Sains Malaysiana 44(4)(2015): 635–641

Solvability of Cubic Equations over $\mathbb{Q}_3$

(Kebolehselesaian Persamaan Kubik ke atas $\mathbb{Q}_3$)

MANSOOR SABUROV* & MOHD ALI KHAMEINI AHMAD

ABSTRACT

We provide a solvability criterion for a cubic equation in domains $\mathbb{Z}_3^*$, $\mathbb{Z}_3$, *and* $\mathbb{Q}_3$.

Keywords: Cubic equation; p-adic number; solvability criterion

ABSTRAK

Kami memberi kriteria kebolehselesaian untuk persamaan kubik dalam domain $\mathbb{Z}_3^*$, $\mathbb{Z}_3$, *dan* $\mathbb{Q}_3$.

Kata kunci: Kriteria kebolehselesaian; nombor p-adic; persamaan kubik

INTRODUCTION

This study is a continuation of papers Mukhamedov et al. (2014, 2013), Mukhamedov and Saburov (2013) and Saburov and Ahmad (2014) where a solvability criterion for a cubic equation over the p–adic field $\mathbb{Q}_p$, where $p \neq 3$, was provided. In this paper, we shall provide a solvability criterion for the cubic equation over domains, $\mathbb{Z}_3^*$, $\mathbb{Z}_3$, *and* $\mathbb{Q}_3$.

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

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

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

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

Any p–adic number $x \in \mathbb{Q}_p$ can be uniquely represented in the following canonical form

$$x = p^{ord_p(x)}\,(x_0 + x_1 \cdot p + x_2 \cdot p^2 + \ldots)$$

where $x_0 \in \{1,2,\ldots p-1\}$ and $x_i \in \{0,1,2,\ldots p-1\}$, $i \geq 1$, (Borevich & Shafarevich 1966; Koblitz 1984)

More recently, numerous applications of p–adic numbers have shown up in theoretical physics and quantum mechanics (Beltrametti & Cassinelli 1972; Khrennikov 1994, 1991; Volovich 1987).

Unlike the field $\mathbb{R}$ of real numbers, in general, the cubic equation $ax^3 + bx^2 + cx + \mathrm{d} = 0$ is not necessary to have a solution in $\mathbb{Q}_p$, where $a,b,c,d \in \mathbb{Q}_p$ with $a \neq 0$. For example, the following simple cubic equation $x^3 = \mathrm{p}$ does not have any solution in $\mathbb{Q}_p$. Therefore, it is natural to find a solvability criterion for the cubic equation in $\mathbb{Q}_p$. One of methods to find solutions of the cubic equation in a local field is the Cardano method. However, by means of the Cardano method, we could not tell an existence of solutions of any cubic equations (Mukhamedov et al. 2014, 2013).

To the best of our knowledge, we could not find the solvability criterion in an explicit form for the cubic equation in the Bible books of p-adic analysis and algebraic number theory (Apostol 1972; Cohen 2007; Gouvea 1997; Koblitz 1984; Lang 1994; Neukirch 1999; Schikhof 1984; Serre 1979). The solvability criterion for the cubic equation over $\mathbb{Q}_p$, for all prime $p \neq 3$, was provided in papers Mukhamedov et al. (2014, 2013) and Saburov and Ahmad (2014). This problem was open for the case $p = 3$ and we are aiming to solve it in this paper.

We know that, by means of suitable substitutions, any cubic equation can be written *a depressed cubic equation* form

$$x^3 + ax = b, \tag{2}$$

where $a, b \in \mathbb{Q}_p$. It is worth mentioning that there are some cubic equations which do not have any solutions in $\mathbb{Z}_p^*$ (resp. in $\mathbb{Z}_p$) but have solutions in $\mathbb{Z}_p$(resp. in $\mathbb{Q}_p$) (Mukhamedov et al. (2014, 2013). Therefore, finding a solvability criterion for the depressed cubic equation (2) in domains $\mathbb{Z}_p^*, \mathbb{Z}_p, \mathbb{Q}_p$ is of independent interest. In this paper, we provide a solvability criterion for a cubic equation in the domains $\mathbb{Z}_3^*$, $\mathbb{Z}_3$ and $\mathbb{Q}_3$.

The solvability criterion for the cubic equation (2) over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where $a, b \in \mathbb{F}_p$ was provided in papers Serre 2003 and Sun 2007. Since $\mathbb{F}_p$ is a subgroup of $\mathbb{Q}_p$, our results extend the results of papers Serre 2003 and Sun 2007.

Some Auxiliary Results

In this section, we shall present some auxiliary results which assist us to find a solvability criterion for a cubic equation

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

over $\mathbb{Z}_3^*$, where $a, b \in \mathbb{Q}_3$. In the case $ab = 0$, the solvability criterion for the cubic equation (4) was given in Mukhamedov and Saburov (2013). In what follows we assume that $ab \neq 0$.

Let

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

be sets of p–adic integers and unities, respectively.

We know that any p–adic unity $x \in \mathbb{Z}_p^*$ has a unique canonical representation

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

where $x_0 \in \{1,2,\ldots p-1\}$ and $x_i \in \{0,1,2,\ldots p-1\}$ for any $i \geq 1$. Moreover, any nonzero p–adic number $x \in \mathbb{Q}_p$ has a unique representation of the form $x = \frac{x^*}{|x|_p}$, where $x^* \in \mathbb{Z}_p^*$.

Let us introduce some notations which will be used throughout this paper.

Let $x \in \mathbb{Q}_p$ be a nonzero p–adic number and $x = \frac{x^*}{|x|_p}$ with $x^* \in \mathbb{Z}_p^*$

$$x^* = x_0 + x_1 p + x_2 p^2 + \ldots + x_k p^k + \ldots$$

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

For given numbers $i_0, j_0 \in \{1,\ldots, p-1\}$ and $i_1, \ldots, i_k, j_1, \ldots, j_l \in \{0,1,\ldots, p-1\}$, we define the following sets

$$\mathbb{Z}_p^*[i_0,i_1,\ldots,i_k] = \{x^* \in \mathbb{Z}_p^* : x^* = i_0 + i_1 p + \ldots + i_k p^k + x_{k+1} p^{k+1} + \ldots\}$$

$$\mathbb{Z}_p^*[i_0,i_1,\ldots,i_k | j_0,j_1,\ldots,j_l] = \mathbb{Z}_p^*[i_0,i_1,\ldots,i_k] \times \mathbb{Z}_p^*[j_0,j_1,\ldots,j_l]$$

The following results are rather simple and might be well-known in the literature.

