RESEARCH ARTICLE
doi: 10.2306/scienceasia1513-1874.2017.43S.001

ScienceAsia 43S (2017): **1–8**

On the solvability of general cubic equations over $\mathbb{Z}_p^*$

Mansoor Saburov*, **Mohd Ali Khameini Ahmad**

Faculty of Science, International Islamic University Malaysia, 25200 Kuantan, Pahang, Malaysia

*Corresponding author, e-mail: msaburov@gmail.com

Received 22 Aug 2014
Accepted 21 May 2017

ABSTRACT: The p-adic models of statistical mechanics require an investigation of the roots of polynomial equations over p-adic fields in order to construct p-adic Gibbs measures. The most frequently asked question is whether a root of a polynomial equation belongs to some given domains. In this paper, we study the solvability of general cubic equations over $\mathbb{Z}_p^*$ where prime $p > 3$. Our investigation enables us to describe all translation invariant p-adic Gibbs measures on a Cayley tree of order three.

KEYWORDS: solvability criterion, p-adic number

INTRODUCTION

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

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

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

where $x = p^k m/n$ with $k, m \in \mathbb{Z}$, $n \in \mathbb{N}$, $\gcd(m, p) = \gcd(n, p) = 1$. A number k is called an *order* of x and is denoted by $\mathrm{ord}_p(x) = k$. Any p-adic number $x \in \mathbb{Q}_p$ can be uniquely represented in the following canonical form:

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

where $x_0 \in \{1, 2, \ldots p-1\}$ and $x_i \in \{0, 1, 2, \ldots p-1\}$, $i \geqslant 1$. We denote the sets of all *p-adic integers* and *units* of $\mathbb{Q}_p$, respectively, by $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}$, and $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}$. Any p-adic unit $x \in \mathbb{Z}_p^*$ has the following unique canonical form: $x = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots$ where $x_0 \in \{1, 2, \ldots p-1\}$ and $x_i \in \{0, 1, 2, \ldots p-1\}$, $i \in \mathbb{N}$. Any non-zero $x \in \mathbb{Q}_p$ has a unique representation $x = x^*/|x|_p$, where $x^* \in \mathbb{Z}_p^*$ (for more details, see Refs. 1–3).

The p-adic models of statistical mechanics require the investigation of roots of polynomial equations over p-adic fields in order to construct p-adic Gibbs measures[4–6]. The most frequently asked question is whether a root of a polynomial equation belongs to the domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \backslash \mathbb{Z}_p^*$, $\mathbb{Z}_p$, $\mathbb{Q}_p \backslash \mathbb{Z}_p^*$, $\mathbb{Q}_p \backslash (\mathbb{Z}_p \backslash \mathbb{Z}_p^*)$, $\mathbb{Q}_p \backslash \mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{S}_{p^m}(0)$ or not[7–9]. This problem has a different solution for the cases $\mathbb{R}$ and $\mathbb{Q}_p$. For instance, $x^2 + 1 = 0$ is not solvable in $\mathbb{R}$ but it is solvable in $\mathbb{Q}_p$ for $p \equiv 1 \pmod 4$. On the other hand, any cubic equation is solvable in $\mathbb{R}$ but the simplest cubic equation $x^3 = p$ is not solvable in $\mathbb{Q}_p$. Hence a solvability criterion over $\mathbb{Q}_p$ should be differently treated from the case $\mathbb{R}$. To the best of our knowledge, in the literature[3,10,11], little attention has been given to this problem. Recently, this problem was studied for monomial equations[12], quadratic equations[13], depressed cubic equations for primes $p > 3$ in Refs. 14–16 and for primes $p = 2, 3$ in Refs. 17–19, and for bi-quadratic equations[20]. The application was presented in Refs. 13, 21. However, this problems was open for general cubic equations. In this paper, we provide the solvability criterion for general cubic equations over the domain $\mathbb{Z}_p^*$ for $p > 3$.

It is worth mentioning that the solvability of general cubic equations over $\mathbb{Z}_p^*$ is completely different from the solvability of depressed cubic equations over $\mathbb{Z}_p^*$ (some examples are given in the next section). That is why we aimed to have the separate study for general cubic equations.

PRELIMINARIES

Throughout this paper, we assume that $p > 3$. Consider the general cubic equation

$$x^3 + ax^2 + bx + c = 0 \qquad (1)$$

where $a, b, c \in \mathbb{Q}_p$. Let $a = a^*/|a|_p$, $b = b^*/|b|_p$, $c = c^*/|c|_p$ where $a^* = a_0 + a_1p + a_2p^2 + \cdots$, $b^* = b_0 + b_1p + b_2p^2 + \cdots$, $c^* = c_0 + c_1p + c_2p^2 + \cdots$, and $a_0, b_0, c_0 \in \{1, 2, \ldots, p-1\}$, $a_i, b_i, c_i \in \{0, 1, \ldots, p-1\}$, $i \geqslant 1$. The general cubic (1) can be reduced to the depressed cubic equation

$$w^3 + Aw = B \tag{2}$$

where $w = x + \frac{1}{3}a$, $A = \frac{1}{3}(3b - a^2)$, and $B = \frac{1}{27}(-2a^3 + 9ab - 27c)$. Let $\Delta = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc = -4A^3 - 27B^2$ be the discriminant of the general cubic (1). At the same time, it is the discriminant of the depressed cubic (2). Let $A = A^*/|A|_p$, $B = B^*/|B|_p$, and $\Delta = \Delta^*/|\Delta|_p$ whenever $AB\Delta \neq 0$, where $\Delta^* = D_0 + D_1p + D_2p^2 + \cdots$, $A^* = A_0 + A_1p + A_2p^2 + \cdots$, $B^* = B_0 + B_1p + B_2p^2 + \cdots$, and $A_0, B_0, D_0 \in \{1, 2, \ldots, p-1\}$, $A_i, B_i, D_i \in \{0, 1, \ldots, p-1\}$, $i \geqslant 1$. The solvability of the general cubic (1) over $\mathbb{Q}_p$ is equivalent to the solvability of the depressed cubic (2) over $\mathbb{Q}_p$. The depressed cubic equation has already been studied in Ref. 14. Hence we can give the solvability criterion of the general (1) in terms of $A, B \in \mathbb{Q}_p$.

