Universidad de La Laguna

Sección de Matemáticas | Facultad de Ciencias

Claudia Ballester Niebla

Números Primos

Algunas cuestiones históricas, polinomios ciclotómicos y tests de primalidad

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Julio de 2017

Dirigido por

Evelia Rosa García Barroso

Evelia Rosa García Barroso
Departamento de Matemáticas,
Estadística e I.O.
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

A Evelia Rosa García Barroso,
por guiarme, aconsejarme y dedicar su tiempo al proceso
que ha conllevado la elaboración de esta memoria.
A todos mis profesores,
porque sin ellos no hubiese sido
posible llegar hasta aquí.
A mis compañeros y amigos,
por ayudarme tanto en estos años.
A mi familia,
por ser un apoyo incondicional en
la lucha por alcanzar mis metas.
Y a mi pareja,
por creer siempre en mí.

Resumen · Abstract

Resumen

Empezamos esta memoria estudiando el algoritmo de Euclides y mostramos las cotas dadas por algunos matemáticos franceses del siglo XIX. Probamos que la mejor de ellas fue dada por Gabriel Lamé, en la que los números de Fibonacci juegan un papel fundamental. Después pasamos a trabajar con aritmética modular, definiendo el concepto de residuo cuadrático y los llamados símbolos de Legendre y de Jacobi, que son de utilidad para los enunciados que probamos. El estudio de los polinomios ciclotómicos nos permitirá factorizar enteros de la forma $a^n \pm 1$. Por último, presentamos algunos tests de primalidad, comenzando con la Criba de Eratóstenes, continuando con los tests probabilísticos de Fermat y de Miller-Rabin, y finalizando con el algoritmo AKS, un algoritmo determinístico y en tiempo polinomial.

Palabras clave: *Números primos – Algoritmo de Euclides – Polinomios ciclotómicos – Test de Primalidad.*

Abstract

This degree thesis starts with the study of the Euclidean algorithm. Then, we show the bounds given by some French mathematicians in the 19th century. The best one was given by Gabriel Lamé and it is connected to Fibonacci's numbers. Then, we start working with modular arithmetic. We define quadratic residues, Legendre's symbol and Jacobi's symbol. They will be useful while proving some important results. The study of cyclotomic polynomials will help us factoring integer numbers of the type $a^n \pm 1$. Finally, we present some primality tests. We start with the Sieve of Eratosthenes, we follow with Fermat's and Miller-Rabin's probabilistic tests and we end with the AKS algorithm, which is a deterministic polynomial time algorithm.

Keywords: *Prime numbers – The Euclidean Algorithm – Cyclotomic polynomials – Primality Test.*

Contenido

Introducción

El estudio de los números primos constituye un amplio campo de investigación tanto desde el punto de vista teórico como de las aplicaciones de los mismos. Uno de sus objetivos principales es la identificación de enteros que sean números primos, ayudándonos de algoritmos para ello. En esta memoria presentamos algunos de estos algoritmos. El interés de tal identificación se ha acentuado en las últimas décadas, pues los primos son fundamentales para ciertos sistemas criptográficos. Otro objetivo fundamental de esta teoría es, una vez detectado que un entero no es primo, determinar sus distintos factores primos.

En el primer capítulo de esta memoria nos centramos en el Algoritmo de Euclides. Dicho algoritmo nos permite calcular el máximo común divisor entre dos números enteros. Una vez presentado, es natural preguntarse cuántos pasos son necesarios para la obtención de dicho máximo común divisor. Mostraremos las cotas dadas por algunos matemáticos franceses del siglo XIX y probaremos que la mejor de ellas fue dada por Gabriel Lamé, en la que los números de Fibonacci jugarán un papel fundamental. Si bien el estudio de esta memoria es eminentemente teórico, finalizamos el capítulo primero demostrando que el algoritmo de Euclides es un algoritmo eficiente.

En el segundo capítulo pasamos a trabajar con aritmética modular. Definimos el concepto de residuo cuadrático y los llamados símbolos de Legendre y de Jacobi, que nos son de utilidad para los enunciados que probamos. También estudiamos algunas funciones especiales como la función de Möbius, la función de Euler y la función ω, así como sus propiedades. El estudio de los polinomios ciclotómicos cierra esta sección. En particular, relacionamos dichos polinomios con la función de Möbius y los aplicamos para la factorización de los enteros de la forma $a^n \pm 1$.

Por último, en el tercer capítulo, presentamos algunos tests de primalidad. Comenzamos con la criba de Eratóstenes, un método clásico de identificación de primos. Continuamos con el test de Fermat y el algoritmo de Miller-Rabin. Estos dos últimos son tests probabilísticos. En la última sección describimos, sin entrar en mucho detalle dadas las limitaciones de espacio, el algoritmo AKS, un algoritmo determinístico y en tiempo polinomial para el estudio de la primalidad.

A lo largo del tiempo se han ido desarrollando algoritmos de primalidad cada vez más eficientes. Esto resulta de gran utilidad a la hora de obtener números primos cada vez más grandes y poder utilizarlos en las diferentes aplicaciones que éstos presentan, como puede ser la criptografía. Por motivos de espacio no ha sido posible llevar a cabo un estudio computacional de los algoritmos, sino que éste ha sido meramente teórico, aunque cuando ha sido posible se ha proporcionado referencias sobre este estudio para el interés del lector. Esto nos permite dejar una línea abierta para trabajos futuros, en los que se podría realizar el análisis computacional de los algoritmos y posteriormente tratar algunas de las aplicaciones prácticas donde los números primos juegan un papel fundamental.

La metodología empleada ha sido la usual en un trabajo de esta índole, es decir, revisión de diferente bibliografía que se detalla al final de esta memoria, reuniones periódicas con la tutora y redacción de la memoria. En la consulta bibliográfica hemos recorrido desde los artículos clásicos del siglo XIX referenciados en el primer capítulo, hasta referencias más recientes como la [12] y la [17]. Además, en las distintas secciones se señala la bibliografía que se ha usado principalmente, aunque también se han revisado las referencias [2] y [5].

Esta memoria representa una introducción a algunos resultados de la amplia teoría que se encarga del estudio de los números primos, números que han fascinado a los matemáticos desde la Antigüedad hasta nuestros días.

1

Números primos y Euclides

En este capítulo se introducirá la noción de números primos y algunos resultados sobre ellos. Esto nos permitirá enunciar el conocido como *Algoritmo de Euclides*, que se ha ido analizando a lo largo del tiempo. En particular, nos pararemos en el análisis realizado por cuatro matemáticos franceses del siglo XIX. Así, el contenido histórico del presente capítulo está inspirado, principalmente, de [15, páginas 401-419]. Hemos consultado, además, los trabajos originales [6] y [9, páginas 868-870].

1.1. Números primos. Definición y resultados

Definición 1.1. *Sea $p \in \mathbb{Z}$, $p \geq 2$. Diremos que p es primo si sus únicos divisores positivos son 1 y p. Así, si $n \in \mathbb{Z}^+$ no es primo, diremos que es compuesto.*

Teorema 1.2 (Teorema Fundamental de la Aritmética). *Todo entero mayor que uno puede descomponerse, de forma única salvo el orden en la escritura, en un producto de potencias de primos, es decir, $n = \prod_{i=1}^{n} p_i^{\alpha_i}$, donde p_i es un número primo y α_i un entero positivo.*

Demostración. Tendremos que probar dos cosas.

1. **Existencia.** Sea $\mathcal{S} := \{n \in \mathbb{N}, n > 1$ tal que n no se puede escribir como producto de primos$\}$. Debemos demostrar que $\mathcal{S} = \emptyset$. Sabemos que $\mathcal{S} \subseteq \mathbb{N}$ y suponemos que $\mathcal{S} \neq \emptyset$. Aplicando el principio de buen orden a $\mathcal{S}$, existe $m \in \mathcal{S}$ que es mínimo de $\mathcal{S}$. Como $m \in \mathcal{S}$, éste no puede ser primo. Por tanto, es compuesto. Es decir, existen $m_1, m_2 \in \mathbb{N}$ tales que $m = m_1 m_2$ y $1 < m_1, m_2 < m$. Como m es mínimo en $\mathcal{S}, m_1, m_2 \notin \mathcal{S}$. Por tanto, podemos escribir $m_1 = p_1 \cdots p_r$ y $m_2 = q_1 \cdots q_s$, donde p_i, q_j son primos y $1 \leq i \leq r$,

$1 \leq j \leq s$. Así, llegamos a que $m = m_1 m_2 = p_1 \cdots p_r q_1 \cdots q_s$, que es absurdo, pues $m \in \mathcal{S}$, por lo que no se puede escribir como producto de primos.

2. **Unicidad.** Sea $n \in \mathbb{Z}, n > 1$ y supongamos que $n = p_1 \cdots p_r = q_1 \cdots q_s$, $r, s \in \mathbb{N} \setminus \{0\}$, con p_i, q_j primos y $1 \leq i \leq r$, $1 \leq j \leq s$. En particular, p_1 divide a $q_1 \cdots q_s$. Luego, existe $j_1 \in \{1, \ldots, s\}$ tal que $p_1 = q_{j_1}$. Así, $p_2 \cdots p_r = q_1 \cdots q_{j_1 - 1} q_{j_1 + 1} \cdots q_s$. Repitiendo el proceso, concluimos que $r \leq s$.
   A continuación, demostraremos que $r \geq s$. Para ello, supongamos que $r < s$. Así, tras reescritura si fuera necesario, $1 = q_{r+1} \cdots q_s$, lo cual es un absurdo porque los q_j son primos, y por tanto mayores que 1.
   Queda demostrado entonces, que $r = s$, lo que prueba la unicidad.

□

Una vez conocido este resultado, es común preguntarse cuántos números primos existen. En el año 300 a.C., en Alejandría, Euclides encontró la respuesta a esta pregunta.

Teorema 1.3 (Teorema de Euclides). *Existen infinitos números primos.*

Demostración. Supongamos que el conjunto de los números primos es finito y coincide con $\{p_1, \ldots, p_n\}$. Consideremos el número $m = p_1 \cdots p_n + 1$. Sabemos que p_i, con $i \in \{1, \ldots, n\}$ no es divisor de m, pues el resto de la división sería 1. Así, como $\{p_1, \ldots, p_n\}$ es el conjunto de los números primos, deducimos que m no se puede descomponer en un producto de potencias de primos, contradiciendo el Teorema Fundamental de la Aritmética. □

1.2. Algoritmo de Euclides

En esta sección trabajaremos con el Algoritmo de Euclides. Para ello será necesario introducir algunos conceptos previos.

Teorema 1.4 (Teorema de la división euclídea).
Sean $a, b \in \mathbb{Z}$, $b \neq 0$. Existen $q, r \in \mathbb{Z}$, $0 \leq r < |b|$, tales que $a = qb + r$. Además, q, r son únicos y los llamaremos cociente y resto, respectivamente.

Demostración. Habrá que probar existencia y unicidad.

1. **Existencia.** Sea $\mathcal{S} := \{a - hb \text{ tal que } 0 \leq a - hb,\ h \in \mathbb{Z}\} \subseteq \mathbb{N}$. Queremos aplicar el principio de buen orden a $\mathcal{S}$. Para ello demostraremos que $\mathcal{S} \neq \emptyset$.
   - Si $a \geq 0$, se tiene que $a = a - 0b \geq 0$, por lo que $a \in \mathcal{S}$ y $\mathcal{S} \neq \emptyset$.
   - Si $a < 0$, se diferencian dos casos.
     - Cuando $1 \leq b$, se verifica $a - ab = a(1 - b) \geq 0$, de modo que $a - ab \in \mathcal{S}$ y $\mathcal{S} \neq \emptyset$.

- Cuando $b < 1$ entonces $a - (-a)b = a + ab = a(1 + b) \geq 0$. Por tanto, $a - (-a)b \in \mathcal{S}$ y $\mathcal{S} \neq \emptyset$.

Se puede aplicar el principio de buen orden a $\mathcal{S}$, por lo que tiene elemento mínimo $a - h_0 b$, $h_0 \in \mathbb{Z}$. Considerando $q := h_0$ y $r := a - h_0 b$, se obtiene que $r = a - qb$. De este modo, $a = qb + r$. Además, como $r \in \mathcal{S} \subseteq \mathbb{N}$ se verifica que $r \geq 0$. Queda demostrar que $r < |b|$. Se pueden dar dos casos.

- Si $b > 0$, entonces $|b| = b$. Suponiendo, por reducción al absurdo, que $r \geq |b| = b$, se obtiene que $r - b \geq 0$. Esto es $a - qb - b \geq 0$, es decir, $a - b(q + 1) \geq 0$. Por tanto, $a - b(q + 1) \in \mathcal{S}$ y $a - b(q + 1) < r$, lo cual es un absurdo.
- Si $b < 0$, entonces $|b| = -b$. Suponiendo, por reducción al absurdo, que $r \geq |b| = -b$, se llega a que $r + b \geq 0$. Así, $a - qb + b \geq 0$, obteniéndose que $a - b(q - 1) \geq 0$ y $a - b(q - 1) < r$, siendo esto un absurdo.

2. **Unicidad.** Supongamos que existen $q, q', r, r' \in \mathbb{N}$ distintos tales que $a = qb + r$ y $a = q'b + r'$, donde $0 \leq r, r' < |b|$. Como $r' \in \mathcal{S}$ y r es mínimo en $\mathcal{S}$, tenemos que $0 \leq r < r'$. De esto, $r' - r > 0$. Pero $r' - r = (q' - q)b \geq |b|$, lo cual es un absurdo. Así, $r = r'$ y $a = qb + r = q'b + r$, de donde deducimos que $q = q'$.

□

Definición 1.5. *Sean $x, y \in \mathbb{Z}$. Diremos que $d \in \mathbb{Z}^+$ es el máximo común divisor de x e y si se verifica:*

1. *d divide a x e y.*
2. *Si existe un $c \in \mathbb{Z}^+$ que divide a x e y entonces c divide a d.*

Lo denotaremos por $d = \text{m.c.d.}(x, y)$.

Teorema 1.6. *Sean $x, y \in \mathbb{Z}$, no nulos simultáneamente. Entonces, existen $a, b \in \mathbb{Z}$ tales que $ax + by = \text{m.c.d.}(x, y)$.*

Demostración. Sea g el menor entero positivo tal que $g = ax + by$, $a, b \in \mathbb{Z}$. Demostraremos que $g = \text{m.c.d.}(x, y)$.

1. m.c.d.(x, y) divide a g: por definición, el máximo común divisor de x e y los divide a ambos. Así, m.c.d.(x, y) divide a $ax + by = g$.

2. g divide a m.c.d.(x, y): será equivalente probar que g divide a x e y.
Supongamos que g no divide a x. Entonces $x = tg + r$, $t \in \mathbb{Z}$, $0 < r < g$. Así, $r = x - tg = x - t(ax + by)$. Luego, $r = x(1 - ta) + y(-tb) = xa' + yb'$, $a', b' \in \mathbb{Z}$, $0 < r < g$, lo cual es un absurdo, pues g era el menor entero positivo verificando $g = ax + by$, $a, b \in \mathbb{Z}$.
Análogamente, probamos que g divide a y.

□

Lema 1.7. *Sean* $a, b \in \mathbb{Z}$, $b \neq 0$ *y* $a = qb + r$ *la división euclídea de* a *y* b. *Entonces* $\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r)$.

Demostración. De la definición del máximo común divisor y del Teorema 1.6, tenemos la igualdad de ideales $(\text{m.c.d.}(a, b)) = (a, b)$. Concluiremos el lema demostrando la igualdad de ideales $(a, b) = (b, r)$. Obsérvese que $(a, b) = \{na+mb$, con $n, m \in \mathbb{Z}\} = \{n(qb + r) + mb$, con $n, m \in \mathbb{Z}\} = \{(nq + m)b + nr$, con $n, m \in \mathbb{Z}\} = \{n'b + m'r$, con $n', m' \in \mathbb{Z}\} = (b, r) = (\text{m.c.d.}(b, r))$. Concluimos la igualdad de ideales principales $(\text{m.c.d.}(a, b)) = (\text{m.c.d.}(b, r))$. Además, como el máximo común divisor de dos números es un entero positivo, obtenemos la igualdad de sus generadores. □

El Lema 1.7 determina el Algoritmo de Euclides, que permite calcular el máximo común divisor de dos números enteros y que garantiza que finaliza tras un número finito de pasos.

Algoritmo 1 Algoritmo de Euclides

Entrada: $a, b \in \mathbb{Z}$ tales que $0 \leq b \leq a$ y $a = qb + r$
Salida: El máximo común divisor de a e b.

```
while b > 0 do
    (a, b) = (b, r)
end while
return a
```

Al tener este algoritmo, es natural preguntarse: ¿cuántos pasos debemos dar para obtener el máximo común divisor de dos números enteros? La respuesta fue dada por Lamé en 1844, y se basa en los llamados actualmente *números de Fibonacci*, introducidos en Europa por Leonardo de Pisa en su libro *Liber abaci* (1902), aunque con este nombre fueron llamados posteriormente por Édouard Lucas (1842-1891). De la demostración del Lema 1.7 tenemos que $\text{m.c.d.}(-a, -b) = \text{m.c.d.}(a, b)$ para todo $a, b \in \mathbb{Z}^+$. Por tanto, bastará calcular el número de pasos en el algoritmo de Euclides para $a, b \in \mathbb{Z}^+$. Daremos todos los detalles en la siguiente sección.

1.3. Fibonacci y el Teorema de Lamé

Empezamos definiendo los números de Fibonacci.

Definición 1.8. *Los números de Fibonacci son los elementos de la sucesión* $\{\mathcal{U}_n\}$, *donde* $\mathcal{U}_0 = \mathcal{U}_1 = 1$, $\mathcal{U}_{n+1} = \mathcal{U}_n + \mathcal{U}_{n-1}$, *con* $n \geq 1$.

Las siguientes propiedades de los números de Fibonacci serán necesarias posteriormente.

Proposición 1.9. *Sea $\mathcal{U}_i$ un número de Fibonacci, con $i \geq 0$. Entonces $\mathcal{U}_{i+5} > 10\mathcal{U}_i$.*

Demostración. La proposición es cierta para $i \in \{0, 1, 2\}$. Supongamos ahora $i \geq 3$. De la definición de $\mathcal{U}_i$ se tiene que $\mathcal{U}_{i+5} = 8\mathcal{U}_i + 5\mathcal{U}_{i-1}$. Probemos la desigualdad por reducción al absurdo. Supongamos que $\mathcal{U}_{i+5} \leq 10\mathcal{U}_i$, es decir, $8\mathcal{U}_i + 5\mathcal{U}_{i-1} \leq 10\mathcal{U}_i$. Por tanto, $5\mathcal{U}_{i-1} \leq 2\mathcal{U}_i = 2(\mathcal{U}_{i-1} + \mathcal{U}_{i-2})$ y $3\mathcal{U}_{i-1} \leq 2\mathcal{U}_{i-2}$, o equivalentemente $3(\mathcal{U}_{i-2} + \mathcal{U}_{i-3}) \leq 2\mathcal{U}_{i-2}$.
Así, $\mathcal{U}_{i-2} + 3\mathcal{U}_{i-3} \leq 0$, lo cual es un absurdo, pues los números de Fibonacci son no negativos. □

De la Proposición 1.9 deducimos que si consideramos dos números de Fibonacci que difieren en, al menos, cinco posiciones, el mayor de ellos tendrá al menos una cifra más que el más pequeño (cuando ambos están escritos en base diez). Más precisamente:

Corolario 1.10. *Sea $k \in \mathbb{N}\backslash\{0\}$. Si $5k + 1 \leq i < 5(k + 1) + 1$ entonces $\mathcal{U}_i$ tiene al menos $i + 1$ cifras (escrito en base diez).*

Demostración. De la Proposición 1.9 sabemos que si $5+1 \leq i < 5 \cdot 2+1$ entonces $\mathcal{U}_i$ tiene al menos 2 cifras. Si $5 \cdot 2 + 1 \leq i < 5 \cdot 3 + 1$, entonces $\mathcal{U}_i$ tiene al menos 3 cifras. En general, si $5k + 1 \leq i < 5(k + 1) + 1$, entonces $\mathcal{U}_i$ tiene al menos $k + 1$ cifras. □

Proposición 1.11. *Sea $\alpha = \frac{1+\sqrt{5}}{2}$ el número de oro. Entonces $\mathcal{U}_n \geq \alpha^{n-1}$, para todo $n \in \mathbb{N}$.*

Demostración. Obsérvese, en primer lugar, que α es solución de la ecuación $x^2 - x - 1 = 0$ y por tanto $\alpha^2 = \alpha + 1$. Procederemos a probar la proposición por inducción sobre n. Si $n = 0$, $\mathcal{U}_0 = 1 \geq \alpha^{0-1} = \alpha^{-1} = \frac{1}{\alpha}$, pues $\alpha \geq 1$. En el caso de $n = 1$, se tiene que $\mathcal{U}_1 = 1 \geq \alpha^0 = 1$. Para $n = 2$, $\mathcal{U}_2 = 2 \geq \alpha$, lo cual es cierto, pues $2 > \frac{1+\sqrt{5}}{2}$ (de no serlo, tendríamos que $4 < 1 + \sqrt{5}$, y esto es un absurdo). Supongamos cierta la proposición para todo $0 \leq k < n$ y vamos a demostrarla para $n \geq 3$. Por hipótesis de inducción, tenemos $\mathcal{U}_n = \mathcal{U}_{n-1} + \mathcal{U}_{n-2} \geq \alpha^{n-2} + \alpha^{n-3} = \alpha^{n-3}(\alpha + 1)$ y como se verificaba que $\alpha^2 = \alpha + 1$, se tiene que $\alpha^{n-3}(\alpha + 1) = \alpha^{n-3}\alpha^2 = \alpha^{n-1}$. □

Diferentes matemáticos quisieron encontrar una buena cota superior para el número de iteraciones del Algoritmo de Euclides. Resaltamos, entre ellos, a cuatro matemáticos franceses del siglo XIX. Denotemos por $E(u, v)$ al número de iteraciones de la división euclídea de u entre v, donde $u > v > 0$.

