Surveys in Mathematics and its Applications

ISSN 1842-6298 (electronic), 1843-7265 (print)
Volume 21 (2026), 177 – 209

THE STRUCTURE OF THE n-TH ROOTS OF UNITY IN RESIDUE RINGS OF PRIME IDEALS P OVER p IN ALGEBRAIC NUMBER FIELDS

Boaz Cohen

Abstract. Let $\mathbb{K}$ be an algebraic number field and let $O_{\mathbb{K}}$ be its ring of integers. In this paper, we study the structure of incongruent solutions of $x^n \equiv 1 \pmod{P^a}$ in $O_{\mathbb{K}}$, where P is a prime ideal, in order to apply these results to solving $x^n = 1$ over the P-adic field $\mathbb{K}_P$.

1 Introduction

Given a prime number p and a positive integer n, the p-adic *n-th roots of unity* are the solutions of the equation

$$x^n = 1, \tag{1}$$

in the ring of integers $\mathbb{Z}_p$ of the p-adic field $\mathbb{Q}_p$. Equation (1) is extensively discussed in the literature and in a variety of different contexts (see [1, 10, 11]). One approach for solving (1) is to use congruences. Let

$$\theta_0 + \theta_1 p + \theta_2 p^2 + \dots$$

be the p-adic expansion of x, where the θ_i's belong to a complete residue system modulo p. Hence, in order to solve (1), it suffices to determine the coefficients θ_i. This may be done by considering the *n-th roots of unity modulo p^a*, namely the incongruent solutions in $\mathbb{Z}$, of the list of congruences

$$x^n \equiv 1 \pmod{p^a}, \quad a \geqslant 1.$$

To illustrate this process, we shall solve the equation $x^{p^b} = 1$ in $\mathbb{Z}_p$, where p is an odd prime and b is an arbitrary positive integer. For this purpose, let us consider the list of congruences $x^{p^b} \equiv 1 \pmod{p^a}$ in $\mathbb{Z}$. As we shall see later in this study, if $b < a$, then the incongruent solutions of the congruence $x^{p^b} \equiv 1 \pmod{p^a}$ are

$$x \equiv 1 + tp^{a-b} \pmod{p^a},$$

2020 Mathematics Subject Classification: 11-02; 11Y40; 11R04; 11K41; 11F85
Keywords: congruences; p-adic field; algebraic fields; roots of unity

where $t \in \{0, 1, \ldots, p^b - 1\}$ is arbitrary. Now, by taking $a \to \infty$, we obtain that $p^{a-b} \to 0$ in $\mathbb{Q}_p$, which, in turn, produces the unique solution $x = 1$ over $\mathbb{Z}_p$.

The concept of p-adic n-th roots of unity can be carried on into a wider medium: given an algebraic number field $\mathbb{K}$ and a prime ideal P, we shall be interested in the solutions of the equation $x^n = 1$ in the ring of integers $\mathcal{O}_P$ of the P-adic field $\mathbb{K}_P$. The field $\mathbb{K}_P$ is constructed similarly to the p-adic field $\mathbb{Q}_p$, using the completion process relative to a suitable valuation $|\cdot|_P$. It can be shown that the elements of $\mathcal{O}_P$ are sums of the form

$$\theta_0 + \theta_1\gamma + \theta_2\gamma^2 + \ldots,$$

where $\gamma \in P \setminus P^2$ is pre-chosen element and the θ_i's belong to a complete residue system modulo P. Similarly to the p-adic case, the equation $x^n = 1$ in $\mathcal{O}_P$ may be solved by considering the *n-th roots of unity modulo P^a*, namely the incongruent solutions in the ring of integers $O_{\mathbb{K}}$ of $\mathbb{K}$, of the list of congruences

$$x^n \equiv 1 \pmod{P^a}, \quad a \geqslant 1. \tag{2}$$

Finding the solutions of the congruences (2) requires great effort, since the structure of the solutions strongly depends upon the different configurations of a, n, and the ramification index e of the prime ideal P.

The goal of this paper is to study the structure of the incongruent solutions of (2) over $O_{\mathbb{K}}$ in order to apply these results to solving the equation $x^n = 1$ over the P-adic field $\mathbb{K}_P$. It is worth mentioning that our results for congruences are of independent interest and may also be used in further applications such as [6].

The following theorem from Section 8 is one of our main results, in which we describe the structure of the p^b-th roots of unity in $\mathbb{K}_P$.

Theorem (Theorem 19, Section 8)**.** *Let $\mathbb{K}$ be an algebraic number field and let P be a prime ideal lying above the rational prime p with ramification index e, that is $P^e \| (p)$. In addition, let $\mathfrak{M}$ be a complete residue system modulo P and let b be a positive integer.*

(a) *If $p - 1 \nmid e$, then the only P-adic p^b-th root of unity is $x = 1$.*

(b) *If $p - 1 \mid e$, then set*

$$\Gamma_r = \frac{e}{p^r(p-1)} \quad \text{and} \quad \Gamma_0 = \frac{e}{p-1},$$

where $r = \min\{c, b-1\}$ and c is the non-negative integer such that $p^c \| e$. Then the P-adic p^b-th roots of unity are

$$x = 1 + \beta_{\Gamma_r}\gamma^{\Gamma_r} + \ldots + \beta_{\Gamma_0}\gamma^{\Gamma_0} + \beta_{\Gamma_0+1}\gamma^{\Gamma_0+1} + \ldots$$

where $\gamma \in P \setminus P^2$ and the β's are in $\mathfrak{M}$ and satisfy the following conditions:

$$\begin{cases} (1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b} \equiv 1 \pmod{P^{eb+\Gamma_0}} \\ p^b\beta_{\Gamma_0}\gamma^{\Gamma_0}+\binom{p^b}{p}(\beta_{\Gamma_0}\gamma^{\Gamma_0})^p \equiv 1-(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b} \pmod{P^{eb+\Gamma_0+1}} \\ p^b\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1} \equiv 1-(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0}\gamma^{\Gamma_0})^{p^b} \pmod{P^{eb+\Gamma_0+2}} \\ p^b\beta_{\Gamma_0+2}\gamma^{\Gamma_0+2} \equiv 1-(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1})^{p^b} \pmod{P^{eb+\Gamma_0+3}} \\ \quad\vdots \end{cases}$$

if $\Gamma_r < \Gamma_0$, and

$$\begin{cases} \beta_{\Gamma_0} \equiv 0 \pmod{P} \quad \text{or} \quad (\gamma^{\Gamma_0}\beta_{\Gamma_0})^{p-1} \equiv -p \pmod{P^{e+1}} \\ p^b\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1} \equiv 1-(1+\beta_{\Gamma_0}\gamma^{\Gamma_0})^{p^b} \pmod{P^{eb+\Gamma_0+2}} \\ p^b\beta_{\Gamma_0+2}\gamma^{\Gamma_0+2} \equiv 1-(1+\beta_{\Gamma_0}\gamma^{\Gamma_0}+\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1})^{p^b} \pmod{P^{eb+\Gamma_0+3}} \\ p^b\beta_{\Gamma_0+3}\gamma^{\Gamma_0+3} \equiv 1-(1+\beta_{\Gamma_0}\gamma^{\Gamma_0}+\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1}+\beta_{\Gamma_0+2}\gamma^{\Gamma_0+2})^{p^b} \pmod{P^{eb+\Gamma_0+4}} \\ \quad\vdots \end{cases}$$

if $\Gamma_r = \Gamma_0$.

As an illustrative example, consider the equation $x^4 = 1$ in the P-adic field $\mathbb{K}_P$, where $\mathbb{K} = \mathbb{Q}(i)$ and $P = (1+i)$. Here, the ring of integers of $\mathbb{K}$ is the Gaussian ring $O_{\mathbb{K}} = \mathbb{Z}[i]$. Note that, since $1+i$ is irreducible in $\mathbb{Z}[i]$, P is a prime ideal. Furthermore, $P^2 = (2)$, so P lies above the prime $p = 2$ with ramification index $e = 2$. Hence, the norm of P is $\mathrm{N}P = 2$, so we may choose $\mathfrak{M} = \{0, 1\}$ as a complete residue system modulo P.

Since $p-1 \mid e$, $p \| e$ and $b = 2$, it follows that $c = 1$, so $r = 1$. Thus $\Gamma_1 = \frac{e}{p(p-1)} = 1$ and $\Gamma_0 = \frac{e}{p-1} = 2$, so $\Gamma_r < \Gamma_0$. Hence, by Theorem 19(b), the solutions of $x^4 = 1$ over $\mathbb{K}_P$ are of the form

$$x = 1 + \beta_1\gamma + \beta_2\gamma^2 + \beta_3\gamma^3 + \ldots,$$

where $\gamma = 1+i$, and $(\beta_1, \beta_2, \beta_3, \ldots)$ are taken from $\mathfrak{M} = \{0, 1\}$ and satisfy the following system of congruences

$$\begin{cases} (1+\beta_1\gamma)^4 \equiv 1 \pmod{P^6} \\ 4\beta_2\gamma^2+\binom{4}{2}(\beta_2\gamma^2)^2 \equiv 1-(1+\beta_1\gamma)^4 \pmod{P^7} \\ 4\beta_3\gamma^3 \equiv 1-(1+\beta_1\gamma+\beta_2\gamma^2)^4 \pmod{P^8} \\ 4\beta_4\gamma^4 \equiv 1-(1+\beta_1\gamma+\beta_2\gamma^2+\beta_3\gamma^3)^4 \pmod{P^9} \\ \quad\vdots \end{cases}$$

Clearly, the first congruence is satisfied by $\beta_1 = 0$. Furthermore, since

$$(1+\gamma)^4 - 1 = -8 + 24i = (-3-i)\gamma^6 \in P^6,$$

it follows that $(1+\gamma)^4 \equiv 1 \pmod{P^6}$, so the first congruence is also satisfied by $\beta_1 = 1$. Similarly, it can be shown that the second congruence is satisfied by each $(\beta_1, \beta_2) \in \{(0,0),(0,1),(1,0),(1,1)\}$. Next, substituting any choice of (β_1, β_2) into the third congruence yields a linear congruence that is satisfied only by $\beta_3 = 1$. As one can verify, by continuing this process, we get that $\beta_3 = \beta_4 = \ldots = 1$, yielding the following four solutions:

$$\begin{aligned} x &= 1 \\ x &= 1 + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5 + \ldots \\ x &= 1 + \gamma + \gamma^3 + \gamma^4 + \gamma^5 + \ldots \\ x &= 1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \ldots \end{aligned}$$

We remark that, with respect to the P-adic valuation, we get that $|\gamma|_P < 1$, so $1 + \gamma + \gamma^2 + \gamma^3 + \ldots = \frac{1}{1-\gamma} = i$. Using this fact, it can be shown that these four solutions can be reduced to $1, -1, -i$ and i, respectively, as expected.

The determination of the solutions of $x^n \equiv 1 \pmod{P^a}$ over $O_{\mathbb{K}}$ will be performed in three cases: In Case 1, we shall study these congruences when $p \nmid n$, and in Case 2 and 3 when $n = p^b$ and b is a positive integer. More precisely, in Case 2, we study the solutions of $x^{p^b} \equiv 1 \pmod{P^a}$ under the assumption that $P \| (p)$ and in Case 3, we continue this study for an arbitrary P, regardless of whether $P \| (p)$ or $P^2 \mid (p)$. Finally, we shall describe the solutions for an arbitrary n.

This paper is intended as a short synopsis of the four articles [2, 3, 4, 5], discussing the structure of the solutions of $x^n \equiv 1 \pmod{P^a}$. Therefore, all statements in this paper are given without proofs, which can be found in the papers cited above.

2 Preliminaries

Let $\mathbb{K}$ be an algebraic number field. Denote by $O_{\mathbb{K}}$ the ring of integers of $\mathbb{K}$ and by P a prime ideal in $O_{\mathbb{K}}$. The group of units of the residue ring $O_{\mathbb{K}}/P^a$, where a is a positive integer, will be denoted by $(O_{\mathbb{K}}/P^a)^*$. The residue class modulo P^a of an element $\alpha \in O_{\mathbb{K}}$ will be denoted by $[\alpha]_{P^a}$.

Recall that for any prime ideal P there is a *unique* (positive) rational prime number such that $P \mid (p)$. In this case, it can be shown that the norm of P is $\mathrm{N}P = p^f$. The number f is called the *inertial degree* of P and p is called the rational prime number *lying below* P (as $(p) \subseteq P$). Alternatively, it is also customary to say that P *lies above* p. The positive integer e such that $P^e \| (p)$ (that is, such $P^e \mid (p)$ but $P^{e+1} \nmid (p)$) is called the *ramification index* of P over p.

As a consequence of the theory developed in this article, we obtain several results regarding the structure of the solutions of the equation $x^n = 1$ within the framework of the *P-adic number field* $\mathbb{K}_P$. The field $\mathbb{K}_P$ is constructed similarly to the p-adic

field $\mathbb{Q}_p$, using the completion process, relative to the valuation

$$|x|_P := p^{-\mathrm{ord}_P(x)}$$

defined on $\mathbb{K}$, where $\mathrm{ord}_P(x)$ is the integer satisfying $P^{\mathrm{ord}_P(x)} \| (x)$. As in the field $\mathbb{Q}_p$, given an element $\gamma \in P \setminus P^2$, every P-adic integer $\mathfrak{a}$ has a P-adic expansion of the form

$$\mathfrak{a} = \theta_0 + \theta_1\gamma + \theta_2\gamma^2 + \dots,$$

where the $\theta_i \in O_{\mathbb{K}}$ are uniquely determined modulo P. In this setting, the P-adic integers are denoted by $\mathcal{O}_P$. The element γ is called a *uniformizer* for $\mathbb{K}_P$. Note that $P \| (\gamma)$.

