BULLETIN *of the*
MALAYSIAN MATHEMATICAL
SCIENCES SOCIETY
http://math.usm.my/bulletin

Bull. Malays. Math. Sci. Soc. (2) **37**(3) *(2014), 853–863*

Solvability Criteria for the Equation $x^q = a$ in the Field of p-adic Numbers

[1]J. M. CASAS, [2]B. A.OMIROV AND [3]U. A. ROZIKOV
[1]Department of Applied Mathematics, E.U.I.T. Forestal, University of Vigo, 36005, Pontevedra, Spain
[2,3] Institute of Mathematics, Tashkent, Uzbekistan
[1]jmcasas@uvigo.es, [2]omirovb@mail.ru and [3]rozikovu@yandex.ru

Abstract. We establish the solvability criteria for the equation $x^q = a$ in the field of p-adic numbers, for any q in two cases: (i) q is not divisible by p; (ii) $q = p$. Using these criteria we show that any p-adic number can be represented in finitely many different forms and we describe the algorithms to obtain the corresponding representations. Moreover it is shown that solvability problem of $x^q = a$ for any q can be reduced to the cases (i) and (ii).

2010 Mathematics Subject Classification: 11S05

Keywords and phrases: p-adic number, solvability of an equation, congruence.

1. Introduction

The p-adic number system for any prime number p extends the ordinary arithmetic of the rational numbers in a way different from the extension of the rational number system to the real and complex number systems. This extension is achieved by an alternative interpretation of the concept of absolute value.

First described by Kurt Hensel in 1897, the p-adic numbers were motivated primarily by an attempt to bring the ideas and techniques of power series methods into number theory. Their influence now extends far beyond this. For example, the field of p-adic analysis essentially provides an alternative form of calculus.

More formally, for a given prime p, the field $\mathbb{Q}_p$ of p-adic numbers is a completion of the rational numbers. On the field $\mathbb{Q}_p$ is also given a topology derived from a metric, which is itself derived from an alternative valuation on the rational numbers. This metric space is complete in the sense that every Cauchy sequence converges to a point in $\mathbb{Q}_p$. This is what allows the development of calculus on $\mathbb{Q}_p$ and it is the interaction of this analytic and algebraic structure which gives the p-adic number systems their power and utility.

For about a century after the discovery of p-adic numbers, they were mainly considered as objects of pure mathematics. However, numerous applications of these numbers to theoretical physics have been proposed in papers [1, 5, 10, 19], to quantum mechanics [8], to p-adic-valued physical observables [8] and many others [7, 18]. As in real case, to solve a

Communicated by Ang Miin Huey.
Received: June 2, 2012; *Revised:* July 29, 2012.

problem in p-adic case there arises an equation which must be solved in the field of p-adic numbers (see for example [11–13, 18]). For classification problems of varieties of algebras over a field $\mathbb{Q}_p$ of p-adic numbers one has to solve an equation of the form: $x^2 = a$. It is well known the criteria of solvability of this equation. In fact, in the classification of Leibniz algebras of dimensions less than 4 over a field $\mathbb{Q}_p$ (see [3, 9]) it is enough to solve the equation $x^2 = a$. However, in the classification tasks of larger dimensions one has to solve an equation of the form $x^q = a$, $q \geq 2$, in $\mathbb{Q}_p$. In this paper we present a criteria for solvability of the equation $x^q = a$ in $\mathbb{Q}_p$ (where p is a fixed prime number) for arbitrary q in two cases: $(q, p) = 1$ and $q = p$. Moreover, in the cases of existing the solutions of the equation we present the algorithm of finding the solutions. Also we show that any equation $x^q = a$ in $\mathbb{Q}_p$ can be reduced to both cases. Note that in [14] the same criterion has been proved by a different method.

2. Preliminaries

2.1. Solvability of congruences

The sources of the information in this subsection are [2, 4, 15]. If n is a positive integer, the integers between 1 and $n-1$ which are coprime to n (or equivalently, the congruence classes coprime to n) form a group with multiplication modulo n as the operation; it is denoted by $\mathbb{Z}_n^\times$ and is called the *group of units modulo n* or the group of primitive classes modulo n. Multiplicative group of integers modulo n is cyclic if and only if n is equal to $1, 2, 4, p^k$ or $2p^k$, where p^k is a power of an odd prime number. A generator of this cyclic group is called *a primitive root modulo n* or a primitive element of $\mathbb{Z}_n^\times$.

For any integers a, b and n, we say that a is congruent to b modulo n (notated $a \equiv b \mod n$) if $n \mid (b-a)$. The order of $\mathbb{Z}_n^\times$ is given by Euler's totient function $\varphi(n)$. Euler's theorem says that $a^{\varphi(n)} \equiv 1 \mod n$ for every a coprime to n; the smallest k for which $a^k \equiv 1 \mod n$ is called the multiplicative order of a modulo n. In other words, for a to be a primitive root modulo n, $\varphi(n)$ has to be the smallest power of a which is congruent to 1 mod n.

Lemma 2.1. *Suppose that $m \in \mathbb{N}$ has a primitive root r. If a is a positive integer with $(a, m) = 1$, then there is a unique integer x with $1 \leq x \leq \varphi(m)$ such that*

$$r^x \equiv a \mod m.$$

Definition 2.1. *If $m \in \mathbb{N}$ has a primitive root r and α is a positive integer with $(\alpha, m) = 1$, then the unique integer x, $1 \leq x \leq \varphi(m)$ and $r^x \equiv \alpha \mod m$ is called the index (or discrete logarithm) of α to the base r modulo m and denoted by* $\mathrm{ind}_r \alpha$.

