Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas -Programa de Magíster en Matemática

El problema de Büchi para números *p*-ádicos
(Büchi's problem for *p*-adic numbers)

MARIANELA ISABEL CASTILLO FERNÁNDEZ
CONCEPCIÓN-CHILE
2011

Profesor Guía: Xavier Vidaux
Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas -Programa de Magíster en Matemática

El problema de Büchi para números *p*-ádicos
(Büchi's problem for *p*-adic numbers)

Xavier Vidaux (director)
José Aguayo (evaluador interno, miembro del jurado)
Jerzy Browkin (evaluador externo)
Jacqueline Ojeda (evaluador interno, miembro del jurado)
Carlos Videla (evaluador externo, miembro del jurado)

TESIS DEFENDIDA EL 31 DE MARZO DE 2011

MARIANELA ISABEL CASTILLO FERNÁNDEZ
CONCEPCIÓN-CHILE
2011

Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

El problema de Büchi para números p-ádicos

Marianela Castillo
Universidad de Concepción

Agradezco a quienes me ayudaron a realizar este trabajo: J. Browkin, A. Escassut, H. Pasten y C. Videla. Agradezco además a mis profesores del Departamento de Matemáticas por el tiempo que me dedicaron y por haberme apoyado en los momentos en que más lo necesité. Agradezco también al señor X. Vidaux, director de mi tesis, por sus consejos, su dedicación y por la confianza puesta en mi.

Dedico este trabajo a mi familia, quienes me han convertido en la persona que soy.

Contents

Introducción

Motivado por un problema de lógica matemática, J.R. Büchi propuso el siguiente problema en los años 70'.

Problema (Problema de Büchi)**.** $\mathbf{B}^2(\mathbb{Z})$. *¿Existe un entero positivo M tal que cualquier sucesión de M enteros cuadrados, cuya sucesión de segundas diferencias es igual a la sucesión constante $(2)_n$, es de la forma $\left((x+n)^2\right)_n$, donde $n = 1, \ldots, M$, para algún entero x?*

$\mathbf{B}^2(\mathbb{Z})$ es un problema abierto. Sin embargo, en 2001, P. Vojta mostró que $\mathbf{B}^2(\mathbb{Z})$ tendría una respuesta positiva si la conjetura de Bombieri fuera cierta para superficies. En [12], Pheidas y Vidaux propusieron una generalización del problema de Büchi a cualquier anillo unitario y a cualquier potencia.

Definición. *Sea $k \geq 0$ un entero. Una sucesión de elementos de un anillo unitario conmutativo A de característica 0 se llama* k-sucesión de Büchi en A *si la sucesión de sus k-ésimas potencias tiene k-ésimas diferencias constantes igual a $(k!)_n$. Toda sucesión cuya sucesión de k-ésimas potencias es de la forma $\left((x+n)^k\right)_n$, para algún x en A, se llama* k-sucesión de Büchi trivial.

Notamos que una k-sucesión de Büchi trivial es una sucesión de Büchi. El problema de Büchi se generaliza de la siguiente manera:

Problema. $\mathbf{B}^k(A)$. *Sean $k \geq 2$ un entero y A un anillo unitario conmutativo de característica* 0. *¿Existe un entero M tal que toda k-sucesión de Büchi en A de largo M es una sucesión de Büchi trivial?*

Podemos notar que si $\mathbf{B}^k(A)$ tiene una respuesta positiva, entonces para cualquier subanillo B de A, $\mathbf{B}^k(B)$ tiene respuesta positiva. En esta Tesis, estamos interesados en los anillos en que el problema de Büchi tiene respuesta negativa en una *forma no trivial* (intuitivamente, anillos sin muchas

potencias k-ésimas). Por ejemplo, si $A = \bar{\mathbb{Q}}$ es el campo de los números algebraicos, toda sucesión de la forma

$$\left(x_1, x_2, x_3 = \sqrt{2 + 2x_2^2 - x_1^2}, \ldots, x_M = \sqrt{2 + 2x_{M-1}^2 - x_{M-2}^2}, \ldots\right)$$

es una 2-sucesión de Büchi (que, en general, es no trivial). Con una idea similar, podemos ver fácilmente que $\mathbf{B}^k(\bar{\mathbb{Q}})$ tiene respuesta negativa para todo $k \geq 2$. La sucesión

$$(\sqrt[k]{n^k + 1})_{n \geq 0}$$

es una k-sucesión de Büchi de largo infinito, y con ella vemos que $\mathbf{B}^k(\bar{\mathbb{Z}} \cap \mathbb{R})$ tiene respuesta negativa para todo $k \geq 2$. En los dos ejemplos anteriores, la respuesta negativa al problema de Büchi se debe a la existencia de una sucesión de Büchi no trivial de largo infinito.

En el survey [11] sobre el problema de Büchi, Pasten, Pheidas y Vidaux plantean el problema de encontrar anillos para los cuales el problema de Büchi tiene respuesta negativa pero que no tienen sucesiones de Büchi no triviales de largo infinito. Ellos distinguen dos clases de anillos en los que el problema de Büchi puede tener respuesta negativa (en característica 0):

- **Tipo 1**: Anillos en los cuales existe una sucesión de Büchi no trivial de largo infinito.
- **Tipo 2**: Anillos en los cuales existen sucesiones de Büchi no triviales de cualquier largo, pero no de largo infinito.

En [1], Browkin demostró que para $k = 2$, el campo de los números p-ádicos $\mathbb{Q}_p$ es de tipo 1 y el anillo de los enteros p-ádicos $\mathbb{Z}_p$ es de tipo 2. Esta Tesis es un intento de generalizar los resultados de Browkin a potencias más altas. Antes de dar nuestros principales resultados, necesitamos introducir el concepto de sucesión de Hensley:

Definición (Sucesión de Hensley)**.** *Sea $k \geq 0$ un entero. Una sucesión (a_n) de elementos de un anillo unitario conmutativo A de característica 0, cuyas k-ésimas potencias son de la forma*

$$(a + n)^k + b_{k-2}n^{k-2} + \cdots + b_1 n + b_0,$$

para algunos $a, b_{k-2}, \ldots, b_0 \in A$, se llama k-sucesión de Hensley*. Si*

$$b_0 = \cdots = b_{k-2} = 0$$

entonces (a_n) se llama k-sucesión de Hensley trivial*.*

Problema (Formulación de Hensley del problema de Büchi)**.** $\mathbf{HF}^k(A)$. *Sea $k \geq 2$ un entero y A un anillo unitario conmutativo de característica 0. ¿Existe un entero $M \geq k+1$ tal que toda k-sucesión de Hensley en A de largo M es una k-sucesión de Hensley trivial?*

En esta Tesis, consideramos el siguiente problema (más débil), conocido como problema de Hensley:

Problema. $\mathbf{HP}^k(A)$ *Sea $k \geq 2$ un entero y A un anillo unitario conmutativo de característica 0. ¿Existe un entero M tal que, dados a y b arbitrarios en A, si las expresiones*

$$(n+a)^k + b$$

son potencias k-ésimas para $n = 1, \ldots, M$, entonces $b = 0$?

Es bien sabido que el grupo multiplicativo de invertibles en el anillo de enteros módulo n es un grupo cíclico si y sólo si $n = 2$, o $n = 4$, o n es de la forma p^m, o n es de la forma $2p^m$, para cualquier número primo impar p y para cualquier entero positivo m. Cuando el grupo es cíclico, se llama *raíz primitiva módulo n* a cualquier entero cuya clase de congruencia módulo n es un generador del grupo.