Given a positive integer a, we define $\mathfrak{M}_a(\mathcal{O}_P)$ to be a complete residue system of P-adic integers modulo P^a. That is, each P-adic integer is congruent modulo P^a to a unique element of $\mathfrak{M}_a(\mathcal{O}_P)$. The residue class modulo P^a of an element $\mathfrak{a} \in \mathcal{O}_P$ will be denoted by $[\mathfrak{a}]_{P^a}$. We remark that $\mathfrak{M}_a(\mathcal{O}_P)$ is finite, since $\mathcal{O}_P/\gamma^a\mathcal{O}_P \cong O_{\mathbb{K}}/P^a$. A detailed discussion can be found in [2, p. 444].

3 The lifting method

Our method of solving the congruence $x^n \equiv 1 \pmod{P^a}$ is by applying the *lifting method*. This method is based on the observation that the solutions of $x^n \equiv 1 \pmod{P^a}$ are to be found among those of $x^n \equiv 1 \pmod{P^{a-1}}$. In more detail, suppose that $x \equiv \alpha \pmod{P^{a-1}}$ is a solution of $x^n \equiv 1 \pmod{P^{a-1}}$ and let $\gamma \in P \setminus P^2$ be chosen arbitrarily. Now, it can be shown that

$$x \equiv \alpha \pmod{P^{a-1}} \Leftrightarrow x \equiv \alpha + \theta_1\gamma^{a-1}, \dots, \alpha + \theta_{\mathrm{N}P}\gamma^{a-1} \pmod{P^a},$$

where $\mathfrak{M} = \{\theta_1, \theta_2, \dots, \theta_{\mathrm{N}P}\}$ is a complete residue system modulo P (see [3, p. 459]). It may happen, of course, that not every number $\alpha + \theta_i\gamma^{a-1}$ in the above list is a solution of the original congruence modulo P^a. Thus, it is necessary to determine the θ_i's so that $\alpha + \theta_i\gamma^{a-1}$ satisfies the congruence modulo P^a. Since this process is recursive in nature, it first requires solving the congruence $x^n \equiv 1 \pmod{P}$.

Example 1. *Let us consider the congruence*

$$x^3 \equiv 1 \pmod{P^3}$$

over $\mathbb{Z}$ *for* $P = (7)$. *Here,* $P = (7)$ *is a prime ideal in* $\mathbb{Z}$ *with* $\mathrm{N}P = 7$, *so we can choose the complete residue system* $\mathfrak{M} = \{0, 1, 2, \dots, 6\}$ *and* $\gamma = 7$.

We first identify the solutions modulo P, *that is, the solutions to* $x^3 \equiv 1 \pmod{7}$. *By testing the numbers* $0, 1, 2, \dots, 6$, *we find that* $x \equiv 1, 2, 4 \pmod{P}$ *are the solutions to* $x^3 \equiv 1 \pmod{P}$. *The next step is to determine the* θ*'s for which* $1 + \theta\gamma$, $2 + \theta\gamma$, $4 + \theta\gamma$ *are solutions of* $x^3 \equiv 1 \pmod{P^2}$. *Let us illustrate this process for*

$2+\theta\gamma$. *We wish to find the* θ*'s in* $\{0,1,2,\ldots,6\}$ *for which* $(2+\theta\gamma)^3 \equiv 1 \pmod{P^2}$. *Since*

$$(2+\theta\gamma)^3 = 8+12\theta\gamma+6\theta^2\gamma^2+\theta^3\gamma^3 \equiv 8+12\theta\gamma \pmod{P^2},$$

the congruence we need to solve is $8+12\theta\gamma \equiv 1 \pmod{P^2}$, *which implies* $12\theta\gamma \equiv -7 \pmod{P^2}$. *Since* $\gamma = 7$, *it follows that* $12\theta \equiv -1 \pmod{P}$ *and hence* $\theta \equiv 4 \pmod{P}$. *Therefore* $\theta = 4$, *which yields the following solution of* $x^3 \equiv 1 \pmod{P^2}$*:*

$$x \equiv 2+4\gamma \pmod{P^2}.$$

Similarly, applying this process to $1+\theta\gamma$ *and* $4+\theta\gamma$ *yields the following two solutions:*

$$x \equiv 1+0\gamma \pmod{P^2} \quad ; \quad x \equiv 4+2\gamma \pmod{P^2}.$$

We continue by determining the θ*'s for which* $1+0\gamma+\theta\gamma^2$, $2+4\gamma+\theta\gamma^2$, $4+2\gamma+\theta\gamma^2$ *satisfy* $x^3 \equiv 1 \pmod{P^3}$. *Again, we shall illustrate this process to* $2+4\gamma+\theta\gamma^2$*:*

$$\begin{gathered}
(2+4\gamma+\theta\gamma^2)^3 \equiv 1 \pmod{P^3} \\
8+48\gamma+96\gamma^2+12\theta\gamma^2+\gamma^3\cdot(\text{someting}) \equiv 1 \pmod{P^3} \\
48\gamma+12\theta\gamma^2+96\gamma^2 \equiv -7 \pmod{P^3} \\
\Updownarrow \\
48+12\theta\gamma+96\gamma \equiv -1 \pmod{P^2} \\
12\theta\gamma+96\gamma \equiv -49 \pmod{P^2} \\
\Updownarrow \\
12\theta+96 \equiv 0 \pmod{P} \\
\Updownarrow \\
\theta \equiv 6 \pmod{P}.
\end{gathered}$$

Therefore $\theta = 6$, *which yields the following solution of* $x^3 \equiv 1 \pmod{P^3}$*:*

$$x \equiv 2+4\gamma+6\gamma^2 \pmod{P^3}.$$

Similarly, applying this process for $1+0\gamma+\theta\gamma^2$ *and* $4+2\gamma+\theta\gamma^2$, *we obtain two more solutions:*

$$x \equiv 1+0\gamma+0\gamma^2 \pmod{P^3} \quad ; \quad x \equiv 4+2\gamma+0\gamma^2 \pmod{P^3}.$$

To conclude, the incongruent solutions of $x^3 \equiv 1 \pmod{P^3}$ *are*

$$\begin{gathered}
x \equiv 1+0\gamma+0\gamma^2 = 1 \pmod{P^3} \\
x \equiv 2+4\gamma+6\gamma^2 = 324 \pmod{P^3} \\
x \equiv 4+2\gamma+0\gamma^2 = 18 \pmod{P^3}.
\end{gathered}$$

The lifting method can be described schematically using a rooted tree. The vertices of the tree in the a-th level, are the incongruent solutions of $x^n \equiv 1 \pmod{P^a}$.

The "children" of a vertex in the a-th level are the solutions (if there are any) of $x^n \equiv 1 \pmod{P^{a+1}}$ which were lifted by their parent vertex. For example, the first four levels of the tree which corresponds to the congruence $x^3 \equiv 1 \pmod{7^a}$ over $\mathbb{Z}$, from Example 1, are shown in Figure 1 below.

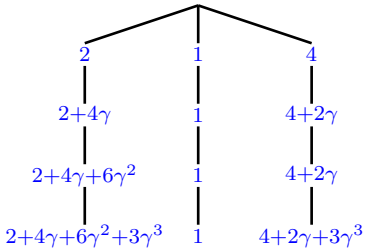


Figure 1

Suppose that p is a prime number and b is a positive integer. In the special case of p^b-th roots of unity modulo P^a, where P lies above p, the lifting method can be applied in a more streamlined manner. If $a = 1$, then it can be shown that the congruence $x^{p^b} \equiv 1 \pmod{P}$ has only one solution, namely $x \equiv 1 \pmod{P}$ (see [2, p. 449]). If $a \geqslant 2$ and the p^b-th roots of unity modulo P^{a-1} are known, then the p^b-th roots of unity modulo P^a can be determined by the following procedure: If α satisfies $x^{p^b} \equiv 1 \pmod{P^{a-1}}$, then we check whether α satisfies $\alpha^{p^b} \equiv 1 \pmod{P^a}$. If so, this root "produces" the solutions $x \equiv \alpha + \theta\gamma^{a-1} \pmod{P^a}$ of $x^{p^b} \equiv 1 \pmod{P^a}$, where θ is an arbitrary element from a complete residue system modulo P (see [4, p. 20]).

Example 2. *Let us consider the congruence*

$$x^3 \equiv 1 \pmod{P^4}$$

over $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, *where* $P = (\sqrt{3})$. *Here* $O_{\mathbb{K}} = \mathbb{Z} + \mathbb{Z}\sqrt{3}$, $P^2 = (3)$ *and we can choose* $\gamma = \sqrt{3}$.

Before solving this congruence, we need to characterize the elements of P^a. *If* $a = 2k$, *then* $P^{2k} = (3^k)$, *so* $x + y\sqrt{3} \in P^{2k}$ *if and only if* $3^k \mid x$ *and* $3^k \mid y$. *If* $a = 2k + 1$, *then*

$$\begin{aligned} P^{2k+1} &= (3)^k P = (3^k\sqrt{3}) = \{3^k\sqrt{3}(x + y\sqrt{3}) : x, y \in \mathbb{Z}\} \\ &= \{3^{k+1}y + 3^k x\sqrt{3} : x, y \in \mathbb{Z}\}. \end{aligned}$$

Hence, $x + y\sqrt{3} \in P^{2k+1}$ *if and only if* $3^{k+1} \mid x$ *and* $3^k \mid y$. *Furthermore, since* $\mathrm{N}P = 3$, *we may choose* $\mathfrak{M} = \{0, 1, -1\}$ *as a complete residue system modulo* P.

Now we can begin solving the congruence. As mentioned above, the congruence $x^3 \equiv 1 \pmod{P}$ *has only one solution, namely* $x \equiv 1 \pmod{P}$. *Turning now to the*

case modulo P^2, we need only to check whether $x = 1$ satisfies $x^3 \equiv 1 \pmod{P^2}$. This is clearly true and hence the solutions modulo P^2 are $x \equiv 1 + \theta_1\gamma \pmod{P^2}$, where $\theta_1 \in \mathfrak{M}$, that is $x \equiv 1, 1+\gamma, 1-\gamma \pmod{P^2}$. To solve the congruence modulo P^3, we need to check which elements of $\{1, 1+\gamma, 1-\gamma\}$ satisfies $x^3 \equiv 1 \pmod{P^3}$. Clearly, $x = 1$ satisfies this congruence and therefore produces the solutions $x \equiv 1 + \theta_2\gamma^2 \pmod{P^3}$, where $\theta_2 \in \mathfrak{M}$.

For the options $x = 1 + \gamma$ and $x = 1 - \gamma$, we have

$$(1 \pm \gamma)^3 = (1 \pm \sqrt{3})^3 = 10 \pm 6\sqrt{3} \equiv 1 \pmod{P^3}.$$

Hence, we obtain six additional solutions $x \equiv 1 \pm \gamma + \theta_2\gamma^2 \pmod{P^3}$, where $\theta_2 \in \mathfrak{M}$. Altogether, we obtain that the solutions modulo P^3 are $x \equiv 1 + \theta_1\gamma + \theta_2\gamma^2 \pmod{P^3}$, where $\theta_1, \theta_2 \in \mathfrak{M}$. For the case modulo P^4, note that

$$\begin{aligned}
1^3 &= 1 \pmod{P^4} \\
(1+\gamma^2)^3 &= 4^3 = 64 \equiv 1 \pmod{P^4} \\
(1-\gamma^2)^3 &= (-2)^3 = -8 \equiv 1 \pmod{P^4} \\
(1 \pm \gamma)^3 &= (1 \pm \sqrt{3})^3 = 10 \pm 6\sqrt{3} \not\equiv 1 \pmod{P^4} \\
(1 \pm \gamma + \gamma^2)^3 &= (4 \pm \sqrt{3})^3 = 100 \pm 51\sqrt{3} \not\equiv 1 \pmod{P^4} \\
(1 \pm \gamma - \gamma^2)^3 &= (-2 \pm \sqrt{3})^3 = -26 \pm 15\sqrt{3} \not\equiv 1 \pmod{P^4}.
\end{aligned}$$

This produces the following 9 solutions: $x \equiv 1 + \theta_2\gamma^2 + \theta_3\gamma^3 \pmod{P^4}$, where $\theta_2, \theta_3 \in \mathfrak{M}$.

The first five levels of the tree corresponding to the congruence $x^3 \equiv 1 \pmod{P^4}$ over $\mathbb{Q}(\sqrt{3})$, from Example 2, are shown in Figure 2 below.

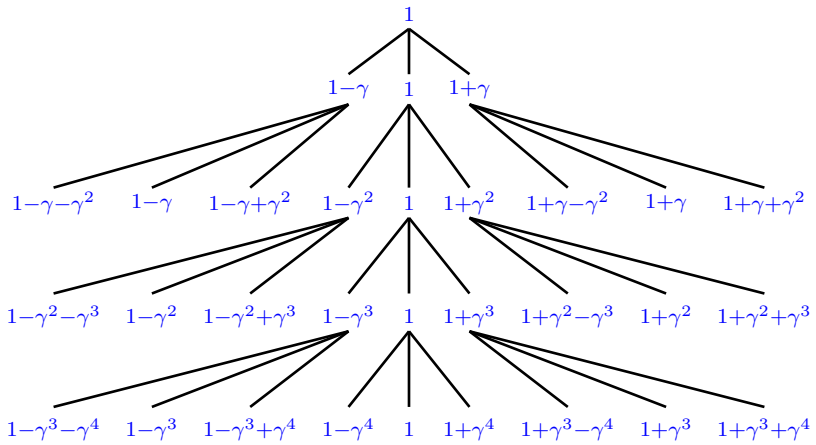


Figure 2

One of our main goals in this paper is to characterize the structure of the tree corresponding to the n-th roots of unity modulo P^a.