Antoine-André-Louis Reynaud, probó en [13, Página 34, Nota 60] que $E(u, v) \leq v$. En efecto, en el Algoritmo de Euclides, como poco, el resto irá disminuyendo cada vez en una unidad. Si en cada iteración del algoritmo el

resto baja exactamente una unidad con respecto al resto anterior, tendríamos un resto inicial $r = v - 1$, y acabaríamos al llegar a un resto $r' = 0$.

Aunque en la actualidad nos puede parecer trivial, fue importante, dado que se trató del primer análisis que se realizó, de forma explícita, al Algoritmo de Euclides. Esto fue lo que dio lugar a que, más tarde, fuesen apareciendo otras cotas mejoradas. Entre ellas, una dada por el propio Reynaud en 1821 (ver [14, Sección 27, página 367]), quien afirmaba que $E(u, v) \leq \frac{v}{2}$. Esta cota es falsa para el Algoritmo de Euclides presentado, puesto que, por ejemplo, $E(3, 5) = 3$. Sin embargo, dicha cota fue propuesta por Reynaud para una pequeña modificación del Algoritmo de Euclides. La modificación consiste en que el algoritmo debe terminar inmediatamente cuando se encuentran dos restos consecutivos que difieren en una unidad. Ello es debido a que si la diferencia entre dos restos consecutivos de la división de u entre v es igual a uno, entonces por la Identidad de Bézout tenemos que dichos restos son coprimos y aplicando el Lema 1.7 concluimos que u y v también lo son. Incluso para esta modificación del algoritmo, la cota $E(u, v) \leq \frac{v}{2}$ es incorrecta, puesto que el algoritmo modificado para los números 5 y 3 consta de dos divisiones: $5 = 1 \cdot 3 + 2$ y $3 = 1 \cdot 2 + 1$. La cota correcta para el algoritmo modificado sería $E(u, v) \leq \frac{v}{2} + 2$. En efecto, supongamos $u = a_{n+1} > v = a_n > 0$ y que el algoritmo de Euclides modificado de la división de u entre v tiene n pasos:

$$\begin{aligned} a_{n+1} &= q_n a_n + a_{n-1} \\ a_n &= q_{n-1} a_{n-1} + a_{n-2} \\ &\vdots \\ a_3 &= q_2 a_2 + a_1 \\ a_2 &= q_1 a_1 + a_0 \end{aligned} \tag{1.1}$$

donde $a_0 \geq 0$, $1 = a_1 - a_0$ y $a_i \geq a_{i-1} + 2$ para todo $2 \leq i \leq n - 1$. Por tanto $1 = a_1 - a_0 < 2 \leq a_2 \leq a_3 - 2 \leq a_4 - 2 \cdot 2 \leq \cdots \leq a_i - (i - 2) \cdot 2 \leq \cdots \leq a_{n-1} - (n - 3) \cdot 2$, es decir, $1 < a_n - 2n + 6$, y $2n \leq a_n + 4$, concluyendo que $n \leq \frac{a_n}{2} + 2$.

Émile Léger, en [10] y mediante el uso del desarrollo en fracciones continuas, hizo la siguiente observación, que aquí escribimos en función de los números de Fibonacci.

Proposición 1.12. *Sea n un número natural no nulo. El menor par de números naturales u, v tales que $u > v > 0$ y $E(u, v) = n$ son $u = \mathcal{U}_{n+1}$ y $v = \mathcal{U}_n$.*

Demostración. Consideremos a_n, a_{n+1} dos números enteros tales que $a_{n+1} > a_n > 0$ y $E(a_{n+1}, a_n) = n$. Supongamos que el Algoritmo de Euclides de a_{n+1} y a_n es:

$$
\begin{aligned}
&a_{n+1} = a_n m_n + a_{n-1}, \text{ con } 0 < a_{n-1} < a_n \\
&a_n = a_{n-1} m_{n-1} + a_{n-2}, \text{ con } 0 < a_{n-2} < a_{n-1} \\
&\vdots \\
&a_3 = a_2 m_2 + a_1, \text{con } 0 < a_1 < a_2 \\
&a_2 = a_1 m_1.
\end{aligned}
$$

El par de números a_{n+1}, a_n será mínimo cuando $m_n = m_{n-1} = m_{n-2} = \cdots = m_2 = a_1 = 1$ y $m_1 = 2$ (de tener $m_1 = 1$ se daría $a_1 = a_2$ por lo que no tendríamos n iteraciones, sino $n-1$). Así, $a_1 = 1$, $a_2 = 2$, $a_3 = 3$, $a_4 = 5$, $a_5 = 8$, $a_6 = 13$ y en general $a_k = a_{k-1} + a_{k-2}$, por tanto a_k es el k-ésimo número de Fibonacci. □

Pierre-Joseph-Étienne Finck, analizando el Algoritmo de Euclides, probó lo siguiente en [6, páginas 353-355]:

Lema 1.13. *Sean $u, v \in \mathbb{N}$, $u > v > 0$ y $u = qv + r$ la división euclídea de u entre v. Entonces $r < \frac{u}{2}$ y $r \leq \frac{u-1}{2}$.*

Demostración. Para demostrar la primera desigualdad distinguimos tres casos :

- Si $v = \frac{u}{2}$, entonces $u = 2v$ y como $u > 0$ se obtiene que $q = 2$ y $r = 0 < \frac{u}{2}$.
- Si $v > \frac{u}{2}$, entonces $2v > u$ y de aquí $q = 1$ y $r = v - u > \frac{u}{2} - u = \frac{u}{2}$.
- Si $v < \frac{u}{2}$, entonces $r < v < \frac{u}{2}$.

Para demostrar la segunda desigualdad supongamos, por reducción al absurdo, que $r > \frac{u-1}{2}$. Así, $2r + 1 > u$ y utilizando la desigualdad ya probada tenemos que $2r + 1 > u > 2r$, lo cual es un absurdo, pues $u \in \mathbb{N}$. □

Proposición 1.14. *Sean $u, v \in \mathbb{Z}^+$ tales que $u > v$. Entonces $E(u, v) \leq 2n$, donde $n = max\{i : 2^i \leq v + 1\}$.*

Demostración. Sean $u, v \in \mathbb{Z}^+$ tales que $u > v$. Renombremos $u = A$, $v = B$ y supongamos que el Algoritmo de Euclides de A y B es de la forma:

$$
\begin{aligned}
&A = q_0 B + B_1, \\
&B = q_1 B_1 + B_2, \\
&B_1 = q_2 B_2 + B_3, \\
&\vdots \\
&B_{s-2} = q_{s-1} B_{s-1} + B_s,
\end{aligned}
$$

donde $A > B > B_1 > \ldots > B_s = 0$. Con esta notación, $E(u, v) = E(A, B) = s$. Por el Lema 1.13, se cumple que:

$$B_1 < \tfrac{A}{2} \;\; y \;\; B_1 \leq \tfrac{A-1}{2},$$

$$B_2 < \tfrac{B}{2} \;\; y \;\; B_2 \leq \tfrac{B-1}{2},$$

$$B_3 < \tfrac{B_1}{2} < \tfrac{A}{2^2} \;\; y \;\; B_3 \leq \tfrac{B_1-1}{2} \leq \tfrac{\frac{A-1}{2}-1}{2} = \tfrac{A-1-2}{2^2},$$

$$B_4 < \tfrac{B_2}{2} < \tfrac{B}{2^2} \;\; y \;\; B_4 \leq \tfrac{B_2-1}{2} \leq \tfrac{\frac{B-1}{2}-1}{2} = \tfrac{B-1-2}{2^2},$$

$$\vdots$$

$$B_{2n-1} \leq \tfrac{A-1-2-\ldots-2^{n-1}}{2^n},$$

$$B_{2n} \leq \tfrac{B-1-2-\ldots-2^{n-1}}{2^n}.$$

Probemos por inducción que $1+2+2^2+\cdots+2^{n-1} = 2^n-1$ para $n \in \mathbb{Z}\setminus\{0\}$. Si $n=1$, se tiene que $2^0 = 1 = 2^1-1$. Supongámoslo cierto para n, y demostremos que se verifica para $n+1$. Esto es, $1+2+\ldots+2^{n-1}+2^n = (1+2+\ldots+2^{n-1})+2^n = 2^n-1+2^n = 2\cdot 2^n - 1 = 2^{n+1}-1$.

Con esto, nos queda que:

$$B_{2n-1} \leq \tfrac{A-1-2-\ldots-2^{n-1}}{2^n} = \tfrac{A-2^n+1}{2^n},$$

$$B_{2n} \leq \tfrac{B-1-2-\ldots-2^{n-1}}{2^n} = \tfrac{B-2^n+1}{2}.$$

Distinguiremos, entonces, dos casos:

- Si $E(A,B) = s = 2n$, entonces $B_s = 0$, o equivalentemente, $B_{2n} = 0$. Así, teniendo en cuenta que $B_{2n} \leq \frac{B-2^n+1}{2^n}$, se obtiene que $0 \leq \frac{B-2^n+1}{2^n}$. Esto es, $0 \leq B-2^n+1$ y de aquí $2^n \leq B+1$.
- Si $E(A,B) = s = 2n-1$, entonces $B_s = 0$, o equivalentemente, $B_{2n-1} = 0$. De aquí, $B_{2n-2} \geq 1$ pero $B_{2n-2} = B_{2(n-1)} \leq \frac{B-2^{n-1}+1}{2^{n-1}}$. Así, $\frac{B-2^{n-1}+1}{2^{n-1}} \geq B_{2n-2} \geq 1$. Esto es, $B-2^{n-1}+1 \geq 2^{n-1}$ y por tanto $B+1 \geq 2\cdot 2^{n-1} = 2^n$.

□

Obsérvese que la cota de Finck mejora, considerablemente, la cota de Reynaud pues, por ejemplo, si $u = 89$ y $v = 55$, la cota de Reynaud nos da $E(89,55) \leq \frac{55}{2}+2 = \frac{59}{2}$, mientras que para Finck $E(89,55) \leq 12$. Ahora bien, **Gabriel Lamé** mejoró la cota de Finck, tal y como muestra el siguiente teorema.

Teorema 1.15 (Teorema de Lamé). *El número de divisiones necesarias en el Algoritmo de Euclides, para la obtención del máximo común divisor de dos enteros, no excede de 5 veces el número de dígitos del más pequeño de los dos (cuando este número está escrito en base decimal).*

Demostración. Sean a_n, a_{n+1} dos números naturales con $a_n < a_{n+1}$. Supongamos que sean necesarias exactamente n iteraciones del Algoritmo de Euclides

para a_n y a_{n+1}. De la Proposición 1.12, tenemos que el menor par de números naturales cuya división requiere n pasos son los dos números de Fibonacci consecutivos $\mathcal{U}_n, \mathcal{U}_{n+1}$. Por tanto, $a_n \geq \mathcal{U}_n$. Supongamos que a_n tiene k cifras, escrito en base diez. Debemos demostrar que $n \leq 5k$.

Supongamos, por reducción al absurdo, que $n > 5k$. Por tanto, $n \geq 5k+1$, y aplicando el Corolario 1.10 tenemos que $\mathcal{U}_n$ tiene al menos $k+1$ cifras (escrito en base diez), y por tanto $a_n \geq \mathcal{U}_n$ tiene al menos $k+1$ cifras (escrito en base diez), lo que es un absurdo. □

Si retomamos el caso en que $u = 89$ y $v = 55$, la cota de Lamé nos dice que $E(89, 55) \leq 5 \cdot 2 = 10$, lo que mejora la cota de Finck. Por otra parte, si $u = 144$ y $v = 89$, la cota de Lamé nos dice que $E(144, 89) \leq 5 \cdot 2$, y en este caso se alcanza la igualdad.

La prueba que se presenta en el Teorema 1.15 no es la original de Lamé, sino la dada en [8, página 443]. Ambas usan las mismas ideas, pero la presentada es más corta que la original.

A continuación mostraremos otra prueba del Teorema de Lamé (Teorema 1.15) utilizando la Proposición 1.11.

Sean a_n, a_{n+1} dos números naturales con $a_n < a_{n+1}$ y $\alpha = \frac{1+\sqrt{5}}{2}$ el número de oro. Supongamos que sean necesarias exactamente n iteraciones del Algoritmo de Euclides para a_n y a_{n+1}. De la Proposición 1.12, tenemos que el menor par de números naturales cuya división requiere n pasos son los dos números de Fibonacci consecutivos $\mathcal{U}_n$, $\mathcal{U}_{n+1}$. Por tanto, $a_n \geq \mathcal{U}_n$ y a su vez, por el Teorema 1.11, $\mathcal{U}_n \geq \alpha^{n-1}$. Como estamos interesados en las cifras de a_n en base 10, aplicamos $\log_{10}$. Así, $\log_{10} a_n \geq \log_{10} \mathcal{U}_n \geq \log_{10} \alpha^{n-1}$ y deducimos que:

$$\log_{10} a_n \geq (n-1) \cdot \log_{10} \alpha. \tag{1.2}$$

Por otra parte, se tiene que $(\frac{1+\sqrt{5}}{2})^5 = (\frac{5+5\sqrt{5}}{10})^5 = (\frac{5+\sqrt{125}}{10})^5 > (\frac{5+11}{10})^5 = \frac{16^5}{10^5} = \frac{1024^2}{10^5} > \frac{1000^2}{10^5} = 10$; y obtenemos que $5 \log_{10} \frac{1+\sqrt{5}}{2} > 1$, o equivalentemente, $\log_{10} \frac{1+\sqrt{5}}{2} > \frac{1}{5}$. Aplicando esta desigualdad a (1.2), tenemos:

$$\log_{10} a_n > (n-1)\frac{1}{5}. \tag{1.3}$$

Ahora, suponiendo que a_n tiene exactamente k cifras, se verifica que $a_n < 10^k$. De aquí,

$$\log_{10} a_n < k. \tag{1.4}$$

Utilizando (1.3) y (1.4), se obtiene que $\frac{n-1}{5} < \log_{10} a_n < k$, es decir, $n - 1 < 5k$, o equivalentemente, $n \leq 5k$, lo que prueba el Teorema de Lamé (Teorema 1.15).

Dado un algoritmo es natural preguntarse si es posible ejecutarlo en la práctica. Por tanto, debemos preocuparnos por los recursos requeridos por un

algoritmo. La manera en que éstos dependen de la *entrada* se llama *complejidad del algoritmo* y su estudio se conoce como *teoría de la complejidad*. En particular, se estudia el aspecto temporal de la complejidad, es decir, el tiempo que se tarda en llevar a cabo el procedimiento. Si A es un algoritmo e I es una entrada para A, entonces el *tiempo de ejecución* de A sobre I se define como el número de instrucciones elementales que se realizan cuando A se aplica a I. La función del tiempo de ejecución del algoritmo asocia a cada $n \in \mathbb{N}$ el tiempo de ejecución más alto de A en una entrada de longitud n. Dicho número se denotará $s(n)$. El valor preciso de $s(n)$ depende de lo que entendamos exactamente por instrucción elemental, pues ésta a su vez depende del modelo de máquina utilizado. Sin embargo, lo importante será que tal operación se pueda terminar dentro de una cierta cantidad fija de tiempo, generalmente no más que la fracción más pequeña de un segundo.

Usualmente se evalúa la eficiencia de un algoritmo usando la función de su tiempo de ejecución, pero hemos visto que depende de las operaciones elementales y estas a su vez del modelo de máquina usado. Además, en vista de los rápidos avances tecnológicos, se considera que una medida de eficiencia que sea significativa más allá del estado de la tecnología informática debería tener las siguientes propiedades:

1. No debe distinguir entre funciones de tiempo de ejecución que difieren a lo sumo por una constante multiplicativa (ya que tal diferencia podría resultar simplemente de un cambio en el modelo o en la implementación de la máquina).
2. Debe limitarse a conclusiones sobre el comportamiento del algoritmo para entradas suficientemente grandes.

El concepto matemático de *crecimiento asintótico de una función* satisface ambas propiedades.

Definición 1.16. *Sean $f, g : \mathbb{N} \to \mathbb{R}$ dos aplicaciones. Diremos que f crece asintóticamente más rápido que g para $n \to \infty$, y escribimos $f(n) = \mathcal{O}\big(g(n)\big)$ si existe una constante $C > 0$ tal que $|f(n)| \leq C|g(n)|$ para n suficientemente grande (es decir, que existe $N \in \mathbb{N}$ tal que la desigualdad se da para todo $n \in \mathbb{N}$, $n \geq N$).*

Diremos que un algoritmo es *eficiente* si su función de tiempo de ejecución $s(n)$ es polinomial, es decir, $s(n) = \mathcal{O}(n^k)$ para cierto $k \in \mathbb{N} \setminus \{0\}$. Obsérvese que el nombre es debido a que si $P(x) = a_0 + a_1 x + \ldots a_d x^d \in \mathbb{Z}[x]$, entonces para todo $n \in \mathbb{N}$ se tiene que $P(n) = a_0 + a_1 n + \ldots + a_d n^d \leq (a_0 + \ldots + a_d) n^d$, es decir, $P(n) = \mathcal{O}(n^d)$.

Si u, v son dos enteros positivos tales que $u > v$, entonces el Teorema de Lamé (Teorema 1.15) afirma que $E(u, v) \leq 5v$. Por tanto, $E(u, v) = \mathcal{O}(v)$ y concluimos que el algoritmo de la división euclídea es eficiente.

2

Aritmética modular y polinomios ciclotómicos

Recordemos la siguiente relación binaria, que es una relación de equivalencia. Sean $x, y \in \mathbb{Z}$ y $n \in \mathbb{N}$, entonces $x \equiv y \pmod{n}$ si y sólo si, $x - y \in (n)$, donde (n) es el ideal generado por n. Teniendo en cuenta esta relación, consideraremos el conjunto cociente:

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \ldots, [n-1]_n\}, \text{ donde } [a]_n = \{b \in \mathbb{Z} \text{ tales que } b \equiv a \pmod{n}\}.$$

El conjunto $\mathbb{Z}/n\mathbb{Z}$, con la suma y el producto definidos como $[a]_n + [b]_n = [a+b]_n$ y $[a]_n \cdot [a]_n = [ab]_n$ para $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$, es un anillo conmutativo y unitario. Veamos cómo se caracterizan sus unidades.

Teorema 2.1. *Sean $n \in \mathbb{Z}$, $n > 1$ y $[a]_n \in \mathbb{Z}/n\mathbb{Z}$. Entonces $[a]_n$ es una unidad en $\mathbb{Z}/n\mathbb{Z}$ si y sólo si,* m.c.d.$(a, n) = 1$.

Demostración. Para la implicación directa, como $[a]_n$ es unidad, existe $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ tal que $[a]_n \cdot [b]_n = [1]_n$. Es decir, $[ab]_n = [1]_n$, lo que significa que $ab \equiv 1 \pmod{n}$, o equivalentemente, $ab - 1 \in (n)$. Por tanto, existe $q \in \mathbb{Z}$ tal que $ab - 1 = qn$. De aquí, $1 = ab - qn$ con $q \in \mathbb{Z}$, y $1 =$ m.c.d.(a, n).

