Lecturas Matemáticas
Volumen **34** *(2) (2013), páginas 187–203*
ISSN 0120–1980

La conjetura de Goldbach en mundos paralelos al mundo de los enteros

Goldbach's conjecture in worlds parallel to the world of integers

Leonardo Fabio Chacón–Cortés.
Universidad Nacional de Colombia, Bogotá

Resumen. En este trabajo expositivo se plantean análogos de la conjetura de Goldbach en ciertos anillos de polinomios y se dan respuestas a los mismos.

Key words and phrases. Goldbach's conjecture, polynomial rings.

Abstract. In this expository paper analogous of Goldbach's conjecture are stated and studied in certain polynomial rings.

2010 AMS Mathematics Subject Classification. 11T55

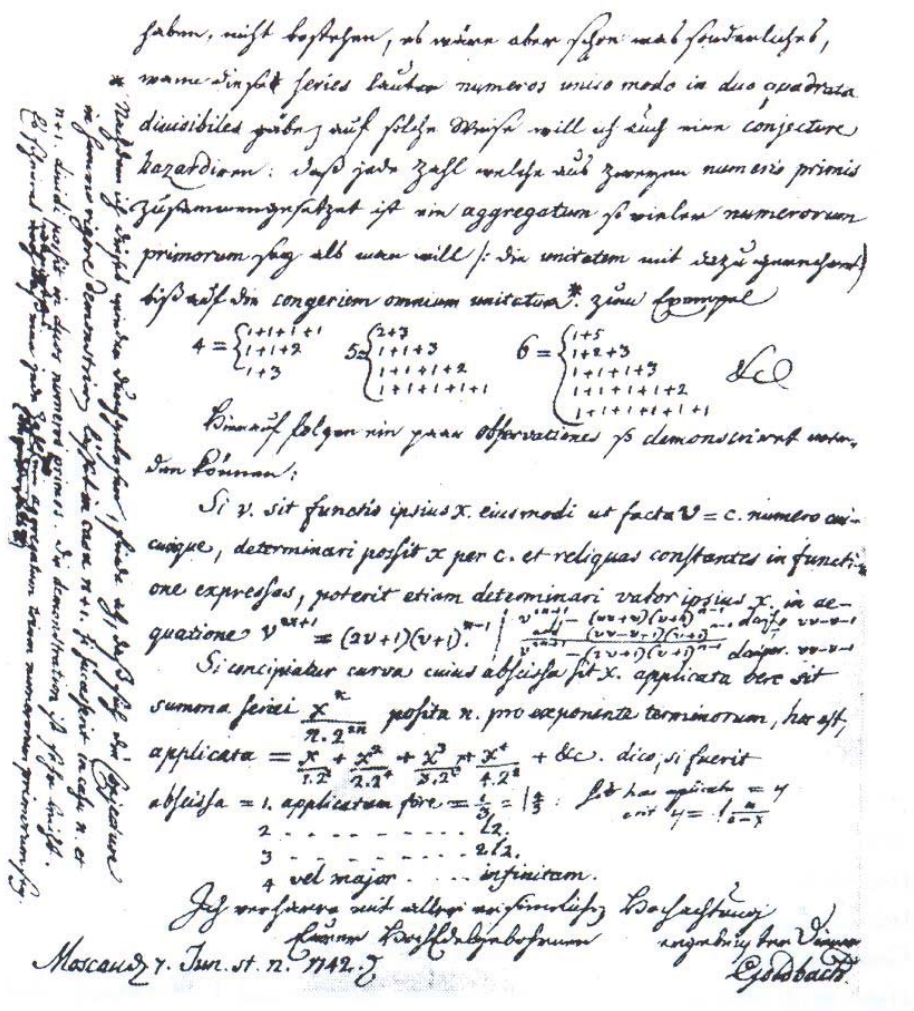
1. Introducción

La conjetura de Goldbach para los números enteros aparece en 1742 en una carta enviada a Leonhard Euler (1707-1783) por Christian Goldbach (1690-1764). En esencia el problema propuesto se concreta, hoy en día, en las siguientes dos conjeturas:

> **Conjetura 1.** *Todo número entero impar $n \geq 7$ puede expresarse como la suma de tres números primos.*

> **Conjetura 2.** *Todo número entero par ≥ 4 se puede expresar como suma de dos primos.*

La segunda conjetura implica la primera, pues si todo número par ≥ 4 se escribe como $2n - 2 = p_1 + p_2$ donde $n > 3$ y p_1, p_2 son primos, entonces podemos escribir $2n + 1 = p_1 + p_2 + 3 > 7$. Por esta razón la segunda conjetura se llama la *conjetura fuerte* (o *par* o *binaria*) de Goldbach, mientras que la primera se llama la *conjetura débil* (o *impar* o *ternaria*). Es fácil ver que estas descomposiciones en sumas de números primos no son únicas. Por ejemplo, $9 = 3 + 3 + 3 = 2 + 2 + 5$.



Carta de 1742 de Goldbach a Euler

Daremos ahora noticia de algunas de las vicisitudes de ambas conjeturas. Con respecto a la conjetura débil, HARDY & LITTLEWOOD [16] en 1932, usando su famoso método del círculo y asumiendo la hipótesis generalizada de Riemann (véase la sección de preliminares), probaron que existe una constante $N \in \mathbb{N}$ tal que todo $n > N$ es suma de tres números primos (véase [23, cap. X]). Más tarde, I. M. VINOGRÁDOV probó en 1937 ([32], [33] y [23, pág. 204]) el mismo resultado sin asumir la hipótesis generalizada de Riemann. Este resultado se conoce como el *teorema de Vinográdov* y se ha verificado que es suficiente

tomar $N = 3^{3^{15}}$ o $N = \exp(100\,000)$ [9]. La tarea que algunos se han impuesto ha sido tratar rebajar el valor de la constante N para tener la posibilidad de usar los ordenadores. Así, recientemente, en 2012, Oliveira e Silva ha encontrado que podemos tomar $N = 4 \times 10^{18}$ [25]. Por otro lado, más tarde (1997), asumiendo nuevamente la hipótesis de Riemann generalizada, Deshouiller, Effinger, te Riele & Zinoviev (véase [11]) demuestran que todo número entero impar $n > 7$ es la suma de tres primos. Recientemente, 2012, sin usar la hipótesis de Riemann, Terence Tao ha publicado que todo número impar mayor que 7 puede expresarse como la suma de a lo sumo cinco primos [31]. Sorprendentemente, este año de 2013, Harald Andrés Helfgott (matemático peruano) mediante su trabajo [21], que complementa su anterior trabajo [20], ha demostrado que la conjetura débil de Goldbach es cierta. Por su parte, el trabajo de Tao que acabamos de mencionar complementa un resultado de O. Ramaré [28] que dice que todo número natural par puede expresarse como la suma de a lo sumo seis números primos, resultado que tiene que ver con la conjetura fuerte. En cuanto a esta tenemos el siguiente resultado parcial, el mejor hasta el momento, debido a Jing-Run Chen [8]: *todo número entero par suficientemente grande es la suma de un número primo y un producto de no más de dos números primos*. Actualmente la mayoría de los matemáticos creen que la conjetura fuerte también es cierta y se basan en resultados como los mencionados anteriormente y la evidencia numérica obtenida por numerosos autores.

