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 $p \nmid n$

Boaz Cohen

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

Abstract

This paper is the first of a series of papers in which we shall determine the solutions over the ring of integers $\mathcal{O}_K$ of the congruence $x^n \equiv 1 \pmod{M}$, where $M$ is an ideal in $\mathcal{O}_K$ and $n$ is a positive integer. This paper deals with the solutions of $x^n \equiv 1 \pmod{P^a}$, where $a$ is a positive integer, $P$ denotes a prime ideal in $\mathcal{O}_K$ lying over the rational prime number $p$ and $p \nmid n$.

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 $\mathcal{O}_K$ the ring of integers of $K$ and by $M$ an ideal in $\mathcal{O}_K$. The group of units of the residue ring $\mathcal{O}_K/M$ will be denoted by $(\mathcal{O}_K/M)^*$. The multiplicative structure of residue rings of number fields had been researched extensively, with different aims and scope. See for example the
book [1] of H. Hasse and the papers [2] and [3] by M. Elia, R. Rosenbaum and J.C. Interlando. In this paper we are interested in the structure of certain subsets of \((O_K/M)^*\). Let \(n\) denote a positive integer. The subsets which we shall consider are representatives of \(n\)-th roots of unity in \((O_K/M)^*\). We shall denote the \(n\)-th roots of unity subgroup of \((O_K/M)^*\) by

\[ U_M(n) := \{[x]_M : x \in O_K, \ x^n \equiv 1 \pmod{M}\}. \]

This paper is the first of a series of papers in which we shall determine the solutions over \(O_K\) of the congruence

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

Moreover, using our results, we shall derive comprehensive generalizations of the theorem of Bauer (see Hardy and Wright [7], Theorems 126–127) and of a theorem of Wolstenholme (see Theorem 115 in [7]).

The determination of the solutions of \(x^n \equiv 1 \pmod{M}\) over \(O_K\) will be performed in two steps. First we shall consider the solutions of the congruences

\[ x^n \equiv 1 \pmod{P^a}, \]

where \(P\) denotes a prime ideal in \(O_K\) lying over the rational prime number \(p\) and \(a\) is a positive integer, and then we shall describe the solutions for a general \(M\).

The determination of the solutions of \(x^n \equiv 1 \pmod{P^a}\) will also require several steps. This paper deals with the first case: we assume that the prime number \(p\) does not divide \(n\). Later we shall consider the congruences

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

where \(b\) is a positive integer. Here we shall deal separately with the cases \(P \mid (p)\) and \(P^2 \mid (p)\). Finally, we shall describe the solutions for an arbitrary \(n\).

This paper deals with the solutions of \(x^n \equiv 1 \pmod{P^a}\), when \(p \not\mid n\). One of our main results is Theorem 4.1 in which we prove that if \(p \not\mid n\), then

\[ U_P(n) \cong U_{P^a}(n) \]

for every positive integer \(a\), and that this isomorphism is given by the map

\[ [x]_P \mapsto [x^{NP^{a-1}}]_{P^a}. \]

Here \(NP\) denotes the norm of \(P\).

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 \(Z\).
for $a \in \{1, 2, 3, 4\}$. Here $n = 3$, $p = 7$, $P = (7)$, so $p \nmid n$ and $NP = 7$. We start by noticing that the solutions of $x^3 \equiv 1 \pmod{7}$ are $x \equiv 1, 2, 4 \pmod{7}$. By the above map, it follows that the solutions of $x^3 \equiv 1 \pmod{7^2}$ are $x \equiv 1^7, 2^7, 4^7 \pmod{7^2}$, that is $x \equiv 1, 30, 18 \pmod{7^2}$. Next, the solutions of $x^3 \equiv 1 \pmod{7^3}$ are $x \equiv 1^7, 30^7, 18^7 \pmod{7^3}$, that is $x \equiv 1, 324, 18 \pmod{7^3}$ and finally, the solutions of $x^3 \equiv 1 \pmod{7^4}$ are $x \equiv 1^7, 324^7, 18^7 \pmod{7^4}$, that is $x \equiv 1, 1353, 1047 \pmod{7^4}$.

In Section 4, in the discussion to follow we go further and prove deeper results, which describe the $n$-th roots of unity modulo $P$ within the framework of the $P$-adic number field $K_P$. The field $K_P$ is constructed similarly to the $p$-adic field $Q_p$, using the completion process, relative to the valuation $|x|_P := p^{-\ord_P(x)}$ defined on $K$, where $\ord_P(x)$ is the integer satisfying $P^{\ord_P(x)} \| (x)$. As in the field $Q_p$, given an element $\gamma \in P \setminus P^2$, every $P$-adic integer $a$ has a $P$-adic expansion of the form

$$a = a_0 + a_1 \gamma + a_2 \gamma^2 + \ldots,$$

where the $a_i \in O_K$ are uniquely determined modulo $P$.

Using the terminology of $P$-adic numbers, Theorem 4.3 asserts that if $p \nmid n$, then

$$U_{K_P}^*(n) \cong U_P(n)$$

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

$$\psi : U_P(n) \to U_{K_P}^*(n) \quad \text{or} \quad \nu : U_{K_P}^*(n) \to U_P(n)$$

$$[x]_P \mapsto \lim_{k \to \infty} x^{NP^k-1} \quad \text{or} \quad x \mapsto [x]_P$$

Here $U_{K_P}^*(n)$ denotes the subgroup of $n$-th roots of unity in the field $K_P$, that is $U_{K_P}^*(n) := \{ x \in K_P : x^n = 1 \}$. In addition, using this isomorphism, we shall prove that when $p \nmid n$, the equation $x^n = 1$ has exactly $\gcd(NP - 1, n)$ incongruent solutions in $K_P$. Our final result is the following theorem:

**Theorem 4.4.** Suppose that $p$ is a rational prime number, $P$ is a prime ideal in the algebraic number field $K$ lying above $(p)$ and $n$ is a positive integer. If $p \nmid n$, then

$$U_{K_P}^*(n) \cong U_{P^a}(n)$$

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 $\gcd(NP - 1, n)$ incongruent solutions over $O_K$ and they are of the form

$$x \equiv a_{a-1} \pmod{P^a},$$

where $a \in U_{K_P}^*(n)$. 

Here \( a_{a-1} \) denotes the “truncated” \( P \)-adic expansion of \( a \), that is \( a_{a-1} := \alpha_0 + \alpha_1 \gamma + \ldots + \alpha_{a-1} \gamma^{a-1} \).