4 Case 1: n-th roots of unity when $p \nmid n$

We begin by observing that the incongruent solutions of $x^n \equiv 1 \pmod{P^a}$ form a subgroup of the group of units $(O_{\mathbb{K}}/P^a)^*$. This subgroup will be denoted by $\mathrm{U}_{P^a}(n)$, that is,

$$\mathrm{U}_{P^a}(n) \coloneqq \{[x]_{P^a} : x \in O_{\mathbb{K}},\ x^n \equiv 1 \pmod{P^a}\}.$$

The goal of this section is to study the group $\mathrm{U}_{P^a}(n)$, when $p \nmid n$. The following theorem is one of our main results:

Theorem 3 ([2, p. 450]). *Suppose that p is a rational prime number, P is a prime ideal in the algebraic number field $\mathbb{K}$ lying above p and n, a are positive integers. If $p \nmid n$, then*

$$\mathrm{U}_P(n) \cong \mathrm{U}_{P^a}(n)$$

and this isomorphism is given by the map

$$[x]_P \mapsto [x^{\mathrm{N}P^{a-1}}]_{P^a}.$$

This result implies that the solutions of $x^n \equiv 1 \pmod{P^{a+1}}$ can be obtained by raising the solutions of $x^n \equiv 1 \pmod{P^a}$ to the NP-th power. As an illustrative example, let us consider the congruences $x^3 \equiv 1 \pmod{7^a}$ over $\mathbb{Z}$ for $a \in \{1, 2, 3, 4\}$. Here $n = 3$, $p = 7$, $P = (7)$, so $p \nmid n$ and $\mathrm{N}P = 7$. We start by noticing that the solutions of $x^3 \equiv 1 \pmod 7$ are $x \equiv 1, 2, 4 \pmod 7$. Using the map from Theorem 3, it follows that the solutions of $x^3 \equiv 1 \pmod{7^2}$ are $x \equiv 1^7, 2^7, 4^7 \pmod{7^2}$, which simplifies to $x \equiv 1, 30, 18 \pmod{7^2}$. Similarly, the solutions of $x^3 \equiv 1 \pmod{7^3}$ are $x \equiv 1^7, 30^7, 18^7 \pmod{7^3}$, namely $x \equiv 1, 324, 18 \pmod{7^3}$ and finally, the solutions of $x^3 \equiv 1 \pmod{7^4}$ are $x \equiv 1^7, 324^7, 18^7 \pmod{7^4}$, which are $x \equiv 1, 1353, 1047 \pmod{7^4}$.

In the discussion to follow we go further and present deeper results that describe the n-th roots of unity modulo P within the framework of the P-adic number field $\mathbb{K}_P$. Let $\mathrm{U}_{\mathbb{K}_P^*}(n)$ denote the subgroup of n-th roots of unity in the field $\mathbb{K}_P$, namely $\mathrm{U}_{\mathbb{K}_P^*}(n) \coloneqq \{x \in \mathbb{K}_P^* : x^n = 1\}$.

Theorem 4 ([2, p. 452]). *Suppose that p is a rational prime number, P is a prime ideal in the algebraic number field $\mathbb{K}$ lying above p and n is a positive integer. If $p \nmid n$, then*

$$\mathrm{U}_P(n) \cong \mathrm{U}_{\mathbb{K}_P^*}(n)$$

and this isomorphism is given by either of the following two maps:

$$\begin{aligned} \psi :& \mathrm{U}_P(n) \to \mathrm{U}_{\mathbb{K}_P^*}(n) \\ & [x]_P \longmapsto \lim_{k\to\infty} x^{\mathrm{N}P^{k-1}} \end{aligned} \qquad \textit{or} \qquad \begin{aligned} \nu :& \mathrm{U}_{\mathbb{K}_P^*}(n) \to \mathrm{U}_P(n) \\ & x \longmapsto [x]_P \end{aligned}$$

In particular, the equation $x^n = 1$ *has exactly* $\gcd(\mathrm{N}P - 1, n)$ *solutions in* $\mathbb{K}_P^*$.

The proof relies heavily on a version of Hensel's Lemma, suitable for $\mathbb{K}_P$ (see [2, p. 452]). Knowing an explicit isomorphism between $\mathrm{U}_{\mathbb{K}_P^*}(n)$ and $\mathrm{U}_{P^a}(n)$ can assist us in characterizing the solutions of $x^n \equiv 1 \pmod{P^a}$ when $p \nmid n$ in terms of P-adic numbers. Before doing so, let us present a new notation. Let $\mathfrak{a} \in \mathcal{O}_P$ be a P-adic integer and let

$$\mathfrak{a} = \alpha_0 + \alpha_1\gamma + \alpha_2\gamma^2 + \dots$$

be its P-adic expansion, where $\gamma \in P \setminus P^2$. For every non-negative integer n denote by $\mathfrak{a}_n$ the *n-th partial sum* of $\mathfrak{a}$, namely

$$\mathfrak{a}_n \coloneqq \alpha_0 + \alpha_1\gamma + \alpha_2\gamma^2 + \dots + \alpha_n\gamma^n.$$

These partial sums clearly depend upon the choice of γ and hence, should be denoted, say, by $\mathfrak{a}_n^{\gamma}$. However, in our applications we consider $\mathfrak{a}_{n-1}$ modulo P^n, which is independent of the choice of γ. In other words, if $\delta \in P \setminus P^2$, then $\mathfrak{a}_{n-1}^{\gamma} \equiv \mathfrak{a}_{n-1}^{\delta} \pmod{P^n}$. Thus, from now on, we shall omit the superscript γ and use the shorter notation $\mathfrak{a}_{n-1}$. Observe that $\mathfrak{a}_n \in O_{\mathbb{K}}$ and that $\mathfrak{a} \equiv \mathfrak{a}_{n-1} \pmod{P^n}$ for each n.

The following theorem describes the structure of the solutions of the congruence $x^n \equiv 1 \pmod{P^a}$ when $p \nmid n$.

Theorem 5 ([2, p. 454])**.** *Suppose that p is a rational prime number, P is a prime ideal in the algebraic number field $\mathbb{K}$ lying above p and n is a positive integer. If $p \nmid n$, then*

$$\mathrm{U}_{\mathbb{K}_P^*}(n) \cong \mathrm{U}_{P^a}(n)$$

for every positive integer a and this isomorphism is given by the natural map

$$x \mapsto [x]_{P^a}.$$

Consequently, the congruence $x^n \equiv 1 \pmod{P^a}$ has $\gcd(\mathrm{N}P - 1, n)$ incongruent solutions in $O_{\mathbb{K}}$ and they are of the form

$$x \equiv \mathfrak{u}_{a-1} \pmod{P^a},$$

where $\mathfrak{u} \in \mathrm{U}_{\mathbb{K}_P^*}(n)$.

As an illustrative example, let us consider again the congruence $x^3 \equiv 1 \pmod{7^a}$ in $\mathbb{Z}$. As one can verify, one of the solutions of the equation $x^3 = 1$ in the field $\mathbb{Q}_7$ has the following initial expansion:

$$x = 2 + 4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + \dots$$

Truncating this solution yields the solutions $x \equiv 2 \pmod 7$, $x \equiv 30 \pmod{7^2}$, $x \equiv 324 \pmod{7^3}$ and $x \equiv 1353 \pmod{7^4}$ of $x^3 \equiv 1 \pmod{7^a}$ for $a \in \{1, 2, 3, 4\}$, respectively. As we can see, this result is consistent with the results obtained earlier.

Combining the results of Theorem 4 and 5 gives a full picture of the structure of the corresponding tree of $x^n \equiv 1 \pmod{P^a}$ when $p \nmid n$: each one of the solutions of $x^n \equiv 1 \pmod{P}$ produces an infinite branch, which in turn, corresponds to a solution of $x^n = 1$ in $\mathbb{K}_P$. Figure 3 below illustrates a typical structure of such a tree.

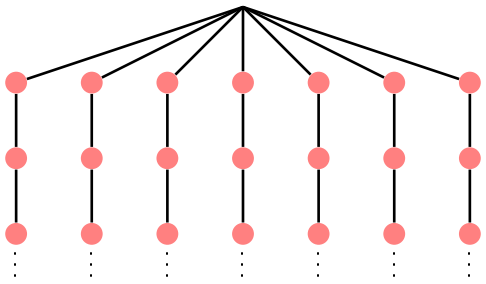


Figure 3

5 Case 2: n-th roots of unity when $P\|(p)$

In this section we shall determine the solutions of the congruence

$$x^{p^b} \equiv 1 \pmod{P^a},$$

where b is a non-negative integer and $P\|(p)$. The analysis of this congruence is dependent upon whether $p = 2$ or $p > 2$ and upon the number $\Delta = \max\{1, a - b\}$. The transition to solving $x^n \equiv 1 \pmod{P^a}$ when $P\|(p)$ and $p \mid n$ is straightforward and will be performed in Section 9 of this study. Our main result is the following theorem.

Theorem 6 ([3, p. 467]). *Suppose that p is a rational prime number, P is a prime ideal in the algebraic number field $\mathbb{K}$ lying above p, a, b are integers such that $a \geqslant 1$, $b \geqslant 0$ and $\mathfrak{M}$ is a complete residue system modulo $P^{a-\Delta}$, where $\Delta = \max\{1, a - b\}$. Suppose also that $P\|(p)$. Then:*

(a) *If $p > 2$, then the congruence $x^{p^b} \equiv 1 \pmod{P^a}$ has exactly $(\mathrm{N}P)^{a-\Delta}$ incongruent solutions $x \equiv 1 + p^{\Delta}\theta \pmod{P^a}$, where $\theta \in \mathfrak{M}$.*

(b) *If $p = 2$ and $\Delta = 1$, then the congruence $x^{2^b} \equiv 1 \pmod{P^a}$ has exactly $(\mathrm{N}P)^{a-1}$ incongruent solutions $x \equiv 1 + 2\theta \pmod{P^a}$, where $\theta \in \mathfrak{M}$.*

(c) *If $p = 2$ and $\Delta > 1$, then the congruence $x^{2^b} \equiv 1 \pmod{P^a}$ has exactly $2(\mathrm{N}P)^{a-\Delta}$ incongruent solutions $x \equiv \pm 1 + 2^{\Delta}\theta \pmod{P^a}$, where $\theta \in \mathfrak{M}$.*

Suppose that $p > 2$. If $1 \leqslant a \leqslant b+1$, then $\Delta = 1$, so $x \equiv 1 + p\theta \pmod{P^a}$, where θ is an element of a complete residue system modulo P^{a-1}. If $b+1 < a$, then $\Delta = a - b$, so $x \equiv 1 + p^{a-b}\theta \pmod{P^a}$, where θ is an element of a complete residue system modulo P^b. Hence, in this case, the growth of the corresponding tree continues up its $(b+1)$th level of the tree and then stabilizes, as illustrated in Figure 4 below in the cases where $p = 3$, $b = 1$ (right) and where $p = 3$, $b = 2$ (left).

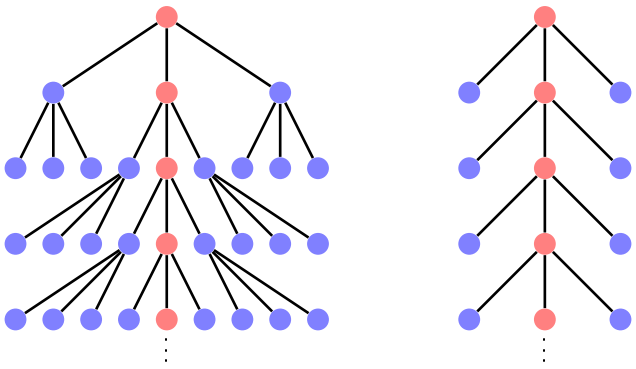


Figure 4

The tree on the right is a typical tree that corresponds to the solutions of the congruence $x^3 \equiv 1 \pmod{P^a}$ and the tree on the left, corresponds to the solutions of the congruence $x^9 \equiv 1 \pmod{P^a}$, both under the assumption that $P\|(3)$. Note that in both trees, there is a single infinite branch, namely the vertices colored red, which corresponds to the unique solution $x = 1$ of $x^3 = 1$ and of $x^9 = 1$ in $\mathbb{K}_P$.

Recall that Theorem 5 states that if $p \nmid n$, then the equation $x^n = 1$ has exactly $\gcd(\mathrm{N}P - 1, n)$ distinct roots in $\mathbb{K}_P$. Provided that $P\|(p)$, we can go further and determine the number of solutions for the equation $x^n = 1$ for *any* n. Specifically, we present the following theorem:

Theorem 7 ([3, p. 465]). *Let $\mathbb{K}$ be a number field, P be a prime ideal lying above the rational prime p and let N be the number of n-th roots of unity in $\mathbb{K}_P$. Set $d = \gcd(\mathrm{N}P - 1, n)$. If $P\|(p)$, then*

$$\mathrm{N} = \begin{cases} d & \text{if } p = 2 \text{ and } 2 \nmid n \\ 2d & \text{if } p = 2 \text{ and } 2 \mid n \\ d & \text{if } p > 2. \end{cases}$$

Note that since the field $\mathbb{Q}_p$ of p-adic numbers is obtained by taking $\mathbb{K} = \mathbb{Q}$ and $P = (p)$, it follows that the number of n-th roots of unity in $\mathbb{Q}_p$ is

$$\mathrm{N} = \begin{cases} 1 & \text{if } p = 2 \text{ and } 2 \nmid n \\ 2 & \text{if } p = 2 \text{ and } 2 \mid n \\ \gcd(p-1, n) & \text{if } p > 2. \end{cases}$$

As we shall see later, Theorem 7 may be false if $P^2 \mid (p)$. This occurs, for instance, if $\mathbb{K} = \mathbb{Q}(\sqrt{6})$, $p = 3$ and $P = (3, \sqrt{6})$. Here $P^2 = (3)$, so $\mathrm{N}P = 3$. In this case, it can be shown that the equation $x^9 = 1$ has at least one non-trivial root in $\mathbb{K}_P$, while $d = \gcd(\mathrm{N}P - 1, 9) = 1$. Moreover, its roots are:

$$\begin{aligned} x &= 1 \\ x &= 1 - \gamma - \gamma^2 - \gamma^4 + \gamma^5 + \dots \\ x &= 1 + \gamma - \gamma^2 - \gamma^4 - \gamma^5 + \dots \end{aligned}$$

where $\gamma = \sqrt{6}$. For more details see Section 8 of this study.

