Сибирский математический журнал
Май—июнь, 2013. Том 54, № 3

УДК 511.53

О РАЗРЕШИМОСТИ КУБИЧЕСКИХ УРАВНЕНИЙ В МНОЖЕСТВЕ ЦЕЛЫХ p–АДИЧЕСКИХ ЧИСЕЛ ($p > 3$)

Ф. М. Мухамедов, Б. А. Омиров, М. Х. Сабуров, К. К. Масутова

Аннотация. Приведен критерий существования решений уравнения вида $x^3+ax = b$, где $a, b \in \mathbb{Q}_p$, в множестве целых p-адических чисел при $p > 3$. Более того, в случае, когда уравнение $x^3 + ax = b$ имеет решение, приведены необходимые и достаточные рекуррентные условия на p-адическое число $x \in \mathbb{Z}_p^*$, при котором оно является решением данного уравнения.

Ключевые слова: кубическое уравнение, p-адическое число, решение, алгоритм.

1. Введение

В настоящее время p-адический анализ является одним из бурно развивающихся направлений математики. Многочисленные приложения p-адических чисел нашли свое отражение в теории p-адических дифференциальных уравнений, p-адической теории вероятностей, p-адической математической физике и т. д. (см. [1–12]).

Известно, что p-адические числа также связаны с диофантовыми уравнениями по модулю возрастающих степеней простого числа p. Одним из простейших таких уравнений является уравнение вида $x^q = a$ над $\mathbb{Q}_p$, где $q \in \mathbb{N}$, $a \in \mathbb{Q}_p$. Критерий разрешимости данного уравнения с точки зрения алгебраической теории чисел дан в [13–15]. Однако следует отметить, что этот критерий не упоминается ни в одной классической монографии по p-адическому анализу (см. [16–18]), за исключением случая $q = 2$. Критерий существования решения упомянутого уравнения с точки зрения p-адического анализа был представлен в [19–22]. Заметим, что применение этого критерия позволило классифицировать алгебраические структуры над p-адическим полем (см. [23, 24]).

Напомним, что в поле комплексных чисел при $n>4$ известна фундаментальная теорема Абеля о неразрешимости общего уравнения n-й степени в радикалах. В этом же поле квадратное уравнение решается при помощи дискриминанта, а для кубического уравнения существуют формулы Кардано. В отличие от поля действительных чисел $\mathbb{R}$, вообще говоря, кубическое уравнение $ax^3 + bx^2 + cx + d = 0$ не всегда может иметь решение в $\mathbb{Q}_p$, где $a, b, c, d \in \mathbb{Q}_p$ ($a \neq 0$). Например, нетрудно проверить, что уравнение $x^3 = p$ не имеет решений в $\mathbb{Q}_p$. Поэтому естественно возникает вопрос нахождения критерия существования (на языке коэффициентов уравнения) решения кубического уравнения

Работа выполнена при финансовой поддержке MOHE (грант FRGS0409–109) и IIUM (грант EDW B13–029–0914).

в $\mathbb{Q}_p$. Известно, что в локальных полях существует общий метод нахождения решения кубических уравнений, так называемый метод Кардано. Однако этот метод не всегда обеспечивает существование решения всех кубических уравнений. Проиллюстрируем это на следующем примере.

Рассмотрим уравнение

$$x^3 - \frac{3}{p}x + \frac{p-3}{p} = 0$$

в $\mathbb{Q}_p$, где $p > 3$. Ясно, что $x_* = -1$ является решением данного уравнения. Согласно методу Кардано общее решение кубического уравнения ищется в виде $x = u + v$. Подставляя $x = u + v$ в уравнение, при помощи элементарных вычислений получим систему уравнений

$$\begin{cases} uv = \frac{1}{p}, \\ u^3 + v^3 = -\frac{p-3}{p}, \end{cases}$$

решение которой сводится к решению квадратного уравнения

$$z^2 + \frac{p-3}{p}z + \frac{1}{p^3} = 0$$

в $\mathbb{Q}_p$, где $z = u^3$. Однако число $\log_p \left|\left(\frac{p-3}{2p}\right)^2 - \frac{1}{p^3}\right|_p = 3$ нечетно. Последнее означает, что квадратное уравнение не имеет решения в $\mathbb{Q}_p$ (см. [12]). Следовательно, метод Кардано не всегда применим для всех кубических уравнений.

Стоит упомянуть тот факт, что достаточные условия существования решений таких уравнений в $\mathbb{Q}_p$ приведены в [14, 19, 20], необходимые условия до сих пор не были рассмотрены.

В силу того, что кубическое уравнение $y^3 + qy^2 + ry + s = 0$ заменой неизвестного $x = y - \frac{q}{3}$ приводится к уравнению вида

$$x^3 + ax = b, \tag{1}$$

в дальнейшем будем рассматривать кубическое уравнение (1) с коэффициентами $a, b \in \mathbb{Q}_p$. А именно, в настоящей работе представлен критерий существования решений уравнения (1) при $p > 3$. Известно (см. [16]), что в p-адическом анализе важными множествами являются следующие: $\mathbb{Q}_p$ — множество всех p-адических чисел, $\mathbb{Z}_p$ — множество всех целых p-адических чисел и $\mathbb{Z}_p^*$ — множество единиц в $\mathbb{Z}_p$. Данная работа посвящена существованию решений кубического уравнения в $\mathbb{Z}_p^*$ с коэффициентами из поля $\mathbb{Q}_p$. Заметим, что существуют кубические уравнения, которые имеют решение в $\mathbb{Z}_p$, но не в $\mathbb{Z}_p^*$ (см. [25]).

Отметим, что случай, когда $a, b \in \mathbb{Q}_3$ и решение ищется в $\mathbb{Z}_3^*$, рассмотрен в [26]. Кроме того, изучению уравнения (1) над конечным полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ посвящены работы [27–31].

2. Предварительные сведения

Пусть $\mathbb{Q}$ — поле рациональных чисел и p — фиксированное простое число. Каждое рациональное число $x \neq 0$ представимо в виде $x = p^{\gamma(x)}\frac{n}{m}$, где $m, n, \gamma(x) \in \mathbb{Z}$ и числа m, n не делятся на p. В поле $\mathbb{Q}$ введем норму $|x|_p$ по правилу

$$|x|_p = \begin{cases} p^{-\gamma(x)}, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

Норма $|x|_p$ называется *p-адической*, и она удовлетворяет сильному неравенству треугольника. Пополнение поля $\mathbb{Q}$ по p-адической норме образует поле p-адических чисел, которое обозначим через $\mathbb{Q}_p$ (см. [16, 17]). Известно, что любое p-адическое число $x \neq 0$ однозначно представляется в каноническом виде $x = p^{\gamma(x)}(x_0 + x_1 p + x_2 p^2 + \dots)$, где $\gamma = \gamma(x) \in \mathbb{Z}$ и x_j — целые числа такие, что $0 \leq x_j \leq p-1$, $x_0 \neq 0$ $(j = 0, 1, \dots)$.

Обозначим $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}$. Элементы множества $\mathbb{Z}_p$ (соответственно $\mathbb{Z}_p^*$) называются *целыми* p-адическими числами (соответственно *единицами* в $\mathbb{Z}_p$).

Лемма 2.1 (лемма Гензеля [31]). *Пусть $f(x)$ — полином с целыми p-адическими коэффициентами. Если для целого p-адического числа θ при некотором $i \geq 0$ имеем*

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

то существует такое единственное целое p-адическое число x_0, что $f(x_0) = 0$ и $x_0 \equiv \theta \pmod{p^{i+1}}$.

Напомним, что $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\}$. Пусть $q \in \mathbb{N}$, $a \in \mathbb{F}_p$ $(a \neq \bar{0})$. Число a называется *вычетом q-й степени по модулю p*, если уравнение

$$x^q = a \tag{2}$$

имеет решение в $\mathbb{F}_p$.

Предложение 2.2 [32]. *Пусть p — нечетное простое число, $q \in \mathbb{N}$, $d = (q, p-1)$ и $a \in \mathbb{F}_p$ $(a \neq \bar{0})$. Тогда справедливы следующие утверждения:*

(i) *a является вычетом q-й степени по модулю p тогда и только тогда, когда $a^{\frac{p-1}{d}} = \bar{1}$;*

(ii) *если $a^{\frac{p-1}{d}} = \bar{1}$, то уравнение (2) имеет d различных решений в $\mathbb{F}_p$.*

Рассмотрим уравнение

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

где p $(p > 3)$ — простое число, $\bar{a}, \bar{b} \in \mathbb{F}_p$ и $\bar{a}\bar{b} \neq \bar{0}$. Через $\mathbf{N}_{\mathbb{F}_p}(x^3 + \bar{a}x - \bar{b})$ обозначим число решений уравнения (3). Положим $\overline{D} = -4\bar{a}^3 - 27\bar{b}^2$, $u_{n+3} = \bar{b}u_n - \bar{a}u_{n+1}$, $n \in \mathbb{N}$, где $u_1 = \bar{0}$, $u_2 = -\bar{a}$, $u_3 = \bar{b}$.