As an illustrative example, let us consider again the congruence \( x^3 \equiv 1 \) (mod \( 7^a \)) over \( \mathbb{Z} \). As one can verify, one of the solutions of the equation \( x^3 = 1 \) in the field \( Q_7 \) begins with the following expansion

\[
x = 2 + 4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^3 + \ldots
\]

Truncating this solutions yields the solutions \( x \equiv 2 \) (mod 7), \( x \equiv 30 \) (mod \( 7^2 \)), \( x \equiv 324 \) (mod \( 7^3 \)) and \( x \equiv 1353 \) (mod \( 7^4 \)) for \( a \in \{1, 2, 3, 4\} \), respectively. As we can see, these results are consistent with the result which we obtained before.

# 2 Preliminaries

The following two subsections survey and summarize the basic facts and notation concerning the theory of congruences and the theory of \( P \)-adic numbers, which are required for this paper and for the companion papers.

## 2.1 General results concerning congruences

In this section we intend to expand the concept of congruences from the perspective of general residue rings. Let \( M \) be an (integral) ideal in an algebraic number field \( K \) and let \( \alpha, \beta \in \mathcal{O}_K \). If \( \alpha - \beta \in M \) or equivalently, if \( M \mid (\alpha - \beta) \), then we write \( \alpha \equiv \beta \) (mod \( M \)), and say that \( \alpha \) is congruent to \( \beta \) modulo \( M \).

Note that if we denote the element \( \alpha + M \) of the quotient ring \( \mathcal{O}_K / M \) by \([\alpha]_M\) (or \([\alpha] \) in short), then the statement “\( \alpha \) is congruent to \( \beta \) modulo \( M \)” is expressed as the equality \([\alpha] = [\beta]\). Notice that if \( M = (1) \), then \( \alpha \equiv \beta \) (mod \( M \)) iff \( \alpha - \beta \in \mathcal{O}_k \), which is trivial since \( \alpha, \beta \in \mathcal{O}_K \). If \( M = (0) \), then \( \alpha \equiv \beta \) (mod \( M \)) iff \( \alpha = \beta \).

In the next proposition we gather several basic properties of congruences. The proofs of these properties are similar to those in the basic case of congruences in \( \mathbb{Z} \) and therefore will be omitted (see [5, pp. 62–74]).

**Proposition 2.1.** Suppose that \( M \) is an ideal in an algebraic number field \( K \) and let \( \alpha, \beta \in \mathcal{O}_K \). Then

(a) If \( \alpha \equiv \beta \) (mod \( M \)) and \( D \mid M \), then \( \alpha \equiv \beta \) (mod \( D \)).

(b) If \( f(x) \) is a polynomial over \( \mathcal{O}_K \) and \( \alpha \equiv \beta \) (mod \( M \)), then \( f(\alpha) \equiv f(\beta) \) (mod \( M \)).

(c) If \( \alpha \theta \equiv \beta \theta \) (mod \( M \)), where \( \theta \in \mathcal{O}_K \), then \( \alpha \equiv \beta \) (mod \( M/D \)), where \( D = \gcd((\theta), M) \).
(d) The congruence \( \alpha x \equiv \beta \pmod{M} \) is solvable if and only if \( D \mid (\beta) \), where \( D = \gcd((\alpha), M) \). The solution, if it exists, is unique modulo \( M/D \).

(e) Euler’s Theorem: If \( \gcd((\alpha), M) = (1) \), then \( \alpha^{\varphi(M)} \equiv 1 \pmod{M} \), where \( \varphi(M) := |(O_K/M)^*| \).

It should be mentioned that the quantity \( \varphi(M) \) which appears in Proposition 2.1(e), can be computed in terms of the prime ideal factors of \( M \) as follows (see [1, p. 369]):

\[
\varphi(M) = N M \prod_{P \mid M} \left(1 - \frac{1}{NP}\right),
\]

where the product extends over all distinct prime ideals which divide \( M \). Here \( NM \) denotes the norm of \( M \). Note that in particular, if \( M = P^a \) is a power of a prime ideal, then \( \varphi(P^a) = N P^{a-1} (NP - 1) \).

When dealing with congruences modulo a fixed ideal \( M \), the set of all algebraic integers in \( O_K \) breaks down into \( NM \) classes, such that any two elements of the same class are congruent and two elements from two different classes are incongruent. For many purposes it is immaterial which elements of one of these residue classes is used. In these cases it suffices to consider an arbitrary set of representatives of the various residue classes. Such a set \( \mathfrak{M}(O_K/M) = \{\theta_1, \theta_2, \ldots, \theta_{NM}\} \), called a complete residue system modulo \( M \) in \( O_K \), is characterized by the following properties: (a) If \( i \neq j \), then \( \theta_i \not\equiv \theta_j \pmod{M} \). (b) For every \( \alpha \in O_K \), there is an index \( 1 \leq i \leq NM \) for which \( \alpha \equiv \theta_i \pmod{M} \). Examples of complete residue systems modulo \( M = (m) \) in \( \mathbb{Z} \), where \( m \in \mathbb{Z} \), are \( \mathfrak{M}(\mathbb{Z}/(m)) = \{0, 1, 2, \ldots, m - 1\} \) and \( \mathfrak{M}(\mathbb{Z}/(m)) = \{1, 2, \ldots, m\} \). An example of a complete residue system modulo \( M = (3) \) in \( \mathbb{Z}[i] \) is \( \mathfrak{M}(\mathbb{Z}[i]/(3)) = \{0, 1, 2, i, 1 + i, 2 + i, 2i, 1 + 2i, 2 + 2i\} \). In sequel, when there is no fear of confusion, we shall drop the reference to \( O_K \) and refer to \( \mathfrak{M}(O_K/M) \) as “a complete residue system modulo \( M \)” and denote it simply by \( \mathfrak{M} \).

For the purposes of this paper, we shall narrow our discussion to prime power ideals. 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 \( NP = p^f \). The number \( f \) is called the inertial degree of \( P \) and \( p \) is called the rational prime number lying below \( P \) (as \( (p) \subseteq P \)). The positive integer \( e \) such that \( P^e \mid (p) \) (that is such \( P^e \mid (p) \) but \( P^{e+1} \nmid (p) \)) is called the ramification index of \( P \) in \( p \). One can prove that \( e \leq n \), where \( n \) is the degree of the field \( K \). For example, in \( \mathbb{Q}(i) \) we have that \( P = (7) \) is a prime ideal, so here \( p = 7 \). The ramification index of \( P \) is \( e = 1 \) and the inertial degree is \( f = 2 \). Regarding the prime ideal \( P = (2 + i) \), we have that \( PQ = (5) \), where \( Q = (2 - i) \), so here \( p = 5 \). The ramification index of \( P \) is also \( e = 1 \), but here the inertial degree is \( f = 1 \). Taking the prime ideal \( P = (1 + i) \) we have that \( P^2 = (2) \), so
here \( p = 2 \). The ramification index is therefore \( e = 2 \) and the inertial degree is \( f = 1 \).

