

# An Explicit Construction of Orthogonal Basis in $p$ -adic Fields

Chi Zhang<sup>1,2,\*</sup> and Yingpu Deng<sup>1,2</sup>

<sup>1</sup> *State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, P.R. China.*

<sup>2</sup> *School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, P.R. China.*

Received 16 June 2025; Accepted 10 November 2025

---

**Abstract.** In 2021, the  $p$ -adic signature scheme and public-key encryption cryptosystem were introduced. These schemes have good efficiency but are shown to be not secure. The attack succeeds because the extension fields used in these schemes are totally ramified. In order to avoid this attack, the extension field should have a large residue degree. In this paper, we propose a method of constructing a kind of specific orthogonal basis in  $p$ -adic fields with a large residue degree, which would be helpful to modify the  $p$ -adic signature scheme and public-key encryption cryptosystem.

**AMS subject classifications:** Primary 11F85; Secondary 94A60

**Key words:** Local field, orthogonal basis,  $p$ -adic lattice.

---

## 1 Introduction

Since Shor [13] proved that the classical public-key cryptosystems such as RSA and ElGamal would be broken by future quantum computer, researchers have been dedicated to finding cryptographic primitives which are quantum-resistant. In 2022, NIST [11] announced four algorithms which passed the third round of post-quantum cryptography standardization solicitation and began the fourth

---

\*Corresponding author. *Email addresses:* zhangchi171@mailsucas.ac.cn (C. Zhang), dengyp@amss.ac.cn (Y. Deng)

round. They are CRYSTALS-Kyber [2], CRYSTALS-Dilithium [6], Falcon [8] and SPHINCS<sup>+</sup> [1]. Three of them are lattice-based and one of them is hash-based. The lack of diversity among post-quantum assumptions is widely recognized as a big, open issue in the field. Therefore, finding new post-quantum assumptions is of vital significance.

The  $p$ -adic numbers  $\mathbb{Q}_p$  were invented by Hensel in the late 19th century. The concept of a local field is an abstraction of the field  $\mathbb{Q}_p$ . Local fields provide a natural tool to solve many number-theoretic problems. They are ubiquitous in modern algebraic number theory and arithmetic geometry. Lattices can also be defined in local fields such as  $p$ -adic fields, see [15]. Interestingly,  $p$ -adic lattices possess some properties which lattices in Euclidean spaces do not have, see [17]. However, applications of  $p$ -adic lattices in cryptography were developed only recently.

In 2021, by introducing a trapdoor function with an orthogonal basis of a  $p$ -adic lattice, Deng *et al.* [5] constructed the first signature scheme and public-key encryption cryptosystem based on  $p$ -adic lattices. As the  $p$ -adic analogues of the lattices in Euclidean spaces, it is reasonable to expect hard problems in  $p$ -adic lattices to be quantum-resistant, which might provide new alternative candidates to construct post-quantum cryptographic primitives.

The experimental results [5] demonstrated that the new schemes achieve good efficiency. As for security, Zhang [16] found that these schemes are not secure because the extension fields used in these schemes are totally ramified. In order to avoid this attack, he suggested that the extension field should have a large residue degree.

In a totally ramified extension field  $K/\mathbb{Q}_p$ , a uniformizer  $\pi$  generates an orthogonal basis of  $K$ . But in a general extension field  $K/\mathbb{Q}_p$ , we can not find an orthogonal basis of  $K$  as easily as in a totally ramified extension field. Therefore, the crucial point of such a scheme is to construct an orthogonal basis of  $K$ .

Given an extension field  $K$  over  $\mathbb{Q}_p$  of degree  $n$ , we can use the Round 2 Algorithm [4] or the Round 4 Algorithm [7] to obtain a basis of the maximal order  $\mathcal{O}_K$  and then compute its orthogonal basis. However, these algorithms involve computation of large matrices. They require storage of the order of  $n^3$  in the worst case.

In order to reduce the storage requirement, we consider the problem from another perspective. Instead of trying computing the maximal order, we construct an orthogonal basis directly and then compute the extension field it generates. The storage requirement of this method is of the order of  $n^2$  in the worst case.

This paper is organized as follows. In Section 2, we recall some basic definitions. In Section 3, we give an equivalent condition for orthogonal basis in the

extension field of  $\mathbb{Q}_p$ . Then, we construct a kind of specific orthogonal basis in Section 4 and realize it with roots of unity in Section 5.

## 2 Preliminaries

In this section, we recall some basic facts about local fields and  $p$ -adic lattices. More details about local fields can be found in [3, 12].

### 2.1 Norm and orthogonal basis

Let  $p$  be a prime. Let  $V$  be a vector space over  $\mathbb{Q}_p$ . A norm  $\|\cdot\|$  on  $V$  is a function

$$\|\cdot\|: V \rightarrow \mathbb{R}$$

such that:

1.  $\|v\| \geq 0$  for any  $v \in V$ , and  $\|v\| = 0$  if and only if  $v = 0$ .
2.  $\|xv\| = |x|_p \cdot \|v\|$  for any  $x \in \mathbb{Q}_p$  and  $v \in V$ .
3.  $\|v+w\| \leq \max\{\|v\|, \|w\|\}$  for any  $v, w \in V$ .

Here,  $|x|_p$  is the  $p$ -adic absolute value for a  $p$ -adic number  $x \in \mathbb{Q}_p$ .

