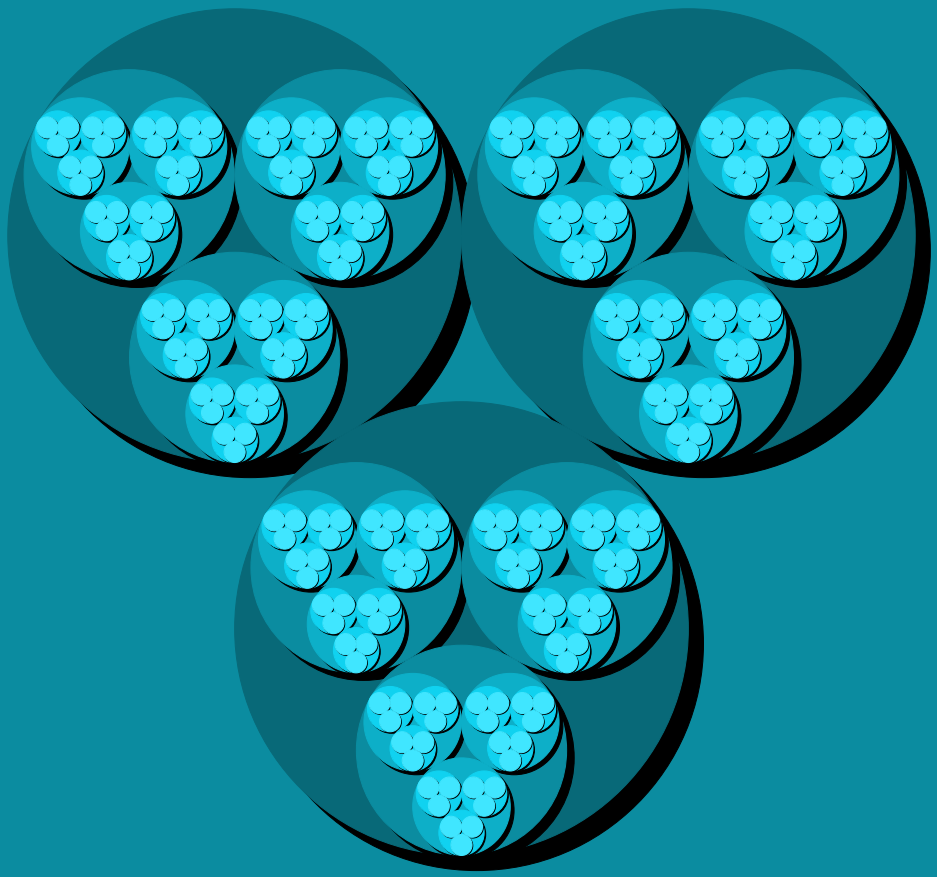
Universidad Nacional del Litoral
Facultad de Ingeniería Química

Donde la distancia acerca

Una introducción a los números p-ádicos



Mercedes Berger

Concurso de Monografías UMA - 2025

Prefacio

No recuerdo cuándo fue exactamente la primera vez que escuché hablar de los números primos, pero recuerdo haberlos visto en múltiplos problemas en las Olimpíadas de Matemática en la escuela, y, por supuesto, en grandes resultados de la teoría de números en las materias del ciclo básico de mi carrera de Matemática Aplicada. Y nada había sido tan revelador para mí hasta ahora, como descubrir que, después de años de haber estudiado a los números primos, y de no prestarles demasiada atención, terminarían siendo centrales en un tema que lograría cautivarme por completo: los números p-ádicos.

La primera vez que escuché hablar de los números p-ádicos sí que la recuerdo, fue en un video divulgativo que ví: *"Los Matemáticos NO Usan los Números Igual que Nosotros"* [4] del canal *Veritasium en español*. Al terminar de verlo, mi primer pensamiento sobre el título fue darles totalmente la razón. Aquello encendió un chispa en mí. Esta, me hizo seguir buscando sobre los llamados números p-ádicos de los qué habló. Descubrí que aquello era tan solo la punta del iceberg y que no tenía idea de lo que me esperaba. Pronto comprendí que estos, por más particulares que parezcan, son en realidad una puerta de entrada a una amplia variedad de áreas matemáticas.

La compresión de los números p-ádicos exige herramientas fundamentales provenientes de diversas ramas de la matemática como el álgebra, la topología, el análisis, la teoría de números, e incluso de la geometría algebraica. Y, el no encontrar trabajos introductorios al tema, que "bajen a tierra"los complejos conceptos que presenta, me dió la iniciativa para hacerlo.

Así, el objetivo central de este trabajo es ofrecer al lector un primer acercamiento sencillo a estos números y explorar algunas de sus aplicaciones, sin la necesidad de tener el conocimiento que un libro sobre análisis p-ádico requeriría.

Escribir esta monografía fue algo muy gratificante. Fue una experiencia única que me mantuvo tardes enteras escribiendo, borrando, reescribiendo y reborrando todo lo que a continuación están por leer.

La portada de esta monografía toma inspiración de representaciones visuales de los números p-ádicos, especialmente de las ilustraciones del matemático Heiko Knospe en su blog [10] y de la famosa ilustración del matemático y artista Anatoly Timofeevich Fomenko del disco unidad 3-ádico, que aparece en Koblitz, N. (1984) [11]. Fueron memorables las largas madrugadas en el verano que pasé aprendiendo a usar el paquete de TikZ para crear la portada, que hasta día de hoy observo como a un trofeo.

Agradezco sinceramente a mis compañeros y amigos que me ayudaron a decidir el diseño de la portada, entre varias versiones que fui creando a lo largo del proceso. También agradezco a Eros y a Tomás, quienes me ofrecieron sus valiosas correcciones para algunas partes de esta monografía.

Estructura de la monografía

Las secciones 1 y 5 considero que son las más contextuales. En la primera presento una introducción histórica y en la segunda explico, dando un poco de contexto actual de la criptografía, algunas de las aplicaciones que los números p-ádicos tienen relacionadas a la seguridad digital.

Con el objetivo de hacer accesible el entendimiento de los números p-ádicos a la mayor cantidad posible de personas, tomé la decisión de que la sección 2 de preliminares y la sección 3 estén orientadas a todo público. Después de un par de definiciones básicas y fundamentales, presento una aproximación intuitiva y motivadora al concepto. Expongo explicaciones accesibles, las cuales servirán para comprender las ideas principales, sin contar, quizás, con el suficiente rigor matemático.

En la sección 4 construiré formalmente las definiciones más avanzadas, para introducir mejor el tema, y dejar una buena base para el estudio profundo del mismo.

Notación de la monografía

Con el objetivo de ser fiel a la notación matemática de los textos académicos que he leído sobre el tema, he de aclarar algunas cuestiones de lenguaje y notación que utilizo de forma reiterativa en la monografía.

Menciono los números n-ádicos, donde n es cualquier número natural, siempre que no se indique lo contrario. Algunos autores también los llaman "números b-ádicos" o "números s-ádicos", indistintamente, según qué letra del abecedario prefiera cada uno. En mi caso, la letra n. Cuando n, en particular, sea primo hablaremos entonces de los números p-ádicos.

Para diferenciar a un número n-ádico de otros tipos de números, uso una fuente distinta para cada uno. Así, a es un número real y $\mathfrak{a}$ es un número n-ádico.

Comúnmente, no se trabaja con los números n-ádicos para cualquier valor natural de n. De hecho, es muy probable que el lector no encuentre fácilmente textos académicos sobre ellos. Esto se debe a que, como veremos, estos números carecen de ciertas propiedades fundamentales que sí poseen los números p-ádicos. Sin embargo, he decidido hacer una sección que abarca estos inconvenientes, que resultará útil principalmente como una introducción al tema. Su definición informal permite visualizarlos y comprenderlos con mayor facilidad.

Índice

Introducción

Los números p-ádicos pueden resultar, a primera vista, profundamente contraintuitivos. Mientras que en los números reales estamos acostumbrados a que los decimales se extiendan hacia la derecha, en el mundo p-ádico sucede lo opuesto: las cifras más relevantes están hacia la izquierda, y la "precisión" aumenta al agregar potencias de p cada vez mayores. Lejos de ser una mera curiosidad teórica, esta forma alternativa de ver los números ha demostrado ser una herramienta fundamental en diversas ramas de la matemática moderna, desde el análisis y el álgebra hasta la teoría de números. Esta inversión de perspectiva abre la puerta a una manera completamente nueva de entender la noción de proximidad y convergencia.

La motivación para estudiar los números p-ádicos no surge solamente del deseo de entender una nueva forma de contar o de sumar, sino de la necesidad de completar a los racionales bajo otros puntos de vista. Así como los números reales completan a los racionales usando el valor absoluto usual, los números p-ádicos surgen de una completación distinta, regida por la divisibilidad por un número primo p. Lo notable es que, a pesar de su extraña apariencia, forman estructuras perfectamente coherentes y útiles que permiten resolver problemas que, en el mundo real, serían imposibles de abordar. Problemas como los que planteaba el *Último Teorema de Fermat*, demostrado por Andrew Wiles en 1995, quién utilizó los números p-ádicos para ello.

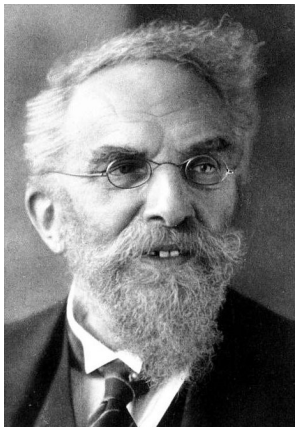
En los últimos años, su importancia se ha extendido incluso a campos como la criptografía. Su forma de codificar información y su comportamiento altamente estructurado en ciertos contextos algebraicos han captado el interés de quienes trabajan en sistemas de seguridad digital.

