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 \( P \| (p) \)

Boaz Cohen

Department of Pure Mathematics
Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel

Copyright © 2017 Boaz Cohen. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

In this paper we continue the study initiated in Part I of determining the solutions over \( O_K \) of the congruence \( x^n \equiv 1 \pmod{M} \), where \( n \) is an arbitrary positive integer. In this part we shall determine the solutions of the special case \( x^n \equiv 1 \pmod{P^a} \), where \( a \) is a positive integer, \( P \) denotes a prime ideal in \( O_K \) lying over the rational prime number \( p \) such that \( P \| (p) \) and \( n = p^b \).

Mathematics Subject Classification: 11R04, 11Sxx, 11A07

Keywords: Roots of unity, Residue rings, Prime ideals, Algebraic number fields, \( p \)-adic fields

1 Introduction

Let \( K \) be an algebraic number field. Denote by \( O_K \) the ring of integers of \( K \) and by \( M \) an ideal in \( O_K \). In these settings, we denote by \( \mathcal{M}(O_K/M) \) a complete residue system modulo \( M \) (see [1]). Given a prime ideal \( P \), we denote by \( K_P \) the \( p \)-adic number field and by \( O_P \) the ring of \( p \)-adic integers of \( K_P \).
In this paper we continue the study initiated in [1], whose aim is to determine the solutions over \( \mathcal{O}_\mathbb{K} \) of the congruence

\[
x^n \equiv 1 \pmod{\mathbb{M}},
\]

where \( n \) is an arbitrary positive integer.

In Part I we determined the solutions of the congruence \( x^n \equiv 1 \pmod{\mathbb{P}^a} \) for a prime ideal \( \mathbb{P} \), when \( p \nmid n \). We proved that if \( p \nmid n \), then the congruence \( x^n \equiv 1 \pmod{\mathbb{P}^a} \) has exactly \( \gcd(N\mathbb{P}^{a-1}, n) \) incongruent solutions over \( \mathcal{O}_\mathbb{K} \), and that they are of the form

\[
x \equiv a_{a-1} \pmod{\mathbb{P}^a},
\]

where \( a \) runs over the \( \mathbb{P} \)-adic \( n \)-th roots of unity. Here \( a_{a-1} \) denotes the “truncated” \( \mathbb{P} \)-adic expansion of \( a \) of length \( a \). For more details, see Part I of this study.

In this paper we shall determine the solutions of the congruence

\[
x^{p^b} \equiv 1 \pmod{\mathbb{P}^a},
\]

where \( b \) is a non-negative integer and \( \mathbb{P} \parallel p \). 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 the solution of \( x^n \equiv 1 \pmod{\mathbb{P}^a} \) when \( \mathbb{P} \parallel p \) and \( p \mid n \) is not very complicated and will be performed in Part III of this study.

Our main result is the following theorem.

**Theorem 4.3.** Suppose that \( p \) is a rational prime number, \( \mathbb{P} \) is a prime ideal in the algebraic number field \( \mathbb{K} \) lying above \( (p) \), \( a, b \) are integers such that \( a \geq 1, b \geq 0 \) and \( \mathfrak{M} \) is a complete residue system modulo \( \mathbb{P}^{a-\Delta} \), where \( \Delta = \max\{1, a - b\} \). Suppose also that \( \mathbb{P} \parallel (p) \). Then

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

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

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

Another important result deals with the \( \mathbb{P} \)-adic \( n \)-th roots of unity for an arbitrary \( n \). In Part I we proved that if \( p \nmid n \), then the equation \( x^n = 1 \) has exactly \( \gcd(N\mathbb{P} - 1, n) \) distinct roots in \( \mathcal{K}_p \). In this paper we shall go further and give the number of solutions for the equation \( x^n = 1 \) for any \( n \), provided that \( \mathbb{P} \parallel (p) \).

We proved the following theorem.
Theorem 3.2. Let $K$ 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 $K_P$. Set $d = \gcd(NP - 1, n)$. If $P || (p)$, then

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

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

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

We remark that this result generalizes a well known theorem which asserts that the number of the $(p - 1)$-th roots of unity in $Q_p$ is exactly $p - 1$ (see [4, pp. 61–63]).

In this paper the notation and preliminaries summarized of Part I are assumed. Furthermore, we shall use freely results from Part I. For clarity, we shall refer to results from Part I by adding the letter “I” to the number of the result. For example, Theorem I.4.3 refers to Theorem 4.3 of Part I.