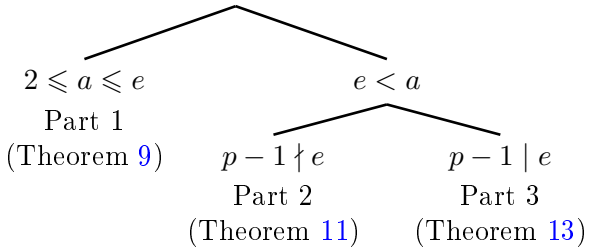
Theorem 7 states, in particular, that if $P \| (p)$, then the solutions of $x^{p^b} = 1$ in $\mathbb{K}_P$ are $x = \pm 1$ if $p = 2$, and $x = 1$ if $p > 2$. Note that these results are consistent with the result of Theorem 6. For instance, if $p > 2$, then the incongruent solutions of $x^{p^b} \equiv 1 \pmod{P^a}$ are of the form $x \equiv 1 + p^{\Delta}\theta \pmod{P^a}$. Now, for a sufficiently large a, we obtain

$$x \equiv 1 + p^{a-b}\theta \pmod{P^a}.$$

Letting $a \to \infty$, we find that $p^{a-b} \to 0$ and therefore $x = 1$, as expected.

6 Case 3: n-th roots of unity when $n = p^b$

In this section we continue studying the case $n = p^b$, for an arbitrary P, regardless of whether $P \| (p)$ or $P^2 \mid (p)$. Solving the congruence $x^{p^b} \equiv 1 \pmod{P^a}$ for P with a general ramification index e will require different methods from those we used in Case 2. Nevertheless, the results will be applicable to both cases. Our study will be carried out separately in three parts, as described in the following diagram:



In order to state this combined result, we need to introduce several additional notations. For convenience, we gather them in the following single "Generic Notation":

Notation 8. *Suppose that*

(1) *p is a rational prime number.*

(2) *P is a prime ideal in the algebraic number field $\mathbb{K}$ lying above p with ramification index $e \geqslant 1$.*

(3) $\mathfrak{M}$ *is a complete residue system of* $O_{\mathbb{K}}$ *modulo* P *with* $0 \in \mathfrak{M}$.

(4) $\gamma \in P \setminus P^2$.

(5) n, a *and* b *are positive integers.*

(6) c *is a non-negative integer satisfying* $p^c \| e$ *and* $r = \min\{c, b-1\}$.

(7) *For each integer* $0 \leqslant t \leqslant c$ *let* Γ_t *be the quantity* $\Gamma_t = \frac{e}{p^t(p-1)}$.

(8) *For each non-negative integer* k, T_k *denotes the real function* $\mathrm{T}_k(u) = kp^u - eu$ *for* $u \in \mathbb{R}$.

(9) m_k *denotes the integral minimal value of* T_k *over the set* $\{0, 1, 2, 3, \ldots\}$, *including* $m_0 = -\infty$.

Part 1: Solving $x^{p^b} \equiv 1 \pmod{P^a}$ when $2 \leqslant a \leqslant e$

The first part covers the cases where $2 \leqslant a \leqslant e$. As mentioned in Section 3, the case $a = 1$ yields only the trivial solution, so it is omitted here.

Theorem 9 ([4, p. 24]). *Assume Notation 8. If* $2 \leqslant a \leqslant e$, *then the incongruent solutions of* $x^{p^b} \equiv 1 \pmod{P^a}$ *are*

$$x \equiv 1 + \theta_\Delta \gamma^\Delta + \theta_{\Delta+1}\gamma^{\Delta+1} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\Delta = \lceil \frac{a}{p^b} \rceil$ *and* $\theta_\Delta, \theta_{\Delta+1}, \ldots, \theta_{a-1} \in \mathfrak{M}$.

Example 10. *Let* $\mathbb{K} = \mathbb{Q}(\sqrt[4]{2})$. *As one can verify,* $P = (\sqrt[4]{2})$ *is a prime ideal lying above* $p = 2$ *with ramification index* $e = 4$. *Furthermore, its norm is* $\mathrm{N}P = 2$, *so* $\mathfrak{M} = \{0, 1\}$ *can be taken as a complete residue system modulo* P. *Now, consider the congruence*

$$x^2 \equiv 1 \pmod{P^a}.$$

According to Theorem 9, $\Delta = \lceil \frac{a}{2} \rceil$ *and the solutions for* $2 \leqslant a \leqslant 4$ *are*

$$\begin{aligned} a = 2: &\quad x \equiv 1 + \theta_1\gamma \pmod{P^2} \\ a = 3: &\quad x \equiv 1 + \theta_2\gamma^2 \pmod{P^3} \\ a = 4: &\quad x \equiv 1 + \theta_2\gamma^2 + \theta_3\gamma^3 \pmod{P^4} \end{aligned}$$

where we may choose $\gamma = \sqrt[4]{2}$ *and* $\theta_i \in \{0, 1\}$. *Therefore, the first four levels of the corresponding tree are described in Figure 5 below.*

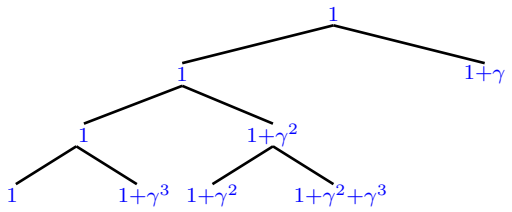


Figure 5

Part 2: Solving $x^{p^b} \equiv 1 \pmod{P^a}$ when $e < a$ and $p-1 \nmid e$

The *integral* minimum value m_k of the functions $\mathrm{T}_k(u) = kp^u - eu$ is important for understanding the structure of the p^b-th roots of unity modulo P^a when $e < a$. Generally, these values can be found directly by considering the functions T_k. Nevertheless, once we have found the *real* minimal value of T_k, it is quite easy to find its *integral* minimal value. In more detail, if T_k attains its real minimal value at $\bar{u}$, which occurs at $\bar{u} = \log_p(\frac{e}{k \ln p})$, then its integral minimal value is obtained at $\lceil \bar{u} \rceil$ or at $\lfloor \bar{u} \rfloor$, possibly both. For example, let us find the integral minimum value m_2 of $\mathrm{T}_k(u)$ for $p = 3$ and $e = 4$. Here $\mathrm{T}_2(u) = 2 \cdot 3^u - 4u$ and $\bar{u} = \log_3(\frac{4}{2 \ln 3}) \approx 0.33$, so $\lceil \bar{u} \rceil = 1$ and $\lfloor \bar{u} \rfloor = 0$. In this case T_2 attains its integral minimal value at both $u = 0$ and $u = 1$, giving $m_2 = 2$. We add two remarks that will be used later. First, it can be shown that if $k \geqslant \frac{e}{p-1}$, then $m_k = k$. Second, the integral minimum values satisfy $-\infty = m_0 < m_1 < m_2 < \cdots < m_k$ for every $k \geqslant 1$ (see [4, p. 27]). Hence, for every integer q, there is a *unique* $k \geqslant 0$ such that $m_k < q \leqslant m_{k+1}$.

Theorem 11 ([4, p. 33])**.** *Assume Notation 8. In addition, let k be the unique non-negative integer such that $m_k < a - eb \leqslant m_{k+1}$ and suppose that the following conditions hold:*

(1) $a \geqslant \mathrm{E} = \max\{2, e\}$, *and*
(2) $p - 1 \nmid e$.

Then the incongruent solutions of $x^{p^b} \equiv 1 \pmod{P^a}$ are

$$x \equiv 1 + \theta_{k+1}\gamma^{k+1} + \theta_{k+2}\gamma^{k+2} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_{k+1}, \theta_{k+2}, \ldots, \theta_{a-1} \in \mathfrak{M}$.

Example 12. *Suppose that $\mathbb{K}$ is a number field and let P be a prime ideal in $\mathbb{K}$ lying above $p = 3$ with ramification index $e = 13$. In addition, suppose that $\mathfrak{M}$ is a complete residue system modulo P with $0 \in \mathfrak{M}$ and let $\gamma \in P \setminus P^2$. We want to describe the solutions of a general congruence $x^{3^b} \equiv 1 \pmod{P^a}$ for all values of $a \geqslant 2$ and b. Since $\mathrm{E} = \max\{2, e\} = 13$, we must distinguish between the cases $2 \leqslant a \leqslant 13$ and $13 < a$.*

For $2 \leqslant a \leqslant 13$, we invoke Theorem 9 to obtain the solutions

$$x \equiv 1 + \theta_\Delta \gamma^\Delta + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_i \in \mathfrak{M}$ and

$$\Delta = \left\lceil \frac{a}{3^b} \right\rceil = \begin{cases} 1 & \text{if } b = 1 \text{ and } 2 \leqslant a \leqslant 3 \\ 2 & \text{if } b = 1 \text{ and } 4 \leqslant a \leqslant 6 \\ 3 & \text{if } b = 1 \text{ and } 7 \leqslant a \leqslant 9 \\ 4 & \text{if } b = 1 \text{ and } 10 \leqslant a \leqslant 12 \\ 5 & \text{if } b = 1 \text{ and } a = 13 \\ 1 & \text{if } b = 2 \text{ and } 2 \leqslant a \leqslant 9 \\ 2 & \text{if } b = 2 \text{ and } 10 \leqslant a \leqslant 13 \\ 1 & \text{if } b \geqslant 3 \text{ and } 2 \leqslant a \leqslant 13 \end{cases}$$

Now assume that $a > 13$. Here $p - 1 \nmid e$, so Theorem 11 can be utilized. In order to describe the solutions, we first need to find the integral minimum values m_k of $\mathrm{T}_k(u) = k3^u - 13u$.

As mentioned above, if $k \geqslant \frac{e}{p-1} = 6.5$, that is, if $k \geqslant 7$, then $m_k = k$. For $1 \leqslant k \leqslant 6$, we shall compute the values m_k directly from the definition. Let u_k be the integral points at which $\mathrm{T}_k(u)$ achieves its integral minimum value m_k and let $\bar{u}_k$ be the real points at which $\mathrm{T}_k(u)$ achieves its real minimum value. Thus $\bar{u}_k = \log_3(\frac{13}{k \ln 3})$. The results are summarized in the table below:

k	u_k	$\bar{u}_k$	m_k
1	2	2.24	-17
2	2	1.61	-8
3	1	1.24	-4
4	1	0.98	-1
5	1	0.78	2
6	1	0.61	5

Hence, by Theorem 11, the solutions of $x^{3^b} \equiv 1 \pmod{P^a}$ for $a > 13$ are $x \equiv 1 + \theta_{k+1}\gamma^{k+1} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a}$, where $\theta_i \in \mathfrak{M}$ and k is the (unique) non-negative integer such that $m_k + 1 \leqslant a - eb \leqslant m_{k+1}$. Note that if $k \geqslant 7$, then $m_k = k$, so in this case $m_k < a - eb \leqslant m_{k+1}$ if and only if $a - eb = k + 1$. Hence, if $a - eb \geqslant 7$, then the solutions are

$$x \equiv 1 + \theta_{a-eb}\gamma^{a-eb} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_i \in \mathfrak{M}$. To conclude, if $a > 13$, then the solutions of $x^{3^b} \equiv 1 \pmod{P^a}$ are

$x \equiv 1 + \theta_\Delta \gamma^\Delta + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a}$, *where* $\theta_i \in \mathfrak{M}$ *and*

$$\Delta = \begin{cases} 0+1 & a - eb \leqslant m_1 \\ 1+1 & m_1 + 1 \leqslant a - eb \leqslant m_2 \\ 2+1 & m_2 + 1 \leqslant a - eb \leqslant m_3 \\ 3+1 & m_3 + 1 \leqslant a - eb \leqslant m_4 \\ 4+1 & m_4 + 1 \leqslant a - eb \leqslant m_5 \\ 5+1 & m_5 + 1 \leqslant a - eb \leqslant m_6 \\ 6+1 & m_6 + 1 \leqslant a - eb \leqslant m_7 \\ a - eb & m_7 \leqslant a - eb, \end{cases}$$

which yields

$$\Delta = \begin{cases} 1 & a - eb \leqslant -17 \\ 2 & -16 \leqslant a - eb \leqslant -8 \\ 3 & -7 \leqslant a - eb \leqslant -4 \\ 4 & -3 \leqslant a - eb \leqslant -1 \\ 5 & 0 \leqslant a - eb \leqslant 2 \\ 6 & 3 \leqslant a - eb \leqslant 5 \\ 7 & 6 \leqslant a - eb \leqslant 7 \\ a - eb & 7 \leqslant a - eb. \end{cases}$$

Part 3: Solving $x^{p^b} \equiv 1 \pmod{P^a}$ when $e < a$ and $p - 1 \mid e$

The analysis of the solutions in this part depends upon the quantities Γ_0 and Γ_r. Recall that $\Gamma_0 = \frac{e}{p-1}$ and $\Gamma_r = \frac{e}{p^r(p-1)}$, where $r = \min\{c, b-1\}$ and $p^c \| e$. Hence, Γ_0 and Γ_r are integers such that $\Gamma_r \leqslant \Gamma_0$.