Esta monografía tiene como objetivo introducir al lector en el fascinante mundo de los números p-ádicos, explicando su construcción desde una mirada accesible, explorando sus propiedades principales, su historia y las motivaciones detrás de su estudio. Además, presentaré algunas de sus aplicaciones, en particular su relación con la criptografía, de forma introductoria. Lejos de ser un trabajo de texto pesado y extenso, esta monografía busca encender la chispa del interés al lector, por una de las estructuras más elegantes y misteriosas con las que esta autora se ha encontrado.

1. Introducción histórica

A lo largo de la historia de las matemáticas, el concepto de lo que es un número ha atravesado múltiples transformaciones, guiadas tanto por la necesidad de resolver problemas concretos como por el querer alcanzar mayor coherencia y generalidad dentro del sistema numérico. Los números p-ádicos, aunque poco conocidos fuera del ámbito matemático avanzado, representan uno de esos saltos conceptuales que ampliaron la noción misma de lo que es un número.

A mitad del siglo XIX, surgió la necesidad de estudiar propiedades de divisibilidad más refinadas que las permitidas por los números reales. Para esa época, la teoría de números ya se había nutrido de aportes de gigantes como Kummer, Dedekind y Kronecker. Existía un interés creciente por entender cómo se comportaban las soluciones de ecuaciones diofánticas y polinómicas, y los métodos de factorización modular estaban cobrando protagonismo. Sin embargo, hacía falta una herramienta que permitiera dar un paso más allá: una forma de unificar todas esas soluciones congruentes y verlas como parte de un objeto único, más grande y más flexible. Estas ideas serían las que sentarían las bases para el desarrollo posterior de los números p-ádicos.



Kurt Hensel, 1861–1941.

Los números p-ádicos fueron descubiertos o inventados[1] por el matemático alemán Kurt Hensel (1861-1941) en 1897. Hensel presentó por primera vez el concepto de números p-ádicos en su artículo *"Über eine neue Begründung der Theorie der algebraischen Zahlen."* [9], donde observó que al extender el concepto de valor absoluto a los números racionales de una manera diferente, se podía definir una nueva topología que daba lugar a los números p-ádicos. Su obra abrió una nueva rama en la teoría de números, proporcionando una herramienta poderosa para entender problemas clásicos desde una perspectiva novedosa.

"Dios hizo los números enteros; el resto es obra del hombre." Leopold Kronecker, 1823–1891.

En las universidades en las que estudió, en Berlín y Bonn, Hensel tuvo la suerte de coincidir con Lipschitz, Weierstrass, Borchardt, Kirchhoff, Helmholtz, Kronecker, entre muchos otros distinguidos profesores. Pero, sin duda, quienes más influencias tuvieron sobre él fueron Leopold Kronecker, quien dirigió su tesis doctoral en 1884, y Karl Weierstrass, cuyo desarrollo de series de potencias para funciones algebraicas en 1897 lo condujo a los números p-ádicos. En 1904, Hensel publicó su artículo *"Neue Grundlagen der Arithmetik"* [8], donde presentó una versión inicial del Lema de Hensel aplicado a polinomios mónicos sobre los enteros p-ádicos, el cual extendería a factorizaciones más generales sin la restricción de ser mónico en el futuro. Mucho más tarde, entre las décadas de 1950 y 1970, otros matemáticos terminarían de consolidar el lema con definiciones equivalentes.

[1] Dejo a opinión del lector, luego de entender el concepto de los números p-ádicos, si estos fueron un invento o un descubrimiento

Mucho del trabajo de Hensel no fue valorado hasta 1921 cuando Helmut Hasse demostró el llamado principio local-global, que establece que una forma cuadrática tiene una solución racional si y sólo si la tiene en los números reales y en los p-ádicos para todo primo p. Más tarde, ambos tendrían la suerte de trabajar juntos.

Hensel dedicó muchos años a la edición de las obras completas de Kronecker y publicó cinco volúmenes de sus obras entre 1895 y 1930. Posteriormente siguió desarrollando toda su teoría sobre los números p-adicos, hasta su muerte en 1941.

Así, a lo largo del siglo XX, los números p-ádicos fueron consolidándose como una herramienta indispensable dentro del análisis y de la teoría algebraica de números. Sin embargo, fue recién hacia finales del siglo que empezaron a emerger aplicaciones inesperadas en campos tan modernos como la criptografía. Lo que alguna vez fue visto como una curiosa construcción numérica, hoy ofrece nuevas formas de proteger información en el mundo digital. En la Sección 5 veremos cómo estos números encuentran un lugar central en el corazón de algunos sistemas criptográficos actuales.

2. Algunos conceptos básicos

Sin importar si el lector es un experto en matemática o si a duras penas se acuerda como multiplicar números de dos cifras, apostaría lo que fuera a que este, ya sea con su debida definición o como un chiste en redes sociales, alguna vez ha escuchado algo sobre los números primos. Se podría pensar que estos forman una hermosa y gran familia de números, aunque esa no es la idea de su denominación. Dado que los números primos son una parte fundamental del tema de esta monografía, permítanme establecer esta sección con el objetivo de repasar algunos conceptos preliminares para quienes los necesiten, e incluso, quizás, señalar detalles que hasta los más conocedores podrían haber pasado por alto.

Definimos al conjunto de los números naturales, que denotamos con $\mathbb{N}$, como el conjunto de los números que se usan para contar los elementos de ciertos conjuntos. Asumiendo que el cero no es un número natural, tenemos que

$$\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}.$$

El conjunto de los números enteros, que denotamos con $\mathbb{Z}$, se compone de todos los números naturales, sus opuestos y el cero. Se puede expresar como

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Estos dos conjuntos constituyen el objeto central de estudio de la Aritmética, también llamada Teoría de Números. Nuestro punto de partida será el concepto de divisibilidad.

Definición 2.1. Dados dos números enteros a y b ($a, b \in \mathbb{Z}$) con $a \neq 0$ decimos que a **divide** a b si y solo si existe $c \in \mathbb{Z}$ tal que $b = ac$. En tal caso usaremos la notación $a \mid b$, mientras que si a no divide a b escribiremos $a \nmid b$.

Equivalentemente podemos decir que a es un divisor de b, que b es divisible por a o que b es múltiplo de a. Llamamos divisores de b al conjunto de números que dividen a b. A continuación, un par de observaciones importantes:

1. 0 es múltiplo de todo número entero, pues $0 = b \cdot 0$ para todo $b \in \mathbb{Z}$.
2. 1 divide a todo número entero, pues $1 \mid b$ para todo $b \in \mathbb{Z}$.
3. Todo número entero no nulo es divisible por si mismo, pues $b = b \cdot 1$ para todo $b \in \mathbb{Z}$. [2]

Es claro que si a es divisor de b su opuesto $-a$ también lo será, por lo que a partir de ahora nos enfocaremos en los divisores positivos.

[2] A pesar de que encontré bibliografía donde se afirma que 0 es divisor de si mismo justificando que $0 = 0 \cdot c$ [14], en nuestra definición ni siquiera consideramos que 0 pueda tomar el rol de quien divide, evitando futuros problemas con la existencia y unicidad de la divisibilidad y evitando quemar las retinas de algunos de los lectores al leer $0 \mid 0$.

2.1. Los números primos: qué son, cuántos hay y para qué sirven

De las observaciones vistas, podemos concluir que todo natural $b > 1$ tiene al menos 2 divisores positivos distintos: 1 y sí mismo, pero es evidente que puede tener más. A partir de esto definiremos a los números primos:

Definición 2.2. Decimos que un número natural $p > 1$ es **primo** si tiene únicamente 2 divisores positivos: 1 y p. Por el contrario diremos que un número natural $a > 1$ es compuesto si tiene otro divisor natural además de 1 y si mismo.

El 1, por convenio, y el 0, por no ser natural, no se consideran primos ni compuestos. Es importante recordar esto para más adelante cuando se tomen p primo y n compuesto en las demostraciones.

Observación 2.3. Algunos autores extienden la definición de los números primos y compuestos a los números negativos, de modo que un número primo p tiene 4 divisores: 1, -1, p y $-p$. Ya que de inmediato se obtiene que p es primo si y solo si $-p$ es primo, para evitar redundancias y debido a que en esta monografía los primos negativos son irrelevantes, solo consideraremos a los primos positivos.

Algo importante a notar, que usaremos en el futuro, es que de la definición de número compuesto obtenemos que un natural $a > 1$ es compuesto si y solo si es posible factorizarlo en la forma $a = bc$ con b y c positivos y distintos de 1.

Para encontrar los primeros números primos usaremos la siguiente propiedad:

Proposición 2.4. Sean $a, b \in \mathbb{N}$. Si $a \mid b$ entonces $a \leq b$.

Demostración. Sean $a, b \in \mathbb{N}$ tales que $a \mid b$. Entonces, existe $c \in \mathbb{Z}$ tal que $b = ac$. Como a y b son positivos, debe ser $c \in \mathbb{N}$. Así tenemos que, $c \geq 1$ y

$$b = ac \geq a \cdot 1 = a.$$

□

Así, para ver si un número p pequeño es primo, tan solo nos hace falta comprobar la cantidad de números entre 1 y p que dividen a p. Encontremos los primeros números primos:

El 2 es primo, pues sus divisores posibles son 1 y 2.

El 3 es primo, pues sus divisores posibles son 1, 2 y 3, pero $2 \nmid 3$.

El 4 no es primo, es compuesto, pues $2 \mid 4$.

