PRIMOS DE MERSENNE

JUAN FERNANDO RUEDA ARIZA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2005

PRIMOS DE MERSENNE

JUAN FERNANDO RUEDA ARIZA

Monografía presentada como
requisito para optar al título
de *Licenciado en Matemáticas*

Sofia Pinzón.
Ph.D Matemática
Directora

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2005

TITULO: PRIMOS DE MERSENNE.*

AUTOR: RUEDA ARIZA Juan Fernando.**

PALABRAS CLAVES: conjetura, congruencia, número primo, número perfecto.

DESCRIPCIÓN

En esta monografía se pueden encontrar algunos de los resultados que se utilizan en la teoría de números pero vistos de una forma diferente a la que estamos acostumbrados, además también se puede encontrar una gran variedad de aplicaciones que tienen los números primos en el estudio de la matemática.

En los dos primeros capítulos se encuentran varios resultados, historia y conjeturas sobre números primos además de un amplió conjunto de resultados sobre congruencias esenciales para el desarrollo del tercer y último capítulo en el cual se muestran algunos aportes de grandes matemáticos en el afán de encontrar una fórmula que nos permita calcular con facilidad y rapidez cuando un número es primo y que hasta el momento no se ha encontrado, pero gracias a esta búsqueda se han encontrado algunos resultados llamados teoremas de primalidad los cuales son herramientas bastante útiles para comprobar cuando un número especialmente si es muy grande es primo o no, también se encuentran varios resultados sobre el tema en que se baso la monografía, "los primos de Mersenne"los cuales son muy importantes ya que hasta el momento y en el transcurso de la historia siempre han sido los primos más grandes encontrados además por cada primo de Mersenne que se encuentra también se encuentra un número perfecto.

Por último esta un anexo donde se encuentran varias tablas con gran diversidad de números primos, que dependiendo de su forma tiene un nombre especial como por ejemplo primos de Fermat generalizado, primos de Sophie Germain, primos de Cullen y primos de Woodall.

*Monografía.

**Facultad de Ciencias. Escuela de matemáticas. Director: Sofía Pinzón Durán.

TITLE: THE MERSENNE PRIME.*

AUTHOR: RUEDA ARIZA Juan Fernando.**

KEY WORDS: conjectures, congruences, prime number, perfect number.

DESCRIPTION

In this monograph you can find some of the results that are used in the number's theory but seen in a different way to the one that we are used to, besides you can find a great variety of applications about the prime numbers in the mathematical study.

In the first two chapters there are several results, history and conjectures on prime numbers in addition to extended the set of results on essential moments for the development of the third and last chapter in which some contributions of great mathematicians are shown in the eagerness to find a formula that allows us to calculate with facility and rapidity when a number is prime, and that until the moment has not been found, but thanks to this search some results have been called "primalidad"theorems which are quite useful tools to verify when a number specially if it is a very big one is prime or not, also there are several results on the subject in which I am based on in this monograph, "the primes of Mersenne"which are very important since until the moment and in the course of history they have always been the biggest prime numers found, besides by each Mersenne's prime number there is also a perfect number.

Finally there is an annex where there are several tables with great diversity of prime numbers, that depending on its form has a special name like for example prime Fermat's generalized numbers, Sophie Germain's prime numbers and Cullen and Woodall's prime numbers.

*Monograph.

**Faculty of sciences. Mathematics school. Director: Sofía Pinzón Durán.

CONTENIDO

INTRODUCCION

La presente monografía es una revisión bibliográfica sobre los primos de Mersenne ($2^p - 1$ donde p es un primo) y algunas de sus características más importantes.

En el primer capítulo "Divisibilidad y Congruencias"presentaremos algunos resultados importantes para el desarrollo de la monografía. En este mismo capítulo aparecen algunos resultados y conjeturas sobre números primos que han aparecido con el tiempo.

En el segundo capítulo "Campos Finitos y Reciprocidad Cuadrática"se ahonda un poco en algebra moderna y se presentan algunos resultados importantes y necesarios para los tópicos a tratar en el tercer y último capítulo de esta monografía. Los ejemplos están escogidos para que contribuyan a la mejor comprensión de estos resultados y por consiguiente de la monografía.

En el tercer capítulo "Primos de Mersenne y Pruebas de Primalidad"se encuentran importantes caracterizaciones para los números primos y no primos conseguidos por algunos matemáticos en su lucha por encontrar una forma de generalizar la búsqueda de estos números.

En anexo presentamos unas tablas donde aparecen los primos de Mersenne conocidos y algunos otros primos bastante grandes obtenidos con la ayuda de potentes computadores; en estas tablas se encuentra el último primo encontrado (febrero de 2005) $2^{25964951} - 1$ el cual es un primo de Mersenne que tiene 7816230 dígitos.

Capítulo 1

Divisibilidad y Congruencias

En este primer capítulo se verán los tópicos básicos de la teoría de números, como divisibilidad, congruencias y aritmética módulo n.

1.1. Teorema Fundamental de la Aritmética

La división euclidiana o división con residuo, es una de las operaciones que se supone que todos prendemos en la escuela. Su formulación precisa es: dados $a \in \mathbb{Z},\ b \in \mathbb{Z}^*$, donde $\mathbb{Z}^* = \mathbb{Z} - \{0\}$ existen $q,\ r \in \mathbb{Z}$ con $0 \leq r < |b|$ y $a = bq + r$, donde q y r son únicos y son llamados respectivamente cociente y residuo de la división de a por b. Si $b > 0$ se puede definir $q = \lfloor a/b \rfloor$ y si $b < 0,\ q = \lceil a/b \rceil$, en cualquier caso, $r = a - bq$. El residuo r es a veces denotado por $a\ mod\ b$; se define $a\ mod\ 0 = a$. Hay que recordar que $\lfloor x \rfloor$ denota un único entero k tal que $k \leq x < k + 1$ y $\lceil x \rceil$ un único entero tal que $k - 1 < x \leq k$.
Dados dos enteros a y b, $b \neq 0$ se dirá que b divide a a, o que a es múltiplo de b y se escribe $b \mid a$, si existe $q \in \mathbb{Z}$ con $a = qb$. Asimismo, $b \mid a$ si y solamente si $a\ mod\ b = 0$.

Proposición 1.1.1. *Dados $a, b \in \mathbb{Z}$ existe un único $d \in \mathbb{N}$ tal que $d \mid a$, $d \mid b$ y para todo $c \in \mathbb{N}$, si $c \mid a$ y $c \mid b$ entonces $c \mid d$. Además existen $x,\ y \in \mathbb{Z}$ con $d = ax + by$.*

Demostración: El caso $a = b = 0$ es trivial (se tiene $d = 0$). En los otros casos, sea $I(a, b) = \{ax + by; x,\ y \in \mathbb{Z}\}$ y sea $d = ax_0 + by_0$ el menor elemento positivo no nulo de $I(a, b)$. Como $d \in \mathbb{N}^*$, existen $q, r \in \mathbb{Z}$ donde $a = dq + r$ con $0 \leq r < d$. Despejando r se tiene que $r = a - dq = a(1 - qx_0) + b(-qy_0) \in I(a, b)$; ahora,como $r < d$ y d es el menor elemento positivo no nulo de $I(a, b),\ r = 0$ y $d \mid a$. Análogamente, $d \mid b$. Para la segunda parte como

$c \mid a$ y $c \mid b$; se tiene que $c \mid (ax + by)$ para cualesquiera valor de x y y, específicamente para x_0 y y_0 entonces $c \mid d$. ■

Teorema 1.1.1. *Sean a y b enteros no ambos nulos. El máximo común divisor (a, b) es el menor entero positivo que puede escribirse de la forma $ax + by$ con $x,\ y$ enteros.*

