Filomat 35:4 (2021), 1115–1131
https://doi.org/10.2298/FIL2104115S

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

The Study on General Cubic Equations over p-Adic Fields

Mansoor Saburov[a], Mohd Ali Khameini Ahmad[b], Murat Alp[a]

[a] *College of Engineering and Technology, American University of the Middle East, Egaila, Kuwait*
[b] *Department of Mathematical Sciences, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia,*

Abstract. A Diophantine problem means to find all solutions of an equation or system of equations in integers, rational numbers, or sometimes more general number rings. The most frequently asked question is whether a root of a polynomial equation with coefficients in a p-adic field $\mathbb{Q}_p$ belongs to domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$ or not. This question is open even for lower degree polynomial equations. In this paper, this problem is studied for cubic equations in a general form. The solvability criteria and the number of roots of the general cubic equation over the mentioned domains are provided.

1. Introduction

A Diophantine problem means to find all solutions of a polynomial equation or a system of polynomial equations in integers, rational numbers, or sometimes more general number rings and to give a bound for those solutions (see [12]). Because of the topology and the completeness, a p-adic field $\mathbb{Q}_p$ gives rise to simpler Diophantine problems than a number field (a finite extension of the rational numbers), and one tries to reduce certain classes of Diophantine problems to p-adic ones. For instance, Artin's conjecture [3] asserts that a form of degree d in n variables with coefficients in a p-adic field $\mathbb{Q}_p$ has a non-trivial zero over $\mathbb{Q}_p$ whenever $n > d^2$. For quadratic and cubic forms, this conjecture is true (the quadratic case is known as the Hasse-Minkowski theorem, for the cubic case see [13]). However, in general, this conjecture is known to be false [9]. Nevertheless, it is "semi-globally" true, i.e. the conjecture holds true for all but a finite number of p-adic fields [4, 5]. Therefore, it gives hope that if the number of variables is not too small we should still have a "local-to-global " principle (to get a global theorem from local ones, and to get solutions if the number of variables is large) similar to the Hasse-Minkowski theorem [7, 8]. Here again, before dealing with the global theory, one can study the local one over a p-adic field.

On the other hand, finding roots of a single variable polynomial is among the old problem of mathematics. In the field of real numbers, this problem found its own solution. However, to the best of our knowledge, in the field of p-adic numbers – in the counterpart of the field of real number, less attention has been paid to this problem in the literature. Recently, by concerning some problems of p-adic lattice models of statistical mechanics, this problem is again raised up (for instance, see [25]). Namely, we may

2010 *Mathematics Subject Classification*. Primary 11D88; Secondary 11D25, 11S05
Keywords. Cubic equation, p-adic field, solvability criterion, number of roots
Received: 24 March 2020; Revised: 23 October 2020; Accepted: 02 November 2020
Communicated by Marko Petković
The first and third authors (M.Saburov and M.Alp) were financially supported by American University of the Middle East, Kuwait. The second author (M. A. K. Ahmad) was financially supported by UTMER Vot 19J34, Universiti Teknologi Malaysia.

Email addresses: msaburov@gmail.com, mansur.saburov@aum.edu.kw (Mansoor Saburov), ma.khameini@utm.my (Mohd Ali Khameini Ahmad), murat.alp@aum.edu.kw (Murat Alp)

come across the following problem in one form or another: *provide a solvability criterion for the polynomial equation with coefficients in the p-adic field over some given set* $\mathbb{A} \subset \mathbb{Q}_p$. The most frequently asked question in the p-adic lattice models of statistical mechanics is whether a root of a polynomial equation belongs to domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$ or not. However, this question was open even for lower degree polynomial equations. The scenario is completely different from the field of real numbers to the field of p-adic numbers. For instance, the quadratic equation $x^2 + 1 = 0$ is not solvable in the real field but solvable in the p-adic field for $p \equiv 1 \ (mod\, 4)$. Vise versa, the cubic equation $x^3 + p = 0$ is not solvable in the p-adic field but solvable in the real field. Therefore, it is of independent interest to provide a solvability criterion for lower degree polynomial equations over the p-adic field. The solvability criterion for quadratic equations over the p-adic field was provided in all classical p-adic analysis books. Moreover, a local description of roots of the quadratic equation was also studied in the paper [29]. Recently, in the series of papers [20–22], [26–32, 34, 36], the solvability criteria and the number of roots of *depressed cubic equations* over the p-adic field were studied. This paper is a continuation of the previous studies and we are aiming to study roots of *a general cubic equation* over the p-adic field for $p > 3$. It is worth mentioning that any cubic equation can be deduced to a depressed one by suitable linear transformation and a local description of roots of a depressed cubic equation over domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$ has been already studied in [20, 34]. However, by means of results of the papers [20, 34], we cannot still derive a local description of roots of a general cubic equation over domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$ (examples are given in the next section). We have to care on some special study in the general case. Thus, the main results of this paper cannot be derived from the papers [20, 34] (a detailed explanation is given in the next section). In fact, all results in this paper are extension and unification of the previous results. Meanwhile, applications of quadratic and cubic equations in the p-adic lattice models of statistical mechanics were presented in the papers [1, 2, 23, 25, 29, 30, 33]. We would like to stress that quadratic and cubic equations have naturally arisen in the investigations of p-adic Gibbs measures of Potts models on Cayley trees. First such investigations have been initiated in the papers [16, 18]. The local description of roots of quadratic equations was also explored in [15]. Recently, the location of roots of some complicated p-adic equations has been investigated in the papers [17, 19].

2. Preliminary

The fields $\mathbb{Q}_p$ of p-adic numbers were introduced by German mathematician K. Hensel by motivating 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. Over the last century, p-adic numbers and p-adic analysis have come to play a central role in modern number theory. This importance comes from the fact that they afford a natural and powerful language for talking about congruences between integers, and allow using the methods borrowed from analysis for studying such problems. Recently, numerous applications of p-adic numbers have also shown up in theoretical physics and quantum mechanics (for example, see [10, 11, 14, 35]).

For a fixed prime p, the field $\mathbb{Q}_p$ of p-adic numbers 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

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

where $x = p^r \frac{m}{n}$ with $r, m \in \mathbb{Z}$, $n \in \mathbb{N}$, $(m, p) = (n, p) = 1$. A number r is called *a p-order* of x and it is denoted by $ord_p(x) = r$. Any p-adic number $x \in \mathbb{Q}_p$ can be uniquely represented in the following canonical form

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

where $x_0 \in \{1, 2, \cdots p-1\}$ and $x_i \in \{0, 1, 2, \cdots p-1\}$ for $i \geq 1$. We respectively denote the set of all *p-adic integers* and *units* of $\mathbb{Q}_p$ by $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}$. Any nonzero p-adic number $x \in \mathbb{Q}_p$ has a unique representation $x = \dfrac{x^*}{|x|_p}$, where $x^* \in \mathbb{Z}_p^*$ (see [6]).

Throughout this paper, we always assume that $p > 3$ unless otherwise stated.

Let us consider a general cubic equation

$$x^3 + ax^2 + bx + c = 0, \tag{2}$$

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

In this paper, the concerned problem is to *provide the solvability criterion and the number of roots of the general cubic equation* (2) *over domains* $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$.

There are two ways to handle this problem. One way to do it is that we first deduce the general cubic equation to the depressed one, then we apply the results of the papers [20] and [34]. However, this way does not work for domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$ in general. For example, the following cubic equation $x^3 + x^2 - 1 = 0$ can be deduced to the following depressed cubic equation $w^3 - \frac{1}{3}w = \frac{25}{27}$ by the substitution $w = x + \frac{1}{3}$. Since $\frac{1}{25} = |\frac{25}{27}|_5 < |\frac{1}{3}|_5 = 1$ and there does not exist $\sqrt{\frac{1}{3}}$ in $\mathbb{Q}_5$, the last depressed cubic equation has a unique root $\bar{w}$ which belongs to $\mathbb{Z}_5 \setminus \mathbb{Z}_5^*$ (see [20, 34]). This means that the last depressed cubic equation is not solvable in $\mathbb{Z}_5^*$. However, the given cubic equation $x^3 + x^2 - 1 = 0$ has a root $\bar{x} = \bar{w} - \frac{1}{3}$ in which $|\bar{x}|_5 = 1$ or equivalently $\bar{x} \in \mathbb{Z}_p^*$. This means that the given cubic equation is solvable in $\mathbb{Z}_5^*$. This example shows that there is a cubic equation which is solvable in $\mathbb{Z}_p^*$ but the depressed one is not solvable in $\mathbb{Z}_p^*$. The similar examples can be also provided in domains $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$.

The second method is the Hensel lemma. 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 lifted up any more to the field $\mathbb{Q}_p$ of p-adic numbers. At this point, we are aiming to study the relation between solutions of the cubic equations over $\mathbb{Q}_p$ and $\mathbb{Z}_p$. We shall show that, indeed, any solution of any cubic equation over $\mathbb{Q}_p$ (or over some special sets) can be uniquely determined by a solution of another cubic equation over $\mathbb{Z}_p^*$. Consequently, in some sense, it is enough to study cubic equations over $\mathbb{Z}_p^*$.

It is worth of mentioning that the solvability of the general cubic equation (2) over $\mathbb{Q}_p$ is equivalent to the solvability of the depressed cubic equation over $\mathbb{Q}_p$. Namely, we know that the general cubic equation (2) can be deduced to the following depressed cubic equation

$$w^3 + Aw = B \tag{3}$$

where $w = x + \frac{a}{3}$, $A = \frac{3b-a^2}{3}$ and $B = \frac{-2a^3+9ab-27c}{27}$. By means of results of [20, 34], we can give the solvability criterion of the general cubic equation (2) over $\mathbb{Q}_p$ in terms of $A, B \in \mathbb{Q}_p$.

Recall that a number $a_0 \in \mathbb{Z}$ is called *an r^{th} power residue modulo p* if the following congruent equation $x^r \equiv a_0 \ (mod\ p)$ is solvable in $\mathbb{Z}$. Let $a_0 \in \mathbb{Z}$ with $(a_0, p) = 1$ and $d = (r, p-1)$. The following statements hold true [24]: a number a_0 is the r^{th} power residue modulo p if and only if $a^{\frac{p-1}{d}} \equiv 1 \ (mod\ p)$; If $a_0^{\frac{p-1}{d}} \equiv 1 \ (mod\ p)$, then the congruent equation $x^r \equiv a_0 \ (mod\ p)$ has d number of distinct (non-congruent) solutions in $\mathbb{Z}$.

Let $a \in \mathbb{Q}_p$ be a nonzero p-adic number such that $a = \frac{a^*}{|a|_p}$ and $a^* \in \mathbb{Z}_p^*$ with $a^* = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots$. We say that there exists $\sqrt[r]{a}$ in $\mathbb{Q}_p$, written $\sqrt[r]{a} - \exists$, if the monomial equation $x^r = a$ is solvable in $\mathbb{Q}_p$. The criterion of the existence of $\sqrt[r]{a}$ was presented in [22]. Particularly, there exists $\sqrt{a}$ in $\mathbb{Q}_p$, written $\sqrt{a} - \exists$, if $a_0^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$ and $\log_p |a|_p$ is even. Moreover, there exists $\sqrt[3]{a}$ in $\mathbb{Q}_p$, written $\sqrt[3]{a} - \exists$, if $a_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \ (mod\ p)$ and $\log_p |a|_p$ is divisible by 3.

Now, we describe the solvability domain of the general cubic equation (2) over $\mathbb{Q}_p$ in terms of A, B defined above. If $abc \neq 0$, then we have that $a = \dfrac{a^*}{|a|_p}$, $b = \dfrac{b^*}{|b|_p}$, $c = \dfrac{c^*}{|c|_p}$ with $a^*, b^*, c^* \in \mathbb{Z}_p^*$ where

$$a^* = a_0 + a_1 p + a_2 p^2 + \cdots, \quad b^* = b_0 + b_1 p + b_2 p^2 + \cdots, \quad c^* = c_0 + c_1 p + c_2 p^2 + \cdots$$

and $a_0, b_0, c_0 \in \{1, 2, \cdots p-1\}$, $a_i, b_i, c_i \in \{0, 1, 2, \cdots p-1\}$ for any $i \in \mathbb{N}$.

