Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Matemáticas

Lema de Hensel y números *p*-ádicos

Autor: Claudia María González Iglesias

Tutor: Félix Delgado de la Mata

Índice general

Introducción

El trabajo tiene como objetivo la construcción, y el estudio de las principales propiedades, del cuerpo de números p-ádico y su correspondiente anillo de enteros. Los números p-ádicos son un tema central en la Teoría de Números y surgen del estudio de las soluciones de congruencias módulo p^n para un primo p fijo y n un entero positivo variable. Esta aproximación, que es la inicial de Hensel, se enriquece enormemente a través del hecho de que también se pueden ver como la compleción del cuerpo de los números racionales con la métrica p-ádica. Este resultado permite incorporar las potentes técnicas topológicas y analíticas al estudio de problemas aritméticos modulares en característica p y, a lo largo del siglo pasado, ha permitido una profunda comprensión de numerosos problemas, tanto aritméticos como geométricos.

El enfoque parte del estudio de las raíces de un polinomio entero, $f(X)$, módulo potencias de un primo; por tanto se trata de un punto de partida algebraico, estrechamente vinculado al Lema de Hensel. Fijado un primo p, a partir de una solución a_1 de la congruencia $f(X) \equiv 0 \mod p$ y bajo ciertas hipótesis, el Lema de Hensel permite calcular de forma inductiva (y efectiva) una sucesión $\{a_n\}_{n\geq 1}$ de manera que $f(a_n) \equiv 0 \mod p^n$. La sucesión, además, presenta condiciones de coherencia, en el sentido de que $a^m \equiv a^n \mod p^n$ si $m \geq n$. Esta sucesión, o su versión equivalente como sumas parciales de una serie p-ádica: $\sum_{n\geq 0} x_n p^n$, con $0 \leq x_n < p$; es la clave que permite identifcar el conjunto de soluciones $\{a_n\}$ en el sistema de anillos $\{\mathbb{Z}/p^n\}$ con una única "solución", α, pero en un nuevo anillo: el anillo de los enteros p-adicos $\mathbb{Z}_p$. Posteriormente el anillo de enteros p-ádicos se formaliza como el límite (proyectivo) del sistema de anillos, libro consultado Atiyah, Macdonald [1]. Dos hechos cruciales proporcionan la base matemática que sustenta nuestro nuevo objeto. El primero es que la expresión de α a través de la serie $\sum x_n p^n$ nos viene a decir que el nuevo número $\alpha = \sum x_n p^n$ se expresa en base p como $\ldots x_n x_{n-1} \ldots x_1 x_0$, de la misma forma que la parte decimal de un número real se expresa como una sucesión (o serie) infinita gracias a la expresión decimal en potencias de $1/10^n$. El segundo es que las propiedades de la valoración p-ádica de un entero (es decir, el número de veces que p divide a dicho entero) permiten, con un pequeño artificio, verla como una norma (no arquimediana en este caso, a diferencia del caso real).

A partir de aquí se comprende la naturalidad de la construcción del cuerpo de números p-ádico como compleción del cuerpo de los números racionales para la distancia p-ádica: exactamente siguendo los mismos pasos de la construcción de los números reales a partir de los racionales cuando consideramos el valor absoluto ordinario, libro consultado Fernández Viña [2]. Pero no sólo es importante la construcción, el desarrollo del análisis p-ádico ha proporcionado una herramienta esencial en la comprensión y resolución de numerosos problemas, tanto de Teoría de Números como de Geometría Algebraica, entre otras cosas por el sólido puente que abre de interacción de problemas puramente aritméticos en característica p con objetos geométricos sobre cuerpos de completos de característica cero.

Las razones anteriores son las que motivan que el desarrollo que hemos adoptado tome como punto de partida el Lema de Hensel. A partir de este primer contacto, en el capítulo uno se trata también una primera aproximación a las que luego serán las funciones exponencial y logaritmo, haciendo hincapié en algunas de sus utilidades para la resolución de algunos problemas aritméticos en los anillos cocientes $\mathbb{Z}/p^n$. Finalmente, este capítulo se cierra con un resulta-

do algebraico (aunque también tiene interesantes aplicaciones en el cálculo modular) sobre la estructura del grupo de unidades de los anillos $\mathbb{Z}/p^n$. Para ello son esenciales las funciones exponencial y logaritmo. Así pues, el primer capítulo se puede ver como aproximación o motivación del objeto que se formalizará en el resto de la memoria.

Las fuente principal de este capítulo es el libro de Hill [5], apoyado en algunos casos por el de Gouvea [4].

El segundo capítulo está dedicado a la construcción del cuerpo de números p-ádico, $\mathbb{Q}$, a partir de las sucesiones de Cauchy de números racionales con la métrica p-adica. Se ha adoptado este punto de vista debido a que es un método perfectamente conocido y que inmediatamente lleva a ver también el aspecto topológico y analítico del cuerpo p-ádico. La naturaleza ultramétrica de dicho espacio hace que algunas de las propiedades más elementales sean fácilmente accesibles. El capítulo se completa con algunas propiedades básicas del cuerpo p-ádico y de su anillo de enteros, tanto algebraicas como topológicas. Nuestra fuente principal en este capítulo ha sido el libro de Gouvea [4], con algunas consultas de textos más avanzados como Roberts [7].

El capítulo tres se dedica al estudio de propiedades más profundas, de hecho se vuelve sobre los mismos tres problemas que se plantean en el capítulo primero. Pero, ya disponemos del objeto natural en el que se plantean. Lo que anteriormente eran objetos hasta cierto punto intuitivos alcanzan ahora plena madurez matemática y se ven como naturales en el contexto del nuevo objeto construido. Esto es así sobre todo en lo que se refiere a la revisión del Lema de Hensel o a la naturalidad de las funciones exponencial y logaritmo. El desarrollo de este capítulo se apoya en los textos de Gouvea [4], Katok [6] y Hill [5].

Notaciones

A lo largo de la memoria usaremos las notaciones habituales para indicar los números naturales, enteros, racionales o reales. Dado un entero $m \in \mathbb{Z}$, el anillo cociente de $\mathbb{Z}$ por el ideal $(m) = m\mathbb{Z}$ lo denotaremos por $\mathbb{Z}/m\mathbb{Z}$ o símplemente por $\mathbb{Z}/m$. Los elementos de dicho anillo son las clases residuales $a+m\mathbb{Z}$, siendo a un entero, no obstante con frecuencia, abusando del lenguaje y cuando no de lugar a equívocos, trataremos un elemento de $\mathbb{Z}/m$ como uno de sus representantes, en este caso siempre supondremos que tomamos como representante de la clase $a+m\mathbb{Z}$ el único entero x congruente con a módulo m con la condición $0 \leq x < m$. Si A es un anillo, denotaremos por A^* al grupo (para el producto del anillo) de las unidades de A, en particular $(\mathbb{Z}/m)^*$ es el grupo de unidades de $\mathbb{Z}/m$ y sabemos que está formado por las clases de los enteros n tales que n es primo con m.

Para un número primo p el ideal $p\mathbb{Z}$ es maximal y por tanto su cociente es un cuerpo, usaremos también la notación $\mathbb{F}_p$ para denotarlo, es decir, $\mathbb{F}_p = \mathbb{Z}/p$. En este caso el grupo de unidades es $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ y sabemos que es un grupo cíclico de orden $p-1$.

En la expresión de un número racional como cociente de enteros supondremos, en general, que la fracción es irreducible. Es decir, que si indicamos $\frac{a}{b} \in \mathbb{Q}$ estamos suponiendo que $mcd(a,b) = 1$.

El localizado de $\mathbb{Z}$ en el ideal $p\mathbb{Z}$, $(\mathbb{Z} \setminus p\mathbb{Z})^{-1}\mathbb{Z}$, es un subanillo de $\mathbb{Q}$. Lo denotaremos por $\mathbb{Z}_{(p)}$ y como subconjunto de $\mathbb{Q}$ es

$$\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b\} \ .$$

Es un anillo local y su único ideal maximal es $p\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} \mid p \not| b \ p|a\}$. El grupo de unidades $\mathbb{Z}_{(p)}^*$ coincide con $\mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)}$, ya que el anillo es local, y está formado por las fracciones irreducibles $\frac{a}{b}$ tales que p no divide a a ni a b.

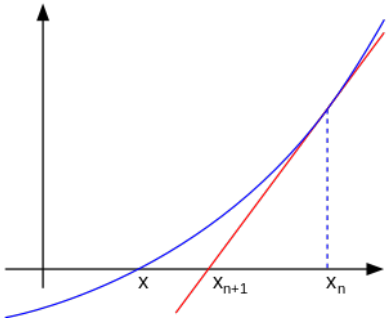
Capítulo 1

Algunos problemas aritméticos

1.1. Soluciones de congruencias. Lema de Hensel

La resolución de ecuaciones, es decir el cálculo de sus raíces, es uno de los problemas más habituales en matemáticas. Por ejemplo, si $f : \mathbb{R} \to \mathbb{R}$ es una función diferenciable y $\alpha \in \mathbb{R}$ es una raíz, $f(\alpha) = 0$, el método de Newton construye una sucesión $\{x_n\}$ de números reales que con "buenas" condiciones converge a α. Para ello partimos de una primera aproximación $x_1 \in \mathbb{R}$. Construimos la recta tangente de f en el punto x_1, esta es $y = f(x_1) + f'(x_1)(x - x_1)$. El punto donde se corta esta recta con el eje de las abscisas, le vamos a llamar x_2, es la nueva aproximación a la raíz. Calculamos ahora la recta tangente de f en el punto x_2.
Iteramos este proceso y obtenemos $f(x_n) + f'(x_n)(x_{n+1} - x_n) = 0$, despejando x_{n+1} de la expresión anterior llegamos a que

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$



El método de Newton asegura que, bajo ciertas hipótesis, si tomamos un x_1 suficientemente próximo a α entonces la sucesión $\{x_n\}$ converge hacia α.

1.1.1. Lema de Hensel

Nos planteamos ahora un problema diferente: dado un polinomio $f(X) \in \mathbb{Z}[X]$ y un número primo p queremos calcular una solución entera, a_n, de la congruencia $f(X) \equiv 0 \mod p^n$ para cada $n \geqslant 1$. Observamos que si tenemos una solución $f(a_n) \equiv 0 \mod p^n$ con $a_n \in \mathbb{Z}$ también es cierto que $f(a_n) \equiv 0 \mod p^r$ para todo $r \leq n$, además podemos suponer que $0 \leq a_n < p^n$, sustituyendo a_n por el resto de dividir a_n por p^n o por su clase en el anillo cociente $\mathbb{Z}/p^n\mathbb{Z}$.
Vemos cómo el método de Newton se puede utilizar con este fin a partir, en primer lugar, de un ejemplo. La idea es proceder de la siguiente manera;

- Partimos de un entero a_0 tal que $f(a_0) \equiv 0 \bmod p^r$, con r un entero "pequeño". Fijamos N, un entero, $N > r$.

- Definimos recursivamente
$$a_{n+1} := a_n - \frac{f(a_n)}{f'(a_n)}.$$

Esperamos que, para n suficientemente grande, $f(a_n) \equiv 0 \bmod p^N$.

Veamos ahora un ejemplo de este algoritmo:

Ejemplo 1. Tomamos el polinomio $f(X) = X^2 + 1$ y el primo $p = 5$. Comenzamos por un número entero a_0 que cumpla $f(a_0) \equiv 0 \bmod 5$. Evidentemente $a_0 = 2$ nos sirve. Como $f'(X) = 2X$, la fórmula recursiva anterior queda de la siguiente manera:

$$a_{n+1} = a_n - \frac{a_n^2 + 1}{2a_n} = \frac{a_n}{2} - \frac{1}{2a_n}\ .$$

Calculamos ahora los términos correspondientes a $n = 1$ y $n = 2$.

$$a_1 = \frac{a_0}{2} - \frac{1}{2a_0} = 1 - \frac{1}{4} = \frac{3}{4}$$
$$a_2 = \frac{a_1}{2} - \frac{1}{2a_1} = \frac{3}{8} - \frac{2}{3} = -\frac{5}{24}$$

Es claro que hemos operado con números racionales, $a_1 = 3/4$ no es un entero. Sin embargo, estamos buscando una solución módulo 5^k para un cierto k. Observamos que 5 no divide a 4. Por tanto 4 es inversible módulo 5^k para todo k. En particular, si ponemos $k = 2$ podemos calcular el inverso de 4 módulo $5^2 = 25$ y tenemos que $4^{-1} \equiv 19 \bmod 5^2$. Por tanto, operando módulo 5^2 tendremos que:

$$a_1 = 3/4 = 3 \cdot 4^{-1} \equiv 3 \cdot 19 \equiv 7 \bmod 5^2$$

y por consiguiente$f(a_1) = 7^2 + 1 = 50 \equiv 0 \bmod 5^2$.

De manera análoga $24^{-1} \equiv 99 \bmod 5^3$ y $a_2 = -7/24 = (-7) \cdot 99 \equiv 27 \bmod 5^3$. Ahora $f(a_2) = 57^2 + 1 = 3250 \equiv 0 \bmod 5^3$.

Démonos cuenta que para llevar a cabo este proceso lo que realmente hemos necesitado es que $f(a_0)/f'(a_0)$ (en la siguiente etapa $f(a_1)/f'(a_1)$) tenga sentido en $\mathbb{Z}/5^2\mathbb{Z}$ (resp. $\mathbb{Z}/5^3\mathbb{Z}$). Mejor aún, nos hemos encontrado en primer lugar con "soluciones racionales"que gracias a que están en el anillo local $\mathbb{Z}_{(p)}$ hemos podido reducir a soluciones en el anillo cociente $\mathbb{Z}/p^n\mathbb{Z}$. (Recordemos que $\mathbb{Z}_{(p)}$ es el localizado de $\mathbb{Z}$ en el ideal $p\mathbb{Z}$, es decir $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid p \not| b\}$).

Veamos que esta construcción no es una casualidad:

Sea $\bar{f} : \mathbb{Z} \longmapsto \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$ el homomorfismo de anillos composición del homomorfismo $f : \mathbb{Z} \longmapsto \mathbb{Z}_{(p)}$ con el paso al cociente $\pi : \mathbb{Z}_{(p)} \longmapsto \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$.
Sea $a \in \mathbb{Z}$ tal que $\bar{f}(a) = 0$, es decir $\bar{f}(a) \in p^n\mathbb{Z}_{(p)}$. Tenemos que $f(a) = \frac{a}{1} = p^n\frac{b}{s}$ con $a, b \in \mathbb{Z}$ y $s \notin p\mathbb{Z}$. Por lo tanto $(as - p^n b)u = 0$ con $u \notin p\mathbb{Z}$, es decir $asu = p^n bu$. Como s y u no son divisibles por p forzosamente p^n divide a a y entonces $a \in p^n\mathbb{Z}$. Así pues $ker\bar{f} = p^n\mathbb{Z}$.
Sea ahora $\frac{a}{s} \in \mathbb{Z}_{(p)}$. Puesto que p no divide a s tenemos que $mcd(p^n, s) = 1$ y s es inversible módulo p^n. Por lo tanto, existe un entero t tal que $st \equiv 1 \bmod p^n$, por tanto existe un entero k que cumple $st = 1 + kp^n$. Así pues $t = \frac{1}{s} + \frac{kp^n}{s}$ y $at = \frac{a}{s} + \frac{ak}{s}p^n$. Como consecuencia $(at - \frac{a}{s}) \in p^n\mathbb{Z}_{(p)}$ y tenemos que $\bar{f}(at) = \frac{a}{s} + p^n\mathbb{Z}_{(p)}$. Es decir, $\bar{f}$ es sobreyectiva.
Tenemos demostrado entonces:

Lema 1. $\mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$

Observación. El resultado anterior es equivalente a decir que si $\frac{a}{s}, \frac{b}{t} \in \mathbb{Z}_{(p)}$, se tiene que $\frac{a}{s} \equiv \frac{b}{t} \bmod p^n\mathbb{Z}_{(p)}$ si y solo si $at = bs$ módulo p^n. Es decir, hemos probado que las congruencias módulo $p^n\mathbb{Z}_{(p)}$ son equivalentes a las congruencias módulo p^n.

Como consecuencia de este hecho el problema se puede plantear de forma más natural en el anillo $\mathbb{Z}_{(p)}$, es decir que podemos partir de un polinomio $f \in \mathbb{Z}_{(p)}[X]$ y buscamos dar soluciones $a_n \in \mathbb{Z}_{(p)}$ tales que $f(a_n) \equiv 0 \bmod p^n\mathbb{Z}_{(p)}$, o si preferimos soluciones de $f(x) = 0$ en $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Las siguientes definiciones serán básicas en toda la memoria:

Definición 1. Sea p primo y n, m enteros, llameremos evaluación p-ádica de n al mayor entero b tal que $p^b|n$. Este valor sera ∞ si $n = 0$. A este valor lo denotaremos $v_p(n)$. Para un número racional $\frac{n}{m}$, definimos $v_p(\frac{n}{m}) = v_p(n) - v_p(m)$.

Nota. Observamos que si $r, s \in \mathbb{Q}$ se tiene que:
1) $v_p(rs) = v_p(r) + v_p(s)$.
2) $v_p(r + s) \geqslant \text{mín}\{v_p(r), v_p(s)\}$.
Con esta notación tenemos:

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geqslant 0\} \quad \text{y} \quad p^n\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geqslant n\}.$$

Además, $\mathbb{Z}^*_{(p)} = \{x \in \mathbb{Q} \,|\, v_p(x) = 0\}$.

El siguiente resultado establece las condiciones en las que el método de Newton del ejemplo anterior proporciona las soluciones que buscamos:

Teorema 1 (Lema de Hensel)**.** *Sea p un número primo y sea f un polinomio con coeficientes en $\mathbb{Z}_{(p)}$. Suponemos que existe $a_0 \in \mathbb{Z}_{(p)}$ con $f'(a_0) \neq 0$ tal que $f(a_0) \equiv 0 \mod p^{2c+1}$, donde $c = v_p(f'(a_0)) \geqslant 0$. Definimos de forma recursiva la sucesión $\{a_n\}_{n\geqslant 0}$ mediante la expresión*

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

Entonces, para $n \geqslant 0$ se tiene que $a_n \in \mathbb{Z}_{(p)}$ y, además,

$$f(a_n) \equiv 0 \mod p^{2c+2^n}.$$

Demostración. Razonaremos por inducción sobre n. Vamos a probar que se dan las siguientes tres afirmaciones para todo n.
a) $a_n \in \mathbb{Z}_{(p)}$ y $a_n \equiv a_0 \mod p^{c+1}$.
b) $v_p(f'(a_n)) = c$.
c) $f(a_n) \equiv 0 \mod p^{2c+2^n}$.
Notemos que probando esto estamos demostrando algo más fuerte de lo que dice el enunciado.

Para el caso en el que $n = 0$, se dan las tres afirmaciones por hipótesis. Supongamos ahora que se dan para a_n y veamos que se cumplen para a_{n+1} .

a) Denotemos $\delta := \frac{f(a_n)}{f'(a_n)}$. Los apartados c) y d) de la hipótesis de inducción implican que $v_p(f(a_n)) \geqslant 2c + 2^n$ y $v_p(f'(a_n)) = c$. Por lo tanto tenemos

$$v_p(\delta) = v_p(f(a_n)) - v_p(f'(a_n)) \geqslant c + 2^n.$$

Puesto que $c+1>0$, se tiene que $v_p(\delta)>0$, es decir $\delta\in\mathbb{Z}_{(p)}$ y también $a_{n+1}=a_n-\delta\in\mathbb{Z}_{(p)}$, ya que $a_n\in\mathbb{Z}_{(p)}$.
También se tiene que $a_{n+1}\equiv a_n \bmod p^{c+1}$, ya que $v_p(\delta)\geqslant c+1$. Puesto que $a_n\equiv a_0 \bmod p^{c+1}$ tenemos ya el apartado a).

b) Recordemos que por hipótesis tenemos que $v_p(f'(a_0))=c$. Esto significa que $f'(a_0)$ es un múltiplo de p^c, pero no es múltiplo de p^{c+1}, pues en otro caso la evaluación p-ádica de $f'(a_0)$ debería de se $c+1$. Por tanto tenemos que

$$f'(a_0)\equiv 0 \quad \text{mód } p^c \quad \text{y} \quad f'(a_0)\not\equiv 0 \quad \text{mód } p^{c+1}.$$

Por otro lado, ya hemos demostrado que, $a_{n+1}\equiv a_0 \ \text{mód } p^{c+1}$ y por consiguiente $f'(a_{n+1})\equiv f'(a_0) \ \text{mód } p^{c+1}$. Utilizando estas dos últimas resultados obtenemos que,

$$f'(a_{n+1})\equiv 0 \quad \text{mód } p^c \quad \text{y} \quad f'(a_{n+1})\not\equiv 0 \quad \text{mód } p^{c+1}.$$

Con esto concluimos $v_p(f'(a_{n+1}))=c$ y queda probado b).

Probamos ahora el apartado c). De la desigualdad $v_p(\delta)\geqslant c+2^n$ obtenemos que $v_p(\delta^2)\geqslant 2c+2^{n+1}$. Esta expresión la podemos reescribir como la congruencia,

$$\delta^2\equiv 0 \quad \text{mód } p^{2c+2^{n+1}}.$$

Sea $r\geqslant 0$ un entero. En la expresión binomial $(a_n-\delta)^r$ módulo $p^{2c}+2^{n+1}$, solo tenemos dos términos distintos de cero, esto es porque el resto de términos son múltiplos de δ^2, es decir:

$$a_{n+1}^r=(a_n-\delta)^r\equiv a_n^r-ra_n^{r-1}\delta \quad \text{mód } p^{2c+2^{n+1}}.$$

Por otro lado, escribimos el polinomio f como:

$$f(X)=\sum_{finita} c_rX^r$$

La evaluación de f en a_{n+1} nos queda:

$$\begin{aligned} f(a_{n+1}) &\equiv \sum_{finita} c_r(a_n^r-ra_n^{r-1}\delta) \quad \text{mód } p^{2c+2^{n+1}} \\ &\equiv \sum_{finita} c_ra_n^r-\left(\sum_{finita} c_rra_n^{r-1}\right)\delta \quad \text{mód } p^{2c+2^{n+1}} \\ &\equiv f(a_n)-f'(a_n)\delta\equiv 0 \quad \text{mód } p^{2c+2^{n+1}}. \end{aligned}$$

(Recordemos que $\delta=f(a_n)/f'(a_n)$). Con esto concluimos que $f(a_{n+1})\equiv 0 \ \text{mód } p^{2c+2^{n+1}}$ y queda demostrada la última afirmación.

□

Ejemplo 2. Tomamos el polinomio $f(X)=X^2+15$, el primo $p=2$ y $a_0=1$. Como la derivada del polinomio es $f'(X)=2X$, entonces $c=v_2(f'(a_0))=1$ y es evidente que $f(a_0)=1+15\equiv 0$ mód 2^3. Estamos en condiciones de aplicar el Lema de Hensel.
Los elementos de la sucesión son de la forma

$$a_{n+1}=a_n-\frac{a_n^2+15}{2a_n}=\frac{a_n}{2}-\frac{15}{2a_n}.$$

Calculamos ahora los términos a_1, a_2, a_3:

$$a_1 = \frac{a_0}{2} - \frac{15}{2a_0} = \frac{1}{2} - \frac{15}{2} = -7$$
$$a_2 = \frac{a_1}{2} - \frac{15}{2a_1} = -\frac{7}{2} + \frac{15}{14} = -\frac{17}{7}$$
$$a_3 = \frac{a_2}{2} - \frac{15}{2a_2} = -\frac{17}{14} + \frac{105}{34} = \frac{223}{119}$$

Ahora comprobamos que estos elementos de la sucesión son soluciones de la congruencia.

$$f(a_1) = (-7)^2 + 15 = 64 \equiv 0 \mod 2^4$$
$$f(a_2) = \left(-\frac{17}{7}\right)^2 + 15 = \frac{1024}{49} \equiv 0 \mod 2^6$$
$$f(a_3) = \left(\frac{223}{199}\right)^2 + 15 = \frac{262144}{14161} \equiv 0 \mod 2^{10}$$

Hemos llegado entonces a que -7, $-17/7$ y $223/119$ son raíces cuadradas de -15 módulo $16, 64$ y 1024 respectivamente. Por último, es evidente que los a_n calculados están en $\mathbb{Z}_{(2)}$ pues tanto 1, 7 y 119, que son los denominadores de a_1,a_2 y a_3, no son múltiplos de 2.