Para el recíproco, suponemos que m.c.d.$(a, n) = 1$. Por la identidad de Bézout, existen $r, s \in \mathbb{Z}$ tales que $1 = ra + sn$. Aplicando clases módulo n, tenemos $[1]_n = [ra + sn]_n = [ra]_n + [sn]_n = [ra]_n = [r]_n \cdot [a]_n$. Luego $[a]_n$ es una unidad de $\mathbb{Z}/n\mathbb{Z}$ y $[r]_n$ es su inverso. □

Denotaremos por $(\mathbb{Z}/n\mathbb{Z})^*$ al conjunto de las unidades de $\mathbb{Z}/n\mathbb{Z}$.

Procederemos a enunciar, y demostrar, algunos teoremas que serán útiles en el desarrollo posterior de esta memoria.

Teorema 2.2 (Pequeño Teorema de Fermat). *Si $a \in \mathbb{Z}$ y p primo tales que* m.c.d.$(a, p) = 1$, *entonces $a^{p-1} \equiv 1 \pmod{p}$.*

Demostración. Se tiene que p es primo, por lo que $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{[0]_p\} = \{[1]_p, \ldots, [p-1]_p\}$. Además, si $[a]_p \in \mathbb{Z}/p\mathbb{Z}$ y m.c.d.$(a,p) = 1$, entonces $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^*$.

De esto, $[1]_p[a]_p, \ldots, [p-1]_p[a]_p \in (\mathbb{Z}/p\mathbb{Z})^*$, y como $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^*$, se tiene que $[a]_p$ es cancelable. Luego $[a]_p[m]_p \neq [a]_p[n]_p$, con $m, n \in \{1, \ldots, p-1\}$, $m \neq n$.
Por tanto, $\{[1]_p, \ldots, [p-1]_p\} = \{[a]_p[1]_p, \ldots, [a]_p[p-1]_p\}$.
Esto nos lleva a que $[1]_p \cdots [p-1]_p = [a]_p[1]_p \cdots [a]_p[p-1]_p = [1]_p \cdots [p-1]_p[a]_p \cdots [a]_p$ y por tanto $[1]_p = [a]_p^{p-1} = [a^{p-1}]_p$. Concluimos entonces que $1 \equiv a^{p-1} \pmod{p}$. □

Teorema 2.3. *Sean p un número primo y $a \in \mathbb{Z}$. Se tiene que $a^2 \equiv 1 \pmod{p}$ si y sólo si $a \equiv 1 \pmod{p}$ o bien $a \equiv p-1 \pmod{p}$.*

Demostración. Supongamos que $a \equiv 1 \pmod{p}$ o bien $a \equiv p-1 \pmod{p}$. Si $a \equiv 1 \pmod{p}$, entonces $a^2 \equiv 1 \pmod{p}$. Por otra parte, si $a \equiv p-1 \pmod{p}$, se tiene que $a^2 \equiv p^2 - 2p + 1 \equiv 1 \pmod{p}$.

Recíprocamente, si $a^2 \equiv 1 \pmod{p}$, se tiene que $a^2 - 1 \equiv 0 \pmod{p}$. Esto es, $(a-1)(a+1) \equiv 0 \pmod{p}$ y teniendo en cuenta que p es primo y $\mathbb{Z}/p\mathbb{Z}$ es un dominio de integridad, tendrá que darse alguno de los siguientes casos:

- $a - 1 \equiv 0 \pmod{p}$, por lo que $a \equiv 1 \pmod{p}$.
- $a + 1 \equiv 0 \pmod{p}$, esto es $a \equiv -1 \equiv p-1 \pmod{p}$.

□

Teorema 2.4 (Teorema de Wilson). *Si p es un número primo, entonces $(p-1)! \equiv -1 \pmod{p}$.*

Demostración. Probemos, en primer lugar, que $1 \cdot 2 \cdots (p-2) \equiv 1 \pmod{p}$.

Sabemos que $(\mathbb{Z}/p\mathbb{Z})^* = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$. Si consideramos $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^*$, con $[1]_p \neq [a]_p \neq [p-1]_p$, es decir, $a \not\equiv 1 \pmod{p}$, $a \not\equiv p-1 \pmod{p}$, entonces por el Teorema 2.3 se tiene que $[a]_p^{-1} \neq [a]_p$. Así, $2 \cdots (p-2) \equiv 1 \pmod{p}$. De aquí se tendrá que $(p-1)! \equiv 1 \cdot 2 \cdots (p-2) \cdot (p-1) \equiv p-1 \pmod{p}$ y a su vez $p - 1 \equiv -1 \pmod{p}$. □

Teorema 2.5 (Teorema Chino del Resto). *Sean $m, n \in \mathbb{Z}^+$, tales que* m.c.d.$(m,n) = 1$. *Entonces:*

$$\begin{aligned} f\colon \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ [x]_{mn} &\longmapsto f([x]_{mn}) := ([x]_m, [x]_n) \end{aligned} \tag{2.1}$$

es una aplicación biyectiva.

Demostración. Se demuestra sin dificultad que f es una aplicación. Además, como $card(\mathbb{Z}/mn\mathbb{Z}) = card(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = mn$, y este número es finito, bastará con probar que f es una función sobreyectiva para tener la biyectividad.

Sea $z = ([x]_m, [y]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Debemos encontrar $[w]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$ tal que $f([w]_{mn}) = ([x]_m, [y]_n)$.
Por hipótesis, m.c.d.$(m, n) = 1$, por lo que podemos aplicar la Identidad de Bézout. Esto es, existen $r, s \in \mathbb{Z}$ tales que $1 = rm + sn$. Multiplicando por x e y, obtenemos:

$$\left.\begin{array}{l} x = rmx + snx \\ y = rmy + sny \end{array}\right\}. \tag{2.2}$$

De aquí, nos queda:

$$\begin{aligned} [x]_m &= [rmx + snx]_m = [rmx]_m + [snx]_n = [snx]_m, \\ [y]_n &= [rmy + sny]_n = [rmy]_n + [sny]_n = [rmy]_n \end{aligned}$$

Si consideramos $w := snx + rmy \in \mathbb{Z}$, entonces $f([w]_{mn}) = ([w]_m, [w]_n) = ([snx]_m, [rmy]_n) = ([x]_m, [y]_n)$. □

2.1. Residuos cuadráticos

Empezaremos esta sección definiendo el concepto de *residuo cuadrático*.

Definición 2.6. *Sean $a, m \in \mathbb{Z}$, $m > 0$ y* m.c.d.$(a, m) = 1$. *Diremos que a es un residuo cuadrático módulo m si y sólo si $x^2 \equiv a \pmod{m}$ es soluble para un entero x. Si la congruencia no tiene solución, entonces diremos que a es un no-residuo cuadrático módulo m.*

Asociados a los residuos cuadráticos, encontramos los *símbolos de Legendre y de Jacobi*.

Definición 2.7. *Sean $a, p \in \mathbb{Z}$, p primo. Definimos el símbolo de Legendre como:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{si } a \equiv 0 \pmod{p} \\ 1, & \text{si } a \text{ es un residuo cuadrático módulo } p \text{ y } a \not\equiv 0 \pmod{p} \\ -1, & \text{si } a \text{ es un no-residuo cuadrático módulo } p \text{ y } a \not\equiv 0 \pmod{p} \end{cases} \tag{2.3}$$

Se tiene entonces, que el símbolo de Legendre responde a si $a \not\equiv 0 \pmod{p}$ es, o no, un residuo cuadrático. En el caso particular de $p = 2$, el símbolo de Legendre determina si a es par o impar. En el primer caso, $\left(\frac{a}{p}\right) = 0$, mientras que en el segundo $\left(\frac{a}{p}\right) = 1$.

Veamos otra forma de calcular los símbolos de Legendre.

Teorema 2.8 (Test de Euler para residuos cuadráticos módulo un número primo impar). *Sean p un primo impar y $a \in \mathbb{Z}$ tales que* m.c.d.$(a,p) = 1$. *Se tiene que:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Demostración. Diferenciaremos tres casos.

1. Si $\left(\frac{a}{p}\right) = 0$, se tiene que p divide a a, por lo que $a \equiv 0 \pmod{p}$ y $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$.

2. Si $\left(\frac{a}{p}\right) = 1$, existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{p}$. Además se tiene por hipótesis que a y p son coprimos, por lo que x y p son coprimos. De no serlo, se tendría que m.c.d.$(x,p) = p$, es decir, p divide a x, y como $a = x^2 - \lambda p$, con $\lambda \in \mathbb{Z}$, se tendría que p divide a a, lo cual es un absurdo. Así, $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \pmod{p}$. Esto es $a^{\frac{p-1}{2}} \equiv x^{p-1} \pmod{p}$ y por el Pequeño Teorema de Fermat (Teorema 2.2) se llega a que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

3. Si $\left(\frac{a}{p}\right) = -1$, no existe solución para la congruencia $x^2 \equiv a \pmod{p}$.

Si consideramos $[m]_p \in (\mathbb{Z}/p\mathbb{Z})^*$, se tiene que $[m]_p x = [a]_p$ tiene solución y es única: $x = [m]_p^{-1}[a]_p$. Así, para cada $[m_i]_p$, con $i \in \{1, \ldots, p-1\}$ existirá un único $[n_i]_p$ tal que $[m_i]_p[n_i]_p = [a]_p$. Además, $[m_i]_p \neq [n_i]_p$ (en caso contrario, se tendría que $[m_i]_p^2 = [a]_p$ y a sería un residuo cuadrático, lo cual es un absurdo). Entonces:

$$\prod_{[i]_p \in (\mathbb{Z}/p\mathbb{Z})^*} [i]_p = [1]_p[2]_p \cdots [p-1]_p = \prod_{i=1}^{\frac{p-1}{2}} [m_i]_p[n_i]_p = \prod_{i=1}^{\frac{p-1}{2}} [a]_p = [a]_p^{\frac{p-1}{2}}. \quad (2.4)$$

Por otra parte, del Teorema de Wilson (2.4) se tiene que

$$\prod_{i=1}^{p-1} i = (p-1)! \equiv -1 \pmod{p}. \quad (2.5)$$

De (2.4) y (2.5) concluimos que $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

□

Definición 2.9. *Sean $m \in \mathbb{N}$, m impar, $a \in \mathbb{Z}$ y $m = \prod_{i=1}^{n} p_i^{t_i}$ la única factorización de m en factores primos. El símbolo de Jacobi se define como $\left(\frac{a}{m}\right) = \prod_{i=1}^{n} \left(\frac{a}{p_i}\right)^{t_i}$, donde $\left(\frac{a}{p_i}\right)$ son símbolos de Legendre y $\left(\frac{a}{1}\right) = 1$.*

Definición 2.10. *Sea $m \in \mathbb{Z}^+$ y $\chi : \mathbb{Z} \to \mathbb{C}$ una aplicación. Se dice que χ es un carácter módulo m si verifica:*

1. *Para todo $n, n' \in \mathbb{Z}$ se tiene que $\chi(nn') = \chi(n) \cdot \chi(n')$.*
2. *χ es periódica módulo m, es decir, si $a \equiv b \pmod{m}$, entonces $\chi(a) = \chi(b)$.*
3. *$\chi(n) = 0$ si y sólo si $\text{m.c.d.}(n, m) > 1$.*

Proposición 2.11. *Sea p un número primo. La aplicación*

$$\begin{aligned} \chi_p : \mathbb{Z} &\longrightarrow \mathbb{C} \\ a &\longmapsto \chi_p(a) := \left(\frac{a}{p}\right) \end{aligned}$$

es un carácter módulo p.

Demostración. Debemos verificar las tres propiedades de la Definición 2.10.

1. Sean $a, b \in \mathbb{Z}$. Diferenciemos dos casos:
   a) Si $p = 2$, se dará una de las siguientes afirmaciones.
      1) ab es par, por lo que a es par o bien b es par.
      2) ab es impar, por lo que a es impar y b es impar.

   b) Si $p \neq 2$, entonces aplicando el Teorema 2.8 tenemos que $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$ y $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p}$. Por tanto, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
2. Sean $a, b \in \mathbb{Z}$, tales que $a \equiv b \pmod{p}$. Diferenciaremos dos casos:
   - Si $p = 2$, entonces a y b son pares, o bien a y b son impares, por lo que ya se tendría.
   - Si $p \neq 2$, como $a \equiv b \pmod{p}$, se tiene que $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}$.
3. Obsérvese que $\left(\frac{a}{p}\right) = 0$ si y sólo si p divide a a. Y esto se verifica si y sólo si $\text{m.c.d.}(a, p) > 1$.

□

Corolario 2.12. *Sea m un número primo. La aplicación*

$$\begin{aligned} \chi_m : \mathbb{Z} &\longrightarrow \mathbb{C} \\ a &\longmapsto \chi_m(a) := \left(\frac{a}{m}\right) \end{aligned}$$

es un carácter módulo m.

Demostración. Sean $a, b \in \mathbb{Z}$ y $m = \prod_{i=1}^{n} p_i^{t_i}$ la única factorización de m en factores primos. Demostraremos las tres propiedades de la Definición 2.10.

1. Tenemos que $\chi_m(ab) = \left(\frac{ab}{m}\right) = \prod_{i=1}^{n}\left(\frac{ab}{p_i}\right)^{t_i}$ y por la Proposición 2.11 concluimos que $\prod_{i=1}^{n}\left(\frac{ab}{p_i}\right)^{t_i} = \prod_{i=1}^{n}\left(\left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)\right)^{t_i} = \prod_{i=1}^{n}\left(\frac{a}{p_i}\right)^{t_i}\left(\frac{b}{p_i}\right)^{t_i} = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.
2. Supongamos que $a \equiv b \pmod{m}$. Como $a \equiv b \pmod{m}$, se tiene que $a \equiv b \pmod{p_i}$. Así, $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$, y $\left(\frac{a}{m}\right) = \prod_{i=1}^{n}\left(\frac{a}{p_i}\right)^{t_i} = \prod_{i=1}^{n}\left(\frac{b}{p_i}\right)^{t_i} = \left(\frac{b}{m}\right)$.
3. Se tiene que $\left(\frac{a}{m}\right) = 0$ si y sólo si $\prod_{i=1}^{n}\left(\frac{a}{p_i}\right)^{t_i} = 0$. A su vez, esto se verifica si y sólo si existe p_i número primo tal que $\left(\frac{a}{p_i}\right) = 0$, o equivalentemente, p_i divide a a, lo cual es cierto si y sólo si existe p_i tal que $\text{m.c.d.}(a, p_i) > 1$. Por último, como p_i es un factor de m, se tendrá que esto último es cierto si y sólo si $\text{m.c.d.}(a, m) > 1$.

□

Lema 2.13 (Lema de Gauss). *Sean $a \in \mathbb{Z}^+$ y p un número primo impar tales que $\text{m.c.d.}(a, p) = 1$. Si n denota el número de enteros en el conjunto $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ cuyos restos al dividir por p son mayores que $p/2$, entonces $\left(\frac{a}{p}\right) = (-1)^n$.*

Demostración. Sean $a \in \mathbb{Z}^+$ y p un número primo impar. Suponiendo que $\text{m.c.d.}(a, p) = 1$, se tiene que ninguno de los $\frac{p-1}{2}$ enteros de S es congruente con 0 módulo p. Además, cualesquiera dos elementos distintos de S tampoco son congruentes módulo p. Sean $r_1, \ldots, r_m, s_1, \ldots, s_n$ los restos resultantes de las divisiones de cada uno de los elementos de S por p, tales que $0 < r_i < \frac{p}{2}$ y $\frac{p}{2} < s_i < p$. Se tiene que $m + n = \frac{p-1}{2}$ y los enteros $r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$ son positivos y menores que $\frac{p}{2}$.

Dado que $r_i \neq r_j$ para $i \neq j$ y $s_k \neq s_t$ para $s \neq t$, para demostrar que todos los enteros $r_1, \ldots, r_m, s_1, \ldots, s_n$ son diferentes, será suficiente con probar

que $p - s_i \neq r_j$, para cualquier $i \in \{1, \ldots, n\}$ y $j \in \{1, \ldots, m\}$. Lo haremos por reducción al absurdo. Supongamos que existen ciertos valores de i y j tales que $p - s_i = r_j$. Así, existen enteros u y v, con $1 \leq u, v \leq \frac{p-1}{2}$, verificando que $s_i \equiv ua \pmod{p}$ y $r_j \equiv va \pmod{p}$. Además, $(u+v)a \equiv s_i + r_j = p \equiv 0 \pmod{p}$. Esto significa que $u + v \equiv 0 \pmod{p}$, lo cual es un absurdo, pues $1 < u + v \leq p - 1$.

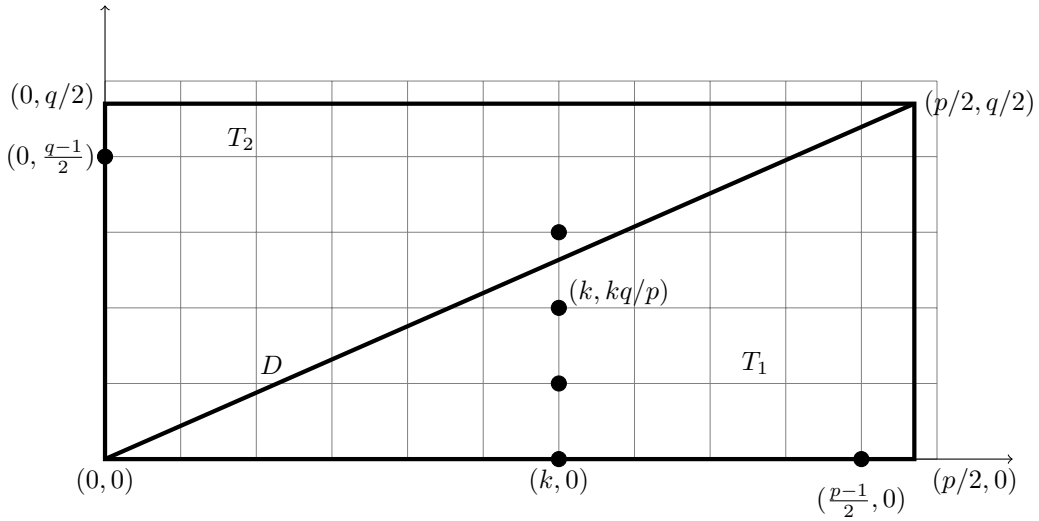
Así, tenemos $\frac{p-1}{2}$ enteros $r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$ verificando $1 \leq r_1, \ldots, r_m, p - s_1, \ldots, p - s_n < \frac{p}{2}$. De aquí, podemos concluir que dichos enteros son exactamente los enteros $1, 2, \ldots, \frac{p-1}{2}$, no necesariamente en este orden de aparición. Por tanto, el producto de todos ellos será $\left(\frac{p-1}{2}\right)! = r_1 \cdots r_m (p - s_1) \cdots (p - s_n) \equiv r_1 \cdots r_m (-s_1) \cdots (-s_n) \equiv (-1)^n r_1 \cdots r_m s_1 \cdots s_n \pmod{p}$. Y sabemos que, no necesariamente en este orden, $r_1, \ldots, r_m, s_1, \ldots, s_n$ son congruentes con $a, 2a, \ldots, \frac{p-1}{2}a$. Por tanto, $\left(\frac{p-1}{2}\right)! \equiv (-1)^n \cdot a \cdot 2a \cdots \frac{p-1}{2}a \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! \pmod{p}$. Además, como $\left(\frac{p-1}{2}\right)!$ es coprimo con p, se tiene que es cancelable en cada uno de los lados de la congruencia, por lo que se obtiene $1 \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \pmod{p}$, o equivalentemente, $(-1)^n \equiv a^{\frac{p-1}{2}} \pmod{p}$. Ahora, utilizando el Test de Euler para residuos cuadráticos módulo un número primo impar (2.8), se verifica que $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$, lo cual implica que $\left(\frac{a}{p}\right) = (-1)^n$, pues $-1 \leq \left(\frac{a}{p}\right), (-1)^n \leq 1 < p$ y $p \neq 2$. □

Proposición 2.14 (Ley de reciprocidad cuadrática). *Sean p, q primos impares. Se tiene:*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Demostración. Consideremos en el plano coordenado xy el rectángulo de vértices $(0,0)$, $(\frac{p}{2}, 0)$, $(0, \frac{q}{2})$ y $(\frac{p}{2}, \frac{q}{2})$. Denotemos por R la región de este rectángulo sin los bordes. El procedimiento consistirá en contar, de dos formas distintas, el número de puntos con coordenadas enteras que hay dentro de la región R. Como p, q son primos impares, los puntos que queremos contar serán de la forma (n, m), donde $1 \leq n \leq \frac{p-1}{2}$ y $1 \leq m \leq \frac{q-1}{2}$. Por tanto, el número total de estos puntos será $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$, ya que $\frac{p-1}{2}$ (respectivamente, $\frac{q-1}{2}$) es el mayor entero positivo menor que $\frac{p}{2}$ (respectivamente, $\frac{q}{2}$). Por otra parte, la diagonal D que pasa por los puntos $(0,0)$ y $(\frac{p}{2}, \frac{q}{2})$ tiene como ecuación $y = \frac{q}{p}x$, o equivalentemente, $py = qx$. Como m.c.d.$(p, q) = 1$, se tiene que los puntos de la diagonal D no tienen intersección con los puntos de coordenadas enteras de la región R. Denotemos por T_1 a la región de R que queda por debajo de la diagonal D, y por T_2 a la que queda por encima. Por lo que hemos visto, será suficiente con contar el número de puntos con coordenadas enteras que hay en cada uno de los triángulos T_1 y T_2.