En este trabajo nos proponemos estudiar análogos de las conjeturas de Goldbach en ciertos anillos de polinomios. En la segunda sección establecemos, muchas veces sin demostraciones (en aras de la brevedad) pero con referencias precisas a literatura que creemos accesible, resultados necesarios para la comprensión de las siguientes secciones. En la tercera sección estudiamos el análogo del problema de Goldbach en el anillo $\mathbb{F}_q[X]$ de los polinomios en la indeterminada X y coeficientes en el cuerpo finito $\mathbb{F}_q$. En la cuarta sección el análogo de la conjetura de Goldbach se extiende a anillos de polinomios en una variable sobre algunos ciertos dominios de integridad. En la quinta sección examinamos Goldbach para el anillo $R[X_1, \ldots, X_m]$, donde R es un anillo que satisface las condiciones del teorema 4.2. Finalmente, en el apéndice se discuten algunos problemas asintóticos y de densidad.

2. Preliminares

2.1. Preliminares algebraicos. Empezamos esta sección con algunos resultados algebraicos conocidos que usaremos después. Supondremos de aquí en adelante que todos los anillos considerados son conmutativos y tienen elemento unidad. El grupo de las unidades de un anillo R lo designaremos con $R^\times$.

Como es costumbre, al polinomio nulo de un anillo de polinomios con coeficientes en un anillo en la indeterminada X no le asignamos grado alguno. El

grado de un polinomio distinto del polinomio cero lo designamos con $\partial A(X)$. Si $A(X)$ es un polinomio en $\mathbb{F}_q[X]$, definimos su norma $|A(X)|$ por la relación

$$|A(X)| = \begin{cases} q^{\partial A} & \text{si } A(X) \neq 0\,, \\ 0 & \text{si } A(X) = 0\,. \end{cases}$$

Dados los ideales $\mathfrak{a}_1$, $\mathfrak{a}_2$, ..., $\mathfrak{a}_n$ de un anillo R, no nulos y distintos entre sí, ellos se dicen *comaximales* si $\mathfrak{a}_i + \mathfrak{a}_j = R$ si $i \neq j$.

Proposición 2.1. *Si $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ son ideales comaximales de R, entonces los ideales $\mathfrak{a}_1^{n_1}, \ldots, \mathfrak{a}_n^{n_k}$ son ideales comaximales distintos de R, donde $n_1, \ldots, n_k \in \mathbb{N}$.*

Demostración. Veamos que $\mathfrak{a}_i$ y $\mathfrak{a}_j^{n_j}$ son comaximales. Como $\mathfrak{a}_i + \mathfrak{a}_j = R$ existen $a_i \in \mathfrak{a}_i$, $a_j \in \mathfrak{a}_j$ tal que $a_i + a_j = 1$, luego $a_j = 1 - a_i$ y $a_j^{n_j} = (1-a_i)^{n_j} = 1 + \sum_{t=1}^{n_j} \binom{n_j}{t} (-a_i)^t$ donde $a_i' = -\sum_{t=1}^{n_j} \binom{n_j}{t} (-a_i)^t \in A_i$, luego $a_j^{n_j} + a_i' = 1$ es decir $\mathfrak{a}_i$ y $\mathfrak{a}_j^{n_j}$ son comaximales. Análogamente se tiene que $\mathfrak{a}_i^{n_i}$ y $\mathfrak{a}_j$ son comaximales. Entonces se tiene que:

$$\begin{aligned} \mathfrak{a}_i + \mathfrak{a}_j^{n_j} &= R \\ \mathfrak{a}_i^{n_i} + \mathfrak{a}_j &= R \\ \mathfrak{a}_i + \mathfrak{a}_j &= R \end{aligned}$$

Sumando las dos primeras ecuaciones y usando la tercera se concluye que $\mathfrak{a}_i^{n_i} + \mathfrak{a}_j^{n_j} = R$, es decir, $\mathfrak{a}_i^{n_i}$, $\mathfrak{a}_j^{n_j}$ son comaximales. ☑

El siguiente teorema es una generalización del clásico teorema chino de los restos en el anillo $\mathbb{Z}$ (véanse [5, pág. 5] y [24]).

Teorema 2.1 (Teorema chino de los restos)**.** *Sea R un anillo, y sean $\mathfrak{a}_1, \ldots \mathfrak{a}_n$ ideales comaximales de R. Entonces, dada una familia finita cualquiera de elementos $a_1, \ldots, a_n \in R$, existe un elemento $a \in R$, tal que $a - a_i \in \mathfrak{n}_i$ para cada $1 \leq i \leq n$.*

Lema 2.1. *Dados dos primos distintos p, q, existen enteros r, s tales que $rp + sq = 1$, $p \nmid r$ y $q \nmid s$.*

Demostración. Considerando el siguiente sistema de congruencias $rp \equiv 1 \pmod{q}$ y $r \equiv 1 \pmod{p}$, el cual por el teorema 2.1 tiene solución para r. Es decir existen enteros r', s' tales que $r'p + s'q = 1$ y $p \nmid r'$. Intercambiando los papeles de p y q en el sistema tenemos que existen enteros r'', s'' tales que $r''p + s''q = 1$ y $q \nmid s''$. Si $q \nmid s'$ o $p \nmid r''$ hemos terminado. Ahora si $q \mid s'$ y $p \mid r''$ considere $2(r'p + s'q) - (r''p + s''q) = 1$, luego $(2r' - r'')p + (2s' - s'')q = 1$ como $p \nmid r'$, $p \mid r''$, $q \nmid s''$ y $q \mid s'$. Entonces $r = 2r' - r''$ y $s = 2s' - s''$, cumplen lo pedido. ☑

Un conocido resultado acerca de polinomios irreducibles en $\mathbb{Z}[\mathbb{X}]$ es el siguiente.

Teorema 2.2 (Criterio de Eisenstein)**.** *Sea p un primo en $\mathbb{Z}[\mathbb{X}]$, $H(X) = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ con $a_n \neq 0 \pmod p$, pero $a_i \equiv 0 \pmod p$ para todo $i < n$, $a_0 \neq 0 \pmod{p^2}$. Entonces $H(X)$ es irreducible sobre $\mathbb{Q}$ (por tanto, irreducible en $\mathbb{Z}[\mathbb{X}]$)* (véase [15]).

Definición 2.1. Si $H(X) = a_nX^n + \cdots + a_1X + a_0 \in R[X]$ y el ideal generado por $(a_0, a_1, \ldots, a_n)$ es el anillo R decimos que $H(X)$ es un *polinomio primitivo.*

La siguiente proposición es la versión generalizada del criterio de Eisenstein para dominios de integridad y tendrá un papel central en el estudio del problema de Goldbach en cierto tipo de dominios. Como veremos en seguida, su prueba es similar a la del clásico teorema anterior, el cual es uno de sus corolarios.

