

# ANÁLOGOS EN $\mathbb{F}_q[X]$ DE CONJETURAS FAMOSAS DE LA TEORÍA DE LOS NÚMEROS

por

Víctor S. Albis González<sup>1</sup>

## Resumen

**Víctor S. Albis González:** Análogos en  $\mathbb{F}_q[X]$  de conjeturas famosas de la teoría de los números. Rev. Acad. Colomb. Cienc. **17** (66) (1990), 489–504. ISSN 0370-3908.

Se discuten las conjeturas de Goldbach, Fermat, Catalan, Riemann (hipótesis), Weil, Artin (sobre raíces primitivas) y Borevich y Shafarevich (sobre la serie de Poincaré de un polinomio de coeficientes  $p$ -ádicos). Para las mismas se formulan análogos más fácilmente demostrables mediante la substitución del anillo  $\mathbb{Z}$  de los números enteros por el anillo  $\mathbb{F}_q[X]$  de los polinomios en la indeterminada  $X$  y coeficientes en un cuerpo finito  $\mathbb{F}_q$  de  $q$  elementos. Se proporcionan datos históricos y se señalan algunas posibilidades de investigación adicional.

## Introducción

Uno de los campos de la matemática que ha atraído nuestra atención en los últimos años es la *teoría aritmética de polinomios*. Esta teoría es el análogo de la teoría de los números, cuando sustituimos el anillo  $\mathbb{Z}$  de los números enteros por el anillo  $\mathbb{F}_q[X]$  de los polinomios en la indeterminada  $X$  y coeficientes en un cuerpo finito  $\mathbb{F}_q$  de  $q$  elementos. La analogía se basa en el hecho de que tanto  $\mathbb{Z}$  como  $\mathbb{F}_q[X]$  son *dominios euclídeos* y, por tanto, no sólo *dominios principales* sino también *dominios factoriales* (o, si se prefiere, *dominios con factorización única en irreducibles*), cuyas propiedades aritméticas básicas (en especial las de divisibilidad)

comparten con  $\mathbb{Z}$ . Es, pues, natural pretender estudiar la aritmética de  $\mathbb{F}_q[X]$  examinando los análogos (cuando tienen sentido) de los resultados o conjeturas formulados en  $\mathbb{Z}$ . En general, los análogos en  $\mathbb{F}_q[X]$  pueden demostrarse con mayor facilidad; y, cuando de conjeturas se trata, muchas han encontrado comprobación en  $\mathbb{F}_q[X]$  sin que lo propio, hasta el momento, haya sucedido en  $\mathbb{Z}$ . Nuestro propósito en este trabajo divulgativo es precisamente formular los análogos en  $\mathbb{F}_q[X]$  de las siguientes conjeturas famosas:

- a) Conjetura de Goldbach,
- b) Conjetura de Fermat,
- c) Conjetura de Catalan,

---

<sup>1</sup>Departamento de Matemáticas y Estadística, Universidad Nacional de Colombia, Apartado aéreo 91480, Santafé de Bogotá, Colombia.

- d) Conjetura de Riemann,
- e) Conjetura de Artin sobre las raíces primitivas,
- f) Conjetura de Borevich-Shafarevich sobre la serie de Poincaré de un polinomio de coeficientes  $p$ -ádicos.

acompañados de algo de historia y discusión, señalando de paso algunas posibilidades de investigación adicional.

En la primera sección establecemos las notaciones y algunos resultados necesarios para la comprensión de las secciones subsiguientes. Las correspondientes demostraciones se pueden hallar sistematizadas en nuestro trabajo [3].

### §1. Algunos resultados preliminares

En las secciones subsiguientes supondremos que el lector está familiarizado no sólo con las propiedades generales de los anillos de polinomios  $A[X]$ , donde  $A$  es un anillo conmutativo unitario (en particular, un cuerpo conmutativo), sino también con la teoría de los números  $p$ -ádicos y las extensiones de cuerpos conmutativos. Aquí tan sólo recordaremos explícitamente algunos resultados especiales en el anillo  $\mathbb{F}_q[X]$  que usaremos principalmente en la segunda sección.

Sea  $h(X) = \epsilon p_1(X)^{e_1} \cdots p_r(X)^{e_r}$ , donde  $\epsilon \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ , los  $p_i(X)$  ( $1 \leq i \leq r$ ) son polinomios irreducibles de  $\mathbb{F}_q[X]$  y  $e_i \geq 1$ , la descomposición canónica de  $h(X)$  en factores irreducibles. Si  $(h(X))$  es el ideal generado por  $h(X)$  en  $\mathbb{F}_q[X]$ , sabemos que subsiste el siguiente análogo del *teorema chino de los restos*:

$$\mathbb{F}_q[X]/(h(X)) \approx \prod_{i=1}^r \mathbb{F}_q[X]/(p_i(X)^{e_i}), \quad (1.1)$$

y que, además,

$$[\mathbb{F}_q[X]/(h(X))]^* \approx \prod_{i=1}^r [\mathbb{F}_q[X]/(p_i(X)^{e_i})]^*. \quad (1.2)$$

Por tanto, como en el caso de  $\mathbb{Z}$ , podemos restringirnos a estudiar sólo los anillos residuales de la forma

$$\mathbb{F}_q[X]/(p(X)^e), \quad e \geq 1,$$

donde  $p(X)$  es un polinomio irreducible de  $\mathbb{F}_q[X]$ . Si el coeficiente superior o director de un polinomio es igual a 1, diremos que el polinomio es *unitario* (o *mónico*); al conjunto de todos los polinomios unitarios de  $\mathbb{F}_q[X]$ , lo designaremos con  $\mathbb{M}(q; X)$ , y al conjunto de todos los polinomios unitarios irreducibles con  $\mathbb{P}(q; X)$ . Con estas notaciones, el teorema fundamental de la descomposición en factores irreducibles puede expresarse diciendo

que  $\mathbb{M}(q; X)$  es el monoide abeliano libre generado por  $\mathbb{P}(q; X)$ .

Si  $\partial h(X) = \partial h$  designa al grado del polinomio  $h(X) \in \mathbb{F}_q[X]$ , el número  $|h(X)| = |h| = q^{\partial h(X)}$  se llama su *norma*. Podemos, pues, enunciar las siguientes proposiciones:

**Proposición 1.1** Si  $h(X), p(X) \in \mathbb{F}_q[X]$  y  $p(X)$  es irreducible, entonces:

- a)  $\text{card}(\mathbb{F}_q[X]/(h(X))) = |h(X)|$ ;
- b)  $\text{card}([\mathbb{F}_q[X]/(p(X)^e)]^*) = (|p| - 1)|p|^{e-1}$ , ( $e \geq 1$ )
- c)  $\text{card}([\mathbb{F}_q[X]/(h(X))]^*) = |h| \prod_{p \in \mathbb{P}(q; X)} \left(1 - \frac{1}{|p|}\right)^{e_p}$

donde  $\text{card}(E)$  designa al cardinal de un conjunto  $E$ .

La función  $\varphi(h) = \varphi(h(X))$  se llama, por analogía con el caso del anillo  $\mathbb{Z}$ , la *función indicatriz de Euler*.

El siguiente resultado se debe a GAUSS:

**Proposición 1.2** El número de polinomios irreducibles unitarios de grado  $r$  en  $\mathbb{F}_q[X]$  está dado por

$$\frac{1}{r} \sum_{d|r} \mu(d) q^{r/d},$$

donde  $\mu$  es la función de Möbius del anillo  $\mathbb{Z}$ .