Demostración: Supóngase que $d = (a, b)$ y sea $S = \{z \in \mathbb{Z}^+ \mid z = ax + by \text{ con } x,\ y \in \mathbb{Z}\}$. $S \neq \emptyset$ puesto que $z = a^2 + b^2 \in S$. Luego, S posee un mínimo, que se llamará g y que se puede escribir de la forma $g = ax_0 + by_0$. Se probará que $g = d = (a, b)$. En efecto g es divisor común de de a y b, pues si se divide a entre g se tiene,

$$\begin{aligned} a = qg + r,\ \text{con } 0 &\leq r < g,\ \text{luego,} \\ r &= a - qg \\ &= a - q(ax_0 + by_0) \\ &= a(1 - qx_0) + b(-qy_0) \\ &= ax' + by'. \end{aligned}$$

ahora si $r \neq 0$ entonces $r \in S$ lo cual contradice la minimalidad de g, en consecuencia $r = 0$ y así $g \mid a$. Análogamente se verifica que $g \mid b$. Como $d = (a, b)$ y g es un divisor común entonces $g \leq d$. De otra parte $g = ax_0 + by_0$ y $d \mid a$ y $d \mid b$ entonces $d \mid g$ y como ambos números son positivos $d \leq g$ y en consecuencia $d = g$. ■

Proposición 1.1.2. *Si $a = bq + r$ entonces $(a, b) = (b, r)$.*

Demostración: Supongamos que $d = (a, b)$ y $d' = (b, r)$. Como $d \mid a$ y $d \mid b$ entonces $d \mid r = a - bq$ entonces $d \mid d'$. Análogamente $d' \mid a = bq + r$ entonces $d' \mid d$. Como d y d' son positivos entonces $d = d'$. ■

El algoritmo de Euclides para calcular el máximo común divisor (mcd) se basa en las siguientes observaciones simples. Si $a = bq + r,\ 0 \leq r < b$, se tiene (con la notación de la anterior demostración) $I(a, b) = I(b, r)$, donde $(a, b) = (b, r)$. Definiendo $a_0 = a,\ a_1 = b$ y $a_n = a_{n+1}q_{n+2} + a_{n+2},\ 0 \leq a_{n+2} < a_{n+1}$ (o sea a_{n+2} es el residuo de dividir a_n por a_{n+1}) se tiene $(a, b) = (a_0, a_1) = (a_1, a_2) = \cdots = (a_n, a_{n+1})$ para cualquier valor de n. Sea N el menor natural para el cual $a_{N+1} = 0$ o sea el menor entero para el cual el residuo es 0, entonces se tiene que $(a, b) = (a_N, 0) = a_N$

Teorema 1.1.2. *Sean a y b enteros no ambos nulos. Entonces $(a, b) = 1$ si y solo si existen enteros $x,\ y$ tales que $1 = ax + by$.*

Demostración: Si $(a,b)=1$ entonces el Teorema 1.1.1 garantiza la existencia de tales $x,\ y$. Recíprocamente, si existen $x,\ y$ tales que $1=ax+by$ entonces $(a,b)\mid 1$ y por lo tanto, $(a,b)=1$. ■

Lema 1.1.1. *Si $a\mid bc$ y $(a,b)=1$ entonces $a\mid c$.*

Demostración: Como $a\mid bc$ existe k tal que $bc=ak$. Como $(a,b)=1$ existen enteros x,y tales que $ax+by=1$. Por lo tanto, $c=c(ax+by)=acx+bcy=acx+aky=a(cx+ky)$ es decir $a\mid c$. ■

Cuando $(a,b)=1$ se dirá que a y b son primos entre si. Un natural $p>1$ es llamado primo si los únicos divisores positivos de p son 1 y p. Un natural $n>1$ es llamado compuesto si admite otros divisores además de 1 y n.

Claramente, si p es primo y $p\nmid a$ se tiene que $(p,a)=1$. Utilizando el lema anterior e inducción se tiene el siguiente resultado:

Corolario 1.1.1. *Si p es primo y $p\mid a_1a_2\cdots a_n$, entonces $p\mid a_i$ para algún $i, 1\leq i\leq n$.*

Demostración: La demostración es hecha por inducción,

para $n=2$, veamos que

$$p\mid a_1a_2\Rightarrow p\mid a_1\vee p\mid a_2$$

Si $p\nmid a_1\Rightarrow (p,a_1)=1$ y por el teorema anterior $p\mid a_2$. De la misma manera se hace para a_1.

Para $n=k$, supóngase que

$$p\mid a_1a_2\cdots a_k\Rightarrow p\mid a_i$$

para algún i con $1\leq i\leq k$

Sea $a_{k+1}\neq a_i$ para todo i tal que $1\leq i\leq k$ y supóngase que $p\mid a_1a_2\cdots a_ka_{k+1}=(a_1a_2\cdots a_k)a_{k+1}$. Si $p\mid a_{k+1}$ entonces $p\mid a_i$ para algún i con $1\leq i\leq k+1$. Si $p\nmid a_{k+1}$ entonces $(p,a_{k+1})=1$ y por el lema anterior $p\mid a_1a_2\cdots a_k$, entonces $p\mid a_i$ para algún i con $1\leq i\leq k$ y también para algún i con $1\leq i\leq k+1$ lo que concluye la demostración. ■

Ahora ya se puede enunciar y probar el teorema que dice que todo entero admite una única factorización como producto de primos pero antes se enunciará el segundo principio de inducción matemática (P.I.M.2) que dice: Sea a un número natural. Sea S un subconjunto de $\{k\in\mathbb{N}|k\geq a\}$ que satisface:

1. $a\in S$.

2. Para cada $n > a,\ n \in S$ siempre que $k \in S$ para todo $k \in \mathbb{N}$ tal que $a \leq k < n$. Entonces $S = \{k \in \mathbb{N} | k \geq a\}$.

Teorema 1.1.3 (Teorema Fundamental de la Aritmética). *Todo entero $n > 1$, ó es primo, ó se puede factorizar como producto de primos. Este producto es único salvo por el orden de los factores.*

Demostración:

1. Sea S el conjunto de todos los números naturales que son primos o que pueden escribirse como producto de primos. Claramente $S \subseteq \{k \in \mathbb{N} | k \geq 2\}$ y además se tiene:

   a) $2 \in S$ porque 2 es un número primo.

   b) Supóngase que $n > 2$ y que $k \in S$ para todo k tal que $2 \leq k < n$. Se verá que $n \in S$. Si n es primo entonces $n \in S$. Si n no es primo existen r y t tales que $n = rt$ con $2 \leq r < n$ y $2 \leq t < n$ y por hipótesis, ellos o son primos, o productos de primos. En consecuencia n es producto de primos y así $n \in S$.
   El P.I.M.2 nos afirma entonces que $S = \{k \in \mathbb{N} | k \geq 2\}$

2. ***Unicidad***. Haciendo inducción sobre n. Para $n = 2$ claramente la representación es única. Supóngase ahora que para todo entero con $2 \leq k < n$ la representación es única y que,

   $$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$$

   donde p_i y q_i son primos con $p_1 \leq p_2 \dots \leq p_s$ y $q_1 \leq q_2 \dots \leq q_t$. Así, $p_1 \mid q_1 q_2 \cdots q_t$ y entonces $p_1 = q_j$ para algún j por lo tanto $q_1 \leq p_1$. Análogamente $q_1 \mid p_1 p_2 \cdots p_s$ y entonces $q_1 = p_i$ para algún i por lo tanto $p_1 \leq q_1$. Lo anterior demuestra que $p_1 = q_1$ y cancelando se tiene

   $$\frac{n}{p_1} = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t$$

   Como $\frac{n}{p_1} < n$ la hipótesis de inducción garantiza que estas dos representaciones de $\frac{n}{p_1}$ son idénticas y en consecuencia $s = t$ y para cada $i,\ p_i = q_i$. por el P.I.M. la prueba queda completa.

■

Otra forma de escribir la factorización es

$$n = p_1^{e_1} \cdots p_m^{e_m},$$

con $p_1 < \cdots < p_m,\ e_i > 0$, y una forma más de escribirlo es

$$n = 2^{e_2}3^{e_3}5^{e_5}\cdots p^{e_p},$$

donde el producto es tomado sobre todos los primos pero apenas un número finito de exponentes es mayor que cero.

