La conjetura de los primos gemelos en un mundo paralelo al mundo de los números enteros

Erika Lorena Barrero Angulo
Matemático

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
2013

La conjetura de los primos gemelos en un mundo paralelo al mundo de los números enteros

Erika Lorena Barrero Angulo
Matemático

Trabajo de tesis para optar al título de
Maestría en Ciencias Matemáticas

Director
Dr. Víctor Albis
Profesor Titular
Universidad Nacional de Colombia
Bogotá D.C.

Universidad Nacional de Colombia
Facultad de Ciencias
Departamento de Matemáticas
Bogotá, D.C.
2013

Título en español

La conjetura de los primos gemelos en un mundo paralelo al mundo de los números enteros

Title in English

The twin prime conjecture in a parallel world to the world of integers

Resumen: Estudiamos la conjetura de los números primos gemelos en el anillo de polinomios con coeficientes en un cuerpo finito $\mathbb{F}_q[X]$, estableciendo conjeturas análogas a las de la teoría de números clásica.

Abstract: The analogue in the ring of polynomials with coefficients in a finite field of the twin primes conjecture in the ring of integers is studied.

Palabras clave: Primos gemelos, Polinomios irreducibles gemelos, Teoría aritmética de polinomios

Keywords: Twin prime, Twin irreducible polynomials, Arithmetical theory of polynomials

Dedicatoria

A Luisa Angulo, mi madre,
que siempre me ha apoyado,
me apoya y seguirá apoyando.

Agradecimientos

Al profesor Víctor Samuel Albis, por su asesoría constante en el desarrollo del trabajo.

A Leonardo Chacon por sus instrucciones para dominar el LaTeX.

A Tulio Enrique Vargas Morales por su constante apoyo durante la elaboración de este trabajo.

A todos mis amigos que colaboraron en el desarrollo y la entrega de este trabajo.

Índice general

Índice general **I**

Índice de símbolos **III**

Introducción **IV**

1. Preliminares **1**

1.1. El problema en los números enteros 1

1.2. Estimaciones asintóticas 3

1.3. La norma de un elemento 3

1.4. La fórmula de Gauss 3

1.5. Las L-funciones de Dirichlet 5

1.6. Algunas propiedades del semigrupo $\mathbb{M}$ 6

1.6.1. Relaciones de equivalencia sobre $\mathbb{M}$ 7

1.7. El conjunto Dir ($\mathbb{M}$) 10

2. Polinomios Irreducibles Gemelos sobre Cuerpos Finitos I **12**

2.1. El caso del grado fijo 12

2.2. El Caso de Cuerpos de Bases Fijas 13

3. Polinomios irreducibles gemelos sobre cuerpos finitos II **18**

3.1. Una conjetura uniforme 18

3.2. Una fórmula explícita para el número de polinomios irreducibles 21

3.3. Teorema de Pollack 23

4. Conclusiones **29**

A. Una cota superior para las parejas de primos gemelos en $\mathbb{F}_q[T]$ **30**

Bibliografía **34**

Índice de símbolos

Símbolo	Nombre
$O(x)$	O grande de x (Notacion Landau), 3
$o(x)$	o pequeño de x, 3
$\sim$	asintóticamente igual, 3
$\|Q\|$	norma del polinomio Q, 3
$\mathbb{M}(q;X) = \mathbb{M}$	El conjunto de los polinomios unitarios de $\mathbb{F}_q[X]$, 3
$\phi(M)$	La función indicatriz de Euler, 3
$\pi(n;q)$	número de irreducibles de grado n en $\mathbb{F}_q[X]$, 4
$\chi(g)$	carácter de Dirichlet, 5
$\hat{G}$	conjunto de los caracteres de G, 5
$L(s,\chi)$	L-funciones de Dirichlet, 6
$A \equiv B \pmod{\mathcal{R}}$	congruencia, 7
$\mathcal{C}(\mathcal{R})$	conjunto de todas las clases de equivalencia módulo $\mathcal{R}$, 7
$\mathcal{G}(R)$	grupo de las clases invertibles,7
Dir $(\mathbb{M})$	funciones aritméticas sobre $\mathbb{M}$, 10
$\pi_2(n;q)$	número de irreducibles gemelos de grado n sobre $\mathbb{F}_q$, 14
$S(k)$	número de polinomios especiales de grado k, 14
$\mathbf{R}(n;M,q)$	número de pares de irreducibles gemelos $(P, P+M)$, 18
$\mathcal{R}_{l,M}$	relación de equivalencia especial, 21

Introducción

El problema de los primos gemelos en el caso de anillos de polinomios sobre cuerpos finitos es el siguiente: Encontrar el número de parejas de polinomios de la forma $(P, P + M)$, donde P es un polinomio irreducible de grado n y M un polinomio diferente de cero, fijado de antemano sobre un cuerpo finito $\mathbb{F}_q$ y tales que $P + M$ sea irreducible.

Aquí examinaremos algunas conjeturas sobre el número de polinomios primos gemelos para el anillo de polinomios de coeficientes en un cuerpo finito $\mathbb{F}_q[X]$.

El trabajo se divide en tres capítulos. En el primero establecemos los requerimientos mínimos de la teoría aritmética de polinomios sobre un cuerpo finito $\mathbb{F}_q$, en el segundo, examinamos el trabajo de Effinger, Hincks y Mullen [7] donde se establece una conjetura aun no demostrada. En el tercero, se estudia el trabajo de Pollack [12], donde se establece una nueva conjetura y se establece, bajo algunas condiciones, una estimativa para la existencia de polinomios primos gemelos.

CAPÍTULO 1

Preliminares

1.1. El problema en los números enteros

La conjetura de los números primos gemelos en los números enteros.

Dos números primos (p, q) son primos gemelos si están separados por una distancia de 2, es decir, si $q = p + 2$. El primero en llamarlos así fue Paul Stäckel $(1862 - 1919)$.

La lista de las primeras parejas de primos gemelos comienza así: $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)\ldots$ Conforme se van considerando primos más grandes la frecuencia de aparición de pares de primos gemelos va disminuyendo, pero aún así se ha visto computacionalmente que siguen surgiendo pares de primos gemelos aún entre números de tamaños enormes.

De momento, los primos gemelos más grandes conocidos son:

- $(3756801695685 \times 2^{666669}) - 1$ y $(3756801695685 \times 2^{666669}) + 1$, números que constan de 200700 dígitos. Fueron descubiertos en 2011 por Timothy D Winslow (norteamericano) (véase [3]).
- $(65516468355 \times 2^{333333}) - 1$ y $(65516468355 \times 2^{333333}) + 1$, números que constan de 100355 dígitos. Fueron descubiertos en 2009 por Peter Kaiser (alemán) y Keith Klahn (norteamericano) (véase [3]).
- $(2003663613 \times 2^{195000}) - 1$ y $(2003663613 \times 2^{195000}) + 1$, que tienen 58711 dígitos. Fueron descubiertos en 2007 por Vautier, McKibbon, Gribenko et al (véase [3]).
- $(100314512544015 \times 2^{171960}) - 1$ y $(100314512544015 \times 2^{171960}) + 1$, que tiene 51780 dígitos y fue descubierto en el 2006 por los matemáticos húngaros: Zoltán Járai, Gabor Farkas, Timea Csajbok, Janos Kasza y Antal Járai (véase [3]).

Todos los números naturales se pueden escribir de una, y sólo una, de las siguientes maneras: $6k$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$, $6k + 5$, donde $k \in \mathbf{Z}$. Ahora bien, $6k$ es divisible por 6; $6k + 2$, $6k + 4$ son divisibles por 2; $6k + 3$ es divisible por 3, por lo que no son primos. Luego los posibles primos son los de la forma $6k + 1$, $6k + 5$, que módulo 6 pueden ser escritos como $(6k - 1, 6k + 1)$. Por lo tanto, todo par posible de números primos gemelos

mayores que 3 debe ser de la forma $(6k-1, 6k+1)$. Además, se ha demostrado que el par $(p, p+2)$ (cuando p es primo) son primos gemelos si y sólo si:

$$4[(p-1)!+1] \equiv -p \pmod{p(p+2)}.$$

Véanse [5] y [13] para una demostración de este resultado, muy poco práctico.

La conjetura de los primos gemelos en el anillo $\mathbb{Z}$ de los números enteros dice: *Existen infinitas parejas $(p, p+2)$ de números primos gemelos. Ésta es una de las más famosas y antiguas cuestiones no resueltas de la teoría de números.*

Esté problema ha interesado a varios matemáticos los cuales han encontrado algunos resultados parciales interesantes (véase [14]). He aquí algunos que hemos tomado de [13]:

- En 1849 Alphonse de Polignac (1817-1890) formuló una conjetura según la cual, para todo número par k, existen infinitos números enteros p para los que p y $p+k$ son primos. Por el momento no sabemos demostrar si hay infinitas "parejas de primos" $(p, p+k)$ para ningún valor de k . Cuando $k = 2$, es la Conjetura de los Primos Gemelos.
- En 1919, Viggo Brun demostró la convergencia de la serie de los inversos de los números primos gemelos, contrariamente a la serie de los inversos de todos los números primos la cual diverge.
- En 1940, Erdös demostró que existe una constante $c < 1$ e infinitos primos p tales que $q - p < c \times ln(q)$, donde q denota el número primo que sigue a p. Esté resultado fue mejorado sucesivamente en 1986 cuando Maier probó que podía emplearse una constante $c < 0,25$.
- En 1966 Jing-run Chen mostró que existen infinitos números primos p tales que $p+2$ es un producto de, a lo sumo, dos factores primos. Para conseguir este resultado se basó en la llamada teoría de cribas, y consiguió tratar la Conjetura de los Primos Gemelos y la Conjetura de Goldbach de forma similar.
- Sea ahora $\pi_2(x)$ el número de parejas de primos $(p, p+2)$ con $p \leq x$. La siguiente conjetura sobre la cantidad de tales pares que hay hasta un numero x, dado, se debe esencialmente a Hardy y Littlewood (1923), y nos dice que el numero $\pi_2(x)$ de primos gemelos $(p, p+2)$ con $p \leq x$ es asintóticamente equivalente a lo siguiente:

  $$2 \prod_{p>2, p \text{ primo}} \left[1 - \frac{1}{(p+2)^2}\right] \int_2^x \frac{1}{[ln(t)]^2} dt,$$

  donde

  $$\prod_{p>2, p \text{ primo}} \left[1 - \frac{1}{(p+2)^2}\right] = \Pi_2 = 0,660161815846869573927812110014 5...$$

  es la llamada Constante de los números primos gemelos. En 1961 Wrench calculó sus primeros 45 decimales, e incluso se conocen sus primeras 60 cifras gracias a los trabajos de Gourdon y Sebah [18]. Los mismos autores señalan que es posible estimar miles de dígitos usando propiedades de la función zeta de Riemann; ya han calculado 5000 dígitos usando este método .

- Finalmente en el 2004, Richard F. Arenstorf, de la Vanderbilt University, presentó una posible demostración de la conjetura, en 38 páginas, utilizando métodos de la teoría de números analítica clásica, la cual infortunadamente se basaba en unos lemas incorrectos.

Lo anterior hace que el problema análogo en el caso del anillo $\mathbb{F}_q[X]$, donde $\mathbb{F}_q$ es un cuerpo finito de q elementos amerita estudiarse. Nuestro propósito es pues empezar a estudiar el análogo de la conjetura de los números primos gemelos en este mundo paralelo al de $\mathbb{Z}$. Como veremos este análogo es más parecido a la conjetura de Polignac.

1.2. Estimaciones asintóticas

Definición 1.1. Sean $f(x)$ y $g(x)$ dos funciones definidas sobre un mismo subconjunto de los números reales. Escribimos $f(x) = O(g(x))$ cuando x tiende a infinito si y sólo si existe una constante positiva M y un real x_0 tal que $\frac{|f(x)|}{g(x)} < M$ para todo $x > x_0$. Si $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$ escribimos $f(x) = o(g(x))$ cuando x tiende a infinito y si $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ decimos que $f(x)$ es *asintóticamente igual* a $g(x)$ cuando x tiende a infinito y notamos $f \sim g$ cuando $x \to \infty$.

Estas notaciones fueron introducidas por Landau.

1.3. La norma de un elemento

Recordemos que $\mathbb{F}_q[X]$ es un dominio factorial

Definición 1.2. Dado $Q \in \mathbb{F}_q[X]$ la norma de Q es:

$$|Q| = \begin{cases} q^{\partial Q}, & \text{si } Q \neq 0, \\ 0, & \text{si } Q = 0, \end{cases}$$

donde ∂Q es el grado del polinomio Q.