The following theorem will be very useful in our discussions:

**Proposition 2.2.** Suppose that \( p \) is a rational prime number, \( P \) is a prime ideal in the algebraic number field \( K \) lying above \((p)\) with ramification index \( e \geq 1 \), \( \alpha, \beta \in \mathcal{O}_K \) and \( a, k \) are integers such that \( a \geq 1 \) and \( k \geq 0 \). Then

\[
\alpha \equiv \beta \pmod{P^a} \implies \alpha^{p^k} \equiv \beta^{p^k} \pmod{P^{a+k}}.
\]

**Proof.** We use induction on \( k \). If \( k = 0 \), then the assertion is clear. So suppose that \( k \geq 1 \). If \( \alpha \equiv \beta \pmod{P^a} \), then there is \( \theta \in P^a \) such that \( \alpha = \beta + \theta \). Note that

\[
\alpha^p = (\beta + \theta)^p = \beta^p + \sum_{j=1}^{p-1} \binom{p}{j} \beta^{p-j} \theta^j + \theta^p.
\]

If \( 1 \leq j \leq p - 1 \), then \( p \mid \binom{p}{j} \). In addition, since \( P^a \mid (\theta) \) we get \( P^{aj} \mid (\theta)^j \).

Using the fact that \( P^e \parallel \mathcal{O}_K \) we obtain therefore \( \binom{p}{j} \beta^{p-j} \theta^j \equiv 0 \pmod{P^{e+aj}} \).

Since clearly \( e + a \leq e + aj \) we get \( \alpha^p \equiv \beta^p + \theta^p \pmod{P^{a+e}} \).

Suppose that \( k = 1 \). Note that since \( P^a \mid (\theta) \) and \( a + 1 \leq ap \), we get \( \theta^p \equiv 0 \pmod{P^{a+1}} \) and therefore \( \alpha^p \equiv \beta^p \pmod{P^{a+1}} \), as desired.

Take \( k > 1 \) and assume that the assertion is true for \( 1, 2, \ldots, k-1 \). If \( \alpha \equiv \beta \pmod{P^a} \), then by the induction hypothesis we get \( \alpha^{p^{k-1}} \equiv \beta^{p^{k-1}} \pmod{P^{a+k-1}} \).

The assertion then follows using the case \( k = 1 \). \( \square \)

### 2.2 Constructing the \( P \)-adic number field

If \( K \) is an algebraic number field and \( P \) is a prime ideal, we construct the \( P \)-adic numbers field \( \mathcal{K}_P \). Our construction of \( \mathcal{K}_P \) is routine and similar to the construction of the \( p \)-adic numbers field \( \mathbb{Q}_p \) for a prime number \( p \), so the details will be omitted (see [8, pp. 36–37]). Let \( \mathcal{O}_K \) denote the algebraic integers in \( K \) and let \( P \) be a prime ideal in \( \mathcal{O}_K \) lying above \((p)\) for a unique prime number \( p \).

If \( x \in K \setminus \{0\} \), then the ideal \((x) = x \mathcal{O}_K \) is a fractional ideal in \( K \) and it can be uniquely factored as a product of positive or negative integer powers of prime ideals in \( \mathcal{O}_K \). We write \( \text{ord}_P(x) \) for the exponent of \( P \) in this factorization.

Letting

\[
|x|_P := p^{-\text{ord}_P(x)}
\]

defines a discrete, non-archimedean valuation on \( K \). Completing \( K \) with respect to this valuation yields the \( P \)-adic numbers field \( \mathcal{K}_P \). In this setting, the \( P \)-adic integers are denoted by \( \mathcal{O}_P \). Note that the \( p \)-adic number field \( \mathbb{Q}_p \) is obtained in this way by taking in particular the prime ideal \( P = (p) \). It is customary to designate the set of \( p \)-adic integers in \( \mathbb{Q}_p \) by \( \mathbb{Z}_p \). Recall that in this case, the elements of \( \mathbb{Z}_p \cap \mathbb{Q} \) are exactly the elements of the form \( a/b \),
where $a, b \in \mathbb{Z}$ such that $p \nmid b$. Similarly, it can be shown that the elements of
$\mathcal{O}_P \cap K$ are exactly the elements of the form $\alpha/\beta$, where $\alpha, \beta \in \mathcal{O}_K$ such that $\text{ord}_P(\beta) = 0$.

In these setting it can be shown that every element $a \in \mathcal{O}_P$ can be written
uniquely in the form $a = e\gamma^n$, where $\gamma$ is a fixed (but arbitrary) element of
$P \setminus P^2$ such that $|\gamma|_P = p^{-1}$, $e$ is a unit (that is, $|e|_P = 1$) and $|a|_P = p^{-n}$. It
can be also shown that every $\gamma \in P \setminus P^2$ will be suitable for this presentation.
Such an element is called a uniformizer. As an example, a uniformizer in the
field $\mathbb{Q}_p$ is any integer of the form $kp$, where $p \nmid k$.

As in the field $\mathbb{Q}_p$, any element of $K_P$ has a unique canonical expansion.
We shall be interested especially in the canonical expansion of $P$-adic integers.
If $a$ is a $P$-adic integer and $\gamma$ is a fixed element of $P \setminus P^2$, then $a$ has a unique
$P$-adic expansion
$$a = a_0 + a_1\gamma + a_2\gamma^2 + \ldots$$
where $a_i \in \mathcal{O}(\mathcal{O}_K/P)$.

The notion of congruences modulo $P^a$ can be further generalized to $P$-
adic integers. Suppose that $a, b \in \mathcal{O}_P$, $a$ is a positive integer and choose a
uniformizer $\gamma \in P \setminus P^2$. We say that $a$ and $b$ are congruent modulo $P^a$, written
$a \equiv b \pmod{P^a}$ if $a - b \in \gamma^a\mathcal{O}_P$. Since $\mathcal{O}_P/(\gamma^a)$ is a ring, the above congruence
relation satisfies the usual arithmetic laws, namely if $a, b, a', b' \in \mathcal{O}_P$ satisfy
$a \equiv b \pmod{P^a}$ and $a' \equiv b' \pmod{P^a}$, then $a + a' \equiv b + b' \pmod{P^a}$ and
$aa' \equiv bb' \pmod{P^a}$. Even though we use the same relation over the ring $\mathcal{O}_K$,
there is no place for confusion, since this “new” definition generalizes the “old”
one, as the following proposition shows:

**Proposition 2.3.** Let $K$ be a number field, $P$ a prime ideal, $\gamma \in P \setminus P^2$,
$\alpha, \beta \in \mathcal{O}_K$ and $a$ a positive integer. Then $\alpha - \beta \in P^a$ iff $\alpha - \beta \in \gamma^a\mathcal{O}_P$.

