Facultad de Ciencias

Sobre los coeficientes de los polinomios ciclotómicos

(On the Coefficients of Cyclotomic Polynomials)

Trabajo de Fin de Grado
para acceder al

Grado en Matemáticas

Autor: Pablo Señas Peón

Director: María Pilar Fernández-Ferreirós Erviti

Julio - 2019

Resumen/Abstract

Para cada n, el conjunto de raíces sobre $\mathbb{Q}$ del polinomio $x^n - 1$ es un grupo cíclico multiplicativo de orden n. Los $\varphi(n)$ generadores de este grupo, donde φ es la función de Euler, se llaman raíces n-simas primitivas de la unidad, y el polinomio mónico de menor grado que se anula en ellas es el n-simo polinomio ciclotómico, denotado por $g_n(x)$.

Siempre que $n < 105$, los coeficientes de $g_n(x)$ toman valores en $\{-1, 0, 1\}$. Este hecho motivó que los coeficientes de dichos polinomios fueran objeto de investigaciones que continúan hasta el día de hoy; actualmente se sabe que esto ocurre cuando n sea producto de dos primos impares distintos. Por otro lado, desde que Schur probó en 1931 que existen coeficientes de polinomios ciclotómicos de magnitud arbitrariamente grande, son de interés los resultados que acotan los coeficientes en casos particulares.

En el siguiente trabajo se expondrán y demostrarán algunos de estos resultados.

Palabras clave: Polinomio, Ciclotómico

For each n, the set of roots over $\mathbb{Q}$ of the polynomial $x^n - 1$ is a multiplicative cyclic group of order n. The $\varphi(n)$ generators of this group, where φ is Euler's totient function, are called primitive nth roots of unity, and the monic polynomial of smallest degree that vanishes at each of these elements is the nth cyclotomic polynomial, denoted by $g_n(x)$.

Whenever $n < 105$, the coefficients of $g_n(x)$ belong to $\{-1, 0, 1\}$. This fact encouraged the study of the coefficients of these polynomials, which continues to this day; nowadays it is known that the coefficients of $g_n(x)$ belong to that set if n is product of two odd primes. Furthermore, since Schur proved in 1931 that there exist coefficients of cyclotomic polynomials arbitrarily large, it has also been a topic of interest to bound the size of the coefficients in particular cases.

In this article we aim to expose and prove some of these results.

Palabras clave: Polynomial, Cyclotomic

Índice general

Introducción **1**

1. Propiedades Generales **3**
1.1. Conceptos Básicos 3
1.2. La función de Möbius 8

2. Polinomios ciclotómicos de orden 2 **11**
2.1. Acotando los coeficientes 11
2.2. Determinando los coeficientes 13

3. Polinomios ciclotómicos de orden 3 **21**
3.1. Una expresión de los coeficientes 21
3.2. Teoremas de periodicidad 24
3.3. Polinomios ternarios planos 29

4. Sobre la magnitud de los coeficientes **33**
4.1. Teorema de Schur 33
4.2. Cotas sobre polinomios ternarios 36
4.3. Polinomios ciclotómicos de órdenes mayores 43
4.3.1. Teoremas de periodicidad 43
4.3.2. Polinomios ciclotómicos planos 43

Bibliografía **44**

Introducción

La ciclotomía es el problema de dividir una circunferencia en partes iguales. Este desafío se remonta a la Grecia clásica y sus geómetras, que intentaban dividir una circunferencia en partes iguales con la única ayuda de una regla y un compás. Si queremos dividir una circunferencia en el plano complejo, de centro el origen y radio 1, en n partes iguales, cada uno de estos puntos que la cortan es solución de la ecuación $x^n - 1 = 0$, y como sabemos el conjunto de soluciones es $\{e^{\frac{2\pi i}{n}} : 0 \leq i \leq n-1\}$. El n-simo polinomio ciclotómico, denotado por $g_n(x)$, tiene como raíces a aquellas del conjunto anterior que además cumplen $(i, n) = 1$.

Según [8], la ciclotomía comenzó a estudiarse desde un punto de vista analítico a principios del siglo XVIII: Abraham de Moivre intenta expresar las raíces de la unidad usando funciones trigonométricas. Posteriormente, se estudiarían casos particulares de los polinomios ciclotómicos. Por ejemplo, en 1711 Euler estudia los 10 primeros polinomios ciclotómicos, y en el mismo año Vandermonde se centra en $g_{11}(x)$. En 1796, un joven Gauss prueba que el polígono regular de 17 lados es construible con regla y compás, lo que se consideró un gran descubrimiento: hasta entonces, nadie pensaba que nada más allá del pentágono regular fuera construible de tal forma ([25]). La importancia de este resultado animó a Gauss, que en ese momento tenía 19 años, a dedicarse a las matemáticas en vez de a la filología. Hoy en día sabemos que el n-gono regular es construible con regla y compás si y solo si $n = 2^m p_1 \cdots p_k$, donde p_i es un primo de Fermat, es decir, es primo de la forma $p_i = 2^{2^{k_i}} + 1$ (este resultado se conoce como Teorema de Gauss-Wantzel, quienes probaron en 1801 y 1837 que esa hipótesis era condición suficiente y necesaria, respectivamente).

En ese momento, Gauss también probó que $g_n(x)$ era irreducible. Su prueba, así como otras, se pueden encontrar en [27]. En la primera mitad del siguiente siglo, Abel prueba que los polinomios $g_n(x)$ son resolubles por radicales, es decir, que las soluciones de $g_n(x) = 0$ pueden expresarse a partir de sumas, restas, multiplicaciones, divisiones, potencias y raíces de los coeficientes del polinomio. Los siguientes resultados estarían centrados en estudiar los coeficientes de $g_n(x)$. En 1883 el matemático alemán Adolf Migotti prueba que cuando n es producto de dos primos, el valor absoluto de los coeficientes no excede de 1. En 1931, Schur

probó que el valor absoluto de los coeficientes no está acotado, tomando n como producto de un número suficientemente grande de primos impares. Rolf Bungers afinó este resultado tres años más tarde, y probó que cuando n es el producto de tres primos impares pueden encontrarse coeficientes suficientemente grandes en el supuesto de que existan infinitos pares de primos gemelos. En 1936 Emma Lehmer eliminaría esta última hipótesis. Por otra parte, en 1987 Jiro Suzuki mejora la demostración de Schur, probando que todo entero es coeficiente de algún polinomio ciclotómico.

Sabiendo que la magnitud de los coeficientes no está acotada cuando n es solamente el producto de 3 primos, nace el interés por buscar, en este contexto, cotas de los coeficientes para casos particulares. Un primer resultado es de 1895, donde Bang prueba que si $n = pqr$, donde $p < q < r$ son primos impares, entonces la magnitud de los coeficientes no excede de $p - 1$. El interés por mejorar esta cota llega hasta nuestros días: en 2009 se probaría que no excede de $\frac{2p}{3}$.

El siguiente trabajo pretende repasar el conocimiento existente sobre los coeficientes de los polinomios ciclotómicos. En el primer capítulo se definirán los conceptos más básicos y se mostrarán las propiedades más elementales de estos polinomios, que serán necesarias en el resto del trabajo. El segundo y el tercer capítulo están dedicados al n-simo polinomio ciclotómico, cuando n es producto de dos y de tres primos impares, respectivamente. Como podremos ver, hay un conocimiento muy completo de los coeficientes en el primer caso, pero se complica sustancialmente en el segundo. El último capítulo tendrá un enfoque más amplio: expondremos cotas generales para pasar a estudiar cotas sobre polinomios ternarios, complementando así el estudio comenzado en el capítulo 3. Por último, hablaremos de los últimos avances hechos en este tema, y de todos los interrogantes que aún quedan por responder.

En general, se han seleccionado algunos de los resultados entre los muchos que pueden encontrarse en la literatura pasada y actual. De los escogidos, no se han demostrado todos por falta de espacio. La bibliografía sirve no solamente como referencia de los resultados demostrados aquí, sino que también permitirá al lector interesado en ampliar el conocimiento acceder a las pruebas no expuestas.

Por último, el cálculo de todos los polinomios ciclotómicos no referenciado ha sido computado por cuenta propia, utilizando la plataforma gratuita WolframAlpha: el comando *cyclotomic[n,f(x)]* devuelve $g_n(f(x))$.

Capítulo 1

Propiedades Generales

1.1. Conceptos Básicos

Definición 1.1.1 *Sea $u \in \mathbb{C}^*$. Se dice que u tiene orden finito si existe un entero $n > 0$ tal que $u^n = 1$, y se define su orden como*

$$o(u) := \text{mín}\{n \geq 1 \colon u^n = 1\}$$

Definición 1.1.2 *Sea $\epsilon \in \mathbb{C}$ y n un entero positivo. Se dice que ϵ es una raíz n-sima de la unidad si $\epsilon^n = 1$ o, equivalentemente, si ϵ es raíz del polinomio $x^n - 1$.*

Proposición 1.1.3 *ϵ es una raíz n-sima de la unidad $\Leftrightarrow o(\epsilon)|n$*

Dem: Sea ϵ tal que $o(\epsilon)|n$. Entonces $o(\epsilon) = \frac{n}{d}$ para algún $d \in \mathbb{N}$ y $\epsilon^{\frac{n}{d}} = 1$, lo que implica que $\epsilon^n = 1$. Por otra parte, si $\epsilon^n = 1$, escribiendo $n = q \cdot o(\epsilon) + r$ con $q, r \in \mathbb{N}$ y $0 \leq r < o(\epsilon)$, se tiene que $\epsilon^n = \epsilon^{q \cdot o(\epsilon) + r} = \epsilon^{q \cdot o(\epsilon)} \epsilon^r = \epsilon^r = 1$. Ha de ser $r = 0$, luego $o(\epsilon)|n$.

Como consecuencia, resulta que el conjunto de raíces de $x^n - 1$ en $\mathbb{C}$ coincide con el conjunto de números complejos cuyo orden es finito y divide a n.

Definición 1.1.4 *Las raíces de $x^n - 1$ cuyo orden es exactamente n se llaman raíces primitivas n-simas de la unidad.*

Proposición 1.1.5 *Para cada $n \in \mathbb{N}$, las raíces de $x^n - 1$ en $\mathbb{C}$ forman un grupo cíclico de orden n, generado por $e^{2\pi i/n}$.*

Este grupo contiene, por tanto, exactamente $\varphi(n)$ elementos de orden n que son todos los de la forma $e^{2\pi ik}/n$ con $1 \leq k \leq n$ y $(k, n) = 1$.

Dem: Si se representa por $R(x^n-1)$ el conjunto de raíces n-simas de la unidad en $\mathbb{C}$, es obvio que $e^{2\pi i/n}$ es un elemento de $R(x^n-1)$ de orden n, luego el número de elementos de $R(x^n-1)$ es al menos n.

Por otro lado, al tener x^n-1 grado n, esta ecuación no puede tener más de n raíces en $\mathbb{C}$; luego $R(x^n-1)$ tiene n elementos y coincide con el conjunto de las n potencias distintas de $e^{2\pi i/n}$. Resulta así que $R(x^n-1)$ un grupo cíclico de orden n generado por $e^{2\pi i/n}$.

Definición 1.1.6 *Para cada entero positivo n, se define el n-simo polinomio ciclotómico como*

$$g_n(x) := \prod_{o(u)=n} (x-u)$$

Por la Proposición 1.1.5, sabemos que el grado de $g_n(x)$ es $\varphi(n)$ y que sus raíces en $\mathbb{C}$ son los complejos $e^{2\pi ik/n}$ donde k recorre los valores de $\{1,\ldots,n\}$ tales que $(k,n)=1$.

De las propiedades elementales de la Teoría de Galois se deduce fácilmente que cada polinomio ciclotómico tiene coeficientes racionales. Una vez probada su irreducibilidad, que no es trivial y tampoco vamos a tratar aquí por no desviarnos del tema objeto del trabajo, se puede caracterizar también por ser el polinomio mínimo sobre $\mathbb{Q}$ de cualquier raíz primitiva n-sima de la unidad.

Lo que sí probaremos es que los coeficientes de cualquier polinomio ciclotómico son además números enteros, así como algunas otras propiedades generales que serán necesarias a lo largo del trabajo.

Proposición 1.1.7 $x^n-1 = \prod_{d|n} g_d(x)$

Dem: Como hemos visto, las n raíces de x^n-1 son distintas. Además, el orden de cada raíz en el grupo multiplicativo es divisor de n. Por tanto:

$$x^n-1 = \prod_{o(\epsilon)|n} (x-\epsilon) = \prod_{d|n} \left(\prod_{o(\epsilon)=d} (x-\epsilon) \right) = \prod_{d|n} g_d(x)$$

A partir de las dos expresiones, y si se hace doble conteo sobre el grado de $g_n(x)$, este resultado nos permite probar una propiedad interesante de la función de Euler, cuya prueba estándar (se puede encontrar en el Teorema 2.2 de [1]) es más complicada:

Corolario 1.1.8 *Para cada entero $n>1$, se cumple que $n = \sum_{d|n} \varphi(d)$*

Como se muestra en el ejemplo siguiente, la Proposición 1.1.7 resulta útil para determinar polinomios ciclotómicos.

Ejemplo 1.1.9 a) *Para cada p primo, se tiene que*

$$g_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

b) $x^{10} - 1 = g_1(x)g_2(x)g_5(x)g_{10}(x)$*:*

$$\begin{aligned} g_{10}(x) =& \frac{x^{10} - 1}{g_1(x)g_2(x)g_5(x)} = \frac{x^{10} - 1}{(x-1)(x+1)\frac{x^5-1}{x-1}} \\ =& \frac{x^{10} - 1}{(x-1)(x+1)(x^4 + x^3 + x^2 + x + 1)} \\ =& x^4 - x^3 + x^2 - x + 1 \end{aligned}$$

Proposición 1.1.10 $\forall n \geq 1\ g_n(x) \in \mathbb{Z}[x]$

Dem: Inducción sobre n:

- $n = 1$: $g_1(x) = x - 1 \in \mathbb{Z}[x]$
- Sea $n > 1$ y suponemos el resultado cierto para todo $k < n$.
- Sea $f(x) = \prod_{d|n, d<n} g_d(x)$. Se tiene que $f(x) \in \mathbb{Z}[x]$ por hipótesis de inducción.

  Por otra parte, resulta de Proposición 1.1.7 que $x^n - 1 = f(x)g_n(x)$ en $\mathbb{Q}[x]$ con $f(x) \in \mathbb{Z}[x]$ mónico. Aplicando el algoritmo de la división en $\mathbb{Z}[x]$ a $x^n - 1$ y $f(x)$:

  $$x^n - 1 = f(x)q(x) + r(x)$$

  con $q(x), r(x) \in \mathbb{Z}[x] \subseteq \mathbb{Q}[x]$ y $\deg(r(x)) < \deg(f(x))$ o $r(x) = 0$.

  Por tanto,

  $$x^n - 1 = f(x)g_n(x) = f(x)q(x) + r(x) \text{ en } \mathbb{Q}[x]$$

  y ahora, por la unicidad del cociente y del resto en $\mathbb{Q}[x]$, se cumple que $r(x) = 0$ y $q(x) = g_n(x)$, lo que prueba el resultado.

Proposición 1.1.11 *Para cada $n > 1$, $g_n(x)$ es un polinomio recíproco. Es decir, si $g_n(x) = \sum_{k=0}^{\varphi(n)} a_k x^k$, entonces $a_k = a_{\varphi(n)-k}$ para $k \in \{1, \cdots, \varphi(n)\}$.*

Dem: Dado $f(x) = \sum_{k=0}^{n} a_k x^k$, se cumple que $x^n f\left(\frac{1}{x}\right) = \sum_{k=0}^{n} a_{n-k} x^k$.

$$x^n f\left(\frac{1}{x}\right) = x^n \left(a_0 + a_1 \frac{1}{x} + \cdots + a_n \frac{1}{x^n}\right) = \sum_{k=0}^{n} a_k x^{n-k} = \sum_{k=0}^{n} a_{n-k} x^k$$

Como para todo $\epsilon \in \mathbb{C}^*$, $o(\epsilon) = o(\epsilon^{-1})$, los polinomios $x^{\varphi(n)} g_n(\frac{1}{x})$ y $g_n(x)$ tienen los mismos ceros. Además, tienen el mismo grado y son mónicos, luego coinciden.

Proposición 1.1.12 a) *Si p es primo y k es un entero positivo,*

$$g_{p^k}(x) = g_p\left(x^{p^{k-1}}\right)$$

b) *Si $n = {p_1}^{k_1} \dots p_r^{k_r}$ con $p_1, \dots, p_r$ primos distintos,*

$$g_n(x) = g_{p_1 \dots p_r}\left(x^{p_1^{k_1-1} \dots p_r^{k_r-1}}\right)$$

c) *Si n es entero positivo impar, $g_{2n}(x) = g_n(-x)$*

d) *Si p primo y n entero positivo primo con p, $g_{pn}(x) = \frac{g_n(x^p)}{g_n(x)}$*

e) *$g_n(0) = 1$ para cada $n > 1$.*

f) *$g_n(1) = p$ si n es potencia de un primo p y $g_n(1) = 1$ en otro caso.*

Dem: Puesto que los polinomios ciclotómicos no tienen raíces múltiples y son mónicos, para probar las igualdades en a) b) y c) bastará comprobar que los polinomios implicados en cada igualdad tienen el mismo grado y que cada raíz de uno cualquiera de ellos es raíz del otro.

a) En este caso, $\operatorname{gr}\left(g_{p^k(x)}\right) = \varphi\left(p^k\right) = p^{k-1}(p-1) = \operatorname{gr}\left(g_p\left(x^{p^{k-1}}\right)\right)$.