If  $\|\cdot\|$  is a norm on  $V$ , and if  $\|v\| \neq \|w\|$  for  $v, w \in V$ , then one can prove  $\|v+w\| = \max\{\|v\|, \|w\|\}$ . Weil [15, p. 26] proved the following proposition.

**Proposition 2.1** ([15]). *Let  $V$  be a vector space over  $\mathbb{Q}_p$  of finite dimension  $n > 0$ , and let  $\|\cdot\|$  be a norm on  $V$ . Then there is a decomposition  $V = V_1 + V_2 + \cdots + V_n$  of  $V$  into a direct sum of subspaces  $V_i$  of dimension 1 such that*

$$\left\| \sum_{i=1}^n v_i \right\| = \max_{1 \leq i \leq n} \|v_i\|$$

for any  $v_i \in V_i, i = 1, 2, \dots, n$ .

Thus, we can define the orthogonal basis.

**Definition 2.1** (Orthogonal Basis). *Let  $V$  be a vector space over  $\mathbb{Q}_p$  of finite dimension  $n > 0$ , and let  $\|\cdot\|$  be a norm on  $V$ . We call  $\alpha_1, \alpha_2, \dots, \alpha_n$  an orthogonal basis of  $V$  over  $\mathbb{Q}_p$  if  $V$  can be decomposed into the direct sum of  $n$  one-dimensional subspaces  $V_i$  ( $1 \leq i \leq n$ ) such that*

$$\left\| \sum_{i=1}^n v_i \right\| = \max_{1 \leq i \leq n} \|v_i\|$$

for any  $v_i \in V_i$ ,  $i=1,2,\dots,n$ , where  $V_i$  is spanned by  $\alpha_i$ . Two subspaces  $U, W$  of  $V$  are said to be orthogonal if the sum  $U+W$  is a direct sum and

$$\|\mathbf{u} + \mathbf{w}\| = \max\{\|\mathbf{u}\|, \|\mathbf{w}\|\}$$

for all  $\mathbf{u} \in U$ ,  $\mathbf{w} \in W$ . Actually, the former assumption can be deduced from the latter assumption.

## 2.2 Residue degree and ramification index

Let  $K$  be a finite extension of degree  $n$  over the field  $\mathbb{Q}_p$  of  $p$ -adic numbers. Hence,  $K$  is locally compact and complete. Let us choose an element  $\pi$  of maximal absolute value smaller than 1 and call it a uniformizer. Let

$$R = \{x \in K \mid |x| \leq 1\}$$

and its maximal ideal  $P = \pi R$ , where  $|\cdot|$  denotes the unique extension of the  $p$ -adic absolute value to the field  $K$ , see [12, p. 94]. If we consider  $K$  as a finite-dimensional vector space over  $\mathbb{Q}_p$ , then the extended absolute value is also a norm on this vector space. For this absolute-value norm, the second property of norm holds not only for  $x \in \mathbb{Q}_p$ , but also for  $x \in K$ . The residue field  $k = R/P$  is finite, hence a finite extension over  $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ .

**Definition 2.2** (Residue Degree and Ramification Index). *The residue degree of the finite extension  $K$  over  $\mathbb{Q}_p$  is the integer*

$$f = [k : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(k).$$

*The ramification index of  $K$  over  $\mathbb{Q}_p$  is the integer*

$$e = [ |K^*| : |Q_p^*| ] = [ |K^*| : |p^{\mathbb{Z}}| ] = \#( |K^*| / |p^{\mathbb{Z}}| ),$$

where  $|K^*|$  denotes the value group of  $K^*$ .

Similar to the finite extension field over the rational number field  $\mathbb{Q}$ , we have the following theorem.

**Theorem 2.1** ([12, p. 99]). *For each finite extension  $K$  over  $\mathbb{Q}_p$ , we have*

$$ef = [K : \mathbb{Q}_p] = n.$$

### 2.3 Lattice in $p$ -adic fields

As in the previous subsection, let  $p$  be a prime number, and let  $K$  be an extension field of  $\mathbb{Q}_p$  of degree  $n$ . Let  $m$  be a positive integer with  $1 \leq m \leq n$ . Let  $\alpha_1, \alpha_2, \dots, \alpha_m \in K$  be  $m$   $\mathbb{Q}_p$ -linearly independent vectors. A lattice in  $K$  is the set

$$\mathcal{L}(\alpha_1, \alpha_2, \dots, \alpha_m) = \left\{ \sum_{i=1}^m a_i \alpha_i \mid a_i \in \mathbb{Z}_p, 1 \leq i \leq m \right\}$$

of all  $\mathbb{Z}_p$ -linear combinations of  $\alpha_1, \alpha_2, \dots, \alpha_m$ . The sequence of vectors  $\alpha_1, \alpha_2, \dots, \alpha_m$  is called a basis of the lattice  $\mathcal{L}(\alpha_1, \alpha_2, \dots, \alpha_m)$ . The integer  $m$  is called the rank of the lattice, respectively. When  $n = m$ , we say that the lattice is of full rank.

## 3 An equivalent condition for orthogonal basis

In this section, we give an equivalent condition for orthogonal basis in the extension field of  $\mathbb{Q}_p$ . We begin with some simple lemmas.