2 More results concerning congruences

When considering polynomial congruences, the solutions may be represented in a modulus different from the original one. Nevertheless, it is customary to present the solutions in the original modulus. The transition to the original modulus may produce more solutions. For example, consider the linear congruence $8x \equiv 4 \pmod{12}$ in $\mathbb{Z}$. To find that solution, observe that the original congruence is equivalent to $8x \equiv 16 \pmod{12}$. Since $\gcd(8, 12) = 4$, it follows by Proposition I.2.1(c) that the solution is $x \equiv 2 \pmod{3}$. By going back to the original modulus we get four solutions $x \equiv 2, 5, 8, 11 \pmod{12}$. The transition was made by the following relation known in $\mathbb{Z}$, which is the converse of Proposition I.2.1(a): if $d \mid m$, then

$$x \equiv a \pmod{d} \iff x \equiv a, a + d, a + 2d, \ldots, a + (\frac{m}{d} - 1) d \pmod{m}.$$ 

The following proposition is the generalized version of the above assertion.

Proposition 2.1. Suppose that $A, B$ are nontrivial ideals in the algebraic number field $K$, $\mathfrak{M} = \{\theta_1, \theta_2, \ldots, \theta_{NB}\}$ is a complete residue system modulo $B$ and $\alpha \in O_K$. If $\gamma \in A$ is an algebraic integer such that $\gcd((\gamma), AB) = A$, then

$$x \equiv \alpha \pmod{A} \iff x \equiv \alpha + \gamma \theta_1, \alpha + \gamma \theta_2, \ldots, \alpha + \gamma \theta_{NB} \pmod{AB}.$$ 

Moreover, the numbers $\alpha + \gamma \theta_i$ are incongruent modulo $AB$. 

Proof. If there exists $1 \leq i \leq NB$ such that $x \equiv \alpha + \gamma \theta_i \pmod{AB}$, then by Proposition I.2.1(a), $x \equiv \alpha + \gamma \theta_i \pmod{A}$. But $\gamma \in A$, so $\gamma \equiv 0 \pmod{A}$. Therefore $x \equiv \alpha + \gamma \theta_i \equiv \alpha \pmod{A}$.

Conversely, suppose that $x \equiv \alpha \pmod{A}$, that is $A \mid (x - \alpha)$. Consider the congruence $x - \alpha \equiv \gamma t \pmod{AB}$ with the unknown $t$. Since by our assumptions $\gcd((\gamma), AB) = A$, it follows that $\gcd((\gamma), AB) \mid (x - \alpha)$. Therefore, by Proposition I.2.1(d), there is a solution modulo $AB/A = B$, say $\xi$, for the congruence $x - \alpha \equiv \gamma t \pmod{AB}$. Since $\theta_1, \ldots, \theta_{NB}$ is a complete residue system modulo $B$, there is an index $i$ such that $\xi \equiv \theta_i \pmod{B}$. Hence we may choose $\theta_i$ as a solution of the congruence, so $x - \alpha \equiv \gamma \theta_i \pmod{AB}$ and $x \equiv \alpha + \gamma \theta_i \pmod{AB}$ follows, as desired.

Assuming that $\alpha + \gamma \theta_i \equiv \alpha + \gamma \theta_j \pmod{AB}$, we get that $\gamma \theta_i \equiv \gamma \theta_j \pmod{AB}$. Now, since $\gcd((\gamma), AB) = A$, we deduce by Proposition I.2.1(c) that $\theta_i \equiv \theta_j \pmod{B}$. Therefore, the numbers $\alpha + \gamma \theta_i$ are indeed incongruent modulo $AB$.

We remark that by [3, pp. 69-70] the $\gamma$ of Proposition 2.1 always exists. Next we prove the following lemma, which will be most useful later on.

**Proposition 2.2.** Suppose that $p$ is a prime number and let $t$ be a positive integer such that $p \nmid t$. If $a, b$ are integers such that $0 \leq b \leq a$ and $t \leq p^{a-b}$ then

$$p^{a-b} \parallel \left( \frac{p^a}{p^b t} \right).$$

Proof. If $a = b$, then $t = 1$ and the result certainly holds. So assume that $a > b$. For a positive number $n$ define $\nu_p(n)$ to be the multiplicity of $p$ in $n$, namely $\nu_p(n)$ is the non-negative integer such that $p^{\nu_p(n)} \parallel n$. By [2, pp. 90–91], we know that