Sea $\epsilon \in \mathbb{C}$ raíz de $g_{p^k}(x)$:

$$\begin{aligned} o(\epsilon) = p^k \Rightarrow & o\left(\epsilon^{p^{k-1}}\right) = p \Rightarrow \epsilon^{p^{k-1}} \text{ es raíz de } g_p(x) \\ \Rightarrow & \epsilon \text{ es raíz de } g_p\left(x^{p^{k-1}}\right) \end{aligned}$$

b) Comprobamos que ambos polinomios tienen el mismo grado:

$$\operatorname{gr}(g_n(x)) = \varphi(n) = \varphi(p_1^{k_1} \cdots p_r^{k_r}) = (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1})$$

$$\begin{aligned} \operatorname{gr}\left(g_{p_1 \cdots p_r}\left(x^{p_1^{k_1-1} \cdots p_r^{k_r-1}}\right)\right) &= \varphi(p_1 \cdots p_r)\left(p_1^{k_1-1} \cdots p_r^{k_r-1}\right) = \\ &= (p_1 - 1) \cdots (p_r - 1)(p_1^{k_1-1} \cdots p_r^{k_r-1}) \\ &= (p_1^{k_1} - p_1^{k_1-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) \end{aligned}$$

Sea $\epsilon \in \mathbb{C}$ raíz de $g_n(x)$:

$$\begin{aligned} o(\epsilon) = p_1^{k_1} \cdots p_r^{k_r} \Rightarrow & o\left(\epsilon^{p_1^{k-1} \cdots p_r^{k_r-1}}\right) = p_1 \cdots p_r \\ \Rightarrow & \epsilon^{p_1^{k-1} \cdots p_r^{k_r-1}} \text{ es raíz de } g_{p_1 \cdots p_r}(x) \\ \Rightarrow & \epsilon \text{ es raíz de } g_{p_1 \cdots p_r}\left(x^{p_1^{k_1-1} \cdots p_r^{k_r-1}}\right) \end{aligned}$$

c) Como n es impar, $\varphi(2n) = \varphi(n)$. Si ϵ es raíz de $g_{2n}(x)$,

$$o(\epsilon) = 2n \Rightarrow o(\epsilon^n) = 2 \Rightarrow \epsilon^n = -1 \Rightarrow (-\epsilon)^n = 1$$

Se deduce ahora que $o(-\epsilon)|n$, pero, para que $o(\epsilon) = 2n$, debe ser $o(-\epsilon) = n$, lo que implica que $-\epsilon$ es raíz de $g_n(x)$ y, por tanto, que ϵ es raíz de $g_n(-x)$.

d) Probaremos que $g_{pn}(x)g_n(x) = g_n(x^p)$ por el procedimiento seguido en los apartados anteriores. En primer lugar, vemos que

$$\mathrm{gr}(g_{pn}(x)g_n(x)) = \varphi(pn)+\varphi(n) = (p-1)\varphi(n)+\varphi(n) = p\varphi(n) = \mathrm{gr}(g_n(x^p))$$

Si ϵ es raíz de $g_{pn}(x)g_n(x)$, distinguimos dos casos:

- Si ϵ es raíz de $g_{pn}(x)$, $o(\epsilon) = pn \Rightarrow o(\epsilon^p) = n \Rightarrow \epsilon^p$ es raíz de $g_n(x) \Rightarrow$ ϵ es raíz de $g_n(x^p)$.
- Si ϵ es raíz de $g_n(x)$, $o(\epsilon) = n \Rightarrow o(\epsilon^p) = n \Rightarrow \epsilon^p$ es raíz de $g_n(x) \Rightarrow$ ϵ es raíz de $g_n(x^p)$

Por tanto, cada raíz de $g_{pn}(x)g_n(x)$ es raíz de $g_n(x^p)$ y ambos polinomios coinciden.

e) Inducción sobre n:

- $n = 2$: $g_2(x) = x + 1$, con $g_2(0) = 1$
- Sea $n > 2$ y suponemos el resultado cierto para todo k con $1 < k < n$.
- Sea $f(x) = \prod_{d|n,1<d<n} g_d(x)$. Se tiene que $f(0) = 1$ por hipótesis de inducción. Por otra parte, $x^n - 1 = (x - 1)f(x)g_n(x)$. Evaluando en 0:

$$-1 = -1f(0)g_n(0) \Rightarrow g_n(0) = 1$$

f)

- Si n es primo, entonces $g_n(x) = x^{n-1} + x^{n-2} + \cdots + x + 1$, y $g_n(1) = p$. Si $n = p^k$, entonces por a)

$$g_n(x) = g_p(x^{p^{k-1}})$$

y de nuevo $g_n(1) = p$.

- Sea $n = p_1^{k_1} \cdots p_r^{k_r}$ con $p_1, \cdots, p_r$ primos distintos. Como queremos evaluar en $x = 1$, por b) podemos suponer sin pérdida de generalidad que $n = p_1 \cdots p_r$. Sea $m = p_2 \cdots p_r$. Entonces, por d):

$$g_n(1) = g_{p_1 m}(1) = \tfrac{g_m(1)}{g_m(1)} = 1$$

Corolario 1.1.13 *Para estudiar los coeficientes de $g_n(x)$ con n entero positivo cualquiera, es suficiente considerar el caso que n es producto de primos impares distintos.*

Dem: En efecto, por los apartados a) y b) se puede reducir el problema al caso en que n es libre de cuadrados. Finalmente, por c) se puede suponer que es impar.

Como se muestra en el corolario anterior, las propiedades vistas en la Proposición 1.1.12 permiten reducir el problema de estudiar los coeficientes de un polinomio ciclotómico cualquiera $g_n(x)$ al caso en el que n es producto de primos impares distintos. Esto motiva la siguiente definición, sobre la que se estructurará gran parte de este trabajo.

Definición 1.1.14 *Si n es producto de t primos impares distintos, se dice que el polinomio ciclotómico $g_n(x)$ tiene orden t.*

La sección siguiente tiene como objeto obtener una nueva expresión del polinomio ciclotómico que será de utilidad en algunas demostraciones posteriores.

1.2. La función de Möbius

Definición 1.2.1 *La función de Möbius μ está definida sobre los enteros positivos y toma valores en el conjunto $\{-1, 1, 0\}$ de un dominio cualquiera. Se define de la manera siguiente: $\mu(1) = 1$ y, para cada $n > 1$ es*

$$\mu(n) = \begin{cases} (-1)^r & \text{si } n \text{ es producto de } r \text{ primos distintos} \\ 0 & \text{si } n \text{ no es libre de cuadrados} \end{cases}$$

Proposición 1.2.2 *La función μ cumple:*

a) *Si m, n son enteros positivos tales que $(m, n) = 1$, entonces $\mu(nm) = \mu(n)\mu(m)$.*

b) *Si $n = p_1 \dots p_t$, es $\sum_{d/n} \mu(n) = 0$.*

c)

$$\sum_{d/n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n > 1 \end{cases}$$

Dem:

a) Si alguno de los enteros n o m es 1, el resultado es trivial y también lo es si alguno de ellos no es libre de cuadrados, puesto que entonces mn tampoco lo es.

Supongamos entonces que m y n son libres de cuadrados: $m = p_1 \dots p_r$ y $n = q_1 \dots q_s$ con $p_1, \dots, p_r, q_1, \dots, q_s$ primos distintos ya que $(m, n) = 1$. Entonces, es $\mu(n) = (-1)^r$ y $\mu(m) = (-1)^s$ y $\mu(nm) = (-1)^{r+s} = \mu(m)\mu(n)$.

b) Si $n = p_1 \dots p_r$ con $p_1, \dots, p_r$ primos distintos, los divisores de n son: $1, p_1, \dots, p_r, p_1p_2, p_1p_3, \dots, p_{r-1}p_r, \dots, p_1 \dots p_r$.

Para el divisor $d = 1$, es $\mu(d) = 1$.

Para los $\binom{t}{1}$ divisores d que son primos, es $\mu(d) = -1$.

Para los $\binom{t}{2}$ divisores d que son producto de dos primos, es $\mu(d) = 1$.

Para los $\binom{t}{3}$ divisores d que son primos, es $\mu(d) = -1$, y así sucesivamente hasta llegar al divisor $d = n$ para el cual $\mu(d) = 1$ si t es par y -1 si t impar.

Por tanto

$$\sum_{d/n} \mu(d) = 1 - \binom{t}{1} + \binom{t}{2} - \binom{t}{3} + \cdots + (-1)^{t-1}t + (-1)^t = (1 + (-1))^t = 0$$

c) Se considera ahora la función $s(n) = \sum_{d|n} \mu(d)$ que, para un primo p y un entero $r \geq 0$, cumple $s(p^r) = 1$ si $r = 0$ y, si $r > 0$,

$$s(p^r) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) = 1 - 1 + 0 + \cdots + 0 = 0$$

Si $n = p_1^{k_1} \dots p_r^{k^r}$ con $p_1, \dots, p_r$ primos distintos, se cumple que $\mu(d) = 0$ para cada divisor d de n salvo para los que sean libres de cuadrados. Entonces, $\mu(n) = \mu(p_1 \dots p_r) = 0$ por el apartado anterior.

Proposición 1.2.3 *(Fórmula de inversión de Möbius) ([24]) Si $f(x)$ es una función definida sobre los enteros positivos que toma valores en un dominio cualquiera D y, para cada entero $n \geq 1$, se define la función g mediante $g(n) = \sum_{d/n} f(d)$, se cumple que*

$$f(n) = \sum_{d/n} g(d)\mu\left(\frac{n}{d}\right) = \sum_{d/n} g\left(\frac{n}{d}\right)\mu(d)$$

donde μ es la función de Möbius.

Dem: Se considera la suma

$$\sum_{d|n} g\left(\frac{n}{d}\right)\mu(d) = \sum_{d_1d_2=n} \mu(d_1)g(d_2) = \sum_{d_1d_2=n} \left(\mu(d_1) \sum_{d|d_2} f(d)\right) =$$

$$= \sum_{d_1 d/n} \mu(d_1)f(d) = \sum_{d/n} f(d) \sum_{d_1/\frac{n}{d}} \mu(d_1)$$

Puesto que, según lo probado en la Proposición 1.2.2, todos los sumandos de $\sum_{d_1|\frac{n}{d}} \mu(d_1)$ son cero cuando $n/d \neq 1$, resulta que solamente queda el sumando corespondiente a $d = n$, es decir,

$$\sum_{d|n} f(d) \sum_{d_1|\frac{n}{d}} \mu(d_1) = f(n)$$

Como la fórmula obtenida en la Proposición 1.2.3 es válida para cualquier función $f : \mathbb{N} \longrightarrow D$ donde D es un dominio, tiene también la correspondiente versión multiplicativa que es la que utilizaremos en adelante:

Proposición 1.2.4 *(Fórmula de inversión de Möbius: versión multiplicativa)*
Si D es un dominio, $f(x)$ una función $\mathbb{N} \to D$ y se considera la función g definida, para cada entero $n \geq 1$, por $g(n) = \prod_{d|n} f(d)$, se cumple que

$$f(n) = \prod_{d|n} g(d)^{\mu(\frac{n}{d})} = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}$$

donde μ es la función de Möbius.

Dem:

$$\prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)} = \prod_{d_1 d_2 = n} g(d_2)^{\mu(d_1)} = \prod_{d_1 d_2 = n} \left(\prod_{d|d_2} f(d)^{\mu(d_1)} \right) =$$

$$= \prod_{d_1 d | n} f(d)^{\mu(d_1)} = \prod_{d|n} f(d)^{\sum_{d_1 | \frac{n}{d}} \mu(d_1)}$$

Puesto que $\sum_{d_1 | \frac{n}{d}} \mu(d_1) = 0$ salvo cuando $\frac{n}{d} = 1$, entonces $\prod_{d|n} g(\frac{n}{d})^{\mu(d)} = f(n)$.

Corolario 1.2.5 *Si n es un entero positivo y $g_n(x)$ el n-simo polinomio ciclotómico,*

$$g_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

donde μ es la función de Möbius.

Dem: Se considera la función $f : \mathbb{N} \to \mathbb{Z}[x]$ dada por $f(n) = g_n(x)$; entonces, para cada $n \geq 1$, es $g(n) = \prod_{d|n} f(d) = \prod_{d|n} g_d(x) = x^n - 1$ por la Proposición 1.1.7. Aplicando ahora la Fórmula de Inversión de Möbius se obtiene que

$$g_n(x) = f(n) = \prod_{d|n} g_d(x)^{\mu(n/d)} = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Capítulo 2

Polinomios ciclotómicos de orden 2

El primer caso a estudiar es cuando n es de la forma $2^a p^b q^c$ con p, q primos impares distintos. Como se ha visto en el Corolario 1.1.13, para conocer cómo son los coeficientes de esta familia de polinomios ciclotómicos basta suponer que $n = pq$.

$$\begin{aligned}
g_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\
g_{35}(x) &= x^{24} - x^{23} + x^{19} - x^{18} + x^{17} - x^{16} + x^{14} - x^{13} + x^{12} - \\
&\quad -x^{11} + x^{10} - x^8 + x^7 - x^6 + x^5 - x + 1 \\
g_{77}(x) &= x^{60} - x^{59} + x^{53} - x^{52} + x^{49} - x^{48} + x^{46} - x^{45} + x^{42} - x^{41} + x^{39} \\
&\quad -x^{37} + x^{35} - x^{34} + x^{32} - x^{30} + x^{28} - x^{26} + x^{25} - x^{23} + x^{21} \\
&\quad -x^{19} + x^{18} - x^{15} + x^{14} - x^{12} + x^{11} - x^8 + x^7 - x + 1
\end{aligned}$$

Estos tres polinomios tienen muchas cosas en común, como se puede observar. Por ejemplo, todos los coeficientes están en el conjunto $\{-1, 0, 1\}$; también se tiene que los coeficientes no nulos se alternan entre 1 y -1. Además, todos tienen un número impar de términos. Sin embargo, existen algunas diferencias, como la del valor del coeficiente intermedio, que no siempre es el mismo: los coeficientes intermedios de $g_{15}(x)$ y $g_{77}(x)$ ($-x^4$ y $-x^{30}$) son -1, mientras el de $g_{35}(x)$ (x^{12}) es 1. En este capítulo se abordarán todos estos aspectos.

2.1. Acotando los coeficientes

A continuación se presenta un lema que ayudará a probar el primer resultado importante de este capítulo: si n no tiene como factores a más de dos primos impares, los coeficientes del n-simo polinomio ciclotómico son -1, 0 o 1.

Lema 2.1.1 *[7] Sean p y q primos distintos. Se tiene que*

a) $g_q(x^p) = g_{pq}(x)g_q(x)$

b) $(x^{pq}-1)g_{pq}(x) = g_q(x^p)g_p(x^q)(x-1)$

Dem:

a) Es un caso particular del apartado d) en la Proposición 1.1.12.

b) Los divisores de pq son 1, p, q y pq y, por tanto, $g_{pq}(x)g_p(x)g_q(x)g_1(x) = x^{pq}-1$. Además, por el apartado anterior

$$g_p(x) = \frac{g_p(x^q)}{g_{pq}(x)} \qquad \text{y} \qquad g_q(x) = \frac{g_q(x^p)}{g_{pq}(x)}.$$

Sustituyendo estas expresiones en la primera identidad y multiplicando ambos miembros por $g_{pq}(x)$ resulta que

$$(x^{pq}-1)g_{pq}(x) = g_p(x^q)g_q(x^p)g_1(x) = g_p(x^q)g_q(x^p)(x-1).$$

Proposición 2.1.2 *[7] Si p y q son primos distintos, los coeficientes del polinomio $g_q(x^p)g_p(x^q)$ están en $\{0,1\}$.*

Dem: Recordamos que $g_p(x) = \sum_{i=0}^{p-1} x^i$, y de igual forma para $g_q(x)$. Con ello, se obtiene:

$$g_q(x^p)g_p(x^q) = (1+x^p+\cdots+x^{(q-1)p})(1+x^q+\cdots+x^{(p-1)q}) = \sum_{m,n} x^{mp+nq},$$

donde $0 \le m < q$ y $0 \le n < p$. Si probamos que cada uno de los pq monomios que hay en el sumatorio tienen distinto grado, habremos terminado. Vamos a suponer que existen $n, n', m, m' \in \mathbb{N}$ de tal manera que $pm+qn = pm'+qn'$ y, sin pérdida de generalidad, que $0 \le m < m' < q$. Se tiene entonces que $p(m'-m) = q(n-n')$. Se deduce que $q|p$ o $q|(m'-m)$. Ninguna de las dos cosas es posible, porque $0 < m'-m < q$, y por tanto todos los monomios tienen distinto grado.

Teorema 2.1.3 *[7] Si p y q son primos distintos, los coeficientes de $g_{pq}(x)$ están en $\{-1,0,1\}$.*

Dem: Por el Lema 2.1.1, se sabe que $(x^{pq}-1)g_{pq}(x) = g_q(x^p)g_p(x^q)(x-1)$.

Prestando atención al miembro de la izquierda de esta igualdad, se observa que los coeficientes del polinomio $(x^{pq}-1)g_{pq}(x)$ son, salvo el signo, los mismos que los de $g_{pq}(x)$. Esto se debe a que $\mathrm{gr}(x^{pq}-1) = pq > (p-1)(q-1) = \mathrm{gr}(g_{pq}(x))$, y entonces no coinciden los grados de ninguno de los monomios de $x^{pq}g_{pq}(x)$ y $g_{pq}(x)$. Por tanto, es suficiente probar que los coeficientes de $g_q(x^p)g_p(x^q)(x-1)$ están en $\{-1,0,1\}$. De la Proposición 2.1.2 se deduce que los coeficientes de $g_q(x^p)g_p(x^q)$ están en $\{0,1\}$ y los de $-g_q(x^p)g_p(x^q)$ en $\{-1,0\}$, lo que completa la demostración.

Hemos conseguido uno de los dos objetivos de esta sección: probar que, para todo n de la forma $n = 2^a p^b q^c$, los coeficientes del n-simo polinomio están en $\{-1, 0, 1\}$.

2.2. Determinando los coeficientes

El siguiente objetivo será especificar el valor de cada coeficiente de $g_{pq}(x)$. Además, esto permitirá probar la relación entre los signos de los monomios adyacentes que se observaba al principio de la sección. Para ello, comenzamos exponiendo un lema que nos garantiza que $(p-1)(q-1)$ admite una expresión como combinación lineal de p y q donde los coeficientes son enteros no negativos. Este resultado es un caso particular del problema resuelto en [6].

Lema 2.2.1 *[6] Dados p, q primos, existen $r, s \in \mathbb{N} \cup \{0\}$ tales que*

$$rp + sq = pq - p - q + 1$$

Además $0 < r < q - 1$ y $0 < s < p - 1$.

Dem: En primer lugar, se observa que $pq - p - q + 1 = (p-1)(q-1) = \varphi(pq)$.

