El diablo de los números

Sección a cargo de

Fernando Chamizo Lorente

¿Y quién es... Miguel Monsalve**?** *El lector curioso puede encontrar la respuesta en esta misma sección, en el volumen 20, número 1, y de paso disfrutar de un interesante artículo. Añadimos que actualmente está realizando el doctorado en el Departamento de Análisis Matemático de la Universidad Complutense de Madrid.*

Una aplicación del análisis p-ádico

por

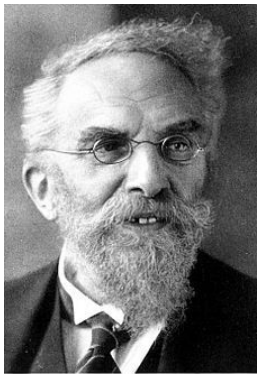
Miguel Monsalve López

1. Bienvenidos al mundo p-ádico

1.1. Para empezar: un poco de historia p-ádica

El artículo seminal en el que fueron introducidos los números p-ádicos, véase [10], data del año 1897 y viene firmado de la mano del matemático alemán Kurt Hensel. En dicho artículo, adoptando ciertas ideas de algunos matemáticos anteriores tales como su mentor Ernst Kummer, Hensel exploraba las analogías aparentes entre las estructuras de $\mathbb{Z}$ y su cuerpo de fracciones $\mathbb{Q}$ con las del anillo de polinomios $\mathbb{C}[X]$ y su cuerpo de fracciones $\mathbb{C}(X)$. Como bien sabrá el lector, tanto $\mathbb{Z}$ como $\mathbb{C}[X]$ son anillos en los que gozamos de factorización única[1]: por un lado, todo entero puede expresarse únicamente como producto de primos

$$m = (\pm 1) \cdot p_1^{n_1} \cdots p_k^{n_k};$$



K. Hensel (1861–1941)

[1] No deja de ser justicia y casualidad histórica que, en ambos casos, los teoremas en los que se describen estas propiedades lleven el calificativo de «fundamental».

mientras que, por otro lado, todo polinomio puede expresarse únicamente en la forma

$$p(X) = \alpha(X - \beta_1)^{n_1} \cdots (X - \beta_k)^{n_k}$$

para ciertos números complejos $\beta_1, \ldots, \beta_k$, a los que denominamos raíces. Así pues, queda patente que el papel que juegan los números primos en $\mathbb{Z}$ es análogo al que juegan los polinomios lineales $X - \beta$ en $\mathbb{C}[X]$.

No obstante, Hensel fue un paso más allá en la búsqueda de estas analogías: es sabido que, dados un polinomio $p(X)$ y un número $\beta \in \mathbb{C}$, podemos expresar (por ejemplo, jugando con los desarrollos de Taylor) el polinomio $p(X)$ en la forma

$$p(X) = \sum_{j=0}^{n} \alpha_j (X - \beta)^j, \quad \text{para ciertos } \alpha_j \in \mathbb{C} \text{ y } n \in \mathbb{N};$$

asimismo, dados un entero positivo m y un primo cualquiera $p \in \mathbb{Z}$, podemos escribir m «en base p», es decir,

$$m = \sum_{j=0}^{n} a_j p^j, \quad \text{para ciertos enteros } 0 \leq a_j \leq p - 1 \text{ y } n \in \mathbb{N}.$$

Es evidente que, salvando las distancias, ambas expresiones son de una naturaleza más que similar; pero, ¿por qué nos son de interés este tipo de desarrollos? Bien, la razón fundamental es que en ambos casos obtenemos información sobre el comportamiento «local» de dichos objetos: por un lado, el desarrollo en potencias de $X - \beta$ nos revela cómo se comporta $p(X)$ cerca de β, es decir, si $p(X)$ se anula en β (o cuánto le falta para anularse en β) y hasta qué orden; mientras que el desarrollo en potencias de p nos revela si m es divisible entre p (o cuánto le falta para ser divisible entre p) y hasta qué orden.

Del mismo modo, si consideramos potencias negativas de $X - \beta$ o de p, se puede llevar a cabo un tratamiento similar para funciones o números racionales, respectivamente. Veamos: en este caso, dadas una función racional $f(X) \in \mathbb{C}(X)$ y un número $\beta \in \mathbb{C}$, calculando el desarrollo de Laurent, uno puede expresar $f(X)$ en la forma

$$f(X) = \sum_{j=n}^{+\infty} \alpha_j (X - \beta)^j, \quad \text{para ciertos } \alpha_j \in \mathbb{C} \text{ y } n \in \mathbb{Z}.$$

De esta manera, aunque analíticamente la igualdad no sea cierta globalmente, algebraicamente la inmersión de cuerpos $\mathbb{C}(X) \hookrightarrow \mathbb{C}((X - \beta))$ está perfectamente definida. Por supuesto, este desarrollo de Laurent sigue otorgándonos información relativa al comportamiento local de $f(X)$ en las proximidades del punto β.

Asimismo, como anticipábamos, un tratamiento análogo es viable para números racionales; esto es, dados $x \in \mathbb{Q}$ y un primo $p \in \mathbb{Z}$, existe un único desarrollo de la forma

$$x = \sum_{j=n}^{+\infty} a_j p^j, \quad \text{para ciertos enteros } 0 \leq a_j \leq p - 1 \text{ y } n \in \mathbb{Z}.$$

A dicha expresión se la conoce como **desarrollo *p*-ádico de *x*** y, evidentemente, continúa revelándonos qué papel juegan las potencias de p a la hora de confeccionar el número racional x.

Por ejemplo, veamos qué desarrollo resultaría con $x = 1/11$ y $p = 3$: antes de nada, puesto que ni 1 ni 11 son divisibles entre 3, el primer término que aparecerá será el de la potencia $3^0 = 1$; así pues, lo único que necesitamos es encontrar el $a_0 \in \{0, 1, 2\}$ de modo que $\frac{1}{11} - a_0 = 3 \cdot (\text{otra fracción})$; pero esto es equivalente a resolver la ecuación $1 - 11a_0 \equiv 0$ mód 3, que, despejando, nos lleva a $a_0 = 2$ y

$$\frac{1}{11} = 2 + 3 \cdot \frac{(-7)}{11}.$$

Repitiendo la misma metodología, llegamos a que $a_1 = 1$ y, de nuevo, restando,

$$\frac{1}{11} = 2 + 1 \cdot 3 + 3^3 \cdot \frac{(-2)}{11},$$

con lo que, además, vemos que $a_2 = 0$. Una vez más, si repetimos lo anterior, llegamos a que $a_3 = 2$ y

$$\frac{1}{11} = 2 + 1 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + 3^4 \cdot \frac{(-8)}{11}.$$

Y así, indefinidamente, calculando potencias de 3 cada vez mayores, obtendríamos el desarrollo 3-ádico de 1/11.

Como ocurría con las funciones racionales, volvemos a sufrir problemas (en el sentido usual) con la convergencia de esta última serie, pues, como observará el lector, el «término de error» que obtenemos es cada vez mayor; sin embargo, algebraicamente, todo guarda perfecto sentido.

Tranquilo, lector, que tras esta puesta en escena inicial, en los siguientes apartados analizaremos más pormenorizadamente el álgebra de los p-ádicos y formalizaremos la convergencia de estas series.

1.2. Los rudimentos de los números p-ádicos

Hay diversas maneras de introducir formalmente los números p-ádicos. Quizás la más adecuada para el lector que se enfrente por vez primera a ellos sea la siguiente: dado p un número primo cualquiera, consideremos todas las sucesiones (recalco, ¡sucesiones!) de la forma

$$(x_0, x_1, x_2, \ldots), \quad \text{donde } x_j \in \mathbb{Z}/p^{j+1}\mathbb{Z}, \tag{1}$$

que sean «consistentes» en el siguiente sentido: para todo par de naturales $k \geq j$ debe cumplirse $x_k \equiv x_j \mod p^{j+1}$. A este conjunto se lo conoce como **enteros *p*-ádicos** y se denota por $\mathbb{Z}_p$. Por ejemplo, $(2, 5, 5, 5, 86, 86, \ldots)$ define un entero 3-ádico, mientras que $(1, 0, 1, 0, \ldots)$ no es un entero 2-ádico. Existe una inmersión natural $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ dada por $x \mapsto (x \mod p, x \mod p^2, x \mod p^3, \ldots)$. Además, la imagen de $\mathbb{N}$ por dicha aplicación se corresponde con aquellas sucesiones que sean estacionarias; así, por ejemplo, 47 se representa en $\mathbb{Z}_2$ como $(1, 3, 7, 15, 15, 47, 47, 47, \ldots)$.