### §2. La conjetura de Goldbach

El problema que encierra la llamada conjetura de GOLDBACH en la teoría de los números, apareció en 1742 en la correspondencia que aquél sostuvo con EULER. Esta hipótesis es originalmente la siguiente:

*Todo número entero, mayor que 3, puede expresarse en forma de una suma de no más de tres números primos.*

Todo parece indicar que GOLDBACH llegó experimentalmente a su conjetura utilizando una larga tabla, cuyos primeros términos presentamos a continuación.

$$\begin{array}{ll} 4 = 2 + 2 & 9 = 2 + 7 = 3 + 2 + 5 \\ 5 = 2 + 3 & 10 = 5 + 5 = 3 + 7 \\ 6 = 3 + 3 & 11 = 2 + 2 + 7 = 3 + 3 + 5 \\ \\ 7 = 2 + 5 = 2 + 2 + 3 & 12 = 5 + 7 \\ 8 = 3 + 5 & 13 = 3 + 3 + 7 \\ & 14 = 7 + 7 \text{ etc. } , \end{array}$$

Huelga decir que EULER no pudo validarla o invalidarla, y todos los intentos en este sentido hechos antes del

siglo XX resultaron fallidos. Observemos en la tabla anterior que los impares, a partir de 7, parecen admitir a lo menos una expresión de tres primos, y los pares sólo de dos. Esto condujo a I. M. VINOGRÁDOV, en 1937 [37], a demostrar que todo número impar, mayor que cierto  $N_0$  (la llamada *constante de Vinogradov*), se expresa en forma de una suma de no más de tres primos. También demostró que el número  $\mathbb{P}(n; 3)$  de expresiones del número impar  $n > 0$  en forma de una suma de tres números primos:  $n = p_1 + p_2 + p_3$ ,  $p_i \in \mathbb{P}$ , donde  $\mathbb{P}$  designa al conjunto de todos los números primos, es decir, el número de soluciones de la ecuación diofántica  $n = x_1 + x_2 + x_3$  en el conjunto  $\mathbb{P}$ , se expresa por la fórmula asintótica

$$\mathbb{P}(n; 3) = \frac{n^2}{2 \log^3(n)} S(n) + O\left(\frac{n^2}{(\log n)^{3.5-\epsilon}}\right),$$

donde  $S(n) > 0,6$  y  $\epsilon > 0$  es un número arbitrariamente pequeño. También se ha demostrado que  $N_0 < \exp(\exp 16,038)$ . En virtud de lo anterior, podemos restringirnos a los enteros pares y enunciar entonces lo que queda de la conjetura así:

Si  $\mathbb{P}^*$  designa al conjunto de los números primos impares, entonces  $\mathbb{P}^*(n; 2) \geq 1$  si  $n$  es un número par  $> 4$ , donde  $\mathbb{P}^*(n; 2)$  es el número de soluciones de  $n = x_1 + x_2$  con  $x_1, x_2 \in \mathbb{P}^*$ .

Para esta última hipótesis, en 1966, CHENG JING-RUN [12] demostró que *todo número par suficientemente grande es la suma de un primo y de un número que no tiene más de dos factores primos distintos*. Es claro que hasta ahora el problema de GOLDBACH, a pesar de los resultados anteriores, no tiene todavía una solución numérica definitiva. La evidencia numérica alcanzada por las computadoras de alta velocidad, usando algoritmos rápidos, sigue, empero, evidenciando que la conjetura tiene muchas posibilidades de ser válida.

El problema de Goldbach pertenece a la categoría de los problemas que en teoría de los números suelen denominarse *problemas aditivos*, cuya caracterización general es la siguiente: Dado un subconjunto  $A$  de  $\mathbb{Z}$ , ¿puede un elemento arbitrario de  $\mathbb{Z}$  escribirse como la suma de  $k$  elementos de  $A$ , donde  $k$  es menor o igual a un número prefijado  $m$ ?

Nuestro análogo en  $\mathbb{F}_q[X]$  de la conjetura de Goldbach, encuentra las siguientes respuestas:

**Proposición 2.1** Si  $h(X) \in \mathbb{F}_q[X]$  es un polinomio de grado  $h$  y  $q \gg h$ , entonces  $h(X)$  es la suma de dos polinomios irreducibles de grado  $h + 1$ .

En efecto, sabemos (proposición 1.2) que el número de polinomios unitarios irreducibles de grado  $h + 1$  está dado por

$$\frac{1}{h+1} \sum_{d|(h+1)} \mu(d) q^{(h+1)d} = \frac{q^{h+1}}{h+1} + O\left(\frac{q^{(h+1)/2}}{h+1}\right)$$

(cuando  $q \rightarrow \infty$ ). Por otra parte, el número de clases de equivalencia mód  $h(X)$  está dado por

$$1 + q + \dots + q^{h-1} < hq^{h-1} < \frac{q^{h+1}}{h+1},$$

si  $q \gg h$ , pues en tal caso  $h(h+1) < q^2$ . Luego, en por lo menos una clase módulo  $h(X)$  hay dos irreducibles unitarios distintos,  $p_1(X)$ ,  $p_2(X)$ , de grado  $h + 1$ . Es decir,  $p_1(X) - p_2(X) = h(X)a(X)$ , para algún polinomio no nulo  $a(X)$  en  $\mathbb{F}_q[X]$ . Pero  $h + \partial a(X) = \partial[p_1(X) - p_2(X)] \leq h$ , lo que obliga a que  $\partial a(X) = 0$ , es decir,  $a(X) = \alpha^{-1} \in \mathbb{F}_q^*$ . Luego  $h(X) = \alpha p_1(X) - \alpha p_2(X)$ .

Esta representación no es, en general, única. Por ejemplo, en  $\mathbb{F}_3[X]$  los polinomios irreducibles

$$\begin{aligned} p_1(X) &= X^3 + 2X + 1, & p_2(X) &= X^3 + 2X^2 + 2, \\ p_3(X) &= X^3 + 2X + 2, & p_4(X) &= X^3 + X^2 + X + 1, \end{aligned}$$

En el mismo trabajo [20], HAYES establece el siguiente análogo de la fórmula asintótica de VINOGRÁDOV:

**Proposición 2.2** Sea  $h(X)$  un polinomio unitario de grado  $h$  y designemos con  $N$  al número de parejas  $(p_1(X), p_2(X))$  de polinomios irreducibles de grado  $h + 1$  que cumplen  $p_1(X) \equiv p_2(X) \pmod{h(X)}$ , con  $p_1(X) \neq p_2(X)$ . Si una de las dos condiciones siguientes se cumple:

- (a)  $h(X)$  no admite factores cuadráticos.
- (b)  $h + 1$  no es divisible por la característica de  $\mathbb{F}_q$ ,

entonces

$$N = \frac{q^{2(h+1)}}{(h+1)^2 \varphi(h(X))} + O(q^{h+1}),$$

cuando  $q \rightarrow \infty$ .

Omitimos, para no alargar nuestra exposición, la demostración de este último resultado (véanse [20] y [21]).

Pero, ¿a qué equivalen las nociones de par e impar en  $\mathbb{F}_q[X]$ ? Se ha encontrado conveniente proponer lo siguiente: si  $q > 2$ , todo polinomio  $h(X)$  en  $\mathbb{F}_q[X]$  es simultáneamente *par e impar*; si  $q = 2$ ,  $h(X)$  se dice *par*

si es divisible por el polinomio  $X(X+1)$ , e *impar* en caso contrario. Con estas convenciones, CAR [9] y HAYES [22] han demostrado lo siguiente:

**Proposición 2.3** *Todo polinomio impar de grado  $h$  se puede expresar como una suma  $h(X) = p_1(X) + p_2(X) + p_3(X)$  de polinomios irreducibles de grado a lo sumo  $h$ , si  $h$  es suficientemente grande.*

Por su parte, CAR [10] ha demostrado el siguiente análogo del teorema de CHENG JING-RUN:

**Proposición 2.4** *Todo polinomio par  $h(X)$  en  $\mathbb{F}_q[X]$ , de grado  $h$  suficientemente grande, puede expresarse como una suma  $h(X) = p(X) + q(X)$ , donde  $p(X)$  es un polinomio irreducible de grado a lo sumo  $h$  y  $q(X)$  es un polinomio irreducible o el producto de dos polinomios irreducibles. Además, si  $G(h)$  es el número de tales expresiones, entonces*

$$G(h) \geq (0,33) \frac{2^{h+1}}{h^2} N(h) \varphi(h)^{-1} \prod_{\substack{p(X) \nmid h(X) \\ p(X) \in \mathbb{F}(q;X)}} \left(1 - \frac{1}{\varphi(h)^2}\right).$$

Recientemente, WEBB [39], usando un análogo de la criba de A. SELBERG en  $\mathbb{F}_q[X]$ , ha demostrado lo siguiente:

**Proposición 2.5** *Sea  $h(X)$  en  $\mathbb{F}_q[X]$  un polinomio de grado  $h$ . Sea  $N(h+1; h(X))$  el número de polinomios primos y unitarios de grado  $h+1$  para los cuales  $p(X) + h(X)$  es irreducible. Entonces*

$$N(h+1; h(X)) \leq C \frac{q^{h+1}}{(h+1)^2},$$

donde  $C$  es una constante. Además  $N(h+1; h(X)) = s +$  número de irreducibles unitarios  $p(X)$  tales que  $h(X) + p(X)$  es irreducible y  $\partial p(X) \leq h/2$ , donde  $s$  es el cardinal del “resultado de la criba”.