Proposición 2.2 (Criterio de Einsentein para anillos de polinomios sobre un dominio de integridad)**.** *Sea $\mathfrak{p}$ un ideal primo de un dominio de integridad R y $H(X) = a_nX^n + \cdots + a_1X + a_0 \in R[X]$ un polinomio no constante para el cual sus coeficientes satisfacen*

(1) $a_0, a_1, \ldots, a_{n-1} \in \mathfrak{p}$.
(2) $a_0 \notin \mathfrak{p}^2$.
(3) $a_n \notin \mathfrak{p}$.
(4) $(a_0, a_1, \ldots, a_{n-1}, a_n) = R$, *es decir, H es primitivo.*

Entonces H es irreducible en $R[X]$.

Demostración. Supongamos que H no es irreducible de modo que $H(X) = A(X)B(X)$ donde $A(X)$, $B(X) \in R[X]$ y no son ambos nulos. Tomando la factorización módulo $\mathfrak{p}$ tenemos $\overline{H}(X) = \overline{A}(X)\overline{B}(X) = \overline{a}_nX^n \in (R/\mathfrak{p})[X]$. Por la factorización única en el anillo factorial $(R/\mathfrak{p})[X]$, tenemos $\overline{A}(X) = \overline{a}X^i$, $\overline{B}(X) = \overline{b}X^j$, donde $\overline{a}_n = \overline{ab}$. Si $\overline{A}(X)$, $\overline{B}(X)$ son ambos polinomios no constantes entonces los términos constantes de $A(X)$ y $B(X)$ están en $\mathfrak{p}$; luego el término constante de H esta en $\mathfrak{p}^2$ contrariando la hipótesis (2). Entonces $\overline{A}(X)$ o $\overline{B}(X)$ debe ser constante. Como $a_n \notin \mathfrak{p}$ entonces ninguno de los coeficientes directores de $A(X)$ y de $B(X)$ están en $\mathfrak{p}$. Luego

$$\partial\overline{A}(X) = \partial A(X);$$
$$\partial\overline{B}(X) = \partial B(X);$$

como $\overline{A}(X)$ o $\overline{B}(X)$ es constante entonces $A(X)$ o $B(X)$ debe ser constante. Sin pérdida de generalidad, supongamos que $A(X) = c$, de modo que $H(X) = cB(X)$, así $c \mid a_i$ para $i = 0, \ldots, n$. Finalmente, $R = (a_0, \ldots, a_{n-1}, a_n) \subset (c)$, es decir, c es unidad en R; lo que implica que H es irreducible sobre R. ☑

Recordemos la siguiente definición [4, pág. 5]:

Definición 2.2. El *radical de Jacobson* $\mathrm{Rad}\,(R)$ de un anillo conmutativo es la intersección de todos los ideales maximales de R.

En términos del radical de Jacobson podemos enunciar el siguiente utilísimo resultado:

Lema 2.2 (Lema de Nakayama)**.** *Sea M un R-módulo finitamente generado (f.g.) y $\mathfrak{a}$ un ideal de R contenido en radical de Jacobson $Rad(R)$ de R. Entonces $\mathfrak{a}M = M$ implica $M = 0$* (véase [4]).

Dado que $K[X]$ es un dominio de factorización única, el siguiente resultado permite hablar de los elementos primos e irreducibles de $K[X]$, el anillo de polinomios en la indeterminada X y coeficientes en un cuerpo K, sin hacer ningún tipo de distinción entre ellos [5, pág. 42].

Teorema 2.3. *R es un dominio de factorización única (UFD) si y sólo si para todo elemento no nulo diferente de una unidad de R se escribe como un producto de elementos primos.*

2.2. Preliminares de la teoría de números. Con $\mathbb{N}^*$ designamos al conjunto de los enteros positivos, es decir, al conjunto de los enteros estrictamente mayores que 0. Una función $f : \mathbb{N}^* \to \mathbb{C}$ se dice una *función aritmética*. Si $f(mn) = f(m)f(n)$ cuando $\text{m. c. d.}(m, n) = 1$ decimos que f es *multiplicativa*. Si $f(mn) = f(m)f(n)$ para todo m y todo n, decimos que F *completamente multiplicativa*.

Definición 2.3. Si $n \in \mathbb{N}^*$ la función de Möbius $\mu(n) : \mathbb{N}^* \to \mathbb{C}$ está definida por

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1\,, \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ si los primos } p_i \text{ son distintos}\,, \\ 0 & \text{si } n \text{ tiene factores cuadráticos}\,. \end{cases}$$

El siguiente es un célebre resultado de Möbius. Su demostración puede encontrarse en numerosos libros de teoría de números, en particular, en [2].

Proposición 2.3 (Fórmula de inversión de Möbius)**.** *Si f y g son funciones aritméticas, entonces*

$$g(m) = \sum_{d|m} f(d) \quad \Leftrightarrow \quad f(m) = \sum_{d|m} \mu(d) g\left(\frac{m}{d}\right)\,.$$

Un *carácter de Dirichlet* es una función aritmética completamente multiplicativa $\chi : \mathbb{N}^* \to \mathbb{C}$ para la cual existe un entero positivo k con $\chi(n+k) = \chi(n)$ para todo $n \in \mathbb{N}^*$ y $\chi(n) \neq 0$ siempre que $\text{m. c. d.}(n, k) > 1$ y $\chi(n) = 0$ en caso contrario.

Para cada carácter χ de Dirichlet se define la función L o serie de Dirichlet correspondiente mediante

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

y todo número complejo s con parte real > 1.

La *hipótesis generalizada de Riemann* establece que para todo carácter de Dirichlet χ y todo número complejo s tal que $L(\chi, s) = 0$, si la parte real de s se encuentra comprendida entre 0 y 1, entonces es $1/2$. El caso $\chi(n) = 1$ para todo n conduce a la hipótesis original de Riemann.

El siguiente resultado se conoce como el *teorema de los números primos*: *Si $\pi(x)$ denota el número de primos que son menores o iguales a x, entonces $\pi(x) \sim \dfrac{x}{\log x}$ para valores grandes de x.*

3. El problema de Goldbach en $\mathbb{F}_q[X]$

El análogo del problema de Goldbach en el caso de anillos de polinomios sobre cuerpos finitos y algunos dominios de integridad, es de una sencillez envidiable comparado con el mismo problema en los números enteros. Además, en $\mathbb{F}_q[X]$ es válido el análogo de la hipótesis generalizada de Riemann ([14, págs. 299 & sigs.], [34]), lo cual nos proporciona información sobre la distribución de los primos en $\mathbb{F}_q[X]$.

Como $\mathbb{F}_q[X]$ es factorial las nociones de elemento primo y de elemento irreducible coinciden (teorema 2.3). Designaremos con $M(q\,;X)$ al conjunto de los polinomios unitarios de $\mathbb{F}_q[X]$ y con $P(q;X)$ a los polinomios unitarios irreducibles de $\mathbb{F}_q[X]$.

La siguiente proposición se debe Gauss y cuenta el número elementos de $P(q;X)$ de grado m.

Proposición 3.1. *El número de elementos de $P(q;X)$ de grado m está dado por*

$$\natural(m) = \frac{1}{m}\sum_{d|m}\mu\Big(\frac{m}{d}\Big)q^d = \frac{1}{m}\Big\{q^m - \sum_{p_i} q^{m/p_i} + \sum_{p_i\,,p_j} q^{m/p_ip_j} - \cdots\Big\}$$

Una demostración de esta proposición se encuentra en [12, pág. 377].