Theorem 13 ([4, p. 39]). *Assume Notation 8. In addition, let k be the unique non-negative integer satisfying*

$$m_k < a - eb \leqslant m_{k+1}$$

and suppose that the following conditions hold:

(1) $a \geqslant \mathrm{E} = \max\{2, e\}$, *and*
(2) $p - 1 \mid e$

Then the following statements hold:
(A) *If* $0 \leqslant k < \Gamma_r$, *then the incongruent solutions of* $x^{p^b} \equiv 1 \pmod{P^a}$ *are*

$$x \equiv 1 + \theta_{k+1}\gamma^{k+1} + \theta_{k+2}\gamma^{k+2} + \cdots + \theta_{a-2}\gamma^{a-2} + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_{k+1}, \ldots, \theta_{a-2}, \theta_{a-1} \in \mathfrak{M}$ *are arbitrary.*
(B) *If* $\Gamma_r \leqslant k$, *then the incongruent solutions of* $x^{p^b} \equiv 1 \pmod{P^a}$ *are*

$$x \equiv 1 + \beta_{\Gamma_r}\gamma^{\Gamma_r} + \ldots + \beta_k\gamma^k + \theta_{k+1}\gamma^{k+1} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_{k+1},\dots,\theta_{a-1}\in\mathfrak{M}$ *are arbitrary and* $\beta_{\Gamma_r},\dots\beta_k\in\mathfrak{M}$ *satisfy one of the following systems of congruences, depending upon the value of* k*:*

(a) *If* $\Gamma_r=k=\Gamma_0$*, then*

$$p^b\beta_{\Gamma_0}\gamma^{\Gamma_0}+\binom{p^b}{p}(\beta_{\Gamma_0}\gamma^{\Gamma_0})^p\equiv 0 \pmod{P^a}.$$

(b) *If* $\Gamma_r\leqslant k<\Gamma_0$*, then*

$$(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\beta_{\Gamma_r+1}\gamma^{\Gamma_r+1}+\ldots+\beta_k\gamma^k)^{p^b}\equiv 1 \pmod{P^a}.$$

(c) *If* $\Gamma_r<k=\Gamma_0$*, then*

$$\begin{cases}(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b}\equiv 1 \pmod{P^{a-1}}\\ p^b\beta_{\Gamma_0}\gamma^{\Gamma_0}+\binom{p^b}{p}(\beta_{\Gamma_0}\gamma^{\Gamma_0})^p\equiv 1-(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b} \pmod{P^a}.\end{cases}$$

(d) *If* $\Gamma_r=\Gamma_0<k$*, then*

$$\begin{cases}p^b\beta_{\Gamma_0}\gamma^{\Gamma_0}+\binom{p^b}{p}(\beta_{\Gamma_0}\gamma^{\Gamma_0})^p\equiv 0 \pmod{P^{a-(k-\Gamma_0)}}\\ p^b\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1}\equiv 1-(1+\beta_{\Gamma_0}\gamma^{\Gamma_0})^{p^b} \pmod{P^{a-(k-\Gamma_0)+1}}\\ \qquad\vdots\\ p^b\beta_k\gamma^k\equiv 1-(1+\beta_{\Gamma_0}\gamma^{\Gamma_0}+\ldots+\beta_{k-1}\gamma^{k-1})^{p^b} \pmod{P^a}.\end{cases}$$

(e) *If* $\Gamma_r<\Gamma_0<k$*, then*

$$\begin{cases}(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b}\equiv 1 \pmod{P^{a-1-(k-\Gamma_0)}}\\ p^b\beta_{\Gamma_0}\gamma^{\Gamma_0}+\binom{p^b}{p}(\beta_{\Gamma_0}\gamma^{\Gamma_0})^p\equiv 1-(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b} \pmod{P^{a-(k-\Gamma_0)}}\\ p^b\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1}\equiv 1-(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0}\gamma^{\Gamma_0})^{p^b} \pmod{P^{a-(k-\Gamma_0)+1}}\\ \qquad\vdots\\ p^b\beta_k\gamma^k\equiv 1-(1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{k-1}\gamma^{k-1})^{p^b} \pmod{P^a}.\end{cases}$$

Let us add a few remarks concerning Theorem 13. First, note that even though Theorem 13 gives us the general structure of the solutions, these solutions depend upon the tuples $(\beta_{\Gamma_r},\dots,\beta_k)$ which are not given explicitly, but only as solutions of another set of congruences. Thus, in order to find the solutions explicitly, we need to find these β's first. If $\Gamma_r<\Gamma_0\leqslant k$, then the β's in the first $\Gamma_0-\Gamma_r$ positions satisfy a non-linear congruence; in which case, unfortunately, there is not much we can say about the solutions, unless we know more about the structure of the field $\mathbb{K}$. For instance, as will be demonstrated in Section 9 of this study, if $\mathbb{K}$

is a cyclotomic field, then the structure of the solutions can be fully determined. However, it is important to notice that we have at least one certain tuple, namely $(\beta_{\Gamma_r}, \ldots, \beta_{\Gamma_0-1}) = (0, 0, \ldots, 0)$, which trivially satisfies this non-linear congruence.

Next, β_{Γ_0} satisfies another non-linear congruence of degree p. It can be shown that this congruence can always be reduced to a congruence modulo P. In particular, this means that β_{Γ_0} can have at most p possible values. Note that choosing $\beta_{\Gamma_r} = \ldots = \beta_{\Gamma_0} = 0$ will surely solve the first two congruences. Each of the remaining β's satisfies a linear congruence, which in the same way as above, can be reduced to a congruence modulo P. Unlike the other two congruences, this linear congruence is uniquely solvable for every appropriate choice of $\beta_{\Gamma_r}, \ldots, \beta_{\Gamma_0}$.

Example 14. *Let us consider again the congruence*

$$x^2 \equiv 1 \pmod{P^a}$$

in $\mathbb{K} = \mathbb{Q}(\sqrt[4]{2})$, *where* $P = (\sqrt[4]{2})$. *Here* $p = 2$, $b = 1$ *and* $e = 4$. *Furthermore,* $\mathrm{N}P = 2$, *so* $\mathfrak{M} = \{0, 1\}$ *can be taken as a complete residue system modulo* P.

According to Example 10, the solutions for $2 \leqslant a \leqslant 4$ *are*

$$\begin{aligned} a = 2: &\quad x \equiv 1 + \theta_1\gamma \pmod{P^2} \\ a = 3: &\quad x \equiv 1 + \theta_2\gamma^2 \pmod{P^3} \\ a = 4: &\quad x \equiv 1 + \theta_2\gamma^2 + \theta_3\gamma^3 \pmod{P^4}, \end{aligned}$$

where we may choose $\gamma = \sqrt[4]{2}$ *and* $\theta_i \in \{0, 1\}$. *For* $a > 4$ *we shall evoke Theorem 13 (note that indeed* $p - 1 \mid e$*). In order to do so, we need first to determine the integral minimum values* m_k *of* $\mathrm{T}_k(u) = k2^u - 4u$. *Similar to Example 12, it can be shown that these values are*

$$\underbrace{m_0}_{-\infty} < \underbrace{m_1}_{-4} < \underbrace{m_2}_{0} < \underbrace{m_3}_{2} < \underbrace{m_4}_{4} < \underbrace{m_5}_{5} < \cdots$$

and $m_k = k$ *for* $k \geqslant 4$. *In this case, according to Notation 8, in this case* $p^2 \| e$, *so* $c = 2$ *and* $r = \min\{c, b - 1\} = 0$. *Thus* $\Gamma_0 = \Gamma_r = \frac{e}{p-1} = 4$.

Now, if $5 \leqslant a \leqslant 6$, *then* $m_2 < a - eb \leqslant m_3$, *so* $k = 2$. *Similarly, if* $7 \leqslant a \leqslant 8$, *then* $m_3 < a - eb \leqslant m_4$, *so* $k = 3$. *It follows that if* $5 \leqslant a \leqslant 8$, *then* $0 \leqslant k < \Gamma_0$. *Therefore, by Theorem 13(A), the solutions for* $5 \leqslant a \leqslant 8$ *are*

$$\begin{aligned} a = 5: &\quad x \equiv 1 + \theta_3\gamma^3 + \theta_4\gamma^4 \pmod{P^5} \\ a = 6: &\quad x \equiv 1 + \theta_3\gamma^3 + \theta_4\gamma^4 + \theta_5\gamma^5 \pmod{P^6} \\ a = 7: &\quad x \equiv 1 + \theta_4\gamma^4 + \theta_5\gamma^5 + \theta_6\gamma^6 \pmod{P^7} \\ a = 8: &\quad x \equiv 1 + \theta_4\gamma^4 + \theta_5\gamma^5 + \theta_6\gamma^6 + \theta_7\gamma^7 \pmod{P^8}. \end{aligned}$$

If $a = 9$, *then* $m_4 < a - eb \leqslant m_5$, *so* $k = 4$. *Since here* $\Gamma_0 = \Gamma_r = k$, *it follows by Part (a) of Theorem 13(B) that the solutions are*

$$x \equiv 1 + \beta_4\gamma^4 + \theta_5\gamma^5 + \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 \pmod{P^9},$$

where β_4 satisfies the congruence

$$2\beta_4\gamma^4 + (\beta_4\gamma^4)^2 \equiv 0 \pmod{P^9}.$$

By recalling that $2 = \gamma^4$, we obtain $(\beta_4 + \beta_4^2)\gamma^8 \equiv 0 \pmod{P^9}$, specifically satisfied by either $\beta_4 = 0$ or $\beta_4 = 1$. Therefore, the solutions are

$$a = 9: \quad x \equiv 1 + \theta_4\gamma^4 + \theta_5\gamma^5 + \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 \pmod{P^9}.$$

Suppose now that $a > 9$. Then $a - eb = a - 4 > 5$, so $m_{a-eb} = a - eb$ and $k = a - 5$. Since here $\Gamma_0 = \Gamma_r < k$, it follows by Part (d) of Theorem 13(B), that the solutions are

$$x \equiv 1 + \beta_4\gamma^4 + \ldots + \beta_{a-5}\gamma^{a-5} + \theta_{a-4}\gamma^{a-4} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\beta_4, \ldots, \beta_{a-5}$ satisfy the system

$$\begin{cases} 2\beta_4\gamma^4 + (\beta_4\gamma^4)^2 \equiv 0 \pmod{P^9} \\ 2\beta_5\gamma^5 \equiv 1 - \left(1 + \beta_4\gamma^4\right)^2 \pmod{P^{10}} \\ \quad \vdots \\ 2\beta_{a-5}\gamma^{a-5} \equiv 1 - \left(1 + \beta_4\gamma^4 + \ldots + \beta_{a-6}\gamma^{a-6}\right)^2 \pmod{P^a}. \end{cases}$$

As shown above, the first congruence is satisfied by either $\beta_4 = 0$ or $\beta_4 = 1$. If $\beta_4 = 0$, then we shall prove that $\beta_4 = \beta_5 = \ldots = \beta_{a-5} = 0$ using induction on $a \geqslant 9$. If $a = 9$, then we are done. If $a > 9$, then by the induction hypothesis, $\beta_4 = \beta_5 = \ldots = \beta_{a-6} = 0$, and substituting these values into the last congruence we get $2\beta_{a-5}\gamma^{a-5} \equiv 0 \pmod{P^a}$. Since $2 = \gamma^4$, it follows that $\gamma^4\beta_{a-5}\gamma^{a-5} \equiv 0 \pmod{P^a}$, which implies that $\beta_{a-5} = 0$, completing the induction step.

Suppose now that $\beta_4 = 1$. We shall prove using induction on $a \geqslant 9$ that for every $4 \leqslant i \leqslant a - 5$, we get $\beta_i = 1$ for $4 \mid i$ and $\beta_i = 0$ otherwise. If $a = 9$, then we are done. If $a > 9$, then by the induction hypothesis for every $4 \leqslant i \leqslant a - 6$, we get $\beta_i = 1$ for $4 \mid i$ and $\beta_i = 0$ otherwise. We are left to determine β_{a-5}. To do so, let ℓ be the maximal positive integer such that $4\ell \leqslant a - 6$. By the induction hypothesis, it follows that β_{a-5} satisfies the congruence

$$2\beta_{a-5}\gamma^{a-5} \equiv 1 - \left(1 + \gamma^4 + \gamma^8 + \ldots + \gamma^{4\ell}\right)^2 \pmod{P^a}.$$

Note that since $\gamma^4 = 2$, we get $1 + \gamma^4 + \gamma^8 + \ldots + \gamma^{4\ell} = \gamma^{4\ell+4} - 1$, so

$$\gamma^{a-1}\beta_{a-5} \equiv \gamma^{4\ell+8}(1 - \gamma^{4\ell}) \pmod{P^a}.$$

First, assume that $4 \mid a - 5$. We shall prove that $\beta_{a-5} = 1$. Note that since $a > 9$, the first a which satisfies the assumption $4 \mid a - 5$ is $a = 13$, so $a \geqslant 13$. In this case

$\ell = \frac{a-5}{4} - 1$, so $\gamma^{4\ell+8} = \gamma^{a-1}(1-\gamma^{a-9})$, and the above congruence is equivalent to $\beta_{a-5} \equiv 1 - \gamma^{a-9} \pmod{P}$. But $\gamma^{a-9} \equiv 0 \pmod{P}$ since $a - 9 \geqslant 4$, so $\beta_{a-5} = 1$, completing this case.

Next, assume that $4 \nmid a-5$. We shall prove that $\beta_{a-5} = 0$. Since $4 \nmid a-5$, it follows that at least one of $a-6, a-7, a-8$ is divisible by 4. Thus $\frac{a-8}{4} \leqslant \ell$, so $\gamma^{4\ell+8} = \gamma^a(1-\gamma^{a-8}) \equiv 0 \pmod{P}$ and the above congruence is equivalent to $\beta_{a-5} \equiv 0 \pmod{P}$. Hence $\beta_{a-5} = 0$, as required.

To conclude, the solutions for $10 \leqslant a$ are either

$$x \equiv 1 + \theta_{a-4}\gamma^{a-4} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

or

$$x \equiv 1 + \gamma^4 + \gamma^8 + \ldots + \gamma^{4\ell} + \theta_{a-4}\gamma^{a-4} + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where ℓ satisfies $a - 4\ell \in \{5, 6, 7, 8\}$.

Figure 6 below describes the first twelve levels of the tree corresponding to the solutions of $x^2 \equiv 1 \pmod{P^a}$. Note that this tree has two infinite branches (specifically, the vertices colored red), which correspond to the solutions $x = 1$ and $x = -1$ of $x^2 = 1$ in $\mathbb{K}_P$.