Corolario 1.1.2. *Si* $(a,b) = 1$ *y* $(a,c) = 1$ *entonces* $(a,bc) = 1$.

Demostración: Puesto que $(a,b) = 1$ y $(a,c) = 1$ se tiene que,

$$1 = ax + by \text{ y también } 1 = ar + cs$$

con x, y, r, s enteros y por lo tanto,

$$\begin{aligned} 1 &= (ax + by)(ar + cs) \\ &= a(xar + xsc + byr) + bc(ys) \end{aligned}$$

y en consecuencia $(a,bc) = 1$. ■

Teorema 1.1.4. *(Euclides) Existen infinitos números primos.*

Demostración: Supóngase por absurdo que solo hay un número finito de primos, $p_1, p_2, \ldots, p_n$ y sea $N = p_1p_2\ldots p_n + 1$.
Como $N > 1$, entonces N es primo o se expresa como producto de primos. Ya que N es mayor que cada uno de los primos p_i entonces N no es primo y por lo tanto existe p_i donde $1 \leq i \leq n$ tal que $p_i \mid N$ entonces $p_i \mid (N - p_1p_2\ldots p_n) = 1$ lo que es absurdo. ■
Obsérvese que no se prueba que $p_1 \cdot p_2 \cdots p_m + 1$ es primo para algún conjunto finito de primos. De hecho $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509,\ 2 \cdot 3 \cdot 5 \cdot 7 - 1 = 11 \cdot 19,\ 4! + 1 = 25 = 5^2$ y $8! - 1 = 40319 = 23 \cdot 1753$ no son primos. No existe ninguna fórmula simple conocida que genere siempre números primos.

1.2. Congruencias

Sean $a,\ b,\ n \in \mathbb{Z}$. Se dice que a es congruente con b módulo n, y se escribe $a \equiv b(mod\ n)$ si $n \mid (b - a)$. Como una congruencia módulo 0 es una igualdad y cualquier par de enteros son congruentes módulo 1, en general estamos interesados en $n > 1$.

Proposición 1.2.1. *Para cualquier* $a,\ a',\ b,\ b',\ c,\ n \in \mathbb{Z}$ *se tiene que:*

(a) $a \equiv a(mod\ n)$*;*

(b) si $a \equiv b(mod\ n)$ *entonces* $b \equiv a(mod\ n)$*;*

(c) si $a \equiv b(mod\ n)$ *y* $b \equiv c(mod\ n)$*; entonces* $a \equiv c(mod\ n)$*;*

(d) si $a \equiv a'(mod\ n)$ *y* $b \equiv b'(mod\ n)$ *entonces* $a + b \equiv a' + b'(mod\ n)$*;*

(e) si $a \equiv a'(mod\ n)$ *entonces* $-a \equiv -a'(mod\ n)$*;*

(f) si $a \equiv a'(mod\ n)$ *y* $b \equiv b'(mod\ n)$ *entonces* $a \cdot b \equiv a' \cdot b'(mod\ n)$*;*

Demostración:

(a) Para cualquier entero $a,\ n \mid (a - a) = 0$ es decir $a \equiv a(mod\ n)$.

(b) Si $n \mid (a - b)$, entonces $n \mid -(a - b) = b - a$, entonces $n \mid (b - a)$, luego $b \equiv a(mod\ n)$.

(c) $n \mid (a-b)$ y $n \mid (b-c)$, por lo tanto $n \mid ((a-b)+(b-c)) = a-c$, es decir $a \equiv c(mod\ n)$.

(d) Si $n \mid (a' - a)$ y $n \mid (b' - b)$ entonces $n \mid (a' + b') - (a + b)$, luego $a + b \equiv a' + b'(mod\ n)$.

(e) Si $n \mid (a' - a)$ entonces $n \mid ((-a') - (-a))$, luego $-a \equiv -a'(mod\ n)$.

(f) Si $n \mid (a' - a)$ y $n \mid (b' - b)$, obsérvese que $n \mid (a'(b' - b) + b(a' - a))$, luego $n \mid (a'b' - ab)$, entonces $a \cdot b \equiv a' \cdot b'(mod\ n)$.

■

Los ítems (a), (b), (c) de ésta proposición muestran, en ese orden, que la relación $\equiv (mod\ n)$ (ser congruente módulo n) es una relación reflexiva, simétrica y transitiva. Las relaciones que satisfacen estas tres propiedades son llamadas relaciones de equivalencia. Dada una relación de equivalencia $\sim$ sobre un conjunto X y un elemento x de X se define una clase de equivalencia $\overline{x}$ de x como

$$\overline{x} = \{y \in X | y \sim x\};$$

obsérvese que $x \sim y$ si y solamente si $\overline{x} = \overline{y}$. Las clases de equivalencia forman una partición de X, esto es, una colección de subconjuntos no vacíos y disjuntos de X cuya unión es X. El conjunto $\{\overline{x} | x \in X\}$ de clases de equivalencia es llamado *cociente* de X por la relación de equivalencia $\sim$ y es denotado por $X/\sim$.

Aplicando esta construcción general a este caso, se define el cociente $\mathbb{Z}/(\equiv (mod\, n)))$, llamado

por simplicidad de notación $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$ o a veces $\mathbb{Z}_n$. Dado $a,\ a' \in \mathbb{Z}$, $\overline{a} = \overline{a'}$ si y solamente si $a \equiv a'(mod\ n)$. Si $n > 0$, la división euclidiana dice que todo entero a es congruente con un único entero a' con $0 \leq a' < n$; se puede reescribir este hecho en éste nuevo lenguaje como

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Cuando no haya posibilidad de confusión se omitirán las barras y se llamarán a los elementos de $\mathbb{Z}/(n)$ simplemente $0, 1, 2, ..., n-1$.
Los ítems (d), (e) y (f) de la proposición dicen que la suma, la diferencia y el producto son compatibles con la relación de congruencia. Es ésta propiedad la que hace a las congruencias tan útiles, posibilitan hacer operaciones módulo n. Por ejemplo se puede escribir

$$\begin{aligned} 284593 &= 2 \cdot 10^5 + 8 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 9 \cdot 10^1 + 3 \cdot 10^0 \\ &= 2 \cdot 1^5 + 8 \cdot 1^4 + 4 \cdot 1^3 + 5 \cdot 1^2 + 9 \cdot 1^1 + 3 \cdot 1^0 \\ &= 2 + 8 + 4 + 5 + 9 + 3 \\ &= 31 \\ &= 4\ (mod\ 9), \end{aligned}$$

ya que $10 \equiv 1(mod\ 9)$. Una formulación más abstracta de la misma idea es decir que las operaciones $+$ y $\cdot$ se pueden definir como

$$+ : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(n) \quad \cdot : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(n)$$

por $\overline{a} + \overline{b} = \overline{a+b}$ y $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. Una duda que se puede presentar es si no importa los representantes de las clases de equivalencia que escoja a y b: después de todo existen infinitos enteros a' y b' tal que $\overline{a} = \overline{a'}$ y $\overline{b} = \overline{b'}$. Los ítems (d) y (f) de la Proposición 1.2.1 son exactamente lo que se necesita: ellos dicen que en estas condiciones $\overline{a+b} = \overline{a'+b'}$ y $\overline{a \cdot b} = \overline{a' \cdot b'}$.

Proposición 1.2.2. *Sean $a, n \in \mathbb{Z}$, $n > 0$. Entonces existe $b \in \mathbb{Z}$ con $ab \equiv 1(mod\ n)$ si y solo si $(a, n) = 1$.*

Demostración: Sea $ab \equiv 1(mod\ n)$, se tiene que $n \mid 1-ab$ entonces para algún k, $nk = 1-ab$, luego $nk + ab = 1$ y como $(a, n) \mid (ab + nk) = 1$ entonces $(a, n) = 1$. Si $(a, n) = 1$, se tiene que $ax + ny = 1$ para ciertos enteros x y y donde $ny = 1 - ax$, luego $n \mid 1 - ax$ entonces $ax \equiv 1(mod\ n)$. ■

Corolario 1.2.1. *Si* $(a, n) = 1$ *y* $ab \equiv ab'(mod\ n)$ *entonces* $b \equiv b'(mod\ n)$.

