ISSN 0037–4466, Siberian Mathematical Journal, 2023, Vol. 64, No. 2, pp. 443–458. © Pleiades Publishing, Ltd., 2023.

TRINOMIAL EQUATIONS OF DEGREE 6 OVER $\mathbb{Q}_p$

M. Alp, M. Ismail, and M. Saburov

UDC 511.53

Abstract: Finding roots of a single variable polynomial is among the oldest problems of mathematics. This problem is solved in the field of reals but was paid less attention in the field of p-adic numbers, the counterpart of the field of reals. Recently, this problem has been raised up again in considering the p-adic lattice models of statistical mechanics. We introduce a cube root function over the p-adic field $\mathbb{Q}_p$, which enables us to explicitly prescribe the roots of the trinomial equation of degree 6 over $\mathbb{Q}_p$. Namely, we calculate the p-adic absolute value and the first digit of roots of the trinomial equation of degree 6 over $\mathbb{Q}_p$.

DOI: 10.1134/S0037446623020167

Keywords: trinomial equation, cube root function, p-adic field

1. Introduction

The fields of p-adic numbers were introduced by the German mathematician Kurt Hensel. The p-adic numbers were primarily motivated by attempt to bring the ideas and techniques of power series into number theory (see [1]). The canonical representation, analogous to the expansion of analytic functions into power series, 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 began to play a central role in modern number theory. This is due to the fact that they afford a natural and powerful language for talking about congruences between integers, and allow one to use the methods of analysis for studying some problems in modern number theory such as concern elliptic curves, modular forms, and Galois representations. Recently, the applications of p-adic functional and harmonic analysis have appeared in theoretical physics and quantum mechanics (see [2–5]). Moreover, the general theory of p-adic probability was applicable to the problem of the probability interpretation of quantum theories with non-Archimedean valued wave functions (see [6–11]).

Unlike the real case (see [12–15]), the set of p-adic Gibbs measures of the lattice models on the Cayley tree has a complex structure in a sense that it is strongly tied up with a Diophantine problem (i.e. the finding of all solutions of a system of polynomial equations or the giving of a bound for the number of solutions) over $\mathbb{Q}_p$. In general, the same Diophantine problem may have different solutions in the field of p-adic numbers different from the field of reals because of the different topological structures. On the other hand, the rise of the order of the Cayley tree complicates to the studying of the corresponding Diophantine problem over $\mathbb{Q}_p$. In this aspect, the question arises as to whether a root of a polynomial equation belongs to the domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Z}_p$, $\mathbb{Q}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus \left(\mathbb{Z}_p \setminus \mathbb{Z}_p^*\right)$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, and $\mathbb{Q}_p$ or not. Recently, this problem was fully studied for monomial equations (see [16]), quadratic and cubic equations (see [17–20]).

Finding roots of polynomials is among the oldest problems of mathematics. A Diophantine problem consists in finding all solutions of a polynomial equation or a system of polynomial equations in integers, rationals, or sometimes more general number rings and to give a bound for those solutions. The scenario for the field of p-adic numbers is completely different from that for the field of reals. On the one hand, the quadratic equation $x^2+1=0$ is not solvable in the real field but solvable in the p-adic field for $p \equiv 1 \pmod 4$. On the other hand, the cubic equation $x^3+p=0$ is not solvable in the p-adic field but solvable

This work was supported by American University of the Middle East, Kuwait.

The article was submitted by the authors in English.

Original article submitted September 29, 2022; accepted January 10, 2023.

in the real field. Therefore, it is of interest in its own right to provide a solvability criterion for lower degree polynomial equations over the p-adic field. In the field of reals, this problem found its own solution. The solvability criteria and local descriptions of roots of lower degree polynomial equations over $\mathbb{Q}_p$ with applications were presented in the literature.

The solvability criterion of the quadratic equation over the p-adic field was provided in all classical books on p-adic analysis (see [1, 4]). However, no information is available on the p-adic absolute value or the first digit of the roots of the quadratic equation over $\mathbb{Q}_p$. The square root function over the p-adic field was introduced in [21]. This enabled us to explicitly prescribe the roots of the quadratic equation. Namely, the p-adic absolute value and the first digit of roots of the quadratic equation over $\mathbb{Q}_p$ were calculated in [21].

In this paper, we introduce the cube root function over $\mathbb{Q}_p$ (see Definition 5.5) which enables us to calculate the p-adic absolute value and the first digit of roots of the trinomial equation of degree 6 over $\mathbb{Q}_p$ (see Theorems 6.1 and 6.2).

2. Preliminaries

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

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

where $x = p^k \frac{m}{n}$ with $k, m \in \mathbb{Z}$, $n \in \mathbb{N}$, and $(m,p) = (n,p) = 1$. The number k is a *p-order* of x and we write $\mathrm{ord}_p(x) = k$.

Each p-adic number $\mathrm{x} \in \mathbb{Q}_p$ can be uniquely represented in canonical form

$$\mathrm{x} = p^{\mathrm{ord}_p(\mathrm{x})} \left(x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots \right),$$

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

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

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

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

$$\mathrm{x} = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots,$$

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

Each nonzero p-adic number $\mathrm{x} \in \mathbb{Q}_p$ has the unique representation $\mathrm{x} = \frac{\mathrm{x}^*}{|\mathrm{x}|_p}$, where $\mathrm{x}^* \in \mathbb{Q}_p^*$.

3. Square Root Functions

In this section, we recall a definition and some properties of a square root function over $\mathbb{F}_p$ and $\mathbb{Q}_p$ which was introduced and studied in [21]. We will always assume that $p > 3$, unless otherwise specified.

3.1. The square root function over $\mathbb{F}_p$. We recall the definition of square root function on a finite field $\mathbb{F}_p := \{[0]_p, [1]_p, \ldots, [p-1]_p\}$ for a prime $p > 3$. Here $[a]_p := \{b \in \mathbb{Z} : b \equiv a \pmod{p}\}$ for all $0 \leq a \leq p-1$. We always use the *canonical representation* of $\mathbb{F}_p$. Let $[a]_p \in \mathbb{F}_p$ be a nonzero element. We know that the quadratic equation

$$[x]_p^2 = [a]_p \tag{3.1}$$

is solvable in $\mathbb{F}_p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or, equivalently, a is a quadratic residue. In this case, (3.1) has the two roots $[x_1]_p$ and $[x_2]_p$ in $\mathbb{F}_p$ where $1 \leq x_1, x_2 \leq p-1$.

Definition 3.1 [21]. Let $[a]_p \in \mathbb{F}_p$ be a nonzero quadratic residue, and let $[x_1]_p$ and $[x_2]_p$ be the roots of the quadratic equation $[x]_p^2 = [a]_p$ such that $1 \le x_1, x_2 \le p-1$. An element $[\min\{x_1, x_2\}]_p$ of $\mathbb{F}_p$ is a *square root* of $[a]_p$ denoted by $\sqrt{[a]_p}$.

Remark 3.2. We know that if $[a]_p \in \mathbb{F}_p$ with $1 \le a \le p-1$ is a quadratic residue then the quadratic equation $[x]_p^2 = [a]_p$ has the two roots $[x_1]_p$ and $[x_2]_p$ in which $1 \le x_1, x_2 \le p-1$. Moreover, it is easy to check that $[\max\{x_1, x_2\}]_p = [p - \min\{x_1, x_2\}]_p$. By definition $\sqrt{[a]_p} := [\min\{x_1, x_2\}]_p$. We use the notation $-\sqrt{[a]_p} := [\max\{x_1, x_2\}]_p$. Hence, $\sqrt{[a]_p}$ and $-\sqrt{[a]_p}$ are the two roots of the quadratic equation $[x]_p^2 = [a]_p$. In what follows, for the convenience, we use the notation $\sqrt{a}$ instead of $\sqrt{[a]_p}$ whenever we deal with $\mathbb{F}_p$.

3.2. The square root function over $\mathbb{Q}_p$. We recall the square root function over $\mathbb{Q}_p$ for primes $p > 3$. To this end, we need some auxiliary notations.

Let $\mathrm{a} \in \mathbb{Z}_p^*$ be such that

$$\mathrm{a} = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots ,$$

where $a_0 \in \{1, 2, \ldots, p-1\}$ and $a_i \in \{0, 1, \ldots, p-1\}$ for $i \in \mathbb{N}$. We use the notations

$$\mathrm{a}_{[n,m]} = a_n p^n + a_{n+1} p^{n+1} + \cdots + a_m p^m,$$
$$\mathrm{a}^*_{[n,m]} = a_n + a_{n+1} p + a_{n+2} p^2 + \cdots + a_m p^{m-n},$$
$$\mathrm{a}^*_{[n,+\infty)} = a_n + a_{n+1} p + a_{n+2} p^2 + \cdots + a_{n+k} p^k + \cdots .$$

It is clear that $\mathrm{a}_{[n,m]}$ and $\mathrm{a}^*_{[n,m]}$ are integers and $\mathrm{a}^*_{[n,+\infty)}$ is a p-adic integer.

Theorem 3.3 [1, 21]. *Let a belong to $\mathbb{Z}_p^*$ with $\mathrm{a} = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots$ and let a_0 be a quadratic residue modulo p. Then the quadratic equation*

$$\mathrm{x}^2 = \mathrm{a} \tag{3.2}$$

has the two roots $\mathrm{x}^\dagger$ and $\mathrm{x}^\ddagger$ over $\mathbb{Z}_p^*$ which are defined as follows:

$$\mathrm{x}^\dagger = x_0^\dagger + x_1^\dagger p + x_2^\dagger p^2 + \cdots \quad \textit{and} \quad \mathrm{x}^\ddagger = x_0^\ddagger + x_1^\ddagger p + x_2^\ddagger p^2 + \cdots ,$$

where

$$x_0^\dagger \equiv \sqrt{a_0} \pmod p \quad \textit{and} \quad x_0^\ddagger \equiv -\sqrt{a_0} \pmod p, \tag{3.3}$$

$$x_k^\dagger \equiv (2x_0^\dagger)^{p-2} \left(\frac{\mathrm{a}_{[0,k-1]} - \left(\mathrm{x}^\dagger_{[0,k-1]}\right)^2}{p^k} + a_k \right) \pmod p \quad \textit{for all } k \in \mathbb{N}, \tag{3.4}$$

$$x_k^\ddagger \equiv (2x_0^\ddagger)^{p-2} \left(\frac{\mathrm{a}_{[0,k-1]} - \left(\mathrm{x}^\ddagger_{[0,k-1]}\right)^2}{p^k} + a_k \right) \pmod p \quad \textit{for all } k \in \mathbb{N}. \tag{3.5}$$