In particular, $r^{\mathrm{ind}_r a} \equiv a \mod m$.

Theorem 2.1. *Let m be a positive integer with the primitive root r. If a, b are positive integers coprime to m and k is a positive integer, then*

(i) $\mathrm{ind}_r 1 \equiv 0 \mod \varphi(m)$

(ii) $\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r a + \mathrm{ind}_r b \mod \varphi(m)$

(iii) $\mathrm{ind}_r a^k \equiv k \cdot \mathrm{ind}_r a \mod \varphi(m)$.

Theorem 2.2. *If p is a prime number, $\alpha \in \mathbb{N}$, m is equal to p^α or $2p^\alpha$, $(n, \varphi(m)) = d$ then the congruence*

$$x^n \equiv a \mod m$$

has solution if and only if d divides $\mathrm{ind}_x a$. *In case of solvability the congruence equation has d solutions.*

Fermat's Little Theorem says: Let a be a nonzero integer, and let $p \nmid a$ be prime. Then $a^{p-1} \equiv 1 \mod p$.

Proposition 2.1. *Let* $a,b,n \in \mathbb{Z}$ *with* $n \neq 0$. *The congruence* $ax \equiv b \mod n$ *has solutions if and only if* $(a,n) \mid b$. *When the congruence has a solution* $x_0 \in \mathbb{Z}$ *then the full solution set is* $\{\frac{x_0+tn}{(a,n)} : t \in \mathbb{Z}\}$.

It follows that the equation $ax = b$ in $\mathbb{Z}_n$ has (a,n) solutions. In particular, if $(a,n) = 1$, then the equation $ax = b$ has unique solution in $\mathbb{Z}_n$.

2.2. Divisibility of binomial coefficients

(see [6]) In 1852, Kummer proved that if m and n are nonnegative integers and p is a prime number, then the largest power of p dividing $\binom{m+n}{m}$ equals p^c, where c is the number of carries when m and n are added in base p. Equivalently, the exponent of a prime p in $\binom{n}{k}$ equals the number of nonnegative integers j such that the fractional part of k/p^j is greater than the fractional part of n/p^j. It can be deduced from the fact that $\binom{n}{k}$ is divisible by $n/gcd(n,k)$. Another fact: an integer $n \geq 2$ is prime if and only if all the intermediate binomial coefficients $\binom{n}{k}$, $k = 1,\ldots,n-1$ are divisible by n.

2.3. p-adic numbers

Let $\mathbb{Q}$ be the field of rational numbers. Every rational number $x \neq 0$ can be represented in the form $x = p^r \frac{n}{m}$, where $r,n \in \mathbb{Z}$, m is a positive integer, $(p,n) = 1$, $(p,m) = 1$ and p is a fixed prime number. The p-adic norm of x is given by

$$|x|_p = \begin{cases} p^{-r} \text{ for } x \neq 0 \\ 0 \text{ for } x = 0. \end{cases}$$

This norm satisfies the so called strong triangle inequality

$$|x+y|_p \leq \max\{|x|_p, |y|_p\},$$

and this is a non-Archimedean norm.

The completion of $\mathbb{Q}$ with respect to p-adic norm defines the p-adic field which is denoted by $\mathbb{Q}_p$. Any p-adic number $x \neq 0$ can be uniquely represented in the canonical form

$$x = p^{\gamma(x)}(x_0 + x_1 p + x_2 p^2 + \cdots), \tag{2.1}$$

where $\gamma = \gamma(x) \in \mathbb{Z}$ and x_j are integers, $0 \leq x_j \leq p-1$, $x_0 > 0$, $j = 0,1,2,\ldots$ (see more details [7, 16, 18]). In this case $|x|_p = p^{-\gamma(x)}$.

Theorem 2.3. [4, 7, 18] *In order to the equation* $x^2 = a$, $0 \neq a = p^{\gamma(a)}(a_0 + a_1 p + \cdots), 0 \leq a_j \leq p-1$, $a_0 > 0$ *has a solution* $x \in \mathbb{Q}_p$, *it is necessary and sufficient that the following conditions are fulfilled:*

(i) $\gamma(a)$ *is even;*

(ii) a_0 *is a quadratic residue modulo p if* $p \neq 2$; $a_1 = a_2 = 0$ *if* $p = 2$.

In this paper we shall generalize this theorem.

3. Equation $x^q = a$

In this section we consider the equation $x^q = a$ in $\mathbb{Q}_p$, where p is a fixed prime number, $q \in \mathbb{N}$ and $a \in \mathbb{Q}_p$. Our goal is to find conditions under which the equation has a solution $x \in \mathbb{Q}_p$. The case $q = 2$ is well known (see Theorem 2.3), therefore we consider $q > 2$.