Recall that there exists[12] $\sqrt{B}$ (respectively, $\sqrt[3]{B}$) if and only if $B_0^{(p-1)/2} \equiv 1 \pmod p$ (respectively, $B_0^{(p-1)/(3,p-1)} \equiv 1 \pmod p$) and $\log_p |B|_p$ is divisible by 2 (respectively by 3). We shall use the notation $\exists\sqrt{B}$ (respectively, $\exists\sqrt[3]{B}$) whenever there exists $\sqrt{B}$ (respectively, $\sqrt[3]{B}$). We set $D_0 \equiv -4A_0^3 - 27B_0^2 \pmod p$ 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 $n = \overline{1, p-3}$.

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

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

The set $\Phi \subset \mathbb{Q}_p \times \mathbb{Q}_p$ is the solvability domain of the depressed cubic (2) over $\mathbb{Q}_p$[14]. It is clear that the set Φ is also the solvability domain of the general cubic (1) over $\mathbb{Q}_p$. However, the solvability of the general cubic (1) over $\mathbb{Z}_p^*$ is completely different from the solvability of the depressed cubic (2) over $\mathbb{Z}_p^*$.

Example 1 Let $p = 5$. We consider the general cubic equation $x^3 + x^2 - 1 = 0$. If we choose the substitution $w = x + \frac{1}{3}$ then we obtain the depressed cubic equation $w^3 - \frac{1}{3}w = \frac{25}{27}$. Since $\frac{1}{25} = |\frac{25}{27}|_5 < |\frac{1}{3}|_5 = 1$ and there does not exist $1/\sqrt{3}$ in $\mathbb{Q}_5$, the above depressed cubic equation has a unique solution $\bar{w}$ which belongs in $\mathbb{Z}_5\backslash\mathbb{Z}_5^*$[14,16]. This means that this depressed cubic equation is not solvable in $\mathbb{Z}_5^*$. However, the given general cubic equation 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 general cubic equation is solvable in $\mathbb{Z}_5^*$.

Example 2 Let $p = 7$. We consider the general cubic equation $x^3 + 3x^2 + \frac{1}{2}x + 7 = 0$. If we choose the substitution $w = x + 1$ then we obtain the depressed cubic equation $w^3 - \frac{5}{2}w = -\frac{17}{2}$. Since $|\Delta|_7 < |\frac{5}{2}|_7 = |\frac{17}{2}|_7 = 1$ and there does not exist $\sqrt{\Delta}$, the above depressed cubic equation has a unique root $\bar{w} \in \mathbb{Z}_7^*$ such that $\bar{w} \equiv 1 \pmod 7$. However, the given general equation has a unique root $\bar{x} = \bar{w} - 1$ which belongs to $\mathbb{Z}_7\backslash\mathbb{Z}_7^*$. This means that the given general cubic equation is not solvable in $\mathbb{Z}_7^*$.

These two examples show that we have to study the solvability of the general cubic (1) over $\mathbb{Z}_p^*$ separately.

We review some auxiliary results. Consider the following depressed cubic equation in the field $\mathbb{F}_p$ (where $\mathbb{F}_p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$):

$$w^3 + \bar{A}w = \bar{B} \tag{3}$$

where $\bar{A}, \bar{B} \in \mathbb{F}_p$.

Proposition 1 (Ref. 14) *Let $p > 3$ be a prime number and $\bar{A}, \bar{B} \in \mathbb{F}_p$ with $\bar{A}\bar{B} \neq \bar{0}$. Let $\bar{D} = -4\bar{A}^3 - 27\bar{B}^2$ and $u_{n+3} = \bar{B}u_n - \bar{A}u_{n+1}$ for $n \in \mathbb{N}$ with $u_1 = \bar{0}$, $u_2 = -\bar{A}$, $u_3 = \bar{B}$. If $N_{\mathbb{F}_p}(w^3 + \bar{A}w - \bar{B})$ is the number of the roots of (3) then the following holds true:*

$$N_{\mathbb{F}_p}(w^3 + \bar{A}w - \bar{B}) = \begin{cases} 3, & \bar{D}u_{p-2}^2 = \bar{0}, \\ 0, & \bar{D}u_{p-2}^2 = 9\bar{A}^2, \\ 1, & \bar{D}u_{p-2}^2 \neq \bar{0}, 9\bar{A}^2 \end{cases}$$

Proposition 2 (Ref. 14) *Let $p > 3$ be a prime number with $\bar{A}, \bar{B} \in \mathbb{F}_p$, $\bar{A}\bar{B} \neq \bar{0}$. Let $\bar{D} = -4\bar{A}^3 - 27\bar{B}^2$ and $u_{n+3} = \bar{B}u_n - \bar{A}u_{n+1}$ with $\bar{D}u_{p-2}^2 \neq 9\bar{A}^2$, $u_1 = \bar{0}$, $u_2 = -\bar{A}$, $u_3 = \bar{B}$.*

I *Let $\bar{D}u_{p-2}^2 = \bar{0}$. Then the following statements hold true.*

I.1 *Eq. (3) has 3 distinct solutions in $\mathbb{F}_p$ if and only if $\bar{D} \neq \bar{0}$. Moreover, $3\bar{w}^2 + \bar{A} \neq 0$ for any root $\bar{w}$.*

I.2 *Eq. (3) has 2 distinct solutions in $\mathbb{F}_p$ while one of them is of multiplicity 2 if and only if $\bar{D} = \bar{0}$. If $\bar{w}_1$, $\bar{w}_2$ are 2 distinct solutions while if $\bar{w}_1$ is a multiple solution then $\bar{w}_1 = 3\bar{B}/2\bar{A}$, $\bar{w}_2 = -3\bar{B}/\bar{A}$, $3\bar{w}_2^2 + \bar{A} \neq \bar{0}$.*

I.3 *Eq.* (3) *does not have any solution of multiplicity* 3.