Remark 3.4. We know that if $\mathrm{x}^\dagger$ and $\mathrm{x}^\ddagger$ are the two roots of (3.2) then $\mathrm{x}^\ddagger = -\mathrm{x}^\dagger$. It is worth mentioning that using the representations of (3.3)–(3.5) of $\mathrm{x}^\dagger$ and $\mathrm{x}^\ddagger$, it is also possible to show that $\mathrm{x}^\ddagger = -\mathrm{x}^\dagger$. To this end, it suffices to note that $x_0^\ddagger \equiv -x_0^\dagger \pmod p$ and $x_k^\ddagger \equiv -(x_k^\dagger + 1) \pmod p$ for any $k \ge 1$. In fact, it is true for $k = 0$, i.e., $x_0^\ddagger \equiv -\sqrt{a_0} \pmod p$ and $x_0^\dagger \equiv \sqrt{a_0} \pmod p$. We assume that it is true for all $k = 1, 2, \dots, n-1$. We would like to show it for $k = n$; i.e., $x_n^{\ddagger} \equiv -(x_n^{\dagger} + 1) \pmod{p}$. Indeed, it follows from the assumption and $0 \le x_k^{\dagger},\ x_k^{\ddagger} \le p-1$ that $\mathrm{x}^{\ddagger}_{[0,n-1]} = p^n - \mathrm{x}^{\dagger}_{[0,n-1]}$ and

$$\left(\mathrm{x}^{\ddagger}_{[0,n-1]}\right)^2 \equiv \left(\mathrm{x}^{\dagger}_{[0,n-1]}\right)^2 - 2p^n \mathrm{x}^{\dagger}_{[0,n-1]} \equiv \left(\mathrm{x}^{\dagger}_{[0,n-1]}\right)^2 - 2x_0^{\dagger} p^n \pmod{p^{n+1}},$$

$$\frac{\mathrm{a}_{[0,n-1]} - \left(\mathrm{x}^{\ddagger}_{[0,n-1]}\right)^2}{p^n} + a_k \equiv \frac{\mathrm{a}_{[0,n-1]} - \left(\mathrm{x}^{\dagger}_{[0,n-1]}\right)^2}{p^n} + a_k + 2x_0^{\dagger} \pmod{p}.$$

Since $p > 2$; therefore,

$$(2x_0^{\ddagger})^{p-2} \equiv -(2x_0^{\dagger})^{p-2} \pmod{p} \quad \text{and} \quad x_n^{\ddagger} \equiv -(x_n^{\dagger} + 1) \pmod{p}.$$

Hence, we are now free to say that the property $\mathrm{x}^{\ddagger} = -\mathrm{x}^{\dagger}$ of the roots $\mathrm{x}^{\dagger}$ and $\mathrm{x}^{\ddagger}$ of (3.2) is well captured in the representations of (3.3)–(3.5) of $\mathrm{x}^{\dagger}$ and $\mathrm{x}^{\ddagger}$.

Let $\mathrm{x} \in \mathbb{Q}_p$ and $\mathrm{x} = \frac{\mathrm{x}^*}{|\mathrm{x}|_p}$ where $\mathrm{x}^* \in \mathbb{Z}_p^*$ such that $\mathrm{x}^* = x_0 + x_1 p + x_2 p^2 + \cdots$. We introduce the set

$$\mathbb{Q}_p^{\mathrm{sroot}} = \{\mathrm{x} \in \mathbb{Q}_p : \log_p |\mathrm{x}|_p - \text{even},\ x_0^{\frac{p-1}{2}} \equiv 1 \pmod{p}\}.$$

Definition 3.5 [21]. The square root function $f : \mathbb{Q}_p^{\mathrm{sroot}} \to \mathbb{Q}_p$, $\mathrm{y} = f(\mathrm{x}) = \sqrt{\mathrm{x}}$ is defined as $\mathrm{y} = \frac{\mathrm{y}^*}{|\mathrm{y}|_p}$ such that $|\mathrm{y}|_p = \sqrt{|\mathrm{x}|_p}$ and

$$y_0 = \sqrt{x_0}, \quad y_k \equiv (2y_0)^{p-2} \left(\frac{\mathrm{x}_{[0,k-1]} - \mathrm{y}^2_{[0,k-1]}}{p^k} + x_k \right) \pmod{p} \quad \text{for all } k \in \mathbb{N}.$$

Remark 3.6. It follows from Theorem 3.3 that one root of (3.2) is $\sqrt{\mathrm{a}}$ in which $(\sqrt{\mathrm{a}})^* \equiv \sqrt{a_0} \pmod{p}$. Moreover, it follows from Remark 3.4 that another root of (3.2) is $-\sqrt{\mathrm{a}}$ in which $(-\sqrt{\mathrm{a}})^* \equiv -\sqrt{a_0} \pmod{p}$. In this sense, Definition 3.5 elegantly captures the property that the quadratic equation $\mathrm{x}^2 = \mathrm{a}$ has the two roots $\pm\sqrt{\mathrm{a}}$, which was the case for the reals.

4. Quadratic Equations

In this section, we are aiming to overview the main results of the papers [10, 21] which will be used in the upcoming sections.

Let us consider the quadratic equation

$$\mathrm{x}^2 + \mathrm{a}\mathrm{x} = \mathrm{b}. \tag{4.1}$$

We assume that $\mathrm{ab} \neq 0$. Otherwise, it is easy to study (4.1).

Let $\mathrm{D} = \mathrm{a}^2 + 4\mathrm{b}$ be a discriminant of (4.1). Then $\mathrm{D} = \frac{\mathrm{D}^*}{|\mathrm{D}|_p}$ where $\mathrm{D}^* \in \mathbb{Z}_p^*$ such that $\mathrm{D}^* = d_0 + d_1 p + d_2 p^2 + \cdots$. We know that (4.1) is solvable in $\mathbb{Q}_p$ if and only if $\log_p |\mathrm{D}|_p$ is even and d_0 is a quadratic residue modulo p or equivalently $\mathrm{D} \in \mathbb{Q}_p^{\mathrm{sroot}}$ (see [1]). In this case

$$\sqrt{\mathrm{D}} = \frac{1}{\sqrt{|\mathrm{D}|_p}}(\delta_0 + \delta_1 p + \delta_2 p^2 + \cdots),$$

where

$$\delta_0 = \sqrt{d_0} \quad \text{and} \delta_k \equiv (2\delta_0)^{p-2} \left(\frac{\mathrm{d}_{[0,k-1]} - \delta^2_{[0,k-1]}}{p^k} + d_k \right) \pmod{p} \quad \text{for all } k \ge 1.$$

Moreover, the roots of (4.1) have the form

$$\mathrm{x}^{(1)} = \frac{-\mathrm{a} + \sqrt{\mathrm{D}}}{2}, \qquad \mathrm{x}^{(2)} = \frac{-\mathrm{a} - \sqrt{\mathrm{D}}}{2}. \tag{4.2}$$

The solvability criterion of the quadratic equation (4.1) in terms of a and b was given in [10].

Theorem 4.1 [10]. *Quadratic equation* (4.1) *is solvable in* $\mathbb{Q}_p$ *if and only if one of the following holds:*

(i) $|\mathrm{a}|_p^2 < |\mathrm{b}|_p$ *and* $\mathrm{b} \in \mathbb{Q}_p^{\mathrm{sroot}}$*;*

(ii) $|\mathrm{a}|_p^2 = |\mathrm{b}|_p$ *and* $\mathrm{D} \in \mathbb{Q}_p^{\mathrm{sroot}}$*;*

(iii) $|\mathrm{a}|_p^2 > |\mathrm{b}|_p$.

The set $\Delta := \Delta_1 \cup \Delta_2 \cup \Delta_3$ is called the *solvability domain* (see [10]) where

(i) $\Delta_1 = \{(\mathrm{a},\mathrm{b}) \in \mathbb{Q}_p^2\colon\ |\mathrm{a}|_p^2 < |\mathrm{b}|_p,\ \mathrm{b} \in \mathbb{Q}_p^{\mathrm{sroot}}\}$;

(ii) $\Delta_2 = \{(\mathrm{a},\mathrm{b}) \in \mathbb{Q}_p^2\colon\ |\mathrm{a}|_p^2 = |\mathrm{b}|_p,\ \mathrm{D} \in \mathbb{Q}_p^{\mathrm{sroot}}\}$;

(iii) $\Delta_3 = \{(\mathrm{a},\mathrm{b}) \in \mathbb{Q}_p^2\colon\ |\mathrm{a}|_p^2 > |\mathrm{b}|_p\}$.

We describe the p-adic absolute values and the first digits of the roots $\mathrm{x}^{(1)}$ and $\mathrm{x}^{(2)}$ of (4.1). Let

$$\mathrm{a} = \frac{\mathrm{a}^*}{|\mathrm{a}|_p}, \quad \mathrm{b} = \frac{\mathrm{b}^*}{|\mathrm{b}|_p}, \quad \mathrm{D} = \frac{\mathrm{D}^*}{|\mathrm{D}|_p}, \quad \mathrm{D} = \mathrm{a}^2 + 4\mathrm{b},$$

$$\mathrm{a}^* = a_0 + a_1 p + a_2 p^2 + \cdots, \quad \mathrm{b}^* = b_0 + b_1 p + b_2 p^2 + \cdots, \quad \mathrm{D}^* = d_0 + d_1 p + d_2 p^2 + \cdots,$$

$$\sqrt{\mathrm{D}} = \frac{1}{\sqrt{|\mathrm{D}|_p}}(\delta_0 + \delta_1 p + \delta_2 p^2 + \cdots).$$

Let $\mathrm{x}^{(1)}$ and $\mathrm{x}^{(2)}$ be the roots of (4.1) defined by (4.2) where

$$\mathrm{x}^{(1)} = \frac{(\mathrm{x}^{(1)})^*}{|\mathrm{x}^{(1)}|_p}, \quad \mathrm{x}^{(2)} = \frac{(\mathrm{x}^{(2)})^*}{|\mathrm{x}^{(2)}|_p},$$

and

$$(\mathrm{x}^{(1)})^* = x_0^{(1)} + x_1^{(1)} p + x_2^{(1)} p^2 + \cdots, \quad (\mathrm{x}^{(2)})^* = x_0^{(2)} + x_1^{(2)} p + x_2^{(2)} p^2 + \cdots.$$

Theorem 4.2 [21]. *Let* $(a,b) \in \Delta$. *The following are true:*

(i) *If* $(a,b) \in \Delta_1$ *then* $|\mathrm{x}^{(1)}|_p = |\mathrm{x}^{(2)}|_p = \sqrt{|b|_p} > |a|_p$ *and*

$$2x_0^{(1)} \equiv \sqrt{4b_0} \pmod p, \qquad 2x_0^{(2)} \equiv -\sqrt{4b_0} \pmod p;$$

(ii) *If* $(a,b) \in \Delta_2$ *and* $a_0^2 \not\equiv -4b_0 \pmod p$ *then*

$$|\mathrm{x}^{(1)}|_p = |\mathrm{x}^{(2)}|_p = \sqrt{|b|_p} = |a|_p,$$

$$2x_0^{(1)} \equiv -a_0 + \sqrt{a_0^2 + 4b_0} \pmod p, \quad 2x_0^{(2)} \equiv -a_0 - \sqrt{a_0^2 + 4b_0} \pmod p;$$

(iii) *If* $(a,b) \in \Delta_2$ *and* $a_0^2 \equiv -4b_0 \pmod p$ *then*

$$|\mathrm{x}^{(1)}|_p = |\mathrm{x}^{(2)}|_p = \sqrt{|b|_p} = |a|_p, \quad 2x_0^{(1)} = 2x_0^{(2)} \equiv -a_0 \pmod p;$$