Proposition 1 Let $r, s \in \mathbb{F}_3$. The quadratic equation

$$x^2 + rx = s, \tag{4}$$

has a solution in $\mathbb{F}_3$ if and only if either one of the following conditions holds true: (*i*) $s = 0$ or (*ii*) $s = 1$ and $r = 0$ or (*iii*) $s = -1$ and $r \neq 0$. Moreover, the following statements hold true:

If $s = 0$ then $x = 0, -r$ are solutions of the quadratic equation (4);

If $s = 1$ and $r = 0$ then $x = \pm 1$ are solutions of the quadratic equation (4); and

If $s = -1$ and $r \neq 0$ then $x = r$ is a solution of the quadratic equation (4).

Corollary 2 If the quadratic equation (4) has solutions in $\mathbb{F}_3$ then for any $\varepsilon \neq 0$, there exists at least one solution x_0 of the quadratic equation (4) such that $x_0 \neq r + \varepsilon$.

Let us consider the following sets in

$$\begin{aligned} \Delta &= \Delta_1 \cup \Delta_2, \\ \Delta_1 &= \Delta_{11} \cup \Delta_{12} \cup \Delta_{13}, \\ \Delta_2 &= \Delta_{21} \cup \Delta_{22} \cup \Delta_{23}, \end{aligned} \tag{5}$$

where

$$\Delta_{11} = \bigcup_{\substack{i=0 \\ j=0}}^{2} \mathbb{Z}_3^*[2,i,j|1,2,i,j], \quad \Delta_{12} = \bigcup_{j=0}^{2} \mathbb{Z}_3^*[2,1,j|1,2,1,j+1],$$

$$\Delta_{13} = \bigcup_{\substack{i=1 \\ j=0}}^{2} \mathbb{Z}_3^*[2,i+1,j+1|1,2,i+1,j],$$

$$\Delta_{21} = \bigcup_{\substack{i=0 \\ j=0}}^{2} \mathbb{Z}_3^*[2,i+j,i|2,0,2-(i+j),j],$$

$$\Delta_{22} = \bigcup_{j=0}^{2} \mathbb{Z}_3^*[2,0,2-j|2,0,2,j],$$

$$\Delta_{23} = \bigcup_{\substack{i=1 \\ j=0}}^{2} \mathbb{Z}_3^*[2,3-i,j|2,0,i-1,1-(i+j)],$$

and all entries of $\mathbb{Z}_3^*[2, \ldots| 1, \ldots]$ and $\mathbb{Z}_3^*[2, \ldots| 2, \ldots]$ belong to the set $\{0,1,2\}$.

We need the following auxiliary results.

Proposition 3 Let $|a|_3 = \frac{1}{3}, |b|_3 = 1, \; a = 3a^*, a^* \in \mathbb{Z}_3^*$ with

$$a^* = a_0 + 3a_1 + 9a_2 + \ldots,$$
$$b = b^* = b_0 + 3b_1 + 9b_2 + \ldots.$$

Then the following statements hold true:

One has that $b_0^3 \equiv b \; (mod\; 9)$ if and only if $b^* \in \mathbb{Z}_3^*[1,0] \cup \mathbb{Z}_3^*[2,2]$;

One has that $b_0^3 + ab_0 \equiv b \; (mod\; 9)$ with $a_0 = 1$ if and only if $(a^*, b^*) \in \mathbb{Z}_3^*[1| 1,1] \cup \mathbb{Z}_3^*[1| 2,1]$; and

One has that $b_0^3 + ab_0 \equiv b\ (mod\ 27)$ with $a_0 = 2$ if and only if

$$\left(a^*,b^*\right)\in\bigcup_{i=0}^{2}\left(\mathbb{Z}_3^*\left[2,i|1,2,i\right]\cup\mathbb{Z}_3^*\left[2,2-i|2,0,i\right]\right). \quad (6)$$

Moreover, the quadratic congruent equation

$$x^2 + (b_0 + 1 + b_0a_1)x \equiv b_0\frac{b-ab_0-b_0^3}{27}\ (mod\ 3) \quad (7)$$

has a solution if and only if $(a^*, b^*) \in \Delta$, where the set Δ is defined by (5).

Proof. We shall prove the theorem case by case.

The congruent equation $b_0^3 \equiv b\ (mod\ 9)$ has a solution if and only if $b_0^3 \equiv b_0 + 3b_1\ (mod\ 9)$ has a solution. It is clear that the last congruent equation has a solution if and only if $b_0 = 1$, $b_1 = 0$ or $b_0 = 2$, $b_1 = 2$. It means that $b^* \in \mathbb{Z}_3^*[1,0] \cup \mathbb{Z}_3^*[2,2]$.

Let $a_0 = 1$. The congruent equation $b_0^3 \equiv ab_0 \equiv b\ (mod\ 9)$ has a solution if and only if $b_0^3 + 3b_0 \equiv b_0 + 3b_1\ (mod\ 9)$ has a solution. It is clear that the last congruent equation has a solution if and only if $b_0 = 1, b_1 = 1$ or $b_0 = 2, b_1 = 1$. It means that $(a^*, b^*) \in \mathbb{Z}_3^*[1|1,1] \cup \mathbb{Z}_3^*[1|2,1]$.

