} - \exists$ then the condition III is satisfied with $k = \frac{1}{2}\log_p \frac{|b|_p}{|a|_p} \in \mathbb{N}_-$.

4. Let us consider the condition IV: $|A_k|_p = |B_k|_p = 1 \neq |D_k|_p$, $\sqrt{D_k} - \exists$, and $\sqrt{-2A_k} - \exists$.

We have that $|A_k|_p = 1$ and $|B_k|_p = 1$, simultaneously, if and only if $2k = \log_p |a|_p$ and $4k = \log_p |b|_p$. This means that $|a|_p^2 = |b|_p$ and $\log_p |a|_p$ is even. It is clear that $k \in \mathbb{N}_-$ if and only if $|a|_p < 1$, $|b|_p < 1$, $\log_p |a|_p$ is even and $|a|_p^2 = |b|_p$. From here, if $\log_p |a|_p$ is even then $\log_p |b|_p$ is also divisible by 4. We know that $\log_p |D_k|_p = -4k + \log_p |D|_p$. So, $\log_p |D_k|_p$ is even if and only if $\log_p |D|_p$ is even. Besides that, we have that $|D_k|_p < 1$ if and only if $|D|_p < |a|_p^2 = |b|_p$, where $k = \frac{1}{2}\log_p |a|_p = \frac{1}{4}\log_p |b|_p$. Therefore, if $|D|_p < |a|_p^2 = |b|_p < 1$, $\sqrt{D} - \exists$, and $\sqrt{-2a} - \exists$ then the condition V is satisfied with $k = \frac{1}{2}\log_p |a|_p = \frac{1}{4}\log_p |b|_p \in \mathbb{N}_-$.

5. Let us consider the condition V: $|A_k|_p = |B_k|_p = 1 = |D_k|_p$, $\sqrt{D_k} - \exists$, $\left(\sqrt{\frac{-A_k+\sqrt{D_k}}{2}} \vee \sqrt{\frac{-A_k-\sqrt{D_k}}{2}}\right) - \exists$.

We have that $|A_k|_p = 1$ and $|B_k|_p = 1$, simultaneously, if and only if $2k = \log_p |a|_p$ and $4k = \log_p |b|_p$. This means that $|a|_p^2 = |b|_p$ and $\log_p |a|_p$ is even. It is clear that $k \in \mathbb{N}_-$ if and only if $|a|_p < 1$, $|b|_p < 1$, $\log_p |a|_p$ is even, and $|a|_p^2 = |b|_p$. Besides that, we have that $|D_k|_p = 1$ if and only if $|D|_p = |a|_p^2 = |b|_p$, where $k = \frac{1}{2}\log_p |a|_p = \frac{1}{4}\log_p |b|_p$. From here, if $\log_p |a|_p$ is even then $\log_p |b|_p$ and $\log_p |D|_p$ are also divisible by 4. In this case, $\left(\sqrt{\frac{-A_k+\sqrt{D_k}}{2}} \vee \sqrt{\frac{-A_k-\sqrt{D_k}}{2}}\right) - \exists$ is equivalent to $\left(\sqrt{\frac{-a+\sqrt{D}}{2}} \vee \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$. Therefore, if $|D|_p = |a|_p^2 = |b|_p < 1$, $\sqrt{D} - \exists$, $\left(\sqrt{\frac{-a+\sqrt{D}}{2}} \vee \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$ then the condition V is satisfied with $k = \frac{1}{2}\log_p |a|_p = \frac{1}{4}\log_p |b|_p \in \mathbb{N}_-$. This completes the proof. □

3.3 The Solvability Criteria over $\mathbb{Q}_p \setminus \mathbb{Z}_p$ and $\mathbb{Q}_p$

The proof of the following theorem is similar to the proof of Theorem 3.2.