Let $\Delta = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc = -4A^3 - 27B^2$ be the discriminant of the cubic equation (2). At the same time, it is the discriminant of the depressed cubic equation (3).

If $AB\Delta \neq 0$, then we have that $A = \frac{A^*}{|A|_p}$, $B = \frac{B^*}{|B|_p}$, $\Delta = \frac{\Delta^*}{|\Delta|_p}$ with $A^*, B^*, \Delta^* \in \mathbb{Z}_p^*$ where

$$\Delta^* = D_0 + D_1p + D_2p^2 + \cdots, \quad A^* = A_0 + A_1p + A_2p^2 + \cdots, \quad B^* = B_0 + B_1p + B_2p^2 + \cdots.$$

and $A_0, B_0, D_0 \in \{1, 2, \cdots, p-1\}$, $A_i, B_i, D_i \in \{0, 1, \cdots, p-1\}$, $i \in \mathbb{N}$. We set $D_0 \equiv -4A_0^3 - 27B_0^2 \ (mod\ p)$ and $u_{n+3} = B_0u_n - A_0u_{n+1}$ with $u_1 = 0$, $u_2 = -A_0$, and $u_3 = B_0$ for $n \geq 1$.

We define a set $\Phi = \Phi_1 \cup \Phi_2 \cup \Phi_3$ where

$$\begin{aligned}
\Phi_1 &= \left\{(A, B) \in \mathbb{Q}_p \times \mathbb{Q}_p : |A|_p^3 < |B|_p^2, \sqrt[3]{B} - \exists\right\},\\
\Phi_2 &= \left\{(A, B) \in \mathbb{Q}_p \times \mathbb{Q}_p : |A|_p^3 = |B|_p^2, D_0u_{p-2}^2 \not\equiv 9A_0^2 \ (mod\ p)\right\},\\
\Phi_3 &= \left\{(A, B) \in \mathbb{Q}_p \times \mathbb{Q}_p : |A|_p^3 > |B|_p^2\right\}.
\end{aligned}$$

The set $\Phi \subset \mathbb{Q}_p \times \mathbb{Q}_p$ is the solvability domain of the depressed cubic equation (3) over $\mathbb{Q}_p$ (see [20, 34]). Consequently, the set Φ is also the solvability domain of the general cubic equation (2) over $\mathbb{Q}_p$. The aim of this paper is to describe the solvability domain Φ of the general cubic equation (2) in terms of $a, b, c \in \mathbb{Q}_p$.

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.

The proof of the following proposition is straightforward.

Proposition 2.1. *Let p be any prime, $a, b, c \in \mathbb{Q}_p$, and $\mathbb{A} \subset \mathbb{Z}$ be any subset. The cubic equation* (2) *is solvable in the set $\frac{\mathbb{Z}_p^*}{p^{\mathbb{A}}}$ if and only if there exists a pair $(y^*, k) \in \mathbb{Z}_p^* \times \mathbb{A}$ such that y^* is a solution of the following cubic equation*

$$y^3 + A_ky^2 + B_ky + C_k = 0 \tag{4}$$

where $A_k = ap^k$, $B_k = bp^{2k}$ and $C_k = cp^{3k}$. Moreover, in this case, a solution of the cubic equation (2) *has the form $x = \frac{y^*}{p^k}$.*

This shows that it is enough to study the solvability of the general cubic equation (2) over $\mathbb{Z}_p^*$.

Let $\mathcal{S} = \left\{|a|_p, |b|_p, |c|_p\right\}$ and $\max(\mathcal{S}) = \max\left\{|a|_p, |b|_p, |c|_p\right\}$. We define the set $M(\mathcal{S}) = \{s \in \mathcal{S} : s = \max(\mathcal{S})\}$. Let $|M(\mathcal{S})|$ be the number of elements of the set $M(\mathcal{S})$.

Proposition 2.2. *Let p be any prime. Suppose the cubic equation* (2) *is solvable in $\mathbb{Z}_p^*$ where $a, b, c \in \mathbb{Q}_p$. Then the following statements hold true:*

(*i*) *If* $|M(\mathcal{S})| = 1$, *then* $\max(\mathcal{S}) = 1$;

(*ii*) *If* $|M(\mathcal{S})| \geq 2$, *then* $\max(\mathcal{S}) \geq 1$.

Proof. Let the cubic equation (2) be solvable in $\mathbb{Z}_p^*$. Then one can get that

$$\begin{aligned} |a|_p = |ax^2|_p = |x^3 + bx + c| &\le \max\{1, |b|_p, |c|_p\}, \\ |b|_p = |bx|_p = |x^3 + ax^2 + c| &\le \max\{1, |a|_p, |c|_p\}, \\ |c|_p = |x^3 + ax^2 + bx| &\le \max\{1, |a|_p, |b|_p\}, \\ 1 = |x^3|_p = |ax^2 + bx + c| &\le \max\{|a|_p, |b|_p, |c|_p\}. \end{aligned}$$

If $|M(\mathcal{S})| = 1$, then $|a|_p \neq |b|_p \neq |c|_p$ with $\max\{|a|_p, |b|_p, |c|_p\} = 1$; or $|a|_p = |b|_p < |c|_p = 1$; or $|a|_p = |c|_p < |b|_p = 1$; or $|b|_p = |c|_p < |a|_p = 1$. If $|M(\mathcal{S})| = 2$, then $|a|_p < |b|_p = |c|_p$ with $|b|_p = |c|_p \ge 1$; or $|b|_p < |a|_p = |c|_p$ with $|a|_p = |c|_p \ge 1$; or $|c|_p < |a|_p = |b|_p$ with $|a|_p = |b|_p \ge 1$. If $|M(\mathcal{S})| = 3$, then $|a|_p = |b|_p = |c|_p \ge 1$. This completes the proof. □

This proposition gives necessary conditions for the solvability of the general cubic equation (2) over $\mathbb{Z}_p^*$. To get the solvability criterion over $\mathbb{Z}_p^*$, we need Hensel's lifting lemma.

Lemma 2.3 (Hensel's Lemma, [6]). *Let $f(x)$ be a polynomial whose coefficients are p-adic integers. Let θ be a p-adic integer such that for some $i \ge 0$ we have $f(\theta) \equiv 0 \ (mod\ p^{2i+1})$, $f'(\theta) \equiv 0 \ (mod\ p^i)$, $f'(\theta) \not\equiv 0 \ (mod\ p^{i+1})$. 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

In this section, we present the solvability criterion of the general cubic equation (2) over $\mathbb{A}$ where

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

We introduce some notations. Let $\delta_1 = b^2-4ac$, $\delta_2 = a^2-4b$, $\delta_3 = -2a^3-27c$, $A = \frac{3b-a^2}{3}$, $B = \frac{-2a^3+9ab-27c}{27}$, and $\Delta = a^2b^2-4a^3c-4b^3-27c^2+18abc = -4A^3-27B^2$. We set $D = -4(A|A|_p)^3-27(B|B|_p)^2$, $D_0 \equiv -4A_0^3-27B_0^2 \ (mod\ p)$ and $u_{n+3} = B_0u_n - A_0u_{n+1}$ with $u_1 = 0$, $u_2 = -A_0$, and $u_3 = B_0$ for $n \ge 1$.

Throughout this paper, $(\alpha \vee \beta)$ stands for $(\alpha$ or $\beta)$.

3.1. The solvability criterion over $\mathbb{Z}_p^*$

Theorem 3.1. *Let $p > 3$ be a prime. Then the general cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if one of the following conditions holds*

A.
1. $|a|_p = 1,\ |b|_p < 1,\ |c|_p < 1$;
2. $|b|_p = 1,\ |a|_p < 1,\ |c|_p < 1,\ \sqrt{-b} - \exists$;
3. $|c|_p = 1,\ |a|_p < 1,\ |b|_p < 1,\ \sqrt[3]{-c} - \exists$.

B.
4. $|a|_p < |b|_p = |c|_p,\ |b|_p = |c|_p > 1$;
5. $|b|_p < |a|_p = |c|_p,\ |a|_p = |c|_p > 1,\ \sqrt{-ac} - \exists$;
6. $|c|_p < |a|_p = |b|_p,\ |a|_p = |b|_p > 1$;
7. $|a|_p < |b|_p = |c|_p = 1,\ D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$;
8. $|b|_p < |a|_p = |c|_p = 1,\ \left(|\delta_3|_p < 1\right) \vee \left(|\delta_3|_p = 1,\ D_0u_{p-2}^2 \not\equiv a_0^4 \pmod p\right)$;
9. $|c|_p < |a|_p = |b|_p = 1,\ \left(|\delta_2|_p = 1,\ \sqrt{\delta_2} - \exists\right) \vee (|\delta_2|_p < 1,\ \sqrt{\Delta} - \exists)$.

C.
10. $|a|_p = |b|_p = |c|_p > 1,\ \left(|\delta_1|_p = |a|_p^2 = |b|_p^2 = |c|_p^2,\ \sqrt{\delta_1} - \exists\right) \vee (|\delta_1|_p < |a|_p^2 = |b|_p^2 = |c|_p^2,\ \sqrt{\Delta} - \exists)$;
11. $|a|_p = |b|_p = |c|_p = 1,\ (A, B) \in \Phi$.

Proof. Let $\mathcal{S} = \left\{|a|_p, |b|_p, |c|_p\right\}$.

Let $|M(\mathcal{S})| = 1$. We know that, due to Proposition 2.2, if the cubic equation (2) is solvable in $\mathbb{Z}_p^*$, then $\max(\mathcal{S}) = 1$. It means that we have either $|a|_p \neq |b|_p \neq |c|_p$ with $\max\{|a|_p, |b|_p, |c|_p\} = 1$ or $|a|_p = |b|_p < |c|_p = 1$ or $|a|_p = |c|_p < |b|_p = 1$ or $|b|_p = |c|_p < |a|_p = 1$. We shall study each case separately. Consider the function $f_{a,b,c}(x) = x^3 + ax^2 + bx + c$.

Case A.1: Let $|a|_p = 1$. We want to show that the general cubic equation (2) has a solution in $\mathbb{Z}_p^*$. Let us choose $\bar{x} = -a_0$. We then get that $f_{a,b,c}(\bar{x}) \equiv \bar{x}^3 + a_0\bar{x}^2 \equiv 0\ (mod\ p)$ and $f'_{a,b,c}(\bar{x}) \equiv 3\bar{x}^2 + 2a_0\bar{x} \equiv a_0^2 \not\equiv 0\ (mod\ p)$. According to Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Case A.2: Let $|b|_p = 1$. We want to show that the general cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if $\sqrt{-b} - \exists$.

If part: Let $x \in \mathbb{Z}_p^*$ be a solution of the cubic equation (2). Then we get $x_0^3 + b_0x_0 \equiv x_0(x_0^2 + b_0) \equiv x_0^2 + b_0 \equiv 0\ (mod\ p)$. It means $(-b_0)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ or there exists $\sqrt{-b}$.

Only if part: Let $\sqrt{-b} - \exists$. Let us choose $\bar{x}$ such that $\bar{x}^2 + b_0 \equiv 0\ (mod\ p)$. We then obtain that $f_{a,b,c}(\bar{x}) \equiv \bar{x}(\bar{x}^2 + b_0) \equiv 0\ (mod\ p)$ and $f'_{a,b,c}(\bar{x}) \equiv 3\bar{x}^2 + b_0 \equiv -2b_0 \not\equiv 0\ (mod\ p)$. Due to Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Case A.3: Let $|c|_p = 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if $\sqrt[3]{-c} - \exists$.

If part: Let $x \in \mathbb{Z}_p^*$ be a solution of the cubic equation (2). Then we have $x_0^3 + c_0 \equiv 0\ (mod\ p)$. It means $(-c_0)^{\frac{p-1}{(3,p-1)}} \equiv 0\ (mod\ p)$ or equivalently there exists $\sqrt[3]{-c}$.

