Journal of Number Theory 133 (2013) 55–58

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On equation $x^q = a$ over $\mathbb{Q}_p$

Farrukh Mukhamedov [*], Mansoor Saburov

Department of Computational & Theoretical Sciences, Faculty of Sciences, International Islamic University Malaysia, P.O. Box 141, 25710 Kuantan, Pahang, Malaysia

ARTICLE INFO

Article history:
Received 29 June 2011
Revised 15 July 2012
Accepted 16 July 2012
Available online 13 September 2012
Communicated by David Goss

MSC:
11D88
11S05

Keywords:
Solvability criterion
Monomial equation
p-adic number

ABSTRACT

In this paper we provide a solvability criterion for the monomial equation $x^q = a$ over $\mathbb{Q}_p$ for any natural number q. As an application of the result, we describe a relationship between q and p in which the number -1 is the q-th power of some p-adic number.

1. Introduction

Over the last century, p-adic numbers and p-adic analysis have come to play a central role in modern number theory.

To the best of our knowledge, we could not find any solvability criterion in the explicit form[1] for the monomial equation

$$x^q = a, \tag{1.1}$$

where q is an integer $\geqslant 2$ and $a \in \mathbb{Q}_p$ (except for $q = 2$, see [1] or [4]).

[*] Corresponding author.
E-mail addresses: far75m@yandex.ru, farrukh_m@iium.edu.my (F. Mukhamedov), msaburov@gmail.com, msaburov@iium.edu.my (M. Saburov).

[1] Any kind of solvability criterion was not mentioned in the classical books of the p-adic analysis except $q = 2$.

0022-314X/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2012.07.006

Recently, J.M. Casas et al. [2] have attempted to provide a solvability criterion for the monomial equation (1.1) concerning classification problems of high order Leibnitz algebras (see [3]). They provided a criterion in the explicit form for two cases (i) $(q,p)=1$, (ii) $q=p$, and it was stated that the solvability problem for $q=mp^s$ can be reduced to the cases (i) and (ii). It is worth to mention that statements of the solvability criteria given in [2] were correct in the mentioned cases but their proofs are long and complicate. Moreover, the provided algorithm for $q=mp^s$ does not properly work. In this paper, we want to show it by presenting rigorous and accurate proofs. More precisely, we provide the solvability criterion in an explicit form of the general case $q=mp^s$. Note that our method is completely different from [2].[2] As it is usual, the solvability criteria of Eq. (1.1) in $\mathbb{Q}_2$ and in $\mathbb{Q}_p$, where $p>2$, are slightly different from each other. Therefore, we shall separately study them. As an application of the result, we describe the relationship between q and p in which the number -1 is the q-th power of some p-adic number.

2. Preliminaries

We recall that $\mathbb{Z}_p=\{x\in\mathbb{Q}_p\colon |x|_p\leqslant 1\}$ are $\mathbb{Z}_p^*=\{x\in\mathbb{Q}_p\colon |x|_p=1\}$ and the set of all *p-adic integers* and *units* of $\mathbb{Q}_p$, respectively. Any element $x\in\mathbb{Z}_p^*$ has a unique canonical form $x=x_0+x_1\cdot p+x_2\cdot p^2+\cdots$, where $x_0\in\{1,2,\dots,p-1\}$ and $x_i\in\{0,1,2,\dots,p-1\}$, $i\geqslant 1$. It is well-known (see [1]) that any nonzero p-adic number x has a unique representation of the form $x=p^{ord_p(x)}x_*$, where $x_*\in\mathbb{Z}_p^*$.

We are aiming to solve the monomial equation (1.1) in $\mathbb{Q}_p$ whenever $a\in\mathbb{Q}_p$ and $a\neq 0$. After substituting the forms $x=p^{ord_p(x)}x_*$, $a=p^{ord_p(a)}a_*$ into (1.1), we can get that $p^{q\cdot ord_p(x)}x_*^q=p^{ord_p(a)}a_*$. This means that Eq. (1.1) has a solution in $\mathbb{Q}_p$ whenever $a\in\mathbb{Q}_p$ if and only if the number $ord_p(a)$ is divisible by q and the equation $x_*^q=a_*$ has a solution in $\mathbb{Z}_p^*$.

Therefore, it is enough to solve (1.1) in $\mathbb{Z}_p^*$, where $a\in\mathbb{Z}_p^*$. The main idea to find a solvability criterion for some polynomial equations over $\mathbb{Z}_p^*$ is to apply Hensel's Lemma in a suitable form to the given equation.

Lemma 2.1 *(Hensel's Lemma). (See [1].) Let $f(x)$ 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 that*

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

Then $f(x)$ has a p-adic integer root x_0 such that $x_0\equiv\theta \pmod{p^{i+1}}$.

3. Auxiliary results

The proof of the following lemma is straightforward.