Definición 3.1. Un polinomio $H(X) \in M(q\,;X)$ se llama *par* si $q = 2$ y $H(X)$ es divisible por X o $X + 1$; en caso contrario, $H(X)$ se llama *impar*. Es decir, para todo $q \neq 2$, todo $H(X)$ es impar.

Como veremos ahora existen diversas versiones del problema de Goldbach en el anillo $\mathbb{F}_q[X]$. La primera que expondremos, debida a Hayes [17], está contenida en el siguiente teorema :

Teorema 3.1. *Sea $H(X)$ un polinomio no constante en $\mathbb{F}_q[X]$ con $q \gg \partial H$. Entonces podemos escribir $H(X) = P_1(X) + P_2(X)$ donde P_1 y P_2 son irreducibles en $\mathbb{F}_q[X]$ y $\partial P_1 = \partial P_2 = \partial H + 1$.*

Demostración. Sea $\partial H = h$. Por la proposición 3.1 tenemos

$$\natural(h+1) = \frac{1}{h+1} \sum_{d|(h+1)} q^{\frac{h+1}{d}} \mu(d);$$

desarrollando esta suma, obtenemos

$$\natural(h+1) = \frac{q^{h+1}}{h+1} + \frac{1}{h+1} \sum_{2 \leq d|(h+1)} q^{\frac{h+1}{d}} \mu(d)$$

Ahora consideremos:

$$\left| \natural(h+1) - \frac{q^{h+1}}{h+1} \right| = \frac{1}{h+1} \left| \sum_{2 \leq d|(h+1)} q^{\frac{h+1}{d}} \mu(d) \right| \leq \frac{1}{h+1} \sum_{d=1}^{\left\lfloor \frac{h+1}{2} \right\rfloor} q^d$$
$$\leq \frac{q^{\left\lfloor \frac{h+1}{2} \right\rfloor}}{h+1} (1 + \frac{1}{q} + \dots) \leq \frac{q^{\frac{h+1}{2}}}{h+1} \frac{q}{q-1} < \frac{q^{\frac{h+1}{2}}}{h+1} 2 \,.$$

Luego

$$\natural(h+1) = \frac{q^{h+1}}{h+1} + O\left(\frac{q^{\frac{h+1}{2}}}{h+1} \right)$$

cuando $q \to \infty$. Por otro lado, al considerar el conjunto $\{A \in P(q;X) : \partial A = h+1\}$ módulo H tenemos $\varphi(H)$ clases de equivalencia, donde $\varphi(H)$ es el número de polinomios de grado menor $\partial H = h$ que son primos relativos con H. Entonces $\varphi(H) < q^h$ ya que tenemos q^h polinomios de grado $h-1$ sobre F_q contando el polinomio nulo. Entonces

$$\varphi(H) < \natural(h+1);$$

es decir, en al menos una clase hay dos polinomios P_1 y P_2 de grado $h+1$, luego $P_1(X) - P_2(X) \equiv 0$ (mód H). Esto significa que existe $A(x) \in \mathbb{F}_q[X]$ no nulo tal que $P_1(X) - P_2(X) = A(X)H(X)$. Como $\partial(P_1 - P_2) \leq h$ pues son polinomios unitarios y $\partial(AH) = \partial A + h$, entonces $\partial A = 0$, $A \in \mathbb{F}_q^{\times}$; luego $P_1(X) - P_2(X) = AH(X)$ implica que $A^{-1}P_1(X) - A^{-1}P_2(X) = H(X)$, lo que se quería demostrar. ☑

Nota. Esta descomposición de H no es única, como se muestra en los siguientes ejemplos.

Ejemplo 3.1. En $\mathbb{F}_3[X]$

$$\underbrace{X^3 + X + 1}_{P_1} - (\underbrace{X^3 - X^2 + X + 1}_{P_2}) = \underbrace{X^2}_{H}$$

$$\underbrace{X^3 + X^2 - X + 1}_{P_1'} - (\underbrace{X^3 - X + 1}_{P_2'}) = \underbrace{X^2}_{H}$$

Ejemplo 3.2. En $\mathbb{F}_3[X]$

$$\underbrace{-X^3-X^2-1}_{P_1}+\underbrace{X^3-X^2+X+1}_{P_2}=\underbrace{-2X^2+X}_{H}$$

$$\underbrace{X^3-X^2+1}_{P_1'}+\underbrace{-X^3-X^2+X-1}_{P_2'}=\underbrace{-2X^2+X}_{H}$$

El lector podrá verificar fácilmente que P_1, P_2, P_1', P_2' son irreducibles en $\mathbb{F}_3[X]$.

También tenemos una fórmula asintótica para calcular el número de tales descomposiciones de H. Más precisamente, si $H \in \mathbb{F}_q[X]$ y $N(H)$ es el número de parejas P_1 y P_2 irreducibles en $\mathbb{F}_q[X]$ que satisfacen: $\partial P_1 = \partial P_2 = \partial H + 1$, $P_1 \neq P_2$ y $P_1 - P_2 \equiv 0 \pmod{H}$. Entonces

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

cuando $h \to \infty$. Esta fórmula es reminiscente de la que demostró Vinográdov para el caso de los números enteros (véanse [32] y [23, pág. 203]).

En la sección 6 se encuentra un esbozo de la prueba de este resultado.

Otros análogos de la conjetura de Goldbach en $\mathbb{F}_q[X]$ son los siguientes resultados:

Proposición 3.2. *Todo polinomio $H(X) \in M(q;X)$ de grado n, donde la característica de $\mathbb{F}_q$ es impar y s es suficientemente grande, puede escribirse como $H = P_1 + P_2$ donde los polinomios P_1, $P_2 \in \mathbb{F}_{q^s}[X]$ son irreducibles y unitarios con $\partial P_1 = n$, $\partial P_2 = n-1$. Además si $\partial H = n$ y q satisface la desigualdad $q > 8(n+6)^{2n^2}$, entonces P_1 y P_2 pueden tomarse en $\mathbb{F}_q[X]$.*

Este resultado fue demostrado por Andreas O. Bender usando geometría algebraica (véase [7]).

Proposición 3.3. *Todo polinomio $H(X) \in M(q;X)$ con $\partial H = r \geq 2$ excepto cuando q es par. Puede expresarse como $H = P_1 + P_2 + P_3$ donde P_1, P_2, P_3 son irreducibles unitarios en $\mathbb{F}_q[X]$ y $\partial P_1 = r$, $\partial P_2 < r$ y $\partial P_3 < r$.*

Este resultado fue obtenido por G. Effinger y David R. Hayes (véase [13]) y su demostración se hace en tres pasos: primero se obtiene un teorema asintótico análogo al teorema de Vinográdov para el caso de los números enteros; luego con una serie de teoremas se reducen los casos no cubiertos por el teorema asintótico a un número finito bastante manejable, y por último se realiza una verificación computarizada de todos los casos restantes.

Los siguientes ejemplos justifican la restricción de la proposición anterior.