**Lemma 3.1.** *Let  $V$  be a vector space over  $\mathbb{Q}_p$  of finite dimension  $n > 0$ . Let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be a basis of  $V$  over  $\mathbb{Q}_p$ . Then  $\alpha_1, \alpha_2, \dots, \alpha_n$  is an orthogonal basis of  $V$  over  $\mathbb{Q}_p$  if and only if*

$$\left\| \sum_{i=1}^n a_i \alpha_i \right\| = \max_{1 \leq i \leq n} \|a_i \alpha_i\|$$

for all  $a_i \in \mathbb{Z}_p$ ,  $1 \leq i \leq n$ , where at least one  $a_i \in \mathbb{Z}_p - p\mathbb{Z}_p$ .

*Proof.* Necessity follows immediately from the definition of the orthogonal basis. Now we prove the sufficiency. If there is any  $a_i = 0$ , we can just ignore it. So we may assume that  $a_i \in \mathbb{Q}_p$  and  $a_i \neq 0$ ,  $1 \leq i \leq n$ . For  $x \in \mathbb{Q}_p$  and  $x \neq 0$ , write  $x = p^t u$  with a unit  $u \in \mathbb{Z}_p^*$ , we define  $\text{ord}(x) = t$ . Let  $s = \min_{1 \leq i \leq n} \{\text{ord}(a_i)\}$  so that  $p^{-s} a_i \in \mathbb{Z}_p$  for all  $1 \leq i \leq n$  and at least one  $a_i \in \mathbb{Z}_p - p\mathbb{Z}_p$ . Then,

$$|p^{-s}|_p \cdot \left\| \sum_{i=1}^n a_i \alpha_i \right\| = \left\| \sum_{i=1}^n p^{-s} a_i \alpha_i \right\| = \max_{1 \leq i \leq n} \|p^{-s} a_i \alpha_i\| = |p^{-s}|_p \cdot \max_{1 \leq i \leq n} \|a_i \alpha_i\|.$$

Therefore,

$$\left\| \sum_{i=1}^n a_i \alpha_i \right\| = \max_{1 \leq i \leq n} \|a_i \alpha_i\|$$

for all  $a_i \in \mathbb{Q}_p$ ,  $1 \leq i \leq n$ . Hence,  $\alpha_1, \alpha_2, \dots, \alpha_n$  is an orthogonal basis of  $V$  over  $\mathbb{Q}_p$ .  $\square$

**Lemma 3.2.** *Let  $V$  be a vector space over  $\mathbb{Q}_p$  of finite dimension  $n > 0$ . Let  $\alpha_1, \alpha_2, \dots, \alpha_n$  be a basis of  $V$  over  $\mathbb{Q}_p$  such that  $\|\alpha_1\| = \|\alpha_2\| = \dots = \|\alpha_n\|$ . Let  $\lambda_1 = \|\alpha_1\|$ . Then  $\alpha_1, \alpha_2, \dots, \alpha_n$  is an orthogonal basis of  $V$  over  $\mathbb{Q}_p$  if and only if for all  $a_1, a_2, \dots, a_n \in \mathbb{Z}_p$  such that*

$$\left\| \sum_{i=1}^n a_i \alpha_i \right\| < \lambda_1,$$

*we have  $p|a_i$  for  $1 \leq i \leq n$ .*

*Proof.* Assume  $\alpha_1, \alpha_2, \dots, \alpha_n$  is an orthogonal basis of  $V$  over  $\mathbb{Q}_p$ . Then

$$\left\| \sum_{i=1}^n a_i \alpha_i \right\| = \max_{1 \leq i \leq n} \|a_i \alpha_i\| = \lambda_1 \cdot \max_{1 \leq i \leq n} \|a_i\|.$$

Therefore,  $\|\sum_{i=1}^n a_i \alpha_i\| < \lambda_1$  implies that  $\max_{1 \leq i \leq n} |a_i|_p < 1$ . Hence,  $p|a_i$  for all  $1 \leq i \leq n$ .

Conversely, if  $\alpha_1, \alpha_2, \dots, \alpha_n$  is not an orthogonal basis of  $V$  over  $\mathbb{Q}_p$ , then by Lemma 3.1, there exists  $a_i \in \mathbb{Z}_p$ ,  $1 \leq i \leq n$ , and at least one  $a_i \in \mathbb{Z}_p - p\mathbb{Z}_p$  such that

$$\left\| \sum_{i=1}^n a_i \alpha_i \right\| < \max_{1 \leq i \leq n} \|a_i \alpha_i\| = \lambda_1,$$

which contradicts the assumption of sufficiency in this lemma.  $\square$

Then we can prove our main theorem of this section. From now on, we use  $|\cdot|$  to denote the  $p$ -adic absolute value on an extension field  $K$  over  $\mathbb{Q}_p$  for simplicity. The following theorem is a well-known result, see [14, p. 167, Exercise 5A], showing the relation between orthogonality and linear independence. For the sake of completeness, we provide a proof here.