Demostración: Como $ab \equiv ab'(mod\ n)$, entonces $n \mid (ab - ab') \Rightarrow n \mid a(b - b')$. Como por hipótesis $(a, n) = 1$ entonces $n \mid (b - b')$ y $b \equiv b'(mod\ n)$. ■

Definición 1.2.1. Se define $(\mathbb{Z}/(n))^* \subset \mathbb{Z}/(n)$ por

$$(\mathbb{Z}/(n))^*) = \{\bar{a}; (a, n) = 1\}$$

Obsérvese que el producto de elementos de $(\mathbb{Z}/(n))^*$ es siempre un elemento de $(\mathbb{Z}/(n))^*$ (Corolario 1.1.2).

Utilizando esta forma de notación se obtiene una forma del Teorema Chino diferente a la que estamos acostumbrados a ver.

Teorema 1.2.1. *[Teorema Chino del Residuo] Si* $(m, n) = 1$ *entonces*

$$\begin{aligned} f : \mathbb{Z}/(mn) &\rightarrow \mathbb{Z}/(m) \times \mathbb{Z}/(n) \\ \overline{a} &\rightarrow (\overline{a}, \overline{a}) \end{aligned}$$

es una biyección. Además la imagen por f *de* $(\mathbb{Z}/(mn))^*$ *es* $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$

Demostración: Como $\mathbb{Z}/(mn)$ y $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ tienen la misma cardinalidad mn, para probar que f es biyectiva basta verificar que f es inyectiva. Si $a \equiv a'(mod\, m)$ y $a \equiv a'(mod\, n)$ entonces $m \mid (a - a')$ y $n \mid (a - a')$, donde $mn \mid (a - a')$ porque $(m, n) = 1$ y $a \equiv a'(mod\, mn)$. La imagen de $(\mathbb{Z}/(mn))^*$ es $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$ pues $(a, mn) = 1$ si y solo si $(a, m) = (a, n) = 1$. ■

Corolario 1.2.2. *Si* $m_1, m_2, \ldots, m_r$ *son enteros primos entre si. Entonces*

$$\begin{aligned} f : \mathbb{Z}/(m_1 m_2 \ldots m_r) &\rightarrow \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2) \ldots \times \mathbb{Z}/(m_r) \\ \overline{a} &\rightarrow (\overline{a}, \overline{a} \ldots \overline{a}) \end{aligned}$$

es una biyección.

Demostración: Basta aplicar el teorema chino r veces. ■

1.3. Función de Euler y el Pequeño Teorema de Fermat

Definición 1.3.1. Se define $\Phi(n) = |(\mathbb{Z}/(n))^*|$ donde $|X|$ denota el número de elementos de X. La función Φ es conocida como la función de Euler, claramente $\Phi(1) = \Phi(2) = 1$ y para $n > 2,\ 1 < \Phi(n) < n$.

Otra forma de definir $\Phi(n)$ es como el número de enteros positivos menores e iguales que n y primos relativos con n. Como ejemplo se tiene la siguiente tabla de valores de $\Phi(n)$:

$$\begin{array}{rcccccccccc} n & : & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \Phi(n) & : & 1 & 1 & 2 & 2 & 4 & 2 & 6 & 4 & 6 & 4. \end{array}$$

Teorema 1.3.1. *Si p es primo y a es un entero positivo, entonces $\Phi(p^a) = p^a - p^{a-1}$.*

Demostración: Los enteros positivos menores o iguales que p^a que no son primos relativos con p son precisamente los p^{a-1} múltiplos de p,

$$1 \cdot p,\ 2 \cdot p, \ldots, p^{a-1} \cdot p.$$

Por lo tanto

$$\Phi(p^a) = p^a - p^{a-1}.$$

En particular, cuando $a = 1$ se obtiene la fórmula $\Phi(p) = p - 1$ para cada primo p. ■

Definición 1.3.2. Se dice que los n números enteros $a_1, a_2, \ldots a_n$ forman un sistema completo de residuos (s.c.r.) módulo n si $\{\overline{a_1}, \overline{a_2}, \ldots \overline{a_n}\} = \mathbb{Z}/(n)$, esto es si los a_i representan todas las clases de congruencia módulo n.

Equivalentemente, se puede decir que $a_1, a_2, \ldots a_n$ forman un s.c.r. módulo n si y solamente si $a_i \equiv a_j (mod\ n)$ implica que $i = j$.

Definición 1.3.3. Se dice que los $\Phi(n)$ números enteros $b_1, b_2, \ldots b_{\Phi(n)}$ forman un sistema completo de invertíbles (s.c.i.) módulo n si $\{\overline{b_1}, \overline{b_2}, \ldots \overline{b_{\Phi(n)}}\} = (\mathbb{Z}/(n))^*$, esto es si los b_i representan todas las clases de congruencias invertíbles módulo n.

Equivalentemente, se puede decir que $b_1, b_2, \ldots b_{\Phi(n)}$ forman un s.c.i. módulo n si y solamente si $(b_i, n) = 1$ para todo i y $a_i \equiv a_j (mod\ n)$ implica que $i = j$.

Proposición 1.3.1. *Sean* $q,\ r,\ n \in \mathbb{Z},\ n > 0$, q *invertible módulo* n, $a_1,\ a_2, \ldots, a_n$ *un s.c.r. módulo* n *y* $b_1, b_2, \ldots, b_{\Phi(n)}$ *un s.c.i. módulo* n. *Entonces* $qa_1 + r,\ qa_2 + r, \ldots, qa_n + r$ *forman un s.c.r. módulo* n *y* $qb_1,\ qb_2, \ldots, qb_{\Phi(n)}$ *forman un s.c.i. módulo* n.

Demostración: Si $qa_i + r \equiv qa_j + r(mod\ n)$ entonces $n \mid q(a_i - a_j)$ y como q es invertible módulo n, $(n, q) = 1$ entonces $a_i \equiv a_j(mod\ n)$, donde $i = j$; con esto se prueba que $qa_1 + r,\ qa_2 + r, \ldots, qa_n + r$ forman un s.c.r.. Como $(q, n) = (b_i, n) = 1$, se tiene $(qb_i, n) = 1$. Por otro lado si $qb_i \equiv qb_j(mod\ n)$ se tiene que $b_i \equiv b_j(mod\ n)$ y $j = i$. Esto concluye la demostración. ■

Teorema 1.3.2 (Euler). *Si* $(a, n) = 1$ *entonces* $a^{\Phi(n)} \equiv 1(mod\ n)$.

Demostración: Sea $\{b_1,\ b_2, \ldots, b_{\Phi(n)}\}$ un s.c.i. módulo n. Por la Proposición 1.3.1 $\{ab_1, ab_2, \ldots, ab_{\Phi(n)}\}$ también forman un s.c.i. módulo n. Por lo tanto el producto de los enteros del primer conjunto es congruente al producto de los enteros del segundo conjunto. Luego

$$b_1 \cdot b_2 \cdots b_{\Phi(n)} \equiv ab_1 \cdot ab_2 \cdots ab_{\Phi(n)}(mod\ n)$$
$$b_1, b_2, \ldots, b_{\Phi(n)} \equiv a^{\Phi(n)} b_1, b_2, \ldots, b_{\Phi(n)}(mod\ n)$$

Como cada b_i es primo relativo con n, por el Corolario 1.2.1 se tiene

$$1 \equiv a^{\Phi(n)}(mod\ n).$$

■

Teorema 1.3.3 (Pequeño Teorema de Fermat). *Si* p *es un número primo, entonces para todo entero* $a,\ a^p \equiv a(mod\ p)$.

Demostración: Si $p \mid a$, se tiene que

$$a \equiv 0(mod\ p) \text{ y } a^p \equiv 0(mod\ p)$$

y por las propiedades de congruencias $a^p \equiv a(mod\ p)$.
Si $p \nmid a$ entonces $\Phi(p) = p - 1,\ a^{p-1} \equiv 1(mod\ p)$ y nuevamente $a^p \equiv a(mod\ p)$. ■

Teorema 1.3.4. *Si* $(m, n) = 1$, *entonces* $\Phi(m.n) = \Phi(m)\Phi(n)$.