Más que una construcción curiosa, los p-ádicos adquieren una entidad propia al estudiar sus propiedades algebraicas. Por ejemplo, es sencillo comprobar que con la suma y el producto definido coordenada a coordenada, $\mathbb{Z}_p$ adquiere estructura de anillo conmutativo unitario cuyas unidades son, respectivamente, $0 \coloneqq (0,0,\ldots)$ y $1 \coloneqq (1,1,\ldots)$. Cierto es que, por el momento, éstas no parecen propiedades especialmente reseñables. No obstante, si además atendemos a la hipótesis sobre la primalidad de p, puede verse que $\mathbb{Z}_p$ es un dominio de integridad; afinando algo más, se deduce que $\mathbb{Z}_p$ es de hecho un dominio de factorización única cuyo único elemento irreducible resulta ser $(0,p,p,\ldots)$; y afinando otro poco más, llegamos a que $\mathbb{Z}_p$ resulta ser un dominio de ideales principales generados respectivamente por los elementos de la forma $(0,p,p,\ldots)$, $(0,0,p^2,p^2,\ldots)$, $(0,0,0,p^3,p^3,\ldots)$,…, que, vía la inmersión $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ que describimos al inicio del apartado, se corresponden con los enteros p, p^2, p^3,…; es por ello que, en lo que sigue, denotaremos a dichos ideales mediante $p\mathbb{Z}_p$, $p^2\mathbb{Z}_p$, $p^3\mathbb{Z}_p$,…

Así pues, tras lo expuesto, es inmediato deducir que el retículo de ideales de $\mathbb{Z}_p$ no es sino (todas las inclusiones de ideales son propias)

$$\mathbb{Z}_p \supset p\mathbb{Z}_p \supset p^2\mathbb{Z}_p \supset p^3\mathbb{Z}_p \supset \cdots \supset \{0\}. \tag{2}$$

Además, es posible inferir la estructura algebraica explícita de los cocientes residuales:

$$p^m\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^{n-m}\mathbb{Z}, \qquad \text{para enteros } n \geq m \geq 0.$$

Bien, lector, vista y entendida el álgebra de los enteros p-ádicos, nos asalta la duda lógica: ¿qué relación guarda esta construcción con lo visto en el apartado 1.1? Es relativamente inmediato comprobar que existe una correspondencia entre los elementos de $\mathbb{Z}_p$, tal y como los hemos descrito en (1), y las series formales (hago hincapié en el calificativo «formales») del tipo

$$\sum_{j=0}^{\infty} a_j p^j, \quad \text{donde } a_j \in \mathbb{Z}/p\mathbb{Z}. \tag{3}$$

Un ejemplo de dicha correspondencia sería el número 5-ádico

$$(2, 22, 97, 222, 1472, \ldots) \quad \longmapsto \quad 2 + 4\cdot 5 + 3\cdot 5^2 + 1\cdot 5^3 + 2\cdot 5^4 + \cdots .$$

Note, lector, que para efectuar dicho cálculo basta con ir restando entradas consecutivas de la sucesión y dividir por potencias sucesivas del primo en cuestión, 5 en nuestro caso.

Inevitablemente, la notación en (3) nos traslada de nuevo al juego que llevamos a cabo al final del apartado 1.1 para calcular el desarrollo 3-ádico de $1/11$. Y es que ésta es otra posible definición de los enteros p-ádicos, el anillo de todas las series formales de la forma

$$\mathbb{Z}_p \coloneqq \left\{ \sum_{j=0}^{\infty} a_j p^j : a_j \in \mathbb{Z}/p\mathbb{Z} \right\};$$

no obstante, si se ha preferido usar la definición mediante sucesiones es porque deducir la mayoría de las propiedades algebraicas de $\mathbb{Z}_p$ (o incluso, llevar a cabo algunos cálculos explícitos sencillos tales como sumas, productos o divisiones) es, en mi opinión, más sencillo a partir de la notación (1). Sin embargo, la notación mediante series formales también guarda sus ventajas: por un lado, es más intuitiva y conecta de manera inmediata y transparente con las ideas germinales de los números p-ádicos; y por otro lado, como veremos a continuación, se puede extender a...

Es el momento de definir $\mathbb{Q}_p$, el cuerpo de los **racionales *p*-ádicos**, que no es sino el cuerpo de fracciones de $\mathbb{Z}_p$ (recordemos que $\mathbb{Z}_p$ era un dominio de integridad). Convénzase, lector, de que los únicos denominadores patológicos en $\mathbb{Z}_p$ son los elementos divisibles entre p (observe de nuevo, si fuera necesario, el retículo de ideales de $\mathbb{Z}_p$ que describimos en (2)), es decir, aquéllos para los que $a_0 = 0$:

$$a_1 p + a_2 p^2 + a_3 p^3 + a_4 p^4 + \cdots, \quad a_j \in \mathbb{Z}/p\mathbb{Z}.$$

Por lo que es posible dar una definición alternativa de los racionales p-ádicos sin más que «añadir» $1/p$ al anillo $\mathbb{Z}_p$; esto es, $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$. Este hecho nos permite rescatar la notación en (3) que usábamos en $\mathbb{Z}_p$ para representar elementos de $\mathbb{Q}_p$:

$$\mathbb{Q}_p = \left\{ \sum_{j=m}^{+\infty} a_j p^j : m \in \mathbb{Z},\ a_j \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

De la aplicación $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ que vimos anteriormente, se deduce asimismo la existencia de la inmersión $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$; así pues, por ejemplo,

$$\frac{5}{14} \underset{\mathbb{Q}_7}{\hookrightarrow} 6 \cdot 7^{-1} + 3 + 3 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^3 + \cdots.$$

De hecho, a colación de este último ejemplo, no es demasiado complicado observar que las expansiones p-ádicas que se corresponden con números racionales son aquéllas cuyos coeficientes a_j son periódicos a partir de alguna potencia; por ejemplo,

$$\frac{7}{8} \underset{\mathbb{Q}_3}{\hookrightarrow} 2 + 0 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 1 \cdot 3^4 + \cdots,$$
$$\frac{77}{18} \underset{\mathbb{Q}_7}{\hookrightarrow} 0 + 1 \cdot 7 + 5 \cdot 7^2 + 2 \cdot 7^3 + 0 \cdot 7^3 + 5 \cdot 7^4 + 2 \cdot 7^5 + 0 \cdot 7^6 + \cdots.$$

1.3. Un nexo entre lo discreto y lo continuo

El principal objetivo del presente apartado es el de acabar de dar una base sólida a toda la teoría que hemos visto durante las primeras páginas. Para ello, estudiaremos extensivamente la topología que subyace tras los números p-ádicos.

Definamos sobre $\mathbb{Z}$ una manera especial de medir, el **valor absoluto *p*-ádico**:

$$|x|_p \coloneqq \begin{cases} p^{-\mathrm{v}_p(x)} & \text{si } x \neq 0; \\ 0 & \text{si } x = 0; \end{cases} \quad \text{para } p \text{ primo y } x \in \mathbb{Z}; \tag{4}$$

donde la aplicación $\mathrm{v}_p(x)$, denominada **valoración *p*-ádica**, denota al máximo exponente de p que divide a x. Así, por ejemplo, $|6|_3 = 3^{-1}$ o $|49|_7 = 7^{-2}$. Atendiendo a las propiedades de la valoración p-ádica,

$$\begin{aligned} \mathrm{v}_p(xy) &= \mathrm{v}_p(x) + \mathrm{v}_p(y) \quad \text{para todo } x, y \in \mathbb{Z}, \\ \mathrm{v}_p(x+y) &\geq \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\} \quad \text{para todo } x, y \in \mathbb{Z}, \end{aligned} \tag{5}$$

no es difícil comprobar que $|\cdot|_p$ cumple las propiedades que definen a un valor absoluto si y sólo si p es primo: una muestra de la necesidad de la primalidad de p es que $|\cdot|_p$ dejaría de ser multiplicativo en el caso en que p fuese un número compuesto, verbigracia,

$$1 = |2|_6 \cdot |3|_6 \neq |2 \cdot 3|_6 = \frac{1}{6}.$$

Al igual que con el valor absoluto usual, podemos aprovechar $|\cdot|_p$ para definir la **norma *p*-ádica** de la manera lógica, $\|\cdot\|_p := |\cdot|_p$. Y ahora, para el lector que aún no se lo haya preguntado, ¿qué mide exactamente la norma p-ádica? En contraposición a la norma euclídea (a la que estamos ciegamente acostumbrados), la norma p-ádica no mide distancias sino cuánto es de divisible un número entre el primo p en el siguiente sentido: cuanto mayor sea la potencia de p que divida al número, menor será su norma. Además, la norma p-ádica satisface una propiedad que la distingue de la norma euclídea: cumple una versión muy particular de la desigualdad triangular, la llamada **desigualdad ultramétrica**, consecuencia directa de la propiedad (5):

$$\|x+y\|_p \leq \max\{\|x\|_p, \|y\|_p\} \text{ para todo par } x, y \in \mathbb{Z}.$$

A las normas que cumplen la desigualdad ultramétrica se las dice **no arquimedianas** (ya que, con dichas normas, la propiedad arquimediana[2] deja de ser válida).