El 5 es primo, pues sus divisores posibles son 1, 2, 3, 4 y 5, pero $2 \nmid 5$, $3 \nmid 5$ y $4 \nmid 5$.

El 6 no es primo, es compuesto, pues $2 \mid 6$.

El 7 es primo pues sus divisores posibles son 1, 2, 3, 4, 5, 6 y 7, y de estos solo el primero y el último lo dividen.

Otra forma más rápida de encontrar números primos pequeños, es encontrar los números compuestos y descartarlos. Por ejemplo, podemos deducir que todo número par mayor que 2, será divisible por 2, por lo que será compuesto. También, todo múltiplo de 3 mayor que 3, será divisible por 3 y por lo tanto, compuesto. Para ello, tenemos la siguiente proposición

Proposición 2.5. Si $a \mid b_1$ y $a \mid b_2$ entonces $a \mid b_1x_1 + b_2x_2$, para cualesquiera $x_1, x_2 \in \mathbb{Z}$. Más generalmente, si $n \in \mathbb{N}$ y $a \mid b_i$ para $i = 1, 2 \ldots, n$ entonces $a \mid b_1x_1 + b_2x_2 + \cdots + b_nx_n$ para cualesquiera $x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

Demostración. Para el primer caso, tenemos que como $a \mid b_1$ y $a \mid b_2$, $b_1 = ac_1$ y $b_2 = ac_2$. Luego, $b_1x_1 = ac_1x_1$ y $b_2x_2 = ac_2x_2$ por lo que $a \mid b_1x_1$ y $a \mid b_2x_2$. Entonces,

$$b_1x_1 + b_2x_2 = ac_1x_1 + ac_2x_2 = a(c_1x_1 + c_2x_2),$$

y por lo tanto $a \mid b_1x_1 + b_2x_2$. En cuanto a la generalización aludida en el enunciado, sigue fácilmente por inducción en n. □

Así, en particular, si $a \mid b_1$ entonces $a \mid b_1x_1$ para todo $x_1 \in \mathbb{Z}$, es decir sus múltiplos. Podemos armar una tabla con los primeros 25 números primos, haciendo lo antes mencionado:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Números naturales del 1 al 100. Los primos están marcados en celeste y los compuestos en azul.

Luego de encontrar algunos, la pregunta natural que surge es ¿cuántos hay? La respuesta está dada por el siguiente resultado, dado por Euclides en el año 300 a. C.

Proposición 2.6. Existen infinitos números primos.

Demostración. Supongamos que existe una cantidad finita de números primos (así llegaremos a un absurdo y concluiremos lo contrario). Así, sea $P = \{p_1, p_2, \ldots, p_n\}$ el conjunto finito de todos los primos. Consideremos el número

$$c = 1 + \prod_{j=1}^{n} p_j = 1 + p_1p_2 \ldots p_n.$$

Esto es, el producto de todos los primos más uno. Un resultado intuitivo, que se deja al lector para probar, es que todo natural $a > 1$ admite al menos un divisor primo. Sea

q tal primo, de modo que $q \mid c$. Por otro lado, $p_j \nmid c$ cualquiera sea j, ya que en caso contrario resultaría que, como $p_j \mid \prod_{i=1}^{n} p_i$ y $p_j \mid c$, entonces p_j divide a $1 = c - \prod_{i=1}^{n} p_i$ por 2.5, lo que es absurdo. Luego $q \neq p_j$ para todo j, y hemos encontrado un nuevo primo, que no estaba en nuestro conjunto P de todos los primos, por lo que estos en realidad son infinitos. □

Probablemente el resultado más importante del área, o al menos el más elemental, es el Teorema Fundamental de la Aritmética, el cual, establece el carácter de "átomos" de los números primos en la multiplicación entera. Este establece que todo número entero mayor que uno puede descomponerse de manera única como producto de números primos. Por ello, es natural pensar que, para comprender mejor a los números, conviene entender a fondo a los primos.

Pero comprenderlos no implica controlarlos porque, por más que sepamos que hay infinitos primos, no existe una fórmula que los genere de forma directa y sistemática. Existen funciones que permiten verificarlos con eficiencia, o que los enumeran con estructuras matemáticas complejas, pero ninguna expresión simple devuelve únicamente números primos. Además el teorema de los números primos nos dice que a medida que uno se adentra en números más grandes, los primos se vuelven escurridizos. Su frecuencia disminuye, y detectarlos se vuelve cada vez más costoso en términos computacionales.

En palabras de Enrique Gracián, "En un sentido metafórico, los números primos son como un virus maléfico que, cuando ataca la mente de un matemático, es muy difícil de erradicar. Euclides, Fermat, Euler, Gauss, Riemann, Ramanujan y una larga lista de los matemáticos de más renombre de la historia cayeron en sus redes..." [6]

Esta dificultad no es meramente teórica, tiene implicancias prácticas. En particular, la seguridad de muchos sistemas criptográficos modernos se basa justamente en lo difícil que resulta encontrar o factorizar primos grandes. El famoso algoritmo RSA, por ejemplo, parte de la elección de dos primos muy grandes cuya multiplicación da lugar a una clave pública. Para romper este sistema habría que encontrar los factores primos de un número enorme, tarea que, con los métodos actuales, sería inviable en tiempos razonables.

De este modo, los números primos, lejos de ser una rareza o una curiosidad matemática, además de formar el esqueleto mismo de la aritmética, son una pieza clave para proteger transacciones, comunicaciones y datos personales en todo el mundo.

Y, aunque dejemos de hablar de los números convencionales, los números primos vuelven a tener un papel especial en la criptografía, con los ahora números p-ádicos.

3. Los enteros n-ádicos

Cuando vemos una serie que diverge, por ejemplo la suma de todos los naturales

$$\sum_{i=1}^{\infty} i = 1 + 2 + 3 + \ldots,$$

casi al instante asociamos esta suma con el infinito y normalmente no operamos con ésta, ni nos interesa, porque no toma ningún valor. Si no tiene límite, no tenemos un número al que es igual, con el cual podemos sumar y multiplicar como estamos acostumbrados.

Sin embargo, podríamos definir un nuevo tipo de objeto no en sí infinito, al que asignarle a algunas de estas sumas infinitas.

3.1. Una forma intuitiva de pensarlos: series de potencias

Definición 3.1. Dado $n \in \mathbb{N}$, $n > 1$ definimos un entero $\mathfrak{a}$ n-ádico como la serie

$$\mathfrak{a} = (\ldots a_3 a_2 a_1 a_0)_n = \sum_{i \geq 0} a_i n^i = a_0 + a_1 n + a_2 n^2 + \ldots, \quad a_i \in \{0, 1, \ldots, n-1\}.$$

La n indica la base en la que estamos trabajando, es decir, los dígitos posibles que pueden tomar los coeficientes a_i, que van de 0 hasta $n-1$. La notación $(\ldots a_3 a_2 a_1 a_0)_n$ representa un número escrito en base n, donde a_0 es el dígito de las "unidades", a_1 el de las "decenas", a_2 el de las "centenas", y así sucesivamente. Por ahora n no nos preocupa si es compuesto o si es primo. A diferencia de los números decimales habituales, esta expresión tiene infinitos dígitos hacia la izquierda. Por eso, los números n-ádicos pueden pensarse como números en base n, pero extendidos hacia el infinito por la izquierda.

Denotamos al conjunto de los enteros n-ádicos por $\mathbb{Z}_n$.

Podemos identificar un número n-ádico por su sucesión de coeficientes $\{a_i\}_{i \geq 0}$. Así dados $\mathfrak{a} = \sum_{i \geq 0} a_i n^i$ y $\mathfrak{b} = \sum_{i \geq 0} a_i n^i$ tenemos que

$$\mathfrak{a} = \mathfrak{b} \iff a_i = b_i \text{ para todo } i \geq 0.$$

Los coeficientes, vistos como los dígitos hacia la izquierda, podrían tener algún periodo, como por ejemplo el 10-ádico

$$\ldots 1212_{10} = 2 + 10 + 200 + 1000 + \ldots = \sum_{i=0}^{\infty} a_i 10^i, \quad a_i = \begin{cases} 1, & \text{si } i \text{ es impar} \\ 2, & \text{si } i \text{ es par.} \end{cases}$$

O, podrían no tener periodo, como el número 10-ádico $\ldots 2951413_{10}$ cuyo i-ésimo dígito (contando de derecha a izquierda) es el i-ésimo dígito de π (contando de izquierda a derecha).

Es importante notar que, un número natural se puede escribir como una expansión finita en base n, así que todo número natural se puede ver como un número n-ádico que simplemente tiene todos los coeficientes $a_i = 0$ a partir de cierto punto. Por lo que podríamos pensar que los enteros n-ádicos son una "extensión" de los naturales.

A partir de la definición, podemos deducir que el conjunto de los enteros n-ádicos no es numerable. En efecto, suponiendo que podríamos enumerar todos los enteros n-ádicos en una lista como

$$1 = \sum_{i=0}^{\infty} a_i n^i, \quad 2 = \sum_{i=0}^{\infty} b_i n^i, \quad 3 = \sum_{i=0}^{\infty} c_i n^i, \ldots$$

Podemos entonces construir un nuevo entero n-ádico $\mathfrak{x} = \sum_{i=0}^{\infty} x_i n^i$ de modo que

$$x_0 \neq a_0, \quad x_1 \neq b_1, \quad x_2 \neq c_2, \quad \ldots,$$

Este nuevo número $\mathfrak{x}$ difiere de un x_i en al menos el i-ésimo dígito, por lo que no puede estar en la lista. Esto contradice la hipótesis de que el conjunto de los enteros n-ádico es numerable, por lo que no lo es. Esta demostración, basada en el argumento de diagonalización de Cantor, nos permite concluir que el cardinal de $\mathbb{Z}_n$ es en realidad el mismo que el de $\mathbb{R}$: el cardinal del continuo.