*Proof.* Suppose that $\alpha - \beta \in P^a$ and set $k = \text{ord}_P(\alpha - \beta)$. By the assumption,
$P^a \mid (\alpha - \beta)$. Hence $a \leq k$. Since $\alpha - \beta \in \mathcal{O}_K \subseteq \mathcal{O}_P$, there is a unit $e \in \mathcal{O}_P$
such that $\alpha - \beta = e\gamma^k$. Thus
$$\frac{\alpha - \beta}{\gamma^a} = e\gamma^{k - a},$$
and since $0 \leq k - a$, we get $e\gamma^{k - a} \in \mathcal{O}_P$. Hence $(\alpha - \beta)/\gamma^a \in \mathcal{O}_P$, that is
$\alpha - \beta \in \gamma^a\mathcal{O}_P$, as desired.

Conversely, suppose that $\alpha - \beta \in \gamma^a\mathcal{O}_P$. Note that $(\alpha - \beta)/\gamma^a \in \mathcal{O}_P \cap K$,
so there exist $\eta, \theta \in \mathcal{O}_K$ for which
$$\alpha - \beta = \gamma^a\frac{\theta}{\eta},$$
and $\text{ord}_P(\eta) = 0$. Thus $(\eta)(\alpha - \beta) = (\gamma)^a(\theta)$. But $P \mid (\gamma)$, so $P^a \mid (\gamma)^a$ and
therefore $P^a \mid (\eta)(\alpha - \beta)$. Since $\text{ord}_P(\eta) = 0$, $P^a$ and $(\eta)$ are relatively prime.
Thus $P^a \mid (\alpha - \beta)$. The proof is therefore complete. □
The congruence relation with respect to $\mathcal{O}_P$ can be also expressed using the notion of valuation:

**Proposition 2.4.** Let $K$ be a number field, $P$ a prime ideal lying above the rational prime $p$, $a, b \in \mathcal{O}_P$ and $a$ a positive integer. Then $a \equiv b \pmod{P^a}$ iff $|a - b|_P \leq p^{-a}$.

*Proof.* If $a \equiv b \pmod{P^a}$, then $a - b \in \gamma^a\mathcal{O}_P$, and there is $c \in \mathcal{O}_P$ such that $a - b = \gamma^a c$. Therefore, $|a - b|_P = (|\gamma|_P)^a|c|_P$, that is $|a - b|_P = p^{-a}|c|_P$. But $|c|_P \leq 1$, so $|a - b|_P \leq p^{-a}$.

Conversely, suppose that $|a - b|_P \leq p^{-a}$. Since $a - b \in \mathcal{O}_P$, it can be written of the form $a - b = c\gamma^k$, where $c \in \mathcal{O}_P$ is a unit, $\gamma \in P \setminus P^2$ and $|a - b|_P = p^{-k}$. Hence $p^{-k} \leq p^{-a}$ so $a \leq k$, that is $0 \leq k - a$. Thus

$$a - b = c\gamma^k = \gamma^a(c\gamma^{k-a}) \in \gamma^a\mathcal{O}_P,$$

as desired. \qed

The relation found in Proposition 2.4 between congruences modulo $P^a$ and the $P$-adic valuation allows us to express sequences of congruences in terms of convergence of elements in $\mathcal{O}_P$ and vice-versa.

**Proposition 2.5.** Let $K$ be a number field, $P$ be a prime ideal lying above the rational prime $p$, $a \in \mathcal{O}_P$ and $n_0$ a positive integer. If $(a_1, a_2, a_3, \ldots)$ is a sequence in $\mathcal{O}_P$ such that $a_n \equiv a \pmod{P^n}$ for each $n \geq n_0$, then $a_n \to a$.

*Proof.* Take $\varepsilon > 0$ and let $n_1$ be a positive integer such that $p^{-n_1} < \varepsilon$. Set $N = \max\{n_0, n_1\}$. By Proposition 2.4 we get that for each $n \geq N$

$$|a_n - a|_P \leq p^{-n} \leq p^{-N} \leq p^{-n_1} < \varepsilon$$

and the assertion follows. \qed

**Proposition 2.6.** Suppose that $K$ is a number field and let $P$ be a prime ideal in $K$. Then for each $a \in \mathcal{O}_P$ there is an infinite sequence $(\alpha_1, \alpha_2, \alpha_3, \ldots)$ in $\mathcal{O}_K$ such that $a \equiv \alpha_n \pmod{P^n}$ for every $n$, that is such that $\alpha_n \to a$.

*Proof.* Given $\gamma \in P \setminus P^2$, let

$$a = \theta_0 + \theta_1\gamma + \theta_2\gamma^2 + \theta_3\gamma^3 + \ldots,$$

be the canonical expression of $a$. In this expression, each $\theta_k$ is an element of a complete residue system modulo $P$. If we define $\alpha_n$ to be the partial sum $\alpha_n = \theta_0 + \theta_1\gamma + \theta_2\gamma^2 + \ldots + \theta_{n-1}\gamma^{n-1}$, then clearly $\alpha_n \in \mathcal{O}_K$, $a \equiv \alpha_n \pmod{P^n}$ for every $n$ and $\alpha_n \to a$, as required. \qed
By the above proposition, if \( a \) is a positive integer and if \( a \in \mathcal{O}_P \), then there is \( \alpha \in \mathcal{O}_K \) such that \( \alpha \equiv a \pmod{P^a} \). It follows that every congruence modulo a prime power \( P^a \) involving elements from \( \mathcal{O}_P \) is equivalent to a congruence with elements from \( \mathcal{O}_K \). Now, given a polynomial congruence over \( \mathcal{O}_P \), say \( f(x) \equiv 0 \pmod{P^a} \), then by replacing every coefficient of \( f(x) \) by an equivalent coefficient from \( \mathcal{O}_K \), we obtain an equivalent congruence over \( \mathcal{O}_K \). Moreover, it suffices to consider solutions over \( \mathcal{O}_K \).

Recall that regarding the field \( \mathbb{Q}_p \) we have that \( \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/(p^n) \) (see [9, p. 61]). This assertion can be generalized in the same way regarding the \( P \)-adic field \( K_P \) as follows:

**Theorem 2.7.** Suppose that \( p \) is a rational prime number, \( P \) is a prime ideal in the algebraic number field \( K \) lying above \( (p) \) and let \( \gamma \in P \setminus P^2 \). Then

\[
\mathcal{O}_P/\gamma^n\mathcal{O}_P \cong \mathcal{O}_K/P^n
\]

for every positive integer \( n \).