Only if part: Let $\sqrt[3]{-c} - \exists$. Let us choose $\bar{x}$ such that $\bar{x}^3 + c_0 \equiv 0\ (mod\ p)$. We then get $f_{a,b,c}(\bar{x}) \equiv \bar{x}^3 + c_0 \equiv 0\ (mod\ p)$ and $f'_{a,b,c}(\bar{x}) \equiv 3\bar{x}^2 \not\equiv 0\ (mod\ p)$. Again, due to Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Let $|M(\mathcal{S})| = 2$. We know due to Proposition 2.2 that if the cubic equation (2) is solvable in $\mathbb{Z}_p^*$, then $\max(\mathcal{S}) \geq 1$. It means that we have either one of the following conditions: $|a|_p < |b|_p = |c|_p$ with $|b|_p = |c|_p \geq 1$; or $|b|_p < |a|_p = |c|_p$ with $|a|_p = |c|_p \geq 1$; or $|c|_p < |a|_p = |b|_p$ with $|a|_p = |b|_p \geq 1$.

Case B.4: Let $|a|_p < |b|_p = |c|_p$, $|b|_p = |c|_p > 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$. Since $|b|_p = |c|_p = p^k$ for some $k \geq 1$, it is clear that the solvability of the following two cubic equations $x^3 + ax^2 + bx + c = 0$ and $p^kx^3 + p^kax + b^*x + c^* = 0$ are equivalent. Moreover, any solution of the first cubic equation is a solution of the second one and vise versa. On the other hand, the second cubic equation is suitable to apply Hensel's lemma. Let us choose $\bar{x}$ such that $b_0\bar{x} + c_0 \equiv 0\ (mod\ p)$. Suppose that $g_{b,c}(x) = p^kx^3 + p^kax + b^*x + c^*$. We have that $g_{b,c}(\bar{x}) \equiv b_0\bar{x} + c_0 \equiv 0\ (mod\ p)$ and $g'_{b,c}(\bar{x}) \equiv b_0 \not\equiv 0\ (mod\ p)$. Due to Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $g_{b,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Case B.5: Let $|b|_p < |a|_p = |c|_p$, $|a|_p = |c|_p > 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{-ac}$. Since $|a|_p = |c|_p = p^k$ for some $k \geq 1$, it is clear that the solvability of the following two cubic equations $x^3 + ax^2 + bx + c = 0$ and $p^kx^3 + a^*x + p^kbx + c^* = 0$ are equivalent and moreover, any solution of the first cubic equation is a solution of the second one and vise versa. On the other hand, the second cubic equation is suitable to apply Hensel's lemma.

If part: Let $x \in \mathbb{Z}_p^*$ be a solution of the cubic equation (2). Then we have that $a_0x_0^2 + c_0 \equiv 0\ (mod\ p)$. It means that $(-a_0c_0)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ or equivalently there exists $\sqrt{-ac}$.

Only if part: We assume that there exists $\sqrt{-ac}$. Let us choose $\bar{x}$ such that $a_0\bar{x}^2 + c_0 \equiv 0\ (mod\ p)$. Suppose that $g_{a,c}(x) = p^kx^3 + a^*x + p^kbx + c^*$. We then obtain that $g_{a,c}(\bar{x}) \equiv a_0\bar{x}^2 + c_0 \equiv 0\ (mod\ p)$ and $g'_{a,c}(\bar{x}) \equiv 2a_0\bar{x} \not\equiv 0\ (mod\ p)$. According to Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $g_{a,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Case B.6: Let $|c|_p < |a|_p = |b|_p$, $|a|_p = |b|_p > 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$. Since $|a|_p = |b|_p = p^k$ for some $k \geq 1$, it is clear that the solvability of the following two cubic equations $x^3 + ax^2 + bx + c = 0$ and $p^kx^3 + a^*x + b^*x + p^kc = 0$ are equivalent and moreover, any solution of the first cubic equation is a solution of the second one and vise versa. On the other hand, the second cubic equation is suitable to apply Hensel's lemma.

Let us choose $\bar{x}$ such that $a_0\bar{x} + b_0 \equiv 0\ (mod\ p)$. Suppose that $g_{a,b}(x) = p^k x^3 + a^* x + b^* x + p^k c$. We then have that $g_{a,b}(\bar{x}) \equiv \bar{x}(a_0\bar{x} + b_0) \equiv 0\ (mod\ p)$ and $g'_{a,b}(\bar{x}) \equiv 2a_0\bar{x} + b_0 \equiv a_0\bar{x} \not\equiv 0\ (mod\ p)$. 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 $x \in \mathbb{Z}_p^*$.

Case B.7: Let $|a|_p < |b|_p = |c|_p = 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if $D_0 u_{p-2}^2 \not\equiv 9b_0^2\ (mod\ p)$.

If part: Let $x \in \mathbb{Z}_p^*$ be a solution of the cubic equation (2). Then we have that $x_0^3 + b_0x_0 + c_0 \equiv 0\ (mod\ p)$. Since the last equation is solvable in $\mathbb{F}_p$ (x_0 is a solution), one should have that $D_0 u_{p-2}^2 \not\equiv 9b_0^2\ (mod\ p)$ (see [20, 34]).

Only if part: We assume that $D_0 u_{p-2}^2 \not\equiv 9b_0^2\ (mod\ p)$. Then there exists $\bar{x}$ such that $\bar{x}^3 + b_0x_0 + c_0 \equiv 0\ (mod\ p)$ and $3\bar{x}^2 + b_0 \not\equiv 0\ (mod\ p)$ which imply $f_{a,b,c}(\bar{x}) \equiv \bar{x}^3 + b_0\bar{x} + c_0 \equiv 0\ (mod\ p)$ and $f'_{a,b,c}(\bar{x}) \equiv 3\bar{x}^2 + b_0 \not\equiv 0\ (mod\ p)$. Based on Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Case B.8: Let $|b|_p < |a|_p = |c|_p = 1$ and $\delta_3 = -2a^3 - 27c$. In this case, by means of the substitution $w = x + \frac{a}{3}$, we may get the following depressed cubic equation $w^3 + Aw = B$ where $A = \frac{3b-a^2}{3}$ and $B = \frac{-2a^3+9ab-27c}{27}$. It is clear that $|A|_p = |3b - a^2|_p = 1$ $|B|_p = |-2a^3 + 9ab - 27c|_p = |9ab + \delta_3| \le \max\{|b|_p, |\delta_3|_p\} \le 1$.

Case 8(i): Let $|\delta_3|_p < 1$. In this case, we want to show that the cubic equation (2) is solvable over $\mathbb{Z}_p^*$. We have $|B|_p < |A|_p = 1$. In this case (see [20, 34]), the depressed cubic equation $w^3 + Aw = B$ is always solvable and one of its solutions w_1 in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$. Since $|x|_p = \left|w_1 - \frac{a}{3}\right| = 1$, the cubic equation (2) is solvable over $\mathbb{Z}_p^*$.

Case 8(ii): Let $|\delta_3|_p = 1$. We want to show that the cubic equation (2) is solvable over $\mathbb{Z}_p^*$ if and only if $D_0 u_{p-2}^2 \not\equiv a_0^4\ (mod\ p)$. In this case, one can see that $|B|_p = |A|_p = 1$. We then have that $D_0 \equiv -4A_0^3 - 27B_0^2\ (mod\ p)$, $3A_0 \equiv -a_0^2\ (mod\ p)$ and $27B_0 \equiv -4a_0^3c_0 - 27c_0^2\ (mod\ p)$. In this case (see [20, 34]), the depressed cubic equation $w^3 + Aw = B$ is solvable if and only if $D_0 u_{p-2}^2 \not\equiv 9A_0^2 \equiv a_0^4\ (mod\ p)$. Moreover, all solutions of the last depressed cubic equation belong to $\mathbb{Z}_p^*$. Now, we want to show that all solutions of the cubic equation (2) such that $x = w - \frac{a}{3}$ also belong to the set $\mathbb{Z}_p^*$. Equivalently, we want to show that $3w \not\equiv a\ (mod\ p)$.

Suppose the contrary, i.e., $3w \equiv a\ (mod\ p)$. One can get that $(3w)^3 + 3(3b - a^2)(3w) - (-2a^3 + 9ab - 27c) \equiv a_0^3 - 3a_0^3 + 2a_0^3 + 27c_0\ (mod\ p) \equiv 27c_0 \not\equiv 0\ (mod\ p)$. However, this is a contradiction. Therefore, we have that $3w \not\equiv a\ (mod\ p)$ or $|x|_p = \left|w - \frac{a}{3}\right|_p = 1$. Consequently, all solutions of the cubic equation (2) belong to $\mathbb{Z}_p^*$.

Case B.9: Let $|c|_p < |a|_p = |b|_p = 1$ and $\delta_2 = a^2 - 4b$. The cubic equation (2) can be written as

$$x(2x + a)^2 - x\delta_2 + 4c = 0. \tag{5}$$

Case 9(i): Assume that $|\delta_2|_p = 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\delta_2}$.

If part: Let $x \in \mathbb{Z}_p^*$ be a solution of the cubic equation (2). Since $|\delta_2|_p = 1$ and $x \in \mathbb{Z}_p^*$, we obtain from (5) that $[(2x + a)]^2 \equiv \delta_2\ (mod\ p)$. Thus, there exists $\sqrt{\delta_2}$.

Only if part: Assume that there exists $\sqrt{\delta_2}$. We choose $\bar{x}$ such that $2\bar{x} + a \equiv \delta_2\ (mod\ p)$. Then $(2\bar{x} + a)^2 - \delta_2 \equiv 0\ (mod\ p)$. Suppose that $f_{a,b,c}(x) = x^3 + ax^2 + bx + c$. We then get $4f_{a,b,c}(\bar{x}) = \bar{x}((2\bar{x} + a)^2 - \delta_2) + 4c \equiv 0\ (mod\ p)$ and $4f'_{a,b,c}(\bar{x}) \equiv 4\bar{x}(2\bar{x} + a) \not\equiv 0\ (mod\ p)$. Based on Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Case 9(ii): Let $|\delta_2|_p < 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\Delta}$.

Let us again consider the depressed cubic equation $w^3 + Aw = B$ where $w = x + \frac{a}{3}$, $A = \frac{3b-a^2}{3}$ and $B = \frac{-2a^3+9ab-27c}{27}$. Then $|A|_p = |-\delta_2 - b|_p = 1$, $|B|_p = |ab - 2a\delta_2 - 27c|_p = 1$.

We also get that $3A_0 \equiv -b_0\ (mod\ p)$, $27B_0 \equiv a_0b_0\ (mod\ p)$ and $27D_0 \equiv 27(-4A_0^3 - 27B_0^2) \equiv -4(3A_0)^3 - (27B_0)^2 \equiv b_0^2(4b_0 - a_0^2) \equiv 0\ (mod\ p)$. Then (see [20, 34]) the depressed cubic equation $w^3 + Aw = B$ is always solvable and all solutions belong to $\mathbb{Z}_p^*$. Moreover, we have that (see [20, 34])

A) If $\Delta = 0$, then $w_1 = -\frac{3B}{A}$, $w_2 = w_3 = \frac{3B}{2A}$ are solutions of the cubic equation $w^3 + Aw = B$.

B) Let $0 < |\Delta|_p < 1$.

  a) If there exists $\sqrt{\Delta}$, then the cubic equation $w^3 + Aw = B$ has three solutions w_1, w_2, w_3 such that $w_1 \equiv -\frac{3B}{A}\ (mod\ p)$ and $w_2 \equiv w_3 \equiv \frac{3B}{2A}\ (mod\ p)$.

  b) If there does not exist $\sqrt{\Delta}$, then the cubic equation $w^3 + Aw = B$ has a unique solutions w_1 such that $w_1 \equiv -\frac{3B}{A}\ (mod\ p)$.

Let us analyze each case.

Suppose that there exists $\sqrt{\Delta}$. We want to show that $\left|w_1 - \frac{a}{3}\right|_p < 1$ and $\left|w_2 - \frac{a}{3}\right|_p = \left|w_3 - \frac{a}{3}\right|_p = 1$.

Since $9Aw_1 \equiv -27B\ (mod\ p), 9A \equiv -3b_0\ (mod\ p)$ and $-27B \equiv -a_0b_0\ (mod\ p)$, we get that $3w_1 \equiv a_0\ (mod\ p)$, i.e., $\left|w_1 - \frac{a}{3}\right|_p < 1$.

