RESEARCH ARTICLE
doi: 10.2306/scienceasia1513-1874.2015.41.209

ScienceAsia 41 (2015): **209–215**

Quadratic equations over p-adic fields and their applications in statistical mechanics

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

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

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

Received 16 Sep 2014
Accepted 8 Apr 2015

ABSTRACT: The p-adic models of statistical mechanics require the investigation of the roots of polynomial equations over p-adic fields in order to construct p-adic Gibbs measures. The most frequently asked question is that whether a root of a polynomial equation belongs to the domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Z}_p$, $\mathbb{Q}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus (\mathbb{Z}_p \setminus \mathbb{Z}_p^*)$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{S}_{p^m}(0)$ or not. This question was open even for a quadratic equation. In this paper, by using the Newton polygon, we provide solvability criteria for quadratic equations over the domains mentioned above for all odd primes p. We also study the number of roots of quadratic equations over all domains given above. This study allows us to present a local description of roots of quadratic equations over p-adic fields whenever $p > 2$.

KEYWORDS: solvability criterion, number of roots, Potts model, p-adic Gibbs measure, Newton polygon

MSC2010: 11S05 11S31 82B20 82B26

INTRODUCTION

The field of p-adic numbers

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

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

Here, $x = p^k m/n$ with $k, m \in \mathbb{Z}$, $n \in \mathbb{N}$, $(m, p) = (n, p) = 1$. The number k is called a p-order of x and it is denoted by $\mathrm{ord}_p(x) = k$.

Any p-adic number $x \in \mathbb{Q}_p$ can be uniquely represented in the following canonical form: $x = p^{\mathrm{ord}_p(x)}(x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots)$ where $x_0 \in \{1, 2, \ldots p-1\}$ and $x_i \in \{0, 1, 2, \ldots p-1\}$, $i \geqslant 1$ [1,2]. We denote the set of all p-adic integers and units of $\mathbb{Q}_p$ by $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}$ and $\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}$, respectively. Any p-adic unit $x \in \mathbb{Z}_p^*$ has the unique canonical form $x = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots$ where $x_0 \in \{1, 2, \ldots p-1\}$ and $x_i \in \{0, 1, 2, \ldots p-1\}$, $i \in \mathbb{N}$. Any non-zero $x \in \mathbb{Q}_p$ has a unique representation $x = x^*/|x|_p$, where $x^* \in \mathbb{Z}_p^*$.

A number $a \in \mathbb{Z}$ is called a quadratic residue modulo p if the congruent equation $x^2 = a \pmod p$ is solvable in $\mathbb{Z}$.

Proposition 1 (Ref. 3) *Let p be an odd prime, $a \in \mathbb{Z}$, and $(a, p) = 1$. The number a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$.*

Proposition 2 (Refs. 1, 4) *Let p be an odd prime, $a \in \mathbb{Q}_p$ be a non-zero p-adic number, and $a = a^*/|a|_p$ with $a^* = a_0 + a_1 p + a_2 p^2 + \cdots$. The quadratic equation $x^2 = a$ is solvable in $\mathbb{Q}_p$ if and only if $\log_p |a|_p$ is even and $a_0^{(p-1)/2} \equiv 1 \pmod p$.*

p-adic Gibbs measures on a Cayley tree

Statistical mechanics is a mathematical theory of a mechanical system having uncertain state systems in which probabilistic concepts and explanation play a fundamental role. In Ref. 5, a p-adic counterpart of statistical mechanics is also studied in the context of the p-adic theory of probability and stochastic processes. More recently, numerous applications of p-adic numbers have shown up in theoretical physics and quantum mechanics [6–9].

By following Refs. 10–13, we briefly mention some notions and notation from p-adic Gibbs measure theory on a Cayley tree for the sake of a self-contained exposition. A Cayley tree Γ^k of order $k \geqslant 1$ is an infinite tree, i.e., a graph without cycles, such that exactly $k+1$ edges originate from each vertex. Let $\Gamma^k_+ = (V, L)$ be a semi-infinite Cayley tree of order $k \geqslant 1$ with the root Θ (each vertex has exactly $k+1$ edges except for the root Θ which has k edges) where V is the set of vertices and L is the set of edges. Two vertices v_1 and v_2 are called nearest neighbours if there exists an edge $l \in L$ connecting them. We shall use the notation $l = \langle v_1, v_2\rangle$. A collection of nearest neighbour pairs $\langle v', v_1\rangle, \langle v_1, v_2\rangle, \ldots, \langle v_{d-1}, v''\rangle$ is called a path from v' to v''. The distance $d(v', v'')$ on the Cayley tree is the number of edges of the shortest path from v' to v''. For a fixed $v_0 \in V$, called the root, we let $W_n = \{v \in V : \ d(x, x_0) = n\}$, $V_n = \bigcup_{m=0}^{n} W_m$. The set $S(v) = \{w \in W_{n+1} : d(w, v) = 1\}$ is called a set of direct successors of $v \in W_n$.