Desde la escuela se nos enseña que cuando tenemos un número, en cierto sentido, es más importante conocer el dígito en su decena que el de su unidad, y más importante conocer el de su centena que el de su decena, y así sucesivamente. Esto por supuesto lo aplicamos también en la vida cotidiana. La razón es lógica: ¿Por que nos importaría saber que la unidad de un cierto número es 3, si no sabemos si se trata de 1 000 003, de 2 000 003, o de alguno mucho más grande?.

Sin embargo, en el mundo de los números n-ádicos, sucede algo curioso: lo que en la escritura decimal sería considerado lo "menos importante" (los dígitos en las potencias bajas de n) pasa a tener un rol central. Esto se debe a que, al construir un número n-ádico, lo hacemos a partir de sus residuos módulo n, n^2, n^3, etc., es decir, comenzamos por conocer su comportamiento "local" en los múltiplos pequeños de n, y a partir de ahí lo vamos extendiendo.

Cuando vemos estos números n-ádicos, tan solo vemos sus últimas cifras y, por ello, para nuestras operaciones futuras, estas serán las esenciales. Así como cuando uno no puede ver un número irracional en su totalidad, y tan solo trabaja con las primeras cifras después de la coma para hacer cálculos en la vida real, veremos como podemos trabajar con estos números n-ádicos sin necesidad de usar sus infinitos dígitos a la izquierda.

3.2. Hacia una estructura algebraica

Veamos ahora las operaciones y estructuras que podemos tener a partir de nuestros nuevos números.

3.2.1. Suma de n-ádicos

Ya bien definidos, podemos empezar a operar con ellos. Primero definimos nuestra suma de números n-ádicos digito a dígito recursivamente[3], como lo hacemos con los números comúnmente. Así, dados dos números n-ádicos $\mathfrak{a} = \sum_{i\geq 0} a_i n^i$ y $\mathfrak{b} = \sum_{i\geq 0} a_i n^i$ tenemos que:

[3]Esto es, un proceso en el que, después de fijar un caso base, se define un objeto n arbitrario en términos de un objeto anterior.

- El primer dígito de su suma es $a_0 + b_0$, si $a_0 + b_0 \leq n - 1$ y $a_0 + b_0 - n$ sino. En el primer caso definimos $q_0 = 0$ y en el segundo $q_0 = 1$. Esto es, el acarreo que sumaremos al siguiente digito.
- Luego, definimos que el i-ésimo dígito de la suma es $a_i+b_i+q_{i-1}$, si $a_i+b_i+q_{i-1} \leq n-1$ y $a_i + b_i + q_{i-1} - n$ sino, donde q_{i-1} es 1 o 0, dependiendo si sobró acarreo o no, en el paso anterior. En el primer caso definimos $q_i = 0$ y en el segundo $q_i = 1$.

Para aquellos lectores a los que les haya disgustado haber visto tantas variables para una suma, veamos cómo se realiza la suma de dos números n-ádicos en algunos casos, y qué es lo que puede ocurrir.

Por supuesto, para n-ádicos donde todos los a_i son 0 a partir de un i, la suma actúa exactamente igual a la suma de naturales. En este caso, se encuentra el n-ádico $\sum_{i\geq 0} 0 \cdot n^i = \ldots 0000_n = 0$, el cual es el elemento neutro debido a que cumple que $\mathfrak{a} + 0 = \mathfrak{a}$.

Ahora veamos algunas sumas de n-ádicos con dígitos infinitos.

Ejemplo 3.2. Sumemos los números 5-ádicos $\ldots 24242_5 = \sum_{i\geq 0} a_i 5^i$ donde $a_{2k} = 2$ y $a_{2k+1} = 4$ para $k \in \mathbb{N}_0$, y $\sum_{i\geq 0} 5^i = \ldots 11111_5$:

$$\begin{array}{r} \overset{1}{\cdots}\overset{1}{4}\overset{1}{2}\overset{1}{4}\overset{1}{2}4242 \\ +1111111111 \\ \hline \cdots 0404040403 \end{array}$$

En este caso, la suma de 2 números 5-ádicos que tienen un periodo en sus dígitos resulta periódica también.

Ejemplo 3.3. Sumemos el número 10-ádicos $\sum_{i\geq 0} \pi_i \cdot 10^i = \ldots 51413_1 0$, con π_i el i-ésimo dígito de π ($\pi_0 = 3$, $\pi_1 = 1$, $\pi_2 = 4$ $\ldots$) con él mismo:

$$\begin{array}{r} \overset{1}{\cdots}\overset{1}{3}562\overset{1}{9}51\overset{1}{4}13 \\ +3562951413 \\ \hline \cdots 7125902826 \end{array}$$

En este caso, la suma de 2 números 10-ádicos que no tiene un periodo resulta en otro que tampoco lo tiene.

Ejemplo 3.4. Sumemos los números 10-ádicos $\sum_{i\geq 0} 9 \cdot 10^i = \ldots 99999$ y 1

$$\begin{array}{r} \overset{1}{\cdots}\overset{1}{9}\overset{1}{9}\overset{1}{9}\overset{1}{9}\overset{1}{9}\overset{1}{9}\overset{1}{9}\overset{1}{9}\overset{1}{9}9 \\ +\qquad\qquad 1 \\ \hline \cdots 0000000000 \end{array}$$

Tenemos así que $\ldots 99999 + 1 = 0$, es decir que $\ldots 99999$ es el inverso aditivo del 1.

Este último ejemplo nos da la pista de algo interesante: sin la necesidad de definir una resta, podemos encontrar el opuesto de un número:

Proposición 3.5. Dado el número n-ádico $\mathfrak{a} = \sum_i^\infty a_i n^i$ tenemos que

$$-\mathfrak{a} := \sum_i^\infty (n-1-a_i)n^i + 1$$

es su opuesto, tal que $\mathfrak{a} + (-\mathfrak{a}) = 0$.

Demostración. Sea $\mathfrak{b} = \sum_i^\infty b_i n^i = \mathfrak{a} + (-\mathfrak{a})$. Queremos ver que $\mathfrak{b} = 0$, es decir $b_i = 0$ para todo $i \geq 0$. Tenemos que $b_0 = a_0 + (n-1-a_0) + 1 = n$, pero como debe ser $0 \leq b_0 \leq n-1$, entonces b_0, y sumaremos 1 al siguiente dígito. Luego, $b_1 = a_1 + (n-1-a_i) + q_0$, donde q_0 es el acarreo. Esto nos devuelve que $b_1 = 0$ y que sumaremos 1 al siguiente dígito, lo que nos deja concluir que resultará en que $b_i = 0$ para todo $i \geq 0$. □

Definimos la suma de dos números n-ádicos como

$$\mathfrak{a} + \mathfrak{b} = \sum_{i\geq 0} a_i n^i + \sum_{i \geq 0} b_i n^i = \sum_{i \geq 0} r_i n^i$$

donde $r_0 = a_0 + b_0 \bmod n$ y $r_i = (a_i + b_i + r_{i-1}) \bmod n$ Esto es, la suma digito a dígito en base n.

3.2.2. Producto de n-ádicos

Análogo a la suma, nuestro producto será una extensión del producto usual de números. Saltándonos la explicación del proceso (ya que es demasiado larga y complicada en comparación con lo que es la propia multiplicación), veamos algunos ejemplos.

Ejemplo 3.6. Multipliquemos $\ldots 121212_7$ por $\ldots 545_7$

$$\begin{array}{r} \cdots 1212121212 \\ \times \cdots \qquad\qquad 545 \\ \hline \cdots 6363636363 \\ \cdots 151515151 \\ + \cdots 63636363 \\ \hline \cdots 0606060503 \end{array}$$

Estos casos nos muestra lo fácil que el acarreo nos puede complicar los cálculos en la multiplicación en el caso de números n-ádicos sin patrones periódicos, lo cual no es para nada práctico para demostraciones formales.

Ejemplo 3.7. Multipliquemos el 10-ádico $\ldots 5555_{10}$ por si mismo

$$
\begin{array}{r}
\overset{2\,2\,2\,2\,2\,2\,2\,2\,2}{\cdots 5555555555} \\
\times \cdots 5555555555 \\
\hline
\overset{6\,5\,5\,4\,3\,2\,2\,1}{\cdots 7777777775} \\
\cdots 777777775 \\
\cdots 77777775 \\
\cdots 7777775 \\
\cdots 777775 \\
\cdots 77775 \\
\cdots 7775 \\
\cdots 775 \\
\cdots 75 \\
\cdots 5 \\
+ \ddots \quad \vdots \\
\hline
\cdots 4691358025
\end{array}
$$

Este caso nos muestra lo fácil que el acarreo nos puede complicar los cálculos en la multiplicación, lo cual no es para nada práctico para demostraciones formales.

Del mismo modo que en el producto usual, el neutro resulta ser el $1 = \ldots 0001_n$ debido a que para $\mathfrak{a} = (\ldots a_3 a_2 a_1 a_0)_n$

$$
\begin{array}{r}
\cdots a_9\, a_8\, a_7\, a_6\, a_5\, a_4\, a_3\, a_2\, a_1\ \ a_0 \\
\times \cdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad 1. \\
\hline
\cdots a_9\, a_8\, a_7\, a_6\, a_5\, a_4\, a_3\, a_2\, a_1\ \ a_0 \\
\cdots \ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0 \\
\cdots \ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0 \\
\cdots \ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0 \\
\cdots \ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0 \\
+ \ddots \quad \vdots \\
\hline
\cdots a_9\, a_8\, a_7\, a_6\, a_5\, a_4\, a_3\, a_2\, a_1\, a_0.
\end{array}
$$

Después de haber visto las operaciones $+$ y $\cdot$, veamos las estructuras algebraicas que podemos formar.