Definición 1.3. Dos polinomios de la forma $P, P + M \in \mathbb{F}_q[X]$ irreducibles de grado n donde M es un polinomio diferente de cero y grado menor que n se llaman *polinomios primos gemelos.*

Definición 1.4. Un polinomio unitario es aquel que tiene como coeficiente principal uno. El conjunto de los polinomios unitarios de $\mathbb{F}_q[X]$, se designa con $\mathbb{M}(q; X) = \mathbb{M}$

Definición 1.5 (La función indicatriz de Euler). Sea $\phi : \mathbb{M} \to \mathbb{R}$ donde $M \to \phi(M) = Card(\mathbb{F}_q[X]/M)^\times$

1.4. La fórmula de Gauss

Gauss encontró la siguiente fórmula:

Lema 1.1 (Lema de Gauss). *Si $\pi(n;q)$ es el número de polinomios primos unitarios de grado n en $\mathbb{F}_q[X]$ entonces*

$$\pi(n;q) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \tag{1.1}$$

donde μ es la función de Möbius en $\mathbb{Z}$.

Gauss sólo demostró esta fórmula para el caso $q = p$, p primo, pues todavía Galois no había inventado los cuerpos finitos generados como extensiones finitas de $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$. Una demostración debida a E. Landau, se encuentra expuesta en [1]. Usando la fórmula de inversión de Möbius para funciones aritméticas definida en $\mathbb{N}$, obtenemos de (1.1) la ecuación

$$q^n = \sum_{d|n} d\pi(d;q), n = 1, 2, ...$$

Más adelante usaremos las siguientes desigualdades

$$\frac{q^n}{n} - 2\frac{q^{n/l}}{n} \leq \pi(n;q) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \leq \frac{q^n}{n} \tag{1.2}$$

donde l es el menor factor primo de n. Su demostración es como sigue:

El primer término de la expresión (1.1) lo obtenemos si hacemos $d = 1$ y si aplicamos valor absoluto y teniendo en cuenta que $|\mu(d)| \leq 1$ para $\forall d$:

$$\pi(n;q) = \frac{1}{n}\mu(1)q^{n/1} + \frac{1}{n}\sum_{\substack{d|n \\ d>1}}\mu(d)q^{n/d}$$

$$\left|\pi(n;q) - \frac{1}{n}q^n\right| = \left|\frac{1}{n}\sum_{\substack{d|n \\ d>1}}\mu(d)q^{n/d}\right|$$

$$\leq \frac{1}{n}\sum_{\substack{d|n \\ d>1}} q^{n/d} = \frac{1}{n}q^{n/l}\sum_{\substack{d|n \\ d>1}}\frac{q^{n/d}}{q^{n/l}}$$

$$\left|\pi(n;q) - \frac{1}{n}q^n\right| \leq \frac{q^{n/l}}{n}\frac{q}{q-1} \quad \text{Como } \frac{q}{q-1} \leq 2 \text{ obtenemos}$$

$$\left|\pi(n;q) - \frac{1}{n}q^n\right| \leq \frac{q^{n/l}}{n}\frac{q}{q-1} \leq 2\frac{q^{n/l}}{n}$$

$$-2\frac{q^{n/l}}{n} \leq \pi(n;q) - \frac{1}{n}q^n \leq 2\frac{q^{n/l}}{n}$$

Por otro lado de (1.1) tenemos

$$\begin{aligned} q^n &= \sum_{d|n} d\pi(d;q) \\ &= d_1\pi(d_1;q) + d_2\pi(d_2;q) + d_3\pi(d_3;q) + ... + n\pi(n;q) \\ q^n &> n\pi(n;q) \\ \frac{q^n}{n} &> \pi(n;q) \end{aligned}$$

Obteniendo así la cota superior

1.5. Las L-funciones de Dirichlet

1. **Caracteres de un grupo abeliano finito.** Sea G un grupo finito denotado multiplicativamente y sea $\mathbb{C}^*$ el grupo multiplicativo de los números complejos (excepto el cero). Un homomorfismo $\chi : G \to \mathbb{C}^*$ se dice un *carácter* de G. Tenemos, pues, $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$, si $g_1, g_2 \in G$, y $\chi(e) = 1$ si e es el elemento unidad de G. El conjunto de todos los caracteres de G se designa con $\hat{G}$.

   Con $\mathbb{T}$ designamos al grupo multiplicativo $\{z \in \mathbb{C}^*; |z| = 1\}$ (la circunferencia de radio 1 y centro en el origen). Este grupo es un subgrupo de $\mathbb{C}^*$.
   Los siguientes resultados son bien conocidos (véase, por ejemplo, Apostol[2])

   Proposición 1.1. *Si $\chi \in \hat{G}$, entonces $\chi(g) \in \mathbb{T}$ para todo $g \in G$. Es decir, $\chi(g)$ es una raíz $o(G) -$ ésima de la unidad en $\mathbb{C}$.*

   Demostración Si $o(G)$ es el orden del grupo G el cual es finito, es conocido que $g^{o(G)} = e$ para todo $g \in G$. Es decir, $\chi(g^{o(G)}) = \chi(e) = 1$, puesto que χ es homomorfismo de grupos y envía la unidad en la unidad.

   Definición 1.6. Todo grupo admite, por lo menos, un carácter χ_0 definido por $\chi_0(g) := 1$ para todo $g \in G$. Este carácter se dice *principal*.

   Definición 1.7. Si $\chi_1, \chi_2 \in \hat{G}$, definimos una ley de composición interna sobre $\hat{G}$, de la siguiente manera:

$$\chi_1\chi_2(g) := \chi_1(g)\chi_2(g) \ \forall g \in G.$$

   Es claro que χ_0 actúa como identidad en $\hat{G}$.

   Los dos resultados siguientes pueden encontrarse en [1].

   Proposición 1.2. *Sea G un grupo finito. Con la ley definida antes $\hat{G}$ es un grupo abeliano. Además, $\chi^{-1}(g) = \frac{1}{\chi(g)} = \overline{\chi(g)}$.*

   Proposición 1.3. *Se tienen las siguientes relaciones de ortogonalidad:*

$$\sum_{g \in G} \chi(g) = \begin{cases} o(G), & si\ \chi = \chi_0, \\ 0, & si\ \chi \neq \chi_0, \end{cases}$$

$$\sum_{\chi\in\hat{G}}\chi(g)=\begin{cases}o(G), & si\ g=e,\\ 0, & si\ g\neq e,\end{cases}$$

2. **Caracteres módulo $\mathbf{H}(X)$** Sea $H(X)\in\mathbb{F}_q[X]$. Una función $\chi:\mathbb{F}_q[X]\to\mathbb{C}$ es un carácter multiplicativo módulo $H(X)$ si para $A(X),B(X)\in\mathbb{F}_q[X]$ tenemos:

   (i) $\chi(A)=0$ si $m.c.d.(A,H)\neq 1$.
   (ii) $\chi(1)\neq 0$.
   (iii) $\chi(A)\chi(B)=\chi(AB)$.
   (iv) $A\equiv B \pmod{h}\Rightarrow\chi(A)=\chi(B)$

   Como es fácil ver, un carácter multiplicativo módulo $H(X)$ es un carácter del grupo $(\mathbb{F}_q[X]/(H(X)))^\times$, que se extiende a $\mathbb{F}_q[X]/(H(X))$ haciendo $\chi(\alpha)=0$ para todo α divisor de cero en este anillo.

   Proposición 1.4. *Si χ es un carácter de $\mathbb{F}_q[X]$ módulo $H(X)$, tenemos*

   (i) $\chi(1)=1$.
   (ii) $\overline{\chi}(A)=\overline{\chi(A)}$ *es un carácter módulo $H(X)$, donde la barra encima de $\chi(A)$ indica que se trata de su conjugado complejo.*
   (iii) Si $m.c.d.(A,H)=1$, entonces $(\chi(A))^{\varphi(H)}=1$, donde $\varphi(H)=card(\mathbb{F}_q[X]/H(X))^\times$.
   (iv) Los caracteres de $\mathbb{F}_q[X]$ módulo $H(X)$ aparecen en número finito.
   (v) Si $m.c.d.(A,H)=1$, entonces $\chi(A)\overline{\chi}(A)=1$.

3. **Las funciones $\mathbf{L}(s,\chi)$.** Para un carácter χ módulo $h(X)$, definimos

$$L(s,\chi):=\sum_{a\in M(q;X)}\frac{\chi(a)}{|a|^s}$$

   como la función L asociada a χ.

1.6. Algunas propiedades del semigrupo $\mathbb{M}$

En esta sección citaremos algunos hechos conocidos acerca del semigrupo de polinomios unitarios con coeficientes en $\mathbb{F}_q[X]$.

Sea $\mathbb{M}=\mathbb{M}(q,X)$ el conjunto de todos los polinomios unitarios en $\mathbb{F}_q[X]$, el cual es un monoide libre, en virtud de la factorialidad de $\mathbb{F}_q[X]$.

Los primos generadores son los irreducibles unitarios, denotamos por $\mathbb{P}$ el conjunto de primos generadores. Esto implica que $\mathbb{M}$ es un monoide de factorización única para el cual se tienen propiedades análogas de divisibilidad en $\mathbb{N}$. Además, para un polinomio $A(X)\in\mathbb{M}$, escribimos A en lugar de $A(X)$.

La aplicación grado $\partial:\mathbb{M}\to\mathbb{N}\cup\{0\}$ que asigna a cada polinomio $A\in\mathbb{M}$ su grado ∂A satisface las siguientes condiciones:

(D1) $\partial 1 = 0$, y $\partial P \geq 1$, para todo $P \in \mathbb{P}$

(D2) $\partial(AB) = \partial A + \partial B$, para todo A y B en $\mathbb{M}$

(D3) $G(k) = \sum_{\partial A = k} 1 = q^k$, para cada $k = 0, 1, 2, ...$

1.6.1. Relaciones de equivalencia sobre $\mathbb{M}$

Definición 1.8. Sea $\mathcal{R}$ una relación de equivalencia sobre $\mathbb{M}$. Para indicar que $A\mathcal{R}B$ escribiremos $A \equiv B \pmod{\mathcal{R}}$. Si $A \equiv B \pmod{\mathcal{R}}$ implica que $AC \equiv BC \pmod{\mathcal{R}}$, para cada $C \in \mathbb{M}$, decimos que $\mathcal{R}$ es una *relación de congruencia*.

Definición 1.9. Un polinomio $A \in \mathbb{M}$ se dice *invertible* módulo una relación de congruencia $\mathcal{R}$ sobre $\mathbb{M}$ si existe un polinomio $B \in \mathbb{M}$ tal que $AB \equiv 1 \pmod{\mathcal{R}}$.

Claramente, cada elemento en la clase de un elemento invertible es invertible módulo $\mathcal{R}$, en virtud de las definiciones anteriores. Por tanto podemos hablar de clases invertibles módulo $\mathcal{R}$.

Definición 1.10. Dada una relación de congruencia $\mathcal{R}$ en $\mathbb{M}$:

- Denotamos por $\mathcal{C}(\mathcal{R})$ el conjunto de todas las clases de equivalencia módulo $\mathcal{R}$
- Denotamos por $\mathcal{G}(R) \neq \phi$ el grupo de las clases invertibles el cual, por lo menos contiene la clase del 1.
- Si $\mathcal{C}(\mathcal{R})$ es un conjunto finito decimos que $\mathcal{R}$ es una *relación de congruencia finita*. Obviamente en este caso $\mathcal{G}(\mathcal{R})$ es también finito. Sin embargo $\mathcal{G}(\mathcal{R})$ podría ser finito sin que $\mathcal{C}(\mathcal{R})$ lo sea.

Con la siguiente definición queremos dar una definición que cobije al caso de los enteros módulo n, $\mathbb{Z}_n$ con $n > 0$ y que la extienda.

Definición 1.11. Una relación de congruencia se dice que es *aritméticamente distribuida* si tenemos las siguientes condiciones:

(AD1) Solo un número finito de irreducibles en $\mathbb{M}$ no son invertibles módulo $\mathcal{R}$

(AD2) Existe un entero m, dependiente solo de $\mathcal{R}$, tal que si $r > m$, entonces el número de polinomios unitarios en $\mathbb{M}$ de grado r en cada una de las clases de equivalencia $\mathcal{G}(\mathcal{R})$ es el mismo que el número de cualquier otra clase de equivalencia de $\mathcal{G}(\mathcal{R})$.