Poseemos evidencias de que posiblemente  $N(h+1; h(X)) > 0$ , con lo cual la condición  $q \gg h$  parece no ser necesaria en la proposición 2.1.

### §3. Las conjeturas de Fermat y Catalan

La famosa *conjetura de Fermat* sobre la inexistencia de soluciones enteras de la ecuación

$$x^n + y^n - z^n = 0, \quad (x, y) = (x, z) = (y, z) = 1, \quad (3.1)$$

si  $n \geq 3$ , es muy conocida. Los esfuerzos hechos por demostrarla han generado una enorme cantidad de excelente matemática, lo que por sí solo bastaría para justificarlos. A los interesados en conocer detalles de estos esfuerzos recomendamos vehementemente la lectura del

erudito libro de RIBENBOIM [32]. Menos conocida es la siguiente conjetura de CATALAN [11]:

*Las únicas potencias consecutivas enteras son 8 y 9.*

Es decir, la única solución en enteros  $x, y, m, n$ , mayores que 1, de la ecuación

$$x^m - y^n = 1 \quad (3.2)$$

está dada por  $x = n = 3$  é  $y = m = 2$ . La ecuación (3.2) es un caso particular de la llamada *conjetura de Cassels-Catalan*:

*Para enteros fijos  $a, b$  y  $c$ , distintos de cero, la ecuación*

$$ax^m + by^n = c \quad (3.3)$$

*tiene sólo un número finito de soluciones enteras  $x, y, m, n$  que satisfacen  $m \geq 3, n, |x|, |y| \geq 2$ ,*

pues basta tomar  $a = -b = c = 1$ . En 1976, TIJDEMAN [36] demostró que en este caso la conjetura de Cassels-Catalan es correcta; es decir, si existen potencias consecutivas de números enteros, éstas aparecen en número finito, sin que aún podamos decidir si 8 y 9 sean las únicas.

El estudio de estas ecuaciones en los anillos de polinomios se puede realizar sin suponer de entrada que los coeficientes estén en un cuerpo finito  $\mathbb{F}_q$ . Es decir, podemos estudiar soluciones en  $K[X]$ , donde  $K$  es en principio un cuerpo arbitrario. En efecto, en 1789 LIOUVILLE [30] demostró que si  $x(X), y(X)$  y  $z(X)$  son polinomios *no constantes* de coeficientes en el cuerpo  $\mathbb{C}$  de los números complejos, que cumplen las condiciones  $(x(X), y(X)) = (x(X), z(X)) = (y(X), z(X)) = 1$ , entonces no pueden satisfacer la ecuación (3.1) si  $n \geq 3$ . Dicho de otra manera, la conjetura de Fermat es válida en el anillo  $\mathbb{C}[X]$  si excluimos las múltiples soluciones constantes de (3.1). En 1880, KORKINE [29] dio una demostración algebraica más elegante del resultado de LIOUVILLE, quien había utilizado la teoría de funciones de variables complejas. El problema lo retoma casi un siglo después, en 1969, GREENLEAF [17], quien da una nueva demostración elemental utilizando ideas básicas de la teoría de las ecuaciones algebraicas (al parecer GREENLEAF desconocía el trabajo de KORKINE). Un poco más tarde, en 1974, NATANSON anota que la demostración de GREENLEAF continúa siendo válida en un cuerpo de característica  $\ell > 0$  siempre y cuando  $\ell \nmid n$  (esta condición es importante por razones de separabilidad), pues  $x(X) = X+1, y(X) = X-1$  y  $z(X) = X$  son soluciones de (3.1) en  $K[X]$  si  $n = 3$  y  $K$  es un cuerpo de característica 3. En el mismo trabajo, NATANSON

demuestra que la conjetura de Catalan es correcta en  $K[X]$  si la característica  $\ell$  de  $K$  no divide a  $mn$ ; más precisamente, si  $\ell \nmid mn$  la ecuación (3.2) no tiene soluciones no constantes en  $K[X]$ . Más recientemente, RIBENBOIM [33] generaliza el resultado de NATANSON a una clase más amplia de ecuaciones.

Para beneficio del lector, daremos aquí las demostraciones de los resultados de GREENLEAF y RIBENBOIM, obteniendo de contera el de NATANSON.

**Proposición 3.1** (GREENLEAF) *Sea  $K$  un cuerpo de característica  $\ell > 0$ . Si  $\ell \nmid n$  y  $n > 2$ , entonces no existen  $x(X), y(X), z(X) \in K[X]$ , no constantes, que satisfagan (3.1). Es decir, las únicas soluciones posibles de la ecuación de Fermat en  $K[X]$  son polinomios constantes.*

*Demostración.* Supongamos que (3.1) tenga soluciones en  $K[X]$  y que  $K$  sea algebraicamente cerrado. Tomemos entonces  $x(X), y(X)$  y  $z(X)$  en forma tal que  $r = \max \{\partial x(X), \partial y(X), \partial z(X)\}$  sea mínimo. Sea  $\zeta$  una raíz primitiva  $n$ -ésima de 1, la cual pertenece a  $K$  puesto que  $\ell \nmid n$ . Bajo estas condiciones, (3.1) puede escribirse así:

$$x(X)^n = \prod_{k=0}^{n-1} [z(X) - \zeta^k y(X)] \quad (3.4)$$

en  $K[X]$ . Como  $z(X)$  é  $y(X)$  son primos entre sí, los polinomios  $z(X) - y(X), z(X) - \zeta y(X), \dots, z(X) - \zeta^{n-1} y(X)$ , son primos entre sí dos a dos (esto es de fácil verificación). De aquí resulta, usando la factorialidad de  $K[X]$ , que  $z(X) - \zeta^k y(X) = g_k(X)^n$ , donde  $g_k(X) \in K[X]$ . Consideremos ahora el  $K$ -espacio vectorial generado por  $z(X)$  é  $y(X)$ , el cual tiene dimensión 2. Es claro entonces que  $z(X) - y(X), z(X) - \zeta y(X), z(X) - \zeta^2 y(X)$  pertenecen a este subespacio. Por tanto, son linealmente dependientes sobre  $K$ . Luego existen  $\alpha_0, \alpha_1, \alpha_2$  en  $K$ , no todos nulos, tales que

$$\alpha_0 g_0(X)^n + \alpha_1 g_1(X)^n = \alpha_2 g_2(X)^n .$$

Ahora bien, como  $K$  es algebraicamente cerrado existen  $\beta_0, \beta_1, \beta_2$  en  $K$  tales que  $\alpha_i = \beta_i^n$  ( $i = 0, 1, 2$ ). Luego (3.1) tiene una solución  $\beta_0 g_0(X), \beta_1 g_1(X), \beta_2 g_2(X)$  en  $K[X]$ , polinomios primos entre sí, tales que  $\max \{\partial \beta_i g_i(X)\} \leq \frac{r}{n} < r$ , lo que contradice la minimalidad de  $r$ . Supongamos finalmente que  $K$  no sea algebraicamente cerrado y consideremos su clausura algebraica  $\hat{K}$ . Entonces si  $x(X), y(X)$  y  $z(X)$  en  $K[X]$  satisfacen (3.1), también la satisfacen en  $\hat{K}[X]$ . Luego  $x(X), y(X), z(X) \in \hat{K}$ . Pero  $\hat{K} \cap K[X] = K$ .  $\checkmark$