We need the following

Lemma 3.1. *The following are true*

(i)

$$\left(\sum_{i=0}^{\infty} x_i p^i\right)^q = x_0^q + \sum_{k=1}^{\infty} \left(q x_0^{q-1} x_k + N_k(x_0, x_1, \dots, x_{k-1})\right) p^k, \tag{3.1}$$

where $x_0 \neq 0$, $0 \leq x_j \leq p-1$, $N_1 = 0$ *and for* $k \geq 2$

$$N_k = N_k(x_0, \dots, x_{k-1}) = \sum_{\substack{m_0, m_1, \cdots, m_{k-1}: \\ \sum_{i=0}^{k-1} m_i = q, \ \sum_{i=1}^{k-1} i m_i = k}} \frac{q!}{m_0! m_1! \cdots m_{k-1}!} x_0^{m_0} x_1^{m_1} \cdots x_{k-1}^{m_{k-1}}. \tag{3.2}$$

(ii) *Let* $q = p$ *be a prime number, then* $p \mid N_k$ *if and only if* $p \nmid k$.

Proof. (i) Formulas (3.1) and (3.2) easily can be obtained by using multinomial theorem. (ii) The following formula is known:

$$\frac{p!}{m_0! m_1! \cdots m_{k-1}!} = \binom{m_0}{m_0} \binom{m_0 + m_1}{m_1} \cdots \binom{m_0 + m_1 + \cdots + m_{k-1}}{m_{k-1}}. \tag{3.3}$$

By the condition $\sum_{i=0}^{k-1} m_i = p$ we get $0 \leq m_i \leq p$. Moreover if $m_{i_0} = p$ for some i_0, then $m_i = 0$ for all $i \neq i_0$. In this case from the condition $\sum_{i=1}^{k-1} i m_i = k$ we obtain $k = i_0 p$.

Assume $p \mid k$, i.e., $k = pk_0$ for some k_0, where $1 \leq k_0 < k-1$. Putting $m_{k_0} = p$ and $m_i = 0$ for $i \neq k_0$, we get $N_k(x_0, \dots, x_{k-1}) = x_{k_0}^p + S_k$, where

$$S_k = \sum_{\substack{0 \leq m_0, m_1, \dots, m_{k-1} < p: \\ \sum_{i=0}^{k-1} m_i = p, \ \sum_{i=1}^{k-1} i m_i = k}} \frac{p!}{m_0! m_1! \cdots m_{k-1}!} x_0^{m_0} x_1^{m_1} \dots x_{k-1}^{m_{k-1}}.$$

Since $x_{k_0}^p$ is not a multiple of p (otherwise, if we assume that $r^p = pT$ for some $r \in \{2, \dots, p-1\}$ and $T \in \mathbb{N}$, then it follows that r divides T since p is a prime number. Hence, $r^{p-1} = pT'$, where $T' = T/r$. By the same way we get $r^{p-2} = pT''$ and iterating the process finally we get $1 = p\tilde{T}$, for some $\tilde{T} \in \mathbb{N}$, which is not possible), but S_k is divisible by p since each coefficient of S_k contains (see formula (3.3)) a factor $\binom{p}{m_{i_0}}$ (with $0 < m_{i_0} < p$) which is divisible by p thanks to the divisibility property of binomial coefficients mentioned in the previous section. Therefore $p \nmid N_k$.

Assume $p \nmid k$ then by the arguments mentioned above we get $m_i < p$, for all $i = 0, \dots, k-1$, therefore each term of N_k is divisible by p consequently $p \mid N_k$. ∎

3.1. *The case* $(q, p) = 1$. In this subsection we are going to analyze under what conditions the equation $x^q = a$ has solution in $\mathbb{Q}_p$, when q and p are coprimes. In this case the following is true.

Theorem 3.1. *Let* $q > 2$ *and* $(q, p) = 1$. *The equation*

$$x^q = a, \tag{3.4}$$

$0 \neq a = p^{\gamma(a)}(a_0 + a_1 p + \cdots)$, $0 \leq a_j \leq p-1$, $a_0 \neq 0$, *has a solution* $x \in \mathbb{Q}_p$ *if and only if*

(1) q *divides* $\gamma(a)$*;*

(2) a_0 *is a* q *residue* $\mod p$.

Proof. Necessity. Assume that equation (3.4) has a solution

$$x = p^{\gamma(x)}(x_0 + x_1 p + \cdots), \quad 0 \leq x_j \leq p-1, x_0 \neq 0,$$

then

$$p^{q\gamma(x)}(x_0 + x_1 p + \cdots)^q = p^{\gamma(a)}(a_0 + a_1 p + \cdots), \tag{3.5}$$

i.e., $\gamma(a) = q\gamma(x)$ and $a_0 \equiv x_0^q \mod p$.

Sufficiency. Let a satisfies the conditions (1) and (2). We construct a solution x of equation (3.4) using the idea of reduction to canonical form of a p-adic number using a system of carries. Put

$$\gamma(x) = \frac{1}{q}\gamma(a).$$

Then by the condition (2) and due to $1 \leq a_0 \leq p-1$ there exists x_0 such that

$$x_0^q \equiv a_0 \mod p, \quad 1 \leq x_0 \leq p-1.$$

In other words, there exists $M_1(x_0)$ such that $x_0^q = a_0 + M_1(x_0)p$.

Using the notations of Lemma 3.1 due to the fact that qx_0^{q-1} is not a multiple of p, (see Proposition 2.1) there exists x_1 such that

$$qx_0^{q-1}x_1 + N_1(x_0) + M_1(x_0) \equiv a_1 \mod p, \quad 1 \leq x_1 \leq p-1.$$

Therefore, there exists $M_2(x_0, x_1)$ such that $qx_0^{q-1}x_1 + N_1(x_0) + M_1(x_0) = a_1 + M_2(x_0, x_1)p$.