Definición 3.8. Un **anillo** es un conjunto no vacío A dotado de dos operaciones internas, **suma** $(+)$ y **producto** $(\cdot)$, tales que:

(i) $(A, +)$ es un grupo abeliano. Esto significa que:

- Existe un elemento neutro para la suma (lo denotamos 0) tal que $a + 0 = a$ para todo $a \in A$.
- Todo elemento $a \in A$ tiene un opuesto $-a \in A$ tal que $a + (-a) = 0$.
- La suma es asociativa: $(a + b) + c = a + (b + c)$.
- La suma es conmutativa: $a + b = b + a$.

(ii) El producto es una operación interna asociativa en A, es decir:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{para todo } a, b, c \in A.$$

(Nota: no exigimos que el producto sea conmutativo ni que todos los elementos tengan inverso multiplicativo.)

(iii) El producto es distributiva respecto de la suma, es decir, para todo $a, b, c \in A$:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{(distributiva izquierda)},$$

$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{(distributiva derecha)}.$$

Si además A posee un elemento neutro multiplicativo (denotado 1) tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$, diremos que A es un **anillo con unidad**.

Si la multiplicación también es conmutativa, es decir $a \cdot b = b \cdot a$ para todo $a, b \in A$, entonces decimos que A es un **anillo conmutativo**.

Revisando lo que hemos definido y demostrado para la suma (que actúa de forma muy similiar a la suma entera y mantiene la asociatividad y la conmutatividad), tenemos que se cumple el item (i): $\mathbb{Z}_n$ forma un grupo abeliano con la suma. De la misma forma, por la definición análoga a del producto usual, tenemos que se cumplen los items (ii) y (iii). Además, por la misma razón, el producto es conmutativo y vimos que posee el elemento neutro 1, por lo que llegamos a que conjunto de los enteros n-ádicos conforma un anillo conmutativo con unidad. Para la demostración completa con los pasos que aquí hemos omitido ver [1]

3.3. Un pequeño problema

Definición 3.9. Sea A un anillo. Decimos que un elemento $a \in A$ es un **divisor de cero** si existe otro elemento $b \neq 0$ tal que $a \cdot b = 0$.

Definición 3.10. Un **dominio íntegro** es un anillo conmutativo con unidad que no tiene divisores de cero.

Ejemplo 3.11. Consideramos el número 10-ádico $\ldots 212890625_{10}$ y lo multiplicamos por sí, viendo que por construcción

$$\begin{array}{r} \cdots 2890625 \\ \times \cdots 2890625 \\ \hline \cdots 4453125 \\ \cdots 781250 \\ \cdots 43750 \\ \cdots 625 \\ \cdots 00 \\ \cdots 0 \\ + \ \ddots \\ \hline \cdots 2890625 \end{array}$$

Notar que este 10-ádico satisface:

$$n^2 = n \Leftrightarrow n^2 - n = 0 \Leftrightarrow n(n-1) = 0.$$

Sin embargo, $\ldots 212890625_{10}$ no es 0 ni 1, lo que significa que $n(n-1) = 0$ no implica que alguno de los factores sea 0. De esta forma, $\ldots 212890625_{10}$ es un divisor de cero y hemos encontrado que $\mathbb{Z}_{10}$ tiene divisores de cero, lo que hace que este no sea un dominio íntegro.

Pero, ¿que tan importante es realmente contar con un dominio íntegro? Y, ¿cuándo podemos estar seguros de que lo tenemos?

La propiedad de que el producto de dos elementos sea cero sin que ninguno de ellos necesariamente lo sea, es decir, la existencia de divisores de cero, representa una gran dificultad, especialmente a la hora de resolver ecuaciones, no solo en estructuras como $\mathbb{Z}_n$, sino en contextos más generales y comunes.

Un ejemplo muy familiar se presenta al factorizar polinomios. ¿Alguna vez se preguntaron por qué existen tantos métodos para hacerlo: la fórmula resolvente, el Teorema de Gauss, la regla de Ruffini, entre otros? La razón es que, en cuerpos como $\mathbb{R}$, o en dominios íntegros más en general, podemos confiar en la siguiente implicación: si un polinomio se factoriza como

$$a(x - r_1)(x - r_2) \cdots (x - r_n) = 0, \quad a \neq 0,$$

entonces, necesariamente, alguna de las raíces r_i satisface $x = r_i$, ya que no hay divisores de cero. En otras palabras, la igualdad

$$(x - r_1)(x - r_2) \cdots (x - r_n) = 0$$

equivale a que alguno de los factores sea nulo, lo que nos permite encontrar las soluciones del polinomio de forma directa.

Esta propiedad, que puede parecer tan natural cuando trabajamos con los reales, es en realidad muy poderosa: sustenta muchos de los métodos que usamos para resolver ecuaciones. Cuando se pierde, nuestra capacidad de deducir soluciones se ve seriamente limitada.

La respuesta a cuándo podemos asegurar que tenemos la doble implicación $a \cdot b = 0 \Leftrightarrow a = 0$ o $b = 0$, nos la da el siguiente teorema, que nos presenta al fin el papel de los números primos en los n-ádicos:

Teorema 3.12. $\mathbb{Z}_n$ es un dominio integro $\iff$ n es primo.

La demostración de este teorema con las herramientas que tenemos hasta ahora, es muy engorrosa y la saltearemos. Con la construcción de $\mathbb{Z}_p$ con el valor absoluto $|\cdot|_p$, este teorema será tan solo un resultado de otro mucho más fuerte: que $\mathbb{Q}_p$, el conjunto de los racionales p-ádicos, es un cuerpo.

Este problema justifica en parte por qué la mayoría de los desarrollos teóricos (en álgebra, topología, análisis o criptografía) se enfocan en los números p-ádicos con p primo. La condición de primalidad de p asegura que la estructura resultante sea mucho más robusta desde el punto de vista algebraico.

Así que, trabajar con números n-adicos cuando n no es primo necesariamente, puede traer problemas que queremos evitar (en especial si los queremos definir formalmente valores absolutos) y puede limitarnos. Por esta razón es que no nos interesa cuando n es compuesto y nos centramos en los números p-ádicos.

Otra propiedad muy importante para los conjuntos y operaciones es la del inverso multiplicativo. Es decir, que para todo $a \in A$, $a \neq 0$ exista $a^{-1} \in A$ tal que $aa^{-1} = a^{-1}a = 1$.

Sin embargo, no se puede asegurar que todo elemento de $\mathbb{Z}_n$ tenga un inverso[4]. Veamos el siguiente ejemplo.

Ejemplo 3.13. Si tomamos el $10-$ádico 5_{10} (o de hecho cualquier 10-ádico cuyo primer digito sea 5), vemos que si suponemos que $\mathfrak{a}$ es su inverso y los multiplicamos,

$$\begin{array}{cccccccccccc} \cdots & a_9 & a_8 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \\ \times & & & & & & & & & & 5 \\ \hline \cdots & 5a_9 & 5a_8 & 5a_7 & 5a_6 & 5a_5 & 5a_4 & 5a_3 & 5a_2 & 5a_1 & 5a_0 \end{array}$$

obtenemos que debe ser $5a_0 \equiv 1 \bmod 10$ con $a_0 \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ lo cual no es posible porque el miembro izquierdo siempre será congrente módulo 0 o 5.

[4]Para un análisis sobre cuales sí son los elementos invertibles de $\mathbb{Z}_n$ con esta representación ver [5].

4. Los números p-ádicos

Como los números p-ádicos son en particular un número n-ádico, todas las definiciones y operaciones antes vistas aún nos sirven. Sin embargo, aquí los construiremos desde cero, de una forma más formal, con ciertas herramientas que nos ofrece el análisis.

4.1. Construcción formal

Los números racionales, esos viejos conocidos que se portan tan bien cuando se trata de fracciones y reglas de tres, tienen una gran virtud: dentro de todo, forman un cuerpo bastante completo. Podemos sumar, restar, multiplicar y dividir, y resolver muchas ecuaciones sin mayores complicaciones. Son eficientes, precisos, y hasta simpáticos cuando de operaciones finitas se trata... salvo cuando se los necesita con precisión absoluta.

Para eso, los matemáticos completamos $\mathbb{Q}$ con respecto al valor absoluto usual, y así obtenemos los reales. Pero, como suele ocurrir en matemáticas, esta no es la única forma de mirar las cosas. ¿Qué pasaría si en lugar del valor absoluto común, eligiéramos otro? Uno que mida la "divisibilidad" por un número primo p, en lugar de la distancia convencional. Definiendo un nuevo valor absoluto p-ádico, es que definiremos nuestro conjunto de números p-ádicos.

Definición 4.1. Sea p un número primo. Llamamos **orden p-ádico** (o valoración p-ádica) en $\mathbb{Z}$ a la función $v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R}$, definida como

$$v_p(a) := \text{máx}\{k \in \mathbb{N}_0 : p^k \mid a\}.$$

Esto es, el exponente de la mayor potencia de p que divide a x, donde la existencia y unicidad del orden p-ádico proviene de la descomposición única en factores primos. De esta forma $x = p^{v_p(x)}x'$ con $p \nmid x'$.