**Proposición 3.2** (RIBENBOIM) *Sean  $m, n > 2, \ell \nmid mn$ . Si  $x(X), y(X) \in K[X]$  satisfacen  $y(X)^n = P(x(X))$ , donde  $P(t) \in K[t]$  es un polinomio de grado  $m$  y raíces distintas, entonces  $x(X)$  é  $y(X)$  pertenecen a  $K$ .*

*Demostración.* Como en la proposición anterior, podemos suponer que  $K$  es algebraicamente cerrado, sin perder sustancialmente la generalidad. Demostremos ahora que si  $x(X) \in K$  entonces  $y(X) \in K$ . En efecto, si  $x(X) \in K$ , entonces  $y(X)^n = c \in K$ ; como  $K$  es algebraicamente cerrado, existe  $d \in K$  tal que  $d^n = c$ . Pero  $\ell \nmid n$ , de modo que  $K$  contiene las raíces  $n$ -ésimas de la unidad y, por consiguiente,

$$[y(X) - d][y(X) - \zeta d] \cdots [y(X) - \zeta^{n-1} d] = 0 .$$

Esto obliga a que  $y(X) \in K$ . Recíprocamente, si  $y(X) \in K$  y  $Q(t) = P(t) - y(X)^n \in K[t]$ , entonces  $x(X)$  es una raíz de  $Q(t)$ . Como  $K$  es algebraicamente cerrado,  $x(X) \in K$ . Sea ahora

$$P(t) = a_0 t^m + a_1 t^{m-1} + \cdots + a_m = a_0 \prod_{i=0}^m (t - r_i) ,$$

donde  $a_i, r_i \in K$  ( $i = 1, \dots, m$ ), todos los  $r_i$  son distintos y  $a_0 \in K, a_0 \neq 0$ . Sean  $x = x_1/x_0, y = y_1/y_0$ , con  $x_0, x_1, y_0, y_1 \in K[X]$  y supongamos, además, que  $(x_0, x_1) = (y_0, y_1) = 1$ . Entonces

$$y_1^m x_0^m = (x_0, a_0 x_0^m + \cdots + a_m x_0^m) y_0^n .$$

Como

$$(x, a_0 x_0^m + \cdots + a_m x_0^m) = 1 ,$$

resulta

$$y_0^n = h x_0^m \quad \text{donde } h \in K[X]$$

De  $(y_0, y_1) = 1$  se obtiene:

$$a_0 x_0^m + \cdots + a_m x_0^m = h' y_1^n x_0^m ,$$

donde  $h' \in K[X]$ . Por tanto,  $hh' = 1$  y necesariamente  $h, h' \in K[X]$ . Sea  $d \in K$  tal que  $d^n = h'$ ; entonces, de (3.5):

$$(dy_1)^n = a_0 \prod_{i=1}^m (x_1 - r_i x_0) .$$

Como las raíces  $r_i$  son todas distintas, los polinomios  $x_1 - r_i x_0$  son primos dos a dos. Luego, como  $K[X]$  es factorial, cada  $x_1 - r_i x_0$  es una potencia  $n$ -ésima en  $K[X]$ :

$$x_1 - r_i x_0 = h_i^n \quad (i = 1, \dots, m), \quad h_i \in K[X] .$$

Dado que  $\ell \geq 3$ , los elementos  $x_1 - r_1 x_0, x_1 - r_2 x_0, x_1 - r_3 x_0$  son  $K$ -linealmente independientes en el  $K$ -espacio generado por  $x_0$  y  $x_1$  en  $K[X]$ , el cual tiene

dimensión 2. Por tanto, existen  $b_i \in K$  ( $i = 1, 2, 3$ ), no todos nulos, tales que

$$\begin{aligned} 0 &= b_1(x_1 - r_1x_0) + b_2(x_1 - r_2x_0) + b_3(x_1 - r_3x_0) \\ &= b_1h_1^n + b_2h_2^n + b_3h_3^n. \end{aligned}$$

Más aún, todos los  $b_i$  son distintos de cero, pues  $(x_0, x_1) = 1$ . Sean, pues,  $c_i \in K$  tales que  $c_i = b_i$  ( $i = 1, 2, 3$ ), de modo que

$$(c_1h_1)^n + (c_2h_2)^n + (c_3h_3)^n = 0.$$

Por la proposición 3.1,  $h_1, h_2, h_3 \in K$ . Usando ahora la observación hecha al comienzo de la demostración, vemos que  $h_i^n = x_1 - r_ix_0$  implica que  $x_1 - r_ix_0 \in K$  ( $i = 1, 2, 3$ ). Esto implica a su vez que  $(r_1 - r_2)x_0 \in K$  y, en consecuencia, que  $x_0$  y  $x_1$  pertenecen a  $K$ , lo cual es contrario a la hipótesis.

**Proposición 3.3.** (NATANSON) *La ecuación (3.2) no tiene soluciones no constantes en  $K[X]$  si  $m, n \geq 2$  y  $\ell \nmid mn$ .*

*Demostración.* Tomemos  $P(t) = t^n - 1$ ,  $\ell \nmid mn$ . Si  $m, n \geq 2$ , apliquemos la proposición 3.2. Si  $m = 2$  y  $n > 2$ , tenemos  $y^n = x^2 - 1 = (-1)(x + 1)$ . Como  $x - 1, x + 1 = 1$ , existen  $h, k \in K[X]$ ,  $(h, k) = 1$ , tales que  $x + 1 = h^n$ ,  $x - 1 = k^n$ . Entonces  $h^n - k^n = 2$ , de donde  $((2^{1/n})^n) + k^n + ((-1)^{1/n})^n h^n$ , lo que produce una solución no constante de la ecuación de Fermat, contrariamente a la proposición 3.1. De manera semejante se procede en los casos  $m > 2$  y  $n = 2$  ( $\ell \nmid 2$ ). Observemos finalmente que si  $m = n = 2$  y  $x, y \in K[X]$  satisfacen  $1 = (x - y)(x + y) = x^2 - y^2$ , entonces tanto  $x - y$  como  $x + y$  pertenecen a  $K$  y, por consiguiente,  $x$  é  $y$  también pertenecen a  $K$ .

Volvamos ahora a la conjetura de Cassels-Catalan en  $K(X)$ , empezando por observar que si  $m = n = 2$ , la ecuación (3.2) admite soluciones no constantes en  $K(X)$ :

$$\left(\frac{x^2 - 1}{x^2 + 1}\right)^2 - \left(\frac{2\sqrt{-1}x}{x^2 + 1}\right)^2 = 1,$$

si  $\sqrt{-1} \in K$ , aunque no las admita en  $K[X]$ . Por otra parte, usando el resultado de RIBENBOIM, la ecuación (3.3) no admite soluciones no constantes en  $K(X)$  si  $m, n > 2$  y  $\ell \nmid mn$ . Todo esto conduce a preguntarnos qué sucede con la conjetura de Cassels-Catalan en una extensión algebraica finita  $L$  de  $K(X)$ , o lo que es casi lo mismo en el cuerpo de funciones de una variedad proyectiva regular (no singular). La respuesta a esta pregunta la da el siguiente resultado de SILVERMAN [35]:

**Proposición 3.4.** *Sea  $K$  un cuerpo de característica  $\ell$  (posiblemente con  $\ell = 0$ ), y sea  $L/K$  el cuerpo de funciones de una variedad proyectiva regular. Fijemos  $a, b, c \in L^*$ .*