Sea $1 \leq k \leq \frac{p-1}{2}$. El número de enteros que hay en el intervalo cerrado $[0, \frac{kq}{p}]$ es exactamente $\left\lfloor \frac{kq}{p} \right\rfloor$, donde $\lfloor x \rfloor$ denota el mayor entero menor que x. Así, hay exactamente $\left\lfloor \frac{kq}{p} \right\rfloor$ puntos con coordenadas enteras en el segmento vertical de T_1 que une $(k, 0)$ con $(k, \frac{kq}{p}) \in D$. De aquí, el número total de puntos con coordenadas enteras contenidos en el triángulo T_1 será $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$.



Análogamente, intercambiando el papel de p por el de q, se obtiene que el número de puntos con coordenadas enteras contenidos en el triángulo T_2 viene dado por $\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$.

Así, el número de puntos con coordenadas enteras contenidos en la región R vendrá dado por $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$ y además sabíamos que coincide con $\frac{(p-1)}{2}\frac{(q-1)}{2}$. Por tanto, $\sum_{k=1}^{\frac{(p-1)}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor = \frac{(p-1)}{2}\frac{(q-1)}{2}$.

Aplicando, ahora, el Lema 2.13, se tiene que $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{card(T_2)}\cdot (-1)^{card(T_1)} = (-1)^{\sum_{j=1}^{\frac{q-1}{2}}\left\lfloor \frac{jp}{q}\right\rfloor}\cdot(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{kq}{p}\right\rfloor} = (-1)^{\sum_{j=1}^{\frac{q-1}{2}}\left\lfloor \frac{jp}{q}\right\rfloor + \sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{kq}{p}\right\rfloor} = (-1)^{\frac{(p-1)(q-1)}{4}}$. □

2.2. Funciones aritméticas

Definición 2.15. *Diremos que una función f es aritmética si $f : \mathbb{Z}^+ \to \mathbb{C}$.*

Definición 2.16. *Diremos que una función f es aditiva si f es una función aritmética que verifica $f(mn) = f(m) + f(n)$, para cualesquiera $m, n \in \mathbb{Z}$ tales que* m.c.d.$(m, n) = 1$.

Definición 2.17. *Diremos que una función f es multiplicativa si f es una función aritmética verificando $f(mn) = f(m)f(n)$, para cualesquiera $m, n \in \mathbb{Z}$ tales que* m.c.d.$(m, n) = 1$.

Definición 2.18. *Sea f una función aritmética. Llamaremos función suma de f a $F : \mathbb{Z}^+ \to \mathbb{C}$, donde $F(n) = \sum_{d\in\mathbb{Z}^+;d|n} f(d)$.*

Teorema 2.19. *Si f es una función multiplicativa, entonces su función suma también es multiplicativa.*

Demostración. Sean $m, n \in \mathbb{Z}^+$ coprimos, consideramos $F(mn) = \sum_{d\in\mathbb{Z}^+;d|mn} f(d)$. Como m.c.d.$(m, n) = 1$, si d es un divisor de mn, se verifica que $d = d_1d_2$, siendo d_1, d_2 divisores de m y n, respectivamente. Así, se tiene que m.c.d.$(d_1, d_2) = 1$. De aquí, $F(mn) = \sum_{d\in\mathbb{Z}^+;d|mn} f(d) = \sum_{d_i\in\mathbb{Z}^+;d_1|m;d_2|n} f(d_1d_2)$. Además, como f es una función multiplicativa, $\sum_{d_i\in\mathbb{Z}^+;d_1|m;d_2|n} f(d_1d_2) = \sum_{d_i\in\mathbb{Z}^+;d_1|m;d_2|n} f(d_1)f(d_2) = \sum_{d_1\in\mathbb{Z}^+;d_1|m} f(d_1)\sum_{d_2\in\mathbb{Z}^+;d_2|n} f(d_2) = F(m)F(n)$. Por tanto, F es una función multiplicativa. □

2.2.1. Función de Möbius

Definición 2.20. *La función de Möbius $\mu : \mathbb{Z}^+ \to \mathbb{C}$ se define como:*

$$\mu(n) = \begin{cases} 1, & \text{si } n = 1, \\ (-1)^k, & \text{si } n \textit{ es el producto de } k \textit{ primos distintos}, \\ 0, & \text{si } n \textit{ no es libre de cuadrados}, \end{cases} \tag{2.6}$$

para todo $n \in \mathbb{Z}^+$.

Proposición 2.21. *La función de Möbius* μ *es multiplicativa.*

Demostración. Sean $m, n \in \mathbb{Z}^+$ con m.c.d.$(m, n) = 1$. Se tiene que $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ y $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$, con $p_i \neq q_j$, $i \in \{1, \dots r\}$, $j \in \{1, \dots s\}$. Si existe algún $\alpha_i > 1$, o bien algún $\beta_j > 1$, entonces m o n tiene un divisor múltiple (aparece al menos 2 veces), que también será divisor de mn. Por tanto, $\mu(mn) = \mu(m)\mu(n) = 0$.

En el caso en que $\alpha_1 = \cdots = \alpha_r = \beta_1 = \cdots = \beta_s = 1$, se verifica que $\mu(m) = \mu(p_1 \cdots p_r) = (-1)^r$, $\mu(n) = \mu(q_1 \cdots q_s) = (-1)^s$ y $\mu(p_1 \cdots p_r q_1 \cdots q_s) = (-1)^{r+s}$. □

Teorema 2.22 (Suma de Möbius). *Sea* $n \in \mathbb{Z}$. *Se tiene que:*

$$\sum_{d|n; d \in \mathbb{Z}^+} \mu(d) = \begin{cases} 1, & \text{si } n = 1, \\ 0, & \text{si } n > 1. \end{cases} \tag{2.7}$$

Demostración. Si $n = 1$ se tiene que $\displaystyle\sum_{d|n} \mu(d) = \mu(1) = 1$. Supongamos, ahora, $n > 1$. Vamos a considerar la función aritmética M, donde $M(n) = \displaystyle\sum_{d \in \mathbb{Z}^+; d|n} \mu(d)$. Se tiene, por la Proposición 2.21, que la función de Möbius es multiplicativa y aplicando el Teorema 2.19 M también lo es. De aquí, si $n = \displaystyle\prod_{i=1}^{r} p_i^{\alpha_i}$, donde $p_1, \dots, p_r$ son factores primos diferentes y $\alpha_i \in \mathbb{N}$ con $i \in \{1, \dots, r\}$, entonces $M(n) = \displaystyle\prod_{i=1}^{r} M(p_i^{\alpha_i})$. Por tanto, si determinamos $M(p_i^{\alpha_i})$, tendremos el valor de $M(n)$. Obsérvese que $M(p_i^{\alpha_i}) = \displaystyle\sum_{d|p_i^{\alpha_i}} \mu(d) = \mu(1) + \mu(p_i) + \mu(p_i^2) + \cdots + \mu(p_i^{\alpha_i}) = 1 + (-1) + 0 + \cdots + 0 = 0$. Por tanto, si $n > 1$, se tendrá que $M(n) = 0$. □

Teorema 2.23 (Fórmula de inversión de Möbius). *Sean* g *una función aritmética y* f *la función suma de* g, *es decir,* $f(n) = \displaystyle\sum_{d \in \mathbb{Z}^+; d|n} g(d)$, *entonces* $g(n) = \displaystyle\sum_{d \in \mathbb{Z}^+; d|n} f(d)\mu\Big(\frac{n}{d}\Big)$, *o equivalentemente* $\displaystyle\sum_{d \in \mathbb{Z}^+; d|n} f(d)\mu\Big(\frac{n}{d}\Big) = \sum_{d \in \mathbb{Z}^+; d|n} f\Big(\frac{n}{d}\Big)\mu(d)$.

Demostración. Si d divide a n, entonces $n = ed$, con $e \in \mathbb{Z}$ y se puede considerar $e = \frac{n}{d}$. Por tanto, $\sum_{d\in\mathbb{Z}^+;ed=n} f(d)\mu(e) = \sum_{e\in\mathbb{Z}^+;ed=n} f(e)\mu(d)$.
Debemos probar que $\sum_{d\in\mathbb{Z}^+;d|n} f(d)\mu\Big(\frac{n}{d}\Big) = g(n)$, o equivalentemente
$\sum_{d\in\mathbb{Z}^+;d|n} f\Big(\frac{n}{d}\Big)\mu(d) = g(n)$. Para ello, se tiene que $f\Big(\frac{n}{d}\Big) = \sum_{e\in\mathbb{Z}^+;e|\frac{n}{d}} g(e)$, y por esto:

$$\sum_{d\in\mathbb{Z}^+;d|n} \mu(d) f\Big(\frac{n}{d}\Big) = \sum_{d\in\mathbb{Z}^+;d|n} \Big(\mu(d) \sum_{e\in\mathbb{Z}^+;e|nd} g(e)\Big). \tag{2.8}$$

Como e divide a $\frac{n}{d}$, entonces e divide a n. Recíprocamente, cada divisor positivo de n será un número entero e, que divide a $\frac{n}{d}$ si y sólo si d divide a $\frac{n}{e}$. Luego d divide a n.

Por tanto, el coeficiente de $g(e)$ es $\sum_{d\in\mathbb{Z}^+;d|\frac{n}{e}} \mu(d)$ y aplicando el Teorema 2.7 tenemos:

$$\sum_{d\in\mathbb{Z}^+;d|\frac{n}{e}} \mu(n) = \begin{cases} 1, & \text{si } \frac{n}{e} = 1, \\ 0, & \text{si } \frac{n}{e} > 1; \end{cases} \tag{2.9}$$

y concluimos que $g(n)$ es igual a (2.8). Por tanto, $g(n) = \sum_{d\in\mathbb{Z}^+;d|n} f\Big(\frac{n}{d}\Big)\mu(d)$. □

Hemos visto la versión aditiva de la fórmula de inversión de Möbius, pero también existe una versión multiplicativa, cuya prueba es análoga a la anterior, y la expresión quedaría de la siguiente forma:

$$g(n) = \prod_{d\in\mathbb{Z}^+;d|n} f(d)^{\mu\left(\frac{n}{d}\right)} = \prod_{d\in\mathbb{Z}^+;d|n} f\Big(\frac{n}{d}\Big)^{\mu(d)}. \tag{2.10}$$

2.2.2. Función de Euler

Definición 2.24. *Sea $n \in \mathbb{Z}^+$. La función de Euler $\varphi : \mathbb{Z}^+ \to \mathbb{C}$ evaluada en n se define como el número de enteros positivos menores o iguales que n que son coprimos con él.*

Del Teorema 2.1 se tiene que $\varphi(n)$ coincide con el número de unidades de $\mathbb{Z}/n\mathbb{Z}$. Es decir, $\varphi(n) = card(\mathbb{Z}/n\mathbb{Z})^*$.

Teorema 2.25. *Si p es un número primo, entonces $\varphi(p) = p - 1$.*

Demostración. Como p es primo, el único divisor de p distinto del 1 es él mismo, y p no puede dividir a los enteros positivos menores que él. De modo que $\varphi(p) = p - 1$. □

Veamos ahora una generalización del Teorema 2.25.

Teorema 2.26. *Si p es un número primo y $\alpha \in \mathbb{N}\backslash\{0\}$, entonces $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.*

Demostración. El número de enteros positivos que hay en el intervalo $[1, p^\alpha]$ es $card([1, p^\alpha] \cap \mathbb{N}) = p^\alpha$. Consideremos, ahora, aquellos que no son coprimos con p^α, es decir, $m \in \mathbb{N}$, $m \leq p^\alpha$, con m.c.d.$(m, p^\alpha) \neq 1$. Además, como p es primo, si m y p^α no son coprimos, entonces p divide a m. Por tanto, el número de enteros positivos no coprimos con p^α será $card([1, p^\alpha] \cap (p)) = p^{\alpha-1}$. Así, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$. □

Teorema 2.27. *Sean $d, n \in \mathbb{Z}^+$. Se tiene que* $\displaystyle\sum_{d\in\mathbb{Z}^+;d|n} \varphi(d) = n.$

Demostración. Lo probaremos por inducción sobre el número de factores primos diferentes de n. Supongamos que n solo tiene un factor primo, entonces $n = p^\alpha$, con p un número primo y:

$$\begin{aligned}\sum_{d\in\mathbb{Z}^+;d|n} \varphi(d) = \sum_{d\in\mathbb{Z}^+;d|p^\alpha} \varphi(d) &= \varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^\alpha)\\ &= 1 + (p-1) + (p^2-p) + \cdots + (p^\alpha - p^{\alpha-1})\\ &= p^\alpha = n.\end{aligned}$$

Supongamos que el teorema es cierto para números enteros con k factores primos distintos. Consideramos, ahora, un entero positivo N con $k+1$ factores primos diferentes. Sea p factor primo de N y p^α la mayor potencia de p que divide a N. Podemos escribir $N = p^\alpha \cdot n$, con m.c.d.$(p, n) = 1$. Así, para cada divisor d de n, tenemos que $\{d, dp, dp^2, \ldots, dp^\alpha\}$ es un conjunto de divisores de N. Entonces, podemos escribir:

$$\begin{aligned}\sum_{d\in\mathbb{Z}^+;d|N} \varphi(d) &= \sum_{d\in\mathbb{Z}^+;d|n} \varphi(d) + \sum_{d\in\mathbb{Z}^+;d|n} \varphi(dp) + \sum_{d\in\mathbb{Z}^+;d|n} \varphi(dp^2) + \cdots + \sum_{d\in\mathbb{Z}^+;d|n} \varphi(dp^\alpha)\\ &= \sum_{d\in\mathbb{Z}^+;d|n} \varphi(d) + \sum_{d\in\mathbb{Z}^+;d|n} \varphi(d)\varphi(p) + \sum_{d\in\mathbb{Z}^+;d|n} \varphi(d)\varphi(p^2) + \cdots +\\ &+ \sum_{d\in\mathbb{Z}^+;d|n} \varphi(d)\varphi(p^\alpha)\\ &= \sum_{d\in\mathbb{Z}^+;d|n} \varphi(d)[1 + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^\alpha)]\\ &= \sum_{d\in\mathbb{Z}^+;d|n} \varphi(d) \sum_{e\in\mathbb{Z}^+;e|p^\alpha} \varphi(e) = np^\alpha = N,\end{aligned}$$

lo que finaliza la prueba del teorema. □

El siguiente teorema muestra una relación entre la función φ de Euler y la función μ de Möbius.

Teorema 2.28. *Sea $m \in \mathbb{Z}^+$. Entonces $\varphi(m) = m \sum_{d\in\mathbb{Z}^+;d|m} \frac{\mu(d)}{d}$, donde μ es la función de Möbius.*

Demostración. Sabemos, por el Teorema 2.27, que $\sum_{d\in\mathbb{Z}^+;d|m} \varphi(d) = m$. Considerando $F(m) = \sum_{d\in\mathbb{Z}^+;d|m} \varphi(d) = m$ y usando el Teorema 2.23, se obtiene $\varphi(m) = \sum_{d\in\mathbb{Z}^+;d|m} F(d)\mu\Big(\frac{m}{d}\Big) = \sum_{d\in\mathbb{Z}^+;d|m} F\Big(\frac{m}{d}\Big)\mu(d) = \sum_{d\in\mathbb{Z}^+;d|m} \frac{m}{d}\mu(d) = m \sum_{d\in\mathbb{Z}^+;d|m} \frac{\mu(d)}{d}$. □

Proposición 2.29. *La función de Euler φ es multiplicativa.*

Demostración. Sean $m, n \in \mathbb{Z}^+$ tales que m.c.d.$(m, n) = 1$. Se tiene que $\varphi(mn) = card\big((\mathbb{Z}/mn\mathbb{Z})^*\big)$. Además, como m, n son coprimos, por el Teorema 2.5 se verifica que $\mathbb{Z}/mn\mathbb{Z}$ es isomorfo a $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Por otra parte, $card\big((\mathbb{Z}/mn\mathbb{Z})^*\big) = card\big((\mathbb{Z}/m\mathbb{Z})^*\big) \times card\big((\mathbb{Z}/n\mathbb{Z}^*)\big) = \varphi(m)\varphi(n)$. Por tanto, $\varphi(mn) = \varphi(m)\varphi(n)$, cuando m.c.d.$(m, n) = 1$. □

El siguiente teorema generaliza el Pequeño Teorema de Fermat (Teorema 2.2).

Teorema 2.30 (Teorema de Euler). *Sean $a, m \in \mathbb{Z}$ tales que* m.c.d.$(a, m) = 1$. *Entonces, $a^{\varphi(m)} \equiv 1$ (mód m).*

Demostración. Supongamos que $\varphi(m) = r$. Entonces $(\mathbb{Z}/m\mathbb{Z})^* = \{[a_1]_m, \ldots, [a_r]_m\}$. Además, $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ y m.c.d.$(a, m) = 1$. Por tanto, $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^*$ y $[a]_m[a_1]_m, \ldots, [a]_m[a_r]_m \in (\mathbb{Z}/m\mathbb{Z})^*$. Dado que $[a]_m \in (\mathbb{Z}/m\mathbb{Z})^*$, tenemos que $[a]_m$ es cancelable. Luego $[a]_m[a_i]_m \neq [a]_m[a_j]_m$, para $i \neq j$.
Por tanto, $\{[a_1]_m, \ldots, [a_r]_m\} = \{[a]_m[a_1]_m, \ldots, [a]_m[a_r]_m\}$, y concluimos que $[a_1]_m \cdots [a_r]_m = [a]_m[a_1]_m \cdots [a]_m[a_r]_m = [a_1]_m \cdots [a_r]_m[a]_m \cdots [a]_m$, es decir, $[1]_m = [a]_m^r = [a^r]_m$, o equivalentemente, $1 \equiv a^r$ (mód m). Concluimos entonces que $a^{\varphi(m)} \equiv 1$ (mód m). □

2.2.3. La función ω

Definición 2.31. *Sea $m \in \mathbb{Z}^+$. La función $\omega : \mathbb{Z}^+ \to \mathbb{C}$ evaluada en m es el número de factores primos distintos que tiene m.*

Teorema 2.32. *La función ω es una función aditiva.*

Demostración. Sean $m, n \in \mathbb{Z}^+$ tales que m.c.d.$(m,n) = 1$. Se tiene que $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ y $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$, con $p_i \neq q_j$ donde $i \in \{1, \ldots, r\}$, $j \in \{1, \ldots, s\}$ y $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_s \in \mathbb{Z}^+$. De aquí, $\omega(m) = r$, $\omega(n) = s$ y se verifica que $\omega(mn) = \omega(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}) = r + s = \omega(m) + \omega(s)$. □

A continuación relacionaremos la función ω con la función μ de Möbius y con la función φ de Euler.

Lema 2.33. *Sea $m \in \mathbb{Z}$, consideramos $\alpha = card(\{d$ divisor de m verificando que $\mu(d) = 1\})$. Se tiene, entonces, que $\alpha = 2^{\omega(m)-1}$.*

Demostración. Sea $m \in \mathbb{Z}$, si consideramos los divisores no negativos d de m que no son libres de cuadrado, obtendremos $\mu(d) = 0$. Así, como queremos trabajar únicamente con aquellos divisores que son libres de cuadrado, podemos suponer que m es libre de cuadrados. La prueba de este lema se llevará a cabo por inducción. Supongamos que $\omega(m) = r$.

Si $r = 1$ se tiene que m es primo, de modo que sus únicos divisores serán 1 y m. Además, $\mu(1) = 1$ y $\mu(m) = -1$, por lo que $\alpha = 1$. Se verifica, entonces, que $\alpha = 1 = 2^{1-1} = 2^0$.