Let $a_0 = 2$. It is clear that

$$a = 3a^* = 6 + 9a_1 + 27a_2 + \ldots,$$
$$ab_0 = 6b_0 + 9a_1b_0 + 27a_2b_0 + \ldots.$$

The congruent equation $b_0^3 + ab_0 \equiv b\ (mod\ 27)$ has a solution if and only if $b_0^3 + 6b_0 + 9a_1b_0 \equiv b_0 + 3b_1 + 9b_2\ (mod\ 27)$ has a solution. We then have that

$$b_0^3 + 5b_0 + 9a_1b_0 \equiv 3b_1 + 9b_2\ (mod\ 27). \quad (8)$$

We know that $b_0 \in \{1,2\}$ if and only if $b_0^2 + 2 = 3b_0$. Therefore, we get that

$$b_0^2 = 3b_0 - 2,\quad b_0^3 = 3b_0^2 - 2b_0,$$
$$b_0^3 + 5b_0 = 3b_0^2 + 3b_0 = 12b_0 - 6.$$

The congruence equation (8) takes the following form

$$12b_0 - 6 + 9a_1b_0 \equiv 3b_1 + 9b_2\ (mod\ 27) \text{ or } 4b_0 - 2 + 3a_1b_0 \equiv b_1 + 3b_2\ (mod\ 9). \quad (9)$$

This yields that $4b_0 - 2 \equiv b_1\ (mod\ 3)$ or $b_1 \equiv b_0 + 1\ (mod\ 3)$. Thus, if $b_0 = 1$ then $b_1 = 2$ and it follows from (9) that $a_1 = b_2$; if $b_0 = 2$ then $b_1 = 0$ and it follows from (9) that $a_1 = 2 - b_2$. Consequently, we have that $(a^*, b^*) \in \cup_{i=0}^{2} (\mathbb{Z}_3^*[2,i|1,2,i] \cup \mathbb{Z}_3^*[2,2-i|2,0,i]$.

In this case, we want to show that

$$\frac{b-ab_0-b_0^3}{27} \equiv \begin{cases} b_3 - a_2\ (mod\ 3), & if\ \left(a^*,b^*\right)\in\bigcup_{i=0}^{2}\mathbb{Z}_3^*\left[2,i|1,2,i\right] \\ b_2 + b_3 + a_2 + 1\ (mod\ 3), & if\ \left(a^*,b^*\right)\in\bigcup_{i=0}^{2}\mathbb{Z}_3^*\left[2,2-i|2,0,i\right]. \end{cases} \quad (10)$$

Let $(a^*,b^*) \in \cup_{i=0}^{2}\mathbb{Z}_3^*[2, i| 1,2,i]$. This means that $a_0 = 2$, $a_1 = b_2$, $b_0 = 1$, $b_1 = 2$. Then

$$a \equiv 3a_0 + 9a_1 + 27a_2\ (mod\ 81),$$
$$b \equiv b_0 + 3b_1 + 9b_2 + 27b_3 \equiv 1 + 6 + 9b_2 + 27b_3\ (mod\ 81),$$
$$ab_0 \equiv 3a_0b_0 + 9a_1b_0 + 27a_2b_0 \equiv 6 + 9b_2 + 27a_2\ (mod\ 81),$$
$$b - ab_0 - b_0^3 \equiv 27(b_3 - a_3)\ (mod\ 81)$$

This yields that $\frac{b-ab_0-b_0^3}{27} \equiv b_3 - a_2\ (mod\ 3)$.

Let $(a^*,b^*) \in \cup_{i=0}^{2}\mathbb{Z}_3^*[2, 2 - i| 2,0, i]$. This means that $a_0 = 2$, $a_1 = 2 - b_2$, $b_0 = 2$, $b_1 = 0$. Then

$$a \equiv 3a_0 + 9a_1 + 27a_2\ (mod\ 81),$$
$$b \equiv b_0 + 3b_1 + 9b_2 + 27b_3 \equiv 2 + 9b_2 + 27b_3\ (mod\ 81),$$
$$ab_0 \equiv 3a_0b_0 + 9a_1b_0 + 27a_2b_0 \equiv 12 + 18(2 - b_2) + 54a_2\ (mod\ 81),$$
$$b - ab_0 - b_0^3 \equiv 27(b_2 + b_3 - 2a_3 - 2)\ (mod\ 81)$$

This yields that $\frac{b-ab_0-b_0^3}{27} \equiv b_2 + b_3 + a_2 + 1\ (mod\ 3)$.

We now study the quadratic congruent equation (7).

Case I. Let $(a^*,b^*) \in \cup_{i=0}^{2}\mathbb{Z}_3^*[2, i| 1,2, i]$. In this case, the equation (7) takes the following form

$$x^2 + (2 + b_2)x \equiv b_3 - a_2\ (mod\ 3).$$

Then, due to Proposition 1, the last quadratic congruent equation has a solution if and only if either one of the following conditions holds true:

a) $b_3 - a_2 \equiv 0\ (mod\ 3)$;
b) $b_3 - a_2 \equiv 1\ (mod\ 3)$ and $2 + b_2 \equiv 0\ (mod\ 3)$; and
c) $b_3 - a_2 \equiv -1\ (mod\ 3)$ and $2 + b_2 \not\equiv 0\ (mod\ 3)$.

Therefore, we get that

a) $a_0 = 2, a_1 = b_2, a_2 = b_3, b_0 = 1, b_1 = 2$ or
$$\left(a^*,b^*\right)\in\Delta_{11}=\bigcup_{\substack{i=0\\j=0}}^{2}\mathbb{Z}_3^*\left[2,i,j|1,2,i,j\right];$$

b) $a_0 = 2, a_1 = 1, b_0 = 1, b_1 = 2, b_2 = 1, b_3 \equiv a_2 + 1\ (mod\ 3)$ or
$$\left(a^*,b^*\right)\in\Delta_{12}=\bigcup_{j=0}^{2}\mathbb{Z}_3^*\left[2,1,j|1,2,1,j+1\right];$$

c) $a_0 = 2, a_1 = b_2, a_2 \equiv b_3 + 1\ (mod\ 3)$,
$b_0 = 1, b_1 = 2, b_2 \neq 1$ or

$$\left(a^*,b^*\right) \in \Delta_{13} = \bigcup_{\substack{i=1\\ j=0}}^{2} \mathbb{Z}_3^*\left[2,i+1,j+1|1,2,i+1,j\right].$$