(iv) *If* $(a,b) \in \Delta_3$ *then*

$$\max\left\{|\mathrm{x}^{(1)}|_p, |\mathrm{x}^{(2)}|_p\right\} = |a|_p > \frac{|b|_p}{|a|_p} = \min\left\{|\mathrm{x}^{(1)}|_p, |\mathrm{x}^{(2)}|_p\right\},$$

$$x_0^{(\max)} \equiv -a_0 \pmod p, \quad a_0 x_0^{(\min)} \equiv b_0 \pmod p,$$

where $x^{(\max)}, x^{(\min)} \in \{x^{(1)}, x^{(2)}\}$ *are such that*

$$\left|\mathrm{x}^{(\max)}\right|_p = \max\left\{|\mathrm{x}^{(1)}|_p, |\mathrm{x}^{(2)}|_p\right\} \quad \textit{and} \quad \left|\mathrm{x}^{(\min)}\right|_p = \min\left\{|\mathrm{x}^{(1)}|_p, |\mathrm{x}^{(2)}|_p\right\}.$$

Remark 4.3. Let $(\mathrm{a},\mathrm{b}) \in \Delta_3$. In this case, $|\mathrm{D}|_p = |\mathrm{a}|_p^2$ and $\mathrm{D}^* = (\mathrm{a}^*)^2 + 4\mathrm{b}|\mathrm{a}|_p$. Hence, $d_0 \equiv a_0^2 \pmod p$ and $\delta_0 = \sqrt{d_0} = \sqrt{a_0^2} = \min\{a_0, p - a_0\}$. Consequently,

$$\text{if } a_0 < \frac{p}{2} \text{ then } \begin{cases} \mathrm{x}^{(\max)} = \frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2} \\ \mathrm{x}^{(\min)} = \frac{-\mathrm{a}+\sqrt{\mathrm{D}}}{2} \end{cases} \quad \text{and} \quad \text{if } a_0 > \frac{p}{2} \text{ then } \begin{cases} \mathrm{x}^{(\max)} = \frac{-\mathrm{a}+\sqrt{\mathrm{D}}}{2} \\ \mathrm{x}^{(\min)} = \frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2} \end{cases}.$$

The next corollary, ensuing from the proof of Theorem 4.2 and Remark 4.3, might be useful in the study of p-adic Gibbs measures over the Cayley trees (see [9–11]).

Corollary 4.4 [21]. *Let $(a, b) \in \Delta$ and let $\mathrm{x}^{(1)}$ and $\mathrm{x}^{(2)}$ be the roots of* (4.1) *defined by* (4.2). *Then the following are true:*

Case $(a, b) \in \Delta_1$. *We have* $|D|_p = |b|_p$, $D^* = 4b^* + \mathrm{a}^2|b|_p$, $d_0 \equiv 4b_0 \pmod p$ *and* $|\sqrt{D}|_p = \sqrt{|D|_p} = \sqrt{|b|_p} > |\mathrm{a}|_p$, $\left(\sqrt{D}\right)^* = \sqrt{4b^* + \mathrm{a}^2|b|_p}$, $\delta_0 \equiv \sqrt{4b_0} \pmod p$. *Moreover,* $|\mathrm{x}^{(1)}|_p = |\mathrm{x}^{(2)}|_p = \sqrt{|b|_p} > |\mathrm{a}|_p$, $2x_0^{(1)} \equiv \sqrt{4b_0} \pmod p$, *and* $2x_0^{(2)} \equiv -\sqrt{4b_0} \pmod p$.

Case $(a, b) \in \Delta_2$, $|D|_p = |\mathrm{a}|_p^2 = |b|_p$. *We have* $\left|(\mathrm{a}^*)^2 + 4b^*\right|_p = 1$, $D^* = (\mathrm{a}^*)^2 + 4b^*$, $d_0 \equiv a_0^2 + 4b_0 \pmod p$ *and* $|\sqrt{D}|_p = \sqrt{|D|_p} = |\mathrm{a}|_p = \sqrt{|b|_p}$, $\left(\sqrt{D}\right)^* = \sqrt{(\mathrm{a}^*)^2 + 4b^*}$, $\delta_0 \equiv \sqrt{a_0^2 + 4b_0} \pmod p$. *Moreover,* $|\mathrm{x}^{(1)}|_p = |\mathrm{x}^{(2)}|_p = \sqrt{|b|_p} = |\mathrm{a}|_p$, $2x_0^{(1)} \equiv -a_0 + \sqrt{a_0^2 + 4b_0} \pmod p$, *and* $2x_0^{(2)} \equiv -a_0 - \sqrt{a_0^2 + 4b_0} \pmod p$.

Case $(a, b) \in \Delta_2$, $|D|_p < |\mathrm{a}|_p^2 = |b|_p$. *We have* $|(\mathrm{a}^*)^2 + 4b^*|_p < 1$, $|D|_p = |b|_p|(\mathrm{a}^*)^2 + 4b^*|_p$, *and* $D^* = ((\mathrm{a}^*)^2 + 4b^*)^*$. *Moreover,* $|\mathrm{x}^{(1)}|_p = |\mathrm{x}^{(2)}|_p = \sqrt{|b|_p} = |\mathrm{a}|_p$ *and* $2x_0^{(1)} \equiv 2x_0^{(2)} \equiv -a_0 \pmod p$.

Case $(a, b) \in \Delta_3$, $a_0 < \frac{p}{2}$. *We have* $|D|_p = |\mathrm{a}|_p^2$, $D^* = (\mathrm{a}^*)^2 + 4b|\mathrm{a}|_p$, $d_0 \equiv a_0^2 \pmod p$ *and* $|\sqrt{D}|_p = \sqrt{|D|_p} = |\mathrm{a}|_p$, $\left(\sqrt{D}\right)^* = \sqrt{(\mathrm{a}^*)^2 + 4b|\mathrm{a}|_p}$, $\delta_0 \equiv a_0 \pmod p$. *Moreover,* $|\mathrm{x}^{(1)}|_p = \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}$, $a_0x_0^{(1)} \equiv b_0 \pmod p$, $|\mathrm{x}^{(2)}|_p = |\mathrm{a}|_p$, *and* $x_0^{(2)} \equiv -a_0 \pmod p$.

Case $(a, b) \in \Delta_3$, $a_0 > \frac{p}{2}$. *We have* $|D|_p = |\mathrm{a}|_p^2$, $D^* = (\mathrm{a}^*)^2 + 4b|\mathrm{a}|_p$, $d_0 \equiv a_0^2 \pmod p$ *and* $|\sqrt{D}|_p = \sqrt{|D|_p} = |\mathrm{a}|_p$, $\left(\sqrt{D}\right)^* = \sqrt{(\mathrm{a}^*)^2 + 4b|\mathrm{a}|_p}$, $\delta_0 \equiv -a_0 \pmod p$. *Moreover,* $|\mathrm{x}^{(1)}|_p = |\mathrm{a}|_p$, $x_0^{(1)} \equiv -a_0 \pmod p$, $|\mathrm{x}^{(2)}|_p = \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}$, *and* $a_0x_0^{(2)} \equiv b_0 \pmod p$.

5. Cube Root Functions

In this section, we introduce to the cube root functions over $\mathbb{F}_p$ and $\mathbb{Q}_p$. We always assume that $p > 3$ unless otherwise specified.

5.1. The cube root function over $\mathbb{F}_p$. We first introduce the cube root function over $\mathbb{F}_p := \{[0]_p, [1]_p, \ldots, [p-1]_p\}$. We always use *this canonical representation* of $\mathbb{F}_p$.

Let $[a]_p \in \mathbb{F}_p$ be a nonzero element. We know that the cubic congruent equation

$$[x]_p^3 = [a]_p \tag{5.1}$$

is solvable in $\mathbb{F}_p$ if and only if $a^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod p$ or equivalently, a is a cubic residue. In this case, if $p \equiv 2 \pmod 3$ then (5.1) has a unique root $[x_1]_p$, $1 \leq x_1 \leq p-1$ for all $1 \leq a \leq p-1$ (this is due to the fact that $(a^{\frac{2p-1}{3}})^3 \equiv a \pmod p$). If $p \equiv 1 \pmod 3$ with $a^{\frac{p-1}{3}} \equiv 1 \pmod p$ then (5.1) has three distinct roots $[x_1]_p$, $[x_2]_p$, and $[x_3]_p$ where $1 \leq x_1, x_2, x_3 \leq p-1$.

Definition 5.1. Let $[a]_p \in \mathbb{F}_p$ be a nonzero cubic residue and let $[x_1]_p$, $[x_2]_p$, and $[x_3]_p$ be (possibly one or three) roots of the cubic congruent equation $[x]_p^3 = [a]_p$ such that $1 \leq x_1, x_2, x_3 \leq p-1$. The element $[\min\{x_1, x_2, x_3\}]_p$ of $\mathbb{F}_p$ is a *cube root* of $[a]_p$ denoted by $\sqrt[3]{[a]_p}$.

Example 5.2. Let us consider some primes $p \equiv 1 \pmod 3$.

- Let $p = 7$. In this case, $[1]_7$ and $[6]_7$ are cubic residues modulo 7. Thus, $\sqrt[3]{[1]_7} = [1]_7$ and $\sqrt[3]{[6]_7} = [3]_7$.

- Let $p = 19$. In this case, $[1]_{19}$, $[7]_{19}$, $[8]_{19}$, $[11]_{19}$, $[12]_{19}$, and $[18]_{19}$ are cubic residues modulo 19. Consequently, $\sqrt[3]{[1]_{19}} = [1]_{19}$, $\sqrt[3]{[7]_{19}} = [4]_{19}$, $\sqrt[3]{[8]_{19}} = [2]_{19}$, $\sqrt[3]{[11]_{19}} = [5]_{19}$, $\sqrt[3]{[12]_{19}} = [10]_{19}$, and $\sqrt[3]{[18]_{19}} = [8]_{19}$.

Remark 5.3. Obviously, the cubic congruent equation $[x]_p^3 = [1]_p$ for a prime $p \equiv 2 \pmod 3$ always has a unique root $[\varepsilon_1]_p$ where $\varepsilon_1 := 1$. Moreover, if $p \equiv 1 \pmod 3$ then the equation has two more roots $[\varepsilon_2]_p$ and $[\varepsilon_3]_p$ such that $\varepsilon_1 < \varepsilon_2 < \varepsilon_3$. In both cases, $\sqrt[3]{[1]_p} = [\varepsilon_1]_p$ for every prime p. It is worth mentioning that if $p \equiv 1 \pmod 3$ with $a^{\frac{p-1}{3}} \equiv 1 \pmod p$ then $\varepsilon_1 \sqrt[3]{[a]_p}$, $\varepsilon_2 \sqrt[3]{[a]_p}$, and $\varepsilon_3 \sqrt[3]{[a]_p}$ are roots of the cubic congruent equation $[x]_p^3 = [a]_p$. In what follows, for the convenience, we use the notation $\sqrt[3]{a}$ instead of $\sqrt[3]{[a]_p}$ whenever we deal with $\mathbb{F}_p$.