*Entonces sólo hay número finito de parejas de enteros  $m, n \geq 2$  (primos con  $\ell$  si  $\ell \neq 0$ ) para las cuales la ecuación (3.3) tiene siquiera una única solución no constante  $x, y \in L$ ,  $x, y \notin K$ .*

*Además, para cualquier par particular  $(m, n)$  de éstos sólo habrá un número finito de soluciones  $x, y \in K$ , a menos que: (i)  $a/c$  sea una potencia  $m$ -ésima y  $b/c$*

*una potencia  $n$ -ésima en  $L$ , en cuyo caso pueden existir infinitas soluciones  $(x, y) = (\alpha(a/c)^{1/m}, \beta(b/c)^{1/n})$  con  $\alpha, \beta \in K$  que cumplen  $\alpha^m + \beta^n = 1$ ; o (ii)*

*$(m, n) \in \{(2, 2), (2, 3), (3, 2), (2, 4), (4, 2), (3, 3)\}$ , en cuyo caso la ecuación de Cassels-Catalan define una curva de género 0 ó 1 sobre  $L$ .*

De modo que las soluciones no constantes de (3.3), con  $m, n > 2$ , sólo pueden aparecer si  $L/K(X)$  es una extensión propia de  $K(X)$ . Sería muy interesante estudiar tanto (3.3) como (3.2) en los cuerpos cuadráticos de funciones algebraicas sobre  $K = \mathbb{F}_q$ , cuya estructura es bien conocida desde ARTIN [5], en el sentido de precisar en el resultado de SILVERMAN la forma de sus soluciones y su cantidad.

#### §4. La hipótesis de Riemann y las conjeturas de Weil

En un artículo trascendental de ocho páginas, *Ueber die Anzahl der Primzahlen unter eine gegebenen Grösse* [34], Riemann introduce la función de variable compleja

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} (1 - p^{-s})^{-1},$$

que converge absoluta y uniformemente si  $\Re(z) > 1$ , para intentar “calcular” el número  $\pi(x)$  de primos menores que  $x$  mediante una “fórmula analítica” que no vamos a discutir aquí. La importancia del artículo de RIEMANN no estriba tanto en sus resultados como en los métodos que inaugura, los que en manos de HADAMARD, VON MANGOLDT y DE LA VALLÉE-POUSSIN, por ejemplo, condujeron a demostraciones correctas de la fórmula de Riemann para  $\pi(x)$  y del llamado *teorema de los números primos*. Las personas interesadas en obtener más detalles sobre este trabajo de RIEMANN pueden hojear el interesante libro de H. M. EDWARDS [14].

La función  $\zeta(s)$  puede prolongarse analíticamente a todo el plano complejo, con excepción del polo  $s = 1$ , usando una ecuación funcional, dada por RIEMANN, en la cual interviene la función factorial  $\Gamma(s)$ . Al estudiar los ceros de la función  $\zeta(s)$  (ver, para detalles, [14] y [34]), RIEMANN concluye que es “muy probable” que los siguiente sea cierto:

*Todos los ceros de  $\zeta(s)$  están en la recta  $\Re(s) = 1/2$ .*

Esta es la famosa *hipótesis de Riemann*, incluida por HILBERT [24] en su célebre lista de problemas de 1900. Hasta hoy nadie ha podido demostrarla o invalidarla, aunque sabemos [18], por ejemplo, que existen números complejos  $s = \frac{1}{2} + it$  que satisfacen  $\zeta(\frac{1}{2} + it) = 0$  y que su cantidad es infinita.

Cuando trasladamos el problema al anillo  $\mathbb{F}_q[X]$ , obtenemos el siguiente análogo de la función  $\zeta$  de Riemann:

$$\zeta^*(s) = \sum_{a \in \mathbb{M}(q; X)} |a|^s = \sum_{k=0}^{\infty} \left[ \sum_{\partial a=k} 1 \right] q^{-ks},$$

de donde

$$\zeta^*(s) = \sum_{k=0}^{\infty} q^{-k(s-1)} = (1 - q^{1-s})^{-1}. \quad (4.1)$$

Claramente la serie en (4.1) converge absoluta y uniformemente si  $\Re(s) > 1$  y define así una función anaítica en este semiplano. Pero  $1/(1 - q^{1-s})$  es una función meromorfa en  $\mathbb{C}$  con un único polo en  $s = 1$  (pues  $\lim_{s \rightarrow 1^+} (1 - q^{1-s})^{-1} = +\infty$ ), de modo que  $\zeta^*(s)$  admite como prolongación analítica a la función  $(1 - q^{1-s})^{-1}$ . Para tener en cuenta la llamada “valuación en  $\infty$ ”, se acostumbra definir la función zeta de  $\mathbb{F}_q(X)$  por la ecuación:

$$\zeta(s, \mathbb{F}_q(X)) = (1 - q^{-s})(1 - q^{1-s})^{-1},$$

la cual evidentemente no posee ceros y satisface entonces trivialmente la hipótesis de Riemann, lo que de por sí no es muy interesante. Sin embargo, sin en vez de  $\mathbb{F}_q(X)$  tomamos una extensión finita  $L$  de  $\mathbb{F}_q(X)$ , es decir, un cuerpo aritmético de funciones algebraicas, la situación tiene otro cariz. En efecto, en este caso la función zeta de  $L$  está dada por

$$\zeta(s, L) = \zeta(s, \mathbb{F}_q(X))r(s, L), \quad (4.2)$$

donde  $r(s, L)$  es un polinomio en  $q^{-s}$ . Se puede ver ([40]) que con el cambio de variables  $u = q^{-s}$ , (4.2) deviene

$$\begin{aligned} Z(u, L) &= Z(u, \mathbb{F}_q(X))P(u) \\ &= P(u)(1 - u)^{-1}(1 - qu)^{-1}. \end{aligned} \quad (4.3)$$

donde

$$P(u) = \prod_{i=1}^{2g} (1 - \alpha_i u) \in \mathbb{Z}[u], \quad (4.4)$$

donde  $\alpha_i \bar{\alpha}_i = q$  ( $1 \leq i \leq 2g$ ) y  $g$  es el *género* del cuerpo  $L$ . Por tanto, los ceros de (4.2) corresponden a los ceros de (4.4). Pero WEIL [40] ha demostrado también que todos los ceros de (4.4) satisfacen  $|\alpha| = q^{-1/2}$ . Como  $|q^{-(\sigma+it)}| = q^{-\sigma}$  si  $s = \sigma + it$ , resulta entonces que  $s = \sigma + it$  es un cero de  $\zeta(s, L)$  sólo si  $s = \frac{1}{2} + it$ . Es decir, la función zeta  $\zeta(s, L)$  del cuerpo aritmético de funciones  $L$  satisface la hipótesis de Riemann.

Naturalmente, WEIL atacó el problema a sabiendas de que ARTIN [5] ya había demostrado la hipótesis para algunos casos de extensiones cuadráticas de  $\mathbb{F}_q(X)$  y la había conjeturado en el caso más general de funciones sobre  $\mathbb{F}_q$ . Por otra parte, la demostración de WEIL se realiza estudiando la “función zeta de un polinomio homogéneo regular” (no singular), cosa que es esencialmente equivalente a estudiar la función zeta de un cuerpo aritmético de funciones sobre  $\mathbb{F}_q$ . Este hecho condujo a WEIL [41] a introducir la función zeta de una variedad algebraica sobre  $\mathbb{F}_q$  y a proponer una serie de conjeturas, entre las cuales estaba la hipótesis de Riemann para estas nuevas funciones zeta, no sin antes demostrarlas para cierto tipo de hipersuperficies proyectivas. Algunas de estas conjeturas de WEIL fueron demostradas muy rápidamente, pero sólo en 1973 pudo DELIGNE demostrar que efectivamente la función zeta de una variedad algebraica sobre  $\mathbb{F}_q$  satisface la hipótesis de Riemann, lo que muchos consideran una de las grandes proezas de este siglo. Para un análisis de la demostración de DELIGNE y una discusión de los aspectos históricos de las conjeturas de WEIL, recomendamos mirar el artículo de KATZ [28].