Theorem 3.3. *The bi-quadratic equation* (7) *is*

(*A*) *Solvable in* $\mathbb{Q}_p \setminus \mathbb{Z}_p$ *iff either one of the following conditions holds true:*

1. $|a|_p^2 < |b|_p$, $|b|_p > 1$, $\sqrt[4]{b} - \exists$;
2. $|a|_p^2 > |b|_p$, $|a|_p > 1$, $\sqrt{-a} - \exists$;

3. $|a|_p^2 > |b|_p, \quad |a|_p < |b|_p, \quad \sqrt{ab} - \exists;$
4. $|D|_p < |a|_p^2 = |b|_p, \quad |b|_p > 1, \quad \left(\sqrt{D} \ \bar{\bar{\wedge}} \ \sqrt{-2a}\right) - \exists;$
5. $|D|_p = |a|_p^2 = |b|_p > 1, \ \sqrt{D} - \exists, \ \left(\sqrt{\frac{-a+\sqrt{D}}{2}} \vee \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists.$

(*B*) *Solvable in* $\mathbb{Q}_p$ *iff either one of the following conditions holds true:*

1. $|a|_p^2 < |b|_p, \quad \sqrt[4]{b} - \exists;$
2. $|a|_p^2 > |b|_p, \quad \left(\sqrt{-a} \ \vee \ \sqrt{ab}\right) - \exists;$
3. $|a|_p^2 = |b|_p > |D|_p, \quad \left(\sqrt{D} \ \bar{\bar{\wedge}} \ \sqrt{-2a}\right) - \exists;$
4. $|a|_p^2 = |b|_p = |D|_p, \quad \sqrt{D} - \exists, \quad \left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \vee \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists.$

Remark 3.1. *In the p−adic analysis, the field* $\mathbb{Q}_2$ *should be treated in a completely different way from the field* $\mathbb{Q}_p$ *for* $p > 2$. *In a forthcoming paper, we are aiming to study the bi-quadratic equation in* $\mathbb{Q}_2$.

4. The Number of Roots

In this section, we present the number $\mathbf{N}_{\mathbb{A}}(x^4 + ax^2 - b)$ of roots (including multiplicity) of bi-quadratic equation

$$x^4 + ax^2 = b \tag{12}$$

where

$$\mathbb{A} \in \left\{\mathbb{Z}_p^*, \ \ \mathbb{Z}_p \setminus \mathbb{Z}_p^*, \ \ \mathbb{Q}_p \setminus \mathbb{Z}_p, \ \ \mathbb{Q}_p\right\}.$$

Theorem 4.1. *Let the bi-quadratic equation* (12) *be solvable in* $\mathbb{A}$ *where* $\mathbb{A} \in \left\{\mathbb{Z}_p^*, \ \mathbb{Z}_p \setminus \mathbb{Z}_p^*, \ \mathbb{Q}_p \setminus \mathbb{Z}_p, \ \mathbb{Q}_p\right\}$. *Then the following statements hold true:*

$$\mathbf{N}_{\mathbb{Z}_p^*}(x^4 + ax^2 - b) =$$

$$= \begin{cases} 4, & |a|_p < |b|_p = 1, \ \sqrt[4]{b} - \exists, \ p \equiv 1 \ (mod \ 4) \\ 4, & |a|_p = |b|_p = 1 > |D|_p, \ \left(\sqrt{D} \ \bar{\bar{\wedge}} \ \sqrt{-2a}\right) - \exists \\ 4, & |a|_p = |b|_p = 1 = |D|_p, \ \sqrt{D} - \exists, \left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \bar{\bar{\wedge}} \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists \\ 2, & |a|_p < |b|_p = 1, \ \sqrt[4]{b} - \exists, \ p \equiv 3 \ (mod \ 4) \\ 2, & |b|_p < |a|_p = 1, \ \sqrt{-a} - \exists \\ 2, & |a|_p = |b|_p > 1, \ \sqrt{ab} - \exists \\ 2, & |a|_p = |b|_p = 1 = |D|_p, \ \sqrt{D} - \exists, \left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \bar{\wedge} \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists \end{cases}$$