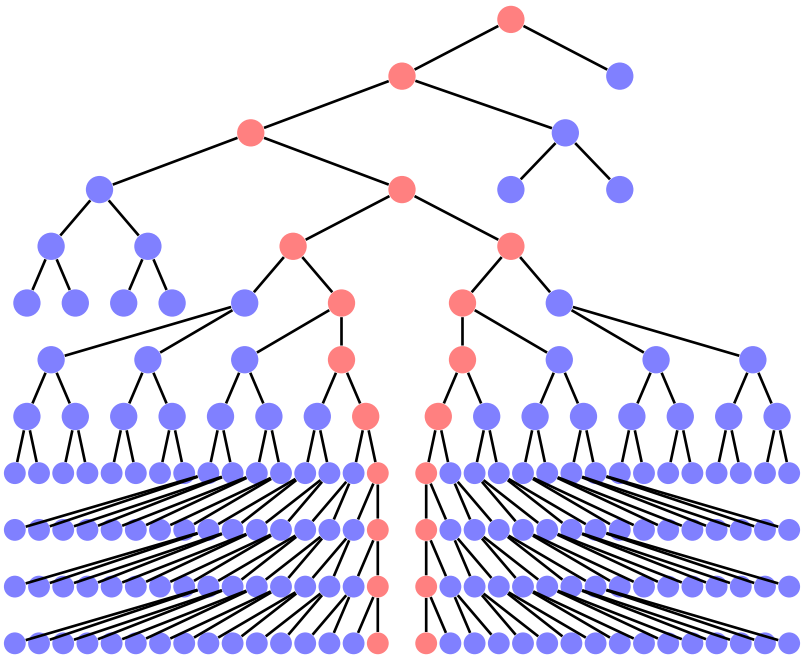


Figure 6

As an example, for $10 \leqslant a \leqslant 13$, *the solutions are*

$$\begin{aligned}
a=10: \quad & x \equiv 1 + \quad \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 \pmod{P^{10}} \\
& x \equiv 1 + \gamma^4 + \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 \pmod{P^{10}} \\
a=11: \quad & x \equiv 1 + \quad \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 + \theta_{10}\gamma^{10} \pmod{P^{11}} \\
& x \equiv 1 + \gamma^4 + \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 + \theta_{10}\gamma^{10} \pmod{P^{11}} \\
a=12: \quad & x \equiv 1 + \quad \theta_8\gamma^8 + \theta_9\gamma^9 + \theta_{10}\gamma^{10} + \theta_{11}\gamma^{11} \pmod{P^{12}} \\
& x \equiv 1 + \gamma^4 + \theta_8\gamma^8 + \theta_9\gamma^9 + \theta_{10}\gamma^{10} + \theta_{11}\gamma^{11} \pmod{P^{12}} \\
a=13: \quad & x \equiv 1 + \quad \theta_9\gamma^9 + \theta_{10}\gamma^{10} + \theta_{11}\gamma^{11} + \theta_{12}\gamma^{12} \pmod{P^{13}} \\
& x \equiv 1 + \gamma^4 + \gamma^8 + \theta_9\gamma^9 + \theta_{10}\gamma^{10} + \theta_{11}\gamma^{11} + \theta_{12}\gamma^{12} \pmod{P^{13}}.
\end{aligned}$$

When $p-1 \mid e$ but $p \nmid e$, the β's satisfy only one congruence of degree p and a series of linear congruences, all of which depend upon the value of β_{Γ_0}. In this special case, the system takes a simpler form:

Theorem 15 ([4, p. 50]). *Assume Notation 8. Set* $\Delta = a - eb$, $\Gamma = \frac{e}{p-1}$ *and suppose that* $\Gamma < \Delta$. *If* $p-1 \mid e$ *but* $p \nmid e$, *then the incongruent solutions of* $x^{p^b} \equiv 1 \pmod{P^a}$ *are*

$$x \equiv 1 + \beta_\Gamma\gamma^\Gamma + \ldots + \beta_{\Delta-1}\gamma^{\Delta-1} + \theta_\Delta\gamma^\Delta + \ldots + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_\Delta, \ldots, \theta_{a-1} \in \mathfrak{M}$ *are arbitrary and* $\beta_\Gamma \in \mathfrak{M}$ *satisfies one of the following congruences: either*

$$\beta_\Gamma \equiv 0 \pmod{P} \quad \text{or} \quad (\gamma^\Gamma\beta_\Gamma)^{p-1} \equiv -p \pmod{P^{e+1}}.$$

Moreover, if $\Gamma < \Delta - 1$, *then* $\beta_\Gamma, \ldots, \beta_{\Delta-1} \in \mathfrak{M}$ *satisfy the following system of congruences:*

$$\begin{cases}
p^b\beta_{\Gamma+1}\gamma^{\Gamma+1} \equiv 1 - (1 + \beta_\Gamma\gamma^\Gamma)^{p^b} \pmod{P^{a-(\Delta-\Gamma)+2}} \\
p^b\beta_{\Gamma+2}\gamma^{\Gamma+2} \equiv 1 - (1 + \beta_\Gamma\gamma^\Gamma + \beta_{\Gamma+1}\gamma^{\Gamma+1})^{p^b} \pmod{P^{a-(\Delta-\Gamma)+3}} \\
\qquad\qquad \vdots \\
p^b\beta_{\Delta-1}\gamma^{\Delta-1} \equiv 1 - (1 + \beta_\Gamma\gamma^\Gamma + \ldots + \beta_{\Delta-2}\gamma^{\Delta-2})^{p^b} \pmod{P^a}.
\end{cases}$$

Example 16. *Suppose that* $\mathbb{K} = \mathbb{Q}(\sqrt{6})$. *As one can verify,* $O_\mathbb{K} = \mathbb{Z} + \mathbb{Z}\sqrt{6}$. *We want to solve the congruence*

$$x^9 \equiv 1 \pmod{P^{10}}, \quad \text{where} \quad P = (3, \sqrt{6}).$$

In this case: $a = 10$, $b = 2$ *and* $P^2 = (3)$. *Thus* P *lies above* $p = 3$, *with ramification index* $e = 2$. *Since* $\mathrm{N}P = 3$, *we can choose* $\mathfrak{M} = \{-1, 0, 1\}$ *to be a complete residue system modulo* P. *Here*

$$\Delta = a - eb = 6, \qquad \Gamma = \frac{e}{p-1} = 1, \qquad \Delta - 1 = 5$$

and we may choose $\gamma = \sqrt{6}$. *Since* $p-1 \mid e$ *and* $p \nmid e$, *it follows by Theorem 15 that the solutions are of the form*

$$x \equiv 1 + \beta_1\gamma + \beta_2\gamma^2 + \beta_3\gamma^3 + \beta_4\gamma^4 + \beta_5\gamma^5 + \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 \pmod{P^{10}},$$

where θ_6, θ_7, θ_8 *and* θ_9 *are arbitrary elements from* $\mathfrak{M}$ *and either* $\beta_1 = \beta_2 = \beta_3 = \beta_4 = \beta_5 = 0$ *or* β_1 *satisfies* $(\gamma\beta_1)^2 \equiv -3 \pmod{P^3}$ *and* $\beta_2, \beta_3, \beta_4, \beta_5$ *satisfy the following system of congruences*

$$\begin{cases} 9\gamma^2\beta_2 \equiv 1 - (1+\gamma\beta_1)^9 \pmod{P^7} \\ 9\gamma^3\beta_3 \equiv 1 - (1+\gamma\beta_1+\gamma^2\beta_2)^9 \pmod{P^8} \\ 9\gamma^4\beta_4 \equiv 1 - (1+\gamma\beta_1+\gamma^2\beta_2+\gamma^3\beta_3)^9 \pmod{P^9} \\ 9\gamma^5\beta_5 \equiv 1 - (1+\gamma\beta_1+\gamma^2\beta_2+\gamma^3\beta_3+\gamma^4\beta_4)^9 \pmod{P^{10}}. \end{cases}$$

We first solve:

$$\begin{gathered} (\gamma\beta_1)^2 \equiv -3 \pmod{P^3} \\ 6\beta_1^2 \equiv -3 \pmod{P^3} \\ \Updownarrow \\ 2\beta_1^2 \equiv -1 \pmod{P} \\ -\beta_1^2 \equiv -1 \pmod{P} \\ \beta_1^2 \equiv 1 \pmod{P}. \end{gathered}$$

Hence $\beta_1 \equiv \pm 1 \pmod{P}$. *Assigning* $\beta_1 = 1$ *in the first congruence of the system, and noticing that* $\gamma = \sqrt{6} \in P$, *yields*

$$\begin{gathered} 54\beta_2 \equiv 1 - (1+\sqrt{6})^9 \pmod{P^7} \\ 54\beta_2 \equiv 34560 - 14121\sqrt{6} \pmod{P^7} \\ \Updownarrow \\ 2\beta_2 \equiv -1280 - 523\sqrt{6} \pmod{P} \\ -\beta_2 \equiv -1280 - 523\sqrt{6} \pmod{P} \\ \beta_2 \equiv 1280 \pmod{P} \\ \beta_2 \equiv -1 \pmod{P}. \end{gathered}$$

As one can verify, substituting $\beta_1 = 1$ *and* $\beta_2 = -1$ *into the second congruence of the system gives* $\beta_3 \equiv 0 \pmod{P}$. *Similarly, we can determine the other* β*'s. Continuing this process finally yields the tuple* $(1, -1, 0, -1, -1)$. *Starting from* $\beta_1 = -1$ *will produce the tuple* $(-1, -1, 0, -1, 1)$. *Computing* $1 + \beta_1\gamma + \ldots + \beta_5\gamma^5$ *for all the three tuples gives the following roots*

$$\begin{aligned} x &\equiv 1 + \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 \pmod{P^{10}} \\ x &\equiv 1 + \gamma - \gamma^2 - \gamma^4 - \gamma^5 + \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 \pmod{P^{10}} \\ x &\equiv 1 - \gamma - \gamma^2 - \gamma^4 + \gamma^5 + \theta_6\gamma^6 + \theta_7\gamma^7 + \theta_8\gamma^8 + \theta_9\gamma^9 \pmod{P^{10}}. \end{aligned}$$

where $\theta_i \in \{-1, 0, 1\}$.

7 The tree structure of the p^b-th roots of unity modulo P^a

The results of Theorem 9, Theorem 11 and Theorem 13 help us to understand the structure of the tree corresponding to the p^b-th roots of unity modulo P^a. These theorems describe different levels of the tree. Theorem 9 discusses the initial levels of the tree, namely the first e levels. In these levels the "growth" of the tree is determined by the number $\Delta = [a/p^b]$. Theorem 11 and Theorem 13 discuss further levels of the tree, namely where $e < a$. The structure of the tree for levels $a > e$ depends upon whether $p-1 \nmid e$ or $p-1 \mid e$. In both cases, the number of branches in the initial and intermediate levels gradually increases. This growth "stabilizes" at some point and becomes a fixed pattern. The following theorem asserts that this stabilization occurs when $\frac{e}{p-1} < a - eb$. Recall that we denote $\frac{e}{p-1}$ by Γ_0.

Theorem 17 ([4, p. 55]). *Assume Notation 8. Set $\Delta = a - eb$ and suppose that $\Gamma_0 < \Delta$. Then the following statements hold.*

(a) *If $p-1 \nmid e$, then the incongruent solutions modulo P^a of $x^{p^b} \equiv 1 \pmod{P^a}$ are*

$$x \equiv 1 + \theta_\Delta \gamma^\Delta + \ldots + \theta_{a-1}\gamma^{a-1},$$

where $\theta_\Delta, \ldots, \theta_{a-1} \in \mathfrak{M}$ are arbitrary.

Consequently, the a-th level of the tree corresponding to these solutions contains $(\mathrm{N}P)^{eb}$ vertices. Moreover, only $(\mathrm{N}P)^{eb-1}$ of these vertices have children; specifically, the vertices with children are those where $\theta_\Delta = 0$ and each such vertex has exactly $\mathrm{N}P$ children.

(b) *If $p-1 \mid e$, then the incongruent solutions modulo P^a of $x^{p^b} \equiv 1 \pmod{P^a}$ are*

$$x \equiv 1+\beta_{\Gamma_r}\gamma^{\Gamma_r}+\ldots+\beta_{\Gamma_0}\gamma^{\Gamma_0}+\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1}+\ldots+\beta_{\Delta-1}\gamma^{\Delta-1}+\theta_\Delta\gamma^\Delta+\ldots+\theta_{a-1}\gamma^{a-1},$$

where $\theta_\Delta, \ldots, \theta_{a-1} \in \mathfrak{M}$ are arbitrary, $\beta_{\Gamma_r}, \ldots, \beta_{\Gamma_0} \in \mathfrak{M}$ satisfy the systems in parts (d) or (e) of Theorem 13, respectively, by taking $k = \Delta - 1$, and $\beta_{\Gamma_0+1}, \ldots, \theta_\Delta \in \mathfrak{M}$ uniquely determined by the values $\beta_{\Gamma_r}, \ldots, \beta_{\Gamma_0}$.

Consequently, the a-th level of the tree corresponding to these solutions contains $s(\mathrm{N}P)^{eb}$ vertices, where s is the number of the tuples $(\beta_{\Gamma_r}, \ldots, \beta_{\Gamma_0})$. Moreover, only $s(\mathrm{N}P)^{eb-1}$ of these vertices have children; specifically, those with children are the solutions where $\theta_\Delta = \beta_\Delta$, and each such vertex has exactly $\mathrm{N}P$ children.

Example 18. *To illustrate the fixed pattern described in Theorem 17, let us consider the congruence $x^3 \equiv 1 \pmod{P^a}$ under two different settings: one where $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ and $P = (\sqrt{3})$ and the other where $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ and $P = (\sqrt{-3})$.*

In both settings, $p = 3$, $e = 2$, $b = 1$, so $p-1 \mid e$, $p \nmid e$, $r = 0$, $\Gamma_0 = 1$. In addition, in both settings $\mathfrak{M} = \{-1, 0, 1\}$, so $\mathrm{N}P = 3$. Furthermore, in the first setting we may choose $\gamma = \sqrt{3}$ and in the other $\gamma = \sqrt{-3}$.