**Theorem 3.1.** *Let  $K$  be an extension field of degree  $n$  over  $\mathbb{Q}_p$ . Let  $V$  be a subspace of  $K$  over  $\mathbb{Q}_p$ . Assume that  $\alpha_1, \alpha_2, \dots, \alpha_m$  ( $m \leq n$ ) is a basis of  $V$  over  $\mathbb{Q}_p$  and  $|\alpha_1| = |\alpha_2| = \dots = |\alpha_m|$ . Let  $\lambda_1 = |\alpha_1|$ . Let  $\pi$  be a uniformizer of  $K$ , so there is an integer  $s$  such that  $|\pi^s| = \lambda_1$ . Then  $\alpha_1, \alpha_2, \dots, \alpha_m$  is an orthogonal basis of  $V$  over  $\mathbb{Q}_p$  if and only if  $\overline{\alpha_1}, \overline{\alpha_2}, \dots, \overline{\alpha_m}$  are linearly independent over  $\mathbb{F}_p$ , where  $\overline{\alpha_i}$  is the image of  $\pi^{-s} \cdot \alpha_i$  in  $k = R/P$ .*

*Proof.* By Lemma 3.2,  $\alpha_1, \alpha_2, \dots, \alpha_m$  is an orthogonal basis of  $V$  over  $\mathbb{Q}_p$  if and only if

$$\left| \sum_{i=1}^m a_i \alpha_i \right| < \lambda_1, \quad a_i \in \mathbb{Z}_p \Rightarrow p|a_i \quad \text{for all } 1 \leq i \leq m.$$

Recall that  $|ab| = |a||b|$  for  $a, b \in K$ . The above statement is equivalent to

$$\left| \sum_{i=1}^m a_i \pi^{-s} \alpha_i \right| < 1, \quad a_i \in \mathbb{Z}_p \Rightarrow p|a_i| \quad \text{for all } 1 \leq i \leq m.$$

And this is equivalent to

$$\sum_{i=1}^m \overline{a_i \alpha_i} = \overline{0}, \quad a_i \in \mathbb{Z}_p \Rightarrow \overline{a_i} = \overline{0} \quad \text{for all } 1 \leq i \leq m,$$

which is the definition of linear independence of  $\overline{\alpha_1}, \overline{\alpha_2}, \dots, \overline{\alpha_m}$  over  $\mathbb{F}_p$ . □

**Remark 3.1.** In general, it is not efficient to determine orthogonal basis by this theorem. However, in some special cases, it will be useful. For example, in a totally ramified extension field, since  $k = \mathbb{F}_p$ , any two vectors  $\alpha_1$  and  $\alpha_2$  such that  $|\alpha_1| = |\alpha_2|$  can not be extended to an orthogonal basis of  $V$  over  $\mathbb{Q}_p$ .

## 4 Construction of specific orthogonal basis

In this section, we use Theorem 3.1 to construct a kind of specific orthogonal basis.

**Lemma 4.1.** *Let  $K = \mathbb{Q}_p(\theta)$  be an extension field of degree  $n$  over  $\mathbb{Q}_p$  with  $|\theta| = 1$ . Let  $F$  be the minimal polynomial of  $\theta$  over  $\mathbb{Q}_p$ . Assume that  $F$  is reducible modulo  $p$ . Then  $1, \theta, \theta^2, \dots, \theta^{n-1}$  is not an orthogonal basis of  $K$  over  $\mathbb{Q}_p$ .*

*Proof.* Let  $F \equiv gh \pmod{p}$  where  $g$  and  $h$  have coefficients in  $\mathbb{F}_p$ . Since  $g(\theta)h(\theta) \in pR \subset P$ , at least one of  $g(\theta)$  and  $h(\theta)$  is in  $P$ . We may assume that  $g(\theta) \in P$ . Then  $\overline{g(\theta)} = \overline{0}$ . Since  $\deg(g) \leq n-1$ ,  $\overline{1}, \overline{\theta}, \overline{\theta^2}, \dots, \overline{\theta^{n-1}}$  are linearly dependent over  $\mathbb{F}_p$ . By Theorem 3.1,  $1, \theta, \theta^2, \dots, \theta^{n-1}$  is not an orthogonal basis of  $K$  over  $\mathbb{Q}_p$ . □

**Example 4.1.** Let  $\theta$  be a primitive  $p^l$ -th root of unity. Then  $K = \mathbb{Q}_p(\theta)$  is a totally ramified extension field of degree  $n = \varphi(p^l) = p^{l-1}(p-1)$ . Since  $X^{p^l} - 1 \equiv (X-1)^{p^l} \pmod{p}$  and the minimal polynomial of  $\theta$  is a factor of  $X^{p^l} - 1$ , by Lemma 4.1,  $1, \theta, \theta^2, \dots, \theta^{n-1}$  is not an orthogonal basis of  $K$  over  $\mathbb{Q}_p$ . Moreover, we can deduce from the proof of Lemma 4.1 that  $|\theta - 1| < 1$ . In fact,  $|\theta - 1| = |p|^{1/\varphi(p^l)}$ .

The converse proposition is also true in an unramified extension field, so we have the following theorem.

**Theorem 4.1.** *Let  $K = \mathbb{Q}_p(\theta)$  be an unramified extension field of degree  $n$  over  $\mathbb{Q}_p$  with  $|\theta| = 1$ . Let  $F$  be the minimal polynomial of  $\theta$  over  $\mathbb{Q}_p$ . Then  $1, \theta, \theta^2, \dots, \theta^{n-1}$  is an orthogonal basis of  $K$  over  $\mathbb{Q}_p$  if and only if  $F$  is irreducible modulo  $p$ .*