Nota. El Lema de Hensel proporciona una forma efectiva de construir una sucesión $\{a_n\}$ de elementos de $\mathbb{Z}_{(p)}$ que, partiendo de una aproximación inicial; a_1, "aproxima" cada vez más una raíz del polinomio $f(X)$ en el sentido de que si $m > n$ y $f(a_n) \equiv 0 \mod p^{r_n}$ entonces $f(a_m) \equiv 0 \mod p^{r_m}$ con $r_m > r_n$. Además, dicha sucesión mantiene una relación de "coherencia" modular expresada en el hecho de que $a_m \equiv a_n \mod p^{r_n}$. Es sencillo ver que gracias a esta propiedad podemos completar esta sucesión a una sucesión $\{\alpha_n\}$; $\alpha_n \in \mathbb{Z}_{(p)}$ de manera que $f(\alpha_n) \equiv 0 \mod p^n$ para todo $n \geqslant 1$ y además $\alpha_m \equiv \alpha_n \mod p^n$ si $m \geqslant n$. Además, puesto que $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p^n\mathbb{Z}$ podemos sustituir α_n por un entero $\beta_n \in \mathbb{Z}$ tal que $\alpha_n \equiv \beta_n \mod p^n$ sin que ello altere las propiedades de la sucesión. Así pues, el Lema prueba la existencia de una sucesión de enteros $\{\beta_n\}$ tales que $f(\beta_n) \equiv 0 \mod p^n$ y $\beta_m \equiv \beta_n \mod p^n$ si $m \geqslant n$. La propiedad de "coherencia" $\beta_m \equiv \beta_n \mod p^n$ si $m \geqslant n \geqslant 1$ (o la semejante en la sucesión inicial $\{a_n\}$) es análoga a la propiedad de que la sucesión $\{x_n\}$ que construye el método de Newton es (con buenas condiciones iniciales) de Cauchy, y por tanto convergente. En el Capítulo 3 veremos que esta comparación no es solo una analogía formal.
Finalmente señalemos que si $f \in \mathbb{Z}[X]$ y $\alpha \in \mathbb{Z}$ es una raíz simple, tomando como dato inicial $a_1 \in \mathbb{Z}$ con $\alpha \equiv a_1 \mod p$ la sucesión de enteros $\{a_n\}$ se estabiliza en α, es decir, existe $n_0 \in \mathbb{N}$ tal que $a_n = \alpha$ para $n \geqslant n_0$. Para ello basta tomar n_0 suficientemente grande de forma que todas las operaciones necesarias no requieran reducciones modulares módulo p^n.

1.1.2. Ecuaciones cuadráticas

En esta subsección vamos a desarrollar un caso completo de resolución de congruencias. La ecuación con la que vamos a trabajar es $X^2 \equiv a \mod n$, donde tanto a como n son enteros. Conociendo la factorización de n, el problema se divide en varios pasos hasta llegar a la congruencia $X^2 \equiv a \mod p$, siendo p un factor primo de n. Una vez obtenida una solución módulo p vamos a utilizar el Lema de Hensel, sobre el polinomio $f(X) = X^2 - a$ para levantar la solución, y de esta manera, tener una solución de la congruencia módulo p^k con $k \in \mathbb{N}$.
Así pues, nuestro problema es si dado un entero a existen enteros $x \in \mathbb{Z}$ tales que $x^2 \equiv a \mod n$ y cómo calcularlos.

Definición 2. Diremos que $a \in \mathbb{Z}/n\mathbb{Z}$ es un residuo cuadrático módulo n si existe un $x \in \mathbb{Z}$ tal que $x^2 \equiv a \bmod n$. El conjunto de todos los residuos cuadráticos se denota por QR_n .

Distinguimos dos partes en el problema de resolver la congruencia $X^2 \equiv a \bmod n$:

1. Saber si la congruencia tiene o no solución.
2. Calcular las soluciones.

En primer lugar veremos que el estudio de las soluciones de la congruencia módulo n se puede reducir al estudio de las soluciones de las congruencias módulo p_i, siendo p_i, $i = 1, ..., s$ todos los números primos que aparecen en la factorización de n. Es importante observar que, si no contamos con una factorización del número n el problema es computacionalmente imposible. De hecho es un problema que está en la base de algunos métodos criptográficos.

Teorema 2 (Teorema Chino de los Restos)**.** *Sean $m_1, ..., m_n$ enteros no nulos primos entre si,y sean $a_1, ..., a_n$ elementos de $\mathbb{Z}$. Entonces el sistema de ecuaciones en congruencias*

$$\begin{aligned} X &\equiv a_1 \bmod m_1 \\ X &\equiv a_2 \bmod m_2 \\ &\cdots \\ X &\equiv a_n \bmod m_n \end{aligned}$$

tiene solución única módulo $m = m_1...m_n$ y ésta viene dada por

$$x' = M_1M_1'a_1 + M_2M_2'a_2 + ... + M_nM_n'a_n \bmod m,$$

donde para todo $j = 1, ..., n$, $M_j = m/m_j$ y M_j' es el inverso de M_j módulo m_j.

Supongamos que $n = {p_1}^{r_1}{p_2}^{r_2}...{p_s}^{r_s}$ con $p_1, ..., p_s$ primos distintos. Estudiamos $X^2 \equiv a \bmod p_i^{r_i}$ para todo $i = 1, ..., s$ y gracias al teorema anterior, ya tenemos resuelto nuestra congruencia inicial $X^2 \equiv a \bmod n$. Así pues, hemos reducido nuestro problema a estudiar las soluciones de la congruencia $X^2 \equiv a \bmod p^m$, siendo p un número primo.

Proposición 1. *Sea p un primo impar y sea a un entero primo con p. Si la congruencia $X^2 \equiv a \bmod p$ tiene solución, entonces también tiene solución la congruencia $X^2 \equiv a \bmod p^n$ para todo n.*

Demostración. Suponemos que a_0 es la solución de la congruencia módulo p. Definimos $f(X) = X^2 - a$. Entonces $f(a_0) \equiv 0 \bmod p$. Además tenemos que $a_0 \not\equiv 0 \bmod p$, pues de otra forma $a_0^2 \equiv 0 \bmod p$. Como $f'(a_0) = 2a_0 \not\equiv 0 \bmod p$ y $c = v_p(f'(a_0)) = 0$, estamos en condiciones de aplicar el Lema de Hensel, y podemos definir una sucesión $\{a_n\}$ de tal manera que $f(a_n) \equiv 0 \bmod p^{2^n}$.

□

La conclusión a la que llegamos después de esta proposición es que si tenemos la solución de $X^2 \equiv a \bmod p$ entonces el Lema de Hensel nos garantiza que $X^2 \equiv a \bmod p^n$ también tiene solución y nos da una forma de calcularla.

En la proposición anterior hemos descartado el caso $p = 2$. Sabemos que 3 es cuadrado módulo 2, pero es fácil probar que 3 no es cuadrado módulo 4. Es decir, en este caso no siempre se verifica la proposición.

Proposición 2. *Sea a un entero impar. Si la congruencia $X^2 \equiv a \bmod 8$ tiene solución, entonces tiene solución módulo 2^n para todo $n > 0$. Además esto se da si y solamente si $a \equiv 1 \bmod 8$.*

Demostración. Supongamos que $a \equiv 1 \bmod 8$ y definimos $f(X) = X^2 - a$. Vamos a ver que $a_0 = 1$ satisface las hipótesis del Lema de Hensel. Es evidente que $c = v_2(f'(1)) = v_2(2) = 1$, entonces $2^{2c+1} = 8$. Como estábamos suponiendo que $a \equiv 1 \bmod 8$, tenemos que $f(1) \equiv 0 \bmod 8$. Podemos aplicar el Lema de Hensel y elevar las raíces de f módulo 2^n para cualquier n.

Si a es un cuadrado módulo 2^n para todo n, es claro que a es un cuadrado módulo 8 (es el caso particular 2^3). Es fácil probar que los únicos valores posibles para a son: $1, 3, 5, 7$, por tanto $a \equiv 1 \bmod 8$.

□

Pasamos ahora al estudio de la ecuación $X^2 \equiv a \bmod p$, siendo p primo.

Lema 2. *Sea $X^2 \equiv a \bmod p$. Si $a \not\equiv 0 \bmod p$ hay o bien exactamente dos soluciones conjugadas o no hay ninguna solución. En particular las soluciones de $X^2 \equiv 1 \bmod p$ son $\{\pm 1\}$.*

Demostración. Supongamos que $x, y \in \mathbb{Z}$ son soluciones, entonces tenemos que $x^2 \equiv y^2 \bmod p$ que es lo mismo que decir $(x - y)(x + y) \equiv 0 \bmod p$. Concluimos que

$$\begin{array}{ll} p & |(x - y) \Rightarrow x \equiv y \bmod p. \\ & \text{o} \\ p & |(x + y) \Rightarrow x \equiv -y \bmod p. \end{array}$$

□

Veamos ahora cuantos residuos cuadráticos módulo p hay. Denotamos por $(\mathbb{Z}/p)^*$ el conjunto de elementos de $\mathbb{Z}/p$ que tienen inverso, este conjunto es un grupo para el producto. Como $\mathbb{Z}/p$ es un cuerpo con p elementos, todo elemento menos el nulo tiene inverso, por consiguiente el cardinal de $(\mathbb{Z}/p)^*$ es $p - 1$. Tomamos ahora el morfismo de grupos

$$\begin{array}{rccc} f\colon & (\mathbb{Z}/p)^* & \longrightarrow & (\mathbb{Z}/p)^* \\ & x & \longmapsto & x^2 = f(x) \end{array}$$

Es evidente que $kerf = \{x \in (\mathbb{Z}/p)^* \mid f(x) = 1\}$ y entonces el núcleo de f tiene dos elementos, $kerf = \{\pm 1\}$. Por el Primer Teorema de Isomorfía tenemos que $Im(f) \simeq (\mathbb{Z}/p)^*/kerf$. Es claro que $Im(f) = QR_p$. Concluimos que hay $(p - 1)/2$ residuos cuadráticos módulo p.

Un criterio eficiente para determinar si un entero es o no un cuadrado módulo p se deduce de un resultado bien conocido en Teoria de Números.
Sea n un entero positivo, llamaremos $\varphi(n)$ a su indicador de Euler, es decir, $\varphi(n)$ es el número de enteros positivos menores que n y primos con n.

Teorema 3 (Teorema de Euler-Fermat)**.** *Sea $n > 0$ un número entero y $\varphi(n)$ su indicador de Euler. Entonces, para todo $m \in \mathbb{Z}$ primo con n se tiene que $m^{\varphi(n)} \equiv 1 \bmod n$.*

Nota. Si tenemos $n = p$ entonces $\varphi(p) = p - 1$ y si a es un entero no divisible por p entonces $a^{(p-1)} \equiv 1 \bmod p$. Este resultado es el conocido como el Pequeño Teorema de Fermat.

Enunciamos ahora una condición necesaria y suficiente para poder afirmar si $X^2 \equiv a \bmod p$ tiene o no soluciones.

Teorema 4 (Criterio de Euler)**.** *Sea p un primo impar y a un entero no divisible por p. Entonces $a \in QR_p$ si y solo si $a^{(p-1)/2} \equiv 1 \bmod p$.*

Demostración. Aplicando el Teorema de Euler-Fermat, tenemos que $a^{(p-1)} \equiv 1 \bmod p$ y por consiguiente $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.
Supongamos que a es un residuo cuadrádico módulo p, por definición tenemos que existe un entero b tal que $b^2 \equiv a \bmod p$. Como $p \not| a$ es evidente que $p \not| b^2$. Utilizando el Teorema de Euler-Fermat

$$a^{\frac{(p-1)}{2}} \equiv (b^2)^{(p-1)/2} \equiv b^{(p-1)} \equiv 1 \bmod p$$

como queríamos.
Supongamos ahora que $a^{(p-1)/2} \equiv 1 \bmod p$. Como $\mathbb{Z}/p$ es un cuerpo finito, el grupo multiplicativo $(\mathbb{Z}/p)^*$ es cíclico y, por tanto, si g es un elemento que genera todo el grupo, $a = g^\alpha$ para un cierto α y además $g^{(p-1)/2} \equiv -1 \bmod p$. Por otro lado, observemos que el hecho de que $a \in QR_p$ es equivalente a decir que α es par porque si queremos que $a \equiv b^2 \bmod p$ y sabemos que existe un β tal que $b = g^\beta$ entonces $g^\alpha \equiv g^{2\beta} \bmod p$. Por tanto como

$$a^{\frac{(p-1)}{2}} \equiv g^{\alpha(p-1)/2} \equiv 1 \bmod p,$$

es claro que α ha de ser par.

□

Con todo esto ya tenemos lo necesario para determinar si $X^2 \equiv a \bmod n$ tiene o no solución. Suponiendo ahora que existen,vamos a ver como calcularlas.
En el caso particular en el que $p \equiv 3 \bmod 4$ es fácil comprobar que $a^{(p+1)/4}$ es solución de $X^2 \equiv a \bmod p$, en efecto:

$$(a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} a \equiv a \bmod p.$$

Veamos ahora un algoritmo para calcularlas en el caso $p \equiv 1 \bmod 4$. Este algoritmo también sirve para $p \equiv 3 \bmod 4$, aunque es evidente que en este caso no merece la pena.

Algoritmo (Tonelli-Shanks).

- Comprobamos que $a \in QR_p$.
- Escribimos $p - 1 = 2^e n$ con n impar.
- Calculamos b, un no residuo cuadrático módulo p.
- Iniciamos con $A := a^n \bmod p, B := b^n \bmod p, R := a^{(n+1)/2} \bmod p$
- Mientras $A \neq 1$
  - Calculamos k mínimo tal que $A^{2^k} \equiv 1 \bmod p$
  - Definimos $t := e - k$
  - $B := B^{2^t}, A := B^{2^t} A, R := B^{2^{t-1}} R, e := k$
- Devolvemos $R, -R$

Demostración. Observamos que, dado que la mitad de los elementos de $(\mathbb{Z}/p)^*$ son no cuadrados, la búsqueda del elemento b del algoritmo es eficiente.
Además nos damos cuenta que tal y como hemos definido A es una raíz 2^{e-1} de la unidad, pues $A^{2^{e-1}} = a^{(p-1)/2} = 1$ (recordemos que $a \in QR_p$). También tenemos que $B^{2^e} = b^{n2^e} = 1$ por el Teorema de Euler-Fermat y $B^{2^{e-1}} = b^{(p-1)/2}$ por ser b un no residuo cuadrático módulo p, concluimos que B es una raíz primitiva 2^e- ésima de la unidad módulo p.Como B es una raíz primitiva y $A \in \mathbb{Z}^*$, entonces existe un $l \in \mathbb{Z}$ tal que $A = B^l$. El orden de A es par ($a \in QR_p$) $l = 2v$. Entonces

$$A = \frac{R^2}{a} = B^{2v} \Rightarrow \frac{(B^{-v}R)^2}{a} = 1$$

Esto quiere decir que $x = B^{-v}R$ es solución de $X^2 \equiv a \bmod p$. Existe un entero positivo m tal que $-v = m$ y como $l < 2^e$ y $2^e - l = 2m$ concluimos que $m < 2^{e-1}$. Si llamamos $r = 2^e - l$ el problema se reduce a calcular $r = 2m$ que cumpla $B^r A = 1$. Escribimos $r = 2^t(1 + r')$, $0 < t < e$ y r' par. Tenemos que $1 = B^r A$ si y solo si $A = B^{-r}$. Como r' es par, entonces $B' = B^{1+r'}$ sigue siendo una raíz 2^e-ésima. Sea k el menor entero tal que $A^{2^k} = 1$. Tenemos que $A = B^{-r} = B^{-2^t(1+r')} = (B')^{-2^t}$ por tanto tenemos que $1 = A^{2^k} = (B')^{-2^{t+k}}$ y entonces $t+k \geqslant l$. Por tanto, el menor t es $t = e - k$. De esta manera $x = B^m R = (B^{2^t})^{r'/2}(B^{2^{t-1}}R) = (B_1)^{r'/2}R_1$. Este proceso se puede ir iterando.

□

Ley de reciprocidad
Volviendo al Criterio de Euler, es necesario conocer $a^{(p-1)/2}$ para saber si a es un residuo cuadrático módulo p. Calcular ese número directamente puede ser complicado. En lo que sigue vamos a obtener una forma más sencilla de deducirlo.

Definición 3. Sea p un primo impar y $a \in \mathbb{Z}$. El símbolo de Legendre viene dado por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \neq 0 \quad \text{es cuadrado módulo} \quad p \\ -1 & \text{si } a \neq 0 \quad \text{no es cuadrado módulo} \quad p \\ 0 & \text{si } a = 0 \end{cases}$$

A la vista del criterio de Euler, otra forma de definirlo es:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Por lo tanto si calculamos el símbolo de Legendre $(\frac{a}{p})$ podemos determinar si $X^2 \equiv a \bmod p$ tiene o no solución.

Algunas propiedades elementales del símbolo de Legendre son:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- Si $a \equiv b \bmod p$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$
- $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Lo que hace relativamente sencillo el cálculo del símbolo de Legendre es uno de los Teoremas más importantes de la Teoria de Números.
Ley de reciprocidad cuadrática de Gauss

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$$

Veamos en un ejemplo el cálculo del símbolo de Legendre.

Ejemplo 3. Veamos si $X^2 \equiv 87 \bmod 127$ tiene solución.
Por el criterio de Euler, 87 es residuo cuadrático módulo 127 si $87^{(127-1)/2} \equiv 1 \bmod 127$. Vamos a utilizar el símbolo de Legendre para calcular ese valor.

$$\left(\frac{87}{127}\right) = \left(\frac{3}{127}\right)\left(\frac{29}{127}\right)$$

Tenemos que calcular esos dos símbolos de Jacobi.

$$\left(\frac{3}{127}\right) = (-1)^{\frac{252}{4}}\left(\frac{127}{3}\right) = (-1)\left(\frac{127}{3}\right) = (-1)\left(\frac{1}{3}\right) = -1$$

Calculamos ahora el otro factor:

$$\left(\frac{29}{127}\right) = (-1)^{\frac{3528}{4}}\left(\frac{127}{29}\right) = \left(\frac{11}{29}\right) =$$
$$(-1)^{\frac{280}{4}}\left(\frac{29}{11}\right) = \left(\frac{7}{11}\right) = (-1)^{\frac{60}{4}}\left(\frac{11}{7}\right) =$$
$$(-1)\left(\frac{4}{7}\right) = (-1)\left(\frac{2}{11}\right)\left(\frac{2}{11}\right) =$$
$$(-1)(-1)^{\frac{7^2-1}{8}}(-1)^{\frac{7^2-1}{8}} = -1$$

Por lo tanto $\left(\frac{87}{127}\right) = 1$ luego 87 es residuo cuadrático módulo 127.

En el cálculo anterior hemos usado la factorización del entero a ($a = 87$ en el ejemplo), pero esto en general no es posible ya que no hay métodos eficientes. El símbolo de Jacobi, que extiende el de Legendre, nos permitirá evitar este problema.

Definición 4. Dados $a \in \mathbb{Z}$ y n un entero impar positivo, suponemos conocida la factorización de $n = {p_1}^{r_1} \cdots {p_t}^{r_t}$, el símbolo de Jacobi de a respecto de n es

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{r_1} \cdots \left(\frac{a}{p_t}\right)^{r_t}.$$

Con esta definición las propiedades anteriores y la Ley de reciprocidad siguen siendo válidas. Es decir, que podemos sustituir el primo p en ellos por un entero cualquiera. Lo que deja de ser válido es la igualdad $(\frac{a}{m}) \equiv a^{\frac{m-1}{2}} \bmod p$. De hecho se tiene que si $a \in QR_m$, entonces $(\frac{a}{m}) = 1$ pero no es cierta la recíproca. Sin embargo, estas propiedades facilitan el cálculo del símbolo de Jacobi (y por tanto también el de Legendre).
Veamos como se calcula $(\frac{n}{m})$:
1. Si $n \geqslant m$ hacemos la división y llamamos r al resto, tenemos $(\frac{n}{m}) = (\frac{r}{m})$
2. Si $n < m$ aplicamos la Ley de reciprocidad y se reduce a calcular $(\frac{m}{n})$, volviendo así al apartado anterior.
3. Una vez llegados a $(\frac{-1}{m})$ o $(\frac{2}{m})$ tenemos como en el símbolo de Legendre lo siguiente
$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}$ y $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$.

Veamos un ejemplo del cálculo del símbolo de Jacobi.

Ejemplo 4. Calcular $(\frac{219}{383})$ utilizando las indicaciones anteriores.
Aplicando la Ley de reciprocidad:

$$\left(\frac{219}{383}\right) = (-1)^{\frac{(218)(382)}{4}}\left(\frac{383}{219}\right).$$

Como $383 \equiv 164 \mod 219$ y $164 = 2^2 41$ obtenemos

$$\left(\frac{219}{383}\right) = -\left(\frac{2}{219}\right)^2 \left(\frac{41}{219}\right)$$

Utilizamos ahora la tercera propiedad y llegamos a que $(\frac{2}{219}) = (-1)$. Esto nos reduce la expresión a $(\frac{219}{383}) = -(\frac{41}{219})$. Razonando de la misma forma con las indicaciones anteriores:

$$\begin{aligned}\left(\frac{219}{383}\right) &= -\left(\frac{41}{219}\right) = -\left(\frac{219}{41}\right) \\ &= -\left(\frac{14}{41}\right) = -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) \\ &= -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) \\ &= -\left(\frac{-1}{7}\right) = (-1)(-1)^3\end{aligned}$$

Concluimos que $(\frac{219}{383}) = 1$.

1.2. Series p-ádicas

Sea $f(X) \in \mathbb{Z}_{(p)}[X]$, p primo y supongamos que hemos calculado, para $n \geqslant 1$ un entero a_n, $0 \leq a_n < p^n$ de manera que $f(a_n) \equiv 0 \mod p^n$. Tal y como ocurre en el método descrito en la sección anterior, suponemos que, si además $n > m$, entonces $a_n \equiv a_m \mod p^m$. Observamos que $a_2 \equiv a_1 \mod p$, por tanto $a_2 = a_1 + px_1$ con $0 \leq x_1 < p$ ya que $a_2 < p^2$. Si tomamos ahora $n > 1$, tendríamos $a_{n+1} \equiv a_n \mod p^n$ y por tanto

$$a_{n+1} = a_n + x_n p^n,$$

con x_n único $0 \leq x_n < p$.
Así pues, usando recurrencia, tenemos que

$$a_{n+1} = x_0 + x_1 p + \cdots + x_n p^n \quad \text{con} \quad 0 \leq x_i < p \quad \forall i = 1, ..., n.$$

Evidentemente la información de la sucesión $\{a_n\}_{n\geqslant 1}$ es equivalente a la sucesión $\{x_n\}_{n\geqslant 0}$. Una forma agradable de escribir esta última información es mediante la serie:

$$s = \sum_{i\geqslant 0} x_i p^i.$$

Por el momento s no es más que una expresión formal, pero observamos que para cada $n \geqslant 0$ tiene sentido la reducción de s módulo p^{n+1} y además esta es:

$$x_0 + x_1 p + \cdots + x_n p^n = a_{n+1} \quad \text{es decir} \quad s \equiv a_{n+1} \mod p^{n+1} \quad \text{para todo} \quad n.$$

Sistematizamos un poco más este tipo de series:
Sea $\{x_n\}_{n\geqslant 1}$ una sucesión de elementos de $\mathbb{Z}_{(p)}$, convenimos en denotar la sucesión formalmente como $s = \sum_{n\geqslant 1} x_n$ y diremos que es una serie.

Definición 5. Diremos que la serie $s = \sum_{n\geqslant 1} x_n$ converge p-ádicamente si para cada $n \geqslant 1$ hay solamente un número finito de términos x_k tales que $x_k \not\equiv 0 \mod p^n$.

Observamos que una serie s convergente p-ádicamente representa una clase residual módulo p^n para cada n, es decir, que para todo $n \geqslant 1$ existe a_n único con $0 \leq a_n < p^n$ tal que $s \equiv a_n \bmod p^n$. Además de forma evidente $a_n \equiv a_m \bmod p^m$ si $m \leq n$. Por lo tanto, s es una manera de representar $\{a_n\}_{n\geqslant 1}$.
Si procedemos como antes y escribimos $a_{n+1} = z_0 + z_1 p + ... + z_n p^n$ con $0 \leq z_i < p$, podemos reescribir la información de la serie $s = \sum_{i\geqslant 1} x_i$ como $s' = \sum_{i\geqslant 0} z_i p^i$ ya que ambas tienen la misma información módulo p^n para todo n, es decir $s \equiv s' \bmod p^n$, para todo $n \geqslant 1$. Por tanto, tiene sentido decir que ambas series son iguales.
El siguiente lema expresa otra forma de definir la convergencia p-ádica.

Lema 3. *Una serie $\sum x_n$ de elementos de $\mathbb{Z}_{(p)}$ converge p-ádicamente si y solamente si $v_p(x_n) \to \infty$ cuando n tienda a ∞.*

Demostración. Supongamos que $v_p(x_n)$ tiende a infinito cuando $n \to \infty$, esto significa que dado un r existe un n_0 suficientemente grande tal que $v_p(x_n) \geqslant r$ para todo $n \geqslant n_0$ y este hecho es equivalente a decir que $x_n \equiv 0 \bmod p^r$, es decir, la serie $\sum x_n$ de elementos de $\mathbb{Z}_{(p)}$ converge p-ádicamente.

□

1.2.1. Series formales

Vamos a denotar por $\mathbb{Z}_{(p)}[[X]]$ al conjunto de series de potencias formales con coeficientes en $\mathbb{Z}_{(p)}$, es decir a los elementos del tipo

$$\sum_{n=0}^{\infty} a_n X^n \quad \text{con} \quad a_n \in \mathbb{Z}_{(p)}, \quad \text{para todo} \quad n \geqslant 0.$$

Es evidente que los polinomios con coeficientes en $\mathbb{Z}_{(p)}$ son un subconjunto de $\mathbb{Z}_{(p)}[[X]]$: son las series de potencias con un número finito de a_n distintos de cero. Podemos definir la suma y el producto en $\mathbb{Z}_{(p)}[[X]]$ de la misma manera que lo hacemos con los polinomios. De esta forma tenemos que $\mathbb{Z}_{(p)}[[X]]$ es un anillo.