Supongamos cierto el enunciado para todo m con $r - 1$ factores primos distintos. Ahora, si consideramos m con r factores primos diferentes, se tiene que $\omega(m) = \omega(m') + 1$, donde m' tiene $r - 1$ factores primos distintos. Quedaría ver quién es α. Antes de calcularlo, es conveniente conocer la siguiente propiedad combinatoria: sea $r \in \mathbb{N}$, se tiene que $\sum_{0 \leq i \ par \leq r} \binom{r}{i} = \sum_{0 \leq i \ impar \leq r} \binom{r}{i}$ y que $\sum_{0 \leq i \leq r} \binom{r}{i} = 2^r$. Una prueba de esto se podrá encontrar en [7, páginas 100-101]. Así, si tenemos en cuenta estas propiedades y diferenciamos todos los divisores posibles de m con un número de factores primos par y menor o igual que r, se obtiene que $\alpha = \sum_{0 \leq i \ par \leq r} \binom{r}{i} = \frac{1}{2} \sum_{0 \leq i \leq r} \binom{r}{i} = \frac{1}{2} 2^r = 2^{r-1}$. Además, $2^{\omega(m)-1} = 2^{\omega(m')+1-1} = 2^{\omega(m')} = 2^{r-1}$. Por tanto, $\alpha = 2^{\omega(m)-1}$. □

Teorema 2.34. *Si $m \in \mathbb{Z}^+$, entonces $\varphi(m) \geq 2^{\omega(m)-1}$.*

Demostración. Sea p un número primo impar y e un número entero positivo. Se tiene que $\varphi(p^e) = p^{e-1}(p-1) \geq 2$. Supongamos que m tiene n factores primos diferentes, y sea $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ su descomposición en factores primos. Teniendo en cuenta que 2 podría ser un factor primo de n, concluimos que éste tendrá al menos $n - 1$ factores primos impares. Si consideramos, sin pérdida de generalidad, que $p_n = 2$, nos queda $\varphi(m) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \cdots \varphi(p_n^{\alpha_n}) \geq 2 \cdot 2 \cdots 2 \cdot 1 = 2^{n-1} = 2^{\omega(m)-1}$. □

2.3. Polinomios ciclotómicos

El contenido de esta sección ha sido consultado, en su mayor parte, de [17].

Definición 2.35. *Sea $f(x) \in \mathbb{Q}[x]$ un polinomio no constante. Diremos que $f(x)$ es reducible si se puede expresar como el producto de dos polinomios no constantes $p(x), q(x) \in \mathbb{Q}[x]$ tales que $\deg(p(x)) < \deg(f(x))$ y $\deg(q(x)) < \deg(f(x))$. En caso contrario, diremos que $f(x)$ es un polinomio irreducible.*

Se puede probar que todo polinomio no constante en $\mathbb{Q}[x]$ se puede expresar como producto de polinomios irreducibles. En particular, si consideramos a $x^m - 1$, éste tiene m ceros en $\mathbb{C}$, denominadas raíces m-ésimas de la unidad. Así, si $m > 1$, demostraremos que $x^m - 1$ se factoriza en $\mathbb{Q}[x]$, cuyos factores son llamados *polinomios ciclotómicos*. Demos una definición formal.

Definición 2.36. *Llamaremos n-ésimo polinomio ciclotómico al polinomio:*

$$\Phi_n(x) = \prod_{\xi \text{ primitiva } n\text{-ésima de la unidad}} (x - \xi) = \prod_{\text{m.c.d.}(a,n)=1} (x - \xi^a).$$

De esta definición se tiene que $\Phi_n(x)$ es mónico, además de que $deg(\Phi_n(x)) = \varphi(n)$.

Lema 2.37. *Sea $n \in \mathbb{Z}^+$, entonces:*

$$x^n - 1 = \prod_{d \in \mathbb{Z}^+; d|n} \Phi_d(x).$$

Demostración. Las raíces de $x^n - 1$ son exactamente las raíces n-ésimas de la unidad. Por otro lado, si ξ es una raíz n-ésima de la unidad y tiene orden d, entonces ξ es una raíz primitiva d-ésima de la unidad. Por tanto, ξ es raíz de $\Phi_d(x)$ y como d divide a n, se tiene que ξ es una raíz de $\prod_{d \in \mathbb{Z}^+; d|n} \Phi_d(x)$. De aquí, concluimos que $x^n - 1$ y $\prod_{d \in \mathbb{Z}^+; d|n} \Phi_d(x)$ tienen las mismas raíces, por lo que son iguales. □

Corolario 2.38. *Sea $n \in \mathbb{Z}^+$, entonces:*

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d \in \mathbb{Z}^+; d|n; d \neq n} \Phi_d(x)}.$$

Los primeros polinomios ciclotómicos son $\Phi_1(x) = x-1$, $\Phi_2(x) = \frac{x^2-1}{\Phi_1(x)} = \frac{x^2-1}{x-1} = x+1$, $\Phi_3(x) = \frac{x^3-1}{\Phi_1(x)} = x^2+x+1$, $\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = \frac{x^4-1}{x^2-1} = x^2+1$.

En particular, si $p \in \mathbb{N}$ es primo entonces $\Phi_p(x) = \frac{x^p-1}{\Phi_1(x)} = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1$.

Mostraremos a continuación otra forma de expresar al n-ésimo polinomio ciclotómico, usando la función de Möbius.

Teorema 2.39. *Sean $n \in \mathbb{Z}^+$ y μ la función de Möbius, entonces:*

$$\Phi_n(x) = \prod_{d\in\mathbb{Z}^+;d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Demostración. Sean $f, g : \mathbb{N} \to \mathbb{Q}(x)$, donde $f(n) = x^n - 1$ y $g(n) = \Phi_n(x)$. Por el Lema 2.37, se tiene que $f(n) = \prod_{d\in\mathbb{Z}^+;d|n} g(d)$, y por el Teorema 2.23 en su versión multiplicativa (ver (2.10)) obtenemos $g(n) = \prod_{d\in\mathbb{Z}^+;d|n} f\left(\frac{n}{d}\right)^{\mu(d)}$. □

Ejemplo 2.40. El polinomio ciclotómico $\Phi_6(x) = \prod_{d\in\mathbb{Z}^+;\, d|n} (x^{\frac{6}{d}} - 1)^{\mu(d)} = (x^6 - 1)^{\mu(1)}(x^3-1)^{\mu(2)}(x^2-1)^{\mu(3)}(x-1)^{\mu(6)} = \dfrac{(x^6-1)(x-1)}{(x^3-1)(x^2-1)} = x^2 - x + 1.$

Proposición 2.41. *Sea $f(x) \in \mathbb{Z}[x]$ tal que $f(x) = h(x)g(x)$, con $h(x) \in \mathbb{Z}[x]$ y con $f(x), g(x), h(x)$ mónicos. Se tiene que $g(x) \in \mathbb{Z}[x]$.*

Demostración. Consideremos $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x^r + b_{r-1}x^{r-1} + \cdots + b_0)(x^s + c_{s-1}x^{s-1} + \cdots + c_0) = h(x)g(x)$. Desarrollando el producto e igualando los coeficientes del polinomio de la izquierda con los del polinomio de la derecha, se obtiene que $a_k = \sum_{i+j=k} b_i c_j$. Así, demostremos por inducción que $c_j \in \mathbb{Z}$.

Si $j = 0$, $a_0 = b_0c_0$, y como $a_0, b_0 \in \mathbb{Z}$, $c_0 \in \mathbb{Z}$. Para $j = 1$, $a_1 = b_0c_1 + b_1c_0$, y como $a_1, b_0, c_0 \in \mathbb{Z}$ y acabamos de probar que $c_0 \in \mathbb{Z}$, se tiene que $c_1 \in \mathbb{Z}$. Supongámoslo cierto hasta c_{k-1}, y veamos qué ocurre con c_k.

Tenemos que $a_k = b_0c_k + b_1c_{k-1} + \cdots + b_kc_0$, es decir, $a_k - b_1c_{k-1} - \cdots - b_kc_0 = b_0c_k$. Y como se tenía que los coeficientes de $f(x)$ y $g(x)$ son enteros, y por hipótesis de inducción lo tenemos para los de $h(x)$ hasta el c_{k-1},se obtiene que $c_k \in \mathbb{Z}$. □

Proposición 2.42. *Los polinomios ciclotómicos tienen coeficientes enteros, es decir, $\Phi_n(x) \in \mathbb{Z}[x]$. Además $\Phi_n(0) = \pm 1$.*

Demostración. Lo demostraremos por inducción sobre n. En el caso $n = 1$, $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Para $d < n$, supongamos que $\Phi_d(x) \in \mathbb{Z}[x]$. Veamos qué ocurre con el caso n. Se tiene que $x^n - 1 = \prod_{d|n; d<n} \Phi_d(x)\Phi_n(x)$, donde $x^n - 1 \in \mathbb{Z}[x]$ y por hipótesis de inducción, $\Phi_d(x) \in \mathbb{Z}[x]$. Aplicando la Proposición 2.41, se obtiene que $\Phi_n(x) \in \mathbb{Z}[x]$. Del Teorema 2.39 deducimos que $\Phi_n(0) = \pm 1$. □

También se tiene que los polinomios ciclotómicos son irreducibles. Para una prueba de esto, ver [4, Teorema 9.1.9.].

Teorema 2.43. *Sean $n = p_1^{k_1} \cdots p_r^{k_r}$, $k_i \in \mathbb{N} \setminus \{0\}$, p_i primos, $p_i \neq p_j$, para todo $i \neq j$. Sea $n_0 = p_1 \cdots p_r$. Entonces:*

$$\Phi_n(x) = \Phi_{n_0}(x^{n_1}),$$

donde $n_1 = \frac{n}{n_0} = p_1^{k_1 - 1} \cdots p_r^{k_r - 1}$.

Demostración. Sea $D(n_0)$ el conjunto de divisores de n_0. Entonces $D(n_0) = \left\{ \prod_{j=1}^{r} p_j^{\epsilon_j},\ \epsilon_j \in \{0, 1\} \right\}$, y por el Teorema 2.39 tenemos $\Phi_{n_0}(x) = \prod_{d \in D(n_0)} (x^d - 1)^{\mu(\frac{n_0}{d})}$.

Por otra parte, los divisores e de n con $\mu(\frac{n}{e}) \neq 0$ son aquellos divisores e de n tales que $\frac{n}{e} = 1$ o $\frac{n}{e}$ es libre de cuadrados. Por tanto, $e = \prod_{j=1}^{r} p_j^{\alpha_j}$ con $k_j - 1 \leq \alpha_j \leq k_j$, y concluimos que $e = n_1 d$ con $d \in D(n_0)$. En particular tenemos que $\frac{n}{e} = \frac{n}{n_1 d} = \frac{n_0}{d}$.

Aplicando el Teorema 2.39 concluimos que $\Phi_n(x) = \prod_{e \in \mathbb{Z}^+;\ e|n;\ \mu(\frac{n}{e}) \neq 0} (x^e - 1)^{\mu(\frac{n}{e})} = \prod_{d \in \mathbb{Z}^+;\ d|n_0} (x^{n_1 d} - 1)^{\mu(\frac{n_0}{d})} = \Phi_{n_0}(x^{n_1})$. □

Corolario 2.44. *Sean $p, m, k \in \mathbb{N}$, p primo que no divide a m y $k \geq 1$. Entonces $\Phi_{mp^k}(x) = \Phi_{mp^{k-1}}(x^p) = \Phi_{mp}(x^{p^{k-1}})$.*

Demostración. Sean $n = mp^{k-1}$ y $n' := mp^k$ y escribimos $n = n_0 n_1$ y $n' = n_0' n_1'$ como en el Teorema 2.43. Entonces, aplicando dicho teorema tenemos que $\Phi_{n'}(x) = \Phi_n(x^p)$ e iterando el mismo razonamiento concluimos que $\Phi_{mp^k}(x) = \Phi_{n'}(x) = \Phi_n(x^p) = \Phi_{mp^{k-1}}(x^p) = \Phi_{mp}(x^{p^{k-1}})$. □

Corolario 2.45. *Sean $p, m, k \in \mathbb{Z}^+$, p primo que no divide a m y $k \geq 1$. Entonces $\Phi_{mp^k}(x) = \frac{\Phi_m(x^{p^k})}{\Phi_m(x^{p^{k-1}})}$.*

Demostración. Sea $n := mp^k$. Los divisores j de n con $\mu(\frac{n}{j}) \neq 0$ son los de la forma dp^k, dp^{k-1} con d divisor de m. Por tanto, aplicando el Teorema 2.39 tenemos que:

$$\begin{aligned}\Phi_n(x) &= \prod_{j\in\mathbb{N};\ j|n} (x^j-1)^{\mu(\frac{n}{j})} \\ &= \prod_{d\in\mathbb{N};\ dp^k|n;\ d|m} (x^{dp^k}-1)^{\mu(\frac{n}{dp^k})} \cdot \prod_{d\in\mathbb{N};\ dp^{k-1}|n;\ d|m} (x^{dp^{k-1}}-1)^{\mu(\frac{n}{dp^{k-1}})}.\end{aligned} \tag{2.11}$$

Obsérvese que $\frac{n}{dp^k} = \frac{m}{d}$ y como p es primo $\mu(\frac{pm}{d}) = -\mu(\frac{m}{d})$ y concluimos de (2.11) que:

$$\begin{aligned}\Phi_n(x) &= \prod_{d\in\mathbb{N};\ d|m} \left((x^{p^k})^d-1\right)^{\mu(\frac{m}{d})} \cdot \prod_{d\in\mathbb{N};\ d|m} \left(\left(x^{p^{k-1}}\right)^d-1\right)^{-\mu(\frac{m}{d})} \\ &= \Phi_m(x^{p^k})\left(\Phi_m\left(x^{p^{k-1}}\right)\right)^{-1} = \frac{\Phi_m(x^{p^k})}{\Phi_m(x^{p^{k-1}})}.\end{aligned}$$

□

En particular, deducimos del Corolario 2.45 que si p es primo y no divide a m entonces:

$$\Phi_{mp}(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)}. \tag{2.12}$$

Con un razonamiento similar concluimos que si p es primo y p divide a m, entonces:

$$\Phi_{mp}(x) = \Phi_m(x^p). \tag{2.13}$$

En general,

Proposición 2.46. *Sea $m \in \mathbb{N}$ tal que $m = q^a m_1$, con q primo y donde q no divide a m_1, entonces $\Phi_m(x) = \frac{\Phi_{m_1}(x^{q^a})}{\Phi_{m_1}(x^{q^{a-1}})}$.*

Demostración. Lo probaremos por inducción sobre a. Si $a = 1$, como q es primo y q no divide a m_1, aplicando (2.12) se tiene que $\Phi_m(x) = \frac{\Phi_{m_1}(x^q)}{\Phi_{m_1}(x)}$. Supongámoslo cierto para $a-1$, es decir, $m' = q^{a-1}m_1$ y $\Phi_{m'}(x) = \frac{\Phi_{m_1}(x^{q^{a-1}})}{\Phi_{m_1}(x^{q^{a-2}})}$. Veamos qué ocurre con el caso a. Tenemos que $m = q^a m_1 = q^{a-1}m_1 q = m'q$. Así, $\Phi_m(x) = \Phi_{m'q}(x)$ y como q es primo y q divide a m', podemos aplicar (2.13). Nos queda, entonces, que $\Phi_m(x) = \Phi_{m'q}(x) = \Phi_{m'}(x^q)$ y utilizando la hipótesis de inducción, $\Phi_{m'}(x^q) = \frac{\Phi_{m_1}((x^q)^{q^{a-1}})}{\Phi_{m_1}((x^q)^{q^{a-2}})} = \frac{\Phi_{m_1}(x^{q^a})}{\Phi_{m_1}(x^{q^{a-1}})}$. □

2.3.1. Factorización de enteros del tipo $a^n - 1$

Presentamos un método para encontrar la factorización de $a^n - 1$ en producto de primos, basado en los polinomios ciclotómicos. Del Lema 2.37 sabemos que $x^n - 1 = \prod_{d\in\mathbb{Z}^+;\ d|n} \Phi_d(x)$, $n \geq 1$. Por tanto, si $a \in \mathbb{Z}$ entonces:

$$a^n - 1 = \prod_{d\in\mathbb{Z}^+;\ d|n} \Phi_d(a), \tag{2.14}$$

y en particular si conocemos los factores primos de $\Phi_d(a)$ conoceremos la descomposición en primos de $a^n - 1$.

Por ejemplo, $2^6 - 1 = \Phi_1(2)\Phi_2(2)\Phi_3(2)\Phi_6(2) = (2-1)(2+1)(2^2+2+1)(2^2-2+1) = 3 \cdot 7 \cdot 3 = 3^2 \cdot 7$.

En general, $\Phi_d(a)$ no es primo, como muestra por ejemplo $\Phi_2(3) = 3+1 = 4$. Estudiemos, entonces, la factorización en primos de $\Phi_n(a)$.

Sea p un número primo. Si m.c.d.$(p, a) = 1$ entonces $[a]_p$ es una unidad de $\mathbb{Z}/p\mathbb{Z}$. Denotemos por $ord_p(a)$ al menor natural no nulo n tal que $a^n \equiv 1$ (mód p), es decir, al orden de $[a]_p$ como elemento del grupo $(\mathbb{Z}/p\mathbb{Z})^*$. Recordemos que si $ord_p(a) = n$ y $r \in \mathbb{N} \setminus \{0\}$ tal que $a^r \equiv 1$ (mód p) entonces r es un múltiplo de n. Del Pequeño Teorema de Fermat (Teorema 2.2)observamos que si p es primo y $ord_p(a) = n$ entonces n divide a $p-1$, es decir, $p \equiv 1$ (mód n).

Lema 2.47. *Si $p \in \mathbb{N}$ es un factor primo de $\Phi_n(a)$, entonces p no divide a a.*

Demostración. Sea $\Phi_n(x) = x^r + b_1x^{r-1} + \ldots + b_r$, con $b_r = \pm 1$. Entonces se tiene $\Phi_n(a) = a^r + b_1a^{r-1} + \ldots + b_{r-1}a + b_r$. Si p dividiera a a, entonces p dividiría a $\Phi_n(a) - (a^r + b_1a^{r-1} + \ldots b_{r-1}a) = b_r = \pm 1$ que es un absurdo. □

Lema 2.48. *Si $p \in \mathbb{N}$ es primo y $ord_p(a) = n$, entonces p divide a $\Phi_n(a)$.*

Demostración. Como $ord_p(a) = n$, entonces $a^n \equiv 1$ (mód p) y $a^d \not\equiv 1$ (mód p) para todo $d \in \mathbb{N}$, $d < n$. En particular, p divide a $a^n - 1$ pero no divide a $a^d - 1$, para todo $d \in \mathbb{N}$, $d < n$.

Del Lema 2.37 deducimos entonces que p no divide a $\Phi_d(a)$ con $d \in \mathbb{N}$, $d < n$. Pero aplicando dicho lema tenemos que $a^n - 1 = \Phi_n(a) \cdot \prod_{d\in\mathbb{Z}^+;\ d>1;\ d|n} \Phi_d(a)$. Entonces, como p divide a $a^n - 1$, p es primo y p no divide a $\prod_{d\in\mathbb{Z}^+;\ d>1;\ d|n} \Phi_d(a)$, necesariamente p divide a $\Phi_n(a)$. □

A todo número primo p verificando $ord_p(a) = n$ se le denomina *factor de Zsigmondy* de $\Phi_n(a)$, en honor al matemático Karl Zsigmondy (1867 – 1925). A dicho número p también se le denomina *factor primitivo* de $a^n - 1$.

Recordemos el *Teorema de Lagrange*, cuya prueba puede encontrarse en [11, Teorema 1.16].

Teorema 2.49 (Teorema de Lagrange). *Sea H un subgrupo de un grupo finito G, entonces el cardinal de H divide al cardinal de G.*

Lema 2.50. *Si p es un factor de Zsigmondy de $\Phi_n(a)$ entonces $p \equiv 1 \pmod{n}$.*

Demostración. Tenemos que $ord_p(a) = n$ y por el Teorema de Lagrange (Teorema 2.49) n divide al orden de $(\mathbb{Z}/p\mathbb{Z})^*$, es decir, que n divide a $p - 1$. □

Demostraremos, a continuación, que también existen factores primos de $\Phi_n(a)$ que no son factores de Zsigmondy. Necesitamos el siguiente lema.