Предложение 2.3 [29]. *Справедлива следующая формула:*

$$\mathbf{N}_{\mathbb{F}_p}(x^3 + \bar{a}x - \bar{b}) = \begin{cases} 3, & \text{если } \overline{D}u_{p-2}^2 = \bar{0}, \\ 0, & \text{если } \overline{D}u_{p-2}^2 = 9\bar{a}^2, \\ 1, & \text{если } \overline{D}u_{p-2}^2 \neq \bar{0}, 9\bar{a}^2. \end{cases}$$

Отметим, что в [27] изучено число $\mathbf{N}_{\mathbb{F}_p}(x^3 - x - \bar{1})$.

Непосредственно доказывается

Предложение 2.4. *Справедливы следующие утверждения:*

I. *Пусть $\overline{D}u_{p-2}^2 = \bar{0}$.*

(i) *Уравнение (3) имеет три различных решения в $\mathbb{F}_p$ тогда и только тогда, когда $\overline{D} \neq \bar{0}$. Более того, для любого решения имеет место $3\bar{x}^2 + \bar{a} \neq 0$.*

(ii) *Уравнение (3) имеет два различных решения в $\mathbb{F}_p$, при этом одно из них кратности 2, тогда и только тогда, когда $\bar{D} = \bar{0}$. Если $\bar{x}_1$, $\bar{x}_2$ — два различных решения, при этом $\bar{x}_1$ кратное решение, то $\bar{x}_1 = \frac{3\bar{b}}{2\bar{a}}$, $\bar{x}_2 = -\frac{3\bar{b}}{\bar{a}}$ и $3\bar{x}_2^2 + \bar{a} \neq \bar{0}$.*

(iii) *Уравнение* (3) *не имеет решения кратности три.*

II. *Пусть* $\overline{D}u_{p-2}^2 \neq \bar{0}$ *и* $\overline{D}u_{p-2}^2 \neq 9\bar{a}^2$. *Если* $\bar{x}$ — *решение уравнения* (3), *то* $3\bar{x}^2 + \bar{a} \neq 0$.

III. *Пусть* $\overline{D}u_{p-2}^2 \neq 9\bar{a}^2$, *тогда существует такое решение* $\bar{x}$ *уравнения* (3), *что* $3\bar{x}^2 + \bar{a} \neq 0$.

Далее нам понадобится

Лемма 2.5 [22]. *Справедливо следующее равенство:*

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

где $x_0 \neq 0$, $0 \leq x_j \leq p-1$, $N_1 = 0$ *и для* $k \geq 2$

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

При $q = 3$ имеем

$$\left(\sum_{i=0}^{\infty} x_i p^i\right)^3 = x_0^3 + \sum_{k=1}^{\infty} \big(3 x_0^2 x_k + N_k(x_0, x_1, \dots, x_{k-1})\big) p^k.$$

Отметим справедливость равенства

$$\left(\sum_{i=0}^{\infty} a_i p^i\right)\left(\sum_{j=0}^{\infty} x_j p^j\right) = \sum_{k=0}^{\infty} \left(\sum_{s=0}^{k} x_s a_{k-s}\right) p^k. \tag{4}$$

В дальнейшем нам также понадобится следующая

Теорема 2.6 [31]. *Сравнение* $ax \equiv b \pmod{m}$ *имеет единственное решение тогда и только тогда, когда* $(a, m) = 1$.

3. Критерий существования решения в $\mathbb{Z}_p^*$

В этом разделе приводим критерий существования решения уравнения (1) в множестве $\mathbb{Z}_p^*$ при $p > 3$ и $a, b \in \mathbb{Q}_p$ $(ab \neq 0)$.

Сначала докажем следующий вспомогательный результат.

Предложение 3.1. *Пусть* p — *простое число и* $a, b \in \mathbb{Q}_p$, $ab \neq 0$. *Если уравнение* (1) *имеет решение в* $\mathbb{Z}_p^*$, *то выполняется одно из следующих условий:*

(i) $|a|_p < |b|_p = 1$;

(ii) $|b|_p < |a|_p = 1$;

(iii) $|a|_p = |b|_p \geq 1$.

Доказательство. Пусть $x \in \mathbb{Z}_p^*$ — решение (1). Тогда из сильного неравенства треугольника имеем

$$|b|_p = |x^3 + ax|_p \leq \max\{1, |a|_p\}, \quad |a|_p = |ax|_p = |b - x^3|_p \leq \max\{1, |b|_p\},$$

$$1 = |x^3|_p = |b - ax|_p \leq \max\{|a|_p, |b|_p\}.$$

Если $|a|_p \neq |b|_p$, то $\max\{|a|_p, |b|_p\} = 1$, и если $|a|_p = |b|_p$, то $|a|_p = |b|_p \geq 1$. $\square$

Пусть $a, b \in \mathbb{Q}_p$ — ненулевые p-адические числа ($p > 3$). Тогда их можно представить в виде

$$a = \frac{a^*}{|a|_p}, \quad b = \frac{b^*}{|b|_p},$$

где $a^*, b^* \in \mathbb{Z}_p^*$ и $a^* = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \ldots$, $b^* = b_0 + b_1 \cdot p + b_2 \cdot p^2 + \ldots$.

Положим $D_0 = -4a_0^3 - 27b_0^2$ и $u_{n+3} = b_0 u_n - a_0 u_{n+1}$, $n \in \mathbb{N}$, при $u_1 = 0$, $u_2 = -a_0$, $u_3 = b_0$.

Следующая теорема является основным результатом данного раздела.

Теорема 3.2. *Уравнение* (1) *имеет решение в* $\mathbb{Z}_p^*$ *тогда и только тогда, когда выполнено одно из следующих условий:*

(i) $|a|_p < |b|_p = 1$ *и* $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod p$;
(ii) $|b|_p < |a|_p = 1$ *и* $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod p$;
(iii) $|a|_p = |b|_p = 1$ *и* $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$;
(iv) $|a|_p = |b|_p > 1$.

Доказательство. Пусть уравнение (1) имеет решение в $\mathbb{Z}_p^*$. Тогда в силу предложения 3.1 одно из следующих условий выполняется: (i) $|a|_p < 1$, $|b|_p = 1$; (ii) $|a|_p = 1$, $|b|_p < 1$; (iii) $|a|_p = |b|_p \geq 1$. Рассмотрим каждый случай отдельно.

(i) Пусть уравнение (1) имеет решение в $\mathbb{Z}_p^*$ и $|a|_p < 1$, $|b|_p = 1$. Предположим, что $x \in \mathbb{Z}_p^*$ — решение (1). Тогда из условий $|a|_p < 1$ и $|b|_p = 1$ имеем

$$x_0^3 + ax_0 \equiv x_0^3 \equiv b_0 \pmod p.$$

Из последнего сравнения ввиду предложения 2.2 получим $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod p$.

Теперь докажем обратное: если $|a|_p < 1$, $|b|_p = 1$ и $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod p$, то уравнение (1) имеет решение в $\mathbb{Z}_p^*$. Действительно, из $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod p$ вытекает существование $x_0 \in \mathbb{Z}$ такого, что $x_0^3 \equiv b_0 \pmod p$ и $(x_0, p) = 1$.

Рассмотрим полином

$$f_{a,b}(x) = x^3 + ax - b. \tag{5}$$

Из $|a|_p < 1$, $p > 3$ следует, что

$$f_{a,b}(x_0) = x_0^3 + ax_0 - b \equiv x_0^3 - b_0 \equiv 0 \pmod p, \quad f'_{a,b}(x_0) = 3x_0^2 + a \not\equiv 0 \pmod p.$$

Использование леммы Гензеля приводит к тому, что уравнение (1) имеет решение $x \in \mathbb{Z}_p$ такое, что $|x - x_0|_p \leq \frac{1}{p}$ и $|x_0|_p = 1$. Это означает, что $|x|_p = 1$, т. е. $x \in \mathbb{Z}_p^*$.

(ii) Предположим, что уравнение (1) имеет решение в $\mathbb{Z}_p^*$ при $|a|_p = 1$, $|b|_p < 1$. Покажем, что $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Пусть $x \in \mathbb{Z}_p^*$ — решение. Из $|a|_p = 1$, $|b|_p < 1$ получим

$$x_0^3 + a_0 x_0 \equiv x_0\bigl(x_0^2 + a_0\bigr) \equiv b \equiv 0 \pmod p.$$

Это означает, что $x_0^2 + a_0 \equiv 0 \pmod p$. По предложению 2.2 $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Теперь покажем, что из $|a|_p = 1$, $|b|_p < 1$ и $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod p$ следует существование решения уравнения (1) в $\mathbb{Z}_p^*$. Действительно, из условия $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod p$ получим существование такого $x_0 \in \mathbb{Z}$, что $x_0^2 + a_0 \equiv 0 \pmod p$ и $(x_0, p) = 1$.

Рассмотрим полином $f_{a,b}(x)$ (см. (5)). Учитывая, что $|b|_p < 1$, получим

$$f_{a,b}(x_0) = x_0^3 + ax_0 - b \equiv x_0(x_0^2 + a_0) \equiv 0 \pmod p,$$
$$f'_{a,b}(x_0) = 3x_0^2 + a \equiv 3(x_0^2 + a_0) - 2a_0 \not\equiv 0 \pmod p.$$

Применение Леммы Гензеля приводит к существованию решения $x \in \mathbb{Z}_p$ уравнения (1), удовлетворяющего свойству $|x - x_0|_p \leq \frac{1}{p}$, где $|x_0|_p = 1$. Отсюда следует, что $x \in \mathbb{Z}_p^*$.