Consequently, we have that $(a^*,b^*) \in \Delta_1 = \Delta_{11} \cup \Delta_{12} \cup \Delta_{13}$

CASE II. Let $(a^*,b^*) \in \cup_{i=0}^{2} \mathbb{Z}_3^*\ [2,2 - i| 2,0, i]$. In this case, the equation (7) takes the following form

$$x^2 + 2(2 - b_2)x \equiv 2(b_2 + b_3 + a_2 + 1)\ (mod\ 3)$$

Then, due to Proposition 1, the last quadratic congruent equation has a solution if and only if either one of the following conditions holds true:

a) $2(b_2 + b_3 + a_2 + 1) \equiv 0\ (mod\ 3)$;
b) $2(b_2 + b_3 + a_2 + 1) \equiv 1\ (mod\ 3)$ and $2(2 - b_2) \equiv 0\ (mod\ 3)$; and
c) $2(b_2 + b_3 + a_2 + 1) \equiv -1\ (mod\ 3)$ and $2(2 - b_2) \not\equiv 0\ (mod\ 3)$.

Therefore, we have that

a) $a_0 = 2, a_1 \equiv a_2 + b_3\ (mod\ 3), b_0 = 2, b_1 = 0, b_2 \equiv 2 - (a_2 + b_3)\ (mod\ 3)$ or

$$\left(a^*,b^*\right) \in \Delta_{21} = \bigcup_{\substack{i=1\\ j=0}}^{2} \mathbb{Z}_3^*\left[2,i+j,i|2,0,2-(i+j),j\right];$$

b) $a_0 = 2, a_1 \equiv 0, a_2 = 2 - b_3 b_0 = 2, b_1 = 0, b_2 \equiv 2$ or

$$\left(a^*,b^*\right) \in \Delta_{22} = \bigcup_{j=1}^{2} \mathbb{Z}_3^*\left[2,0,2-j|2,0,2,j\right]$$

c) $a_0 = 2, a_1 = 2 - b_2, b_0 = 2, b_1 = 0, b_2 \neq 2, b_3 \equiv -(b_2 + a_3)\ (mod\ 3)$ or

$$\left(a^*,b^*\right) \in \Delta_{23} = \bigcup_{\substack{i=1\\ j=0}}^{2} \mathbb{Z}_3^*\left[2,3-i,j|2,0,i-1,1-(i+j)\right].$$

Consequently, we obtain that $(a^*,b^*) \in \Delta_2 = \Delta_{21} \cup \Delta_{22} \cup \Delta_{23}$

Therefore, the quadratic congruent equation (7) has a solution if and only if $(a^*,b^*) \in \Delta = \Delta_1 \cup \Delta_2$. This completes the proof.

Finally, Hensel's lemma would be a powerful tool in order to obtain the solvability criterion for the cubic equation (3) in the domain $\mathbb{Z}_3^*$.

Lemma 4 (**Hensel's Lemma, [3]**) Let $f(x)$ be polynomial whose the coefficients are p–adic integers. Let θ be a p–adic integer such that for some $i \geq 0$ we have

$$f(\theta) \equiv 0\ (mod\ p^{2i+1}),$$
$$f'(\theta) \equiv 0\ (mod\ p^i),\ f'(\theta) \not\equiv 0\ (mod\ p^{i+1}).$$

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

SOLVABILITY CRITERIA OVER DOMAINS $\mathbb{Z}_3^*$, $\mathbb{Z}_3$ AND $\mathbb{Q}_3$

In this section, we provide the main results of the paper in the domains $\mathbb{Z}_3^*$.

Theorem 5. Let $a, b \in \mathbb{Q}_3$ with $ab \neq 0$ and Δ be the set given by (5). Then the following statements hold true:

1) The cubic equation (3) is solvable in $\mathbb{Z}_3^*$ if and only if either one of the following conditions holds true:
   I. $|b|_3 = |a|_3 > 1$;
   II. $|b|_3 = |a|_3 = 1, a^* \in \mathbb{Z}_3^*[1]$;
   III. $|b|_3 < |a|_3 = 1, a^* \in \mathbb{Z}_3^*[2]$;
   IV. $|a|_3 < |b|_3 = 1$ and
      (i) $|a|_3 = \frac{1}{3}, (a^*,b^*- \in \mathbb{Z}_3^*[1| 1] \cup \mathbb{Z}_3^*[1| 2,1] \cup \Delta$;
      (ii) $|a|_3 < \frac{1}{3}, b^* \in \mathbb{Z}_3^*[1,0] \cup \mathbb{Z}_3^*[2,2]$.

2) The cubic equation (3) is solvable in $\mathbb{Z}_3$ if and only if either one of the following conditions holds true:
   I. $|a|_3^3 > |b|_3^2,\ |a|_3 \geq |b|_3$;
   II. $|a|_3^3 = |b|_3^2 \leq 1,\ a^* \in \mathbb{Z}_3^*[1]$;
   III. $|a|_3^3 < |b|_3^2 \leq 1,\ 3|\log_3|b|_3$, and
      (i) $\left|\frac{a}{3}\right|_3^3 = |b|_3^2,\ \left(a^*,b^*\right) \in \mathbb{Z}_3^*\left[1|1,1\right] \cup \mathbb{Z}_3^*\left[1|2,1\right] \cup \Delta$;
      (ii) $\left|\frac{a}{3}\right|_3^3 < |b|_3^2,\ b^* \in \mathbb{Z}_3^*\left[1,0\right] \cup \mathbb{Z}_3^*\left[2,2\right]$.

3) The cubic equation (3) is solvable in $\mathbb{Q}_3$ if and only if either one of the following conditions holds true:
   I. $|a|_3^3 > |b|_3^2$;
   II. $|a|_3^3 = |b|_3^2,\ a^* \in \mathbb{Z}_3^*[1]$;
   III. $|a|_3^3 < |b|_3^2,\ 3|\log_3|b|_3$, and
      (i) $\left|\frac{a}{3}\right|_3^3 = |b|_3^2,\ \left(a^*,b^*\right) \in \mathbb{Z}_3^*\left[1|1,1\right] \cup \mathbb{Z}_3^*\left[1|2,1\right] \cup \Delta$;
      (ii) $\left|\frac{a}{3}\right|_3^3 < |b|_3^2,\ b^* \in \mathbb{Z}_3^*\left[1,0\right] \cup \mathbb{Z}_3^*\left[2,2\right]$.