Suppose that $3w_2 \equiv 3w_3 \equiv a\ (mod\ p)$. Since $18Aw_2 \equiv 18Aw_3 \equiv 27B\ (mod\ p)$ and $9A \equiv -3b_0\ (mod\ p)$, $27B \equiv a_0b_0\ (mod\ p)$, we get that $-6w_2 \equiv -6w_3 \equiv a_0\ (mod\ p)$. It shows that $9w_2 \equiv 9w_3 \equiv 0\ (mod\ p)$ which contradicts to $w_2, w_3 \in \mathbb{Z}_p^*$. Thus, $3w_2 \equiv 3w_3 \not\equiv a\ (mod\ p)$ and $\left|w_2 - \frac{a}{3}\right|_p = \left|w_3 - \frac{a}{3}\right|_p = 1$.

Suppose that there does not exist $\sqrt{\Delta}$. As we already showed that $\left|w_1 - \frac{a}{3}\right|_p < 1$.

Therefore, if there exists $\sqrt{\Delta}$, then the cubic equation (2) has solutions x_1, x_2, x_3 in which $|x_1|_p = \left|w_1 - \frac{a}{3}\right|_p < 1$, $|x_2|_p = \left|w_2 - \frac{a}{3}\right|_p = 1$, and $|x_3|_p = \left|w_3 - \frac{a}{3}\right|_p = 1$. This means that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$. If there does not exists $\sqrt{\Delta}$, then the cubic equation (2) has a unique solution x_1 in which $|x_1|_p = \left|w_1 - \frac{a}{3}\right|_p < 1$. This means that the cubic equation (2) is not solvable in $\mathbb{Z}_p^*$. Consequently, the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\Delta}$.

Let $|M(\mathcal{S})| = 3$. We know that, due to Proposition 2.2, if the cubic equation (2) is solvable in $\mathbb{Z}_p^*$, then $\max(\mathcal{S}) \geq 1$. It means that $|a|_p = |b|_p = |c|_p \geq 1$.

Case C.10: Let $|a|_p = |b|_p = |c|_p > 1$ with $|a|_p = |b|_p = |c|_p = p^k$ or $a = p^{-k}a^*,\ b = p^{-k}b^*,\ c = p^{-k}c^*$ where $k \geq 1$. Let $\delta_1 = b^2 - 4ac = p^{-2k}\psi$ where $\psi = b^{*2} - 4a^*c^*$. We can rewrite the cubic equation (2) as $p^kx^3 + a^*x^2 + b^*x + c^* = 0$. We get from the last equation that

$$\begin{aligned} 4a^*p^kx^3 + (2a^*x + b^*)^2 - \psi &= 0, & (6)\\ p^k(2a^*x)^3 + 2(a^*)^2\left[(2a^*x + b^*)^2 - \psi\right] &= 0. & (7)\end{aligned}$$

Case 10(i): Assume that $|\delta_1|_p = |a|_p^2 = |b|_p^2 = |c|_p^2$. It means that $|\psi|_p = 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\delta_1}$.

If part: Let $x \in \mathbb{Z}_p^*$ be a solution of the cubic equation (2). We get from (6) that $(2a^*x + b^*)^2 \equiv \psi\ (mod\ p)$. It means that there exists $\sqrt{\psi}$ or equivalently $\sqrt{\delta_1}$.

Only if part: Assume that there exists $\sqrt{\delta_1}$ (or $\sqrt{\psi}$). We choose $\bar{x}$ such that $2a^*\bar{x} + b^* \equiv \psi\ (mod\ p)$ and $(2a^*\bar{x} + b^*)^2 - \psi \equiv 0\ (mod\ p)$. Suppose that $\bar{f}_{a,b,c}(x) = p^kx^3 + a^*x^2 + b^*x + c^*$. We then have that $(2a^*)^3\bar{f}_{a,b,c}(\bar{x}) = p^k(2a^*\bar{x})^3 + 2(a^*)^2\left[(2a^*\bar{x} + b^*)^2 - \psi\right] \equiv 0\ (mod\ p)$ and $(2a^*)^3\bar{f}'_{a,b,c}(\bar{x}) \not\equiv 0\ (mod\ p)$. Due to Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $\bar{f}_{a,b,c}(x) = 0$ and $x \equiv \bar{x}\ (mod\ p)$. Since $\bar{x} \not\equiv 0\ (mod\ p)$, we have that $x \in \mathbb{Z}_p^*$.

Case 10(ii): Assume that $|\delta_1|_p < |a|_p^2 = |b|_p^2 = |c|_p^2$. It means that $|\psi|_p < 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\Delta}$. We can rewrite the cubic equation (2) as $z^3 + \overline{A}z - \overline{B} = 0$ where $z = p^kx + \frac{a^*}{3}$, $\overline{A} = \frac{3p^kb^* - (a^*)^2}{3}$ and $\overline{B} = \frac{-2(a^*)^3 + 9p^ka^*b^* - 27p^{2k}c^*}{27}$. It is clear that $|\overline{A}|_p = |3p^kb^* - (a^*)^2|_p = 1$ and $|\overline{B}|_p = |-2(a^*)^3 + 9p^ka^*b^* - 27p^{2k}c^*|_p = 1$.

Let $\overline{A} = \overline{A}_0 + \overline{A}_1p + \cdots$, $\overline{B} = \overline{B}_0 + \overline{B}_1p + \cdots$ and $\overline{D} = -4\overline{A}^3 - 27\overline{B}^2$ where $\overline{A}_0,\ \overline{B}_0 \in \{1, 2, \cdots, p-1\}$, $\overline{A}_i,\ \overline{B}_i \in \{0, 1, \cdots, p-1\},\ i \geq 1$.

We have that $3\overline{A}_0 \equiv -a_0^2$ $(mod\ p)$, $27\overline{B}_0 \equiv -2a_0^3$ $(mod\ p)$ and $27\overline{D}_0 \equiv -4(3A_0)^3 - (27B_0)^2 \equiv 0$ $(mod\ p)$. Then (see [20, 34]) the depressed cubic equation $z^3 + \overline{A}z - \overline{B} = 0$ is always solvable and all its solutions belong to $\mathbb{Z}_p^*$. Moreover, we have that (see [20, 34])

A) If $\overline{D} = 0$, then $z_1 = -\frac{3\overline{B}}{\overline{A}}$, $z_2 = z_3 = \frac{3\overline{B}}{2\overline{A}}$ are solutions of the cubic equation $z^3 + \overline{A}z - \overline{B} = 0$.

B) Let $0 < |\overline{D}|_p < 1$.

   a) If there exists $\sqrt{\overline{D}}$, then the cubic equation $z^3 + \overline{A}z - \overline{B} = 0$ has three solutions z_1, z_2, z_3 such that $z_1 \equiv -\frac{3\overline{B}}{\overline{A}}$ $(mod\ p)$ and $z_2 \equiv z_3 \equiv \frac{3\overline{B}}{2\overline{A}}$ $(mod\ p)$.

   b) If there does not exists $\sqrt{\overline{D}}$, then the cubic equation $z^3 + \overline{A}z - \overline{B} = 0$ has a unique solutions z_1 such that $z_1 \equiv -\frac{3\overline{B}}{\overline{A}}$ $(mod\ p)$.

Since $\overline{D} = p^{2k}\psi\left[(a^*)^2 - 4p^k b^*)\right] + 2p^{3k}a^*b^*c^* - 27p^{4k}(c^*)^2$ and $|\psi|_p < 1$, we then have that $|\overline{D}|_p \leq p^{-(2k+1)}$. If $|\overline{D}|_p = p^{-L}$, then $L \geq 2k+1$.

Suppose that there exists $\sqrt{\overline{D}}$. Then $z_1 \equiv -\frac{3\overline{B}}{\overline{A}}$ $(mod\ p)$, $2\overline{A}z_2 - 3\overline{B} \equiv p^l t_1^2$ $(mod\ p^{l+1})$ and $2\overline{A}z_3 - 3\overline{B} \equiv p^l t_2^2$ $(mod\ p^{l+1})$ where $l = \frac{L}{2}$. We want to show that $\left|z_1 - \frac{a^*}{3}\right|_p = 1$ and $\left|z_2 - \frac{a^*}{3}\right|_p = \left|z_3 - \frac{a^*}{3}\right|_p = \frac{1}{p^k}$. Indeed, we get that $3z_1 - a^* \equiv 3(a^*)^3 + 12p^k a^*b^* + 27p^{2k}c^* \equiv 3(a^*)^3 \not\equiv 0$ $(mod\ p)$. On the other hand, since L is even and $L \geq 2k+1$, we get that $2l = L \geq 2k+2$ or $l \geq k+1$. We then have that $6\overline{A}z_2 - 2\overline{A}a^* \equiv 3(2\overline{A}z_2 - 3\overline{B}) - (2\overline{A}a^* - 9\overline{B}) \equiv -(2\overline{A}a^* - 9\overline{B}) \equiv -9p^{2k}c^* + p^k a^*b^* \equiv p^k a^*b^* \not\equiv 0$ $(mod\ p^{k+1})$. It means that $\left|z_2 - \frac{a^*}{3}\right|_p = \frac{1}{p^k}$. Similarly, we can obtain that $\left|z_3 - \frac{a^*}{3}\right|_p = \frac{1}{p^k}$.

Hence, we have that $|x_1|_p = \left|\frac{1}{p^k}\left(z_1 - \frac{a^*}{3}\right)\right|_p = p^k > 1$ and $|x_2|_p = |x_3|_p = \left|\frac{1}{p^k}\left(z_2 - \frac{a^*}{3}\right)\right|_p = 1$.

If there does not exist $\sqrt{\overline{D}}$, then $z_1 \equiv -\frac{3\overline{B}}{\overline{A}}$ $(mod\ p)$ and $\left|z_1 - \frac{a}{3}\right|_p = 1$ or equivalently $|x_1|_p = p^k$.

Therefore, the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\overline{D}}$. Since $\overline{D} = p^{6k}\Delta$, there exists $\sqrt{\overline{D}}$ if and only if so does $\sqrt{\Delta}$. Consequently, the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\Delta}$.

Case C.11: Let $|a|_p = |b|_p = |c|_p = 1$. We want to show that the cubic equation (2) is solvable in $\mathbb{Z}_p^*$ if and only if $(A, B) \in \Phi$. Let us consider the depressed cubic equation $w^3 + Aw = B$. It is clear that $|A|_p = |3b - a^2|_p \leq 1$ and $|B|_p = |-2a^3 + 9ab - 27c|_p \leq 1$. Then, the last depressed cubic equation is solvable in $\mathbb{Q}_p$ if and only if $(A, B) \in \Phi$.

We know (see [20, 34]) that if $|A|_p^3 < |B|_p^2 < 1$ or $|A|_p^3 = |B|_p^2 < 1$ or $|B|_p^2 < |A|_p^3 < 1$ with $(A, B) \in \Phi$, then all solutions of the depressed cubic equation $w^3 + Aw = B$ in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$. In this case, since $x = w - \frac{a}{3}$, it implies that all solutions of the cubic equation (2) belong to $\mathbb{Z}_p^*$.

Let $|A|_p < |B|_p = 1$, $(A, B) \in \Phi$. We want to show that $|x|_p = \left|w - \frac{a}{3}\right|_p = 1$ or $3w \not\equiv a$ $(mod\ p)$ for any solution x. Suppose the contrary, i.e., $3w \equiv a$ $(mod\ p)$. One can get that $(3w)^3 + 3(3b - a^2)(3w) - (-2a^3 + 9ab - 27c) \equiv a^3 + 2a^3 - 9ab + 27c \equiv 3a(a^2 - 3b) + 27c \equiv 27c \equiv 0$ $(mod\ p)$. However, it contradicts to $c \not\equiv 0$ $(mod\ p)$. Therefore, all solutions of the cubic equation (2) belong to $\mathbb{Z}_p^*$.