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Here the lower square-bracket notation $\lfloor x \rfloor$ denotes the largest integer not exceeding the real number $x$. Hence

$$\nu_p((p^b t)!) = \left\lfloor \frac{p^b t}{p} \right\rfloor + \left\lfloor \frac{p^b t}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{p^b t}{p^{b+1}} \right\rfloor + \left\lfloor \frac{p^b t}{p^{b+2}} \right\rfloor + \ldots$$

$$= (p^{b-1} + p^{b-2} + \ldots + p + 1)t + \left\lfloor \frac{t}{p} \right\rfloor + \left\lfloor \frac{t}{p^2} \right\rfloor + \ldots$$

$$= \frac{p^b - 1}{p - 1} + \nu_p(t!).$$

Now, for a real number $x$ and an integer $n$, we have $\lfloor n + x \rfloor = n + \lfloor x \rfloor$ and $\lfloor -x \rfloor = -1 - \lfloor x \rfloor$ if $x$ is not an integer (see [2, p. 90]). Therefore, as $a > b$,
we get
\[ \nu_p((p^{a-b} - t)!) = \left\lfloor \frac{p^{a-b} - t}{p} \right\rfloor + \left\lfloor \frac{p^{a-b} - t}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{p^{a-b} - t}{p^{a-b}} \right\rfloor = (p^{a-b-1} + \ldots + p + 1) + \left\lfloor \frac{-t}{p} \right\rfloor + \left\lfloor \frac{-t}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{-t}{p^{a-b}} \right\rfloor = \frac{p^{a-b} - 1}{p-1} - \left( \frac{t}{p} \right)_{\text{a-b times}} \left( \left\lfloor \frac{t}{p} \right\rfloor + \left\lfloor \frac{t}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{t}{p^{a-b}} \right\rfloor \right) = \frac{p^{a-b} - 1}{p-1} - (a - b) - \nu_p(t). \]

Observe that the third equality follows from the fact that \( p \nmid t \). From the first formula we deduce that
\[ \nu_p(p^a!) = 1 \cdot \frac{p^a - 1}{p-1} + \nu_p(1) = \frac{p^a - 1}{p-1}, \]
and the first and the second formulas yield:
\[ \nu_p((p^a - p^b t)!) = \nu_p((p^b (p^{a-b} - t))!) = (p^{a-b} - t) \frac{p^b - 1}{p-1} + \nu_p((p^{a-b} - t)!) = (p^{a-b} - t) \frac{p^b - 1}{p-1} + \frac{p^{a-b} - 1}{p-1} - (a - b) - \nu_p(t). \]

Hence
\[ \nu_p \left( \left\lfloor \frac{p^a}{p^b t} \right\rfloor \right) = \nu_p(p^a!) - \nu_p((p^b t)!) - \nu_p((p^a - p^b t)!) = a - b \]
and the proof is complete.

In the next proposition we shall prove the converse of Proposition I.2.2 in the case where \( P \parallel (p) \).

**Proposition 2.3.** Suppose that \( p \) is a rational prime number, \( P \) is a prime ideal in the algebraic number field \( K \) lying above \( (p) \), \( \alpha, \beta \in \mathcal{O}_K \) and \( a, k \) are integers such that \( 1 \leq a \) and \( 0 \leq k \). Suppose also that \( P \parallel (p) \) and that \( \beta \) is invertible modulo \( P \). Then the following statements hold.

(a) if \( p > 2 \), then \( \alpha^k \equiv \beta^k \pmod{P^{a+k}} \implies \alpha \equiv \beta \pmod{P^a} \).

(b) if \( p = 2 \), then \( \alpha^k \equiv \beta^k \pmod{P^{a+k}} \implies \alpha \equiv \pm \beta \pmod{P^a} \).
Proof. First note that it is sufficient to prove the proposition for \( \beta = 1 \). Indeed, suppose that the proposition holds for \( \beta = 1 \) and let \( \alpha^p \equiv \beta^p (\mod P^{a+k}) \). Since \( \beta \) is invertible modulo \( P \), it is also invertible modulo any power of \( P \). Therefore \( (\alpha^{-1})^p \equiv 1 (\mod P^{a+k}) \) and the proposition follows.