Demostración: Por el Teorema 1.2.1

$$f : \mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$

es biyectiva, entonces

$$(\mathbb{Z}/(mn))^* \cong (\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$$

luego

$$|\ (\mathbb{Z}/(mn))^*\ | = |\ (\mathbb{Z}/(m))^*\ | \cdot |\ (\mathbb{Z}/(n))^*\ |$$

entonces $\Phi(mn) = \Phi(m)\Phi(n)$. ■

Teorema 1.3.5. *Si* $n = \prod_{i=1}^{k} p_i^{n_i}$ *es la representación canónica de un entero positivo* n*, entonces*

$$\begin{aligned} \Phi(n) &= \prod_{i=1}^{k} \left(p_i^{n_i} - p_i^{n_i-1}\right) \\ \Phi(n) &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right). \end{aligned}$$

Demostración: Por el teorema anterior y usando la fórmula para $\Phi(p^a)$ se tiene que

$$\Phi(n) = \prod_{i=1}^{k} \Phi(p_i^{n_i}) = \prod_{i=1}^{k} \left(p_i^{n_i} - p_i^{n_i-1}\right)$$

De otra parte,

$$\begin{aligned} \prod_{i=1}^{k} \left(p_i^{n_i} - p_i^{n_i-1}\right) &= \prod_{i=1}^{k} p_i^{n_i} \left(1 - \frac{1}{p_i}\right) \\ &= \prod_{i=1}^{k} p_i^{n_i} \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \\ &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right), \end{aligned}$$

luego

$$\Phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

■

En particular, si $n > 2$ entonces $\Phi(n)$ es par. Más adelante se estudiarán ecuaciones de segundo grado en $\mathbb{Z}/(p)$; se verá desde ya un pequeño resultado de este tipo que garantiza que los únicos a que son sus propios inversos módulo p son 1 y -1.

Lema 1.3.1. *Si p es primo entonces las únicas soluciones de $x^2 = 1$ en $\mathbb{Z}/(p)$ son 1 y -1. En particular si $x \in (\mathbb{Z}/(p))^* - \{1, -1\}$ entonces $x^{-1} \neq x$ en $\mathbb{Z}/(p)$.*

Demostración: Se puede reescribir la ecuación como $(x-1)(x+1) = 0$ entonces $(x-1) = 0$ o $(x+1) = 0$, de aquí se tiene que $x = 1$ o $x = -1$. Entonces las soluciones de la ecuación son 1 y -1. ■

Teorema 1.3.6 (Teorema de Wilson). *Sea $n > 4$. Entonces $(n-1)! + 1 \equiv 0(mod\ n)$ si n es primo y $(n-1)! \equiv 0(mod\ n)$ si n es compuesto.*

Demostración: Si n es compuesto pero no es un cuadrado de un primo se puede escribir $n = ab$ con $1 < a < b < n$; en este caso tanto a como b aparecen en $(n-1)!$ y $(n-1)! \equiv 0(mod\ n)$. Si $n = p^2,\ p > 2$, entonces p y $2p$ aparecen en $(n-1)!$ y $(n-1)! \equiv 0(mod\ n)$, esto demuestra que para todo n compuesto, $n > 4$, se tiene que $(n-1)! \equiv 0(mod\ n)$.
Si n es primo se puede escribir $(n-1)! \equiv -(2 \cdot 3 \cdots (n-2))(mod\ n)$; pero por el lema anterior y teniendo en cuenta que en el producto $2 \cdot 3 \cdots (n-2)$ aparece cada número con su inverso, juntándolos se tiene que $(n-1)! \equiv -1(mod\ n)$. ■

1.4. Función de Möbius

Se verá inicialmente una propiedad de la función Φ

Teorema 1.4.1. *Para cada entero positivo n, se tiene que*

$$\sum_{d|n} \Phi(d) = n.$$

Demostración: Considérese primero el número p^k cuyos divisores son $1, p, p^2, \ldots, p^k$. Entonces,

$$\begin{aligned} \Phi(1) + \Phi(p) + \Phi(p^2) + \cdots + \Phi(p^k) &= 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) \\ &= p^k. \end{aligned}$$

Por lo tanto, si $n = p_1^{n_1} p_2^{n_2} p_1^{n_1} \cdots p_r^{n_r}$ donde los primos son distintos, se tiene que

$$n = \prod_{i=1}^{r} (1 + \Phi(p_i) + \cdots + \Phi(p_i^{n_i})).$$

Desarrollando el producto y aplicando el Teorema 1.3.4, se tiene que el producto consiste en la suma de todos los términos de la forma

$$\Phi(p_1^{t_1})\Phi(p_2^{t_2})\cdots\Phi(p_r^{t_r}) = \Phi(d),$$

donde $d = p_1^{t_1}p_2^{t_2}\cdots p_r^{t_r}$ con $0 \leq t_i \leq n_i$ donde están todos los divisores de n. ■

Se define ahora la función de Möbius $\mu : \mathbb{N}^* \longrightarrow \mathbb{Z}$

Definición 1.4.1. La función μ de Möbius se define mediante las ecuaciones,

$\mu(1) = 1$.

$$\mu(n) = \begin{cases} (-1)^k & \text{Si } n = p_1p_2\ldots p_k \text{ con } p_1,\ p_2, \ldots, p_k \text{ primos diferentes;} \\ 0 & \text{si } p^2 \mid n \text{ para algún primo p.} \end{cases}$$

Teorema 1.4.2. *Para todo entero positivo n se tiene,*

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & si\ n = 1; \\ 0 & si\ n > 1. \end{cases}$$

Demostración: El caso en que $n = 1$ es evidente. Si $n > 1$, sea p un divisor primo de n y sea $n = p^e n'$. Se tiene

$$\begin{aligned} \sum_{d|n}\mu(d) &= \sum_{d|n,\ p\nmid d}\mu(d) + \sum_{d|n,\ p|d,\ p^2\nmid d}\mu(d) + \sum_{d|n,\ p^2|d}\mu(d) \\ &= \sum_{d|n'}\mu(d) + \sum_{d'|n'}\mu(pd') + 0 \\ &= \sum_{d|n'}\mu(d) - \sum_{d'|n'}\mu(d') \\ &= 0 \end{aligned}$$

■

Definición 1.4.2. Una función se denomina numérica si tiene como dominio el conjunto de los enteros positivos con valores en $\mathbb{C}$.

Teorema 1.4.3 (Fórmula de inversión de Möbius). *Si f es una función numérica y $F(n) = \sum_{d|n} f(d)$ para todo $n \geq 1$, entonces*

$$f(n) = \sum_{d|n}\mu(d)F\left(\frac{n}{d}\right).$$

Demostración: Se tiene,

$$\begin{aligned}\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right) &= \sum_{d|n}\left[\mu(d)\sum_{b|\frac{n}{d}}f(b)\right]\\ &= \sum_{d|n}\sum_{b|(\frac{n}{d})}\mu(d)f(b)\\ &= \sum_{b|n}\sum_{d|(\frac{n}{b})}\mu(d)f(b)\\ &= \sum_{b|n}\left[f(b)\sum_{d|(\frac{n}{b})}\mu(d)\right]\\ &= f(n).\end{aligned}$$

ya que por el teorema anterior, la suma interior en la última expresión es igual a cero, excepto en el caso en el cual $b = n$, cuando vale 1. ■

1.5. Otros Resultados y Conjeturas Sobre Números Primos

En esta sección presentaremos el enunciado de algunos resultados clásicos sobre números primos, así como también varios problemas famosos.