Para expresar nuestro Teorema Principal, necesitamos introducir la siguiente notación:

Notación. *1. Escribimos*

$$q = q(p,k) = p^{\varepsilon+1+ord_p k},$$

donde ε es igual a 1 si $p = 2$ y es igual a 0 si $p \neq 2$.

2. *Decimos que* se satisface la condición $C(p,k)$ *si existe una raíz primitiva módulo q, digamos g, tal que*

$$x^k + y^k \equiv g \bmod q$$

para algunos enteros x e y cuyas clases de congruencia módulo q están en $(\mathbb{Z}/q\mathbb{Z})^\times$.

La condición $C(p,k)$ no se satisface (trivialmente) cuando q es de la forma 2^m, para $m \geq 3$, ya que simplemente no existen raíces primitivas en este caso (no sabemos si existen otros pares (p,k) para los cuales la condición no se satisface). Por el siguiente teorema (ver por ejemplo [19]), vemos que se satisface la condición $C(p,k)$ cuando $q > (k-1)^4$ y, o bien p es un primo impar, o bien $p = 2$ y $\operatorname{ord}_p k = 0$.

Teorema. *Sea $\mathbb{F}_p$ un campo finito con p elementos y $k \geq 2$ un entero. Si $p > (k-1)^4$, entonces toda forma diagonal de grado k en dos variables sobre $\mathbb{F}_p$ es universal.*

Notamos además que cuando $g = 2$ es una raíz primitiva módulo q entonces, por la elección $x = y = 1$, la condición $C(p, k)$ se satisface trivialmente.

Ahora podemos expresar nuestros principales resultados.

Teorema (Teorema Principal)**.** *Sea p un número primo y $k \geq 2$ un entero.*

1. *Para cada $n \in \mathbb{Z}$, cuando $p > 2$ la expresión $n^k + p^{-k}$ es una potencia k-ésima en $\mathbb{Q}_p$. Por lo tanto, cualquier sucesión (a_n), $n \geq 1$, tal que cada a_n tiene k-ésima potencia igual a $n^k + p^{-k}$, es una k-sucesión de Büchi no trivial de largo infinito en $\mathbb{Q}_p$.*

2. *Para cada $n \in \mathbb{Z}$, la expresión $n^k + 2^{-(2+k)}$ es una potencia k-ésima en $\mathbb{Q}_2$. Por lo tanto, cualquier sucesión (a_n), $n \geq 1$, tal que a_n tiene k-ésima potencia igual a $n^k + 2^{-(2+k)}$, es una k-sucesión de Büchi no trivial de largo infinito en $\mathbb{Q}_2$.*

3. *Para cada $m \in \mathbb{Z}$, la expresión $n^k + p^{mk+1}$ es una potencia k-ésima en $\mathbb{Z}_p$ cuando $n = 1, \ldots, p^m - 1$. Por lo tanto, si $p^m \geq k + 2$, entonces cualquier sucesión (a_n), $n = 1, \ldots, p^m - 1$, donde cada a_n tiene k-ésima potencia igual a $n^k + p^{mk+1}$, es una k-sucesión de Büchi no trivial en $\mathbb{Z}_p$.*

4. *Supongamos que se satisface la condición $C(p, k)$ y, o bien k no es coprimo con p, o bien p es impar y k no es coprimo con $p - 1$. Sean a y b dos enteros p-ádicos. Si para todo $n \geq 1$ la expresión*

$$(n + a)^k + b$$

es una potencia k-ésima en $\mathbb{Z}_p$, entonces $b = 0$.

Itemes 1 y 2 muestran que $\mathbb{Q}_p$ es de tipo 1. Item 3 muestra que en $\mathbb{Z}_p$ hay sucesiones de Büchi no triviales de cualquier largo finito. Item 4 muestra que, cuando la hipótesis sobe p y k se satisface, no hay sucesión de Büchi infinita no trivial en $\mathbb{Z}_p$ cuya sucesión de potencias k-ésimas es de la forma $\left((n + a)^k + b\right)_n$, para algún a y b en $\mathbb{Z}_p$.

Para $k = 2$, el teorema anterior fue probado recientemente por J. Browkin en [1]. Nosotros adaptamos sus técnicas a potencias más altas. En el

Capítulo 1 introducimos las herramientas básicas que necesitamos para demostrar el Teorema Principal. En el Capítulo 2, damos una caracterización del conjunto de las potencias k-ésimas en $\mathbb{Z}_p$, para cada k y p, y probamos algunas propiedades de estos conjuntos. En el Capítulo 3, vamos a probar los items 1, 2 y 3 del Teorema Principal. Vamos a probar el item 4 del Teorema Principal en el Capítulo 4.

Introduction

Motivated by a mathematical logic problem, J.R. Büchi proposed the following problem in the early 1970's.

Problem (Büchi's problem)**.** $\mathbf{B}^2(\mathbb{Z})$*. Does there exist a positive integer* M *such that any sequence of* M *integer squares, with second difference constant equal to the constant sequence* $(2)_n$*, is of the form* $\left((x+n)^2\right)_n$*, where* $n = 1, \ldots, M$*, for some integer* x*?*

Büchi's problem is open. However, in 2001, P. Vojta showed that it would have a positive answer if Bombieri's conjecture were true for surfaces.

In [12], Pheidas and Vidaux proposed a generalization of Büchi's problem to any unitary commutative ring and to higher powers.

Definition. *Let* $k \geq 0$ *be an integer. A sequence of elements of a unitary commutative ring* A *of characteristic* 0 *is called a* k-Büchi sequence in A *if the sequence of its* k*-th powers has* k*-th difference constant equal to* $(k!)_n$*. Every sequence whose sequence of* k*-th powers is of the form* $\left((x+n)^k\right)_n$ *for some* x *in* A *will be referred to as* trivial k-Büchi sequence*.*

Note that a trivial k-Büchi sequence is a Büchi sequence. Büchi's problem is generalized as follows.

Problem. $\mathbf{B}^k(A)$*. Let* $k \geq 2$ *be an integer and* A *a unitary commutative ring of characteristic* 0*. Does there exists an integer* M *such that every* k*-Büchi sequence in* A *of length* M *is trivial?*

Observe that if $\mathbf{B}^k(A)$ has a positive answer, then for any subring B of A, $\mathbf{B}^k(B)$ has a positive answer. In this thesis, we are interested in those rings for which Büchi's problem has a negative answer in a *non-trivial way* (intuitively, rings with not too many k-powers). For example, if $A = \bar{\mathbb{Q}}$ is the field of algebraic numbers, every sequence of the form

$$\left(x_1, x_2, x_3 = \sqrt{2 + 2x_2^2 - x_1^2}, \ldots, x_M = \sqrt{2 + 2x_{M-1}^2 - x_{M-2}^2}, \ldots\right)$$

is a 2-Büchi sequence (which, in general, is non-trivial). With a similar idea, one sees easily that $\mathbf{B}^k(\bar{\mathbb{Q}})$ has a negative answer for every $k \geq 2$. The sequence

$$(\sqrt[k]{n^k+1})_{n\geq 0}$$

being a non-trivial k-Büchi sequence of infinite length, we see that $\mathbf{B}^k(\bar{\mathbb{Z}}\cap\mathbb{R})$ has a negative answer for every $k \geq 2$. In both examples above, the negative answer to Büchi's problem is due to the existence of an infinite non-trivial Büchi sequence.