(a) We use induction on \( a \). For \( a = 1 \), assume that \( \alpha^p \equiv 1 (\mod P^{a+1}) \). Hence \( \alpha^p \equiv 1 (\mod P) \) and by Proposition I.3.3 we deduce that \( \alpha \equiv 1 (\mod P) \), as desired. Take \( a > 1 \) and assume that the assertion is true for \( 1, 2, \ldots, a-1 \). If \( \alpha^p \equiv 1 (\mod P^{a+k}) \), then \( \alpha^p \equiv 1 (\mod P^{a+k-1}) \), so by the induction hypothesis \( \alpha \equiv 1 (\mod P^{a-1}) \). Hence, there is \( \theta \in P^{a-1} \) such that \( \alpha = 1 + \theta \). Now,

$$\alpha^p = (1 + \theta)^p = 1 + p^k \theta + \sum_{j=2}^{p^k} \binom{p^k}{j} \theta^j.$$ 

We shall prove now that \( \binom{p^k}{j} \theta^j \equiv 0 (\mod P^{a+k}) \) for every \( 2 \leq j \leq p^k \). Suppose that \( 2 \leq j \leq p^k \) and let \( t \) be the non-negative integer such \( p^t \| j \). By Proposition 2.2, \( p^{k-t}\| \binom{p^k}{j} \). In addition, since \( P \| (p) \) and \( P^{j(a-1)} | (\theta)^j \), we conclude that

$$\binom{p^k}{j} \theta^j \equiv 0 (\mod P^{k-t+j(a-1)}) \cdot$$

It suffices to show that \( a + k \leq k - t + j(a - 1) \), that is \( a + t \leq j(a - 1) \). If \( t = 0 \), then \( a \leq 2(a - 1) \leq j(a - 1) \) since \( a \geq 2 \), as required. So assume that \( t > 0 \). First note that by the Bernoulli inequality

$$t = (t + 1) - 1 \leq 2^t - 1 = 2^t + 1 - 2 \leq (2 + 1)^t - 2 \leq p^t - 2.$$ 

Now, since \( a \geq 2 \) and \( t > 0 \), we get

$$a + t \leq a - 2 + p^t \leq (a - 2)p^t + p^t = (a - 1)p^t \leq (a - 1)j,$$

as desired. Thus \( \alpha^{p^k} \equiv 1 + p^k \theta (\mod P^{a+k}) \). On the other hand, by the assumption, \( \alpha^{p^k} \equiv 1 (\mod P^{a+k}) \), so \( p^k \theta \equiv 0 (\mod P^{a+k}) \). Since \( P \| (p) \), we have \( \gcd((p^k, P^{a+k}) = P^k \), so by Proposition I.2.1(c), we conclude that \( \theta \equiv 0 (\mod P^a) \). Thus \( \alpha = 1 + \theta \equiv 1 (\mod P^a) \), as desired.

(b) First note that for \( k = 0 \) the assertion is trivial, so we may assume that \( k > 0 \). We use induction on \( a \). If \( a = 1 \), then the assertion follows exactly as in the odd case, namely \( \alpha \equiv 1 (\mod P) \). If \( a = 2 \), assume that \( \alpha^{2^k} \equiv 1 (\mod P^{k+2}) \). Hence \( \alpha^{2^k} \equiv 1 (\mod P^{k+1}) \) and from the case \( a = 1 \) we deduce that \( \alpha \equiv 1 (\mod P) \). Thus, there is \( \theta \in P \) such that \( \alpha = 1 + \theta \). If \( P^2 \| (\theta) \), then \( \alpha = 1 + \theta \equiv 1 (\mod P^2) \) and we are done. So suppose that \( P \| (\theta) \).
Note that
\[
\alpha^{2^k} = (1 + \theta)^{2^k} = \begin{cases} 
1 + 2^k \theta + \left(\frac{2^k}{2}\right) \theta^2 & k = 1 \\
1 + 2^k \theta + \left(\frac{2^k}{2}\right) \theta^2 + \sum_{j=3}^{2^k} \left(\frac{2^k}{j}\right) \theta^j & k > 1.
\end{cases}
\]

First we shall prove that if \( k > 1 \), then \( \left(\frac{2^k}{j}\right) \theta^j \equiv 0 \pmod{P^{k+2}} \) for every \( 3 \leq j \leq 2^k \). Suppose that \( 3 \leq j \leq 2^k \) and let \( t \) be the non-negative integer such that \( 2^t \| j \). By Proposition 2.2, \( 2^{k-t} \| \left(\frac{2^k}{j}\right) \). In addition, since \( P \| (2) \) and \( P^j \mid (\theta)^j \), we conclude that
\[
\left(\frac{2^k}{j}\right) \theta^j \equiv 0 \pmod{P^{k-t+j}}.
\]

It suffices to show that \( k + 2 \leq k - t + j \), that is \( t + 2 \leq j \). Indeed, if \( 0 \leq t \leq 1 \), then clearly \( 2 + t \leq 3 \leq j \). If \( t \geq 2 \), then
\[
t + 2 = (1 + (t - 1)) + 2 \leq 2t - 1 + 2 \leq 2t - 1 + 2t - 1 = 2^t - 1 = 2^t \leq j.
\]