Let $\Phi = \{1, 2, \ldots, q\}$ be a finite set. A configuration (respectively, a finite volume configuration, a boundary configuration) is a function $\sigma : V \to \Phi$ (respectively, $\sigma_n : V_n \to \Phi$, $\sigma^{(n)} : W_n \to \Phi$). We denote by Ω (respectively, Ω_{V_n}, Ω_{W_n}) a set of all configurations (respectively, all finite volume configurations, all boundary configurations). For given configurations $\sigma_{n-1} \in \Omega_{V_{n-1}}$ and $\sigma^{(n)} \in \Omega_{W_n}$, we define their concatenation to be a finite volume configuration $\sigma_{n-1} \vee \sigma^{(n)} \in \Omega_{V_n}$ such that

$$\sigma_{n-1} \vee \sigma^{(n)}(v) = \begin{cases} \sigma_{n-1}(v), & v \in V_{n-1}, \\ \sigma^{(n)}(v), & v \in W_n. \end{cases}$$

Let G_k be a free product of $k+1$ cyclic groups of the second order with generators $a_1, a_2, \ldots, a_{k+1}$. It is known that there exists a one-to-one correspondence between the set of vertices V of the Cayley tree and the group G_k. Hence, without loss of generality, we may assume that any two vertices can be multiplied. A function $f : V \to \mathbb{Q}_p$ is called translation invariant if $f(vw) = f(v)$ for any $v, w \in V$. The Hamiltonian of a p-adic Potts model with the spin value set $\Phi = \{1, 2, \ldots q\}$ on the finite volume configuration is defined as follows:

$$H_n(\sigma_n) = J \sum_{\langle x,y\rangle \in L_n} \delta_{\sigma_n(x)\sigma_n(y)}, \qquad (1)$$

for all $\sigma_n \in \Omega_{V_n}$, $n \in \mathbb{N}$ where J is a coupling constant, $\langle x, y\rangle$ stands for nearest neighbour vertices, and δ is the Kronecker delta.

Let us present a construction of a p-adic Gibbs measure corresponding to the p-adic Potts model with q states. We define a p-adic measure $\mu^{(n)}_{\tilde{\mathbf{h}}} : \Omega_{V_n} \to \mathbb{Q}_p$ associated with a boundary function $\tilde{\mathbf{h}} : V \ni x \to \tilde{\mathbf{h}}_x = (\tilde{h}^{(1)}_x, \ldots, \tilde{h}^{(q)}_x) \in \mathbb{Q}^q_p$ by

$$\mu^{(n)}_{\tilde{\mathbf{h}}}(\sigma_n) = \frac{1}{\mathscr{Z}^{(n)}_{\tilde{\mathbf{h}}}} \exp_p \left\{ H_n(\sigma_n) + \sum_{x \in W_n} \tilde{h}^{(\sigma_n(x))}_x \right\} \qquad (2)$$

for all $\sigma_n \in \Omega_{V_n}$, $n \in \mathbb{N}$ where $\exp_p(\cdot) : \mathbb{B}(0, p^{-1/(p-1)}) \to \mathbb{B}(1, 1)$ is a p-adic exponential function and $\mathscr{Z}^{(n)}_{\tilde{\mathbf{h}}}$ is a partition function defined by

$$\mathscr{Z}^{(n)}_{\tilde{\mathbf{h}}} = \sum_{\sigma_n \in \Omega_{V_n}} \exp_p \left\{ H_n(\sigma_n) + \sum_{x \in W_n} \tilde{h}^{(\sigma_n(x))}_x \right\}$$

for all $n \in \mathbb{N}$. The p-adic measures (2) are called compatible if one has that

$$\sum_{\sigma^{(n)} \in \Omega_{W_n}} \mu^{(n)}_{\tilde{\mathbf{h}}}(\sigma_{n-1} \vee \sigma^{(n)}) = \mu^{(n-1)}_{\tilde{\mathbf{h}}}(\sigma_{n-1}) \qquad (3)$$

for all $\sigma_{n-1} \in \Omega_{V_{n-1}}$ and $n \in \mathbb{N}$.

From the Kolmogorov extension theorem of the p-adic measures (2)[5], there exists a unique p-adic measure $\mu_{\mathbf{h}} : \Omega \to \mathbb{Q}_p$ such that

$$\mu_{\tilde{\mathbf{h}}}(\{\sigma \mid_{V_n} = \sigma_n\}) = \mu^{(n)}_{\tilde{\mathbf{h}}}(\sigma_n)$$

for all $\sigma_n \in \Omega_{V_n}$ and n. Depending on choices of a coupling constant J and a boundary function $\tilde{\mathbf{h}} : V \to \mathbb{Q}^q_p$, the extended measure $\mu_{\tilde{\mathbf{h}}} : \Omega \to \mathbb{Q}_p$ is called a p-adic (quasi) Gibbs measure[11,13].

The following theorem provide a criterion for an existence of a translation invariant p-adic Gibbs measure (TIpGM) associated with the boundary function $\mathbf{h}_x = \mathbf{h} = (h_1, \ldots, h_{q-1}), \forall \ x \in V$ where $h_i = \tilde{h}_i - \tilde{h}_q \in \mathbb{B}(0, p^{-1/(p-1)})$ for all $i \in \Phi$. Let $J \in \mathbb{B}(0, p^{-1/(p-1)})$, $\theta = \exp_p(J)$, $\exp_p(\mathbf{h}) := (\exp_p(h_1), \ldots, \exp_p(h_{q-1}))$.

Theorem 1 (Existence of TIpGM[12]) *There exists a TIpGM $\mu_{\mathbf{h}} : \Omega \to \mathbb{Q}_p$ associated with a boundary function $\mathbf{h}_x = \mathbf{h} = (h_1, \ldots, h_{q-1})$ for all $x \in V$ if and only if $\mathbf{z} = \exp_p(\mathbf{h})$ is a solution of*

$$z_i = \left(\frac{(\theta - 1)z_i + \sum_{j=1}^{q-1} z_j + 1}{\theta + \sum_{j=1}^{q-1} z_j} \right)^k, \quad i = \overline{1, q-1}, \qquad (4)$$

where $\mathbf{z} = (z_1, \ldots, z_{q-1})$.