(iii) Пусть уравнение (1) имеет решение в $\mathbb{Z}_p^*$ при $|a|_p = |b|_p = 1$ и $x \in \mathbb{Z}_p^*$ — решение. Так как $|a|_p = |b|_p = 1$, из (1) имеем $x_0^3 + a_0x_0 \equiv b_0 \pmod p$. Следовательно, уравнение $x^3 + a_0x = b_0$ имеет по крайней мере одно решение в конечном поле $\mathbb{F}_p$. Поэтому условие $D_0u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ вытекает из предложения 2.3.

Докажем, что при $|a|_p = 1$, $|b|_p = 1$ и $D_0u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ уравнение (1) имеет решение в $\mathbb{Z}_p^*$. Из $D_0u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ следует, что уравнение $x^3 + a_0x \equiv b_0 \pmod p$ имеет хотя бы одно решение. Из предложения 2.4 выводим, что среди всех решений можно найти такое $x_0 \in \mathbb{Z}$, что $(x_0, p) = 1$ и $3x_0^2 + a_0 \not\equiv 0 \pmod p$.

Снова применяя лемму Гензеля к полиному $f_{a,b}(x)$ в точке $x = x_0$, получим существование решения $x \in \mathbb{Z}_p$ уравнения (1) такого, что $x \in \mathbb{Z}_p^*$.

(iv) Докажем, что из $|a|_p = |b|_p > 1$ следует существование решения (1) в $\mathbb{Z}_p^*$. Пусть $|a|_p = |b|_p = p^m$, где $m \geq 1$. Тогда $a = p^{-m}a^*$, $b = p^{-m}b^*$, при этом $a^*, b^* \in \mathbb{Z}_p^*$. Ясно, что уравнение $x^3 + p^{-m}a^*x = p^{-m}b^*$ имеет решение в $\mathbb{Z}_p^*$ тогда и только тогда, когда уравнение $p^mx^3 + a^*x = b^*$ имеет решение в $\mathbb{Z}_p^*$, где $a^*, b^* \in \mathbb{Z}_p^*$. Поэтому рассмотрим полином $f(x) = p^mx^3 + a^*x - b^*$. Пусть a_0, b_0 — первые члены в разложении p-адических чисел a^*, b^* соответственно. Тогда существует $x_0 \in \mathbb{Z}$ такое, что $a_0x_0 \equiv b_0 \pmod p$ и $(x_0, p) = 1$. Поэтому

$$f(x_0) \equiv p^mx_0^3 + a_0x_0 - b_0 \equiv 0 \pmod p, \quad f'(x_0) \equiv 3p^mx_0^2 + a_0 \not\equiv 0 \pmod p.$$

Применяя лемму Гензеля, получим, что уравнение $p^mx^3 + a^*x = b^*$, а следовательно, и уравнение (1) имеют решение в $\mathbb{Z}_p^*$. $\square$

4. Алгоритм нахождения решения

В настоящем разделе разработан алгоритм нахождения решения уравнения (1) в $\mathbb{Z}_p^*$, $p > 3$.

Пусть

$$x = p^{\gamma(x)}(x_0 + x_1p + \dots), \quad a = p^{\gamma(a)}(a_0 + a_1p + \dots), \quad b = p^{\gamma(b)}(b_0 + b_1p + \dots),$$

где $x_j, a_j, b_j \in \{0, 1, \dots, p-1\}$ для $j = 0, 1, \dots$ и $x_0a_0b_0 \neq 0$.

Подставив канонические выражения x, a и b в уравнение (1), получим

$$\left(\sum_{k=0}^{\infty} x_kp^k\right)^3 + p^{\gamma(a)}\left(\sum_{k=0}^{\infty} a_kp^k\right)\left(\sum_{k=0}^{\infty} x_kp^k\right) = p^{\gamma(b)}\sum_{k=0}^{\infty} b_kp^k.$$

С учетом леммы 2.5 и соотношения (4) равенство (1) примет вид

$$x_0^3 + \sum_{k=1}^{\infty}\big(3x_0^2x_k + N_k(x_0, x_1, \dots, x_{k-1})\big)p^k + p^{\gamma(a)}\left(a_0x_0 + \sum_{k=1}^{\infty}\left(\sum_{s=0}^{k} x_sa_{k-s}\right)p^k\right) = p^{\gamma(b)}\left(b_0 + \sum_{k=1}^{\infty} b_kp^k\right). \quad (6)$$

Учитывая теорему 3.2, будем рассматривать только те случаи, когда решение уравнения (1) существует.

В следующей теореме предложен алгоритм нахождения решения нашего уравнения при условии $|a|_p < 1$, $|b|_p = 1$.

Теорема 4.1. *Пусть* $|a|_p < |b|_p = 1$, $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod p$ *и* $\log_p |a|_p = -m$, *где* $m \geq 1$. *Тогда* x *является решением уравнения* (1) *в* Z_p^* *тогда и только тогда, когда выполняются следующие сравнения:*

$$x_0^3 \equiv b_0 \pmod p,$$

$$3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + M_k(x_0, \ldots, x_{k-1}) \equiv b_k \pmod p, \quad 1 \leq k \leq m-1,$$

$$3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-m}a_0 + x_{k-m-1}a_1 + \cdots + x_0 a_{k-m} \\ + M_k(x_0, \ldots, x_{k-1}) \equiv b_k \pmod p, \quad k \geq m,$$

где $M_k(x_0, x_1, \ldots, x_{k-1})$ *последовательно определяются из соотношений*

$$x_0^3 = b_0 + M_1(x_0) \cdot p,$$

$$3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + M_k(x_0, \ldots, x_{k-1}) = b_k + M_{k+1}(x_0, \ldots, x_k) \cdot p, \\ 1 \leq k \leq m-1,$$

$$3x_0^2 x_m + N_m(x_0, x_1, \ldots, x_{m-1}) + a_0 x_0 + M_m(x_0, \ldots, x_{m-1}) \\ = b_m + M_{m+1}(x_0, \ldots, x_m) \cdot p,$$

$$3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-m}a_0 + x_{k-m-1}a_1 + \cdots + x_0 a_{k-m} \\ + M_k(x_0, \ldots, x_{k-1}) = b_k + M_{k+1}(x_0, \ldots, x_k) \cdot p, \quad k \geq m+1.$$

Доказательство. Пусть $x = x_0 + x_1 p + x_2 p^2 + \ldots$, $0 \leq x_j \leq p-1$, $x_0 \neq 0$, — решение, тогда равенство (6) можно записать в виде

$$x_0^3 + \sum_{k=1}^{\infty} \big(3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1})\big) \\ + p^m \left(a_0 x_0 + \sum_{k=1}^{\infty} \left(\sum_{s=0}^{k} x_s a_{k-s} \right) p^k \right) = b_0 + \sum_{k=1}^{\infty} b_k p^k. \quad (7)$$

Далее,

$$x_0^3 + \sum_{k=1}^{m-1} \big(3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1})\big) p^k \\ + \big(3x_0^2 x_m + N_m(x_0, x_1, \ldots, x_{m-1}) + a_0 x_0\big) p^m + \sum_{k=m+1}^{\infty} \big(3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1}) \\ + x_{k-m}a_0 + x_{k-m-1}a_1 + \cdots + x_0 a_{k-m}\big) p^k = b_0 + \sum_{k=1}^{\infty} b_k p^k,$$

откуда следует необходимость выполнения сравнений теоремы.

Пусть x удовлетворяет сравнениям теоремы. В силу того, что $\big(3x_0^2, p\big) = 1$, по теореме 2.6 существуют единственные решения x_k следующих сравнений:

$$x_0^3 \equiv b_0 \pmod p,$$

$$3x_0^2 x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + M_k(x_0, \ldots, x_{k-1}) \equiv b_k \pmod p, \quad 1 \leq k \leq m-1,$$

$$3x_0^2x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-m}a_0 + x_{k-m-1}a_1 + \dots + x_0a_{k-m} \\ + M_k(x_0, \dots, x_{k-1}) \equiv b_k \pmod p, \quad k \geq m,$$

где $M_k(x_0, x_1, \dots, x_{k-1})$ удовлетворяют условиям теоремы.