Dadas dos series de potencias $f(X)$ y $g(X)$, la composición de f con g, denotada por $(f \circ g)(X)$, consiste en cambiar la variable X de la serie f por $g(X)$, así pues, $(f \circ g)(X) = f(g(X))$. No siempre va a estar bien definida. A continuación, veremos que si f es un polinomio o g no tiene término independiente, entonces sí va a tener sentido la composición.
Si g tuviera término independiente y f no fuera un polinomio, estaríamos por ejemplo en la situación $f(X) = \sum_{n=0}^{\infty} X^n$ y $g(X) = \alpha + X$ con $\alpha \neq 0$, entonces es fácil ver que el término independiente de $f(\alpha + X)$, que sería la composición, no está bien definido pues queda $1 + \alpha + \alpha^2 + \alpha^3 + \cdots$. Con la g anterior y tomando f un polinomio, es claro que el término independiente es una suma finita de potencias de α y está bien definido.

A continuación, pasamos a estudiar la composición $(f \circ g)(X)$ cuando $f(X) = \sum_{n=0}^{\infty} a_n X^n$ y $g(X) = \sum_{n=1}^{\infty} b_n X^n$.

$$f(g(X)) = a_0 + a_1(g(X)) + a_2(g(X))^2 + \cdots + a_n(g(X))^n + \cdots$$

Ordenando los términos obtenemos que $f(g(X)) = \sum_{n=0}^{\infty} c_n X^n$.
Como $g(X)$ no tiene término independiente, para todo n, $(g(X))^n$ tampoco. Este hecho nos va a garantizar poder encontrar los coeficientes de $f(g(X))$ y por lo tanto nos va a permitir definir la composición.

$$\begin{aligned} c_0 + c_1 X + c_2 X^2 + c_3 X^3 + \cdots &= a_0 + a_1(b_1 X + b_2 X^2 + b_3 X^3 + \cdots) + \\ &+ a_2(b_1^2 X^2 + 2 b_1 b_2 X^3 + \cdots) + a_3(b_1^3 X^3 + \cdots) + \cdots \end{aligned}$$

- $c_0 = a_0$
- $c_1 = a_1 b_1$
- $c_2 = a_1 b_2 + a_2 b_1^2$
- $c_3 = a_1 b_3 + 2a_2 b_1 b_2 + a_3 b_1^3$
- El coeficiente n-ésimo: Si definimos

$$(g(X))^m = \sum_{n=m}^{\infty} d_{m,n} X^n, \quad \text{con} \quad d_{m,n} = \sum b_{i_1} b_{i_2} b_{i_3} \cdots b_{i_m} \text{ siendo } i_1 + i_2 + \cdots + i_m = n$$

Entonces $c_n = \sum_{m=1}^{n} d_{m,n}$

Los coeficientes c_n cumplen una serie de propiedades.
1) La suma que define c_n es finita, por consiguiente $f \circ g$ es un elemento de $\mathbb{Z}_{(p)}[[X]]$.
2) El sumatorio que define c_n depende solo de los coeficientes a_d y b_d de f y g respectivamente con $d \leq n$. Es claro que si conocemos $f(X)$ y $g(X)$ hasta orden n, también conocemos $f(g(X))$ hasta orden n.
3) Las clases de equivalencia de c_n módulo p^r dependen exclusivamente de las clases de a_d y b_d módulo p^r. Esto se traduce en decir que si escribimos $\bar{f}$, imagen de f en $(\mathbb{Z}/p^r)[[X]]$, tenemos $\overline{f \circ g} = \bar{f} \circ \bar{g}$

Nota. Sea $f(X) = \sum_{i \geqslant 0} a_i X^i$, $g(X) = \sum_{i \geqslant 0} b_i X^i \in \mathbb{Z}_{(p)}[[X]]$ dos series formales. Obsérvese que $f(X) = g(X)$ si y solo si $a_i = b_i$ para todo $i \geqslant 0$. Puesto que $\mathbb{Z}_{(p)} \subset \mathbb{Q} \subset \mathbb{R}$, si $x \in \mathbb{R}$ podemos considerar la serie numérica $f(x) = \sum_{i \geqslant 0} a_i x^i$. Supongamos que $f(x)$ converge para $|x| < r$, es decir, la serie de potencias $f(x) = \sum_{i \geqslant 0} a_i x^i$ tiene radio de convergencia $\geqslant r$. En este caso $f : (-r, r) \longrightarrow \mathbb{R}$ es una función diferenciable y, para $|y| < r$ $f'(y) = \sum_{i \geqslant 1} i a_i y^{i-1}$. Reduciendo el intervalo $(-r, r)$ podemos también suponer que f' es acotada, es decir que existe $c > 0$ tal que $|f'(y)| < c$ para todo y con $|y| < r$. Evidentemente la convergencia de $f(x)$ implica que para $n > 0$ existe una constante k tal que $|f(x) - f_n(x)| < k|x|^{n+1}$ en un intervalo abierto I de 0, siendo $f_n(x) = \sum_{i=0}^{n} a_i x^i$.
Si suponemos que $f(x)$, $g(x)$ son convergentes con $|x| < r$ y además $|f(x) - g_n(x)| < k|x|^{n+1}$ para una constante k y para todo x con $|x| < r$, entonces necesariamente $a_i = b_i$ para todo $i \leq n$. En efecto, supongamos que $a_i = b_i$ para todo $i < k$, $a_k \neq b_k$ con $k \leq n$. En este caso $|f(x) - g_n(x) = |x|^k |s(x)|$ con $s(x)$ convergente y $s(0) = s_0 \neq 0$. Por tanto $|x|^k |s(x)| < k|x|^{n+1}$ que es equivalente a decir $|x|^{-(n+1-k)} |s(x)| < k$ para todo $x \in (-r, r)$. Pero esto es imposible ya que $|s(x)| \neq 0$ en un entorno de 0 y por tanto $|x|^{-(n+1-k)} |s(x)| \to \infty$ si $x \to 0$.

Lema 4. *Sean $f(X)$, $g(X)$ y $h(X)$ series de potencias con coeficientes en $\mathbb{Z}_{(p)}$, es decir elementos de $\mathbb{Z}_{(p)}[[X]]$ y supongamos que g no tiene término constante o que f es un polinomio. Suponemos también:*
i) $f(x)$, $g(x)$, $h(x)$ convergen para valores reales de x suficientemente pequeños y $f(g(x)) = h(x)$.
ii) $f(z)$, $g(z)$, $h(z)$ convergen p-ádicamente para todo $z \in \mathbb{Z}_{(p)}$.
Entonces, $h = f \circ g$ como serie de potencias, es decir $h(X) = (f \circ g)(X)$ y además para todo $z \in \mathbb{Z}_{(p)}$ y $n \geqslant 1$ tenemos $f(g(z)) \equiv h(z) \bmod p^n$.

Demostración. Tenemos que ver dos cosas
1) La igualdad de las series de potencias formales $h(X) = (f \circ g)(X)$.

2) $f(g(z)) \equiv h(z) \bmod p^n$ para todo $z \in \mathbb{Z}_{(p)}$.

1) Por hipótesis tenemos que o bien g no tiene término independiente o bien f es un polinomio, por tanto $f \circ g$ está bien definida.
a) Estudiaremos primero el caso en el que g no tiene término independiente. Sean $f(X) = \sum_{i=0}^{\infty} a_i X^i$, $g(X) = \sum_{i=1}^{\infty} b_i X^i$ y para $n \geqslant 1$ definimos:

$$f_n(X) = \sum_{i=0}^{n} a_i X^i, \quad g_n(X) = \sum_{i=1}^{n} b_i X^i$$

De la misma manera definimos $(f \circ g)_n$, el polinomio formado por los n primeros términos de la serie de potencias $f \circ g$.
Sea $h(X) = \sum_{i=0}^{\infty} \alpha_i X^i$, $f \circ g = \sum_{i=0}^{\infty} \beta_i X^i$, lo que tenemos que ver es que $\alpha_i = \beta_i$ para todo $i \geqslant 0$.
• Sea J un intervalo abierto de 0 tal que $f(y)$ converge, es evidente que $f'(y)$ es también convergente y además $f'(y)$ es acotada en J.
• Sea I otro intervalo abierto que contiene al 0 tal que $g(x)$ y $h(x)$ converjan en el y $g(x)$, $g_n(x) \in J$ para todo $x \in I$.
Por otro lado, $f(x)$ y $g(x)$ son convergentes para valores reales próximos a 0. Esto quiere decir que existen constantes K_1 y K_2 tal que $|f(x) - f_n(x)| \leq K_1|x|^{n+1}$ y $|g(x) - g_n(x)| \leq K_2|x|^{n+1}$ para todo $x \in I$. El problema de ver $\alpha_i = \beta_i$ se reduce a comprobar $|h(x) - (f \circ g)_n(x)| \leq K|x|^{n+1}$ para todo $x \in I$.
Por hipótesis $h(x) = f(g(x))$ para todo $x \in I$ y aplicando la desigualdad triangular tenemos:

$$|h(x) - (f \circ g)_n(x)| \leq |f(g(x)) - f(g_n(x))| + |f(g_n(x)) - f_n(g_n(x))| + |f_n(g_n(x)) - (f \circ g)_n(x)|.$$

Estudiamos cada uno de los sumandos.
Con ayuda del Teorema de Valor Medio y utilizando los hechos de que $f'(y)$ es acotada y g convergente:

$$|f(g(x)) - f(g_n(x))| \leq c_1|g(x) - g_n(x)| \leq c_2|x|^{n+1}.$$

Como x es próximo a 0 y g no tiene término independiente, entonces $|g_n(x)| \leq c_3|x|$ y además f es convergente:

$$|f(g_n(x)) - f_n(g_n(x))| \leq c_4|g_n(x)|^{n+1} \leq c_5|x|^{n+1}.$$

Por último, los n primeros coeficientes de $f \circ g$ vienen dados por los n primeros coeficientes de f y g. Además coinciden con los n primeros coeficientes del polinomio $f_n(g_n(x))$:

$$|f_n(g_n(x)) - (f \circ g)_n(x)| \leq c_6|x|^{n+1}.$$

Por lo tanto tenemos que $|h(x) - (f \circ g)_n(x)| \leq K|x|^{n+1}$ como queríamos.
b) Veamos que se cumple la igualdad de series de potencias, $h = f \circ g$ cuando g no tiene término independiente pero f es un polinomio.
Definimos las siguientes series de potencias

$$G(X) = g(X) - g(0), \quad F(X) = f(X + g(0)).$$

Sea $x \in \mathbb{R}$ suficientemente pequeño $F(G(x)) = f(G(x) - g(0)) = f(g(x)) = h(x)$. Démonos cuenta que tal y como hemos definido G es una serie sin término independiente, por lo tanto podemos repetir todo el proceso anterior para G y F y llegamos a que $h(X) = (f \circ g)(X)$ como serie de potencias.
2)Pasamos ahora a demostrar que $f(g(z)) \equiv h(z) \bmod p^n$ para todo $z \in \mathbb{Z}_{(p)}$.
Como $1 \in \mathbb{Z}_{(p)}$ sabemos por ii) que $f(1)$, $g(1)$ y $h(1)$ convergen convergen p-ádicamente, esto

significa que existe un número finito de términos en $f(1)$, $g(1)$ y $h(1)$ no congruentes con 0 módulo p^n. Entonces $f(X)$, $g(X)$ y $h(X)$ tienen un número finito de coeficientes distintos de 0 módulo p^n y $f(X) \bmod p^n$, $g(X) \bmod p^n$, $h(X) \bmod p^n$ son polinomios. Ya hemos visto que $h = f \circ g$ luego $\bar{h} = \bar{f} \circ \bar{g}$. Si z es la redución de $z \in \mathbb{Z}_{(p)}$ módulo p^n, $\bar{h} = \bar{f}(\overline{g(\bar{z})}) \bmod p^n$ y por tanto $h = f(g(z)) \bmod p^n$ para todo $z \in \mathbb{Z}_{(p)}$.

□

En muchas series de potencias tenemos el número $n!$ en sus coeficientes. En el siguiente lema vamos a ver una forma de calcular $v_p(n!)$.

Lema 5. *Para cada número n, entero y positivo, $v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$. Además, $v_p(n!) \leq \frac{n}{p-1}$. Si la expresión en base p de n es $a_0+a_1p+a_2p^2+...+a_kp^k$ y definimos $s = a_0+a_1+...+a_k$, entonces $v_p(n!) = \frac{n-s}{p-1}$.*

Demostración. Sabemos que $v_p(nm) = v_p(n) + v_p(m)$, por lo tanto $v_p(n!) = \sum_{i=1}^{n} v_p(i)$. Vamos a escribir $v_p(n!)$ de otra forma.

$$v_p(n!) = 1s(1) + 2s(2) + 3s(3) + \cdots,$$

donde $s(r)$ es el número de términos del conjunto $\{v_p(i),\, i = 1, ..., k\}$ que toman el valor r. Entonces $s(r)$ es el número de enteros de enteros i entre 1 y n tal que $v_p(i) = r$.
Entre 1 y n existen $\left\lfloor \frac{n}{p^r} \right\rfloor$ valores múltiplos de p^r de los cuales $\left\lfloor \frac{n}{p^{r+1}} \right\rfloor$ también son múltiplos de p^{r+1}. Es evidente que el número de valores entre 1 y n, múltiplos de p^r pero no múltiplos de p^{r+1} son $\left\lfloor \frac{n}{p^r} \right\rfloor - \left\lfloor \frac{n}{p^{r+1}} \right\rfloor$. De esta manera

$$s(r) = \left\lfloor \frac{n}{p^r} \right\rfloor - \left\lfloor \frac{n}{p^{r+1}} \right\rfloor.$$

Utilizando esta información obtenemos que:

$$\begin{aligned} v_p(n!) &= \left(\left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + 2 \left(\left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + 3 \left(\left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor \right) \cdots \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \end{aligned}$$

Observamos que la suma es finita pues para valores grandes de i tenemos $\frac{n}{p^r} < 1$, luego $\left\lfloor \frac{n}{p^r} \right\rfloor = 0$.
Ya tenemos probada la primera parte del lema. Veamos ahora la desigualdad. Sabemos que $\lfloor x \rfloor \leq x$. Es evidente:

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor \leq \sum_{i=1}^{\infty} \frac{n}{p^i} = \frac{n}{p-1}.$$

Por último, dado que $|\sum_{j=1}^{r} \frac{a_{r-j}}{p^j}| \leq (p-1)\sum_{j=1}^{r} \frac{1}{p^j} < (p-1)\sum_{j=1}^{\infty} \frac{1}{p^j} = 1$ tenemos que $\left\lfloor \frac{n}{p^r} \right\rfloor = \left\lfloor \frac{a_0}{p^r} + \frac{a_1}{p^{r-1}} + ... + a_r + a_{r+1}p + a_kp^{k-r} \right\rfloor = a_r + a_{r+1}p + ... + a_kp^{k-r}$ y entonces, $v_p(n!) = \sum_{r=1}^{k} \left\lfloor \frac{n}{p^r} \right\rfloor = \sum_{r=1}^{k}(a_r+a_{r+1}p+...+a_kp^{k-j})$. El factor a_i aparece como $a_ip^{i-1}+a_ip^{i-2}+...+a_ip+a_i$

y por lo tanto $v_p(n!) = \sum_{r=1}^{k} a_r \sum_{i=1}^{r} p^{r-i}$. Puesto que $\sum_{i=1}^{r} p^{r-i} = \frac{p^r-1}{p-1}$ llegamos a que $v_p(n!) = \sum_{r=1}^{k} a_r \frac{p^r-1}{p-1}$ y sacando factor común:

$$v_p(n!) = \frac{1}{p-1}\left(\sum_{r=1}^{k} a_r p^r - \sum_{r=1}^{k} a_r\right) = \frac{1}{p-1}\left(\sum_{r=0}^{k} a_r p^r - \sum_{r=0}^{k} a_r\right) = \frac{n-s}{p-1}$$

□

1.2.2. Exponencial y logaritmo: Aplicación al PLD

Dados los enteros a, b, m; si existe un entero x de manera que $a^x \equiv b \bmod m$ dicho elemento x se llama el "logaritmo discreto de b en base a módulo m". El cálculo de x, cuando existe, se llama de forma genérica el "problema del logaritmo discreto" (PLD). Incluso en casos sencillos no se conocen algoritmos eficientes para resolver el PLD. Por ejemplo, si p es un número primo, g es un generador multiplicativo de $(\mathbb{Z}/p)^*$ y b es un entero no divisible por p el PLD $g^x \equiv b \bmod p$ tiene siempre solución, pero el cálculo de x es muy complejo computacionalmete. De hecho la seguridad de algunos sistemas criptográficos como el Gamal o protocolos como el intercambio de claves de Diffie-Hellman se basan en la imposibilidad computacional de resolver el PLD en este caso concreto.

Las funciones logaritmo y exponencial ayudan a resolver el PLD en algunos casos.

Dos grupos fundamentales. Puesto que $p^n\mathbb{Z} \subset p\mathbb{Z}$, el cociente $p\mathbb{Z}/p^n$ es un subgrupo aditivo de $(\mathbb{Z}/p^n, +)$. Identificando las clases $a + p^n\mathbb{Z}$ de $\mathbb{Z}/p^n$ su único representante x con $0 \leq x < p^n$ el grupo $p\mathbb{Z}/p^n$ se puede describir como

$$p\mathbb{Z}/p^n = \{0,\, p,\, 2p,\, 3p, ...,\, (p^{n-1}-1)p\} = \{kp \,|\, k = 0, \cdots, p^{n-1}-1\}.$$

Es un grupo con p^{n-1} elementos.

El segundo grupo nos interesa es:

$$1 + p\mathbb{Z}/p^n = \{1 + px \,|\, x \in \mathbb{Z}/p^n\}.$$

Si $\alpha, \beta \in 1 + p\mathbb{Z}/p^n$, $\alpha = 1 + pm$, $\beta = 1 + pu$ tenemos que: $\alpha\beta = (p^2mu) + pm + pu + 1 = 1 + p(m + n + pmu) \in 1 + p\mathbb{Z}/p^n$. Además, el máximo común divisor de p^n con un elemento de la forma $1 + pm$ es 1. Por lo tanto $1 + p\mathbb{Z}/p^n$ es un subgrupo multiplicativo del grupo de unidades $(\mathbb{Z}/p^n)^*$. Es evidente que tiene el mismo cardinal p^{n-1} que el subgrupo aditivo $p\mathbb{Z}/p^n$.

Exponencial y logaritmo. Recordemos que si $x \in \mathbb{R}$, la función exponencial se expresa como la serie

$$exp(x) = e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots,$$

serie que es convergente para todo $x \in \mathbb{R}$. La función logaritmo, $log : \mathbb{R}_+ \to \mathbb{R}$ es la inversa de la exponencial, es decir $log(exp(x)) = x$ para todo $x \in \mathbb{R}$ y $exp(log(x)) = x$ para todo $x \in \mathbb{R}_+$. Es conocida su expresión como series de potencias

$$log(1 + x) = x - \frac{x}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots,$$

que converge cuando $|x| < 1$. Basándonos en estas expresiones, definimos $exp(X)$, $log(X) \in \mathbb{Q}[[X]]$ las series formales

$$exp(X) = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \cdots.$$

$$log(1+X) = X - \frac{X}{2} + \frac{X^3}{3} - \frac{X^4}{4} + \cdots .$$

En estos términos podemos enunciar el siguiente teorema.

Teorema 5. *Sea p un primo impar. Entonces $log(1+px)$ y $exp(px)$ son series de potencias en $\mathbb{Z}_{(p)}$ que convergen p-ádicamente para todo $x \in \mathbb{Z}_{(p)}$. Además, las aplicaciones*

$$log\colon \quad 1 + p\mathbb{Z}/p^n \quad \longrightarrow \quad p\mathbb{Z}/p^n$$

$$exp\colon \quad p\mathbb{Z}/p^n \quad \longrightarrow \quad 1 + p\mathbb{Z}/p^n$$

definen isomorfismos, inversos uno del otro, entre los grupos $(p\mathbb{Z}/p^n, +)$ y $(1 + p\mathbb{Z}/p^n, \cdot)$.

Demostración. Veamos que $exp(px)$ y $log(1+px)$ son series de potencias que convergen p-ádicamente para todo $x \in \mathbb{Z}_{(p)}$.
Usamos para ello el Lema 3, es decir que la serie $\sum y_i$ de elementos de $\mathbb{Z}_{(p)}$ converge p-ádicamente si y solo si $v_p(y_n)$ tiende a infinito cuando $n \to \infty$.
Para la exponencial, tenemos

$$exp(px) = \sum_{n=0}^{\infty} \frac{(px)^n}{n!}.$$

Para aplicar el resultado que acabamos de enunciar lo primero que tenemos ver es si los términos $\frac{(px)^n}{n!}$ son elementos de $\mathbb{Z}_{(p)}$, siendo $x \in \mathbb{Z}_{(p)}$. Es decir, hay que demostrar que $v_p\left(\frac{(px)^n}{n!}\right) \geqslant 0$.
Como queremos utilizar el lema citado, tenemos que probar

$$v_p\left(\frac{(px)^n}{n!}\right) \to \infty \quad \text{mientras} \quad n \to \infty.$$

Sabemos que $v_p(\frac{(px)^n}{n!}) = v_p((px)^n) - v_p(n!) = nv_p(px) - v_p(n!) = n(v_p(p) + v_p(x)) - v_p(n!) \geqslant -v_p(n!)$, ya que $v_p(x) \geqslant 0$ al ser $x \in \mathbb{Z}_{(p)}$. Tambíen tenemos que $v_p(n!) \leq \frac{n}{p-1}$, por tanto nos queda:

$$v_p\left(\frac{(px)^n}{n!}\right) \geqslant n - \frac{n}{p-1} = n\frac{p-2}{p-1}.$$

Por hipótesis $p \neq 2$, por tanto $v_p(\frac{(px)^n}{n!}) \geqslant 0$ y además, la expresión $n\frac{p-2}{p-1}$ tiende a ∞ cuando $n \to \infty$ y por consiguiente $exp(px)$ converge p-ádicamente para todo elemento $x \in \mathbb{Z}_{(p)}$.
Es evidente que, salvo en el caso $n = 0$, tenemos $v_p(\frac{(px)^n}{n!}) > 0$. Esto significa que el primer término de la serie de potencias $exp(px)$ es 1 y el resto son múltiplos de p, entonces $exp(px) \equiv 1 \bmod p$.
En el logaritmo tenemos que los términos de la serie de potencias son $\pm\frac{(px)^n}{n}$ siendo $n \geqslant 1$. Con un razonamiento análogo al caso exponencial tenemos que $v_p(\pm\frac{(px)^n}{n}) \geqslant n - v_p(n)$ y como n es un factor de $n!$, $v_p(n) \leq v_p(n!)$ y

$$v_p\left(\pm\frac{(px)^n}{n}\right) \geqslant n\frac{p-2}{p-1}.$$

Como $p \neq 2$, entonces $v_p(\pm\frac{(px)^n}{n}) > 0$ y la expresión $n\frac{p-2}{p-1}$ tiende a infinito cuando $n \to \infty$. Por lo tanto, $log(1+px)$ converge p-ádicamente para todo $x \in \mathbb{Z}_{(p)}$. Además es evidente que todos los términos de la serie son múltiplos de p, es decir $log(1+px) \equiv 0 \bmod p$.
Para lo que sigue nos resultarán útiles las series de potencias $f(X), g(X) \in \mathbb{Z}_{(p)}[[x]]$ definidas por:

$$f(X) = \frac{exp(pX) - 1}{p}, \quad g(X) = \frac{1}{p}log(1+pX).$$

A continuación, vamos a ver que las funciones $log(X)$ y $exp(X)$ definen los homomorfismos del del enunciado. Para ello vamos a utilizar f y g.
Para la función exponencial, tenemos que

$$f(x) - f(y) = (x - y) + \frac{p}{2!}(x^2 - y^2) + \frac{p^2}{3!}(x^3 - y^3) + \cdots$$

Para cada $n \in \mathbb{N}$ si reducimos esta expresión módulo p^n, tenemos que es una suma finita de términos.
Supongamos que $px \equiv py \bmod p^n$ entonces $x \equiv y \bmod p^{n-1}$, por consiguiente se tiene que $f(x) \equiv f(y) \bmod p^{n-1}$ y multiplicando por p obtenemos que $exp(px) \equiv exp(py) \bmod p^n$. Luego $exp(px)$ está bien definida para todo $px \in p\mathbb{Z}/p^n$. Además como $exp(px) \equiv 1 \bmod p$ entonces $exp(px) \in 1 + p\mathbb{Z}/p^n$.
Vamos ahora con el logaritmo. Tenemos:

$$g(x) - g(y) = (x - y) + \frac{p}{2}(-x^2 + y^2) + \frac{p^2}{3}(x^3 - y^3) + \cdots$$

es una suma finita si lo reducimos módulo p^n para cualquier $n \in \mathbb{N}$.
Si $px \equiv py \bmod p^n$, con un razonamiento análogo al anterior, llegamos a que $log(1 + px) \equiv log(1 + py) \bmod p^n$. Por tanto $log(1 + px)$ está bien definida para todo $1 + px \in 1 + p\mathbb{Z}/p^n$. Dado que $log(1 + px) \equiv 0 \bmod p$ entonces $log(1 + px) \in p\mathbb{Z}/p^n$.
Veamos ahora que exp y log, definidas en los conjuntos correspondientes, son inversas la una de la otra. Para demostrarlo vamos a aplicar el Lema 4 sobre las series de potencias $f(X)$ y $g(X)$. Las composiciones $f \circ g$ y $g \circ f$ están bien definidas dado que ni $f(X)$ ni $g(X)$ tienen término independiente. Para valores reales de x próximos a 0 tenemos que:

$$g(f(x)) = g\left(\frac{exp(px) - 1}{p}\right) = \frac{1}{p} log\left(1 + p\left(\frac{exp(px) - 1}{p}\right)\right) = \frac{1}{p} log(exp(px)) = x.$$

$$f(g(x)) = f\left(\frac{1}{p} log(1 + px)\right) = \frac{exp\left(p\left(\frac{1}{p} log(1 + px)\right)\right) - 1}{p} = \frac{exp(log(1 + px)) - 1}{p} = x.$$

Por otro lado, como $exp(z)$ y $log(z)$ convergen p-ádicamente para todo $z \in \mathbb{Z}_{(p)}$ entonces $f(z)$ y $g(z)$ también. En virtud del Lema 4, $f(g(z)) \equiv z \bmod p^n$ y $g(f(z)) \equiv x \bmod p^n$, multiplicamos en ambas expresiones por p, nos queda $exp(log(1 + pz)) \equiv 1 + pz \bmod p^{n+1}$ y $log(exp(pz)) \equiv pz \bmod p^{n+1}$.
Para probar el isomorfismo entre el grupo aditivo $p\mathbb{Z}/p^n$ y el grupo multiplicativo $1 + p\mathbb{Z}/p^n$ basta demostrar que exp es un homomorfismo de grupos, es decir que para todo $px, py \in p\mathbb{Z}/p^n$ se tiene $exp(px + py) \equiv exp(px)exp(py) \bmod p^n$.
Vamos a aplicar de nuevo el Lema 4 sobre $\hat{g}(X) = aX$ y $\hat{f}(X) = exp(pX)$. Para cada entero positivo a y para todo $x \in \mathbb{R}$ tenemos $exp(pax) = exp(px)^a$, por tanto $\hat{h}(X) = exp(pX)^a$. Dado que $\hat{f}(z)$, $\hat{g}(z)$ y $\hat{h}(z)$ convergen p-ádicamete para todo $z \in \mathbb{Z}_{(p)}$ aplicando el Lema 4 tenemos $exp(paz) \equiv exp(pz)^a \bmod p^n$. Sustituyendo en dicha expresión $z = 1$ obtenemos lo deseado

$$exp(p(a + b)) \equiv exp(p)^{a+b} \equiv exp(pa)exp(pb) \bmod p^n.$$

□

Aplicación al cálculo del logaritmo discreto

Este teorema nos permite resolver el problema del logaritmo discreto $a^x \equiv b \bmod p^m$ siempre y cuando a, $b \in 1 + p\mathbb{Z}/p^m$. Lo primero que tenemos que hacer es encontrar α y β tales que $a = 1 + p\alpha$ y $b = 1 + p\beta$ para utilizar la expresión de $log(1 + px)$ y así calcular más

fácilmente $log(a)$ y $log(b)$. Por último, tomamos logaritmos en ambos lados de la ecuación inicial $a^x \equiv b \bmod p^m$ reducimos nuestro problema a resolver $xlog(a) = log(b) \bmod p^m$.