Ejemplo 3.3. Este es un polinomio par de grado arbitrario el cual no admite la anterior descomposición. El polinomio $X^{4r} + X^{2r} \in \mathbb{F}_2[X]$ ($r \in \mathbb{N}$), es par

ya que $H(X) = X^{4r} + X^{2r} = (X+1).(X^{4r-1} - X^{4r-2} + \cdots + X^{2r}) = (X+1).X.(X^{4r-2} - X^{4r-3} + \cdots + X^{2r-1})$. Si H admite tal descomposición $X^{4r} + X^{2r} = P_1(X) + P_2(X) + P_3(X)$, sean a_0, b_0, c_0 los términos constantes de P_1, P_2 ,P_3 respectivamente, luego $a_0 + b_0 + c_0 \equiv 0$ (mód 2), es decir, alguno de estos términos debe ser cero módulo 2. Si $a_0 \equiv 0$ (mód 2), como $\partial P_1 = 4r \geq 1$, $X \mid P_1$ lo cual es una contradicción pues P_1 es irreducible. Si $b_0 \equiv 0$ (mód 2) y si $\partial P_2 \geq 2$, $X \mid P_2$ lo cual es una contradicción pues P_2 es irreducible. Si $c_0 \equiv 0$ (mód 2) y si $\partial P_3 \geq 2$, $X \mid P_3$ lo cual es una contradicción pues P_3 es irreducible. Ahora si $b_0 \equiv 0$ (mód 2) y si $\partial P_2 = 1$ entonces $P_2(X) = X$, así $X^{4r} + X^{2r} - X - P_1(X) = P_3(X)$, pero esto es una contradicción ya que todo polinomio irreducible sobre $\mathbb{F}_2$ debe tener un número impar de términos de lo contrario 1 sería raíz. Similarmente se llega a una contradicción si $c_0 \equiv 0$ (mód 2) y si $\partial P_1 = 1$. Entonces H no admite tal descomposición.

Ejemplo 3.4. Veamos que los polinomios de la forma $H(X) = X^2 + \alpha \in \mathbb{F}_{2^n}[X]$ no admiten la anterior descomposición. En efecto,

$$\underbrace{X^2 + \alpha}_{H} = \underbrace{X^2 + bX + c}_{P_1} + \underbrace{X + d}_{P_2} + \underbrace{X + e}_{P_3},$$

luego $bX + X + X = 0X$, pero $bX + X + X = bX = 0X$ entonces $b = 0$. Entonces $P_1(X) = X^2 + c$, pero este polinomio no es irreducible ya que la ecuación $X^2 + c = 0$ tiene solución en $\mathbb{F}_{2^n}$ para todo $c \in \mathbb{F}_{2^n}$. En efecto, todo elemento $c \in \mathbb{F}_{2^n}$ es raiz del polinomio $X^{2^n} - X$, es decir $(c^{2^{n-1}})^2 - c = 0$, como la característica de $\mathbb{F}_{2^n}$ es 2 se tiene que $(c^{2^{n-1}})^2 + c = 0$ $(1 = -1)$.

4. Una conjetura de Goldbach para el anillo de polinomios en una variable sobre algunos dominios de integridad

D. Hayes [18, 1965] es el primero en establecer el primer análogo de Goldbach para $\mathbb{Z}[X]$. Él demostró que para todo polinomio unitario $H(X) \in \mathbb{Z}[\mathbb{X}]$, existen polinomios P_1 y P_2 irreducibles en $\mathbb{Z}[X]$ tal que $H(X) = P_1(X) + P_2(X)$. Este resultado puede ser extendido a cualquier polinomio no constante $H(X) \in \mathbb{Z}[X]$ [29]. Usando el criterio de Eisenstein se prueba el siguiente resultado.

Teorema 4.1 (Goldbach para $\mathbb{Z}[X]$)**.** *Para todo polinomio no constante $H(X) \in \mathbb{Z}[X]$, existen polinomios P_1 y P_2 irreducibles en $\mathbb{Z}[X]$ con $\partial P_1 = \partial P_2 = \partial H$ tal que $H(X) = P_1(X) + P_2(X)$.*

Demostración. Sea $H(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, construyamos $P_1(X) = b_nX^n + a_{n-1}X^{n-1} + \cdots + b_1X + b_0$ y $P_2(X) = c_nX^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ que verifiquen el teorema. Tomemos b_n y $c_n \in \mathbb{Z}$ con $a_n = b_n + c_n$ y dos primos impares p, q tales que $p \nmid b_n$, $p \nmid a_0$, $q \nmid c_n$ y $q \nmid a_0$. Por el algoritmo de Euclides existen enteros k, m tales que $kp + mq = 1$ tomemos $b_i = a_ikp$ y $c_i = a_imq$ para $1 \leq i \leq n-1$. En consecuencia $b_i + c_i = a_i$, $p \mid b_i$ y $q \mid c_i$ por el lema 2.1 existen enteros r, s tales que $rp + sq = 1$ y $p \nmid r$, $q \nmid s$, sea

$b_0 = a_0rp$ y $c_0 = a_0sq$, luego $a_0 = b_0 + c_0$ y además $p \mid b_0$, $q \mid c_0$, $p^2 \nmid b_0$ y $q^2 \nmid c_0$. En conclusión P_1 y p satisfacen las hipótesis del teorema 2.2, luego P_1 es irreducible, similarmente se concluye que P_2 es irreducible y por construcción tenemos $H(X) = P_1(X) + P_2(X)$. ☑

La anterior demostración no sólo prueba la existencia de una descomposición de H, si no que además muestra un algoritmo para encontrar tal descomposición, la cual claramente no es única.

Ejemplo 4.1. Sea $H(X) = 2011X^{2010} + 2010X^{2009} + \cdots + (i+1)X^i + \cdots + 1 \in \mathbb{Z}[X]$.

$$P_1(X) = 11X^{2010} + 2010 \times 25X^{2009} + \cdots + (i+1) \times 25X^i + \cdots - 11 \times 5$$
$$P_2(X) = 2000X^{2011} - 2010 \times 24X^{2009} - \cdots - (i+1) \times 24X^i - \cdots + 22 \times 3.$$

Luego $H = P_1 + P_2$, donde P_1, P_2 son irreducibles en $\mathbb{Z}[X]$ (teorema 2.2, $p = 5$ y $q = 3$ respectivamente). Otra descomposición de H es:

$$P_1'(X) = 2001X^{2010} + 2010 \times 22X^{2009} + \cdots + (i+1) \times 22X^i + \cdots + 22$$
$$P_2'(X) = 10X^{2011} - 2010 \times 21X^{2009} - \cdots - (i+1) \times 21X^i - \cdots - 21.$$

Luego $H = P_1' + P_2'$, donde P_1', P_2' son irreducibles en $\mathbb{Z}[X]$ (teorema 2.2, $p = 11$ y $q = 7$ respectivamente).

Con un poco más de cuidado es posible generalizar el anterior teorema cuando sustituimos $\mathbb{Z}$ por ciertos dominios de integridad.

Teorema 4.2. *Sea R un dominio de integridad para el cual existen dos ideales maximales distintos $\mathfrak{p}$ y $\mathfrak{q}$ que satisfacen*

1. $\mathfrak{p} \subsetneq \mathfrak{p}^2$ *y* $\mathfrak{q} \subsetneq \mathfrak{q}^2$.
2. $R/\mathfrak{p}$ *y* $R/\mathfrak{q}$ *tienen al menos dos elementos* ($N(\mathfrak{p}) \geq 2$ *y* $N(\mathfrak{p}) \geq 2$).