La ecuación $xp \equiv (p-1)(q-1)$ mód q tiene solución en $\mathbb{F}_q$: por ser $p \neq q$, existe un solo $a \in \{0, \ldots, q-1\}$ tal que $ap \equiv 1$ mód q y entonces se tiene que $(p-1)(q-1)a$ mód q es solución de la ecuación.

Tomando ahora como r el único entero en $\{0, \ldots, q-1\}$ de forma que $r \equiv (p-1)(q-1)a$ mód q, resulta que $rp \equiv (p-1)(q-1)$ mód q y existe entonces $s \in \mathbb{Z}$ tal que $rp + sq = (p-1)(q-1)$. Finalmente, como $0 \leq r \leq q-1$ y

$$s = \frac{(p-1)(q-1) - rp}{q} \geq \frac{(p-1)(q-1) - (q-1)p}{q} = \frac{-q+1}{q} > -1,$$

luego $s \geq 0$. Teniendo ahora en cuenta que $rp + sq = (p-1)(q-1) < pq$, debe ser $s < p$.

Se puede probar, además, que $r < q-1$ y $s < p-1$. Para ello se considera la ecuación inicial, $rp + sq = pq - (p+q) + 1$, y suponemos que $r = q-1$. Sustituyendo, se obtiene que $sq = 1 - q < 0$, cosa que no es posible porque $s \geq 0$; por otra parte, si se toma $s = p-1$, obtenemos que $rp = 1 - p < 0$.

Teorema 2.2.2 *[18] Sean p, q primos impares distintos y r, s como en el Lema 2.2.1. Entonces el pq-ésimo polinomio ciclotómico está dado por*

$$g_{pq}(x) = \sum_{i=0}^{r} x^{ip} \sum_{j=0}^{s} x^{jq} - \sum_{i=r+1}^{q-1} x^{ip} \sum_{j=s+1}^{p-1} x^{jq} x^{-pq}.$$

Dem: En primer lugar, se recuerda que $r < q-1$ y que $s < p-1$. Se observa además que cada monomio obtenido al desarrollar el primer sumando de la

expresión anterior tiene grado $\leq rp+sq$ y que al desarrollar el segundo el grado mínimo obtenido es

$$(r+1)p+(s+1)q-pq = rp+sq-pq+p+q = (pq-p-q+1)-pq+p+q = 1$$

Queda visto que $\sum_{i=0}^{r} x^{ip} \sum_{j=0}^{s} x^{jq} - \sum_{i=r+1}^{q-1} x^{ip} \sum_{j=s+1}^{p-1} x^{jq} x^{-pq}$ es, en efecto, un polinomio. Se procede a probar que es el pq-ésimo polinomio ciclotómico. Sea ϵ una raíz primitiva pq-ésima de la unidad: como $o(\epsilon) = pq$, entonces $o(\epsilon^p) = q$ y $o(\epsilon^q) = p$. Por tanto:

$$g_q(\epsilon^p) = 0 \qquad g_p(\epsilon^q) = 0$$

Por el Ejemplo 1.1.9, se sabe que $g_t(x) = \sum_{i=0}^{t-1} x^i$ para t primo. En virtud de esto

$$\sum_{i=0}^{q-1} (\epsilon^p)^i = 0 \qquad \sum_{j=0}^{p-1} (\epsilon^q)^j = 0$$

En el Lema 2.2.1 se vio que $r < q-1$ y que $s < p-1$, así que las expresiones precedentes pueden separarse de la siguiente manera:

$$\sum_{i=0}^{r} \epsilon^{ip} = -\sum_{i=r+1}^{q-1} \epsilon^{ip} \qquad \sum_{j=0}^{s} \epsilon^{jq} = -\sum_{j=s+1}^{p-1} \epsilon^{jq}$$

Multiplicando ambas identidades y restando, se obtiene que

$$\sum_{i=0}^{r} \epsilon^{ip} \sum_{j=0}^{s} \epsilon^{jq} - \sum_{i=r+1}^{q-1} \epsilon^{ip} \sum_{j=s+1}^{p-1} \epsilon^{jq} = 0$$

Como ϵ es una raíz primitiva pq-ésima, $\epsilon^{-pq} = 1$, y se tiene que

$$\sum_{i=0}^{r} \epsilon^{ip} \sum_{j=0}^{s} \epsilon^{jq} - \sum_{i=r+1}^{q-1} \epsilon^{ip} \sum_{j=s+1}^{p-1} \epsilon^{jq} \epsilon^{-pq} = 0.$$

Se considera el polinomio

$$f(x) = \sum_{i=0}^{r} x^{ip} \sum_{j=0}^{s} x^{jq} - \sum_{i=r+1}^{q-1} x^{ip} \sum_{j=s+1}^{p-1} x^{jq} x^{-pq},$$

del que se hacen las siguientes consideraciones:

- $f(x)$ se anula en las $\varphi(pq)$ raíces primitivas pq-ésimas de la unidad.
- El grado del primer sumando es $rp+sq = (p-1)(q-1) = \varphi(pq)$.
- El grado del segundo sumando es $p(q-1)+q(p-1)-pq = pq-q-p < (p-1)(q-1)$.

Por tanto, $f(x)$ es un polinomio mónico de grado $\varphi(pq)$ que tiene como raíces las primitivas pq-ésimas de la unidad. Ha de ser $f(x) = g_{pq}(x)$.

Corolario 2.2.3 *[18] Sean p, q primos impares distintos, r, s enteros no negativos de forma que $rp + sq = (p-1)(q-1)$, y $g_{pq}(x) = \sum_{k=0}^{\varphi(pq)} a_k x^k$ el pq-ésimo polinomio ciclotómico. Se tiene que:*

- *$a_k = 1$ si y solo si existen $i \in \{0, \cdots, r\}$ y $j \in \{0, \cdots, s\}$ de forma que $k = ip + jq$.*
- *$a_k = -1$ si y solo si existen $i \in \{r+1, \cdots, q-1\}$ y $j \in \{s+1, \cdots, p-1\}$ de forma que $k + pq = ip + jq$.*
- *$a_k = 0$ en otro caso.*

Dem: En el teorema anterior se ha demostrado que

$$g_{pq}(x) = \sum_{i=0}^{r} x^{ip} \sum_{j=0}^{s} x^{jq} - \sum_{i=r+1}^{q-1} x^{ip} \sum_{j=s+1}^{p-1} x^{jq} x^{-pq} \tag{2.1}$$

En primer lugar, se tendría que ver que en el desarrollo de las expresiones $\sum_{i=0}^{r} x^{ip} \sum_{j=0}^{s} x^{jq}$ y $\sum_{i=r+1}^{q-1} x^{ip} \sum_{j=s+1}^{p-1} x^{jq} x^{-pq}$, considerándolas por separado, no hay dos monomios con el mismo grado. Esta prueba es análoga a la que se hace en la Proposición 2.1.2. Para completar la demostración, falta ver que no hay ningún grado repetido si consideramos ambos desarrollos juntos. En caso de que ocurriera lo contrario, entonces existirían $i \in \{0, \cdots, r\}, j \in \{0, \cdots, s\}, i' \in \{r+1, \cdots, q-1\}, j' \in \{s+1, \cdots, p-1\}$ de forma que $ip + jq = i'p + j'q - pq$, y por tanto

$$pq = (i' - i)p + (j' - j)q.$$

Entonces $p|(j' - j)q$, y se tiene que $p|(j' - j)$ o $p|q$. Ninguna de las dos cosas es posible, porque q es primo y $1 \leq j' - j \leq p-1$. Por tanto, los monomios de $g_{pq}(x)$ con coeficiente 1 son los que vienen de $\sum_{i=0}^{r} x^{ip} \sum_{j=0}^{s} x^{jq}$; los de coeficiente -1 provienen de $\sum_{i=r+1}^{q-1} x^{ip} \sum_{j=s+1}^{p-1} x^{jq} x^{-pq}$ y solamente tienen coeficientes nulos los monomios cuyos grados no admiten una representación de ninguna de las dos formas descritas.

Hasta el momento ha quedado probado que los coeficientes son $-1, 0$ o 1 y además se ha especificado cuándo toman cada uno de esos valores. A continuación se probarán unos resultados sobre la relación entre los coeficientes y el valor del coeficiente intermedio, terminando así con el estudio de todas las propiedades vistas en los primeros ejemplos.

Proposición 2.2.4 *Sean p, q primos impares. Entonces la diferencia entre el número de coeficientes 1 y -1 de $g_{pq}(x)$ es de 1.*

Dem: Consideramos también r y s como hasta ahora. La expresión del pq-ésimo polinomio ciclotómico dada en la Ecuación 2.1 permite calcular cuántos términos hay de cada tipo: se obtienen $(r+1)(s+1)$ monomios con coeficiente 1, y $(p-s-1)(q-r-1)$ con coeficiente -1. Restando ambas cantidades se obtiene el resultado deseado:

$$\begin{aligned} & (r+1)(s+1) - (p-s-1)(q-r-1) = \\ = \; & (r+1)(s+1) - (p-(s+1))(q-(r+1)) = \\ = \; & -pq + (s+1)q + p(r+1) = -pq + (p-1)(q-1) + p + q = \\ = \; & -pq + (rp+sq) + p + q = 1 \end{aligned}$$

Como la diferencia entre ambos tipos de términos es 1, entonces hay un número impar de monomios con coeficientes no nulos en $g_{pq}(x)$. En los ejemplos de polinomios expuestos al principio del capítulo se observaba cómo, considerando todos los términos, el coeficiente del medio nunca era nulo. Una de las preguntas que cabe hacerse es si esto siempre es así, y más concretamente: ¿qué valor toma el coeficiente del medio del pq-ésimo polinomio ciclotómico?

Proposición 2.2.5 *[18] Sean p, q primos impares distintos, r, s enteros no negativos de forma que $rp + sq = (p-1)(q-1)$, $l = \frac{(p-1)(q-1)}{2}$, y $g_{pq}(x) = \sum_{k=0}^{\varphi(pq)} a_k x^k$ el pq-ésimo polinomio ciclotómico. Entonces se tiene que $a_l = (-1)^r = (-1)^s$.*

Dem: De la identidad $(p-1)(q-1) = rp + sq$ se deduce que r y s tienen la misma paridad: como p y q son impares, el miembro de la izquierda de la identidad es par, y el de la derecha solamente puede serlo si r y s son o bien ambos pares o bien ambos impares. Se distinguen ahora casos dependiendo de la paridad:

- Si r es par, entonces $l = \frac{r}{2}p + \frac{s}{2}q$ y en virtud del Corolario 2.2.3 se tiene que $a_l = 1$.
- Si r es impar, entonces se tiene:

  $$\left(\frac{r+q}{2}\right)p + \left(\frac{s+p}{2}\right)q = \frac{rp+sq}{2} + pq = l + pq$$

  Como $r \leq q-2$, entonces $\frac{r+q}{2} \leq q-1$ y, por otro lado, $\frac{r+q}{2} \geq r+1$. Análogamente, $s+1 \leq \frac{s+p}{2} \leq p-1$. De nuevo, por el mismo corolario $a_l = -1$.

Proposición 2.2.6 *[20] Si $n = pq$ donde p, q son primos impares distintos, los coeficientes no nulos de $g_{pq}(x)$ toman alternativamente los valores 1 y -1.*

Dem: Como

$$x^{pq}-1 = g_1(x)g_p(x)g_q(x)g_{pq}(x) = (x-1)g_p(x)g_q(x)g_{pq}(x),$$

podemos escribir $g_{pq}(x)$ de la siguiente forma:

$$\begin{aligned} g_{pq}(x) &= \frac{x^{pq}-1}{(x-1)g_p(x)g_q(x)} = \frac{(x-1)(x^{pq}-1)}{(x^p-1)(x^q-1)} = \\ &= \frac{x^{pq}-1}{x^q-1}\,\frac{1-x}{1-x^p} = (1-x)\sum_{i=0}^{p-1} x^{iq}\sum_{j=0}^{\infty} x^{jp} \end{aligned}$$

El producto $\sum_{i=0}^{p-1} x^{iq}\sum_{j=0}^{\infty} x^{jp}$ se puede escribir en la forma $\sum x^t$, donde los exponentes t recorren los enteros de la forma $iq+jp$ con $j \geq 0$ y $0 \leq i \leq p-1$, con lo que $g_{pq}(x) = (1-x)\sum x^t$.

Ninguno de los exponentes t tiene más de una representación de esta forma: si $iq+jp = i'q+j'p$, entonces $(i-i')q = p(j'-j)$, de donde se deduce que p divide a $i-i'$. Esto solo es posible cuando $i-i'=0$, en cuyo caso $i=i'$ y $j=j'$.

Es claro ahora que al desarrollar el producto $(1-x)\sum x^t$ se obtiene un polinomio que es suma de un cierto número de pares de monomios del tipo $x^{iq+jp} - x^{iq+jp+1}$.

Si $g_{pq}(x) = \sum_{k=0}^{\varphi(pq)} a_k x^k$, diremos que el entero $k \in \{0,\ldots\varphi(pq)\}$ es representable cuando $k = iq+jp$ para algún $i \in \{0,\ldots,p-1\}$ y algún $j \geq 0$. En la lista de monomios $x^{iq+jp}-x^{iq+jp+1}$ aparecen con coeficiente 1 todos aquellos cuyo exponente k es representable y con coeficiente -1 los de exponente $k+1$ siendo k representable. Pero hay que tener en cuenta que el número consecutivo de un entero k representable puede ser también representable, en cuyo caso en la suma que da lugar al polinomio $g_{pq}(x)$ aparecen $(x^k-x^{k+1})+(x^{k+1}-x^{k+2}) = x^k-x^{k+2}$. Si $k+2$ no es representable, aparecerá el monomio x^{k+2} con coeficiente -1.

Queda claro así que x^k tendrá coeficiente 1 cuando k sea representable y $k-1$ no lo sea. Y tendrá coeficiente 0 cuando $k-1$ sea también representable. Por otro lado, si k no es representable y $k-1$ sí lo es, el sumando $x^{k-1}-x^k$ forma parte de g_{pq} y el sumando x^k-x^{k-1} no aparece, luego x^k tendrá coeficiente -1 y finalmente, si ni k ni $k-1$ son representables, los sumandos $x^{k-1}-x^k$ y x^k-x^{k+1} no aparecen, luego x^k tendrá coeficiente 0.

En resumen, para $k=0$ es siempre $a_0=1$ y para $k>0$ se dan los siguientes casos:

1. k y $k-1$ representables: entonces $a_k = 0$.

2. k representable y $k-1$ no representable: entonces $a_k = 1$.

3. k no representable y $k-1$ representable: entonces $a_k = -1$.

4. k y $k-1$ no representables: entonces $a_k = 0$.

Se observa ahora que los coeficientes no nulos del polinomio corresponden a los casos en que k y $k-1$ son uno representable y el otro no, en un caso toman el valor 1 y en el otro -1. Es claro entonces que van alternando los valores 1 y -1.

A modo de ejemplo, analizamos ahora la situación mostrada en la demostración anterior en el caso del polinomio $g_{77}(x)$.

Ejemplo 2.2.7

$p = 7$, $q = 11$, $\mathrm{gr}(g_{77}(x)) = 60$. Entonces

$$g_{77}(x) = (1-x)\sum_{i,j} x^{11i+7j} = \sum_{ij} (x^{11i+7j} - x^{11i+7j+1})$$

con $i \in \{0,1,2,3,4,5,6\}$ y $j \geq 0$. Relacionamos ahora las sumas de monomios del tipo $(x^{11i+7j} - x^{11i+7j+1})$ con grado ≤ 60:

- $i = 0$: $x^{7j} - x^{7j+1}$:

$$(1-x) + (x^7 - x^8) + (x^{14} - x^{15}) + (x^{21} - x^{22}) + (x^{28} - x^{29}) + \\ +(x^{35} - x^{36}) + (x^{42} - x^{43}) + (x^{49} - x^{50}) + (x^{56} - x^{57})$$

- $i = 1$: $x^{7j+11} - x^{7j+12}$

$$(x^{11} - x^{12}) + (x^{18} - x^{19}) + (x^{25} - x^{26}) + (x^{32} - x^{33}) + (x^{39} - x^{40}) \\ +(x^{46} - x^{47}) + (x^{53} - x^{54}) + x^{60}$$

- $i = 2$: $x^{7j+22} - x^{7j+23}$

$$(x^{22} - x^{23}) + (x^{29} - x^{30}) + (x^{36} - x^{37}) + (x^{43} - x^{44}) + (x^{50} - x^{51}) \\ +(x^{57} - x^{58})$$

- $i = 3$: $x^{7j+33} - x^{7j+34}$

$$(x^{33} - x^{34}) + (x^{40} - x^{41}) + (x^{47} - x^{48}) + (x^{54} - x^{55})$$

- $i = 4$: $x^{7j+44} - x^{7j+45}$

$$(x^{44} - x^{45}) + (x^{51} - x^{52}) + (x^{58} - x^{59})$$

- $i = 5$: $x^{7j+55} - x^{7j+56}$

$$(x^{55} - x^{56})$$

- $i = 6$: $x^{7j+66} - x^{7j+67}$ tienen grado mayor que 60 para cada j

Los enteros de la forma $11i + 7j$ del conjunto $\{0, \ldots, 60\}$ son

$$0, 7, 11, 14, 18, \boxed{21{,}22}, 25, \boxed{28{,}29}, \boxed{32{,}33}, \boxed{35{,}36}, \boxed{39{,}40}, \boxed{42{,}43{,}44},$$
$$\boxed{46{,}47}, \boxed{49{,}50{,}51}, \boxed{53{,}54{,}55{,}56{,}57{,}58}, 60$$

donde se han agrupado en cajas los que forman una serie de enteros consecutivos.