5.2. The cube root function over $\mathbb{Q}_p$. We need the following auxiliary result:

Theorem 5.4. *Let $p > 3$ and $\mathrm{a} \in \mathbb{Z}_p^*$. The cubic equation*

$$\mathrm{x}^3 = \mathrm{a} \tag{5.2}$$

is solvable in $\mathbb{Z}_p^*$ if and only if a_0 is a cubic residue modulo p or equivalently $a_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod p$. Moreover, the root of (5.2) takes the form

$$\mathrm{x} = x_0 + x_1 p + x_2 p^2 + \cdots ,$$

where

$$x_0 \in \begin{cases} \{\varepsilon_1 \sqrt[3]{a_0}, \varepsilon_2 \sqrt[3]{a_0}, \varepsilon_3 \sqrt[3]{a_0}, \}, & \text{if } \ p \equiv 1 \pmod 3, \\ \{\varepsilon_1 \sqrt[3]{a_0}\}, & \text{if } \ p \equiv 2 \pmod 3, \end{cases}$$

$$x_k \equiv (3x_0^2)^{p-2} \left(\frac{\mathrm{a}_{[0,k-1]} - \mathrm{x}_{[0,k-1]}^3}{p^k} + a_k \right) \pmod p \quad \text{for all } k \in \mathbb{N}.$$

Proof. Only if part: We suppose that (5.2) has some solution in $\mathbb{Z}_p^*$ of the form of $\mathrm{x} = x_0 + \mathrm{x}_{[1,+\infty)}^* p$. Then

$$\begin{aligned} \mathrm{x}^3 &= \left(x_0 + \mathrm{x}_{[1,+\infty)}^* p\right)^3 \\ &= x_0^3 + \left(\mathrm{x}_{[1,+\infty)}^*\right)^3 p^3 + 3x_0^2 \mathrm{x}_{[1,+\infty)}^* p + 3x_0 \left(\mathrm{x}_{[1,+\infty)}^*\right) p^2 \\ &= a_0 + \mathrm{a}_{[1,+\infty)}^* p. \end{aligned}$$

We have $x_0^3 \equiv a_0 \pmod p$, which means that a_0 is a cubic residue modulo p.

If part: Suppose now that a_0 is a cubic residue modulo p. It means that there exists $x_0 \in \mathbb{Z}$ such that $x_0^3 \equiv a_0 \pmod p$. This implies that

$$x_0 \in \begin{cases} \{\varepsilon_1 \sqrt[3]{a_0}, \varepsilon_2 \sqrt[3]{a_0}, \varepsilon_3 \sqrt[3]{a_0}, \}, & \text{if } \ p \equiv 1 \pmod 3, \\ \{\varepsilon_1 \sqrt[3]{a_0}\}, & \text{if } \ p \equiv 2 \pmod 3. \end{cases}$$

Show that each of these roots can be lifted to $\mathbb{Z}_p^*$. Let $\mathrm{x} = \mathrm{x}_{[0,k-1]} + x_k p^k + \mathrm{x}_{[k+1,+\infty)}^* p^{k+1}$. Suppose that $x_0, x_1, \ldots, x_{k-1}$ were already found. We have to find x_k. Our aim is to obtain some recurrent formula to calculate x_k in terms of $x_0, x_1, \ldots, x_{k-1}$ for all $k \geq 1$. It is easy to see that

$$\begin{aligned} \mathrm{x}^3 = \mathrm{x}_{[0,k-1]}^3 &+ x_k^3 p^{3k} + \left(\mathrm{x}_{[k+1,+\infty)}^*\right)^3 p^{3k+3} + 3\mathrm{x}_{[0,k-1]}^2 x_k p^k + 3\mathrm{x}_{[0,k-1]}^2 \mathrm{x}_{[k+1,+\infty)}^* p^{k+1} \\ &+3\mathrm{x}_{[0,k-1]} x_k^2 p^{2k} + 3\mathrm{x}_{[0,k-1]} \left(\mathrm{x}_{[k+1,+\infty)}^*\right)^2 p^{2k+2} + 3x_k^2 \mathrm{x}_{[k+1,+\infty)}^* p^{3k+1} \\ &+3x_k \left(\mathrm{x}_{[k+1,+\infty)}^*\right)^2 p^{3k+2} + 6\mathrm{x}_{[0,k-1]} x_k \mathrm{x}_{[k+1,+\infty)}^* p^{2k+1} \\ &= \mathrm{a}_{[0,k-1]} + a_k p^k + \mathrm{a}_{[k+1,+\infty)}^* p^{k+1}. \end{aligned}$$

This implies that

$$\begin{aligned} \mathrm{x}^3_{[0,k-1]} &\equiv \mathrm{a}_{[0,k-1]} \pmod{p^k}, \\ \mathrm{x}^3_{[0,k-1]} + 3\mathrm{x}^2_{[0,k-1]} x_k p^k &\equiv \mathrm{a}_{[0,k-1]} + a_k p^k \pmod{p^{k+1}}, \\ 3\mathrm{x}^2_{[0,k-1]} x_k &\equiv \frac{\mathrm{a}_{[0,k-1]} - \mathrm{x}^3_{[0,k-1]}}{p^k} + a_k \pmod{p}. \end{aligned}$$

Since $\mathrm{x}^2_{[0,k-1]} \equiv x_0^2 \pmod{p}$; therefore,

$$x_k \equiv (3x_0^2)^{p-2} \left(\frac{\mathrm{a}_{[0,k-1]} - \mathrm{x}^3_{[0,k-1]}}{p^k} + a_k \right) \pmod{p}.$$

Consequently, we derive a formula to calculate x_k in terms of $x_0, x_1, \ldots, x_{k-1}$. □

Let us now consider the cubic equation

$$\mathrm{x}^3 = \mathrm{a} \tag{5.3}$$

where $\mathrm{a} \in \mathbb{Q}_p$ is a nonzero p-adic number.

Put $\mathrm{a} = \frac{\mathrm{a}^*}{|\mathrm{a}|_p}$ where $\mathrm{a}^* = a_0 + a_1 p + a_2 p^2 + \cdots$. Cubic equation (5.3) is solvable in $\mathbb{Q}_p$ if and only if $\log_p |\mathrm{a}|_p$ is divisible by 3 and a_0 is a cubic residue modulo p (see [16]). Moreover,

(i) if $p \equiv 1 \pmod 3$ then (5.3) has the three roots

$$\mathrm{x}^{(1)} = \frac{(\mathrm{x}^{(1)})^*}{|\mathrm{x}^{(1)}|_p}, \quad \mathrm{x}^{(2)} = \frac{(\mathrm{x}^{(2)})^*}{|\mathrm{x}^{(2)}|_p} \quad \mathrm{x}^{(3)} = \frac{(\mathrm{x}^{(3)})^*}{|\mathrm{x}^{(3)}|_p},$$

where $|\mathrm{x}^{(i)}|_p = \sqrt[3]{|\mathrm{a}|_p}$ and $(\mathrm{x}^{(i)})^* = x_0^{(i)} + x_1^{(i)} p + x_2^{(i)} p^2 + \cdots$ for all $i = 1, 2, 3$ such that

$$\begin{aligned} x_0^{(i)} &\equiv \varepsilon_i \sqrt[3]{a_0} \pmod{p}, \\ x_k^{(i)} &\equiv (3(x_0^{(i)})^2)^{p-2} \left(\frac{\mathrm{a}_{[0,k-1]} - \mathrm{x}^3_{[0,k-1]}}{p^k} + a_k \right) \pmod{p} \quad \text{for all } k \in \mathbb{N}; \end{aligned}$$

(ii) if $p \equiv 2 \pmod 3$, then the cubic equation (5.3) has the unique root

$$\mathrm{x}^{(1)} = \frac{(\mathrm{x}^{(1)})^*}{|\mathrm{x}^{(1)}|_p},$$

where $|\mathrm{x}^{(1)}|_p = \sqrt[3]{|\mathrm{a}|_p}$ and $(\mathrm{x}^{(1)})^* = x_0^{(1)} + x_1^{(1)} p + x_2^{(1)} p^2 + \cdots$ such that

$$\begin{aligned} x_0^{(1)} &\equiv \varepsilon_1 \sqrt[3]{a_0} \pmod{p}, \\ x_k^{(1)} &\equiv (3(x_0^{(1)})^2)^{p-2} \left(\frac{\mathrm{a}_{[0,k-1]} - \mathrm{x}^3_{[0,k-1]}}{p^k} + a_k \right) \pmod{p} \quad \text{for all } k \in \mathbb{N}. \end{aligned}$$

Let $\mathrm{x} \in \mathbb{Q}_p$, $\mathrm{x} = \frac{\mathrm{x}^*}{|\mathrm{x}|_p}$ where $\mathrm{x}^* \in \mathbb{Z}_p^*$ such that $\mathrm{x}^* = x_0 + x_1 p + x_2 p^2 + \cdots$. We introduce the set

$$\mathbb{Q}_p^{\mathrm{croot}} = \left\{ \mathrm{a} \in \mathbb{Q}_p : \log_p |\mathrm{a}|_p \text{ is divisible by 3 and } a_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p} \right\}.$$

Definition 5.5. The cube root function $f : \mathbb{Q}_p^{\mathrm{croot}} \to \mathbb{Q}_p$, $\mathrm{y} = f(\mathrm{x}) = \sqrt[3]{\mathrm{x}}$ is defined as $\mathrm{y} = \frac{\mathrm{y}^*}{|\mathrm{y}|_p}$ such that $|\mathrm{y}|_p = \sqrt[3]{|\mathrm{x}|_p}$, $y_0 = \sqrt[3]{x_0}$, and $y_k = (3y_0^2)^{p-2} \left(\frac{\mathrm{x}_{[0,k-1]} - \mathrm{y}^3_{[0,k-1]}}{p^k} + x_k \right) \pmod{p}$ for all $k \in \mathbb{N}$.

Example 5.6. Let $p = 7$ and $\mathrm{x} = -1$. Thus, $x_0 = 6$ and $x_k = 6$ for all $k \in \mathbb{N}$. We know that $\sqrt[3]{[6]_7} = [3]_7$ (see Example 5.2) and $y_0 = 3$. We can find y_k by using the recurrent formula

$$y_k = (3y_0^2)^{p-2}\left(\frac{\mathrm{x}_{[0,k-1]} - \mathrm{y}^3_{[0,k-1]}}{p^k} + x_k\right) \pmod p \quad \text{for all } k \in \mathbb{N}.$$

For instance, $y_1 = 4$, $y_2 = 6$, $y_3 = 3$, $y_4 = 0$ and so on. Also, $|\mathrm{y}|_p = \sqrt[3]{|\mathrm{x}|_p} = \sqrt[3]{1} = 1$. Hence,

$$\sqrt[3]{-1} = y_0 + y_1 p + y_2 p^2 + \cdots$$

such that $y_0 = 3$, $y_1 = 4$, $y_2 = 6$, $y_3 = 3$, $y_4 = 0$, and so on.