Тогда

$$x_0^3 + \sum_{k=1}^{m-1} \big(3x_0^2x_k + N_k(x_0, x_1, \dots, x_{k-1})\big)p^k \\ + \big(3x_0^2x_m + N_m(x_0, x_1, \dots, x_{m-1}) + a_0x_0\big)p^m$$

$$+ \sum_{k=m+1}^{\infty} \big(3x_0^2x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-m}a_0 + x_{k-m-1}a_1 + \dots + x_0a_{k-m}\big)p^k$$

$$= b_0 + M_1(x_0) \cdot p + \sum_{k=1}^{m-1} (b_k - M_k(x_0, x_1, \dots, x_{k-1}) \cdot p + M_{k+1}(x_0, x_1, \dots, x_k))p^k$$

$$+ \sum_{k=m}^{\infty} (b_k - M_k(x_0, x_1, \dots, x_{k-1}) + M_{k+1}(x_0, x_1, \dots, x_k) \cdot p) \cdot p^k = b_0 + \sum_{k=1}^{\infty} b_kp^k.$$

Таким образом, $x = \sum\limits_{k=0}^{\infty} x_kp^k$ является решением уравнения (1). $\square$

Теперь рассмотрим случай $|b|_p < |a|_p = 1$, $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Пусть $|a|_p = 1$ и $\log_p |b|_p = -m$, $m \geq 1$, тогда из равенства (6) получаем следующее:

$$x_0^3 + \sum_{k=1}^{\infty} \big(3x_0^2x_k + N_k(x_0, x_1, \dots, x_{k-1})\big)p^k + a_0x_0 + \sum_{k=1}^{\infty} \left(\sum_{s=0}^{k} x_sa_{k-s}\right)p^k$$

$$= x_0^3 + a_0x_0 + \sum_{k=1}^{\infty} \big(3x_0^2x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_ka_0 + x_{k-1}a_1 + \dots + x_0a_k\big)p^k$$

$$= x_0^3 + a_0x_0 + \sum_{k=1}^{\infty} \big(\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_1 + \dots + x_0a_k\big)p^k \\ = b_0p^m + \sum_{k=1}^{\infty} b_kp^{m+k}.$$

Теорема 4.2. *Пусть $|b|_p < |a|_p = 1$, $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod p$ при $\log_p |b|_p = -m$, $m \geq 1$. Тогда x является решением уравнения (1) в $\mathbb{Z}_p^*$ в том и только в том случае, когда справедливы сравнения*

$$x_0^2 + a_0 \equiv 0 \pmod p,$$

$$\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_0 + \dots + x_0a_k \\ + M_k(x_0, \dots, x_{k-1}) \equiv 0 \pmod p, \quad 1 \leq k \leq m-1,$$

$$\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_0 + \dots + x_0a_k \\ + M_k(x_0, \dots, x_{k-1}) \equiv b_{k-m} \pmod p, \quad k \geq m,$$

где $M_k(x_0, x_1, \ldots, x_{k-1})$ *рекуррентно определяются из соотношений*

$$\begin{aligned}\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-1}a_0 + \cdots + x_0a_k \\ + M_k(x_0, \ldots, x_{k-1}) = M_{k+1}(x_0, \ldots, x_k) \cdot p, \quad 1 \le k \le m-1,\end{aligned}$$

$$\begin{aligned}\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-1}a_0 + \cdots + x_0a_k \\ + M_k(x_0, \ldots, x_{k-1}) = b_{k-m} + M_{k+1}(x_0, \ldots, x_k) \cdot p, \quad k \ge m.\end{aligned}$$

Доказательство. Если уравнение (1) имеет решение $x \in \mathbb{Z}_p^*$, то

$$x_0^3 + a_0x_0 + \sum_{k=1}^{\infty}\big(\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-1}a_1 + \cdots + x_0a_k\big)p^k = b_0p^m + \sum_{k=1}^{\infty} b_kp^{m+k}.$$

Отсюда следует, что $x_0^3 + a_0x_0 \equiv 0 \pmod p$, т. е. $x_0^2 + a_0 \equiv 0 \pmod p$, и справедливость других сравнений теоремы.

Пусть выполнены сравнения теоремы для числа x. Тогда $x_0^2+a_0 \equiv 0 \pmod p$ имеет решение x_0. Существует число $M_1(x_0)$ такое, что $x_0^3 + a_0x_0 = M_1(x_0) \cdot p$.

Из условия $\big(3x_0^2 + a_0, p\big) = (-2a_0, p) = 1$ и теоремы 2.6 вытекает существование единственных решений x_k следующих сравнений:

$$\begin{aligned}\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-1}a_0 + \cdots + x_0a_k \\ + M_k(x_0, \ldots, x_{k-1}) \equiv 0 \pmod p, \quad 1 \le k \le m-1,\end{aligned}$$

$$\begin{aligned}\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-1}a_0 + \cdots + x_0a_k \\ + M_k(x_0, \ldots, x_{k-1}) \equiv b_{k-m} \pmod p, \quad k \ge m.\end{aligned}$$

Тогда

$$\begin{aligned}x_0^3 &+ a_0x_0 + \sum_{k=1}^{\infty}\big(\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \ldots, x_{k-1}) + x_{k-1}a_0 + \cdots + x_0a_k\big)p^k \\ &= M_1(x_0) \cdot p + \sum_{k=1}^{m-1}(-M_k(x_0, x_1, \ldots, x_{k-1}) + M_{k+1}(x_0, x_1, \ldots, x_k) \cdot p) \cdot p^k \\ &\quad + \sum_{k=m}^{\infty}(b_{k-m} - M_k(x_0, x_1, \ldots, x_{k-1}) + M_{k+1}(x_0, x_1, \ldots, x_k) \cdot p) \cdot p^k \\ &= p^mb_0 + \sum_{k=0}^{\infty} b_kp^{m+k}.\end{aligned}$$

Таким образом, x — решение уравнения (1). $\square$

Теперь рассмотрим случай $|a|_p = |b|_p = 1$, т. е. $a, b \in \mathbb{Z}_p^*$ и $D_0u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ (см. теорему 3.2). Для $j \le k$ положим

$$P_k^j = P_k^j(x_0, x_1, \ldots, x_{j-1}) = \sum_{\substack{m_0, m_1, \ldots, m_{j-1}: \\ \sum_{i=0}^{j-1} m_i = 3,\ \sum_{i=1}^{j-1} im_i = k}} \frac{6}{m_0!m_1!\ldots m_{j-1}!} x_0^{m_0}x_1^{m_1}\ldots x_{j-1}^{m_{j-1}}.$$

Введем следующие обозначения:

$$A_0 = 3x_0^2 + a_0, \quad A_k = \frac{A_{k-1}}{p} + a_k + 3R_k, \text{ где } R_k = \sum_{j=0}^{k} x_jx_{k-j},\ k \ge 1.$$

Теорема 4.3. *Пусть* $|a|_p = |b|_p = 1$, $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ *и* $x \in \mathbb{Z}_p^*$ *такое, что* $A_0 = 3x_0^2 + a_0 \not\equiv 0 \pmod p$. *Тогда* x *является решением уравнения* (1) *тогда и только тогда, когда верны сравнения*

$$x_0^3 + a_0x_0 \equiv b_0 \pmod p,$$

$$\begin{aligned}\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_0 + \dots + x_0a_k \\ + M_k(x_0, \dots, x_{k-1}) \equiv b_k \pmod p, \quad k \geq 1,\end{aligned}$$

где $M_k(x_0, x_1, \dots, x_{k-1})$ *рекуррентно определяются из следующих соотношений:*

$$\begin{aligned}\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_0 + \dots + x_0a_k \\ + M_k(x_0, \dots, x_{k-1}) = b_k + M_{k+1}(x_0, \dots, x_k) \cdot p, \quad k \geq 1.\end{aligned}$$

Доказательство. Пусть $x \in \mathbb{Z}_p^*$ — решение, тогда

$$\begin{aligned}x_0^3 + \sum_{k=1}^{\infty} \big(3x_0^2x_k + N_k(x_0, x_1, \dots, x_{k-1})\big)p^k + a_0x_0 + \sum_{k=1}^{\infty}\left(\sum_{s=0}^{k} x_s a_{k-s}\right)p^k \\ = x_0^3 + a_0x_0 + \sum_{k=1}^{\infty} \big(\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_1 + \dots + x_0a_k\big)p^k \\ = b_0 + \sum_{k=1}^{\infty} b_k p^k.\end{aligned}$$

Следовательно, сравнения из утверждения теоремы выполняются.

Пусть $x_0^3 + a_0x_0 \equiv b_0 \pmod p$ имеет решение x_0. Тогда существует число $M_1(x_0)$ такое, что $x_0^3 + a_0x_0 = b_0 + M_1(x_0) \cdot p$.