$$\mathbf{N}_{\mathbb{Z}_p\setminus\mathbb{Z}_p^*}(x^4+ax^2-b)=$$
$$=\begin{cases} 4, & |a|_p^2<|b|_p<1,\ \sqrt[4]{b}-\exists,\ p\equiv 1\ (mod\ 4)\\ 4, & |b|_p<|a|_p^2<1,\ \left(\sqrt{-a}\ \bar{\bar{\wedge}}\ \sqrt{ab}\right)-\exists\\ 4, & |D|_p<|a|_p^2=|b|_p<1,\ \left(\sqrt{D}\ \bar{\bar{\wedge}}\sqrt{-2a}\right)-\exists\\ 4, & |D|_p=|a|_p^2=|b|_p<1,\sqrt{D}-\exists,\ \left(\sqrt{\frac{-a+\sqrt{D}}{2}}\bar{\bar{\wedge}}\sqrt{\frac{-a-\sqrt{D}}{2}}\right)-\exists\\ 2, & |a|_p^2<|b|_p<1,\ \sqrt[4]{b}-\exists,\ p\equiv 3\ (mod\ 4)\\ 2, & |b|_p<|a|_p^2<1,\ \left(\sqrt{-a}\ \bar{\wedge}\ \sqrt{ab}\right)-\exists\\ 2, & |a|_p>|b|_p,\ |a|_p\geq 1,\ \sqrt{ab}-\exists\\ 2, & |D|_p=|a|_p^2=|b|_p<1,\ \sqrt{D}-\exists,\left(\sqrt{\frac{-a+\sqrt{D}}{2}}\bar{\wedge}\sqrt{\frac{-a-\sqrt{D}}{2}}\right)-\exists \end{cases}$$

$$\mathbf{N}_{\mathbb{Q}_p\setminus\mathbb{Z}_p}(x^4+ax^2-b)=$$
$$=\begin{cases} 4, & |a|_p^2<|b|_p,\ |b|_p>1,\ \sqrt[4]{b}-\exists,\ p\equiv 1\ (mod\ 4)\\ 4, & |a|_p^2>|b|_p,\ |a|_p<|b|_p,\ \left(\sqrt{-a}\,\bar{\bar{\wedge}}\,\sqrt{ab}\right)-\exists\\ 4, & |D|_p<|a|_p^2=|b|_p,\ |b|_p>1,\ \left(\sqrt{D}\,\bar{\bar{\wedge}}\sqrt{-2a}\right)-\exists\\ 4, & |D|_p=|a|_p^2=|b|_p>1,\ \sqrt{D}-\exists,\left(\sqrt{\frac{-a+\sqrt{D}}{2}}\bar{\bar{\wedge}}\sqrt{\frac{-a-\sqrt{D}}{2}}\right)-\exists\\ 2, & |a|_p^2<|b|_p,\ |b|_p>1,\ \sqrt[4]{b}-\exists,\ p\equiv 3\ (mod\ 4)\\ 2, & |a|_p^2>|b|_p,\ |a|_p<|b|_p,\ \left(\sqrt{-a}\,\bar{\wedge}\,\sqrt{ab}\right)-\exists\\ 2, & |a|_p\geq|b|_p,\ |a|_p>1,\ \sqrt{-a}-\exists\\ 2, & |D|_p=|a|_p^2=|b|_p>1,\ \sqrt{D}-\exists,\ \left(\sqrt{\frac{-a+\sqrt{D}}{2}}\,\bar{\wedge}\,\sqrt{\frac{-a-\sqrt{D}}{2}}\right)-\exists \end{cases}$$

$$\mathbf{N}_{\mathbb{Q}_p}(x^4+ax^2-b)=$$
$$=\begin{cases} 4, & |a|_p^2<|b|_p,\ \sqrt[4]{b}-\exists,\ p\equiv 1\ (mod\ 4)\\ 4, & |a|_p^2>|b|_p,\ \left(\sqrt{-a}\ \bar{\bar{\wedge}}\ \sqrt{ab}\right)-\exists\\ 4, & |a|_p^2=|b|_p>|D|_p,\ \left(\sqrt{D}\ \bar{\bar{\wedge}}\sqrt{-2a}\right)-\exists\\ 4, & |a|_p^2=|b|_p=|D|_p,\ \sqrt{D}-\exists,\ \left(\sqrt{\frac{-a+\sqrt{D}}{2}}\bar{\bar{\wedge}}\sqrt{\frac{-a-\sqrt{D}}{2}}\right)-\exists\\ 2, & |a|_p^2<|b|_p,\ \sqrt[4]{b}-\exists,\ p\equiv 3\ (mod\ 4)\\ 2, & |a|_p^2>|b|_p,\ \left(\sqrt{-a}\ \bar{\wedge}\ \sqrt{ab}\right)-\exists\\ 2, & |a|_p^2=|b|_p=|D|_p,\ \sqrt{D}-\exists,\ \left(\sqrt{\frac{-a+\sqrt{D}}{2}}\bar{\wedge}\sqrt{\frac{-a-\sqrt{D}}{2}}\right)-\exists \end{cases}$$