In their survey [11] on Büchi's problem, Pasten, Pheidas and Vidaux posed the problem of finding rings for which Büchi's problem had a negative answer without having non-trivial sequences of infinite length. They distinguish two kinds of rings in which Büchi's problem can have a negative answer (in characteristic 0):

- **Type 1**: Rings for which there exists an infinite non-trivial Büchi sequence.
- **Type 2**: Rings for which there exist non-trivial Büchi sequences of any finite length, but there is no infinite one.

In [1], J. Browkin proved that for $k = 2$, the field of p-adic numbers $\mathbb{Q}_p$ is of type 1 and the ring of p-adic integers $\mathbb{Z}_p$ is of type 2. This Thesis is an attempt to generalize Browkin's result to higher powers. Before we state our main results, let us introduce the notion of an Hensley sequence:

Definition (Hensley sequences)**.** *Let $k \geq 0$ be an integer. A sequence (a_n) of elements of a unitary commutative ring A of characteristic 0, whose k-th powers are of the form*

$$(a+n)^k + b_{k-2}n^{k-2} + \cdots + b_1 n + b_0,$$

for some $a, b_{k-2}, \ldots, b_0 \in A$, is called k-Hensley sequence*. If*

$$b_0 = \cdots = b_{k-2} = 0$$

then (a_n) is called a trivial k-Hensley sequence*.*

Problem (Hensley's formulation of Büchis's problem)**.** $\mathbf{HF}^k(A)$*. Let $k \geq 2$ be an integer and A a unitary commutative ring of characteristic 0. Does there exist an integer $M \geq k+1$ such that every k-Hensley sequence in A of length M is a trivial sequence?*

In this thesis we consider the following weaker problem, known as Hensley's problem:

Problem. HP$^k(A)$. *Let $k \geq 2$ be an integer and A a unitary commutative ring of characteristic 0. Does there exist an integer M such that, for any fixed elements a and b in A, if the quantities*

$$(n+a)^k + b$$

are k-th powers for $n = 1, \ldots, M$, then $b = 0$?

It is well known that the multiplicative group of invertibles in the ring of integers modulo n is a cyclic group if and only if $n = 2$, or $n = 4$, or n is of the form p^m, or n is of the form $2p^m$, for some odd prime p and some positive integer m. When the group is cyclic, we call *a primitive root modulo* n any integer whose congruence class modulo n is a generator of it.

In order to state our Main Theorem, we need to introduce the following notation:

Notation. *1. We will write*

$$q = q(p,k) = p^{\varepsilon+1+ord_p k},$$

where ε is equal to 1 if $p = 2$ and is equal to 0 if $p \neq 2$.

2. We will say that the condition $C(p,k)$ is satisfied *if there exists a primitive root modulo q, say g, such that*

$$x^k + y^k \equiv g \bmod q$$

for some integers x and y whose congruence classes modulo q are in $(\mathbb{Z}/q\mathbb{Z})^\times$.

The condition $C(p,k)$ is (trivially) not satisfied when q is of the form 2^m for $m \geq 3$, simply because there is no primitive root at all in that case (we do not know whether there exists any other pair (p,k) for which the condition is not satisfied). From the following well-known theorem (see for example [19]), we see that the condition $C(p,k)$ is satisfied when $q > (k-1)^4$ and, either p is an odd prime, or $p = 2$ and $\operatorname{ord}_p k = 0$.

Theorem. *Let $\mathbb{F}_p$ be a finite field with p elements and $k \geq 2$ an integer. If $p > (k-1)^4$, then every diagonal form of degree k in two variables over $\mathbb{F}_p$ is universal.*

Note also that whenever $g = 2$ is a primitive root modulo q then, by choosing $x = y = 1$, the condition $C(p, k)$ is trivially satisfied.

We can now state our main results.

Theorem (Main Theorem)**.** *Let p be a prime number and $k \geq 2$ an integer.*

1. *For each $n \in \mathbb{Z}$, when $p > 2$ the quantity $n^k + p^{-k}$ is a k-th power in $\mathbb{Q}_p$. Moreover, any sequence (a_n), $n \geq 1$, such that a_n has k-th power $n^k + p^{-k}$, is a non-trivial k-Büchi sequence of infinite length in $\mathbb{Q}_p$.*

2. *For each $n \in \mathbb{Z}$, the quantity $n^k + 2^{-(2+k)}$ is a k-th power in $\mathbb{Q}_2$. Moreover, any sequence (a_n), $n \geq 1$, such that a_n has k-th power $n^k + 2^{-(2+k)}$, is a non-trivial k-Büchi sequence of infinite length in $\mathbb{Q}_2$.*

3. *For each $m \in \mathbb{Z}$, the quantity $n^k + p^{mk+1}$ is a k-th power in $\mathbb{Z}_p$ when $n = 1, \ldots, p^m - 1$. Moreover, if $p^m \geq k + 2$, then any sequence (a_n), $n = 1, \ldots, p^m - 1$, where a_n has k-th power $n^k + p^{mk+1}$, is a non-trivial k-Büchi sequence in $\mathbb{Z}_p$.*

4. *Suppose that Condition $C(p, k)$ is satisfied and, either k is not coprime to p, or p is odd and k is not coprime to $p - 1$. Let a and b be p-adic integers. If for every $n \geq 1$ the quantity*

$$(n + a)^k + b$$

is a k-th power in $\mathbb{Z}_p$, then $b = 0$.

Items 1 and 2 show that $\mathbb{Q}_p$ is of type 1. Item 3 shows that in $\mathbb{Z}_p$ there exist non-trivial Büchi sequences of any finite length. Item 4 shows that, when the hypothesis on p and k is satisfied, there is no infinite non-trivial Büchi sequence in $\mathbb{Z}_p$ whose sequence of k-th powers is of the form $\big((n + a)^k + b\big)_n$, for some a and b in $\mathbb{Z}_p$.

When $k = 2$, the Main Theorem was recently proven by J. Browkin in [1]. We essentially adapt his techniques to higher powers. In Chapter 1 we will introduce the basic tools that we need to prove the Main Theorem. In Chapter 2, we give a characterization of the set of k-th powers in $\mathbb{Z}_p$, for each k and p, and prove some properties of these sets. In Chapter 3, we will prove Items 1, 2 and 3 of the Main Theorem. We will prove the Item 4 of the Main Theorem in Chapter 4.

Chapter 1

Preliminaries: p-adic numbers

All the results in this section are well-known. See for example [4], [6] or [14].

Fix a prime number p.

Definition 1.1. *The* p-adic valuation $\operatorname{ord}_p a$ *(or* p*-adic order) of an integer* a *is the highest power of* p *which divides* a*, or equivalently, the highest integer* m *such that* $a \equiv 0 \bmod p^m$*.*

If $a = 0$, we write $\operatorname{ord}_p a = \infty$, where ∞ is a symbol such that for every $x \in \mathbb{Z}$, we have $x < \infty$ and $\infty + x = x + \infty = \infty$. The p-adic valuation on $\mathbb{Z}$ extends in a unique way to a valuation on $\mathbb{Q}$ by letting

$$\operatorname{ord}_p \left(\frac{a}{b}\right) = \operatorname{ord}_p(a) - \operatorname{ord}_p(b).$$

Note that this definition does not depend on the choice of a and b.