Como ejemplo, calculamos el logaritmo discreto de 16 respecto de la base -5 módulo 81. Se sabe que $1 + 3\mathbb{Z}/3^4 \simeq 3\mathbb{Z}/3^4$ y este isomorfismo viene dado por exp y log.
Es evidente que $-5 \equiv 76 \bmod 81$ y como $75 \in 3\mathbb{Z}/3^4$ entonces $76 \in 1 + 3\mathbb{Z}/3^4$. De la misma forma como 15 es múltiplo de 3 y menor que 81 se tiene que $16 \in 1 + 3\mathbb{Z}/3^4$.
Vamos a calcular el polinomio $log(1 + 3x)$ módulo 81.

$$log(1 + 3x) = 3x - \frac{9x^2}{2} + \frac{3^3x^3}{3} - \frac{3^4x^4}{4} + \cdots$$

Reduciendo módulo 81

$$\begin{aligned} log(1 + 3x) &\equiv 3x - \frac{9x^2}{2} + 9x^3 \bmod 81 \\ &\equiv 3x + 36x^2 + 9x^3 \bmod 81 \end{aligned}$$

Por lo tanto nos queda

$$log(76) = log(1 + 3 \cdot 25) = 3 \cdot 25 + 36 \cdot (25)^2 + 9 \cdot (25)^3 = 163200 \equiv 66 \bmod 81.$$

$$log(16) = log(1 + 3 \cdot 5) = 3 \cdot 5 + 36 \cdot (5)^2 + 9 \cdot (5)^3 = 2040 \equiv 15 \bmod 81.$$

Hemos reducido el problema inicial a lo siguiente $xlog(-5) \equiv log(16) \bmod 81$, es decir $66x \equiv 15 \bmod 81$. Llegamos a que $x = 26$ es solución de $22x \equiv 5 \bmod 27$. Podemos comprobar que $x = 26$ es también solución de nuestro problema.

La funciones exponenciales y logaritmo son una herramienta importante en muchos otros contextos, por ejemplo permiten definir $a^b \bmod p^n$ cuando $b \in \mathbb{Z}_{(p)}$ y $a \equiv 1 \bmod p$ mediante $a^b := exp(log(a)) \bmod p^n$.

1.3. Estructura de los cocientes de $\mathbb{Z}$

En esta sección vamos a descomponer el grupo de las unidades de $\mathbb{Z}/p^n$, $(\mathbb{Z}/p^n)^*$ como producto directo interno de dos subgrupos suyos. Uno de estos subgrupos será $(1 + p\mathbb{Z}/p^n, \cdot)$ subgrupo que sabemos que es isomorfo al subgrupo $(p\mathbb{Z}/p^n, +)$ de $(\mathbb{Z}/p^n, +)$.

Además del interés teórico que tiene conocer la estructura del grupo $(\mathbb{Z}/p^n)^*$ en términos de grupos sencillos, la descomposición permite simplificar notablemente muchos cálculos en $\mathbb{Z}/p^n$.

Definición 6. Sea p un primo impar y $x \not\equiv 0 \bmod p$. Entonces se conoce como levantamiento de Teichmüller de x hasta $\mathbb{Z}/p^n$ al elemento $T(x) \in \mathbb{Z}/p^n$ dado por:

$$T(x) \equiv x^{p^{n-1}} \bmod p^n.$$

Nota. Sea x un elemento de $\mathbb{Z}_{(p)}$ que no sea múltiplo de p, consideramos la sucesión,

$$x, x^p, x^{p^2}, x^{p^3}, \cdots$$

Notemos que cada término de la sucesión es la potencia p-ésima del término anterior. Además, como p y x son primos entre sí se puede aplicar el Teorema de Euler-Fermat y tenemos que $x^{p-1} \equiv 1 \bmod p$. Multiplicando ambos lados por x, tenemos que $x^p \equiv x \bmod p$ y es evidente que la secuencia anterior es constante módulo p.
Ahora examinamos la sucesión anterior módulo p^2. En este caso $\varphi(p^2) = p^2 - p$, por lo tanto por el teorema de Euler-Fermat, $x^{p^2-p} \equiv 1 \bmod p^2$ y multiplicando por x^p, $x^{p^2} \equiv x^p \bmod p^2$.

Por tanto, la secuencia anterior módulo p^2 tiene distintos el primer y el segundo elementos y a partir del segundo son todos iguales.
En la definición anterior hemos llamado levantamiento de Teichmüller de x al valor en que se estabiliza la sucesión anterior cuando la reduzco módulo p^n en $(\mathbb{Z}/p^n)^*$.
Sin embargo, esta definición no es muy útil a la hora de calcular los levantamientos de Teichmüller, por ejemplo si queremos calcular $T(17) \bmod 5^4$ tendríamos que hallar $17^{125} \bmod 5^4$ pero este cálculo es bastante tedioso. Por este motivo vamos a presentar un método para calcular los levantamientos de Teichmüller sin acudir a la definición.

Lema 6. *Sea p un primo impar y n un entero positivo. Si $x \equiv y \bmod p^n$, entonces $x^p \equiv y^p \bmod p^{n+1}$.*

Demostración. Suponemos que $x \equiv y \bmod p^n$ que es lo mismo que decir que $x = y + kp^n$ para un entero k. Elevando a la p en ambos lados de la igualdad

$$\begin{aligned} x^p &= (y + kp^n)^p \\ &= y^p + \binom{p}{1} y^{p-1}(kp^n) + \binom{p}{2} y^{p-2}(kp^n)^2 + \cdots + \binom{p}{p}(kp^n)^p. \end{aligned}$$

Es evidente que salvo el primer término el resto son todos múltiplos de p^{n+1}, luego $x^p \equiv y^p \bmod p^{n+1}$.

□

Nótese que, como consecuencia, si $x \equiv y \bmod p^n$ entonces $T(x) \equiv T(y) \bmod p^n$. Por tanto, tiene sentido también $T(x)$ para $x \in (\mathbb{Z}/p^n)^*$.

Ejemplo 5. Vamos a utilizar el lema para calcular $T(17)$ módulo 5^4.
Lo primero es darnos cuenta que $17 \equiv 2 \bmod 5$, aplicando el Lema 6, $17^5 \equiv 2^5 \bmod 25$ y como $2^5 = 32 \equiv 7 \bmod 25$ llegamos a $17^5 \equiv 7 \bmod 25$. Volvemos a utilizar el lema $17^{25} \equiv 7^5 \bmod 125$, observamos que $7^5 \equiv 57 \bmod 125$. Llegados a este punto usamos el resultado por última vez y tenemos $17^{125} \equiv 57^5 \bmod 625$.

$$\begin{aligned} 57^5 &= (32 + 5^2)^5 \\ &= \binom{5}{0}32^5 + \binom{5}{1}32^4 5^2 + \binom{5}{2}32^3(5^2)^2 + \binom{5}{3}32^2(5^2)^3 + \binom{5}{4}32^1(5^2)^4 + \binom{5}{5}(5^2)^5. \end{aligned}$$

Reducimos la expresión módulo 5^4 y como los cuatro últimos términos son múltiplos de 625 nos quedan:

$$\begin{aligned} 57^2 &\equiv (32 + 5^2)^5 \bmod 625 \\ &\equiv 57 + 125 \bmod 625 \\ &\equiv 182 \bmod 625. \end{aligned}$$

Por tanto $T(17) \equiv 182 \bmod 5^4$.

En la siguiente proposición vamos a ver unas propiedades del levantamiento de Teichmüller.

Proposición 3. *Sea p un primo impar y $x \in (\mathbb{Z}/p^n)^*$.*
1. El elemento $T(x)$ cumple la igualdad $T(x)^{p-1} \equiv 1 \bmod p^n$
2. Para todo $r > n-1$, tenemos que $x^{p^r} \equiv T(x) \bmod p^n$.
3. $T(x)$ depende solo de la clase de x módulo p. Además, $T(x) \equiv x \bmod p$.
4. La aplicación

$$T\colon \quad (\mathbb{Z}/p)^* \longrightarrow (\mathbb{Z}/p^n)^*$$

es un homomorfismo inyectivo de grupos.

Demostración. 1. Puesto que $\varphi(p^n) = p^{n-1}(p-1)$, aplicando el teorema de Euler-Fermat obtenemos $x^{p^{n-1}(p-1)} \equiv 1 \bmod p^n$. Por definición $T(x) \equiv x^{p^{n-1}} \bmod p^n$, por tanto $T(x)^{p-1} \equiv 1 \bmod p^n$.

2. Por el apartado anterior sabemos que $T(x)^{p-1} \equiv 1 \bmod p^n$, por lo tanto $T(x)^p \equiv T(x) \bmod p^n$. Por otro lado, de la definición de $T(x)$ deducimos que $T(x)^p \equiv x^{p^n} \bmod p^n$. Utilizando estas dos expresiones llegamos a que $x^{p^n} \equiv T(x) \bmod p^n$. Iterando tenemos que $x^{p^r} \equiv T(x) \bmod p^n$ para todo $r \geqslant n$.

3. Para ver que $T(x)$ depende solo de x módulo p vamos a demostrar que si $x \equiv y \bmod p$ entonces $T(x) \equiv T(y) \bmod p^n$. Por el lema previo $x \equiv y \bmod p$ implica que $x^p \equiv y^p \bmod p^2$, iterando este procedimiento $n-1$ veces llegamos a que $x^{p^{n-1}} \equiv y^{p^{n-1}} \bmod p^n$ y por tanto tenemos que $T(x) \equiv T(y) \bmod p^n$.
La segunda parte del enunciado, $T(x) \equiv x \bmod p$. Ya la conocemos.

4.Puesto que $T(x)$ depende solo de la clase de x módulo p, la aplicación $T : (\mathbb{Z}/p)^* \to (\mathbb{Z}/p^n)^*$ está bien definida. Dado $x, y \in {\mathbb{F}_p}^*$ por la definicion de $T(x) \bmod p^n$,

$$T(xy) \equiv (xy)^{p^{n-1}} \equiv x^{p^{n-1}} y^{p^{n-1}} \equiv T(x)T(y) \bmod p^n.$$

Probamos ahora la inyectividad. Suponemos $T(x) \equiv T(y) \bmod p^n$ entonces $T(x) \equiv T(y) \bmod p$ y como por el apartado anterior tenemos que $T(x) \equiv x \bmod p$ y $T(y) \equiv x \bmod p$, entonces $x \equiv y \bmod p$.

□

El subgrupo $\mathbb{T} = T((\mathbb{Z}/p)^*) \subset (\mathbb{Z}/p^n)^*$ se llama grupo de levantamientos de Teichmüller. Es isomorfo a $(\mathbb{Z}/p)^*$, por tanto hay solamente $p-1$ levantamientos de Teichmüller distintos.

Ejemplo 6. Calculemos todos los levantamientos de Teichmüller módulo 5^4.
Sabemos que hay 4 diferentes.
Empezamos con $T(1)$, utilizando directamente la definición tenemos que $T(1) \equiv 1^{125} \bmod 5^4$, luego $T(1) \equiv 1 \bmod 5^4$.
Veamos ahora $T(2)$, este valor ya lo habíamos calculado antes, pues $17 \equiv 2 \bmod 5$ luego $T(17) \equiv T(2) \bmod 5^4$.
Nos preguntamos ahora por $T(4)$. Sabemos que $4 \equiv -1 \bmod 5$ por tanto $T(4) \equiv T(-1) \bmod 5^4$ y concluimos que $T(4) \equiv T(-1) \equiv (-1)^{125} \equiv -1 \bmod 5^4$.
Por último vamos a calcular el levantamiento de Teichmüller de 3 módulo 5^4. Es evidente que $3 \equiv -2 \bmod 5$, por tanto el problema se reduce a calcular $T(-2) \bmod 5^4$. Como la aplicación T es un homomorfismo de grupos $T(-2) \equiv T(-1)T(2) \equiv (-1)182 \equiv 443 \bmod 5^4$.
Conclusión:

$$T(1) \equiv 1 \bmod 5^4.$$

$$T(2) \equiv 182 \bmod 5^4.$$

$$T(3) \equiv 443 \bmod 5^4.$$

$$T(4) \equiv 624 \bmod 5^4.$$

El siguiente teorema es un resultado importante pues nos va a dar una descomposición del grupo $(\mathbb{Z}/p^n)^*$ que, además del interés teórico, será muy útil para abordar problemas como calcular potencias modulares, calcular el orden de un elemento en un grupo o calcular congruencias con potencias.

Teorema 6. *Sea p un primo impar. Dado un elemento $a \in (\mathbb{Z}/p^n)^*$, existen $x \in (\mathbb{Z}/p)^*$, $py \in p\mathbb{Z}/p^n$ únicos tales que $a \equiv T(x)exp(py) \bmod p^n$. Como consecuencia, la aplicación $a \to (x, py)$ define un isomorfismo de grupos*

$$(\mathbb{Z}/p^n)^* \simeq ((\mathbb{Z}/p)^*, \cdot) \times (p\mathbb{Z}/p^n, +).$$

Demostración. Tanto el grupo de levantamiento de Teichmüller, $\mathbb{T} = T(\mathbb{Z}/p)^*$ como el grupo $1 + p\mathbb{Z}/p^n$ son subgrupos del grupo de las unidades $(\mathbb{Z}/p^n)^*$. Puesto que este último es abeliano el producto

$$\mathbb{T} \cdot (1 + p\mathbb{Z}/p^n) = \{t(1 + px) \,|\, t \in \mathbb{T},\, 1 + px \in 1 + p\mathbb{Z}/p^n\}$$

es un subgrupo de $(\mathbb{Z}/p^n)^*$. Veamos que $\mathbb{T} \cap (1 + p\mathbb{Z}/p^n) = \{1\}$. En efecto, sean $a \in (\mathbb{Z}/p)^*$, $x \in \mathbb{Z}/p^n$ tales que $1 + px \equiv T(a) \bmod p^n$. Reduciendo módulo p: $1 \equiv T(a) \bmod p$ y, como $T(a) \equiv a \bmod p$ tenemos que $a = 1 \in (\mathbb{Z}/p)^*$. Por tanto, $T(a) = 1 \in (\mathbb{Z}/p^n)^*$ y $x = 0$. En este caso sabemos que el grupo producto $\mathbb{T} \times (1 + p\mathbb{Z}/p^n)$ es isomorfo a $\mathbb{T} \cdot (1 + p\mathbb{Z}/p^n)$. En particular $|\mathbb{T} \cdot (1 + p\mathbb{Z}/p^n)| = |\mathbb{T}| \cdot |(1 + p\mathbb{Z}/p^n)| = (p-1)p^{n-1}$, pero sabemos que $|(\mathbb{Z}/p^n)^*| = \varphi(p^n) = p^{n-1}(p-1)$ y por lo tanto tenemos:

$$(\mathbb{Z}/p^n)^* = \mathbb{T} \cdot (1 + p\mathbb{Z}/p^n) \simeq \mathbb{T} \times (1 + p\mathbb{Z}/p^n).$$

Ahora, basta usar los isomorfismo $\mathbb{T} : T((\mathbb{Z}/p)^*) \xrightarrow{\sim} (\mathbb{Z}/p)^*$ y $log : (1+p\mathbb{Z}/p^n) \xrightarrow{\sim} (p\mathbb{Z}/p^n, +)$ para tener el isomorfismo buscado:

$$(\mathbb{Z}/p^n)^* \simeq \mathbb{T} \times (1 + p\mathbb{Z}/p^n) \simeq ((\mathbb{Z}/p)^*, \cdot) \times (p\mathbb{Z}/p^n, +).$$

Observemos que el isomorfismo se realiza de la siguiente forma: Sea $a \in (\mathbb{Z}/p^n)^*$, tomamos x con $0 \leq x < p$ tal que $x \equiv a \bmod p$. Tenemos que $T(x) \equiv a \bmod p$. Puesto que $T(x) \in (\mathbb{Z}/p^n)^*$, $T(x)^{-1}a \equiv 1 \bmod p$, es decir, $T(x)^{-1}a \in 1 + p\mathbb{Z}/p^n$. Sea $y \in \mathbb{Z}/p^n$ único tal que $py \equiv log(T(x)^{-1}a) \bmod p^n$. En este caso tenemos:

$$\begin{array}{ccccc} (\mathbb{Z}/p^n)^* & \xrightarrow{\sim} & \mathbb{T} \times (1 + p\mathbb{Z}/p^n) & \xrightarrow{\sim} & (\mathbb{Z}/p)^* \times p\mathbb{Z}/p^n \\ a & \mapsto & (T(x), T(x)^{-1}a) & \mapsto & (x, py) \end{array}$$

Observamos que $a \equiv T(x)exp(py) \bmod p^n$.

□

La presentación del isomorfismo en el enunciado del Teorema se debe a que queremos poner de manifiesto precisamente la identificación $a \to (x, py)$ que es la formulación más útil en algunos cálculos. Veamos un ejemplo:

Ejemplo 7. Vamos a encontrar la descomposición de 13 mod 5^4. Es decir, calcularemos x e y tal que $13 \equiv T(x)exp(5y) \bmod 5^4$.
Es evidente que $13 \equiv 3 \bmod 5$, esto significa que $x = 3$. Calculemos ahora y. Tiene que ocurrir $exp(py) \equiv 13 \cdot T(3)^{-1}$. Sabíamos que $T(3) = 443$, como $3^{-1} \equiv 2 \bmod 5$, entonces $T(3)^{-1} = T(2) = 182$. Por tanto la expresión anterior queda de la siguiente manera:

$$exp(py) \equiv 13 \cdot 182 \equiv 491 \bmod 625.$$

Tomando logaritmos en ambos lados tendremos $py = log(491) \bmod 625$. Ahora el problema está en calcular $log(491) \bmod 625$. Como $log(491) = log(1 + 5 \cdot 98)$, veamos en primer lugar la expresión de $log(1 + 5x) \bmod 625$ a partir de la expresión como serie:

$$log(1 + 5x) = 5x - \frac{5^2x^2}{2} + \frac{5^3x^3}{3} - \frac{5^4x^4}{4} + \cdots .$$

Es evidente que si reducimos módulo 625 entonces todos los términos, excepto los tres primeros, son nulos y nos queda:

$$log(1+5x) \equiv 5x + 300x^2 + 250x^3 \bmod 625$$

Sustituyendo $x = 98$ tenemos $log(491) = 315 \bmod 625$ y concluimos con la congruencia

$$13 \equiv T(3)exp(315) \bmod 5^4. \tag{1.1}$$

Veremos ahora que la expresión anterior permite simplificar los cálculos en $\mathbb{Z}/5^4$:
a) Cálculo de $13^{234} \bmod 5^4$.
Utilizando (1.1) y la demostración del Teorema 6 tenemos que $13^2 \equiv T(3 \cdot 3)exp(315 + 315) \bmod 625$, luego

$$13^{234} \equiv T(3^{234})exp(315 \cdot 234) \bmod 625.$$

Como $234 = 58 \cdot 4 + 2$ y utilizando el Pequeño Teorema de Fermat llegamos a que $3^{234} \equiv 3^2 \bmod 5$ que es lo mismo que decir que $3^{234} \equiv 4 \bmod 5$. Por tanto, reducimos nuestro problema $T(3^{234}) \equiv T(4) \bmod 625$. Como ya hemos calculado $T(4)$ llegamos a que $T(3^{234}) \equiv 624 \bmod 5^4$. Por otro lado $234 \cdot 315 \equiv 585 \bmod 625$, y se tiene que: $exp(585) = 1 + 585 + \frac{585^2}{2} + \frac{585^3}{3!} \equiv 511 \bmod 5^4$. Por tanto $13^{234} \equiv 624 \cdot 511 \equiv 114 \bmod 5^4$.

b) Cálculo del orden del elemento 13 en $(\mathbb{Z}/5^4)^*$.
En este caso tenemos que calcular el n más pequeño tal que $13^n \equiv 1 \bmod 5^4$. Utilizando la expresión (1.1) tenemos que $T(3^n)exp(315 \cdot n) \equiv T(1)exp(0) \bmod 625$ y por su unicidad tenemos

$$3^n \equiv 1 \bmod 5 \Rightarrow n \equiv 0 \bmod 4$$

$$315 \cdot n \equiv 0 \bmod 625 \Rightarrow n \equiv 0 \bmod 125$$

Como 4 y 125 son enteros primos entre sí podemos aplicar el Teorema Chino de los Restos y concluimos $n \equiv 0 \bmod 500$, luego $13^{500} \equiv 1 \bmod 625$.

c) Resolver la ecuación $x^{47} \equiv 13 \bmod 5^4$.
Como $x = T(a)exp(5 \cdot b)$ y teniendo en cuenta la expresión (1.1) debe ser:

$$T(a^{47})exp(47 \cdot 5 \cdot b) \equiv T(3)exp(315) \bmod 625.$$

Es evidente que si calculamos a y b tendríamos resuelto el problema. Por la unicidad de la expresión anterior tenemos que $a^{47} \equiv 3 \bmod 5$ y $47 \cdot 5 \cdot b \equiv 315 \bmod 625$. Como sabemos que $47^{-1} \equiv 3 \bmod 625$ y utilizando el Pequeño Teorema de Fermat sacamos de la primera expresión que $a \equiv 2 \bmod 5$.
De la segunda ecuación obtenemos que $5 \cdot b \equiv 315 \cdot 133 \equiv 20 \bmod 625$, por tanto $exp(20) \equiv 1 + 20 + \frac{20^2}{2} + \frac{20^3}{3!} \equiv 96 \bmod 625$.
Con todo lo anterior llegamos a que $x \equiv T(2)exp(20) \bmod 625$, luego $x \equiv 597 \bmod 625$.

Nota. La descomposición de $(\mathbb{Z}/p^n)^*$ permite calcular una descomposición del grupo de unidades $(\mathbb{Z}/m)^*$ para cualquier $m \in \mathbb{Z}$: Si $m = p_1^{r_1} \cdots p_s^{r_s}$ es la factorización de m en primos distintos, el Teorema Chino nos proporciona el isomorfismo:

$$(\mathbb{Z}/m)^* \simeq (\mathbb{Z}/p_1^{r_1})^* \times \cdots \times (\mathbb{Z}/p_s^{r_s})^*.$$

Por tanto, podemos describir la estructura de $(\mathbb{Z}/m)^*$ a partir de la de $(\mathbb{Z}/p_i^{r_i})^*$ para $i = 1, ..., s$.