Lemma 3.1. *Let p be a prime, α and s be two positive integers. If $p=2$ assume that $\alpha\geqslant 2$.*

(i) *For all $x,y\in\mathbb{Z}_p$, we have $(x+p^\alpha y)^p\equiv x^p+p^{\alpha+1}x^{p-1}y \pmod{p^{\alpha+2}}$;*
(ii) *For all $x\in\mathbb{Z}_p^*$, $y\in\mathbb{Z}_p$ we have $(x+p^\alpha y)^{p^s}\equiv x^{p^s}+p^{\alpha+s}y \pmod{p^{\alpha+s+1}}$;*
(iii) *For every $x\in\mathbb{Z}_p^*$ we have $x^{p^s}\equiv 1 \pmod{p^{s+2}}$.*

By means of the previous lemma, we can prove the following result.

Lemma 3.2. *Let p be a prime, $q=p^s$ where $s\in\mathbb{N}$, and $a\in\mathbb{Z}_p^*$. Let $k_0=s+1$ if $p\neq 2$ and $k_0=s+2$ if $p=2$. The equation*

[2] Note that in [5] we have used other applications of these methods for cubic equations over $\mathbb{Q}_p$.

$$x^q \equiv a \pmod{p^k} \tag{3.1}$$

has a solution in $\mathbb{Z}$ for all $k \in \mathbb{N}$ iff it has a solution in $\mathbb{Z}$ for some $k \geqslant k_0$.

Proof. The "only if" part is clear. Let Eq. (3.1) have a solution $x_n \in \mathbb{Z}$ for $k = n$, where $n \geqslant k_0$. Now we want to show that $x_{n+1} = x_n + \varepsilon p^{n-s}$ is a solution of (3.1) for $k = n + 1$, where

$$\varepsilon = a_n - \frac{x_n^q - a_0 - a_1 \cdot p - \cdots - a_{n-1} \cdot p^{n-1}}{p^n}.$$

One can easily check (due to Lemma 3.1) that

$$x_{n+1}^q \equiv x_n^q + \varepsilon \cdot p^n \pmod{p^{n+1}}.$$

We obtain that $x_{n+1}^q \equiv a \pmod{p^{n+1}}$. □

4. A criterion for the existence of a solution in $\mathbb{Z}_p^*$ with $p > 2$

Recall that $a \in \mathbb{Z}$ is called *an m-th power residue modulo p* if the congruence equation $x^m \equiv a \pmod{p}$ has a solution in $\mathbb{Z}$. Let $p > 2$ and $(a, p) = 1$. It is well-known (see [6]) that $a \in \mathbb{Z}$ is an m-th power residue modulo p if and only if $a^{\frac{p-1}{d}} \equiv 1 \pmod{p}$, where $d = (m, p-1)$.

Theorem 4.1. *Let $p > 2$ be a prime, $q = mp^s$ where $p \nmid m$ with $s \geqslant 0$, and $d = (m, p-1)$. Eq. (1.1) with $a \in \mathbb{Z}_p^*$ has a solution in $\mathbb{Z}_p^*$ if and only if*

(i) *a_0 is an m-th power residue modulo p, i.e., $a_0^{\frac{p-1}{d}} \equiv 1 \pmod{p}$;*
(ii) *$a_0^{p^s} \equiv a \pmod{p^{s+1}}$.*

Proof. We shall consider two cases $(p, q) = 1$ and $q = p^s$, where $s \geqslant 1$. The general case $q = mp^s$ can be easily derived from the mentioned cases.

Case I. Let $(p, q) = 1$. Suppose that Eq. (1.1) has a solution $x \in \mathbb{Z}_p^*$. Then $x_0^q \equiv a_0 \pmod{p}$, i.e. a_0 is a q-th power residue modulo p.

Suppose that a_0 is a q-th power residue modulo p, i.e. there is $\bar{x} \in \mathbb{Z}$ such that $\bar{x}^q \equiv a_0 \pmod{p}$. Let us consider the polynomial $f_{a,q}(x) = x^q - a$. Then, it is clear that $f_{a,q}(\bar{x}) = \bar{x}^q - a \equiv a_0 - a \equiv 0 \pmod{p}$. On the other hand, we get $f'_{a,q}(\bar{x}) = q\bar{x}^{q-1} \not\equiv 0 \pmod{p}$. Therefore, due to Hensel's Lemma 2.1, we conclude that (1.1) has a solution $x \in \mathbb{Z}_p^*$.

Case II. Let $q = p^s$ where $s \geqslant 1$. Suppose that (1.1) has a solution $x \in \mathbb{Z}_p^*$. Then, by Lemma 3.1(ii) $a = x_0^q + p^{s+1}x_1 \pmod{p^{s+2}}$. This yields that $x_0^q \equiv a \pmod{p^{s+1}}$. Since $x_0^q \equiv a_0 \pmod{p}$ and $x_0^p \equiv x_0 \pmod{p}$, we obtain that $x_0 = a_0$ and $a_0^q \equiv a \pmod{p^{s+1}}$.