II *Let* $\bar{D}u_{p-2}^2 \neq \bar{0}$, $9\bar{A}^2$. *If* $\bar{w}$ *is a solution of* (3) *then* $3\bar{w}^2+\bar{A} \neq \bar{0}$.

Remark 1 From Proposition 2 one may conclude that under the assumption of Proposition 2, there always exists at least one solution $\bar{w}$ of (3) such that $3\bar{w}^2+\bar{A} \neq \bar{0}$.

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

Proposition 3 *Let* p *be any prime. Suppose the general cubic* (1) *is solvable in* $\mathbb{Z}_p^*$ *where* $a, b, c \in \mathbb{Q}_p$. *Then the following statements hold true:*
(i) *if* $|M(\mathscr{S})| = 1$ *then* $\max(\mathscr{S}) = 1$;
(ii) *if* $|M(\mathscr{S})| \geqslant 2$ *then* $\max(\mathscr{S}) \geqslant 1$.

Proof: Let the general cubic (1) be solvable in $\mathbb{Z}_p^*$. One can obtain

$$|a|_p = |ax^2|_p = |x^3+bx+c| \leqslant \max\{1, |b|_p, |c|_p\},$$
$$|b|_p = |bx|_p = |x^3+ax^2+c| \leqslant \max\{1, |a|_p, |c|_p\},$$
$$|c|_p = |x^3+ax^2+bx| \leqslant \max\{1, |a|_p, |b|_p\},$$
$$1 = |x^3|_p = |ax^2+bx+c| \leqslant \max\{|a|_p, |b|_p, |c|_p\}.$$

Thus if $|M(\mathscr{S})| = 1$ 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 $|M(\mathscr{S})| = 2$ then $|a|_p < |b|_p = |c|_p$ with $|b|_p = |c|_p \geqslant 1$ or $|b|_p < |a|_p = |c|_p$ with $|a|_p = |c|_p \geqslant 1$ or $|c|_p < |a|_p = |b|_p$ with $|a|_p = |b|_p \geqslant 1$, if $|M(\mathscr{S})| = 3$ then $|a|_p = |b|_p = |c|_p \geqslant 1$. □

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

Lemma 1 (Hensel's lemma [1]) *Let* f *be a polynomial whose coefficients are p-adic integers. Let* θ *be a p-adic integer such that for some* $i \geqslant 0$ *we have* $f(\theta) \equiv 0 \pmod{p^{2i+1}}$, $f'(\theta) \equiv 0 \pmod{p^i}$, $f'(\theta) \not\equiv 0 \pmod{p^{i+1}}$. *Then* f *has a unique p-adic integer root* x_0 *which satisfies* $x_0 \equiv \theta \pmod{p^{i+1}}$.

SOLVABILITY CRITERION OVER $\mathbb{Z}_p^*$

We introduce some notation. Let $\delta_1 = b^2-4ac$, $\delta_2 = a^2-4b$, $\delta_3 = -2a^3-27c$, $A = \frac{1}{3}(3b-a^2)$, $B = \frac{1}{27}(-2a^3+9ab-27c)$, and $\Delta = a^2b^2-4a^3c-4b^3-27c^2+18abc = -4A^3-27B^2$. We set $D_0 \equiv -4A_0^3-27B_0^2 \pmod{p}$ 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 $n = \overline{1, p-3}$.

Theorem 1 *Let* $p > 3$ *and* $|M(\mathscr{S})| = 1$. *Then the general cubic* (1) *is solvable in* $\mathbb{Z}_p^*$ *if and only if one of the following conditions holds true:*
I. $|a|_p = 1$, $|b|_p < 1$, $|c|_p < 1$;
II. $|b|_p = 1$, $|a|_p < 1$, $|c|_p < 1$ *and* $\exists\sqrt{-b}$;
III. $|c|_p = 1$, $|a|_p < 1$, $|b|_p < 1$, *and* $\exists\sqrt[3]{-c}$.

Proof: Let $|M(\mathscr{S})| = 1$. From Proposition 3, if the general cubic (1) is solvable in $\mathbb{Z}_p^*$ then $\max(\mathscr{S}) = 1$. It means that we have one of the following conditions: $|a|_p \neq |b|_p \neq |c|_p$ 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 these case by case. Suppose that $f_{a,b,c}(x) = x^3+ax^2+bx+c$.

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

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

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

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

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

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

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

Theorem 2 *Let $p > 3$ and $|M(\mathscr{S})| = 2$. Then the general cubic (1) is solvable in $\mathbb{Z}_p^*$ if and only if one of the following conditions holds true:*
I. $|a|_p < |b|_p = |c|_p$, $|b|_p = |c|_p > 1$;
II. $|b|_p < |a|_p = |c|_p$, $|a|_p = |c|_p > 1$, $\exists\sqrt{-ac}$;
III. $|c|_p < |a|_p = |b|_p$, $|a|_p = |b|_p > 1$;
IV. $|a|_p < |b|_p = |c|_p = 1$, $D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$;
V. $|b|_p < |a|_p = |c|_p = 1$, *and*
(i) $|\delta_3|_p < 1$, *or*
(ii) $|\delta_3|_p = 1$, $D_0u_{p-2}^2 \not\equiv a_0^4 \pmod p$;
VI. $|c|_p < |a|_p = |b|_p = 1$, *and*
(i) $|c|_p < |\delta_2|_p$, $\exists\sqrt{\delta_2}$, *or*
(ii) $|c|_p = |\delta_2|_p$, $\exists\sqrt{\Delta}$, *or*
(iii) $|c|_p > |\delta_2|_p$, $\exists\sqrt{2ac}$.