Definición 1.12. Si $\mathcal{R}$ esta aritméticamente distribuida, definimos a $m(\mathcal{R})$ como el más pequeño de los enteros no negativos m para los cuales (AD2) se tiene para $\mathcal{R}$.

Lema 1.2. *Sean M un polinomio en $\mathbb{M}$ y $l \geq 0$ entero, si $\partial M = m$ y si $r \geq m + l$ entonces para cada polinomio B y cada uno de los elementos $\alpha_1, \alpha_2, \ldots, \alpha_l$ existen exactamente q^{r-m-l} polinomios unitarios A de grado r tales que:*

(1) Los primeros l coeficientes de A son $\alpha_1, \alpha_2, \ldots, \alpha_l$

(2) $A \equiv B \pmod{M}$

Demostración Definimos un polinomio *regular* como un polinomio unitario de grado r cuyos primeros l coeficientes son $\alpha_1, \alpha_2, \ldots, \alpha_l$ y es congruente a B módulo M. Si A es regular entonces los polinomios de la forma $A + MR$ donde $\partial R < r - m - l$ también son regulares.

Recíprocamente cada polinomio regular es necesariamente de la forma $A + MR$, porque tal polinomio es congruente con $A \pmod{M}$ y tiene los mismos l primeros coeficientes que A. De tal forma que si existe algún polinomio regular entones hay exactamente q^{r-m-l} polinomios regulares. Como todo polinomio es congruente módulo M a un polinomio de grado menor que m y dado que $r \geq m+l$, existen, exactamente q^{r-m-l} polinomios unitarios que satisfacen las condiciones *(1)* y *(2)*. □

Para un polinomio $M \in \mathbb{F}_q[x]$ fijo la relación de congruencia $\mathcal{R}_M$ módulo M es una relación de congruencia finita sobre $\mathbb{M}$. Está relación provee un ejemplo importante de las relaciones de congruencia aritméticamente distribuidas. Utilizando la función indicatriz de Euler para polinomios, los polinomios que no son invertibles módulo M son aquellos que tienen un factor común con M. Por lo tanto, un irreducible que no es invertible módulo M es necesariamente uno de los divisores irreducibles de M. Como solo tenemos un número finito de irreducibles no invertibles módulo M se cumple (AD1). (AD2) es una consecuencia inmediata del Lema (1.2) con $l = 0$. En efecto, si $l = 0$ en cada clase B módulo M existen exactamente q^{r-m} polinomios unitarios A de grado r. Si $r > m$ supongamos que $AZ \equiv 1 \pmod{M}$ entonces $AZ \equiv BZ \equiv 1 \pmod{M}$ si y solo si B es invertible módulo M y entonces todos los elementos de la clase de B son invertibles, en particular, los de grado r. Entonces la cantidad de elementos de grado r invertibles congruentes a $B \pmod{M}$ es q^{r-m}

Los siguientes dos teoremas se encuentran demostrados en [11]

Teorema 1.1. *La intersección $\mathcal{R}$ de dos relaciones de congruencia $\mathcal{R}_1$ y $\mathcal{R}_2$ sobre $\mathbb{M}$ es nuevamente una relación de congruencia sobre $\mathbb{M}$. El conjunto de las clases de equivalencia de $\mathcal{R}$ consiste de todas las intersecciones no vacías de la forma $c \cap d$ donde c es una clase de equivalencia de $\mathcal{R}_1$ y d es una clase de equivalencia de $\mathcal{R}_2$. Si $\mathcal{R}_1$ y $\mathcal{R}_2$ son finitas y si A en $\mathbb{M}$ es invertible módulo $\mathcal{R}_1$ y $\mathcal{R}_2$, entonces A es también invertible módulo $\mathcal{R}$.*

Para el caso en que $\mathcal{R}_1$ y $\mathcal{R}_2$ son congruencias finitas aritméticamente distribuidas evidentemente $\mathcal{R}_1 \cap \mathcal{R}_2$ satisface (AD1). (AD2) también se cumple; en efecto, existe un m_1 tal que si $r > m_1$, entonces en cada una de las clases $c \pmod{\mathcal{R}_1}$ existe la misma cantidad de polinomios de grado r. Análogamente para $\mathcal{R}_2$ existe m_2 tal que si $r > m_2$ cada una de las clases $d \pmod{\mathcal{R}_2}$ existe la misma cantidad de polinomios de grado r. Luego si $r > max\{m_1, m_2\} = m$, en cada intersección $c \cap d$ existe la misma cantidad de polinomios de grado r.

Teorema 1.2. *Sean $\mathcal{R}_1$ y $\mathcal{R}_2$ relaciones de congruencia finita independientes sobre $\mathbb{M}$, y sea $\mathcal{R}$ su intersección. Entonces:*

1º $\mathcal{G}(\mathcal{R})$ es isomorfo al producto directo de $\mathcal{G}(\mathcal{R})_1$ y $\mathcal{G}(\mathcal{R})_2$

2º A es invertible módulo $\mathcal{R}$ si y sólo si es invertible para ambas $\mathcal{R}_1$ y $\mathcal{R}_2$

3º Los caracteres de $\mathcal{R}$ son exactamente las funciones de la forma $\chi_1\chi_2$, donde χ_1 es un carácter de $\mathcal{R}_1$ y χ_2 es un carácter de $\mathcal{R}_2$.

Presentamos un ejemplo de relaciones de congruencia aritméticamente distribuidas tomado de Hayes [11]

Ejemplo 1.1. Sea $A = \alpha_0+\alpha_1X+...+\alpha_{m-1}X^{m-1}+X^m$ y $B = \beta_0+\beta_1X+...+\beta_{n-1}X^{n-1}+X^n$ son dos elementos de $\mathbb{M}$. Decimos que $A\mathcal{R}B$ si $\alpha_1 = \beta_1$ y $\alpha_{m-1} = \beta_{m-1}$. Es fácil verificar que $\mathcal{R}$ es una relación de congruencia finita sobre $\mathbb{M}$ para la cual $card(\mathcal{C}(\mathcal{R})) = q^2$ y $card(\mathcal{G}(\mathcal{R})) = q(q-1)$. Esta relación satisface (AD1) ya que el único irreducible que no es invertible módulo $\mathcal{R}$ es el polinomio X. Es más, si $r > 1$, entonces cada clase de equivalencia módulo $\mathcal{R}$ contiene q^{r-2} polinomios de grado r y esto implica $m(\mathcal{R}) = 1$ lo cual demuestra la condición (AD2).

Proposición 1.5. *Si $\mathcal{R}$ es una relación de congruencia sobre $\mathbb{M}$, cada función que satisface*

(i) $\chi(1) = 1$.

(ii) $\chi(AB) = \chi(A)\chi(B)$, *para cada A y B en $\mathbb{M}$.*

(iii) $\chi(A) = 0$, *si A es no invertible módulo $\mathcal{R}$.*

(v) Si $\chi(A) = \chi(B)$, *si* $A \equiv B \pmod{\mathcal{R}}$.

es llamada un carácter módulo $\mathcal{R}$.

Claramente si χ_1 y χ_2 son caracteres módulo $\mathcal{R}$, la función $\chi(A) = \chi_1(A)\chi_2(A)$, para cada $A \in \mathbb{M}$ es un nuevo carácter módulo $\mathcal{R}$, llamado el carácter producto. El carácter principal χ_0, definido por $\chi_0(A) = 1$ si A es invertible módulo $\mathcal{R}$, $\chi_0(A) = 0$ en otro caso, actúa como un elemento de unidad para esta multiplicación. Además, si χ es un carácter módulo $\mathcal{R}$ la función $\chi^{-1}(A) = 1/\chi(A)$ si $\chi(A) \neq 0$, $\chi^{-1}(A) = 0$ en otro caso, también es un carácter módulo $\mathcal{R}$ que satisface $\chi\chi^{-1} = \chi^{-1}\chi = \chi_0$. Por lo tanto, el conjunto $\mathbb{X}$ de todos los caracteres módulo $\mathcal{R}$ es un grupo abeliano.

De ahora en adelante designaremos Γ por $\mathcal{G}(R)$ y $\hat{\Gamma} = Hom_{\mathbb{Z}}(\Gamma, \mathbb{C})$ será el conjunto de los caracteres de $\mathcal{G}(R)$ de grupo de Γ. Ahora es clara la existencia de una correspondencia uno a uno entre $\mathbb{X}$ y $\hat{\Gamma}$. Frecuentemente usaremos las propiedades de caracteres de grupos abelianos (vea [1]).

En particular, si $\mathcal{R}$ una relación de congruencia finita tenemos la siguiente relación

$$\sum_{A\in\Gamma} \chi(A) = \begin{cases} h, & \text{si } \chi = \chi_0, \\ 0, & \text{si } \chi \neq \chi_0, \end{cases}$$

$$\sum_{\chi\in\mathbb{X}} \chi^{-1}(A)\chi(B) = \begin{cases} h, & \text{si } A \equiv B, \\ 0, & \text{en otro caso,} \end{cases}$$

donde A es la clase de A módulo $\mathcal{R}$ y $h = card(\Gamma) = card(\hat{\Gamma})$

1.7. El conjunto Dir ($\mathbb{M}$)

Los elementos de $\mathrm{Dir}(\mathbb{M}) = \{f : \mathbb{M} \to \mathbb{C}\}$ se conocen como las *funciones aritméticas* sobre $\mathbb{M}$.

Definición 1.13. Sea $\mathrm{Dir}(\mathbb{M})$ el conjunto de todas las funciones $\{f : \mathbb{M} \to \mathbb{C}\}$, tiene estructura de $\mathbb{C}$-álgebra con las siguientes operaciones:

- $(f+g)(A) := f(A) + g(A)$; $A \in \mathbb{M}$.
- $(\lambda f)(A) = \lambda f(A)$; $\lambda \in \mathbb{C}$.
- $(\lambda\mu)f(A) = \lambda(\mu f(A))$; $\lambda, \mu \in \mathbb{C}$.
- $(\lambda + \mu)f(A) = \lambda f(A) + \mu f(A)$; $\lambda, \mu \in \mathbb{C}$.
- $(f * g)(A) := \sum_{D|A} f(A)g(A/D)$; $A, D \in \mathbb{M}$.

Esta álgebra es conmutativa y su elemento unidad es la función I definida por

$$I(A) = \begin{cases} 1, & \text{si } A = 1, \\ 0, & \text{en otro caso,} \end{cases}$$

Proposición 1.6. *Sea $f \in Dir(\mathbb{M})$ es invertible si y solo si $f(1) \neq 0$*

Definición 1.14. El grupo de elementos invertibles en $\mathrm{Dir}(\mathbb{M})$ es denotado por $\mathrm{Dir}^*(\mathbb{M})$

Definición 1.15. Una función aritmética f es multiplicativa, si f es distinta de cero y $f(AB) = f(A)f(B)$, si $(A, B) = 1$. Si esta relación se cumple para todas las parejas $A, B \in \mathbb{M}$ decimos que f es completamente multiplicativa

Definición 1.16 (Series de Dirichlet). Si $f \in$Dir($\mathbb{M}$) es completamente multiplicativa, definimos su serie de Dirichlet por

$$L(u, f) = \sum_{d=0}^{\infty} S(d; f)q^{-du}, u \in \mathbb{C} \tag{1.3}$$

donde

$$S(d; f) = \sum_{\partial A = d} f(A) \tag{1.4}$$

Observemos que

$$|S(d; f)| \leq \sum_{\partial A = d} |f(A)| \leq q^d$$

Si $\mathcal{R}$ es una relación de congruencia aritméticamente distribuida sobre $\mathbb{M}$, y $\chi \neq \chi_0$ es un carácter módulo $\mathcal{R}$, entonces $S(d; \chi) = 0$ si $d > m(\mathcal{R})$. De hecho, sea $C(\mathcal{R}) = \{H_1, ...H_k\}$. Si $d > m(\mathcal{R})$, obtenemos

$$S(d; \chi) = \sum_{i=1}^{k} \left(\sum_{\substack{\partial A = d \\ A \in H_i}} \chi(A) \right) = \sum_{i=1}^{k} \chi(A) \left(\sum_{\substack{\partial A = d \\ A \in H_i}} 1 \right) = k \sum_{i=1}^{k} \chi(A_i),$$

donde $A_i \in H_i$ y k es el valor común de cada término $\sum_{\substack{\partial A=d \\ A\in H_i}} 1$.