Los enteros no representables del conjunto anterior son

$$1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 15, 16, 17, 19, 20, 23, 24, 26, 27, 30, 31, 34, 37, 38,$$
$$41, 45, 48, 52, 59$$

Los coeficientes 1 del polinomio corresponden en este caso a los valores de k que son representables pero $k + 1$ no lo es, es decir

$$0, 7, 11, 14, 18, 21, 25, 28, 32, 35, 39, 42, 46, 49, 53, 60$$

Los coeficientes -1 van asociados a aquellos k que no son representables pero su predecesor sí lo es. Son

$$1, 8, 12, 15, 19, 23, 26, 30, 34, 37, 41, 45, 48, 52, 59$$

Los demás valores k, cuyo coeficiente es cero, se corresponden con los casos 1 y 4 considerados en la Proposición anterior y son, respectivamente,

$$22, 29, 33, 36, 40, 43, 44, 47, 50, 51, 54, 55, 56, 57, 58$$

y

$$9, 13, 16, 17, 20, 24, 27, 31, 38, 10.$$

En efecto,

$$\begin{aligned} g_{77}(x) \;=\; & x^{60} - x^{59} + x^{53} - x^{52} + x^{49} - x^{48} + x^{46} - x^{45} + x^{42} - x^{41} + x^{39} \\ & - x^{37} + x^{35} - x^{34} + x^{32} - x^{30} + x^{28} - x^{26} + x^{25} - x^{23} + x^{21} - x^{19} \\ & + x^{18} - x^{15} + x^{14} - x^{12} + x^{11} - x^{8} + x^{7} - x + 1 \end{aligned}$$

El proceso mostrado anteriormente y la distribución de los coeficientes se puede visualizar de manera más gráfica en un diagrama sencillo de construir, llamado diagrama LLL, que recibe el nombre de los matemáticos Lenstra Jr., Lam y Leung. El origen de este diagrama no está claro, pero se ha visto expuesto en [22]. La idea es la siguiente:

Teniendo en cuenta que el grupo $(\mathbb{Z}/pq\mathbb{Z})$ es suma directa de sus subgrupos $< p >$ y $< q >$, es claro que cada entero k mód pq se escribe de una sola manera en la forma $rp + sq$ con $0 \leq r \leq q - 1$ y $0 \leq s \leq p - 1$. Se colocan sobre el plano euclídeo los puntos (r, s) correspondientes a los enteros $0, \ldots pq - 1$ y se denota por (r_0, s_0) la posición asociada al 1, es decir, que $r_0 p + s_0 q \equiv 1$ mód pq.

Sea $k = rp + sq$ mód pq un elemento cualquiera de este diagrama, y c_k el coeficiente de x^k en el pq-ésimo polinomio ciclotómico. Se tiene que:

- Si $r \geq r_0$ y $s \geq s_0$, entonces $c_k = -1$.
- Si $r < r_0$ y $s < s_0$, entonces $c_k = 1$.
- En los otros dos casos, $c_k = 0$.

Una demostración de este resultado se puede encontrar en [23]. En continuación con el ejemplo anterior, dibujaremos el diagrama para los casos $p = 7$, $q = 11$. Se puede notar cómo coinciden ambos procedimientos.

66	73	3	10	17	24	31	38	45	52	59
55	62	69	76	6	13	20	27	34	41	48
44	51	58	65	72	2	9	16	23	30	37
33	40	47	54	61	68	75	5	12	19	26
22	29	36	43	50	57	64	71	1	8	15
11	18	25	32	39	46	53	60	67	74	4
0	7	14	21	28	35	42	49	56	63	70

El estudio de los polinomios ciclotómicos de orden 2 no termina aquí, y en todo momento está relacionado con las ecuaciones $rp + sq = k$ con $r, s \geq 0$. A su vez, esto está estrechamente relacionado con los semigrupos numéricos, que son subconjuntos de los enteros no negativos que contienen al 0, cerrados bajo la suma y cuyo complemento en $\mathbb{N}$ es finito. Se puede consultar [22] para más información sobre esto. Otro resultado interesante, probado originalmente en [12] y demostrado de otra forma en la fuente anterior, está relacionado con la diferencia máxima entre los coeficientes de dos monomios consecutivos en $g_{pq}(x)$: este salto es $p-1$ y ocurre exactamente $2\lfloor \frac{q}{p} \rfloor$ veces. Volviendo al Ejemplo 2.2.7, puede comprobarse que el salto máximo es de longitud $p - 1 = 6$ y ocurre en 2 ocasiones, entre los monomios x^7 y $-x$ y entre $-x^{59}$ y x^{53}.

Capítulo 3

Polinomios ciclotómicos de orden 3

Se define $\mathrm{A}(n)$ como el máximo de los valores absolutos de los coeficientes de $g_n(x)$. En el capítulo anterior se ha probado que $\mathrm{A}(n) = 1$ siempre que n es producto de dos primos impares distintos y libre de cuadrados.

Definición 3.0.1 *Los polinomios ciclotómicos de la forma $g_{pqr}(x)$ con p, q, r primos impares distintos se denominan polinomios ciclotómicos ternarios.*

La estructura de este capítulo está motivada por el cálculo del primer polinomio ciclotómico ternario:

$$\begin{aligned} g_{105}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} \\ & + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^{9} - x^{8} - \mathbf{2}x^{7} - x^{6} - x^{5} + x^{2} + x + 1 \end{aligned}$$

Se observa que $A(105) = 2$, lo que es una novedad respecto a los polinomios estudiados en previamente. En este capítulo, primero se estudiarán los coeficientes de un polinomio ciclotómico ternario $g_n(x)$ donde $n = pqr$ y p, q, r son primos impares tales que $p < q < r$. Posteriormente se presentarán familias de polinomios ciclotómicos ternarios planos, es decir, que $A(n) = 1$.

3.1. Una expresión de los coeficientes

Exponemos en primer lugar un importante resultado de Kaplan ([16]) que permite expresar los coeficientes c_k de $g_{pqr}(x)$ en función de los coeficientes a_i de $g_{pq}(x)$.

Teorema 3.1.1 *[16] Sean $p < q < r$ primos impares y $g_{pqr}(x)$, $g_{pq}(x)$ los correspondientes polinomios ciclotómicos:*

$$g_{pqr}(x) = \sum_{k=0}^{\varphi(pqr)} c_k x^k \qquad g_{pq}(x) = \sum_{i=0}^{\varphi(pq)} a_i x^i.$$

Sea $k \in \{0, \cdots, \varphi(pqr)\}$. Se define

$$a'_i = \begin{cases} a_i & ri \leq k \\ 0 & ri > k \end{cases}.$$

Finalmente, para cada $m \in \{0, \cdots, pq-1\}$ y cada $k \in \{0, \cdots, \varphi(pqr)\}$ se define $f_k(m)$ como el único valor $0 \leq f_k(m) < pq$ tal que $f_k(m) \equiv r^{-1}(k-m)$ mód pq. Bajo estas condiciones se tiene que

$$c_k = \sum_{m=0}^{p-1} a'_{f_k(m)} - \sum_{m=q}^{p+q-1} a'_{f_k(m)}.$$

Se probará primero un lema para aplicar al final de la demostración.

Lema 3.1.2 *Sean $p < q < r$ primos impares. Sean $m \in \{0, \cdots, pq-1\}$ y $f_k(m)$ como definido arriba. Entonces para todo $k \in \{0, \cdots, \varphi(pqr)\}$ se tiene que $rf_k(m) \leq k$ si y solo si $rf_k(m) + m \leq k$.*

Dem: Como $rf_k(m) \equiv k-m$ mód pq, existe $t \in \mathbb{Z}$ tal que $rf_k(m)+m-k = tpq$. Si $rf_k(m) - k \leq 0$, entonces $rf_k(m) + m - k = tpq \leq m$. Sin embargo, $m < pq$, luego $t \leq 0$. Esto significa que $rf_k(m) + m - k \leq 0$, es decir, $rf_k(m) + m \leq k$. La otra implicación es clara.

Demostración del Teorema 3.1.1: Notación: por simplicidad se escribirá $f(m)$ en vez de $f_k(m)$; k será el grado de un monomio de $g_{pqr}(x)$ y se considera fijado.

En primer lugar, aplicando la Proposición 1.1.12 d) se tiene que $g_{pqr}(x) = \frac{g_{pq}(x^r)}{g_{pq}(x)}$. A su vez, esto puede expresarse como

$$\frac{g_{pq}(x^r)}{g_{pq}(x)} = \frac{g_{pq}(x^r)g_1(x)g_p(x)g_q(x)}{x^{pq}-1} = -(1 + x^{pq} + \cdots)g_{pq}(x^r)g_1(x)g_p(x)g_q(x),$$

donde se ha utilizado la Proposición 1.1.7 y desarrollado $(x^{pq}-1)^{-1}$ en serie formal de potencias. Como $g_1(x)g_q(x) = x^q - 1$ y $g_p(x) = \sum_{i=0}^{p-1} x^i$, se obtiene que

$$(x-1)\sum_{i=0}^{p-1} x^i \sum_{i=0}^{q-1} x^i = (x^q-1)\sum_{i=0}^{p-1} x^i = -(1+x+\cdots-x^{p-1})+x^q+x^{q+1}+\cdots+x^{q+p-1}$$

Finalmente el pqr-ésimo polinomio ciclotómico queda expresado como

$$g_{pqr}(x) = (1 + x^{pq} + \cdots)(1 + x + \cdots + x^{p-1} - x^q - x^{q+1} - \cdots - x^{q+p-1})g_{pq}(x^r).$$

Se observa que el exponente k de los monomios x^k obtenidos al hacer el producto de los dos primeros factores de la igualdad anterior son todos de la forma $k = apq + m$ con $m \in \{0, \ldots, p-1\} \cup \{q, \ldots, q+p-1\}$ y $a \in \mathbb{N}$. Los correspondientes a los valores de $m \in \{0, \ldots, p-1\}$ llevan signo positivo y los correspondientes a los valores de $m \in \{q, \ldots, q+p-1\}$ llevan signo negativo. Si se define ahora,

$$\chi_m = \begin{cases} 1 & \text{cuando } m \in \{0, \ldots, p-1\} \\ -1 & \text{cuando } m \in \{q, \ldots, q+p-1\} \end{cases}$$

todos ellos son de la forma $\chi_m x^{apq+m}$. Por tanto, los exponentes de los monomios obtenidos al hacer el producto de la derecha en la igualdad anterior son de la forma $k = apq + m + rl$ con $a \in \mathbb{N}$, $m \in \{0, \ldots, p-1\} \cup \{q, \ldots, q+p-1\}$ y $l \in \{0, \ldots, \varphi(pq)\}$.

Esto último significa que $k \equiv m + rl$ mód pq y, con las restricciones sobre m y l, ha de ser $l = f(m)$. Además, si tenemos en cuenta la restricción $a \geq 0$, entonces $m + rf(m) \leq k$. Por el último lema, esto es equivalente a decir que $rf(m) \leq k$, y el término en el desarrollo de $g_{pqr}(x)$ es, para cada m y supuesto que $rf(m) \leq k$, $\chi_m a_{f(m)} x^{apq+m+rf(m)}$. Es decir, $\chi_m a'_{f(m)} x^{apq+m+rf(m)}$. Se concluye que recorriendo todos los valores de m obtenemos los términos que componen c_k, y por tanto:

$$c_k = \sum_{m=0}^{pq-1} \chi_m a'_{f(m)} = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)}.$$

Ejemplo 3.1.3

Para ilustrar el teorema de esta sección, se calcularán unos coeficientes del primer ciclotómico ternario. Recordamos que es el siguiente:

$$\begin{aligned} g_{3\cdot5\cdot7}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - \mathbf{2}x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} \\ & + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} \\ & + x^{14} + x^{13} + x^{12} - x^9 - x^8 - \mathbf{2}x^7 - x^6 - x^5 + x^2 + x + 1 \end{aligned}$$

Calcularemos c_7 y c_{41}, los dos términos de valor -2. Necesitamos para ello el decimoquinto polinomio ciclotómico, que es $g_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$. Por otra parte, para el cómputo de $f(m)$ hacemos notar que 7^{-1} mód $15 = 13$, puesto que $13 \cdot 7 = 91 = 15 \cdot 6 + 1$. Los sumatorios van de 0 a $p-1$ y de q a $q+p-1$, así que m está restringido al conjunto $\{0, 1, 2, 5, 6, 7\}$.

c_7 En primer lugar, observamos que $f(m) \equiv 13(7-m)$ mód $15 = -13m+13 \cdot 7$ mód $15 \equiv 2m+1$ mód 15, puesto que $2 \equiv -13$ mód 15. Por otra parte, $a'_{f(m)} = a_{f(m)}$ cuando $7f(m) \leq 7$, es decir, cuando $f(m) = 0$ o 1.

m	**0**	**1**	**2**	**5**	**6**	**7**
f(m)	1	3	5	11	13	0
$\mathbf{a'_{f(m)}}$	-1	0	0	0	0	1

Por tanto, $c_7 = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)} = -1 - 1 = -2$.

c_{41} Como $41 = 2 \cdot 15 + 11$ y $143 = 9 \cdot 15 + 8$, se tiene que $f(m) \equiv 13(11 - m)$ mód $15 \equiv 2m + 8$ mód 15. Además, $7f(m) \leq 41$ implica que $f(m)$ pertenece a $\{0, 1, 2, 3, 4, 5\}$.

m	**0**	**1**	**2**	**5**	**6**	**7**
f(m)	8	10	12	3	5	7
$\mathbf{a'_{f(m)}}$	0	0	0	1	1	0

Se obtiene que $c_{41} = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)} = 0 - (1 + 1) = -2$

3.2. Teoremas de periodicidad

Una vez se han determinado los coeficientes c_k el estudio se centrará en la función A(pqr). Los dos teoremas siguientes probarán que, fijados p y q, el valor de A(pqr) depende únicamente de r mód pq.

Teorema 3.2.1 *[16] Sean $p < q < r$ primos impares. Si $s > q$ es otro primo impar tal que $r \equiv s$* mód *pq, entonces* A(pqr) = A(pqs).

La demostración original expuesta aquí resulta bastante larga. Por comodidad para el lector, se dividirá en varias partes. En primer lugar, se probará que para cualquier coeficiente en $g_{pqr}(x)$, hay un término de igual valor en $g_{pqs}(x)$. Esto demuestra que A(pqr) $\leq$ A(pqs). Posteriormente, probaremos que para cualquier coeficiente de $g_{pqs}(x)$ o bien existe otro mayor o bien existe un término igual en $g_{pqr}(x)$, lo que prueba la desigualdad opuesta.

Sin pérdida de generalidad podemos suponer que $s > r$. Esto implica que $s > pq$, porque como $r \equiv s$ mód pq, entonces $s = apq + r$ para algún $a \in \mathbb{N}$. Entonces se tiene que $s > apq > pq$, como habíamos afirmado.

Proposición 3.2.2 *Sean $g_{pqr}(x) = \sum_{k=0}^{\varphi(pqr)} c_k x^k$ y $g_{pqs}(x) = \sum_{j=0}^{\varphi(pqs)} d_j x^j$. Entonces* A($pqr$) $\leq$ A(pqs).

Dem: Nuestro primer objetivo, como hemos comentado, es probar que dado c_{k_r} existe k_s con $c_{k_r} = d_{k_s}$. Basta buscarlo entre los que cumplen $k_s \equiv k_r$ mód pq.

Análogo al Teorema 3.1.1, fijado k_r se define $f(i) \in \{0, \cdots, pq-1\}$ de forma que $f(i) \equiv r^{-1}(k_r - i)$ mód pq. Como $k_r \equiv k_s$ mód pq y $r \equiv s$ mód pq, entonces $r^{-1}(k_r - i) \equiv s^{-1}(k_s - i)$ mód pq. También se define

$$a'_i = \begin{cases} a_i & \text{cuando } ri \leq k_r \\ 0 & \text{cuando } ri > k_r \end{cases} \qquad a^*_i = \begin{cases} a_i & \text{cuando } si \leq k_s \\ 0 & \text{cuando } si > k_s \end{cases},$$

y en virtud del mismo teorema tenemos que

$$c_{k_r} = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)} \qquad d_{k_s} = \sum_{m=0}^{p-1} a^*_{f(m)} - \sum_{m=q}^{q+p-1} a^*_{f(m)}.$$

Notamos que hemos podido escribir los términos de d_{k_s} utilizando los mismos $f(m)$ que en la expresión de c_{k_r} por la congruencia $r^{-1}(k_r - i) \equiv s^{-1}(k_s - i)$ mód pq. Las condiciones para definir a'_i y a^*_i pueden ser definidas como $i \leq \lfloor \frac{k_r}{r} \rfloor$ y $i \leq \lfloor \frac{k_s}{s} \rfloor$, respectivamente. Por tanto, si encontramos k_s tal que $\lfloor \frac{k_r}{r} \rfloor = \lfloor \frac{k_s}{s} \rfloor$, entonces $a'_i = a^*_i \ \forall i$, y por tanto $c_{k_r} = d_{k_s}$.

Aplicando el algoritmo de la división a k_r y r, se escribe $k_r = \lfloor \frac{k_r}{r} \rfloor r + n_0$ $(0 \leq n_0 < r)$. Podemos tomar $k_s = \lfloor \frac{k_r}{r} \rfloor s + n_0$. Se tiene entonces que $k_r \equiv k_s$ mód pq y $\lfloor \frac{k_s}{s} \rfloor = \lfloor \frac{k_r}{r} \rfloor + \lfloor \frac{n_0}{s} \rfloor = \lfloor \frac{k_r}{r} \rfloor$, porque $n_0 < r < s$. En consecuencia, para cada coeficiente de $g_{pqr}(x)$ existe un término en $g_{pqs}(x)$ cuyo coeficiente es del mismo valor, y $\mathrm{A}(pqr) \leq \mathrm{A}(pqs)$.

Esto completa la primera parte de la demostración. Para probar la otra desigualdad se hace necesario probar el siguiente lema. Volvemos a definir $\chi_m = 1$ si $m \in \{0, \cdots, p-1\}$, -1 si $m \in \{q, \cdots, q+p-1\}$ y 0 en otro caso. Entonces:

Lema 3.2.3 *Si $\chi_m a_{f(m)}$ y $\chi_{m+r} a_{f(m+r)}$ son ambos no nulos, entonces son iguales.*

Dem:

$$g_{pqr}(x) = (1 + x^{pq} + \cdots)(1 + x + \cdots + x^{p-1} - x^q - \cdots - x^{q+p-1}) g_{pq}(x^r)$$
$$g_{pqs}(x) = (1 + x^{pq} + \cdots)(1 + x + \cdots + x^{p-1} - x^q - \cdots - x^{q+p-1}) g_{pq}(x^s).$$

Si nos fijamos en $g_{pqs}(x)$, los términos no nulos del miembro de la derecha cuyo exponente es congruente con k_s mód pq tienen la forma $x^{apq} \chi_m x^m a_{f(m)} x^{sf(m)}$. Como $s > pq$ y $\chi_m \neq 0$, entonces ha de ser $m < s$ (en caso contrario, $m \geq s > pq > q + p - 1$ y $\chi_m = 0$). Esto indica que cada uno de estos términos tiene exponente distinto: de existir m_1, m_2 distintos con $m_1 + sf(m_1) = m_2 + sf(m_2)$, debe ser $f(m_1) - f(m_2) \neq 0$ y entonces $s = \frac{m_1 - m_2}{f(m_1) - f(m_2)}$, lo que no es posible porque $m_1, m_2 < s$.