Proof: Let $|M(\mathscr{S})| = 2$. From Proposition 3, if the general cubic (1) is solvable in $\mathbb{Z}_p^*$ then $\max(\mathscr{S}) \geqslant 1$. It means that we have one of the following conditions: $|a|_p < |b|_p = |c|_p$ with $|b|_p = |c|_p \geqslant 1$, or $|b|_p < |a|_p = |c|_p$ with $|a|_p = |c|_p \geqslant 1$, or $|c|_p < |a|_p = |b|_p$ with $|a|_p = |b|_p \geqslant 1$.

Case I. Let $|a|_p < |b|_p = |c|_p$, $|b|_p = |c|_p > 1$. We want to show that the general cubic (1) is solvable in $\mathbb{Z}_p^*$. Since $|b|_p = |c|_p = p^k$ for some $k \geqslant 1$, 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 vice versa. On the other hand, the second cubic equation is suitable for applying Hensel's lemma to. Let us choose $\bar{x}$ such that $b_0\bar{x} + c_0 \equiv 0 \pmod p$. Let $g_{b,c}(x) = p^kx^3 + p^kax + b^*x + c^*$. We have $g_{b,c}(\bar{x}) \equiv b_0\bar{x} + c_0 \equiv 0 \pmod p$ and $g'_{b,c}(\bar{x}) \equiv b_0 \not\equiv 0 \pmod p$. From Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $g_{b,c}(x) = 0$ and $x \equiv \bar{x} \pmod p$. Since $\bar{x} \not\equiv 0 \pmod p$, we have $x \in \mathbb{Z}_p^*$.

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

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

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

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

Let us choose $\bar{x}$ such that $a_0\bar{x}+b_0 \equiv 0 \pmod p$. Suppose that $g_{a,b}(x) = p^kx^3 + a^*x^2 + b^*x + p^kc$. We then have $g_{a,b}(\bar{x}) \equiv \bar{x}(a_0\bar{x} + b_0) \equiv 0 \pmod p$ and $g'_{a,b}(\bar{x}) \equiv 2a_0\bar{x} + b_0 \equiv a_0\bar{x} \not\equiv 0 \pmod p$. From Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $g_{a,b}(x) = 0$ and $x \equiv \bar{x} \pmod p$. Since $\bar{x} \not\equiv 0 \pmod p$, we have $x \in \mathbb{Z}_p^*$.

Case IV. Let $|a|_p < |b|_p = |c|_p = 1$. We want to show that the general cubic (1) is solvable in $\mathbb{Z}_p^*$ if and only if $D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$.

If part. Let $x \in \mathbb{Z}_p^*$ be a solution of the general cubic (1). Then we have $x_0^3 + b_0x_0 + c_0 \equiv 0 \pmod p$. From Proposition 1, since the last equation is solvable in $\mathbb{F}_p$ (x_0 is a solution), it follows that $D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$.

Only if part. We assume that $D_0u_{p-2}^2 \not\equiv 9b_0^2 \pmod p$. From Proposition 2, there exists $\bar{x}$ such that $\bar{x}^3 + b_0x_0 + c_0 \equiv 0 \pmod p$ and $3\bar{x}^2 + b_0 \not\equiv 0 \pmod p$. We can obtain $f_{a,b,c}(\bar{x}) \equiv \bar{x}^3 + b_0\bar{x} + c_0 \equiv 0 \pmod p$ and $f'_{a,b,c}(\bar{x}) \equiv 3\bar{x}^2 + b_0 \not\equiv 0 \pmod p$. From Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b,c}(x) = 0$ and $x \equiv \bar{x} \pmod p$. Since $\bar{x} \not\equiv 0 \pmod p$, we have $x \in \mathbb{Z}_p^*$.

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

Case V(i). Let $|\delta_3|_p < 1$. In this case, we want to show that the general cubic (1) is solvable over $\mathbb{Z}_p^*$. We then have $|B|_p < |A|_p = 1$. In this case[14],

the depressed cubic equation $w^3+Aw=B$ is always solvable and one of its solutions w_1 is in $\mathbb{Z}_p\backslash\mathbb{Z}_p^*$. Since $|x|_p=|w_1-\frac{1}{3}a|=1$, the general cubic (1) is solvable over $\mathbb{Z}_p^*$.

Case V(ii). Let $|\delta_3|_p=1$. We want to show that the general cubic (1) is solvable over $\mathbb{Z}_p^*$ if and only if $D_0u_{p-2}^2\not\equiv a_0^4 \pmod p$. In this case, one can see $|B|_p=|A|_p=1$. We then have $D_0\equiv -4A_0^3-27B_0^2 \pmod p$, $3A_0\equiv -a_0^2 \pmod p$, and $27B_0\equiv -2a_0^3-27c_0 \pmod p$. In this case[14], the depressed cubic equation $w^3+Aw=B$ is solvable if and only if $D_0u_{p-2}^2\not\equiv 9A_0^2\equiv a_0^4 \pmod p$. Moreover, all solutions of the above depressed cubic equation belong to $\mathbb{Z}_p^*$. We now want to show that all solutions of the general cubic (1) such that $x=w-\frac{1}{3}a$ also belong to the set $\mathbb{Z}_p^*$. Equivalently, we want to show that $3w\not\equiv a \pmod p$.

Suppose the contrary, i.e., $3w\equiv a \pmod p$. One can obtain $(3w)^3+3(3b-a^2)(3w)-(-2a^3+9ab-27c)\equiv a_0^3-3a_0^3+2a_0^3+27c_0 \pmod p\equiv 27c_0\not\equiv 0 \pmod p$ which contradicts the fact that w is a root of the depressed cubic equation. Hence we have that $3w\not\equiv a \pmod p$ or $|x|_p=|w-\frac{1}{3}a|=1$. Consequently, all solutions of the general cubic (1) belong to $\mathbb{Z}_p^*$.