Teorema 1.5.1 (Dirichlet). *Dados naturales $a,\ d$ con $(a, d) = 1$, existen infinitos primos de la forma $a + dn$ (con n natural).*

Las demostraciones usuales de este teorema usan variables complejas. Muchos casos particulares admiten demostraciones elementales mas o menos sencillas, como por ejemplo, que existen infinitos primos de la forma $4n + 3$ o $6n + 5$.
Existen varios refinamientos conocidos del teorema de Dirichlet. Se define $\Pi_{d,a}(x)$ como el número de primos de la forma $a + dn$ en el intervalo $[2, x]$. De la Vallée Poussin probó que

$$\lim_{x\longrightarrow+\infty}\frac{\Pi_{d,a}(x)}{\Pi(x)} = \frac{1}{\Phi(d)},$$

esto es, todas las posibles clases módulo d tienen aproximadamente la misma proporción de primos.
Por otro lado, Tchebycheff observó que para valores pequeños de x, $\Pi_{3,2}(x) - \Pi_{3,1}(x)$ y

$\Pi_{4,3}(x) - \Pi_{4,1}(x)$ son positivos. Un teorema de Littlewood, sin embargo, demostró que estas funciones cambian de signo infinitas veces. En 1957, Leech demostró que el menor valor de x para el cual $\Pi_{4,3}(x) - \Pi_{4,1}(x) = -1$ es 26861 y en 1978 Bays y Hudson demostraron que el menor valor de x para el cual $\Pi_{3,2}(x) - \Pi_{3,1}(x) = -1$ es 608981813029.
Sea $p(d, a)$ el menor primo de la forma $a + dn$, con n entero y

$$p(d) = max\{p(d, a)|\ 0 < a < d,\ mcd(a, d) = 1\}.$$

Linnik (1994) probó que existe $L > 1$ con $p(d) < d^L$ para todo d suficientemente grande. La mejor estimación conocida para L es $L \leq 5, 5$, debido a Heath-Brown (1992), que también conjeturó que

$$p(d) \leq Cd(\ln d)^2.$$

Por otro lado, no se ha podido demostrar que existan infinitos primos de la forma $n^2 + 1$, de hecho, no existe ningún polinomio P con una variable y de grado mayor que 1, para el cual se sepa demostrar que existen infinitos primos de la forma $P(n),\ n \in \mathbb{Z}$. Por otro lado, Friedlander e Iwaniec probaron recientemente un resultado mucho más difícil: existen infinitos primos de la forma $a^2 + b^4$.
Uno de los problemas abiertos más famosos de la matemática es la conjetura de Goldbach, una de sus versiones es: todo número par mayor o igual que 4 se puede expresar como la suma de dos primos. Chen demostró que todo número par suficientemente grande es la suma de un primo con un número que tiene a lo máximo dos factores primos. Vinogradov demostró que todo impar suficientemente grande (por ejemplo mayor que $3^{3^{15}}$) es la suma de tres primos. Cuando p y $p+2$ son ambos primos, diremos que son *primos gemelos*. Se conjetura, pero no se sabe demostrar que existen infinitos primos gemelos. Brun, por otro lado, probó que los primos gemelos son escasos en el siguiente sentido: si $\Pi_2(x)$ es el número de pares de primos gemelos hasta x entonces

$$\Pi_2(x) < \frac{100x}{(\ln x)^2}$$

para x suficientemente grande. En particular,

$$\sum_{p\ primo\ gemelo} \frac{1}{p} < +\infty.$$

Se cree que $\Pi_2(x)$ es asintótico a $Cx/(\ln x)^2$ para alguna constante positiva C. Gracias a Clement se tiene la siguiente caracterización de primos gemelos. Sea $n \geq 2$; los enteros n y

$n+2$ son ambos primos si y solamente si $4((n-1)!+1)+n \equiv 0(mod\ n(n+2))$.
Sea p_n el enésimo número primo. El teorema de los números primos equivale a decir que

$$\lim_{n\to\infty} \frac{p_n}{n \ln n} = 1.$$

Por otro lado, se sabe muy poco sobre el comportamiento de la función $d_n = p_{n+1} - p_n$. Por ejemplo, la conjetura de que existen infinitos primos gemelos equivale a decir que $\liminf d_n = 2$. Ni siquiera se sabe demostrar que

$$L = \liminf \frac{d_n}{\ln p_n} = 0;$$

Erdös probó que $L < 1$ y Maier que $L \leq 0{,}248$. Erdös también probó que el conjunto D de los puntos de acumulación de $d_n/\ln p_n$ tiene medida positiva, resultado que posteriormente fué mejorado por Hildebrand y Maier, que probaron entre cosas, que existe una constante positiva c tal que si x es lo suficientemente grande, la medida de Lebesgue de $D \cap [0,x]$ es mayor o igual a cx. Por otro lado, hay un teorema clásico, conocido como el postulado de Bertrand, que dice que siempre existe por lo menos un primo entre m y $2m$, o sea, $d_n < p_n$. En 1931, Westzynthius probó que $\limsup \frac{d_n}{\ln p_n} = \infty$, y en 1963 Rankin, completando un trabajo de Erdös, mostró que

$$\limsup \frac{d_n (\ln\ln\ln p_n)^2}{\ln p_n \ln\ln p_n \ln\ln\ln\ln p_n} \geq e^{\gamma} \approx 1,78107,$$

donde γ es la constante de Euler-Mascheroni,

$$\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \ln n\right) \approx 0,5772156649;$$

este resultado fué mejorado posteriormente por Pomerance y Pintz, que probaron que el lado izquierdo es mayor o igual a $2e^{\gamma}$. Se conjetura que

$$\limsup \frac{d_n}{(\ln p_n)^2} = C,$$

para alguna constante positiva C. Otra conjetura famosa es que siempre hay por lo menos un primo entre n^2 y $(n+1)^2$. Obsérvese que la primera vez que $d_n > 1000$ ocurre para $p_n = 1693182318746371$, cuando $d_n = 1132$, lo que fué descubierto recientemente por T. Nicely y D. Nyman.
Sierpinsky probó que existen infinitos números naturales k tales que $k \cdot 2^n + 1$ es compuesto para todo natural n y Riesel probó el mismo resultado para $k \cdot 2^n - 1$. Se conjeturó que

los menores valores de k con las propiedades descritas anteriormente son respectivamente 78557 y 509203. Hay un proyecto cooperativo que consiste en encontrar primos grandes, para demostrar estas conjeturas (vea http://vamri.xray.ufl.edu/proths/).

Otro problema famoso es el de determinar si existen progresiones aritméticas arbitrariamente largas formadas exclusivamente por primos. Van der Corput probó en 1939 que hay una infinidad de progresiones aritméticas formadas por tres primos. Una respuesta afirmativa al problema general seguiría de la veracidad de una conjetura de Erdös, según en el cuál si $A \subset \mathbb{N}$ y tal que la serie de inversos de sus elementos diverge, entonces A contiene progresiones aritméticas arbitrariamente largas. Actualmente la mayor progresión aritmética de primos que se conoce está formada por 22 términos $11410337850553 + 4609098694200k$, con $0 \leq k \leq 21$, y fué encontrada por Pritchard en 1993.

M. Toplic, uno de los miembros de un proyecto conjunto realizado con la ayuda de la internet encontró el 15 de enero de 1998 el primer ejemplo de 10 números primos consecutivos en progresión aritmética, que son los primos $p + 210k$ con $0 \leq k \leq 9$ donde

$$\begin{aligned} p &= 1009969724697142476377866555879698403295093246891 \\ &\quad 900418036034177589043417033488821590672297 19 \end{aligned}$$

por otro lado, el 23 de Abril de 1999 un grupo de 6 investigadores halló 10 primos palindromes (cuya representación decimal es simétrica) consecutivos en progresión aritmética, que son

$$p + 1010100000000000k, \ con \ 0 \leq k \leq 9$$

donde

$$p = 74295029087000007809205924 7.$$

Capítulo 2

Campos Finitos y Reciprocidad Cuadrática

En este capítulo se verán algunos resultados de álgebra y teoría de números un poco más modernos, abstractos y avanzados que en el capítulo 1. El lector que conoce un poco de algebra tendrá más facilidad para acompañar los resultados que se trabajarán más adelante.