Capítulo 2

Números p-ádicos

2.1. Cuerpos normados

En este capítulo vamos a construir el cuerpo de los números p-ádicos. Para ello vamos seguir un método similar al que se utiliza para construir $\mathbb{R}$ a partir de $\mathbb{Q}$ mediante sucesiones de Cauchy. Este procedimiento es estándar en la construcción de espacios métricos completos a partir de otros que no lo son.

Definición 7. Sea $\mathbb{K}$ un cuerpo, un valor absoluto en $\mathbb{K}$ es una función $|\cdot| : \mathbb{K} \to \mathbb{R}_+$, que satisface las siguientes propiedades:
1) $|x| = 0 \Leftrightarrow x = 0$.
2) $|xy| = |x||y|$ para todo $x, y \in \mathbb{K}$.
3) $|x + y| \leq |x| + |y|$ para todo $x, y \in \mathbb{K}$.
Se dice, además, que es *no arquimediano* si, para todo $x, y \in \mathbb{K}$:
4) $|x + y| \leq \text{máx}\{|x|, |y|\}$.

A partir de un valor absoluto en $\mathbb{K}$ se define una distancia mediante $d(x, y) = |x - y|$ para $x, y \in \mathbb{K}$. Así pues, un valor absoluto en $\mathbb{K}$ permite definir en $\mathbb{K}$ una estructura de espacio métrico y en particular dota a $\mathbb{K}$ de una topología. Si el valor absoluto es no arquimediano decimos también que $\mathbb{K}$ es un espacio *ultramétrico*.

Nota. La asignación $|x|_0 = 1$ si $x \neq 0$ y $|x|_0 = 0$ si $x = 0$ define un valor absoluto (al que llamaremos trivial) en cualquier cuerpo. Si $\mathbb{K}$ es un cuerpo finito el valor absoluto trivial es el único posible. Sobre el cuerpo de los números racionales $\mathbb{Q}$, el valor absoluto "clásico": $|x|_\infty = x$ si $x \geqslant 0$ y $|x|_\infty = -x$ si $x < 0$ es, por supuesto un valor absoluto.

Tradicionalmente se dice que el valor absoluto $|\cdot|$ es $\mathbb{K}$ es arquimediano si para todos $x, y \in \mathbb{K}$, $x \neq 0$, entonces existe $n \in \mathbb{K}$ tal que $|nx| > |y|$.

Definición 8. Sea p un número primo y $x \in \mathbb{Q}$, definimos el valor absoluto p-ádico o la norma p-ádica de x como

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$$

Proposición 4. *El valor absoluto p-ádico que acabamos de definir es un valor absoluto no arquimediano sobre $\mathbb{Q}$.*

Demostración. Las condiciones 1), 2) y 3) son inmediatas a partir de las propiedades de $v_p(x)$. Para ver que es no arquimediano tenemos que probar que $|x + y|_p \leq \text{máx}\ \{|x|_p, |y|_p\}$. Cuando en el Capítulo 1 definíamos la evaluación p-ádica de los números racionales vimos que $v_p(x + y) \geqslant \text{mín}\{v_p(x), v_p(y)\}$, siendo $x, y \in \mathbb{Q}$. Por este motivo

$$|x + y|_p = p^{-v_p(x+y)} \leq p^{-\text{mín}\{v_p(x),\, v_q(y)\}}$$

y por tanto, tenemos lo que deseábamos, ya que $v_p(x) \leq v_p(y) \Leftrightarrow p^{-v_p(x)} \geqslant p^{-v_p(y)}$.

□

Definición 9. Se dice que dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ en el mismo cuerpo $\mathbb{K}$ son equivalentes si definen la misma topología sobre $\mathbb{K}$, es decir, si todo conjunto abierto en una topología es también un conjunto abierto en la otra.

Proposición 5. *Sean p y q dos primos distintos, entonces los valores absolutos $|\cdot|_p$ y $|\cdot|_q$ no son equivalentes. Además $|\cdot|_\infty$ no es equivalente a $|\cdot|_p$ para cualquier p primo.*

Demostración. La sucesión $\{p^n\}$ converge a 0 con la norma p-ádica, pero evidentemente no converge para $|\cdot|_\infty$ ni para $|\cdot|_q$ si q es un número primo distinto p.

□

Nota. En general si $|\cdot|_1$ y $|\cdot|_2$ son valores absolutos sobre $\mathbb{K}$, se tiene que son equivalentes si y solo si la condición $|x|_1 < 1$ equivale a $|x|_2 < 1$ para $x \in \mathbb{K}$. Nótese que $|x|_1 < 1$ equivale a su vez a que $\lim_{n\to\infty} x^n = 0$ para $|\cdot|_1$.

Un resultado importante es que los valores absolutos que hemos definido en $\mathbb{Q}$ son todos los que hay, más precisamente:

Teorema 7 (Ostrowski)**.** *Todo valor absoluto no trivial sobre $\mathbb{Q}$ es equivalente al valor absoluto p-ádico $|\cdot|_p$, donde p es o bien un primo o bien es equivalente a $|\cdot|_\infty$.*

Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto. Sea a un elemento de $\mathbb{K}$ y $r \in \mathbb{R}_+$. La bola abierta de centro a y radio r será:

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

La bola cerrada de centro a y radio r será:

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

Si $|\cdot|$ es un valor absoluto no arquimediano, se tienen las siguientes propiedades, todas ellas fáciles de comprobar

1. Si $b \in B(a,r)$, entonces $B(a,r) = B(b,r)$.

2. Si $b \in \overline{B}(a,r)$, entonces $\overline{B}(a,r) = \overline{B}(b,r)$.

3. El conjunto $B(a,r)$ es abierto y cerrado a la vez.

4. El conjunto $\overline{B}(a,r)$ es abierto y cerrado a la vez.

Proposición 6. *Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano en $\mathbb{K}$. El conjunto*

$$\mathcal{O} = \overline{B}(0,1) = \{x \in \mathbb{K} : |x| \leq 1\}$$

es un subanillo de $\mathbb{K}$. El conjunto

$$\mathfrak{p} = B(0,1) = \{x \in \mathbb{K} : |x| < 1\}$$

es un ideal de $\mathcal{O}$. Además, $\mathfrak{p}$ es un ideal maximal de $\mathcal{O}$ y todo elemento de $\mathcal{O} - \mathfrak{p}$ es invertible en $\mathcal{O}$. Así pues $(\mathcal{O}, \mathfrak{p})$ es un anillo local.

Demostración. Para probar que es un subanillo debemos probar que $\mathcal{O}$ respeta la suma y el producto y que el elemento nulo y el elemento unidad están en él. Evidentemente $1, 0 \in \overline{B}(0,1)$. Además, como estamos trabajando con un valor absoluto no arquimediano, si $x,\ y \in \mathcal{O}$, entonces $|x+y| \leq max\{|x|,\ |y|\} \leq 1$, luego $x+y \in \mathcal{O}$ y $|x \cdot y| = |x||y| \leq 1$. Puesto que $|-x|_p = |x|_p$, tenemos que $\mathcal{O}$ es un subanillo de $\mathbb{K}$.
Para ver que $\mathfrak{p}$ es el único ideal maximal de $\mathcal{O}$ basta con probar que $\mathcal{O} - \mathfrak{p} = (\mathcal{O})^*$. Consideramos un elemento $x \in \mathcal{O}$ pero que no está en $\mathfrak{p}$, luego no puede ser el elemento nulo y además, $|x| = 1$. Denotamos por x^{-1} al inverso de x en el cuerpo $\mathbb{K}$, luego $1 = |1| = |xx^{-1}| = |x||x^{-1}|$ y como $|x| = 1$, $x^{-1} \in \mathcal{O}$ y por tanto x es un elemento invertible del anillo.

□

Definición 10. Sea $\mathbb{K}$ un cuerpo y $|\cdot|$ un valor absoluto no arquimediano. El subanillo $\mathcal{O}$ se llama el anillo valoración de $(\mathbb{K}, |\cdot|)$ y al ideal $\mathfrak{p}$ se le llama el ideal de valoración. Al cociente

$$\mathbf{k} = \mathcal{O}/\mathfrak{p}$$

se le llama el cuerpo residual de $(\mathbb{K}, |\cdot|)$.

Proposición 7. *Sea $\mathbb{K} = \mathbb{Q}$ y consideramos $|\cdot|_p$ el valor absoluto p-ádico. Entonces:*
1) $\mathcal{O} = \mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} :\ mcd(a,b) = 1\, y\, p \not| b\}$.
2) $\mathfrak{p} = p\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} :\ mcd(a,b) = 1,\ p \not| b,\ p|a\}$.
3) El cuerpo cociente es $\mathbf{k} \simeq \mathbb{Z}/p$.

Demostración. Si consideramos un elemento de $\mathcal{O}$, llamémosle $\frac{a}{b}$ con $mcd(a,b) = 1$, entonces $|\frac{a}{b}|_p = p^{-v_p(a/b)} \leq 1$. Esta condición equivale a $v_p(\frac{a}{b}) \geqslant 0$, es decir, $p \not| b$. Por definición esto quiere decir que $\frac{a}{b} \in \mathbb{Z}_{(p)}$.
El razonamiento de la prueba de 2) es muy similar a la de 1). En efecto $|\frac{a}{b}|_p < 1$ equivale a $v_p(\frac{a}{b}) > 0$, luego $p \not| b$ y además $p|a$.
Por último, para demostrar 3) consideramos la aplicación:

$$\begin{array}{rccc} \phi\colon & \mathbb{Z}_{(p)} & \longrightarrow & \mathbb{F}_p \\ & \frac{a}{b} & \longmapsto & ab^{-1} \end{array}$$

cuyo núcleo es precisamente $p\mathbb{Z}_{(p)}$. Entonces, en virtud del primer teorema de isomorfía, tenemos que $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{F}_p$.

□

Nota. Todo elemento $x \in p\mathbb{Z}_{(p)}$ cumple que $v_p(x) \geqslant 1$ y entonces $|x|_p \leq p^{-1} < 1$ por tanto, $B(0,1) = p\mathbb{Z}_{(p)}$. De manera análoga, los elementos de $p^n\mathbb{Z}_{(p)}$ son aquellos que tienen valor absoluto p-ádico menor o igual que p^{-n}, por consiguiente, se da la siguiente igualdad $p^n\mathbb{Z}_{(p)} = \overline{B}(0, p^{-n})$. Las bolas abiertas de centro a y radio 1 son las traslaciones $a + p\mathbb{Z}_{(p)}$.

Nota. Si $x, y \in \mathbb{Q}$, usamos la notación $x \equiv y \bmod p^r$ como sinónimo de $x - y \in p^r\mathbb{Z}_{(p)}$, es decir $x \in y + p^r\mathbb{Z}_{(p)}$. Nótese que sobre $\mathbb{Q}$ la relación "$\equiv$" anterior es una congruencia para la operación suma ($(p^r\mathbb{Z}_{(p)}, +)$ es un subgrupo de $(\mathbb{Q}, +)$), pero no para el producto: por ejemplo si $x = (p^2+1)/p$, $y = 1/p$ se tiene $x \equiv y \bmod p$ ya que $x - y = p \subset p\mathbb{Z}_{(p)}$. Pero tomando $z = 1/p$ no es cierto que $zx \equiv zy \bmod p$ ya que $zx - zy = 1 \notin p\mathbb{Z}_{(p)}$.

2.2. Cuerpo de números p-ádicos. Enteros p-ádicos

Dado un cuerpo $\mathbb{K}$, denotamos por $\{x_n\}$ la sucesión de elementos de $\mathbb{K}$: $\{x_n : n = 1, ...\}$, así mismo $\{x\}$ denota la sucesión constantemente igual a x, es decir, la sucesión $\{x_n\}$ con $x_n = x$

para todo $n \geqslant 1$.

Dado un primo p, el cuerpo de los números racionales con la distancia p-ádica no es completo. En esta sección construiremos el completado p-ádico de $\mathbb{Q}$, $\mathbb{Q}_p$, es decir el menor cuerpo completo que contiene a $\mathbb{Q}$ respetando su estructura métrica. La construcción sigue los mismos pasos, sobradamente conocidos, de la construcción de $\mathbb{R}$ como completado de $\mathbb{Q}$ con la distancia $|\cdot|_\infty$

Proposición 8. *Sea $\{x_n\}$ una sucesión de números racionales. Entonces son equivalentes:*
1) $\{x_n\}$ es una sucesión p-ádica de Cauchy (es decir, una sucesión de Cauchy para la norma p-ádica $|\cdot|_p$).
2) La sucesión de números reales $\{|x_{n+1} - x_n|_p\}$ tiende a 0, es decir para cada $\epsilon \in \mathbb{R}_+$, existe $n_0 \in \mathbb{N}$ tal que $|x_{n+1} - x_n|_p < \varepsilon$ para todo $n \geqslant n_0$.
3) Para todo $r \in \mathbb{N}$, existe $n_0 \in \mathbb{N}$ tal que $x_n \equiv x_{n_0} \bmod p^r$ para todo $n \geqslant n_0$.
Además, si $\{x_n\}$ es una sucesión p-ádica de Cauchy, entonces $\{|x_n|_p\}$ es una sucesión acotada.

Demostración. La implicación de 1) a 2) es obvia. Recíprocamente suponemos cierta la condición 2) y sea $\varepsilon \in \mathbb{R}_+$. Existe entonces $n_0 \in \mathbb{N}$ tal que $|x_{n+1} - x_n|_p < \varepsilon$ para $n \geqslant n_0$. Ahora, si $m > n \geqslant n_0$ se tiene

$$\begin{aligned} |x_m - x_n|_p &= |x_m - x_{m-1} + x_{m-1} - \cdots - x_{n+1} + x_{n+1} - x_n|_p \\ &\leq max\{|x_{i+1} - x_i|_p : i = n, ..., m-1\} < \varepsilon. \end{aligned}$$

Supongamos que $\{x_n\}$ es de Cauchy y sea $r \in \mathbb{N}$. Existe $n_0 \in \mathbb{N}$ tal que $|x_m - x_{n_0}|_p \leq p^{-r}$ para todo $m \geqslant n_0$. Por lo tanto $x_m - x_{n_0} \equiv 0 \bmod p^r$, es decir $x_m \equiv x_{n_0} \bmod p^r$ para todo $m \geqslant n_0$. Recíprocamente, sea $\varepsilon > 0$ un número real y sea $r \in \mathbb{N}$ tal que $p^{-r} < \varepsilon \leq p^{-(r-1)}$. Existirá entonces $n_0 \in \mathbb{N}$ tal que $x_m \equiv x_{n_0} \bmod p^r$ para todo $m \geqslant n_0$. Si tomamos $m, n \geqslant n_0$ tendremos entonces que $x_m - x_n \equiv x_m - x_{n_0} \bmod p^r$, es decir, $|x_m - x_n|_p \leq p^{-r} < \varepsilon$.

Veamos ahora que si $\{x_n\}$ es de Cauchy, entonces $\{|x_n|_p\}$ es una sucesión acotada de números reales. Sea r un entero, sabemos que existe un $n_0 \in \mathbb{N}$ tal que $x_n - x_{n_0} \equiv 0 \bmod p^r$ para todo $n \geqslant n_0$, es decir $x_n \in x_{n_0} + p^r\mathbb{Z}_{(p)}$ y por tanto existe un elemento $k \in \mathbb{Z}_{(p)}$ con $x_n = x_{n_0} + p^r k$. En este caso, $|x_n|_p \leq \text{máx}\{|p^r k|_p, |x_{n_0}|_p\}$. Obsérvese que k depende de n; sin embargo, $|p^r k|_p = |p^r|_p |k|_p \leq |p^r|_p$ pues $k \in \mathbb{Z}_{(p)}$ y por tanto $|k|_p \leq 1$. Así pues tendremos que

$$|x_n|_p \leq \text{máx}\{|p^r k|_p, |x_{n_0}|_p\} \leq \text{máx}\{|p^r|_p, |x_{n_0}|_p\} = \text{máx}\{p^{-r}, |x_{n_0}|_p\}$$

para todo $n \geqslant n_0$. Ahora basta tomar $C = \text{máx}\{|x_1|_p, ..., |x_{n_0}|_p, p^{-r}\}$ y tenemos que $|x_n|_p \leq C$ para todo $n \geqslant 1$.

□

Vamos a denotar por $\mathcal{C}_p$ al conjunto de sucesiones de Cauchy de números racionales respecto de la norma p-ádica. Estamos interesados en ver que $\mathcal{C}_p$ tiene estructura de anillo conmutativo y unitario. Para ello tendremos que definir dos operaciones binarias.

Proposición 9. *Sean $\{x_n\}$ e $\{y_n\}$ dos sucesiones de números racionales de Cauchy respecto del valor absoluto p-ádico. Las siguientes operaciones*
a) $\{x_n\} + \{y_n\} = \{x_n + y_n\}$.
b) $\{x_n\} \cdot \{y_n\} = \{x_n y_n\}$.
Definen una estructura de anillo conmutativo en $\mathcal{C}_p$.

Demostración. Para ver que están bien definidas tenemos que ver que tanto $\{x_n + y_n\}$ como $\{x_n y_n\}$ son sucesiones de Cauchy.

a) Sabemos que $\{x_n\}$, $\{y_n\}$ son p-ádicas de Cauchy. Dado $\varepsilon > 0$ existen enteros n_x y n_y

tales que $|x_n - x_m|_p < \varepsilon$ para todo $n,\, m \geqslant n_x$ y $|y_n - y_m|_p \leq \varepsilon$ para todo $n,\, m \geqslant n_y$. Tomamos $N = \text{máx}\{n_x,\, n_y\}$, si $n,\, m \geqslant N$, $|(x_n + y_n) - (x_m + y_m)|_p \leq \text{máx}\{|x_n - x_m|_p,\, |y_n - y_m|_p\} < \varepsilon$. Por tanto, $\{x_n + y_n\}_n$ es una sucesión p-ádica de Cauchy.

b) Sabemos que $\{x_n\}$ e $\{y_n\}$ son sucesiones p-ádicas de Cauchy y por consiguiente existen dos constantes K' y K'' tales que $|x_n|_p \leq K'$ y $|y_n|_p \leq K''$ para todo $n \in \mathbb{N}$.
Sea $\varepsilon > 0$, sabemos que existe dos enteros n_x y n_y tales que $|x_n - x_m|_p < \varepsilon/K''$ para todo $n,\, m \geqslant n_x$ y $|y_n - y_m|_p \leq \varepsilon/K'$ para todo $n,\, m \geqslant n_y$.
Definimos $n_0 = \text{máx}\{n_x,\, n_y\}$. Para $n,\, m \geqslant n_0$ se verifican las dos expresiones anteriores y como consecuencia $|x_n \cdot y_n - x_m \cdot y_m|_p = |(x_n y_m - x_m y_m) + (x_n y_n - x_n y_m)|_p \leq \text{máx}\{|y_m|_p |x_n - x_m|_p,\, |x_n|_p |y_n - y_m|_p\}$
Si este máximo fuera $|y_m|_p |x_n - x_m|_p$, entonces $|x_n y_n - x_m y_m|_p < K''(\varepsilon/K'') = \varepsilon$ y si fuera $|x_m|_p |y_n - y_m|_p$, entonces $|x_n y_n - x_m y_m|_p < K'(\varepsilon/K') = \varepsilon$. Por tanto, $\{x_n y_n\}_n$ es una sucesión p-ádica de Cauchy.

Comprobar que $\mathcal{C}_p$ es un anillo es inmediato. Evidentemente es un grupo abeliano para la adición con elemento neutro la sucesión constantemente 0 y si $\{x_n\}$ es un elemto de $\mathcal{C}_p$, su elemento simétrico es $\{-x_n\}$, es decir la sucesión formada por los elementos simétricos de cada número racional x_n. Como también tenemos que si $\{x_n\},\, \{y_n\} \in \mathcal{C}_p$ entonces $\{x_n\} \cdot \{y_n\}_n = \{y_n x_n\}$, la sucesión $\{1\}$ es el elemento neutro del producto. Concluimos pues que $\mathcal{C}_p$ es un anillo conmutativo y unitario.

□

Sea $x \in \mathbb{Q}$. Es evidente que $\{x\} \in \mathcal{C}_p$. Por tanto, tenemos que la aplicación que va de $\mathbb{Q}$ en $\mathcal{C}_p$ y me lleva cada número racional x en la sucesión $\{x\}$ es una aplicación inyectiva y podemos ver $\mathbb{Q}$ como un subconjunto de $\mathcal{C}_p$.

Definición 11. Denotaremos por $\mathcal{N}$ al conjunto formado por las sucesiones $\{x_n\}$ de números racionales que convergen a 0 respecto al valor absoluto p-ádico. Es decir,

$$\mathcal{N} = \{\{x_n\} \,\text{con}\, x_n \in \mathbb{Q} :\ \{x_n\} \to 0\}.$$

Como toda sucesión convergente es de Cauchy, es evidente que $\mathcal{N}$ es un subconjunto de $\mathcal{C}_p$. Veamos ahora que además $\mathcal{N}$ es un ideal de $\mathcal{C}_p$. Si tenemos $\{x_n\},\, \{y_n\} \in \mathcal{N}$, entonces es claro que $\{x_n - y_n\}$ tiende a 0 y por tanto $\{x_n - y_n\} \in \mathcal{N}$, por tanto $\mathcal{N}$ es un subgrupo aditivo de $\mathcal{C}_p$. Supongamos ahora que tenemos dos sucesiones, la primera de ellas $\{x_n\} \in \mathcal{N}$ y la segunda $\{y_n\} \in \mathcal{C}_p$. Sabemos que existe una constante K de tal manera que $|y_n|_p \leq K$ para todo n. Dado $\varepsilon > 0$ sabemos que existe un $n_0 \in \mathbb{N}$ tal que $|x_n|_p < \varepsilon/K$ para todo $n \geqslant n_0$, por ser $\{x_n\}$ un elemento de $\mathcal{N}$. Por tanto $|x_n y_n - 0|_p = |x_n|_p |y_n|_p < (\varepsilon/K) \cdot K$ y entonces $\{x_n y_n\} \in \mathcal{N}$.

Nota. Podemos comprobar que si tenemos una sucesión $\{x_n\}$ de Cauchy que admite una subsucesión $\{x_{n_i}\} \in \mathcal{N}$, entonces $\{x_n\}$ está en $\mathcal{N}$. Fijamos $\varepsilon > 0$. Por un lado, como $\{x_{n_i}\}$ tiende a 0 entonces existe un entero N_1 tal que $|x_{n_i}|_p < \varepsilon$ para todo $n_i \geqslant N_1$. Por otro lado, al ser $\{x_n\}$ de Cauchy, existe un entero N_2 tal que $|x_n - x_m|_p < \varepsilon$ para todo $n, m \geqslant N_2$. Denotamos $N = \text{máx}\{N_1, N_2\}$ y tomando $n, n_i \geqslant N$ tenemos que $|x_n|_p = |x_n - x_{n_i} + x_{n_i}|_p \leq \text{máx}\{|x_n - x_{n_i}|_p, |x_{n_i}|_p\} < \varepsilon$.

Lema 7. *$\mathcal{N}$ es un ideal maximal de $\mathcal{C}_p$.*

Demostración. Tenemos que ver que $\mathcal{N}$ no esta contenido en ningún otro ideal propio. Sea $\{x_n\}$ una sucesión de Cauchy pero que no tiende a cero, es decir que está en $\mathcal{C}_p$ pero no en $\mathcal{N}$. Denotamos por I al ideal generado por la sucesión $\{x_n\}$ y el ideal $\mathcal{N}$, es evidente que $\mathcal{N} \subset I$, por lo tanto si vemos que I es en realidad todo el anillo $\mathcal{C}_p$ habríamos acabado.

Como la sucesión $\{x_n\}$ no tiende a 0 y es de Cauchy quiere decir que existe una constante C y un entero n_0 tal que $|x_n|_p \geqslant C$ para todo $n \geqslant n_0$, pues si no fuera así para cualquier $C > 0$ y un entero N existiría un $n > N$ tal que $|x_n|_p < C$. Esto significa que podríamos extraer una subsucesión de $\{x_n\}$ que estuviera en $\mathcal{N}$ y por la nota anterior $\{x_n\}$ estaría en $\mathcal{N}$. Teniendo en cuenta esto, construimos una nueva sucesión $\{y_n\}$ mediante:

$$y_n = \begin{cases} 0 & \text{si } n < n_0 \\ \frac{1}{x_n} & \text{si } n \geqslant n_0. \end{cases}$$

A continuación, vamos a comprobar que esta nueva sucesión $\{y_n\}$ está en $\mathcal{C}_p$. Dado $\varepsilon > 0$, al ser $\{x_n\}$ una sucesión de Cauchy, existe un entero n' tal que $|x_n - x_{n+1}|_p < C^2\varepsilon$ para todo $n \geqslant n'$. De esta manera tenemos que:

$$|y_{n+1} - y_n|_p = \left|\frac{1}{x_{n+1}} - \frac{1}{x_n}\right|_p = \left|\frac{x_n - x_{n+1}}{x_n x_{n+1}}\right|_p \leq \frac{|x_n - x_{n+1}|_p}{C^2} < \varepsilon.$$

Por tanto $\{y_n\}$ es una sucesión de Cauchy.