Entonces para todo polinomio $H(X) \in R(X)$ no constante, $H(X) = P_1(X) + P_2(X)$, donde P_1 y P_2 son irreducibles en $R[X]$ y $\partial P_1 = \partial P_2 = \partial H$.

Demostración. Tomemos $H(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in R[X]$ no constante ($a_n \neq 0$). Si $\partial H = 1$ y H no es unitario

$$H(X) = a_1X + a_0 = \underbrace{(a_1 - 1)X + 1}_{P_1} + \underbrace{X + (a_0 - 1)}_{P_2}$$

como P_1 y P_2 son lineales, son irreducibles en $R[X]$. Ahora si $\partial H = 1$ y H es unitario escojamos un $r \in R$, $r \neq 0$ y $r \neq -1$; esto es posible ya que de no ser así $R \cong \mathbb{Z}/2\mathbb{Z}$ el cual es un cuerpo y no tendría ideales maximales no nulos contradiciendo la hipótesis.

$$H(X) = X + a_0 = \underbrace{(rX + 1)}_{P_1} + \underbrace{(1 - r)X - 1 + a_0}_{P_2}$$

como P_1 y P_2 son lineales, son irreducibles en $R[X]$. Finalmente si $\partial H \geq 2$, el objetivo es construir los polinomios $P_1(X) = \sum_{i=1}^{n} b_i X^i$ y $P_2(X) = \sum_{i=1}^{n} c_i X^i$ que cumplan las hipótesis de la proposición 2.2(para $\mathfrak{p}$ y $\mathfrak{q}$ respectivamente) y además $P_2(X) = H(X) - P_1(X)$. Tomemos $p \in \mathfrak{p} - \mathfrak{p}^2$ y $q \in \mathfrak{q} - \mathfrak{q}^2$, luego se debe tener que:

1. $b_i \equiv 0 \pmod{\mathfrak{p}}$; $c_i = a_i - b_i \equiv 0 \pmod{\mathfrak{q}}$ $\forall i = 1, 2 \ldots, n-1$,
2. $b_0 \equiv p \pmod{\mathfrak{p}^2}$; $c_0 = a_0 - b_0 \equiv q \pmod{\mathfrak{q}^2}$,
3. $b_n \neq 0, a_n \pmod{\mathfrak{p}}$; $b_n \neq 0, a_n \pmod{\mathfrak{q}}$. Esta elección de b_n es posible ya que $R/\mathfrak{p}$ y $R/\mathfrak{q}$ tienen más de dos elementos.

Para resolver (1) apliquemos el **teorema chino de los residuos(T.C.R)** 2.1 a (1) ya que los ideales $\mathfrak{p}$ y $\mathfrak{q}$ son maximales (en particular comaximales) de igual manera resolvemos (2) ya $\mathfrak{p}^2$ y $\mathfrak{q}^2$ son comaximales. La solución de los anteriores tres sistemas garantizan la existencia de P_1, P_2 satisfaciendo las tres primeras condiciones del criterio de Eisentein 2.2. Para verificar la condición (4) del criterio de Eisenstein, sea $(b_2, \ldots, b_n)$ parte de la solución de (1) y (3) y consideremos el sistema

$$\begin{aligned} b_0 &\equiv p \pmod{\mathfrak{p}^2}, \\ a_0 - b_0 &\equiv q \pmod{\mathfrak{q}^2}, \\ b_0 &\equiv 1 \pmod{b_n}. \end{aligned}$$

como b_n no esta en $\mathfrak{q}^2$ ni en $\mathfrak{p}^2$ (es solución de (3)) $\mathfrak{q}^2$, $\mathfrak{p}^2$ y (b_n) son comaximales. Aplicando el **T.C.R** encontramos b_0.

Para encontrar b_1 consideramos el sistema

$$\begin{aligned} b_1 &\equiv 0 \pmod{\mathfrak{p}}, \\ a_1 - b_1 &\equiv 0 \pmod{\mathfrak{q}}, \\ a_1 - b_1 &\equiv 1 \pmod{a_n - b_n}. \end{aligned}$$

como $\mathfrak{p}$,$\mathfrak{q}$ y (a_n, b_n) son comaximales ya que $a_n - b_n$ no está en $\mathfrak{p}$ ni en $\mathfrak{q}$(son solución de (3)) aplicando el **T.C.R** encontramos b_1.

Luego $(b_0, \ldots, b_n) \supset (b_0, b_n) = (1)$ ya que $b_0 - 1 \in (b_n)$.

Como $c_i = a_i - b_i$ $i = 0, 1, 2 \ldots, n$. Tomemos $(c_0, \ldots, c_n) \supset (c_1, c_n) = (a_1 - b_1, a_n - b_n) = (1)$ ya que $a_1 - b_1 - 1 \in (a_n - b_n)$. Así tenemos la cuarta condición para P_1 y P_2. Entonces por la proposición 2.2 P_1 y P_2 son irreducibles y por construcción $H(X) = P_1(X) + P_2(X)$. ☑

La anterior demostración no solo garantiza la existencia de una descomposición para H, sino que además proporciona un algoritmo para encontrarla y deja ver claramente que dicha descomposición no es única.

El siguiente lema muestra que existen bastantes anillos para los cuales se puede aplicar el teorema anterior .

Lema 4.1. *Sea R un dominio noetheriano y M un ideal máximal no nulo de R. Entonces $M^2 \subsetneq M$.*

Demostración. Trivialmente tenemos $M^2 \subseteq M$, supongamos que $M = M^2$, tomemos $S = R - M$, así $S^{-1}R$ es noetheriano (en particular f.g) y además local con ideal maximal $S^{-1}M$; si vemos a la vez a $S^{-1}M$ como un $S^{-1}R-$módulo tenemos que:

$$S^{-1}M(S^{-1}M)_{S^{-1}R} = S^{-1}M^2 = S^{-1}M_{S^{-1}R};$$

entonces por el lema de Nakayama $S^{-1}M_{S^{-1}R} = 0$ entonces $M = 0$ así $M^2 \subsetneq M$. ☑

5. Goldbach para el anillo $\mathbf{R[X_1, \ldots, X_m]}$

Proposición 5.1. *Suponga que R es un dominio que satisface las condiciones (1) y (2) del teorema 4.2. Entonces el dominio $R[X_1, \ldots, X_m]$ $(m \geq 2)$ también satisface las condiciones (1) y (2) del teorema 4.2.*

Demostración. Supongamos que $\mathfrak{p}$ y $\mathfrak{q}$ son los ideales maximales de R para los cuales se satisfacen las condiciones (1) y (2) del teorema anterior, consideremos los ideales $P[X_1, \ldots, X_m]$, $Q[X_1, \ldots, X_m]$ de $R[X_1, \ldots, X_m]$ y el siguiente isomorfismo

$$R[X_1, \ldots, X_m]/P[X_1, \ldots, X_m] \cong R/\mathfrak{p};$$

entonces $P[X_1, \ldots, X_m]$ es un ideal máximal de $R[X_1, \ldots, X_m]$ el cual tiene más de dos elementos (pues $R/\mathfrak{p}$ tiene más de dos elementos). Para ver (1), sea $p \notin \mathfrak{p} - \mathfrak{p}^2$. Entonces $p \notin (P[X_1, \ldots, X_m])^2$ y así $(P[X_1, \ldots, X_m])^2 \subsetneq P[X_1, \ldots, X_m]$. Similarmente se verifican las condiciones (1) y (2) para el ideal $Q[X_1, \ldots, X_m]$ de $R[X_1, \ldots, X_m]$. ☑