Let K be a field. A norm $||\ ||$ on K is called *non-Archimedean* if for all $x, y \in K$ we have

$$||x + y|| \leq \max\left(||x||, ||y||\right).$$

The *trivial norm* on K is the norm that sends 0 to 0 and every non-zero x to 1. The map

$$|x|_p = \begin{cases} p^{-\operatorname{ord}_p x} & \text{if } x \neq 0 \\ 0 & \text{if not,} \end{cases}$$

called the *p-adic norm*, is a non-Archimedean norm on $\mathbb{Q}$. The p-adic norm induces a metric d_p on $\mathbb{Q}$, defined as usual by $d_p(x, y) = |x - y|_p$. We call this metric the *p-adic metric*.

Given a non-Archimedean norm $||\ ||$ on a field K, following [14], we will call

$$B(a,r) = \{x \in K : ||x-a|| < r\},$$

the *stripped ball of radius* $r > 0$ *and center* $a \in K$ and

$$\bar{B}(a,r) = \{x \in K : ||x-a|| \leq r\}$$

the *dressed ball of radius* r *and center* a. In this context, one can show that all balls are clopen sets and that any point in a ball is a center of the ball.

In a field K, two metrics d_1 and d_2 are said to be *equivalent* if any sequence which is a Cauchy sequence with respect to d_1 is a Cauchy sequence with respect to d_2, and vice-versa. We say that two norms are *equivalent* if they induce equivalent metrics. For example, for every ρ in the open real interval $]0,1[$, the function defined by

$$|x| = \begin{cases} \rho^{\mathrm{ord}_p\, x} & \text{if } x \neq 0 \\ 0 & \text{if not} \end{cases}$$

is a non-Archimedean norm on $\mathbb{Q}$ which is equivalent to the p-adic norm.

If p_1 and p_2 are distinct prime numbers, then the p_1-adic norm is not equivalent to the p_2-adic norm.

Theorem 1.2 (Ostrowski's Theorem)**.** *Any norm in* $\mathbb{Q}$ *is equivalent to either the trivial norm, or the Archimedean norm, or the* p*-adic norm.*

A field K is called *complete* with respect to a metric d if every sequence which is a Cauchy sequence with respect to d has a limit in K. The field $\mathbb{Q}$ is not complete with respect to the p-adic norm.

Two Cauchy sequences (a_i) and (b_i) are *equivalent* if the p-adic distance $|a_i - b_i|_p$ between a_i and b_i tends to 0 as i tends to ∞.

Definition 1.3. *The field* $\mathbb{Q}_p$ *is the completion of* $\mathbb{Q}$ *with respect to the* p*-adic metric, i.e. it is the set of equivalence classes of sequences of elements of* $\mathbb{Q}$ *which are Cauchy sequences with respect to the* p*-adic metric, together with the field laws induced by the field laws of* $\mathbb{Q}$*. The elements of* $\mathbb{Q}_p$ *are called* p-adic numbers*.*

See for example [6] for a proof of the following Theorem.

Theorem 1.4. *Every equivalence class* $a \in \mathbb{Q}_p$ *for wich* $|a|_p \leq 1$ *has exactly one representative Cauchy sequence* $(a_i)_{i\geq 1}$ *that satisfies, for each* $i \in \mathbb{N}$*:*

1. $0 \leq a_i < p^i$; *and*

2. $a_i \equiv a_{i+1} \bmod p^i$.

If $|a|_p = p^m > 1$ then multiplying a by p^m we obtain a p-adic number $a' = ap^m$ that satisfies

$$|a'|_p = |ap^m|_p = p^{-m}|a|_p = 1.$$

The p-adic number a' is represented by a sequence (a'_i) (due Theorem 1.4) and $a = a'p^{-m}$ is represented by the sequence (a_i) where $a_i = a'_i p^{-m}$ for each i.

By Theorem 1.4, we can write

$$a'_i = b_0 + b_1 p + \cdots + b_{i-1}p^{i-1}$$

where the b_j are integers in $\{0, 1, 2, \ldots, p-1\}$. We notice that the condition $a'_i \equiv a'_{i+1} \bmod p^i$ means that

$$a'_{i+1} = b_0 + b_1 p + \cdots + b_{i-1}p^{i-1} + b_i p^i$$

for some integer b_i such that $0 \leq b_i < p$. Intuitively, a' can be seen as a number written in base p with infinite extension to the right. Finally we obtain

$$a = b_0 p^{-m} + b_1 p^{-(m-1)} + \cdots + b_{m-1}p^{-1} + b_m + b_{m+1}p + b_{m+2}p^2 + \ldots$$

which is called the *p-adic expansion* of a.

Note that for any $a \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$, the inequality

$$|a|_p \leq p^{-n}$$

says that the first non-zero digit of the p-adic expansion of a occurs no sooner than the p^n-th place.

Proposition 1.5. *1. The set of p-adic integers*

$$\mathbb{Z}_p = \Big\{ a \in \mathbb{Q}_p : |a|_p \leq 1 \Big\}$$

is a subring of $\mathbb{Q}_p$ (it is the dressed unit ball in $\mathbb{Q}_p$).

2. *The set $\mathbb{Z}_p$ is the set of p-adic numbers whose expansion do not have negative powers of p.*

3. *The ring $\mathbb{Z}_p$ is local with maximal ideal the stripped unit ball*

$$\left\{a \in \mathbb{Q}_p : |a|_p < 1\right\}$$

and, therefore, its multiplicative group of p-adic units *is the set*

$$\mathbb{Z}_p^{\times} = \left\{a \in \mathbb{Q}_p : |a|_p = 1\right\}.$$

4. *We have*

$$\begin{aligned} a + p^n\mathbb{Z}_p &= \{a + p^n x : x \in \mathbb{Z}_p\} \\ &= \left\{y \in \mathbb{Z}_p : |y - a|_p \leq p^{-n}\right\} \\ &= \bar{B}\left(a, p^{-n}\right) \\ &= B\left(a, p^{-(n-1)}\right) \end{aligned}$$

for each $a \in \mathbb{Z}_p$ and $n \in \mathbb{Z}$. Note that if $n > m$ then

$$\bar{B}(a, p^{-n}) \subsetneq \bar{B}(a, p^{-m}).$$

5. *The field $\mathbb{Q}$ can be identified with the subfield of $\mathbb{Q}_p$ which consists of the equivalence classes containing a constant Cauchy sequence.*

6. *The ring $\mathbb{Z}$ can be identified with the subring of $\mathbb{Z}_p$ which consists of the equivalence classes containing a constant Cauchy sequence.*

Proposition 1.6. *1. The (canonical) inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ has dense image.*

2. The (canonical) inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ has dense image. In particular, given $x \in \mathbb{Z}_p$ and $n \geq 1$, there is an integer α such that $0 \leq \alpha \leq p^n - 1$ and $|x - \alpha|_p \leq p^{-n}$. The integer α with these properties is unique.

From the proposition above and since density is a topological invariant, we deduce immediately that for each $a \in \mathbb{Z}_p$, the canonical inclusion $a + \mathbb{N} \hookrightarrow \mathbb{Z}_p$ has dense image.

Definition 1.7. *If a and b are p-adic numbers, we say that a is congruent to b modulo p^n, denoted by $a \equiv b \bmod p^n$, if $|a - b|_p \leq p^{-n}$.*

Note that $a, b \in \mathbb{Z}$ are congruent modulo p^n if and only if they are congruent modulo p^n when seen as elements of $\mathbb{Z}_p$.