*Proof.* Since  $1, \theta, \theta^2, \dots, \theta^{n-1}$  is a basis of  $K$  over  $\mathbb{Q}_p$ , by Theorem 3.1,  $1, \theta, \theta^2, \dots, \theta^{n-1}$  is not an orthogonal basis of  $K$  over  $\mathbb{Q}_p$  if and only if  $\overline{1}, \overline{\theta}, \overline{\theta^2}, \dots, \overline{\theta^{n-1}}$  are linearly dependent over  $\mathbb{F}_p$ . So there is a polynomial

$$g(X) = \sum_{i=0}^{n-1} a_i X^i$$

with coefficients  $a_i \in \mathbb{Z}_p$  for  $0 \leq i \leq n-1$  such that  $\overline{g(X)} \neq \overline{0}$  and  $\overline{g(\theta)} = \overline{0}$ . Let  $G$  be the minimal polynomial of  $\overline{\theta}$  over  $\mathbb{F}_p$ . Then,

$$\deg(G) \leq \deg(g) \leq n-1 < \deg(F).$$

Since  $\overline{F(\theta)} = \overline{0}$ , we have  $F \equiv G \cdot (F/G) \pmod{\pi}$ . Since  $K$  is unramified, the uniformizer  $\pi$  is  $p$  multiplied by some unit in  $K$ , so we have  $F \equiv G \cdot (F/G) \pmod{p}$  is reducible modulo  $p$ .  $\square$

**Remark 4.1.** We can see from the proof of Theorem 4.1 that if we want to drop the unramifiedness assumption in this theorem, then the modulus will be  $\pi$  instead of  $p$ . However, finding a uniformizer requires additional computation. Hence, we do not use this stronger result.

**Corollary 4.1.** *Let  $K = \mathbb{Q}_p(\theta)$  be an unramified extension field of degree  $n$  over  $\mathbb{Q}_p$  with  $|\theta| = 1$ . Let  $G$  be the minimal polynomial of  $\overline{\theta}$  over  $\mathbb{F}_p$ . If  $\deg(G) = m$ , then  $1, \theta, \theta^2, \dots, \theta^{m-1}$  is an orthogonal basis of  $V$  over  $\mathbb{Q}_p$ , where  $V$  is the vector space generated by  $1, \theta, \theta^2, \dots, \theta^{m-1}$  over  $\mathbb{Q}_p$ .*

*Proof.* Similar to Theorem 4.1.  $\square$

We now begin to construct an orthogonal basis for a ramified extension field. The following lemma is an obvious corollary of [5, Proposition 3.3]. It can be concluded by induction.

**Lemma 4.2.** *Let  $K$  be an extension field of over  $\mathbb{Q}_p$ . Let  $V_i \subset K$  be a vector space over  $\mathbb{Q}_p$  of finite dimension  $n_i > 0$ ,  $1 \leq i \leq s$ . Let  $\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in_i}$  be an orthogonal basis of  $V_i$  over  $\mathbb{Q}_p$ . If*

$$\{ |v_i| \mid v_i \in V_i \} \cap \{ |v_j| \mid v_j \in V_j \} = \{0\}$$

*for all  $1 \leq i < j \leq s$ . Then  $\alpha_{11}, \alpha_{12}, \dots, \alpha_{1n_1}, \dots, \alpha_{s1}, \alpha_{s2}, \dots, \alpha_{sn_s}$  is an orthogonal basis of  $V = \bigoplus_{i=1}^s V_i$  over  $\mathbb{Q}_p$ .*



**Theorem 4.2.** *Let  $K$  be an extension field of degree  $n$  over  $\mathbb{Q}_p$ . Let  $f$  and  $e$  be the residue degree and ramification index respectively. Let  $\pi$  be a uniformizer of  $K$  and  $(s_i)_{1 \leq i \leq f}$  be a family in  $R$  such that the image  $\bar{s}_i \in k$  make up a basis of  $k$  over  $\mathbb{F}_p$ . Then the family  $(s_i \pi^j)_{1 \leq i \leq f, 0 \leq j \leq e-1}$  is an orthogonal basis of  $K$  over  $\mathbb{Q}_p$ .*

*Proof.* By Theorem 2.1,  $n = ef$ . We can prove that the elements in this family are linearly independent over  $\mathbb{Q}_p$ , see [12, p. 99], so it is a basis of  $K$  over  $\mathbb{Q}_p$ . Let  $V_j$  be the vector space generated by  $(s_i \pi^j)_{1 \leq i \leq f}$  over  $\mathbb{Q}_p$ ,  $0 \leq j \leq e-1$ . Then  $K = \bigoplus_{j=0}^{e-1} V_j$ . Since  $(\bar{s}_i)_{1 \leq i \leq f}$  are linearly independent over  $\mathbb{F}_p$ , by Theorem 3.1,  $(s_i \pi^j)_{1 \leq i \leq f}$  is an orthogonal basis of  $V_j$  over  $\mathbb{Q}_p$ . Since  $|\pi| = p^{-1/e}$ , we have

$$\{ |v_j| \mid v_j \in V_j \} = \{0\} \cup p^{\mathbb{Z} - j/e}.$$

Then by Lemma 4.2, the family  $(s_i \pi^j)_{1 \leq i \leq f, 0 \leq j \leq e-1}$  is an orthogonal basis of  $K$  over  $\mathbb{Q}_p$ . □

**Example 4.2.** Let  $K = \mathbb{Q}_3(\sqrt{3} + i) = \mathbb{Q}_3(\sqrt{3}, i)$  where  $i^2 = -1$ . Then  $K$  is an extension field of degree  $n = 4$  over  $\mathbb{Q}_3$ . Its residue degree is  $f = 2$  and ramification index is  $e = 2$ . Since  $\sqrt{3}$  is a uniformizer of  $K$  and  $1, i$  are linearly independent over  $\mathbb{F}_3$ ,  $\{1, i, \sqrt{3}, \sqrt{3}i\}$  is an orthogonal basis of  $K$  over  $\mathbb{Q}_3$ .