Por lo tanto, $S(d,\chi) = 0$, por propiedades de ortogonalidad. Luego podemos deducir que la serie de Dirichlet es de hecho un polinomio en q^{-z}.

$$L(u,\chi) = \sum_{d=0}^{m(\mathcal{R})} S(d;\chi) q^{-du}, \tag{1.5}$$

que define una función analítica de u sobre el plano complejo.

Si $\chi = \chi_0$, tenemos la siguiente igualdad formal

$$L(u,\chi_0) = \prod_P \left(1 - |P|^{-u}\right)^{-1}, \tag{1.6}$$

donde P recorre sobre los elementos de $\mathbb{P}$ los cuales son irreducibles.

Sea ahora $\chi \neq \chi_0$ y considere el polinomio en Z con coeficientes en $\mathbb{C}$:

$$\pi(Z,\chi) = \sum_{d=0}^{m(\mathcal{R})} S(d;\chi) Z^{m(\mathcal{R})-d}.$$

Ya que este polinomio tiene grado $m(\mathcal{R})$, podemos escribir $\pi(Z,\chi) = \prod(Z-a)$, donde a recorre sus $m(\mathcal{R})$ raíces. Observemos que $S(0;\chi) = 1$ es el coeficiente principal, de manera que

$$L(Z,\chi) = q^{-m(\mathcal{R})z}\pi(q^z,\chi). \qquad (\chi \neq \chi_0)$$

expresión que nos permite un estudio muy conveniente de las raíces de $L(z,\chi)$ para $\chi \neq \chi_0$ contrastando con la situación análoga en la teoría de números analítica clásica. Una útil extensión de la L-serie de Dirichlet es la siguiente:

Si $f \in Dir(\mathbb{M})$ es una función completamente multiplicativa y $h \in Dir(\mathbb{M})$, tenemos

$$h(z,f) = \sum_{A\in\mathbb{M}} h(A)f(A)|A|^{-z} = \sum_{d=0}^{\infty}\left(\sum_{\partial A=d} h(A)f(A)\right) q^{-dz}.$$

Si $h(A) = 1$, para todo $A \in \mathbb{M}$, tenemos $L(z,f) = h(z,f)$. En particular podemos obtener la función zeta de Riemann de $\mathbb{M}$

$$\zeta(z) = L(z,u) = \sum_{A\in\mathbb{M}} |A|^{-z} = \sum_{d=0}\left(\sum_{\partial A=d} 1\right) q^{-dz} = \frac{1}{(1-q^{1-z})}.$$

CAPÍTULO 2

Polinomios Irreducibles Gemelos sobre Cuerpos Finitos I

En este capítulo examinaremos el artículo de Effinger, Hicks y Mullen. [7]

2.1. El caso del grado fijo

Sea q una potencia prima, sea $\mathbb{F}_q$ el cuerpo finito de orden q. Todos los polinomios de $\mathbb{F}_q[X]$ considerados aquí son unitarios, los cuales son el correcto análogo polinomial a los primos en los enteros positivos y los llamaremos irreducibles gemelos cuando estos difieran tan poco como sea posible, en el siguiente sentido:

Definición 2.1. Dos polinomios irreducibles P_1 y P_2, ambos de grado r sobre $\mathbb{F}_q$, se dice que son *polinomios irreducibles gemelos* o simplemente *irreducibles gemelos* a condición de que $|P_2 - P_1| = 4$ si $q = 2$ o $|P_2 - P_1| = 1$ en otro caso. De manera más general, una colección de k polinomios irreducibles distintos P_1, P_2, P_3,...,P_k todos de grado r sobre $\mathbb{F}_q$, se dice que es una k-tupla de irreducibles gemelos, si cada pareja de ellos son irreducibles gemelos.

Para los casos cuando $q > 2$, esto significa que P_i y P_j, $i \neq j$ difieren solamente en sus términos constantes, mientras que en el caso $q = 2$ no difieren en sus términos constantes sino en sus términos lineales y cuadráticos.

Ejemplo 2.1.

- Sobre $\mathbb{F}_2$, los polinomios $P_1 = x^3 + x + 1$ y $P_2 = x^3 + x^2 + 1$ son irreducibles gemelos, pues su diferencia es $x - x^2$ que tiene como grado 2 luego, $|P_1 - P_2| = 2^2 = 4$;
- Sobre $\mathbb{F}_5$, los polinomios $P_1 = x^2 + 2$ y $P_2 = x^2 + 3$ son irreducibles gemelos, lo cual se puede verificar fácilmente $P_1 - P_2 = 1$, entonces $|P_1 - P_2| = 5^0 = 1$;
- Sobre $\mathbb{F}_7$, los polinomios $P_1 = x^2 + 1$ y $P_2 = x^2 + 2$ y $P_3 = x^2 + 4$ al restar los polinomios en cualquier orden obtenemos una constante, luego la norma siempre es 1. Entonces los polinomios forman una 3-tupla (e.d. tripleta) de irreducibles gemelos.

El siguiente resultado nos garantiza la existencia de k-tuplas de polinomios irreducibles gemelos para un grado fijo:

Proposición 2.1. *Para cada $r \geq 2$ y cada $k \geq 2$ existe al menos una k-tupla de dos polinomios irreducibles gemelos de grado r sobre $\mathbb{F}_q$, siempre que $q \geq 2(k-1)r$.*

Demostración Observemos que si $q \geq 2(k-1)r \geq 2r \implies \frac{q}{2} \geq (k-1)r \geq r$ además $2 < 2q^{r/2-1} \implies 1 < q^{r/2-1}$ entonces,

$$\begin{aligned}(k-1)rq^{r-1} \leq \frac{q^r}{2} &= q^r\left(1-\frac{1}{2}\right)\\ &\leq q^r\left(1-\frac{1}{2q^{\frac{r}{2}-1}}\right) = q^r\left(1-\frac{q}{2}\left(\frac{1}{q^{r/2}}\right)\right)\\ &\leq q^r\left(1-r\left(\frac{1}{q^{r/2}}\right)\right)\\ &\leq q^r - rq^r\left(\frac{1}{q^{r/2}}\right) = q^r - rq^{r/2}\end{aligned}$$

Sea l el menor divisor de r, de modo que $r/2 \geq r/l$ y dado que $r \geq 2$,

$$\begin{aligned}q^r - rq^{r/2} &\leq q^r - 2q^{r/l}\\ &= q^r - q^{r/l} - q^{r/l} \leq \sum_{d|r}\mu(d)q^{r/d} - q^{r/l}\\ &< \sum_{d|r}\mu(d)q^{r/d}\end{aligned}$$

Dividiendo por r, obtenemos que si $q \geq 2(k-1)r$ entonces $(k-1)q^{r-1} < \pi(r,q)$, en virtud de la fórmula de Gauss. Pero ahora supongamos que entre los polinomios irreducibles de grado r sobre $\mathbb{F}_q$ existe solamente $(k-1)$-tuplas, entonces para cada una de los q^{r-1} combinaciones de todos los coeficientes podría haber a lo sumo $k-1$ irreducibles, por lo que el número total de irreducibles $\pi(r,q)$ sería menor o igual que $(k-1)q^{r-1}$ lo cual contradice el resultado anterior. Por lo tanto $q \geq 2(k-1)r$ nos garantiza al menos una k-tupla de irreducibles gemelos de grado r sobre $\mathbb{F}_q$

Es claro ahora el siguiente corolario:

Corolario 2.1. *En la colección de todos los polinomios sobre todos los cuerpos finitos, existen infinitas k-tuplas de irreducibles gemelos para cada $k \geq 2$*

Este corolario nos garantiza la existencia de k-tuplas de irreducibles gemelos a partir de suficientes coeficientes constantes. Sin embargo no es el correcto análogo de la conjetura clásica de los primos gemelos. El correcto análogo está en el caso de la base fija, caso mucho más problemático.

2.2. El Caso de Cuerpos de Bases Fijas

La siguiente conjetura es un análogo más preciso de la conjetura de los primos gemelos en $\mathbb{Z}$

Conjetura 2.1. *Por cada cuerpo finito $\mathbb{F}_q$, existen infinitos polinomios irreducibles gemelos sobre $\mathbb{F}_q$.*

Esta conjetura parece ser más difícil que lo expuesto anteriormente. Con la hipótesis del cuerpo fijo el número de coeficientes constantes se mantiene fijo cuando el grado de n tiende a infinito y por lo tanto la densidad de los irreducibles gemelos decrece rápidamente, al igual que las k-tuplas de irreducibles gemelos para todo k.

Pongamos la siguiente definición:

Definición 2.2. $\pi_2(n;q)$ denota el número de irreducibles gemelos de grado n sobre $\mathbb{F}_q$.

Y planteamos la siguiente conjetura.

Conjetura 2.2. *Para los polinomios irreducibles de grado n finito se tiene*

$$\pi_2(n;q) \sim \delta \left(\frac{q-1}{2}\right) \frac{q^n}{n^2} \prod_P \left(1 - \frac{1}{(|P-1|)^2}\right).$$

Cuando usamos $\sim$ nos referimos a que el cociente de los dos lados se aproxima a 1, donde $\delta = 4$ si $q = 2$ y 1 en otro caso, y el producto se toma sobre todos los polinomios irreducibles P sobre $\mathbb{F}_q$ siempre que $q > 2$, y sobre todos los irreducibles de grado ≥ 2 cuando $q = 2$.

Para establecer heurísticamente esta conjetura imitamos el argumento presentado en la sección 22.20 de [9] adaptándolo al conjunto $\mathbb{F}_q[X]$ de polinomios según sea necesario. En particular necesitamos una versión polinomial del teorema de Mertens la cual presentamos a continuación.

Teorema 2.1 (Teorema de Mertens para polinomios). *Cuando $n \to \infty$*

$$\prod_{\partial P \leq n} \left(1 - \frac{1}{|P|}\right) \sim \frac{e^{-\gamma}}{n},$$

donde P recorre los polinomios unitarios irreducibles y γ es la constante de Euler.

Una demostración de este teorema se encuentra en [17]. Ahora continuamos trabajando en función de la conjetura 2.2.

Definición 2.3. Para un grado r fijo. Definamos un *polinomio primorial* M tal que;

$$M = \prod_{\partial P \leq r/2} P,$$

P polinomio irreducible. El grado de M lo denotamos por m.

Definición 2.4. Un polinomio Y que sea primo relativo con M, sera llamado *polinomio especial*.

Proposición 2.2. *Para cada grado k, sea $S(k)$ el número de polinomios especiales de grado k. Entonces*

$$S(m) = \Phi_q(M) = |M| \prod_{\partial P \leq r/2} \left(1 - \frac{1}{|P|}\right) \sim |M| \frac{2e^{-\gamma}}{r}$$

donde Φ_q es la función definida para polinomios $f \neq 0 \in \mathbb{F}_q[X]$ que cuenta el número de polinomios en $\mathbb{F}_q[X]$ que son de menor grado que el grado de f y son primos relativos con f

Demostración Se encuentra en [6].

La función Φ_q es multiplicativa y si $f = P_1^{e_1}...P_r^{e_r}$ con cada P_i irreducible de grado n_i entonces

$$\Phi_q(f) = \prod_i (q^{n_i} - q^{n_i(e_i-1)})$$

Ahora, el número total de polinomios unitarios cuyo grado es m es $q^m = |M|$ por lo que la proporción de polinomios especiales de grado m es del orden

$$\frac{2e^{-\gamma}}{r}.$$

Ahora consideremos $S(r)$ y observemos que r es mucho más pequeño que m. En efecto por la definición de M tenemos que $S(r)$ es justamente el número de polinomios irreducibles de grado r. Por lo tanto

$$S(r) = \pi(r; q) \sim \frac{q^r}{r}$$

Dado que el total de polinomios de grado r es q^r, la proporción de polinomios especiales de grado r es de orden $\frac{1}{r}$.
Denotaremos por R la relación de las proporciones calculadas de polinomios especiales de grado r y m respectivamente, obteniendo

$$R \sim \frac{1}{2e^{-\gamma}}$$

Ahora dirigimos nuestra atención a los polinomios irreducibles gemelos. Es razonable conjeturar que la relación R_2 de proporcionalidad de parejas especiales de grado r y m respectivamente podría ser

$$R_2 = R^2 \sim \frac{1}{4e^{-2\gamma}}$$

Esto es razonable porque si la probabilidad de que los polinomios $Y(x)$ y $Y(x) + \alpha$ (o $Y(x) + x^2 + x$ cuando $q = 2$) sean irreducibles asumiendo que estas probabilidades son independientes, entonces la probabilidad de que ambos sean irreducibles es justamente el producto de las probabilidades separadas.