The operations of addition, subtraction, multiplication and division in $\mathbb{Z}_p$ are very similar to the analogous operations with expansions of real numbers, and we will then not describe them.

We finish this section with two versions of Hensel's lemma. They are the main tools that we will use to compute, when possible, k-th roots of elements of $\mathbb{Q}_p$.

Theorem 1.8 (Hensel's lemma)**.** *Let*

$$F(x) = c_0 + c_1 x + ... + c_n x^n$$

be a polynomial function over $\mathbb{Z}_p$. Let

$$F'(x) = c_1 + 2c_2 x + ... + nc_n x^{n-1}$$

be the formal derivative of $F(x)$. If $a_0 \in \mathbb{Z}_p$ is such that

1. *$F(a_0) \equiv 0 \bmod p$; and*
2. *$F'(a_0) \not\equiv 0 \bmod p$.*

then there is a unique p-adic integer a such that

$$F(a) = 0 \text{ and } a \equiv a_0 \bmod p.$$

If for each a_0 in $\mathbb{Z}_p$ we have $F'(a_0)$ congruent to 0 modulo p, we use the following generalization of Hensel's lemma.

Theorem 1.9 (Generalized Hensel's lemma)**.** *Let*

$$F(x) = c_0 + c_1 x + \cdots + c_n x^n$$

be a polynomial function in $\mathbb{Z}_p$. Let

$$F'(x) = c_1 + 2c_2 x + \cdots + nc_n x^{n-1}$$

be the formal derivative of $F(x)$. If $a_0 \in \mathbb{Z}_p$ and M is an integer such that

1. *$F(a_0) \equiv 0 \bmod p^{2M+1}$,*
2. *$F'(a_0) \equiv 0 \bmod p^M$, and*
3. *$F'(a_0) \not\equiv 0 \bmod p^{M+1}$,*

then there is a unique p-adic integer a such that

$$F(a) = 0 \text{ and } a \equiv a_0 \bmod p^{M+1}.$$

Chapter 2

Powers in $\mathbb{Z}_p$ and in $\mathbb{Q}_p$

Fix an integer $k \geq 2$ for the whole chapter.

When p is an odd prime, Lemmas 2.1, 2.3 and Corollary 2.5 were shown to us by J. Browkin in a personal communication. There is an alternative (and much shorter) proof using the exponential function which covers all cases when p is odd and the case when $n > 1$ and p is 2 (the point is that the exponential function is a group isomorphism between the additive group $p^n\mathbb{Z}_p$ and the multiplicative group $1+p^n\mathbb{Z}_p$ whenever n is strictly bigger than $\frac{1}{p-1}$ - see [10, p. 38, Thm 1.2]). The case $p = 2$ and $n = 1$ needs to be done separately (see Lemmas 2.2 and 2.4).

Lemma 2.1. *Let $n \geq 1$ be an integer and suppose that either p is an odd prime or $n \neq 1$. The following equality holds:*

$$(1 + p^n\mathbb{Z}_p)^p = 1 + p^{1+n}\mathbb{Z}_p.$$

Proof. Let us prove that for all $c \in \mathbb{Z}_p$, the quantity $(1 + p^n c)^p$ belongs to the set $1 + p^{1+n}\mathbb{Z}_p$. We have

$$\begin{aligned}(1 + p^n c)^p &= 1 + p^{n+1}c + \sum_{j=2}^{p} \binom{p}{j} p^{jn} c^j \\ &= 1 + p^{n+1}\left(c + \frac{1}{p^{n+1}} \sum_{j=2}^{p} \binom{p}{j} p^{jn} c^j\right) \\ &= 1 + p^{n+1}\left(c + \sum_{j=2}^{p} \binom{p}{j} p^{n(j-1)-1} c^j\right),\end{aligned}$$

and since $n \geq 1$, the quantity

$$\sum_{j=2}^{p} \binom{p}{j} p^{n(j-1)-1} c^j$$

belongs to $\mathbb{Z}_p$.

Let us prove the other inclusion. Given $c \in \mathbb{Z}_p$ we want to find $b \in \mathbb{Z}_p$ such that

$$(1 + p^n b)^p = 1 + p^{1+n} c,$$

namely,

$$\sum_{j=1}^{p} \binom{p}{j} p^{jn} b^j = p^{1+n} c.$$

In order to apply Hensel's Lemma, we define the polynomial

$$f(x) = \frac{1}{p} \left(-pc + \sum_{j=1}^{p} \binom{p}{j} p^{(j-1)n} x^j \right).$$

We can write

$$\begin{aligned} f(x) &= -c + \sum_{j=1}^{p} \binom{p}{j} p^{(j-1)n-1} x^j \\ &= x - c + p \sum_{j=2}^{p} \binom{p}{j} p^{(j-1)n-2} x^j \end{aligned}$$

and since $n \geq 1$ and, either $p > 2$ or $n \neq 1$, the quantity

$$\sum_{j=2}^{p} \binom{p}{j} p^{(j-1)n-2} x^j$$

belongs to $\mathbb{Z}_p$. Therefore, $f(x)$ is congruent to $x - c$ modulo p. The derivative of f is given by

$$f'(x) = \sum_{j=1}^{p} \frac{j}{p} \binom{p}{j} p^{(j-1)n} x^{j-1}.$$

So finally, we have

$$f(c) \equiv 0 \bmod p$$

and

$$f'(c) = 1 + pd \not\equiv 0 \bmod p,$$

for some $d \in \mathbb{Z}_p$. By Hensel's Lemma, there exists $b \in \mathbb{Z}_p$ such that $f(b) = 0$, namely,

$$-pc + \sum_{j=1}^{p} \binom{p}{j} p^{(j-1)n} b^j = 0.$$

Multiplying by p^n we obtain

$$\sum_{j=1}^{p} \binom{p}{j} p^{jn} b^j = p^{1+n} c,$$

hence

$$(1 + p^n b)^p = 1 + p^{1+n} c.$$

□

Lemma 2.2. *The following equality holds:*

$$(1 + 2\mathbb{Z}_2)^2 = 1 + 8\mathbb{Z}_2$$

Proof. Given $c \in \mathbb{Z}_2$, we have

$$(1 + 2c)^2 = 1 + 4c + 4c^2 = 1 + 4(c + c^2).$$

Since the first term of c and of c^2 are either both 1 or both a positive power of 2, the quantity $c + c^2 \in 2\mathbb{Z}_2$. Therefore we have

$$(1 + 2\mathbb{Z}_2)^2 \subseteq 1 + 8\mathbb{Z}_2.$$

As in Lemma 2.1, we use Hensel's Lemma to prove the other inclusion. Given $c \in \mathbb{Z}_p$, we shall prove that $1 + 8c$ is a square of some $1 + 2d$ with $d \in \mathbb{Z}_p$. Consider the function

$$f(x) = x^2 - (1 + 8c)$$

and its derivative

$$f'(x) = 2x.$$

We have

$$f'(1) = 2 \equiv 0 \bmod 2,$$

$$f'(1) = 2 \not\equiv 0 \bmod 2^2$$

and

$$f(1) = -8c \equiv 0 \bmod 2^3.$$

By Hensel's Lemma, there exists $a \in \mathbb{Z}_2$ such that $f(a) = 0$ and

$$a \equiv 1 \bmod 2^2.$$

So, in particular, a belongs to $1 + 2\mathbb{Z}_2$. □

Lemma 2.3. *Let $n \geq 0$ be an integer and suppose that p is an odd prime. The following equality holds:*

$$(1 + p\mathbb{Z}_p)^{p^n} = 1 + p^{1+n}\mathbb{Z}_p. \tag{2.1}$$

Proof. Equality (2.1) is trivially true for $n = 0$. We prove the lemma by induction on n. By Lemma 2.1, we have

$$(1 + p\mathbb{Z}_p)^p = 1 + p^2\mathbb{Z}_p$$

and Equality (2.1) holds for $n = 1$.