Thus \( \alpha^{2^k} \equiv 1 + 2^k \theta + 2^{k-1}(2^k - 1)\theta^2 \pmod{P^{k+2}} \) for every \( k \geq 1 \). On the other hand, by the assumption, \( \alpha^{2^k} \equiv 1 \pmod{P^{k+2}} \), so \( 2^{k-1} \theta(2 + (2^k - 1)\theta) \equiv 0 \pmod{P^{k+2}} \). Since \( P \| (2) \) and \( P \| (\theta) \), it follows that \( \gcd((2^{k-1} \theta), P^{k+2}) = P^k \).

Therefore, by Proposition I.2.1(c), we deduce that \( 2 + (2^k - 1)\theta \equiv 0 \pmod{P^2} \). Assigning \( \theta = \alpha - 1 \) yields \( 2 + (2^k - 1)(\alpha - 1) \equiv 0 \pmod{P^2} \), that is \( (2^k - 1)\alpha \equiv 2^k - 3 \pmod{P^2} \). If \( k = 1 \), then \( \alpha \equiv -1 \pmod{P^2} \). If \( k \geq 2 \), then \( P^2 \mid (2^k) \) so \( -\alpha \equiv -3 \pmod{P^2} \), that is \( \alpha \equiv 3 \pmod{P^2} \). Notice that \( P^2 \mid (4) \), so \( 3 \equiv -1 \pmod{P^2} \) and we get that \( \alpha \equiv -1 \pmod{P^2} \), as desired.

Take now \( a > 2 \) and assume that the assertion is true for \( 1, 2, \ldots, a - 1 \). If \( \alpha^{2^k} \equiv 1 \pmod{P^{a+k}} \), then \( \alpha^{2^k} \equiv 1 \pmod{P^{a+k-1}} \), so by the induction hypothesis \( \alpha \equiv \pm 1 \pmod{P^{a-1}} \). Hence there is \( \theta \in \mathbb{P}^{a-1} \) such that either \( \alpha = 1 + \theta \) or \( \alpha = -1 + \theta \). Since \( k > 0 \), we get
\[
\alpha^{2^k} = (\pm 1 + \theta)^{2^k} = 1 \pm 2^k \theta + \sum_{j=2}^{2^k} (\pm 1)^j \left(\frac{2^k}{j}\right) \theta^j.
\]

We shall prove now that \( \left(\frac{2^k}{j}\right) \theta^j \equiv 0 \pmod{P^{a+k}} \) for every \( 2 \leq j \leq 2^k \). Suppose that \( 2 \leq j \leq 2^k \) and let \( t \) be the non-negative integer such that \( 2^t \| j \). By Proposition 2.2, \( 2^{k-t} \| \left(\frac{2^k}{j}\right) \). In addition, since \( P \| (2) \) and \( P^{j(a-1)} \| (\theta)^j \), we conclude that
\[
\left(\frac{2^k}{j}\right) \theta^j \equiv 0 \pmod{P^{k-t+j(a-1)}}.
\]
It suffices to show that \( a + k \leq k - t + j(a - 1) \), that is \( a + t \leq j(a - 1) \). If \( 0 \leq t \leq 1 \), then \( a + t \leq a + 1 \leq 2(a - 1) \leq j(a - 1) \) since \( a \geq 3 \), as required. If \( 2 \leq t \), then as shown above \( t + 2 \leq 2^t \), so again

\[
a + t = (a - 1) + (t + 1) \leq (a - 1) + 2^t - 1 \leq (a - 1) + (a - 1)(2^t - 1) = 2^t(a - 1) \leq j(a - 1).
\]

Thus \( \alpha^{2^k} \equiv 1 \pm 2^k \theta \pmod{P^{a + k}} \). On the other hand, by the assumption, \( \alpha^{2^k} \equiv 1 \pmod{P^{a + k}} \), so \( 2^k \theta \equiv 0 \pmod{P^{a + k}} \). Since \( P \parallel (2) \), it follows that \( \gcd(2^k, P^{k + a}) = P^k \), so by Proposition I.2.1(c), we conclude that \( \theta \equiv 0 \pmod{P^a} \). Thus \( \alpha \equiv \pm 1 + \theta \equiv \pm 1 \pmod{P^a} \), as desired.