Lema 2.51. *Sean $p, a \in \mathbb{N}$, p primo con $a \equiv 1 \pmod{p}$. Entonces:*

(1) $\frac{a^p-1}{a-1} = a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv 0 \pmod{p}$.
(2) $a^p \equiv 1 \pmod{p^2}$.
(3) *Si $p \geq 3$, entonces $a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv p \pmod{p^2}$ (y por tanto no es múltiplo de p).*

Demostración. Dado que $a \equiv 1 \pmod{p}$, entonces $a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv 1^{p-1} + 1^{p-2} + \ldots + 1 + 1 \equiv p \equiv 0 \pmod{p}$. Además, como $a^p - 1 = (a^{p-1} + a^{p-2} + \ldots + a + 1)(a - 1)$ y ambos factores son múltiplos de p, entonces $a^p - 1$ es múltiplo de p^2. A continuación demostraremos (3).

Dado que $a \equiv 1 \pmod{p}$, existe $k \in \mathbb{Z}$ tal que $a = kp + 1$, y del binomio de Newton tenemos que $a^r = (kp + 1)^r = 1^r + \binom{r}{1} kp 1^{r-1} + tp^2$, para cierto $t \in \mathbb{Z}$. Por tanto, $a^r \equiv 1 + rkp \pmod{p^2}$ y como $p - 1$ es par, entonces $\sum_{r=0}^{p-1} a^r \equiv \sum_{r=0}^{p-1}(1 + rkp) = p + kp\sum_{r=1}^{p-1} r = p + kp\frac{p(p-1)}{2} \equiv p \pmod{p^2}$. □

Recordemos que si p es primo, entonces $\Phi_p(a) = a^{p-1} + a^{p-2} + \ldots + a + 1$. Si $a \equiv 1 \pmod{p}$, entonces $ord_p(a) = 1$ y $\Phi_p(a) \equiv 1 + \ldots + 1 \equiv p \pmod{p}$, es decir, $\Phi_p(a) \equiv 0 \pmod{p}$ y el propio p es un factor primo de $\Phi_p(a)$ pero no es un factor de Zsigmundy. Esto se generaliza como sigue:

Proposición 2.52. *Sean p primo con $ord_p(a) = m$ y $n = p^k m$, con $k \geq 1$, donde p no divide a m. Entonces:*

(a) *p divide a $\Phi_n(a)$.*
(b) *Si $n \geq 3$ entonces p^2 no divide a $\Phi_n(a)$.*

Demostración. Del Teorema 2.39 sabemos que

$$\Phi_n(a) = \prod_{d\in\mathbb{Z}^+} (a^d - 1)^{\mu(\frac{n}{d})}. \tag{2.15}$$

Sea $D = \{d \in \mathbb{N},\ d \text{ divisor de } m,\ \mu(\frac{m}{d}) \neq 0\}$. Entonces los divisores j de n con $\mu(\frac{n}{j}) \neq 0$ son los de la forma dp^k y dp^{k-1} con $d \in D$.

Tenemos que m.c.d.$(m, p^k) = 1$, por tanto m divide a dp^k solo si $d = m$. En particular, si $d < m$ entonces p no divide a $a^{dp^k} - 1$. En efecto, si lo hiciera entonces $a^{dp^k} \equiv 1 \pmod 1$ y $ord_p(a) = m$ dividiría a dp^k, que sería un absurdo.

De (2.15) tenemos que:

$$\begin{aligned}
\Phi_n(x) &= \prod_{j\in\mathbb{Z}^+;\ j|n;\ \mu(\frac{n}{j})\neq 0} (x^j - 1)^{\mu\left(\frac{n}{j}\right)} \\
&= \prod_{dp^k;\ d|m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^k} - 1\right)^{\mu\left(\frac{n}{dp^k}\right)} \cdot \prod_{dp^{k-1};\ d|m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^{k-1}} - 1\right)^{\mu\left(\frac{n}{dp^{k-1}}\right)} \\
&= \prod_{d|m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^k} - 1\right)^{\mu\left(\frac{m}{d}\right)} \cdot \prod_{d|m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^{k-1}} - 1\right)^{\mu\left(\frac{pm}{d}\right)},
\end{aligned} \tag{2.16}$$

y como $\mu(\frac{m}{d}) = -\mu(\frac{pm}{d})$, entonces:

$$\begin{aligned}
\Phi_n(x) &= \frac{\displaystyle\prod_{d|m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^k} - 1\right)^{\mu\left(\frac{m}{d}\right)}}{\displaystyle\prod_{d|m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^{k-1}} - 1\right)^{\mu\left(\frac{m}{d}\right)}} \\
&= \frac{(x^n - 1)}{(x^{\frac{n}{p}} - 1)} \frac{\displaystyle\prod_{d|m;\ d\neq m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^k} - 1\right)^{\mu\left(\frac{m}{d}\right)}}{\displaystyle\prod_{d|m;\ d\neq m;\ \mu(\frac{m}{d})\neq 0} \left(x^{dp^{k-1}} - 1\right)^{\mu\left(\frac{m}{d}\right)}},
\end{aligned} \tag{2.17}$$

y por tanto

$$\Phi_n(a) = \frac{(a^n - 1)}{(a^{\frac{n}{d}} - 1)} \cdot \prod_{d\in D;\ d<m} \frac{f_d(a)}{g_d(a)},$$

donde $f_d(a)$ y $g_d(a)$ no son múltiplos de p.

Pero $a^{\frac{n}{p}} \equiv 1 \pmod p$ pues $\frac{n}{p} = mp^{k-1}$ y $ord_p(a) = m$, y aplicando el Lema 2.51 (1) tenemos que $\frac{a^n-1}{a^{\frac{n}{p}}-1}$ es múltiplo de p y por tanto $\Phi_n(a)$ también

lo es. Además, del Lema 2.51 (3) si $p \geq 3$ entonces p^2 no divide a $\frac{a^n-1}{a^{\frac{n}{p}}-1}$ y por tanto tampoco divide a $\Phi_n(a)$.

Si ahora $p = 2$ y $n > 2$, $ord_2(a) \leq 2-1$ y por tanto $m = 1$ (en particular a es impar). Entonces $n = 2^k$, $k \geq 2$ y aplicando (2.13) reiteradamente concluimos que $\Phi_{2^k}(x) = \Phi_2\left(x^{2^{k-1}}\right)$ y en particular $\Phi_n(a) = \left(a^{2^{k-1}}\right)^2 + 1$. Sea $r := a^{2^{k-1}}$, que es impar, pues a lo es. Se tiene que $r^2 \equiv 1 \pmod 4$ y $\Phi_n(a) = 1 + 1 = 2 \pmod 4$. Por tanto, $4 = p^2$ no divide a $\Phi_n(a)$. □

Corolario 2.53. *Sean p primo con $ord_p(a) = m$ y $n = p^k m$ con $k \geq 1$ y donde p no divide a m. Entonces p es el mayor factor primo de n.*

Demostración. Como $ord_p(a) = m$ entonces por el Teorema de Lagrange (Teorema 2.49) m divide a $p-1$, en particular $m \leq p-1$ y como $n = p^k m$ entonces p es el mayor factor primo de n. □

Observación 2.54. Nótese que la Proposición 2.52 (b) no se cumple si $n = 2$, pues en tal caso $m = 1$, $p = 2$ y $\Phi_2(7) = 8 = 2^3$.

Recordemos que si m divide a $p-1 = card\left((\mathbb{Z}/p\mathbb{Z})^*\right)$ entonces $card\left(\{[a]_p$ tal que $ord_p(a) = m\}\right) = \varphi(m)$, donde φ es la Phi de Euler.

Demostraremos a continuación que los factores primos de $\Phi_n(a)$ que no son Zsigmondy solo aparecen como son descritos en la Proposición 2.52, por tanto para n fijado, $\Phi_n(a)$ tiene a lo más un factor primo que no es Zsigmondy y en tal caso es el mayor de los factores primos de n.

Consideremos primero el caso especial donde $n = p$ primo. Sea q un factor primo de $\Phi_n(a)$ que no es Zsigmondy. En particular q divide a $\Phi_p(a)$ y por el Lema 2.37 entonces q divide a $a^p - 1$, es decir $a^p \equiv 1 \pmod q$. Por tanto $ord_p(a)$ divide a p. Por hipótesis, $ord_p(a) \neq p$, por tanto $ord_p(a) = 1$ y $a \equiv 1 \pmod q$, y concluimos que $\Phi_p(a) = 1 + a + \ldots a^{p-1} \equiv p \pmod q$. Pero $\Phi_p(a)$ es un múltiplo de q, y deducimos entonces que $q = p$. Por tanto, el único factor primo de $\Phi_p(a)$ que no es Zsigmondy es el propio p y es factor exactamente cuando $a \equiv 1 \pmod p$.

Podemos adaptar el mismo razonamiento para el caso general.

Teorema 2.55. *Sean $n, a \in \mathbb{N}$, $n, a \geq 2$. Sea p el mayor factor primo de n y sea $n = mp^k$, donde p no divide a m. Entonces:*

(a) *p es un factor primo de $\Phi_n(a)$ si y sólo si $ord_p(a) = m$ (en cuyo caso m divide a $p-1$).*
(b) *cualquier otro factor primo q de $\Phi_n(a)$ verifica $ord_q(a) = n$ (y por tanto $q \equiv 1 \pmod n$).*

Demostración. Sea q un factor primo de $\Phi_n(a)$ con $ord_q(a) = s < n$. Del Lema 2.37 tenemos que q divide a $a^n - 1$, es decir $a^n \equiv 1 \pmod q$. Por tanto s divide a n. También s divide a $q-1$ por el Teorema de Lagrange (Teorema 2.49). Sea

r un factor primo de $\frac{n}{s}$ y escribamos $h := \frac{n}{r}$. Entonces existe $\alpha \in \mathbb{Z}$ tal que $\frac{n}{s} = r\alpha$ y por tanto $h = \frac{n}{r} = s\alpha$ y s divide a h.

Dado que $s = ord_q(a)$ entonces $a^h \equiv 1 \pmod{q}$. Sea $c := a^h$. Del Lema 2.37 tenemos que $x^n - 1 = \prod_{d\in\mathbb{Z}^+;\ d|n} \Phi_d(x) = \prod_{d\in\mathbb{Z}^+;\ d|n;\ d|h} \Phi_d(x) \cdot \prod_{d\in\mathbb{Z}^+;\ d|n;\ d\not|h} \Phi_d(x)$, es decir, $x^n - 1 = (x^h - 1) \prod_{d\in\mathbb{Z}^+;\ d|n;\ d\not|h} \Phi_d(x) = (x^h - 1)\Phi_n(x) \prod_{d\in\mathbb{Z}^+;\ d|n;\ d\neq n;\ n\not|h} \Phi_d(x)$, en particular $\Phi_n(a)$ divide a $\frac{a^n-1}{a^h-1} = \frac{a^{hr}-1}{a^h-1} = \frac{c^r-1}{c-1} = c^{r-1} + c^{r-2} + \ldots + c + 1$. Pero $c = a^h \equiv 1 \pmod{q}$, por tanto $c^{r-1} + c^{r-2} + \ldots + c + 1 \equiv r \pmod{q}$. Además, como q divide a $\Phi_n(a)$ y $\Phi_n(a)$ divide a $c^{r-1} + c^{r-2} + \ldots + c + 1$, se tiene que $c^{r-1} + c^{r-2} + \ldots + c + 1$ es múltiplo de q y congruente con r módulo q, donde r y q son primos. Por tanto, $r = q$. Así, q es el único factor primo de $\frac{n}{s}$ y $n = sq^{k_0}$ para cierto $k_0 \in \mathbb{N}$, $k_0 \geq 1$.

Como s divide a $q - 1$, en particular $s \leq q - 1$ y q es el mayor factor primo de n, es decir, $q = p$. Por tanto, $n = sq^{k_0} = mq^k$ y $s < q$, y concluimos que $p = q$ y $s = m$; en definitiva, p es el único factor irreducible de $\Phi_n(a)$ que no es de Zsigmondy y $ord_p(a) = m$. El recíproco se concluye de la Proposición 2.52. □

Corolario 2.56. *Sea q un factor primo de $\Phi_n(a)$. Son equivalentes:*

(1) $ord_q(a) = n$.
(2) *q no divide a n.*
(3) $q \equiv 1 \pmod{n}$.

Ejemplo 2.57. Queremos factorizar $\Phi_{48}(2)$. Del Teorema 2.43 tenemos que $\Phi_{48}(x) = \Phi_6(x^8) = x^{16} - x^8 + 1$. Por tanto, $\Phi_{48}(2) = 65281$ y cualquiera de sus factores primos debe ser congruente con 1 módulo 48. El primer candidato es 97 y encontramos que $\Phi_{48}(2) = 97 \cdot 673$, y como 673 también es primo hemos factorizado $\Phi_{48}(2)$.

Lema 2.58. *Sean $n, m, p \in \mathbb{N}$ tales que p es primo que no divide a n y m es un divisor propio de n ($n \neq m$). Entonces $\Phi_n(x)$ y $x^m - 1$ no tienen una raíz común módulo p.*

Demostración. Supongamos por reducción al absurdo que a es raíz de $\Phi_n(x)$ y $x^m - 1$ módulo p. En particular, $a^m \equiv 1 \pmod{p}$. Por tanto, $[a]_p$ es unidad de $\mathbb{Z}/p\mathbb{Z}$ y aplicando el Teorema 2.1 concluimos que m.c.d.$(a, p) = 1$, es decir, p no divide a a.

Por otra parte, del Lema 2.37 tenemos que $x^n - 1 = \prod_{d\in\mathbb{N};\ d|n} \Phi_d(x) = \Phi_n(x) \prod_{d\in\mathbb{N};\ d|n;\ d<n} \Phi_d(x)$, y además $x^m - 1 = \prod_{e\in\mathbb{N};\ e|m} \Phi_e(x)$. Como m es un divisor propio de n, entonces $x^n - 1 = \Phi_n(x)(x^m - 1)g(x)$, para cierto $g(x) \in \mathbb{Z}[x]$, y como $\Phi_n(a) \equiv a^m - 1 \equiv 0 \pmod{p}$, entonces a es raíz múltiple de $x^n - 1$ módulo

p. Por tanto, a es raíz de la derivada de $x^n - 1$, es decir, $na^{n-1} \equiv 0 \pmod{p}$, lo que es un absurdo pues p es primo y no divide ni a n ni a a. □

Proposición 2.59. *Sea $n \in \mathbb{Z}^+$. Existen infinitos números primos congruentes con 1 módulo n.*

Demostración. Supongamos, por reducción al absurdo, que existe un número finito de primos $p - 1, \ldots, p_N$ congruentes con 1 módulo n. Para todo $l \in \mathbb{Z}$ escribimos $a_l := lnp_1 \cdots p_N$ y $M_l = \Phi_n(a_l)$, donde Φ_n es el n-ésimo polinomio ciclotómico. Como Φ_n es mónico, existe $l \in \mathbb{N}$ suficientemente grande tal que $M_l > 1$, y dado que $M_l \in \mathbb{Z}$ admite factorización en primos, sea p primo que divide a M_l, es decir, $M_l = \Phi_n(a_l) \equiv 0 \pmod{p}$, afirmamos que m.c.d.$(p, a_l) = 1$. En efecto, si m.c.d.$(p, a_l) \neq 1$, entonces necesariamente m.c.d.$(p, a_l) = p$ y p dividiría a a_l.

Pero si $\Phi_n(x) = x^r + b_1 x^{r-1} + \ldots + b_{r-1}x + b_r$, sabemos que $b_r = \pm 1$ y $\Phi_n(a_l) = a_l^r + b_1 a_l^{r-1} + \ldots + b_{r-1}a_l + b_r$, es decir, $\pm 1 = b_r = M_l - (a_l^r + b_1 a_l^{r-1} + \ldots + b_{r-1}a_l)$ sería múltiplo de p, que es absurdo. Obsérvese que $p \neq p_i$, $1 \leq i \leq N$, pues m.c.d.$(p, a_l) = 1$.

Por otra parte, dado que $\Phi_n(a_l) \equiv 0 \pmod{p}$, tenemos del Lema 2.37 que $a_l^n \equiv 1 \pmod{p}$ y del Lema 2.58 tenemos que $a_l^m \not\equiv 1 \pmod{p}$ para todo divisor m de n, $m < n$.

Por tanto, el orden de $[a_l]_p$ como elemento de $\left(\mathbb{Z}/p\mathbb{Z}\right)^*$ es exactamente n y por el Teorema de Lagrange (Teorema 2.49) n divide a $p - 1$, es decir, $p \equiv 1 \pmod{n}$. Por tanto, encontramos un número primo congruente con 1 módulo n que es distinto de p_i, $1 \leq i \leq N$, que es un absurdo. □

2.3.2. Factorización de enteros de la forma $a^n + 1$

Si queremos factorizar enteros de la forma $a^n + 1$ basta tener en cuenta que $a^{2n} - 1 = (a^n - 1)(a^n + 1)$, y por tanto $a^n + 1 = \frac{a^{2n}-1}{a^n-1}$, es decir, podemos factorizar los enteros de la forma $a^n + 1$ haciendo uso de la factorización de $a^{2n} - 1$ y $a^n - 1$ mostrada en la sección anterior. Por tanto, escribiendo $2n = 2^t m$ con m impar y relacionando los divisores de $2n$ con los de n se tiene que $a^n + 1 = \prod_{d|n} \Phi_{2^t d}(a)$.

Ejemplo 2.60. Si $n = 78$, entonces $2^{78} + 1 = \prod_{d|39} \Phi_{4d}(2) = \Phi_4(2)\Phi_{12}(2)\Phi_{52}(2)\Phi_{156}(2)$. Ahora, de (2.13) se tiene que $\Phi_4(2) = \Phi_2(2^2) = 2^2 + 1 = 5$. Por la Proposición 2.46, $\Phi_{12}(2) = \Phi_{2^2 3}(2) = \frac{\Phi_3(2^4)}{\Phi_3(2^2)} = \frac{(2^4)^2+2^4+1}{(2^2)^2+2^2+1} = \frac{273}{21} = 13$. De (2.13), $\Phi_{52}(2) = \Phi_{2^2 13}(2) = \Phi_{2\cdot 13}(2^2)$ y por la Proposición 2.46, $\Phi_{2\cdot 13}(2^2) = \frac{\Phi_2\left((2^2)^{13}\right)}{\Phi_2(2^2)} = \frac{2^{26}+1}{2^2+1} = 53 \cdot 157 \cdot 1613$. Por último, de la Proposición 2.46, $\Phi_{156}(2) = \Phi_{13\cdot 12}(2) = \frac{\Phi_{12}(2^{13})}{\Phi_{12}(2)} = \frac{(2^{13})^8+(2^{13})^4+1}{(2^{13})^4+(2^{13})^2+1}$ y $\Phi_{156}(2) = 13 \cdot 313 \cdot 1249 \cdot 3121 \cdot 21841$. Así, $2^{78} + 1 = 5 \cdot 13^2 \cdot 53 \cdot 157 \cdot 313 \cdot 1249 \cdot 1613 \cdot 3121 \cdot 21841$.

3

Tests de primalidad

A lo largo de este capítulo mostraremos algunos de los métodos que se utilizan para intentar determinar si un número es primo o no. Para ello, se ha tomado como referencia [12].

3.1. La criba de Eratóstenes

Uno de los métodos de identificación de números primos más antiguos que existe es *la criba de Eratóstenes*. Este, en la Antigua Grecia, quiso obtener los primeros números primos, y por ello ideó esta técnica.

El algoritmo consiste en tomar todos los enteros desde el 1 hasta un n dado. Se elabora una tabla con ellos, eliminamos el 1, pues es una unidad y por tanto no es primo, y pasamos al siguiente número disponible en la tabla, el 2. Tachamos todos sus múltiplos. Así, al volver al inicio de la tabla, el primer número que encontramos sin tachar y mayor que 2 será primo. De este modo, se tiene que 3 es primo. Repitiendo este procedimiento, Eratóstenes obtuvo todos los números primos menores o iguales que un entero n, donde $n > 1$. Pero, ¿cuántas veces habrá que realizar este procedimiento? Obsérvese que no es necesario comprobar hasta $n - 1$, sino hasta $\sqrt{n}$, pues si n tuviera un divisor mayor que $\sqrt{n}$ tendría otro más pequeño que $\sqrt{n}$ que ya habríamos detectado.

La criba de Eratóstenes no solo verifica si un número es primo o no, sino que también determina todos los primos menores que dicho número. La criba de Eratóstenes es un algoritmo determinístico, es decir, cuando empezamos con el mismo input, siempre sigue los mismos pasos y siempre da el mismo resultado. Sin embargo, no es un algoritmo eficiente pues tiene complejidad $\mathcal{O}(n \log \log n)$ (ver [16]).