2.1. Campos y Polinomios

Definición 2.1.1. Un grupo $(G, *)$ es un conjunto G dotado de una operación binaria clausurativa $*$ que satisface los axiomas siguientes:

◦ La operación $*$ es asociativa, es decir para todo a, b, c en G se tiene que $a*(b*c) = (a*b)*c$.

◦ Existe un elemento e en G tal que $a * e = e * a = a$ para todo a en G.

◦ Para cada a en G existe un elemento a' en G tal que $a * a' = a' * a = e$.

Definición 2.1.2. Un grupo G se llama abeliano o conmutativo si satisface la condición $a * b = b * a$ para todo a y b en G.

Cuando una operación $*$ se simboliza con $+$ se dice que G es un grupo aditivo y se denota al elemento neutro e, como 0. Si la operación se simboliza con $\cdot$ se dice que G es un grupo multiplicativo y se denota al elemento neutro e por 1. Así, $\mathbb{Z}/(n)$ es un grupo abeliano aditivo y $(\mathbb{Z}/(n))^*$ es un grupo abeliano multiplicativo.

Definición 2.1.3. Un anillo $(A, +, \cdot)$ es un conjunto A dotado de operaciones $+$ y $\cdot$ llamadas adición y multiplicación que satisface los siguientes axiomas:

∘ $(A, +)$ es un grupo abeliano.

∘ La multiplicación es asociativa.

∘ Las dos operaciones están relacionadas por las propiedades distributivas

$$a(b+c) = ab + ac,$$
$$b(a+c) = ba + bc,$$

para todo $a, b, c \in A$.

Definición 2.1.4. Un anillo donde la multiplicación es conmutativa se dice un *anillo conmutativo*. Un anillo que posee identidad para la multiplicación, el cual se representa usualmente por 1, es una *anillo con unitario*.

Definición 2.1.5. Si R es un anillo y $U \subset R$, U es ideal de R si:

(a) U es subgrupo de R.

(b)Para todo $r \in R,\ u \in U;\ ru \in U,\ ur \in U$.

Definición 2.1.6. Un campo es un anillo conmutativo con unitario donde para todo $a \in K$ con $a \neq 0$ existe $b \in K$ tal que $a \cdot b = 1$, o sea K es dotado de dos operaciones $+ : K \times K \longrightarrow K$ y $\cdot : K \times K \longrightarrow K$, de una función $- : K \longrightarrow K$ y dos elementos especiales distintos llamados 0 y 1, satisfaciendo las siguientes propiedades:

$$\begin{aligned} a + (b + c) &= (a + b) + c, \\ a + 0 &= a, \\ a + (-a) &= 0, \\ a + b &= b + a, \\ a(b + c) &= ab + ac, \\ a(bc) &= (ab)c, \\ a1 &= a, \\ ab &= ba; \end{aligned}$$

en donde para todo $a \in K,\ a \neq 0$ existe $b \in K$ tal que

$$ab = 1.$$

Los ejemplos más conocidos de campos son $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$.

Definición 2.1.7. Dado un campo K, se define un anillo conmutativo con unidad $K[x]$ como el conjunto de expresiones de la forma $P = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, donde $n \in \mathbb{N}$ llamados polinomios con coeficientes en K.

Obsérvese que x es un símbolo formal y no un elemento de K, a pesar de eso, cada polinomio define una función polinomial

$$\begin{aligned} P : K &\longrightarrow K \\ c &\longrightarrow P(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n \end{aligned}$$

también llamada P. La diferencia entre un polinomio y una función polinomial es bien ilustrada por el polinomio $P = x^p - x \in (\mathbb{Z}/(p))[x]$: este polinomio es no nulo, pues sus coeficientes son no nulos, pero para todo $x \in \mathbb{Z}/(p)$ por el pequeño teorema de Fermat se tiene que $P(x) = 0$.
Si $P = \sum a_ix^i$ y $Q = \sum b_ix^i$ son polinomios se define la suma como $P + Q = \sum(a_i + b_i)x^i$ y su producto como $PQ = \sum c_ix^i$ donde $c_k = \sum_{i+j=k} a_ib_j$; se define también *grad* P el grado de un polinomio $P = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ como n si $a_n \neq 0$ pero $a_m = 0$ para $m > n$ y el grado del polinomio 0 como $-\infty$.

Lema 2.1.1. *Para cualesquier polinomios, P y Q se tiene grad $(PQ) = grad\ (P) + grad\ (Q)$ y grad $(P + Q) \leq max\{grad\ (P),\ grad\ (Q)\}$.*

Demostración:

(i) *grad* $(PQ) = grad\ (P) + grad\ (Q)$
Sea $P = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$ y $Q = b_0 + b_1x + \cdots + b_mx^m$ con $b_m \neq 0$; $grad\ (P) = n,\ grad\ (Q) = m$, ahora

$$\begin{aligned} grad\ (PQ) &= grad\ [(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m)] \\ &= grad\ [a_0b_0 + a_0b_1x + \cdots + a_0b_mx^m + a_1b_0x + a_1b_1x^2 + \cdots \\ &\quad + a_1b_mx^{m+1} + \cdots + a_nb_0x^n + a_nb_1x^{n+1} + \cdots + a_nb_mx^{n+m}], \end{aligned}$$

ahora como $a_n \neq 0$ y $b_m \neq 0$, se tiene que $a_nb_m \neq 0$, entonces

$$\begin{aligned} grad\ (PQ) &= n + m \\ &= grad\ (P) + grad\ (Q), \end{aligned}$$

(ii) $grad\ (P+Q) \leq max\{grad\ (P),\ grad\ (Q)\}$

Sea $P = a_0 + a_1x + \cdots + a_nx^n$ con $a_n \neq 0$ y $Q = b_0 + b_1x + \cdots + b_mx^m$ con $b_m \neq 0$; $grad\ (P) = n,\ grad\ (Q) = m$, ahora, supóngase que $m \leq n$

$$\begin{aligned} grad\ (P+Q) &= grad\ [(a_0 + a_1x + \cdots + a_nx^n) + (b_0 + b_1x + \cdots + b_mx^m)] \\ &= grad\ [(a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + a_{m+1}x^{m+1} \\ &\quad + \cdots + a_nx^n], \end{aligned}$$

entonces se tiene que el $grad\ (P+Q) \leq n$. Igualmente para $n \leq m$ se tiene que $grad\ (P+Q) \leq m$, entonces

$$grad\ (P+Q) \leq max\{grad\ (P),\ grad\ (Q)\}.$$

■

Teorema 2.1.1. *Sean $A, B \in K[x], B \neq 0$. Entonces existen únicos polinomios $Q, R \in K[x]$ con $A = QB + R$ y* $\text{grad}(R) < \text{grad}(B)$.

Demostración: Esta demostración es hecha por inducción sobre el grado de A. Si $grad(A) < grad(B)$, se toma $Q = 0,\ R = A$. Caso contrario, sea $A = ax^n + a_1x^{n-1} + ...a_n$ y $B = bx^m + b_1x^{m-1} + ...b_m$. Se puede escribir

$$A = \left(\frac{a}{b}\right) x^{n-m}B + A_1,\ con\ grad(A_1) < grad(A).$$

Por la hipótesis de inducción, se tiene

$$A_1 = Q_1B + R,\ con\ grad\ (R) < grad\ (B),$$

reemplazando se tiene

$$\begin{aligned} A &= \left(\frac{a}{b}\right) x^{n-m}B + Q_1B + R. \\ A &= \left(\left(\frac{a}{b}\right) x^{n-m} + Q_1\right) B + R. \end{aligned}$$

Haciendo $Q = \left(\frac{a}{b}\right)x^{n-m} + Q_1$ se tiene

$$A = QB + R,\ con\ grad\ (R) < grad\ (B).$$

La unicidad de obtiene del lema anterior. ■

Un polinomio tiene a a como raíz ($P(a) = 0$) si y solo si $(x-a) \mid P$. Más generalmente, $P(a)$ es el residuo de la división de P por $(x-a)$.