It should be noted that if \( a > 1 \), then Proposition 2.3 may be invalid if \( \beta \) is not invertible modulo \( P \), since for instance \( 3^3 \equiv 6^3 \pmod{27} \) in \( \mathbb{Z} \) but \( 3 \not\equiv 6 \pmod{9} \).

### 3 The number of \( P \)-adic \( n \)-th roots of unity when \( p \nmid P \)

It is well known that the equation \( x^{p-1} = 1 \) has exactly \( p - 1 \) distinct roots in the \( p \)-adic field \( \mathbb{Q}_p \) (see [4, pp. 61–63]). In Theorem I.4.3 we proved that if \( p \nmid n \), then the equation \( x^n = 1 \) has exactly \( \gcd(NP - 1, n) \) distinct roots in the \( P \)-adic field \( \mathbb{K}_P \). Since \( \mathbb{Q}_p \) is obtained by taking \( \mathbb{K} = \mathbb{Q}, P = (p) \), it follows that this assertion is clearly a generalization of the above claim. In this section we shall go further and give the number of solutions for the equation \( x^n = 1 \) for any \( n \), provided that \( P \parallel (p) \). First we prove the following proposition.

**Proposition 3.1.** Let \( K \) be a number field, \( P \) be a prime ideal lying above the rational prime \( p \), \( a \in \mathcal{O}_P \) and \( k \) a positive integer. Suppose that \( P \parallel (p) \). Then

(a) if \( p > 2 \), then \( a^{p^k} = 1 \iff a = 1 \).

(b) if \( p = 2 \), then \( a^{2^k} = 1 \iff \) either \( a = 1 \) or \( a = -1 \).

**Proof.** (a) If \( a = 1 \), then clearly \( a^{p^k} = 1 \). Conversely, suppose that \( a^{p^k} = 1 \), \( a \in \mathcal{O}_P \). By Proposition I.2.6, there is a sequence \( (\alpha_n) \) in \( \mathcal{O}_K \) such that \( \alpha_n \equiv a \pmod{P^n} \) for each \( n \). In particular \( \alpha_{n+k} \equiv a \pmod{P^{n+k}} \) for each \( n \). Thus

\[
\alpha_{n+k}^{p^k} \equiv a^{p^k} \equiv 1 \pmod{P^{n+k}}.
\]

Now, \( P \parallel (p) \), so by Proposition 2.3(a) we deduce that \( \alpha_{n+k} \equiv 1 \pmod{P^n} \) for each \( n \). Therefore, by Proposition I.2.5, \( \alpha_{n+k} \to 1 \) when \( n \to \infty \). But \( \alpha_{n+k} \to a \) when \( n \to \infty \) and by the uniqueness of limits we conclude that \( a = 1 \), as desired.
(b) If \( a = 1 \) or \( a = -1 \), then clearly \( a^{2k} = 1 \). Conversely, suppose that \( a^{2k} = 1 \). As in part (a), let \( (\alpha_n) \) be a sequence in \( O_K \) such that \( \alpha_n \to a \). Then \( \alpha_{n+k}^2 \equiv 1 \pmod{P^{n+k}} \) and by Proposition 2.3(b) we deduce that either \( \alpha_{n+k} \equiv 1 \pmod{P^n} \) or \( \alpha_{n+k} \equiv -1 \pmod{P^n} \). Since \( (\alpha_n) \) converges, there is \( n_0 \) such that for every \( n \geq n_0 \) we get \( \alpha_{n+k} \equiv 1 \pmod{P^n} \) or for every \( n \geq n_0 \) we get \( \alpha_{n+k} \equiv -1 \pmod{P^n} \). As in part (a), by Proposition I.2.5 we conclude that either \( a = 1 \) or \( a = -1 \).

**Theorem 3.2.** Let \( K \) 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 \( K_P \). Set \( d = \gcd(NP - 1, n) \). If \( P \| (p) \), then

\[
N = \begin{cases} 
  d & \text{if } p = 2 \text{ and } 2 \nmid n \\
  2d & \text{if } p = 2 \text{ and } 2 \mid n \\
  d & \text{if } p > 2 
\end{cases}
\]

**Proof.** If \( p = 2 \) but \( 2 \nmid n \), then by Theorem I.4.3 the equation \( x^n = 1 \) has \( N = \gcd(NP - 1, n) = d \) solutions, as desired.