In Ref. 13, a full description of all TIpGMs was given for the case $k=2$. Let $M \subset \{1,\dots,q-1\}$ be a subset and $|M|=m$. Let us consider the quadratic equation

$$m^2z^2+(2m(q-m)-(\theta-1)^2)z+(q-m)^2=0. \quad (5)$$

Theorem 2 (Description of TIpGM[13]) *Let $\mu_{\mathbf{h}}:\Omega\to\mathbb{Q}_p$ be a TIpGM on Γ_+^2 associated with a boundary function $\mathbf{h}_x=\mathbf{h}=(h_1,\dots,h_{q-1})$, for all $x\in V$. Then there exists $M_{\mathbf{h}}\subset\{1,\dots,q-1\}$ such that*

$$h_i=\begin{cases}0, & i\notin M_{\mathbf{h}},\\ \log_p z^*, & i\in M_{\mathbf{h}},\end{cases}$$

where $z^*\in\mathscr{E}_p=\{x\in\mathbb{Z}_p^*:|x-1|_p<p^{-1/(p-1)}\}$ is a solution of (5).

From Theorem 2, in order to explicitly describe a TIpGM, we have to provide a criterion for (5) in which at least one of the solutions should belong to the set $\mathscr{E}_p$.

Generally, we may come across the following problem in one form or another: provide a solvability criterion for the polynomial equation $a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0$ over the given set $\mathbb{A}\subset\mathbb{Q}_p$. This problem has different solutions for the cases $\mathbb{A}\subset\mathbb{R}$ and $\mathbb{A}\subset\mathbb{Q}_p$ For instance, $x^2+1=0$ is not solvable in $\mathbb{R}$ but it is solvable in $\mathbb{Q}_p$ for $p\equiv 1 \pmod 4$. On the other hand, any cubic equation is solvable in $\mathbb{R}$ but the simplest cubic equation $x^3=p$ is not solvable in $\mathbb{Q}_p$. Hence a solvability criterion over $\mathbb{Q}_p$ should be treated differently from the case $\mathbb{R}$. In the literature little attention was given to this problem. Recently, in Refs. 14–17, this problem was partially studied for the lower degree polynomial equations over $\mathbb{Q}_p$. In this paper, we study the abovementioned problem for a quadratic equation.

We know that any quadratic equation can be written in the form

$$x^2+ax=b \quad (6)$$

where $a,b\in\mathbb{Q}_p$. By means of completing the square, (6) takes the form $(2x+a)^2=a^2+4b$. Let $y=2x+a$ and $D=a^2+4b$ be the discriminant. Then $y^2=D$. The solvability criterion for (6) can be given in terms of the discriminant as follows. If $D=0$ then the quadratic equation always has two solutions $x_1=x_2=-\frac{1}{2}a$. Let $D=a^2+4b\neq 0$. We then have that $D=D^*/|D|_p$ with $D^*\in\mathbb{Z}_p^*$, i.e., $D^*=d_0+d_1p+d_2p^2+\cdots$ where $d_0\in\{1,2,\dots p-1\}$ and $d_i\in\{0,1,2,\dots p-1\}$ for any $i\in\mathbb{N}$.

Theorem 3 (Solvability criterion by D) *Let $p>2$. The quadratic equation (6) is solvable in $\mathbb{Q}_p$ if and only if $\log_p|D|_p$ is even and $d_0^{(p-1)/2}\equiv 1 \pmod p$.*

In this case, the two solutions of the quadratic equation (6) are formally given by $x_\pm=\frac{1}{2}(-a\pm\sqrt{D})$. Based on the last formula, it is quite difficult to verify whether the solution of the quadratic equation (6) belongs to the classical sets $\mathbb{Z}_p^*$, $\mathbb{Z}_p\setminus\mathbb{Z}_p^*$, $\mathbb{Z}_p$, $\mathbb{Q}_p\setminus\mathbb{Z}_p^*$, $\mathbb{Q}_p\setminus(\mathbb{Z}_p\setminus\mathbb{Z}_p^*)$, $\mathbb{Q}_p\setminus\mathbb{Z}_p$, $\mathbb{Q}_p$ or not. For instance, in Ref. 13, the authors have used this long and technically difficult method for the quadratic equation (5). In this paper, we are suggesting another approach to give the solvability criteria of the quadratic equation (6) over the domains given above.

The main problems

Let $\mathbb{A},\mathbb{B}\subset\mathbb{Q}_p$ be two nonempty disjoint sets.

Definition 1 We say that (6) is solvable in $\mathbb{A}$ if at least one solution belongs to $\mathbb{A}$. We say that (6) is solvable in $\mathbb{A}\sqcup\mathbb{A}$ if two solutions belong to $\mathbb{A}$. We say that (6) is solvable in $\mathbb{A}\sqcup\mathbb{B}$ if one solution belongs to $\mathbb{A}$ and another solution belongs to $\mathbb{B}$.

The main problems of the paper are as follows. Let $a,b\in\mathbb{Q}_p$.

(i) Provide solvability criteria in domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p\setminus\mathbb{Z}_p^*$, $\mathbb{Z}_p$, $\mathbb{Q}_p\setminus\mathbb{Z}_p^*$, $\mathbb{Q}_p\setminus(\mathbb{Z}_p\setminus\mathbb{Z}_p^*)$, $\mathbb{Q}_p\setminus\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{S}_{p^m}(0)$.

(ii) Provide the number $\mathbf{N}(x^2+ax-b)$ of solutions in domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p\setminus\mathbb{Z}_p^*$, $\mathbb{Z}_p$, $\mathbb{Q}_p\setminus\mathbb{Z}_p^*$, $\mathbb{Q}_p\setminus(\mathbb{Z}_p\setminus\mathbb{Z}_p^*)$, $\mathbb{Q}_p\setminus\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{S}_{p^m}(0)$.