First, it can be shown using Theorem 13(A), for both settings, that the solutions of $x^3 \equiv 1 \pmod{P^a}$ *for* $1 \leqslant a \leqslant 3$ *are*

$$\begin{aligned} x &\equiv 1 \pmod{P} \\ x &\equiv 1 + \theta_1\gamma \pmod{P^2} \\ x &\equiv 1 + \theta_1\gamma + \theta_2\gamma^2 \pmod{P^3}, \end{aligned}$$

where $\theta_1, \theta_2 \in \mathfrak{M}$.

Suppose now that $a \geqslant 4$. *Hence* $1 = \Gamma_0 < \Delta = a - 2$; *so by Theorem 15, the incongruent solutions of* $x^3 \equiv 1 \pmod{P^a}$, *in both settings, are*

$$x \equiv 1 + \beta_1\gamma + \beta_2\gamma^2 + \ldots + \beta_{a-3}\gamma^{a-3} + \theta_{a-2}\gamma^{a-2} + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_{a-2}, \theta_{a-1} \in \mathfrak{M}$, $\beta_1 = 0$ *or satisfies*

$$(\gamma\beta_1)^2 \equiv -3 \pmod{P^3} \tag{3}$$

and for $a > 4$, *the rest of the coefficients* $(\beta_2, \ldots\ldots, \beta_{a-3})$ *satisfy the following system of linear congruences which are uniquely solvable.*

$$\begin{cases} 3\beta_2\gamma^2 \equiv 1 - (1 + \beta_1\gamma)^3 \pmod{P^5} \\ 3\beta_3\gamma^3 \equiv 1 - (1 + \beta_1\gamma + \beta_2\gamma^2)^3 \pmod{P^6} \\ \qquad\qquad \vdots \\ 3\beta_{a-3}\gamma^{a-3} \equiv 1 - (1 + \beta_1\gamma + \beta_2\gamma^2 + \ldots + \beta_{a-4}\gamma^{a-4})^3 \pmod{P^a}. \end{cases}$$

Hence, if $a > 4$ *and if* s *is the number of solutions to (3), including* $\beta_1 = 0$, *then the* a*-th level of the tree has* $s(\mathrm{N}P)^{eb} = 9s$ *vertices. Moreover, only* $s(\mathrm{N}P)^{eb-1} = 3s$ *of these vertices have* $\mathrm{N}P = 3$ *children.*

First assume that $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *and* $P = (\sqrt{3})$. *Under these settings,* $P^2 = (3)$ *and* $\gamma^2 = 3$, *so (3) is equivalent to the congruence* $\beta_1^2 \equiv -1 \pmod{P}$. *By testing the elements of* $\mathfrak{M}$, *we find that none of them is a solution to* $\beta_1^2 \equiv -1 \pmod{P}$. *Hence, we conclude that* $\beta_1 = 0$, *so the solutions of* $x^3 \equiv 1 \pmod{P^4}$ *are*

$$x \equiv 1 + \theta_2\gamma^2 + \theta_3\gamma^3 \pmod{P^4},$$

where $\theta_2, \theta_3 \in \mathfrak{M}$. *In particular,* $s = 1$. *If* $a > 4$, *then by substituting* $\beta_1 = 0$ *into the rest of the congruences we obtain that* $\beta_2 = \ldots = \beta_{a-3} = 0$. *Therefore, if* $a > 4$, *the solutions of* $x^3 \equiv 1 \pmod{P^a}$ *in* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *are*

$$x \equiv 1 + \theta_{a-2}\gamma^{a-2} + \theta_{a-1}\gamma^{a-1} \pmod{P^a},$$

where $\theta_{a-2}, \theta_{a-1} \in \mathfrak{M}$ *are arbitrary. Consequently, if* $a > 4$, *then the* a*-th level of the tree corresponding to these solutions has* 9 *vertices. Moreover,* 3 *of these vertices*

have 3 children each. As can be seen, these results are reflected in the tree diagram presented in Figure 7 below.

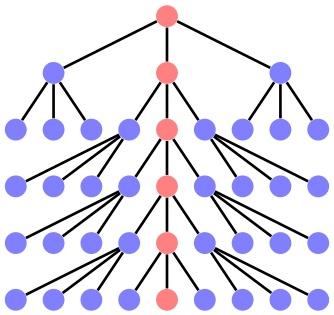


Figure 7

Next, suppose that $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ *and* $P = (\sqrt{-3})$. *Under these settings,* $P^2 = (3)$ *and* $\gamma^2 = -3$. *Hence, the congruence* $(\gamma\beta_1)^2 \equiv -3 \pmod{P^3}$ *is equivalent to* $\beta_1^2 \equiv 1 \pmod{P}$, *so* $\beta_1 = 1$ *or* $\beta_1 = -1$. *Including* $\beta_1 = 0$ *we deduce that the solutions of* $x^3 \equiv 1 \pmod{P^4}$ *are*

$$x \equiv 1 + \theta_1\gamma + \theta_2\gamma^2 + \theta_3\gamma^3 \pmod{P^4},$$

where $\theta_1, \theta_2, \theta_3 \in \mathfrak{M}$.

If $a > 4$, *then the tuples* $(\beta_2, \ldots, \beta_{a-3})$ *are uniquely determined by the choice of* β_1. *Consequently, if* $a > 4$, *then the* a*-th level of the tree corresponding to these solutions has 27 vertices. Moreover, 9 of these vertices have 3 children each. As can be seen, these results are reflected in the tree diagram presented in Figure 8 below.*

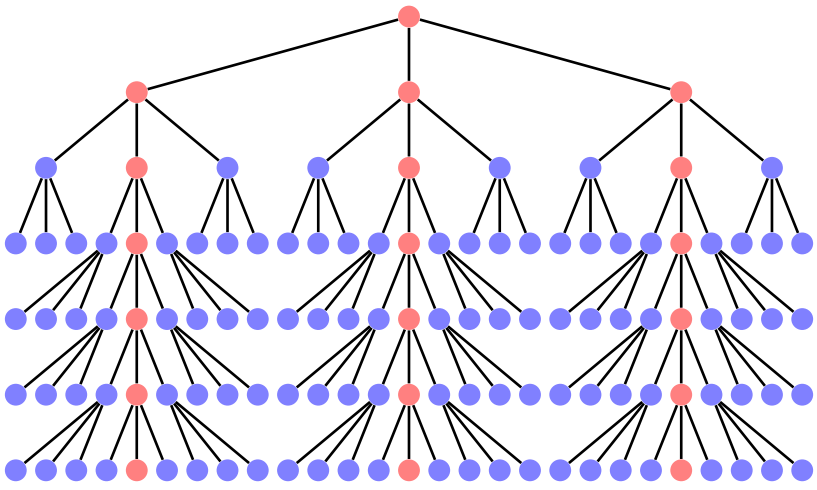


Figure 8

8 The general structure of the P-adic p^b-th roots of unity

We turn now to discuss the results we have obtained from the perspective of P-adic fields. Recall that each infinite "branch" of the tree corresponding to the solutions of $x^{p^b} \equiv 1 \pmod{P^a}$, converges to a solution of $x^{p^b} = 1$ in the P-adic field $\mathbb{K}_P$. As we shall see, when $p-1 \nmid e$ there is only one infinite "branch" and this branch converges to the trivial solution $x = 1$ (see Figures 4 and 7). When $p-1 \mid e$ the tree may have several infinite branches (see Figures 6 and 8). The following theorem characterizes the general structure of the P-adic p^b-th roots of unity.

Theorem 19 ([4, p. 58]). *Assume Notation 8.*

(a) *If $p-1 \nmid e$, then the only P-adic p^b-th root of unity is $x = 1$.*

(b) *If $p-1 \mid e$, then the P-adic p^b-th roots of unity are*

$$x = 1 + \beta_{\Gamma_r}\gamma^{\Gamma_r} + \ldots + \beta_{\Gamma_0}\gamma^{\Gamma_0} + \beta_{\Gamma_0+1}\gamma^{\Gamma_0+1} + \ldots$$

where the β's are in $\mathfrak{M}$ and satisfy the following conditions:

$$\begin{cases} (1 + \beta_{\Gamma_r}\gamma^{\Gamma_r} + \ldots + \beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b} \equiv 1 \pmod{P^{eb+\Gamma_0}} \\ p^b\beta_{\Gamma_0}\gamma^{\Gamma_0} + \binom{p^b}{p}(\beta_{\Gamma_0}\gamma^{\Gamma_0})^p \equiv 1 - (1 + \beta_{\Gamma_r}\gamma^{\Gamma_r} + \ldots + \beta_{\Gamma_0-1}\gamma^{\Gamma_0-1})^{p^b} \pmod{P^{eb+\Gamma_0+1}} \\ p^b\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1} \equiv 1 - (1 + \beta_{\Gamma_r}\gamma^{\Gamma_r} + \ldots + \beta_{\Gamma_0}\gamma^{\Gamma_0})^{p^b} \pmod{P^{eb+\Gamma_0+2}} \\ p^b\beta_{\Gamma_0+2}\gamma^{\Gamma_0+2} \equiv 1 - (1 + \beta_{\Gamma_r}\gamma^{\Gamma_r} + \ldots + \beta_{\Gamma_0+1}\gamma^{\Gamma_0+1})^{p^b} \pmod{P^{eb+\Gamma_0+3}} \\ \quad \vdots \end{cases}$$

if $\Gamma_r < \Gamma_0$, and

$$\begin{cases} \beta_{\Gamma_0} \equiv 0 \pmod{P} \quad \text{or} \quad (\gamma^{\Gamma_0}\beta_{\Gamma_0})^{p-1} \equiv -p \pmod{P^{e+1}} \\ p^b\beta_{\Gamma_0+1}\gamma^{\Gamma_0+1} \equiv 1 - (1 + \beta_{\Gamma_0}\gamma^{\Gamma_0})^{p^b} \pmod{P^{eb+\Gamma_0+2}} \\ p^b\beta_{\Gamma_0+2}\gamma^{\Gamma_0+2} \equiv 1 - (1 + \beta_{\Gamma_0}\gamma^{\Gamma_0} + \beta_{\Gamma_0+1}\gamma^{\Gamma_0+1})^{p^b} \pmod{P^{eb+\Gamma_0+3}} \\ p^b\beta_{\Gamma_0+3}\gamma^{\Gamma_0+3} \equiv 1 - (1 + \beta_{\Gamma_0}\gamma^{\Gamma_0} + \beta_{\Gamma_0+1}\gamma^{\Gamma_0+1} + \beta_{\Gamma_0+2}\gamma^{\Gamma_0+2})^{p^b} \pmod{P^{eb+\Gamma_0+4}} \\ \quad \vdots \end{cases}$$

if $\Gamma_r = \Gamma_0$.

To illustrate Theorem 19, consider the equation $x^9 = 1$ in $\mathbb{K}_P$, where $\mathbb{K} = \mathbb{Q}(\sqrt{6})$ and $P = (3, \sqrt{6})$. Here $p = 3$ and $e = 2$, so $p-1 \mid e$. According to the computation performed in Example 16, it follows that this equation has 3 distinct solutions and that the P-adic expansions of these roots are

$$\begin{aligned} x &= 1 \\ x &= 1 - \gamma - \gamma^2 - \gamma^4 + \gamma^5 + \ldots \\ x &= 1 + \gamma - \gamma^2 - \gamma^4 - \gamma^5 + \ldots \end{aligned}$$

where $\gamma = \sqrt{6}$.

In Theorem 7, we described the number of p^b-th roots of unity in $\mathbb{K}_P$ in the case where $P \| (p)$. In the next theorem we shall provide results for specific ramified cases.

Theorem 20 ([4, p. 61]). *Let $\mathbb{K}$ be a number field, b is a positive integer, P is a prime ideal lying above the rational prime p with ramification index $e \geqslant 2$ and let* N *denote the number of p^b-th roots of unity in $\mathbb{K}_P$. Then, the following statements hold:*

(a) *If $p-1 \nmid e$, then* $\mathrm{N} = 1$.

(b) *If $p-1 \mid e$ but $p \nmid e$, then*

$$\mathrm{N} = \begin{cases} p & \text{if } x^{p-1} \equiv -p \pmod{P^{e+1}} \text{ is solvable} \\ 1 & \text{otherwise.} \end{cases}$$

As we can see, the question of whether the congruence $x^{p-1} \equiv -p \pmod{P^{e+1}}$ is solvable is crucial for determining the structure of the p^b-th roots of unity. Theorem 21 below gives a sufficient condition for the solvability of this congruence.

Theorem 21 ([4, p. 62]). *Let $\mathbb{K}$ be a number field and let P be a prime ideal lying above the prime number p with ramification index e. If $\mathbb{K}$ contains a non-trivial (i.e., $\zeta \neq 1$) complex p-th root of unity ζ, then $x = \zeta - 1$ satisfies the congruence $x^{p-1} \equiv -p \pmod{P^{e+1}}$.*

9 The "concise" form of the n-th roots of unity modulo P^a

Theorem 5 states that if $p \nmid n$, then the incongruent solutions of $x^n \equiv 1 \pmod{P^a}$ are of the form

$$x \equiv \mathfrak{u}_{a-1} \pmod{P^a},$$

where $\mathfrak{u} \in \mathrm{U}_{\mathbb{K}_P^*}(n)$. Recall that $\mathfrak{u}_{a-1}$ denotes the $(a-1)$-th partial sum of the P-adic integer $\mathfrak{u} = \theta_0 + \theta_1\gamma + \theta_2\gamma^2 + \ldots$. Our goal in this section is to express the solutions of $x^n \equiv 1 \pmod{P^a}$ when $p \mid n$ in the same manner, in terms of P-adic expansions. Consider the quantity $a - eb$ and let k be the *unique* non-negative integer such that $m_k < a - eb \leqslant m_{k+1}$. In Section 6, we determined the structure of the solutions of $x^{p^b} \equiv 1 \pmod{P^a}$ according to several cases. These cases were determined by the values of the quantities k, $a - eb$, Γ_0 and Γ_r. Table 1 below summarizes the cases addressed when $p \mid n$.