Esta unicidad, sin embargo, no se da en el caso de $g_{pqr}(x)$: dado un término de exponente k_r, los términos de la derecha no nulos con exponente congruente con k_r mód pq son $\chi_m x^m a_{f(m)} x^{rf(m)}$. Esta vez, $r > q$, y como $\chi_m \neq 0$, entonces $m < 2r$: de ser $m \geq 2r$ se tendría $m \geq 2r > 2q > p + q - 1$ (porque $p < q < r$), luego $\chi_m = 0$. Como

$$f(m + r) \equiv r^{-1}(k_r - m - r) \equiv r^{-1}(k_r - m) - 1 \equiv f(m) - 1 \text{ mód } pq$$

entonces $f(m + r) = f(m) - 1$.

A continuación se observa que:

- El término $a_{f(m)}$ es no nulo, y de la relación $m + rf(m) = (m + r) + rf(m+r)$ se deduce que $a_{f(m+r)} = a_{f(m)-1}$ es también no nulo. Como los coeficientes no nulos de $g_{pq}(x)$ alternan entre 1 y -1, ha de ser $a_{f(m)} = -a_{f(m)-1}$.
- A su vez, si los términos χ_m y χ_{m+r} son también no nulos, como $r > q$, ha de ser $\chi_m = -\chi_{m+r}$.
- En conclusión, si $\chi_m a_{f(m)}$ y $\chi_{m+r} a_{f(m+r)}$ son no nulos, han de ser iguales.

Proposición 3.2.4 *Sean* $g_{pqr}(x) = \sum_{k=0}^{\varphi(pqr)} c_k x^k$ *y* $g_{pqs}(x) = \sum_{j=0}^{\varphi(pqs)} d_j x^j$. *Entonces* $\mathrm{A}(pqs) \leq \mathrm{A}(pqr)$.

Probaremos ahora que dado d_{k_s} un coeficiente de $g_{pqs}(x)$ se tiene que o bien existe un coeficiente c_{k_r} de $g_{pqr}(x)$ con $c_{k_r} = d_{k_s}$ o $\mathrm{A}(pqs) \neq d_{k_s}$. Supongamos que $d_{k_s} = \mathrm{A}(pqs)$ y que $\nexists c_{k_r} = d_{k_s}$. Se define J de tal manera que $f(J)$ es máximo con $\chi_J a^*_{f(J)} \neq 0$, y j de tal forma que $f(j)$ es mínimo, con $\chi_j a_j \neq 0$ y $a^*_{f(j)} = 0$. A continuación probaremos que $j + sf(j) > J + sf(J)$, desigualdad que usaremos más adelante. Es equivalente a decir que $s(f(j) - f(J)) > J - j$: como $a_{f(j)} \neq 0$ pero $a^*_{f(j)} = 0$, mientras que $a^*_{f(J)} \neq 0$, entonces $f(j) > f(J)$. Además, $s > pq$ y $j, J \leq q + p - 1$. Esto prueba la desigualdad.

Sin pérdida de generalidad, afirmamos que $k_s = J + sf(J)$: como $f(J) = \text{máx}\{f(x) : \chi_x a^*_{f(x)} \neq 0\}$, entonces $d_{k_s} = d_{J+f(J)}$. Probaremos ahora que:

- $d_{k_s - pq} = d_{k_s} - \chi_J a_{f(J)}$:
  Se recuerda que $d_{k_s-pq} = \sum_{m=0}^{p-1} a^*_{f(m)} - \sum_{m=q}^{q+p-1} a^*_{f(m)}$. Sin embargo, como $k_s - pq \equiv k_s$ mód pq, entonces $f(m)$ tiene el mismo valor calculando los coeficientes de d_{k_s} y los de d_{k_s-pq} (porque $r^{-1}(k_s - pq - m)$ mód $pq \equiv r^{-1}(k_s - m)$ mód pq). Por tanto, la única diferencia entre ambos coeficientes está en el valor $a^*_{f(m)}$. En este último caso, para un m cualquiera:

$$a^*_{f(m)} = \begin{cases} a_{f(m)} & \text{si } sf(m) \leq k_s - pq \\ 0 & \text{si } sf(m) > k_s - pq \end{cases}$$
$$= \begin{cases} a_{f(m)} & \text{si } sf(m) + pq \leq sf(J) + J \\ 0 & \text{si } sf(m) + pq > sf(J) + J \end{cases}.$$

Por una parte, se tiene que $pq > J$, lo que implica que $a^*_{f(J)} = 0$. Por otra parte, para cualquier $f(x) < f(J)$, se tiene que $sf(x) + pq \leq sf(J) + J$, como veremos inmediatamente: sea $f(x) = f(J) - a$, con $a \geq 1$: $s(f(J) - a) + pq \leq sf(J) + J \Leftrightarrow -sa + pq \leq J$, que se cumple porque $s > pq$.
Esto implica que el único término que se queda fuera del cómputo de $d_{k_s - pq}$ es $\chi_J a_{f(J)}$, y por eso $d_{k_s - pq} = d_{k_s} - \chi_J a_{f(J)}$.

- $d_{j+sf(j)} = d_{k_s} + \chi_j a_{f(j)}$:
De nuevo, como $j + sf(j) \equiv k_s$ mód pq, los valores de $f(m)$ coinciden al calcular los coeficientes de $d_{j+sf(j)}$ y los de d_{k_s}. Se tiene ahora que

$$a^*_{f(m)} = \begin{cases} a_{f(m)} & \text{si } sf(m) \leq j + sf(j) \\ 0 & \text{si } sf(m) > j + sf(j) \end{cases}.$$

En primer lugar, $sf(j) \leq j + sf(j)$, así que el término $\chi_j a_{f(j)}$ se encuentra ahora dentro del cómputo. Salvo este término no hay ningún otro que se haya tenido en cuenta en d_{k_s} y no esté aquí, porque: (1) vemos que $a^*_{f(J)} = a_{f(J)}$ al ser $sf(J) < j + sf(j)$, (2) como $j + sf(j) > J + sf(J)$ y $f(J)$ es máximo con $\chi_j a^*_{f(j)} \neq 0$, $\forall f(x) > f(J)$, $\chi_x a^*_{f(x)} = 0$ y (3) $f(j) = \text{mín}\{f(x) : \chi_x a_x \neq 0, a^*_{f(x)} = 0\}$ y si $f(x) < f(j)$, entonces $\chi_x a_x = 0$. Esto prueba que $d_{j+sf(j)} = d_{k_s} + \chi_j a_{f(j)}$.

- Acabamos de probar que $d_{k_s - pq} = d_{k_s} - \chi_J a_{f(J)}$, $d_{j+sf(j)} = d_{k_s} + \chi_j a_{f(j)}$. Además, $\chi_J a_{f(J)}$ y $\chi_j a_{f(j)}$ son ambos no nulos. Como $d_{k_s} = \text{A}(pqs)$, entonces $\chi_J a_{f(J)} = -\chi_j a_{f(j)} =:$ de otro modo, de ser iguales, o bien $d_{k_s - pq}$ o bien $d_{j+sf(j)}$ serían mayores en valor absoluto que d_{k_s}.

En las siguientes líneas probaremos que $j + r + rf(j + r) = J + rf(J)$. Por el Lema 3.2.3, esto significa que $\chi_j a_{f(j)} = \chi_J a_{f(J)}$, en contradicción con lo que acabamos de demostrar.

Recordemos que habíamos supuesto que no existe ningún coeficiente de $g_{pqr}(x)$ igual a d_{k_s}. Tomamos ahora $k_r = J + rf(J)$ (por hipótesis, $c_{k_r} \neq d_{k_s}$). Como $rf(J) \leq k_r$, entonces $\forall f(i) \leq f(J)$ con $a^*_{f(i)} \neq 0$, se tiene $a'_{f(i)} \neq 0$. Además, $f(j) = \text{mín}\{f(x) : \chi_x a_{f(x)} \neq 0 \text{ y } a^*_{f(x)} = 0\}$, luego ha de ser $a'_{f(j)} \neq 0$: en caso contrario, si k es tal que $f(J) < f(k) < f(j)$ se tiene que $\chi_k a_{f(k)} = 0$ y si $f(k) > f(j)$, entonces $a'_{f(k)} = 0$ porque $rf(k) > rf(j) > J + rf(J)$ (esta última desigualdad viene precisamente de suponer que $a'_{f(j)} = 0$). Esto implicaría que $c_{k_r} = d_{k_s}$, en contra de lo supuesto.

Como $a'_{f(j)} \neq 0$, entonces $rf(j) \leq J + rf(J)$, que en virtud del Lema 3.1.2 es equivalente a decir que $j + rf(j) \leq J + rf(J)$. Podemos afirmar que

$$0 < r(f(j) - f(J)) \leq J - j \leq q + p - 1 < 2r.$$

Se observa ahora lo siguiente:

- $r(f(j) - f(J)) < 2r \Rightarrow 0 < f(j) - f(J) < 2 \Rightarrow f(j) - f(J) = 1$.

- $$\begin{aligned} f(j) - f(J) = 1 &\Longrightarrow r^{-1}(k_r - j) \equiv 1 + r^{-1}(k_r - J) \text{ mód } pq \\ &\Longrightarrow k_r - j \equiv r + k_r - J \text{ mód } pq \\ &\Longrightarrow J - j \equiv r \text{ mód } pq \end{aligned}$$

  Entonces $J - j = apq + r$ para algún $a \in \mathbb{Z}$. Como $r \leq J - j = apq + r$ ha de ser $a \geq 0$. Sin embargo, $J - j \leq q + p - 1$, lo que implica que $a = 0$ y $J - j = r$.

- Con anterioridad se probó que $f(x + r) = f(x) - 1$. Entonces

  $$j + f(j)r = (j + r) + f(j + r)r = J + f(J)r,$$

  y en virtud del Lema 3.2.3 $\chi_j a_{f(j)} = \chi_{j+r} a_{f(j+r)} = \chi_J a_{f(J)}$. Como ya se ha indicado, esto es una contradicción. Por tanto, o bien existe k_r con $c_{k_r} = d_{k_s}$ o bien $\mathrm{A}(pqs) \neq d_{k_s}$. Esto prueba que $\mathrm{A}(pqs) \leq \mathrm{A}(pqr)$.

Este último teorema no solamente da una condición suficiente para que $\mathrm{A}(pqr) = \mathrm{A}(pqs)$. También implica que si fijamos p y q, para conocer el rango de $\mathrm{A}(pqr)$ nos basta estudiar tantos casos como valores distintos de r mód pq existan, que son $(p-1)(q-1)$: como $(pq, r) = 1$, entonces $(r \text{ mód } pq, pq) = 1$, y existen $\varphi(pq) = (p-1)(q-1)$ valores que cumplan esa condición.

Teorema 3.2.5 *[16] Sean $p < q < r, s$ primos impares. Si $r \equiv -s$ mód pq, entonces $\mathrm{A}(pqr) = \mathrm{A}(pqs)$.*

Dem: En primer lugar se recuerda el Teorema de Dirichlet sobre Primos en Progresiones Aritméticas: se pueden encontrar infinitos primos en la progresión $a_n = a + bn$ si $(a, b) = 1$. Por tanto, se pueden encontrar primos de la forma $r' = r + t_1 pq$ y $s' = s + t_2 pq$ para $t_1, t_2 \in \mathbb{N}$, y en virtud del teorema anterior $\mathrm{A}(pqr') = \mathrm{A}(pqr)$ y $\mathrm{A}(pqs') = \mathrm{A}(pqs)$. Por tanto, sin pérdida de generalidad se puede suponer que r y s son mayores que pq.

Sea c_{k_r} un coeficiente de $g_{pqr}(x)$. Queremos encontrar d_{k_s} coeficiente de $g_{pqs}(x)$ con $d_{k_s} = -c_{k_r}$: esto implicaría que $\mathrm{A}(pqs) \leq A(pqr)$ y, por simetría sobre r y s, se podría concluir que $\mathrm{A}(pqr) = \mathrm{A}(pqs)$. Como antes, se define $f(i)$ como el único entero en $\{0, \cdots, pq - 1\}$ que cumple $f(i) \equiv r^{-1}(k_r - i)$ mód pq. De manera análoga, se define $F(i) \equiv s^{-1}(k_s - i)$. En virtud del Teorema 3.1.1:

$$c_{k_r} = \sum_{m=0}^{p-1} a'_{f(m)} - \sum_{m=q}^{q+p-1} a'_{f(m)} \qquad d_{k_s} = \sum_{m=0}^{p-1} a^*_{F(m)} - \sum_{m=q}^{q+p-1} a^*_{F(m)},$$

donde

$$a'_{f(m)} = \begin{cases} a_{f(m)} & \text{si } rf(m) \leq k_r \\ 0 & \text{si } rf(m) > k_r \end{cases} \qquad a^*_{F(m)} = \begin{cases} a_{F(m)} & \text{si } sF(m) \leq k_s \\ 0 & \text{si } sF(m) > k_s \end{cases}.$$

Podemos suponer que $k_s \equiv q+p-1-k_r$ mód pq. Esto implica que $F(i) \equiv s^{-1}(k_s - i)$ mód $pq \equiv -r^{-1}(q+p-1-k_r-i)$ mód $pq \equiv s^{-1}(k_r-(q+p-1-i))$ mód $pq = f(q+p-1-i)$ mód pq, y por tanto $F(i) = f(q+p-1-i)$. Como $F(0) = f(q+p-1)$, $F(1) = f(q+p-2), \cdots, F(q+p-1) = f(0)$, los índices en las sumas de d_{k_s} se están recorriendo en sentido inverso. Esto significa que

$$d_{k_s} = \sum_{m=0}^{p-1} a^*_{F(m)} - \sum_{m=q}^{q+p-1} a^*_{F(m)} = \sum_{m=0}^{p-1} a^*_{f(q+p-1-m)} - \sum_{m=q}^{q+p-1} a^*_{f(q+p-1-m)}$$
$$= \sum_{m=q}^{q+p-1} a^*_{f(m)} - \sum_{m=0}^{p-1} a^*_{f(m)} = -\left(\sum_{m=0}^{p-1} a^*_{f(m)} - \sum_{m=q}^{q+p-1} a^*_{f(m)}\right)$$

Atendiendo a las condiciones que definen $a'_{f(m)}$ y $a^*_{f(m)}$, si encontramos k_s con $\lfloor \frac{k_s}{s} \rfloor = \lfloor \frac{k_r}{r} \rfloor$, entonces $a'_{f(m)} = a^*_{f(m)} \forall m$ y $d_{k_s} = -c_{k_r}$. Sea $k_r = \lfloor \frac{k_r}{r} \rfloor r + k_0 (0 \leq k_0 \leq r-1)$ y k_1 el único valor en $\{0, \cdots, pq-1\}$ que cumple que $k_1 \equiv q+p-1-k_0$ mód pq. Tomemos $k_s = \lfloor \frac{k_r}{r} \rfloor s + k_1$. Hay que comprobar que $k_s \equiv q+p-1-k_r$ mód pq, que ha sido una suposición necesaria, y que $\lfloor \frac{k_s}{s} \rfloor = \lfloor \frac{k_r}{r} \rfloor$.

- $k_s \equiv \lfloor \frac{k_r}{r} \rfloor s + k_1$ mód $pq \equiv -\lfloor \frac{k_r}{r} \rfloor r + q + p - 1 - k_0$ mód $pq \equiv q+p-1-\left(\lfloor \frac{k_r}{r} \rfloor r + k_0\right)$ mód $pq \equiv q+p-1-k_r$ mód pq
- $\frac{k_s}{s} = \lfloor \frac{k_r}{r} \rfloor + k_1$, y se tiene que

$$\left\lfloor \frac{k_s}{s} \right\rfloor = \left\lfloor \frac{k_r}{r} \right\rfloor + \left\lfloor \frac{k_1}{s} \right\rfloor = \left\lfloor \frac{k_r}{r} \right\rfloor \qquad \left(k_1 < pq < s \Rightarrow \left\lfloor \frac{k_1}{s} \right\rfloor = 0\right)$$

Por tanto, $a'_{f(m)} = a^*_{f(m)} \forall m$ y $c_{k_r} = -d_{k_s}$. Se tiene que $\mathrm{A}(pqr) \leq \mathrm{A}(pqs)$. Este razonamiento puede repetirse análogamente tomando un coeficiente de $g_{pqs}(x)$ y buscando uno opuesto en $g_{pqr}(x)$, y se llegaría a que $\mathrm{A}(pqs) \leq \mathrm{A}(pqr)$, lo que termina la demostración.