**Proof.** By Proposition 2.6, for every \( a \in \mathcal{O}_P \) there is a sequence \( (\alpha_1, \alpha_2, \alpha_3, \ldots) \) in \( \mathcal{O}_K \) such \( \alpha_k \equiv a \pmod{P^k} \) for each \( k \). Hence for every positive integer \( n \), we may define a function

\[
\psi : \mathcal{O}_P \to \mathcal{O}_K/P^n
\]

by \( \psi(a) = [\alpha_n]_{P^n} \). This function is a well defined homomorphism, since if also \( \beta_n \equiv a \pmod{P^n} \), then \( \alpha_n \equiv \beta_n \pmod{P^n} \) so \( [\alpha_n]_{P^n} = [\beta_n]_{P^n} \). Let us compute its kernel and image. If \( \psi(a) = [0]_{P^n} \), then \( \alpha_n \equiv 0 \pmod{P^n} \). But \( \alpha_n \equiv a \pmod{P^n} \), so \( a \equiv 0 \pmod{P^n} \), that is \( a \in \gamma^n\mathcal{O}_P \). Hence \( \ker \psi = \gamma^n\mathcal{O}_P \). Let \( [\alpha]_{P^n} \in \mathcal{O}_K/P^n \), \( \alpha \in \mathcal{O}_K \). Since \( \mathcal{O}_K \subseteq \mathcal{O}_P \) we obtain that \( \psi(\alpha) = [\alpha]_{P^n} \). Thus \( \text{im} \psi = \mathcal{O}_K/P^n \). We can conclude therefore that

\[
\mathcal{O}_P/\gamma^n\mathcal{O}_P = \mathcal{O}_P/\ker \psi \cong \text{im} \psi = \mathcal{O}_K/P^n.
\]

The proof is therefore complete.

In the above proof, the homomorphism \( \psi \) sent every \( a \in \mathcal{O}_P \) to a unique element \( [\alpha]_{P^n} \in \mathcal{O}_K/P^n \) for which \( a \equiv \alpha \pmod{P^n} \). Henceforth, we will denote the element \( [\alpha]_{P^n} \) by \( [a]_{P^n} \). This notation allows us to define a quotient map

\[
\mathcal{O}_P \to \mathcal{O}_P/\gamma^n\mathcal{O}_P \cong \mathcal{O}_K/P^n.
\]

by the natural correspondence \( x \mapsto [x]_{P^n} \). We shall denote by \( \mathcal{M}(\mathcal{O}_P/\gamma^a\mathcal{O}_P) \) a complete residue system modulo \( P^n \) of \( P \)-adic integers. Note that in view of the above isomorphism \( \mathcal{M}(\mathcal{O}_P/\gamma^a\mathcal{O}_P) \) is of course finite.
3 The $n$-th roots of unity subgroup

For a group $G$ and a positive number $n$, let us define the set of $n$-th roots of unity in $G$ by

$$U_G(n) := \{x \in G : x^n = 1_G\}.$$ 

An equivalent definition of $U_G(n)$ can be made using the notion of order. If $\text{ord}(x)$ denotes the order of the element $x \in G$, then $x \in U_G(n)$ if and only if $\text{ord}(x) \mid n$. If $G$ is abelian, then $U_G(n)$ forms a subgroup of $G$ called the $n$-th roots of unity subgroup. For example, taking $G = \mathbb{C}^*$ under multiplication gives the group of complex $n$-th roots of unity $U_{\mathbb{C}^*}(n)$. In particular, for $n = 3$ we get $U_{\mathbb{C}^*}(3) = \{1, \omega, \omega^2\}$ where $\omega = -1/2 + i\sqrt{3}/2$.

Given an (integral) ideal $M$ in the algebraic number field $K$, consider the group of units $G = (O_K/M)^*$. In this case the $n$-th roots of unity subgroup $U_{(O_K/M)^*}(n)$ will be called the $n$-th roots of unity modulo $M$. Henceforth, for the sake of convenience this group will be denoted in short by $U_M(n)$, that is

$$U_M(n) := \{[x] \in (O_K/M)^* : x^n \equiv 1 \pmod{M}\}.$$ 

For example, if $K = \mathbb{Q}$ and $M = (8)$, then $O_K = \mathbb{Z}$, so $U_M(2) = \{[1], [3], [5], [7]\}$. As another example, by taking the field $K = \mathbb{Q}(i)$ (so $O_K = \mathbb{Z}[i]$) and the ideal $M = (11)$ we obtain $U_M(3) = \{[1], [5 + 3i], [5 + 8i]\}$.

The following proposition gathers several basic properties of the group $U_G(n)$.

**Proposition 3.1.** Let $n, m$ be positive integers and let $G$ be a finite abelian group. Then

(a) $U_G(n) \cap U_G(m) = U_G(\gcd(n, m))$.

(b) If $n \mid m$, then $U_G(n) \subseteq U_G(m)$.

(c) $U_G(n) = U_G(\gcd(n, |G|))$.

(d) If $G$ is cyclic, then $|U_G(n)| = \gcd(n, |G|)$.

*Proof.*

(a) Note that

$$x \in U_G(n) \cap U_G(m) \iff \text{ord}(x) \mid n \text{ and ord}(x) \mid m \iff \text{ord}(x) \mid \gcd(n, m) \iff x \in U_G(\gcd(n, m)).$$

(b) Clear.
(c) We have $g^{\lvert G \rvert} = 1_G$ for every $g \in G$. Therefore $U_G(\lvert G \rvert) = G$, and the assertion follows by applying part (a).

(d) Let $g$ be a generator of $G$ and set $d = \gcd(n, \lvert G \rvert)$. In order to solve the equation $x^n = 1_G$ it is sufficient to find the integers $k$ which satisfy $g^{kn} = 1_G$. Now

$$g^{kn} = 1_G \iff \lvert G \rvert \mid kn \iff \lvert G \rvert \mid k \iff k = t\frac{\lvert G \rvert}{d}, \text{ for some } t \in \mathbb{Z}.$$ 

Since $g^{k_1} = g^{k_2}$ iff $k_1 \equiv k_2 \mod \lvert G \rvert$, we may deduce that the different solutions of $x^n = 1_G$ are

$$x = g^{t\frac{\lvert G \rvert}{d}},$$

where $t \in \{0, 1, 2, \ldots, d - 1\}$, so $\lvert U_G(n) \rvert = d$ as required.

The following results, which are applications of the above proposition, will be useful in the sequel.

**Proposition 3.2.** Suppose that $P$ is a prime ideal in the algebraic number field $K$ and $n$ is a positive integer. Then the congruence $x^n \equiv 1 \mod P$ has exactly $\gcd(n, NP - 1)$ solutions, which constitute a cyclic subgroup of $(O_K/P)^\ast$.

In particular, if $p$ is the rational prime number lying below $P$, then for every prime power $p^k$, the congruence $x^{p^k} \equiv 1 \mod P$ has only one solution, namely $x \equiv 1 \mod P$.