Suppose that Equality (2.1) holds up to n and let us prove that it holds for $n + 1$. Indeed, we have

$$\begin{aligned}(1 + p\mathbb{Z}_p)^{p^{1+n}} &= \left((1 + p\mathbb{Z}_p)^{p^n}\right)^p \\ &= \left(1 + p^{1+n}\mathbb{Z}_p\right)^p \quad \text{(by induction hypothesis)} \\ &= 1 + p^{2+n}\mathbb{Z}_p \quad \text{(by Lemma 2.1).}\end{aligned}$$

□

Lemma 2.4. *For $n \geq 1$, the following equality holds:*

$$(1 + 2\mathbb{Z}_2)^{2^n} = 1 + 2^{2+n}\mathbb{Z}_2. \tag{2.2}$$

Proof. We prove the lemma by induction on n. By Lemma 2.2, we have

$$(1 + 2\mathbb{Z}_2)^2 = 1 + 8\mathbb{Z}_2$$

and Equality 2.2 holds for $n = 1$.

Suppose that Equality (2.2) holds up to n and let us prove that it holds for $n + 1$. Indeed, we have

$$\begin{aligned}(1 + 2\mathbb{Z}_2)^{2^{1+n}} &= \left((1 + 2\mathbb{Z}_2)^{2^n}\right)^2 \\ &= \left(1 + 2^{2+n}\mathbb{Z}_2\right)^2 \quad \text{(by induction hypothesis)} \\ &= 1 + 2^{3+n}\mathbb{Z}_2,\end{aligned}$$

where the last equality comes from the fact that $2 + n \neq 1$ and we can therefore apply Lemma 2.1. □

Corollary 2.5. *For all integers $k \geq 2$ and p an odd prime, the following equalities hold:*

$$(1 + p\mathbb{Z}_p)^k = 1 + p^{1+\mathrm{ord}_p\, k}\mathbb{Z}_p$$

and

$$(1 + 2\mathbb{Z}_2)^k = 1 + 2^{2+\mathrm{ord}_2\, k}\mathbb{Z}_2.$$

Proof. Write $k = p^{\mathrm{ord}_p\, k} r$, where p does not divide r. Since p does not divide r, the map $x \mapsto x^r$ defines an automorphism of the multiplicative group of one-units $1 + p\mathbb{Z}_p$ (see Hasse [5, Ch. 15, Section 2, p. 215-217]) - note that the existence of an r-th root comes immediately from Hensel's Lemma, hence the map $x \mapsto x^r$ is a surjective morphism. Indeed, Hasse defines a map

$$\begin{array}{ccc} 1 + p\mathbb{Z}_p & \longrightarrow & 1 + p\mathbb{Z}_p \\ x & \longmapsto & x^c \end{array}$$

for any $c \in \mathbb{Z}_p$ and shows that it is an homomorphism of groups. Since r is invertible in $\mathbb{Z}_p$, the above map with $c = \frac{1}{r}$ is the reciprocal of $x \mapsto x^r$, which, therefore, is injective.

For $p > 2$, Lemma 2.3 gives

$$(1 + p\mathbb{Z}_p)^k = ((1 + p\mathbb{Z}_p)^r)^{p^{\mathrm{ord}_p\, k}} = (1 + p\mathbb{Z}_p)^{p^{\mathrm{ord}_p\, k}} = 1 + p^{1+\mathrm{ord}_p\, k}\mathbb{Z}_p,$$

and for $p = 2$ we apply Lemma 2.4 and find

$$(1 + 2\mathbb{Z}_2)^k = ((1 + 2\mathbb{Z}_2)^r)^{2^{\mathrm{ord}_2\, k}} = (1 + 2\mathbb{Z}_2)^{2^{\mathrm{ord}_2\, k}} = 1 + 2^{2+\mathrm{ord}_2\, k}\mathbb{Z}_2.$$

□

Notation 2.6. *1. Let ε be 1 if $p = 2$ and 0 if $p \neq 2$.*

2. We will denote by S_p^k the set of non-zero k-th powers in $\mathbb{Z}_p$.

Lemma 2.7. *Let $g \in \mathbb{N}$ be a fixed primitive root modulo p. We have*

$$S_p^k = \left\{ p^{km} g^{k\ell} (1 + p^{\varepsilon+1+\mathrm{ord}_p\, k} c) \colon m \geq 0, \ell \geq 0, c \in \mathbb{Z}_p \right\}$$

Proof. Let α be a non-zero k-th power in $\mathbb{Z}_p$, i.e. there is an integer $m \geq 0$ and there exist $\beta \in \mathbb{Z}_p^\times$ such that

$$\alpha = p^{km} \beta^k.$$

Since $\beta \in \mathbb{Z}_p^\times$, there are integers $a_i \in \{0, 1, \ldots, p-1\}$ such that

$$\beta = a_0 + a_1 p + a_2 p^2 + \ldots$$

where $a_0 \neq 0$. Since the residue class modulo p of a_0 is not 0, it is generated by the residue class of g in $\mathbb{F}_p^\times$, so there exists an integer $\ell \geq 0$ and an integer z such that $a_0 = g^\ell + pz$. We have

$$\begin{aligned}\beta &= (g^\ell + pz) + a_1 p + a_2 p^2 + a_3 p^3 + \dots \\ &= g^\ell \left(1 + p\left(\frac{1}{g^\ell}(z + a_1 + a_2 p + a_3 p^2 + \dots)\right)\right).\end{aligned}$$

Write

$$c = \frac{1}{g^\ell}(z + a_1 + a_2 p + a_3 p^2 + \dots).$$

Since $\mathrm{ord}_p(c) \geq 0$, we conclude that, for all non-zero k-th power α, there are integers $m \geq 0$ and $\ell \geq 0$, and a p-adic integer c such that

$$\alpha = p^{km} g^{k\ell} (1 + pc)^k$$

On the other hand, for all $c \in \mathbb{Z}_p$, the quantity $p^{km} g^{k\ell}(1+pc)^k$ is trivially a k-th power. Finally we have

$$S_p^k = p^{km} g^{k\ell}(1 + p\mathbb{Z}_p)^k = p^{km} g^{k\ell}(1 + p^{\varepsilon+1+\mathrm{ord}_p\, k}\mathbb{Z}_p),$$

by Corollary 2.5. □

Remark 2.8. *1. Note that when $p = 2$ one can choose $g = 1$ in the above characterization.*

2. Also, whenever p is odd, we can use in the above characterization a primitive root modulo p^n, for some integer $n \geq 1$, instead of g.