Proof. Let $a,b \in \mathbb{Q}_3$, $ab \neq 0$ and Δ be the set given by (5).

CASE I. We know (Mukhamedov et al. 2014) that if the cubic equation (3) has a solution in $\mathbb{Z}_3^*$ then it is necessary to have either one of the following conditions: $|a|_3 = |b|_3 \geq 1$ or $|b|_3 < |a|_3 = 1$ or $|a|_3 < |b|_3 = 1$. We shall study case by case.

I.1. Let $|a|_3 = |b|_3 > 1$. In this case, we want to show that the cubic equation (3) always solvable in $\mathbb{Z}_3^*$.

Since $|a|_3 = |b|_3 = 3^k$ for some $k \in \mathbb{N}$, it is clear that the solvability of the following two cubic equations is equivalent

$$x_3 + ax = b, \qquad |a|_3 x^3 + a^* x = b^*. \tag{11}$$

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. Let us consider the following polynomial function $g_{a,b}(x) = |a|_3 x^3 + a^* x - b^*$. Let $\bar{x}$ be a solution of the linear congruent equation $a^* \bar{x} \equiv b^* \ (mod\ 3)$ (it always exists). Then we get that

$$g_{a,b}(\bar{x}) = |a|_3 \bar{x}^3 + a^*\bar{x} - b^* \equiv a^*\bar{x} - b^* \equiv 0 \ (mod\ 3),$$

$$g'_{a,b}(\bar{x}) = 3|a|_3 \bar{x}^2 + a^* \equiv a^* \equiv 0 \ (mod\ 3).$$

Then due to Hensel's Lemma, there exists $x \in \mathbb{Z}_3$ such that $g_{a,b}(x) = 0$. Since $x \equiv \bar{x} \not\equiv 0 \ (mod\ 3)$, we have that $x \in \mathbb{Z}_3^*$. This shows that the cubic equation (3) is solvable in $\mathbb{Z}_3^*$ whenever $|a|_3 = |b|_3 > 1$.

I.2. Let $|b|_3 = |a|_3 = 1$. In this case, we want to show that the equation (3) is solvable in $\mathbb{Z}_3^*$ if and only if $a^* \in \mathbb{Z}_3^*[1]$.

Only if part: Let $x \in \mathbb{Z}_3^*$ be a solution of the cubic equation (3). Since $|b|_3 = 1$, we have that $x^3 + ax \equiv b \not\equiv 0 \ (mod\ 3)$. This yields that $x^2 + a \not\equiv 0 \ (mod\ 3)$. We know that for any $x \in \mathbb{Z}_3^*$ one has that $x^2 \equiv 1 \ (mod\ 3)$. Then we get that $1 + a \not\equiv 0 \ (mod\ 3)$ or $a \not\equiv 2 \ (mod\ 3)$. This means that $a_0 \equiv a \equiv 1 \ (mod\ 3)$ or $a \in \mathbb{Z}_3^*[1]$.

If part: Let $a \in \mathbb{Z}_3^*[1]$. Let us consider the following polynomial function $f_{a,b}(x) = x^3 + ax - b$. Let $\bar{x} = 2b_0$. Then it is clear that

$$f_{a,b}(\bar{x}) = 8b_0^3 + 2ab_0 - b \equiv 8b_0 + 2b_0 - b_0 \equiv 9b_0 \equiv 0 \ (mod\ 3),$$

$$f_{a,b}'(\bar{x}) = 12b_0^2 + a \equiv a \equiv 1 \not\equiv 0 \ (mod\ 3).$$

Then due to Hensel's Lemma, there exists $x \in \mathbb{Z}_3$ such that $f_{a,b}(x) = 0$. Since $x \equiv \bar{x} \equiv 2b_0 \ (mod\ 3)$, we have that $x \in \mathbb{Z}_3^*$.

I.3. Let $|b|_3 < |a|_3 = 1$. In this case, we want to show that the cubic equation (3) is solvable in $\mathbb{Z}_3^*$ if and only if $a^* \in \mathbb{Z}_3^*[2]$.

Only if part: Let $x \in \mathbb{Z}_3^*$ be a solution of the cubic equation (3). Since $|b|_3 < 1$, we have that $x^3 + ax \equiv b \equiv 0 \ (mod\ 3)$. This yields that $x^2 + a \equiv 0 \ (mod\ 3)$ or $x^2 \equiv -a \ (mod\ 3)$. We know that for any $x \in \mathbb{Z}_3^*$ one has that $x^2 \equiv 1 \ (mod\ 3)$. We then get that $a \equiv -1 \ (mod\ 3)$. This means that $a_0 \equiv a \equiv 2 \ (mod\ 3)$ or $a \in \mathbb{Z}_3^*[2]$.

If part: Let $a \in \mathbb{Z}_3^*[2]$. Let us again consider the same polynomial function $f_{a,b}(x) = x^3 + ax - b$. Let $\bar{x} = 1$. Then it is clear that

$$f_{a,b}(\bar{x}) = 1 + a - b \equiv 1 + a_0 \equiv 0 \ (mod\ 3),$$

$$f_{a,b}'(\bar{x}) = 3 + a \equiv a \equiv 2 \not\equiv 0 \ (mod\ 3)$$

Then due to Hensel's Lemma, there exists $x \in \mathbb{Z}_3$ such that $f_{a,b}(x) = 0$. Since $x \equiv \bar{x} \equiv 1 \ (mod\ 3)$, we have that $x \in \mathbb{Z}_3^*$.

I.4. Let $|a|_3 = \frac{1}{3}$. We shall separately study two cases: $(i)\ |a|_3 = \frac{1}{3}$ and $(ii)\ |a|_3 < \frac{1}{3}$.