A partir de la norma p-ádica podemos definir una topología métrica muy particular sobre $\mathbb{Z}$, que resulta estar fuertemente relacionada con ciertas propiedades aritméticas de los enteros, ¿acaso ésta no es una idea fascinante? Pero ahora viene lo mejor, ¿qué ocurre si consideramos la compleción de $\mathbb{Z}$ mediante la norma p-ádica? Bien, en tal caso, estaríamos considerando todos los límites de sucesiones de enteros que fueran congruentes módulo p^n para n arbitrariamente grande, ¡pero, lector, vuelva al comienzo del apartado 1.2 y verá que ésta es justamente la definición de $\mathbb{Z}_p$! Así pues, lector, si todavía andaba preguntándose en qué sentido (topología) convergían las expansiones p-ádicas de los apartados anteriores 1.1 y 1.2, he aquí su tan ansiada respuesta: los «términos de error» que aparecían en tales series, y que con ojos euclídeos se hacían más y más grandes, ahora con ojos p-ádicos se hacen cada vez más y más pequeños. De esta manera, hemos conseguido que todo lo que antes tenía sentido algebraicamente, ahora también lo tenga analíticamente.

[2] La **propiedad arquimediana**, estudiada normalmente durante los cursos básicos de cálculo para números reales, aunque extrapolable a otras estructuras algebraicas tales como grupos o anillos, dice que dados dos números reales cualesquiera a y b, existe un entero n de modo que $|na| > |b|$.

Por supuesto, la norma p-ádica se extiende a $\mathbb{Z}_p$ de la manera canónica: si $b \in \mathbb{Z}_p$ es el límite de la sucesión de Cauchy[3] $(b_n)_{n\geq 0} \subset \mathbb{Z}$, entonces

$$\|b\|_p := \lim_{n\to\infty} \|b_n\|_p.$$

Así, por ejemplo, una posible sucesión de Cauchy (compruébelo, si no me cree) que converge a $b = 5 \cdot 7^2 + \sum_{j=3}^{\infty} 7^j \in \mathbb{Z}_7$ es

$$\begin{aligned} b_0 = 245, \quad b_1 = 588, \quad b_2 = 2989, \ldots \\ b_n = 5 \cdot 7^2 + \sum_{j=3}^{n+2} 7^j \in \mathbb{Z}, \quad \text{para } n \geq 1; \end{aligned} \tag{6}$$

pero ahora, teniendo en cuenta que $\|b_n\|_7 = 1/49$ para todo $n \geq 0$, se deduce que $\|b\|_7 := \lim_{n\to\infty} \|b_n\|_7 = 1/49$. De hecho, remedando (o mejor dicho, formalizando) este argumento para el caso general puede deducirse el siguiente resultado.

Proposición 1.1. *Sea* $a = \sum_{j=0}^{\infty} a_j p^j \in \mathbb{Z}_p$ *para cierto* p *primo; entonces,*

$$\|a\|_p = p^{-\min\{j\,:\,a_j \neq 0\}}.$$

Desde luego, reconozca, lector, que todo lo expuesto en los párrafos anteriores es, cuando menos, sorprendente: $\mathbb{Z}_p$, que *a priori* lo habíamos construido a partir de sucesiones de enteros, es en realidad un espacio métrico completo con la norma $\|\cdot\|_p$ en el que podremos hacer análisis de un modo similar al que lo hacemos en $\mathbb{R}$.

A partir de la propiedad multiplicativa, podemos ampliar el dominio de definición de la norma p-ádica a todo $\mathbb{Q}_p$. Aunque es válido extender directamente la norma p-ádica de $\mathbb{Z}_p$ a $\mathbb{Q}_p$, tomemos el camino «largo» por ser más explícito: la idea es comenzar definiendo la norma p-ádica en todo $\mathbb{Q}$, en vez de sólo en $\mathbb{Z}$ como hacíamos en (4), para luego tomar la compleción mediante $\|\cdot\|_p$. Si se ha preferido dar el rodeo definiendo en primer lugar la norma p-ádica en $\mathbb{Z}$ es porque intuir que $\mathbb{Z}_p$ es la compleción de $\mathbb{Z}$ mediante la norma $\|\cdot\|_p$ es relativamente sencillo a partir de la definición (1).

Sin más dilación, de nuevo la norma p-ádica viene definida como

$$\|x\|_p := \begin{cases} p^{-\mathrm{v}_p(x)} & \text{si } x \neq 0; \\ 0 & \text{si } x = 0; \end{cases} \quad \text{para } p \text{ primo y } x \in \mathbb{Q};$$

en este caso, la valoración p-ádica $\mathrm{v}_p(x)$ se define como el único entero

$$\frac{a}{b} = p^{\mathrm{v}_p(a/b)} \cdot \frac{a'}{b'}$$

[3]Desde luego, dado un $b \in \mathbb{Z}_p$ existen infinitas sucesiones de Cauchy en $\mathbb{Z}$ que convergen a b. Por supuesto, ni la existencia ni la unicidad de b ni su norma se ven comprometidas por la elección de una sucesión u otra (pues, en tal caso, estaríamos considerando sucesiones de Cauchy equivalentes).

para el que a', b' son coprimos con p. Por supuesto, las definiciones actuales son consistentes con aquéllas que vimos en (4); así pues, $\|\frac{7}{242}\|_{11} = 121$ o $\|\frac{19}{162}\|_3 = 81$. Asimismo, las propiedades satisfechas por la norma p-ádica que describimos anteriormente continúan vigentes, es decir, sigue cumpliendo la desigualdad ultramétrica y siendo no arquimediana.

Como de seguro intuye el lector, de nuevo sucede que la compleción de $\mathbb{Q}$ mediante la norma $\|\cdot\|_p$ resulta ser $\mathbb{Q}_p$, el cuerpo de los racionales p-ádicos. Un ejemplo similar al visto en (6) y que elucide este hecho podría ser

$$b_{-2} = \frac{2}{25}, \quad b_{-1} = \frac{12}{25}, \quad b_0 = \frac{62}{25}, \quad b_1 = \frac{312}{25}, \dots$$
$$b_n = \sum_{j=-2}^{n} 2 \cdot 5^j \in \mathbb{Q}, \quad \text{para } n \geq 0,$$

que converge al racional 5-ádico $\frac{-1}{50} \underset{\mathbb{Q}_5}{\hookrightarrow} \sum_{j=-2}^{\infty} 2 \cdot 5^j$. Asimismo, si tomásemos normas p-ádicas en el ejemplo anterior, se inferiría (o al menos se intuiría) que la proposición 1.1 sigue siendo cierta en $\mathbb{Q}_p$.

Para acabar, es razonable que nuestra curiosidad se haga la siguiente pregunta: ¿existe algún valor absoluto en $\mathbb{Q}$, además del usual y los p-ádicos? La respuesta es (esencialmente) negativa.

Teorema 1.2 (Ostrowski, 1916). *Todo valor absoluto no trivial sobre $\mathbb{Q}$ es equivalente al usual o a $|\cdot|_p$ para algún primo p.*

Note, lector, que este último teorema nos caracteriza todas y cada una de las posibles compleciones de $\mathbb{Q}$: por un lado, la única compleción arquimediana es $\mathbb{R}$ (¡ahora resulta que la norma rara es la euclídea...!); mientras que el resto de compleciones vienen dadas por los diferentes $\mathbb{Q}_p$, una por cada p primo. Además, la elección que hemos tomado de la normas p-ádicas nos lleva a la elegantísima identidad

$$\|x\| \cdot \prod_p ||x||_p = 1, \quad \text{para todo } x \in \mathbb{Q} \setminus \{0\}. \tag{7}$$

A cada una de las (clases de equivalencias de) normas factibles en $\mathbb{Q}$ se las denomina **lugares**; por consiguiente, si adoptamos el criterio usual de asignar al valor absoluto usual el lugar ∞, podemos resumir el teorema de Ostrowski sucintamente mediante la igualdad

$$\mathcal{M}_{\mathbb{Q}} = \{\infty, 2, 3, 5, 7, \dots\},$$

donde $\mathcal{M}_{\mathbb{Q}}$ denota el conjunto de lugares posibles en $\mathbb{Q}$, y reescribir la identidad (7) como

$$\prod_{\nu \in \mathcal{M}_{\mathbb{Q}}} \|x\|_\nu = 1, \quad \text{para todo } x \in \mathbb{Q} \setminus \{0\}.$$

2. Números p-ádicos y polinomios

No es de extrañar que, por su estructura, los números p-ádicos fueran empleados históricamente como una herramienta en el estudio de las soluciones enteras y racionales de ecuaciones algebraicas. Así pues, sea $Q(X) = 0$ una ecuación polinómica con coeficientes en $\mathbb{Z}$ e imaginemos que queremos estudiar simultáneamente todas las soluciones módulo $p, p^2, p^3, \ldots$, para p un número primo cualquiera.