Now let \( k \) be the non-negative integer such that \( p^k \| n \). Suppose that \( p = 2 \) and \( 2 \mid n \). Then \( k \geq 1 \) and if \( x \in O_P \), then Proposition 3.1 yields

\[
x^n = 1 \\
\uparrow \\
(x^{n/2^k})^{2^k} = 1 \\
\downarrow \\
\text{either } x^{n/2^k} = 1 \text{ or } x^{n/2^k} = -1 \\
\uparrow \\
\text{either } x^{n/2^k} = 1 \text{ or } (-x)^{n/2^k} = 1.
\]

Note that the last step follows from the fact that \( n/2^k \) is odd. By Theorem I.4.3 the equation \( y^{n/2^k} = 1 \) has \( \gcd(n/2^k, NP - 1) \) solutions in \( K_P \). But since \( 2 \nmid NP - 1 \), this number of solutions is actually \( \gcd(n, NP - 1) = d \). Now, if \( a \) is one of them, then by the above equivalence, also \( (-a) \) needs to be counted. Moreover, if \( a \) and \( b \) are different solutions of \( y^{n/2^k} = 1 \), then \( a \neq -b \) since otherwise

\[1 = a^{n/2^k} = (-b)^{n/2^k} = -b^{n/2^k} = -1,
\]

a contradiction. Hence the number of solutions is \( 2d \). Suppose finally, that \( p > 2 \) and \( x \in O_P \). By Proposition 3.1

\[
x^n = 1 \\
\uparrow \\
(x^{n/p^k})^{p^k} = 1 \\
\downarrow \\
x^{n/p^k} = 1.
\]
Since \( p \) does not divide \( n/p^k \), Theorem I.4.3 implies that the equation \( x^{n/p^k} = 1 \) has \( \gcd(n/p^k, NP - 1) \) solutions in \( K_P \). But \( p^k \) and \( NP - 1 \) are relatively prime, so \( \gcd(n/p^k, NP - 1) = d \) and the proof is complete. \( \square \)

**Corollary 3.3.** Suppose that \( p \) is a prime number, \( n \) is a positive integer and \( N \) is the number of \( n \)-th roots of unity in \( Q_p \). Then

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

As we shall see in Part III to come, Theorem 3.2 may be false if \( P \) is a ramified ideal. This occurs, for instance, if \( K = Q(\sqrt{6}) \), \( p = 3 \) and \( P = (3, \sqrt{6}) \). Here \( P^2 = (3) \), so \( NP = 3 \) and \( P \) is ramified. In this case, it can be shown that the equation \( x^3 = 1 \) has at least one non-trivial root in \( K_P \), while \( d = \gcd(NP - 1, 9) = 1 \). Moreover, its roots are:

\[
x = 1 \\
x = 1 - \gamma - \gamma^2 - \gamma^4 + \gamma^5 + \ldots \\
x = 1 + \gamma - \gamma^2 - \gamma^4 - \gamma^5 + \ldots
\]

where \( \gamma = \sqrt{6} \). For more details see Part III of this study.

## 4 Solving \( x^{pb} \equiv 1 \pmod{P^a} \) when \( P \| (p) \)

In this and in the next paper we shall discuss the solutions of the congruence \( x^n \equiv 1 \pmod{P^a} \) in the case when \( p \mid n \). Practically, it is enough to focus on the case where \( n = pb, b \geq 1 \). The transition to the general solution is then not very complicated and will be performed in Part III of this study.

We return now to the problem of solving \( x^{pb} \equiv 1 \pmod{P^a} \), when \( P \| (p) \).

**Proposition 4.1.** Suppose that \( p \) is a rational prime number, \( P \) is a prime ideal in the algebraic number field \( K \) lying above \( (p) \), \( a, b \) are integers such that \( 0 \leq b < a \) and \( M \) is a complete residue system modulo \( P^b \). Suppose also that \( P \| (p) \). Then

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

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

(c) If \( p = 2 \) and \( a - b > 1 \), then the congruence \( x^{2b} \equiv 1 \pmod{P^a} \) has exactly \( 2(NP)^b \) incongruent solutions \( x \equiv \pm 1 + 2^{a-b} \theta \pmod{P^a} \), where \( \theta \in M \).
Proof. (a) By Proposition 2.3(a) and Proposition I.2.2 the congruence $x^{pb} \equiv 1 \pmod{P^a}$ is equivalent to the congruence $x \equiv 1 \pmod{P^{a-b}}$. By Proposition 2.1 the latter congruence is equivalent to the congruence $x \equiv 1 + \gamma \theta \pmod{P^a}$, where $\theta \in \mathfrak{M}$ and $\gamma$ satisfies $\gcd((\gamma), P^a) = P^{a-b}$. Since $P\parallel (p)$, it follows that $P^{a-b}\parallel (p^{a-b})$, so if we choose $\gamma = p^{a-b}$, we get $\gcd((\gamma), P^a) = P^{a-b}$. Therefore, the solutions are exactly $x \equiv 1 + p^{a-b} \theta \pmod{P^a}$, where $\theta \in \mathfrak{M}$. Note that this provides us with $N(P^b) = (NP)^b$ incongruent solutions.