**Proof.** Since $O_K$ is a Dedekind domain, each prime ideal $P$ in $K$ is a maximal ideal (see [4, p. 194]). This implies that $O_K/P$ is a field (see [4, p. 18]) and hence $(O_K/P)^\ast$ is a cyclic group. Therefore, its subgroup $U_P(n)$ is also cyclic, and by Proposition 3.1(d), we get that $\lvert U_P(n) \rvert = \gcd(n, \lvert (O_K/P)^\ast \rvert) = \gcd(n, NP - 1)$, as desired.

By the first part of this proposition, the congruence $x^{p^k} \equiv 1 \mod P$ has $\gcd(p^k, NP - 1)$ solutions. But $NP$ is of the form $p^f$, so $\gcd(p^k, NP - 1) = 1$ and since $x = 1$ obviously satisfies the congruence, we conclude that $x \equiv 1 \mod P$.

**Proposition 3.3.** Suppose that $p$ is a rational prime number, $P$ is a prime ideal in the algebraic number field $K$ lying above (p), $\alpha, \beta \in O_K$ and $k$ is a non-negative integer. Then

$$\alpha^{p^k} \equiv \beta^{p^k} \mod P \implies \alpha \equiv \beta \mod P$$

**Proof.** If $\beta$ is invertible modulo $P$ then the congruence $\alpha^{p^k} \equiv \beta^{p^k} \mod P$ is equivalent to $(\alpha \beta^{-1})^{p^k} \equiv 1 \mod P$. By Proposition 3.2, $x \equiv 1 \mod P$ is
the only solution of the congruence $x^{pk} \equiv 1 \pmod{P}$, so we may conclude that
$\alpha \beta^{-1} \equiv 1 \pmod{P}$, that is $\alpha \equiv \beta \pmod{P}$, as required.

If $\beta$ is not invertible modulo $P$ then $P \mid (\beta)$, so $P \mid (\beta)^{pk}$ that is $\beta^{pk} \equiv 0 \pmod{P}$. Therefore by the assumption, $\alpha^{pk} \equiv 0 \pmod{P}$, that is $P \mid (\alpha)^{pk}$. But $P$ is a prime ideal, so $P \mid (\alpha)$. As $P \mid (p)$, the assertion follows. \hfill \Box

4 Solving $x^n \equiv 1 \pmod{P^a}$ when $p \not\mid n$

Recall that if $M$ is an integral ideal in the number field $K$, then $U_M(n)$ denotes the subgroup of $n$-th roots of unity in $(O_K/M)^*$, that is $U_M(n) := \{[x]_M \in (O_K/M)^*: x^n \equiv 1 \pmod{M}\}$.

**Theorem 4.1.** Suppose that $p$ is a rational prime number, $P$ is a prime ideal in the algebraic number field $K$ lying above $(p)$ and $n, a$ are positive integers. If $p \not\mid n$, then

(a) $U_P(n) \cong U_{P^a}(n)$ by the map $\phi_a : [x]_P \mapsto [x^{NP^{a-1}}]_{P^a}$.

(b) $|U_{P^a}(n)| = \gcd(n, NP - 1)$.

(c) If $\alpha_1, \alpha_2, \ldots, \alpha_d$ are the incongruent solutions of the congruence $x^n \equiv 1 \pmod{P^a}$, then $\alpha_1^{NP}, \alpha_2^{NP}, \ldots, \alpha_d^{NP}$ are the incongruent solutions of $x^n \equiv 1 \pmod{P^{a+1}}$.

**Proof.** (a) Henceforth we set $NP = p^f$. For each $a$, define the function $\phi_a : U_P(n) \rightarrow U_{P^a}(n)$ by the rule

$$\phi_a([x]_P) = [x^{NP^{a-1}}]_{P^a}.$$ 

We begin by proving that the function $\phi_a$ is well defined. Indeed, if $[x]_P \in U_P(n)$, then $x^n \equiv 1 \pmod{P}$ which implies, by Proposition 2.2, that $(x^{NP^{a-1}})^n = (x^n)^{Pf(a-1)} \equiv 1 \pmod{P^{f(a-1)+1}}$. Since clearly $a \leq f(a-1) + 1$, we deduce that $(x^{NP^{a-1}})^n \equiv 1 \pmod{P^a}$, so $[x^{NP^{a-1}}]_{P^a} \in U_{P^a}(n)$. Moreover, if $[x]_P, [y]_P \in U_P(n)$ satisfy $[x]_P = [y]_P$, then $x \equiv y \pmod{P}$ and by Proposition 2.2, $x^{Pf(a-1)} \equiv y^{Pf(a-1)} \pmod{P^{1+f(a-1)}}$. Hence $x^{NP^{a-1}} \equiv y^{NP^{a-1}} \pmod{P^a}$, that is $\phi_a([x]_P) = \phi_a([y]_P)$.

Next we prove that $\phi_a$ is an isomorphism. Obviously, $\phi_a$ is a group homomorphism. To prove that $\phi_a$ is injective, let $[x]_P \in U_P(n)$ such that $\phi_a([x]_P) = [1]_{P^a}$, that is $x^{NP^{a-1}} \equiv 1 \pmod{P^a}$. Hence $x^{NP^{a-1}} \equiv 1 \pmod{P}$ and by Proposition 3.2 we obtain $x \equiv 1 \pmod{P}$, as required.

We prove now that $\phi_a$ is surjective. Let $[\alpha]_{P^a} \in U_{P^a}(n)$. We need to find a solution for the congruence $x^{NP^{a-1}} \equiv \alpha \pmod{P^a}$. Since $\gcd(NP^{a-1}, n) = 1$, there exist $s, t \in \mathbb{Z}$ such that $NP^{a-1}t + ns = 1$. We shall show that
The structure of the \( n \)-th roots of unity

\[ x = \alpha^t \] is a suitable solution. First, note that \([\alpha^t]_p \in U_p(n)\). Since \((\alpha^t)^n = (\alpha^n)^t \equiv 1^t = 1 \pmod{P^a}\), it follows that \((\alpha^t)^n \equiv 1 \pmod{P}\). In addition,

\[ (\alpha^t)^{NP^{a-1}} = (\alpha^t)^{NP^{a-1}}1^s \equiv (\alpha^t)^{NP^{a-1}}(\alpha^n)^s = \alpha \pmod{P^a}. \]

We conclude that \(\phi_a\) is an isomorphism, as desired.

(b) By part (a) and Proposition 3.2, \(|U_p(n)| = |U_p(n)| = \gcd(n, NP - 1)|.

(c) For each \(a\) define the function \(\psi_a : U_p(n) \to U_{p+1}(n)\) by the rule \(\psi_a([x]_p) = [x^{NP}]_{p+1}\). Note that the functions \(\psi_a\) are well defined. The proof of that fact resembles the one given in part (a) for \(\phi_a\). We shall prove now that every \(\psi_a\) is an isomorphism using induction on \(a\). If \(a = 1\), then \(\psi_1 = \phi_2\) and we are done. Take \(a > 1\) and suppose that the assertion is true for \(1, 2, \ldots, a - 1\). It is easy to see that \(\psi_{a+1} = \psi_a \circ \psi_{a-1} \circ \cdots \psi_2 \circ \psi_1\).