В силу условия $\big(3x_0^2 + a_0, p\big) = 1$ и теоремы 2.6 существуют решения x_k сравнений

$$\begin{aligned}\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_0 + \dots + x_0a_k \\ + M_k(x_0, \dots, x_{k-1}) \equiv b_k \pmod p, \quad k \geq 1.\end{aligned}$$

Цепочка равенств

$$\begin{aligned}x_0^3 + a_0x_0 + \sum_{k=1}^{\infty} \big(\big(3x_0^2 + a_0\big)x_k + N_k(x_0, x_1, \dots, x_{k-1}) + x_{k-1}a_0 + \dots + x_0a_k\big)p^k \\ = b_0 + M_1(x_0) \cdot p + (b_1 - M_1(x_0) + M_2(x_0, x_1) \cdot p) \cdot p \\ + \sum_{k=2}^{\infty}(b_k - M_k(x_0, x_1, \dots, x_{k-1}) + M_{k+1}(x_0, x_1, \dots, x_k) \cdot p) \cdot p^k = b_0 + \sum_{k=0}^{\infty} b_k p^k\end{aligned}$$

показывает, что x является решением уравнения (1). □

Лемма 4.4. *Пусть* $|a|_p = |b|_p = 1$, $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ *и* x *такой, что для некоторого* k *имеет место* $A_{k-j} \equiv 0 \pmod p), 1 \leq j \leq k$, $A_k \not\equiv 0 \pmod p$. *Если* x *является решением* (1), *то справедлива система сравнений*

$$x_0^3 + a_0x_0 \equiv b_0 \pmod p,$$

$$\begin{aligned}x_{j-1}a_j + x_{j-2}a_{j+1} + \dots + x_0a_{2j-1} + P_{2j-1}^j(x_0, x_1, \dots, x_{j-1}) \\ + M_{2j-1}(x_0, x_1, \dots, x_{j-1}) \equiv b_{2j-1} \pmod p,\end{aligned}$$

$$(A_j - 3x_0x_j)x_j + x_{j-1}a_{j+1} + x_{j-2}a_{j+2} + \cdots + x_0a_{2j} + P_{2j}^{j}(x_0, x_1, \ldots, x_{j-1}) + M_{2j}(x_0, x_1, \ldots, x_{j-1}) \equiv b_{2j} \pmod p,$$

$$A_kx_{k+i} + x_{k+i-1}a_{k+1} + x_{k+i-2}a_{k+2} + \cdots + x_0a_{2k+i} + P_{2k+i}^{k+i}(x_0, x_1, \ldots, x_{k+i-1}) + M_{2k+i}(x_0, x_1, \ldots, x_{k+i-1}) \equiv b_{2k+i} \pmod p,$$

где $1 \le j \le k$, $i \ge 1$, *и*

$$p \cdot M_1(x_0) = x_0^3 + a_0x_0 - b_0,$$

$$p \cdot M_{2j}(x_0, x_1, \ldots, x_{j-1}) = x_{j-1}a_j + x_{j-2}a_{j+1} + \cdots + x_0a_{2j-1} + P_{2j-1}(x_0, x_1, \ldots, x_{j-1}) + M_{2j-1}(x_0, x_1, \ldots, x_{j-1}) - b_{2j-1},$$

$$p \cdot M_{2j+1}(x_0, x_1, \ldots, x_j) = (A_j - 3x_0x_j)x_j + x_{j-1}a_{j+1} + x_{j-2}a_{j+2} + \cdots + x_0a_{2j} + P_{2j}(x_0, x_1, \ldots, x_{j-1}) + M_{2j}(x_0, x_1, \ldots, x_{j-1}) - b_{2j},$$

$$p \cdot M_{2k+i+1}(x_0, x_1, \ldots, x_{k+i}) = A_kx_{k+i} + x_{k+i-1}a_{k+1} + x_{k+i-2}a_{k+2} + \cdots + x_0a_{2k+i} + P_{2k+i}(x_0, x_1, \ldots, x_{k+i-1}) + M_{2k+i}(x_0, x_1, \ldots, x_{k+i-1}) - b_{2k+i}.$$

Доказательство. Пусть $|a|_p = |b|_p = 1$. Доказательство проведем по индукции. Пусть $k = 1$, т. е.

$$A_0 = 3x_0^2 + a_0 \equiv 0 \pmod p, \quad A_1 = \frac{A_0}{p} + a_1 + 6x_0x_1 \not\equiv 0 \pmod p,$$

тогда справедлива система сравнений:

a) $x_0^3 + a_0x_0 \equiv b_0 \pmod p$, следует $x_0^3 + a_0x_0 = b_0 + M_1(x_0) \cdot p$,

b) $x_0a_1 + M_1(x_0) \equiv b_1 \pmod p$, следует $x_0a_1 + M_1(x_0) = b_1 + M_2(x_0) \cdot p$,

c) $(A_1 - 3x_0x_1)x_1 + x_0a_2 + M_2(x_0) \equiv b_2 \pmod p$, следует

$$(A_1 - 3x_0x_1)x_1 + x_0a_2 + M_2(x_0) = b_2 + M_3(x_0, x_1) \cdot p,$$

и нетрудно получить, что

$$A_1x_{t-1} + x_{t-2}a_2 + x_{t-3}a_3 + \cdots + x_0a_t + N_t(x_0, \ldots, x_{t-1}) - 6x_0x_1x_{t-1} + M_t(x_0, \ldots, x_{t-2}) \equiv b_t \pmod p, \quad t \ge 3,$$

Заметим, что $P_1^1(x_0) = 0$, $P_2^1(x_0) = 0$ и

$$P_t^{t-1}(x_0, x_1, \ldots, x_{t-2}) = N_t(x_0, \ldots, x_{t-1}) - 6x_0x_1x_{t-1}, \quad t \ge 3.$$

Таким образом, показана справедливость системы сравнений при $k = 1$.

Пусть $k = 2$, т. е. $A_0 \equiv 0 \pmod p$, $A_1 \equiv 0 \pmod p$ и $A_2 = \frac{A_1}{p} + a_2 + 3x_1^2 + 6x_0x_2 \not\equiv 0 \pmod p$. Тогда к системе:

a) $x_0^3 + a_0x_0 \equiv b_0 \pmod p$, следует $x_0^3 + a_0x_0 = b_0 + M_1(x_0) \cdot p$,

b) $x_0a_1 + M_1(x_0) \equiv b_1 \pmod p$, следует $x_0a_1 + M_1(x_0) = b_1 + M_2(x_0) \cdot p$,

c) $(A_1 - 3x_0x_1)x_1 + x_0a_2 + M_2(x_0) \equiv b_2 \pmod p$, следует

$$(A_1 - 3x_0x_1)x_1 + x_0a_2 + M_2(x_0) = b_2 + M_3(x_0, x_1) \cdot p,$$

добавятся следующие сравнения:

d) $x_1^3 + x_1 a_2 + x_0 a_3 + M_3(x_0, x_1) \equiv b_3 \pmod p$, следует

$$x_1^3 + x_1 a_2 + x_0 a_3 + M_3(x_0, x_1) = b_3 + M_4(x_0, x_1) \cdot p,$$

e) $(A_2 - 3x_0x_2)x_2 + x_1 a_3 + x_0 a_4 + M_4(x_0, x_1) \equiv b_4 \pmod p$, следует

$$(A_2 - 3x_0x_2)x_2 + x_1 a_3 + x_0 a_4 + M_4(x_0, x_1) = b_4 + M_5(x_0, x_1, x_2) \cdot p.$$

Так как $A_2 = \frac{A_1}{p} + a_2 + 3x_1^2 + 6x_0x_2 \not\equiv 0 \pmod p$, при $t \geq 5$ имеем

$$\begin{aligned} &A_2 x_{t-2} + x_{t-3} a_3 + x_{t-4} a_4 + \dots + x_0 a_t + N_t(x_0, \dots, x_{t-1}) \\ &\qquad - 6x_0x_1x_{t-1} - \big(3x_1^2 + 6x_0x_2\big)x_{t-2} + M_t(x_0, \dots, x_{t-3}) \equiv b_t \pmod p, \end{aligned}$$

т. е.

$$\begin{aligned} &A_2 x_{t-2} + x_{t-3} a_3 + x_{t-4} a_4 + \dots + x_0 a_t + N_t(x_0, \dots, x_{t-1}) - 6x_0x_1x_{t-1} \\ &\qquad - \big(3x_1^2 + 6x_0x_2\big)x_{t-2} + M_t(x_0, \dots, x_{t-3}) = b_t + M_{t+1}(x_0, \dots, x_{t-2}) \cdot p. \end{aligned}$$

Отметим, что $P_1^1(x_0) = 0$, $P_2^1(x_0) = 0$, $P_3^2(x_0, x_1) = x_1^3$, $P_4^2(x_0, x_1) = 0$ и

$$P_t^{t-2} = N_t(x_0, \dots, x_{t-1}) - 6x_0x_1x_{t-1} - \big(3x_1^2 + 6x_0x_2\big)x_{t-2}, \quad t \geq 5.$$

Таким образом, показана справедливость системы сравнений при $k = 2$.