3. If $x \in \mathbb{Z}_p$ is a k-th power, then $\mathrm{ord}_p\, x$ is a multiple of k.

Note that we have

$$\begin{aligned}S_p^k &= \bigcup_{\ell\geq 0}\bigcup_{m\geq 0}\left\{p^{km}g^{k\ell}\left(1 + p^{\varepsilon+1+\mathrm{ord}_p\, k}c\right) : c \in \mathbb{Z}_p\right\} \\ &= \bigcup_{\ell\geq 0}\bigcup_{m\geq 0}\left\{p^{km}g^{k\ell} + p^{km+\varepsilon+1+\mathrm{ord}_p\, k}c : c \in \mathbb{Z}_p\right\} \\ &= \bigcup_{\ell\geq 0}\bigcup_{m\geq 0}\bar{B}\left(p^{km}g^{k\ell}, p^{-(km+\varepsilon+1+\mathrm{ord}_p\, k)}\right).\end{aligned}$$

Since in $\mathbb{Z}_p$ all balls are open sets, we conclude that S_p^k is open as a union of open sets.

Notation 2.9. *Given a prime number p and an integer $k \geq 2$, we will write*

$$\bar{S_p^k} = S_p^k \cup \{0\}\,.$$

Lemma 2.10. *For each prime number p and integer $k \geq 2$, the set $\bar{S}_p^k$ of k-th powers in $\mathbb{Z}_p$ is closed.*

Proof. Let (b_n^k) be a sequence of k-th powers with limit $a \in \mathbb{Z}_p$. We prove that a is a k-th power. If $a = 0$ there is nothing to prove, so we may suppose $a \neq 0$. Fix N large enough so that for each $n > N$, $\operatorname{ord}_p a = \operatorname{ord}_p(b_n^k) = k \operatorname{ord}_p(b_n)$. Consider the polynomial $f(x) = x^k - a$, with derivative $f'(x) = kx^{k-1}$. For $n > N$,

$$s = \operatorname{ord}_p k + (k-1) \operatorname{ord}_p b_n = \operatorname{ord}_p k + (k-1)\frac{\operatorname{ord}_p a}{k}$$

does not depend on n and is the order of $f'(b_n)$ at p. So we have

$$f'(b_n) \equiv 0 \bmod p^s \quad \text{and} \quad f'(b_n) \not\equiv 0 \bmod p^{s+1}.$$

Since (b_n^k) tends to a we can choose n large enough so that $b_n^k - a$ is congruent to 0 modulo p^{2s+1}. We deduce from Hensel's Lemma that f has a root in $\mathbb{Z}_p$, hence a is a k-th power.

□

Chapter 3

Büchi sequences in $\mathbb{Z}_p$ and $\mathbb{Q}_p$ for any power

Fix an integer $k \geq 2$ for the whole chapter.

Notation 3.1. *The notation $\sqrt[k]{x}$ will refer to any specific k-th root of x.*

Lemma 3.2. *For any prime number p and for any non-zero $b \in \mathbb{Q}_p$, the sequence (a_n) defined by*

$$a_n = \sqrt[k]{n^k - b}, \qquad 1 \leq n \leq M$$

is a non-trivial Büchi sequence over the algebraic closure of $\mathbb{Q}_p$, whenever $M \geq k$.

Proof. If (a_n) is trivial then, by definition, there exists $x \in \bar{\mathbb{Q}}_p$ such that

$$n^k - b = (x + n)^k$$

for each $n \geq 1$. If $x = 0$ then trivially $b = 0$, and if x is non-zero then b is a polynomial in n of degree $k - 1 \geq 1$, which is impossible since the sequence has length greater than $k - 1$. □

Proof of Item 1 of the Main Theorem. By Lemma 3.2 we need only prove that for each integer $n \in \mathbb{Z}$, the quantity $n^k + p^{-k} \in \mathbb{Q}_p$ is a k-th power in $\mathbb{Q}_p$, which is equivalent to prove that $p^k n^k + 1$ is a k-th power in $\mathbb{Z}_p$. For each k and p we have

$$k \geq 1 + \operatorname{ord}_p k,$$

hence the quantity

$$c = p^{k-1-\operatorname{ord}_p k} n^k$$

is a p-adic integer and we deduce that

$$1 + p^k n^k = 1 + p^{1+\operatorname{ord}_p k} \left(p^{k-1-\operatorname{ord}_p k} n^k \right)$$

is a k-th power by Lemma 2.7. □

Proof of Item 2 of the Main Theorem. By Lemma 3.2 we need only prove that for each integer $n \in \mathbb{Z}$, the quantity $n^k + 2^{-(2+k)}$ is a k-th power in $\mathbb{Q}_2$, which is equivalent to prove that $2^{2+k} n^k + 1$ is a k-th power in $\mathbb{Z}_2$. Since for each k we have $k \geq \operatorname{ord}_2 k$, we deduce that

$$c = 2^{k-\operatorname{ord}_2 k} n^k$$

is a p-adic integer and therefore

$$1 + 2^{2+k} n^k = 1 + 2^{2+\operatorname{ord}_2 k} \left(2^{k-\operatorname{ord}_2 k} n^k \right)$$

is a k-th power by Lemma 2.7. □

Proof of Item 3 of the Main Theorem. By Lemma 3.2 we need only prove that for every $m \geq 1$, the quantity

$$n^k + p^{km+1}$$

is a k-th power in $\mathbb{Z}_p$ for $n = 1, \ldots, p^m - 1$. By Lemma 2.7, since

$$n^k + p^{km+1} = n^k \left(1 + p^{2+\operatorname{ord}_p k} \frac{p^{km-1-\operatorname{ord}_p k}}{n^k} \right)$$

we need only prove that the quantity

$$\frac{p^{km-1-\operatorname{ord}_p k}}{n^k}$$

is a p-adic integer. Since $n < p^m$, we have $\operatorname{ord}_p n \leq m - 1$, hence

$$\operatorname{ord}_p n^k \leq km - k \leq km - (1 + \operatorname{ord}_p k).$$

Finally we obtain

$$\operatorname{ord}_p \left(\frac{p^{km-1-\operatorname{ord}_p k}}{n^k} \right) = km - (1 + \operatorname{ord}_p k) - \operatorname{ord}_p n^k \geq 0.$$

□

Note that the sequence used for the above proof can not be extended to an infinite sequence. Actually, if $n = p^{m+1}$, then

$$\begin{aligned}
\mathrm{ord}_p\left(n^k + p^{km+1}\right) &= \mathrm{ord}_p\left(p^{km+k} + p^{km+1}\right) \\
&= \min\left\{\mathrm{ord}_p\left(p^{km+k}\right), \mathrm{ord}_p\left(p^{km+1}\right)\right\} \\
&= km + 1
\end{aligned}$$

which is not a multiple of k, therefore, by Remark 2.8, $n^k + p^{km+1}$ is not a k-th power in $\mathbb{Z}_p$.

Chapter 4

Non-existence of infinite Hensley sequences in $\mathbb{Z}_p$

Fix an integer $k \geq 2$. Recall that $q = q(p,k) = p^{\varepsilon+1+\mathrm{ord}_p\, k}$ where ε is equal to 1 if $p = 2$ and is equal to 0 if $p \neq 2$.

Proof of Item 4 of the Main Theorem. Let p be any prime number. Let a and b be p-adic integers and suppose that for any integer $n \geq 1$ the quantity

$$(n+a)^k + b$$

is a k-th power in $\mathbb{Z}_p$. For the sake of contradiction, we suppose $b \neq 0$.