Let $|B|_p < |A|_p = 1$, $(A, B) \in \Phi$. We want to show that $|x|_p = \left|w - \frac{a}{3}\right|_p = 1$ or $3w \not\equiv a$ $(mod\ p)$ for any solution x. Suppose the contrary, i.e., $3w \equiv a$ $(mod\ p)$. Similarly, one can check that $(3w)^3 + 3(3b - a^2)(3w) - (-2a^3 + 9ab - 27c) \equiv -2a^3 + 9ab \equiv -2a^3 + 9ab - 27c + 27c \equiv 27c \equiv 0$ $(mod\ p)$. However, it contradicts to $c \not\equiv 0$ $(mod\ p)$. It means that all solutions of the cubic equation (2) belong to $\mathbb{Z}_p^*$.

Let $|A|_p = |B|_p = 1$, $(A, B) \in \Phi$. In this case, the similar calculation also shows that $|x|_p = \left|w - \frac{a}{3}\right|_p = 1$. It means that all solutions of the cubic equation (2) belong to $\mathbb{Z}_p^*$. Therefore the cubic equation (2) is solvable over $\mathbb{Z}_p^*$ if and only if $(A, B) \in \Phi$. This completes the proof. □

3.2. *The solvability criterion over $\mathbb{Q}_p$*

We are aiming to describe the solvability domain Φ of the general cubic equation (2) in terms of $a, b, c \in \mathbb{Q}_p$ except one case $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$ in which we have to stick on $A, B \in \mathbb{Q}_p$.

Theorem 3.2. *Let $p > 3$ be a prime. Then the general cubic equation* (2) *is solvable over $\mathbb{Q}_p$ if and only if one of the following conditions holds*

A. *1.* $\sqrt{|b|_p} < |a|_p, \quad \sqrt[3]{|c|_p} < |a|_p;$

2. $|a|_p < \sqrt{|b|_p}, \quad \sqrt[3]{|c|_p} < \sqrt{|b|_p};$

3. $|a|_p < \sqrt[3]{|c|_p}, \quad \sqrt{|b|_p} < \sqrt[3]{|c|_p}, \quad \sqrt[3]{-c} - \exists.$

B. *4.* $|a|_p < \sqrt{|b|_p} = \sqrt[3]{|c|_p}, \quad D_0 u_{p-2}^2 \not\equiv 9b_0^2 \pmod p);$

5. $\sqrt{|b|_p} < |a|_p = \sqrt[3]{|c|_p}, \quad \left(|\delta_3|_p < |a|_p^3 = |c|_p\right) \vee \left(|\delta_3|_p = |a|_p^3 = |c|_p,\ D_0 u_{p-2}^2 \not\equiv a_0^4 \pmod p)\right);$

6. $\sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p}.$

C. *7.* $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}, \quad (A, B) \in \Phi.$

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 cubic equation (2) in $\mathbb{Q}_p$ if and only if $y = p^k x$ is a solution of the cubic equation (4).

Let $\Delta_1 = B_k^2 - 4A_kC_k$, $\Delta_2 = A_k^2 - 4B_k$, $\Delta_3 = -2A_k^3 - 27C_k$, $\tilde{A} = \frac{3B_k - A_k^2}{3}$, $\tilde{B} = \frac{-2A_k^3 + 9A_kB_k - 27C_k}{27}$, and $\Delta_k = A_k^2B_k^2 - 4A_k^3C_k - 4B_k^3 - 27C_k^2 + 18A_kB_kC_k = -4\tilde{A}^3 - 27\tilde{B}^2$. It is clear that $A_k^* = a^*$, $B_k^* = b^*$ and $C_k^* = c^*$ where $|A_k|_p = p^{-k}|a|_p$, $|B_k|_p = p^{-2k}|b|_p$ and $|C_k|_p = p^{-3k}|c|_p$. We set $\tilde{D}_0 \equiv -4\tilde{A}_0^3 - 27\tilde{B}_0^2$ $(mod\ p)$ and $\tilde{u}_{n+3} = \tilde{B}_0\tilde{u}_n - \tilde{A}_0\tilde{u}_{n+1}$ with $\tilde{u}_1 = 0$, $\tilde{u}_2 = -\tilde{A}_0$, and $\tilde{u}_3 = \tilde{B}_0$ for $n \geq 1$. We know that, due to Theorem 3.1, the cubic equation (4) is solvable over $\mathbb{Z}_p^*$ if and only if either one of the following conditions holds true

1. I. $|A_k|_p = 1,\ |B_k|_p < 1,\ |C_k|_p < 1;$

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

III. $|C_k|_p = 1,\ |A_k|_p < 1,\ |B_k|_p < 1$ and $\sqrt[3]{-C_k} - \exists.$

2. I. $|A_k|_p < |B_k|_p = |C_k|_p,\ |B_k|_p = |C_k|_p > 1,$

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

III. $|C_k|_p < |A_k|_p = |B_k|_p,\ |A_k|_p = |B_k|_p > 1,$

IV. $|A_k|_p < |B_k|_p = |C_k|_p = 1,\ \tilde{D}_0\tilde{u}_{p-2}^2 \not\equiv 9b_0^2\ (mod\ p),$

V. $|B_k|_p < |A_k|_p = |C_k|_p = 1,$ and

(i) $|\Delta_3|_p < 1,$ or

(ii) $|\Delta_3|_p = 1,\ \tilde{D}_0\tilde{u}_{p-2}^2 \not\equiv a_0^4\ (mod\ p)$

VI. $|C_k|_p < |A_k|_p = |B_k|_p = 1,$ and

(i) $|\Delta_2|_p = 1,\ \sqrt{\Delta_2} - \exists,$ or

(ii) $|\Delta_2|_p < 1,\ \sqrt{\Delta_k} - \exists$

3. I. $|A_k|_p = |B_k|_p = |C_k|_p > 1$ and

(i) $|\Delta_1|_p = |A_k|_p^2 = |B_k|_p^2 = |C_k|_p^2,\ \sqrt{\Delta_1} - \exists$ or

(ii) $|\Delta_1|_p < |A_k|_p^2 = |B_k|_p^2 = |C_k|_p^2,\ \sqrt{\Delta_k} - \exists$

II. $|A_k|_p = |B_k|_p = |C_k|_p = 1,\ (A, B) \in \Phi.$

We want to describe all p-adic numbers $a, b, c \in \mathbb{Q}_p$ for which at least one of the conditions given above is satisfied for some $k \in \mathbb{Z}$.

Firstly, we look at the condition 2.I: $|A_k|_p < |B_k|_p = |C_k|_p,\ |B_k|_p = |C_k|_p > 1$. Since $|B_k|_p = |C_k|_p$, we obtain that $k = \log_p \frac{|c|_p}{|b|_p}$. It follows from $|B_k|_p > 1$ and $|C_k|_p > 1$ that $|c|_p^2 < |b|_p^3$. Moreover, from $|A_k|_p < |B_k|_p$ and $|A_k|_p < |C_k|_p$ we get that $|a|_p|c|_p < |b|_p^2$. Therefore, if $\sqrt[3]{|c|_p} < \sqrt{|b|_p}$ and $|a|_p|c|_p < |b|_p^2$, then the condition 2.I is satisfied with $k = \log_p \frac{|c|_p}{|b|_p} \in \mathbb{Z}$. It is clear that $\mathbf{G} = \mathbf{G}_1 \cup \mathbf{G}_2 \cup \mathbf{G}_3$ where

$$\begin{aligned}
\mathbf{G} &= \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt[3]{|c|_p} < \sqrt{|b|_p},\ |a|_p|c|_p < |b|_p^2\right\},\\
\mathbf{G}_1 &= \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt[3]{|c|_p} < \sqrt{|b|_p},\ |a|_p|c|_p < |b|_p^2,\ \sqrt{|b|_p} < |a|_p\right\},\\
\mathbf{G}_2 &= \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt[3]{|c|_p} < \sqrt{|b|_p},\ |a|_p|c|_p < |b|_p^2,\ \sqrt{|b|_p} = |a|_p\right\}\\
&= \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt[3]{|c|_p} < \sqrt{|b|_p} = |a|_p\right\},\\
\mathbf{G}_3 &= \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt[3]{|c|_p} < \sqrt{|b|_p},\ |a|_p|c|_p < |b|_p^2,\ \sqrt{|b|_p} > |a|_p\right\}\\
&= \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt[3]{|c|_p} < \sqrt{|b|_p},\ |a|_p < \sqrt{|b|_p}\right\}.
\end{aligned}$$

Case A.1

Condition 1.I: $|A_k|_p = 1,\ |B_k|_p < 1,\ |C_k|_p < 1$. From $|A_k|_p = 1$, we obtain that $k = \log_p |a|_p$. It follows from $|B_k|_p < 1$ and $|C_k|_p < 1$ that $|b|_p < |a|_p^2$ and $|c|_p < |a|_p^3$ respectively. Therefore, if $\sqrt{|b|_p} < |a|_p$ and $\sqrt[3]{|c|_p} < |a|_p$, then the condition 1.I is satisfied with $k = \log_p |a|_p \in \mathbb{Z}$. Let

$$\mathbf{H} = \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p\right\}.$$

Condition 2.II: $|B_k|_p < |A_k|_p = |C_k|_p,\ |A_k|_p = |C_k|_p > 1$ and $\sqrt{-A_kC_k} - \exists$. From $|A_k|_p = |C_k|_p$, we obtain that $2k = \log_p \frac{|c|_p}{|a|_p}$. It follows from $|A_k|_p > 1$ and $|C_k|_p > 1$ that $|c|_p < |a|_p^3$. Moreover, from $|B_k|_p < |A_k|_p$ and $|B_k|_p < |C_k|_p$ we get that $|b|_p^2 < |a|_p|c|_p$. It is clear that the existence of $\sqrt{-A_kC_k}$ is equivalent to the existence of $\sqrt{-ac}$. Therefore, if $\sqrt[3]{|c|_p} < |a|_p,\ |a|_p|c|_p > |b|_p^2$ and $\sqrt{-ac} - \exists$, then the condition 2.II is satisfied with $k = \frac{1}{2}\log_p \frac{|c|_p}{|a|_p} \in \mathbb{Z}$. Let

$$\mathbf{H}_1 = \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt[3]{|c|_p} < |a|_p,\ |a|_p|c|_p > |b|_p^2,\ \sqrt{-ac} - \exists\right\}.$$

Condition 2.III: $|C_k|_p < |A_k|_p = |B_k|_p,\ |A_k|_p = |B_k|_p > 1$. From $|A_k|_p = |B_k|_p$, we obtain that $k = \log_p \frac{|b|_p}{|a|_p}$. It follows from $|A_k|_p > 1$ and $|B_k|_p > 1$ that $|b|_p < |a|_p^2$. Moreover, from $|C_k|_p < |A_k|_p$ and $|C_k|_p < |B_k|_p$ we get that $|a|_p|c|_p < |b|_p^2$. Therefore, if $\sqrt{|b|_p} < |a|_p$ and $|a|_p|c|_p < |b|_p^2$, then the condition 2.III is satisfied with $k = \log_p \frac{|b|_p}{|a|_p} \in \mathbb{Z}$. Let

$$\mathbf{H}_2 = \left\{(a,b,c) \in \mathbb{Q}_p^3 : \sqrt{|b|_p} < |a|_p,\ |a|_p|c|_p < |b|_p^2\right\}.$$