Пусть система сравнений справедлива для k, покажем, что она верна для $k+1$. По предположению индукции имеем

$$x_0^3 + a_0 x_0 \equiv b_0 \pmod p,$$

$$\begin{aligned} &x_{j-1} a_j + x_{j-2} a_{j+1} + \dots + x_0 a_{2j-1} + P_{2j-1}^j(x_0, x_1, \dots, x_{j-1}) \\ &\qquad\qquad + M_{2j-1}(x_0, x_1, \dots, x_{j-1}) \equiv b_{2j-1} \pmod p, \end{aligned}$$

$$\begin{aligned} &(A_j - 3x_0x_j)x_j + x_{j-1} a_{j+1} + x_{j-2} a_{j+2} + \dots + x_0 a_{2j} + P_{2j}^j(x_0, x_1, \dots, x_{j-1}) \\ &\qquad\qquad + M_{2j}(x_0, x_1, \dots, x_{j-1}) \equiv b_{2j} \pmod p. \end{aligned}$$

Так как $A_k \equiv 0 \pmod p$, из

$$\begin{aligned} &A_k x_{k+i} + x_{k+i-1} a_{k+1} + x_{k+i-2} a_{k+2} + \dots + x_0 a_{2k+i} + P_{2k+i}^{k+i}(x_0, x_1, \dots, x_{k+i-1}) \\ &\qquad\qquad + M_{2k+i}(x_0, x_1, \dots, x_{k+i-1}) \equiv b_{2k+i} \pmod p \end{aligned}$$

получим

$$\begin{aligned} &x_k a_{k+1} + x_{k-1} a_{k+2} + \dots + x_0 a_{2k+1} + P_{2k+1}^{k+1}(x_0, x_1, \dots, x_k) \\ &\qquad\qquad + M_{2k+1}(x_0, x_1, \dots, x_k) \equiv b_{2k+1} \pmod p, \end{aligned}$$

$$\begin{aligned} &\frac{A_k}{p} x_{k+1} + x_{k+1} a_{k+1} + x_k a_{k+2} + \dots + x_0 a_{2k+2} + P_{2k+2}^{k+2}(x_0, x_1, \dots, x_{k+1}) \\ &\qquad\qquad + M_{2k+2}(x_0, x_1, \dots, x_k) \equiv b_{2k+2} \pmod p, \end{aligned}$$

$$\begin{aligned} &\frac{A_k}{p} x_{k+2} + x_{k+2} a_{k+1} + x_{k+1} a_{k+2} + \dots + x_0 a_{2k+3} + P_{2k+3}^{k+3}(x_0, x_1, \dots, x_{k+2}) \\ &\qquad\qquad + M_{2k+3}(x_0, x_1, \dots, x_{k+1}) \equiv b_{2k+3} \pmod p, \end{aligned}$$

$$\frac{A_k}{p}x_{k+1+i}+x_{k+1+i}a_{k+1}+x_{k+i}a_{k+2}+\dots+x_0a_{2k+2+i}+P^{k+2+i}_{2k+2+i}(x_0,x_1,\dots,x_{k+1+i}) \\ +M_{2k+2+i}(x_0,x_1,\dots,x_{k+i})\equiv b_{2k+2+i}\ (\mathrm{mod}\,p),\quad i\ge 1.$$

Нетрудно проверить, что

$$\begin{aligned}P^{k+2}_{2k+2}(x_0,x_1,\dots,x_{k+1}) &= P^{k+1}_{2k+2}(x_0,x_1,\dots,x_k)+3R_kx_{k+1}+3x_0x^2_{k+1}\\ &= P^{k+1}_{2k+2}(x_0,x_1,\dots,x_k)+3R_kx_{k+1}+6x_0x^2_{k+1}-3x_0x^2_{k+1}\\ &= P^{k+1}_{2k+2}(x_0,x_1,\dots,x_k)+3(R_k+6x_0x_{k+1})x_{k+1}-3x_0x^2_{k+1}\\ &= P^{k+1}_{2k+2}(x_0,x_1,\dots,x_k)+3R_{k+1}x_{k+1}-3x_0x^2_{k+1},\end{aligned}$$

а при $i\ge 3$

$$P^{k+2+i}_{2k+2+i}(x_0,x_1,\dots,x_{k+1+i})=P^{k+1+i}_{2k+2+i}(x_0,x_1,\dots,x_{k+i})+3R_{k+1}x_{k+1+i}.$$

Используя эти соотношения, имеем

$$\begin{aligned}&\frac{A_k}{p}x_{k+1}+x_{k+1}a_{k+1}+x_ka_{k+2}+\dots+x_0a_{2k+2}+P^{k+2}_{2k+2}(x_0,x_1,\dots,x_{k+1})\\ &\qquad +M_{2k+2}(x_0,x_1,\dots,x_k)\\ &= \frac{A_k}{p}x_{k+1}+x_{k+1}a_{k+1}+x_ka_{k+2}+\dots+x_0a_{2k+2}+P^{k+1}_{2k+2}(x_0,x_1,\dots,x_k)\\ &\qquad +3R_{k+1}x_{k+1}-3x_0x^2_{k+1}+M_{2k+2}(x_0,x_1,\dots,x_k)\\ &= \left(\frac{A_k}{p}+a_{k+1}+3R_{k+1}-3x_0x_{k+1}\right)x_{k+1}+x_ka_{k+2}+\dots+x_0a_{2k+2}\\ &\qquad +P^{k+1}_{2k+2}(x_0,x_1,\dots,x_k)+M_{2k+2}(x_0,x_1,\dots,x_k)\\ &= (A_{k+1}-3x_0x_{k+1})x_{k+1}+x_ka_{k+2}+\dots+x_0a_{2k+2}+P^{k+1}_{2(k+1)}(x_0,x_1,\dots,x_k)\\ &\qquad +M_{2(k+1)}(x_0,x_1,\dots,x_k),\end{aligned}$$

а при $i\ge 1$

$$\begin{aligned}&\frac{A_k}{p}x_{k+1+i}+x_{k+1+i}a_{k+1}+x_{k+i}a_{k+2}+\dots+x_0a_{2k+2+i}\\ &\qquad +P^{k+2+i}_{2k+2+i}(x_0,x_1,\dots,x_{k+1+i})+M_{2k+2+i}(x_0,x_1,\dots,x_{k+i})\\ &= \frac{A_k}{p}x_{k+1+i}+x_{k+1+i}a_{k+1}+x_{k+i}a_{k+2}+\dots+x_0a_{2k+2+i}\\ &\qquad +P^{k+1+i}_{2k+2+i}(x_0,x_1,\dots,x_{k+i})+3R_{k+1}x_{k+1+i}+M_{2k+2+i}(x_0,x_1,\dots,x_{k+i})\\ &= \left(\frac{A_k}{p}+a_{k+1}+3R_{k+1}\right)x_{k+1+i}+x_{k+i}a_{k+2}+\dots+x_0a_{2k+2+i}\\ &\qquad +P^{k+1+i}_{2k+2+i}(x_0,x_1,\dots,x_{k+i})+M_{2k+2+i}(x_0,x_1,\dots,x_{k+i})\\ &= A_{k+1}x_{k+1+i}+x_{k+i}a_{k+2}+\dots+x_0a_{2(k+1)+i}\\ &\qquad +P^{k+1+i}_{2(k+1)+i}(x_0,x_1,\dots,x_{k+i})+M_{2(k+1)+i}(x_0,x_1,\dots,x_{k+i}).\end{aligned}$$

Таким образом, система сравнений верна для $k+1$. □

Теорема 4.5. *Пусть* $|a|_p = |b|_p = 1$, $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ *и* x *такой, что для некоторого* k $(k \geq 1)$ *имеет место* $A_{k-j} \equiv 0 \pmod p$, $1 \leq j \leq k$, $A_k \not\equiv 0 \pmod p$. *Тогда* $x \in \mathbb{Z}_p^*$ *является решением уравнения* (1) *в том и только в том случае, когда следующая система сравнений имеет решение:*

$$x_0^3 + a_0 x_0 \equiv b_0 \pmod p,$$

$$x_{j-1}a_j + x_{j-2}a_{j+1} + \dots + x_0 a_{2j-1} + P_{2j-1}(x_0, x_1, \dots, x_{j-1}) \\ + M_{2j-1}(x_0, x_1, \dots, x_{j-1}) \equiv b_{2j-1} \pmod p, \quad (8)$$

$$(A_j - 3x_0 x_j)x_j + x_{j-1}a_{j+1} + x_{j-2}a_{j+2} + \dots + x_0 a_{2j} + P_{2j}(x_0, x_1, \dots, x_{j-1}) \\ + M_{2j}(x_0, x_1, \dots, x_{j-1}) \equiv b_{2j} \pmod p,$$

где $1 \leq j \leq k$ *и*

$$p \cdot M_1(x_0) = x_0^3 + a_0 x_0 - b_0,$$

$$p \cdot M_{2j}(x_0, x_1, \dots, x_{j-1}) = x_{j-1}a_j + x_{j-2}a_{j+1} + \dots + x_0 a_{2j-1} \\ + P_{2j-1}(x_0, x_1, \dots, x_{j-1}) + M_{2j-1}(x_0, x_1, \dots, x_{j-1}) - b_{2j-1},$$

$$p \cdot M_{2j+1}(x_0, x_1, \dots, x_j) = (A_j - 3x_0 x_j)x_j + x_{j-1}a_{j+1} + x_{j-2}a_{j+2} + \dots + x_0 a_{2j} \\ + P_{2j}(x_0, x_1, \dots, x_{j-1}) + M_{2j}(x_0, x_1, \dots, x_{j-1}) - b_{2j}.$$

Доказательство. Необходимость. Если уравнение (1) имеет решение $x \in \mathbb{Z}_p^*$, т. е.

$$x = x_0 + x_1 p + x_2 p^2 + \dots, \quad 0 \leq x_j \leq p-1, \ x_0 \neq 0,$$

то по лемме 4.4 имеет место система сравнений.

Достаточность. Пусть система сравнений (8) имеет решение, т. е. существует решение $x_1, x_2, \dots, x_k$.