Al igual que el Teorema 3.2.1, este resultado nos ayuda a acotar el número de valores de r que tenemos que estudiar para conocer el rango de $\mathrm{A}(pqr)$, fijados p y q. Podemos concluir que tenemos que estudiar la mitad de casos, dado que ahora al estudiar $\mathrm{A}(pqr)$ con $r \equiv k$ mód pq también conocemos $\mathrm{A}(pqs)$, donde $s \equiv -k$ mód pq. Acabamos de probar que:

Corolario 3.2.6 *Sean p, q primos impares. Para conocer el rango de $\mathrm{A}(pqr)$, solamente hay que comprobar $\frac{(p-1)(q-1)}{2}$ valores distintos de r.*

3.3. Polinomios ternarios planos

Como se ha visto en el ejemplo el primer polinomio ternario tiene altura 2. Sin embargo, también existen polinomios planos ternarios de este tipo. Por

ejemplo:

$$\begin{aligned} g_{231}(x) = {} & x^{120} + x^{119} - x^{113} - x^{112} - x^{111} - x^{109} - x^{108} - x^{107} + x^{102} + x^{101} \\ & + x^{100} + x^{99} + x^{98} + x^{97} - x^{92} - x^{91} - x^{90} - x^{88} + x^{85} + x^{81} + x^{77} \\ & - x^{75} - x^{74} - x^{71} - x^{70} + x^{68} + x^{64} + x^{60} + x^{56} + x^{52} - x^{50} - x^{49} \\ & - x^{46} - x^{45} + x^{43} + x^{39} + x^{35} - x^{32} - x^{30} - x^{29} - x^{28} + x^{23} + x^{22} \\ & + x^{21} + x^{20} + x^{19} + x^{18} - x^{13} - x^{12} - x^{11} - x^{9} - x^{8} - x^{7} + x^{2} + x \\ & + 1 \end{aligned}$$

Como $231 = 3 \cdot 7 \cdot 11$, los teoremas de periodicidad nos proporcionan una familia infinita de polinomios ciclotómicos planos: $g_{21 \cdot r}$, donde $r \equiv \pm 11$ mód 21. Esta manera de construir familias necesita encontrar primero un polinomio plano. El siguiente resultado proporciona una herramienta más general:

Teorema 3.3.1 *[16] Sean $p < q$ primos, y $r \equiv \pm 1$ mód pq primo. Entonces $g_{pqr}(x)$ es plano.*

Lema 3.3.2 *Si $r \equiv \pm 1$ mód pq y $g_{pqr}(x) = \sum_{k=0}^{\varphi(pqr)} c_k x^k$, para todo k se tiene que $\sum_{j=0}^{p-1} a_{f(j)} = \sum_{j=q}^{q+p-1} a_{f(j)}$.*

Dem: Como $r \equiv 1$ mód pq, tenemos que $f(m) \equiv k - m$ mód pq, así que $f(m) = apq + (k - m)$ para algún entero a. Como se verá al final de la prueba no se pierde generalidad si se supone que $a = 0$ tomando $k + apq$ en vez de k.

Si $f(m) = k - m$, se tiene que:

$$\sum_{m=0}^{p-1} a_{f(m)} = \sum_{m=0}^{p-1} a_{k-m} \qquad \sum_{m=q}^{q+p-1} a_{f(m)} = \sum_{m=q}^{q+p-1} a_{k-m}$$

Podemos observar que cada una de estas sumas se corresponde con un coeficiente de $g_{pq}(x)g_p(x)$: en efecto, $\sum_{m=0}^{p-1} a_{k-m}$ es el coeficiente del monomio de grado k de $g_{pq}(x)g_p(x) = (1 + x + \cdots + x^{p-1}) \sum_{i=0}^{\varphi(pq)} a_i x^i$. Por el mismo motivo, $\sum_{m=q}^{q+p-1} a_{k-m}$ es el coeficiente $k - q$ del mismo polinomio. Por el apartado d) de la Proposición 1.1.12, $g_{pq}(x)g_p(x) = g_p(x^q) = 1 + x^q + \cdots + x^{(p-1)q}$.

Es claro que cada uno de los coeficientes del polinomio anterior son iguales cuando los exponentes son congruentes módulo q, como es el caso de k y $k - q$. Por tanto, $\sum_{m=0}^{p-1} a_{k-m} = \sum_{m=q}^{q+p-1} a_{k-m}$ y $\sum_{j=0}^{p-1} a_{f(j)} = \sum_{j=q}^{q+p-1} a_{f(j)}$.

Dem: En primer lugar, demostraremos que cuando $r \equiv 1$ mód pq, entonces $g_{pqr}(x)$ es plano. Después, por el Teorema 3.2.5 quedará demostrado que $g_{pqr}(x)$ es plano en el caso $r \equiv -1$ mód pq. Sea k un exponente en el desarrollo de g_{pqr} y c_k el correspondiente coeficiente. Como $r \equiv 1$ mód pq, entonces $r^{-1} \equiv 1$ mód pq y $f(m) \equiv k - m$ mód pq. Sean

$$S = \sum_{m=0}^{p-1} a'_{f(m)} \qquad T = \sum_{m=q}^{q+p-1} a'_{f(m)}$$

Por el Teorema 3.1.1, se tiene que $c_k = S - T$. A continuación, probaremos que $|S|$, $|T| \leq 1$:

Sea $i = \text{máx}\{m \in [0, p-1], a'_{f(m)} \neq 0\}$ (si $a'_{f(m)} = 0$ para $0 \leq m \leq p-1$, entonces $S = 0$). Por una parte, esto implica que $f(i) \leq \varphi(pq)$ y $rf(i) \leq k$. Es fácil ver que $f(i-1) = f(i) + 1$: $f(i-1) \equiv k - i + 1 \text{ mód } pq \equiv f(i) + 1 \text{ mód } pq$ y $f(i) + 1 \leq (p-1)(q-1) + 1 < pq$, luego la congruencia es una igualdad. De forma general, los elementos de la sucesión $f(i)$, $f(i-1), \cdots, f(0)$ son también consecutivos: para todo $j \in [0, i]$ se tiene que $f(i-j) \equiv f(i) + j \text{ mód } pq$, y como $f(i) + j \leq (p-1)(q-1) + (p-1) < pq$, entonces $f(i-j) = f(i) + j$. Además, como esta sucesión es creciente, si para algún elemento $f(M)$ se tiene que $rf(M) > k$, entonces la desigualdad también se cumple para todos los que le siguen, y $a'_{f(m)} = 0$ para todo $m \leq M$. Por tanto, S consiste en una suma de elementos correlativos de $g_{pq}(x)$, y como los coeficientes no nulos alternan entre ± 1, entonces $|S| \leq 1$. De manera análoga puede razonarse para $|T|$.

Naturalmente, si $T = 0$, entonces es claro que $|c_k| \leq 1$ porque $|S| \leq 1$. Vamos a ver qué ocurre si $T = 1$ (el caso $T = -1$ es análogo, como se podrá observar). Se distinguen dos casos:

- Existe $m \in [q, q + p - 1]$ con $a_{f(m)} \neq 0$ pero $a'_{f(m)} = 0$. Esto quiere decir que $rf(m) > k$. En estas condiciones, se tiene que $S = 0$ y, por tanto, $c_k = 1$. Procedemos a probar esto último:

  Afirmamos que no se puede dar a la vez que $f(m) = (p-1)(q-1)$ y $m = q + p - 1$. Si esto ocurriera, para cualquier $j \in [q, q + p - 1]$ se tendría que

  $$f(j) \equiv (k - m) + (m - j) \text{ mód } pq \equiv f(m) + (q + p - 1 - j) \text{ mód } pq.$$

  Además, $f(m) + (p + q - 1 - j) \leq (p-1)(q-1) + (p + q - 1 - j) = pq - j < pq$, luego la congruencia sería una igualdad y $f(j) = f(m) + q + p - 1 - j$. Como $rf(m) > k$ y $f(j) > f(m)$ para todo $j \in [q, q + p - 1]$, $a'_{f(j)} = 0$ y $T = 0$, en contradicción con $T = 1$. Por tanto, no se tiene a la vez que $f(m) = (p-1)(q-1)$ y $m = q + p - 1$. Esto quiere decir que $m + f(m) < (p-1)(q-1) + q + p - 1 = pq$.

  Sea ahora $j \in [0, p-1]$. Haciendo una manipulación similar a la anterior congruencia, $f(j) \equiv f(m) + (m - j) \text{ mód } pq$, y dado que $f(m) + (m - j) \leq f(m) + m < pq$, entonces $f(j) = f(m) + m - j > f(m)$. Por tanto, $rf(j) > k$, y $a'_{f(j)} = 0$ para todo $j \in [0, p-1]$. Por tanto, $S = 0$ y $c_k = S - T = -1$.

- Para todo $m \in [q, q+p-1]$, $a'_{f(m)} = a_{f(m)}$. Entonces $T = \sum_{m=q}^{q+p-1} a_{f(m)} = 1$, y por el lema probado, $\sum_{m=0}^{p-1} a_{f(m)} = 1$. Como los elementos correlativos no nulos de este sumatorio toman alternativamente valores 1 y -1, si $f(j)$ y $f(J)$ son el menor y mayor valor respectivamente de $\{f(m) : 0 \leq m \leq p-1\}$, ha de ser $a_{f(j)} = a_{f(J)} = 1$. Pasando a S, esto implica que $S = 0$ o $S = 1$. En el primer caso, se tiene que $c_k = S - T = -1$, mientras que si $S = 1$, entonces $c_k = 0$.

Esta condición supone una mejora muy fuerte respecto del anterior intento, que se puede encontrar en [3], y construye una familia infinita de polinomios ciclotómicos planos con las siguientes condiciones:

$$p \geq 5 \qquad q \equiv -1 \text{ mód } p \qquad r \equiv 1 \text{ mód } pq$$

Sin embargo, este resultado no acaba de caracterizar completamente los polinomios ternarios planos, como se puede observar con $g_{231}(x)$. En [17] se expone una conjetura, citada de otra fuente, que pretende avanzar en este problema:

Definición 3.3.3 *Para cada terna de primos impares $p < q < r$ se define ω como el único entero en $\{1, \cdots, \frac{pq-1}{2}\}$ de forma que $r \equiv \pm\omega$ mód pq. Se dice que:*

- *(p, q, r) es de Tipo 1 si $\omega = 1$.*
- *(p, q, r) es de Tipo 2 si $\omega > 1$, $q \equiv 1$ mód $p\omega$ y $p \equiv 1$ mód w.*
- *(p, q, r) es de Tipo 3 si $\omega > p$, $q > p(p-1)$, $q \equiv \pm 1$ mód p y $\omega \equiv \pm 1$ mód p.*

Conjetura 3.3.4

- *Si (p, q, r) es de Tipo 1 o 2, $g_{pqr}(x)$ es plano.*
- *Si (p, q, r) no es de ninguno de esos tipos, entonces $g_{pqr}(x)$ no es plano.*
- *Si (p, q, r) es de Tipo 3, entonces $\mathrm{A}(pqr) = 1$ si y solamente si $\frac{g_{pq}(x^s)}{g_{pq}(x)}$ es plano, donde s es el menor entero positivo con $s \equiv 1$ mód p y $s \equiv \pm r$ mód pq.*

Desafortunadamente, la fuente original de la definición y conjetura anteriores no está disponible, y por tanto no es fácil suponer cuál es la idea detrás de esto, sobre todo con las pocas herramientas disponibles en el estudio de los coeficientes de estos polinomios. Sin embargo, la mitad de la primera parte de la conjetura ya la hemos probado en el Teorema 3.3.1. Por otra parte, en una complicada prueba en [9] (Teorema 42) se expone la prueba a la otra mitad: si (p, q, r) es de Tipo 2, entonces $g_{pqr}(x)$ es plano. Hasta donde el autor sabe, estos son los únicos avances relacionados con estas conjeturas. Existen otros resultados sobre polinomios terciarios planos que van en una dirección distinta. Se pueden nombrar los siguientes:

- Si $2r \equiv \pm 1$ mód pq, $g_{pqr}(x)$ es plano si y solo si $p = 3$ y $q \equiv 1$ mód p. ([13], 2010)
- Si $q \equiv \pm 1$ mód pq y $4r \equiv \pm 1$ mód pq, $g_{pqr}(x)$ es plano si y solo si (1) $p = 3$, $q > 7$ y $q \equiv -1$ mód 3 o mód2m o (2) $p = 5$, $q > 11$ y $q \equiv 1$ mód 5. ([28], 2015)
- Si $3r \equiv \pm 1$ mód pq, entonces $g_{pqr}(x)$ **no** es plano. ([29], 2017)
- Si $5r \equiv \pm 1$ mód pq, $g_{pqr}(x)$ es plano si y solo si $p = 3$, $q \geq 13$ y $q \equiv 1$ mód 3. ([29], 2017)

Capítulo 4

Sobre la magnitud de los coeficientes

En el capítulo anterior se probó que existen polinomios ciclotómicos de orden 3 con altura mayor que 1, y los teoremas de periodicidad proporcionaron herramientas para construir familias infinitas de polinomios ternarios de una altura determinada, supuesto que ya tengamos un polinomio de esa altura. El estudio hecho anteriormente culminará con el siguiente resultado: la altura de los polinomios ciclotómicos ternarios no está acotada. La riqueza de este caso nos hace preguntarnos sobre la variedad y complejidad de polinomios ciclotómicos de órdenes superiores. A día de hoy solamente se conocen resultados parciales sobre los polinomios de orden 4, y muy poco sobre otros órdenes. Por tanto, aprovecharemos también para exponer algunas conjeturas y problemas abiertos.

4.1. Teorema de Schur

Uno de los resultados más clásicos es el Teorema de Schur, que prueba que la altura de los polinomios ciclotómicos no está acotada. Este resultado fue probado por Issai Schur en una carta dirigida a Edmund Landau en 1931, aunque está publicado por Emma Lehmer en 1936 ([19]).

Teorema 4.1.1 *[19] Existen polinomios ciclotómicos con coeficientes arbitrariamente grandes en valor absoluto.*

La idea consiste en tomar un entero t impar y buscar una cadena de primos $p_1 < \cdots < p_t$ con $p_1 + p_2 > p_t$. Entonces, si $n = p_1 \cdots p_t$, el coeficiente p_t de $g_n(x)$ es $1 - t$. Esto prueba el resultado. Sin embargo, para completar la demostración se hace necesario probar que, para cualquier t, pueden encontrarse secuencias de t primos con las condiciones anteriores.

Proposición 4.1.2 *[26] Para todo $t > 2$ existen primos $p_1 < \cdots < p_t$ con $p_1 + p_2 > p_t$.*

Dem: Supongamos que existe $t \geq 3$ tal que para toda cadena de primos $p_1 < \cdots < p_t$ se tiene que $p_1 + p_2 \leq p_t$. Esto implica que $2p_1 < p_t$. Entonces para todo $k \geq 1$ el número de primos p tales que $2^{k-1} < p < 2^k$ es menor que t. Finalmente, si $\pi(x)$ es la función que cuenta todos los primos menores o iguales que x, por las razones anteriores se concluye que $\pi(2^k) < kt$, porque, cuando $1 \leq i \leq k$, hay k conjuntos de la forma $[2^{i-1}, 2^i] \cap \mathbb{N}$ y en cada uno de ellos hay menos de t primos.

La condición $\pi(2^k) < kt$ va en contra del Teorema del Número Primo, demostrado por Hadamard y de la Vallée Poussin en 1896 de forma independiente, que asegura que

$$\pi(x) \sim \frac{x}{\log(x)},$$

donde log representa el logaritmo neperiano. Para valores de k suficientemente grandes, se tiene que $\pi(2^k) \sim \frac{2^k}{\log(2^k)} = \frac{2^k}{k\log(2)}$, que es considerablemente mayor que kt. Por tanto, deben existir primos $p_1 < \cdots < p_t$ con $p_1 + p_2 > p_t$.

Ahora estamos en condiciones de proporcionar una prueba completa del teorema:

Demostración del Teorema de Schur:

Sean $t > 1$ impar, $p_1 < p_2 < \ldots < p_t$ una cadena de primos tales que $p_1 + p_2 < p_t$ y n el producto de todos ellos. Aplicando la Fórmula de Inversión de Möbius (1.2.5) se obtiene que $g_n(x) = \prod_{d|n}(x^d - 1)^{\mu\left(\frac{n}{d}\right)}$, donde se recuerda que $\mu(m) = 1$ si m es producto de un número par de primos y libre de cuadrados, -1 si es producto de un número impar de primos y libre de cuadrados y 0 en otro caso.

Como n es libre de cuadrados, para cada divisor d de n es $\mu(d) = \pm 1$ y además, por ser t impar, los divisores de n se pueden agrupar en parejas $(d, \frac{n}{d})$ con $\mu(d) = 1$ y $\mu(\frac{n}{d}) = -1$. Entonces

$$g_n(x) = \prod_{\mu\left(\frac{n}{d}\right)=1} (x^d - 1) \prod_{\mu\left(\frac{n}{d}\right)=-1} \frac{1}{x^{\frac{n}{d}} - 1} = \prod_{\mu(\frac{n}{d})=1} \left[(x^d - 1)\frac{1}{x^{\frac{n}{d}} - 1}\right] =$$

$$= \prod_{\mu(\frac{n}{d})=1} \left[(1 - x^d)\frac{1}{1 - x^{\frac{n}{d}}}\right] = \prod_{\mu(\frac{n}{d})=1} \left[(1 - x^d)(1 + x^{\frac{n}{d}} + \cdots)\right] =$$

La genial idea de Schur consiste en reducir $g_n(x)$ módulo x^{p_t+1}. Por una parte, se hace notar que para $d = p_i$, $\mu\left(\frac{n}{d}\right) = 1$ y $\mu(n) = -1$, porque t es impar. Por otra parte, como $p_1 + p_2 > p_t$, los únicos divisores de n menores que $p_t + 1$ son $1, p_1, \cdots, p_t$. Por todo lo anterior, esta congruencia es de la forma:

$$g_n(x) \equiv (1 + x + \cdots + x^{p_t}) \prod_{i=1}^{t} (1 - x^{p_i}) \text{ mód } x^{p_t+1}$$

Además, al multiplicar dos polinomios de la forma $(1 - x^{p_i})(1 - x^{p_j})$ se obtiene $1 - x^{p_i} - x^{p_j}$ tras reducir. Siguiendo este razonamiento, es claro ahora ver que

$$g_n(x) \equiv (1 - x^{p_1} - \cdots - x^{p_t})(1 + x + \cdots + x^{p_t}) \text{ mód } x^{p_t+1}$$

De esta manera, se comprueba que el coeficiente de x^{p_t} es $1 - t$: en efecto, si $p_0 := 1$, el número de términos que contribuyen a este monomio se corresponden con las soluciones de la ecuación $p_i + x = p_t$, donde $0 \leq x \leq p_t$, y $0 \leq i \leq t$. Existen $t + 1$ soluciones de la anterior ecuación, donde solo una de ellas contribuye al monomio con $+1$, mientras que el resto de los términos son -1. Queda probado que $A(n) \geq t - 1$, y por tanto existen polinomios ciclotómicos con altura arbitrariamente grande.