**Lemma 4.3.** *Let  $K_1 = \mathbb{Q}_p(\theta)$  be an unramified extension field of degree  $f$  over  $\mathbb{Q}_p$  and  $K_2 = \mathbb{Q}_p(\pi)$  be a totally ramified extension field of degree  $e$  over  $\mathbb{Q}_p$ . Then  $K = \mathbb{Q}_p(\theta, \pi)$  is an extension field of degree  $n = ef$  over  $\mathbb{Q}_p$ . Its residue degree is  $f$  and ramification index is  $e$ .*

*Proof.* Since its residue degree is at least  $f$  and ramification index is at least  $e$  and  $[K : \mathbb{Q}_p] \leq ef$ , we have  $[K : \mathbb{Q}_p] = ef$ . Hence, its residue degree is  $f$  and ramification index is  $e$ . □

Finally, we can present our crucial result for constructing orthogonal basis.

**Theorem 4.3.** *Let  $K_1 = \mathbb{Q}_p(\theta)$  be an unramified extension field of degree  $f$  over  $\mathbb{Q}_p$  with  $|\theta| = 1$ . Let  $F$  be the minimal polynomial of  $\theta$  over  $\mathbb{Q}_p$ . Let  $K_2 = \mathbb{Q}_p(\pi)$  be a totally ramified extension field of degree  $e$  over  $\mathbb{Q}_p$ . Assume that  $F$  is irreducible modulo  $p$  and  $\pi$  is a uniformizer of  $K_2$ . Then the family  $(\theta^i \pi^j)_{0 \leq i \leq f-1, 0 \leq j \leq e-1}$  is an orthogonal basis of  $K = \mathbb{Q}_p(\theta, \pi)$  over  $\mathbb{Q}_p$ .*

*Proof.* By Lemma 4.3,  $K$  is an extension field of degree  $n = ef$  over  $\mathbb{Q}_p$ . Its residue degree is  $f$  and ramification index is  $e$ . By Theorem 4.1,  $1, \theta, \theta^2, \dots, \theta^{f-1}$  is an orthogonal basis of  $K_1$  over  $\mathbb{Q}_p$ . Then by Theorem 3.1, their image in  $k$  are linearly

independent over  $\mathbb{F}_p$  and therefore make up a basis of  $k$  over  $\mathbb{F}_p$ . Finally, by Theorem 4.2, the family  $(\theta^i \pi^j)_{0 \leq i \leq f-1, 0 \leq j \leq e-1}$  is an orthogonal basis of  $K = \mathbb{Q}_p(\theta, \pi)$  over  $\mathbb{Q}_p$ .  $\square$

## 5 Constructing orthogonal basis with roots of unity

Notice that roots of unity are helpful for us to construct an extension field which satisfies the assumption in Theorem 4.1.

**Theorem 5.1.** *Let  $K = \mathbb{Q}_p(\theta)$  be an extension field of degree  $n$  over  $\mathbb{Q}_p$  and  $\theta$  is a root of unity of order prime to  $p$ . Then  $1, \theta, \theta^2, \dots, \theta^{n-1}$  is an orthogonal basis of  $K$  over  $\mathbb{Q}_p$ .*

*Proof.* Since a root of unity of order prime to  $p$  generates over  $\mathbb{Q}_p$  an unramified extension field, see [12, p. 105], and the minimal polynomial of  $\theta$  over  $\mathbb{Q}_p$  is irreducible modulo  $p$ , the theorem is immediately from Theorem 4.1.  $\square$

**Example 5.1.** Let  $K = \mathbb{Q}_3(i)$  where  $i^2 = -1$ . Since  $X^2 + 1$  is irreducible modulo 3,  $\{1, i\}$  is an orthogonal basis of  $K$  over  $\mathbb{Q}_3$ .

In order to determine whether  $F$  is irreducible modulo  $p$ , we need some results about cyclotomic cosets to factor  $X^n - 1$  modulo  $p$  ( $\gcd(n, p) = 1$ ).

**Definition 5.1** (Cyclotomic Coset). *Suppose  $p$  is a prime number and  $\gcd(n, p) = 1$ . For integer  $s \in \{0, 1, \dots, p-1\}$ , the cyclotomic coset mod  $n$  over  $\mathbb{F}_p$  which contains integer  $s$  is defined as*

$$C_s = \{s, sp, sp^2, \dots, sp^{m_s-1}\},$$

where  $sp^{m_s} \equiv s \pmod{n}$ , i.e.,  $m_s$  is the least positive integer satisfying  $sp^{m_s} \equiv s \pmod{n}$ .

The following lemma is a well known result of cyclotomic polynomial. We omit the proof here.

**Lemma 5.1** ([10]). *Let  $p$  be a prime number. Let  $\alpha$  be a primitive  $n$ -th root of unity over  $\mathbb{F}_p$ . Let  $s \in \{0, 1, \dots, p-1\}$ . Then*

$$M^{(s)}(X) = \prod_{i \in C_s} (X - \alpha^i) \in \mathbb{F}_p[X]$$

is the minimal polynomial of  $\alpha^s$  over  $\mathbb{F}_p$ . Moreover,

$$X^n - 1 = \prod_s M^{(s)}(X),$$

where  $s$  runs over a set of cyclotomic coset representatives modulo  $n$ , gives the factorization of  $X^n - 1$  over  $\mathbb{F}_p$ .