(iii) Provide solvability criteria in $\mathbb{A}\sqcup\mathbb{B}$ where

$$\mathbb{A},\mathbb{B}\in\{\mathbb{Z}_p^*,\mathbb{Z}_p\setminus\mathbb{Z}_p^*,\mathbb{Q}_p\setminus\mathbb{Z}_p\}.$$

THE MAIN RESULTS

In this section, we provide the main results of the paper. Throughout this paper, we always assume that $p>2$ unless otherwise mentioned.

Let $a,b\in\mathbb{Q}_p$ and $D=a^2+4b$. If $abD\neq 0$ then we have that $a=a^*/|a|_p$, $b=b^*/|b|_p$, $D=D^*/|D|_p$ with a^*, b^*, $D^*\in\mathbb{Z}_p^*$, i.e., $a^*=a_0+a_1p+a_2p^2+\cdots$, $b^*=b_0+b_1p+b_2p^2+\cdots$, $D^*=d_0+d_1p+d_2p^2+\cdots$ where $a_0,b_0,d_0\in\{1,2,\dots p-1\}$ and $a_i,b_i,d_i\in\{0,1,2,\dots p-1\}$ for any $i\in\mathbb{N}$.

Let us first consider the quadratic congruent equation $x^2\equiv a_0 \pmod p$. From Proposition 1, the quadratic congruent equation is solvable if and only if $a_0^{(p-1)/2}\equiv 1 \pmod p$. In this case, it has two distinct non-congruent solutions in the set $\{-\frac{1}{2}(p-1),\dots,-1,0,1,\dots,\frac{1}{2}(p-1)\}$. It is clear that one

solution belongs to $\{-\frac{1}{2}(p-1),\dots,-2,-1\}$ and another solution belongs to $\{1,2,\dots,\frac{1}{2}(p-1)\}$.

We denote by $\sqrt{a_0}$ (respectively, $-\sqrt{a_0}$) the solution of the quadratic congruent equation $x^2 \equiv a_0 \pmod p$ which is in $\{1,2,\dots,\frac{1}{2}(p-1)\}$ (respectively, in $\{-\frac{1}{2}(p-1),\dots,-2,-1\}$). In other words, there exists $\sqrt{a_0}$ if and only if $a_0^{(p-1)/2} \equiv 1 \pmod p$.

Let us now consider the quadratic equation $x^2 = a$ over $\mathbb{Q}_p$ where $a \in \mathbb{Q}_p$ is a non-zero p-adic number. Let $a = a^*/|a|_p$ with $a^* = a_0 + a_1 p + a_2 p^2 + \cdots$ such that $a_0 \in \{1,2,\dots,p-1\}$, $a_i \in \{0,1,2,\dots,p-1\}$, for all $i \in \mathbb{N}$. We know that the last quadratic equation is solvable in $\mathbb{Q}_p$ if and only if $a_0^{(p-1)/2} \equiv 1 \pmod p$ and $\log_p |a|_p$ is even. Moreover, it has two distinct solutions x_+ and x_- such that $x_+^* \equiv \sqrt{a_0} \pmod p$ and $x_-^* \equiv -\sqrt{a_0} \pmod p$.

We denote the solution x_+ (respectively, x_-) of the quadratic equation $x^2 = a$ by $\sqrt{a}$ (respectively, $-\sqrt{a}$). In other words, for the given non-zero $a \in \mathbb{Q}_p$, $\sqrt{a}$ exists if and only if $a_0^{(p-1)/2} \equiv 1 \pmod p$ and $\log_p |a|_p$ is even. Moreover, $\sqrt{a}$ is the solution such that $(\sqrt{a})^* \equiv \sqrt{a_0} \pmod p$ and $-\sqrt{a}$ is the solution such that $(-\sqrt{a})^* \equiv -\sqrt{a_0} \pmod p$. We use the notation $\sqrt{a} - \exists$ when there exists $\sqrt{a}$.

Theorem 4 (Solvability domain) *The quadratic equation* (6) *is solvable in* $\mathbb{Q}_p$ *if and only if one the following conditions holds true: (i)* $|a|_p^2 < |b|_p, \sqrt{b} - \exists$*; or (ii)* $|a|_p^2 = |b|_p, \sqrt{D} - \exists$*; or (iii)* $|a|_p^2 > |b|_p$.

Let us define the following set $\Delta = \Delta_1 \cup \Delta_2 \cup \Delta_3$ where

$$\Delta_1 = \{(a,b) \in \mathbb{Q}_p \times \mathbb{Q}_p : \ |a|_p^2 < |b|_p, \ \sqrt{b} - \exists\}$$
$$\Delta_2 = \{(a,b) \in \mathbb{Q}_p \times \mathbb{Q}_p : \ |a|_p^2 = |b|_p, \ \sqrt{D} - \exists\}$$
$$\Delta_3 = \{(a,b) \in \mathbb{Q}_p \times \mathbb{Q}_p : \ |a|_p^2 > |b|_p\}.$$

The set $\Delta \subset \mathbb{Q}_p \times \mathbb{Q}_p$ is called a solvability domain of the quadratic equation (6). Since $\mathbb{Q}_p$ is a disordered field, we could not describe the solvability domain Δ in the picture. However, we can describe the p-adic absolute value of elements of the set Δ in Fig. 1. We refer it as the solvability domain (6).

The following result gives a full description of p-adic absolute values of solutions of (6) in the solvability domain Δ.