La demostración original de Schur termina en las líneas anteriores. Sin embargo, siguiendo un razonamiento similar al anterior, se comprueba que el coeficiente de x^{p_t-2} es $2 - t$: los términos involucrados son $1 \cdot x^{p_t-2}, -x^{p_1} \cdot x^{p_t-2-p_1}, \cdots, -x^{p_{t-1}} \cdot x^{p_t-2-p_{t-1}}$. Por tanto, todo entero negativo es coeficiente de algún polinomio ciclotómico, dado que $1 - t$ y $2 - t$ recorren tal conjunto si $t \geq 3$. Por la Proposición 1.1.12 c), se tiene que $g_{2m}(x) = g_m(-x)$ cuando m es impar. Como t y $t - 2$ también son impares, entonces los coeficientes acompañando a monomios de esos grados en $g_{2n}(x)$ son $t-1$ y $t-2$, respectivamente. Finalmente, es claro que 0 es coeficiente de algún polinomio ciclotómico. Acabamos de probar que:

Teorema 4.1.3 *[26] Todo número entero es coeficiente de algún polinomio ciclotómico.*

Si $a(n, k)$ es el k-ésimo coeficiente de $g_n(x)$, hemos probado que $\{a(n, k) : n \geq 1, k \geq 0\} = \mathbb{Z}$. Esta mejora de la demostración original data de 1987 y se debe a Jiro Suzuki. Desde entonces, las condiciones para obtener todos los enteros como coeficientes en algún polinomio ciclotómico se han hecho más sencillas. Cabe destacar los siguientes avances:

- En 2007, se prueba que, fijado un primo p p y un exponente e, $\{a(p^e n, k) : n \geq 1, k \geq 0\} = \mathbb{Z}$. La demostración, que se puede encontrar en [14], es muy similar a la del Teorema de Schur.
- Al año siguiente se prueba que $\{a(mn, k) : n \geq 1, k \geq 0\} = \mathbb{Z}$ para cualquier entero positivo m. Los detalles se pueden encontrar en [15].
- En 2011 se prueba el siguiente resultado, donde (x, y) denota el máximo común divisor en $\mathbb{Z}$ de los enteros x e y:

Teorema 4.1.4 *[10] Para cada n, se define $S(n) = \frac{n}{\prod_{p|n} p}$. Se fijan a, b, d y f, cuatro enteros positivos con las condiciones $a < d$ y $b < f$. Se tiene que*

$$\{a(n, k) : n \equiv a \text{ mód } d, k \equiv b \text{ mód } f, n \geq 1, k \geq 0\} = \begin{cases} \mathbb{Z} & \text{si } (S((a, d)), f)|b \\ \{0\} & \text{en otro caso} \end{cases}$$

Una vez queda probado que, en efecto, la altura de los polinomios ciclotómicos no está acotada, se plantea como interés acotar $\mathrm{A}(n)$ en casos particulares. En [16] se exponen algunas cotas. Si n es libre de cuadrados y de orden k, es decir, tiene k primos impares en su factorización, entonces:

$$A(n) \leq n^{2^{k-1}} \qquad \mathrm{A}(n) \leq n^{\frac{2^{k-1}}{k}-1}$$

La primera data de 1949, mientras que la segunda, significativamente mejor, de 1984, y están probadas con técnicas analíticas. Aunque puedan parecer cotas demasiado amplias, sobre todo con los ejemplos que hemos visto hasta ahora, lo cierto es que $\mathrm{A}(n)$ crece muy rápido. Por ejemplo, según cita [7], si tomamos n como el producto de los 9 primeros primos impares, obtenemos que:

$$\mathrm{A}(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29) = 2888582082500892851$$

Además, este comportamiento es impredecible. Si consideramos otro producto de 9 primos impares distintos, el resultado es muy distinto:

$$\mathrm{A}(3{\cdot}5{\cdot}7{\cdot}11{\cdot}13{\cdot}19{\cdot}29{\cdot}37{\cdot}43) = 546580867667055786353697795803169543042863 3$$

Resultados análogos a estos y otros relacionados con la computación de polinomios ciclotómicos pueden verse en [2] y http://www.cecm.sfu.ca/~ada26/cyclotomic/.

La siguiente sección se centrará en cotas sobre una familia de polinomios ciclotómicos más fácil de manejar, pero igual de rica en este aspecto, esto es, la familia de los polinomios ciclotómicos ternarios.

4.2. Cotas sobre polinomios ternarios

El siguiente resultado, además de ser uno de los más importantes en el estudio de la magnitud de los coeficientes de los polinomios ciclotómicos, motiva esta sección. Se ha llamado Teorema de Bungers-Lehmer, y fue probado por primera vez en 1934 por Rolf Bungers, bajo la suposición de que existen infinitas parejas de primos gemelos (cuya distancia es 2). En 1936 Emma Lehmer lo probó sin usar esta última hipótesis, que sigue siendo un misterio a día de hoy.

Teorema 4.2.1 *[19] Pueden elegirse ternas de primos impares $p < q < r$ para las cuales existen coeficientes de $g_{pqr}(x)$ arbitrariamente grandes en valor absoluto.*

Dem: La idea de esta demostración es similar a la del Teorema de Schur: reducir $g_n(x)$ módulo un monomio determinado y probar que un coeficiente está acotado inferiormente por una función creciente de uno de los primos. Sin embargo, esta tarea se hace sustancialmente más complicada. En primer lugar, hay que añadir estas condiciones sobre los primos q y r:

$$q = kp + 2 \qquad r = \frac{mpq - 1}{2},$$

para ciertos k y m. La existencia de estos primos está asegurada por el Teorema de Dirichlet sobre progresiones aritméticas.

Por la Fórmula de Inversión de Möbius,

$$g_{pqr}(x) = \frac{(x^{pqr}-1)(x^p-1)(x^q-1)(x^r-1)}{(x-1)(x^{pq}-1)(x^{pr}-1)(x^{qr}-1)}$$

De nuevo la idea va a ser reducir módulo un polinomio conveniente. Por una parte, tenemos que

$$\frac{x^p-1}{x-1} = 1 + x + \cdots + x^{p-1} \qquad (x^q-1)(x^r-1) = 1 - x^q - x^r + x^{q+r},$$

por lo que $g_{pqr}(x) = \frac{(1-x^{pqr})(1+x+\cdots+x^{p-1})(1-x^q-x^r+x^{q+r})}{(1-x^{pq})(1-x^{pr})(1-x^{qr})}$. Desarrollando ahora los términos del denominador como serie geométrica y reduciendo módulo x^{pqr}, la expresión resultante es:

$$g_{pqr}(x) \equiv (1 + x + \cdots + x^{p-1})(1 - x^q - x^r + x^{q+r}) \sum x^{\nu qr+\lambda pr+\mu pq} \text{ mód } x^{pqr},$$

donde ν, λ y μ recorren los números naturales. Sobre esta última congruencia se va a probar que $a(pqr,h) \geq \frac{p-1}{2}$, donde $h = \frac{(p-3)(qr+1)}{2}$. Cada uno de los términos involucrados en el cómputo del coeficiente de x^h está relacionado con una solución de la ecuación

$$\nu qr + \lambda pr + \mu pq + \omega + \epsilon q + \eta r = h \tag{4.1}$$

donde $\nu, \lambda, \mu \geq 0$, $0 \leq \omega \leq p-1$ y $\epsilon, \eta \in \{0,1\}$. Además, esto impone de manera natural las siguientes restricciones:

$$\nu qr \leq h \qquad \lambda pr \leq h \qquad \mu pq \leq h.$$

Como las cuatro posibles combinaciones del par (ϵ, η) se corresponden con los términos $1, -x^q, -x^r, x^{q+r}$, entonces $a(pqr,h)$ viene dado por el número de soluciones a la Ecuación 4.1 cuando $\epsilon = \eta$ menos el número de soluciones cuando $\epsilon \neq \eta$. Nuestro objetivo es probar lo siguiente:

- Cuando $\epsilon = \eta = 0$, existen exactamente $\frac{p-1}{2}$ soluciones a la ecuación.
- No existen soluciones si $\epsilon \neq \eta$.

A continuación, tomaremos congruencias en la Ecuación 4.1 módulo p, q y r para extraer relaciones sobre las soluciones de la ecuación. Después de notar que $qr = (kp+2)\left(\frac{mpq-1}{2}\right) \equiv 2 \cdot \left(\frac{mpq-1}{2}\right)$ mód $p \equiv -1 \mod p$, es inmediato ver que se tiene:

$$\begin{array}{rcll} \nu qr + \omega + \epsilon q + \eta r & \equiv & 0 & \text{mód} p \\ \lambda pr + \omega + \eta r & \equiv & \frac{p-3}{2} & \text{mód} q \\ \mu pq + \omega + \epsilon q & \equiv & \frac{p-3}{2} & \text{mód} r \end{array}$$

Observamos ahora las siguientes congruencias: $kpr \equiv 1$ mód q, $mpq \equiv 1$ mód r, $q \equiv 2$ mód p, $r \equiv -\frac{1}{2}$ mód pq donde $-\frac{1}{2}$ mód pq hace referencia al inverso de $pq-2$ en el grupo de unidades de $(\mathbb{Z}/pq\mathbb{Z})$, que existe porque $(2, pq) = 1$. Probaremos solamente la primera congruencia, porque el resto son inmediatas de la definición de q o r:

$$kpr = kp\frac{mpq-1}{2} \equiv (q-2)\frac{mpq-1}{2} \text{ mód } q \equiv 1 \text{ mód } q$$

En virtud de lo anterior, y multiplicando las dos últimas congruencias por k y m, respectivamente, se tiene que:

- $\omega \equiv -\nu qr - \epsilon q - \eta r$ mód $p \equiv -2\nu\frac{-1}{2} - 2\epsilon + \frac{\eta}{2}$ mód $p \equiv \nu - 2\epsilon + \frac{\eta}{2}$ mód p.
- $\lambda \equiv \lambda prk$ mód $q \equiv k\left(\frac{p-3}{2} - \omega - \eta r\right)$ mód $q \equiv k\left(\frac{p-3}{2} - \omega + \frac{\eta}{2}\right)$ mód q
- $\mu \equiv \mu pqm$ mód $r \equiv m\left(\frac{p-3}{2} - \omega - \epsilon q\right)$ mód r

Estas tres congruencias van a ser claves en la demostración, y se pide al lector que las tenga presente en todo momento:

$$\omega \equiv \nu - 2\epsilon + \frac{\eta}{2} \text{ mód } p \tag{4.2}$$

$$\lambda \equiv k\left(\frac{p-3}{2} - \omega + \frac{\eta}{2}\right) \text{ mód } q \tag{4.3}$$

$$\mu \equiv m\left(\frac{p-3}{2} - \omega - \epsilon q\right) \text{ mód } r \tag{4.4}$$

Nos encontramos ahora en condiciones de distinguir casos según los valores de ϵ y η.

Caso 1: $\epsilon = \eta = 0$

Probaremos que existen $\frac{p-1}{2}$ soluciones en este caso. En primer lugar, por 4.2, $\omega \equiv \nu$ mód p. Además, como ambos son positivos y menores que p (es claro que $\nu \leq p$, $\lambda \leq q$ y $\mu \leq r$ para cualquiera de los casos), ha de ser $\omega = \nu$. Sustituyendo en las ecuaciones 4.3 y 4.4, se tiene que

$$\lambda \equiv k\left(\frac{p-3}{2} - \nu\right) \text{ mód } q \qquad \mu \equiv m\left(\frac{p-3}{2} - \nu\right) \text{ mód } r.$$

Sin embargo, estas congruencias son en realidad igualdades. Esto es consecuencia de que:

- $\nu \leq \frac{p-3}{2}$: una de las restricciones de la Ecuación 4.1 es $\nu qr \leq \frac{p-3}{2}(qr+1)$, que es equivalente a $\nu \leq \frac{p-3}{2} + \frac{p-3}{2qr}$. Como $\nu \in \mathbb{N}$ y $\frac{p-3}{2qr} < 1$, ha de ser $\nu \leq \frac{p-3}{2}$.
- $\frac{k(p-3)}{2} < q$: es inmediato escribiendo $q = kp + 2$.

- $\frac{m(p-3)}{2} < r$: si escribimos $r = \frac{mpq-1}{2}$, la desigualdad es equivalente a $-m(pq-p+3) < -1$.

Probaremos ahora, a partir de la congruencia, que $\lambda = k\left(\frac{(p-3)}{2} - \nu\right)$. Por una parte, se tiene que $\lambda < q$. Como $\frac{k(p-3)}{2} < q$ y $k\nu \leq \frac{k(p-3)}{2}$, $\frac{k(p-3)}{2} - k\nu$ está entre 0 y q. Como $\lambda \equiv \frac{k(p-3)}{2} - k\nu$ mód q, han de ser iguales. De manera análoga, con las otras desigualdades, se prueba que $\mu = m\left(\frac{p-3}{2} - \nu\right)$. Sustituyendo $\epsilon = \eta = 0$ y $\omega = \nu$ en la Ecuación 4.1:

$$\nu qr + \lambda pr + \mu pq + \nu = \frac{p-3}{2}(qr+1)$$

Por las igualdades probadas anteriormente, cada uno de los valores de ν determina correspondientes valores de μ y λ y, por tanto, soluciones a la ecuación. Además, como $\nu \leq \frac{p-3}{2} = \frac{p-1}{2} - 1$, hay exactamente $\frac{p-1}{2}$ soluciones a la ecuación: $\nu = 0, \cdots, \nu = \frac{p-1}{2} - 1$. Finalmente, es mera comprobación que $\nu qr, \lambda pr, \mu pq < h$:

- $\nu qr < h$ es equivalente a $\nu \leq \frac{p-3}{2}$.
- Como $\lambda = \frac{k(p-3)}{2} - k\nu$, entonces $\lambda \leq \frac{k(p-3)}{2}$. Además, recordando que $q = kp + 2$:

$$\lambda pr \leq \frac{kpr(p-3)}{2} < \frac{p-3}{2}qr < \frac{p-3}{2}(qr+1) = h$$

- Por motivos semejantes, $\mu \leq \frac{m(p-3)}{2}$, y por tanto

$$\mu pq \leq \frac{mpq(p-3)}{2} \leq \frac{p-3}{2}(2r+1) < \frac{(p-3)}{2}(qr+1) = h$$

Caso 2: $\epsilon = 1, \eta = 0$

Por la Ecuación 4.2 se tiene que $\omega \equiv \nu - 2$ mód p. Es decir, existe $a \in \mathbb{Z}$ tal que $\omega = ap + \nu - 2$. Como ambos son menores que p (la cota $\nu \leq \frac{p-3}{2}$ probada en el caso anterior no utilizaba que $\epsilon = \eta = 0$), ha de ser $\omega = \nu - 2$ en los casos en que $\nu \geq 2$. Si $\nu = 0$, entonces $\omega = ap - 2$, y como $\omega \leq p$, ha de ser $a = 1$. De la misma manera se razona en el caso $\nu = 1$. Por tanto, $\omega = \nu - 2$, $\omega = p - 1$ o $\omega = p - 2$. Vamos a ver que los dos últimos casos no son posibles.

Se tiene que $\frac{p-3}{2} - (p-1) = -\frac{p+1}{2}$ y $\frac{p-3}{2} - (p-2) = -\frac{p-1}{2}$. Usando la Ecuación 4.3, $\lambda \equiv k\left(\frac{p-3}{2} - \omega\right)$ mód $q \equiv -\frac{k(p\pm1)}{2}$ mód q en los casos $\omega = p-1$ y $\omega = p-2$. De esta congruencia se obtiene que $\lambda = q - k\left(\frac{p\pm1}{2}\right)$. Veamos por qué: se tiene $\lambda = aq - \frac{k(p\pm1)}{2}$, donde, naturalmente, $a \geq 1$. Por otra parte, $\lambda \leq q$, que es equivalente a decir que $(a-1)q \leq \frac{k(p\pm1)}{2}$ mediante la igualdad anterior. Como $q = kp + 2$, esto solo es posible cuando $a = 1$.

Sin embargo, si $\omega = p-1$ o $p-2$, puede comprobarse que $\lambda pr > h$, como haremos a continuación, y por tanto se viola una de las condiciones de la Ecuación 4.1:

Como $\lambda = q - \frac{k(p\pm1)}{2}$, entonces $\lambda pr = qpr - \frac{kpr(p\pm1)}{2} > qpr - \frac{kpr(p+1)}{2} > pqr - \frac{qr(p+1)}{2}$. Es fácil de ver que esta última desigualdad es equivalente a $kp < q$, que es cierta porque $q = kp + 2$. Probaremos que este último término de la desigualdad es mayor que h:

$$\begin{aligned} pqr - \frac{qr(p+1)}{2} > \frac{(p-3)(qr+1)}{2} &\Leftrightarrow 2pqr > qr(p+1) + (p-3)(qr+1) \\ &\Leftrightarrow 2pqr > pqr + pqr + qr + p - 3qr - 3 \\ &\Leftrightarrow 0 > -2qr + p - 3 \end{aligned}$$

El problema queda reducido al caso $\omega = \nu - 2$. Probaremos que tampoco hay soluciones, esta vez porque $\mu pq > h$. De la Ecuación 4.4 se tiene que $\mu = ar + m\left(\frac{p-3}{2} - \omega - q\right)$ para cierto entero a. Con un razonamiento análogo al seguido para probar que $\lambda = q - \frac{k(p\pm1)}{2}$ en los casos $\omega = p-1$ o $p-2$, se concluye que $\mu = r + m\left(\frac{p-3}{2} - \omega - q\right)$. Como paso intermedio para probar que $\mu pq > h$, probaremos primero que $\mu = r + m\left(\frac{p-3}{2} - \omega - q\right) \geq r + m(2-q)$:

$$\begin{aligned} r + m\left(\frac{p-3}{2} - \omega - q\right) \geq r + m(2-q) &\Longleftrightarrow \frac{p-3}{2} - \omega - q \geq 2 - q \\ &\Longleftrightarrow \omega \leq \frac{p-3}{2} - 2 = \frac{p-7}{2} \end{aligned}$$

Como $\omega = \nu - 2 \leq \frac{p-3}{2} - 2 = \frac{p-7}{2}$, queda probada la desigualdad. Finalmente, se tiene que:

$$\begin{aligned} \mu pq \geq& (r + m(2-q))pq = rpq + mpq(2-q) = rpq + (2r+1)(2-q) \\ \overset{*}{=}& (qr+1)(p-2) + (4r - p - q + 4) \overset{**}{>} (qr+1)(p-2) \\ >& h \end{aligned}$$

El paso $*$ es fácil de ver desarrollando los términos. Para ver el paso $**$ es suficiente probar que $4r - p - q + 4 > 0$, que es lo mismo que decir que $2mpq - p - q + 2 > 0$. Esto se deduce del hecho de que

$$\frac{2(m+1)pq}{p+q} > \frac{pq}{p+q} > \frac{pq}{2q} > \frac{p}{2} > 1$$

.