Haciendo el producto de la sucesión $\{x_n\}_n$ con la sucesión $\{y_n\}$ obtenemos otra sucesión de $\mathcal{C}_P$ y será la que tiene todo ceros en las primeras $n_0 - 1$ posiciones y desde la posición n_0 en adelante tiene unos. Definimos ahora una última sucesión, que también es de Cauchy, $\{1\} - \{x_n y_n\}$ es la sucesión que tiene unos en las primeras $n_0 - 1$ posiciones y el resto son ceros. Además, es claro que $\{1\} - \{x_n y_n\}$ tiende a 0, luego está en el ideal $\mathcal{N}$. Ahora se puede escribir $\{1\}$ como un múltiplo de $\{x_n\}_n$ más un elemento de $\mathcal{N}$, luego $\{1\}$, que es el elemento unidad del anillo $\mathcal{C}_p$, está en I y esto quiere decir que el ideal I es el total. Por tanto $\mathcal{N}$ es un ideal maximal.

□

Definición 12. Dado que $\mathcal{N}$ es un ideal maximal de $\mathcal{C}_p$, el anillo cociente es un cuerpo. Definimos el cuerpo de los números p-ádicos como

$$\mathbb{Q}_p := \mathcal{C}_p/\mathcal{N}.$$

Vamos a estudiar cómo son los elementos del cuerpo $\mathbb{Q}_p$.

Nota. Consideramos $x, a \in \mathbb{Q}_p$. Si $|a - x|_p < |x|_p$, entonces $|a|_p = |x|_p$. La explicación es la siguiente: utilizando el hecho de ser una norma no arquimediana y $|a - x|_p < |x|_p$ llegamos a $|a|_p = |a - x + x|_p \leq \text{máx}\{|a - x|_p, |x|_p\} = |x|_p$. De manera similar, $|x|_p \leq \text{máx}\{|x - a|_p, |a|_p\}$, observamos que $|a|_p \leq |x-a|_p$ es imposible, pues en ese caso $|x|_p \leq |x-a|_p$. Por tanto $|x|_p \leq |a|_p$ y se concluye con $|x|_p = |a|_p$.

Denotando $a = y + x$ y $x = x$ el enunciado queda: Si $|y|_p \neq |x|_p$, entonces $|x + y|_p = \text{máx}\{|x|_p, |y|_p\}$.

Lema 8. *Sea $\{x_n\}$ una sucesión que pertenece a $\mathcal{C}_p$ pero no a $\mathcal{N}$, entonces existe un entero N de tal manera que $|x_n|_p = |x_m|_p$ para todo $n, m \geqslant N$. Es decir, la sucesión de números reales $\{|x_n|_p\}$ es estacionaria. Además, si $\{y_n\} \in \{x_n\} + \mathcal{N}$, se tiene que $|y_n|_p = |x_n|_p$ para n suficientemente grande.*

Demostración. Al ser $\{x_n\}$ una sucesión de Cauchy que no converge a 0, existen dos enteros c y N_1 tales que para todo $n \geqslant N_1$ se tiene $|x_n|_p \geqslant c > 0$. Para ese mismo c y por ser una sucesión de Cauchy, existe otro N_2 tal que para todo $n, m \geqslant N_2$, $|x_n - x_m|_p < c$.
Definimos $N = \text{máx}\{N_1, N_2\}$, luego para todo $n, m \geqslant N$ sabemos que $|x_n - x_m|_p < c \leq \text{máx}\{|x_n|_p, |x_m|_p\}$ y por lo tanto, en virtud de la nota anterior, $|x_n|_p = |x_m|_p$.

Sea ahora $\{y_n\} = \{x_n\} + \{z_n\}$ con $\{z_n\} \in \mathcal{N}$ y supongamos que $C = |x_n|_p$ para $n \geqslant n_0$. Puesto que $\{z_n\} \to 0$, existe $n_1 \in \mathbb{N}$ tal que $|z_n|_p < C$ para $n \geqslant n_1$. Si tomamos $n \geqslant n_0$, $n \geqslant n_1$ tenemos que: $|z_n|_p < |x_n|_p$ y por tanto

$$|y_n|_p = |x_n + z_n|_p = \text{máx}\{|x_n|_p, |z_n|_p\} = |x_n|_p$$

□

Observamos que, como consecuencia, podemos definir:

Definición 13. Si λ es un elemento del cuerpo $\mathbb{Q}_p$ y $\{x_n\}$ es una sucesión que representa a λ, se define

$$|\lambda|_p := \lim_{n\to\infty} |x_n|_p.$$

Es claro que $|0|_p = 0$, ya que $0 \in \mathbb{Q}_p$ está representado por una sucesión de $\{x_n\} \in \mathcal{N}$ y $\lim_{n\to\infty} |x_n|_p = 0$. Si $\lambda \in \mathbb{Q}_p$, $\lambda \neq 0$, existe un entero $v_p(\lambda)$ único de manera que $|\lambda|_p = p^{-v_p(\lambda)}$, justamente $v_p(\lambda) = v_p(x_n)$ para n suficientemente grande y $\{x_n\} \in \mathcal{C}_p$ un representante de λ. Así pues $|\cdot|_p : \mathbb{Q}_p \longrightarrow \mathbb{R}_+$ es un valor absoluto no arquimediano que extiende a $|\cdot|_p$ sobre $\mathbb{Q}$. Además el conjunto de valores es $\{0\} \cup \{p^r : r \in \mathbb{Z}\}$.

Estamos interesados en probar que el cuerpo $\mathbb{Q}_p$ es completo respecto al valor absoluto que acabamos de definir, pero antes vamos a ver que otro resultado que nos será útil.

Proposición 10. *$\mathbb{Q}$ es denso en $\mathbb{Q}_p$.*

Demostración. Sea $\lambda \in \mathbb{Q}_p$ y fijamos $\varepsilon > 0$. Veamos que $B(\lambda, \varepsilon) \cap \mathbb{Q} \neq \emptyset$.
Sea $\{x_n\} \in \mathcal{C}_p$ un representante de λ. Como es una sucesión de Cauchy, dado $\varepsilon' > 0$, $\varepsilon' < \varepsilon$, existe un entero N tal que $|x_n - x_m|_p < \varepsilon'$ para todo n, $m \geqslant N$. Definimos $\{y\}$ como la sucesión constantemente igual al valor x_N, evidentemente $\{y\}$ está en $\mathbb{Q}$, visto como subconjunto de $\mathbb{Q}_p$. Vamos a estudiar $|\lambda - \{y\}|_p$, o lo que es lo mismo $|\{x_n\} - \{y\}|_p$. Por definición sabemos que $|\{x_n\} - \{y\}|_p = \lim_{n\to\infty} |x_n - x_N|_p = 0$. Si consideramos $n \geqslant N$, es claro que $|x_n - x_N|_p < \varepsilon'$, por tanto $|\{x_n\} - \{y\}|_p < \varepsilon' < \varepsilon$ y se tiene que $\{y\} \in B(\lambda, \varepsilon)$ como deseábamos.

□

Teorema 8. *$\mathbb{Q}_p$ es completo respecto al valor absoluto $|\cdot|_p$*

Demostración. Sea $\{\lambda_n\}$ una sucesión de Cauchy en $\mathbb{Q}_p$. Dado que $\mathbb{Q}$ es denso es $\mathbb{Q}_p$ sabemos que para cada n existe un $q_n \in \mathbb{Q}$ tal que, si denotamos por $\hat{q}_n$ la sucesión constantemente igual a q_n, entonces $|\lambda_n - \hat{q}_n|_p < 1/n$. Entonces, $|\lambda_n - \hat{q}_n|_p \to 0$ si $n \to \infty$, por tanto la sucesión $\{\lambda_n - \hat{q}_n\}$ converge a 0 y también es una sucesión de Cauchy en $\mathbb{Q}_p$.

La sucesión $\{\hat{q}_n\}$ también es de Cauchy en $\mathbb{Q}_p$. En efecto, dado que $\{\hat{q}_n\} = \{\lambda_n\} - \{\lambda_n - \hat{q}_n\}$ se concluye que $\{\hat{q}_n\}$ es de Cauchy por ser diferencia de sucesiones de Cauchy.

Dado que $|\hat{q}_n - \hat{q}_m|_p = |q_n - q_m|_p$ y como $\hat{q}_n$ es de Cauchy, para $\varepsilon > 0$ existe una entero N tal que para todo $n, m \geqslant N$ tenemos $|q_n - q_m|_p = |\hat{q}_n - \hat{q}_m|_p < \varepsilon$. Por tanto, la sucesión de números racionales $\{q_n\}$ es de Cauchy y, por consiguiente, define un número p-ádico que denotaremos por q. Finalmente probaremos que $\lim_{n\to\infty} \lambda_n = q$ y concluiremos la demostración. Como $\{\lambda_n - q\} = \{\lambda_n - \hat{q}_n\} + \{\hat{q}_n - q\}$, por lo visto anteriormente, tenemos que $\{\lambda_n - \hat{q}_n\} \to 0$ si $n \to \infty$. Por otro lado, $|\hat{q}_n - q|_p = \lim_{i\to\infty} |q_n - q_i|_p$ que tiende a cero cuando n tiende a infinito por ser $\{q_n\}$ una sucesión de Cauchy, con lo que $\{\hat{q}_n - q\} \to 0$ cuando $n \to \infty$. Por lo tanto $\{\lambda_n - q\} \to 0$ cuando $n \to \infty$.

□

Nótese que en la demostración hemos usado el hecho trivial de que la Proposición 9 es cierta para sucesiones de Cauchy en $\mathbb{Q}_p$.

2.3. Anillo de los enteros p-ádicos $\mathbb{Z}_p$

Definición 14. Llamaremos anillo de los enteros p-ádicos al anillo valoración de $(\mathbb{Q}_p, |\cdot|_p)$, es decir $\{x \in \mathbb{Q}_p \text{ tal que } |x|_p \leq 1\}$ y lo denotaremos por $\mathbb{Z}_p$.

Veamos algunas propiedades del anillo de los enteros p-ádicos que nos van a permitir seguir estudiando el cuerpo $\mathbb{Q}_p$.

Proposición 11. *El grupo de los elementos invertibles de $\mathbb{Z}_p$ es $(\mathbb{Z}_p)^* = \{x \in \mathbb{Q}_p \text{ tal que } |x|_p = 1\}$. El anillo $\mathbb{Z}_p$ es un anillo local y su único ideal maximal es $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \text{ tal que } |x|_p < 1\}$.*

Es un caso particular de la Proposición 6.

Proposición 12. *Se tienen las siguientes propiedades:*
1. $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$.
2. $\mathbb{Z}$ es denso en $\mathbb{Z}_p$. En particular, dados $x \in \mathbb{Z}_p$ y $n \geqslant 1$, existe un $\alpha \in \mathbb{Z}$ con $0 \leq \alpha < p^n$ tal que $|x - \alpha|_p \leq p^{-n}$. El entero α con estas propiedades es único.
3. Para todo $x \in \mathbb{Z}_p$, existe una sucesión de Cauchy de números enteros, $\{\alpha_n\}$, que converge a x y tal que $0 \leq \alpha_n \leq p^n - 1$ y $\alpha_{n+1} \equiv \alpha_n \bmod p^n$ para todo $n \geqslant 1$. Además la sucesión $\{\alpha_n\}$ con estas propiedades es única.

Demostración. 1. $\mathbb{Q} \cap \mathbb{Z}_p = \{x \in \mathbb{Q} \,|\, |x|_p \leq 1\} = \{x \in \mathbb{Q} \,|\, v_p(x) \geqslant 0\} = \mathbb{Z}_{(p)}$.

2. Sea $x \in \mathbb{Z}_p$, por ser $\mathbb{Q}$ denso en $\mathbb{Q}_p$, dado $n \geqslant 1$ existe $\frac{a}{b} \in \mathbb{Q}$ tal que $|x - \{\frac{a}{b}\}|_p \leq p^{-n} < 1$. Estamos interesados en encontrar un número $\alpha \in \mathbb{Z}$ en lugar del que ya tenemos $\frac{a}{b} \in \mathbb{Q}$. Tenemos que $|\frac{a}{b}|_p = |\frac{a}{b} - x + x|_p \leq \text{máx}\{|x|_p, |x - \frac{a}{b}|_p\} \leq 1$. Por lo tanto como $\{\frac{a}{b}\}$ está en $\mathbb{Q}$ y en $\mathbb{Z}_p$ y por la propiedad anterior está en $\mathbb{Z}_{(p)}$. Tomando $\frac{a}{b}$ reducida, es decir $mcd(a, b) = 1$, $\frac{a}{b} \in \mathbb{Z}_{(p)}$ equivale a $p \not| b$. Así pues $mcd(p^n, b) = 1$ y existe $b' \in \mathbb{Z}$ tal que $bb' \equiv 1 \bmod p^n$. Puesto que $p \not| b : |\frac{a}{b} - ab'|_p = |\frac{a(1-bb')}{b}|_p \leq p^{-n}$. Ahora:

$$\begin{aligned} |x - ab'|_p &= |x - \frac{a}{b} + \frac{a}{b} - ab'|_p \\ &\leq max\{|x - \frac{a}{b}|_p, |\frac{a}{b} - ab'|_p\} \leq p^{-n}. \end{aligned}$$

Por tanto, ya tenemos la existencia de un entero ab' tal que $|x - ab'|_p \leq p^{-n}$.
Tomando $\alpha \in \mathbb{Z}$ el único entero con $0 \leq \alpha < p^{-n}$ y $\alpha \equiv ab' \bmod p^n$ terminamos.

3. Para $n \geqslant 1$ tenemos $\alpha_n \in \mathbb{Z}$ el único entero con $0 \leq \alpha_n < p^{-n}$ y $|x - \alpha_n|_p \leq p^{-n}$. La sucesión $\{\alpha_n\}$ es la sucesión de Cauchy buscada.

□

Como ya habíamos anunciado, el anillo de los enteros p-ádicos y sus propiedades nos van a ayudar a seguir estudiando las propiedades el cuerpo de los números p-ádicos. A continuación, daremos un sistema fundamental de entornos del $0 \in \mathbb{Q}_p$.

Corolario 1. *$\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, es decir, para cada $x \in \mathbb{Q}_p$ existe un $n \geqslant 0$ tal que $p^n x \in \mathbb{Z}_p$. La aplicación $\mathbb{Q}_p \to \mathbb{Q}_p$ dada por $x \mapsto px$ es un homeomorfismo. Los conjuntos $p^r\mathbb{Z}_p$, $r \in \mathbb{Z}$ forman un sistema fundamental de entornos del $0 \in \mathbb{Q}_p$ y además recubren $\mathbb{Q}_p$.*

Demostración. Sea $x \in \mathbb{Q}_p$. Si $v_p(x) \geqslant 0$ entonces $x \in \mathbb{Z}_p$. Si $v_p(x) < 0$ tenemos que $v_p(p^{-v_p(x)}x) = -v_p(x) + v_p(x) = 0$ y entonces $|p^{-v_p(x)}x|_p = 1$, por lo tanto $p^{-v_p(x)}x \in \mathbb{Z}_p$ y $-v_p(x) > 0$.

Es claro que la aplicación $x \mapsto px$ es continua, además $\mathbb{Q}_p$ es un cuerpo por tanto podemos considerar p^{-1} y entonces la aplicación es biyectiva. Su inversa es $x \mapsto p^{-1}x$.

Sabemos que $\overline{B}(0, p^{-n}) = p^n\mathbb{Z}_p$ es un entorno abierto y cerrado del 0 ya que $\mathbb{Z}_p$ lo es y la multiplicación por p^n es un homeomorfismo. Sea $x \in \mathbb{Q}_p$, entonces existe un n tal que $p^n x \in \mathbb{Z}_p$

esto implica que $p^n x = y \in \mathbb{Z}_p$ luego $x = p^{-n} y \in \mathbb{Z}_p$ y por tanto, $x \in \bigcup_{n\in\mathbb{Z}} p^n\mathbb{Z}_p$. Ya tenemos que $\bigcup_{n\in\mathbb{Z}} p^n\mathbb{Z}_p$ recubre todo el cuerpo de los números p-ádicos.
Es evidente que los conjuntos $p^n\mathbb{Z}_p$ forman un sistema fundamental de entornos de 0, pues para cada bola de radio ε puedo encontrar un entero n lo suficientemente grande como para que $\frac{1}{p^n} \leq \varepsilon$ y por lo tanto $p^n\mathbb{Z}$ esté contenido en la bola de radio ε.

□

Proposición 13. $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Demostración. Sea $p^n : \mathbb{Z}_p \to \mathbb{Z}_p$ la aplicación que envía cada elemento $x \in \mathbb{Z}_p$ a $p^n x \in \mathbb{Z}_p$. Es claro que esta aplicación es inyectiva. Definimos otra aplicación $f : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$: dado $x \in \mathbb{Z}_p$, entonces $f(x) = \alpha \in \mathbb{Z}$ siendo α el único entero $0 \leq \alpha < p^n$ tal que $|x - \alpha|_p \leq p^{-n}$. Esta aplicación está bien definida por la Proposición 12. Además es sobreyectiva. Si vemos que

$$0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}/p^n\mathbb{Z} \to 0$$

es una sucesión exacta, en virtud del teorema de isomorfía quedaría terminada la demostración. Para probar la exactitud de la serie basta comprobar que $Im(p^n) = Ker(f)$. Suponemos $x \in Ker(f)$ luego $f(x) = \alpha \equiv 0 \mod p^n$, por tanto $x \in p^n\mathbb{Z}_p = Im(f)$ ya que $|x - 0|_p \leq p^{-n}$. Recíprocamente, sea $x \in Im(p^n)$, o lo que es lo mismo $x \in p^n\mathbb{Z}_p$, sabemos que $|x|_p \leq p^{-n}$ y por otro lado, si $f(x) = \alpha$ se tiene que $|x - \alpha|_p \leq p^{-n}$ y por la unicidad de α se concluye que $\alpha \equiv 0 \mod p^n$.

□

Dado $x \in \mathbb{Z}_p$, a partir de la Proposición 12 podemos definir la sucesión $\{\alpha_n\}$ de números enteros de manera que para $n \geqslant 1$, α_n es el único entero con $0 \leq \alpha_n < p^n$ y tal que $|x - \alpha_n|_p \leq p^{-n}$. Además, la sucesión es "coherente" en el sentido de que $\alpha_{n+1} \equiv \alpha_n \mod p^n$ para todo $n \geqslant 1$. Obsérvese la semejanza de esta sucesión con las sucesiones $\{a_n\}$ descritas al comienzo de la sección 1.2. Como ya se hizo allí, podemos definir otra sucesión $\{b_n\}$ de la forma siguiente: $b_0 = \alpha_1$, ahora $\alpha_2 \equiv \alpha_1 \mod p$, por tanto se tiene que $\alpha_2 = \alpha_1 + b_1 p$. Además, $0 \leq b_1 < p$, ya que $\alpha_2 < p^2$, y b_1 es único. Recursivamente, si suponemos definidos $b_0, ..., b_{n-1}$ con $0 \leq b_i < p$ y $\alpha_n = b_0 + b_1 p + \cdots + b_{n-1}p^{n-1}$, el hecho que $\alpha_{n+1} \equiv \alpha_n \mod p^n$ implica la existencia de $b_n \in \mathbb{Z}$ único con $0 \leq b_n < p$ y tal que:

$$\alpha_{n+1} \equiv \alpha_n + b_n p^n = b_0 + b_1 p + \cdots + b_n p^n.$$

Sea $s = \sum_{i\geqslant 0} b_i p^i$ la serie numérica de potencias definida a partir de la sucesión $\{b_n\}$. Puesto que la sucesión de sumas parciales es la sucesión $\{\alpha_n\}$ que es convergente (es trivialmente de Cauchy), s es una serie convergente y su límite es x:

$$x = \sum_{i\geqslant 0} b_i p^i = b_0 + b_1 p + \cdots$$

Este resultado se puede extender a todo $\mathbb{Q}_p$:

Teorema 9. *Sea $x \in \mathbb{Q}_p$. Entonces existe $m \in \mathbb{Z}$ y $\{b_n : n \geqslant m\}$ enteros, únicos, con la condición $0 \leq b_i < p$ tales que $x = \sum_{n\geqslant m} b_n p^n$.*

Demostración. Si $x \in \mathbb{Z}_p$ ya conocemos el resultado. Si $x \in \mathbb{Q}_p - \mathbb{Z}_p$, sea $k \geqslant 0$ el menor entero tal que $p^k x \in \mathbb{Z}_p$. La expresión como serie de $p^k x$ proporciona la expresión de x como $\sum_{i\geqslant m} b_i p^i$ tomando $m = -k$:

$$x = b_m \frac{1}{p^m} + \cdots + b_{-1}\frac{1}{p} + b_0 + b_1 p + \cdots$$

□

Nota. La expresión de $x \in \mathbb{Z}_p$ como $x = \sum_{i \geqslant 0} b_i p^i$ es la escritura p-ádica de x, esencialmente semejante a la expresión decimal de un número real, $x = \cdots b_n b_{n-1} \cdots b_1 b_0$. En el caso $x \in \mathbb{Q}_p - \mathbb{Z}_p$ los dígitos $b_{-1}, b_{-2}, ..., b_{-k}$ son las cifras decimales.

$$x = \cdots b_m \cdots b_1 b_0, b_{-1} b_{-2} \cdots b_{-k} = \sum_{i \geqslant -k} b_i p^i.$$

Nótese que $x \in \mathbb{Z}$ si y solo si la expresión de x es finita y no tiene decimales. Por otro lado, en general la expresión de un número p-ádico $x \in \mathbb{Q}_p$ tiene infinitas cifras, pero sólo un número finito de "decimales", justo al contrario de la expresión decimal de un número real.

Finalizaremos esta sección con algunas propiedades topológicas de $\mathbb{Q}_p$ que completan una primera aproximación a la comprensión del cuerpo p-ádico $\mathbb{Q}_p$.

Proposición 14. *Sea $s = \{x_n\}$ una sucesión de enteros p-ádicos, es decir, $x_n \in \mathbb{Z}_p$ para todo $n \geqslant 1$. Entonces existe una subsucesión convergente. En otras palabras, $\mathbb{Z}_p$ es secuencialmente compacto.*

Demostración. Para cada $m \geqslant 1$, sea $\{\alpha_n^m\}$ la sucesión definida por x_m en la Proposición 12. Es decir, $\alpha_n^m \in \mathbb{Z}$ con $0 \leq \alpha_n^m < p^n$ y $|x_m - \alpha_n^m|_p \leq p^{-n}$. Para $n = 1$ tenemos: $\{\alpha_1^m \,|\, m = 1, ...\} \subset \{0, 1, 2, ..., p-1\}$. Por lo tanto, existe un entero $\beta_1 \in \{0, 1, ..., p-1\}$ y un subconjunto $S_1 \subset \mathbb{N}$ de manera que $\alpha_1^i = \beta_1$ para todo $i \in S_1$. Por tanto, $s_1 = \{x_i \,|\, i \in S_1\}$ es una subsucesión de s de manera que todos los elementos empiezan por β_1. Ahora, tenemos $\{\alpha_2^m \,|\, m \in S_1\} \subset \{0, 1, ..., p^2 - 1\}$. Como antes, existe $S_2 \subset S_1$ infinito y $\beta_2 \in \{0, 1, ...p^2 - 1\}$ de manera que $\alpha_2^m = \beta_2$ para $m \in S_2$. De esta forma se construyen recursivamente subconjuntos infinitos:

$$\mathbb{N} \supset S_1 \supset S_2 \supset ... \supset S_k \supset ...$$

y por tanto subsucesiones $s_i = \{x_i \,|\, i \in S_i\}$ de manera que para cada $i \geqslant 1$ todos los elementos de s_i comienzan por $\beta_i ... \beta_2 \beta_1$, es decir $\alpha_k^m = \beta_k$ para todo $m \in S_i$ y para todo $k \leq i$. Definimos ahora la sucesión $\{y_n\}$ de $\{x_n\}$ tomando como y_n el elemento n-ésimo de la sucesión $s_n = \{x_i \,|\, i \in S_n\}$. Evidentemente es una subsucesión de $\{x_n\}$ y es sencillo probar que $\{y_n\} \to \beta$, siendo $\beta \in \mathbb{Z}_p$ el límite de la sucesión de Cauchy $\{\beta_n\}$.

□

Teorema 10. *Se tiene las siguientes propiedades topológicas de $\mathbb{Q}_p$:*
1) $\mathbb{Q}_p$ es totalmente desconectado y Hausdorff.
2) $\mathbb{Z}_p$ es uniformemente acotado.
3) $\mathbb{Z}_p$ es compacto y completo y $\mathbb{Q}_p$ es localmente compacto.

Demostración. 1) Si $x, y \in \mathbb{Q}_p$, $x \neq y$, sea $p^{-m} < d(x, y)$, $m \in \mathbb{Z}$. Evidentemente $y \notin x + p^m \mathbb{Z}_p$ y también $x \notin y + p^m \mathbb{Z}_p$. Por tanto $\overline{B}(x, p^m)$ y $\overline{B}(y, p^m)$ son entornos abiertos disjuntos de x e y. El hecho de que las bolas abiertas sean también cerradas garantizan que la componente conexa de $x \in \mathbb{Q}_p$ es el conjunto unipuntual $\{x\}$.