Remark 5.7. Let $p \equiv 1 \pmod 3$ and let e_1, e_2, and e_3 be the roots of the cubic equation $\mathrm{x}^3 = 1$ over $\mathbb{Q}_p$ where $\mathrm{e}_1 := 1$. If $\mathrm{a} \in \mathbb{Q}_p^{\mathrm{croot}}$ then $\mathrm{e}_1\sqrt[3]{\mathrm{a}}$, $\mathrm{e}_2\sqrt[3]{\mathrm{a}}$, and $\mathrm{e}_3\sqrt[3]{\mathrm{a}}$ are the roots of the cubic equation $\mathrm{x}^3 = \mathrm{a}$. Moreover, for all $i = 1, 2, 3$ we have

$$\begin{aligned}
\left(\mathrm{e}_i\sqrt[3]{\mathrm{a}}\right)^* &= e_0^{(i)} + e_1^{(i)}p + e_2^{(i)}p^2 + \cdots,\\
e_0^{(i)} &\equiv \varepsilon_i\sqrt[3]{a_0} \pmod p,\\
e_k^{(i)} &\equiv (3(e_0^{(i)})^2)^{p-2}\left(\frac{\mathrm{a}_{[0,k-1]} - \mathrm{e}^3_{[0,k-1]}}{p^k} + a_k\right) \pmod p \quad \text{for all } k \in \mathbb{N}.
\end{aligned}$$

6. The Trinomial Equations of Degree 6

In this section, we provide an application of the cube root function in describing the roots of polynomial equations over p-adic fields. All results of Section 6 are new and can potentially have applications to the study of the p-adic Gibbs measures over the Cayley trees.

Let us now study the trinomial equation of degree 6; i.e.,

$$\mathrm{x}^6 + \mathrm{a}\mathrm{x}^3 = \mathrm{b}, \tag{6.1}$$

where $\mathrm{ab} \neq 0$ and $\mathrm{a}, \mathrm{b} \in \mathbb{Q}_p$. The case $\mathrm{ab} = 0$ was studied in [16, 17].

We use the following notations for $A, B \in \mathbb{Q}_p$:

- $(A \bigvee B) - \exists$ means that there exists at least one of the members A and B;
- $(A \overline{\bigwedge} B) - \exists$ means that there exists only one of the members A and B.
- $(A \overline{\overline{\bigwedge}} B) - \exists$ means that there exist both members A and B.

In this sense,

$$(A \bigvee B) - \exists = \left[(A \overline{\bigwedge} B) - \exists\right] \cup \left[(A \overline{\overline{\bigwedge}} B) - \exists\right].$$

Theorem 6.1 (Solvability Criteria). *Let* $\mathrm{D} = \mathrm{a}^2 + 4\mathrm{b}$. *Equation* (6.1) *is solvable in* $\mathbb{Q}_p$ *if and only if either one of the conditions hold:*

(I) $|\mathrm{a}|_p^2 < |b|_p$, $\left(\sqrt{b} - \exists\right)$ *and* $\left(\sqrt[3]{\sqrt{b}} \bigvee \sqrt[3]{-\sqrt{b}} - \exists\right)$;

(II) $|\mathrm{a}|_p^2 = |b|_p = |D|_p$, $\left(\sqrt{D} - \exists\right)$ *and* $\left(\sqrt[3]{\frac{-\mathrm{a}+\sqrt{\mathrm{D}}}{2}} \bigvee \sqrt[3]{\frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2}} - \exists\right)$;

(III) $|\mathrm{a}|_p^2 = |b|_p > |D|_p$, *and* $\left(\sqrt{D} \overline{\overline{\bigwedge}} \sqrt[3]{-\frac{\mathrm{a}}{2}} - \exists\right)$;

(IV) $|\mathrm{a}|_p^2 > |b|_p$, *and* $\left(\sqrt[3]{-\mathrm{a}} \bigvee \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}} - \exists\right)$.

Proof. Let $\mathrm{x}^3 = \mathrm{t}$. In this case, we have the quadratic equation

$$\mathrm{t}^2 + \mathrm{at}{=}\mathrm{b}. \tag{6.2}$$

Equation (6.2) is solvable if and only if (a,b) $\in \Delta$. Let $\mathrm{t}^{(1)} = \frac{(\mathrm{t}^{(1)})^*}{|\mathrm{t}^{(1)}|_p}$ and $\mathrm{t}^{(2)} = \frac{(\mathrm{t}^{(2)})^*}{|\mathrm{t}^{(2)}|_p}$ be the roots of (6.2), where

$$(\mathrm{t}^{(1)})^* = t_0^{(1)} + t_1^{(1)}p + t_2^{(1)}p^2 + \cdots, \qquad (\mathrm{t}^{(2)})^* = t_0^{(2)} + t_1^{(2)}p + t_2^{(2)}p^2 + \cdots.$$

Then, (6.1) is solvable in $\mathbb{Q}_p$ if and only if one of the cubic equation is solvable

$$\mathrm{x}^3 = \mathrm{t}^{(1)}, \tag{6.3}$$

$$\mathrm{x}^3 = \mathrm{t}^{(2)}. \tag{6.4}$$

Case **(I)**. Let (a,b) $\in \Delta_1$. In this case, by Theorem 4.2

$$|\mathrm{t}^{(1)}|_p = |\mathrm{t}^{(2)}|_p = \sqrt{|\mathrm{b}|_p} > |\mathrm{a}|_p,$$
$$t_0^{(1)} \equiv \sqrt{b_0} \pmod{p}, \quad t_0^{(2)} \equiv -\sqrt{b_0} \pmod{p}.$$

Equation (6.3) (respectively (6.4)) is solvable if and only if $3 \mid \log_p |\mathrm{t}^{(1)}|_p$ and $t_0^{(1)}$ is a cubic residue (respectively $3 \mid \log_p |\mathrm{t}^{(2)}|_p$ and $t_0^{(2)}$ is a cubic residue). We know that

$$\log_p |\mathrm{t}^{(1)}|_p = \log_p |\mathrm{t}^{(2)}|_p = \log_p \sqrt{|\mathrm{b}|_p} = \frac{1}{2} \log_p |\mathrm{b}|_p.$$

It follows from the last equality that

$$3 \mid \log_p |\mathrm{t}^{(1)}|_p = \log_p |\mathrm{t}^{(2)}|_p$$

if and only if $3 \mid \frac{1}{2} \log_p |\mathrm{b}|_p$ or equivalently $6 \mid \log_p |\mathrm{b}|_p$.

Moreover, $t_0^{(1)}$ (respectively $t_0^{(2)}$) is a cubic residue if and only if there exist $\sqrt[3]{\sqrt{b_0}}$ (respectively $\sqrt[3]{-\sqrt{b_0}}$). Consequently, $|\mathrm{a}|_p^2 < |\mathrm{b}|_p$, $\sqrt{\mathrm{b}} - \exists$, and $\left(\sqrt{3}\sqrt{\mathrm{b}} \bigvee \sqrt[3]{-\sqrt{\mathrm{b}}}\right) - \exists$.

Case **(II)**. Let $(\mathrm{a}, \mathrm{b}) \in \Delta_2$ and $|\mathrm{a}|_p^2 = |\mathrm{b}|_p = |\mathrm{D}|$. In this case, by Theorem 4.2

$$|\mathrm{t}^{(1)}|_p = |\mathrm{t}^{(2)}|_p = \sqrt{|\mathrm{b}|_p} = |\mathrm{a}|_p = \sqrt{|\mathrm{D}|_p},$$
$$2t_0^{(1)} \equiv -a_0 + \sqrt{a_0^2 + 4b_0} \pmod{p}, \quad 2t_0^{(2)} \equiv -a_0 - \sqrt{a_0^2 + 4b_0} \pmod{p}.$$

Equation (6.3) (respectively (6.4)) is solvable if and only if $3 \mid \log_p |\mathrm{t}^{(1)}|_p$ and $t_0^{(1)}$ is a cubic residue (respectively $3 \mid \log_p |\mathrm{t}^{(2)}|_p$ and $t_0^{(2)}$ is a cubic residue). We know that

$$\log_p |\mathrm{t}^{(1)}|_p = \log_p |\mathrm{t}^{(2)}|_p = \log_p \sqrt{|\mathrm{b}|_p} = \log_p |\mathrm{a}|_p = \log_p \sqrt{|\mathrm{D}|_p} = |\frac{-\mathrm{a} \pm \sqrt{D}}{2}|_p.$$

It follows from the last equality that $3 \mid \left(\log_p |\mathrm{t}^{(1)}|_p = \log_p |\mathrm{t}^{(2)}|_p\right)$ if and only if

$$3 \mid \log_p \left|\frac{-\mathrm{a} \pm \sqrt{D}}{2}\right|_p.$$

Moreover, $t_0^{(1)}$ (respectively $t_0^{(2)}$) is a cubic residue if and only if $\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}$ (respectively $\frac{-a_0-\sqrt{a_0^2-4b_0}}{2}$) is a cubic residue. Consequently, $|\mathrm{a}|_p^2 = |\mathrm{b}|_p = |\mathrm{D}|$, $\sqrt{\mathrm{D}} - \exists$, and $\left(\sqrt[3]{\frac{-\mathrm{a}+\sqrt{D}}{2}} \bigvee \sqrt[3]{\frac{-\mathrm{a}-\sqrt{D}}{2}}\right) - \exists$.

Case **(III)**. Let $(\mathrm{a},\mathrm{b}) \in \Delta_2$ and $|\mathrm{a}|_p^2 = |\mathrm{b}|_p > |\mathrm{D}|$. In this case, by Theorem 4.2

$$|\mathrm{t}^{(1)}|_p = |\mathrm{t}^{(2)}|_p = \sqrt{|\mathrm{b}|_p} = |\mathrm{a}|_p > \sqrt{|\mathrm{D}|_p},$$
$$2t_0^{(1)} \equiv 2t_0^{(2)} \equiv -a_0 \pmod{p}.$$

Equation (6.3) (respectively (6.4)) is solvable if and only if $3 \mid \log_p |\mathrm{t}^{(1)}|_p$ and $t_0^{(1)}$ is a cubic residue (respectively $3 \mid \log_p |\mathrm{t}^{(2)}|_p$ and $t_0^{(2)}$ is a cubic residue). We know (see Corollary 4.4) that

$$\log_p |\mathrm{t}^{(1)}|_p = \log_p |\mathrm{t}^{(2)}|_p = \log_p \sqrt{|\mathrm{b}|_p} = \log_p |\mathrm{a}|_p = \log_p \left| \frac{-\mathrm{a} \pm \sqrt{\mathrm{D}}}{2} \right|_p .$$

It follows from the last equality that $3 \mid \log_p |\mathrm{t}^{(1)}|_p = \log_p |\mathrm{t}^{(2)}|_p$ if and only if

$$3 \mid \log_p \sqrt{|\mathrm{b}|_p} = \log_p |\mathrm{a}|_p = \log_p \left| \frac{-\mathrm{a} \pm \sqrt{D}}{2} \right|_p .$$

Moreover, $t_0^{(1)}$ (respectively $t_0^{(2)}$) is a cubic residue if and only if $\dfrac{-a_0}{2}$ is a cubic residue. Consequently, $|\mathrm{a}|_p^2 = |\mathrm{b}|_p > |\mathrm{D}|$, and $\left(\sqrt{\mathrm{D}}\, \overline{\overline{\bigwedge}} \sqrt[3]{-\frac{\mathrm{a}}{2}}\right) - \exists$.