Из условия $(A_k, p) = 1$ и теоремы 2.6 имеем существование решений x_{k+i} сравнений

$$A_k x_{k+i} + x_{k+i-1}a_{k+1} + x_{k+i-2}a_{k+2} + \dots + x_0 a_{2k+i} + P_{2k+i}^{k+i}(x_0, x_1, \dots, x_{k+i-1}) \\ + M_{2k+i}(x_0, x_1, \dots, x_{k+i-1}) \equiv b_{2k+i} \pmod p,$$

где $i \geq 1$ и $M_{2k+i+1}(x_0, x_1, \dots, x_{k+i})$ рекуррентно определяются из соотношений

$$p \cdot M_{2k+i+1}(x_0, x_1, \dots, x_{k+i}) = A_k x_{k+i} + x_{k+i-1}a_{k+1} + x_{k+i-2}a_{k+2} + \dots + x_0 a_{2k+i} \\ + P_{2k+i}(x_0, x_1, \dots, x_{k+i-1}) + M_{2k+i}(x_0, x_1, \dots, x_{k+i-1}) - b_{2k+i}.$$

Тогда имеем

$$x_0^3 + a_0 x_0 + \sum_{j=1}^{k} \big(x_{j-1}a_j + x_{j-2}a_{j+1} + \dots + x_0 a_{2j-1} + P_{2j-1}^j(x_0, x_1, \dots, x_{j-1})\big) p^{2j-1}$$

$$+ \sum_{j=1}^{k} \big((A_j - 3x_0 x_j)x_j + x_{j-1}a_{j+1} + x_{j-2}a_{j+2} + \dots + x_0 a_{2j} + P_{2j}^j(x_0, x_1, \dots, x_{j-1})\big) p^{2j}$$

$$+ \sum_{i=1}^{\infty} \big(A_k x_{k+i} + x_{k+i-1}a_{k+1} + x_{k+i-2}a_{k+2} + \dots + x_0 a_{2k+i}$$

$$+ P_{2k+i}^{k+i}(x_0, x_1, \dots, x_{k+i-1})\big)p^{2k+i}$$

$$= b_0 + p \cdot M_1(x_0) + \sum_{j=1}^{k} b_{2j-1} - M_{2j-1}(x_0, x_1, \dots, x_{j-1}) + p \cdot M_{2j}(x_0, x_1, \dots, x_{j-1})$$

$$+ \sum_{j=1}^{k} b_{2j} - M_{2j}(x_0, x_1, \dots, x_{j-1}) + p \cdot M_{2j+1}(x_0, x_1, \dots, x_j)$$

$$+ \sum_{i=1}^{\infty} b_{2k+i} - M_{2k+i}(x_0, x_1, \dots, x_{k+i-1}) + p \cdot M_{2k+i+1}(x_0, x_1, \dots, x_{k+i})$$

$$= b_0 + \sum_{j=1}^{\infty} b_j p^j.$$

Таким образом, $x = \sum\limits_{k=0}^{\infty} x_k p^k$, удовлетворяющее условиям теоремы, является решением уравнения (1). $\square$

Следующая теорема завершает случай $|a|_p = |b|_p = 1$.

Теорема 4.6. *Пусть* $|a|_p = |b|_p = 1$, $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod p$ *и* $x \in \mathbb{Z}_p^*$ *такой, что* $A_k \equiv 0 \pmod p$ *для всех* $k \in \mathbb{N}$. *Тогда* x *является решением уравнения* (1) *тогда и только тогда, когда следующая система сравнений имеет решение:*

$$x_0^3 + a_0 x_0 \equiv b_0 \pmod p,$$

$$x_{j-1}a_j + x_{j-2}a_{j+1} + \dots + x_0 a_{2j-1} + P_{2j-1}^{j}(x_0, x_1, \dots, x_{j-1}) \\ + M_{2j-1}(x_0, x_1, \dots, x_{j-1}) \equiv b_{2j-1} \pmod p,$$

$$(A_j - 3x_0x_j)x_j + x_{j-1}a_{j+1} + x_{j-2}a_{j+2} + \dots + x_0 a_{2j} + P_{2j}^{j}(x_0, x_1, \dots, x_{j-1}) \\ + M_{2j}(x_0, x_1, \dots, x_{j-1}) \equiv b_{2j} \pmod p, \quad (9)$$

где $j \geq 1$,

$$p \cdot M_1(x_0) = x_0^3 + a_0 x_0 - b_0$$

$$p \cdot M_{2j}(x_0, x_1, \dots, x_{j-1}) = x_{j-1}a_j + x_{j-2}a_{j+1} + \dots + x_0 a_{2j-1} \\ + P_{2j-1}(x_0, x_1, \dots, x_{j-1}) + M_{2j-1}(x_0, x_1, \dots, x_{j-1}) - b_{2j-1},$$

$$p \cdot M_{2j+1}(x_0, x_1, \dots, x_j) = (A_j - 3x_0x_j)x_j + x_{j-1}a_{j+1} + x_{j-2}a_{j+2} + \dots + x_0 a_{2j} \\ + P_{2j}(x_0, x_1, \dots, x_{j-1}) + M_{2j}(x_0, x_1, \dots, x_{j-1}) - b_{2j}.$$

Доказательство. Необходимость. Если уравнение (1) имеет решение $x \in \mathbb{Z}_p^*$, т. е.

$$x = x_0 + x_1 p + x_2 p^2 + \dots, \quad 0 \leq x_j \leq p-1,\ x_0 \neq 0,$$

то аналогично доказательству леммы 4.4 имеет место система сравнений.

Достаточность. Пусть система сравнений (9) имеет решение. Тогда

$$x_0^3 + a_0 x_0 + \sum_{j=1}^{\infty}\big(x_{j-1}a_j + x_{j-2}a_{j+1} + \dots + x_0 a_{2j-1} + P_{2j-1}^{j}(x_0, x_1, \dots, x_{j-1})\big)p^{2j-1}$$

$$+\sum_{j=1}^{\infty}\big((A_j-3x_0x_j)x_j+x_{j-1}a_{j+1}+x_{j-2}a_{j+2}+\dots+x_0a_{2j}+P_{2j}^{j}(x_0,x_1,\dots,x_{j-1})\big)p^{2j}$$

$$=b_0+p\cdot M_1(x_0)+\sum_{j=1}^{\infty}(b_{2j-1}-M_{2j-1}(x_0,x_1,\dots,x_{j-1})+p\cdot M_{2j}(x_0,x_1,\dots,x_{j-1}))$$

$$+\sum_{j=1}^{\infty}(b_{2j}-M_{2j}(x_0,x_1,\dots,x_{j-1})+p\cdot M_{2j+1}(x_0,x_1,\dots,x_j))=b_0+\sum_{j=1}^{\infty}b_jp^j,$$

т. е. x является решением уравнения (1). □

Рассмотрим случай $|a|_p=|b|_p>1$.

Теорема 4.7. *Пусть* $|a|_p=|b|_p>1$, *и обозначим*

$$\log_p|a|_p=\log_p|b|_p=-m,\quad m\geq 1.$$

Тогда x *является решением уравнения* (1) *в* $\mathbb{Z}_p^*$ *в том и только в том случае, когда оно удовлетворяет следующим сравнениям:*

$$a_0x_0\equiv b_0 \ (\operatorname{mod} p),$$

$$a_0x_k+a_1x_{k-1}+\dots+a_kx_0+M_k(x_0,\dots,x_{k-1})\equiv b_k \ (\operatorname{mod} p),\quad 1\leq k\leq m-1,$$

$$a_0x_m+a_1x_{m-1}+\dots+a_mx_0+x_0^3+M_m(x_0,\dots,x_{m-1})\equiv b_m \ (\operatorname{mod} p),$$

$$a_0x_k+a_1x_{k-1}+\dots+a_kx_0+3x_0^2x_{k-m}+N_{k-m}(x_0,x_1,\dots,x_{k-m-1}) \\ +M_k(x_0,\dots,x_{k-1})\equiv b_k \ (\operatorname{mod} p),\quad k\geq m+1,$$

где $M_k(x_0,x_1,\dots,x_{k-1})$ *последовательно определяются из соотношений:*

$$a_0x_0=b_0+M_1(x_0)\cdot p,$$

$$a_0x_k+a_1x_{k-1}+\dots+a_kx_0+M_k(x_0,\dots,x_{k-1})=b_k+M_{k+1}(x_0,\dots,x_k)\cdot p, \\ 1\leq k\leq m-1,$$

$$a_0x_m+a_1x_{m-1}+\dots+a_mx_0+x_0^3+M_m(x_0,\dots,x_{m-1})=b_m+M_{m+1}(x_0,\dots,x_m)\cdot p,$$

$$a_0x_k+a_1x_{k-1}+\dots+a_kx_0+3x_0^2x_{k-m}+N_{k-m}(x_0,x_1,\dots,x_{k-m-1}) \\ +M_k(x_0,\dots,x_{k-1})=b_k+M_{k+1}(x_0,\dots,x_k)\cdot p,\quad k\geq m+1.$$

Доказательство. Напомним, что условие $|a|_p=|b|_p>1$ обеспечивает тот факт, что уравнение (1) имеет решение. Умножив уравнение (6) на p^m, получим

$$p^m\left(x_0^3+\sum_{k=1}^{\infty}\left(3x_0^2x_k+N_k(x_0,x_1,\dots,x_{k-1})\right)p^k\right)+a_0x_0+\sum_{k=1}^{\infty}\left(\sum_{s=0}^{k}x_sa_{k-s}\right)p^k$$

$$=a_0x_0+\sum_{k=1}^{m-1}\left(x_0a_k+x_1a_{k-1}+\dots+x_ka_0\right)p^k \\ +\big(x_0^3+x_0a_m+x_1a_{m-1}+\dots+x_ma_0\big)p^m$$

$$+\sum_{k=m+1}^{\infty}\left(3x_0^2x_{k-m}+N_{k-m}(x_0,x_1,\dots,x_{k-m-1})+x_ka_0+x_{k-1}a_1+\dots+x_0a_k\right)p^k$$

$$=b_0+\sum_{k=1}^{\infty}b_kp^k,$$

откуда следует справедливость сравнений теоремы.