Lema 5.1. *Sea R un anillo que satisface las condiciones (1) y (2) del teorema 4.2. Entonces todo $H \in R[X_1, \ldots, X_m]$ no constante es la suma de dos polinomios irreducibles.*

Demostración. Veamos a H como un polinomio en la variable X_m sobre el anillo $R[X_1, \ldots, X_{m-1}]$. Como R satisface las condiciones (1) y (2) entonces el anillo $R[X_1, \ldots, X_{m-1}]$ también las satisface gracias a la proposición 5, luego por el teorema 4.2 se tiene el resultado. ☑

Teorema 5.1. *Sea R un dominio de integridad. Sea $m \geq 2$ entonces para todo $H \in R[X_1, \ldots, X_m]$ no constante es la suma de dos irreducibles P_1 y P_2. Además si en H ocurren más de una variable, en los polinomios P_1 y P_2 ocurren a lo sumo las mismas variables que ocurren en H.*

Demostración. Supongamos que $X_1, \ldots, X_k$ son las variables que ocurren en H donde $1 \leq k \leq m$. Si $k = 1$, $H \in R[X_1]$ luego

$$H(X_1) = a_1X_1 + a_0 = \underbrace{X_2}_{P_1} + \underbrace{H - X_2}_{P_2}$$

donde claramente P_1 y P_2 son irreducibles en $R[X_1, \dots X_2]$. Observemos que como en H sólo ocurre una variable no debemos garantizar que en P_1 y P_2 ocurran las mismas variables que ocurren en H.
Si $k > 1$ veamos que $R[X_1]$ satisface las condiciones (1) y (2) del teorema 4.2, sea M un ideal máximal de R entonces en el anillo $(R/M)[X_1]$ existen infinitos irreducibles no asociados ya que este anillo es factorial. En efecto, suponga que hay un número finito y proceda como en la prueba de la infinitud de los números primos. Como cada irreducible se puede ver como $\overline{f}$(módulo M) donde $f \in R[X_1]$, luego los ideales de la forma $(M, f(X_1))$ de $R[X_1]$ son máximales. Considere el siguiente homomorfismo natural $\varphi : R[X_1] \to (R/M)[X_1]/(\overline{f(X_1)})$ el cual es sobre y tiene núcleo $(M, f(\overline{X_1}))$. Entonces por el primer teorema de isomorfia tenemos:

$$R[X_1]/(M, \overline{f(X_1)}) \cong (R/M)[X_1]/(\overline{f(X_1)}),$$

luego la norma del ideal $\mathfrak{p} = (M, \overline{f(X_1)})$ es diferente de dos y se tiene la condición (2).
Para ver la condición (1) note que los elementos de $\mathfrak{p}$ son exactamente los elementos de $R[X]$ módulo M que son divisibles por $\overline{f}$ sobre R/M entonces todos los elementos de $\mathfrak{p}^2$ son divisibles por $\overline{f}$; como f no es divisible por f^2 (en $R/M[X_1]$) $f \notin \mathfrak{p}^2$ y $\mathfrak{p}^2 \subsetneq \mathfrak{p}$. Similarmente se demuestra que el ideal $\mathfrak{q} = (M, g)$ de $R[X_1]$ satisface (1) y (2) donde $\overline{g}$ es irreducible sobre R/M.
Aplicando el teorema 4.2 al anillo $R[X_1]$ se obtiene el resultado deseado. ☑

6. **Apéndice**

La proposición 3.1 nos da una fórmula $\natural(h)$ para el número de polinomios irreducibles de grado h en $\mathbb{F}_q[X]$. Por otro lado, sabemos que en $\mathbb{F}_q[X]$ existen $q^{h+1} - q^h$ polinomios de grado h. Luego, la densidad de los polinomios irreducibles en $\mathbb{F}_q[X]$ es

$$\frac{\natural(h)}{q^{h+1} - q^h} \sim \frac{1}{h}.$$

Es decir, a medida que aumentamos el grado h es cada vez más difícil dar con polinomios irreducibles en $\mathbb{F}_q[X]$.

Si $m = 2$, sean $N_2(h)$ el número de polinomios en $\mathbb{F}_q[X_1, X_2]$ de grado h, $I_2(H)$ el número de polinomios irreducibles en $\mathbb{F}_q[X_1, X_2]$ de grado h. Arnaud Bodin establece el siguiente hecho (véase [6])

$$1 - \frac{I_2(h)}{N_2(h)} \sim \frac{q+1}{q^h},$$

lo cual implica $\frac{I_2(h)}{N_2(h)} \to 1$, cuando $h \to \infty$. Es decir si consideramos polinomios de grado cada vez mayor es más probable que estos sean irreducibles. Este hecho es totalmente contrario a lo que sucede en el caso de una variable y lo que sucede en el caso de los números enteros pues en este caso sabemos que la densidad de los números primos en los números enteros es nula.

Si $m > 2$. Se puede generalizar el anterior resultado para obtener el siguiente hecho: *Si $N_m(h)$ es el número de polinomios en $\mathbb{F}_q[X_1, \ldots, X_m]$ de grado h y $I_m(h)$ el número de polinomios irreducibles en $\mathbb{F}_q[X_1, \ldots, X_m]$ de grado h. Se tiene:*

$$1 - \frac{I_m(h)}{N_m(h)} \sim N_m(1).\frac{N_m(h-1)}{N_m(h)} \sim \frac{q^{m+1} - q}{q-1}.\frac{1}{q^{\binom{m+h-1}{m-1}}}.$$

Teorema 6.1. *Si $H \in \mathbb{F}_q[X]$ con $\partial H = h$ y $N(H)$ es el número de parejas P_1 y P_2 de polinomios unitarios irreducibles en $\mathbb{F}_q[X]$ que satisfacen:*

1. *$\partial P_1 = \partial P_2 = h + 1$,*
2. *$P_1 \neq P_2$,*
3. *$P_1 - P_2 \equiv 0 \pmod{H}$,*
4. *H es libre de cuadrados o $h + 1$ no es divisible por la característica de $\mathbb{F}_q$.*

Entonces

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

cuando $q \to \infty$.