I.4. (i). Let $|a|_3 = \frac{1}{3}$. In this case, we want to show that the cubic equation (3) is solvable in $\mathbb{Z}_3^*$ if and only if $(a^*, b^*) \in \mathbb{Z}_3^*[1|1,1] \cup \mathbb{Z}_3^*[1|2,1] \cup \Delta$ where the set Δ is defined by (5).

Since $|a|_3 = \frac{1}{3}$, one hast that $a = 3a^*$, where

$$a^* = a_0 + 3a_1 + 9a_2 + \ldots$$

Here, we have two options: $a_0 = 1$ or $a_0 = 2$.

Let $a_0 = 1$. In this case, we especially want to show that cubic equation (3) is solvable in $\mathbb{Z}_3^*$ if and only if $(a^*, b^*) \in \mathbb{Z}_3^*[1|1,1] \cup \mathbb{Z}_3^*[1|2,1]$.

Only if part: Let $x \in \mathbb{Z}_3^*$ be a solution of (3). Particularly, we then get that

$$x^3 + ax \equiv b \ (mod\ 3) \quad (12)$$

$$x^3 + ax \equiv b \ (mod\ 9) \quad (13)$$

Since $a = 3a^*$, it follows from (1) that $x \equiv b \ (mod\ 3)$. It means that $x_0 = b_0$. We know that $x^3 \equiv b_0^3 \ (mod\ 9)$ and $ax \equiv ab_0 \ (mod\ 9)$. Therefore, we have that

$$b \equiv x^3 + ax \equiv b_0^3 + b_0 \ (\text{mod } 9) \quad (14)$$

Due to Proposition 3, the congruent (14) holds true if $(a^*, b^*) \in \mathbb{Z}_3^*[1|1,1] \cup \mathbb{Z}_3^*[1|2,1]$.

If part. Let $(a^*, b^*) \in \mathbb{Z}_3^*[1|1,1] \cup \mathbb{Z}_3^*[1|2,1]$. We consider the same polynomial function $f_{a,b}(x) = x^3 + ax - b$. Let $\bar{x} = b_0 + 3(b_0 - 1 + a_1 b_0 - b_2)$. It is clear that

$$\bar{x}^3 \equiv b_0^3 + 9b_0^2(b_0 - 1 + a_1 b_0 - b_2)$$

$$\equiv b_0^3 + 9(b_0 - 1 + a_1 b_0 - b_2) \ (mod\ 27),$$

$$a\bar{x} \equiv 3a_0\bar{x} + 9a_1\bar{x} \equiv 12b_0 - 9 + 18a_1 b_0 - 9b_2 \ (mod\ 27).$$

Since $b_0^2 + 2 = 3b_0$ for any $b_0 \in \{1,2\}$, we then obtain that

$$\begin{aligned} f_{a,b}(\bar{x}) &\equiv b_0^3 + 9(b_0 - 1) + 9a_1 b_0 - 9b_2 + 12b_0 - 9 \\ &\quad + 18a_1 b_0 - 9b_2 - b_0 - 3b_1 - 9b_2 \ (mod\ 27) \\ &\equiv b_0^3 + 9(b_0 - 1) + 12b_0 - 9 - b_0 - 3b_1 \\ &\equiv 27(b_0 - 1) \ (mod\ 243) \\ f'_{a,b}(\bar{x}) &= 3(\bar{x}^2 + a^*) \equiv 0 \ (mod\ 3) \\ f'_{a,b}(\bar{x}) &= 3(\bar{x}^2 + a^*) \equiv 6 \ (mod\ 9) \end{aligned}$$

So, due to Hensel's Lemma, there exist $x \in \mathbb{Z}_3$ such that $f_{a,b}(x) = 0$. Since $x \equiv \bar{x} \equiv b_0 \ (mod\ 3)$, we have that $x \in \mathbb{Z}_3^*$.

Let $a_0 = 2$. In this case, we especially want to show that cubic equation (3) is solvable in $\mathbb{Z}_3^*$ if and only if $(a^*,b^*) \in \Delta$ where the set Δ is defined by (5).

Only if part: Let $x \in \mathbb{Z}_3^*$ be a solution of the cubic equation (3). Let

$$x \equiv x_0 + 3x_1 + 9x_2 + 27x_3 + 81x_4 \equiv x_0 + 3X_1 \ (mod\ 243)$$
$$X_1 = x_1 + 3x_2 + 9x_3 + 27x_4 = x_1 + 3X_2$$
$$X_2 = x_2 + 3x_3 + 9x_4 = x_2 + 3X_3$$
$$X_3 = x_3 + 3X_4.$$

In this case we can get that

$$X_1^2 = x_1^2 + 6x_1X_2 + 9X_2^2$$
$$X_1^3 = x_1^3 + 9x_1^2X_2 + 27\left(x_1X_2^2 + X_2^3\right)$$
$$X_2^2 = x_2^2 \ \left(mod\ 9\right).$$

Consequently, we obtain that

$$x^3 \equiv x_0^3 + 9x_0^2X_1 + 27\left(x_0X_1^2 + X_1^3\right)(mod\ 243)$$
$$\equiv x_0^3 + 9x_0^2\left(x_1 + 3x_2 + 9x_3\right) + 27x_0\left(x_1^2 + 6x_1x_2\right)$$
$$+ 27x_1^3 \ (mod\ 243)$$
$$a \ \equiv 3a_0 + 9a_1 + 27a_2 + 81a_3 \ \ (mod\ 243)$$
$$ax \equiv 3x_0(a_0 + 3a_1 + 9a_2 + 27a_3) + 9x_1(a_0 + 3a_1 + 9a_2)$$
$$+27x_2\left(a_0 + 3a_1\right) + 81x_3a_0 \ (mod\ 243)$$
$$\equiv ax_0 + 9x_1a_0 + 27\left(x_1a_1 + x_2a_0\right) + 81\left(x_1a_2 + x_2a_1 + x_3a_0\right)$$
$$(mod\ 243).$$