Proof. Let us discuss the case $\mathbb{Z}_p^*$. As we refer to Theorm 3.1, the bi-quadratic equation (12) is solvable in $\mathbb{Z}_p^*$ if and only if one of the conditions $1-5$ should be satisfied. We want to verify the number of solutions for every case.

Condition $1: |a|_p < |b|_p = 1,\ \sqrt[4]{b} - \exists$. This means that $b_0^{\frac{p-1}{4,p-1}} \equiv 1\ (mod\ p)$. In this case, the number of solutions of bi-quadratic equation (12) is the same as the number of solutions of the equation $x_0^4 \equiv b_0\ (mod\ p)$. If $p \equiv 1\ (mod\ 4)$ then the last congruent equation has 4 solutions and if $p \equiv 3\ (mod\ 4)$ then the last congruent equation has 2 solutions . Therefore, if $|a|_p < |b|_p = 1$, there exists $\sqrt[4]{b}$ and $p \equiv 1\ (mod\ 4)$ then the bi-quadratic equation (12) has 4 solutions in $\mathbb{Z}_p^*$ and if $|a|_p < |b|_p = 1$, there exists $\sqrt[4]{b}$ and $p \equiv 3\ (mod\ 4)$ then the bi-quadratic equation (12) has 2 solutions in $\mathbb{Z}_p^*$.

Condition $2: |b|_p < |a|_p = 1,\ \sqrt{-a} - \exists$. In this case, the number of solutions of the bi-quadratic equation (12) is the same as the number of solutions of the congruent equation $x_0^2 + a_0 \equiv 0\ (mod\ p)$. The last equation has two solutions because of $(-a_0)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$. Therefore, if $|b|_p < |a|_p = 1$ and there exists $\sqrt{-a}$ then the bi-quadratic equation (12) has two solutions in $\mathbb{Z}_p^*$.

Condition $3: |a|_p = |b|_p > 1,\ \sqrt{ab} - \exists$. In this case, the number of solutions of the bi-quadratic equation (12) is the same as the number of solution of the equation $a_0 x_0^2 \equiv b_0\ (mod\ p)$. The last congruent equation has two solutions because of $(a_0 b_0)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$. Therefore, if $|a|_p = |b|_p > 1$ and there exists $\sqrt{ab}$ then the bi-quadratic equation (12) has two solutions in $\mathbb{Z}_p^*$.

Now, let us consider the bi-quadratic (12) in the form of

$$(2x^2 + a)^2 = D. \tag{13}$$

Condition $4: |a|_p = |b|_p = 1 > |D|_p,\ \sqrt{D} - \exists,\ \sqrt{-2a} - \exists$.

Let $D = 0$. We have that $(2x^2 + a)^2 = 0$. It is clear that $2x^2 + a = 0$ and it has two solutions because of $(-2a_0)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$. We can easily verify that these solutions are in $\mathbb{Z}_p^*$. Therefore, if $|a|_p = |b|_p = 1,\ D = 0$ and there exists $\sqrt{-2a}$ then the bi-quadratic equation (12) has four solutions (two solutions of multiplicity-2) in $\mathbb{Z}_p^*$.

Let $0 < |D|_p < 1$. The bi-quadratic equation (13) has the same number of solutions as the total number of solutions of equations $2x^2 + a = \sqrt{D}$ and $2x^2 + a = -\sqrt{D}$. Each of the equations have two solutions because of $(-2a \pm \sqrt{D})^{\frac{p-1}{2}} \equiv (-2a_0)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$. It is easily can be checked that these four

solutions are in $\mathbb{Z}_p^*$. Hence, if $|a|_p = |b|_p = 1 > |D|_p \neq 0$, there exist $\sqrt{D}$ and $\sqrt{-2a}$ then the bi-quadratic equation (12) has four solutions in $\mathbb{Z}_p^*$.