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

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

Case VI(i). Assume $|c|_p<|\delta_2|_p$. We want to show that the cubic (1) 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 (1). We know that $c=p^kc^*$, $\delta_2=p^l\delta_2^*$ where $k>l\geqslant 0$ and $c^*,\delta_2^*\in\mathbb{Z}_p^*$. We have from (4) that $|2x+a|_p^2=|x(2x+a)^2|_p=|x\delta_2-4c|_p=|\delta_2|_p$. Hence we can write $l=2m$ where m is the integer such that $|2x+a|_p=p^{-m}$. We then obtain $2x+a=p^m(2x+a)^*$ where $(2x+a)^*\in\mathbb{Z}_p^*$. We obtain from (4) that $x[(2x+a)^*]^2-x\delta_2^*+4p^{k-2m}c^*=0$. Since $k-2m=k-l\geqslant 1$ and $x\in\mathbb{Z}_p^*$, we have that $[(2x+a)^*]^2\equiv\delta_2^* \pmod p$. Thus there exists $\sqrt{\delta_2}$.

Only if part. Assume that there exists $\sqrt{\delta_2}$. We choose $\bar{x}$ and ∇ such that $2\bar{x}+a\equiv p^m\nabla \pmod{p^{m+1}}$ and $\nabla^2\equiv\delta_2^* \pmod p$. Then $(2\bar{x}+a)^2-\delta_2\equiv 0 \pmod{p^{2m+1}}$. Suppose that $f_{a,b,c}(x)=x^3+ax^2+bx+c$. We then obtain $4f_{a,b,c}(\bar{x})=\bar{x}((2\bar{x}+a)^2-\delta_2)+4c\equiv 0 \pmod{p^{2m+1}}$ and $4f'_{a,b,c}(\bar{x})=(2\bar{x}+a)^2-\delta_2+4\bar{x}(2\bar{x}+a)\equiv 0 \pmod{p^m}$ with $4f'_{a,b,c}(\bar{x})\equiv 4\bar{x}(2\bar{x}+a)\not\equiv 0 \pmod{p^{m+1}}$. From Hensel's lemma, there exists $x\in\mathbb{Z}_p$ such that $f_{a,b,c}(x)=0$ and $x\equiv\bar{x} \pmod{p^{m+1}}$. Since $\bar{x}\not\equiv 0 \pmod p$, we have that $x\in\mathbb{Z}_p^*$.

Case VI(ii). Let $|c|_p=|\delta_2|_p$. We want to show that the general cubic (1) 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 $w=x+\frac{1}{3}a$, $A=\frac{1}{3}(3b-a^2)$, and $B=\frac{1}{27}(-2a^3+9ab-27c)$. Then $|A|_p=|-\delta_2-b|_p=1$, $|B|_p=|ab-2a\delta_2-27c|_p=1$.

We also obtain $3A_0\equiv -b_0 \pmod p$, $27B_0\equiv a_0b_0 \pmod p$ and $27D_0\equiv 27(-4A_0^3-27B_0^2)\equiv -4(3A_0)^3-(27B_0)^2\equiv b_0^2(4b_0-a_0^2)\equiv 0 \pmod p$. Then the depressed cubic equation $w^3+Aw=B$ is always solvable and all solutions belong to $\mathbb{Z}_p^*$ [14]. Moreover, we have that [14]

(C_1) If $\Delta=0$ then $w_1=-3B/A$, $w_2=w_3=3B/2A$ are solutions of the cubic equation $w^3+Aw=B$.

(C_2) 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 $w_1\equiv -(3B/A) \pmod p$ and $w_2\equiv w_3\equiv(3B/2A) \pmod p$.

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

Let us analyse each case. Suppose that there exists $\sqrt{\Delta}$. We want to show that $|w_1-\frac{1}{3}a|_p<1$ and $|w_2-\frac{1}{3}a|_p=|w_3-\frac{1}{3}a|_p=1$. Since $9Aw_1\equiv -27B \pmod p$ and $9A\equiv -3b_0 \pmod p$, $-27B\equiv -a_0b_0 \pmod p$, we obtain $3w_1\equiv a_0 \pmod p$, i.e., $|w_1-\frac{1}{3}a|_p<1$.

Suppose the contrary, i.e., $3w_2\equiv 3w_3\equiv a \pmod p$. Since $18Aw_2\equiv 18Aw_3\equiv 27B \pmod p$ and $9A\equiv -3b_0 \pmod p$, $27B\equiv a_0b_0 \pmod p$, we obtain $-6w_2\equiv -6w_3\equiv a_0 \pmod p$. It shows that $9w_2\equiv 9w_3\equiv 0 \pmod p$ which contradicts $w_2,w_3\in\mathbb{Z}_p^*$. Thus $3w_2\equiv 3w_3\not\equiv a \pmod p$ and $|w_2-\frac{1}{3}a|_p=|w_3-\frac{1}{3}a|_p=1$.

Suppose that there does not exist $\sqrt{\Delta}$. By the same argument, we have $|w_1-\frac{1}{3}a|<1$. Hence if there exists $\sqrt{\Delta}$ then the general cubic (1) has solutions x_1, x_2, x_3 in which $|x_1|_p=|w_1-\frac{1}{3}a|_p<1$, $|x_2|_p=|w_2-\frac{1}{3}a|_p=1$, and $|x_3|_p=|w_3-\frac{1}{3}a|_p=1$. This means that the general cubic (1) is solvable in $\mathbb{Z}_p^*$. If there does not exist $\sqrt{\Delta}$ then the general cubic (1) has a unique solution x_1 in which $|x_1|_p=|w_1-\frac{1}{3}a|_p<1$. This means that the general cubic (1) is not solvable in $\mathbb{Z}_p^*$. Consequently, the general cubic (1) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\Delta}$.