В силу того, что $(a_0, p) = 1$, по теореме 2.6 аналогично доказательству теоремы 4.1 существуют решения x_k следующих сравнений:

$$a_0x_0 \equiv b_0 \pmod p,$$

$$a_0x_k + a_1x_{k-1} + \dots + a_kx_0 + M_k(x_0, \dots, x_{k-1}) \equiv b_k \pmod p, \quad 1 \le k \le m-1,$$

$$a_0x_m + a_1x_{m-1} + \dots + a_mx_0 + x_0^3 + M_m(x_0, \dots, x_{m-1}) \equiv b_m \pmod p,$$

$$a_0x_k + a_1x_{k-1} + \dots + a_kx_0 + 3x_0^2x_{k-m} + N_{k-m}(x_0, x_1, \dots, x_{k-m-1}) \\ + M_k(x_0, \dots, x_{k-1}) \equiv b_k \pmod p, \quad k \ge m+1,$$

где $M_k(x_0, x_1, \dots, x_{k-1})$ указаны в утверждении теоремы.

Имеем

$$a_0x_0 + \sum_{k=1}^{m-1}(x_0a_k + x_1a_{k-1} + \dots + x_ka_0)p^k \\ + \big(x_0^3 + x_0a_m + x_1a_{m-1} + \dots + x_ma_0\big)p^m \\ + \sum_{k=m+1}^{\infty}\big(3x_0^2x_{k-m} + N_{k-m}(x_0, x_1, \dots, x_{k-m-1}) + x_ka_0 + x_{k-1}a_1 + \dots + x_0a_k\big)p^k \\ = b_0 + M_1(x_0)\cdot p + \sum_{k=1}^{m-1}(b_k - M_k(x_0, x_1, \dots, x_{k-1})\cdot p + M_{k+1}(x_0, x_1, \dots, x_k))p^k \\ + (b_m - M_m(x_0, x_1, \dots, x_{m-1}) + M_{m+1}(x_0, x_1, \dots, x_m+))p^m \\ + \sum_{k=m+1}^{\infty}(b_k - M_k(x_0, x_1, \dots, x_{k-1}) + M_{k+1}(x_0, x_1, \dots, x_k)\cdot p)\cdot p^k = b_0 + \sum_{k=1}^{\infty} b_kp^k.$$

Следовательно, $x = \sum\limits_{k=0}^{\infty} x_kp^k$, удовлетворяющее сравнениям теоремы, является решением уравнения (1). $\square$

Таким образом, в случае, когда уравнение $x^3 + ax = b$ имеет решение, мы привели необходимые и достаточные условия на p-адическое число $x \in \mathbb{Z}_p^*$, при котором оно является решением данного уравнения.

ЛИТЕРАТУРА

1. *Aref'eva L. Ya., Dragovich B., Frampton P. H., Volovich I. V.* The wave function of the universe and p-adic gravity // Internat. J. Modern Phys. A. 1991. V. 6. P. 4341–4358.
2. *Beltrametti E., Cassinelli G.* Quantum mechanics and p-adic numbers // Found. Phys. 1972. V. 2. P. 1–7.
3. *Freund P. G. O., Witten E.* Adelic string amplitudes // Phys. Lett. B. 1987. V. 199, N 2. P. 191–194.
4. *Khrennikov A. Yu.* p-Adic quantum mechanics with p-adic valued functions // J. Math. Phys. 1991. V. 32, N 4. P. 932–936.
5. *Khrennikov A. Yu.* p-Adic valued distributions in mathematical physics. Dordrecht: Kluwer, 1994.
6. *Manin Yu.* New dimensions in geometry. Berlin: Springer-Verl., 1985. P. 59–101. (Lect. Notes Math.; V. 1111).
7. *Marinari E., Parisi G.* On the p-adic five-point function // Phys. Lett. 1988. V. 203. P. 52–56.
8. *van der Blij F., Monna A.* Models of space and time in elementary physics // J. Math. Anal. Appl. 1968. V. 22. P. 537–545.

9. *Mukhamedov F. M., Rozikov U. A.* On Gibbs measures of p-adic Potts model on the Cayley tree // Indag. Math. (N. S.) 2004. V. 15, N 1. P. 85–100.

10. *Mukhamedov F. M., Rozikov U. A.* On inhomogeneous p-adic Potts model on a Cayley tree // Infin. Dimens. Anal. Quantum Probab. Relat. Top. 2005. V. 8, N 2. P. 277–290.

11. *Volovich I. V.* p-Adic string // Classical Quantum Gravity. 1987. V. 4, N 4. P. 83–87.

12. *Владимиров В. С., Волович И. В., Зеленов Е. И.* p-адический анализ и математическая физика. М.: Физматлит, 1994.

13. *Lang S.* Algebraic number theory. New York: Springer-Verl., 1994.

14. *Neukirch J.* Algebraic number theory. Berlin: Springer-Verl., 1999.

15. *Serre J.-P.* Local fields. New York: Springer-Verl., 1979.

16. *Gouvea F. Q.* P-adic Numbers. An introduction. Berlin: Springer-Verl., 1997.

17. *Koblitz N.* p-Adic numbers, p-adic analysis, and zeta functions. New York: Springer-Verl., 1984.

18. *Schikhof W. H.* Ultrametric calculus: an introduction to p-adic analysis. Cambridge: Cambridge Univ. Press, 1984.

19. *Avendano M., Ibrahim A., Rojas J. M., Rusek K.* Near NP-completeness for detecting p-adic rational roots in one variable // arXiv:1001.4252.

20. *Avendano M., Ibrahim A., Rojas J. M., Rusek K.* Faster p-adic feasibility for certain multivariate sparce polynomials // arXiv:1010.5310.

21. *Mukhamedov F., Saburov M.* On equation $x^q = a$ over $\mathbb{Q}_p$ // J. Number Theory. 2013. V. 13. P. 55–58.

22. *Casas J. M., Omirov B. A., Rozikov U. A.* Solvability criteria for the equation $x^q = a$ in the field of p-adic numbers // arXiv:1102.2156.

23. *Ayupov Sh. A., Kurbanbaev T. K.* The classification of 4-dimensional p-adic filiform Leibniz algebras // TWMS J. Pure Appl. Math. 2010. V. 1, N 2. P. 155–162.

24. *Khudoyberdiyev A. Kh., Kurbanbaev T. K., Omirov B. A.* Classification of three-dimensional solvable p-adic Leibniz algebras // P-Adic Numbers Ultrametric Anal. Appl. 2010. V. 2. P. 207–221.

25. *Mukhamedov F., Omirov B., Saburov M.* On cubic equations over p-adic field // arXiv 1204.1743.

26. *Khudoyberdiyev A. Kh., Kurbanbaev T. K., Masutova K. K.* On the solutions of the equation $x^3 + ax = b$ in $\mathbb{Z}_3^*$ with coefficients from $\mathbb{Q}_3$ // arxiv: 1110.1010.

27. *Serre J.-P.* On a theorem of Jordan // Bull. Amer. Math. Soc. 2003. V. 40. P. 429–440.

28. *Sun Z. H.* On the theory of cubic residues and nonresidues // Acta Arith. 1998. V. 84. P. 291–335.

29. *Sun Z. H.* Cubic and quartic congruences modulo a prime // J. Num. Theory. 2003. V. 102. P. 41–89.

30. *Sun Z. H.* Cubic residues and binary quadratic forms // J. Number Theory. 2007. V. 124. P. 62–104.

31. *Borevich Z. I., Shafarevich I. R.* Number theory. New York: Acad. Press, 1966.

32. *Rosen K. H.* Elementary number theory and its applications. Pearson: Addison Wesley, 2011.

Статья поступила 23 апреля 2012 г.

Мухамедов Фаррух Максутович, Сабуров Мансур Хаджибаевич
Faculty of Science, International Islamic University Malaysia
P.O. Box, 141, Kuantan, Pahang, 25710, Malaysia
far75m@yandex.ru, farrukh_m@iium.edu.my, msaburov@gmail.com

Омиров Бахром Абдазович, Масутова Камилям Камаловна
Институт математики при национальном университете Узбекистана
им. Мирзо Улугбека,
ул. Дурмон Йули, 29, Ташкент 100125, Узбекистан
omirovb@mail.ru, kamilyam81@mail.ru