**Lemma 5.2.** *Let  $q$  be a prime number such that  $q_0 = (q-1)/2$  is also prime i.e.,  $q_0$  is a Sophie Germain prime. Let  $p$  be an integer such that  $p \not\equiv -1 \pmod{q}$ . Then  $p$  is a primitive root modulo  $q$  if and only if  $p$  is not a quadratic residue modulo  $q$ .*

*Proof.*  $p$  is not a quadratic residue modulo  $q$  if and only if  $p^{(q-1)/2} \equiv -1 \pmod{q}$ . Since  $p \not\equiv -1 \pmod{q}$ , this is equivalent to  $p$  is a primitive root modulo  $q$ .  $\square$

Now we choose  $q$ ,  $q_0$  and  $p$  as in Lemma 5.2. Assume  $p$  is not a quadratic residue modulo  $q$  so the order of  $p$  modulo  $q$  is  $q-1$ . Take  $K_1 = \mathbb{Q}_p(\theta)$  where  $\theta$  is a primitive  $q$ -th root of unity. By Lemma 5.1, the degree of the minimal polynomial of  $\theta$  over  $\mathbb{F}_p$  is  $q-1$ , hence it is also  $q-1$  over  $\mathbb{Q}_p$ . Let  $K_2 = \mathbb{Q}_p(\pi)$  be a totally ramified extension field of degree  $e$  over  $\mathbb{Q}_p$ . Then by Theorem 4.3, the family

$$(\theta^i \pi^j)_{0 \leq i \leq q-2, 0 \leq j \leq e-1}$$

is an orthogonal basis of  $K = \mathbb{Q}_p(\theta, \pi)$  over  $\mathbb{Q}_p$ .

To make this orthogonal basis practical, we also need to find a primitive element of  $K = \mathbb{Q}_p(\theta, \pi)$ . It is well known that a finite separable extension is a simple extension, which is known as the primitive element theorem. If we consider this theorem in a field of characteristic 0, then we only need the finiteness in the assumption. Moreover, there is a constructive proof of this theorem, see [9, p. 410]. We summarize the proof as the following lemma.

**Lemma 5.3.** *Let  $K = \mathbb{Q}_p(\theta, \pi)$  be a finite extension field over  $\mathbb{Q}_p$ . Let  $f(X)$  and  $g(X)$  be the minimal polynomial of  $\theta$  and  $\pi$  over  $\mathbb{Q}_p$  respectively. Suppose their roots are  $\theta^{(1)}, \theta^{(2)}, \dots, \theta^{(n)}$  and  $\pi^{(1)}, \pi^{(2)}, \dots, \pi^{(m)}$  respectively. Choose  $h \in \mathbb{Q}_p$  such that*

$$h \neq \frac{\pi^{(u)} - \pi^{(v)}}{\theta^{(s)} - \theta^{(t)}}, \quad 1 \leq s, t \leq n, \quad 1 \leq u, v \leq m.$$

Then  $\zeta = h\theta + \pi$  is a primitive element of  $K$  over  $\mathbb{Q}_p$ , i.e.,  $K = \mathbb{Q}_p(\zeta)$ .

**Lemma 5.4** ([12, p. 105]). *Let  $K$  be any ultrametric extension of  $\mathbb{Q}_p$ . Then the distance between two distinct roots of unity of order prime to  $p$  is 1.*

**Lemma 5.5.** *Let  $q \neq p$  be a prime number and  $\theta$  be a primitive  $q$ -th root of unity whose degree over  $\mathbb{Q}_p$  is  $f = q-1$ . Let  $G$  be an Eisenstein polynomial and  $\pi$  be a root of  $G(X) = 0$ . Let  $K = \mathbb{Q}_p(\theta, \pi)$  and  $\zeta = \theta + \pi$ . Then  $K = \mathbb{Q}_p(\zeta)$ .*

*Proof.* Let  $\pi^{(1)}, \pi^{(2)}, \dots, \pi^{(e)}$  and  $\theta^{(1)}, \theta^{(2)}, \dots, \theta^{(f)}$  be the conjugate elements of  $\pi$  and  $\theta$  over  $\mathbb{Q}_p$  respectively, where  $e = \deg(F)$ . We have  $|\pi^{(u)}| < 1$ . On the other hand, by Lemma 5.4,

$$|\theta^{(s)} - \theta^{(t)}| = 1, \quad 1 \leq s < t \leq f.$$

Since

$$\left| \frac{\pi^{(u)} - \pi^{(v)}}{\theta^{(s)} - \theta^{(t)}} \right| = |\pi^{(u)} - \pi^{(v)}| < 1,$$

we can take  $h = 1$  in Lemma 5.3. Therefore,  $K = \mathbb{Q}_p(\theta + \pi) = \mathbb{Q}_p(\zeta)$ .  $\square$

Finally, let  $H$  be the minimal polynomial of  $\theta$  over  $\mathbb{Q}_p$ . We can use resultant to obtain the minimal polynomial of  $\zeta = \theta + \pi$ , i.e.,

$$F(X) = \text{Res}_Y(G(Y), H(X - Y)).$$

We summarize the construction process as the following algorithm.