Theorem 5 (Local Descriptions of solutions) *Let* $(a,b) \in \Delta$. *The quadratic equation* (6) *is solvable in*

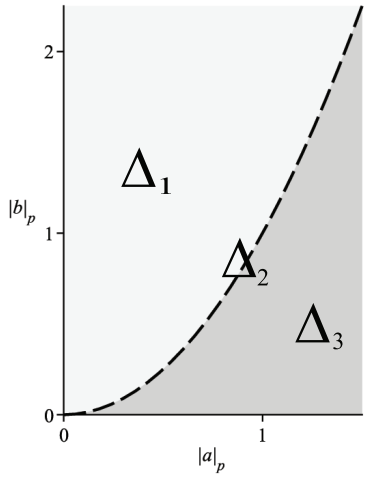

Fig. 1 The solvability domain of the quadratic equation.

(i) $\mathbb{Q}_p \setminus \mathbb{Z}_p \sqcup \mathbb{Q}_p \setminus \mathbb{Z}_p$ *if and only if*

$$|b|_p > |a|_p, |b| > 1;$$

(ii) $\mathbb{Z}_p^* \sqcup \mathbb{Z}_p^*$ *if and only if* $|a|_p \leqslant |b|_p = 1$;
(iii) $\mathbb{Z}_p \setminus \mathbb{Z}_p^* \sqcup \mathbb{Z}_p \setminus \mathbb{Z}_p^*$ *if and only if* $|a|_p < 1$, $|b| < 1$;
(iv) $\mathbb{Z}_p^* \sqcup \mathbb{Z}_p \setminus \mathbb{Z}_p^*$ *if and only if* $|b|_p < |a|_p = 1$;
(v) $\mathbb{Z}_p^* \sqcup \mathbb{Q}_p \setminus \mathbb{Z}_p$ *if and only if* $|b|_p = |a|_p > 1$;
(vi) $\mathbb{Z}_p \setminus \mathbb{Z}_p^* \sqcup \mathbb{Q}_p \setminus \mathbb{Z}_p$ *if and only if*

$$|a|_p > |b|_p, |a|_p > 1.$$

The graphical illustration of Theorem 5 is given in Fig. 2. Theorem 4 is proven in the next section (Theorem 6). Theorem 5 follows from Theorem 9 which describes the number $\mathbf{N}_{\mathbb{Z}_p^*}(x^2+ax-b)$, $\mathbf{N}_{\mathbb{Z}_p \setminus \mathbb{Z}_p^*}(x^2+ax-b)$ and $\mathbf{N}_{\mathbb{Q}_p \setminus \mathbb{Z}_p}(x^2+ax-b)$ of solutions of the quadratic equation (6) in $\mathbb{Z}_p^*, \mathbb{Z}_p \setminus \mathbb{Z}_p^*$, and $\mathbb{Q}_p \setminus \mathbb{Z}_p$. In the last section, we present the application of our results to statistical mechanics problems.

THE SOLVABILITY CRITERIA

In this section, we present a solvability criterion for the quadratic equation

$$x^2 + ax = b \tag{7}$$

over the domains $\mathbb{Z}_p^*$, $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Z}_p$, $\mathbb{Q}_p \setminus \mathbb{Z}_p^*$, $\mathbb{Q}_p \setminus (\mathbb{Z}_p \setminus \mathbb{Z}_p^*)$, $\mathbb{Q}_p \setminus \mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{S}_{p^m}(0)$.

Theorem 6 *The quadratic equation* (7) *is solvable in* $\mathbb{Q}_p$ *if and only if one of the following conditions holds:*

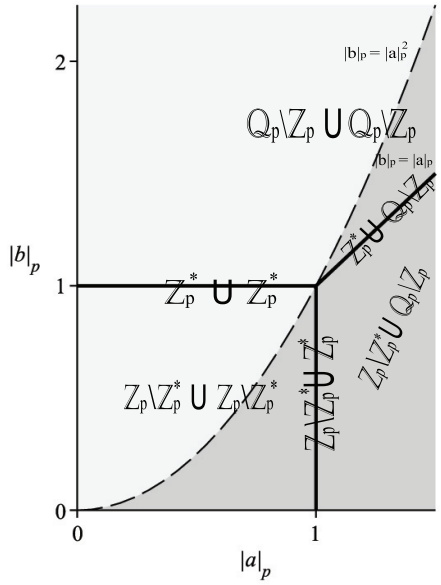

Fig. 2 The description of solutions of the quadratic equation.

(i) $|a|_p^2 < |b|_p$, $\sqrt{b}-\exists$;
(ii) $|a|_p^2 = |b|_p$, $\sqrt{D}-\exists$;
(iii) $|a|_p^2 > |b|_p$.

Proof: We know that (7) is solvable in $\mathbb{Q}_p$ if and only if there exists $\sqrt{D}$. Let us study the Newton polygon of (7) under the condition that $\sqrt{D}-\exists$.

It is clear that the Newton polygon of (7) is the lower convex hull of points $P_0(0, \mathrm{ord}_p(b))$, $P_1(1, \mathrm{ord}_p(a))$, and $P_2(2, 0)$. More precisely, if $\mathrm{ord}_p(b) \leqslant 2\mathrm{ord}_p(a)$ then the Newton polygon is one line segment with the slope $m_1 = -\frac{1}{2}\mathrm{ord}_p(b)$ and if $\mathrm{ord}_p(b) > 2\mathrm{ord}_p(a)$ then the Newton polygon is two line segments with the slopes $m_1 = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$ and $m_2 = -\mathrm{ord}_p(a)$ where $m_1 < m_2$. We study the Newton polygon in each case.