Por un lado, es evidente que dada una solución de $Q(X) \equiv 0 \mod p^n$ para cierto $n \geq 1$, como $Q(X)$ está compuesta por sumas y productos, también tendremos una solución módulo p^j para todos los $1 \leq j \leq n$ que, además, serán congruentes con la solución inicial. Sin embargo, lo que ya no resulta tan evidente es que en algunos casos también es posible llevar a cabo el método inverso; esto es, dada una solución de $Q(X) \equiv 0 \mod p$, la podremos «elevar» de manera única y consistente para así obtener soluciones de $Q(X) \equiv 0 \mod p^n$, para $n \geq 1$ arbitrario. Por ejemplo, observe, lector, que la ecuación $X^2 + 1 = 0$ tiene por solución $x_0 = 3$ módulo 5, que puede elevarse de manera única a la solución $x_1 = 3 + 3 \cdot 5 = 18$ módulo 25, que a su vez puede elevarse de manera única a la solución $x_2 = 3 + 3 \cdot 5 + 2 \cdot 5^2 = 68$ módulo 125, y así sucesivamente…, obteniendo de este modo ¡una solución 5-ádica de la ecuación!

$$x = 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \cdots \in \mathbb{Z}_5.$$

Lector, si atiende a los pormenores de este procedimiento, llegará a la conclusión de que está frente a la versión p-ádica del método de Newton. Conocido como **lema de Hensel**, este método es la herramienta principal a la hora de resolver ecuaciones polinómicas en el universo p-ádico. Su enunciado reza así.

Teorema 2.1 (Lema de Hensel). *Sea $Q(X) \in \mathbb{Z}_p[X]$. Supongamos que existe $a_0 \in \mathbb{Z}/p\mathbb{Z}$ que satisface simultáneamente $Q(a_0) = 0$ y $Q'(a_0) \neq 0$. Entonces, existe un único $a \in \mathbb{Z}_p$ tal que:*

- $a \equiv a_0 \mod p$;
- $Q(a) \equiv 0 \mod p^n$ *para todo entero* $n \geq 1$.

De este modo, los números p-ádicos se convierten, amén de un objeto matemático con su propia entidad, en una notación idónea para hablar de las soluciones enteras de ecuaciones algebraicas.

Otro tema que involucra p-ádicos y polinomios merece ser comentado: suponga, lector, que dada una ecuación $Q(\boldsymbol{X}) = 0$, para $Q \in \mathbb{Q}[X_1, \ldots, X_n]$, existe una solución racional $\boldsymbol{q}$, a la que denominaremos solución global. Teniendo en cuenta que $\mathbb{Q}$ está incluido en cada una de sus compleciones, deducimos que $\boldsymbol{q}$ da lugar asimismo a soluciones tanto en $\mathbb{R}$ como $\mathbb{Q}_p$ para cada primo p, a las que denominaremos soluciones **locales**. El **principio local-global** se pregunta en qué casos ocurre también lo contrario; es decir, que la existencia de soluciones en cada uno de los $\mathbb{Q}_p$ y en $\mathbb{R}$ implique la existencia de soluciones racionales.

Este intento de reflejar soluciones globales a partir de las locales raramente tiene éxito. Uno de los pocos casos en el que sí funciona este esquema es el siguiente.

Teorema 2.2 (Teorema de Hasse-Minkowski, [7]). *Sea $Q(\boldsymbol{X}) \in \mathbb{Q}[X_1, \ldots, X_n]$ una forma cuadrática (homogénea). Entonces, $Q(\boldsymbol{X}) = 0$ tiene una solución no trivial en $\mathbb{Q}$ si y sólo si tiene una solución no trivial en $\mathbb{R}$ y en cada $\mathbb{Q}_p$.*

Aunque existen generalizaciones de este resultado, verbigracia, considerando otro cuerpo de números cualquiera $\mathbb{K}$ en lugar de $\mathbb{Q}$, lo cierto es que, como adelantábamos unas cuantas líneas más arriba, el principio local-global escasas veces es aplicable. Así, por ejemplo, Selmer ([13]) demostró la existencia de una forma cúbica, más concretamente $3X_1^3 + 4X_2^3 + 5X_3^3$, con raíces no triviales en $\mathbb{R}$ y cada $\mathbb{Q}_p$, pero sin ninguna raíz en $\mathbb{Q}$.

2.1. El análogo p-ádico de los números complejos

Quizás el lema de Hensel y tanto juego con polinomios haya provocado en el lector la inquietud de saber si, a diferencia de $\mathbb{R}$, los cuerpos $\mathbb{Q}_p$ son o no algebraicamente cerrados. La respuesta es negativa: $\mathbb{Q}_p$ no es algebraicamente cerrado para ningún primo p. En vez de dar una demostración, dilucidemos este hecho con un ejemplo explícito: consideremos el polinomio $X^2 - 2 \in \mathbb{Q}_5[X]$; atendiendo al criterio de irreducibilidad de Gauss (pues, recuerde, $\mathbb{Z}_5$ es un dominio de factorización única y $\mathbb{Q}_5$ su cuerpo de fracciones) deducimos que, de tener raíces, éstas deben pertenecer a $\mathbb{Z}_5$; sin embargo, esto no es posible porque ni siquiera existen raíces módulo 5.

Colegir la existencia de $\overline{\mathbb{Q}_p}$, la clausura algebraica de $\mathbb{Q}_p$, no supone ningún reto complicado, pues el lema de Zorn implica la existencia de la clausura algebraica de cualquier cuerpo; el trabajo espinoso es dotar a $\overline{\mathbb{Q}_p}$ con una estructura topológica y algebraica consistente con la dada anteriormente a $\mathbb{Q}_p$. Por supuesto, en nuestro ascenso a $\mathbb{C}_p$, el análogo p-ádico de los números complejos (que, al final de este apartado, veremos que no es lo mismo que $\overline{\mathbb{Q}_p}$), no detallaremos más que los puntos necesarios para el debido entendimiento del resto del artículo.

Así pues, en lo que sigue, sea $K/\mathbb{Q}_p$ una extensión algebraica finita, $[K : \mathbb{Q}_p] = n$ el grado de dicha extensión y $\alpha \in K$ un elemento cualquiera cuyo polinomio (mónico) mínimo es

$$p(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0 \in \mathbb{Q}_p[X],$$

para cierto $m = [\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] \leq n$. Entonces, extendemos la norma p-ádica de $\mathbb{Q}_p$ a K mediante

$$\|\alpha\|_p \coloneqq \|a_0\|_p^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]}, \quad \text{para } \alpha \in K.$$

Créame, lector, si le afirmo que esta definición de $\|\cdot\|_p$ en $\overline{\mathbb{Q}_p}$ es la única extensión consistente con la norma p-ádica que escogimos en $\mathbb{Q}_p$; además, ésta sigue satisfaciendo la propiedad más importante de la norma p-ádica, a saber, es no arquimediana.

Pero el trabajo más escabroso se presenta con el estudio de las propiedades algebraicas. En general, el esquema es el siguiente[4]: la clausura entera[5] de $\mathbb{Z}_p$ en K

[4]Tenga en mente, lector, la aducción que seguimos durante la construcción de $\mathbb{Z}_p$ al inicio del apartado 1.2.

[5]La clausura entera de $\mathbb{Z}_p$ en K es el conjunto de todos los $\alpha \in K$ que son raíces de un polinomio mónico y con coeficientes en $\mathbb{Z}_p$. Forma un (sub-)anillo con las operaciones usuales de suma y producto.

resulta ser el conjunto

$$\mathcal{O}_K \coloneqq \{\alpha \in K : \|\alpha\|_p \leq 1\}.$$

Razonando de forma similar al caso de $\mathbb{Z}_p$, se infiere que $\mathcal{O}_K$ es, en primer lugar, un anillo local cuyo ideal maximal es

$$\mathfrak{m}_K \coloneqq \{\alpha \in K : \|\alpha\|_p < 1\}$$

y, en segundo lugar, un dominio de ideales principales generados respectivamente por las potencias de cierto elemento $\pi \in \mathfrak{m}_K$ al que denominaremos **uniformizante** y que satisface las siguientes dos propiedades:

- $\mathfrak{m}_K = \pi\mathcal{O}_K$;
- π tiene norma máxima en $\mathfrak{m}_K$ y ésta es $\|\pi\|_p = p^{-1/e}$ para cierto $e \mid n$.

Por consiguiente, vuelve a deducirse que el retículo de ideales de $\mathcal{O}_K$ es

$$\mathcal{O}_K \supset \pi\mathcal{O}_K \supset \pi^2\mathcal{O}_K \supset \pi^3\mathcal{O}_K \supset \cdots \supset \{0\}$$

y el cuerpo residual es $\mathcal{O}_K/\mathfrak{m}_K \simeq \mathbb{F}_{p^f}$, para cierto $f \mid n$, donde $\mathbb{F}_q$ denota, y denotará de aquí en adelante, al cuerpo finito con q elementos. De modo que podremos recuperar la notación π-ádica en K:

$$\alpha = \sum_{j=m}^{\infty} a_j \pi^j, \text{ para ciertos } m \in \mathbb{Z},\ a_j \in \mathbb{F}_{p^f}.$$

Bien, pero ¿qué información pretenden revelarnos los enteros positivos e y f? Resulta que $n = ef$; por un lado, f nos está diciendo cómo de grande es el cuerpo de coeficientes en el desarrollo π-ádico; mientras que e nos muestra en cuántos «trozos» se ha escindido p. Así pues, existen dos tipos de extensiones algebraicas especiales: aquéllas para las que $e = n$ y $f = 1$, calificadas como **totalmente ramificadas**, por ejemplo, $\mathbb{Q}_5\left(\sqrt{5}\right) \coloneqq \mathbb{Q}_5[X]/\left\langle X^2 - 5\right\rangle$; y aquéllas para las que $e = 1$ y $f = n$, en las que p sigue siendo uniformizante, calificadas como **no ramificadas**, por ejemplo, $\mathbb{Q}_5\left(\sqrt{-3}\right) \coloneqq \mathbb{Q}_5[X]/\left\langle X^2 + 3\right\rangle$.