Proceeding in this way, we find the existence of x_n such that

$$qx_0^{q-1}x_n + N_n(x_0, \ldots, x_{n-1}) + M_n(x_0, \ldots, x_{n-1}) \equiv a_n \mod p, \quad 1 \leq x_n \leq p-1.$$

and $M_{n+1}(x_0, \ldots, x_n)$ such that

$$qx_0^{q-1}x_n + N_n(x_0, \ldots, x_{n-1}) + M_n(x_0, \ldots, x_{n-1}) = a_n + M_{n+1}(x_0, \ldots, x_n)p \tag{3.6}$$

for any $n \in \mathbb{N}$.

Now from Lemma 3.1 and equality (3.6) it follows that

$$\begin{aligned}\left(\sum_{i=0}^{\infty} x_i p^i\right)^q &= x_0^q + \sum_{k=1}^{\infty}\left(qx_0^{q-1}x_k + N_k(x_0, x_1, \ldots, x_{k-1})\right)p^k \\ &= a_0 + M_1(x_0)p + \sum_{k=1}^{\infty}\left(a_k - M_k(x_0, \ldots, x_{k-1}) + M_{k+1}(x_0, \ldots, x_k)p\right)p^k \\ &= a_0 + \sum_{k=1}^{\infty} a_k p^k.\end{aligned}$$

Hence, we found solution $x = \sum_{i=0}^{\infty} x_i p^i$ of equation (3.4) in its canonical form. ∎

Remark 3.1. The condition (2) of Theorem 3.1 is always satisfied if $p = 2$, consequently $x^q = a$ has a solution in $\mathbb{Q}_2$ for any odd q and any $a \in \mathbb{Q}_2$ with $\gamma(a)$ divisible by q.

Corollary 3.1. *Let q be a prime number such that $q < p$ and η be a p-adic unity (i.e. $|\eta|_p = 1$) which is not the q-th power of some p-adic number. Then $p^i\eta^j$, $i,j = 0,1,\dots,q-1$ ($i+j \neq 0$) is not the q-th power of some p-adic number.*

Proof. We shall check that the conditions of Theorem 3.1 fail under the hypothesis. It is easy to see that $\gamma(p^i\eta^j) = i$ for all $i = 1,\dots,q-1$ and $j = 0,\dots,q-1$, consequently q does not divide $\gamma(p^i\eta^j)$, i.e. the condition (1) is not satisfied. But for η^j, $i = 0$, $j = 2,\dots,q-1$ the condition (1) is satisfied, therefore we shall check the condition (2).

Consider the decomposition $\eta = \eta_0 + \eta_1 p + \cdots$, then $\eta^j = \eta_0^j + j\eta_0^{j-1}\eta_1 p + \cdots$. It is known (see Theorem 2.1) that $\eta_0^j \equiv a_0^q \mod p$ has a solution η_0 if and only if $\mathrm{ind}_{a_0}\eta_0^j$ is divisible by $d = (p-1,q)$.

Since η is a unity which is not the q-th power of some p-adic number we have $\eta_0 \equiv a_0^q \mod p$ has not solution thus $\mathrm{ind}_{a_0}\eta_0$ is not divisible by $d = (p-1,q)$. This property implies that for a prime q with $q < p$ the prime number p has a form $p = qk+1$. Consequently, $d = (p-1,q) = (qk,q) = q$.

If $\mathrm{ind}_{a_0}\eta_0 = dl + r$, then $\mathrm{ind}_{a_0}\eta_0^j \equiv j(ql+r) \mod (p-1)$, i.e., $\mathrm{ind}_{a_0}\eta_0^j = j(ql+r) + M(p-1) = q(jl+Mk) + jr$, but since $0 < r < q-1$, $2 \le j \le q-1$ and q is a prime number, jr is not divisible by q. Thus $\mathrm{ind}_{a_0}\eta_0^j$ is not divisible by $d = q$, hence the condition (2) is not satisfied. ∎

Corollary 3.2. *Let q be a prime number such that $q < p = qk+1$, for some $k \in \mathbb{N}$ and η be a unity which is not the q-th power of some p-adic number. Then any p-adic number x can be written in one of the following forms $x = \varepsilon_{ij}y_{ij}^q$, where $\varepsilon_{ij} \in \{p^i\eta^j : i,j = 0,1,\dots,q-1\}$ and $y_{ij} \in \mathbb{Q}_p$.*

Proof. Let $\eta = \eta_0 + \eta_1 p + \cdots$ and $\mu = \mu_0 + \mu_1 p + \cdots$ be unities which are not the q-th power of some p-adic numbers.

We shall show that there exists $i \in \{1,\dots,q-1\}$ such that $\mu = \eta^i y^q$ for some $y \in \mathbb{Q}_p$.

Note that η^i and $\frac{1}{\eta^i}$, $i = 1,\dots,q-1$ are not the q-th power of some p-adic numbers. Consider $\mu = \mu_0 + \mu_1 p + \cdots$ and $\frac{1}{\eta^i} = c_{0i} + c_{1i}p + \cdots$, then $\frac{\mu}{\eta^i} = \mu_0 c_{0i} + (\mu_1 c_{0i} + \mu_0 c_{1i})p + \cdots$.