Case VI(iii). We assume $|c|_p > |\delta_2|_p$. We want to show that the general cubic (1) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{2ac}$.

If part. Let $x \in \mathbb{Z}_p^*$ be a solution of the cubic (1). We know that $c = p^k c^*$, $\delta_2 = p^l \delta_2^*$ where $l > k \geqslant 1$ and c^*, $\delta_2^* \in \mathbb{Z}_p^*$. We then deduce from (4) that $|2x+a|_p^2 = |x(2x+a)^2|_p = |x\delta_2 - 4c|_p = |c|_p$. Hence $k = 2m$ and $2x+a = p^m\nabla$ where $\gcd(\nabla, p) = 1$. We obtain from (4) that $2x\nabla^2 - 2xp^{l-2m}\delta_2^* + 8c^* = 0$. Since $l - 2m = l - k \geqslant 1$, we obtain $a\nabla^2 \equiv 8c^* \pmod p$ or $(a\nabla)^2 \equiv 8ac^* \pmod p$. It means that there exists $\sqrt{2ac}$.

Only if part. Suppose that there exists $\sqrt{2ac}$. We choose $\bar{x}$ such that $2\bar{x}+a = p^m\nabla$ and $(\nabla, p) = 1$ $a\nabla^2 \equiv 8c^* \pmod p$. Then $2\bar{x}(2\bar{x}+a)^2 + 8c \equiv 0 \pmod{p^{2m+1}}$. We have that $8f_{a,b,c}(\bar{x}) = 2\bar{x}(2\bar{x}+a)^2 - 2\bar{x}\delta_2 + 8c \equiv 0 \pmod{p^{2m+1}}$ and $8f'_{a,b,c}(\bar{x}) = 2[(2\bar{x}+a)^2 - \delta_2] + 8\bar{x}(2\bar{x}+a) \equiv 8\bar{x}(2\bar{x}+a) \equiv 0 \pmod{p^m}$ but $8f'_{a,b,c}(\bar{x}) \not\equiv 0 \pmod{p^{m+1}}$. From Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $f_{a,b,c}(x) = 0$ and $x \equiv \bar{x} \pmod{p^{m+1}}$. Since $\bar{x} \not\equiv 0 \pmod p$, we have that $x \in \mathbb{Z}_p^*$. □

Theorem 3 *Let $p > 3$ and $|M(\mathscr{S})| = 3$. Then the general cubic (1) is solvable in $\mathbb{Z}_p^*$ if and only if one of the following conditions holds:*

I. $|a|_p = |b|_p = |c|_p > 1$ *and*
   (i) $|\delta_1|_p > |a|_p = |b|_p = |c|_p$, $\exists\sqrt{\delta_1}$, *or*
   (ii) $|\delta_1|_p = |a|_p = |b|_p = |c|_p$, $\exists\sqrt{\Delta}$, *or*
   (iii) $|\delta_1|_p < |a|_p = |b|_p = |c|_p$, $\exists\sqrt{2b}$;
II. $|a|_p = |b|_p = |c|_p = 1$, $(A, B) \in \Phi$.

Proof: Let $|M(\mathscr{S})| = 3$. We know that, from Proposition 3, if the general cubic (1) is solvable in $\mathbb{Z}_p^*$ then $\max(\mathscr{S}) \geqslant 1$. It means that $|a|_p = |b|_p = |c|_p \geqslant 1$.

Case I. 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 $k \geqslant 1$. Let $\delta_1 = b^2 - 4ac = p^{-2k}\psi$ where $\psi = (b^*)^2 - 4a^*c^*$. We can rewrite the general cubic (1) as $p^k x^3 + a^*x^2 + b^*x + c^* = 0$. We obtain from the last equation that

$$4a^*p^kx^3 + (2a^*x + b^*)^2 - \psi = 0, \quad (5)$$

$$p^k(2a^*x)^3 + 2(a^*)^2[(2a^*x + b^*)^2 - \psi] = 0. \quad (6)$$

Case I(i). Assume that $|\delta_1|_p > |a|_p = |b|_p = |c|_p$. It means that $|\psi|_p > 1/|a|_p = 1/|b|_p = 1/|c|_p$. We want to show that the cubic (1) 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 (1). Let $\psi = p^l\psi^*$ where $k > l \geqslant 0$. We deduce from (5) that $|2a^*x + b^*|_p^2 = |\psi - 4a^*p^kx^3|_p = |\psi|_p$. Hence $l = 2m$ and $2a^*x + b^* = p^m\nabla$ where $(\nabla, p) = 1$. We then deduce from (6) that $p^{k-2m}(2a^*x)^3 + 2(a^*)^2[\nabla^2 - \psi^*] = 0$. Since $k - 2m = k - l \geqslant 1$ and $2(a^*)^2 \in \mathbb{Z}_p^*$, we obtain $\nabla^2 \equiv \psi^* \pmod p$. 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 $2a^*\bar{x} + b^* \equiv p^m\nabla \pmod{p^{m+1}}$, $\nabla^2 \equiv \psi^* \pmod p$ and $(2a^*\bar{x} + b^*)^2 - \psi \equiv 0 \pmod{p^{2m+1}}$. Suppose that $\bar{f}_{a,b,c}(x) = p^kx^3 + a^*x^2 + b^*x + c^*$. We then have that $(2a^*)^3\bar{f}_{a,b,c}(\bar{x}) = p^k(2a^*\bar{x})^3 + 2(a^*)^2[(2a^*\bar{x} + b^*)^2 - \psi] \equiv 0 \pmod{p^{2m+1}}$ and $(2a^*)^3\bar{f}'_{a,b,c}(\bar{x}) \equiv (2a^*)^3(2a^*\bar{x} + b^*) \equiv 0 \pmod{p^m}$ but $(2a^*)^3\bar{f}'_{a,b,c}(\bar{x}) \not\equiv 0 \pmod{p^{m+1}}$. From Hensel's lemma, there exists $x \in \mathbb{Z}_p$ such that $\bar{f}_{a,b,c}(x) = 0$ and $x \equiv \bar{x} \pmod{p^{m+1}}$. Since $\bar{x} \not\equiv 0 \pmod p$, we have $x \in \mathbb{Z}_p^*$.