Condition 3.I: $|A_k|_p = |B_k|_p = |C_k|_p > 1$ and (i) $|\Delta_1|_p < |A_k|_p^2 = |B_k|_p^2 = |C_k|_p^2,\ \sqrt{\Delta_k} - \exists$ or (ii) $|\Delta_1|_p = |A_k|_p^2 = |B_k|_p^2 = |C_k|_p^2,\ \sqrt{\Delta_1} - \exists$. From $|A_k|_p = |B_k|_k$, $|A_k|_p = |C_k|_p$ and $|B_k|_p = |C_k|_p$, we obtain that $k = \log_p \frac{|b|_p}{|a|_p}$, $2k = \log_p \frac{|c|_p}{|a|_p}$ and $k = \log_p \frac{|c|_p}{|b|_p}$ respectively. It means that $|b|_p^2 = |a|_p|c|_p$. Moreover, from $|A_k|_p > 1$, $|B_k|_p > 1$ and $|C_k|_p > 1$, we have that $|b|_p < |a|_p^2$, $|c|_p < |a|_p^3$ and $|c|_p^2 < |b|_p^3$. In addition, from $|\Delta_1|_p \le 1$, we obtain that $|\delta_1|_p \le |b|_p^2 = |a|_p|c|_p$. We can check that the existence of $\sqrt{\Delta_k}$ and $\sqrt{\Delta_1}$ are equivalent to the existence of $\sqrt{\Delta}$

and $\sqrt{\delta_1}$ respectively. Therefore, if $|b|_p^2 = |a|_p|c|_p,\ \sqrt[3]{|c|_p} < \sqrt{|b|_p} < |a|_p$ and (i) $|\delta_1|_p < |b|_p^2 = |a|_p|c|_p,\ \sqrt{\Delta} - \exists$ or (ii) $|\delta_1|_p = |b|_p^2 = |a|_p|c|_p,\ \sqrt{\delta_1} - \exists$, then the condition 3.I is satisfied with $k = \log_p \frac{|b|_p}{|a|_p} = \frac{1}{2}\log_p \frac{|c|_p}{|a|_p} = \log_p \frac{|c|_p}{|b|_p} \in \mathbb{Z}$. Let

$$\mathbf{H}_3 = \left\{(a,b,c) \in \mathbb{Q}_p^3 : |b|_p^2 = |a|_p|c|_p,\ \sqrt[3]{|c|_p} < \sqrt{|b|_p} < |a|_p,\ |\delta_1|_p < |b|_p^2,\ \sqrt{\Delta} - \exists\right\},$$

$$\mathbf{H}_4 = \left\{(a,b,c) \in \mathbb{Q}_p^3 : |b|_p^2 = |a|_p|c|_p,\ \sqrt[3]{|c|_p} < \sqrt{|b|_p} < |a|_p,\ |\delta_1|_p = |b|_p^2,\ \sqrt{\delta_1} - \exists\right\}.$$

We want to show that $\mathbf{H}_1 \subset \mathbf{H}$. Since $|c|_p < |a|_p^3$, we can get that $|b|_p^2 < |a|_p|c|_p < |a|_p^4$. It means that $\sqrt{|b|_p} < |a|_p$. Therefore, we have that $\mathbf{H}_1 \subset \mathbf{H}$. Next, we want to show that $\mathbf{H}_2 = \mathbf{G}_1 \subset \mathbf{H}$. It is clear that $\mathbf{G}_1 \subset \mathbf{H}_2$ and $\mathbf{G}_1 \subset \mathbf{H}$. From $\sqrt{|b|_p} < |a|_p$ and $|a|_p|c|_p < |b|_p^2$ we get that $|a|_p|c|_p < |b|_p^2 < |a|_p^4$ or $\sqrt[3]{|c|_p} < |a|_p$ and we have that $|c|_p^2 < |a|_p^3|c|_p < |a|_p^2|b|_p^2$ or $|c|_p < |a|_p|b|_p$. Moreover, we obtain that $|c|_p^2 < |a|_p|b|_p|c|_p < |b|_p^3$ or $\sqrt[3]{|c|_p} < \sqrt{|b|_p}$. Hence, $\mathbf{G}_1 = \mathbf{H}_2$. Lastly, it is clear that $\mathbf{H}_3 \subset \mathbf{H}$ and $\mathbf{H}_4 \subset \mathbf{H}$. Consequently, the set $\mathbf{H}$ contains the sets $\mathbf{H}_1, \mathbf{H}_2 = \mathbf{G}, \mathbf{H}_3, \mathbf{H}_4$ and it is nothing but the condition A.1.

Case A.2:

Condition 1.II: $|B_k|_p = 1,\ |A_k|_p < 1,\ |C_k|_p < 1$ and $\sqrt{-B_k} - \exists$. From $|B_k|_p = 1$, we obtain that $2k = \log_p |b|_p$. It follows from $|A_k|_p < 1$ and $|C_k|_p < 1$ that $|a|_p^2 < |b|_p$ and $|c|_p^2 < |b|_p^3$ respectively. It is clear that the existence of $\sqrt{-B_k}$ is equivalent to the existence of $\sqrt{-b}$. Therefore, if $|a|_p < \sqrt{|b|_p},\ \sqrt[3]{|c|_p} < \sqrt{|b|_p}$ and $\sqrt{-b} - \exists$, then the condition 1.II is satisfied with $k = \frac{1}{2}\log_p |b|_p \in \mathbb{Z}$. Let

$$\mathbf{I}_1 = \left\{(a,b,c) : |a|_p < \sqrt{|b|_p},\ \sqrt[3]{|c|_p} < \sqrt{|b|_p},\ \sqrt{-b} - \exists\right\}.$$

It is clear that $\mathbf{I}_1 \subset \mathbf{G}_3$. Moreover, the set $\mathbf{G}_3$ is nothing but the condition A.2.

Case A.3:

Condition 1.III: $|C_k|_p = 1,\ |A_k|_p < 1,\ |B_k|_p < 1$ and $\sqrt[3]{-C_k} - \exists$. From $|C_k|_p = 1$, we obtain that $3k = \log_p |b|_p$. It follows from $|A_k|_p < 1$ and $|B_k|_p < 1$ that $|a|_p^3 < |c|_p$ and $|b|_p^3 < |c|_p^2$ respectively. It is clear that the existence of $\sqrt[3]{-C_k}$ is equivalent to the existence of $\sqrt[3]{-c}$. Therefore, if $|a|_p < \sqrt[3]{|c|_p},\ \sqrt{|b|_p} < \sqrt[3]{|c|_p}$ and $\sqrt[3]{-c}$, then the condition 1.III is satisfied with $k = \frac{1}{3}\log_p |c|_p \in \mathbb{Z}$.

Case B.4:

Condition 2.IV: $|A_k|_p < |B_k|_p = |C_k|_p = 1,\ \tilde{D}_0\tilde{u}_{p-2}^2 \not\equiv 9\tilde{A}_0^2 \pmod p$. From $|B_k|_p = 1$ and $|C_k|_p = 1$, we obtain that $2k = \log_p |b|_p$ and $3k = \log_p |c|_p$. It means that $|b|_p^3 = |c|_p^2$. Moreover, it follows from $|A_k|_p < 1,\ |A_k|_p < |B_k|_p$ and $|A_k|_p < |C_k|_p$ that $|a|_p^2 < |b|_p$ and $|a|_p^3 < |c|_p$. We can check that $\tilde{D}_0\tilde{u}_{p-2}^2 \not\equiv 9\tilde{A}_0^2 \pmod p$ is equivalent to $D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$. Therefore, if $|a|_p < \sqrt{|b|_p} = \sqrt[3]{|c|_p}$ and $D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$, then the condition 2.IV is satisfied with $k = \frac{1}{2}\log_p |b|_p = \frac{1}{3}\log_p |c|_p \in \mathbb{Z}$.

Case B.5:

Condition 2.V: $|B_k|_p < |A_k|_p = |C_k|_p = 1$ and (i) $|\Delta_3|_p < 1$ or (ii) $|\Delta_3|_p = 1,\ \tilde{D}_0\tilde{u}_{p-2}^2 \not\equiv 9\tilde{A}_0^2 \pmod p$. From $|A_k|_p = 1$ and $|C_k|_p = 1$, we obtain that $k = \log_p |a|_p$ and $3k = \log_p |c|_p$. It means that $|a|_p^3 = |c|_p$. Moreover, from $|B_k|_p < 1,\ |B_k|_p < |A_k|_p$ and $|B_k|_p < |C_k|_p$ we get that $|b|_p < |a|_p^2$ and $|b|_p^3 < |c|_p^2$. Furthermore, from $|\Delta_3|_p \le 1$ we obtain that $|\delta_3|_p \le |a|_p^3 = |c|_p$. We can check that $\tilde{D}_0\tilde{u}_{p-2}^2 \not\equiv 9\tilde{A}_0^2 \pmod p$ is equivalent to $D_0u_{p-2}^2 \not\equiv a_0^4 \pmod p$. Therefore, if $\sqrt{|b|_p} < |a|_p = \sqrt[3]{|c|_p}$ and (i) $|\delta_3|_p < |a|_p^3 = |c|_p$ or (ii) $|\delta_3|_p = |a|_p^3 = |c|_p,\ D_0u_{p-2}^2 \not\equiv a_0^4 \pmod p$, then the condition 2.V is satisfied with $k = \log_p |a|_p = \frac{1}{3}\log_p |c|_p \in \mathbb{Z}$.

Case B.6:

Condition 2.VI: $|C_k|_p < |A_k|_p = |B_k|_p = 1$ and (i) $|\Delta_2|_p < 1,\ \sqrt{\Delta_k} - \exists$ or (ii) $|\Delta_2|_p = 1,\ \sqrt{\Delta_2} - \exists$. From $|A_k|_p = 1$ and $|B_k|_p = 1$, we obtain that $k = \log_p |a|_p$ and $2k = \log_p |b|_p$. It means that $|a|_p^2 = |b|_p$. Moreover, from $|C_k|_p < 1,\ |C_k|_p < |A_k|_p$ and $|C_k|_p < |B_k|_p$ we have that $|c|_p < |a|_p^3$ and $|c|_p^2 < |b|_p^3$. Meanwhile, from $|\Delta_2|_p \le 1$ we obtain that $|\delta_3|_p \le |a|_p^2 = |b|_p$. We can check that the existence of $\sqrt{\Delta_k}$ and $\sqrt{\Delta_2}$ are equivalent to the existence of $\sqrt{\Delta}$ and $\sqrt{\delta_2}$ respectively. Therefore, if $\sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p}$ and (i) $|\delta_2|_p < |a|_p^2 = |b|_p,\ \sqrt{\Delta}-\exists$ or (ii) $|\delta_2|_p = |a|_p^2 = |b|_p,\ \sqrt{\delta_2}-\exists$, then the condition 2.VI is satisfied with $k = \log_p |a|_p = \frac{1}{2}\log_p |b|_p \in \mathbb{Z}$. Let

$$\mathbf{I}_2 = \left\{(a,b,c) : \sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p},\ |\delta_2|_p < |a|_p^2 = |b|_p,\ \sqrt{\Delta}-\exists\right\},$$

$$\mathbf{I}_3 = \left\{(a,b,c) : \sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p},\ |\delta_2|_p = |a|_p^2 = |b|_p,\ \sqrt{\delta_2}-\exists\right\}.$$

It is clear that $\mathbf{I}_2 \subset \mathbf{G}_2$ and $\mathbf{I}_3 \subset \mathbf{G}_2$. Consequently, the set $\mathbf{G}_2$ contains the sets $\mathbf{I}_1, \mathbf{I}_2$ and it is nothing but the condition B.6.

Case C.7:

Condition 3.II: $|A_k|_p = |B_k|_p = |C_k|_p = 1$ and $(\tilde{A},\tilde{B}) \in \Phi$. From $|A_k|_p = 1,\ |B_k|_p = 1$ and $|C_k|_p = 1$, we obtain that $k = \log_p |a|_p,\ 2k = \log_p |b|_p$ and $3k = \log_p |c|_p$ respectively. It means that $|b|_p = |a|_p^2,\ |c|_p = |a|_p^3$ and $|c|_p^2 = |b|_p^3$. We can check that $(\tilde{A},\tilde{B}) \in \Phi$ is equivalent to $(A,B) \in \Phi$. Therefore, if $\sqrt[3]{|c|_p} = \sqrt{|b|_p} = |a|_p$ and $(A,B) \in \Phi$, then the condition 3.II is satisfied with $k = \log_p |a|_p = \frac{1}{2}\log_p |b|_p = \frac{1}{3}\log_p |c|_p \in \mathbb{Z}$.

We have considered all the conditions which completes the proofs. □

3.3. Descriptions of p-adic absolute values of roots

The following theorem describes the p-adic absolute values of roots of the general cubic equation (2) without knowing their exact values. Its proof follows from Theorem 3.2.