Case **(IV)**. Let $(\mathrm{a},\mathrm{b}) \in \Delta_3$. In this case, by Theorem 4.2

$$|\mathrm{t}^{(\max)}|_p = |\mathrm{a}|_p > \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p} = |\mathrm{t}^{(\min)}|_p,$$
$$t_0^{(\max)} \equiv -a_0 \pmod{p}, \quad a_0 t_0^{(\min)} \equiv b_0 \pmod{p}.$$

Equation (6.3) (respectively (6.4)) is solvable if and only if $3 \mid \log_p |\mathrm{t}^{(\max)}|_p$ and $t_0^{(\max)}$ is a cubic residue (respectively $3 \mid \log_p |\mathrm{t}^{(\min)}|_p$ and $t_0^{(\min)}$ is a cubic residue). We know that $\log_p |\mathrm{t}^{(\max)}|_p = \log_p |\mathrm{a}|_p$ and $\log_p |\mathrm{t}^{(\min)}|_p = \log_p \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}$. It follows from the last equality that $3 \mid \log_p |\mathrm{t}^{(\max)}|_p$ if and only if $3 \mid \log_p |\mathrm{a}|_p$ and $3 \mid \log_p |\mathrm{t}^{(\min)}|_p$ if and only if $3 \mid \log_p \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}$ or equivalently $3 \mid \log_p |\mathrm{a}^2\mathrm{b}|_p$. Moreover, $t_0^{(\max)}$ (respectively $t_0^{(\min)}$) is a cubic residue if and only if $-a_0$ (respectively $\dfrac{b_0}{a_0}$) is a cubic residue. Consequently, $|\mathrm{a}|_p^2 > |\mathrm{b}|_p$, and $\left(\sqrt[3]{-\mathrm{a}} \bigvee \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}}\right) - \exists$. □

Theorem 6.2 (Description of Roots). *Let* $(a,b) \in \Delta$. *The following hold:*
(I) *Let* $|\mathrm{a}|_p^2 < |b|_p$, $\sqrt{b} - \exists$, *and* $\left(\sqrt[3]{\sqrt{b}} \bigvee \sqrt[3]{-\sqrt{b}} - \exists\right)$.
(I.1) *Let* $\left(\sqrt[3]{\sqrt{b}}\, \overline{\bigwedge} \sqrt[3]{-\sqrt{b}}\right) - \exists$. *Equation* (6.1) *has a root,* $\mathrm{x}^{(1)}$ *such that*

$$x_0^{(1)} \equiv \left(\sqrt[3]{\sqrt{b_0}} \barwedge \sqrt[3]{-\sqrt{b_0}}\right) \pmod{p} \quad \mathit{and} \quad |\mathrm{x}^{(1)}|_p = \sqrt[6]{|b|_p}.$$

Moreover, if $p \equiv 1 \pmod{3}$ *then* (6.1) *has two more roots* $\mathrm{x}^{(2)}$ *and* $\mathrm{x}^{(3)}$ *such that*

$$x_0^{(i)} \equiv \varepsilon_i \left(\sqrt[3]{\sqrt{b_0}} \barwedge \sqrt[3]{-\sqrt{b_0}}\right) \pmod{p} \quad \mathit{and} \quad |\mathrm{x}^{(i)}|_p = \sqrt[6]{|b|_p},\ i = 2, 3.$$

(I.2) *Let* $\left(\sqrt[3]{\sqrt{\mathrm{b}}}\,\overline{\overline{\bigwedge}}\sqrt[3]{-\sqrt{\mathrm{b}}}\right)-\exists$. *Equation* (6.1) *has two roots* $\mathrm{x}^{(1)}$ *and* $\mathrm{x}^{(2)}$ *such that* $x_0^{(1)}\equiv\sqrt[3]{\sqrt{b_0}}\pmod p$, $x_0^{(2)}\equiv\sqrt[3]{-\sqrt{b_0}}\pmod p$ *and* $|\mathrm{x}^{(1)}|_p=|\mathrm{x}^{(2)}|_p=\sqrt[6]{|\mathrm{b}|_p}$. *Moreover, if* $p\equiv 1\pmod 3$ *then* (6.1) *has four more roots* $\mathrm{x}^{(3)}$, $\mathrm{x}^{(4)}$, $\mathrm{x}^{(5)}$, *and* $\mathrm{x}^{(6)}$ *such that*

$$x_0^{(2i-1)}\equiv\varepsilon_i\sqrt[3]{\sqrt{b_0}}\pmod p,\quad x_0^{(2i)}\equiv\varepsilon_i\sqrt[3]{-\sqrt{b_0}}\pmod p,\quad i=2,3,$$
$$|\mathrm{x}^{(2i-1)}|_p=|\mathrm{x}^{(2i)}|_p=\sqrt[6]{|\mathrm{b}|_p},\quad i=2,3.$$

(II) *Let* $|\mathrm{a}|_p^2=|b|_p=|D|$, $\sqrt{D}-\exists$, *and* $\left(\sqrt[3]{\frac{-\mathrm{a}+\sqrt{D}}{2}}\bigvee\sqrt[3]{\frac{-\mathrm{a}-\sqrt{D}}{2}}\right)-\exists$.

(II.1) *Let* $\sqrt[3]{\frac{-\mathrm{a}+\sqrt{D}}{2}}\,\overline{\bigwedge}\sqrt[3]{\frac{-\mathrm{a}-\sqrt{D}}{2}}-\exists$. *Equation* (6.1) *always has some root* $\mathrm{x}^{(1)}$ *such that*

$$x_0^{(1)}\equiv\left(\sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}}\,\overline{\bigwedge}\sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}}\right)\pmod p,$$

$$|\mathrm{x}^{(1)}|_p=\sqrt[3]{|\mathrm{a}|_p}=\sqrt[6]{|b|_p}=\sqrt[6]{|D|_p}.$$

Moreover, if $p\equiv 1\pmod 3$ *then* (6.1) *has two more roots* $\mathrm{x}^{(2)}$ *and* $\mathrm{x}^{(3)}$ *such that*

$$|\mathrm{x}^{(i)}|_p=\sqrt[3]{|\mathrm{a}|_p}=\sqrt[6]{|b|_p}=\sqrt[6]{|D|_p},$$

$$x_0^{(i)}\equiv\varepsilon_i\left(\sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}}\bigwedge\sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}}\right)\pmod p,\quad i=2,3.$$

(II.2) *Let* $\left(\sqrt[3]{\frac{-\mathrm{a}+\sqrt{D}}{2}}\,\overline{\overline{\bigwedge}}\sqrt[3]{\frac{-\mathrm{a}-\sqrt{D}}{2}}\right)-\exists$. *Equation* (6.1) *always has two roots* $\mathrm{x}^{(1)}$ *and* $\mathrm{x}^{(2)}$ *such that*

$$x_0^{(1)}\equiv\sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}}\pmod p,\quad x_0^{(2)}\equiv\sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}}\pmod p,$$
$$|\mathrm{x}^{(1)}|_p=|\mathrm{x}^{(2)}|_p=\sqrt[3]{|\mathrm{a}|_p}=\sqrt[6]{|b|_p}=\sqrt[6]{|D|_p}.$$

Moreover, if $p\equiv 1\pmod 3$ *then* (6.1) *has four more roots* $\mathrm{x}^{(3)}$, $\mathrm{x}^{(4)}$, $\mathrm{x}^{(5)}$, *and* $\mathrm{x}^{(6)}$ *such that*

$$x_0^{(2i-1)}\equiv\varepsilon_i\sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}}\pmod p,\quad i=2,3,$$

$$x_0^{(2i)}\equiv\varepsilon_i\sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}}\pmod p,\quad i=2,3,$$
$$|\mathrm{x}^{(2i-1)}|_p=|\mathrm{x}^{(2i)}|_p=\sqrt[3]{|\mathrm{a}|_p}=\sqrt[6]{|b|_p}=\sqrt[6]{|D|_p},\quad i=2,3.$$

(III) *Let* $|\mathrm{a}|_p^2=|b|_p>|D|$ *and* $\left(\sqrt{D}\,\overline{\overline{\bigwedge}}\sqrt[3]{-\frac{\mathrm{a}}{2}}\right)-\exists$. *Equation* (6.1) *always has two roots* $\mathrm{x}^{(1)}$ *and* $\mathrm{x}^{(2)}$ *such that*

$$x_0^{(1)}\equiv x_0^{(2)}\equiv\sqrt[3]{\frac{-a_0}{2}}\pmod p,\quad |\mathrm{x}^{(1)}|_p=|\mathrm{x}^{(2)}|_p=\sqrt[3]{|\mathrm{a}|_p}=\sqrt[6]{|b|_p}.$$

Moreover, if $p \equiv 1 \pmod 3$ *then* (6.1) *has four more roots* $\mathrm{x}^{(3)}$, $\mathrm{x}^{(4)}$, $\mathrm{x}^{(5)}$, *and* $\mathrm{x}^{(6)}$ *such that*

$$x_0^{(2i-1)} \equiv x_0^{(2i)} \equiv \varepsilon_i \sqrt[3]{\frac{-a_0}{2}} \pmod p, \quad |\mathrm{x}^{(2i-1)}|_p = |\mathrm{x}^{(2i)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p}, \quad i = 2, 3.$$

(IV) *Let* $|\mathrm{a}|_p^2 > |\mathrm{b}|_p$ *and* $\left(\sqrt[3]{-\mathrm{a}} \bigvee \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}}\right) - \exists$.

(IV.1) *Let* $\sqrt[3]{-\mathrm{a}} \overline{\bigwedge} \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}} - \exists$. *Equation* (6.1) *always has a root* $\mathrm{x}^{(1)}$ *such that*

$$x_0^{(1)} \equiv \left(\sqrt[3]{-a_0} \overline{\bigwedge} \sqrt[3]{\frac{b_0}{a_0}}\right) \pmod p, \quad |\mathrm{x}^{(1)}|_p = \sqrt[3]{|\mathrm{a}|_p} \overline{\bigwedge} \sqrt[3]{\frac{|b|_p}{|\mathrm{a}|_p}}.$$

Moreover, if $p \equiv 1 \pmod 3$ *then* (6.1) *has two more roots* $\mathrm{x}^{(2)}$ *and* $\mathrm{x}^{(3)}$ *such that*

$$x_0^{(i)} \equiv \varepsilon_i \left(\sqrt[3]{-a_0} \overline{\bigwedge} \sqrt[3]{\frac{b_0}{a_0}}\right) \pmod p, \quad |\mathrm{x}^{(i)}|_p = \sqrt[3]{|\mathrm{a}|_p} \overline{\bigwedge} \sqrt[3]{\frac{|b|_p}{|\mathrm{a}|_p}}, \quad i = 2, 3.$$

(IV.2) *Let* $\left(\sqrt[3]{-\mathrm{a}} \overline{\overline{\bigwedge}} \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}}\right) - \exists$. *Equation* (6.1) *always has two roots* $\mathrm{x}^{(1)}$ *and* $\mathrm{x}^{(2)}$ *such that*

$$x_0^{(1)} \equiv \sqrt[3]{-a_0} \pmod p, \ |\mathrm{x}^{(1)}|_p = \sqrt[3]{|\mathrm{a}|_p},$$

$$x_0^{(2)} \equiv \sqrt[3]{\frac{b_0}{a_0}} \pmod p, \ |\mathrm{x}^{(2)}|_p = \sqrt[3]{\frac{|b|_p}{|\mathrm{a}|_p}}.$$