Para acabar con la sección, apuntemos el desafortunado hecho de que $\overline{\mathbb{Q}_p}$ no es un cuerpo completo. Con el propósito de evitar problemas y poder hacer análisis (por ejemplo, para definir funciones mediante series de potencias), se procede a completar $\overline{\mathbb{Q}_p}$ mediante sucesiones de Cauchy para obtener $\mathbb{C}_p$, el menor cuerpo simultáneamente algebraicamente cerrado y completo que contiene a $\mathbb{Q}_p$.

3. Un poco de análisis p-ádico

Tras «haber construido»[6] $\mathbb{C}_p$, ahora llega el magnífico momento de ensuciarse las manos y empezar a trabajar en él. El objeto principal de estudio serán las **funciones**

[6]Permítanme esta pequeña trampa. Soy consciente de que $\mathbb{C}_p$ es algo difícil de imaginar, pero el espacio apremia.

analíticas *p*-ádicas, expresiones de la forma

$$f(X) = \sum_{j=0}^{\infty} a_j (X-a)^j, \tag{8}$$

para $(a_j)_{j\geq 0}$ una sucesión cualquiera en $\mathbb{C}_p$ y $a \in \mathbb{C}_p$. Éstas definirán funciones $f : \mathbb{C}_p \longrightarrow \mathbb{C}_p$ que albergarán tanto numerosos paralelismos como diferencias significativas con respecto a las funciones holomorfas usuales de variable compleja. La causante de las diferencias y peculiaridades del análisis p-ádico será, por supuesto, la topología definida mediante $\|\cdot\|_p$ y, más precisamente, la propiedad no-arquimediana.

Un ejemplo preeminente de estas diferencias entre los mundos de $\mathbb{C}$ y $\mathbb{C}_p$ es la ausencia de convergencia condicional en el caso p-ádico:

Teorema 3.1. *Sea $(a_j)_{j\geq 0}$ una sucesión en $\mathbb{C}_p$. Entonces, la serie $\sum_{j\geq 0} a_j$ es convergente si y sólo si $\|a_j\|_p \underset{j\to\infty}{\longrightarrow} 0$.*

La demostración de la implicación «⇒» es análoga a la de variable compleja. La implicación «⇐» se sigue de aplicar la desigualdad ultramétrica en $(\star)$ para obtener

$$\|S_N - S_M\|_p = \left\| \sum_{j=M+1}^{N} a_j \right\|_p \underset{(\star)}{\leq} \max_{M+1\leq j\leq N} \|a_j\|_p ,$$

de donde se deduce que, si $\|a_j\|_p$ converge a 0, la sucesión de sumas parciales $(S_N)_{N\geq 0}$ es de Cauchy y, por tanto, convergente.

Paralelismos hay muchos: existe toda una plétora de resultados de variable compleja que pueden traducirse (con mayor o menor precisión) al lenguaje p-ádico; así pues, conocidos teoremas como Cauchy-Hadamard, Picard, Weierstrass[7]... tienen sus equivalentes p-ádicos. Un par de ejemplos de notable interés podrían ser:

Teorema 3.2 (Teorema de Cauchy-Hadamard en $\mathbb{C}_p$). *Sea $f(X) = \sum_{j=0}^{\infty} a_j X^j$ una serie de potencias en $\mathbb{C}_p[[X]]$. Definimos su **radio de convergencia** como*

$$R \coloneqq \left(\limsup_{n\to\infty} \sqrt[n]{\|a_j\|_p} \right)^{-1}.$$

Entonces, se cumple:

- *Si $\|x\|_p < R$, la serie $f(x)$ converge.*
- *Si $\|x\|_p > R$, la serie $f(x)$ no converge.*
- *Si $\|x\|_p = R$ y la serie $f(x)$ converge, entonces también lo hace para todo $z \in \mathbb{C}_p$ tal que $\|z\|_p = R$.*

Teorema 3.3 (Teorema pequeño de Picard en $\mathbb{C}_p$). *Sea $f : \mathbb{C}_p \longrightarrow \mathbb{C}_p$ una función entera y no constante. Entonces, f toma todos los valores sobre $\mathbb{C}_p$. Además, si f es una función trascendente, toma cada valor de $\mathbb{C}_p$ un número infinito de veces.*

[7] ¿Cuál de tantos? Por ejemplo, el teorema de preparación de Weierstrass que nos permite factorizar funciones meromorfas en $\mathbb{C}$ dependiendo de la naturaleza de sus ceros y polos.

Como consecuencia de la completitud de $\mathbb{C}_p$, el lector puede y debe permitirse el lujo de calcular límites p-ádicos. Podrá así comprobar que la derivada usual,

$$f'(b) \coloneqq \lim_{X\to b} \frac{f(X)-f(b)}{X-b} \quad \text{para } b \in \mathbb{C}_p,$$

de una serie de potencias como la que aparece en (8) es (¡oh, vaya sorpresa!)

$$f'(X) \coloneqq \sum_{j=1}^{\infty} j a_j (X-a)^{j-1}$$

y que, además, admite exactamente el mismo disco de convergencia que f.

3.1. Ejemplos de funciones analíticas p-ádicas

Sin más que copiar los coeficientes de sus series de potencias (pues no olvidemos que $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{C}_p$), podemos contruir los equivalentes p-ádicos de algunas funciones de variable compleja ya conocidas tales como $\exp(s)$, $\log(1+s)$, $\cos(s)\ldots$ Estos equivalentes p-ádicos satisfarán, en algunos casos, las mismas propiedades que sus parientes de $\mathbb{C}$, por ejemplo, resuelven las mismas ecuaciones diferenciales; sin embargo, en otros aspectos, como puede ser el dominio de convergencia, son radicalmente diferentes. Por ejemplo, definimos la **exponencial *p*-ádica** como

$$\exp_p(X) \coloneqq \sum_{j=0}^{\infty} \frac{X^j}{j!} \in \mathbb{C}_p\left[[X]\right].$$

Recordemos que $\exp(X)$ funcionaba especialmente bien en $\mathbb{C}$: $|1/j!|$ decrecía tan rápido a 0 que la serie de potencias convergía en todo el plano complejo. No obstante, la norma p-ádica no trata de la misma manera a los $j!$ y, por consiguiente, la serie de potencias tendrá un comportamiento radicalmente diferente en $\mathbb{C}_p$. Así pues, aplicando el teorema de Cauchy-Hadamard

$$\begin{aligned}\frac{1}{R} &= \limsup_{j\to\infty} \left\| \frac{1}{j!} \right\|_p^{1/j} = \limsup_{j\to\infty} p^{\mathrm{v}_p(j!)/j} = \limsup_{j\to\infty} p^{\left(\frac{1}{j}\sum_{k=1}^{\infty}\left\lfloor \frac{j}{p^k}\right\rfloor\right)} \\ &= \lim_{j\to\infty}\left(\sup_{m\geq j} p^{\left(\frac{1}{m}\sum_{k=1}^{\infty}\left\lfloor \frac{m}{p^k}\right\rfloor\right)}\right) = \lim_{j\to\infty}\left(\sup_{m\geq \log_p(j)} p^{\left(\frac{p^m-1}{p^m(p-1)}\right)}\right) = p^{1/(p-1)}.\end{aligned}$$

De donde inferimos que el radio de convergencia de la exponencial es $R = p^{-1/(p-1)}$.

Otro ejemplo de notable interés es el del **logaritmo *p*-ádico** (¡no confundir con el logaritmo en base p!), que viene dado mediante la serie de potencias

$$\log_p(1+X) \coloneqq \sum_{j=1}^{\infty} \frac{(-1)^{j+1}}{j} X^j \in \mathbb{C}_p\left[[X]\right].$$

Procediendo como antes, vemos que su radio de convergencia es 1; es decir, ¡el radio de convergencia de $\exp_p(X)$ es menor que el de $\log_p(1+X)$ en el mundo p-ádico!

4. La racionalidad de la función zeta sobre cuerpos finitos

El objetivo que perseguimos en esta sección es dar a conocer y entender (en la medida de lo posible) una aplicación insigne, histórica y matemáticamente hablando, del análisis p-ádico: la demostración de la primera de las conjeturas de Weil. Con ello evidenciamos que, pese a no ser una herramienta muy conocida en algunos círculos matemáticos, los números p-ádicos sí han protagonizado algún momento de gran relevancia en las matemáticas de los siglos anterior y vigente.