Ejemplo 4.2. Calculamos el orden p-ádico de los siguientes números:

- $v_2(1024) = v_2(2^{10}) = 10$
- $v_3(2430) = v_3(2 \cdot 3^5 \cdot 5) = 5$
- $v_5(1000) = v_5(2^3 \cdot 5^3) = 3$
- $v_7(250) = v_7(2 \cdot 5^3) = 0$

Algunos resultados triviales son:

- $v_p(x) = v_p(-x)$
- $v_p(p^k) = k$
- Si $v_p(x) = r$ entonces $v_p(x^k) = r^k$
- Sea q primo fijo. Entonces $v_p(q) = 0$ para todo $p \neq q$ primo.

Si $x = 0$, definiremos que para todo p, $v_p(0) = \infty$, lo cual es intuitivo ya que 0 es divisible por cualquier primo una cantidad infinita de veces.

Ahora extendamos v_p a los racionales. Si $x \in \mathbb{Q}$, $x = \frac{a}{b}$, tenemos que $a = p^{v_p(a)}a'$ y $b = p^{v_p(b)}b'$. Por lo tanto,

$$x = \frac{p^{v_p(a)}a'}{p^{v_p(b)}b'} = p^{v_p(a)-v_p(b)}\frac{a'}{b'}$$

Veamos que esta expresión es única. Supongamos que hay dos expresiones distintas,

$$x = p^r\frac{a'}{b'} = p^s\frac{a''}{b''}$$

con a',a''',b', b'' coprimos con p. Así, tenemos que $p^r a'b'' = p^s a''b'$, de donde concluimos que $r = s$ y nos queda $a'b'' = b'a''$. Por lo tanto, $\frac{a'}{b'} = \frac{a''}{b''}$. Así que la expresioón es única y no depende de la representación de x como cociente de dos enteros.

Definición 4.3. Sea $x = \frac{a}{b} \in \mathbb{Q} - \{0\}$, el **orden *p*-ádico** en $\mathbb{Q}$ viene determinado por la fórmula

$$x = \frac{a}{b} = p^{v_p(x)}\frac{a'}{b'}$$

donde $(p, a') = 1$ y $(p, b') = 1$.

Lema 4.4. Sean x, $y \in \mathbb{Q} - \{0\}$

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$ Si además $v_p(x) \neq v_p(y)$ se cumple la igualdad.

Demostración. Consideramos $x, y \in \mathbb{Q}$. Por comodidad vamos a llamar $r = v_p(x)$ y $s = v_p(y)$.

1. Tenemos que $x = p^r x'$ y $y = p^s y'$, con x' y y' coprimos con p. Por un lado tenemos que
$$xy = p^{v_p(xy)}(x'y').$$
Y por otra
$$xy = p^r p^s x'y' = p^{r+s}x'y'$$
2. Sean
$$x = \frac{a}{b} = p^r\frac{a'}{b'} \qquad y = \frac{c}{d} = p^s\frac{c'}{d'}$$
con $(a'b', p) = 1 = (c'd', p)$ y $r, s \in \mathbb{Z}$. Primero supongamos que $r < s$. Así,
$$x + y = p^r\frac{a'}{b'} + p^s\frac{c'}{d'} = p^r\frac{a'd' + p^{s-r}b'c'}{b'd'}$$

donde tanto el numerador como el denominador son comprimos con p. Por lo tanto, $v_p(x+y) = r = \text{mín}\{r, s\}$. Ahora supongamos que $r = s$. Así,

$$x + y = p^r \frac{a'}{b'} + p^r \frac{c'}{d'} = p^r \frac{a'd' + b'c'}{b'd'}$$

donde sabemos que $b'd'$ es primo con p pero $a'd' + b'c'$ no tiene por que serlo. Por lo tanto, vamos a escribir $a'd' + b'c' = p^t k$ con $t \geq 0$ y $(k, p) = 1$. Entonces,

$$p^r \frac{a'd' + b'c'}{b'd'} = p^{r+t} \frac{k}{b'd'}.$$

Así, en este caso $v_p(x+y) = r + t \geq r = \text{mín}\{r, s\}$

□

Observación 4.5. De la propiedad 1, también obtenemos su análoga con la división

$$v_p\left(\frac{x}{y}\right) = v_p(x) - v_p(y).$$

Quizás al ver esta identidad, al lector se le haya venido a la mente el logaritmo (si es que no se le ocurrió ya antes con la definición o con esas curiosas propiedades de v_p que vimos). Calmando esa voz interna, he de comentar que, efectivamente, el orden p-ádico y el algoritmo en base p están relacionados, aunque no de un modo muy profundo. Podríamos decir que, mientras que el logaritmo $\log_p(x)$ pregunta "¿qué exponente necesita p para llegar a x?", el orden p-ádico responde "¿cuántas veces entra p exactamente en x?", pero de forma discreta. Dejo de tarea al lector hallar una identidad que los relacione directamente.

Observación 4.6. La propiedad 1 no se cumple si se nos ocurre considerar un orden n-ádico, con n compuesto. Por ejemplo, si $a = 2$, $b = 2$ y consideramos v_4, tenemos que

$$v_4(2 \cdot 2) = 1 \neq 0 = v_4(2) + v_4(2).$$

De hecho, para cualquier $n = n_1 n_2$, con $1 < n_1 \leq n_2 < n$ tomando $a = n_1$ y $b = n_2$, tenemos que

$$v_n(n_1 \cdot n_2) = v_n(n) = 1 \neq 0 = v_n(n_1) + v_n(n_2).$$

Así, vemos cómo los números compuestos nos siguen causando problemas, aún con otras definiciones.

Definición 4.7. Definimos el **valor absoluto *p*-ádico** en $\mathbb{Q}$ como

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

Ahora nos falta comprobar que lo que acabamos de definir es de verdad un valor absoluto.

Proposición 4.8. La función $|\cdot|_p$ es un valor absoluto no arquimediano.

Demostración. Verifiquemos que las 3 propiedades que tiene que cumplir para ser un valor absoluto. Sean $x, y \in \mathbb{Q}$.

1. $|x|_p \geq 0$ y $|x|_p = 0 \Leftrightarrow x = 0$

   Como p es un número primo, $p > 1$ y por lo tanto $|x|_p = p^{-v_p(x)} \geq 0$, el cual solo se anula, por definición cuando $x = 0$.

2. $|x + y|_p \leq |x|_p + |y|_p$

   Por el lema 4.4 sabemos que $v_p(x+y) \geq \text{mín}\{v_p(x), v_p(y)\}$, y suponiendo sin pérdida de generalidad que $v_p(x) \leq v_p(y)$ tenemos que

$$\begin{aligned} |x + y|_p &= p^{-v_p(xy)} \\ &\leq p^{-\text{mín}\{v_p(x),v_p(y)\}} \\ &= p^{-v_p(x)} \\ &\leq p^{-v_p(x)} + p^{-v_p(y)} \\ &= |x|_p + |y|_p. \end{aligned}$$

3. $|xy|_p = |x|_p|y|_p$

   Por el lema 4.4 sabemos que $v_p(xy) = v_p(x) + v_p(y)$, por lo que tenemos que

$$|xy|_p = p^{-v_p(xy)} = p^{-v_p(y)-v_p(y)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$$

   Para comprobar que es no arquimediano basta ver que se cumple la condición

$$|x + y|_p \leq \text{máx}\{|x|_p, |y|_p\}.$$

   Para ello, utilizamos la desigualdad ya probada en 2:

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

   Entonces

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

□

Podemos pensar en el valor absoluto $|\cdot|_p$ como una regla que mide "el tamaño" o la "distancia al cero" de un número, pero no como lo solemos hacer con los números reales. En lugar de fijarnos en lo grande que es un número en valor numérico, como hace el valor absoluto usual, $|\cdot|_p$ nos dice cuánto está "dividido" por una potencia de un número primo.

Recordemos que si p no divide a x, $v_p(x) = 0$ y $|x|_p = 1$, y si p divide a x con multiplicidad k (esto es $p^k \mid x$ pero $p^{k+1} \nmid x$) entonces $|x|_p = \frac{1}{p^k}$, el cual se hace más pequeño a medida que k aumenta.

Esto significa que los números que comparten muchos factores de p están "más cerca entre sí". Así, el número 125 en la norma $|\cdot|_5$ está "más cerca" del 25 (ambos potencias de

5), que del 124, difiriendo con el valor absoluto usual. Y, el número $282475249 = 7^{10}$, está más cerca del 0 en la norma $|\cdot|_7$ que cualquier otro número entre el 1 y $282475248 = 7^{10}-1$.

Que el valor p-ádico sea no arquimediano implica que al sumar dos números, el resultado nunca es "más grande" que el más grande de los dos (según esta forma de medir). En otras palabras, la suma "hereda" el tamaño del número más grande, sin combinar los tamaños como lo haríamos en el mundo real.

4.2. El cuerpo $\mathbb{Q}_p$ de los números p-ádicos

Definamos primero algunos preliminares necesarios.

Definición 4.9. Un cuerpo es un conjunto K no vacío con dos operaciones internas, suma $+$ y producto $\cdot$, tales que:

(i) $(K, +)$ es un grupo abeliano con elemento neutro 0,

(ii) $(K \setminus \{0\}, \cdot)$ es un grupo abeliano con elemento neutro 1,

(iii) La operación producto es distributiva respecto de la suma:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{para todo } a, b, c \in K.$$

Definición 4.10. Sea K un cuerpo y sea $|\cdot|$ un valor absoluto en K. Una sucesión $(x_n) \subset K$ se dice que es una **sucesión de Cauchy** si para todo $\varepsilon > 0$ existe un entero $N \in \mathbb{N}$ (que depende de ε) tal que

$$|x_n - x_m| < \varepsilon \quad \text{para todo } n, m \geq N.$$

Definición 4.11. Sea K un cuerpo y sea $|\cdot|$ un valor absoluto en K. Se dice que K es **completo** si toda sucesión de Cauchy en K converge en K, es decir, existe un $x \in K$ tal que $x_n \to x$.