Demostración. Sea $\pi(r; H, K)$ el número de polinomios unitarios irreducibles P de grado r tal que $P \equiv K \pmod{H}$. Entonces

$$N(H) = \sum_K [\pi(h+1; H, K)]^2 - \natural(h+1), \tag{1}$$

donde K varia en un sistema reducido de residuos módulo H. Sea $\pi_K(r, d)$ el número de polinomios unitarios irreducibles P que satisfacen:

1. $\partial P = \dfrac{r}{d}$,
2. $P^d \equiv K \pmod{H}$

y sea $D(r, K) = \sum_{d|r} \dfrac{\pi_K(r, d)}{d}$. Nótese que $\pi_K(r, 1) = \pi(r; H, K)$. Si $r < 2h$, y, usando la cuarta hipótesis del teorema, se tiene que $\pi_k(r, d) \leq d$ para $d > 1$.[1] Luego

$$D(r, K) - \pi(r; H, K) \leq r, \tag{2}$$

para $r < 2h$. Usando la fórmula de Artin [3], se tiene

$$r\varphi(H)D(r, K) = q^r - \sum_\chi \overline{\chi}(K) \sum_{i=1}^{m(\chi)} \beta_i^r(\chi), \tag{3}$$

[1]Este resultado se tiene sin la hipótesis (4) solo cuando H es irreducible.

donde χ recorre todos los carácteres módulo H y $m(\chi) \leq h$. Los números $\beta_i(\chi)$ para $1 \leq i \leq m(\chi)$ están relacionados con la hipótesis de Riemann para cuerpos de funciones algebraicas [34], de la cual se sigue que

$$|\beta_i(\chi)| \leq hq^{\frac{1}{2}} \tag{4}$$

para todo χ y $1 \leq i \leq m(\chi)$. Usando (2) y (3) se muestra

$$N(H) = \sum_K [D(h+1,K)]^2 - \natural(h+1) + O(q^{h+1}). \tag{5}$$

Esta ultima fórmula no requiere de (4). Después de bastantes cálculos se llega a la fórmula

$$\sum_K [D(h+1,K)]^2 = \frac{q^{2(h+1)}}{(h+1)\varphi(H)} + O(q^{(h+1)}). \tag{6}$$

Reemplazando (6) en (5) y usando la estimación trivial de $\natural(h+1) = O(q^{h+1})$, cuando $q \to \infty$, se tiene

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

Referencias

[1] Víctor Albis. *Análogos en $\mathbb{F}_q[x]$ de conjeturas famosas de la teoría de los números*. Rev. Acad. Colomb. Cienc. **17** (66) (1990), 489–504.

[2] T. M. Apostol. *Introduction to Analytic Number Theory*. Springer–Verlag: New York, 1976.

[3] E. Artin. *Quadratische Körper im Gebiete der höheren Kongruenzen*. Math. Z. **19** (1924), 242–246.

[4] M. F. Atiyah & I. G. Macdonald. *Introduction to Commutative Algebra*. Addison–Wesley: Reading, 1969.

[5] Jacob Barshay. *Topics in ring theory*. W. A. Benjamin: New York, 1969.

[6] Arnaud Bodin. *Number of irreducible polynomials in several variables over finite fields*. Amer. Math. Monthly **115** (2008), 653–660.

[7] Andreas O. Bender. *Representing an element of $\mathbb{F}_q[x]$ as the sum of two irreducibles in $\mathbb{F}_q^s[x]$*. arXiv:0809.4321v1 [math. NT] 25 Sep 2008.

[8] Jing-Run Chen. *On the representation of a large even integer as the sum of a prime and product of at most two primes*. Kexue Tongbao **17** (1966), 365–386.

[9] Jing-Run Chen & T. Wang. *On the odd Goldbach Problem*. Acta Math. Sinica **32** (1989), 702–718.

[10] Javier Cilleruelo Mateo. *La conjetura de Goldbach*. La Gaceta de la RSME **3** (3) (2000), 557–565.

[11] J. M. Deshouillers, Gove Effinger, H. te Riele & D. Zinoviev. *A complete Vinogradov 3−primes theorem under the Riemann hypothesis*. Elect. Res. Annunc. AMS **3** (1997), 99–104.

[12] Larry L. Dornhoff & Franz E. Hohn. *Applied Modern Algebra*. MacMillan: New York, 1978.

[13] Gove W. Effinger & David R. Hayes. *A complete solution to the polynomial 3-primes problem*. Bull. Amer. Math. Soc. **24** (1991) 363–369.

[14] Martin Eichler. *Introduction to the Theory of Algebraic Numbers and Functions*. Academic Press: New York, 1966.

[15] John B. Fraleigh. *A first Course in Abstract Algebra*. Addison–Wesley: Reading, 1995.
[16] G. H. Hardy & J. E. Littlewood. *Some problems of "partitio numerorum": on the expression of number as a sum of primes*. Acta Math. (Stockholm) **44** (1923) 1–70.
[17] David Hayes. *A polynomial analog of the Goldbach conjecture*. Bull. Amer. Math. Soc. **69** (1963),
[18] David Hayes. *A Goldbach theorem for polynomials with integral coefficients*. Amer. Math. Monthly **72** (1965), 45–46.
[19] David Hayes. *The expression of a polynomial as a sum of three polynomials*. Acta Arith. **11** (1966), 461–488.
[20] Harald Andrés Helfgott. *Minor arcs for Goldbach's theorem*. (`http://arxiv.org/abs/1205.5252`).
[21] Harald Andrés Helfgott. *Major arcs for Goldbach's theorem*. (`http://arxiv.org/abs/1305.2897`)
[22] I. N. Herstein. *Topics in algebra*. Blaisdell: New York, 1964.
[23] A. A. Karatsuba. *Fundamentos de la teoría analítica de los números*. Editorial Mir: Moscú, 1979.
[24] Oswaldo Lezama. *Anillos, módulos y categorías*. Universidad Nacional de Colombia: Bogotá, 1991.
[25] Tomás Oliveira e Silva. *Goldbach conjecture verification*. 2012. Disponible en `http://www.ieeta.pt/~tos/goldbach.html`
[26] Paul Pollack. *An analogue of Goldbach's conjecture for certain polynomial rings*. Princeton University, Princeton, New Jersey, 2000.
[27] Paul Pollack. *On polynomial rings with a Goldbach property*. Amer. Math. Monthly **118** (2011), 71–77.
[28] O. Ramaré. *On Šnirel'man's constant*. Ann. Scu. Norm. Pisa **22** (1995), 645–706.
[29] A. Rattan & C. Stewart. *Goldbach's conjecture for* $\mathbb{Z}[X]$. C. R. Math. Acad. Sci. R. Can. **20** (3) (1998), 83–85.
[30] F. Saidak. *On Goldbach's conjecture for integer polynomials*. Amer. Math. Monthly **113** (2006), 541–545.
[31] Terence Tao. *Every Odd Number Greater than 1 is the Sum of at Most Five Primes*, `ArXiv:1201.6656v4 [math. NT] 3 Jul 2012`
[32] I. M. Vinogradov. *Representación de un número impar como la suma de tres primos*. Comptes Rendues (Doklady) de l'Académie des Sciences de l'URSS **15** (1937), 191–294. (En ruso)
[33] I. M. Vinogradov. *The Method of Trigonometric Sums in the Theory of Numbers*. Wiley–Interscience: New York, 1947.
[34] A. Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent*. Hermann: Paris, 1945.

(Recibido en abril de 2013. Aceptado para publicación en agosto de 2013)

Leonardo Fabio Chacón–Cortés
Departamento de Matemáticas
Universidad Nacional de Colombia, Bogotá
e-mail: `lfchaconc@gmail.com, lfchaconc@unal.edu.co`