It is easy to see that $\gamma(\mu/\eta^i) = 0$, consequently the condition (1) of Theorem 3.1 is satisfied. Indeed, if $\mu_0 c_{0i} = pM$, then since p is a prime number, the last equality is possible if and only if μ_0 and c_{0i} divide M, consequently we get $1 = p\tilde{M}$, which is impossible.

Now we shall check the condition (2) of Theorem 3.1.

The equation $x_0^q \equiv \mu_0 c_{0i} \mod p$ has a solution if and only if $\mathrm{ind}_{x_0}\mu_0 c_{0i}$ is divisible by $q = (q, p-1)$ (see Theorem 2.2). We have that $c_{0i} \equiv c_{01}^i \mod p$, consequently $\mathrm{ind}_{x_0}\mu_0 c_{0i} \equiv \mathrm{ind}_{x_0}\mu_0 + i\,\mathrm{ind}_{x_0}c_{01} \mod (p-1)$. Assume $\mathrm{ind}_{x_0}\mu_0 = s$, $\mathrm{ind}_{x_0}c_{01} = r$, $s,r = 1,\dots,q-1$ and take i such that $ir \equiv q-s \mod (p-1)$ (the existence of i follows from the fact that $(r,p-1) = 1$). It is clear that if s varies from 1 to $q-1$ then i also varies in $\{1,\dots,q-1\}$. Consequently we get $\mathrm{ind}_{x_0}\mu_0 c_{0i} \equiv s + ir \mod (p-1) \equiv q \mod (p-1)$. Hence the condition (2) in Theorem 3.1 is also satisfied, so there is a number i such that $\mu = \eta^i y_i^q$, for some $y_i \in \mathbb{Q}_p$.

For $x \in \mathbb{Q}_p$, let $x = p^{\gamma(x)}(x_0 + x_1 p + \cdots)$ and denote $\nu = x_0 + x_1 p + \cdots$ If ν satisfies conditions of Theorem 3.1, then $\nu = y^q$ and $x = p^{\gamma(x)}y^q$. If ν does not satisfy conditions of Theorem 3.1, then (as it was showed above) there exists i such that $\nu = \eta^i y^q$ and in this case we get $x = p^{\gamma(x)}\eta^i y^q$. Taking $\gamma(x) = qN + j$ completes the proof. ∎

Corollary 3.3. *Let q be a prime number such that $q < p \neq qk+1$, for any $k \in \mathbb{N}$. Then any p-adic number x can be written in one of the following forms $x = \varepsilon_i y_i^q$, where $\varepsilon_i \in \{p^i : i = 0,1,\dots,q-1\}$ and $y_i \in \mathbb{Q}_p$.*

Proof. Using arguments in the proof of Corollary 3.2 we conclude that if $p \neq qk+1$ then any unity is the q-th power of a p-adic number. Hence for $x \in \mathbb{Q}_p$ with $\gamma(x) = qN+i$ we get $x = p^i y^q$, $y \in \mathbb{Q}_p$. ∎

3.2. *The case $q = p$.* Now we are going to analyze the solvability conditions for the equation $x^p = a$ in $\mathbb{Q}_p$. In this case, the following is true.

Theorem 3.2. *Let $q = p$. The equation $x^q = a$, $0 \neq a = p^{\gamma(a)}(a_0 + a_1 p + \cdots)$, $0 \le a_j \le p-1$, $a_0 \neq 0$, has a solution $x \in \mathbb{Q}_p$ if and only if*

(i) *p divides $\gamma(a)$;*

(ii) $a_0^p \equiv a_0 + a_1 p \mod p^2$.

Proof. Necessity. Assume that equation (3.4) has a solution

$$x = p^{\gamma(x)}(x_0 + x_1 p + \cdots), \quad 0 \le x_j \le p-1, x_0 \neq 0,$$

then using Lemma 3.1 we get

$$a = p^{p\gamma(x)}(x_0 + x_1 p + \cdots)^p = p^{p\gamma(x)}\left(x_0^p + \sum_{k=1}^{\infty}(p x_0^{p-1} x_k + N_k)p^k\right). \tag{3.7}$$

Using part (ii) of Lemma 3.1, we get RHS of (3.7)

$$\begin{aligned}
&p^{p\gamma(x)}\left(x_0^p + \sum_{\substack{k=1\\ p|k}}^{\infty} x_0^{p-1} x_k p^{k+1} + \sum_{\substack{k=1\\ p|k}}^{\infty} N_k p^k + \sum_{\substack{k=1\\ p\nmid k}}^{\infty}(x_0^{p-1}x_k + p^{-1}N_k)p^{k+1}\right)\\
&= p^{p\gamma(x)}\left(x_0^p + \sum_{k=1}^{\infty} x_0^{p-1} x_{pk} p^{pk+1} + \sum_{k=1}^{\infty} N_{pk} p^{pk}\right.\\
&\quad \left. + \sum_{i=1}^{p-1}\sum_{k=0}^{\infty}(x_0^{p-1}x_{pk+i} + p^{-1}N_{pk+i})p^{pk+i+1}\right)\\
&= p^{p\gamma(x)}\left(x_0^p + \sum_{i=1}^{p-2}(x_0^{p-1}x_i + p^{-1}N_i)p^{i+1} + \sum_{k=1}^{\infty}(x_0^{p-1}x_{pk-1} + N_{pk} + p^{-1}N_{pk-1})p^{pk}\right.\\
&\quad \left. + \sum_{k=1}^{\infty} x_0^{p-1} x_{pk} p^{pk+1} + \sum_{i=1}^{p-2}\sum_{k=1}^{\infty}(x_0^{p-1}x_{pk+i} + p^{-1}N_{pk+i})p^{pk+i+1}\right).
\end{aligned} \tag{3.8}$$