Observemos que la afirmación acerca de R_2 es el único punto en el que somos incapaces de proporcionar una prueba, tal y como ocurre en el caso clásico como se argumenta en [9]

Confirmando, recordemos que buscamos una fórmula asintótica para $\pi_2(r; q)$, el número de parejas de polinomios irreducibles gemelos de grado r. Pero sin embargo dada la conjetura en R_2, ahora podemos obtener nuestro objetivo mediante la búsqueda de la proporción de parejas especiales de grado grande m.

Primero vamos a suponer que $q > 2$. Consideremos un par de polinomios especiales Y y $Y + \alpha$ y nos preguntamos ¿cuántos de estos hay de grado m? Para cada P(irreducible) de

grado menor o igual a $r/2$, debemos tener $Y \not\equiv 0 \pmod{P}$ y $Y \not\equiv -\alpha \pmod{P}$, por lo que tenemos $|P|-2$ clases residuales para cada P, dando un conteo de

$$\prod_{\partial P \le r/2} (|P|-2) = |M| \prod_{\partial P \le r/2} \left(1 - \frac{2}{|P|}\right)$$

tales pares de grado m para un α dado.

Como q es impar, entonces α y $-\alpha$ son distintos. Observemos que si Y y $Y+\alpha$ son una pareja de polinomios especiales, entonces son exactamente la misma pareja $Y+\alpha$ y $Y+\alpha-\alpha$. Por lo tanto podemos obtener distintas parejas especiales utilizando la mitad de elementos distintos de cero de $\mathbb{F}_q$ cuando q es impar. Por otro lado, si q es par y mayor que 2, entonces cada $\alpha \neq 0$ tiene la propiedad; si Y y $Y+\alpha$ son un par de polinomios especiales entonces $Y+\alpha$ y $Y+\alpha+\alpha$ son la misma pareja especial. Por lo tanto una vez más obtenemos un factor de $(q-1)/2$. Concluimos entonces que el número total de parejas de polinomios especiales de grado m para $q > 2$ es

$$\frac{q-1}{2}|M| \prod_{\partial P \le r/2} \left(1 - \frac{2}{|P|}\right).$$

El caso $q = 2$ es algo diferente. Recordemos que aquí las parejas difieren por x^2+x en lugar de por una constante. Si Y (de grado m) satisface $Y \equiv 1 \pmod{x}$ o $Y \equiv 1 \pmod{x+1}$, entonces $Y + x^2 + x$ satisface las mismas condiciones. Ahora si $P_3 = x^2+x+1$ es el único irreducible cuadrático (P_3 es el tercer irreducible sobre $\mathbb{F}_2$), entonces esto facilita chequear si $Y \equiv x \pmod{P_3}$ o $Y \equiv x+1 \pmod{P_3}$ entonces $Y+x^2+x$ es también primo relativo con P_3; pero si $Y \equiv 1 \pmod{P_3}$, entonces P_3 divide $Y + x^2 + x$. Así, P_3 proporciona 2 clases residuales ($= |P_3| - 2$) que producen parejas especiales. Ahora para todos los P irreducibles de grado 3 o más, como es el caso $q > 2$, requerimos $Y \equiv 0 \pmod{P}$ y $Y \not\equiv x^2 + x \pmod{P}$. Así obtenemos $|P| - 2$ clases residuales para cada P. Finalmente, notemos que la pareja especial Y y $Y + x^2 + x$ es idénticamente igual a la pareja especial $Y + x^2 + x$ y $(Y + x^2 + x) + (x^2 + x)$, de modo que debemos dividir nuestro conteo por 2 para eliminar la duplicación. Entonces obtenemos en el caso $q = 2$ un conteo de parejas especiales de grado m

$$\frac{1}{2} \prod_{2 \le \partial P \le r/2} (|P|-2) = \frac{1}{8}|M| \prod_{2 \le \partial P \le r/2} \left(1 - \frac{2}{|P|}\right),$$

donde el factor extra de 4 en el denominador del lado derecho aparece porque los dos irreducibles lineales (cada uno de valor absoluto 2) faltan en el producto pues los dos factores lineales irreducibles no aparecen en el producto cuando factorizamos para obtener $|M|$.

Ahora tenemos toda la información necesaria para obtener nuestra deseada fórmula asintótica. La ecuación básica es

$$R_2 = \frac{\text{proporción de parejas especiales de grado } r}{\text{proporción de parejas especiales de grado } m}$$

y así

$$\pi_2(r;q) \sim \frac{R_2(\text{total de grado } r)(\text{número de parejas especiales de grado } m)}{\text{total de grado } m}$$

Recordemos que por el Teorema de Mertens 2.1

$$\frac{2e^{-\gamma}}{r} \sim \prod_{P,\partial P \leq r/2} \left(1 - \frac{1}{|P|}\right)$$

De aquí podemos computar

$$\begin{aligned}
\pi_2(r;q) &\sim \frac{1}{4e^{-2\gamma}} \frac{q^r}{q^m} q^m \left(\frac{q-1}{2\beta}\right) \prod_{\lambda \leq \partial P \leq r/2} \left(1 - \frac{2}{|P|}\right) \\
&\sim \frac{1}{r^2(4e^{-2\gamma})/r^2} q^r \left(\frac{q-1}{2\beta}\right) \prod_{\lambda \leq \partial P \leq r/2} \left(1 - \frac{2}{|P|}\right) \\
&\sim \left(\frac{q-1}{2\beta}\right) \frac{q^r}{r^2} \frac{\prod_{\lambda \leq \partial P \leq r/2} \left(1 - \frac{2}{|P|}\right)}{\left(\prod_{\lambda \leq \partial P \leq r/2} \left(1 - \frac{2}{|P|}\right)\right)^2} \\
&\sim \delta \left(\frac{q-1}{2}\right) \frac{q^r}{r^2} \prod_{\lambda \leq \partial P} \left(1 - \frac{1}{(|P|-1)^2}\right).
\end{aligned}$$

donde $\beta = \begin{cases} 4, & \text{si } q = 2, \\ 1, & \text{en otro caso} \end{cases}$ $\lambda = \begin{cases} 2, & \text{si } q = 2, \\ 1, & \text{en otro caso} \end{cases}$ $\delta = \begin{cases} 4, & \text{si } q = 2, \\ 1, & \text{en otro caso.} \end{cases}$

$\delta = 4$, aparece en el caso $q = 2$ ya que es necesario eliminar los factores de

$$\left(\prod_{P,\partial P \leq r/2} \left(1 - \frac{1}{|P|}\right)^2\right)$$

correspondientes a los dos irreducibles lineales sobre $\mathbb{F}_2$ del producto, y cada uno aporta $1/4$ al denominador. Entonces uno de esos factores de 4 en el numerador se cancela con $\beta = 4$. Completando el argumento heurístico de la conjetura 2.2.

De las consideraciones heurísticas, Effinger *et al* proponen la siguiente conjetura

$$\pi_2(n;q) \sim \delta \left(\frac{q-1}{2}\right) \frac{q^n}{n^2} \prod_P \left(1 - \frac{1}{(|P-1|)^2}\right),$$

donde $\pi_2(n;q)$ denota el número de irreducibles gemelos de grado n sobre $\mathbb{F}_q$.

CAPÍTULO 3

Polinomios irreducibles gemelos sobre cuerpos finitos II

3.1. Una conjetura uniforme

Si $\mathbf{R}(n; M, q)$ denota el número de pares de irreducibles gemelos $(P, P+M)$ donde P es un polinomio irreducible de grado n y si se razona heuristícamente como en el caso racional (compare con [15, pags 409-411] podemos esperar que para $n > \partial M$.

$$\mathbf{R}(n; M, q) \approx \mathbf{R}_0(n; M, q) \tag{3.1}$$

donde

$$\mathbf{R}_0(n; M, q) := (q-1)\frac{q^n}{n^2} \prod_{Q|M} \left(1 - \frac{1}{|Q|}\right)^{-1} \prod_{Q\nmid M} \left(1 - \frac{2}{|Q|}\right)\left(1 - \frac{1}{|Q|}\right)^{-2} \tag{3.2}$$

y Q recorre los polinomios unitarios irreducibles sobre $\mathbb{F}_q$. El factor $q-1$ en (3.2) sale del hecho que P no se restringe a polinomios unitarios.

Podemos *enunciar* varias maneras de volver la aproximación (3.1) más precisa; quizá una de las más obvias es fijar q y M y leer (3.1) como una estimación asintótica cuando $n \to \infty$. Uno de estos casos es el propuesto por Effinger, Hicks y Mullen conjetura 2.2 del capítulo anterior, pero poco se sabe en esta dirección. Solo recientemente Hall [8] pudo mostrar, cuando M es un polinomio constante y $q > 3$, la existencia de un número infinito de parejas de primos gemelos $(P, P+M)$ sobre $\mathbb{F}_q$.

Un caso especial de la proposición 2.1 dice que si M es un polinomio constante no nulo, se tiene que $\mathbf{R}(n; M, q) > 0$ para $q \geq 2n$. Esto sugiere que $\mathbf{R}(n; M, q)$ puede ser más manejable al estudiarlo como una función de varios parámetros. Con esto en mente, se puede justificar, nuevamente por medios heurísticos, la siguiente conjetura.

Conjetura 3.1. *Sea M un polinomio diferente de cero de grado $< n$ sobre $\mathbb{F}_q$. Entonces*

$$\mathbf{R}(n; M, q) = (1 + o(1))\mathbf{R}_0(n; M, q) \text{ si } q^n \to \infty,$$

uniformemente en M. Con otras palabras, para todo $\epsilon > 0$,existe una constante $B = B(\epsilon)$ con la propiedad de que cada vez que M es un polinomio no nulo sobre $\mathbb{F}_q$ de grado $< n$ y $q^n > B$, se tiene

$$|\mathbf{R}(n; M, q) - \mathbf{R}_0(n; m, q)| = o(1)\mathbf{R}_0(n; M, q) < \epsilon\mathbf{R}_0(n; M, q)$$

El propósito de este capítulo es probar una estimación explícita para $\mathbf{R}(n; M, q)$ que confirma la conjetura 3.1 siempre que q/n^2 tiende a infinito uniformemente en la elección de M en $\mathbb{F}_q[X]$ de grado menor que n

Considerando de nuevo el lado derecho de la aproximación (3.2), observamos que cada factor en el segundo producto es $1 + O(|Q|^{-2})$. En efecto,

$$\begin{aligned}
\left(1 - \frac{2}{|Q|}\right)\left(1 - \frac{1}{|Q|}\right)^{-2} &= \left(\frac{|Q| - 2}{|Q|}\right)\left(\frac{|Q| - 1}{|Q|}\right)^{-2} \\
&= \left(\frac{|Q| - 2}{|Q|}\right)\frac{(|Q|)^2}{(|Q| - 1)^2} \\
&= \frac{|Q|^2 - 2\,|Q|}{(|Q| - 1)^2} \\
&= \frac{|Q|^2 - 2\,|Q| + 1}{(|Q| - 1)^2} + \frac{-1}{(|Q| - 1)^2} \\
&= 1 - \frac{1}{(|Q| - 1)^2} \leq 1 + \frac{1}{|Q|^2}, \text{ luego} \\
\left|\left(1 - \frac{2}{|Q|}\right)\left(1 - \frac{1}{|Q|}\right)^{-2} - 1\right| &\leq \frac{1}{|Q|^2}
\end{aligned}$$

lo que implica que

$$\begin{gathered}
\left(1 - \frac{2}{|Q|}\right)\left(1 - \frac{1}{|Q|}\right)^{-2} - 1 = O\left(\frac{1}{|Q|^2}\right), \text{ es decir,} \\
\left(1 - \frac{2}{|Q|}\right)\left(1 - \frac{1}{|Q|}\right)^{-2} = 1 + O\left(\frac{1}{|Q|^2}\right);
\end{gathered}$$

entonces

$$\prod_{Q \nmid M}\left[1 + O\left(\frac{1}{|Q|^2}\right)\right] = \prod_{Q \nmid M}\left[1 + O\left(\frac{1}{(q^{\partial Q})^2}\right)\right] \leq \prod_{n=1}^{\infty}\left[1 + O\left(\frac{1}{q^{2n}}\right)\right]$$

$$\begin{aligned}\prod_{n=1}^{\infty}\left[1+\left(\frac{1}{q^2}\right)^n\right] &= \left(1+\left(\frac{1}{q^2}\right)\right)\left(1+\left(\frac{1}{q^2}\right)^2\right)\left(1+\left(\frac{1}{q^2}\right)^3\right)\dots \\ &= \left(1+\frac{1}{q^2}+\frac{1}{(q^2)^2}+\frac{1}{(q^2)^3}+\frac{1}{(q^2)^4}+\dots\right) \\ &= \frac{1}{1-\frac{1}{q^2}} \\ &= \frac{q^2}{q^2-1} \\ &= \left(\frac{q}{q-1}\right)\left(\frac{q}{q+1}\right) \\ &= \frac{q}{q-1}\left(\frac{q+1}{q+1}-\frac{1}{q+1}\right) \\ &= \frac{q}{q-1}\left(1-\frac{1}{q+1}\right) \\ &= \frac{q}{q-1}\left(1+O\left(\frac{1}{q}\right)\right)\end{aligned}$$

pues $\left|-\frac{1}{q+1}\right| = \frac{1}{q+1} < \frac{1}{q}$ y entonces $-\frac{1}{q+1} = O\left(\frac{1}{q}\right)$.
Sustituyendo en (3.2),

$$\mathbf{R}_0(n;M,q) = (q-1)\frac{q^n}{n^2}\prod_{Q|M}\left(1-\frac{1}{|Q|}\right)^{-1}\frac{q}{q-1}\left(1+O\left(\frac{1}{q}\right)\right)$$

$$\mathbf{R}_0(n;M,q) = \left(1+O\left(\frac{1}{q}\right)\right)\frac{q^{n+1}}{n^2}\prod_{Q|M}\left(1-\frac{1}{|Q|}\right)^{-1}.$$