2) Para cada $n \geqslant 1$, el conjunto de las bolas cerradas $\overline{B}(\alpha, p^{-n}) = \alpha + p^n \mathbb{Z}_p$ cuando $\alpha \in \{0, 1, ...p^n - 1\}$ recubren $\mathbb{Z}_p$. Puesto que $\{p^{-n}\} \to 0$ si $n \to \infty$, $\mathbb{Z}_p$ es uniformemente acotado.

3) $\mathbb{Z}_p$ es un cerrado de $\mathbb{Q}_p$ que es secuencialmente compacto, por tanto $\mathbb{Z}_p$ es compacto y completo. Además, para cada $x \in \mathbb{Q}_p$, $x + \mathbb{Z}_p$ es un entorno compacto de x.

□

Capítulo 3

Propiedades de los números p-ádicos

En el primer capítulo del trabajo hemos presentado dos problemas sobre el anillo local $\mathbb{Z}_{(p)}$. El primero de ellos era calcular las raíces de un polinomio, a lo que llegábamos era a una sucesión $\{a_n\}$ de elementos de $\mathbb{Z}_{(p)}$ que eran solución del polinomio módulo p^n. El objetivo del segundo problema con el que trabajábamos era poder definir las funciones exponencial y logaritmo en $\mathbb{Z}_{(p)}$, dándolas sentido módulo p^n. En este último capítulo vamos a ver que estos dos problemas se expresan de forma natural cuando los trabajamos sobre el cuerpo de los números p-ádicos $\mathbb{Q}_p$. En el Lema de Hensel vamos a llegar a la existencia de una única raíz del polinomio que será un entero p-ádico. Por último, veremos que podemos definir las funciones exponencial y logaritmo en sus radios de convergencia.

3.1. Lema de Hensel

Una de las propiedades más importantes de los enteros p-ádicos $\mathbb{Z}_p$ es el teorema conocido como Lema de Hensel. Este lema nos va a garantizar, bajo ciertas circunstancias, que un polinomio tenga raíces en $\mathbb{Z}_p$.

Teorema 11 (Lema de Hensel)**.** *Sea $F(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ un polinomio con coeficientes en $\mathbb{Z}_p$. Supongamos que existe un entero p-ádico al que llamaremos α_1 que cumple*

$$F(\alpha_1) \equiv 0 \bmod p\mathbb{Z}_p \quad F'(\alpha_1) \not\equiv 0 \bmod p\mathbb{Z}_p.$$

Denotando por $F'(X)$ la derivada formal de $F(X)$, es decir $F'(X) = a_1 + 2a_2X + 3a_3X^2 + ... + na_nX^{n-1}$. Entonces existe un único entero p-ádico α tal que $\alpha \equiv \alpha_1 \bmod p\mathbb{Z}_p$ y $F(\alpha) = 0$.

Demostración. Sea $\{\alpha_n\}$ una sucesión de enteros p-ádicos que cumplan las siguientes propiedades:
1) $F(\alpha_n) \equiv 0 \bmod p^n\mathbb{Z}_p$.
2) $\alpha_n \equiv \alpha_{n+1} \bmod p^n\mathbb{Z}_p$.
La segunda propiedad es equivalente a decir que dicha sucesión es de Cauchy. Dado que $\mathbb{Z}_p$ es completo, podemos tomar el límite de la sucesión, denotémoslo α, es claro que $\alpha \equiv \alpha_1 \bmod p\mathbb{Z}_p$. Como los polinomios son funciones continuas afirmamos que $F(\alpha) = 0$. El límite de esta sucesión será la raíz buscada.
Veamos que efectivamente podemos construir una sucesión de enteros p-ádicos con esas propiedades. Por hipótesis tenemos $\alpha_1 \in \mathbb{Z}_p$, buscamos $\alpha_2 \in \mathbb{Z}_p$ con las propiedades anteriores. Por tanto $\alpha_2 \equiv \alpha_1 \bmod p$, luego existe $b_1 \in \mathbb{Z}_p$ tal que $\alpha_2 = \alpha_1 + b_1p$, evidentemente si conocemos

b_1 conocemos α_2. Ahora bien,

$$\begin{aligned} F(\alpha_2) = F(\alpha_1 + b_1 p) &= a_0 + a_1(\alpha_1 + b_1 p) + a_2(\alpha_1 + b_1 p)^2 + a_3(\alpha_1 + b_1 p)^3 + ... + a_n(\alpha_1 + b_1 p)^n \\ &= F(\alpha_1) + a_1(b_1 p) + 2a_2\alpha_1(b_1 p) + a_2(b_1 p)^2 + 3a_3\alpha_1^2(b_1 p) + 3a_3\alpha_1(b_1 p)^2 + \\ &+ a_3(b_1 p)^3 + ... + n\alpha_1^n(b_1 p) + a_n \sum_{k=2}^{n-k} \binom{n}{k} \alpha_1^{n-k}(b_1 p)^k \\ &\equiv F(\alpha_1) + F'(\alpha_1) b_1 p \bmod p^2 \end{aligned} \tag{3.1}$$

Queremos que se cumpla la propiedad 1) por lo que $F(\alpha_1) + F'(\alpha_1)b_1 p \equiv 0 \bmod p^2$. Como $F(\alpha_1) \equiv 0 \bmod p$ existe un entero p-ádico tal que $F(\alpha) = px$, y la expresión (3.1) pasaría a ser $px + F'(\alpha_1)b_1 p \equiv 0 \bmod p^2$ y esto implica $x + F'(\alpha_1)b_1 \equiv 0 \bmod p$. Además, como $F'(\alpha_1)$ no pertenece a $p\mathbb{Z}_p$ es una unidad de $\mathbb{Z}_p$, es decir, $(F'(\alpha))^{-1} \in \mathbb{Z}_p$ y $b_1 = -x(F'(\alpha))^{-1} \in \mathbb{Z}_p$. Con esto queda probada la existencia y la unicidad de b_1 y por consiguiente queda probada la existencia y unicidad de α_2. Con el mismo razonamiento, podemos calcular α_{n+1} a partir de α_n y así generamos toda la sucesión. Como tenemos unicidad en cada α_i, tenemos unicidad en la sucesión.

□

A continuación, veremos dos aplicaciones del Lema de Hensel. La primera nos va a determinar que raíces de la unidad están en $\mathbb{Q}_p$. En este caso el polinomio sobre el que vamos a aplicar el Lema de Hensel es $F(X) = X^m - 1$ siendo $m \in \mathbb{N}$, además, buscamos un entero p-ádico λ tal que $F(\lambda) \equiv 0 \bmod p\mathbb{Z}_p$ y $F'(\lambda) \not\equiv 0 \bmod p\mathbb{Z}_p$. Dado que $F'(\lambda) = m\lambda^{m-1} \not\equiv 0 \bmod p\mathbb{Z}_p$ sacamos dos condiciones:

1. m no puede ser múltiplo de p.
2. La aproximación λ a la raíz no está en $p\mathbb{Z}_p$.

Lema 9. *Dados un primo p y un entero m no divisible por p. Entonces, existe un entero α tal que $\alpha^m \equiv 1 \bmod p$ y $\alpha \not\equiv 1 \bmod p$ si y solo si $mcd(m, p-1) > 1$. Además, para cada α el menor entero positivo m con esta propiedad ha de ser un divisor de $p-1$.*

Demostración. Supongamos que $\alpha \not\equiv 1 \bmod p$ y m tales que $\alpha^m \equiv 1 \bmod p$. Entonces, el orden de α en $(\mathbb{Z}/p)^*$, $ord(\alpha)$, divide a m. Además, como $\alpha^{p-1} \equiv 1 \bmod p$, también $ord(\alpha)|p-1$. Por tanto $ord(\alpha)$, que es un entero mayor que uno, divide a m y $p-1$. Como consecuencia $mcd(m, p-1) > 1$. Recíprocamente, supongamos que $d = mcd(m, p-1) > 1$. Sea $g \in \mathbb{Z}$ un generador multiplicativo de $(\mathbb{Z}/p)^*$ y $\alpha = g^{(p-1)/d} \in \mathbb{Z}$. Es evidente que $\alpha^d \equiv 1 \bmod p$ y por tanto, $\alpha^m \equiv 1 \bmod p$.

La segunda afirmación del Lema es evidente, ya que al menos m es el orden de α que es un divisor de $p-1$.

□

Proposición 15. *Para cualquier primo p y cualquier entero positivo que no sea múltiplo de p, existe una raíz primitiva m-ésima de la unidad en $\mathbb{Q}_p$ si y solo si m divide a $p-1$.*

Demostración. Veamos en primer lugar la condición suficiente. Sea m un divisor de $p-1$ y $\alpha_1 \in \mathbb{Z}$, $0 < \alpha_1 < p-1$ tal que $\alpha_1^m \equiv 1 \bmod p$. Sea $F(X) = X^m - 1$, evidentemente $F(\alpha_1) \equiv 0 \bmod p$ y $F'(\alpha_1) \not\equiv 0 \bmod p$. Por el Lema de Hensel (Teorema 11) existe un $\alpha \in \mathbb{Z}_p$ único tal que $\alpha^m = 1$ y $\alpha \equiv \alpha_1 \bmod p$. Si, además, α_1 es primitiva, es decir $\alpha_1^d \not\equiv 1 \bmod p$ para $d < m$ forzosamente α es primitiva, pues $\alpha^d = 1$ implica que $\alpha^d \equiv \alpha_1^d \equiv 1 \bmod p$.

Veamos ahora la condición necesaria. Sea $\lambda \in \mathbb{Q}_p$ una raíz primitiva m-ésima de 1. Observamos que la condición $\lambda^m = 1$ implica que $|\lambda|_p = 1$ y por lo tanto, $\lambda \in \mathbb{Z}_p$. Escribimos

$\lambda = \sum_{i\geqslant 0} a_i p^i$, es claro que $a_0^m \equiv 1 \bmod p$. Si probamos que $a_0^d \not\equiv 1 \bmod p$ para cualquier d distinto de m, entonces $m = ord(a_0)$ en $(\mathbb{Z}/p)^*$ y $m|p-1$. Supongamos que $a_0^d \equiv 1 \bmod p$ pero $d|m$ y $G(X) = X^{m/d} - 1$. Tomemos $\alpha_1 = 1$. Evidentemente el levantamiento de Hensel de α_1 para $G(X)$ es $1 \in \mathbb{Z}_p$. Por otro lado, $\mu = \lambda^d \in \mathbb{Z}_p$ satisface que $G(\mu) = (\lambda^d)^{m/d} - 1 = 0$ y $\mu = \lambda^d \equiv a_0^d \equiv 1 \bmod p$. Por la unicidad del levantamiento $\mu = 1$ y $\lambda^d = 1$ en contra de que λ es primitiva.

□

La segunda aplicación del Lema de Hensel será el estudio de las congruencias cuadráticas en $\mathbb{Q}_p$, es decir, determinar la existencia de soluciones de $X^2 = a$ siendo $a \in \mathbb{Z}_p$. El polinomio que utilizaremos en este caso para aplicar el Lema de Hensel será $F(X) = X^2 - a$.

Proposición 16. *Dado p primo impar y $b \in \mathbb{Z}_p$. Si existe $\alpha \in \mathbb{Z}_p$ tal que $\alpha^2 \equiv b \bmod p\mathbb{Z}_p$, entonces b es el cuadrado de un elemento de $(\mathbb{Z}_p)^*$.*

Demostración. Si aplicamos el Lema de Hensel al el polinomio $F(X) = X^2 - b$ la demostración es directa. Veamos que se cumplen las hipótesis requeridas para utilizar dicho teorema.
1) Como ${\alpha_1}^2 = b \Rightarrow F(\alpha_1) = 0$.
2) Además, sabemos que $|b|_p = 1 \Rightarrow {|\alpha_1|_p}^2 = 1 \Rightarrow |\alpha_1|_p = 1 \Rightarrow \alpha_1 \in {\mathbb{Z}_p}^*$.
La derivada evaluada en α_1 queda $F(\alpha_1) = 2\alpha_1$ y como p no es nulo y $|\alpha_1|_p = 1$, $F(\alpha_1) \not\equiv 0 \bmod p\mathbb{Z}_p$.

□

A continuación, vamos a ver una segunda versión del Lema de Hensel que permite encontrar una factorización de un polinomio a partir de una factorización en $\mathbb{Z}_p$.

Definición 15. Dados $g(X)$, $h(X)$ polinomios de $\mathbb{Z}_p[X]$. Denotamos por $\bar{g}(X)$, $\bar{h}(X) \in \mathbb{F}_p[X]$ los polinomios obtenidos por la reducción de los coeficientes módulo p. Diremos que $\bar{g}(X)$ y $\bar{f}(X)$ son primos entre sí módulo p, si $mcd(\bar{g}, \bar{h}) = 1$ en $\mathbb{F}_p[X]$, es decir si existen polinomios $a(X), b(X) \in \mathbb{Z}_p[X]$ tal que

$$a(X)g(X) + b(X)h(X) \equiv 1 \bmod p.$$

(Las congruencias entre polinomios son coeficiente a coeficiente.)

Teorema 12 (Segunda versión del Lema de Hensel)**.** *Sea $f(X)$ un elemento de $\mathbb{Z}_p[X]$ y supongamos que existen polinomios $g_1(X)$, $h_1(X)$ de $\mathbb{Z}_p[X]$ tal que :*
i) $g_1(X)$ es mónico.
ii) $g_1(X)$ y $h_1(X)$ son primos entre sí módulo p.
iii) $f(X) \equiv g_1(X)h_1(X) \bmod p$.
Entonces existen polinomios $g(X)$, $h(X)$ pertenecientes a $\mathbb{Z}_p[X]$ que cumplen:
1) $g(X)$ es mónico.
2) $g(X) \equiv g_1(X) \bmod p$ y $h(X) \equiv h_1(X) \bmod p$.
3) $f(X) = g(X)h(X)$.

Demostración. Denotaremos por d el grado del polinomio $f(X)$ y m el grado del polinomio $g_1(X)$. Dado que $g_1(X)$ es mónico y quiero que $g(X)$ también lo sea y que $g(X) \equiv g_1(X) \bmod p$, deducimos que el grado de $g(X)$ ha de ser m. Además, es claro que la reducción de $f(X)$ módulo p debe tener grado menor o igual que d, así pues, como $f(X) \equiv g_1(X)h_1(X) \bmod p$ llegamos a que el grado de $h_1(X)$ es menor o igual que $d - m$.
Vamos a definir dos sucesiones de polinomios $g_n(X)$ y $h_n(X)$ que cumplan:
a) $g_n(X)$ es un polinomio mónico de grado m.
b) $g_{n+1}(X) \equiv g_n(X) \bmod p^n$ y $h_{n+1}(X) \equiv h_n(X) \bmod p^n$.

c) $f(X) \equiv g_n(X)h_n(X) \bmod p^n$.
Notemos que los grados de los polinomios h_n están acotados por $d-m$. Una vez definidas estas dos sucesiones de polinomios, definiremos $g(X)$ y $h(X)$ como los límites de $g_n(X)$ y $h_n(X)$, es decir, los coeficientes de $g(X)$ (resp. $h(X)$) serán los límites de los coeficientes de $g_n(X)$ (resp. $h_n(X)$). Solo nos faltaría demostrar que se pueden construir dichas sucesiones de polinomios.
Como $g_1(X)$ y $h_1(X)$ tienen que cumplir b) tenemos que existen $r_1(X)$ y $s_1(X)$ ambos polinomios con coeficientes en $\mathbb{Z}_p$ tal que

$$g_2(X) = g_1(X) + p \cdot r_1(X) \quad h_2(X) = h_1(X) + p \cdot s_1(X).$$

Para probar la existencia de $g_2(X)$ y $h_2(X)$ basta con probar la existencia de $r_1(X)$ y $s_1(X)$. Por otro lado, teniendo en cuenta que se debe verificar c) llegamos a que

$$\begin{aligned} f(X) &\equiv g_2(X)h_2(X) \bmod p^2 \\ &\equiv (g_1(X) + pr_1(X))(h_1(X) + ps_1(X)) \bmod p^2 \\ &\equiv g_1(X)h_1(X) + pr_1(X)h_1(X) + ps_1(X)g_1(X) \bmod p^2. \end{aligned} \tag{3.2}$$

Por otro lado, existe un polinomio con coeficientes en $\mathbb{Z}_p$ que denotaremos por $k_1(X)$ tal que $f(X) - g_1(X)h_1(X) = pk_1(X)$, pues por hipótesis $f(X) \equiv g_1(X)h_1(X) \bmod p$. Utilizando esta última expresión y (3.2) llegamos a que $k_1(X)p \equiv pr_1(X)h_1(X) + ps_1(X)g_1(X) \bmod p^2$ de la que deducimos

$$k_1(X) \equiv r_1(X)h_1(X) + s_1(X)g_1(X) \bmod p. \tag{3.3}$$

Las soluciones para $r_1(X)$ y $s_1(X)$ en esta congruencia serán los polinomios que estamos buscando para definir $g_2(X)$ y $h_2(X)$. Como sabemos que existen $a(X)$ y $b(X)$ de $\mathbb{Z}_p[X]$ tal que $a(X)g_1(X) + b(X)h_1(X) \equiv 1 \bmod p$. Definimos dos polinomios nuevos $\tilde{r}_1(X) = b(X)k_1(X)$ y $\tilde{s}_1(X) = a(X)k_1(X)$. Evidentemente estos dos polinomios son soluciones de la congruencia (4.3). Sin embargo, no conocemos ni el grado del polinomio $\tilde{r}_1(X)$ ni si $g_1(X) + p\tilde{r}_1(X)$ es un polinomio mónico.
Si dividimos $\tilde{r}_1(X)$ entre $g_1(X)$ y denotamos por $r_1(X)$ al resto obtenemos que $\tilde{r}_1(X) = g_1(X)q(X) + r_1(X)$. Está claro que el grado de $r_1(X)$ es menor que el de $g_1(X)$ y esto implica que el polinomio $g_1(X) + pr_1(X)$ es mónico. Definimos $s_1(X) = \tilde{s}_1(X) + h_1(X)q(X)$. Se prueba que estos dos polinomios que acabamos de definir $r_1(X)$ y $s_1(X)$ son soluciones de la congruencia (3.3).
Ya sabemos que a partir de $g_1(X)$ y $h_1(X)$ podemos construir $g_2(X)$ y $h_2(X)$. Además, por la forma en la que los hemos construido podemos asegurar que $g_2(X)$ y $h_2(X)$ son primos entre sí, luego podemos calcular con el mismo procedimiento $g_3(X)$ y $h_3(X)$ y así sucesivamente.
□

Como ya hemos visto, el objetivo de la primera versión del Lema de Hensel es encontrar las raíces de un polinomio, mientras que el objetivo de la segunda versión es encontrar una factorización del mismo. Estos dos problemas, a pesar de no ser iguales, están muy ligados el uno con el otro. Notemos que si en la segunda versión consideramos el polinomio $g_1(X) = X - \alpha$ con $\alpha \in \mathbb{Z}_p$ y $h_1(X)$ otro polinomio primo con $g_1(X)$, entonces dado que $g(X)$ ha de ser mónico y del mismo grado que $g_1(X)$, obtendríamos también una raíz del polinomio.

3.2. Las funciones logaritmo y exponencial

El objetivo principal en esta sección es el estudio de las series de potencias en el cuerpo de los números p-ádicos. Como bien sabemos, las series de potencias nos ofrecen una forma de representar funciones. En general, el análisis p-ádico se va a parecer al análisis real, aunque en algunas algunas ocasiones se vuelve mucho más simple de manejar. En primer lugar, vamos a estudiar unos resultados básicos de las series de $\mathbb{Q}_p$.

Proposición 17. *Una serie infinita* $\sum_{n=1}^{\infty} a_n$ *con* $a_n \in \mathbb{Q}_p$ *es convergente si y solo si* $\lim_{n\to\infty} a_n = 0$*, en este caso también tenemos*

$$\left|\sum_{n=1}^{\infty} a_n\right|_p \leq \max_n |a_n|_p$$

Demostración. En primer lugar veamos la doble implicación. Sabemos que una serie converge cuando lo hace la sucesión de sumas parciales, llamaremos S_n a la suma parcial n-ésima. Además, sabemos que $a_n = S_n - S_{n-1}$.
Si suponemos que $\lim_{n\to\infty} a_n = 0$, aplicando la Proposición 8 sabemos que la sucesión de sumas parciales es de Cauchy, luego es convergente y por tanto la serie es convergente.
Si suponemos que la serie es convergente, tenemos que la sucesión de sumas parciales también lo es y esto implica que es de Cauchy, por tanto $|a_n|_p$ tiene a 0 cuando n tiene a ∞ y tenemos lo pedido.
Por último, vamos a probar la desigualdad. Suponemos que $\sum a_n \neq 0$, pues en caso contrario la desigualdad sería evidente. Como el valor absoluto que estamos utilizando es no arquimediano, para todo entero N tenemos

$$\left|\sum_{n=1}^{N} a_n\right|_p \leq \max_{0\leq n\leq N} |a_n|_p.$$

Ahora bien, como $\lim_{n\to\infty} a_n = 0$ si consideramos un N lo suficientemente grande podemos asegurar que $\max_{0\leq n\leq N} |a_n|_p = \max_n |a_n|_p$. Como además, la sucesión formada por los valores absolutos de elementos de una sucesión de Cauchy de $\mathbb{Q}_p$ es estacionaria, $|\sum_{n=0}^{\infty} a_n|_p = |\sum_{n=0}^{N} a_n|_p$ y ya tendríamos la desigualdad.

□

Lema 10. *Dado* $b_{ij} \in \mathbb{Q}_p$ *siendo* $(i,j) \in \mathbb{N}^2$ *y suponiendo que*
1) Para todo i, $\lim_{j\to\infty} b_{ij} = 0$.
2) $\lim_{i\to\infty} b_{ij} = 0$ *uniformamente en* j.
Entonces, dado $\epsilon > 0$ *existe un entero* N*, que depende de* ε*, tal que, si* $\max(i,j) \geqslant N$ *entonces* $|b_{ij}|_p < \varepsilon$.

Demostración. Fijamos un $\varepsilon > 0$.
Por la hipótesis 2) sabemos que existe un entero N_0, que depende de ε pero no de j, tal que $|b_{ij}|_p < \varepsilon$ para todo $i \geqslant N_0$. Mientras, por 1) sabemos que para cada i existe un entero $N_1(i)$, que depende de i, tal que $|b_{ij}|_p < \epsilon$ para todo $j \geqslant N_1(i)$.
Sea $N = \max\{N_0, N_1(0), N_1(1), \cdots, N_1(N_0-1)\}$. Evidentemente N depende de ε.
Si $i \geqslant N_0$ independientemente de j vamos a tener que $|b_{i,j}|_p < \varepsilon$.
Si $i > N_0$ como estamos suponiendo que $\max\{i,j\} \geqslant N$, entonces $j \geqslant N$ y como i ha de ser un valor del conjunto $\{0, 1, \cdots, N_0 - 1\}$ tenemos que $j \geqslant N_1(i)$ y por lo tanto $|b_{ij}|_p < \varepsilon$.

□

Proposición 18. *Con las mismas hipótesis que en el Lema 10, ambas series:*

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) \quad y \quad \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$$

convergen y dan la misma suma.

Demostración. Por el lema anterior, sabemos que fijado un $\varepsilon > 0$ existe un entero N de tal manera que si $\max(i,j) \geqslant N$, entonces $|b_{ij}|_p < \varepsilon$.

Para cada i fijo, podemos asegurar que $b_{ij} \to 0$ cuando j tiende a ∞ y para cada j fijo, podemos asegurar que $b_{ij} \to 0$ cuando i tiende a ∞. En virtud del Proposición 17 sabemos que tanto $\sum_{j=0}^{\infty} b_{ij}$ para i fijo como $\sum_{i=0}^{\infty} b_{ij}$ para j fijo son series convergentes y cumplen la desigualdad del enunciado del Proposición 17.
Si fijamos un $i > N$,

$$\left|\sum_{j=0}^{\infty} b_{ij}\right|_p \leq \max_j |b_{ij}|_p < \varepsilon \Rightarrow \lim_{i\to\infty} \sum_{j=0}^{\infty} b_{ij} = 0$$

Si fijamos un $j > N$,

$$\left|\sum_{i=0}^{\infty} b_{ij}\right|_p \leq \max_i |b_{ij}|_p < \varepsilon \Rightarrow \lim_{j\to\infty} \sum_{i=0}^{\infty} b_{ij} = 0$$

Utilizando una vez más el corolario obtenemos que

$$\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) \quad \text{y} \quad \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)$$

son ambas convergentes.

Nos falta comprobar que dan la misma suma. Seguimos considerando el ε y el entero N del principio de la demostración. Evidentemente, si probamos que

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right|_p < \varepsilon \tag{3.4}$$

tendríamos terminada la demostración.