4.1. Las conjeturas de Weil

Antes de meternos de lleno en el tema, será necesaria una breve introducción previa: en lo que sigue, X denotará una variedad algebraica proyectiva no singular sobre $\overline{\mathbb{F}_q}$ y definida mediante polinomios con coeficientes en $\mathbb{F}_q$, donde $q = p^r$ es una potencia de un primo p. Motivados por la definición de otras funciones zeta como productos de Euler, podemos definir la **función zeta de la variedad** X como

$$\zeta_X(s) \coloneqq \prod_{\boldsymbol{x}\in X} \left(1 - (\#\mathbb{F}_q(\boldsymbol{x}))^{-s}\right)^{-1}, \quad \text{para } s \in \mathbb{C}, \tag{9}$$

donde $\mathbb{F}_q(\boldsymbol{x})$ denota la menor extensión algebraica de $\mathbb{F}_q$ que contiene a cada una de las coordenadas del punto $\boldsymbol{x} \in X$ y $\#$ el cardinal. Teniendo en cuenta que las extensiones algebraicas de $\mathbb{F}_q$ son de la forma $\mathbb{F}_{q^m}$ para $m \geq 1$, y que éstas tienen q^m elementos, se deduce que $\zeta_X(s)$ define en realidad una serie de Dirichlet que involucra exclusivamente términos de la forma q^{-ms}.

Y el lector se preguntará: «Estupendo, pero ¿qué información relativa a la variedad X puede extraerse de su correspondiente ζ_X?». Espero que el siguiente análisis responda satisfactoriamente a su pregunta: tomando logaritmos en ambos lados de la igualdad en (9) y teniendo en cuenta el desarrollo de Taylor de $\log(1-t)$ se tiene

$$\begin{aligned}\log\left(\zeta_X(s)\right) &= \sum_{\boldsymbol{x}\in X} -\log\left(1 - (\#\mathbb{F}_q(\boldsymbol{x}))^{-s}\right) = \sum_{\boldsymbol{x}\in X}\sum_{m=1}^{\infty} \frac{(\#\mathbb{F}_q(\boldsymbol{x}))^{-ms}}{m} \\ &= \sum_{m=1}^{\infty} \frac{1}{m} \sum_{\boldsymbol{x}\in X} (\#\mathbb{F}_q(\boldsymbol{x}))^{-ms} = \sum_{m=1}^{\infty} \frac{N_m(X)}{m} \cdot q^{-ms},\end{aligned}$$

donde $N_m = N_m(X)$ denota el número de puntos de X cuyas coordenadas pertenecen en su totalidad a la extensión $\mathbb{F}_{q^m}$ (a estos puntos se les denomina $\mathbb{F}_{q^m}$-racionales); con lo que llegamos a la siguiente expresión alternativa para ζ_X:

$$\zeta_X(s) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m(X)}{m} \cdot q^{-ms}\right). \tag{10}$$

Así que, aunque *a priori* no lo pareciese, en realidad ζ_X es una especie de función generatriz que guarda información sobre el número de puntos de X que caen en

cada una de las extensiones $\mathbb{F}_{q^m}$. A partir de la definición (10) podemos calcular rápidamente algunos casos de funciones zeta muy sencillos: por ejemplo, para $\mathbb{P}(\overline{\mathbb{F}_q})$, la variedad algebraica que se corresponde con el polinomio constante e igual a 0, si tenemos en cuenta que $N_m(\mathbb{P}(\overline{\mathbb{F}_q})) = q^m + 1$ se sigue que

$$\zeta_{\mathbb{P}(\overline{\mathbb{F}_q})}(s) = \exp\left(\sum_{m=1}^{\infty} \frac{q^m+1}{m} \cdot q^{-ms}\right) \underset{(\star)}{=} \frac{1}{(1-q^{-s})(1-q^{1-s})},$$

donde en $(\star)$ hemos apelado de nuevo al desarrollo en serie de Taylor de $\log(1-t)$. O, en general, para $\mathbb{P}^d(\overline{\mathbb{F}_q})$ con $d \geq 1$, es sencillo comprobar que

$$\zeta_{\mathbb{P}^d(\overline{\mathbb{F}_q})}(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})\cdots(1-q^{d-s})}. \tag{11}$$

Sin embargo, también es posible entretenerse con otros casos algo más elaborados; le invito, lector, a comprobar que la función zeta del proyectivizado de la hipérbola, es decir, la variedad algebraica definida mediante

$$H \coloneqq \left\{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\overline{\mathbb{F}_q}) \,:\, x_1^2 - x_0^2 = x_2^2\right\},$$

viene dada por

$$\zeta_H(s) = \frac{1}{(1-q^{-s})(1-q^{1-s})}. \tag{12}$$

Las **conjeturas de Weil** surgen históricamente a raíz de una serie de resultados sobre ciertas propiedades que cumplían las funciones zeta de una amplia familia de variedades algebraicas. La historia es como sigue: la primera persona en establecer la definición (9) de función zeta para el caso de curvas algebraicas sobre cuerpos finitos fue Emil Artin en su tesis doctoral, véase [1]; trabajos posteriores de F. K. Schmidt [14] y Helmut Hasse [8] probaban respectivamente la racionalidad y el análogo a la hipótesis de Riemann para curvas elípticas (más adelante, explicaremos con más detenimiento el significado de estas palabras); y finalmente, a principios de la década de los 40, estando preso en una cárcel militar a las afueras de Rouen, André Weil extendía el resultado de Hasse demostrando el análogo a la hipótesis de Riemann para curvas algebraicas cualesquiera y variedades abelianas, véase [16].

En este contexto André Weil formulaba sus conjeturas en 1949, al darse cuenta de que parte de las herramientas e ideas que utilizaba en sus trabajos sobre curvas algebraicas podían extrapolarse a variedades algebraicas generales. Para este fin, Weil pretendía construir una teoría cohomológica apropiada[8] en pos de aplicar la fórmula del punto fijo de Lefschetz, ya que los puntos $\mathbb{F}_{q^m}$-racionales de una variedad coinciden con los puntos fijos del automorfismo de Frobenius $\boldsymbol{x} \longmapsto \boldsymbol{x}^{q^m}$.

Y el lector se preguntará: «¿Qué conjeturaban[9] en concreto las conjeturas de Weil?». Pues bien, dada una variedad algebraica proyectiva y lisa X de dimensión d sobre $\mathbb{F}_q$, donde q es potencia de un primo p, las conjeturas de Weil dicen:

[8] Como veremos más adelante, ésta resultará ser la cohomología *étale*.
[9] No hay otro verbo más preciso.

(1) Racionalidad: $\zeta_X(s)$ es una función racional con coeficientes en $\mathbb{Q}$ en la variable $T = q^{-s}$ (en particular, la racionalidad de la función zeta es cierta para cualquier variedad algebraica, no es necesario que sea proyectiva ni lisa).

(2) Ecuación funcional: La función ζ_X satisface

$$\zeta_X(d-s) = \pm q^{\chi(X)\cdot\left(\frac{d}{2}-s\right)} \cdot \zeta_X(s),$$

donde $\chi(X)$ denota la característica de Euler-Poincaré de la variedad X.

(3) Análogo a la hipótesis de Riemann[10]**:** Más precisamente, podemos escribir

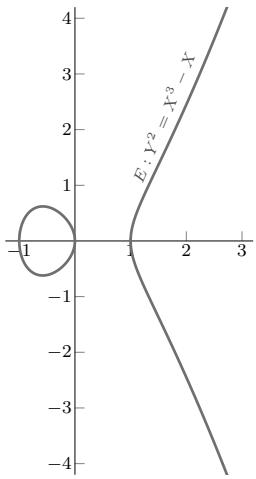
$$\zeta_X(s) = \frac{P_1(q^{-s}) \cdot P_3(q^{-s}) \cdots P_{2d-1}(q^{-s})}{P_2(q^{-s}) \cdot P_4(q^{-s}) \cdots P_{2d}(q^{-s})},$$

donde cada P_i es un polinomio con coeficientes en $\mathbb{Z}$ y que se anula exclusivamente para ciertos $\Re(s) = i/2$.

(4) Relación con los números de Betti[11]**:** El grado de cada polinomio $\deg(P_i)$ coincide con el i-ésimo número de Betti b_i de la variedad X.

Dos preguntas pueden surgir llegados a este punto: la primera, ¿por qué son interesantes las conjeturas de Weil? La razón principal (y original, léase la introducción de [16]) viene de la teoría de números: contar puntos en variedades algebraicas es equivalente a determinar el número de soluciones de un polinomio en cuerpos finitos. Por desgracia, no existe ningún método general a la hora de resolver este problema, y solamente en algunos casos contados (como, por ejemplo, los vistos en (11) y (12)) pueden explotarse algunas propiedades concretas de las ecuaciones o del cuerpo finito para resolverlo mediante métodos particulares.

Veamos un ejemplo algo más complejo: una **curva elíptica** es una curva cúbica, no singular y descrita mediante dos variables sobre un cuerpo cualquiera, en nuestro caso $\overline{\mathbb{F}_q}$. Si la característica del cuerpo es distinta de 2 o 3, ésta puede expresarse mediante su **ecuación de Weierstrass**:



Representación en $\mathbb{R}^2$ de la curva elíptica $Y^2 = X^3 - X$

$$E : Y^2 = X^3 + aX + b, \quad \text{para } a, b \in \overline{\mathbb{F}_q}.$$

Así pues, al igual que antes, supongamos que $a, b \in \mathbb{F}_q$ y que queremos contar cuántos puntos de E yacen en cada una de las extensiones de $\mathbb{F}_q$. Resulta que, a diferencia

[10] Se le suele añadir la coletilla «análogo a la hipótesis de Riemann en característica $p > 0$».