Ahora, asumiendo la conjetura 3.1

$$\mathbf{R}(n;M,q) = (1+o(1))\mathbf{R}_0(n;M,q), \tag{3.3}$$

cuando $q\to\infty$, y conociendo que

$$\begin{aligned}O(1/q) &= 0 \\ 1+O(1/q) &= 1 \\ (1+O(1/q))(1+o(1)) &= (1+o(1));\end{aligned}$$

Si multiplicamos la igualdad (3.3) por $(1+O(1/q))$ tendríamos

$$\mathbf{R}(n;M,q) = (1+o(1))\frac{q^{n+1}}{n^2}\prod_{Q|M}\left(1-\frac{1}{|Q|}\right)^{-1} \tag{3.4}$$

uniformemente en n y M (con $0\le\partial(M)<n$).

3.2. Una fórmula explícita para el número de polinomios irreducibles en ciertas clases residuales

Sea $\mathbb{M}$ el monoide multiplicativo de polinomios unitarios en $\mathbb{F}_q[X]$. Si $l \geq 0$ y $M \in \mathbb{M}$, definimos una relación $\mathcal{R}_{l,M}$ sobre $\mathbb{M}$ diciendo que $A \equiv B \mod \mathcal{R}_{l,M}$ si y sólo si A y B tienen los mismos primeros l coeficientes próximos al coeficiente director y $A \equiv B$ (mód M). Entonces $\mathcal{R}_{l,M}$ es una relación de congruencia sobre $\mathbb{M}$, es decir, una relación de equivalencia que satisface

$$A \equiv B \pmod{\mathcal{R}_{l,M}} \Rightarrow AC \equiv BC \mod \mathcal{R}_{l,M} \text{ para todo} A, B, C \in \mathbb{M}.$$

Por tanto, hay un monoide cociente bien definido $\mathbb{M}/\mathcal{R}_{l,M}$.

Se puede demostrar que un elemento de $\mathbb{M}$ es invertible módulo $\mathcal{R}_{l,M}$ si y sólo si es coprimo con M.

Utilizando el teorema 1.2 podemos mostrar que las unidades de este monoide forman un grupo abeliano de tamaño $q^l\phi(M)$, el cual denotamos por $(\mathbb{M}/\mathcal{R}_{l,M})^\times$.

Escribimos $\phi(M)$ para el número de unidades en el anillo $\mathbb{F}_q[T]/(M)$; notemos que

$$\prod_{Q|M}\left(1-\frac{1}{|Q|}\right)^{-1} = |M|/\phi(M)$$

donde Q es un polinomio unitario irreducible

Lema 3.1. *Sea A un polinomio primo respecto a M. Entonces*

$$q^l\phi(M) \sum_{\substack{Q^j \equiv A \pmod{\mathcal{R}_{l,M}} \\ \partial Q^j = N}} \partial Q = q^N - \sum_{\chi} \bar{\chi}(A) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^N,$$

donde χ recorre todos los caracteres módulo $\mathcal{R}_{l,M}$. Aquí $a(\chi) \leq l + \partial M$ para todos los χ, y cada $|\beta_i(\chi)| \leq q^{1/2}$

Demostración Fijemos $l \geq n$ y $M \in \mathbb{M}$. Sea χ un carácter de $(\mathbb{M}/\mathcal{R}_{l,M})^\times$, este carácter se puede extender a una función sobre $\mathbb{M}$, definiendo χ de tal manera que se anule en los elementos de $\mathbb{M}$ que no son unidades de $(\mathbb{M}/\mathcal{R}_{l,M})$. Para $u \in \mathbb{C}$ con $|u| < 1/q$, definimos

$$L(u,\chi) := \prod_{Q}(1-\chi(Q)u^{\partial Q})^{-1}. \tag{3.5}$$

Si χ no es trivial, entonces $L(u,\chi)$ es un polinomio en u y para algún entero $a(\chi) \leq l+\partial M$, tenemos una factorización

$$L(u,\chi) = \prod_{i=1}^{a(\chi)}(1-\beta_i(\chi)u), \tag{3.6}$$

De aquí usando la hipótesis de Weil-Riemann (ya esta comprobada) encontramos que $|\beta_i(\chi)| \leq q^{1/2}$ para $i = 1, ..., \alpha(\chi)$ De la representación del producto de Euler (3.5), deducimos al aplicarle logaritmo a la ecuación (3.5)

$$\begin{aligned} Log\,|L(u,\chi)| &= Log\left|\prod_Q (1-\chi(Q)u^{\partial Q})^{-1}\right| \\ &= -\sum Log\left(1-\chi(Q)u^{\partial Q}\right); \end{aligned}$$

luego derivamos respecto a u

$$\begin{aligned} \frac{L'(u,\chi)}{L(u,\chi)} &= -\sum_Q \frac{1}{1-\chi(Q)u^{\partial Q}}\left(-\chi(Q)\partial Q u^{\partial Q-1}\right) \\ \frac{L'(u,\chi)}{L(u,\chi)} &= \sum_Q \frac{\chi(Q)\partial Q u^{\partial Q}}{(1-\chi(Q)u^{\partial Q})\,u} \\ u\frac{L'(u,\chi)}{L(u,\chi)} &= \sum_Q \partial Q \frac{\chi(Q)u^{\partial Q}}{1-\chi(Q)u^{\partial Q}} \\ &= \sum_Q \partial Q\left\{\chi(Q)u^{\partial Q}\frac{1}{1-\chi(Q)u^{\partial Q}}\right\} \text{ obteniendo una serie geométrica} \\ &= \sum_Q \partial Q\left\{\chi(Q)u^{\partial Q}\left(1+\chi(Q)u^{\partial Q}+\chi(Q)^2u^{2\partial Q}+\ldots+\chi(Q)^n u^{n\partial Q}\right]\right\} \\ &= \sum_{N=1}^{\infty} u^N \sum_{\partial Q^j = N} \chi(Q^j)\partial Q; \text{ entendiendo por } N = \partial Q^j = j\partial Q, \end{aligned}$$

mientras que a partir de (3.6), tenemos

$$u\frac{L'(u,\chi)}{L(u,\chi)} = -\sum_{i=1}^{a(\chi)} \frac{\beta_i(\chi)u}{1-\beta_i(\chi)u} = -\sum_{N=1}^{\infty} u^N\left(\sum_{i=1}\beta(\chi)^N\right).$$

Comparando los coeficientes en estas dos expresiones, concluimos que

$$\sum_{\partial Q^j = N} \chi(Q^j)\partial Q = -\sum_{i=1}^{a(x)} \beta_i(\chi)^N.$$

Por otra parte, si

$$\chi = \chi_0 = \begin{cases} \chi_0(Q) = 1, & \text{si } Q \text{ es unidad} \\ \chi_0(Q) = 0, & \text{si } Q \text{ no es unidad} \end{cases}$$

(3.5) se transforma en

$$
\begin{aligned}
L(u,\chi) &:= \prod_{Q\nmid M}(1-\chi_0(Q)u^{\partial Q})^{-1}\\
&= \prod_{Q\nmid M}(1-u^{\partial Q})^{-1}\\
&= \prod_{Q\nmid M}(1-u^{\partial Q})^{-1}\prod_{Q|M}(1-u^{\partial Q})^{-1}\prod_{Q|M}(1-u^{\partial Q})\\
&= \prod_{Q}(1-u^{\partial Q})^{-1}\prod_{Q|M}(1-u^{\partial Q})\\
&= \prod_{n}^{\infty}\left(q^n(1-u^n)^{-1}\right)\prod_{Q|M}(1-u^{\partial Q})\\
&= \prod_{n}^{\infty}\left(\frac{q^n}{(1-u^n)}\right)\prod_{Q|M}(1-u^{\partial Q})\\
&= \left(\frac{q}{(1-u)}\right)\left(\frac{q^2}{(1-u^2)}\right)\left(\frac{q^3}{(1-u^3)}\right)\cdots\prod_{Q|M}(1-u^{\partial Q})\\
&= (1+u+u^2+u^3+\ldots)q\times(1+u^2+(u^2)^2+(u^2)^3+\ldots)q^2\times\\
&\times(1+u^3+(u^3)^2+(u^3)^3+\ldots)q^3\times\ldots\prod_{Q|M}(1-u^{\partial Q})\\
&= \frac{1}{1-qu}\prod_{Q|M}(1-u^{\partial Q}),
\end{aligned}
$$

teniendo en cuenta que $|u|<1/q$. Análogamente, podemos tomar (3.6) y obtener,

$$L(u,\chi)=\frac{1}{1-qu}\prod_{Q|M}(1-u^{\partial Q})=\frac{1}{1-qu}\prod_{i=1}^{a(\chi_0)}(1-\beta_i(\chi_0)u),$$

para ciertas raíces $\beta_i(\chi_0)$ de la unidad, el número de las cuales, $a(\chi_0)$, es exactamente $\sum_{Q|M}\partial Q\leq\partial M$. Procediendo como anteriormente encontramos

$$\sum_{\partial Q^j=N}\chi_0(Q^j)\partial Q=q^N-\sum_{i=1}^{a(\chi_0)}\beta_i(\chi_0)^N.$$

Cabe destacar para el uso futuro que la suma de la derecha es siempre no negativa, ya que $\sum_{\partial Q^j=N}\partial Q=q^N$.

3.3. Teorema de Pollack

Empezamos con el resultado obtenido por Hayes [10] el cual es una versión más débil del resultado principal.

Proposición 3.1. *Sea M un polinomio unitario de grado $n-1$. Si una de las dos condiciones se cumple*

(a) M no admite factores cuadráticos.

(b) n no es divisible por la característica de $\mathbb{F}_q[X]$.

entonces

$$\mathbf{R}(n;M,q)=\frac{q^{2n}}{n^2\phi(M(X))}+O(q^n)$$

cuando $q\to\infty$.

Más generalmente enunciamos el teorema principal.

Teorema 3.1 (Teorema de Pollack). *Sean $k\geq 0$ y $n\geq 2$ enteros tales que $0\leq k<n$. Sea M un polinomio de grado k sobre $\mathbb{F}_q$. Entonces*

$$-\frac{q^n}{n}-4\frac{|M|}{\phi(M)}\frac{q^{n/p+1}}{n^2}\leq \mathbf{R}(n;M,q)-\frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}\leq q^n-\frac{q^n}{n}+2\frac{q^{n/p}}{n}, \tag{3.7}$$

donde p es el menor primo que divide a n.

Observaciones respecto al teorema 3.1 En el caso $k=0$ y $n=1$, el cual no es tenido en cuenta en el teorema. Es fácil ver que $\mathbf{R}(n;M,q)=q^2-q$. En efecto, cuando $0=k=\partial M$ y $1=n=\partial P$ entonces $\partial(P+M)=1$. Luego

$$P=aX+b \quad \text{y} \quad P+M=aX+b+c.$$

Como todo polinomio lineal es irreducible y $\mathbb{F}_q[X]$ es un dominio factorial, tenemos $q(q-1)$ polinomios lineales de grado 1. Entonces $\mathbf{R}(1;M,q)=q(q-1)=q^2-q$.