We have

$$N_{pk} = \sum_{\substack{m_0,\dots,m_{pk-1}:\\ \sum_{i=0}^{pk-1} m_i = p,\ \sum_{i=1}^{pk-1} i m_i = pk}} \frac{p!}{m_0!\cdots m_{pk-1}!} x_0^{m_0}\cdots x_{pk-1}^{m_{pk-1}}$$

$$= p(p-1)x_0^{p-2}x_1 x_{pk-1} + \tilde{N}_{pk}, \tag{3.9}$$

where $\tilde{N}_{pk}$ does not depend on x_{pk-1}; moreover $p \nmid \tilde{N}_{pk}$.

Using (3.9), from (3.8) we get RHS of (3.7)

$$
\begin{aligned}
p^{p\gamma(x)}\Bigg(& x_0^p + \sum_{i=1}^{p-2}(x_0^{p-1}x_i + p^{-1}N_i)p^{i+1} + \sum_{k=1}^{\infty}(x_0^{p-1}x_{pk-1} + \tilde{N}_{pk} + p^{-1}N_{pk-1})p^{pk} \\
& + \sum_{k=1}^{\infty}(x_0^{p-1}x_{pk} - x_0^{p-2}x_1x_{pk-1})p^{pk+1} \\
& + \sum_{k=1}^{\infty}(x_0^{p-1}x_{pk+1} + x_0^{p-2}x_1x_{pk-1} + p^{-1}N_{pk+1})p^{pk+2} \\
& + \sum_{i=2}^{p-2}\sum_{k=1}^{\infty}(x_0^{p-1}x_{pk+i} + p^{-1}N_{pk+i})p^{pk+i+1}\Bigg). \qquad (3.10)
\end{aligned}
$$

Consequently, $\gamma(a) = p\gamma(x)$, and $x_0^p \equiv a_0 + a_1 p \mod p^2$, $x_0 = a_0$.

Sufficiency. Assume that a satisfies the conditions (i) and (ii). We shall construct a solution x of the equation $x^p = a$ using the similar process of reduction to canonical form as in the proof of Theorem 3.1. First put

$$\gamma(x) = \frac{1}{p}\gamma(a).$$

Denote $x_0 = a_0$ and let M_1 be such that $x_0^q = a_0 + a_1 p + M_1 p^2$.

Proceeding in this way, since x_0^{p-1} is not a multiple of p and taking into account that integer numbers N_k (see Lemma 3.1) depend only on $x_0, x_1, \ldots, x_{k-1}$ and $\tilde{N}_{pk}$ depends only on $x_0, x_1, \ldots, x_{pk-2}$ we find the existence of x_n and introduce corresponding number M_{n+1} consequently for each $n \geq 1$ such that the following congruences hold:

(1) $$x_0^{p-1}x_i + p^{-1}N_i + M_i \equiv a_{i+1} \mod p,$$

therefore, there exists M_{i+1} such that $x_0^{p-1}x_i + p^{-1}N_i + M_i = a_{i+1} + M_{i+1}p$ for $0 \leq x_i \leq p-1$, $i = 1, \ldots, p-2$;

(2) $$x_0^{p-1}x_{pk-1} + \tilde{N}_{pk} + p^{-1}N_{pk-1} + M_{pk-1} \equiv a_{pk} \mod p,$$

therefore, there exists M_{pk} such that $x_0^{p-1}x_{pk-1} + \tilde{N}_{pk} + p^{-1}N_{pk-1} + M_{pk-1} = a_{pk} + M_{pk}p$ for $k = 1, 2, \ldots$;

(3) $$x_0^{p-1}x_{pk} - x_0^{p-2}x_1x_{pk-1} + M_{pk} \equiv a_{pk+1} \mod p,$$

therefore, there exists M_{pk+1} such that $x_0^{p-1}x_{pk} - x_0^{p-2}x_1x_{pk-1} + M_{pk} = a_{pk+1} + M_{pk+1}p$ for $k = 1, 2, \ldots$;

(4) $$x_0^{p-1}x_{pk+1} + x_0^{p-2}x_1x_{pk-1} + p^{-1}N_{pk+1} + M_{pk+1} \equiv a_{pk+2} \mod p,$$

therefore, there exists M_{pk+2} such that $x_0^{p-1}x_{pk+1} + x_0^{p-2}x_1x_{pk-1} + p^{-1}N_{pk+1} + M_{pk+1} = a_{pk+2} + M_{pk+2}p$ for $k = 1, 2, \ldots$;