[11] Los números de Betti son un concepto topológico estrechamente relacionado con la característica de Euler-Poincaré vía la fórmula $\chi(X) = \sum_{i=0}^{2d} (-1)^i b_i$.

de los ejemplos (11) y (12)[12], ya no es tan fácil realizar dicho cálculo. No obstante, si sabemos que la función zeta de E es[13]

$$\zeta_E(s) = \frac{(1-\alpha q^{-s})(1-\bar{\alpha} q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

para cierto $\alpha \in \mathbb{C}$ tal que $\alpha\bar{\alpha} = q$, se deduce que

$$N_m(E) = q^m + 1 - (\alpha^m + \bar{\alpha}^m).$$

Por tanto, conociendo $N_1(E)$ es posible calcular el resto de $N_m(E)$; asimismo, obtenemos estimaciones no triviales de $N_m(E)$ como la **cota de Hasse**, véase [9],

$$|N_m(E) - (q^m + 1)| = |\alpha^m + \bar{\alpha}^m| = 2\,|\Re(\alpha^m)| < 2\,|\alpha^m| = 2\sqrt{q^m}.$$

La segunda pregunta debería ser: ¿qué se sabe sobre las conjeturas de Weil actualmente? Pues bien, las conjeturas de Weil fueron demostradas en su totalidad: el primer capítulo de esta historia lo protagoniza Bernard Dwork, quien probaba en 1960 la racionalidad de ζ_X mediante métodos p-ádicos (¡ésta es la demostración de la que hablaremos más adelante!), véase [4]; los siguientes protagonistas son Alexander Grothendieck y algunos de sus colaboradores con los que trabajaba durante su etapa en el IHES como, por ejemplo, Pierre Deligne, que demostraron la racionalidad, la ecuación funcional y la relación con los números de Betti usando la cohomología *étale* (una herramienta que tendía puentes entre la topología y la geometría algebraica, predicha por Weil y desarrollada por Grothendieck *ad hoc* para intentar demostrar las conjeturas de Weil); véase [6]. Sin embargo, el análogo a la hipótesis de Riemann todavía se resistía a ser demostrado: los métodos propuestos por Grothendieck no terminaban de ser efectivos. Fue Deligne quien, parece ser que tras una reveladora sugerencia de Jean Pierre Serre, dio definitivamente en 1974 con la demostración, véase [3].

4.2. La demostración de Dwork

En este apartado veremos un breve esquema de la demostración de Dwork sobre la racionalidad de la función zeta e indicaremos el papel que desempeña el análisis p-ádico en ésta. No desespere, lector, si, llegado el momento, la demostración se le hace demasiado cuesta arriba; las siguientes líneas constituyen una mera hoja de ruta (con sus inevitables ausencias) cuyo único propósito es ayudarle a discernir los argumentos clave en la demostración original. Así pues, sin más dilación, enunciemos el teorema de Dwork, para después entrar en una serie de argumentos (un tanto heurísticos, pero que pueden formalizarse adecuadamente) que simplificarán el enunciado a demostrar.

Teorema 4.1 (Dwork, 1960). *La función zeta de una variedad algebraica proyectiva es una función racional en la variable $T = q^{-s}$ y con coeficientes en $\mathbb{Q}$.*

[12]Por cierto, que las funciones zeta de $\mathbb{P}^1(\overline{\mathbb{F}_q})$ y H coincidan es consecuencia que sus géneros son ambos 0. El género de una curva elíptica es 1, y, como vemos, su función zeta es diferente.

[13]Sí, aquí estoy haciendo algo de trampa...


A. Grothendieck (izquierda) y P. Deligne y A. Weil en Princeton en 1990 (derecha).

Como nos será de utilidad de aquí en adelante, introduzcamos la siguiente notación: dada X una variedad algebraica proyectiva en $\mathbb{F}_q$ definimos

$$Z_X(T) \coloneqq \exp\left(\sum_{m=1}^{\infty} \frac{N_m(X)}{m} \cdot T^m\right) \in \mathbb{Q}[[T]];$$

de modo que $Z_X(q^{-s}) = \zeta_X(s)$. Vamos con los argumentos que nos ayudarán a simplificar el enunciado del teorema 4.1.

B. Dwork (1923–1998)

En primer lugar, a partir del principio de inclusión/exclusión y de la identidad

$$Z_{X\cap Y}(T) = \frac{Z_X(T)\cdot Z_Y(T)}{Z_{X\cup Y}(T)},$$

deducimos que basta con demostrar el enunciado para hipersuperficies, esto es, variedades algebraicas del tipo

$$\left\{\boldsymbol{x} \in \mathbb{P}^n(\overline{\mathbb{F}_q}) : f(x_0 : \cdots : x_n) = 0\right\},$$

donde f denota un polinomio homogéneo cualquiera con coeficientes en $\mathbb{F}_q$. En segundo lugar, teniendo en cuenta la descomposición

$$\mathbb{P}^n(\mathbb{F}_{q^m}) = \mathbb{A}^n(\mathbb{F}_{q^m}) \cup \mathbb{A}^{n-1}(\mathbb{F}_{q^m}) \cup \cdots \cup \mathbb{A}^1(\mathbb{F}_{q^m}) \cup \{0\} \quad \text{para todo } m \geq 1,$$

deducimos que basta con considerar exclusivamente hipersuperficies afines. Por consiguiente, el teorema 4.1 puede reducirse al siguiente enunciado:

Teorema 4.2 (Dwork, 1960). *La función zeta de una hipersuperficie afín es una función racional en la variable $T = q^{-s}$ y con coeficientes en $\mathbb{Q}$.*

En lo que sigue, sea H_f la hipersuperficie afín definida por f. El primer paso es demostrar que Z_{H_f} es una función meromorfa p-ádica. Para ello, seguiremos un argumento mediante inducción sobre el número de variables n:

- Para $n = 0$ la afirmación es trivial, pues H_f resulta ser el conjunto vacío.
- Supongamos cierto que Z_{H_f} es meromorfa para todos los polinomios con $1, 2, \ldots, n-1$ variables.

En primer lugar, definamos

$$\tilde{Z}_{H_f}(T) \coloneqq \exp\left(\sum_{m=1}^{\infty} \frac{\tilde{N}_m}{m}\, T^m\right),$$

donde $\tilde{N}_m \coloneqq \#\{(x_1, \ldots, x_n) \in H_f(\mathbb{F}_{q^m}) : x_j \neq 0 \text{ para todo } j\}$. Un sencillo cálculo con aquello de que la exponencial transforma sumas en productos y restas en cocientes nos muestra que

$$Z_{H_f}(T) = \tilde{Z}_{H_f}(T) \cdot \exp\left(\sum_{m=1}^{\infty} \frac{N_m - \tilde{N}_m}{m}\, T^m\right), \tag{13}$$

de donde, aplicando la hipótesis de inducción y el principio de inclusión-exclusión, se deduce que la exponencial que aparece en el lado derecho de (13) es meromorfa. Por consiguiente, basta con que demostremos que $\tilde{Z}_{H_f}$ es asimismo meromorfa. Sea $m \geq 1$ y $\xi \neq 1$ una raíz p-ésima de la unidad en $\mathbb{C}_p$; en primer lugar, es sencillo comprobar que

$$\sum_{x \in \mathbb{F}_{q^m}} \xi^{\mathrm{Tr}(x_0 u)} = \begin{cases} 0, & \text{si } u \in \mathbb{F}_{q^m}^*; \\ q^m, & \text{si } u = 0; \end{cases} \tag{14}$$

donde $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_p$ denota al homomorfismo de grupos (aditivos) dado por

$$\mathrm{Tr}(u) \coloneqq \sum_{\sigma \in \mathrm{Gal}\left(\mathbb{F}_{q^m}/\mathbb{F}_p\right)} \sigma(u) = u + u^p + u^{p^2} + \cdots + u^{p^{rm-1}}.$$

Aplicando la identidad (14) a f, se deduce que

$$\sum_{x_0, \ldots, x_n \in \mathbb{F}_{q^m}^*} \xi^{\mathrm{Tr}(x_0 f(x_1, \ldots, x_n))} + (q^m - 1)^n = q^m \tilde{N}_m;$$

y, si en esta última igualdad reemplazamos los coeficientes de $X_0 f(X_1, \ldots, X_n) \in \mathbb{F}_q[X_0, \ldots, X_n]$ por sus representantes[14] en $\mathbb{C}_p$ para obtener un polinomio

$$F(X_0, \ldots, X_n) = \sum_{j=0}^{N} a_j \boldsymbol{X}^{\boldsymbol{\omega}_j} \in \mathbb{C}_p[X_0, \ldots, X_n]$$

y la evaluamos en los representantes en $\mathbb{C}_p$ de los x_j, denotados mediante α_j, se infiere la existencia de una serie de potencias $\Theta(T) \in \mathbb{Q}_p(\xi)[[T]] \subset \mathbb{C}_p[[T]]$ para la