Condition 5 : $|a|_p = |b|_p = 1 = |D|_p$, $\sqrt{D} - \exists$ and there exists either $\sqrt{\frac{-a+\sqrt{D}}{2}}$ or $\sqrt{\frac{-a-\sqrt{D}}{2}}$.

Let $\left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \bar{\wedge} \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$, i.e., there exist both $\sqrt{\frac{-a+\sqrt{D}}{2}}$ and $\sqrt{\frac{-a-\sqrt{D}}{2}}$. The bi-quadratic equation (13) has the same number of solutions as the total number of solutions of equations $2x^2+a = \sqrt{D}$ and $2x^2+a = -\sqrt{D}$. The total number of solutions of the last two equations is four because each of them has two solutions. We can easily verify that these solutions are in $\mathbb{Z}_p^*$. Therefore, if $|a|_p = |b|_p = 1 = |D|$, there exist $\sqrt{D}$ and $\sqrt{\frac{-a\pm\sqrt{D}}{2}}$ then the bi-quadratic equation (12) has for solutions in $\mathbb{Z}_p^*$.

Let $\left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \bar{\wedge} \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$, i.e., there exists only one of $\sqrt{\frac{-a+\sqrt{D}}{2}}$ and $\sqrt{\frac{-a-\sqrt{D}}{2}}$. The bi-quadratic equation (13) has the same number of solutions as the total number of solutions of equations $2x^2 + a = \sqrt{D}$ and $2x^2 + a = -\sqrt{D}$. The total number of solutions of the last two equations is two because only one of them is solvable (each equation has two solutions if it is solvable). It is also can be checked that these solutions are in $\mathbb{Z}_p^*$. Therefore, if $|a|_p = |b|_p = 1 = |D|$, there exists $\sqrt{D}$ and there exists only one of $\sqrt{\frac{-a+\sqrt{D}}{2}}$ and $\sqrt{\frac{-a-\sqrt{D}}{2}}$ then the bi-quadratic equation (12) has two solutions in $\mathbb{Z}_p^*$.

Let us turn to the case $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$. Due to the Theorem 3.2, the bi-quadratic equation (12) is solvable in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ if and only if one of conditions $1-5$ holds true. We want to find the number of solutions in every case.

Condition 1 : $|a|_p^2 < |b|_p < 1$ and $\sqrt[4]{b} - \exists$. The number of solutions of the bi-quadratic equation (12) in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is the same as the number of solutions of the following bi-quadratic equation in $\mathbb{Z}_p^*$,

$$y^4 + a\sqrt{|b|_p}y^2 = b^*.$$

It is clear that $\left|a\sqrt{|b|_p}\right|_p < |b^*|_p = 1$ and there exists $\sqrt[4]{b}$ or equivalently $b_0^{\frac{p-1}{(4,p-1)}} \equiv 1 \ (mod \ p)$. In this case, we have two distinct solutions in $\mathbb{Z}_p^*$ if

$p \equiv 3\ (mod\ 4)$ and four distinct solutions in $\mathbb{Z}_p^*$ if $p \equiv 1\ (mod\ 4)$. Thus, if $|a|_p^2 < |b|_p < 1$, there exists $\sqrt[4]{b}$ and $p \equiv 3\ (mod\ 4)$ then the bi-quadratic equation (12) has two distinct solutions in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ and if $|a|_p^2 < |b|_p < 1$, there exists $\sqrt[4]{b}$ and $p \equiv 1\ (mod\ 4)$ then the bi-quadratic equation (12) has four distinct solutions in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Conditions $2-3$: $|b|_p < |a|_p^2 < 1$, $\sqrt{-a} - \exists$ and $|a|_p^2 > |b|_p$, $|a|_p > |b|_p$, $\sqrt{ab} - \exists$. Now, let us define the following sets