By the induction hypothesis, \(\psi_1, \ldots, \psi_{a-1}\) are isomorphisms, so \(\psi_{a-1} \circ \cdots \circ \psi_1\) and therefore also \((\psi_{a-1} \circ \cdots \circ \psi_1)^{-1}\) are both isomorphisms. Since \(\psi_a = \phi_{a+1} \circ (\psi_{a-1} \circ \cdots \circ \psi_1)^{-1}\) and since \(\phi_{a+1}\) is also an isomorphism, it follows that \(\psi_a\) is an isomorphism.

\[\Box\]

By part (c) of the above theorem, the elements of \(U_{p+1}(n)\) can be obtained by raising the elements of \(U_p(n)\) to the \(NP\)-th power. To illustrate this fact, consider the group \(U(7)(3) = \{[1], [2], [4]\}\) in \(K = \mathbb{Q}\). Here \(p = 7, P = (7), NP = 7\) and \(7 \nmid 3\). Thus

- \(U_{(7)}(3) = \{[1], [2], [4]\}\)
- \(U_{(49)}(3) = \{[1^7], [2^7], [4^7]\} = \{[1], [30], [18]\}\)
- \(U_{(343)}(3) = \{[1^7], [30^7], [18^7]\} = \{[1], [324], [18]\}\)
- \(U_{(2401)}(3) = \{[1^7], [324^7], [18^7]\} = \{[1], [1353], [1047]\}\)

etc. It turns out that each one of the above sequences of solutions, namely

\[
\begin{align*}
(1, 1, 1, 1, \ldots) \\
(2, 30, 324, 1353, \ldots) \\
(4, 18, 18, 1047, \ldots)
\end{align*}
\]

converges to a different element in the 7-adic field \(\mathbb{Q}_7\). Furthermore, these sequences converge to the solutions of the equation \(x^3 = 1\) in \(\mathbb{Q}_7\). This is the case in general, that is, if \([\alpha] \in U_p(n)\), then the sequence

\[
(\alpha, \alpha^{NP}, \alpha^{NP^2}, \ldots)
\]
converges to an $n$-th root of unity in $K_P$. Recall that $U_{K_P}^*(n) \coloneqq \{x \in K_P^* : x^n = 1\}$. We shall prove this claim and use it to prove a deeper assertion. In our proof we shall use Hensel’s Lemma. The version of Hensel’s lemma suitable for $K_P$ is as follows (see [8, p. 43]):

**Theorem 4.2 (Hensel’s Lemma).** Suppose that $K$ is a number field, $P$ is a prime ideal and $f(x)$ is a polynomial over $O_P$. Suppose also that there exists an $a_1 \in O_P$ such that $f(a_1) \equiv 0 \pmod{P}$ but $f'(a_1) \not\equiv 0 \pmod{P}$.

Then there exists a unique $a \in O_P$ such that $a \equiv a_1 \pmod{P}$ and $f(a) = 0$.

Before we continue, note that although we have assumed in Hensel’s lemma that the polynomial $f(x)$ is over $O_P$, the congruence $f(x) \equiv 0 \pmod{P}$ is equivalent to a congruence over $O_K$. Indeed, as it follows from Proposition 2.6 (and the remark after it), we may replace every coefficient of $f(x)$ by an equivalent coefficient modulo $P$, taken from $O_K$.

**Theorem 4.3.** Suppose that $p$ is a rational prime number, $P$ is a prime ideal in the algebraic number field $K$ lying above $(p)$ and $n$ is a positive integer. If $p \nmid n$, then

$$U_P(n) \cong U_{K_P}^*(n)$$

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

$$\psi : U_P(n) \to U_{K_P}^*(n) \quad \text{or} \quad \nu : U_{K_P}^*(n) \to U_P(n)$$

$$[x]_P \mapsto \lim_{k \to \infty} x^{NP^{k-1}} \quad \text{or} \quad x \mapsto [x]_P$$

In particular, the equation $x^n = 1$ has exactly $\gcd(NP - 1, n)$ solutions in $K_P$.

**Proof.** We begin by proving that the maps $\psi$ and $\nu$ are both well defined and injective.

**The map $\psi$:** For an element $\alpha \in O_K$ define the sequence

$$\alpha_k := \alpha^{NP^{k-1}} \quad (k \geq 1).$$

Let $[\alpha]_P \in U_P(n)$ and let $\psi : U_P(n) \to U_{K_P}^*(n)$ be the function $\psi([\alpha]_P) = \lim_{k \to \infty} \alpha_k$. We begin by proving that the sequence $\alpha_k$ converges to a solution of $x^n = 1$ in $K_P$.

In order to do so, we first prove by induction on $k$ that $\alpha_{k+1} \equiv \alpha_k (\mod{P^k})$, that is $|\alpha_{k+1} - \alpha_k|_P \leq P^{-k}$ for every $k$. This will imply that the sequence $\alpha_k$ is a Cauchy sequence, which converges, by the completeness of $K_P$. Suppose that $k = 1$. By Euler Theorem (Proposition 2.1(e)) we have that $\alpha^{NP-1} \equiv 1 (\mod{P^n})$. Hence $\alpha^{NP} \equiv \alpha (\mod{P})$, that is $\alpha_2 \equiv \alpha_1 (\mod{P})$, as desired. Take $k > 1$.
and assume that the assertion is true for $1, 2, \ldots, k - 1$. By the induction hypothesis $\alpha_k \equiv \alpha_{k-1} \pmod{P^{k-1}}$. Set $NP = p^f$. Applying Proposition 2.2 gives

$$\alpha_k^{p^f} \equiv \alpha_{k-1}^{p^f} \pmod{P^{k-1+f}}.$$ 

But $\alpha_k^{p^f} = \alpha_{k+1}$, $\alpha_{k-1}^{p^f} = \alpha_k$ and $k \leq k - 1 + f$, so we deduce that $\alpha_k = \alpha_k \pmod{P^k}$. Hence our claim follows by induction.

Let $a \in K_P$ be the limit of $\alpha_k$. On the one hand $\alpha_k \to a$, so by the limit arithmetic (see [6, p. 24]) we get $a^n \to a^n$ when $k \to \infty$. On the other hand, we claim that $\alpha^n_k \equiv 1 \pmod{P^k}$ for every $k$. This is done by induction: if $k = 1$, then indeed $\alpha^n_1 = \alpha^n = 1 \pmod{P}$. Take $k > 1$ and assume that the assertion is true for $1, 2, \ldots, k - 1$. By the induction hypothesis $\alpha_{k-1}^n \equiv 1 \pmod{P^{k-1}}$. Hence, by Theorem 4.1(c), $\alpha_{k-1}^{NP} = \alpha_k$ satisfy the congruence $x^n \equiv 1 \pmod{P^k}$, as claimed. So $\alpha^n_k \equiv 1 \pmod{P^k}$ for each $k$. Therefore, by Proposition 2.5, $\alpha_k^n \to 1$ when $k \to \infty$ and by the uniqueness of limit we conclude that $a^n = 1$.