## §5. La conjetura de Artin

Empecemos mencionando que el problema de determinar los números primos  $p$  para los cuales un número entero dado  $a$  es raíz primitiva módulo  $p$  (es decir, aquellos primos  $p$  para los cuales la clase residual  $\bar{a}$  genera al grupo cíclico  $(\mathbb{Z}/\mathbb{Z}p)^*$  de  $p - 1$  elementos), lo investigó GAUSS en el Artículo 303 de sus *Disquisitiones Arithmeticae* [15], dedicado al desarrollo decimal periódico de fracciones de denominador  $p$ . Precisamente GAUSS conjeturó que

*El número de primos  $p$  para los cuales  $10$  es raíz primitiva módulo  $p$  es infinito.*

Una condición necesaria y suficiente para que  $a$  sea una raíz primitiva módulo el primo  $p$  está contenida en la siguiente proposición:

**Proposición 5.1.** *Un entero  $a$  es raíz primitiva del número primo  $p$  si, y sólo si,  $(a, p) = 1$  y  $a$  no satisface ninguna de las congruencias*

$$a^{(p-1)/q} \equiv 1 \pmod{p}$$

cuando  $q$  recorre los distintos divisores primos de  $p - 1$ .

*Demostración.* En efecto, si alguna de las congruencias del enunciado subsiste y adado que  $(p - 1)/q < (p - 1)$  es imposible que  $a$  pueda ser raíz primitiva módulo  $p$ . Recíprocamente, si  $(a, p) = 1$  y  $a$  no satisface ninguna de las congruencias anteriores y suponemos que  $a \equiv 1 \pmod{p}$  para algún  $d < p - 1$ , sabemos que  $d \mid (p - 1)$ , de modo que tendríamos  $(p - 1)/d = uq$ , donde  $q$  es un divisor primo de  $p - 1$ . Por consiguiente,  $(p - 1)/d = ud$ ,  $a^{(p-1)/d} = a^{ud} \equiv 1 \pmod{p}$ , lo que contradice la hipótesis hecha.  $\checkmark$

En lo que sigue usaremos la siguiente notación:  $\mathcal{A}(a) = \{p : p \text{ es un primo y } a \text{ es raíz primitiva módulo } p\}$ . Con ella la conjetura de GAUSS puede expresarse diciendo que  $\mathcal{A}(10)$  es infinito. Desde el siglo XIX se conocía que para algunos  $a$  el conjunto  $\mathcal{A}(a)$  era infinito. Por ejemplo:

**Proposición 5.2.**  $\mathcal{A}(2)$  es infinito.

*Demostración.* Según la proposición 5.1, 2 es raíz primitiva de un primo de la forma  $p = 4q + 1$  si, y sólo si, 2 no satisface ni

$$2^4 \equiv 1 \pmod{4q + 1}$$

ni

$$2^{2q} \equiv 1 \pmod{4q + 1} .$$

Como  $15 \equiv 0 \pmod{4q + 1}$  es imposible pues ni 3 ni 5 son de la forma  $4q + 1$  si  $q >$ , la primera de estas congruencias es imposible si  $q > 1$ . Por otra parte, para un primo  $p \equiv 1 \pmod{4}$  se tiene

$$2^{(p-1)/2} = 2^{2q} \equiv \left( \frac{2}{4q + 1} \right) \pmod{4q + 1} ,$$

donde  $(2/p)$  es el *símbolo de Legendre*. Si  $p = 4q + 1 = 8m + 5$ , sabemos [38] que  $(2/p) = -1$ ; luego, en este caso, la congruencia  $2^{2q} \equiv 1 \pmod{4q + 1}$  es imposible. Pero un famoso teorema de DIRICHLET sobre las progresiones aritméticas, nos dice que el conjunto de los primos  $p$  que satisfacen  $p \equiv 5 \pmod{8}$  es infinito pues  $5, 8) = 1$ . Como  $p \equiv 5 \pmod{8}$  implica que  $p \equiv 1 \pmod{4}$ , resulta entonces que el número de primos de la forma  $p = 4q + 1$

que hacen  $\left( \frac{2}{4aq + 1} \right) = -1$  es infinito, lo que muestra que  $\mathcal{A}(2)$  también lo es.  $\checkmark$

Pero  $\mathcal{A}(a)$  también puede ser finito o vacío. Por ejemplo, si  $a = x^2$  es un cuadrado perfecto ( $x \in \mathbb{Z}$ ), obtenemos de la identidad de FERMAT  $x^{p-1} \equiv 1 \pmod{p}$  la relación  $a^{(p-1)/2} \equiv 1 \pmod{p}$ , la que indica que si  $p \nmid x$  y  $p$  es impar, entonces  $p \notin \mathcal{A}(a)$ . Pero si  $p \mid x$  es claro que  $p \notin \mathcal{A}(a)$ . Luego  $\mathcal{A}(a) = \emptyset$ . Por otro lado, dado que  $(-1)^2 = +1$  vemos que  $p \notin \mathcal{A}(-1)$  si  $p - 1 > 2$ . Pero  $-1$  es una raíz primitiva módulo 3; es decir,  $\mathcal{A}(-1) = \{3\}$ .

Lo anterior, más un razonamiento heurístico de tipo probabilístico –además de seductor– que puede encontrarse explicado en [7], [16] o [25], llevó a ARTIN, en 1927, en el curso de una conversación con HASSE, a proponer la siguiente conjetura:

*Si  $a \neq 0, \pm 1$  y no es un cuadrado perfecto, entonces  $\mathcal{A}(a)$  es infinito.*

Esta conjetura fue demostrada por HOOLEY [25] bajo el supuesto de que la extensión natural de la hipótesis de Riemann a la función zeta de Dedekind de ciertas extensiones galoisianas de  $\mathbb{Q}$  es válida.

El análogo de esta conjetura en  $\mathbb{F}_q[X]$  fue demostrado, en 1937, por BILHARZ [7], un alumno de HASSE, también bajo el supuesto de que la hipótesis de Riemann para las funciones zeta de los cuerpos de funciones algebraicas sobre cuerpos finitos fuese válida. Afortunadamente para BILHARZ, WEIL demostró la validez de esta hipótesis, tal como lo hemos indicado en la sección § 4. Pasamos en seguida a precisar este análogo.

Recordemos que en  $\mathbb{F}_q[X]$  el papel de los primos lo tienen los polinomios irreducibles unitarios. Si  $p(X)$  es uno de estos polinomios, de grado  $r$ , entonces sabemos (véase la sección § 2) que  $(\mathbb{F}_q[X]/(p(X)))$  es un cuerpo finito de  $q^r$  elementos y que  $(\mathbb{F}_q[X]/(p(X)))^\times$  es un grupo cíclico de  $q^r - 1$  elementos. Como en el caso de los números enteros, un polinomio  $a(X) \in \mathbb{F}_q[X]$  se dice una *raíz primitiva* módulo  $p(X)$  si la clase residual  $\overline{a(X)}$  genera al grupo cíclico  $(\mathbb{F}_q[X]/(p(X)))^\times$ . Dado  $a(X)$  designamos con  $\mathcal{A}(a(X)) = \{p(X) \in \mathbb{P}(q; X) ; a(X) \text{ es raíz primitiva módulo } p(X)\}$ . En esta situación subsiste también el análogo de la proposición 5.1.