(5) $$x_0^{p-1}x_{pk+i} + p^{-1}N_{pk+i} + M_{pk+i} \equiv a_{pk+i+1} \mod p,$$

therefore, there exists M_{pk+i+1} such that $x_0^{p-1}x_{pk+i} + p^{-1}N_{pk+i} + M_{pk+i} = a_{pk+i+1} + M_{pk+i+1}p$ for $i = 2, \ldots, p-2$, $k = 1, 2, \ldots$. Now making the substitutions above into equality (3.10)

we obtain RHS of (3.10)

$$
\begin{aligned}
&p^{p\gamma(x)}\Bigg(a_0+a_1p+M_1p^2+\sum_{i=1}^{p-2}(a_{i+1}-M_i+M_{i+1}p)p^{i+1}+\sum_{k=1}^{\infty}(a_{pk}-M_{pk-1}+M_{pk}p)p^{pk}\\
&\quad+\sum_{k=1}^{\infty}(a_{pk+1}-M_{pk}+M_{pk+1}p)p^{pk+1}+\sum_{k=1}^{\infty}(a_{pk+2}-M_{pk+1}+M_{pk+2}p)p^{pk+2}\\
&\quad+\sum_{i=2}^{p-2}\sum_{k=1}^{\infty}(a_{pk+i+1}-M_{pk+i}+M_{pk+i+1}p)p^{pk+i+1}\Bigg)\\
&=p^{p\gamma(x)}\left(\sum_{k=1}^{\infty}a_kp^k+M_1p^2-\sum_{k=1}^{\infty}(M_k-M_{k+1}p)p^{k+1}\right)\\
&=p^{\gamma(a)}\sum_{k=1}^{\infty}a_kp^k=a.
\end{aligned}
$$

Hence, we found the solution $x=\sum_{k=0}^{\infty}x_kp^k$ of the equation $x^p=a$. ∎

Corollary 3.4. *Let p be a prime number.*

(a) *The numbers $\varepsilon\in\mathscr{E}_1=\{1\}\cup\{i+jp : i^p \text{ is not equal } i+jp \text{ modulo } p^2\}$, $\delta\in\mathscr{E}_2=\{p^j : j=0,\dots,p-1\}$ and products $\varepsilon\delta$ are not the p-th power of some p-adic numbers.*

(b) *Any p-adic number x can be represented in one of the following forms $x=\varepsilon\delta y^p$, for some $\varepsilon\in\mathscr{E}_1$, $\delta\in\mathscr{E}_2$ and $y\in\mathbb{Q}_p$.*

Proof. (a) Follows from Theorem 3.2.

(b) If $x=x_0+x_1p+\cdots\neq y^p$ for any $y\in\mathbb{Q}_p$ then by Theorem 3.2 we have $\varepsilon=x_0+x_1p\in\mathscr{E}_1$. We shall show that $x/\varepsilon=(x_0+x_1p+x_2p^2+\cdots)/(x_0+x_1p)=b_0+b_1p+b_2p^2+\cdots$ is the p-th power of some $y\in\mathbb{Q}_p$, i.e., we check the conditions of Theorem 3.2: since $\gamma(x/\varepsilon)=0$ the condition (i) is satisfied; we have $x_0\equiv x_0b_0 \mod p$ and $x_0+x_1p\equiv x_0b_0+(x_0b_1+x_1b_0)p \mod p^2$ which implies that $b_0=1$ and $b_1=0$, consequently $b_0^p\equiv b_0+b_1 \mod p^2$ i.e., the condition (ii) is satisfied.

Thus if $x\in\mathbb{Q}_p$ has the form $x=y^p$, then $\varepsilon=\delta=1$. If $x=x_0+x_1p+\cdots$ is not the p-th power of some p-adic number with $\gamma(x)=pN+j$, then we take $\varepsilon=x_0+x_1p$, $\delta=p^j$ then $x=\varepsilon\delta y^p$ for some $y\in\mathbb{Q}_p$. ∎

Note that for a given $i\in\{1,\dots,p-1\}$ the congruence $i^p\equiv i+jp \mod p^2$ is not satisfied for some values of j. For example, if $p=3$, then for $j=1$ the congruence is not true. Using computer we get the following:

	Values of j s.t. $i^p \equiv i+jp \mod p^2$ has no solution $i \in \{1,\dots,p-1\}$
p=3	1
p=5	2
p=7	1, 3, 5
p=11	1, 4, 5, 6, 9
p=13	2, 3, 4, 8, 9, 10
p=17	1, 5, 8, 11, 15
p=19	4, 7, 8, 9, 10, 11, 14
p=23	3, 4, 6, 9, 10, 12, 13, 16, 18, 19
p=29	3, 5, 10, 11, 12, 13, 15, 17, 18, 23, 25
p=31	1, 2, 5, 6, 8, 9, 11, 15, 19, 21, 22, 24, 25, 28, 29
p=37	1, 4, 5, 6, 7, 10, 13, 14, 16, 20, 22, 26, 29, 30, 31, 32, 35
p=41	2, 4, 6, 8, 10, 16, 24, 26, 30, 32, 34, 36, 38

Remark 3.2. Using this table and Corollary 3.4 we obtain

$p=3$: Any $x \in \mathbb{Q}_3$ has form $x = \varepsilon\delta y^3$, where $\varepsilon \in \{1,4,5\}$, $\delta \in \{1,3,9\}$;

$p=5$: Any $x \in \mathbb{Q}_5$ has form $x = \varepsilon\delta y^5$, where $\varepsilon \in \{1,11,12,13,14\}$, $\delta \in \{1,5,25,125,625\}$;

$p=7$: Any $x \in \mathbb{Q}_7$ has form $x = \varepsilon\delta y^7$, where $\varepsilon \in \{1,8,9,10,11,12,13,22,23,24,25,26,27,28,36,37,38,39,40,41,42\}$, $\delta \in \{7^i : i = 0,1,\dots,6\}$.