Dividiendo la desigualdad del teorema por $\frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}$ tenemos al lado derecho

$$\begin{aligned}\mathbf{R}(n;M,q)-\frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}&\leq q^n-\frac{q^n}{n}+2\frac{q^{n/p}}{n}\\ \mathbf{R}(n;M,q)-1&\leq \frac{q^n n^2\phi(M)}{|M|\,q^{n+1}}-\frac{q^n\phi(M)n^2}{q^{n+1}n\,|M|}+2\frac{q^{n/p}n\phi(M)}{|M|\,q^{n+1}}\\ &\leq \frac{\phi(M)}{|M|}\left[\frac{n^2}{q}-\frac{n}{q}+\frac{2n}{q^{n+1-n/q}}\right].\end{aligned}$$

Tenemos $\mathbf{R}(n;M,q)\leq 1+O\left(\frac{n^2}{q}\right)$ de donde obtenemos

$$1+O(\frac{n}{q})\leq \frac{\mathbf{R}(n;M,q)}{(|M|/\phi(M))q^{n+1}/n^2}\leq 1+O(n^2/q).$$

Por esta razón una cota superior se obtiene si $q^n\to\infty$ en forma tal que $n^2/q\to 0$. Entonces

$$\frac{\mathbf{R}(n;M,q)}{|M|/\phi(M)q^{n+1}/n^2} \leq 1 \text{ es decir, } \mathbf{R}(n;M,q) \leq \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}.$$

Una cota inferior se obtiene si $n/q \to 0$; tenemos

$$\mathbf{R}(n;M,q) \leq (|M|/\phi(M))q^{n+1}/n^2.$$

Luego, si tenemos

$$q^n \to \infty \text{ de tal forma que } n^2/q \to 0, \qquad \text{y} \qquad n/q \to 0$$

obtendríamos la igualdad.

$$\mathbf{R}(n;M,q) = (|M|/\phi(M))q^{n+1}/n^2.$$

Este resultado es más fuerte que

$$\mathbf{R}(n;M,q) \leq 8\frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} \tag{3.8}$$

Pero este resultado se obtiene en general para $n \geq 2$, $M \neq 0$ y no constante de grado $< n$ (ver los detalles de la prueba de (3.8) en el apéndice).

En el caso en que k=n-1 se puede ver la demostración del la proposición anterior en [10].

En el caso general, para obtener la cota superior mencionada en el teorema 3.1 se utiliza la demostración de la proposición 3.1 y para obtener la cota inferior se usa una conocida cota para el lema de Gauss (1.2)

$$\pi(n;q) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \leq \frac{q^n}{n}.$$

Demostración [Teorema de Pollack]

Para la demostración del teorema presentamos un argumento heurístico y luego encontraremos la cota superior e inferior de (3.7)

1 **Un argumento heurístico**
Sea M un polinomio de grado k sobre $\mathbb{F}_q$ y supongamos que $n > k$. Sea $H(T)$ un representante de las unidades módulo $\mathcal{R}_{n-1-k,M}$.
Sea N_H el número de primos unitarios de grado n congruentes con $H(T)$ módulo $\mathcal{R}_{n-1-k,M}$.

Además si escogemos al representante $H(T)$ del conjunto de unitarios de grado n, entonces N_H es el cardinal del conjunto $\{H(T) + \alpha M; \alpha \in \mathbb{F}_q\}$

Entonces $\sum_H N_H^2$ es precisamente el número de parejas de primos unitarios Q, Q' de grado n cuya diferencia es αM.
Si $Q' - Q$ es distinto de cero para una pareja de estos polinomios, entonces necesariamente $Q' - Q = \alpha M$ para algún $\alpha \in \mathbb{F}_q^\times$. Luego $\alpha^{-1}Q$ y $\alpha^{-1}Q'$ forman una pareja de

primos diferentes tal que $\alpha^{-1}Q - \alpha^{-1}Q' = M$. Eliminando las parejas donde $Q = Q'$, encontramos que

$$\mathbf{R}(n; M, q) = \sum_H N_H^2 - \pi(n; q). \tag{3.9}$$

Como existen $q^n\phi(M)/|M|$ polinomios unitarios de grado n que son primos con M, de los cuales cerca de q^n/n son polinomios irreducibles de grado n. Por esto, cualquier polinomio unitario de grado n coprimo con M es irreducible, con probabilidad cercana a $n^{-1}|M|/\phi(M)$. Por lo tanto, podemos suponer que N_H es aproximadamente $(q/n)|M|/\phi(M)$ para cada H, y esto nos lleva a esperar que

$$\begin{aligned}\sum_H N_H^2 &\approx (q/n)^2(|M|/\phi(M))^2 \sum_H 1 \\ &= (q/n)^2(|M|/\phi(M))^2 card\,(\mathbb{M}/\mathcal{R}_{n-1-k,M})^\times \\ &= \frac{q^2}{n^2}\frac{|M|^2}{\phi(M)^2} q^{n-1-k}\phi(M) \\ &= \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2}.\end{aligned}$$

2 **Cota inferior**

Para obtener una cota inferior no es necesario conocer los números de N_H individualmente. Como cada primo unitario de grado n pertenece a alguna clase residual módulo $\mathcal{R}_{n-1-k,M}$, Tenemos $\sum_H N_H = \pi(n, q)$, de tal manera que por la desigualdad de Cauchy-Schwarz, y (1.2),

$$\sum_H 1^2 \sum_H N_H^2 \geq \left(\sum_H N_H\right)^2 \geq \left(\frac{q^n}{n} - 2\frac{q^{n/p}}{n}\right)^2 \geq \frac{q^{2n}}{n^2} - 4\frac{q^{n(1+1/p)}}{n^2},$$

y así

$$\begin{aligned}\sum_H N_H^2 &\geq \frac{1}{q^{n-1-k}\phi(M)}\left(\frac{q^{2n}}{n^2} - 4\frac{q^{n(1+1/p)}}{n^2}\right) \\ &= \frac{|M|}{\phi(M)}\left(\frac{q^{n+1}}{n^2} - 4\frac{q^{n/p+1}}{n^2}\right)\end{aligned}$$

La relación (3.9) ahora implica

$$\mathbf{R}(n; M, q) \geq \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} - 4\frac{|M|}{\phi(M)}\frac{q^{n(1+1/p)}}{n^2} - \pi(n; q). \tag{3.10}$$

Una cota superior para $\pi(n; q)$ es q^n/n, luego

$$\mathbf{R}(n; M, q) - \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} \geq -4\frac{|M|}{\phi(M)}\frac{q^{n(1+1/p)}}{n^2} - \frac{q^n}{n}$$

lo cual completa la demostración de la cota inferior.

3 **Cota superior**

Para demostrar la cota superior se siguen las siguientes ideas: Del lema 3.1, si H es un representante de la clase residual unitaria módulo $\mathcal{R}_{n-1-k,M}$, entonces,

$$q^{n-1-k}\phi(M)nN_H \leq q^{n-1-k}\phi(M) \sum_{\substack{Q^j \equiv H \pmod{\mathcal{R}_{n-1-k,M}} \\ \partial Q^j = n}} \partial Q$$
$$= q^n - \sum_{\chi} \bar{\chi}(H) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^n.$$

Tomando cuadrados a ambos lados y sumado sobre H se tiene:

$$n^2 q^{2(n-1-k)}\phi(M)^2 \sum_H N_H^2 \leq \sum_H q^{2n} - 2q^n \sum_H \sum_{\chi} \overline{\chi}(H) \sum_{i=1}^{a(\chi)} \beta_i(\chi)^n$$
$$+ \sum_H \sum_{\chi,\chi'} \bar{\chi}(H)\bar{\chi}'(H) \sum_{\substack{1\leq i\leq a(\chi) \\ 1\leq j\leq a(\chi')}} \beta_i(\chi)^n \beta j(\chi')^n.$$

Intercambiando las sumas sobre H con las sumas sobre χ y χ', y utilizando las relaciones de ortogonalidad 1.3 una vez más, nos encontramos con que el lado derecho se simplifica, así:

$$q^{n-1-k}\phi(M)q^{2n} - 2q^n q^{n-1-k}\phi(M) \sum_{i=1}^{a(\chi_0)} \beta_i(\chi_0)^n$$
$$+ \sum_H \sum_{\chi} \sum_{\substack{1\leq i\leq a(\chi) \\ 1\leq j\leq a(\chi^{-1})}} \beta_i(\chi)^n \beta_j(\chi^{-1})^n.$$

Como se señaló anteriormente, la primera suma que aparece aquí es no negativa y ya que está multiplicada por un término negativo se convierte en una suma no positiva, por lo tanto puede ser ignorado, ya que estamos buscando una cota superior.
Por otra parte, $|\beta_i(\chi)| \leq q^{1/2}$ y $|\beta_j(\chi^{-1})| \leq q^{1/2}$, $a(\chi) \leq n-1$ y $a(\chi^{-1}) \leq n-1$, luego el lado derecho está acotado por

$$q^{3n-1-k}\phi(M) + q^{3n-2-2k}\phi(M)^2 n^2,$$

y

$$(q^{n-1-k}\phi(M))^2 (q^{n/2})^2 n^2 = q^{3n-2-2k}\phi(M)^2 n^2.$$

Por lo tanto

$$\sum_H N_H^2 \leq \frac{q^{3n-1-k}\phi(M) + q^{3n-2-2k}\phi(M)^2 n^2}{n^2 q^{2n-2-2k}\phi(M)^2}$$
$$= \frac{|M|}{\phi(M)} \frac{q^{n+1}}{n^2} + q^n$$

de manera que

$$\begin{aligned}\mathbf{R}(n;M,q) &= \sum_H N_H^2 - \pi(n;q) \\ &\leq \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} + q^n - \pi(n;q).\end{aligned}$$

Insertando la estimación inferior para $\pi(n,q)$ de (1.2),

$$\mathbf{R}(n;M,q) \leq \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} + q^n - \frac{q^n}{n} + 2\frac{q^{n/p}}{n};$$

luego

$$\mathbf{R}(n;M,q) - \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} \leq q^n - \frac{q^n}{n} + 2\frac{q^{n/p}}{n}.$$

Por lo tanto,

$$-\frac{q^n}{n} - 4\frac{|M|}{\phi(M)}\frac{q^{n/p+1}}{n^2} \leq \mathbf{R}(n;M,q) - \frac{|M|}{\phi(M)}\frac{q^{n+1}}{n^2} \leq q^n - \frac{q^n}{n} + 2\frac{q^{n/p}}{n}.\square$$

Como consecuencia del teorema de Pollack tenemos que

$$1 + O(n/q) \leq \frac{\mathbf{R}(n;M,q)}{|M|\,\phi(M)q^{n+1}/n^2} \leq 1 + O(n^2/q)$$

Por lo tanto si q^n tiende a infinito, de tal manera que n^2/q tiende a cero, tenemos que se cumple la convergencia asintótica para la conjetura de Pollack en los casos cuando q es grande comparado con n^2

CAPÍTULO 4

Conclusiones

1. Es posible definir muchos conceptos de la teoría de números clásica en el anillo de polinomios con coeficientes en un cuerpo finito.
2. Las conjeturas de los irreducibles gemelos en el anillo de polinomios se pueden manejar heurirsicamente al igual que en la teoría de números clásica.
3. Es posible garantizar la existencia de los polinomios irreducibles gemelos en el anillo de polinomios $\mathbb{F}_q[X]$.
4. Hay una convergencia asintótica para el número de polinomios irreducibles gemelos en $\mathbb{F}_q[X]$.

APÉNDICE A

Una cota superior para las parejas de primos gemelos en $\mathbb{F}_q[T]$

Éste apéndice se encuentra en [12]. En el cual se establece la siguiente estimación:

Proposición A.1. *Sea $n \geq 2$ un entero, y sea $M \neq 0$ un polinomio de grado menor que n sobre el cuerpo finito $\mathbb{F}_q[T]$. Entonces,*

$$Card\{P : P, P + M son\ irreducibles\ mónico\ de\ grado\ n\} \leq 8\frac{|M|}{\phi(M)}\frac{q^n}{n^2}.$$

Corolario A.1. *Sea $n \geq 2$ un entero, y sea $M \neq 0$ un polinomio de grado menor que n sobre el cuerpo finito $\mathbb{F}_q[T]$ entonces*

$$\mathbf{R}(n, M, Q) \leq 8\frac{|M|}{\phi(M)}\frac{q^n}{n^2}.$$

siempre que $0 \leq \partial M < n$.