El cuerpo de los números racionales $\mathbb{Q}$ no es completo con el valor absoluto usual y el cuerpo de los números reales $\mathbb{R}$ es su completado respecto a este valor absoluto.

De igual forma, $\mathbb{Q}$ tampoco es completo respecto de ningún valor absoluto p-ádico, y construyendo su completado, de la misma forma que se hace con $\mathbb{R}$ (añadiendo a $\mathbb{Q}$ los límites de todas las sucesiones de Cauchy) es que obtenemos el llamado cuerpo de los números p-ádicos. Esto es, para cada p tenemos una completación no trivial de $\mathbb{Q}$. De hecho, $\mathbb{R}$ y $\mathbb{Q}_p$ no son isomorfos como cuerpos, ni lo son $\mathbb{Q}_p$ y $\mathbb{Q}_q$ si p y q son primos distintos. Así, con la norma $|\cdot|_p$ obtenemos infinitas completaciones distintas de $\mathbb{Q}$. Por supuesto, las demostraciones de estas afirmaciones, y las que siguen, necesitan mucho más contenido preliminar que extendería considerablemente esta monografía, pero se pueden ver en [3]. Sin embargo, enunciaremos a continuación los resultados y definiciones importantes que queriamos llegar a ver.

Definición 4.12. El cuerpo $\mathbb{Q}_p$ de los números p-ádicos se define como el conjunto de todas las clases de equivalencia de sucesiones de Cauchy de números racionales respecto del valor absoluto p-ádico. Dos sucesiones (x_n) y (y_n) son equivalentes si

$$\lim_{n\to\infty} |x_n - y_n|_p = 0.$$

La suma y el producto en $\mathbb{Q}_p$ se definen término a término a partir de representantes de cada clase de equivalencia.

Ejemplo 4.13. Consideremos la sucesión de racionales:

$$x_n = \sum_{k=0}^{n} 5^k = 1 + 5 + 5^2 + \cdots + 5^n.$$

Esta sucesión converge en $\mathbb{Q}_5$, aunque diverge en $\mathbb{R}$, pues no está acotada. En el valor absoluto 5-ádico, cada término adicional hace que el número esté más "cerca" del límite, ya que $|5^k|_5 = 5^{-k}$ se hace cada vez más pequeño. En efecto, la sucesión es de Cauchy y converge a un número p-ádico que puede interpretarse como la suma infinita:

$$\sum_{k=0}^{\infty} 5^k = \frac{1}{1-5} = -\frac{1}{4} \quad \text{en } \mathbb{Q}_5.$$

El ejemplo anterior ilustra una de las diferencias más profundas entre el análisis usual en $\mathbb{R}$ y el análisis p-ádico: ciertas series que divergen en el mundo real pueden tener un comportamiento completamente opuesto en el mundo p-ádico.

4.3. Los enteros p-ádicos

Una vez construido el cuerpo de los números p-ádicos $\mathbb{Q}_p$ como completación de $\mathbb{Q}$ respecto del valor absoluto $|\cdot|_p$, es natural preguntarse si dentro de este nuevo conjunto existen análogos de los números enteros.

Definición 4.14. El anillo de los **enteros p-ádicos**, denotado por $\mathbb{Z}_p$, se define como el conjunto de todos los números $x \in \mathbb{Q}_p$ tales que $|x|_p \leq 1$. Es decir,

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

La condición $|x|_p \leq 1$ implica que su orden p-ádico $v_p(x)$ es mayor o igual que cero. Si pensáramos en un número racional $x = a/b$, estar en $\mathbb{Z}_p$ significa que el denominador b no contiene ningún factor de p. Esto es lógico, comparando con la definición equivalente que de enteros p-ádicos que veíamos antes. Nos ahorraremos la demostración de que definida de esta forma es, efectivamente, un anillo, por la equivalencia de definiciones que viene.

Ejemplo 4.15. Consideremos el número $x = 3 \in \mathbb{Q}_5$. Como 5 no divide a 3, se tiene que $v_5(3) = 0$ y entonces $|3|_5 = 1 \leq 1$. Por lo tanto, $3 \in \mathbb{Z}_5$.

En cambio, si tomamos $x = \frac{1}{5}$, entonces $v_5\left(\frac{1}{5}\right) = -1$ y $\left|\frac{1}{5}\right|_5 = 5$, por lo tanto $\frac{1}{5} \notin \mathbb{Z}_5$, aunque sí está en $\mathbb{Q}_5$.

4.4. Equivalencia de definiciones

A continuación, el teorema que nos relaciona lo que vimos en 3 con la construcción formal definida.

Teorema 4.16. Tenemos las siguientes **expansiones p-ádicas**

1. Todo elemento $x \in \mathbb{Z}_p$ puede ser representado de modo único por una serie

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

donde $0 \leq a_i \leq p-1$. Es decir, tenemos un límite p-ádico

$$x = \lim_{n \to \infty} x_n$$

donde

$$x_n := a_0 + a_1 p + \cdots + a_n p^n.$$

2. En general todo elemento de $\mathbb{Q}_p$ puede ser representado de modo único por una serie

$$x = a_{-m} p^{-m} + a_{-m+1} p^{-m+1} + \cdots + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 + \ldots$$

Demostración. Sabemos que todo elemento de $\mathbb{Q}_p$ puede ser escrito como $\mathfrak{a} = \mathfrak{b} p^k$ para algunos $\mathfrak{b} \in \mathbb{Z}_p$ y $k \in \mathbb{Z}$, asi que 1. implica 2.. La prueba de 1. se puede ver en □

Notar que esta unicidad no se tiene en el caso de los números reales, pues en $\mathbb{R}$, las expresiones decimales $0,99999$ y 1 representan el mismo número real, mientras que si escribimos en base p a una expansión p-ádica, la forma de escribirla es única asegurada por este teorema. Esto es, concretamente, una consecuencia directa del hecho que la norma es no arquimedeana. [5]

Los enteros p-ádicos forman un subconjunto dentro del cuerpo $\mathbb{Q}_p$ que conserva muchas propiedades de los enteros usuales pero con un comportamiento radicalmente distinto desde el punto de vista topológico y algebraico. Son el escenario perfecto para explorar conceptos como divisibilidad, congruencias infinitas y estructuras algebraicas profundas.

5. Aplicaciones en la criptografía

En el paradigma actual de la criptografía moderna existe una tensión constante entre la invención de sistemas de seguridad y la aparición de nuevos métodos para quebrarlos. Desde los cifrados clásicos de sustitución hasta los algoritmos de clave pública que usamos hoy en internet, toda técnica criptográfica está en una carrera contra sus posibles atacantes. Sin embargo, en los últimos años, esta carrera tomó un giro dramático con la amenaza de la computación cuántica. Algunos de los sistemas más extendidos, como RSA o ECC, se basan en problemas que serían relativamente fáciles de resolver por una computadora cuántica suficientemente potente. En 1994, Shor [15] demostró que una computadora cuántica de tamaño polinómico puede factorizar enteros y calcular logaritmos discretos en tiempo polinómico. Esta posibilidad ha impulsado una búsqueda internacional por desarrollar lo que se conoce como criptografía post-cuántica: algoritmos diseñados para resistir incluso ataques con tecnologías del futuro.

En este contexto, las matemáticas puras han vuelto a ser protagonistas. Herramientas que durante décadas parecían confinadas al mundo abstracto como las curvas elípticas, las estructuras algebraicas avanzadas, cuerpos de funciones ahora están en la primera línea de defensa de la información digital. Y entre ellas, los números p-ádicos han comenzado a encontrar un lugar inesperado pero prometedor.

Los números p-ádicos tienen propiedades únicas que los hacen perfectos para ciertas tareas criptográficas: permiten representar información de manera jerárquica, ofrecen operaciones muy eficientes y, en algunos contextos, pueden codificar estructuras complejas con precisión y seguridad. Por eso, algunos investigadores han comenzado a explorar su aplicación en distintos frentes: desde el diseño de cifrados resistentes a la computación cuántica, hasta mejoras en la eficiencia de técnicas como el cifrado homomórfico.

5.1. Los números p-ádicos para la seguridad en sistemas criptográficos

En el contexto actual, donde la seguridad de los sistemas criptográficos clásicos se ve amenazada por el avance de la computación cuántica, algunos investigadores han recurrido a herramientas matemáticas como los números p-ádicos, para diseñar esquemas más resistentes. Este es el caso del trabajo de Cherkaoui, Clarke y Dey. En el artículo "Engel p-adic Supersingular Isogeny-based Cryptography over Laurent series" [2] publicado en junio de 2025, dichos investigadores proponen una nueva forma de construir criptografía postcuántica (algoritmos criptográficos diseñados para ser seguros frente a ataques de computadoras cuánticas) a partir de una mezcla fascinante de herramientas matemáticas: las curvas elípticas, las isogenias supersingulares, los números p-ádicos y unas curiosas secuencias llamadas expansiones de Engel, que se aplican sobre series de Laurent.

La motivación central del trabajo radica en diseñar un esquema de cifrado seguro frente a la amenaza de los futuros ordenadores cuánticos. Como es sabido, algoritmos como el de Shor podrían romper varios sistemas criptográficos actuales. Este no solo propone un enfoque novedoso y elegante desde el punto de vista matemático, sino que lo lleva al terreno práctico con sólidas garantías de eficiencia y seguridad.