Theorem 3.3 (Descriptions of roots of the general cubic equation). *Let $p > 3$ be a prime.*

1. *Let $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p$. Then the cubic equation (2) always has a root x_1 in which $|x_1|_p = |a|_p$. Moreover,*

   (i) If $|a|_p|c|_p < |b|_p^2$, then it has two more roots x_2 and x_3 in which $|x_2|_p = \frac{|b|_p}{|a|_p}$ and $|x_3|_p = \frac{|c|_p}{|b|_p}$. In this case, we have $|x_3|_p < |x_2|_p < |x_1|_p$;

   (ii) If $\left(|a|_p|c|_p = |b|_p^2 > |\delta_1|_p,\ \sqrt{\Delta}-\exists\right) \vee \left(|a|_p|c|_p = |b|_p^2 = |\delta_1|_p,\ \sqrt{\delta_1}-\exists\right)$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \frac{|b|_p}{|a|_p} = \frac{|c|_p}{|b|_p} = \sqrt{\frac{|c|_p}{|a|_p}}$. In this case, we have $|x_3|_p = |x_2|_p < |x_1|_p$;

   (iii) If $|a|_p|c|_p > |b|_p^2,\ \sqrt{-ac}-\exists$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \sqrt{\frac{|c|_p}{|a|_p}}$. In this case, we have $|x_3|_p = |x_2|_p < |x_1|_p$.

2. *Let $|a|_p < \sqrt{|b|_p},\ \sqrt[3]{|c|_p} < \sqrt{|b|_p}$. Then the cubic equation (2) always has a root x_1 in which $|x_1|_p = \frac{|c|_p}{|b|_p}$. Moreover, if $\sqrt{-b}-\exists$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \sqrt{|b|_p}$. In this case, we have $|x_1|_p < |x_2|_p = |x_3|_p$.*

3. *Let $|a|_p < \sqrt[3]{|c|_p},\ \sqrt{|b|_p} < \sqrt[3]{|c|_p},\ \sqrt[3]{-c}-\exists$. Then the cubic equation (2) always has a root x_1 in which $|x_1|_p = \sqrt[3]{|c|_p}$. Moreover, if $p \equiv 1 \pmod 3$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \sqrt[3]{|c|_p}$. In this case, we have $|x_1|_p = |x_2|_p = |x_3|_p$.*

4. *Let $|a|_p < \sqrt{|b|_p} = \sqrt[3]{|c|_p},\ D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$. Then the cubic equation (2) always has a root x_1 in which $|x_1|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$. Moreover, if $\left(|D|_p = 1,\ u_{p-2} \equiv 0 \pmod p\right) \vee \left(0 \le |D|_p < 1,\ \sqrt{D}-\exists\right)$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$. In this case, we have $|x_1|_p = |x_2|_p = |x_3|_p$.*

5. *Let $\sqrt{|b|_p} < |a|_p = \sqrt[3]{|c|_p}, \left(|\delta_3|_p < |a|_p^3 = |c|_p\right) \vee \left(|\delta_3|_p = |a|_p^3 = |c|_p, D_0u_{p-2}^2 \not\equiv a_0^4 (mod\ p)\right)$. Then the cubic equation (2) always has a root x_1 in which $|x_1|_p = |a|_p = \sqrt[3]{|c|_p}$. If $|\delta_3|_p < |a|_p^3 = |c|_p$ with $p \equiv \pm 1 \pmod{12}$ or $|\delta_3|_p = |a|_p^3 = |c|_p$ with $\left(|D|_p = 1,\ u_{p-2} \equiv 0 \pmod p\right) \vee \left(0 \le |D|_p < 1,\ \sqrt{D}-\exists\right)$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = |a|_p = \sqrt[3]{|c|_p}$. In this case, we have $|x_1|_p = |x_2|_p = |x_3|_p$.*

6. *Let* $\sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p}$. *Then the cubic equation* (2) *always has a root* x_1 *in which* $|x_1|_p = \frac{|c|_p}{|b|_p}$. *Moreover, if* $\left(|\delta_1|_p < |b|_p = |a|_p^2,\ \sqrt{\Delta} - \exists\right) \vee \left(|\delta_1|_p = |b|_p = |a|_p^2,\ \sqrt{\delta_1} - \exists\right)$, *then it has two more roots* x_2 *and* x_3 *in which* $|x_2|_p = |x_3|_p = |a|_p = \sqrt{|b|_p}$. *In this case, we have* $|x_1|_p < |x_2|_p = |x_3|_p$.

7. *Let* $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$ *and* $(A, B) \in \Phi$. *Then the cubic equation* (2) *always has a root* x_1 *in which* $|x_1|_p = |a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$. *Moreover, if one has that*

   (*i*) $\left(|B|_p^2 < |A|_p^3,\ \sqrt{-A} - \exists\right)$ *or*

   (*ii*) $\left(|A|_p^3 = |B|_p^2,\ \left(|D|_p = 1,\ u_{p-2} \equiv 0 \pmod p\right) \vee \left(0 \le |D|_p < 1,\ \sqrt{D} - \exists\right)\right)$ *or*

   (*iii*) $\left(|A|_p^3 < |B|_p^2,\ \sqrt[3]{B} - \exists, p \equiv 1 \pmod 3\right)$,

   then it has two more roots x_2 *and* x_3 *in which* $|x_2|_p = |x_3|_p = |a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$. *In this case, we have* $|x_1|_p = |x_2|_p = |x_3|_p$.

Theorem 3.3 takes the following form for the depressed cubic equation

$$x^3 + ax = b. \tag{8}$$

We set $\overline{D} = -4(a|a|_p)^3 - 27(b|b|_p)^2$, $\overline{D}_0 \equiv -4a_0^3 - 27b_0^2 \ (mod\ p)$ and $\overline{u}_{n+3} = b_0\overline{u}_n - a_0\overline{u}_{n+1}$ with $\overline{u}_1 = 0$, $\overline{u}_2 = -a_0$, and $\overline{u}_3 = b_0$ for $n \ge 1$.

Theorem 3.4 (Descriptions of roots of the depressed cubic equation). *Let* $p > 3$ *be a prime.*

1. *Let* $|b|_p^2 < |a|_p^3$. *Then the cubic equation* (8) *always has a root* x_1 *in which* $|x_1|_p = \frac{|b|_p}{|a|_p}$. *Moreover, if* $\sqrt{-a} - \exists$, *then it has two more roots* x_2 *and* x_3 *in which* $|x_2|_p = |x_3|_p = \sqrt{|a|_p}$. *In this case, we have* $|x_1|_p < |x_2|_p = |x_3|_p$.

2. *Let* $|a|_p^3 = |b|_p^2$ *and* $\overline{D}_0\overline{u}_{p-2}^2 \not\equiv 9a_0^2 \pmod p$. *Then the cubic equation* (8) *always has a root* x_1 *in which* $|x_1|_p = \sqrt{|a|_p} = \sqrt[3]{|b|_p}$. *Moreover, if* $\left(|\overline{D}|_p = 1,\ \overline{u}_{p-2} \equiv 0 \pmod p\right) \vee \left(0 \le |\overline{D}|_p < 1,\ \sqrt{\overline{D}} - \exists\right)$, *then it has two more roots* x_2 *and* x_3 *in which* $|x_2|_p = |x_3|_p = \sqrt{|a|_p} = \sqrt[3]{|b|_p}$. *In this case, we have* $|x_1|_p = |x_2|_p = |x_3|_p$.

3. *Let* $|a|_p^3 < |b|_p^2$ *and* $\sqrt[3]{b} - \exists$. *Then the cubic equation* (8) *always has a root* x_1 *in which* $|x_1|_p = \sqrt[3]{|b|_p}$. *Moreover, if* $p \equiv 1 \pmod 3$, *then it has two more roots* x_2 *and* x_3 *in which* $|x_2|_p = |x_3|_p = \sqrt[3]{|b|_p}$. *In this case, we have* $|x_1|_p = |x_2|_p = |x_3|_p$.

3.4. *The solvability criterion over* $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$

Theorem 3.5. *Let* $p > 3$ *be a prime. Then the cubic equation* (2) *is solvable over* $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ *if and only if one of the following conditions holds*

1. $\sqrt{|b|_p} < |a|_p$, $\sqrt[3]{|c|_p} < |a|_p$, *and*

   (*i*) $|b|_p^2 > |a|_p|c|_p$, $|c|_p < |b|_p$

   (*ii*) $|b|_p^2 = |a|_p|c|_p$, $\left(|a|_p < 1\right) \vee \left(|a|_p \ge 1,\ |c|_p < |b|_p < |a|_p, (|\delta_1|_p < |b|_p^2,\ \sqrt{\Delta} - \exists) \vee \left(|\delta_1|_p = |b|_p^2,\ \sqrt{\delta_1} - \exists\right)\right)$

   (*iii*) $|b|_p^2 < |a|_p|c|_p$, $\left(|a|_p < 1\right) \vee \left(|a|_p \ge 1,\ |c|_p < |a|_p,\ \sqrt{-ac} - \exists\right)$;

2. $|a|_p < \sqrt{|b|_p}$, $\sqrt[3]{|c|_p} < \sqrt{|b|_p}$, $|c|_p < |b|_p$;

3. $|a|_p < \sqrt[3]{|c|_p}$, $\sqrt{|b|_p} < \sqrt[3]{|c|_p}$, $|c|_p < 1$, $\sqrt[3]{-c} - \exists$.

4. $|a|_p < \sqrt{|b|_p} = \sqrt[3]{|c|_p} < 1$, $D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$;

5. $\sqrt{|b|_p} < |a|_p = \sqrt[3]{|c|_p} < 1,\ \left(|\delta_3|_p < |a|_p^3\right) \vee \left(|\delta_3|_p = |a|_p^3,\ D_0 u_{p-2}^2 \not\equiv a_0^4 \pmod{p}\right)$

6. $\sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p},\ |c|_p < |b|_p.$

7. $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p} < 1,\ (A,B) \in \Phi.$

Proof. Basically, we derive all assertions from Theorem 3.3.

Case 1: $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p$. For this case, we consider three subclasses

Let $|b|_p^2 > |a|_p|c|_p$. Then we always have three solutions $|x_1|_p = |a|_p,\ |x_2|_p = \frac{|b|_p}{|a|_p}$, and $|x_3|_p = \frac{|c|_p}{|b|_p}$ where $|x_3|_p < |x_2|_p < |x_1|_p$. In order to have a root in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, we should have at least $x_3 \in \mathbb{Z}_p \setminus \mathbb{Z}_p^*$. It means that $|c|_p < |b|_p$. Therefore, if $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p,\ |b|_p^2 > |a|_p|c|_p$, and $|c|_p < |b|_p$, then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Let $|b|_p^2 = |a|_p|c|_p$. In this case, if $\left(|\delta_1|_p < |b|_p^2,\ \sqrt{\Delta} - \exists\right) \vee \left(|\delta_1|_p = |b|_p^2,\ \sqrt{\delta_1} - \exists\right)$, then the cubic equation (2) has three roots $|x_1|_p = \log_p |a|_p$ and $|x_2|_p = |x_3|_p = \frac{|b|_p}{|a|_p} = \frac{|c|_p}{|b|_p} = \sqrt{\frac{|c|_p}{|a|_p}}$ where $|x_3|_p = |x_2|_p < |x_1|_p$ otherwise it has a unique root $|x_1|_p = |a|_p$. Consequently, if either one of the following conditions is satisfied

1. $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p,\ |a|_p|c|_p = |b|_p^2,\ |c|_p < |b|_p < |a|_p,\ |a|_p \geq 1$ and
   (i) $|\delta_1|_p < |b|_p^2 = |a|_p|c|_p,\ \sqrt{\Delta} - \exists$ or
   (ii) $|\delta_1|_p = |b|_p^2 = |a|_p|c|_p,\ \sqrt{\delta_1} - \exists$

2. $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p,\ |b|_p^2 = |a|_p|c|_p$ and $|a|_p < 1$,

then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Let $|b|_p^2 < |a|_p|c|_p$. If $\sqrt{-ac} - \exists$, then the cubic equation (2) has three roots $|x_1|_p = |a|_p,\ |x_2|_p = |x_3|_p = \sqrt{\frac{|c|_p}{|a|_p}}$ where $|x_3|_p = |x_2|_p < |x_1|_p$ otherwise it has a unique root $|x_1|_p = |a|_p$. Therefore, if either one of the following two conditions is satisfied