Case I: $\mathrm{ord}_p(b) < 2\mathrm{ord}_p(a)$. This is equivalent to the condition $|a|_p^2 < |b|_p$. In this case, there exists $\sqrt{D}$ if and only if there exists $\sqrt{b}$. Moreover, (7) has two solutions x_1 and x_2 in $\mathbb{Q}_p$ such that $\mathrm{ord}_p(x_1) = \mathrm{ord}_p(x_2) = \frac{1}{2}\mathrm{ord}_p(b)$ or equivalently $|x_1|_p = |x_2|_p = \sqrt{(}|b|_p) > |a|_p$.

Case II: $\mathrm{ord}_p(b) = 2\mathrm{ord}_p(a)$. This is equivalent to the condition $|a|_p^2 = |b|_p$. In this case, (7) is solvable in $\mathbb{Q}_p$ if and only if there exists $\sqrt{D}$. Moreover, for two solutions x_1 and x_2, one has that $|x_1|_p = |x_2|_p = \sqrt{(}|b|_p) = |a|_p$.

Case III: $\mathrm{ord}_p(b) > 2\mathrm{ord}_p(a)$. This is equivalent to the condition $|a|_p^2 > |b|_p$. In this case, there always exists $\sqrt{D}$. Hence (7) is always solvable in $\mathbb{Q}_p$. Moreover, (7) has two solutions x_1 and x_2 in $\mathbb{Q}_p$ such that $\mathrm{ord}_p(x_1) = \mathrm{ord}_p(b) - \mathrm{ord}_p(a)$ and $\mathrm{ord}_p(x_2) = \mathrm{ord}_p(a)$, or equivalently $|x_1|_p = |b|_p / |a|_p$ and $|x_2|_p = |a|_p$ where $|x_1|_p < |x_2|_p$. □

Theorem 7 *The quadratic equation* (7) *is solvable in* $\mathbb{Z}_p^*$ *if and only if one of the following conditions holds:*
(i) $|a|_p < |b|_p = 1$, $\sqrt{b}-\exists$;
(ii) $|a|_p = |b|_p = 1$, $\sqrt{D}-\exists$;
(iii) $|a|_p = |b|_p > 1$;
(iv) $|b|_p < |a|_p = 1$.

Proof: As we already showed that (i) if $|a|_p^2 < |b|_p$ with $\sqrt{b}-\exists$ then (7) has two solutions x_1, x_2 in $\mathbb{Q}_p$ such that $|x_1|_p = |x_2|_p = \sqrt{(}|b|_p) > |a|_p$; (ii) if $|a|_p^2 = |b|_p$ with $\sqrt{D}-\exists$ then (7) has two solutions x_1, x_2 in $\mathbb{Q}_p$ such that $|x_1|_p = |x_2|_p = \sqrt{(}|b|_p) = |a|_p$; (iii) if $|a|_p^2 > |b|_p$ then (7) has two solutions x_1, x_2 in $\mathbb{Q}_p$ such that $|x_1|_p = |b|_p / |a|_p$ and $|x_2|_p = |a|_p$ where $|x_1|_p < |x_2|_p$.

Let $|a|_p^2 < |b|_p$ and $\sqrt{b}-\exists$. The quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if $|x_1|_p = |x_2|_p = \sqrt{(}|b|_p) = 1$, this is equivalent to $|a|_p < |b|_p = 1$ and $\sqrt{b}-\exists$. In this case, both roots of (7) belong to $\mathbb{Z}_p^*$.

Let $|a|_p^2 = |b|_p$ and $\sqrt{D}-\exists$. The quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if $|x_1|_p = |x_2|_p = \sqrt{(}|b|_p) = |a|_p = 1$. This is equivalent to $|a|_p = |b|_p = 1$ and $\sqrt{D}-\exists$. In this case, both roots of (7) belong to $\mathbb{Z}_p^*$.

Let $|a|_p^2 > |b|_p$. The quadratic equation (7) is solvable in $\mathbb{Z}_p^*$ if and only if either one of the conditions $|x_1|_p = |b|_p / |a|_p = 1$ or $|x_2|_p = |a|_p = 1$ holds. Consequently, if $|a|_p = |b|_p > 1$ then $|x_1|_p = 1$ and if $|b|_p < |a|_p = 1$ then $|x_2|_p = 1$. In this case, only one root of (7) belongs to $\mathbb{Z}_p^*$. □

Similarly, one can prove the following results.

Theorem 8 *The quadratic equation* (7) *is:*

A. solvable in $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ *if and only if one of the following conditions holds:*
(i) $|a|_p^2 < |b|_p < 1$, $\sqrt{b}-\exists$,
(ii) $|a|_p^2 = |b|_p < 1$, $\sqrt{D}-\exists$,
(iii) $|a|_p^2 > |b|_p$, $|a|_p > |b|_p$;

B. solvable in $\mathbb{Q}_p \setminus \mathbb{Z}_p$ if and only if one of the following conditions holds:

(i) $|a|_p^2 < |b|_p, \quad |b|_p > 1, \quad \sqrt{b} - \exists$,
(ii) $|a|_p^2 = |b|_p > 1, \quad \sqrt{D} - \exists$,
(iii) $|a|_p^2 > |b|_p, \quad |a|_p > 1$;

C. solvable in $\mathbb{Z}_p$ if and only if one of the following conditions holds:

(i) $|a|_p^2 < |b|_p \leqslant 1, \quad \sqrt{b} - \exists$,
(ii) $|a|_p^2 = |b|_p \leqslant 1, \quad \sqrt{D} - \exists$,
(iii) $|a|_p^2 > |b|_p, \quad |a|_p \geqslant |b|_p$;

D. solvable in $\mathbb{Q}_p \setminus (\mathbb{Z}_p \setminus \mathbb{Z}_p^*)$ if and only if one of the following conditions holds:

(i) $|a|_p^2 < |b|_p, |b|_p \geqslant 1, \quad \sqrt{b} - \exists$,
(ii) $|a|_p^2 = |b|_p \geqslant 1, \quad \sqrt{D} - \exists$,
(iii) $|a|_p^2 > |b|_p, \quad |a|_p \geqslant 1$;

E. Solvable in $\mathbb{Q}_p \setminus \mathbb{Z}_p^*$ if and only if one of the following conditions holds:

(i) $|a|_p^2 < |b|_p \neq 1, \quad \sqrt{b} - \exists$,
(ii) $|a|_p^2 = |b|_p \neq 1, \quad \sqrt{D} - \exists$,
(iii) $|a|_p^2 > |b|_p$;

F. solvable in $\mathbb{S}_{p^m}(0)$ if and only if one of the following conditions holds:

(i) $|a|_p^2 < |b|_p = p^{2m}, \quad \sqrt{b} - \exists$;
(ii) $|a|_p^2 = |b|_p = p^{2m}, \quad \sqrt{D} - \exists$;
(iii) $|b|_p < |a|_p^2 = p^{2m}$;
(iv) $|a|_p^2 > |b|_p = p^m |a|_p$.

THE NUMBER OF SOLUTIONS

In this section, we present the number $\mathbf{N}_{\mathbb{A}}(x^2 + ax - b)$ of solutions (including multiplicity) of a quadratic equation, where $\mathbb{A} \in \{\mathbb{Z}_p^*, \mathbb{Z}_p \setminus \mathbb{Z}_p^*, \mathbb{Q}_p \setminus \mathbb{Z}_p, \mathbb{Z}_p, \mathbb{Q}_p \setminus (\mathbb{Z}_p \setminus \mathbb{Z}_p^*), \mathbb{Q}_p \setminus \mathbb{Z}_p^*, \mathbb{S}_{p^m}(0)\}$.

It is clear that $\mathbf{N}_{\mathbb{Q}_p}(x^2 + ax - b) = 2$ (including multiplicity) as long as (7) is solvable in $\mathbb{Q}_p$.

The proofs of the following results are already covered in the proof of Theorem 7.

Theorem 9 *Let the quadratic equation (7) be solvable in $\mathbb{A}$. The following statements hold true:*

$$\mathbf{N}_{\mathbb{Z}_p^*}(x^2+ax-b) = \begin{cases} 2, & |a|_p < |b|_p = 1, \ \sqrt{b} - \exists, \\ 2, & |a|_p = |b|_p = 1, \ \sqrt{D} - \exists, \\ 1, & |a|_p = |b|_p > 1, \\ 1, & |b|_p < |a|_p = 1; \end{cases}$$

$$\mathbf{N}_{\mathbb{Z}_p \setminus \mathbb{Z}_p^*}(x^2+ax-b) = \begin{cases} 2, & |a|_p^2 < |b|_p < 1, \ \sqrt{b} - \exists, \\ 2, & |a|_p^2 = |b|_p < 1, \ \sqrt{D} - \exists, \\ 2, & |b|_p < |a|_p^2 < 1, \\ 1, & |a|_p > |b|_p, \quad |a|_p \geqslant 1; \end{cases}$$

$$\mathbf{N}_{\mathbb{Q}_p \setminus \mathbb{Z}_p}(x^2+ax-b) = \begin{cases} 2, & |a|_p^2 < |b|_p, \ |b|_p > 1, \ \sqrt{b} - \exists, \\ 2, & |a|_p^2 = |b|_p > 1, \ \sqrt{D} - \exists, \\ 2, & |a|_p < |b|_p < |a|_p^2, \\ 1, & |a|_p \geqslant |b|_p, \quad |a|_p > 1; \end{cases}$$

$$\mathbf{N}_{\mathbb{Z}_p}(x^2+ax-b) = \begin{cases} 2, & |a|_p^2 < |b|_p \leqslant 1, \ \sqrt{b} - \exists, \\ 2, & |a|_p^2 = |b|_p \leqslant 1, \ \sqrt{D} - \exists, \\ 2, & |b|_p < |a|_p^2 \leqslant 1, \\ 1, & |a|_p \geqslant |b|_p, \quad |a|_p > 1; \end{cases}$$

$$\mathbf{N}_{\mathbb{Q}_p \setminus (\mathbb{Z}_p \setminus \mathbb{Z}_p^*)}(x^2+ax-b) = \begin{cases} 2, & |a|_p^2 < |b|_p, \ |b|_p \geqslant 1, \ \sqrt{b} - \exists, \\ 2, & |a|_p^2 = |b|_p \geqslant 1, \ \sqrt{D} - \exists, \\ 2, & |a|_p \leqslant |b|_p < |a|_p^2, \\ 1, & |a|_p > |b|_p, \quad |a|_p > 1; \end{cases}$$

$$\mathbf{N}_{\mathbb{Q}_p \setminus \mathbb{Z}_p^*}(x^2+ax-b) = \begin{cases} 2, & |a|_p^2 < |b|_p \neq 1, \ \sqrt{b} - \exists, \\ 2, & |a|_p^2 = |b|_p \neq 1, \ \sqrt{D} - \exists, \\ 2, & |a|_p^2 > |b|_p, \ |a|_p \neq 1, \ |a|_p \neq |b|_p, \\ 1, & |b|_p < |a|_p = 1, \\ 1, & |a|_p = |b|_p > 1; \end{cases}$$

$$\mathbf{N}_{\mathbb{S}_{p^m}(0)}(x^2+ax-b) = \begin{cases} 2, & |a|_p^2 < |b|_p = p^{2m}, \ \sqrt{b} - \exists, \\ 2, & |a|_p^2 = |b|_p = p^{2m}, \ \sqrt{D} - \exists, \\ 1, & |b|_p < |a|_p^2 = p^{2m}, \\ 1, & |a|_p^2 > |b|_p = p^m |a|_p. \end{cases}$$