$$\begin{aligned}
\mathbf{A} &= \left\{(a,b) \in \mathbb{Q}_p^2 :\ |b|_p < |a|_p^2 < 1,\ \sqrt{-a} - \exists\right\},\\
\mathbf{B} &= \left\{(a,b) \in \mathbb{Q}_p^2 : |a|_p^2 > |b|_p,\ |a|_p > |b|_p,\ \sqrt{ab} - \exists\right\},\\
\mathbf{S} &= \{(a,b) \in \mathbb{Q}_p^2 :\ |b|_p < |a|_p^2 < 1,\ \left(\sqrt{-a}\ \vee\ \sqrt{ab}\right) - \exists\},\\
\mathbf{B}_1 &= \left\{(a,b) \in \mathbb{Q}_p^2 : |b|_p < |a|_p^2 < 1,\ \sqrt{ab} - \exists\right\},\\
\mathbf{B}_2 &= \{(a,b) \in \mathbb{Q}_p^2 :\ |a|_p > |b|_p,\ |a|_p \geq 1,\ \sqrt{ab} - \exists\},\\
\mathbf{S}_1 &= \{(a,b) \in \mathbb{Q}_p^2 :\ |b|_p < |a|_p^2 < 1,\ \left(\sqrt{-a}\ \bar{\vee}\ \sqrt{ab}\right) - \exists\},\\
\mathbf{S}_2 &= \{(a,b) \in \mathbb{Q}_p^2 :\ |b|_p < |a|_p^2 < 1,\ \left(\sqrt{-a}\ \bar{\wedge}\ \sqrt{ab}\right) - \exists\}.
\end{aligned}$$

One can easily checked that $\mathbf{B} = \mathbf{B}_1 \cup \mathbf{B}_2$, $\mathbf{S} = \mathbf{S}_1 \cup \mathbf{S}_2 = \mathbf{A} \cup \mathbf{B}_1$ and $\mathbf{A} \cup \mathbf{B} = \mathbf{S} \cup \mathbf{B}_2$

Firstly, let us consider the set $\mathbf{S}_1$. In this case, the number of solutions of the bi-quadratic equation (12) in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is the same as the total number of solutions of the following bi-quadratic equations in $\mathbb{Z}_p^*$,

$$y^4 + a^* y^2 = |a|_p^2 b \tag{14}$$

$$z^4 + a\left|\frac{b}{a}\right|_p z^2 = b\left|\frac{b}{a}\right|_p^2 \tag{15}$$

It is clear that $\left||a|_p^2 b\right|_p < |a^*|_p = 1$, $\left|a\left|\frac{b}{a}\right|_p\right|_p = \left|b\left|\frac{b}{a}\right|_p^2\right|_p > 1$, $\left(\sqrt{-a}\ \bar{\bar{\vee}}\ \sqrt{ab}\right) - \exists$. We have already discussed that each bi-quadratic equation given above has two solution in $\mathbb{Z}_p^*$. Thus, if $|b|_p < |a|_p^2 < 1$ and $\left(\sqrt{-a}\ \bar{\bar{\wedge}}\ \sqrt{ab}\right) - \exists$ then the bi-quadratic equation (12) has four distinct solutions in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Next, let us consider the set $\mathbf{S}_2$. In this case, the number of solutions of the bi-quadratic equation (12) in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is the same as the total number of solutions of the bi-quadratic equation (14) and (15) in $\mathbb{Z}_p^*$. It is clear that

$\left||a|_p^2 b\right|_p < |a^*|_p = 1$, $\left|a\left|\frac{b}{a}\right|_p\right|_p = \left|b\left|\frac{b}{a}\right|_p^2\right|_p > 1$ and $\left(\sqrt{-a} \ \bar{\wedge} \ \sqrt{ab}\right) - \exists$. In this case, as we have already discussed, that only one of the equations (14) and (15) is solvable. Therefore, if $|b|_p < |a|_p^2 < 1$ and $\left(\sqrt{-a} \ \bar{\wedge} \ \sqrt{ab}\right) - \exists$ then the bi-quadratic equation (12) has two distinct solutions in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Lastly, let us consider the set $\mathbf{B}_2$. In this case, the number of solutions of the bi-quadratic equation (12) in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is the same as the number of solutions of the bi-quadratic equation (15) $\mathbb{Z}_p^*$. It is clear that $\left|a\left|\frac{b}{a}\right|_p\right|_p = \left|b\left|\frac{b}{a}\right|_p^2\right|_p > 1$ and $\sqrt{ab} - \exists$. We have already discussed that bi-quadratic (15) equation has two solution in $\mathbb{Z}_p^*$. Therefore, if $|a|_p > |b|_p$, $|a|_p \geq 1$ and $\sqrt{ab} - \exists$ then the bi-quadratic equation (12) has two distinct solutions in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Condition 4 : $D|_p < |a|_p^2 = |b|_p < 1$, $\sqrt{D} - \exists$ and $\sqrt{-2a} - \exists$. In this case, the number of solutions of the bi-quadratic equation (12) in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is the same as the number of solutions of the following bi-quadratic equation in $\mathbb{Z}_p^*$,