1. $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p,\ |b|_p^2 < |a|_p|c|_p,\ |a|_p \geq 1,\ |c|_p < |a|_p$ and $\sqrt{-ac} - \exists$ or

2. $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p,\ |b|_p^2 < |a|_p|c|_p$ and $|a|_p < 1$,

then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Case 2: $|a|_p < \sqrt{|b|_p}$ and $\sqrt[3]{|c|_p} < \sqrt{|b|_p}$. The cubic equation (2) always has a root x_1 in which $|x_1|_p = \frac{|c|_p}{|b|_p}$. Moreover, if $\sqrt{-b} - \exists$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \sqrt{|b|_p}$ where $|x_1|_p < |x_2|_p = |x_3|_p$. Therefore, if $|a|_p < \sqrt{|b|_p},\ \sqrt[3]{|c|_p} < \sqrt{|b|_p}$ and $|c|_p < |b|_p$, then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Case 3: $|a|_p < \sqrt[3]{|c|_p},\ \sqrt{|b|_p} < \sqrt[3]{|c|_p}$ and $\sqrt[3]{-c} - \exists$. The cubic equation (2) always has a root x_1 in which $|x_1|_p = \sqrt[3]{|c|_p}$. Moreover, if $p \equiv 1 \pmod 3$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \sqrt[3]{|c|_p}$ where $|x_1|_p = |x_2|_p = |x_3|_p$. Therefore, if $|a|_p < \sqrt[3]{|c|_p},\ \sqrt{|b|_p} < \sqrt[3]{|c|_p},\ |c|_p < 1$ and $\sqrt[3]{-c} - \exists$, then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Case 4: $|a|_p < \sqrt{|b|_p} = \sqrt[3]{|c|_p}$ and $D_0 u_{p-2}^2 \not\equiv 9b_0^2 \pmod{p}$. The cubic equation (2) always has a root x_1 in which $|x_1|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$. Moreover, if $\left(|D|_p = 1,\ u_{p-2} \equiv 0 \pmod{p}\right) \vee \left(0 \leq |D|_p < 1,\ \sqrt{D} - \exists\right)$, then it has two more roots x_2 and x_3 in which $|x_2|_p = |x_3|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$ where $|x_1|_p = |x_2|_p = |x_3|_p$. Therefore, if $|a|_p < \sqrt{|b|_p} = \sqrt[3]{|c|_p} < 1$ and $D_0 u_{p-2}^2 \not\equiv 9b_0^2 \pmod{p}$, then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Case 5: $\sqrt{|b|_p} < |a|_p = \sqrt[3]{|c|_p}$ and

1. $|\delta_3|_p < |a|_p^3 = |c|_p$ or
2. $|\delta_3|_p = |a|_p^3 = |c|_p$, $D_0 u_{p-2}^2 \not\equiv a_0^4 \pmod p$.

Regardless of how many roots does the cubic equation (2) have, the p-adic absolute value of its roots is equal to $|a|_p = \sqrt[3]{|c|_p}$. Therefore, if $\sqrt{|b|_p} < |a|_p = \sqrt[3]{|c|_p} < 1$ and

1. $|\delta_3|_p < |a|_p^3 = |c|_p$ or
2. $|\delta_3|_p = |a|_p^3 = |c|_p$, $D_0 u_{p-2}^2 \equiv a_0^4 \pmod p$

then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Case 6: $\sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p}$. The cubic equation (2) always has a root x_1 in which $|x_1|_p = \frac{|c|_p}{|b|_p}$. Moreover, if $|\delta_1|_p < |b|_p = |a|_p^2$ and $\sqrt{\Delta} - \exists$ or $|\delta_1|_p = |b|_p = |a|_p^2$ and $\sqrt{\delta_1} - \exists$ then it has two more solutions x_2 and x_3 in which $|x_2|_p = |x_3|_p = |a|_p = \sqrt{|b|_p}$ where $|x_1|_p < |x_2|_p = |x_3|_p$. Therefore, if $\sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p}$ and $|c|_p < |b|_p$, then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$.

Case 7: Let $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$ and $(A, B) \in \Phi$. Regardless of how many roots does the cubic equation (2) have, the p-adic absolute value of its roots is equal to $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p}$. Therefore, if $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p} < 1$ and $(A, B) \in \Phi$, then the cubic equation (2) has at least one root over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$. This completes the proof. □

3.5. The solvability criterion over $\mathbb{Q}_p \setminus \mathbb{Z}_p$

Theorem 3.6. *Let $p > 3$ be a prime. Then the cubic equation (2) is solvable over $\mathbb{Q}_p \setminus \mathbb{Z}_p$ if and only if one of the following conditions holds*

1. $\sqrt{|b|_p} < |a|_p,\ \sqrt[3]{|c|_p} < |a|_p,\ |a|_p > 1;$
2. $|a|_p < \sqrt{|b|_p},\ \sqrt[3]{|c|_p} < \sqrt{|b|_p},\ \Big(|c|_p > |b|_p\Big) \vee \Big(|c|_p \le |b|_p,\ |b|_p > 1,\ \sqrt{-b} - \exists\Big);$
3. $|a|_p < \sqrt[3]{|c|_p},\ \sqrt{|b|_p} < \sqrt[3]{|c|_p},\ |c|_p > 1,\ \sqrt[3]{-c} - \exists.$
4. $|a|_p < \sqrt{|b|_p} = \sqrt[3]{|c|_p},\ \sqrt{|b|_p} = \sqrt[3]{|c|_p} > 1,\ D_0 u_{p-2}^2 \not\equiv 9b_0^2 \pmod p;$
5. $\sqrt{|b|_p} < |a|_p = \sqrt[3]{|c|_p},\ |a|_p = \sqrt[3]{|c|_p} > 1, \Big(|\delta_3|_p < |a|_p^3\Big) \vee \Big(|\delta_3|_p = |a|_p^3, D_0 u_{p-2}^2 \not\equiv a_0^4 (mod\ p)\Big)$
6. $\sqrt[3]{|c|_p} < |a|_p = \sqrt{|b|_p}$ *with* $(|c|_p > |b|_p)$ *or*
$$\Big(|c|_p \le |b|_p,\ |a|_p = \sqrt{|b|_p} > 1,\ \Big(|\delta_2|_p < |a|_p^2,\ \sqrt{\Delta} - \exists\Big) \vee \Big(|\delta_2|_p = |a|_p^2,\ \sqrt{\delta_2} - \exists\Big)\Big)$$
7. $|a|_p = \sqrt{|b|_p} = \sqrt[3]{|c|_p} > 1,\ (A, B) \in \Phi.$

The proof is similar to the proof of Theorem 3.5

References

[1] M. A. K. Ahmad, L. Liao, M. Saburov, Periodic p-adic Gibbs measures of q-state Potts model on Cayley trees I: The chaos implies the vastness of the set of p-adic Gibbs measures, Journal of Statistical Physics 171 (2018), 1000–1034.

[2] M. A. K. Ahmad, C. H. Pah, M. Saburov, Dynamics of Potts-Bethe mapping of degree four on $\mathbb{Q}_5$, AIP Conference Proceedings, 2184 (2019) 020001

[3] E. Artin, Collected Papers, Springer, New York, 2013.

[4] J. Ax, S. Kochen, Diophantine problems over local fields I, American Journal of Mathematics 87 (1965) 605–630.

[5] J. Ax, S. Kochen, Diophantine problems over local fields II: A complete set of axioms for p-adic number theory, American Journal of Mathematics 87 (1965), 631–648.

[6] Z. I. Borevich, I. R. Shafarevich, Number Theory, Academic Press, New York, 1966.

[7] D. R. Heath-Brown, Zeros of p-adic forms, Proceedings of the London Mathematical Society 100 (2010) 560–584.

[8] D. R. Heath-Brown, Zeros of systems of p-adic quadratic forms, Compositio Mathematica 146 (2010) 271–287.

[9] D. R. Heath-Brown, Artin's conjecture on zeros of p-adic forms, Proceedings of the International Congress of Mathematicians, Vol. II (2010) 249–257.

[10] A. Yu. Khrennikov, p-adic quantum mechanics with p-adic valued functions, Journal of Mathematical Physics 32 (1991) 932–936.

[11] A. Yu. Khrennikov, p-Adic Valued Distributions in Mathematical Physics, Kluwer Academic Publishers, 1994.

[12] S. Lang, Old and new conjectures in diophantine inequalities, Bulletin of the American Mathematical Society 23 (1990) 37–75.

[13] D. J. Lewis, Cubic homogeneous polynomials over p-adic number fields, Annals of Mathematics 56 (1952) 473–478.

[14] S. Ludkovsky, A. Khrennikov, Stochastic processes on non-Archimedean spaces with values in non-Archimedean fields, Markov Processes and Related Fields 9 (2003) 131–162.

[15] F. Mukhamedov, On existence of generalized Gibbs measures for one dimensional p-adic countable state Potts model, Proceedings of the Steklov Institute of Mathematics 265 (2009) 165–176.

[16] F. Mukhamedov, H. Akin, Phase transitions for p-adic Potts model on the Cayley tree of order three, Journal of Statistical Mechanics: Theory and Experiment (2013) P07014.

[17] F. Mukhamedov, H. Akin, On non-Archimedean recurrence equations and their applications, Journal of Mathematical Analysis and Applications 423 (2015) 1203–1218.

[18] F. Mukhamedov, M. Dogan, H. Akin, Phase transition for the p-adic Ising–Vannimenus model on the Cayley tree, Journal of Statistical Mechanics: Theory and Experiment (2014) P10031.

[19] F. Mukhamedov, O. Khakimov, P-adic monomial equations and their perturbations, Izvestiya: Mathematics 84 (2020) 348–360

[20] F. Mukhamedov, B. Omirov, M. Saburov, On cubic equations over p-adic field, International Journal of Number Theory 10 (2014) 1171–1190.

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

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

[23] F. Mukhamedov, M. Saburov, O. Khakimov, On p-adic Ising-Vannimenus model on an arbitrary order Cayley tree, Journal of Statistical Mechanics: Theory and Experiment (2015) P05032.

[24] K. H. Rosen, Elementary Number Theory and Its Applications, Pearson/Addison Wesley, New York, 2011.

[25] U. Rozikov and O. Khakimov, Description of all translation-invariant p-adic Gibbs measures for the Potts model on a Cayley tree, Markov Processes Related Fields 21 (2015) 177–204.

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

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

[28] M. Saburov, M. A. K. Ahmad, The number of solutions of cubic equations over $\mathbb{Q}_3$, Sains Malaysiana 44 (2015), 765–769.

[29] M. Saburov, M. A. K. Ahmad, Quadratic equations over p-adic fields and their application in statistical mechanics, ScienceAsia 41 (2015) 209–215.

[30] M. Saburov, M. A. K. Ahmad, On descriptions of all translation invariant p-adic Gibbs measures for the Potts model on the Cayley tree of order three, Mathematical Physics, Analysis and Geometry 18 (2015) 1–33.

[31] M. Saburov, M. A. K. Ahmad, Solvability and number of roots of bi-quadratic equations over p-adic fields, Malaysian Journal of Mathematical Sciences 10 (2016) 15–35.

[32] M. Saburov, M. A. K. Ahmad, On solvability of general cubic equations over $\mathbb{Z}_p^*$, ScienceAsia 41S (2017) 1–8.

[33] M. Saburov, M. A. K. Ahmad, The dynamics of Potts–Bethe mapping over $\mathbb{Q}_p$: The case $p \equiv 2 \pmod 3$, Journal of Physics: Conferences Series 819(1) (2017) 012017.

[34] M. Saburov, M. A. K. Ahmad, Local descriptions of roots of cubic equations over p-adic fields, Bulletin of the Malaysian Mathematical Sciences Society 41 (2018) 965–984.

[35] V. S. Vladimirov, I. V. Volovich, I. Zelenov, p-Adic Analysis and Mathematical Physics, World Scientific, Singapore, 1994.

[36] T. Zerzaihi, M. Kecies, M. Knapp, Hensel codes of square roots of p-adic numbers, Applicable Analysis and Discrete Mathematics 4 (2010) 32–44