Remark 3.3. In [17] using Krasners's Lemma a set of irreducible polynomials that defines all cubic extension of the field $\mathbb{Q}_3$ are determined.

3.3. *The case $q = mp^s$.* As is presented above, the proofs of the sufficient part of the solvability criteria in Theorems 3.1 and 3.2 are given in a constructive method. Thus we show not only the existence of a solution, but we also give the algorithm for the constructing of the solution in these cases. After cases 3.1 and 3.2 it remains the case $q = mp^s$ with some $m, s \in \mathbb{N}$, $(m,p) = 1$. Here we shall show that this case can be reduced to cases 3.1 and 3.2: we have to find the solvability condition for $x^{mp^s} = a$. Denoting $y = x^{p^s}$, we get $y^m = a$, which is the equation considered in case 3.1. Assume for the last equation the solvability condition is satisfied and its solution is $y = \tilde{y}$. Then we have to solve $x^{p^s} = \tilde{y}$; here we denote $z = x^{p^{s-1}}$ and get $z^p = \tilde{y}$. The last equation is the equation considered in case 3.2. Suppose it has a solution $z = \tilde{z}$ (i.e. the conditions of Theorem 3.2 are satisfied) then we get $x^{p^{s-1}} = \tilde{z}$ which again can be reduced to the case 3.2. Iterating the last argument after $s-1$ times we obtain $x^p = \tilde{a}$ for some $\tilde{a}$ which is also an equation corresponding to case 3.2. Consequently, by this argument we establish solvability condition of equation $x^{mp^s} = a$, which will be a system of solvability conditions for equations considered in cases 3.1 and 3.2.

Remark 3.4. Note that in [14] for the case 3.3. an explicit formula (condition) for the existence of solution is obtained.

References

[1] I. Y. Aref'eva, B. Dragovich, P. H. Frampton and I. V. Volovich, The wave function of the universe and p-adic gravity, *Internat. J. Modern Phys. A* **6** (1991), no. 24, 4341–4358.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, New York, 1976.

[3] Sh. A. Ayupov and T. K. Kurbanbaev, The classification of 4-dimensional p-adic filiform Leibniz algebras, *TWMS J. Pure Appl. Math.* **1** (2010), no. 2, 155–162.

[4] A. I. Borevich and I. R. Shafarevich, *Number Theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20, Academic Press, New York, 1966.

[5] P. G. O. Freund and E. Witten, Adelic string amplitudes, *Phys. Lett. B* **199** (1987), no. 2, 191–194.
[6] J. M. Holte, Asymptotic prime-power divisibility of binomial, generalized binomial, and multinomial coefficients, *Trans. Amer. Math. Soc.* **349** (1997), no. 10, 3837–3873.
[7] A. Khrennikov, *p-adic Valued Distributions in Mathematical Physics*, Mathematics and its Applications, 309, Kluwer Acad. Publ., Dordrecht, 1994.
[8] A. Yu. Khrennikov, p-adic quantum mechanics with p-adic valued functions, *J. Math. Phys.* **32** (1991), no. 4, 932–937.
[9] A. Kh. Khudoyberdiyev, T. K. Kurbanbaev and B. A. Omirov, Classification of three-dimensional solvable p-adic Leibniz algebras, *p-Adic Numbers Ultrametric Anal. Appl.* **2** (2010), no. 3, 207–221.
[10] E. Marinari and G. Parisi, On the p-adic five-point function, *Phys. Lett. B* **203** (1988), no. 1-2, 52–54.
[11] F. Mukhamedov and U. Rozikov, On rational p-adic dynamical systems, *Methods Funct. Anal. Topology* **10** (2004), no. 2, 21–31.
[12] F. M. Mukhamedov and U. A. Rozikov, On Gibbs measures of p-adic Potts model on the Cayley tree, *Indag. Math. (N.S.)* **15** (2004), no. 1, 85–99.
[13] F. Mukhamedov and U. Rozikov, On inhomogeneous p-adic Potts model on a Cayley tree, *Infin. Dimens. Anal. Quantum Probab. Relat. Top.* **8** (2005), no. 2, 277–290.
[14] F. Mukhamedov and M. Saburov, On equation $x^q = a$ over $\mathbb{Q}_p$, *J. Number Theory* **133** (2013), no. 1, 55–58.
[15] I. Niven and H. S. Zuckerman, *An Introduction to The Theory of Numbers*, fourth edition, John Wiley & Sons, New York, 1980.
[16] W. H. Schikhof, *Ultrametric Calculus*, Cambridge Studies in Advanced Mathematics, 4, Cambridge Univ. Press, Cambridge, 1984.
[17] P.-A. Svensson, Cubic extensions of the 3-adic number field, *Comment. Math. Univ. St. Paul.* **51** (2002), no. 1, 53–62.
[18] V. S. Vladimirov, I. V. Volovich and E. I. Zelenov, *p-adic Analysis and Mathematical Physics* (Russian), VO "Nauka", Moscow, 1994.
[19] I. V. Volovich, p-adic string, *Classical Quantum Gravity* **4** (1987), no. 4, L83–L87.