Table 1

Case 1	Case 2	Case 3	Case 4	Case 5
$2 \leqslant a \leqslant e$	$e < a$ $p-1 \nmid e$	$e < a$ $p-1 \mid e$ $0 \leqslant k < \Gamma_r$	$e < a$ $p-1 \mid e$ $\Gamma_r \leqslant k < \Gamma_0$	$e < a$ $p-1 \mid e$ $\Gamma_0 \leqslant k$

We are now in a position to handle the case of a general exponent n. Theorem 22 below summarizes this discussion and presents the structure of n-th roots of unity modulo P^a for the Cases 1–3 and 5 (excluding Case 4) in terms of P-adic numbers.

Theorem 22 ([5, p. 168]). *Assume Notation 8. In addition, suppose that $a \geqslant 2$, $d = \gcd(n, \mathrm{N}P - 1)$ and let k be the unique non-negative integer such that $m_k < a - eb \leqslant m_{k+1}$. Consider the Cases 1,2,3, and 5 defined in Table 1, and set*

$$\Delta = \begin{cases} \lceil a/p^b \rceil & \text{case } 1 \\ k+1 & \text{cases } 2,3 \\ a-eb & \text{case } 5. \end{cases}$$

If $p \mid n$, then the incongruent solutions of $x^n \equiv 1 \pmod{P^a}$ are of the form

$$x \equiv \mathfrak{u}_{a-1} + \gamma^{\Delta}\mathfrak{t}_{a-\Delta-1} \pmod{P^a},$$

where $\mathfrak{t} \in \mathfrak{M}_{a-\Delta}(\mathcal{O}_P)$ and either $\mathfrak{u} \in \mathrm{U}_{\mathbb{K}_P^*}(d)$ in Cases 1,2,3 or $\mathfrak{u} \in \mathrm{U}_{\mathbb{K}_P^*}(n)$ in Case 5.

Unfortunately, we cannot say much about the structure of solutions in Case 4 in general, due to a lack of information about $\mathrm{U}_{P^a}(p^b)$ in this case. Nevertheless, knowing more about $\mathbb{K}$ and P can be very useful in Case 4, as we shall see in Theorem 23 below, where an explicit analysis for the solutions of certain congruences in the cyclotomic fields of prime degree is provided. Recall that a *cyclotomic field* is the number field $\mathbb{Q}(\zeta_n)$ obtained by adjoining the complex root of unity $\zeta_n := e^{2\pi i/n}$. It can be shown that the ring of integers of $\mathbb{Q}(\zeta_n)$ is $\mathbb{Z}[\zeta_n]$. In addition, if p is a prime number, then $P = (1-\zeta_p)$ is a prime ideal with norm $\mathrm{N}P = p$. Furthermore, the ideal (p) has the factorization $(p) = P^{p-1}$, so the ramification index of P over p is $e = p-1$.

As an illustrative example of our results, we shall give the explicit solutions of the congruences $x^n \equiv 1 \pmod{p}$ and $x^p \equiv 1 \pmod{p^m}$ in the cyclotomic field $\mathbb{Q}(\zeta_p)$, where p is an odd rational prime and m is an arbitrary positive integer.

Theorem 23 ([5, p. 171]). *Suppose that p is an odd rational prime and let $\mathbb{K} = \mathbb{Q}(\zeta_p)$ be the cyclotomic field, where $\zeta_p = e^{2\pi i/p}$ is the primitive p-th root of unity.*

(a) *Given a positive integer n, the solutions of $x^n \equiv 1 \pmod{p}$ over $\mathbb{Z}[\zeta_p]$ are*

$$x \equiv a + t_0(1-\zeta_p) + t_1(1-\zeta_p)^2 + \ldots + t_{p-3}(1-\zeta_p)^{p-2} \pmod{p},$$

where $t_i \in \{0, 1, 2 \ldots, p-1\}$ *and the values of a run over all solutions to* $x^d \equiv 1 \pmod{p}$ *in* $\mathbb{Z}$, *where* $d = \gcd(p-1, n)$. *Consequently, the total number of solutions is* dp^{p-2}.

(b) *Given a positive integer* m, *the solutions to* $x^p \equiv 1 \pmod{p^m}$ *over* $\mathbb{Z}[\zeta_p]$ *are*

$$x \equiv 1 + t_0(1-\zeta_p) + t_1(1-\zeta_p)^2 + \ldots + t_{p-3}(1-\zeta_p)^{p-2} \pmod{p}$$

if $m = 1$, *and*

$$x \equiv \zeta_p^k + p^{m-1}(t_0 + t_1(1-\zeta_p) + t_2(1-\zeta_p)^2 + \ldots + t_{p-2}(1-\zeta_p)^{p-2}) \pmod{p^m}$$

if $m > 1$, *where* $t_i \in \{0, 1, 2 \ldots, p-1\}$ *and* $0 \leqslant k \leqslant p-1$. *Consequently, the total number of solutions is* p^{p-2} *if* $m = 1$, *and* p^p *if* $m > 1$.

Example 24. *We shall illustrate the result of Theorem 23 in detail for* $p = 3$ *and* $m \geqslant 1$, *that is, we shall solve* $x^3 \equiv 1 \pmod{3^m}$ *in the cyclotomic field* $\mathbb{Q}(\zeta_3)$. *In this case we have* $\zeta_3 = \omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\{1, \omega\}$ *is an integral basis for* $\mathbb{Z}[\omega]$, $\langle\omega\rangle = \{1, \omega, \bar{\omega}\}$ *and we may take* $\{-1, 0, 1\}$ *as a complete residue system modulo* $P = (1-\omega)$.

If $m = 1$, *then the solutions to* $x^3 \equiv 1 \pmod{3}$ *are*

$$x \equiv 1 + t(1-\omega) = 1 + t - t\omega \pmod{3},$$

where $t \in \{-1, 0, 1\}$. *Thus* $x \equiv \omega, 1, 2-\omega \pmod{3}$. *But since* $2 - \omega \equiv -1 - \omega = \bar{\omega} \pmod{3}$, *we get the three solutions*

$$x \equiv 1, \omega, \bar{\omega} \pmod{3}.$$

If $m > 1$, *then the solutions to* $x^3 \equiv 1 \pmod{3^m}$ *are*

$$\begin{aligned} x &\equiv 1 + 3^{m-1}(t + s(1-\omega)) \pmod{3^m} \\ x &\equiv \omega + 3^{m-1}(t + s(1-\omega)) \pmod{3^m} \\ x &\equiv \bar{\omega} + 3^{m-1}(t + s(1-\omega)) \pmod{3^m}, \end{aligned}$$

where $t, s \in \{-1, 0, 1\}$. *Using the relation* $\bar{\omega} + \omega + 1 = 0$, *we can reformulate these results as follows*

$$\begin{aligned} x &\equiv \quad 1 + (t+s)3^{m-1} - (3^{m-1}s)\omega \pmod{3^m} \\ x &\equiv \qquad (t+s)3^{m-1} - (3^{m-1}s - 1)\omega \pmod{3^m} \\ x &\equiv -1 + (t+s)3^{m-1} - (3^{m-1}s + 1)\omega \pmod{3^m}, \end{aligned}$$

where $t, s \in \{-1, 0, 1\}$. *The number of solutions in this case is* $3 \cdot 3^2 = 27$.

In particular, for $m = 2$*, the solutions to* $x^3 \equiv 1 \pmod 9$ *over* $\mathbb{Z}[\omega]$ *are*

$$\begin{array}{ccc} 1 & 4 & 7 \\ \omega & 3+\omega & 6+\omega \\ 2+2\omega & 5+2\omega & 8+2\omega \\ 1+3\omega & 4+3\omega & 7+3\omega \\ 4\omega & 3+4\omega & 6+4\omega \\ 2+5\omega & 5+5\omega & 8+5\omega \\ 1+6\omega & 4+6\omega & 7+6\omega \\ 7\omega & 3+7\omega & 6+7\omega \\ 2+8\omega & 5+8\omega & 8+8\omega \end{array}$$

10 Concluding Discussion and Comparative Summary

To conclude this synopsis, it is essential to place the results presented in the preceding sections within the broader context of existing literature. By situating our findings among established research, we highlight how the "lifting and tree" methodology presented here (drawn from [3, 4, 5, 6]) differs from alternative structural, analytic, and geometric approaches in the field.

The traditional approach to p-adic roots, as exemplified by Bachman [1], relies heavily on Hensel's Lemma to establish the existence of solutions in the completion field $\mathbb{K}_P$. While those results provide the theoretical "limit" toward which our infinite branches converge, they do not provide the explicit combinatorial structure of the solutions in the intermediate residue rings. The methodology summarized in this paper provides a constructive, recursive lifting method. This allows for the mapping of every incongruent solution at each level a, providing the "fine structure" of the P-adic expansion that existence proofs generally omit.

Research by Tate and Voloch [10] and Voloch [11] explores p-adic roots of unity primarily within the context of Diophantine geometry and linear forms. Their perspective is metric and geometric, treating roots of unity as points in a valuation field to solve problems related to plane curves and linear forms. In contrast, the work presented here is structural and algorithmic. By representing solutions as rooted trees (as seen in Figures 1–8), we provide a visual and computational framework for understanding how solution bifurcations and patterns of growth are governed specifically by the ramification index e.

A significant point of comparison can be made with the work of Elia et al. [7, 8], who investigated the group structure of units in residue rings to identify isomorphism classes and generators. Furthermore, recent work by Sarkar and Shaikh [9] explores the image of the p-adic logarithm on principal units of p-adic fields. Similar to the investigation presented in this survey, the work of Sarkar and Shaikh deals with the structural properties of cyclotomic fields. However, while their work provides an analytic perspective on the filtration of the unit group through the properties of the

logarithmic map, our survey provides a direct algebraic characterization. Specifically, while the logarithmic approach offers insights into the image of the principal units U_1 within the cyclotomic setting, our Theorems 19 and 22 determine the specific coefficients β_i in the P-adic expansion of the roots themselves. This allows for a granular "coordinate-based" view of the torsion subgroup that complements the analytic mapping of unit groups in cyclotomic extensions.

By bridging the gap between abstract field theory and the concrete group structure of residue rings, this survey offers a complete algorithmic path for determining n-th roots of unity. The characterization of Cases 1 through 5 (Table 1) ensures that regardless of the ramification index or the choice of n, the structure of the solutions is fully accessible through the partial sums of P-adic integers.

Acknowledgement. I would like to express my sincere gratitude to Professor Marcel Herzog for his invaluable guidance and supervision throughout this work. I am also deeply indebted to the late Professor Miriam Cohen, whose insightful suggestion to integrate the four original papers into a comprehensive review article shaped the direction of this project. Special thanks are also due to Professor Dan Levy for his essential role in connecting the participants and facilitating this collaboration.

References

[1] G. Bachman, *p-Adic Numbers and Valuation Theory*, Academic Press, 1964, New York and London. MR169847. Zbl 0192.40103.

[2] Cohen B., *The structure of the n-th roots of unity in Residue rings of prime ideals P over p in Algebraic Number Fields. Part I: n-th roots of unity when* $p \nmid n$, International Mathematical Forum, Vol. **12**, 2017, no. 9, pp. 439-455. DOI: https://doi.org/10.12988/imf.2017.7220.

[3] Cohen B., *The structure of the n-th roots of unity in Residue rings of prime ideals P over p in Algebraic Number Fields. Part II: n-th roots of unity when* $P\|(p)$, International Mathematical Forum, Vol. **12**, 2017, no. 10, pp. 457-468, DOI: https://doi.org/10.12988/imf.2017.7221.

[4] Cohen B., *The structure of the n-th roots of unity in Residue rings of prime ideals P over p in Algebraic Number Fields. Part III: n-th roots of unity when* $n = p^b$, International Mathematical Forum, Vol. **13**, 2018, no. 1, pp. 15-64, DOI: https://doi.org/10.12988/imf.2018.712101.

[5] Cohen B., *The structure of the n-th roots of unity in Residue rings of prime ideals P over p in Algebraic Number Fields. Part IV: n-th roots of unity for general n*, International Mathematical Forum, Vol. **13**, 2018, no. 4, pp. 161-174, DOI: https://doi.org/10.12988/imf.2018.811.

[6] Cohen B., *A Generalization of Bauer's Identical Congruence*, Tokyo J. Math. **44**(2), pp. 515-542, December 2021, MR4379742. Zbl 1537.11006. DOI: https://doi.org/10.3836/tjm/1502179350.

[7] M. Elia, R. Rosenbaum, J.C. Interlando, *On the structure of Residue Rings of Prime Ideals in Algebraic Number Fields - Part I: Unramified Primes*, International Mathematical Forum, **5**(2010), no. 56, 2795-2808.

[8] M. Elia, R. Rosenbaum, J.C. Interlando, *On the structure of Residue Rings of Prime Ideals in Algebraic Number Fields - Part II: Ramified Primes*, International Mathematical Forum, **6**(2011), no. 12, 565-589.

[9] M.A. Sarkar and A.A. Shaikh, *On the image of p-adic logarithm on principal units*, Houston J. Math. **50**(2024), no. 3, 559–591. MR4946537. Zbl 1572.11170.

[10] Tate, J. and Voloch, J.F., *Linear forms in p-adic roots of unity*, International Mathematics Research Notices, (**12**)1996, 589-601, MR1405976. Zbl 0893.11015 DOI: https://doi.org/10.1155/S1073792896000396.

[11] Voloch, J.F., *Plane curves and p-adic roots of unity*, Bulletin of the Australian Mathematical Society, 1999, **60**(3), pp. 479-482, MR1727480. Zbl 0938.11059. DOI: https://doi.org/10.1017/S0004972700036637.

Boaz Cohen, ORCID: https://orcid.org/0009-0004-7641-4522
Department of Computer Science,
The Academic College of Tel-Aviv,
Rabenu Yeruham St., P.O.B 8401 Yaffo, 6818211, Israel.
email: arctanx@gmail.com

License

Received: November 14, 2025; Accepted: April 23, 2026
Published electronically: April 23, 2026