$$y^4 + a^* y^2 = b^*.$$

We can see that $|D|_p < |a^*|_p = |b^*|_p = 1$, $\sqrt{D} - \exists$ and $\sqrt{-2a} - \exists$. Then, the last equation has four solutions in $\mathbb{Z}_p^*$.Therefore, if $|D|_p < |a|_p^2 = |b|_p < 1$, $\sqrt{D} - \exists$ and $\sqrt{-2a} - \exists$ then the bi-quadratic equation (12) has four solutions in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$. It is worth of mentioning that if $D = 0$ then bi-quadratic equations has two solutions of multiplicity-2 in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Condition 5 : $|D|_p = |a|_p^2 = |b|_p < 1$, $\sqrt{D} - \exists$, $\left(\sqrt{\frac{-a+\sqrt{D}}{2}} \vee \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$. In this case, the number of solutions of the bi-quadratic equation (12) in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ is the same as the number of solutions of the following bi-quadratic equation in $\mathbb{Z}_p^*$,

$$y^2 + a^* y = b^*.$$

We can see clearly that $|D|_p = |a^*|_p = |b^*|_p = 1$ and $\sqrt{D} - \exists$.

Let $\left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \bar{\bar{\wedge}} \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$. In this case, the last equation has four solutions in $\mathbb{Z}_p^*$. Let $\left(\sqrt{\frac{-a+\sqrt{D}}{2}} \ \bar{\wedge} \ \sqrt{\frac{-a-\sqrt{D}}{2}}\right) - \exists$. In this case, the last equation has two solutions in $\mathbb{Z}_p^*$.

Similarly, one can prove in the cases $\mathbb{Q}_p \setminus \mathbb{Z}_p$ and $\mathbb{Q}_p$. This completes the proof. □

Acknowledgments

This work has been supported by ERGS13–025–0058 and IIUM EDW B 13–029–0914. The first Author (M.S.) is also grateful to the Junior Associate scheme of the Abdus Salam International Centre for Theoretical Physics, Trieste, Italy.

References

Borevich, Z. I. and Shafarevich, I. R. (1986). *Number Theory*. Academic Press, London, 2th edition.

Mukhamedov, F. and Akin, H. (2013a). On p-adic potts model on the cayley tree of order three. *Theor. Math. Phys.*, 176(3):1267–1279.

Mukhamedov, F. and Akin, H. (2013b). Phase transitions for p-adic potts model on the cayley tree of order three. *J. Stat. Mech.*, (07).

Mukhamedov, F., Omirov, B., and Saburov, M. (2014). On cubic equations over $p-$adic fields. *International Journal of Number Theory*, 10(5):1171–1190.

Mukhamedov, F., Omirov, B., Saburov, M., and Masutova, K. (2013). Solvability of cubic equations in $p-$adic integers, $p > 3$. *Siberian Mathematical Journal*, 54(3):501–516.

Mukhamedov, F. and Saburov, M. (2013). On equation $x^q = a$ over $\mathbb{Q}_p$. *Journal of Number Theory*, 133(1):55–58.

Rosen, K. H. (2011). *Elementary Number Theory and Its Applications*. Pearson, Boston, 6th edition.

Saburov, M. and Ahmad, M. A. K. (2014). Solvability criteria for cubic equations over $\mathbb{Z}_2^*$. *AIP Conference Proceedings*, 1602:792–797.

Saburov, M. and Ahmad, M. A. K. (2015). Solvability of cubic equations over $\mathbb{Q}_3$. *Sains Malaysiana*, 44(4):635–641.