Algoritmo 2 La criba de Eratóstenes

Entrada: $n \in \mathbb{N}$
Salida: Los números primos menores o iguales que n.
Consideramos una lista con todos los enteros menores o iguales que n, a excepción del 1, y la llamamos L.
$p = 2$
for $p \leq \sqrt{n}$ **do**
if $p \in L$ **then**
Asumimos que p es primo, y eliminamos sus múltiplos de la lista L.
end if
$p = p + 1$
end for
return L

3.2. Fermat y la primalidad

En el capítulo anterior hemos enunciado y probado el Pequeño Teorema de Fermat (Teorema 2.2). Este nos será de utilidad para el siguiente algoritmo que vamos a mostrar. Este consiste, principalmente, en tomar un número $n \in \mathbb{Z}$, $n \geq 2$ y $a \in \{1, \cdots, n-1\}$. Se calcula el máximo común divisor de n y a. Si es distinto de 1, significa que ambos números tienen un factor común estrictamente menor que n. Por tanto n es compuesto. En caso de que a y n sean coprimos, se procede a calcular a^{n-1} y ver si se verifica la congruencia $a^{n-1} \equiv 1 \pmod{n}$. Si no se verifica, el Pequeño Teorema de Fermat (Teorema 2.2) nos afirma que n es compuesto. Si se verifica, cabría la posibilidad de que fuese primo. Así, el algoritmo nos queda como mostramos a continuación.

Algoritmo 3 Test de Fermat

Entrada: $n \in \mathbb{Z}$, $n \geq 2$ y se escoge, aleatoriamente, $a \in \{1, \cdots, n-1\}$.
if m.c.d.$(a, n) \neq 1$ **then**
n es compuesto.
else if **then**
Calcular $a^{n-1} \pmod{n}$.
if $a^{n-1} \equiv 1 \pmod{n}$ **then**
n podría ser primo.
else if **then**
n es compuesto.
end if
end if

En este algoritmo, cuando se introduce un número n primo, éste es fácilmente identificable, por el Pequeño Teorema de Fermat (Teorema 2.2). El pro-

blema surge cuando se introduce un número compuesto. En ocasiones, tras la elección de a, el Test de Fermat nos dice que un número n compuesto podría ser primo, pues por ejemplo, m.c.d.$(8,9) = 1$ y $8^8 \equiv 1 \pmod 9$. Sin embargo, 9 no es primo, pues $9 = 3 \cdot 3$. A estos números los denominaremos *pseudo-primos con base a*. Así, es natural preguntarse por el tamaño del conjunto de bases a con respecto a las cuales un número compuesto n es un pseudo-primo.

Sea $n \in \mathbb{N}$. Al conjunto de los números enteros positivos menores que n y coprimos con n lo denotaremos por $\mathcal{CP}(n)$.

Consideremos el siguiente conjunto:

$$\mathcal{A} := \{a \in \mathcal{CP}(n) : \ a^{n-1} \equiv 1 \pmod n\}. \tag{3.1}$$

Obsérvese que si n es un número primo, entonces $\mathcal{A} = \{1, 2, \cdots, n-1\} = \mathcal{CP}(n)$.

Lema 3.1. *Sea $n \in \mathbb{N}$ compuesto, $n \geq 2$ y $\mathcal{A}$ definido como en (3.1). Si $\mathcal{A} \neq \mathcal{CP}(n)$, entonces $\mathcal{A}$ tiene a lo sumo $\frac{\varphi(n)}{2}$ elementos, donde φ denota la función de Euler.*

Demostración. Consideremos el conjunto $\bar{\mathcal{A}} = \{[a]_n \in \mathbb{Z}/n\mathbb{Z} : \ [a]_n^{n-1} = [1]_n\} \subseteq (\mathbb{Z}/n\mathbb{Z})^*$, que tiene la misma cardinalidad que $\mathcal{A}$. Obsérvese que si $n = 2$, entonces $\bar{\mathcal{A}} = \{[1]_2\}$. Además, si $n > 2$, como $[a]_n^{n-2}[a]_n = [1]_n$, se tiene que $(\bar{\mathcal{A}}, \cdot)$ es un subgrupo de $\big((\mathbb{Z}/n\mathbb{Z})^*, \cdot\big)$. Por tanto, utilizando el Teorema de Lagrange (Teorema 2.49), $card(\mathcal{A}) = card(\bar{\mathcal{A}})$ divide a $card\big((\mathbb{Z}/n\mathbb{Z})^*\big) = \varphi(n)$. De aquí, $\varphi(n) = k \cdot card(\mathcal{A})$, para algún $k \in \mathbb{N}$. Por hipótesis, $card(\mathcal{A}) < \varphi(n)$, de modo que $k \geq 2$ y se obtiene que $\mathcal{A}$ tiene a lo sumo $\frac{\varphi(n)}{2}$ elementos. □

Concluimos del Lema 3.1 que si existe una base a para la cual el número compuesto n verifica $a^{n-1} \equiv 1 \pmod n$, entonces la probabilidad de encontrarla es al menos de $\frac{1}{2}$. Ahora bien, existen números compuestos n para los cuales no existe una base a tal que $a^{n-1} \not\equiv 1 \pmod n$, son los llamados *números de Carmichael*, pues Carmichael en [3] demuestra la existencia de dichos números, y en particular que $561 = 3 \cdot 11 \cdot 17$ es el menor de ellos.

Proposición 3.2. *Todo número de Carmichael es compuesto e impar.*

Demostración. Sea n un número de Carmichael. Por definición n es un número compuesto. Demostraremos a continuación que n es impar. Como $n-1$ y n son coprimos, entonces $(n-1)^{n-1} \equiv 1 \pmod n$. Aplicando el Binomio de Newton tenemos que

$$(-1)^{n-1} \equiv \quad \pmod n. \tag{3.2}$$

Dado que n es compuesto, entonces $n > 2$ y $-1 \equiv 1 \pmod n$. De (3.2) concluimos entonces que $(-1)^{n-1} = 1$, por tanto $n-1$ es par y n es impar. □

A continuación, mostraremos una mejora del Test de Fermat, en donde los números de Carmichael no dan problemas.

Teorema 3.3 (Teorema de Fermat-Miller). *Sea p un número primo impar. Escribiremos $p-1 = d2^l$, donde $d, l \in \mathbb{N}$ y d es un número impar. Si $a \in \mathbb{Z}$ no es múltiplo de p, entonces:*

1. *Se tiene que $a^d \equiv 1 \pmod{p}$, o bien*
2. *$a^{2^i d} \equiv -1 \pmod{p}$, para algún $i \in \{0, \ldots, l-1\}$.*

Demostración. En primer lugar, denotemos $b := a^d$. Del Pequeño Teorema de Fermat (Teorema 2.2) se tiene que $b^{2^l} = a^{d2^l} = a^{p-1} \equiv 1 \pmod{p}$. Si $b \equiv 1 \pmod{p}$, se tendría ***1.*** Supongamos que $b \not\equiv 1 \pmod{p}$. Sea i el menor número de $\{0, \ldots, l-1\}$ verificando que $b^{2^{i+1}} \equiv 1 \pmod{p}$. Obsérvese que tal i existe, pues en el peor de los casos para $i = l-1$ tenemos $b^{2^{i+1}} = a^{p-1} \equiv 1 \pmod{p}$. Utilizando el Teorema 2.3, se obtiene que $b^{2^i} \equiv 1 \pmod{p}$, o bien $b^{2^i} \equiv -1 \pmod{p}$. La primera posibilidad no puede darse debido a la forma en que hemos elegido i. De modo que $b^{2^i} \equiv -1 \pmod{p}$, verificándose así ***2.*** □

Corolario 3.4. *Sea $n \in \mathbb{N}$ impar, $n > 1$ con $n-1 = d2^l$, d impar. Supongamos que existe $a \in \mathbb{N}$, $1 < a < n$ tal que $a^d \not\equiv 1 \pmod{n}$ y $a^{d2^i} \not\equiv -1 \pmod{n}$, $0 \leq i \leq l-1$. Entonces n es compuesto.*

Al número a del Corolario 3.4 se le denomina testigo de Miller para n.

Con esto, es posible formular un nuevo test de primalidad denominado *test de Miller-Rabin*, donde partiendo de un número $n \in \mathbb{N}$, $n > 1$ impar y que no sea potencia de otro número natural (pues en este caso, queda claro que n es compuesto), procederemos con $n-1 = d2^l$ y $a \in \{1, \ldots, n-1\}$. Aquí, nuevamente, descartamos el caso en que a y n no son coprimos, pues esto significa que tienen un factor común menor que n y n no sería primo. A continuación será necesario calcular $b := a^d \pmod{n}$. Si $b = 1$, no podemos descartar que sea primo. En caso de verificarse que $a^d \not\equiv 1 \pmod{n}$, habría que calcular $b, b^2, b^4, \ldots, b^{2^{l-1}} \pmod{n}$. Si ninguno de ellos es congruente con -1 módulo n, por el Teorema de Fermat-Miller (Teorema 3.3), n es compuesto. En caso contrario, n podría ser primo.

Tanto el test de Fermat como el de Miller-Rabin son probabilistas. Además, el algoritmo de Fermat-Miller es de los denominados *Monte Carlo*, es decir, su respuesta puede ser incorrecta pero con una probabilidad baja. En efecto, del Lema 3.1 sabemos que su respuesta para números compuestos puede ser correcta con probabilidad mayor o igual que $\frac{1}{2}$.

El algoritmo de Miller-Rabin queda del siguiente modo:

Algoritmo 4 Algoritmo de Miller-Rabin

Entrada: $n \in \mathbb{N}$, $n > 1$.
  if $\{n$ es par y $n > 2\}$ **or** $\{n$ es potencia de otro número natural$\}$ **then**
    n es compuesto.
  else if **then**
    Escribimos $n-1 = d2^l$ y escogemos, aleatoriamente, un número $a \in \{1, \ldots, n-1\}$.

    if m.c.d.$(a, n) > 1$ **then**
      n es compuesto.
    else if **then**
      Calculamos $b := a^d \pmod{n}$.
      if $b = 1$ **then**
        n podría ser primo.
      else if **then**
        Calculamos $b, b^2, b^4, \ldots, b^{2^{l-1}} \pmod{n}$.
        if ninguno de los números anteriores es congruente con -1 módulo n. **then**
          n es compuesto.
        else if **then**
          n podría ser primo.
        end if
      end if
    end if
  end if

Aunque este algoritmo mejora el Test de Fermat (Algoritmo 3.2), aún se sigue obteniendo, al elegir cierta base a, que determinados números compuestos podrían ser primos. A estos se les llamará *fuertemente pseudo-primos con base a*. Con esto, la pregunta que nos hacemos es: si n es compuesto, ¿cuántos números a existen haciendo de n un número fuertemente pseudo-primo?

Teorema 3.5. *Sea $n \in \mathbb{N}$ tal que $n = qr$ con $q, r > 2$, coprimos e impares, entonces existe $a \in \mathbb{N}$ tal que* m.c.d.$(a, n) = 1$ *y* $a^2 \equiv 1 \pmod{n}$ *pero verificando que* $a \not\equiv 1 \pmod{n}$ *y* $a \not\equiv -1 \pmod{n}$. *En particular, n no es fuertemente pseudo-primo con base a.*

Demostración. Del Teorema Chino del Resto (Teorema 2.5) podemos interpretar que si tenemos $n = qr$ con q, r coprimos, entonces dos enteros serán congruentes módulo n si, y sólo si, son congruentes módulo q y módulo r (es decir, si $x, y \in \mathbb{Z}$, $[x]_n = [y]_n$ si y sólo si, $[x]_q = [y]_q$ y $[x]_r = [y]_r$). Con esto, para cualesquiera $a_1, a_2 \in \mathbb{Z}$, existe $x \in \mathbb{Z}$ tal que x es congruente con a_1 módulo q y x es congruente con a_2 módulo r. En nuestro caso, podemos obtener un número a tal que m.c.d.$(a, n) = 1$, $a \equiv -1 \pmod{q}$ y $a \equiv 1 \pmod{r}$. Así, $a \not\equiv 1 \pmod{n}$, pues tendría que darse que $a \equiv 1 \pmod{q}$. Utilizando el mismo razonamiento, $a \not\equiv -1 \pmod{n}$. Por otro lado, sabemos que $a^2 \equiv 1 \pmod{q}$ y $a^2 \equiv 1 \pmod{r}$.

Por tanto, utilizando la interpretación del Teorema Chino del Resto (Teorema 2.5) que hemos visto al principio de la demostración, se obtiene que $a^2 \equiv 1 \pmod{n}$. Ahora escribimos $n = d2^l$, con d impar. Así, $d = 2m + 1$, para un $m \geq 0$. Por tanto, $a^d = (a^2)^m \cdot a \equiv a \not\equiv 1, -1 \pmod{n}$ y $a^{2d} = (a^2)^d \equiv 1 \pmod{n}$. Por definición, n no es fuertemente pseudo-primo con base a. □

Corolario 3.6. *Si n es un número de Carmichael entonces existe $a \in \mathbb{N}$ tal que n no es fuertemente pseudo-primo.*

Demostración. Basta tener en cuenta que por la Proposición 3.2 todo número de Carmichael es compuesto e impar, y por tanto verifica las hipótesis del Teorema 3.5. □

Concluimos entonces, contrariamente a lo que pasa en el Test de Fermat, que todo número de Carmichael n admite una base a que es testigo de Miller para n. Además, no existe el equivalente de los números de Carmichael para el Test de Miller-Rabin.

También se tiene:

Teorema 3.7 (Probabilidad de error en Miller-Rabin). *Sea n un número compuesto, entonces existen a lo sumo $\frac{n-1}{2}$ bases $a \in \mathcal{CP}(n)$ para los cuales n es fuertemente pseudo-primo.*

Demostración. Consideramos el conjunto $\mathcal{W}$ de todos los números $a \in \mathcal{CP}(n)$ tales que n es fuertemente pseudo-primo. En primer lugar, tengamos en cuenta que en el Algoritmo de Miller-Rabin (Algoritmo 3.2) consideramos un número n impar que no es una potencia perfecta, es decir, que $n = qr$, donde $q, r > 2$ y m.c.d.$(q, r) = 1$. Así, escribimos $n - 1 = d2^l$ y veamos qué ocurre con el mayor índice $j \leq l$ tal que $a_0^{d2^j} \not\equiv 1 \pmod{n}$, con $a_0 \in \mathcal{CP}(n)$. Además, se tiene que este índice j existe, por el Teorema 3.5. Denotemos, ahora, $k := d2^j$ y estudiemos el conjunto $\mathcal{G} := \{a \in \mathcal{CP}(n) \text{ tal que } a^k \equiv 1 \pmod{n}, \text{ o bien } a^k \equiv -1 \pmod{n}\}$.

Todo elemento $a \in \mathcal{W}$ también será elemento de $\mathcal{G}$. Además, el conjunto $\mathcal{G}$ es cerrado con el producto módulo n (es decir, si $a, b \in \mathcal{G}$, se tiene que $ab \pmod{n}$ también pertenece a $\mathcal{G}$). Tenemos que probar que existe al menos un elemento $a \in \mathcal{CP}(n)$ tal que $a \notin \mathcal{G}$. Si se verificase que $a_0^k \not\equiv -1 \pmod{n}$, como teníamos que $a_0^{d2^j} = a_0^k \not\equiv 1 \pmod{n}$, ya estaría. En el caso en que $a_0^k \equiv -1 \pmod{n}$, sabemos que el Teorema Chino del Resto (Teorema 2.5) asegura la existencia de un número $a < n$ tal que $a \equiv a_0 \pmod{q}$ y $a \equiv 1 \pmod{r}$. Así, $a^k \equiv -1 \pmod{q}$ y $a^k \equiv 1 \pmod{r}$. Con esto, podemos concluir que $a^k \not\equiv 1, -1 \pmod{n}$ y por tanto $a \notin \mathcal{G}$.

Ya hemos probado que $card(\mathcal{G}) < \varphi(n)$, donde φ denota la función de Euler, y el Teorema de Lagrange (Teorema 2.49) nos dice que $card(\mathcal{G})$ divide a $\varphi(n)$. Por tanto, $\mathcal{G}$ tiene a lo sumo $\frac{\varphi(n)}{2}$ elementos. De aquí, $card(\mathcal{W}) \leq card(\mathcal{G}) \leq \frac{\varphi(n)}{2} < \frac{n-1}{2}$. □

3.3. El Teorema de Fermat para polinomios

Nuestro siguiente objetivo será presentar el conocido como algoritmo AKS, llamado así en honor a sus autores Agrawal, Kayal y Saxena (ver [1]). Empezamos mostrando algunos resultados que nos serán de utilidad.

Lema 3.8. *Sean p un número primo y $1 \leq k \leq p-1$, entonces $\binom{p}{k} \equiv 0 \pmod{p}$.*

Demostración. Sabemos que $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ y reescribiendo esta ecuación se obtiene que $k!(p-k)!\binom{p}{k} = p!$. De aquí, se puede ver que p es divisor del segundo miembro de la igualdad, por lo que también lo será del primero. Como p es primo y los números $1, 2, \ldots, k$ son menores que p, se tiene que p no puede dividir a $k!$. Utilizando este mismo razonamiento, p tampoco puede dividir a $(p-k)!$. Por tanto, p debe dividir a $\binom{p}{k}$. □

Definición 3.9 (Polinomios congruentes módulo un entero). *Sean $n \in \mathbb{N}$, $n > 2$ y $P(x), Q(x) \in \mathbb{Z}[x]$. Diremos que $P(x), Q(x)$ son congruentes módulo n, y lo denotaremos $P(x) \equiv Q(x) \pmod{n}$ si $P(x) = Q(x)$ en $\mathbb{Z}/n\mathbb{Z}[x]$.*

Por ejemplo, $P(x) = 3x^4+7x-2$ es congruente con $Q(x) = x^4+x \pmod{2}$.
El siguiente teorema generaliza el Teorema de Fermat a polinomios.

Teorema 3.10 (Fermat para polinomios). *Sea p un número primo, entonces $\big(P(x)\big)^p \equiv P(x^p) \pmod{p}$, para cualquier polinomio $P(x) \in \mathbb{Z}[x]$.*

Demostración. Lo probaremos por inducción sobre el grado d del polinomio $P(x) \in \mathbb{Z}[x]$. En el caso $d = 0$, $P(x)$ será un polinomio constante y utilizando el *Teorema de Fermat*, ya lo tendríamos. Supongamos, ahora, que el teorema se verifica para todo polinomio $P(x) \in \mathbb{Z}[x]$ de grado, a lo sumo, d. Hay que probar que se verifica también para los de grado $d+1$. Sea $P(x) \in \mathbb{Z}[x]$ de grado $d+1$.

Sea $Q(x)$ el polinomio resultante de restar a $P(x)$ el monomio de mayor grado. Es decir, $Q(x) \in \mathbb{Z}[x]$ y existe $a \in \mathbb{Z} \setminus \{0\}$ tal que $P(x) = ax^{d+1} + Q(x)$. De aquí, se obtiene que $\big(P(x)\big)^p = \big(ax^{d+1} + Q(x)\big)^p$ y desarrollando, $\big(ax^{d+1} + Q(x)\big)^p = (ax^{d+1})^p + \left(\sum_{k=1}^{p-1} \binom{p}{k} (ax^{d+1})^k \big(Q(x)\big)^{p-k}\right) + \big(Q(x)\big)^p$.

Analicemos, uno por uno, los términos de esta última expresión. En primer lugar, $(ax^{d+1})^p = a^p(x^{d+1})^p = a^p x^{p(d+1)} = a^p(x^p)^{d+1} \equiv a(x^p)^{d+1} \pmod{p}$, por el Pequeño Teorema de Fermat (Teorema 2.2). Además, el Lema 3.8 nos dice que p divide a cada uno de los coeficientes $\binom{p}{k}$, por tanto, $\left(\sum_{k=1}^{p-1} \binom{p}{k} (ax^{d+1})^k \big(Q(x)\big)^{p-k}\right) \equiv 0 \pmod{p}$. Por último, por hipótesis de inducción, se tiene que $\big(Q(x)\big)^p \equiv Q(x^p)$. Concluimos entonces que $\big(P(x)\big)^p \equiv a(x^p)^{d+1} + 0 + Q(x^p) \pmod{p}$, es decir, $\big(P(x)\big)^p \equiv P(x^p) \pmod{p}$. □

Corolario 3.11. *Sean p un número primo, $m \in \mathbb{N}$ y $P \in \mathbb{Z}[x]$, entonces* $\Big(P(x)\Big)^{p^m} \equiv P(x^{p^m})$ (mód p).