Moreover, if $p \equiv 1 \pmod 3$ *then* (6.1) *has four more roots* $\mathrm{x}^{(3)}$, $\mathrm{x}^{(4)}$, $\mathrm{x}^{(5)}$, *and* $\mathrm{x}^{(6)}$ *such that*

$$x_0^{(2i-1)} \equiv \varepsilon_i \sqrt[3]{-a_0} \pmod p, \ |\mathrm{x}^{(2i-1)}|_p = \sqrt[3]{|\mathrm{a}|_p}, \quad i = 2, 3,$$

$$x_0^{(2i)} \equiv \varepsilon_i \sqrt[3]{\frac{b_0}{a_0}} \pmod p, \ |\mathrm{x}^{(2i)}|_p = \sqrt[3]{\frac{|b|_p}{|\mathrm{a}|_p}}, \quad i = 2, 3.$$

Proof. Let (a,b) $\in \Delta$. We will consider the several cases:

(I) Let $|\mathrm{a}|_p^2 < |\mathrm{b}|_p$, $\sqrt{\mathrm{b}} - \exists$, and $\left(\sqrt[3]{\sqrt{\mathrm{b}}} \bigvee \sqrt[3]{-\sqrt{\mathrm{b}}}\right) - \exists$. In this case, since $\mathrm{x}^3 = \mathrm{t}^{(1)}$ or $\mathrm{x}^3 = \mathrm{t}^{(2)}$ and $|\mathrm{t}^{(1)}|_p = |\mathrm{t}^{(2)}|_p = \sqrt{|\mathrm{b}|_p}$, we have $\mathrm{x} = \sqrt[3]{\mathrm{t}^{(1)}}$ or $\mathrm{x} = \sqrt[3]{\mathrm{t}^{(2)}}$ and $|\mathrm{x}|_p = \sqrt[3]{|\mathrm{t}^{(1)}|_p} = \sqrt[3]{|\mathrm{t}^{(2)}|_p} = \sqrt[6]{|\mathrm{b}|_p}$.

(I.1) Let $\left(\sqrt[3]{\sqrt{\mathrm{b}}} \overline{\bigwedge} \sqrt[3]{-\sqrt{\mathrm{b}}}\right) - \exists$. If $p \equiv 2 \pmod 3$ then (6.3) or (6.4) has a unique root $\mathrm{x}^{(1)}$. Since $3 \mid \log_p \sqrt{|\mathrm{b}|_p}$ and $\sqrt{b_0} \overline{\wedge} (-\sqrt{b_0})$ is a cubic residue, the first digit of the root $\mathrm{x}^{(1)}$ of the trinomial equation (6.1) is $x_0^{(1)} \equiv \left(\sqrt[3]{\sqrt{b_0}} \overline{\bigwedge} \sqrt[3]{-\sqrt{b_0}}\right) \pmod p$ and its norm is $|\mathrm{x}^{(1)}|_p = \sqrt[6]{|\mathrm{b}|_p}$. If $p \equiv 1 \pmod 3$ then (6.3) or (6.4) has two more roots $\mathrm{x}^{(2)}$ and $\mathrm{x}^{(3)}$. Since $3 \mid \log_p \sqrt{|\mathrm{b}|_p}$ and $\sqrt{b_0} \overline{\wedge} (-\sqrt{b_0})$ is a cubic residue, the first digit of the roots $\mathrm{x}^{(2)}$ and $\mathrm{x}^{(3)}$ are $x_0^{(i)} \equiv \varepsilon_i \left(\sqrt[3]{\sqrt{b_0}} \overline{\bigwedge} \sqrt[3]{-\sqrt{b_0}}\right) \pmod p$ and their norms are $|\mathrm{x}^{(i)}|_p = \sqrt[6]{|\mathrm{b}|_p}$ for $i = 2, 3$.

(I.2) Let $\left(\sqrt[3]{\sqrt{\mathrm{b}}} \overline{\overline{\bigwedge}} \sqrt[3]{-\sqrt{\mathrm{b}}}\right) - \exists$. If $p \equiv 2 \pmod 3$ then each equation (6.3) (respectively (6.4)) has a unique root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$). Since $3 \mid \log_p \sqrt{|\mathrm{b}|_p}$ and $\sqrt{b_0} \overline{\overline{\wedge}} (-\sqrt{b_0})$ is a cubic residue, the first digit of the root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$) is $x_0^{(1)} \equiv \sqrt[3]{\sqrt{b_0}} \pmod{p}$ (respectively $x_0^{(2)} \equiv \sqrt[3]{-\sqrt{b_0}} \pmod{p}$) and its norm is $|\mathrm{x}^{(1)}|_p = \sqrt[6]{|\mathrm{b}|_p}$ (respectively $|\mathrm{x}^{(2)}|_p = \sqrt[6]{|\mathrm{b}|_p}$). If $p \equiv 1 \pmod{3}$ then each equation (6.3) (respectively (6.4)) has two more roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$). Since $3 \mid \log_p \sqrt{|\mathrm{b}|_p}$ and $\sqrt{b_0}\ \overline{\overline{\wedge}}\ (-\sqrt{b_0})$ is a cubic residue, the first digits of the roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$) are $x_0^{(2i-1)} \equiv \varepsilon_i \sqrt[3]{\sqrt{b_0}} \pmod{p}$ (respectively $x_0^{(2i)} \equiv \varepsilon_i \sqrt[3]{-\sqrt{b_0}} \pmod{p}$) and their norms are $|\mathrm{x}^{(2i-1)}|_p = \sqrt[6]{|\mathrm{b}|_p}$ (respectively $|\mathrm{x}^{(2i)}|_p = \sqrt[6]{|\mathrm{b}|_p}$) for $i = 2, 3$.

(II) Let $|\mathrm{a}|_p^2 = |\mathrm{b}|_p = |\mathrm{D}|_p$, $\sqrt{\mathrm{D}} - \exists$, and $\left(\sqrt{[3]}\frac{-\mathrm{a}+\sqrt{\mathrm{D}}2}{\bigvee}\sqrt{[3]}\frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2}\right) - \exists$. In this case, since $\mathrm{x}^3 = \mathrm{t}^{(1)}$ or $\mathrm{x}^3 = \mathrm{t}^{(2)}$ and $|\mathrm{t}^{(1)}|_p = |\mathrm{t}^{(2)}|_p = |\mathrm{a}|_p = \sqrt{|\mathrm{b}|_p} = \sqrt{|\mathrm{D}|_p}$, we have $\mathrm{x} = \sqrt[3]{\mathrm{t}^{(1)}}$ or $\mathrm{x} = \sqrt[3]{\mathrm{t}^{(2)}}$ and $|\mathrm{x}|_p = \sqrt[3]{|\mathrm{t}^{(1)}|_p} = \sqrt[3]{|\mathrm{t}^{(2)}|_p} = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p} = \sqrt[6]{|\mathrm{D}|_p}$.

(II.1) Let $\sqrt[3]{\frac{-\mathrm{a}+\sqrt{\mathrm{D}}}{2}}\ \overline{\bigwedge}\sqrt[3]{\frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2}} - \exists$. If $p \equiv 2 \pmod{3}$ then (6.3) or (6.4) has a unique root $\mathrm{x}^{(1)}$. Since

$$3 \mid \left(\log_p \left|\frac{-\mathrm{a}+\sqrt{\mathrm{D}}}{2}\right|_p \overline{\bigwedge} \log_p \left|\frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2}\right|_p\right)$$

and $\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}\ \overline{\bigwedge}\ \frac{-a_0-\sqrt{a_0^2+4b_0}}{2}$ is a cubic residue, the first digit of the root $\mathrm{x}^{(1)}$ of (6.1) is

$$x_0^{(1)} \equiv \sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}}\ \overline{\bigwedge}\sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}} \pmod{p}$$

and its norm is $|\mathrm{x}^{(1)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p} = \sqrt[6]{|\mathrm{D}|_p}$. If $p \equiv 1 \pmod{3}$ then (6.3) or (6.4) has two more roots $\mathrm{x}^{(2)}$ and $\mathrm{x}^{(3)}$. The first digit of the roots $\mathrm{x}^{(2)}$ and $\mathrm{x}^{(3)}$ are

$$x_0^{(i)} \equiv \varepsilon_i \left(\sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}}\ \overline{\bigwedge}\ \sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}}\right) \pmod{p}$$

and their norms are $|\mathrm{x}^{(i)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p} = \sqrt[6]{|\mathrm{D}|_p}$, $i = 2, 3$.

(II.2) Let $\sqrt[3]{\frac{-\mathrm{a}+\sqrt{\mathrm{D}}}{2}}\ \overline{\overline{\bigwedge}}\sqrt[3]{\frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2}} - \exists$. If $p \equiv 2 \pmod{3}$ then each (6.3) (respectively (6.4)) has a unique root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$). Since

$$3 \mid \left(\log_p \left|\frac{-\mathrm{a}+\sqrt{\mathrm{D}}}{2}\right|_p \overline{\overline{\bigwedge}} \log_p \left|\frac{-\mathrm{a}-\sqrt{\mathrm{D}}}{2}\right|_p\right)$$

and $\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}\ \overline{\overline{\bigwedge}}\ \frac{-a_0-\sqrt{a_0^2+4b_0}}{2}$ is a cubic residue, the first digit of the root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$) is $x_0^{(1)} \equiv \sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}} \pmod{p}$ (respectively $x_0^{(2)} \equiv \sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}} \pmod{p}$) and its norm is $|\mathrm{x}^{(1)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p} = \sqrt[6]{|\mathrm{D}|_p}$. (respectively $|\mathrm{x}^{(2)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p} = \sqrt[6]{|\mathrm{D}|_p}$). If $p \equiv 1 \pmod{3}$ then each (6.3) (respectively (6.4)) has two more roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$). The first digits of the roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$) are $x_0^{(2i-1)} \equiv \varepsilon_i \sqrt[3]{\frac{-a_0+\sqrt{a_0^2+4b_0}}{2}} \pmod{p}$ (respectively $x_0^{(2i)} \equiv \varepsilon_i \sqrt[3]{\frac{-a_0-\sqrt{a_0^2+4b_0}}{2}} \pmod{p}$) and their norms are $|\mathrm{x}^{(2i-1)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p} = \sqrt[6]{|\mathrm{D}|_p}$ (respectively $|\mathrm{x}^{(2i)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p} = \sqrt[6]{|\mathrm{D}|_p}$) for $i = 2, 3$.