Ahora bien, si  $a(X) = b(X)^\ell$ , donde  $\ell$  es un primo y  $\ell \mid (q^r - 1)$ , vemos que

$$a(X)^{(q^r-1)/\ell} \equiv b(X)^{q^r-1} \equiv 1 \pmod{p(X)} ,$$

$(q^r - 1)/\ell < q^r - 1$ , lo que muestra que  $\mathcal{A}((X)) = \emptyset$  si  $a(X)$  es una potencia  $\ell$ -ésima de un divisor  $\ell$  de  $q^r - 1$ . También, si  $a(X) = a$  es un polinomio constante, entonces  $a$  sólo puede ser raíz primitiva de polinomios primos  $p(X) = X - b$  de grado 1, y en este caso sólo si la clase residual  $\bar{a}$  tiene orden  $q - 1$  en el grupo  $(\mathbb{F}_q[X]/(x - b))^\times = \mathbb{F}_q^\times$ . De estos polinomios hay exactamente  $q$ ; luego  $\mathcal{A}(a(X))$  es finito si  $a(X) = a$  es constante. Todo esto condujo a la siguiente conjetura:

*Si  $a(X) \in \mathbb{F}_q[X]$  no es constante ni es una potencia  $\ell$ -ésima de un primo  $\ell$  que divide a  $q - 1$ , entonces  $\mathcal{A}(a(X))$  es infinito.*

La demostración de BILHARZ se reduce a verificar que la llamada *densidad de Dirichlet* de  $\mathcal{A}(a(X))$  es  $> 0$ , lo que implica que  $\mathcal{A}(a(X))$  es infinito, y conduce de manera natural a usar las funciones zeta de Dedekind de cierto tipo de extensiones galoisianas de  $\mathbb{F}_q[X]$ , para las cuales ya sabemos es válida la hipótesis de Riemann.

En realidad BILHARZ demuestra su teorema para la situación más general en que  $\mathbb{F}_q[X]$  es reemplazado por una de sus extensiones algebraicas finitas  $k$  y en vez de polinomios primos se habla de *divisores primos* de  $k$ . Es interesante anotar, finalmente, que en el caso  $k = \mathbb{F}_q[X]$ , la demostración de que  $\mathcal{A}(a(X))$  es infinito no requiere de la hipótesis de Riemann [7].

### §6. La conjetura de Borevich y Shafarevich sobre la serie de Poincaré de un polinomio de coeficientes $\ell$ -ádicos

En [8, problema 9, pág. 47] BOREVICH y SHAFAREVICH hicieron la siguiente pregunta: dado un primo racional fijo  $\ell$ , se  $\mathbb{Q}_\ell$  el cuerpo de los números  $\ell$ -ádicos y  $\mathbb{Z}_\ell$  el anillo de los enteros  $\ell$ -ádicos. Para un polinomio  $H(t_1, \dots, t_s)$  en  $\mathbb{Z}_\ell[t_1, \dots, t_s]$  denotemos con  $c(n; H)$  al número de ceros de la reducción  $H_n(t_1, \dots, t_s)$  de  $H(t_1, \dots, t_s)$  en el anillo residual  $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$ . ¿Es entonces la serie de Poincaré de  $H$

$$P(H; U) = \sum_{n=0}^{\infty} c(n; H)U^n \in \mathbb{Z}[[U]] , \quad (6.1)$$

donde  $c(0; H) = 1$ , una función racional de  $U$ ? Respuestas parciales a esta pregunta se conocían antes de 1973 (para esto remitimos a [13]), año en el cual IGUSA ([26], [27]) dio una respuesta general afirmativa, basada en el teorema de resolución de singularidades en característica cero demostrado antes por HIRONAKA. Sus resultados, sin embargo, no muestran cómo calcular efectivamente (6.1) como el cociente de dos polinomios en  $U$ . Más tarde, DENEFF [13] dio una nueva elegantísima demostración

de la conjetura, usando esencialmente el hecho que  $\mathbb{Q}_\ell$  admite eliminación de cuantificadores, con lo cual evitaba el profundo teorema de HIRONAKA. Relacionada con esta conjetura existe la siguiente, debida a HAYES y NUTT [23]:  $P(H; U) = q(U)/r(U)$ , donde  $q(U)$  y  $r(U)$  son polinomios en  $\mathbb{Z}[U]$  que cumplen las condiciones:  $q(0) = 1$  y  $r(U)$  es el producto de polinomios de la forma  $1 - \ell^m U^n$ , donde  $m \geq 0$  y  $n \geq 1$  son enteros para los cuales subsiste la desigualdad  $m \leq ns$ . Estos autores han denominado esta aserción la  $Q$ -conjetura.

Dada la analogía existente entre los cuerpos aritméticos de característica cero y los de característica  $> 0$  (es decir, las extensiones algebraicas finitas de  $\mathbb{F}_q[X]$ ), es natural plantearse la misma pregunta en este último caso. Sin embargo, en este caso no existe un teorema general de resolución de singularidades ([1], [2]) ni los anillos que interesan admiten eliminación de cuantificadores ([6]). Por estas razones parece que un ataque directo usando métodos elementales à la *Abhyankar*, podría ser interesante. En efecto, nosotros hemos demostrado en algunos casos especiales la validez del análogo de la conjetura de BOREVICH y SHAFAREVICH y, de contera, la  $Q$ -conjetura, usando propiedades aritméticas especiales del cuerpo  $L((Z))$  de las series meromorfas formales sobre un cuerpo finito  $L$ , puesto que el problema puede reducirse a esta situación, como pasamos a verificar ([4]).

Si  $K$  es un cuerpo aritmético de característica  $\ell > 1$ , es decir, una extensión algebraica finita de  $\mathbb{F}_q[X]$ , y si  $\mathfrak{p}$  es un divisor primo de  $K$ , consideremos el completado  $K_{\mathfrak{p}}$  de  $K$  en  $\mathfrak{p}$ . Si  $w_{\mathfrak{p}}$  representa a la correspondiente valuación discreta, denotemos con  $\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}}; w_{\mathfrak{p}}(x) \geq 0\}$  y  $\pi\mathcal{O}_{\mathfrak{p}} = \{x \in K_{\mathfrak{p}}; w_{\mathfrak{p}}(x) > 0\}$ , donde  $w_{\mathfrak{p}}(\pi) = 1$ , al anillo de los enteros  $\mathfrak{p}$ -ádicos y el único ideal primo de  $\mathcal{O}_{\mathfrak{p}}$ , respectivamente. En esta situación,  $L_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\pi\mathcal{O}_{\mathfrak{p}}$  es una extensión finita de  $\mathbb{F}_\ell$ , con, pongamos,  $q$  elementos. Con esta notación nuestra conjetura puede expresarse así:

Sea  $H(t_1, \dots, t_s) \in \mathcal{O}_{\mathfrak{p}}[t_1, \dots, t_s]$  y sea  $c(n; h)$  el número de ceros de la reducción de  $H$  en el anillo residual  $\mathcal{O}_{\mathfrak{p}}/\pi\mathcal{O}_{\mathfrak{p}}$  ( $n = 1, 2, \dots$ ). Entonces

$$P(H; U) := \sum_{n=0}^{\infty} c(n; H)U^n \in \mathbb{Z}[[U]] \quad (6.1)$$

donde  $c(0; H) = 1$ , es una función racional de  $U$ .

Como  $\mathcal{O}_{\mathfrak{p}} = L_{\mathfrak{p}}[[Z]]$ ,  $L_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}/\pi\mathcal{O}_{\mathfrak{p}}$ , basta demostrar la conjetura en un anillo  $L[[Z]]$ , donde  $L$  es un cuerpo finito de característica  $\ell$  y  $q$  elementos. Más precisamente, es suficiente demostrar que si  $c(n; H)$  designa al

número de ceros de  $H$  en el anillo residual  $L[[Z]]/(Z^n)$ , entonces (6.1) es una función racional de  $U$ .