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

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

We have $3\bar{A}_0 \equiv -a_0^2 \pmod p$, $27\bar{B}_0 \equiv -2a_0^3 \pmod p$, and $27\bar{D}_0 \equiv -4(3A_0)^3 - (27B_0)^2 \equiv 0 \pmod p$. Then the depressed cubic equation $z^3 + \bar{A}z - \bar{B} = 0$ is always solvable and all its solutions belong to $\mathbb{Z}_p^*$ [14]. Moreover, we have that [14]

(C_1) If $\bar{D} = 0$ then $z_1 = -3B/A$, $z_2 = z_3 = 3B/2A$ are solutions of the cubic equation $z^3 + \bar{A}z - \bar{B} = 0$.

(C_2) Let $0 < |\bar{D}|_p < 1$.
   (a) If there exists $\sqrt{\bar{D}}$ then the cubic equation $z^3 + \bar{A}z - \bar{B} = 0$ has three solutions z_1, z_2, z_3 such that $z_1 \equiv -(3\bar{B}/\bar{A}) \pmod p$ and $z_2 \equiv z_3 \equiv (3\bar{B}/2\bar{A}) \pmod p$.
   (b) If there does not exist $\sqrt{\bar{D}}$ then the cubic equation $z^3 + \bar{A}z - \bar{B} = 0$ has a unique solutions z_1 such that $z_1 \equiv -(3\bar{B}/\bar{A}) \pmod p$.

Since $\bar{D} = p^{2k}\psi[(a^*)^2 - 4p^kb^*] + 2p^{3k}a^*b^*c^* - 27p^{4k}(c^*)^2$ and $|\psi|_p = p^{-k}$, we then have that $|\bar{D}|_p \leqslant p^{-3k}$. If $|\bar{D}|_p = p^{-L}$ then $L \geqslant 3k$.

Suppose that there exists $\sqrt{\bar{D}}$. Then $z_1 \equiv -(3\bar{B}/\bar{A}) \pmod p$, $2\bar{A}z_2 - 3\bar{B} \equiv p^lt_1^2 \pmod{p^{l+1}}$ and

$2\bar{A}z_3-3\bar{B}\equiv p^l t_2^2 \pmod{p^{l+1}}$ where $l=\frac{1}{2}L$. We want to show that $|z_1-\frac{1}{3}a^*|_p=1$ and $|z_2-\frac{1}{3}a^*|_p=|z_3-\frac{1}{3}a^*|_p=1/p^k$. Indeed, we obtain $3z_1-a^*\equiv(3(a^*)^3-12p^k a^*b^*+27p^{2k}c^*)/3\bar{A}\equiv 3(a^*)^3\not\equiv 0 \pmod p$. On the other hand, since L is even and $L\geqslant 3k\geqslant 2k+1$, we obtain $2l=L\geqslant 2k+2$ or $l\geqslant k+1$. We then have that $6\bar{A}z_2-2\bar{A}a^*\equiv 3(2\bar{A}z_2-3\bar{B})-(2\bar{A}a^*-9\bar{B})\equiv -(2\bar{A}a^*-9\bar{B})\equiv -9p^{2k}c^*+p^k a^*b^*\equiv p^k a^*b^*\not\equiv 0 \pmod{p^{k+1}}$. It means that $|z_2-\frac{1}{3}a^*|_p=1/p^k$. Similarly, we can obtain $|z_3-\frac{1}{3}a^*|_p=1/p^k$. Hence we have $|x_1|_p=|(z_1-\frac{1}{3}a^*)/p^k|_p=p^k>1$ and $|x_2|_p=|x_3|_p=|(z_2-\frac{1}{3}a^*)/p^k|_p=1$.

If there does not exist $\sqrt{\bar{D}}$ then $z_1\equiv -(3\bar{B}/\bar{A}) \pmod p$ and $|z_1-\frac{1}{3}a|_p=1$ or equivalently $|x_1|_p=p^k$. Hence the general cubic (1) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\bar{D}}$. Since $\bar{D}=p^{6k}\Delta$, there exists $\sqrt{\bar{D}}$ if and only if so does $\sqrt{\Delta}$. Consequently, the general cubic (1) is solvable in $\mathbb{Z}_p^*$ if and only if there exists $\sqrt{\Delta}$.

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

If part. Let $x\in\mathbb{Z}_p^*$ be a solution of the cubic (1). Let $\psi=p^l\psi^*$ where $l>k\geqslant 1$. We obtain from (5) that $|2a^*x+b^*|_p^2=|\psi-4a^*p^k x^3|_p=p^{-k}$. Hence $k=2m$ and $2a^*x+b^*=p^m\nabla$ where $(\nabla,p)=1$. We then obtain from (6) that $(p^m\nabla-b^*)^3+2(a^*\nabla)^2-2(a^*)^2p^{l-2m}\psi^*=0$. Since $l-2m=l-k\geqslant 1$, we obtain $2(a^*\nabla)^2\equiv(b^*)^3 \pmod p$. It means that there exists $\sqrt{2b}$.