We then get that

$$x^3 + ax - b \equiv x_0^3 + ax_0 - b + 9x_1(x_0^2 + a_0) + 27x_2(x_0^2 + a_0)$$
$$+ 27(x_1a_1 + x_0x_1^2 + x_1^3) + 81(x_1a_2 + x_2a_1) + 81x_3(x_0^2 + a_0)$$
$$+ 162x_0x_1x_2 \ (mod\ 243)$$

It is easy to check that for any $b_0 \in \{1,2\}$, we have that $x_0^2 + a_0 = b_0^2 + 2 = 3b_0$. Therefore, we have that

$$x^3 + ax - b \equiv b_0^3 + ab_0 - \mathrm{b} + 27b_0x_1 + 27(x_1a_1 + b_0x_1^2 + x_1^3)$$
$$+81b_0x_2 + 81(x_1a_2 + x_2a_1)$$
$$+162b_0x_1x_2 \ (mod\ 243) \tag{15}$$

Since x is a solution of the cubic equation (3), in particular, it follows that

$$x^3 + ax - b \equiv 0 \ (mod\ 3) \tag{16}$$

$$x^3 + ax - b \equiv 0 \ (mod\ 27) \tag{17}$$

$$x^3 + ax - b \equiv 0 \ (mod\ 81) \tag{18}$$

$$x^3 + ax - b \equiv 0 \ (mod\ 243) \tag{19}$$

Since $a = 3a^*$, it follows from (16) that $x^3 \equiv b$ (mod 3) or $x_0 = b_0$. We then obtain from (15) and (17) that $x^3 + ax - b \equiv b_0^3 + ab_0 - b \equiv 0$ (mod 27). Due to Proposition 3, the last congruent holds true if $(a^*, b^*) \in \cup_{i=0}^{2} \mathbb{Z}_3^*[2,i|\,1,2,i] \cup \mathbb{Z}_3^*[2,2-i|\,2,0,i]$.

In this case, we obtain from (18) that

$$x^3 + ax - b \equiv b_0^3 + ab_0 - b + 27x_1b_0 + 27(x_1a_1 + b_0x_1^2 + x_1^3)$$
$$\equiv 0 \ (mod\ 81)$$

and by dividing 27 and having $x_1^3 \equiv x_1$ (mod 3) we get that

$$b_0x_1^2 + \left(1 + b_0 + a_1\right)x_1 \equiv \frac{b - ab_0 - b_0^3}{27} \ \ (mod\ 3) \tag{20}$$

or (by multiplying b_0 and having $b_0^2 \equiv 1$ (mod 3))

$$x_1^2 + \left(b_0 + 1 + a_1b_0\right)x_1 \equiv b_0\frac{b - ab_0 - b_0^3}{27} \ (mod\ 3) \tag{21}$$

Then due to Proposition 3, this quadratic congruent equation has a solution if and only if $(a^*, b^*) \in \Delta$.

If part: Let $(a^*, b^*) \in \Delta$. Let us consider the same polynomial function $f_{a,b}(x) = x^3 + ax - b$. Due to Corollary 2, for $\varepsilon = -b_0$ the last quadratic equation (21) has a solution $\bar{x}_1$ such that $\bar{x}_1 \not\equiv 1 + a_1b_0$ (mod 3). It is worth mentioning that $\bar{x}_1$ is also the solution of the quadratic congruent equation (20).

Now, we choose $\bar{x}_2$ to be a solution of the following linear congruence

$$(b_0 + a_1 - b_0\bar{x}_1)\,\bar{x}_2$$

$$\equiv \frac{\frac{b - ab_0 - b_0^3}{27} - \left(1 + b_0 + a_1\right)\bar{x}_1 - b_0\bar{x}_1^2}{3}$$
$$-a_2\bar{x}_1 - \frac{\bar{x}_1^3 - \bar{x}_1}{3} \ (mod\ 3) \tag{22}$$

Note that the linear congruent (22) always has a solution because of $b_0\bar{x}_1 \not\equiv b_0 + a_1$ (mod 3). We then get from (22) that

$$(b_0 + a_1 + 2b_0\bar{x}_1)\bar{x}_2$$

$$\equiv \frac{\frac{b - ab_0 - b_0^3}{27} - \left(1 + b_0 + a_1\right)\bar{x}_1 - b_0\bar{x}_1^2}{3}$$
$$-a_2\bar{x}_1 - \frac{\bar{x}_1^3 - \bar{x}_1}{3}\left(mod\ 3\right)$$

$(81b_0 + 81a_1 + 162b_0\bar{x}_1)\bar{x}_2 \equiv b - ab_0 - b_0^3 - 27(1 + b_0 + a_1)\bar{x}_1 - 27b_0\bar{x}_1^2 - 81a_2\bar{x}_1 - 27(\bar{x}_1^3 - \bar{x}_1)$ (mod 243)

$$b_0^3 + ab_0 - b + 27b_0\bar{x}_1 + 27(a_1\bar{x}_1 + b_0\bar{x}_1^2 + \bar{x}_1^3)$$
$$+ 81b_0\bar{x}_2 + 81\,(a_2\bar{x}_1 + a_1\bar{x}_2) + 162b_0\bar{x}_1\bar{x}_2$$
$$\equiv 0 \ (mod\ 243)$$

Let $\bar{x} = b_0 + 3\bar{x}_1 + 9\bar{x}_2$. We then have that

$$\begin{aligned} f_{a,b}(\bar{x}) &\equiv b_0^3 + ab_0 - b + 27b_0\bar{x}_1 + 81b_0\bar{x}_2 \\ &\quad + 27(\bar{x}_1a_1 + b_0\bar{x}_1^2 + \bar{x}_1^3) + 81(\bar{x}_1a_2 + \bar{x}_2a_1) \\ &\quad + 162b_0\bar{x}_1\bar{x}_2 \ (mod\ 243) \\ &\equiv 0 \ (mod\ 243) \\ f'_{a,b}(\bar{x}) &= 3(\bar{x}^2 + a^*) \equiv 0 \ (mod\ 3) \\ f'_{a,b}(\bar{x}) &= 3(\bar{x}^2 + a^*) \equiv 3(1+2) \equiv 0 \ (mod\ 9) \\ f'_{a,b}(\bar{x}) &= 3(\bar{x}^2 + a^*) \equiv 3b_0^2 + 18b_0\bar{x}_1 + 3a_0 + 9a_1 \\ &\equiv 3(b_0^2 + 2) + 18b_0\bar{x}_1 + 9a_1 \ (mod\ 27) \\ &\equiv 9b_0 + 18b_0\bar{x}_1 + 9a_1 \equiv 9(b_0 + a_1 + b_0\bar{x}_1) \ (mod\ 27) \\ &\equiv \pm 9 \not\equiv 0 \ (mod\ 27) \end{aligned}$$