Next we prove that $\psi$ is well defined. Suppose that $[a]_P, [\beta]_P \in U_P(n)$ are such that $\alpha \equiv \beta \pmod{P}$. We need to show that $\lim_{k \to \infty} \alpha_k = \lim_{k \to \infty} \beta_k$. Indeed, by Proposition 2.2 we get that for every $k$

$$\alpha^{p^f(k-1)}_k \equiv \beta^{p^f(k-1)} \pmod{P^{1+f(k-1)}},$$

so $\alpha_k \equiv \beta_k \pmod{P^k}$, that is $\alpha_k - \beta_k \equiv 0 \pmod{P^k}$ for every $k$. Thus, by Proposition 2.5 we get that $\alpha_k - \beta_k \to 0$ when $k \to \infty$ and the assertion follows.

By limit arithmetic we deduce that $\psi$ is a group homomorphism. To prove that it is injective, take $[a]_P, [\beta]_P \in U_P(n)$ and suppose that $\alpha_k$ and $\beta_k$ converge to the same element. Hence $\alpha_k - \beta_k \to 0$, so there is $k$ such that $|\alpha_k - \beta_k|_P \leq p^{-1}$, that is $\alpha_k \equiv \beta_k \pmod{P}$. Hence $\alpha^{NP^{k-1}}_k \equiv \beta^{NP^{k-1}} \pmod{P}$ and by Proposition 3.3 it follows that $\alpha \equiv \beta \pmod{P}$, that is $[a]_P = [\beta]_P$.

The map $\nu$: For future use, we shall prove a generalized version of our claim. Let $a$ be a positive integer and consider the map

$$\nu_a : U_{K_P}(n) \to U_P(a)$$

defined by $x \mapsto [x]_P$. (Recall that although $a$ is a $P$-adic integer, in view of Theorem 2.7, we can identify $[x]_P$ with an element of $O_K/P^n$. Clearly, $\nu_1 = \nu$.

First observe that if $a \in U_{K_p}(n)$, then in particular $a^n \equiv 1 \pmod{P^n}$, so indeed $[a]_P \in U_P(a)$. Note that $\nu_a$ is a homomorphism. To show that this homomorphism is injective, it suffices to prove that if $a \in U_{K_P}(n)$ satisfies $[a]_P = [1]_P$, then $a = 1$. To do so, consider the polynomial $f(x) = x^n - 1$ over $K_P$. Hence $f'(x) = nx^{n-1}$. Clearly, $f(1) \equiv 0 \pmod{P}$ and since $p \nmid n$ it follows that $f'(1) \neq 0 \pmod{P}$. Therefore by Hensel’s lemma there exist a unique $b \in O_P$ such that

1. $f(b) = 0$
2. $b \equiv 1 \pmod{P}$. 

On the one hand \( [a]_{P^a} = [1]_{P^a} \), so in particular \( a \equiv 1 \pmod{P} \), and \( f(a) = 1 \) since \( a \in U_{K^*_P}(n) \) by our assumption. Hence \( a \) satisfies conditions (1) and (2) and by the uniqueness of \( b \) we conclude that \( a = b \). But on the other hand, also 1 clearly satisfies conditions (1) and (2). It follows that \( a = 1 \), as required.

Next, we shall prove that the maps \( \psi \) and \( \nu \) are isomorphisms. In order to do so, it suffices to show that these maps are surjective. Indeed, since \( \psi \) and \( \nu \) are injective, it follows that \( |U_P(n)| \leq |U_{K^*_P}(n)| \) and \( |U_P(n)| \geq |U_{K^*_P}(n)| \), respectively. Therefore \( |U_P(n)| = |U_{K^*_P}(n)| \), so \( \psi \) and \( \nu \) are surjective, as claimed. This completes our proof.

Knowing an explicit isomorphism between \( U_{K^*_P}(n) \) into \( U_P(n) \) 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 \( a \in \mathcal{O}_P \) be a \( P \)-adic integer and let

\[
a = a_0 + a_1 \gamma + a_2 \gamma^2 + \ldots
\]

be its \( P \)-adic expansion, where \( \gamma \in P \setminus P^2 \). For every non-negative integer \( n \) denote by \( a_n \) the \( n \)-th partial sum of \( a \), namely

\[
a_n := a_0 + a_1 \gamma + a_2 \gamma^2 + \ldots + a_n \gamma^n.
\]

This partial sum clearly depends upon the choice of the uniformizer \( \gamma \). However, in our applications we consider \( a_{n-1} \) modulo \( P^n \), which is independent of the choice of \( \gamma \). In other words, if \( \delta \) is another uniformizer and if the choice of the uniformizer is indicated by a superscript, then \( a_{n-1}^\gamma \equiv a_{n-1}^\delta \pmod{P^n} \). Thus, from now on, we shall omit the superscript \( \gamma \) and use the shorter notation \( a_{n-1} \).

Observe that \( a_n \in \mathcal{O}_K \) and that \( a \equiv a_{n-1} \pmod{P^n} \) 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 4.4.** Suppose that \( p \) is a rational prime number, \( P \) is a prime ideal in the algebraic number field \( K \) lying above \( (p) \) and \( n \) is a positive integer. If \( p \nmid n \), then

\[
U_{K^*_P}(n) \cong U_{P^a}(n)
\]

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 \( \gcd(NP^a - 1, n) \) incongruent solutions over \( \mathcal{O}_K \) and they are of the form

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

where \( a \in U_{K^*_P}(n) \).
Proof. In Theorem 4.3 we proved that the map $\nu_a : U_{K^l}(n) \to U_{P^a}(n)$ defined by $x \mapsto [x]_{P^a}$ is an injective homomorphism. By Theorems 4.1(a) and 4.3 it follows that $|U_{K^l}(n)| = |U_{P^a}(n)|$. Therefore, $\nu_a$ is an isomorphism as claimed.

Now, by the isomorphism $\nu_a$, it follows that

$$U_{P^a}(n) = \{[a]_{P^a} : a \in U_{K^l}(n)\}.$$ 

The theorem then follows by observing that $[a]_{P^a} = [a_{a-1}]_{P^a}$. □

Acknowledgements. Since a portion of this and the following papers constituted part of my doctoral dissertation at Tel-Aviv University in 2015, I wish to express my thanks to Professor Marcel Herzog under whom it was written.

References


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