---

**Algorithm 1** Constructing Orthogonal Basis with Roots of Unit

---

**Input:** Two prime numbers  $q$  and  $q_0$  such that  $q = 2q_0 + 1$ , a prime number  $p$  such that  $p \not\equiv -1 \pmod{q}$  and  $p$  is not a quadratic residue modulo  $q$  and a positive integer  $e$ .

**Output:** An extension field  $K$  over  $\mathbb{Q}_p$  of degree  $n = (q - 1)e$  and an orthogonal basis of  $K$ .

- 1: Choose a random primitive  $q$ -th root of unity  $\theta$  and denote its minimal polynomial as  $H$ .
  - 2: Choose a random Eisenstein polynomial  $G$  of degree  $e$  and choose a random root  $\pi$  of  $G(X) = 0$ .
  - 3: Let  $\zeta = \theta + \pi$ , by Lemma 5.5,  $\zeta$  is a primitive element of  $\mathbb{Q}_p(\theta, \pi)$  over  $\mathbb{Q}_p$ .
  - 4: Let  $F(X) = \text{Res}_Y(G(Y), H(X - Y))$ .
  - 5: Return  $K = \mathbb{Q}_p(\zeta)$  (given by  $F$ ) and an orthogonal basis  $(\theta^i \pi^j)_{0 \leq i \leq q-2, 0 \leq j \leq e-1}$ , where  $\theta$  and  $\pi$  are given by  $H$  and  $G$  respectively.
- 

## 6 Conclusion

It is clear that the algorithm runs in polynomial time in  $n$ . The resultant in step 4 is an  $(e + q - 1) \times (e + q - 1)$  determinant. If we take  $e \approx q - 1 \approx \sqrt{n}$ , then the storage requirement is only  $\mathcal{O}(n)$  and the time complexity is  $\mathcal{O}(n^{1.5})$  if we use decomposition methods to compute the resultant. In the worst case, where  $\{e, q - 1\} = \{1, n\}$ , the storage requirement is  $\mathcal{O}(n^2)$  and the time complexity is  $\mathcal{O}(n^3)$ . Therefore, our method is better than the Round 2 Algorithm and the Round 4 Algorithm in storage requirement. Moreover, according to [7], the time complexity of the

Round 2 Algorithm is more than  $\mathcal{O}(n^4)$ . Our method is also better than the Round 2 Algorithm in time complexity.

The results in this paper are helpful to modify the  $p$ -adic signature scheme and public-key encryption cryptosystem. Simply using  $\zeta = \theta + \pi$  to generate the extension field  $K$  may be not secure. An adversary can guess the residue degree  $f$  and subtract a primitive  $f$ -th root of unit  $\theta'$  form  $\zeta$ . If it happens that  $\theta' = \theta$ , then the adversary will obtain the uniformizer  $\pi$  and break the scheme. Maybe we need to find a more complex primitive element  $\zeta$  while do not increase time complexity much. More efforts are needed to carry out secure schemes. The method of constructing orthogonal basis in  $p$ -adic fields may have other applications. It is worth for further study and there is much work to do.

## Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant No. 12271517).

## References

- [1] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, *The SPHINCS<sup>+</sup> signature framework*, in: Proceedings of 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS'19), ACM (2019), 2129–2146.
- [2] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehlé, *CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM*, in: Proceedings of 2018 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE Computer Society Press (2018), 353–367.
- [3] J. W. S. Cassels, *Local Fields*, Cambridge University Press, 1986.
- [4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 1993.
- [5] Y. Deng, L. Luo, Y. Pan, Z. Wang, and G. Xiao, *Public-key cryptosystems and signature schemes from  $p$ -adic lattices*, *P-Adic Numbers Ultrametric Anal. Appl.* 16(1) (2024), 23–42.
- [6] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, *CRYSTALS-Dilithium: Digital signatures from module lattices*, *Cryptology ePrint Archive*, Paper 2017/633. <https://eprint.iacr.org/2017/633>.
- [7] D. Ford, *On the Computation of the Maximal Order in a Dedekind Domain*, Ph.D Thesis, Ohio State University, 1978.
- [8] P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, *Falcon: Fast-Fourier Lattice-Based Compact*

*Signatures over NTRU*, Submission to the NIST's post-quantum cryptography standardization process, 2020.

- [9] L. K. Hua, *Collected Works of Loo-keng Hua: Number Theory II*, Science Press, 2010.
- [10] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 2008.
- [11] PQC Project, <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography>, 2024/10/11.
- [12] A. M. Robert, *A Course in  $p$ -adic Analysis*, Springer, 2000.
- [13] P. W. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, in: Proceedings of 35th Annual Symposium on Foundations of Computer Science, Los Alamitos: IEEE Computer Society Press (1994), 124–134.
- [14] A. C. M. van Rooij, *Non-Archimedean Functional Analysis*, Marcel Dekker, 1978.
- [15] A. Weil, *Basic Number Theory*, Springer, 1974.
- [16] C. Zhang, *An attack on  $p$ -adic lattice public-key cryptosystems and signature schemes*, Des. Codes Cryptogr. 93(7) (2025), 2695–2716.
- [17] C. Zhang, Y. Deng, and Z. Wang, *Norm orthogonal bases and invariants of  $p$ -adic lattices*, Linear Algebra Appl. 728 (2026), 186–210.