Suppose first that b is not a k-th power. Since the set $\bar{S_p^k}$ of the k-powers in $\mathbb{Z}_p$ is closed (by Lemma 2.10) and b does not belong to $\bar{S_p^k}$, there exists a positive real number δ such that $B(b,\delta) \cap \bar{S_p^k}$ is empty. Since

$$|(a+n)^k|_p = |a+n|_p^k,$$

and $a + \mathbb{N}$ is dense in $\mathbb{Z}_p$, we can choose n such that

$$|a+n|_p < \sqrt[k]{\delta}.$$

This implies that $(a+n)^k + b$ belongs to the (stripped) ball $B(b,\delta)$, i.e.,

$$(a+n)^k + b$$

is not a k-th power. It is a contradiction, since by hypothesis $(a+n)^k + b$ is a k-th power for every integer $n \geq 1$.

Suppose now that b is a k-th power, and recall that by hypothesis, Condition $C(p,k)$ is satisfied, that is, there exists a primitive root modulo q, say g (that we choose as small as possible and positive), such that

$$x^k + y^k \equiv g \bmod q,$$

for some integers x and y whose congruent classes modulo q are in $(\mathbb{Z}/q\mathbb{Z})^\times$. Hence, there exist integers $\alpha \geq 0$ and $\beta \geq 0$ such that

$$g^{k\alpha} + g^{k\beta} \equiv g \bmod q.$$

Multiplying by $g^{k\ell - k\alpha}$ and writing $t = \beta + \ell - \alpha$ and $r = \ell - \alpha$ we get

$$g^{k\ell} + g^{kt} \equiv g^{1+kr} \bmod q,$$

hence

$$g^{k\ell} + g^{kt} = g^{1+kr} + qz$$

for some $z \in \mathbb{Z}$.

On the other hand, since b is a k-th power, there exist integers $m \geq 0$ and $\ell \geq 0$, and a p-adic integer c_1 such that

$$b = p^{km} g^{k\ell}(1 + qc_1).$$

From the density of the set $\mathbb{N} + a$ in $\mathbb{Z}_p$, we can choose $n \in \mathbb{N}$ such that for any $x \in \mathbb{Z}_p$, the quantity $n + a$ is as close as we want to $p^m g^t(1 + qx)$. Therefore, there exists n such that $n + a$ actually belongs to $p^m g^t(1 + q\mathbb{Z}_p)$, that is,

$$n + a = p^m g^t(1 + qc_2)$$

for some $c_2 \in \mathbb{Z}_p$. We have

$$\begin{aligned}
(n+a)^k + b &= p^{km} g^{kt}(1 + qc_3) + p^{km} g^{k\ell}(1 + qc_1) \\
&= p^{km}\left(g^{kt} + g^{k\ell} + g^{kt} qc_3 + g^{k\ell} qc_1\right) \\
&= p^{km}\left(g^{1+kr} + qz + g^{kt} qc_3 + g^{k\ell} qc_1\right) \\
&= p^{km} g^{1+kr}\left(1 + q\left(\frac{z + g^{kt} c_3 + g^{k\ell} c_1}{g^{1+kr}}\right)\right) \\
&= p^{km} g^{1+kr}(1 + qc_4),
\end{aligned}$$

for some c_3 and c_4 in $\mathbb{Z}_p$, where the last equality comes from the fact that $\operatorname{ord}_p g^{1+kr}$ is equal to zero. Since $p^{km} g^{1+kr}(1 + qc_4)$ is a k-th power and has order km at p, it can be written as

$$p^{km} g^{ks}(1 + qc_5)$$

for some $s \geq 0$ and $c_5 \in \mathbb{Z}_p$. Hence we have

$$g^{1+kr} - g^{ks} = qc_6$$

for some $c_6 \in \mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$. Write c_6 as $\alpha\beta^{-1}$, where α and β are coprime integers such that $\beta > 0$ is coprime with p. We have then

$$\beta(g^{1+kr} - g^{ks}) = \alpha q.$$

Since $1 + kr$ is distinct from ks, β divides $\alpha q \neq 0$. Hence $\beta = 1$ and the equation becomes

$$g^{1+kr} - g^{ks} = \alpha q.$$

Since g is a primitive root modulo q, it is coprime with p. Hence, if $1+kr > ks$ then q divides $g^{1+kr-ks}-1$, and if $1+kr < ks$ then q divides $1-g^{ks-1-kr}$. So in any case, the quantity $g^{|ks-1-kr|}$ is congruent to 1 modulo q. Therefore, denoting by φ the Euler totient function, $\varphi(q) = p^{\varepsilon+\operatorname{ord}_p k}(p-1)$ divides $|1 + k(r - s)|$, which is a contradiction if $\operatorname{ord}_p k$ is not 0 (because $p^{\operatorname{ord}_p k}$ divides k). If p is odd then $\varepsilon = 0$ and $p - 1$ divides $|1 + k(r - s)|$, which is impossible if k is not coprime with $p - 1$.

□

Bibliography

[1] J. Browkin, *Büchi sequences in local fields and local rings*, Bull. Polish Acad. Sci. Math. **58**, 109-115 (2010).

[2] M. Davis, *Hilbert's tenth problem is unsolvable*, American Mathematical Monthly **80**, 233-269 (1973).

[3] M. Davis, Y. Matiyasevich and J. Robinson, *Hilbert's Tenth Problem. Diophantine equations: positive aspects of a negative solution*, Proceedings of Symposia in Pure Mathematics **28**, 323-378 (1976).

[4] F. Q. Gouvêa, *P-Adic numbers, an introduction*, Springer-Verlag (1993).

[5] H. Hasse, *Number Theory*, Springer (1980).

[6] N. Koblitz, *P-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer Graduate Texts in Mathematics, 1996.

[7] H. Koch, *Number theory: algebraic numbers and functions*, Graduate Studies in Mathematics, v. 24, AMS, 2000.

[8] L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations*, in The collected works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.) Springer, 677-680, (1990).

[9] Y. Matiyasevich, *Enumerable sets are diophantine*, Doklady Akademii Nauk SSSR, **191**, 279-282 (1970); English translation, Soviet Mathematics Doklady **11**, 354-358 (1970).

[10] J. Neukirch, *Class field theory*, Springer Verlag, Grundlehren der mathematischen Wissenschaften **280**, A Series of Comprehensive Studies in Mathematics (1986).

[11] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, Zapiski Nauchn. Sem. POMI **377**, 111-140 (2010).

[12] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem : Questions of decidability for addition and n-th powers*, Fundamenta Mathematicae **185**, 171-194 (2005).

[13] —— *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific Journal of Mathematics **238-2**, 349-366 (2008).

[14] A. Robert *A course in p-adic analysis*, Springer Graduate Texts in Mathematics (2000).

[15] C. L. Siegel, *Generalization of Waring's Problem to Algebraic Number Fields*, American Journal of Mathematics **66-1**, 122-136 (1944).

[16] K. Szymiczek, *Bilinear algebra: an introduction to the algebraic theory of quadratic forms*, Algebra, Logic and Applications series, v. 7, CRC (1997).

[17] R. C. Vaughan and T. D. Wooley, *Waring's Problem: A Survey*.

[18] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem*, Contemporary Mathematics **270**, 261-274 (2000).

[19] Christiaan Evert van de Woestijne, *Deterministic equation solving over finite fields*, (1975).