El punto de partida nuestro es la versión especial del teorema de Taylor para la reducción  $H_n(t_1, \dots, t_s)$  módulo  $(Z^n)$  del polinomio  $H_n(t_1, \dots, t_s) \in L[[Z]][t_1, \dots, t_s]$  que nos permite concluir que un cero de  $H_n(t_1, \dots, t_s)$  produce exactamente  $q^{s-1}$  ceros de  $H_{n+q}(t_1, \dots, t_s)$  si la proyección de este cero módulo  $(Z)$  es un cero regular de  $H_1(t_1, \dots, t_s)$ , y en caso contrario, es decir, cuando esa proyección es un cero singular de  $H_1(t_1, \dots, t_s)$ , produce exactamente  $q^s$  si es que  $H_{n+1}(t_1, \dots, t_s)$  admite ceros que descienden del cero dado de  $H_n(t_1, \dots, t_s)$ . Por ejemplo, si todos los ceros de  $H_1(t_1, \dots, t_s)$  son regulares, obtenemos

$$P(H; U) = l + c(l; H) \frac{U}{1 - q^{s-1}U}$$

donde  $c(l; H)$  es el número de ceros de  $H_1(t_1, \dots, t_s)$ . El problema aparece cuando  $H_1(t_1, \dots, t_s)$  admite ceros singulares. El caso más sencillo de esta situación es el monomio

$$H(t) = (t - \alpha(Z))^e,$$

de la sola variable  $t$ , donde  $\alpha(Z) = \alpha_0 + \alpha_1 Z + \alpha_2 Z^2 + \dots + L[[Z]]$  y  $e \geq 1$ , para el cual encontramos

$$P(H; U) = 1 + \frac{U[1 + qU + \dots + q^{e-1}U^{e-1}]}{1 - q^{e-1}U^e}$$

Utilizando este resultado es posible entonces demostrar que la serie de Poincaré de un polinomio arbitrario en una sola variable:

$$H(t) = \beta(0) + \beta(1)t + \dots + \beta(m)t^m, \quad \beta(m) \neq 0$$

$\beta(i) \in L[[Z]]$  ( $0 \leq i \leq m$ ) es una función racional de  $U$ . También es posible de mostrar que la serie de Poincaré de un monomio  $H(t_1, \dots, t_s) = t_1^{e_1} \dots t_s^{e_s}$  es racional. Lo mismo para las formas cuadráticas no degeneradas [4].

#### REFERENCIAS

- [1] ABHYANKAR, S. 1975. *High-School algebra in algebraic geometry*. Historia Mathematica **2**, 567–572.
- [2] ABHYANKAR, S. 1976. *Historical ramblings in algebraic geometry and related algebra*. Amer. Mat. Monthly **83**, 409–449.
- [3] ALBIS, V. S. 1988. *Lecciones sobre la teoría aritmética de polinomios*. Bogotá: Universidad Nacional de Colombia. (Policopiado.)
- [4] 1989. ALBIS, V.S. & CHAPARRO, R. *On a conjecture of Borevich and Shafarevich in arithmetic function fields*. (Manuscrito.)
- [5] ARTIN, E. 1924. *Quadratische Körper in Gebiete der höheren Kongruenzen I, II*. Math. Zeitschrift **19**, 153–246.
- [6] BERLINE, C. & CHERLIN, G. 1981. *QE rings in characteristic p*. Proceedings of the Storrs Conference.
- [7] BILHARZ, H. 1937. *Primdivisoren mit vorgegebener Primdivurzel*. Math. Ann. **114**, 476–492.
- [8] BOREVICH, Z. I. & SHAFAREVICH, I. R. 1966. *Number Theory*. New York: Academic Press.
- [9] CAR, M. 1984. C. R. Acad. Sci. Paris, Ser. **A273**, 201–204
- [10] CAR, M. 1984. *Le théorème de Chen pour  $\mathbb{F}_q[X]$* . Diss. Math., 54 págs.
- [11] CATALAN, E. 1842. *Problème 48*. Nouvelles Annales de Mathématiques **1**, 520.
- [12] CHEN, Jing-run. 1966. *On the representation of a large even integer as the sum of a prime and the product of at most two primes*. Xexue Tongbao **17**, 385–386.
- [13] DENEFF, J. 1984. *The rationality of the Poincaré series associated to the p-adic points in a variety*. Inv. Math. **77**, 1–23.
- [14] EDWARDS, H. M. 1974. *Riemann's Zeta Function*. New York: Academic Press.
- [15] GAUSS, C. F. 1801. *Disquisitiones Arithmeticae*. Leipzig = *Recherches arithmétiques*. París: Courcier, 1806.
- [16] GOLDSTEIN, L. J. *Density questions in algebraic number theory*. Amer. Math. Monthly **78**, 342–353.
- [17] GREENLEAF, N. 1969. *On Fermat's equation in  $C(t)$* . Amer. Math. Monthly **76**, 808–809.
- [18] HARDY, G. H. 1914. *Sur les zéros de la fonction  $\zeta(s)$  de Riemann*. C. R. Acad. Sci. Paris **158**, 1012–1014.
- [19] HASSE, H. 1952. *Ueber die Artinsche Vermutung verwandte Dichtefrage*. Ann. Acad. Sci. Fennicae, Ser. A, I, Math.-Phy. **116**.
- [20] HAYES, D. R. 1963. *A polynomial analog of the Goldbach conjecture*. Bull. Amer. Math. Soc. **69**, 115–116.
- [21] HAYES, D. R. 1963. *Correction to "A polynomial..."*. Bull. Amer. Math. Soc. **69**, 493.
- [22] HAYES, D. R. 1966. *The expression of a polynomial as a sum of three irreducibles*. Acta Arith. **11**, 461–488.
- [23] HAYES, D. R. & NUTT, M. D. 1982. *Reflective functions on p-adic fields*. Acta Arith. **40**, 229–248.
- [24] HILBERT, D. 1902. *Problèmes futures des mathématiques*. C. R. 2éme. Congr. Int. Math. Paris.
- [25] HOOLEY, C. 1967. *On Artin's conjecture*. J. reine angew. Math. **225**, 209–220.
- [26] IGUSA, J.-I. 1974. *Complex powers and asymptotic expansions. I*. J. reine angew. Math. **268/269**, 110–130. II **278-279** (1975), 307–321.
- [27] IGUSA, J.-I. 1977. *Some observations on higher degree characters*. Amer. J. Math. **99**, 393–417.
- [28] KATZ, N. 1976. *An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields*. Proc. of Symposia in Pure Math. **28**, 275–305.
- [29] KORKINE, A. 1880. *sur l'impossibilité de la relation algébrique  $X^n + Y^n + Z^n = 0$* . C. R. Acad. Sci. Paris **90**, 303–304.
- [30] LIOUVILLE, R. 1879. *Sur l'impossibilité de la relation algébrique  $X^n + Y^n + Z^n = 0$* . C. R. Acad. Sci. Paris **87**, 1108–1110.
- [31] NATANSON, M. 1974. *Catalan's equation in  $K(t)$* . Amer. Math. Monthly **81**, 371–373.
- [32] RIBENBOIM, P. 1979. *13 Lectures on Fermat's Last Theorem*. New York/Heidelberg/Berlin: Springer-Verlag.

- [33] RIBENBOIM, P. 1984. *Remarks on existentially closed fields and diophantine equations*. Ren. Sem. Math. Univ. Padova **71**, 229–237.
- [34] RIEMANN, B. 1859. *Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse*. In *Gesammelte Werke*. New York: Dover, 1953.
- [35] SILVERMAN, J. H. 1982. *The Catalan equation over function fields*. Trans. Amer. Math. Soc. **273**, 201–205.
- [36] TIJDEMAN, R. 1976. *On the equation of Catalan*. Acta Arith. **29**, 197–209.
- [37] VINOGRADOV, I. M. 1937. *La representación de un número impar como la suma de tres números primos* (en ruso). Dokl. Akad. Nauk. SSSR, 139–142.
- [38] VINOGRADOV, I. M. 1971. *Fundamentos de la teoría de los números*. Moscú: Mir.
- [39] WEBB, W. A. 1983. *Sieve methods for polynomial rings over finite fields*. J. of Number Theory **16**, 343–355.
- [40] WEIL, A. 1948. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Paris: Hermann.
- [41] WEIL, A. 1949. *Number of solutions of equations in a finite field*. Bull. Amer. Math. Soc. **55**, 497–508.