So, due to Hensel's Lemma, there exist $x \in \mathbb{Z}_3$ such that $f_{a,b}(x) = 0$. Since $x \equiv \bar{x} \equiv b_0$ $(mod\ 3)$, we have that $x \in \mathbb{Z}_3^*$.

I.4. (ii). Let $|a|_3 \le \frac{1}{9}$. In this case, we want to show that the cubic equation (3) is solvable in $\mathbb{Z}_3^*$ if and only if $b^* \in \mathbb{Z}_3^*[1,0] \cup \mathbb{Z}_3^*[2,2]$.

Only if part: Let $x \in \mathbb{Z}_3^*$ be a solution of the cubic equation (3). Since $a \equiv 0$ $(mod\ 9)$, we have that $b \equiv x^3$ $(mod\ 9)$. This yields that $x \equiv b$ $(mod\ 3)$ or $x_0 = b_0$. On the other hand, if $x \equiv b_0$ $(mod\ 3)$ then we obtain that $x^3 \equiv b_0^3 (mod\ 9)$. It means that $b_0^3 \equiv b (mod\ 9)$. Then, due to Proposition 3, we have that $b^* \in \mathbb{Z}_3^*[1,0] \cup \mathbb{Z}_3^*[2,2]$.

If part. Let $b^* \in \mathbb{Z}_3^*[1,0] \cup \mathbb{Z}_3^*[2,2]$. Since $|a|_3 \le \frac{1}{9}$, we have that $a = 9a_0 + 27a_1 + \ldots$ where $a_0, a_i \in \{0,1,2\}$. Let us consider the same polynomial function $f_{a,b}(x) = x^3 + ax - b$. We choose that $\bar{x} = b_0 + 3(b_2 - b_0a_0)$. In this case, we have that

$$\begin{aligned} &\bar{x}^3 \equiv b_0^3 + 9(b_2 - b_0a_0) \ (mod\ 27) \\ &a\bar{x} \equiv 9a_0b_0 \ (mod\ 27) \\ &f'_{a,b}(\bar{x}) \equiv b_0^3 - b_0 - 3b_1 \equiv 0 \ (mod\ 27) \\ &f'_{a,b}(\bar{x}) = 3\bar{x}^2 + a \equiv 0 \ (mod\ 3) \\ &f'_{a,b}(\bar{x}) = 3\bar{x}^2 + a \equiv 3b_0^2 \equiv 3 (mod\ 9) \end{aligned}$$

So, due Hensel's Lemma, there exist $x \in \mathbb{Z}_3$ such that $f_{a,b}(x) = 0$. Since $x \equiv \bar{x} \equiv b_0$ (mod 3), we have that $x \in \mathbb{Z}_3^*$.

Similarly, one can prove the cases 2 and 3. This completes the proof.

In the paper (Saburov & Ahmad 2015 (*in press*) we study the number of solutions of the cubic equations over $\mathbb{Q}_3$.

ACKNOWLEDGMENTS

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

REFERENCES

Apostol, T.M. 1972. *Introduction to Analytic Number Theory*. New York: Springer-Verlag.

Beltrametti, E. & Cassinelli, G. 1972. Quantum mechanics and p–adic numbers. *Foundations of Physics* 2(1): 1-7.

Borevich, Z.I. & Shafarevich, I.R. 1966. *Number Theory*. New York: Acad. Press.

Cohen, H. 2007. *Number Theory, Volume I, II*. New York: Springer.

Gouvea, F.Q. 1997. *P–adic Numbers: An Introduction*. Berlin: Springer-Verlag.

Khrennikov, A. Yu. 1994. *P–Adic Valued Distributions in Mathematical Physics*. Berlin: Kluwer.

Khrennikov, A. Yu. 1991. *P*–adic quantum mechanics with p–adic valued functions. *J. Math. Phys.* 32: 932.

Koblitz, N. 1984. *P–adic numbers, p–adic Analysis, and Zeta Functions*. New York: Springer.

Lang, S. 1994. *Algebraic Number Theory*. New York: Springer-Verlag.

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

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

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

Neukirch, J. 1999. *Algebraic Number Theory*. Berlin: Springer-Verlag.

Saburov, M. & Ahmad, M.A.Kh. 2015. The number of solutions of cubic equations over $\mathbb{Q}_3$ *Sains Malaysiana* (*in press*).

Saburov, M. & Ahmad, M.A.Kh. 2014. Solvability criteria for cubic equations over $\mathbb{Z}_2^*$ *AIP Conference Proceedings* 1602: 792-797.

Schikhof, W.H. 1984. *Ultrametric Calculus: An Introduction to P-adic Analysis*. London: Cambridge University Press.

Serre, J.P. 2003. On a Theorem of Jordan. *Bulletin of the American Mathematical Society* 102(1): 41-89.

Serre, J.P. 1979. *Local Field*. New York: Springer-Verlag.

Sun, Z.H. 2007. Cubic residues and binary quadratic forms, *J. Numb. Theory* 124(1): 62-104.

Volovich, I.V. 1987. p–adic strings. *Class. Quantum Gray.* 4: 83-87.

Department of Computational & Theoretical Sciences
Faculty of Sciences, International Islamic University Malaysia
P.O. Box 25200 Kuantan, Pahang
Malaysia

*Corresponding author; email: msaburov@gmail.com

Received: 15 November 2013
Accepted: 14 May 2014