Caso 3: $\epsilon = 0, \eta = 1$

Sustituyendo en la Ecuación 4.2 se tiene que $\omega \equiv \nu + \frac{1}{2} \pmod p$. Como $0 < \omega < p$ y $\nu \leq \frac{p-3}{2}$, ha de ser $\omega = \nu + \frac{p+1}{2}$. Sustituyendo ahora en la Ecuación 4.4:

$$\mu \equiv m\left(\frac{p-3}{2} - \nu - \frac{p+1}{2}\right) \pmod r \equiv -m(\nu+2) \pmod r$$

Puede verse que $2r - m(\nu+2) > r$, es decir, que $r > m(\nu+2)$. Como $\mu < r$, ha de ser $\mu = r - m(\nu+2)$. Además, $\mu = r - m(\nu+2) \geq r - \frac{m(p+1)}{2}$ ya que $\nu \leq \frac{p-3}{2}$.

Se tiene, por tanto:

$$\mu pq \geq \left(r - \frac{m(p+1)}{2}\right) pq = rpq - \frac{m(p+1)pq}{2} = rpq - \frac{(2r+1)(p+1)}{2}$$
$$= (qr+1)(p-1) + \frac{2r - q - 2p + 3}{2} > (qr+1)(p-1) > h$$

Lo que implica que no existen soluciones cuando $\epsilon = 0$ y $\eta = 1$.

Caso 4: $\epsilon = \eta = 1$

Como el caso $\epsilon = \eta = 1$ solo contribuye con términos positivos a la suma, podemos concluir que $a(pqr, h) \geq \frac{p-1}{2}$ y, consecuentemente, nuestro objetivo inicial: la altura de los polinomios ciclotómicos ternarios es arbitrariamente grande. En realidad, siguiendo un proceso análogo puede verse que tampoco hay soluciones, y $a(pqr, h) = \frac{p-1}{2}$.

Naturalmente, poder encontrar coeficientes arbitrariamente grandes en valor absoluto en los polinomios ciclotómicos de orden 3 lleva a centrar el estudio de las cotas para casos particulares dentro de esta familia. El primer resultado relacionado con esto data de 1895, cuando Bang prueba que $\mathrm{A}(pqr) \leq p-1$, y los últimos avances llegan hasta nuestros días. Para empezar, expondremos la demostración de Bang, que se encuentra esbozada en [5], y después hablaremos de la mejora de las cotas a lo largo de los años.

Teorema 4.2.2 *[5] Si $p < q < r$ son primos impares, $\mathrm{A}(pqr) \leq p-1$.*

Dem: Como ya vimos en el Teorema 4.2.1, por la Fórmula de Inversión de Möbius, desarrollando la serie geométrica y reduciendo módulo x^{pqr},

$$g_{pqr}(x) \equiv (1 + x + \cdots + x^{p-1})(x^q - 1)(x^r - 1) \sum x^{\nu qr + \lambda pr + \mu pq} \text{ mód } x^{pqr}.$$

Sea k un exponente que aparece en el desarrollo de $g_{pqr}(x)$ y c_k el coeficiente asociado. El objetivo es probar que $|c_k| \leq p-1$. Estamos interesados en encontrar las soluciones a la ecuación

$$\nu qr + \lambda pr + \mu pq + \omega + \epsilon q + \eta r = k,$$

donde ν, λ, $\mu \geq 0$, $0 \leq \omega \leq p-1$ y ϵ, $\eta \in \{0, 1\}$. Por la Proposición 1.1.11 podemos suponer que $k \leq \frac{\varphi(pqr)}{2}$, lo que simplificará la discusión y nos permitirá concluir lo que queríamos:

Sea $\alpha \leq \frac{\varphi(pqr)}{2} = \frac{(p-1)(q-1)(r-1)}{2}$, y consideramos la ecuación $\nu qr + \lambda pr + \mu pq = \alpha$, donde ν, λ y μ son enteros no negativos. Como son soluciones de la ecuación, se tiene que $\nu < p$, $\lambda < q$ y $\mu < r$. Esto implica que, como mucho,

existe una solución a esta ecuación: supongamos que $\nu_1 qr + \lambda_1 pr + \mu_1 pq = \nu_2 qr + \lambda_2 pr + \mu_2 pq = \alpha$. Reduciendo módulo p, se tiene que $\nu_1 qr \equiv \nu_2 qr$ mód p, que es equivalente a decir que $\nu_1 \equiv \nu_2$ mód p. Como ambos son menores que p, entonces $\nu_1 = \nu_2$. Reduciendo módulo q y r se obtienen las otras igualdades.

Si se escribe la ecuación original en la forma

$$\nu qr + \lambda pr + \mu pq = k - \omega - \epsilon q - \eta r$$

y se tiene en cuenta que $k - \omega - \epsilon q - \eta r$ va a recorrer un conjunto de p enteros positivos consecutivos puesto que w recorre los valores $0, 1, \ldots, p-1$, lo que buscamos son conjuntos de p enteros positivos consecutivos, menores o iguales que k, que puedan expresarse en la forma $\nu qr + \lambda pr + \mu pq$. Representando por b_k el máximo número de enteros positivos en estas condiciones, resulta que $|c_k| \leq 2b_k$.

Además, como cada uno de estos b_k números está en un intervalo de la forma $[j, j+p-1]$, no existen dos que sean congruentes módulo p, lo que significa que b_k está en correspondencia con los distintos valores de ν, y el número de valores de ν está acotado por $\frac{p-1}{2}$:

$$\nu qr \leq \frac{(p-1)(q-1)(r-1)}{2} \Longrightarrow \nu \leq \frac{p-1}{2} \cdot \frac{q-1}{q} \cdot \frac{r-1}{r} < \frac{p-1}{2}$$

Finalmente, $|c_k| \leq 2b_k \leq 2\frac{(p-1)}{2} = p-1$.

El siguiente avance lo haría Marion Beiter, mejorando esta cota y conjeturando una mejor:

Teorema 4.2.3 *[4] Sean $p < q < r$ primos impares. Entonces:*

- *Si $p = 4k+1$, entonces $\mathrm{A}(pqr) \leq p - k$.*
- *Si $p = 4k+3$, entonces $\mathrm{A}(pqr) \leq p - k - 1$.*

Conjetura 4.2.4 *[4] Si $p < q < r$ son primos impares, $\mathrm{A}(pqr) \leq \frac{p+1}{2}$.*

Estos aportes datan de 1971, y la conjetura, que estuvo durante muchos años sin resolver, se ha llamado Conjetura de Beiter. Además, en ese mismo año, se prueba el siguiente resultado:

Teorema 4.2.5 *[21] Si $p < q < r$ son primos impares con $q \equiv 2$ mód p y $r = \frac{mpq-1}{2}$, entonces $a\left(pqr, \frac{(p-1)(qr+1)}{2}\right) = \frac{p+1}{2}$.*

Por tanto, la Conjetura de Beiter, en caso de ser cierta, hubiese sido el mejor resultado que se podría obtener a este respecto. Sin embargo, en 2008 Gallot y Moree ([11]) dan un contraejemplo: $\mathrm{A}(pqr) > \frac{p+1}{2}$ para todo $p \geq 11$, y prueban que para todo $\epsilon > 0$ existen infinitas ternas $p < q < r$ de primos impares de tal forma que algún coeficiente de $g_{pqr}(x)$ es mayor, en valor absoluto, que $\left(\frac{2}{3} - \epsilon\right) p$. En ese mismo artículo, se propone la Conjetura Mejorada de Beiter, que dice que $\mathrm{A}(pqr) \leq \frac{2}{3}p$. Fue probada en 2009 por Zhao y Zhang ([30]).

4.3. Polinomios ciclotómicos de órdenes mayores

A modo de conclusión, terminaremos este trabajo haciendo un repaso sobre otros resultados relacionados con los coeficientes de los polinomios ciclotómicos y con esta familia de polinomios en general.

4.3.1. Teoremas de periodicidad

Uno de los resultados relevantes sobre los polinomios terciarios planos eran los teoremas de periodicidad (Teorema 3.2.1 y Teorema 3.2.5), que dicen que fijados p y q, si $r \equiv \pm s \mod pq$, entonces $\mathrm{A}(pqr) = \mathrm{A}(pqs)$. Son resultados de gran importancia, no solamente porque nos permiten construir familias infinitas de polinomios ternarios con una altura fijada (supuesto que tengamos primero uno), sino que también limitan en gran medida los valores que puede tomar la altura de $g_{pqr}(x)$ fijados solamente los dos primeros factores primos.

En el paso al estudio de polinomios ciclotómicos de órdenes mayores una de las preguntas naturales que surgen es: ¿existen generalizaciones de estos teoremas? La respuesta es afirmativa. De hecho, no se limitan a polinomios de un orden fijado.

Definición 4.3.1 *Sea $n \in \mathbb{N}$ y $a(n,k)$ el k-ésimo coeficiente de $g_n(x)$. Se define $V(n) = \{a(n,k) : 0 \leq k \leq \frac{\varphi(n)}{2}\}$.*

Como ya sabemos, por la reciprocidad del polinomio ciclotómico, en realidad $\mathrm{V}(n)$ es el conjunto de todos los coeficientes. Sin embargo, veíamos en el Teorema 4.2.2 la utilidad de esa restricción. El siguiente teorema, probado en 2010 ([17]), es la generalización del primer teorema de periodicidad:

Teorema 4.3.2 *[17] Sea $p_1 < \cdots < p_r$ una cadena de primos impares y n su producto. Sean s y t primos mayores que n satisfaciendo $s \equiv t \mod n$. Entonces $\mathrm{V}(ns) = \mathrm{V}(nt)$.*

Bajo las condiciones anteriores se tiene además que $\mathrm{A}(ns) = \mathrm{A}(nt)$, pero este es un resultado mucho más fuerte. Sin embargo, se extraña un resultado que permita extender al caso $s \equiv \pm t \mod n$. Este llegaría dos años más tarde, y debilita la condición $n < s, t$.

Teorema 4.3.3 *[9] Sean $n > 1$ y s, t primos mayores que $n - \varphi(n)$. Si $s \equiv t \mod n$, entonces $V(ns) = V(nt)$; si $s \equiv -t \mod n$, entonces $\mathrm{V}(ns) = -\mathrm{V}(nt)$.*

4.3.2. Polinomios ciclotómicos planos

Otra de las preguntas importantes tiene que ver con los polinomios ciclotómicos planos de órdenes superiores. En este caso, la respuesta es bastante menos clara. Un corolario inmediato al Teorema 4.3.2 es el siguiente:

Corolario 4.3.4 *[17] Si $p_1 < \cdots < p_r$ es una cadena de primos impares, n su producto y $s > n$ es un primo de forma que $g_{sn}(x)$ es plano, entonces existen infinitos polinomios ciclotómicos planos de orden $r+1$.*

Según la misma fuente, $\mathrm{A}(3 \cdot 5 \cdot 31 \cdot 929) = 1$, y $929 > 465 = 3 \cdot 5 \cdot 31$; por tanto, el anterior Corolario es aplicable y tenemos que:

Proposición 4.3.5 *Existe una familia infinita de polinomios ciclotómicos planos de orden 4: $\{g_{465s} : s > 465, s \equiv 929 \text{ mód } 465\}$.*

Este fue el primer ejemplo conocido de familia infinita de polinomios planos de orden 4. Sin embargo, en [9] (Teorema 47) se construye una familia mucho más general, que recuerda a las construcciones de [16] y [3], de las que hemos hablado en el capítulo anterior.

Teorema 4.3.6 *[9] Sean $p < q < r < s$ primos impares tal que $r \equiv \pm 1 \text{ mód } pq$ y $s \equiv \pm 1 \text{ mód } pqr$. Entonces $g_{pqrs}(x) = 1$ si y solo si $q \equiv -1 \text{ mód } p$.*

Según cita el autor de una fuente que ya no está disponible, si $pqrs < 2 \times 10^6$ todos los polinomios $g_{pqrs}(x)$ que son planos tienen precisamente esa estructura (se puede observar que $g_{3 \cdot 5 \cdot 31 \cdot 929}$ está englobado dentro de esta familia), y conjetura que son todos los polinomios planos de orden 4 existentes. A día de hoy, este es el último resultado sobre la planitud de los polinomios ciclotómicos de orden 4.

Menos se sabe todavía de la existencia de polinomios planos de orden 5. Las computaciones citadas por [9] muestran que si $n = pqrst < 10^8$, $\mathrm{A}(n) > 1$. Además, la extensión natural del Teorema 4.3.6 no es cierta esta vez:

Teorema 4.3.7 *[9] Sean $p < q < r < s < t$ primos impares con $r \equiv \pm 1 \text{ mód } pq$, $s \equiv \pm 1 \text{ mód } pqr$ y $t \equiv \pm 1 \text{ mód } pqrs$. Entonces $g_{pqrst}(x)$ no es plano.*

Bibliografía

[1] APOSTOL, Tom M. Introduction to analytic number theory. Springer Science & Business Media, 2013.

[2] ARNOLD, Andrew; MONAGAN, Michael. Calculating cyclotomic polynomials. Mathematics of Computation, 2011, vol. 80, no 276, p. 2359-2379.

[3] BACHMAN, Gennady. Flat cyclotomic polynomials of order three. Bulletin of the London Mathematical Society, 2006, vol. 38, no 1, p. 53-60.

[4] BEITER, Marion, et al. Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}, II. Duke Mathematical Journal, 1971, vol. 38, no 3, p. 591-594.

[5] BLOOM, D. M. On the coefficients of the cyclotomic polynomials. The American Mathematical Monthly, 1968, vol. 75, no 4, p. 372-377.

[6] BOOT, J. C. G.; GREENBERG, Ralph. E1637. The American Mathematical Monthly, 1964, vol. 71, no 7, p. 799-799.

[7] BROOKFIELD, Gary. The Coefficients of Cyclotomic Polynomials. Mathematics Magazine, 2016, vol. 89, no 3, p. 179-188.

[8] DE LA CRUZ, Melissa. Cyclotomic Polynomials. [Última consulta: 14 de junio de 2019] http://kobotis.net/math/MathematicalWorlds/Fall2016/131/Topics/DeLaCruz.pdf

[9] ELDER, Sam. Flat cyclotomic polynomials: a new approach. arXiv preprint arXiv:1207.5811, 2012.

[10] FINTZEN, Jessica. Cyclotomic polynomial coefficients a (n, k) with n and k in prescribed residue classes. Journal of Number Theory, 2011, vol. 131, no 10, p. 1852-1863.

[11] GALLOT, Yves; MOREE, Pieter. Ternary cyclotomic polynomials having a large coefficient. Journal für die reine und angewandte Mathematik (Crelles Journal), 2009, vol. 2009, no 632, p. 105-125.

[12] HONG, Hoon, et al. Maximum gap in (inverse) cyclotomic polynomial. Journal of Number Theory, 2012, vol. 132, no 10, p. 2297-2315.

[13] JI, Chun-Gang. A specific family of cyclotomic polynomials of order three. Science China Mathematics, 2010, vol. 53, no 9, p. 2269-2274.

[14] JI, Chun-Gang; LI, Wei-Ping. Values of coefficients of cyclotomic polynomials. Discrete Mathematics, 2008, vol. 308, no 23, p. 5860-5863.

[15] JI, Chun-Gang; LI, Wei-Ping; MOREE, Pieter. Values of coefficients of cyclotomic polynomials II. arXiv preprint arXiv:0711.4898, 2007.

[16] KAPLAN, Nathan. Flat cyclotomic polynomials of order three. Journal of Number Theory, 2007, vol. 127, no 1, p. 118-126.

[17] KAPLAN, Nathan. Flat cyclotomic polynomials of order four and higher. Integers, 2010, vol. 10, no 3, p. 357-363.

[18] LAM, Tsit-Yeun; LEUNG, Ka Hin. On the cyclotomic polynomial Φpq (X). The American Mathematical Monthly, 1996, vol. 103, no 7, p. 562-564.

[19] LEHMER, Emma. On the magnitude of the coefficients of the cyclotomic polynomial. Bulletin of the American Mathematical Society, 1936, vol. 42, no 6, p. 389-392.

[20] LENSTRA, H. W., et al. Vanishing sums of roots of unity. En Proceedings bicentennial congress Wiskundig Genootschap, Math. Centre Tracts 100/101, Mathematisch Centrum Amsterdam. 1979. p. 249.

[21] MÖLLER, Herbert. Über die Koeffizienten des n-ten Kreisteilungspolynoms. Mathematische Zeitschrift, 1971, vol. 119, no 1, p. 33-40.

[22] MOREE, Pieter. Cyclotomic Coefficients, Yesterday and Tomorrow. [Última consulta: 14 de junio de 2019] https://www.ugr.es/~imns2010/2014/Slides/IMNS_2014_Moree.pdf

[23] MOREE, Pieter. Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers. The American Mathematical Monthly, 2014, vol. 121, no 10, p. 890-902.

[24] ROSE, Harvey E. A course in number theory. Oxford University Press, 1995.

[25] SURY, B. Cyclotomy and cyclotomic polynomials. Resonance, 1999, vol. 4, no 12, p. 41-53.

[26] SUZUKI, Jiro, et al. On coefficients of cyclotomic polynomials. Proceedings of the Japan Academy, Series A, Mathematical Sciences, 1987, vol. 63, no 7, p. 279-280.

[27] WEINTRAUB, Steven H. Several proofs of the irreducibility of the cyclotomic polynomials. The American Mathematical Monthly, 2013, vol. 120, no 6, p. 537-545.

[28] ZHANG, Bin; ZHOU, Yu. On a class of ternary cyclotomic polynomials. Bull. Korean Math. Soc, 2015, vol. 52, no 6, p. 1911-1924.

[29] ZHANG, Bin. Remarks on the flatness of ternary cyclotomic polynomials. International Journal of Number Theory, 2017, vol. 13, no 02, p. 529-547.

[30] ZHAO, Jia; ZHANG, Xianke. A proof of the corrected Beiter conjecture. arXiv preprint arXiv:0910.2770, 2009.