La estimación de la proposición A.1 es análoga a una cota superior explícita generalizada sobre pares de primos gemelos obtenida por Riesel y Vaughan ([[16], Lema 5]), pero trabajar en polinomios nos permite dar una prueba mucho más simple. Comenzamos con un análogo de un enunciado de Selberg, (cf. [Webb 13, Teorema 1]).

Proposición A.2. *(Λ^2-Criba de Selberg $\mathbb{F}_q[T]$). Sea $\mathcal{A}$ un conjunto de polinomios sobre $\mathbb{F}_q$, y sea $\mathcal{Q}$ un conjunto finito de polinomios unitarios irreducibles sobre $\mathbb{F}_q$. Supongamos que f es una función multiplicativa definida sobre los divisores libres de cuadrados de $\prod_{Q\in\mathcal{Q}}$ con $1 < f(Q) \leq |Q|$ para cada $Q \in \mathcal{Q}$, y sea*

$$\sum_{\substack{A\in\mathcal{A}\\ D|A}} 1 = \frac{card(\mathcal{A})}{f(D)} + R_D. \tag{A.1}$$

Sea $\mathcal{D}$ cualquier subconjunto no vacío de divisores unitarios de $\prod_{Q\in\mathcal{Q}} Q$ el cual es cerrado (es decir, todo divisor unitario de un elemento de $\mathcal{D}$ pertenece a $\mathcal{D}$). Entonces,

$$\sum_{\substack{A\in\mathcal{A}\\ mcd(A,\prod_{Q\in\mathcal{Q}})=1}} 1 \leq \frac{card(\mathcal{A})}{\sum_{D\in\mathcal{D}} f(D)^{-1}\prod_{Q|D}(1 - f(Q)^{-1})^{-1}}$$

$$+ \sum_{D_1 D_2 \in \mathcal{D}} |X_{D_1} X_{D_2} R_{[D_1,D_2]}|,$$

donde

$$X_D = \mu(D) f(D) \frac{\sum_{C \in \mathcal{D}, D|C} f(C)^{-1} \prod_{Q|D} (1 - f(Q)^{-1})^{-1}}{\sum_{C \in \mathcal{D}} f(C)^{-1} \prod_{Q|D} (1 - f(Q)^{-1})^{-1}}.$$

Antes de seguir introducimos algo más de notación. Sea A un polinomio diferente de cero sobre $\mathbb{F}_q$. Entonces podemos expresar a A de una única forma:

$$A = \epsilon Q_1^{e_1} Q_2^{e_2} \dots Q_r^{e_r},$$

donde $\epsilon \in \mathbf{F}_q^{\times}$ y los Q_i son polinomios unitarios irreducibles distintos. Se definen las funciones aritméticas $\Omega(\cdot)$, $d(\cdot)$, y $rad(\cdot)$ en analogía con sus homólogos enteros de la siguiente manera

$$\Omega(A) := \sum_{i=1}^{r} e_i, \qquad d(A) := \prod_{i=1}^{r} (e_i + 1), \qquad rad(A) := \prod_{i=1}^{r} Q_i.$$

Demostración de la proposición A.1 En el caso en que $q = 2$, podemos suponer que $T(T+1)$ divide a M, pues de lo contrario no hay parejas de primos $P, P + M$ de grado n. Por lo tanto $|Q| > 2$ para cada primo Q que no divide a M. Se define el conjunto

$$\mathcal{A} := \{A(A + M) : A \text{ unitario, grado } A = n\}.$$

Sea $\mathcal{Q}$ el conjunto de los primos unitarios de grado $\leq n/2$. Entonces el número de parejas de primos unitarios de grado n $P, P+M$ es precisamente el número de elementos de $\mathcal{A}$ coprimos con $\prod_{Q \in \mathcal{Q}} Q$, una cantidad que puede estimarse con la proposición A.2. Tomando a $\mathcal{D}$ el conjunto (divisor-cerrado) de polinomios unitarios de grado $\leq n/2$ libres de cuadrados. Se define la función multiplicativa f que aparece en la proposición A.2 de la siguiente forma (para primos unitarios Q)

$$f(Q) = \begin{cases} |Q|/2 & \text{si } Q \text{ no divide a } M, \\ |Q| & \text{si } Q \text{ divide } M, \end{cases}$$

y extendiendo f para que sea una función completamente multiplicativa sobre el monoide de polinomios unitarios. Es fácil comprobar que si el polinomio libre de cuadrados D tiene un grado $\leq n$, entonces (A.1) se cumple sin ningún tipo de error, es decir, con $R_D = 0$.

Dado que el mínimo común múltiplo de cualquier par $D_1, D_2 \in \mathcal{D}$ tiene grado$\leq n$, obtenemos de la proposición A.2, la siguientes desigualdad:

$$\sum_{\substack{A \in \mathcal{A} \\ mcd(A, \prod_{Q \in \mathcal{Q}}) = 1}} 1 \leq \frac{Card\mathcal{A}}{\sum_{D \in \mathcal{D}} f(D)^{-1} \prod_{Q|D} (1 - f(Q)^{-1})^{-1}} \tag{A.2}$$

Para continuar, necesitamos una cota inferior en el denominador de la expresión A.2. Para cada $D \in \mathcal{D}$, escribimos $D = D_1.D_2$, Donde D_1 divide a M y D_2 es primo para M. Entonces tenemos

$$f(D)^{-1} \prod_{Q|D} (1 - f(Q)^{-1})^{-1} = \prod_{Q|D_1} \frac{1}{|Q| - 1} \prod_{Q|D_2} \frac{2}{|Q| - 2},$$

utilizando $|Q| > 2$ para cada Q que divide a D_2. Entonces, hemos reducido el problema a obtener una cota inferior de

$$\sum_{D \in \mathcal{D}} \prod_{Q|D_1} \frac{1}{|Q| - 1} \prod_{Q|D_2} \frac{2}{|Q| - 2},$$

$$= \sum_{D \in \mathcal{D}} \prod_{Q|D_1} \left(\frac{1}{|Q|} + \frac{1}{|Q|^2} + \frac{1}{|Q|^3} + \dots \right) \prod_{Q|D_2} \left(\frac{2}{|Q|} + \frac{4}{|Q|^2} + \frac{8}{|Q|^3} + \dots \right).$$

Podemos escribir esta expresión como

$$\sum_{A \text{ unitario}} \frac{2^{\Omega(A_2)}}{|A|} \sum_{\substack{D \in \mathcal{D} \\ rad(A) = D}} 1,$$

donde A_2 está compuesto por todos los divisores primos de A que no dividen a M. Luego $\sum_{\substack{D \in \mathcal{D} \\ rad(A) = D}} 1 \geq 1$ cuando el grado de A es $\leq n/2$, lo cual produce una cota inferior de

$$\sum_{\substack{A_2 \text{ unitario} \\ \partial A_2 \leq n/2 \\ mcd(A_2, M) = 1}} \frac{2^{\Omega(A_2)}}{|A_2|} \sum_{\substack{A_1 \text{ unitario} \\ \partial A_1 \leq n/2 - \partial A_2 \\ rad(A_1) | M}} \frac{1}{|A_1|} \tag{A.3}$$

Ahora $2^{\Omega(A_2)} \geq d(A_2)$, mientras que para la suma interna tenemos

$$\begin{aligned} \sum_{\substack{A_1 \text{ unitario} \\ \partial A_1 \leq n/2 - \partial A_2 \\ rad(A_1) | M}} \frac{1}{|A_1|} &= \frac{\phi(M)}{|M|} \sum_{\substack{A_1 \text{ unitario} \\ \partial A_1 \leq n/2 - \partial A_2 \\ rad(A_1) | M}} \frac{1}{|A_1|} \prod_{Q|M} \left(1 - \frac{1}{|Q|} \right)^{-1} \\ &= \frac{\phi(M)}{|M|} \sum_{\substack{A_1 \text{ unitario} \\ \partial A_1 \leq n/2 - \partial A_2 \\ rad(A_1) | M}} \frac{1}{|A_1|} \sum_{\substack{B \text{ unitario} \\ rad(B) | M}} \frac{1}{|B|} \\ &\geq \frac{\phi(M)}{|M|} \sum_{\substack{C \text{ unitario} \\ \partial C \leq n/2 - \partial A_2 \\ rad(C) | M}} \frac{d(C)}{|C|}. \end{aligned}$$

Ensamblando estos resultados, encontramos que (A.3) está acotada por abajo por

$$\frac{\phi(M)}{|M|} \sum_{\substack{A \text{ unitario} \\ \partial A \leq n/2}} \frac{d(A)}{|A|}$$

Por un resultado de Carlitz, tenemos $\sum_{\substack{A \text{ unitario} \\ \partial A = k}} d(A) = (k+1)q^k$(L. Carlitz [4]), por lo que nuestra suma final es

$$\sum_{0 \leq k \leq n/2} (K+1) \geq \frac{n^2}{8},$$

de tal manera que (A.3) está acotada inferiormente por $(\phi(M/|M|)n^2/8$. Dado que el numerador de (A.2) $card(A) = q^n$, obtenemos el resultado deseado.

Si $\mathcal{I}_q(n)$ denota el conjunto de unitarios irreducibles de grado n sobre F_q. Entonces, nuestro argumento muestra que para cualquier polinomio M distinto de cero (sin ninguna estricción de su grado), hay a lo más $8(|M|/\phi(M))q^n/n^2$ valores de $P \in \mathcal{I}_q(n)$ para los cuales $P+M$ es libre de factores primos de grado $\leq n/2$. Como consecuencia, hay a lo más

$$8\frac{|M|}{\phi(M)}\frac{q^n}{n^2} + q^{\lfloor n/2 \rfloor + 1}$$

valores de $P \in \mathcal{I}_q(n)$ para los que $P+M$ es irreducible, donde el término $q^{\lfloor n/2 \rfloor + 1}$ puede ser omitido a menos que M tenga grado n y coeficiente principal -1. (El término adicional se debe a los valores irreductibles de $P+M$ que sin embargo son eliminados en la criba, porque $\partial(P+M) \leq n/2$.)

Bibliografía

[1] Víctor Samuel Albis. *Lecciones sobre la Teoíra Aritmética de Polinomios. Policopiado.* Universidad Nacional de Colombia, Bogotá, 2009.

[2] Tom M. Apostol. *Introduction to analytic number theory.* Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[3] Chris K. Caldwell. Top twenty'ss. *http://primes.utm.edu/top20/page.php?id=1*, 2012.

[4] Leonard Carlitz. The Arithmetic of Polynomials in a Galois Field. *Amer. J. Math.*, 54(1):39–50, 1932.

[5] P. A. Clement. Congruences for sets of primes. *Amer. Math. Monthly*, 56:23–25, 1949.

[6] Gove W. Effinger and David R. Hayes. *Additive number theory of polynomials over a finite field.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1991. Oxford Science Publications.

[7] Gove W. Effinger, Kenneth H. Hicks, and Gary L. Mullen. Twin irreducible polynomials over finite fields. In *Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001)*, pages 94–111. Springer, Berlin, 2002.

[8] Chris Hall. L-functions of twisted Legendre curves. *J. Number Theory*, 119(1):128–147, 2006.

[9] G.H Hardy and E. M Wright. *An Introduction to the Theory of Numbers.* Oxford Science Publications, Oxford, 1979.

[10] David Hayes. A polynomial analog of the Goldbach conjecture. *Bull. Amer. Math. Soc.*, 69:115–116, 1963.

[11] David R. Hayes. The distribution of irreducibles in GF$[q, x]$. *Trans. Amer. Math. Soc.*, 117:101–127, 1965.

[12] Paul Pollack. A polynomial analogue of the twin prime conjecture. *Proc. Amer. Math. Soc.*, 136(11):3775–3784, 2008.

[13] P Ribenboim. *The Book of Prime Number Records.* Springer, New York, 1989.

[14] P. Ribenboim. *The Little Book of Big Primes.* Springer, New York, 1991.

[15] P. Ribenboim. *The New Book of Prime Number Records*. Springer, New York, 1996.

[16] H. Riesel and R. C. Vaughan. On sums of primes. *Ark. Mat.*, 21(1):46–74, 1983.

[17] Michael Rosen. A generalization of Mertens' theorem. *J. Ramanujan Math. Soc.*, 14(1):1–19, 1999.

[18] P. Sebag and X. Gourdon. Introduction to twin primes and Brun primes constant computation. *http://numbers.computation.free.fr/Constants/constants.html*, 2002.