Only if part. Suppose there exists $\sqrt{2b}$. We choose $\bar{x}$ such that $2a^*\bar{x}+b^*=p^m\nabla$ where $(\nabla,p)=1$, $2(a^*\nabla)^2\equiv(b^*)^3 \pmod p$. Then $p^k(2a^*\bar{x})^3+2(a^*)^2(2a^*\bar{x}+b^*)^2\equiv 0 \pmod{p^{2m+1}}$. Suppose that $\bar{f}_{a,b,c}(x)=p^kx^3+a^*x^2+b^*x+c^*$. We then have $(2a^*)^3\bar{f}_{a,b,c}(\bar{x})=p^k(2a^*\bar{x})^3+2(a^*)^2(2a^*\bar{x}+b^*)^2-2(a^*)^2\psi\equiv 0 \pmod{p^{2m+1}}$ and $(2a^*)^3\bar{f}'_{a,b,c}(\bar{x})\equiv(2a^*)^3(2a^*\bar{x}+b^*)\equiv 0 \pmod{p^m}$ but $(2a^*)^3\bar{f}'_{a,b,c}(\bar{x})\not\equiv 0 \pmod{p^{m+1}}$. From Hensel's lemma, there exists $x\in\mathbb{Z}_p$ such that $\bar{f}_{a,b,c}(x)=0$ and $x\equiv\bar{x} \pmod{p^{m+1}}$. Since $\bar{x}\not\equiv 0 \pmod p$, we have that $x\in\mathbb{Z}_p^*$.

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

From Ref. 14, 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 $w^3+Aw=B$ are in $\mathbb{Z}_p\backslash\mathbb{Z}_p^*$. In this case, since $x=w-\frac{1}{3}a$, it implies that all solutions of the general cubic (1) belong to $\mathbb{Z}_p^*$.

Let $|A|_p<|B|_p=1$, $(A,B)\in\Phi$. We want to show that for any solution x one has that $|x|_p=|w-\frac{1}{3}a|_p=1$ or $3w\not\equiv a \pmod p$. Suppose the contrary, i.e., $3w\equiv a \pmod p$. One can obtain $(3w)^3+3(3b-a^2)(3w)-(-2a^3+9ab-27c)\equiv a^3+2a^3-9ab+27c\equiv 3a(a^2-3b)+27c\equiv 27c\not\equiv 0 \pmod p$ which contradicts the fact that w is a root of the depressed cubic equation. Hence all solutions of the general cubic (1) belong to $\mathbb{Z}_p^*$.

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

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

CONCLUSIONS

In this paper, we have studied the solvability of the general cubic equation over the domain $\mathbb{Z}_p^*$. In general, the solvability criterion of the general cubic equation over $\mathbb{Z}_p^*$ is completely different from the solvability criterion of the depressed cubic equation over $\mathbb{Z}_p^*$. Some examples are also presented for that purpose. The study will be continued for other domains elsewhere in the future.

Acknowledgements: This work has been supported by the MOHE grant ERGS13-025-0058.

REFERENCES

1. Borevich ZI, Shafarevich IR (1966) *Number Theory*, Academic Press.
2. Gouvea FQ (1997) *p-adic Numbers: An Introduction*, Springer-Verlag.
3. Koblitz N (1984) *p-adic Numbers, p-adic Analysis, and Zeta Functions*, Springer.
4. Khrennikov AYu (1991) *p*-adic quantum mechanics with *p*-adic valued functions. *J Math Phys* **32**, 932–6.

5. Khrennikov AYu (1994) *p-adic Valued Distributions in Mathematical Physics*, Kluwer.
6. Ludkovsky S, Khrennikov A (2003) Stochastic processes on non-Archimedean spaces with values in non-Archimedean fields. *Markov Process Relat Field* **9**, 131–62.
7. Mukhamedov F (2013) On dynamical systems and phase transitions for q+1-state p-adic Potts model on the Cayley tree. *Math Phys Anal Geom* **16**, 49–87.
8. Mukhamedov F, Akin H (2013) Phase transitions for p-adic Potts model on the Cayley tree of order three. *J Stat Mech* **07**, P07014.
9. Mukhamedov F, Rozikov U (2004) On Gibbs measures of p-adic Potts model on Cayley tree. *Indagat Math* **15**, 85–100.
10. Lang S (1994) *Algebraic Number Theory*, Springer-Verlag.
11. Serre JP (1979) *Local Fields*, Springer-Verlag.
12. Mukhamedov F, Saburov M (2013) On equation $x^q = a$ over $\mathbb{Q}_p$. *J Number Theor* **133**, 55–8.
13. Saburov M, Ahmad MAKh (2015) Quadratic equations over p-adic fields and their applications in statistical mechanics. *Sci Asia* **41**, 209–15.
14. Mukhamedov F, Omirov B, Saburov M (2014) On cubic equations over p-adic field. *Int J Number Theor* **10**, 1171–90.
15. Mukhamedov F, Omirov B, Saburov M, Masutova K (2013) Solvability of cubic equations in p-adic integers, $p > 3$. *Siberian Math J* **54**, 501–16.
16. Saburov M, Ahmad MAKh (2016) Local descriptions of roots of cubic equations over p-adic fields. *Bull Malays Math Sci Soc* (in press). doi:10.1007/s40840-016-0401-8
17. Saburov M, Ahmad MAKh (2014) Solvability criteria for cubic equations over $\mathbb{Z}_2^*$. *AIP Conf Proc* **1602**, 792–7.
18. Saburov M, Ahmad MAKh (2015) Solvability of cubic equations over $\mathbb{Q}_3$. *Sains Malays* **44**, 635–41.
19. Saburov M, Ahmad MAKh (2015) The number of solutions of cubic equations over $\mathbb{Q}_3$. *Sains Malays* **44**, 765–9.
20. Saburov M, Ahmad MAKh (2016) Solvability and number of roots of bi-quadratic equations over p-adic fields. *Malays J Math Sci* **10S**, 15–35.
21. Saburov M, Ahmad MAKh (2015) 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* **18**, 1–33.