(III) Let $|\mathrm{a}|_p^2 = |\mathrm{b}|_p > |\mathrm{D}|_p$ and $\left(\sqrt{\mathrm{D}}\ \overline{\overline{\bigwedge}}\sqrt[3]{-\frac{\mathrm{a}}{2}}\right) - \exists$. In this case, since $\mathrm{x}^3 = \mathrm{t}^{(1)}$ or $\mathrm{x}^3 = \mathrm{t}^{(2)}$ and $|\mathrm{t}^{(1)}|_p = |\mathrm{t}^{(2)}|_p = \sqrt{|\mathrm{b}|_p} = |\mathrm{a}|_p$, we have $\mathrm{x} = \sqrt[3]{\mathrm{t}^{(1)}}$ or $\mathrm{x} = \sqrt[3]{\mathrm{t}^{(2)}}$ and $|\mathrm{x}|_p = \sqrt[3]{|\mathrm{t}^{(1)}|_p} = \sqrt[3]{|\mathrm{t}^{(2)}|_p} = \sqrt[3]{|\mathrm{a}|_p} =$

$\sqrt[6]{|\mathrm{b}|_p}$. If $p \equiv 2 \pmod 3$ then each (6.3) (respectively (6.4)) has a unique root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$). Since $3 \mid \log_p |\frac{\mathrm{a}}{2}|_p$ and $\frac{-a_0}{2}$ is a cubic residue, the first digit of the root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$) is $x_0^{(1)} \equiv \sqrt[3]{\frac{-a_0}{2}} \pmod p$ (respectively $x_0^{(2)} \equiv \sqrt[3]{\frac{-a_0}{2}} \pmod p$) and its norm is $|\mathrm{x}^{(1)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p}$ (respectively $|\mathrm{x}^{(2)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p}$). If $p \equiv 1 \pmod 3$ then each (6.3) (respectively (6.4)) has two more roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$). The first digits of the roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$) are $x_0^{(2i-1)} \equiv \varepsilon_i \sqrt[3]{\frac{-a_0}{2}} \pmod p$ (respectively $x_0^{(2i)} \equiv \varepsilon_i \sqrt[3]{\frac{-a_0}{2}} \pmod p$) and their norms are $|\mathrm{x}^{(2i-1)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p}$ (respectively $|\mathrm{x}^{(2i)}|_p = \sqrt[3]{|\mathrm{a}|_p} = \sqrt[6]{|\mathrm{b}|_p}$) for $i = 2, 3$.

(IV) Let $|\mathrm{a}|_p^2 > |\mathrm{b}|_p$ and $\left(\sqrt[3]{-\mathrm{a}} \bigvee \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}}\right) - \exists$.

(IV.1) Let $\sqrt[3]{-\mathrm{a}} \overline{\bigwedge} \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}} - \exists$. In this case, since $\mathrm{x}^3 = \mathrm{t}^{(\max)} \barwedge \mathrm{t}^{(\min)}$ and

$$|\mathrm{t}^{(\max)}|_p \barwedge |\mathrm{t}^{(\min)}|_p = |\mathrm{a}|_p \barwedge \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p},$$

we have $\mathrm{x} = \sqrt[3]{\mathrm{t}^{(\max)}} \barwedge \sqrt[3]{\mathrm{t}^{(\min)}}$ and $|\mathrm{x}|_p = \sqrt[3]{|\mathrm{a}|_p} \overline{\bigwedge} \sqrt[3]{\frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}}$. If $p \equiv 2 \pmod 3$ then the equation $\mathrm{x}^3 = \mathrm{t}^{(\max)} \barwedge \mathrm{t}^{(\min)}$ has a unique root $\mathrm{x}^{(1)}$. Since

$$3 \mid \left(\log_p |\mathrm{a}|_p \overline{\bigwedge} \log_p \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}\right)$$

and $\left(-a_0 \barwedge \frac{b_0}{a_0}\right)$ is a cubic residue, the first digit of the root $\mathrm{x}^{(1)}$ is $x_0^{(1)} \equiv \left(\sqrt[3]{-a_0} \barwedge \sqrt[3]{\frac{b_0}{a_0}}\right) \pmod p$ and its norm is $|\mathrm{x}^{(1)}|_p = \left(\sqrt[3]{|\mathrm{a}|_p} \barwedge \sqrt[3]{\frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}}\right)$. If $p \equiv 1 \pmod 3$ then the equation $\mathrm{x}^3 = \mathrm{t}^{(\max)} \barwedge \mathrm{t}^{(\min)}$ has two more roots $\mathrm{x}^{(2)}$ and $\mathrm{x}^{(3)}$. The first digits of the roots $\mathrm{x}^{(2)}$ and $\mathrm{x}^{(3)}$ are $x_0^{(i)} \equiv \varepsilon_i \left(\sqrt[3]{-a_0} \barwedge \sqrt[3]{\frac{b_0}{a_0}}\ \right) \pmod p$ and their norms are $|\mathrm{x}^{(i)}|_p = \sqrt[3]{|\mathrm{a}|_p} \overline{\bigwedge} \sqrt[3]{\frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}}$ for $i = 2, 3$.

(IV.2) Let $\sqrt[3]{-\mathrm{a}} \overline{\overline{\bigwedge}} \sqrt[3]{\frac{\mathrm{b}}{\mathrm{a}}} - \exists$. In this case, since $\mathrm{x}^3 = \mathrm{t}^{(\max)} \doublebarwedge \mathrm{t}^{(\min)}$ and

$$|\mathrm{t}^{(\max)}|_p \doublebarwedge |\mathrm{t}^{(\min)}|_p = |\mathrm{a}|_p \doublebarwedge \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p},$$

we have

$$\mathrm{x} = \sqrt[3]{\mathrm{t}^{(\max)}} \doublebarwedge \sqrt[3]{\mathrm{t}^{(\min)}} \quad \text{and} \quad |\mathrm{x}|_p = \sqrt[3]{|\mathrm{a}|_p} \overline{\overline{\bigwedge}} \sqrt[3]{\frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}}.$$

If $p \equiv 2 \pmod 3$ then each equation $\mathrm{x}^3 = \mathrm{t}^{(\max)}$ (respectively $\mathrm{x}^3 = \mathrm{t}^{(\min)}$) has a unique root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$). Since $3 \mid \log_p |\mathrm{a}|_p$ (respectively $3 \mid \log_p \frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}$) and $-a_0$ (respectively $\frac{b_0}{a_0}$) is a cubic residue, the first digit of the root $\mathrm{x}^{(1)}$ (respectively $\mathrm{x}^{(2)}$) is $x_0^{(1)} \equiv \sqrt[3]{-a_0} \pmod p$ (respectively $x_0^{(2)} \equiv \sqrt[3]{\frac{b_0}{a_0}} \pmod p$) and its norm is $|\mathrm{x}^{(1)}|_p = \sqrt[3]{|\mathrm{a}|_p}$ (respectively $|\mathrm{x}^{(2)}|_p = \sqrt[3]{\frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}}$). If $p \equiv 1 \pmod 3$ then each equation $\mathrm{x}^3 = \mathrm{t}^{(\max)}$ (respectively $\mathrm{x}^3 = \mathrm{t}^{(\min)}$) has two more roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$). The first digits of the roots $\mathrm{x}^{(3)}$ and $\mathrm{x}^{(5)}$ (respectively $\mathrm{x}^{(4)}$ and $\mathrm{x}^{(6)}$) are $x_0^{(2i-1)} \equiv \varepsilon_i \sqrt[3]{-a_0} \pmod p$ (respectively $x_0^{(2i)} \equiv \varepsilon_i \sqrt[3]{\frac{b_0}{a_0}} \pmod p$) and their norms are $|\mathrm{x}^{(2i-1)}|_p = \sqrt[3]{|\mathrm{a}|_p}$ (respectively $|\mathrm{x}^{(2i)}|_p = \sqrt[3]{\frac{|\mathrm{b}|_p}{|\mathrm{a}|_p}}$) for $i = 2, 3$. □

References

1. Borevich Z.I. and Shafarevich I.R., *Number Theory*, Academic, New York (1966).
2. Albeverio S., Khrennikov A.Yu., and Shelkovich V.M., *Theory of p-Adic Distributions: Linear and Nonlinear Models*, Cambridge University, Cambridge (2010).
3. Albeverio S., Cianci R., and Khrennikov A.Yu., "p-Adic valued quantization p-adic numbers," Ultra Anal. Appl., vol. 1, no. 2, 91–104 (2009).
4. Vladimirov V.S., Volovich I.V., and Zelenov E.I., *p-Adic Analysis and Mathematical Physics*, World Sci., Singapore (1994).
5. Volovich I.V., "p-Adic strings," Class. Quantum Gravity, vol. 4, no. 4, 83–87 (1997).
6. Beltrametti E. and Cassinelli G., "Quantum mechanics and p-adic numbers," Found. Phys., vol. 2, no. 1, 1–7 (1972).
7. Khrennikov A.Yu., *p-Adic Valued Distributions in Mathematical Physics*, Kluwer, Dordrecht (1994).
8. Khrennikov A.Yu., *Interpretations of Probability*, De Gruyter, Berlin and New York (2009).
9. Ahmad M.A.K., Liao L., and Saburov M., "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," J. Stat. Phys., vol. 171, no. 6, 1000–1034 (2018).
10. Saburov M. and Ahmad M.A.K., "Quadratic equations over p-adic fields and their application in statistical mechanics," Sci. Asia, vol. 41, no. 3, 209–215 (2015).
11. Saburov M. and Ahmad M.A.K., "On descriptions of all translation invariant p-adic Gibbs measures for the Potts model on the Cayley tree of order three," Math. Phys. Anal. Geom., vol. 18, 1–33 (2015).
12. Georgii H.-O., *Gibbs Measures and Phase Transitions*, De Gruyter, Berlin and New York (2011).
13. Kulske C., Rozikov U.A., and Khakimov R.M., "Description of all translation-invariant splitting Gibbs measures for the Potts model on a Cayley tree," J. Stat. Phys., vol. 156, no. 1, 189–200 (2013).
14. Rozikov U.A., *Gibbs Measures on Cayley Trees*, World Sci., Singapore (2013).
15. Rozikov U., "Gibbs measures on Cayley trees: Results and open problems," Rev. Math. Phys, vol. 25, no. 1 (1330001), 112 (2013).
16. Mukhamedov F. and Saburov M., "On equation $x^q = a$ over $\mathbb{Q}_p$," J. Number Theory, vol. 133, no. 1, 55–58 (2013).
17. Mukhamedov F., Omirov B., and Saburov M., "On cubic equations over p-adic field," Int. J. Number Theory, vol. 10, no. 5, 1171–1190 (2014).
18. Mukhamedov F.M., Omirov B.A., Saburov M.Kh., and Masutova K.K., "Solvability of cubic equations in p-adic integers ($p > 3$)," Sib. Math. J., vol. 54, no. 3, 501–516 (2013).
19. Saburov M. and Ahmad M.A.K., "Local descriptions of roots of cubic equations over p-adic fields," Bull. Malaysian Math. Sci. Soc., vol. 41, no. 2, 965–984 (2018).
20. Saburov M., Ahmad M.A.K., and Alp M., "The study on general cubic equations over p-adic fields," Filomat, vol. 35, no. 4, 1115–1131 (2021).
21. Saburov M. and Ismail M.J., "On square root function over $\mathbb{Q}_p$ and its application," J. Phys. Conf. Ser., vol. 819 (2017) (Article no. 012028, 10 pp.).

M. Alp
College of Engineering and Technology
American University of the Middle East, Egaila, Kuwait
E-mail address: murat.alp@aum.edu.kw

M. Ismail
Department of Computational and Theoretical Sciences
Faculty of Science, International Islamic University Malaysia
Kuantan, Malaysia
E-mail address: ezrathinker@live.com

M. Saburov
College of Engineering and Technology
American University of the Middle East, Egaila, Kuwait
E-mail address: mansur.saburov@aum.edu.kw