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right|_p =$$

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right) + \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right) - \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right|_p \leq$$

$$\max\left\{\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right)\right|_p + \left|\sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right) - \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right|_p\right\} \tag{3.5}$$

Estudiamos los dos términos que hay dentro del máximo. En primer lugar

$$\left|\sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right) - \sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right)\right|_p = \left|\sum_{i=0}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right) + \sum_{i=N+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right|_p$$

Para $j \geqslant N+1$ sabemos que $|b_{ij}|_p < \varepsilon$ para cada i, luego por el corolario ya citado $|\sum_{j=N+1}^{\infty} b_{ij}|_p \leq \max_i |b_{ij}|_p < \varepsilon$. Como estamos trabajando con una norma no arquimediana,

$$\left|\sum_{i=0}^{N}\left(\sum_{j=N+1}^{\infty} b_{ij}\right)\right|_p < \varepsilon$$

De manera similar, teniendo en cuenta que si $i \geqslant N+1$ para todo j y la desigualdad de la proposición

$$\left|\sum_{i=N+1}^{\infty}\left(\sum_{j=0}^{\infty} b_{ij}\right)\right|_p < \varepsilon$$

Ya tenemos asegurado que el primer término de (3.5) es menor que ε. Para demostrar que el segundo también es menor que ε basta con saber que $\sum_{i=0}^{N}\left(\sum_{j=0}^{N} b_{ij}\right) = \sum_{j=0}^{N}\left(\sum_{i=0}^{N} b_{ij}\right)$, la segunda expresión queda:

$$\left|\sum_{j=0}^{N}\left(\sum_{i=0}^{N} b_{ij}\right) - \sum_{j=0}^{\infty}\left(\sum_{i=0}^{\infty} b_{ij}\right)\right|_p$$

Intercambiando la i por la j en el razonamiento anterior llegamos a que esa cantidad también es menor que ε y ya tendría probado (3.4).

□

Pasamos ahora al estudio de las series de potencias. En la mayoría de resultados que vamos a ver vamos a trabajar con series de potencias en X, pero estos siguen siendo ciertos para series de potencias en $(X-a)$.
Sean $a_n \in \mathbb{Q}_p$, $n \geqslant 0$ consideramos la serie formal

$$f(X) = \sum_{n=0}^{\infty} a_n X^n.$$

Si consideramos un número p-ádico $x \in \mathbb{Q}_p$, entonces la serie numérica $\sum_{n=0}^{\infty} a_n x^n$ converge si y solo si $|a_n x^n|_p \to 0$ cuando $n \to \infty$ (en virtud del Proposición 17).
En la siguiente proposición vamos a estudiar los casos en los que una serie de potencias es convergente.

Definición 16. Dada una serie formal en $\mathbb{Q}_p$, $f(X) = \sum_{n=0}^{\infty} a_n X^n$ definimos

$$\rho = \frac{1}{\limsup \sqrt[n]{|a_n|_p}}$$

y lo llamaremos radio de convergencia. Es claro que $0 \leq \rho \leq \infty$.

Proposición 19. *Sea $f(X) = \sum_{n=0}^{\infty} a_n X^n$ y sea ρ su radio de convergencia, entonces:*
i) Si $\rho = 0$, entonces $f(x)$ converge solo cuando $x = 0$.
ii) Si $\rho = \infty$, entonces f(x) converge para todo $x \in \mathbb{Q}_p$.
iii) Si $0 < \rho < \infty$ y $\lim_{n\to\infty} |a_n|_p \rho^n = 0$, entonces $f(x)$ converge si y solo si $|x|_p \leq \rho$.
iv) Si $0 < \rho < \infty$ y $\{|a_n|_p \rho^n\}$ no tiende a 0 cuando $n \to \infty$, entonces $f(x)$ converge si y solo si $|x|_p < \rho$.

Demostración. Sabemos que la región de convergencia de la serie de potencias $f(X)$ es

$$\left\{x \in \mathbb{Q}_p \,:\, \lim_{n\to\infty} |a_n x^n|_p = 0\right\}.$$

i) Cuando tomamos $x = 0$, evidentemente $f(x)$ converge.
ii) Si $\rho = \infty$ implica que la serie de números reales $\sum |a_n|_p |x|_p^{\,n}$ es convergente, por lo tanto $\lim_{n\to\infty} |a_n|_p |x|_p^{\,n} = 0$ y, por la Proposición 17, $\sum a_n x^n$ es convergente.
Veamos que si $0 < \rho < \infty$ la serie $\sum a_n x^n$ converge si $|x|_p < \rho$ y diverge si $|x|_p > \rho$.
Si $|x|_p < \rho$, entonces la serie de números reales es $\sum |a_n|_p |x|_p^{\,n}$ converge y por tanto la serie de $\mathbb{Q}_p$ también. Sin embargo, si consideramos ahora $|x|_p > \rho$ afirmamos que a partir de un cierto n lo suficientemente grande los valores $|a_n|_p$ se aproximan a $(\frac{1}{\rho})^n$. Por lo tanto $(\frac{|x|_p}{\rho})^n$ se aleja del 0 a medida que aumenta n, por tanto por el Proposición 17 la serie $\sum a_n x^n$ no es convergente.
Nos falta probar tanto en *iii*) como en *iv*) el carácter de la serie cuando $|x|_p = \rho$.
iii) Tenemos que $|a_n x^n|_p = |a_n|_p \rho^n$ y entonces la serie converge pues por hipótesis tenemos que

$|a_n|\rho^n$ tiende a 0 cuando n tiene a ∞.
iv) Si suponemos que $|x|_p = \rho$, entonces $|a_n x^n|_p = |a_n|_p \rho^n$ y como sabemos que no tiene a 0 entonces la serie no converge.

□

Si el radio de convergencia de la serie $f(X)$ es $\rho > 0$ se suele decir que f es una serie de potencias.
Dadas dos series de potencias en $\mathbb{Q}_p$, $f(X) = \sum_{n=0}^{\infty} a_n X^n$ y $g(X) = \sum_{n=0}^{\infty} b_n X^n$ definimos su suma y producto de la manera habitual. Estas dos operaciones respetan la convergencia de la serie, es decir si $f(X)$ y $g(X)$ son convergentes en $x \in \mathbb{Q}_p$,

1. $(f+g)(x) = f(x) + g(x)$ y es convergente.

2. $(fg)(x) = f(x)g(x)$ y es convergente.

Si consideramos $f(X) = \sum_{n=0}^{\infty} a_n X^n$ y $g(X) = \sum_{n=1}^{\infty} b_n X^n$, definimos la composición $(f \circ g)$ igual que en Capítulo 1 Sección 1.2. Vamos a analizar la convergencia de $h(X) = (f \circ g)(X) = f(g(X))$, no es trivial pues la evaluación de $h(X)$ en $x \in \mathbb{Q}_p$ concreto puede dar un resultado diferente a evaluar primero $g(X)$ en x y luego $f(X)$ en $g(x)$.

Teorema 13. *Dados $f(X) = \sum_{n=0}^{\infty} a_n X^n$ y $g(X) = \sum_{n=1}^{\infty} b_n X^n$, definimos $h(X) = f(g(X))$ como la compopsición. Sea $x \in \mathbb{Q}_p$ y suponemos:*
1) $g(x)$ converge.
2) $f(g(x))$ converge.
3) Para cada n, tenemos $|b_n x^n|_p < |g(x)|_p$.
Entonces $h(x)$ converge y $f(g(x)) = h(x)$.

Demostración. Ya hemos visto como se define cada coeficiente de $h(X)$. Dado que $g(x)$ es convergente, $g(x)^m$ también lo es. Por otro lado, $|d_{m,n}x^n|_p = 0$ cuando $n < m$, sin embargo si $n \geqslant m$ tenemos que $|d_{m,n}x^n|_p = \text{máx}\{|b_{i_1}x^{i_1}|_p, |b_{i_2}x^{i_2}|_p, ..., |b_{i_m}x^{i_m}|_p\}$ siendo $i_1 + ... + i_m = n$. Ahora bien, por hipótesis $|b_n x^n|_p < |g(x)|_p$ para todo n y entonces $|d_{m,n}x^n|_p \leq |g(x)^m|_p$. También sabemos que $f(g(x))$ converge, luego aplicando la Proposición 17 y teniendo en cuenta que $f(g(x)) = a_0 + \sum_{m \geqslant 1} a_m g(x)^m$ afirmamos que $a_m g(x)^m \to 0$ si $m \to 0$.
Por un lado tenemos que

$$f(g(x)) = a_0 + \sum_{m=1}^{\infty} \sum_{n=m}^{\infty} a_m d_{m,n} x^n,$$

mientras que

$$h(x) = a_0 + \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} a_m d_{n,m} x^n.$$

Ahora bien, por lo visto en el principio de la prueba $|a_m d_{m,n} x^n|_p \leq |a_m g(x)^m|_p$ y como $|a_m g(x)^m|_p$ no depende de n y también habíamos visto que convergía a 0, entonces se tiene que $\lim_{m\to\infty} a_m d_{m,n} x^n = 0$ uniformemente en n. Por último, para cada m fijo tenemos $\lim_{n\to\infty} a_n d_{m,n} x^n = 0$ por ser $g(x)^m$ convergente. Está claro que se verifícan todas las hipótesis de la Proposición 18 y por lo tanto $h(x)$ es convergente y $h(x)$ y $f(g(x))$ dan la misma suma.

□

Nuestro objetivo es poder definir en $\mathbb{Q}_p$ la función exponencial y la función logaritmo a partir del estudio de sus series de potencias.

Como bien conocemos, la serie de potencias del logaritmo en el caso real es

$$\mathbf{f}(X) = \mathbf{log}(1+X) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n}. \tag{3.6}$$

Evidentemente, como los coeficientes son funciones racionales podemos ver $\mathbf{f}(X)$ como una serie de potencias en $\mathbb{Q}_p$. Nos preguntamos por su radio de convergencia.

Lema 11. *La serie $\boldsymbol{f}(X)$ converge solo cuando $|x|_p < 1$.*

Demostración. Los coeficientes de $\mathbf{f}(X)$ son $1/n$, por tanto $|1/n|_p = p^{v_p(n)}$, luego $\sqrt[n]{|a_n|_p} = p^{v_p(n)/n}$. Ahora bien , como $v_p(n)$ es el menor m tal que $p^m|n$ es claro que $v_p(n) \leq \frac{log(n)}{log(p)}$, por lo tanto $\frac{v_p(n)}{n} \leq \frac{log(n)}{nlog(p)} \to 0$ cuando $n \to \infty$ y de esta manera tenemos que

$$\rho = \frac{1}{\lim\limits_{n\to\infty}(p^{v_p(n)/n})} \to 1 \quad \text{cuando} \quad n \to \infty.$$

En virtud de la Proposición 19, la serie de potencias $\mathbf{f}(X)$ converge cuando $|x|_p < \rho = 1$. Veamos que sucede cuando $|x|_p = 1$. Como $|\frac{1}{n}|_p\rho^n = |\frac{1}{n}|_p 1^n = p^{v_p(n)}$ no tiende a 0 cuando n tiende a ∞, luego por el apartado $iv)$ de la proposición ya citada se concluye que la serie no converge en este caso.

□

Por lo tanto, $\mathbf{f}(X)$ define una función en los números p-ádicos para los que la serie converge, es decir $\mathbf{f}(X)$ define una función en la bola abierta $B(0,1)$. Recordemos que $\mathbf{f}(X) = \mathbf{log}(1+X)$.

Definición 17. Sea $B = B(1,1) = \{x \in \mathbb{Z}_p : |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$ definimos el logaritmo p-ádico en $x \in B$ como

$$log_p(x) = \mathbf{log}(1+(x-1)) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{(x-1)^n}{n}.$$

Consideramos ahora la serie de potencias de la función exponencial

$$\mathbf{exp}(X) = \sum_{n=0}^{\infty}\frac{X^n}{n!}.$$

Al igual que en el caso del logaritmo podemos ver $\mathbf{exp}(X)$ como una serie de potencias en $\mathbb{Q}_p$.

Lema 12. *La serie de potencias $\boldsymbol{exp}(X)$ converge si y solo si $|x|_p < p^{-1/(p-1)}$.*

Demostración. Como los coeficientes de la serie de potencias son $1/n!$ y $|1/n!|_p = p^{v_p(n!)}$ aplicando el Lema 5, $|1/n!|_p < p^{n/(p-1)}$ luego $\sqrt[n]{|1/n!|_p} \leq p^{1/(p-1)}$. Por lo tanto tenemos una cota inferior para el radio de convergente, $\rho \geqslant p^{-1/(p-1)}$. Aplicando la Proposición 19 llegamos a que si $|x|_p < p^{-1/(p-1)}$ entonces $\mathbf{exp}(X)$ converge.
Supongamos que $|x|_p = p^{-1/(p-1)}$ y $n = p^m$, de nuevo por el Lema 5 sabemos que $v_p(n!) = \frac{p^m-1}{p-1}$. Entonces tenemos que

$$v_p\left(\frac{x^n}{n!}\right) = v_p\left(\frac{x^{p^m}}{p^m!}\right) = \frac{p^m}{p-1} - \frac{p^m-1}{p-1} = \frac{1}{p-1}$$

Entonces, $\frac{x^n}{n!}$ es imposible que tienda a 0 luego llegamos a que la serie de potencias $\mathbf{exp}(X)$ no converge para valores cuyo valor absoluto p-ádico sea $p^{-1/(p-1)}$.

□

Nota. Démonos cuenta que si $p \neq 2$, entonces $|x|_p < p^{-1/(p-1)}$ si y solo si $|x|_p \leq p^{-1}$ y esto equivale a decir que $x \in p\mathbb{Z}_p$ o lo que es lo mismo $|x|_p < 1$. En el caso en el que $p = 2$ tenemos que el radio de convergencia es $\rho = p^{-1/(p-1)} = 2^{-1}$, por tanto $|x|_2 < 2^{-1}$ equivale a decir que $v_p(x) \geqslant 2$ o también $|x|_2 \leq 2^{-2}$. Llegamos a las dos siguientes conclusiones:

1. Si $p \neq 2$, entonces $\mathbf{exp}(x)$ converge cuando $x \in p\mathbb{Z}_p$.
2. Si $p = 2$, entonces $\mathbf{exp}(x)$ converge cuando $x \in 4\mathbb{Z}_2$.

Definición 18. Dado $D = B(0, p^{-1/(p-1)}) = \{x \in \mathbb{Z}_p : |x|_p < p^{-1/(p-1)}\}$ definimos la función exponencial p-ádica que va de D en $\mathbb{Q}_p$ como

$$exp_p(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Es posible probar que las dos funciones p-ádicas que acabamos de definir satisfacen las siguientes propiedades:

1. $log_p(x \cdot y) = log_p(x) + log_p(y)$ siendo $x, y \in 1 + p\mathbb{Z}_p$.
2. $exp_p(x + y) = exp_p(x) \cdot exp_p(y)$ siendo $x, y \in D$.

Por último veamos que, al igual que en $\mathbb{R}$, la función p-ádica exponencial y la función p-ádica logaritmo son inversas la una de la otra.

Proposición 20. *Sea $x \in \mathbb{Z}_p$ con $|x|_p < p^{-1/(p-1)}$. Entonces tenemos que $|exp_p(x) - 1|_p < 1$ por lo que $exp_p(x)$ esta en el dominio de definición de log_p y*

$$log_p(exp_p(x)) = x.$$

Recíprocamente, si $|x|_p < p^{-1/(p-1)}$ tenemos que $|log_p(1+x)|_p < p^{-1/(p-1)}$, luego $log_p(1+x)$ esta en el dominio de definición de exp_p y

$$exp_p(log_p(1 + x)) = 1 + x.$$

Demostración. Suponemos que $x \neq 0$ pues en caso contrario el enunciado es claramente cierto. Tenemos que estudiar $|exp_p(x) - 1|_p = |\sum_{n=1}^{\infty} \frac{x^n}{n!}|_p$. Por otro lado, suponiendo que $n \geqslant 2$ y teniendo en cuenta la nota anterior

$$v_p\left(\frac{x^{n-1}}{n!}\right) = (n-1)v_p(x) - v_p(n!) > \frac{n-1}{p-1} - \frac{n-s}{p-1} = \frac{s-1}{p-1}$$

Evidentemente la última expresión es una cantidad positiva y por tanto hemos llegado a que

$$\left|\frac{x^{n-1}}{n!}\right|_p < 1 \quad \text{luego} \quad \left|\frac{x^n}{n!}\right|_p < |x|_p, \quad \text{para } n \geqslant 2$$

Por lo tanto, como $|exp_p(x) - 1|_p = |x + \sum_{n=2}^{\infty} \frac{x^n}{n!}|_p$ luego $|exp_p(x) - 1|_p = |x|_p$. Por un lado tenemos que $|x|_p < 1$ luego $|exp_p(x) - 1|_p < 1$ y entonces $exp_p(x)$ pertenece al dominio de definición de log_p. Por otro lado tenemos que $|exp_p(x) - 1|_p = |x|_p > |\frac{x^n}{n!}|_p$, entonces se satisfacen las hipótesis del Teorema 13 y afirmamos que $log_p(exp_p(x)) = x$.
Vamos ahora con la otra parte de la demostración. Es claro que como estamos suponiendo $|x|_p < p^{-1}/(p-1)$ tenemos que $v_p(x) > \frac{1}{p-1}$. Si suponemos $n \geqslant 2$

$$v_p\left(\frac{(-1)^{n+1}x^n}{n}\right) - v_p(x) = (n-1)v_p(x) - v_p(n) > (n-1)\left(\frac{1}{p-1} - \frac{v_p(n)}{n-1}\right)$$

Veamos que el signo del último término es positivo. Llamamos $v_p(n) = v$, entonces $n = p^v n'$ siendo n' un entero no divisible por p. Denotamos por $k(p)$ al cociente de dividir $p^v - 1$ entre $p - 1$.

$$\frac{v_p(n)}{n-1} = \frac{v}{p^v n' - 1} \leq \frac{v}{p^v - 1} = \frac{1}{p-1} \cdot \frac{v}{k(p)} \leq \frac{1}{p-1}$$

Por lo tanto,

$$v_p\left(\frac{(-1)^{n+1}x^n}{n}\right) > v_p(x) \quad \text{implica} \quad \left|\frac{(-1)^{n+1}x^n}{n}\right|_p < |x|_p$$

Como $log_p(1+x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}x^n}{n}$, $|log_p(1+x)|_p = |x + \sum_{n=2}^{\infty} \frac{(-1)^{n+1}x^n}{n}|_p$ entonces $|log_p(1+x)|_p = |x|_p$ y por hipótesis $|x|_p < p^{-1}/(p-1)$ tenemos que $log_p(1+x)$ está en el dominio de definición de exp_p. Además se verifican las hipótesis del teorema 13, por tanto $exp_p(log_p(1+x)) = 1 + x$

□

Nota. Fijamos $p = 2$ y tomamos $x = -2$. Observamos que $v_p(-2) = 1$, por tanto $|x|_2 = \frac{1}{p} = \frac{1}{2} < 1$. Puesto que el radio de convergencia de $\mathbf{log}(1+X)$ es 1, $\mathbf{log}(1+x)$ converge p-ádicamente pues $x = -2$ y por tanto $\mathbf{log}(1-2) = \mathbf{log}(-1) \in \mathbb{Z}_p$ está bien definido. De hecho se tiene que $\mathbf{log}(-1) = 0$: en efecto $2\mathbf{log}(-1) = \mathbf{log}((-1)^2) = \mathbf{log}(1) = 0$, ya que la igualdad $\mathbf{log}(1) = \mathbf{log}(1 \cdot 1) = \mathbf{log}(1) + \mathbf{log}(1) = 2\mathbf{log}(1)$ implica $\mathbf{log}(1) = 0$. Nótese que $\mathbf{log}(-1) = -(2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots)$ y la condición $\mathbf{log}(-1) = 0$ equivale a decir que para cada entero $N > 0$ existe n_0 de manera que, si $n \geqslant n_0$, $2 + \frac{2^2}{2} + \frac{2^3}{3} + \cdots + \frac{2^n}{n}$ es divisible por 2^N. Este hecho se puede también probar directamente, aunque lleva algún trabajo.
Siguiendo en el ejemplo, como $\mathbf{log}(1-2) = \mathbf{log}(-1) = 0$ observamos que $|\mathbf{log}(1-2)|_2 < p^{-1/(p-1)}$, por lo tanto podemos ahora componer con la función exponencial, es decir, $\mathbf{exp}(\mathbf{log}(1+x))$ está definido para $x = -2$. Como sabemos $\mathbf{exp}(0) = 1$ y como consecuencia tenemos que $\mathbf{exp}(\mathbf{log}(1+x)) \neq 1 + x$ ya que $1 + (-2) = -1$.

Este ejemplo es importante ya que pone de manifiesto que, aunque $y = \mathbf{log}(1+x)$ está definido y también lo está $\mathbf{exp}(y) = \mathbf{exp}(\mathbf{log}(1+x))$ no tenemos garantizado que $\mathbf{exp}(\mathbf{log}(1+x)) = 1 + x$. Así pues pone de manifiesto la necesidad de tomar $|x|_p < p^{-1/(p-1)}$ en el enunciado y, de paso, la razón de la condición 3 del Teorema 13.

3.3. Grupo de unidades de $\mathbb{Z}_p$

Como ya sabemos el grupo de las unidades de $\mathbb{Z}_p$ es:

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \,|\, v_p(x) = 0\} = \{x \in \mathbb{Z}_p \,|\, |x|_p = 1\}.$$

Recordemos que, puesto que $\mathbb{Z}_{(p)}$ es un subanillo de $\mathbb{Z}_p$, también $\mathbb{Z}_{(p)}^* \subset \mathbb{Z}_p^*$ y $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p^n\mathbb{Z}$ para $n \geqslant 1$.

Sea $x \in \mathbb{Z}_{(p)}^*$, la sucesión $\underline{T}(x) = \{x^{p^n}\}$ es una sucesión de Cauchy en $\mathbb{Z}_p$. Por lo tanto define un elemento de $\mathbb{Z}_p^*$ al que llamaremos $T(x)$. De la misma forma que en la Proposición 3 se tiene que si $x \equiv y \bmod p$, entonces las sucesiones $\underline{T}(x)$ y $\underline{T}(y)$ son equivalentes, es decir, definen el mismo número p-ádico, por tanto $T(x) = T(y)$. Como consecuencia, T define una aplicación

$$\begin{array}{rccc} T\colon (\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)})^* \simeq & \mathbb{F}_p^* & \longrightarrow & \mathbb{Z}_p^* \\ & x & \longmapsto & T(x) \end{array}$$

que es evidentemente un homomorfismo inyectivo de $(\mathbb{F}_p^*, \cdot)$ en $(\mathbb{Z}_p^*, \cdot)$ ya que $T(xy) = T(x)T(y)$ y $T(x) \equiv x \bmod p$. Observemos que $T(\mathbb{F}_p^*) \subset \mathbb{Z}_p^*$ es el subgrupo de raíces $(p-1)$-ésimas de la unidad.

Consideremos ahora el subgrupo aditivo de $\mathbb{Z}_p$ de los múltipos de p, es decir, $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \,|\, |x|_p < 1\}$ y también el grupo multiplicativo $(1 + p\mathbb{Z}_p, \cdot) \subset (\mathbb{Z}_p^*, \cdot)$. Las propiedades de las funciones $log(-)$ y $exp(-)$ (ver Proposición 20) ya conocidas verifican que

$$exp(-) : (p\mathbb{Z}_p, +) \to (1 + p\mathbb{Z}_p, \cdot)$$

$$log(-) : (1 + p\mathbb{Z}_p, \cdot) \to (p\mathbb{Z}_p, +)$$

son isomorfismos de grupos, inversos uno del otro. Como ya ocurría en $(\mathbb{Z}/p^n\mathbb{Z})^*$ tenemos entonces:

Teorema 14. *Sea p un primo impar. Entonces se tiene el isomorfismo de grupos*

$$\varphi : (\mathbb{F}_p^*, \cdot) \times (p\mathbb{Z}_p, +) \xrightarrow{\sim} (\mathbb{Z}_p^*, \cdot).$$

Además, si $x \in \mathbb{F}_p^*$, $y \in \mathbb{Z}_p$ el isomorfismo φ está definido por $\varphi(x, py) = T(x)exp(py)$.

El caso $p = 2$ es un poco diferente, básicamente debido a que en este caso

$$\mathcal{U} = \{x \in \mathbb{Z}_p^* \,|\, |x|_p < p^{-1/(p-1)}\} = 1 + 4\mathbb{Z}_p.$$

De forma similar al caso $p \neq 2$, ahora $\mathcal{U} = 1 + 4\mathbb{Z}_p$ es un subgrupo de $(\mathbb{Z}_p^*, \cdot)$ isomorfo (vía las funciones $exp(-)$ y $log(-)$) el subgrupo aditivo $(4\mathbb{Z}_p, +)$.

Por otro lado, en este caso, las raíces de la unidad de $\mathbb{Q}_2$ forman un subgrupo X de $\mathbb{Z}_p^*$ que es de hecho isomorfo a $(\mathbb{Z}/4\mathbb{Z})^* \simeq (\mathbb{Z}/2, +)$, por tanto cíclico de orden 2. En este caso se tiene:

Teorema 15. $\mathbb{Z}_2^* \simeq X \times (1 + 4\mathbb{Z}_2) \simeq (\mathbb{Z}/2, +) \times (4\mathbb{Z}_2, +)$.

Bibliografía

[1] M. F. Atiyah, I. G. Macdonald, *Introducción al Álgebra Conmutativa*. Reverté. 1973.

[2] J. A. Fernández Viña, *Lecciones de Análisis Matemático I*. tecnos. 1981.

[3] Joachim von zur Gathen, Jürgen Gerhard *Modern Computer Algebra*. Cambridge. 2013.

[4] Fernando Q. Gouvêa, *p-adic Numbers; An Introduction*. Springer. Second Edition 1997.

[5] Richard Michael Hill, *Introduction to Number Theory*. World Scientific. 2018.

[6] Svetlana Katok, *p-adic Analysis Compared with Real*. American Mathematical Society. 2007.

[7] Alain M. Robert, *A Course in p-adic Analysis*. Springer. 2000.