Demostración. Lo demostraremos por inducción sobre m. Si $m = 1$, ya lo tendríamos por el Teorema de Fermat para polinomios (Teorema 3.10). Lo suponemos cierto para m, es decir, $\big(P(x)\big)^{p^m} \equiv P(x^{p^m})$ (mód p), y veamos qué ocurre con el caso $m+1$.

Se tiene que $\big(P(x)\big)^{p^{m+1}} = \big(P(x)\big)^{p^m p} = \Big(\big(P(x)\big)^{p^m}\Big)^p$. Por hipótesis de inducción, $\Big(\big(P(x)\big)^{p^m}\Big)^p \equiv \big(P(x^{p^m})\big)^p$ (mód p). Aplicando, ahora, el caso $m = 1$, se obtiene que $\big(P(x^{p^m})\big)^p \equiv P(x^{p^m p})$ (mód p), es decir, $\big(P(x^{p^m})\big)^p \equiv P(x^{p^{m+1}})$ (mód p). □

Sean $n, p \in \mathbb{N}$ con p primo. Denotemos por $m_p(n) := máx\{j \in \mathbb{N}$ tal que p^j divide a $n\}$. En particular, $p^{m_p(n)}$ divide a n pero $p^{m_p(n)+1}$ no lo divide.

Lema 3.12. *Sean $n \in \mathbb{N}$, $n \geq 2$ y p un factor primo de n. Se tiene:*

(a) $\binom{n}{p}$ *no es divisible por* $p^{m_p(n)}$.
(b) $\binom{n}{p}$ *no es divisible por* n.
(c) $\binom{n}{p^{m_p(n)}}$ *no es divisible por* p.

Demostración. Sea $i_0 := m_p(n)$. Entonces existe $r \in \mathbb{N}$ tal que $n = p^{i_0} r$ y p no divide a r. Por otra parte, $\binom{n}{p} = \frac{n!}{p!(n-p)!}$, es decir, $p!\binom{n}{p} = \frac{n!}{(n-p)!} = n(n-1)\cdots\big(n-(p-1)\big)$, o equivalentemente

$$(p-1)!\binom{n}{p} = p^{i_0-1} r(n-1)\cdots\big(n-(p-1)\big). \tag{3.3}$$

Pero p no divide a $n-i$, $1 \leq i \leq p-1$. En efecto, pues en caso contrario existiría $\lambda \in \mathbb{Z}$ tal que $n - i = \lambda p$, es decir, $i = n - \lambda p = p^{i_0} r - \lambda p$ y p dividiría a i, lo que es un absurdo pues $1 \leq i \leq p-1$. Por tanto, de la igualdad (3.3) tenemos que $m_p\left((p-1)!\binom{n}{p}\right) = m_p\Big(p^{i_0-1} r(n-1)\cdots\big(n-(p-1)\big)\Big) = i_0 - 1$ y en particular p^{i_0} no divide a $\binom{n}{p}$. Es decir, que $p^{m_p(n)}$ no divide a $\binom{n}{p}$ y concluimos el apartado (a).

Por otra parte y dado que $n = p^{i_0} r$ entonces n no divide a $\binom{n}{p}$ y concluimos el apartado (b). Demostremos a continuación el apartado (c).

Podemos escribir

$$p^{i_0}!\binom{n}{p^{i_0}} = n(n-1)\cdots\big(n-(p^{i_0}-2)\big)\big(n-(p^{i_0}-1)\big). \tag{3.4}$$

Además, si $k \in \mathbb{N}$, $k \leq p^{i_0}$ entonces $m_p(k) \leq i_0$ y como $m_p(n) = i_0$ tenemos que $m_p(n - p^{i_0} + k) = m_p(p^{i_0}r - p^{i_0} + k) = m_p(k)$. Por tanto, $m_p(p^{i_0}!) = m_p\left(\prod_{k=1}^{p^{i_0}} k\right) = \sum_{k=1}^{p^{i_0}} m_p(k) = \sum_{k=1}^{p^{i_0}} m_p(n - p^{i_0} + k) = m_p\left(\prod_{k=1}^{p^{i_0}} (n - p^{i_0} + k)\right) = m_p\Big(n(n-1)\cdots\big(n-(p^{i_0}-2)\big)\big(n-(p^{i_0}-1)\big)\Big)$ y concluimos de (3.4) que $m_p\left(\binom{n}{p^{i_0}}\right) = 0$ y por tanto p no divide a $\binom{n}{p^{i_0}}$. □

Teorema 3.13 (Criterio de primalidad). *Sean $n \in \mathbb{N}$, $n \geq 2$ y $a \in \mathbb{N}$ tales que* m.c.d.$(a, n) = 1$*, entonces n es primo si y sólo si* $(x+a)^n \equiv x^n + a \pmod{n}$.

Demostración. Supongamos que n es primo. Aplicando el Teorema 3.10 ya lo tendríamos. Para probar el recíproco, supongamos que n es un número compuesto. Por tanto, tendrá algún divisor primo $p < n$. Además, por el *Teorema del binomio de Newton* se tiene que el p-ésimo coeficiente de $(x+a)^n$ es $a^{n-p}\binom{n}{p}$. Como, por hipótesis, m.c.d.$(a, n) = 1$ y por el Lema 3.12 (b) n no divide a $\binom{n}{p}$, se sigue que el p-ésimo coeficiente de $(x+a)^n$ no es divisible por n. Por otro lado, el p-ésimo coeficiente de $x^n + a$ es cero. Por tanto, $(x + a)^n \not\equiv x^n + a \pmod{n}$. □

Una vez visto el Teorema 3.13, se podría pensar que es fácil saber si un entero $n \geq 2$ es primo o no. Sólo hay que encontrar un entero coprimo con él y ver que se verifica la congruencia. Sin embargo, en la práctica resulta casi imposible pues debemos comparar los coeficientes de $(x + a)^n$ con los de $x^n + a$ módulo n. Por tanto, si bien es un test determinístico, corre en tiempo exponencial. Sin embargo, el Teorema 3.13 servirá de base para formular un test de primalidad determinístico y eficiente, que mostraremos en la siguiente sección.

3.4. El Algoritmo AKS

En primer lugar, veamos una definición que estará presente a lo largo de esta sección.

Definición 3.14 (Congruencia módulo n y Q). *Sean $n \geq 2$ y $Q \in \mathbb{Z}[x]$ un polinomio no constante cuyo coeficiente principal es coprimo con n. Sean $P, H \in \mathbb{Z}[x]$. Decimos que P y H son congruentes módulo n y Q y escribimos $P \equiv H \pmod{n, Q}$ si $P \equiv H$ en $(\mathbb{Z}/n\mathbb{Z})[x]/(Q)$.*

Ejemplo 3.15. Consideremos $n = 2$ y $Q = x^2+1$, $P = x^3+x^2+4x+1$, $H = x^3+2x$ en $\mathbb{Z}[x]$. Entonces $H = x(x^2+1)+x$ y $P = (x+1)(x^2+1)+3x$ en $\mathbb{Z}[x]$. Además $x \equiv 3x \pmod{2}$. Por tanto, $P \equiv H \pmod{2, x^2+1}$.

Para desarrollar un Test de Primalidad eficiente que se base en lo ya probado en la sección anterior, será necesario estudiar congruencias de la forma $\big(P(x)\big)^n \equiv P(x^n) \pmod{n, Q}$, donde P, Q son polinomios y n es un número compuesto. A partir de ahora, denotaremos $R := \big(P(x)\big)^n - P(x^n)$. Así, la congruencia $\big(P(x)\big)^n \equiv P(x^n) \pmod{n, Q}$ puede ser reescrita como $R \equiv 0 \pmod{n, Q}$.

Trabajar con congruencias módulo un número compuesto es mucho más difícil que si trabajamos con congruencias módulo un número primo. Así, si consideramos las congruencias módulo un factor primo p de n, y encontramos dos polinomios P y Q tales que se verifique que $R \not\equiv 0 \pmod{p, Q}$, entonces también se verifica que $R \not\equiv 0 \pmod{n, Q}$. Este factor primo podemos no conocerlo, por lo que en la formulación del algoritmo no podremos utilizarlo. Sin embargo, para el análisis matemático sí. Del Teorema 3.13 tenemos que si n es un número compuesto existe $P(x) = x + a$, con a y n coprimos tal que $R \not\equiv 0 \pmod{n}$. ¿Esto continúa verificándose si en lugar de n consideramos un factor primo p de n? Será necesario diferenciar dos casos.

Proposición 3.16. *Sea $n \in \mathbb{N}$, $n \geq 2$. Si n tiene dos factores primos distintos p y q, entonces se verifica que $(x+a)^n \not\equiv x^n + a \pmod{p}$ para todo $a \in \mathbb{N}$ tal que* m.c.d.$(a, n) = 1$.

Demostración. Supongamos que p^{i_0} es la mayor potencia de p que divide a n. De este modo, $n = rp^{i_0}$, donde p no divide a r. Ahora, por el Teorema del binomio de Newton, se tiene que $(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k} = a^n + \sum_{k=1}^{n-1} \binom{n}{k} x^k a^{n-k} + x^n$, y como m.c.d.$(a, n) = 1$, del Pequeño Teorema de Fermat (Teorema 2.2) concluimos que $a^n \equiv a \pmod{p}$. De aquí, $(x+a)^n \equiv x^n + a + \sum_{k=1}^{n-1} \binom{n}{k} x^k a^{n-k} \pmod{p}$. Además hemos visto que p^{i_0} es un factor de n. Por tanto, $p^{i_0} \in \{1, \ldots, n-1\}$, y por el Lema 3.12 (c) obtenemos que $\binom{n}{p^{i_0}} \not\equiv 0 \pmod{p}$. Es decir, existe al menos un sumando en $\sum_{k=1}^{n-1} \binom{n}{k} x^k a^{n-k}$ al que p no divide. Por tanto, $(x+a)^n \not\equiv x^n + a \pmod{p}$. □

En el caso de que p sea el único factor primo de n, se tendrá que $n = p^k$, para algún $k \in \mathbb{Z}$, $k > 1$. Del Corolario 3.11 deducimos que $\Big(P(x)\Big)^{p^m} \equiv P(x^{p^m}) \pmod{p}$, para todo $m \geq 1$. En particular, $\Big(P(x)\Big)^n \equiv P(x^n) \pmod{p}$, es decir, $R \equiv 0 \pmod{p}$, lo que no nos permite probar que n es compuesto. Pero este problema se puede reducir si, en primer lugar, comprobamos si el número compuesto n es potencia de un único número primo o no. De serlo, lo excluiremos

al comienzo del algoritmo. De este modo consideraremos, únicamente, aquellos números compuestos que tengan al menos dos factores primos distintos.

La estrategia a seguir será seleccionar, de forma oportuna, polinomios $P, Q \in \mathbb{Z}[x]$ cuyos grados están acotados polinomialmente por $\log n$. Entonces comprobamos si se verifica la congruencia:

$$\big(P(x)\big)^n \equiv P(x^n) \pmod{n, Q}. \tag{3.5}$$

Si no se verifica, entonces el Teorema de Fermat para polinomios (Teorema 3.10) nos garantiza que n no es primo. Por supuesto, puede ocurrir que (3.5) se verifique para un número compuesto n, pero se demuestra que si elegimos de forma conveniente p y Q, entonces sólo necesitaremos verificar un número pequeño de congruencias para detectar si un número es compuesto. Ello es debido al siguiente teorema.

Teorema 3.17 (Teorema de Agrawal, Kayal, Saxena). *Sean $r, n \in \mathbb{N}$, r primo,* $\text{m.c.d.}(r, n) = 1$ *donde $ord_r(n) > 4(\log n)^2$. Sea $Q(x) := x^r - 1$. Si n no es una potencia de p, entonces hay a lo sumo r polinomios de la forma $P = x + a$, $a \in \{0, \ldots, p-1\}$ verificando $\big(P(x)\big)^n \equiv P(x^n) \pmod{p, Q}$.*

Dada la limitación de espacio no mostraremos la prueba de dicho teorema. Del enunciado nos percatamos de que al elegir $Q(x) := x^r - 1$, los polinomios ciclotómicos estudiados en el capítulo dos jugarán cierto papel en el algoritmo AKS. Tal y como se demuestra en [1] el algoritmo AKS es un algoritmo determinístico que corre en tiempo polinomial.

Finalizamos mostrando el algoritmo:

Algoritmo 5 Algoritmo AKS

Entrada: $n \in \mathbb{N}$, $n > 1$.
  if $n = a^b$, donde $a < n$ y $b > 1$ **then**
    n es compuesto.
  else if **then**
    Escoger un polimonio Q adecuado y analizar las congruencias $\Big(P_i(x)\Big)^n \equiv P_i(x^n)$ (mód n, Q), donde $P_1, \ldots, P_l$ son polinomios apropiados.
    if Alguna de las congruencias anteriores no se verifica **then**
      n es compuesto.
    else if **then**
      n es primo.
    end if
  end if

Bibliografía

[1] Agrawal, M. & Kayal, N. & Saxena, N. *Primes is in P.* Annals of Mathematics, 160 (2004), 781-793.

[2] Burton, D. M. *Elementary Number Theory.* Fifth edition, McGraw-Hill, 2002.

[3] Carmichael, R. D. *On Composite Numbers P Which Satisfy the Fermat Congruence* $a^{P-1} \equiv 1 \pmod{P}$. The American Mathematical Monthly, Vol. 19, No. 2 (Feb., 1912), pp. 22-27.

[4] Cox, D. *Galois Theory.* Second edition. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, 2012. xxviii+570 pp.

[5] Crandall, R. & Pomerance, C. *Prime Numbers: A Computational Perspective.* Second edition. Springer, New York, 2005. xvi+597 pp.

[6] Finck, P.-J.-E. *Nouvelles annales de mathématiques (1ª serie, tomo 1).* 1842.

[7] Franco Brañas, J.R. & Espinel Febles, M.C. & Almeida Benítez, P.R. *Manual de Combinatoria.*

[8] Grossman, H. *On the Number of Divisions in Finding a G. C. D.* The American Mathematical Monthly, Vol. 31, Nº. 9. Nov., 1924.

[9] Lamé, M. *Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers.* 1844.

[10] Léger, E. *Note sur le partage d'une droite en moyenne et extrême, et sur un problème d'arithmétique, Correspondance mathématique et physique 9.* 1837.

[11] Machì, A. *Groups. An introduction to ideas and methods of the theory of groups.* Springer, Milan, 2012. xiv+371 pp.

[12] Rempe-Gillen, L. & Waldecker, R. *Primality Testing for Beginners.* American Mathematical Society, Providence, RI, 2014. xii+244 pp.
[13] Reynaud, A.-A.-L. *Traité d'arithmétique á l'usage des élèves qui se destinent à l'École Polytechnique (6ª ed.).* París: Courcier, 1811.
[14] Reynaud, A.-A.-L. *Traité d'arithmétique à l'usage de la marine et de l'artillerie, par Bezout; avec des notes et des tables de logarithmes (9ª ed.).* Paris: Courcier, 1821.
[15] Shallit, J. *Historia Mathematica, 21.* 1994.
[16] Sorenson, J. *An introduction to Prime Sieves.* Computer Sciences Technical Report #909, 1990.
[17] Wagstaff, Samuel S., Jr. *The Joy of Factoring.* American Mathematical Society, Providence, RI, 2013. xiv+293 pp.

Prime numbers. Historical issues, cyclotomic polynomials and primality tests

Claudia Ballester Niebla

Facultad de Ciencias · Sección de Matemáticas
Universidad de La Laguna
alu0100815399@ull.edu.es

Abstract

We study prime numbers, showing some algorithms that help us identifying whether an integer number is prime or composite. We start with de Euclidean algorithm. Then, we study the bounds given by some French mathematicians from the 19th century. The best bound was given by Gabriel Lamé and it is connected to Fibonacci's numbers. Then, we start working with modular arithmetic. We define quadratic residues, Legendre's symbol and Jacobi's symbol. They will be useful while proving some important results. The study of cyclotomic polynomials will help us to factorize integer numbers of the type $a^n \pm 1$. Finally, we present some primality tests. We start with the Sieve of Eratosthenes and end with the AKS algorithm, which is a deterministic polynomial time algorithm.

1. Introduction

Studying prime numbers opens a theorical and practical investigation field. One of the main objectives is to identify when an integer number is prime.In this memory we introduce some primality tests. Another objective of this research field is factoring into primes an integer number composite.

2. Euclidean Algorithm

The Euclidean Algorithm is used to find the greatest common divisor of a and b, where $a, b \in \mathbb{Z}$, $a > b$.

Algorithm 1 The Euclidean Algorithm
Input: $a, b \in \mathbb{Z}$ such that $0 \leq b \leq a$ y $a = qb + r$
Output: The greatest common divisor between a and b.
  while $b > 0$ **do**
    $(a, b) = (b, r)$
  end while
  return a

How many steps will it take to find the greatest common divisor of two integer numbers? In the 19th century some French mathematicians gave different bounds. The best one was given by Gabriel Lamé:

Theorem. *The number of steps that will be needed in the Euclidean Algorithm to find the greatest common divisor of two integer does not exceed five times the number of digits of the lower one (when we are using decimal system).*

This statement is connected to Fibonacci's numbers. These numbers are the elements from the sequence $\{\mathcal{U}_n\}$, where $\mathcal{U}_0 = \mathcal{U}_1 = 1$, $\mathcal{U}_{n+1} = \mathcal{U}_n + \mathcal{U}_{n-1}$ and $n \geq 1$. Let's denote by $E(a, b)$ the number of steps needed in the Euclidean Algorithm of a and b. We prove that the smallest pair of natural numbers a, b such that $a > b > 0$ and $E(a, b) = n$ are $a = \mathcal{U}_{n+1}$ and $b = \mathcal{U}_n$.

3. Modular arithmetic and cyclotomic polynomials

Definition. *The n-th cyclotomic polynomial is the polynomial:*

$$\Phi_n(x) = \prod_{\xi \text{ primitive } n\text{-th from unity}} (x - \xi) =$$

$$= \prod_{\gcd(a,n)=1} (x - \xi^a).$$

These polynomials are used to factorize integer numbers of the type $a^n - 1$. By knowing this method we will also be able to factorize numbers of the type $a^n + 1$. We will only need to consider that $a^{2n} - 1 = (a^n - 1)(a^n + 1)$, so $a^n + 1 = \frac{a^{2n}-1}{a^n-1}$. By factoring $a^{2n} - 1$ and $a^n - 1$ we have factorized $a^n + 1$.

4. Primality tests

Eratosthenes, in the ancient Greece, gave a technique to find all the prime numbers lower or equal to an integer n.

Algorithm 2 The sieve of Eratosthenes
Input: $n \in \mathbb{N}$
Output: The prime numbers lower or equal to n.
  Let's consider a list with all the integer numbers lower or equal to n, except for 1, and we call this list L.
  $p = 2$
  for $p \leq \sqrt{n}$ **do**
    if $p \in L$ **then**
      We assume that p is a prime number and delete their multiple numbers from the list L.
    end if
    $p = p + 1$
  end for
  return L

But this algorithm is not efficient. The AKS algorithm is a deterministic polynomial time algorithm. It was carried out by *Agrawal, Kayal and Saxena*. This is why it is called the *AKS Algorithm*.

Algorithm 3 The AKS Algorithm
Input: $n \in \mathbb{N}$, $n > 1$.
  if $n = a^b$, where $a < n$ and $b > 1$ **then**
    n es compose.
  else if then
    Choose a suitable polynomial Q and test the congruences $\left(P_i(x)\right)^n \equiv P_i(x^n) \pmod{n, Q}$, where $P_1, \ldots, P_l$ are suitable polynomials.
    if One of the congruences doesn't hold **then**
      n is composite.
    else if then
      n is prime.
    end if
  end if

References

[1] Agrawal, M. & Kayal, N. & Saxena, N. *Primes is in P.* Annals of Mathematics, 160 (2004), 781-793.

[2] Crandall, R. & Pomerance, C. *Prime Numbers: A Computational Perspective.* Second edition. Springer, New York, 2005. xvi+597 pp.

[3] Lamé, M. *Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers.* 1844.

[4] Rempe-Gillen, L. & Waldecker, R. *Primality Testing for Beginners.* American Mathematical Society, Providence, RI, 2014. xii+244 pp.

[5] Wagstaff, Samuel S., Jr. *The Joy of Factoring.* American Mathematical Society, Providence, RI, 2013. xiv+293 pp.