Corollary 1 *Let the quadratic equation* (7) *be solvable in* $\mathbb{A} \in \{\mathbb{Z}_p^*,\ \mathbb{Z}_p \setminus \mathbb{Z}_p^*\}$. *Then one has that*

$$\mathbf{N}_{\mathbb{Z}_p^*}(x^2+ax-b) = \begin{cases} 2, & |b|_p = 1, \\ 1, & |b|_p \neq 1, \end{cases}$$

$$\mathbf{N}_{\mathbb{Z}_p \setminus \mathbb{Z}_p^*}(x^2+ax-b) = \begin{cases} 2, & |a|_p < 1, \\ 1, & |a|_p \geqslant 1. \end{cases}$$

APPLICATIONS

In this section, we try to solve the following problem which was arisen from the construction of the TIpGM associated with the p-adic Potts model with q-states. Let us consider

$$x^2+ax = b. \tag{8}$$

Let $p > 2$. Provide solvability criteria of (8) over the set $\mathscr{E}_p = \{x \in \mathbb{Z}_p^* : |x-1|_p < 1\}$.

Let $x-1 = y$. Then (8) takes the following form:

$$y^2+(a+2)y = b-a-1. \tag{9}$$

Consequently, the solvability of (8) over $\mathscr{E}_p$ is equivalent to the solvability of (9) over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$. The solvability criterion of (9) over $\mathbb{Z}_p \setminus \mathbb{Z}_p^*$ was given in Theorem 8. It is clear that $x = 1$ is a solution of (8) if and only if $b = a+1$. Moreover, in this case, $x = 1$ and $x = -a-1$ are solutions. Hence we always suppose that $b \neq a+1$. By means of Theorem 8 and Corollary 1, we get the following results.

Theorem 10 *The quadratic equation* (8) *is solvable over* $\mathscr{E}_p$ *if and only if one of the following conditions holds:*

(i) $|a+2|_p^2 < |b-a-1|_p < 1$, $\sqrt{b-a-1} - \exists$,

(ii) $|a+2|_p^2 = |b-a-1|_p < 1$, $\sqrt{a^2+4b} - \exists$,

(iii) $|a+2|_p^2 > |b-a-1|_p$, $|a+2|_p > |b-a-1|_p$.

Theorem 11 *Let the quadratic equation* (8) *be solvable over* $\mathscr{E}_p$. *Then the following holds:*

$$\mathbf{N}_{\mathscr{E}_p}(x^2+ax-b) = \begin{cases} 2, & |a+2|_p < 1, \\ 1, & |a+2|_p \geqslant 1. \end{cases}$$

Acknowledgements: The first author (M.S.) thanks the MOE (grant ERGS13-025-0058) for financial support. The authors wish to express their gratitude to the anonymous referees for several helpful comments concerning the presentation of the paper.

REFERENCES

1. Borevich ZI, Shafarevich IR (1966) *Number Theory*, Academic Press.
2. Koblitz N (1984) *p-adic Numbers, p-adic Analysis, and Zeta Functions*, Springer.
3. Rosen KH (2011) *Elementary Number Theory and its Applications*, Pearson.
4. Gouvea FQ (1997) *p-adic Numbers: An Introduction*, Springer-Verlag.
5. Ludkovsky S, Khrennikov A (2003) Stochastic processes on non-Archimedean spaces with values in non-Archimedean fields. *Markov Process Relat Field* **9**, 131–62.
6. Beltrametti E, Cassinelli G (1972) Quantum mechanics and p-adic numbers. *Found Phys* **2**, 1–7.
7. Khrennikov AYu (1991) p-adic quantum mechanics with p-adic valued functions. *J Math Phys* **32**, 932–6.
8. Khrennikov AYu (1994) *p-adic Valued Distributions in Mathematical Physics*, Kluwer.
9. Volovich IV (1987) p-adic strings. *Class Quant Grav* **4**, 83–7.
10. Mukhamedov F (2013) On dynamical systems and phase transitions for $q+1$-state p-adic Potts model on the Cayley tree. *Math Phys Anal Geom* **16**, 49–87.
11. Mukhamedov F, Akin H (2013) Phase transitions for p-adic Potts model on the Cayley tree of order three. *J Stat Mech* **7**, P07014.
12. Mukhamedov F, Rozikov U (2004) On Gibbs measures of p-adic Potts model on Cayley tree. *Indagat Math* **15**, 85–100.
13. Rozikov U, Khakimov O (2015) Description of all translation-invariant p-adic Gibbs measures for the Potts model on a Cayley tree. *Markov Process Relat Field* **21**, 177–204.
14. Mukhamedov F, Omirov B, Saburov M (2014) On cubic equations over p-adic field. *Int J Number Theor* **10**, 1171–90.
15. Mukhamedov F, Omirov B, Saburov M, Masutova K (2013) Solvability of cubic equations in p-adic integers, $p > 3$. *Siberian Math J* **54**, 501–16.
16. Mukhamedov F, Saburov M (2013) On equation $x^q = a$ over $\mathbb{Q}_p$. *J Number Theor* **133**, 55–8.
17. Saburov M, Ahmad MAKh (2014) Solvability criteria for cubic equations over $\mathbb{Z}_2^*$. *AIP Conf Proc* **1602**, 792–7.