(b) Using the same arguments we conclude that the congruence $x^{2b} \equiv 1 \pmod{P^a}$ is equivalent to the congruence $x \equiv \pm 1 \pmod{P^{a-b}}$. Now, if $a-b = 1$, then $-1 \equiv 1 \pmod{P^{a-b}}$, so the latter congruence is actually $x \equiv 1 \pmod{P^{a-b}}$, which is equivalent to $x \equiv 1 + 2\theta \pmod{P^a}$, where $\theta \in \mathfrak{M}$. Note that also in this case we obtain $(NP)^b$ incongruent solutions.

(c) Similarly, the congruence $x^{2b} \equiv 1 \pmod{P^a}$ is equivalent to the congruence $x \equiv \pm 1 \pmod{P^{a-b}}$, which is equivalent to $x \equiv \pm 1 + 2^{a-b} \theta \pmod{P^a}$, as desired. To show that we have exactly $2(NP)^b$ incongruent solutions, it is sufficient to prove that it is impossible to find $\theta_1, \theta_2 \in \mathfrak{M}$ such that $1 + 2^{a-b} \theta_1 \equiv -1 + 2^{a-b} \theta_2 \pmod{P^a}$. Assume otherwise. Since $a-b > 1$, we get $P^2 \mid (2)^{a-b}$ and $a \geq 2$. Reducing our congruence modulo $P^2$ yields $1 \equiv -1 \pmod{P^2}$. But then $P^2 \mid (2)$, a contradiction. \hfill \Box

Our goal now is to generalize this proposition for all $a \geq 1$ and $b \geq 0$, without any restriction. To do so, we need the following proposition:

**Proposition 4.2.** Suppose that $p$ is a rational prime number, $P$ is a prime ideal in the algebraic number field $K$ lying above $(p)$ and $a, b$ are integers such $a \geq 1$ and $b \geq 0$. Set $c = \min\{b, a-1\}$. Then

$$x^{pb} \equiv 1 \pmod{P^a} \iff x^{pc} \equiv 1 \pmod{P^a}.$$  

**Proof.** If $c = b$, then the assertion is trivial, so suppose that $c = a - 1$. If $x^{pc} \equiv 1 \pmod{P^a}$, then raising both sides to the $P^{b-c}$-power yields $(x^{pc})^{b-c} \equiv 1^{b-c} \pmod{P^a}$, that is $x^{pb} \equiv 1 \pmod{P^a}$. Conversely, if $x^{pb} \equiv 1 \pmod{P^a}$, then clearly $x^{pc} \equiv 1 \pmod{P^a}$ and by Proposition I.3.2 $x \equiv 1 \pmod{P}$. Thus, by Proposition I.2.2, we get $x^{pa-1} \equiv 1 \pmod{P^a}$, as desired. \hfill \Box

**Theorem 4.3.** Suppose that $p$ is a rational prime number, $P$ is a prime ideal in the algebraic number field $K$ lying above $(p)$, $a, b$ are integers such that $a \geq 1$, $b \geq 0$ and $\mathfrak{M}$ is a complete residue system modulo $P^{a-\Delta}$, where $\Delta = \max\{1, a-b\}$. Suppose also that $P\parallel (p)$. Then

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

Proof. If \( c = \min\{b, a - 1\} \), then \( c = a - \Delta \). Now, by Proposition 4.2, the congruence \( x^{p^b} \equiv 1 \pmod{P^a} \) is equivalent to the congruence \( x^{p^{a-\Delta}} \equiv 1 \pmod{P^a} \). Since \( 0 \leq a - \Delta < a \), we may apply Proposition 4.1 to obtain the required result.

Theorem 3.2 claims that if \( P \parallel (p) \), then the solutions of \( x^{p^b} = 1 \) in \( K_P \) are \( x = \pm 1 \) if \( p = 2 \), and \( x = 1 \) if \( p > 2 \). Note that these results are consistent with the result of Theorem 4.3. 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 get \( p^{a-b} \to 0 \) and therefore \( x = 1 \), as expected.

References


Received: February 28, 2017; Published: March 21, 2017