[14] Denominados **representantes de Teichmüller**, se construyen «introduciendo» $\mathbb{F}_{q^m}$ en una extensión no ramificada de $\mathbb{Q}_p$ suficientemente grande.

cual

$$q^m \tilde{N}_m = (q^m-1)^n + \sum_{\substack{\alpha_i \in \mathbb{C}_p \\ \alpha_i^{q^m-1}=1}} \prod_{j=0}^{N} \Theta\left(a_j \boldsymbol{\alpha}^{\boldsymbol{\omega}_j}\right) \Theta\left(a_j^p \boldsymbol{\alpha}^{p\boldsymbol{\omega}_j}\right) \cdots \Theta\left(a_j^{p^{rm-1}} \boldsymbol{\alpha}^{p^{rm-1}\boldsymbol{\omega}_j}\right).$$

Ahora, a partir del cálculo de ciertas sumas de Gauss en $\mathbb{C}_p$, se puede deducir que[15]

$$q^m \tilde{N}_m = (q^m-1)^n + (q^m-1)^{n+1}\ \mathrm{tr}(\psi^m),$$

donde $\psi : \mathbb{C}_p[[X_0,\ldots,X_n]] \longrightarrow \mathbb{C}_p[[X_0,\ldots,X_n]]$ es un operador que puede expresarse en forma matricial. Despejando $\tilde{N}_m$ de esta última igualdad e introduciéndolo en la expresión de $\tilde{Z}_{H_f}$ y operando, llegamos a[16]

$$\begin{aligned} \tilde{Z}_{H_f}(T) &= \exp\left(\sum_{m=1}^{\infty} \frac{\tilde{N}_m}{m}\, T^m\right) \underset{(\star)}{=} \exp_p\left(\sum_{m=1}^{\infty} \frac{\tilde{N}_m}{m}\, T^m\right) \qquad (15) \\ &= \prod_{j=0}^{n} \left(1-q^{(n-j-1)}T\right)^{(-1)^j \binom{n}{j}} \cdot \prod_{j=0}^{n+1} \left[\exp_p\left(\sum_{m=1}^{\infty} \frac{q^{m(n-j)}\,\mathrm{tr}(\psi^m)}{m}\, T^m\right)\right]^{(-1)^j \binom{n+1}{j}}. \end{aligned}$$

Puesto que es evidente que los primeros factores de la fórmula anterior son meromorfos, bastará con demostrar que los segundos también lo son. Para ello, apelamos a una versión infinito-dimensional de la identidad traza-determinante[17]

$$\det\left(I-\Psi T\right) = \exp_p\left(-\sum_{m=1}^{\infty} \frac{\mathrm{tr}\left(\psi^m\right)}{m} \cdot T^m\right), \qquad (16)$$

donde Ψ denota la «matriz» que define al operador ψ y mediante la cual puede deducirse que los segundos factores de (15) son asimismo meromorfos sobre $\mathbb{C}_p$.

Para culminar la demostración, bastará con comprobar que Z_{H_f} satisface el siguiente criterio de racionalidad:

PROPOSICIÓN 4.3 (Criterio de racionalidad de Borel, [2]). *Sea* $F(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathbb{K}[[T]]$, *donde* $\mathbb{K}$ *es un cuerpo. Para* $j,k \geq 0$ *sea*

$$A_{j,k} \coloneqq \begin{pmatrix} a_j & a_{j+1} & \cdots & a_{j+k} \\ a_{j+1} & a_{j+2} & \cdots & a_{j+k+1} \\ \vdots & \vdots & & \vdots \\ a_{j+k} & a_{j+k+1} & \cdots & a_{j+2k} \end{pmatrix}.$$

[15] ¡Cuidado, en este caso sí nos referimos a la traza del operador! Para distinguirla del homomorfismo visto unas líneas más arriba, vamos a denotarla mediante tr.

[16] Es cierto que la igualdad $(\star)$ no tendría sentido de intentar evaluarla en algún T: $\|\cdot\|_p$ y la norma usual no son equivalentes. No obstante, algebraicamente todo concuerda.

[17] La **identidad traza-determinante** dice que para toda matriz A cuadrada y compleja se tiene

$$\det(e^A) = e^{\mathrm{tr}(A)}.$$

El lector puede comprobar esta elegante identidad, por ejemplo, a partir de la descomposición canónica de Jordan. Para llegar a la fórmula (16) basta con comprobar que existe un logaritmo para el operador $I-\Psi T$ y apelar a la linealidad de la traza.

Definimos $N_{j,k} \coloneqq \det(A_{j,k})$. *Entonces,* $F(T)$ *es una función racional si y sólo si existen enteros* $k \geq 0$ *y* J *tales que* $N_{j,k} = 0$ *para todo* $j \geq J$.

En lo que sigue, adoptemos la notación

$$Z_{H_f}(T) \coloneqq \sum_{j=0}^{\infty} a_j T^j \in \mathbb{Q}[[T]].$$

En primer lugar, siguiendo un argumento de teoría de Galois, puede inferirse que, más precisamente, $Z_{H_f}(T) \in \mathbb{Z}[[T]]$ y que $0 \leq a_j \leq q^{nj}$. Así pues, por un lado, teniendo en cuenta que $\|a_j\|_p \leq 1$ y la meromorfía p-ádica de $Z_{H_f}(T)$, realizando ciertas combinaciones lineales en la matriz $A_{j,k}$ llegamos a la acotación

$$\|N_{j,k}\|_p < q^{-nj(k+2)}.$$

Por otro lado, como $|a_j| \leq q^{nj}$, acotando directamente el determinante obtenemos

$$|N_{j,k}| \leq (k+1)!\, q^{2nk(k+1)} q^{nj(k+1)}.$$

Multiplicando ambas cotas obtenemos, para j suficientemente grande,

$$|N_{j,k}| \cdot \|N_{j,k}\|_p < (k+1)!\, q^{n(2k(k+1)-j)} < 1.$$

Pero note, lector, que cualquier entero $m \neq 0$ satisface

$$|m| \cdot \|m\|_p \geq p^{\mathrm{v}_p(m)} \cdot p^{-\mathrm{v}_p(m)} = 1,$$

de donde se deduce que $N_{j,k} = 0$ para j suficientemente grande (pues no olvide que $N_{j,k} \in \mathbb{Z}$); es decir, $Z_{H_f}(T)$ cumple el criterio de racionalidad de Borel.

5. Aclaraciones finales

Reservo estas últimas líneas para comentar algunas de las referencias en las que me he basado para la escritura de estas páginas. Los mimbres del artículo han salido del libro [12]. Más particulares son las referencias [5], de la que he sacado la mayor parte de las ideas que aparecen en la introducción; [11], útil en el desarrollo de la teoría de espacios métricos; y [4], [12] y [15], que han sido las hojas de ruta seguidas para explicar, de la manera más didáctica posible, la demostración de Dwork.

Referencias

[1] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen. I, *Math. Z.* **19** (1924), 153–206; II, *Math. Z.* **19** (1924), 207–246.

[2] É. Borel, Sur une application d'un theorème de M. Hadamard, *Bull. Sci. Math.* **18** (1894), 22–25.

[3] P. Deligne, La conjecture de Weil. I, *Inst. Hautes Études Sci. Publ. Math.* **43** (1974), 273–307.

[4] B. Dwork, On the rationality of the zeta function of an algebraic variety, *Amer. J. Math.* **82** (1960), 631–648.

[5] F. Q. Gouvêa, *p-adic numbers: an introduction*, 2.ª ed., *Springer-Verlag*, Berlin, 1997.

[6] A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, *Séminaire Bourbaki*, vol. 9, 1964/65 y 1965/66, 41–55, W. A. Benjamin, New York-Amsterdam, 1966.

[7] H. Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen in Körper der rationalen Zahlen, *J. Reine Angew. Math.* **152** (1923), 129–148.

[8] H. Hasse, Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, *Abh. Math. Sem. Univ. Hamburg* **10** (1934), 325–348.

[9] H. Hasse, Zur Theorie der abstrakten elliptischen Funktionenkörper. I, *J. Reine Angew. Math.* **175** (1936), 55–62; II, *J. Reine Angew. Math.* **175** (1936), 69–88; III, *J. Reine Angew. Math.* **175** (1936), 193–208.

[10] K. Hensel, Über eine neue Begründung der Theorie der algebraischen Zahlen, *Jahresber. Dtsch. Math.-Ver.* **6** (1897), 83–88.

[11] S. Katok, *p-adic analysis compared with real*, Student Mathematical Library, vol. 37, American Mathematical Society, Providence, 2007.

[12] N. Koblitz, *p-adic numbers, p-adic analysis and zeta functions*, 2.ª ed., Springer-Verlag, New York, 1984.

[13] E. S. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.* **85** (1951), 203–362.

[14] F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p, *Math. Z.* **33** (1931), 1–32.

[15] T. Tao, Dwork's proof of rationality of the zeta function over finite fields, `https://terrytao.wordpress.com/2014/05/13/dworks-proof-of-rationality-of-the-zeta-function-over-finite-fields/`.

[16] A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.

Miguel Monsalve López, Departamento de Análisis Matemático, Universidad Complutense de Madrid
Correo electrónico: `migmonsa@ucm.es`