Suppose that $a_0^q \equiv a \pmod{p^{s+1}}$. According to Lemma 3.2, there is $\bar{x} \in \mathbb{Z}$ such that $\bar{x}^q \equiv a \pmod{p^{2s+1}}$. We want to show that (1.1) has a solution in $\mathbb{Z}_p^*$. In fact, let us consider the same function $f_{a,q}(x) = x^q - a$. We then get that $f_{a,q}(\bar{x}) \equiv 0 \pmod{p^{2s+1}}$. It is clear that $f'_{a,q}(\bar{x}) = q\bar{x}^{q-1} \equiv 0 \pmod{p^s}$, and $f'_{a,q}(\bar{x}) = q\bar{x}^{q-1} \not\equiv 0 \pmod{p^{s+1}}$. Therefore, Hensel's Lemma 2.1 implies that (1.1) has a solution $x \in \mathbb{Z}_p^*$. □

5. A criterion for the existence of a solution in $\mathbb{Z}_2^*$

Theorem 5.1. *Let $q \in \mathbb{N}$ and $a \in \mathbb{Z}_2^*$.*

(i) *If q is odd then Eq. (1.1) has a solution in $\mathbb{Z}_2^*$ for any $a \in \mathbb{Z}_2^*$.*
(ii) *If $q = 2^s m$, where m is odd and $s \geqslant 1$ then Eq. (1.1) has a solution in $\mathbb{Z}_2^*$ if and only if $a \equiv 1 \pmod{2^{s+2}}$.*

Proof. (i) Let q be odd. We shall consider the same function $f_{a,q}(x) = x^q - a$ as before. It is clear that $f_{a,q}(1) \equiv 0 \pmod 2$ and $f'_{a,q}(1) \not\equiv 0 \pmod 2$. Due to Hensel's Lemma 2.1, Eq. (1.1) has a solution $x \in \mathbb{Z}_2^*$.

(ii) We consider only the case $q = 2^s$ where $s \geqslant 1$. The general case $q = 2^s m$ can be easily derived from this case.

Suppose that (1.1) has a solution x in $\mathbb{Z}_2^*$. Then due to Lemma 3.1(iii) we have that $a \equiv 1 \pmod{2^{s+2}}$.

Suppose that $a \equiv 1 \pmod{2^{s+2}}$. According to Lemma 3.2, there is $\bar{x} \in \mathbb{Z}$ such that $\bar{x}^q \equiv a \pmod{2^{2s+1}}$. We again consider the same function $f_{a,q}(x) = x^q - a$. We then obtain that $f_{a,q}(\bar{x}) \equiv 0 \pmod{p^{2s+1}}$. One can see that $f'_{a,q}(\bar{x}) \equiv 0 \pmod{2^s}$ and $f'_{a,q}(\bar{x}) \not\equiv 0 \pmod{2^{s+1}}$. So, Hensel's Lemma 2.1 implies that (1.1) has a solution $x \in \mathbb{Z}_2^*$. □

6. When −1 is the power of some p-adic integer

We are now ready to describe all p, q in which -1 is a q-th power of some p-adic integer.

Proposition 6.1. *Let p be an odd prime and $q \in \mathbb{N}$ with $q \geqslant 2$.*

(i) *The number -1 is any odd power of some 2-adic integer and is not any even power of any 2-adic integer;*
(ii) *If $q = mp^s$ where $p \nmid m$ with $s \geqslant 1$ then the number -1 is a q-th power of some p-adic integer if and only if $\frac{p-1}{(m,p-1)}$ is even.*

Proof. The statement (i) is obvious. We shall prove (ii).

According to Theorem 4.1, -1 is a q-th power of some p-adic integer if and only if $p-1$ is an m-th power residue modulo p and $(p-1)^{p^s} \equiv -1 \pmod{p^{s+1}}$. The last congruence always holds true. However, it is clear that $p-1$ is an m-th power residue modulo p if and only if $\frac{p-1}{(m,p-1)}$ is even. □

Acknowledgments

The authors wish to express their gratitude to an anonymous referee for several helpful comments concerning a nice and compact presentation of the paper. The present study has been done within IIUM Endowment grant EDW A12-621-1412. A part of this work was done at the Abdus Salam International Center for Theoretical Physics (ICTP), Trieste, Italy. The first author thanks the ICTP for providing financial support during his visit as a Junior Associate at the centre.

References

[1] Z.I. Borevich, I.R. Shafarevich, Number Theory, Academic Press, New York, 1966.
[2] J.M. Casas, B.A. Omirov, U.A. Rozikov, Solvability criteria for the equation $x^q = a$ in the field of p-adic numbers, arXiv:1102.2156.
[3] A.Kh. Khudoyberdiyev, T.K. Kurbanbaev, B.A. Omirov, Classification of three-dimensional solvable p-adic Leibniz algebras, P-Adic Numbers Ultrametric Anal. Appl. 2 (2010) 207–221.
[4] N. Koblitz, p-adic Numbers, p-adic Analysis, and Zeta Functions, Springer, New York, 1984.
[5] F. Mukhamedov, B. Omirov, M. Saburov, On cubic equations over p-adic field, arXiv:1204.1743.
[6] K.H. Rosen, Elementary Number Theory and Its Applications, Pearson, 2011.