5.2. PIE: una codificación p-ádica para el cifrado homomórfico

Se busca que el cifrado homomórfico (una técnica que permite operar sobre datos cifrados sin necesidad de desencriptarlos, manteniendo la privacidad de los datos originales) sea práctico para aplicaciones del mundo real, pero surgen algunos problemas al intentar convertir los datos reales o racionales, que suelen aparecer en contextos científicos o estadísticos, a un formato compatible con esquemas de cifrado que operan sobre números enteros.

Una propuesta reciente, conocida como PIE (p-adic Encoding), responde a este problema utilizando precisamente a los números p-ádicos como puente entre el mundo racional y el cifrado. Este esquema, desarrollado por Harmon, Delavignette, Roy y Silva en su artículo "PIE: p-adic Encoding for High-Precision Arithmetic in Homomorphic Encryption" [7] publicado en 2023, se apoya en una idea elegante: codificar números racionales mediante sus expansiones p-ádicas, transformándolos en enteros con propiedades estructurales muy convenientes para la criptografía.

Los autores presentan implementaciones funcionales que confirman su rendimiento y escalabilidad, lo cual lo convierte en una herramienta prometedora para tareas que requieran cálculos cifrados de alta precisión, como análisis estadísticos o procesamiento de señales en la nube.

5.3. Ataque a criptosistemas y firmas basados en p-adic lattices

Chi Zhang, en su artículo "An Attack on -adic Lattice Public-key Cryptosystems and Signature Schemes" [16] publicado en 2024, presenta un análisis crítico sobre los primeros esquemas de cifrado y firma pública construidos a partir de lattices p-ádicos, introducidos originalmente en 2021. Estos esquemas se fundamentan en problemas de aritmética p-ádica, específicamente el Longest Vector Problem (LVP) y el Closest Vector Problem (CVP), considerados difíciles y adecuados para aplicaciones criptográficas El autor demuestra que, en ciertos campos p-ádicos con propiedades específicas, es posible resolver el problema LVP en tiempo polinómico determinista (la cantidad de tiempo que toma un algoritmo para resolver un problema en una máquina de Turing determinista). Esta mejora, inesperada, permite romper completamente los esquemas de cifrado: se puede descifrar mensajes cifrados sin conocer la clave privada.

Este trabajo aporta una advertencia valiosa: incluso criptosistemas construidos sobre estructuras matemáticas aparentemente robustas pueden fallar si no se consideran ciertos detalles algebraicos. En particular, muestra la importancia de elegir cuidadosamente el tipo de campo p-ádico para garantizar resistencia frente a ataques diseñados con comprensión profunda de su estructura.

6. Conclusión y comentarios finales

El estudio de los números p-ádicos ofrece un enfoque novedoso y prometedor para el desarrollo de códigos correctores de errores y protocolos criptográficos. A lo largo de este trabajo, exploramos el universo de los números p-ádicos desde sus fundamentos hasta algunas de sus aplicaciones e implicancias algebraicas y analíticas. La visión alternativa vista, sobre cómo la distancia p-ádica es distinta a la usual, nos llevó a la construcción de $\mathbb{Q}_p$ como cuerpo, y a $\mathbb{Z}_p$ como su anillo de enteros, descubriendo estructuras que si bien pueden parecer contraintuitivas, se revelan ordenadas.

En definitiva, los números p-ádicos nos invitan a repensar lo que creemos entender sobre los números, la distancia, y la convergencia, demostrando que incluso los objetos más familiares, como los enteros y las fracciones, pueden adquirir una forma completamente distinta cuando se los mira con otros anteojos

Algo que me quedó pendiente, fue el Lema de Hensel, el cual es probablemente la propiedad algebraica más importante de los números p-ádicos. Tanto así, que en todo libro y trabajo académico que encontré en mi búsqueda de bibliografía, el lema de Hensel tenía su propia sección. Sin embargo, la complejidad de su formulación e interpretación superaban demasiado los objetivos de esta monografía. A grandes rasgos, el lema de Hensel es una herramienta que permite "mejorar" soluciones de ecuaciones polinómicas que existen módulo una potencia de un primo p, a soluciones más precisas en los números p-ádicos. En cierto sentido, el lema de Hensel es similar al método de Newton. Ya que ambos se basan en procedimientos iterativos que devuelven una solución aceptable.

Para aquellos que les haya interesado el tema y que se hayan quedado con ganas de profundizar en este, en lo personal, recomiendo tres obras que considero fundamentales: el completo y riguroso libro de Alain M. Robert [12], el influyente y completo libro de Neal Koblitz[11], y el ameno y estimulante trabajo de Salinas Hoyas, Omar David [13]. En ellos se abordan los números p-ádicos con un enfoque detallado desde distintas ramas de la matemática, como el álgebra, la topología y el análisis.

Además, recomiendo ver el increíble video que mencioné del canal *Veritasium en español*, *"Los Matemáticos NO Usan los Números Igual que Nosotros"*[4], el cual fue una gran inspiración para mí sobre como abarcar los temas de una forma divulgativa.

Quiero agradecer a cada lector que haya llegado hasta este punto (ya sea si leyó la monografía completa, si fue por partes o si solo dió un vistazo general y de casualidad está leyendo esta oración), por su tiempo.

Mientras el lector se quede con qué significa ser un número p-ádico y que existen objetos matemáticos (que pueden definirse de forma tan compleja a través del análisis o sumas infinitas que no vemos en el mundo real) tienen aplicaciones directas en la realidad mediante la criptografía, estaré más que satisfecha.

7. Bibliografía

Referencias

[1] George Bachman. *Introduction to p-adic Numbers and Valuation Theory*. New York-London: Academic Press, 1964, págs. ix+173.

[2] I. Cherkaoui, C. Clarke e I. Dey. *Engel p-adic Supersingular Isogeny-based Cryptography over Laurent series*. Cryptology ePrint Archive, Paper 2025/1178. 2025. URL: https://eprint.iacr.org/2025/1178.

[3] Paula Echevarría González. "Introducción a los cuerpos p-ádicos". Trabajo Fin de Grado. Universidad de Oviedo, 2016.

[4] Veritasium Español. *Los Matemáticos NO Usan los Números Igual que Nosotros*. Video de YouTube. 2023. URL: https://www.youtube.com/watch?v=gdNFWlgz-F8 (visitado 03-02-2025).

[5] G. García. "Números p-ádicos". En: *Cursos básicos elENA IV* (2008).

[6] Enrique Gracián. *El libro de los números primos*. Barcelona: Crítica, 2009.

[7] L. Harmon et al. *PIE: Codificación p-ádica para aritmética de alta precisión en cifrado homomórfico*. Archivo de Cryptology ePrint, Artículo 2023/700. 2023. URL: https://eprint.iacr.org/2023/700.

[8] K. Hensel. "New foundations of arithmetic." German. En: *Journal für die Reine und Angewandte Mathematik* 127 (1904), págs. 51-84. ISSN: 0075-4102. DOI: 10.1515/crll.1904.127.51.

[9] K. Hensel. "Über eine neue Begründung der Theorie der algebraischen Zahlen." En: *Jahresbericht der Deutschen Mathematiker-Vereinigung* 6 (1897), págs. 83-88. URL: http://eudml.org/doc/144593.

[10] Heiko Knospe. *The p-adic integers and their topology*. Institute of Computer and Communication Technology (ICCT). Consultado el 19 de julio de 2025. 2019. URL: https://www.nt.th-koeln.de/fachgebiete/mathe/knospe/p-adic/.

[11] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Vol. 58. Graduate Texts in Mathematics. New York: Springer-Verlag, 1984.

[12] Alain M. Robert. *A Course in p-adic Analysis*. Vol. 198. Graduate Texts in Mathematics. New York: Springer-Verlag, 2000. ISBN: 978-1-4612-6517-6.

[13] Omar David Salinas Hoyas. "Números p-ádicos". Disponible en UPCommons. Trabajo académico. Universitat Politècnica de Catalunya, 2025. URL: https://upcommons.upc.edu/handle/2117/398820.

[14] Carlos Marcelo Sánchez. *Lecciones de Álgebra*. Fascículo 6. Ver p. 217. Buenos Aires: Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 2014.

[15] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". En: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, págs. 124-134.

[16] Chi Zhang. *An Attack on p-adic Lattice Public-key Cryptosystems and Signature Schemes*. 2024. arXiv: 2409.08774 [cs.CR]. URL: https://arxiv.org/abs/2409.08774.

Fuentes consultadas

- Duplij, S. (2022). Polyadic Rings of p-Adic Integers. Symmetry, 14(12), 2591.
- Niven, I., Zuckerman, H. S., Montgomery, H. L. (1991).Teoría de números. Limusa.
- Fernando Q. Gouvêa. (1997). p-adic Numbers: An Introduction. Springer.
- Ivorra Castillo, C. (2005). Teoría algebraica de números. Universitat de València.
- Rabanillo Novoa, Fernando (2024). Introducción a los números p-ádicos (Trabajo de fin de grado, Universidad de Valladolid).
- Robert, A. (2000). A Course in p-adic Analysis. New York: Springer-Verlag. (Graduate Texts in Mathematics, 198).
- Salinas Hoyas, O. D. (2025). Números p-ádicos (Trabajo académico, Universitat Politècnica de Catalunya). UPCommons.
- MacTutor History of Mathematics Archive. (n.d.). Kurt Hensel. University of St Andrews. Recuperado el 21 de junio de 2025, de https://mathshistory.st-andrews.ac.uk/Biographies/Hensel/
- Veritas. (2024). ¿Qué es el cifrado RSA? Veritas. Recuperado en julio de 2025 de https://www.veritas.com/es/mx/information-center/rsa-encryption
- TechTarget Editorial. (2024). RSA (Rivest–Shamir–Adleman). SearchSecurity. Recuperado en julio de 2025 de https://www.techtarget.com/searchsecurity/definition/RSA