Proposición 2.1.1. *Un polinomio no nulo de grado n tiene máximo n raíces.*

Demostración: Esta demostración es hecha por inducción sobre $n = grad(P)$; los casos $n = 0$ y $n = 1$ son triviales. Supóngase que todo polinomio de grado $n-1$ posee a lo máximo $n-1$ raíces, si P tuviera $n+1$ raíces distintas $a_1,\ a_2, \ldots a_{n+1}$ entonces P sería múltiplo de $(x-a_{n+1});\ P/(x-a_{n+1})$ tiene grado $n-1$ y raíces $a_1,\ a_2, \ldots a_n$ lo que contradice la hipótesis de inducción. ■

Sean $A,\ B \in K[x]$ se define $A \mid B$ si existe C tal que $AC = B$ y se dirá que un polinomio P de grado mayor que $n > 0$, es irreducible si todos sus divisores tienen grado 0 o n, generalizando así el concepto de número primo así como a seguir la generalización de la noción de m.c.d.

Proposición 2.1.2. *Dados polinomios no nulos $A,\ B \in K[x]$ existe un único $D \in K[x]$ (salvo multiplicación por una constante) tal que $D \mid A,\ D \mid B$ y para todo $C \in K[x]$, si $C \mid A$ y $C \mid B$ entonces $C \mid D$. Además existen $E,\ F \in K[x]$ con $D = AE + BF$.*

Demostración: Sea $I(A,B) = \{AE + BF;\ E,\ F \in K[x]\}$ y sea $D = AE_0 + BF_0$ el polinomio de grado menor no nulo de $I(A,B)$. Supóngase que $D \nmid A$, como $D \in K[x]$, existen $Q,\ R \in K[X]$ tal que $A = DQ + R$ con $R \neq 0$ y $0 \leq grad\ (R) \leq grad\ (D)$, ahora

$$\begin{aligned} R &= A - DQ \\ R &= A - (AE_0 + BF_0)Q \\ R &= A(1 - QE_0) + B(-QF_0) \end{aligned}$$

como $(1-QE_0),\ B(-QF_0) \in K[X]$ entonces $R \in I(A,B)$ pero como D es el menor elemento no nulo de $I(A,B)$ y $grad\ (R) \leq grad\ (D)$ entonces $R = 0$, lo que es absurdo, entonces $D \mid A$. Análogamente $D \mid B$. Sea $C \in K[X]$, se supone que $C \mid A$ y $C \mid B$, luego $C \mid (AE + BF)$ para cualquier $E,\ F \in K[X]$, entonces $C \mid D$. ■

Proposición 2.1.3. *Sea P un polinomio irreducible y sean A_1 y A_2 en $K[x]$. Si $P \mid (A_1 \cdot A_2)$ entonces $P \mid A_1$ o $P \mid A_2$.*

Demostración: Supóngase que $P \nmid A_1$ y que $P \nmid A_2$, entonces

$$\begin{aligned} A_1 &= P \cdot Q_1 + R_1 \ \ donde \ \ grad(R_1) < grad(P), \\ A_2 &= P \cdot Q_2 + R_2 \ \ donde \ \ grad(R_2) < grad(P), \end{aligned}$$

multiplicando se tiene

$$\begin{aligned} A_1 \cdot A_2 &= (P \cdot Q_1 + R_1) \cdot (P \cdot Q_2 + R_2), \\ &= P^2 Q_1 Q_2 + P Q_1 R_2 + R_1 P Q_2 + R_1 R_2, \\ &= P(P Q_1 Q_2 + Q_1 R_2 + R_1 Q_2) + R_1 R_2, \\ &= PS + R_1 R_2, \end{aligned}$$

donde $S = PQ_1Q_2 + Q_1R_2 + R_1Q_2$, luego, existen dos posibilidades

1. Si el $grad(R_1R_2) < grad(P)$, se tiene que $P \nmid A_1 \cdot A_2$.

2. Si el $grad(R_1R_2) \geq grad(P)$, se puede escribir $R_1R_2 = P \cdot Q_3 + R_3$ donde $grad(R_3) < grad(P)$ entonces se tiene que

$$\begin{aligned} A_1 \cdot A_2 &= PS + P \cdot Q_3 + R_3, \\ &= P(S + Q_3) + R_3 \end{aligned}$$

de donde se concluye que $P \nmid A_1 \cdot A_2$.

de 1 y 2 se concluye que $P \nmid A_1 \cdot A_2$, lo que es una contradicción.
Entonces $P \mid A_1$ o $P \mid A_2$. ■

Corolario 2.1.1. *Sea P un polinomio irreducible y sean $A_1, A_2, \ldots A_m \in K[x]$. Si $P \mid (A_1A_2 \ldots A_m)$ entonces $P \mid A_i$ para algún $i, 1 \leq i \leq n$.*

Demostración: Para esta prueba basta hacer inducción y hacer un razonamiento similar al que se utilizó para demostrar la proposición anterior.

Teorema 2.1.2. *Todo polinomio puede ser factorizado como un producto de polinomios irreducibles; esta factorización es única salvo por el orden de los factores.*

Demostración: Sea $P \in K[x]$ un polinomio no constante. Si P no es irreducible, entonces $P = QR$ donde el $grad\ (Q) < grad\ (P)$ y el $grad\ (R) < grad\ (P)$. Si P y Q son irreducibles, se para aquí. De no ser así, al menos uno de ellos se factoriza en polinomios de grado menor. Continuando este proceso, se llega a la factorización

$$P = S_1 S_2 \cdots S_k$$

donde S_i es irreducible. Para probar la unicidad se supone que

$$P = S_1 S_2 \cdots S_k = Q_1 Q_2 \cdots Q_r$$

son dos factorizaciones de P en polinomios irreducibles. Entonces, por la Corolario 2.1.1, S_1 divide algún Q_j , supóngase que a Q_1. Como Q_1 es irreducible,

$$Q_1 = U_1 S_1,$$

donde $U_1 \neq 0$, pero U_1 esta en $K[x]$ y es por tanto una unidad (que tiene inverso en $K[x]$). Entonces, al sustituir Q_1 por $U_1 S_1$ y cancelar, se obtiene

$$S_2 \cdots S_k = U_1 Q_2 \cdots Q_r$$

Por un argumento similar, se dice que $Q_2 = U_2 S_2$, así que

$$S_3 \cdots S_k = U_1 U_2 Q_3 \cdots Q_r.$$

Al continuar así, por último se llegará a que

$$1 = U_1 U_2 \cdots U_k Q_{k+1} \cdots Q_r.$$

Claramente, esto es posible sólo si $k = r$ de modo que esta ecuación es en realidad $1 = U_1 U_2 \cdots U_k$. Así, los factores irreducibles S_i y Q_j son los mismos, excepto quizá, por el orden y los factores unidad. ■

Los ejemplos más evidentes de polinomios irreducibles son los de la forma $x - a$, con $a \in K$. Cuando estos son los únicos polinomios irreducibles se dirá que el campo es algebraicamente cerrado. Los polinomios de grado 2 y 3 son irreducibles si y sólo si no tienen raíces.

El pequeño teorema de Fermat también admite una formulación en términos de polinomios.

Teorema 2.1.3. *Sea p primo en $(\mathbb{Z}/(p))[x]$ entonces*

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

Demostración: Los dos polinomios de los dos lados de la ecuación tienen grado p y el coeficiente de x^p es 1 en los dos casos. Así, la diferencia tiene grado menor que p pero se anula en p puntos:$0,\ 1, \ldots p-1$. Por el Teorema 2.1.2, esta diferencia debe ser el polinomio cero. ■

Se puede definir también congruencias en $K[x]$ de la siguiente forma:

$$A \equiv B \ (mod\ P) \Longleftrightarrow P \mid (B - A).$$

Las propiedades básicas de congruencias pueden ser traducidas para este nuevo contexto y se puede definir el cociente $K[x]/(P)$ de la misma forma como se definió $\mathbb{Z}/(n)$.
A continuación se verá un ejemplo de como construir un campo finito como $(\mathbb{Z}/(p)[x])/P$ cuando $P \in (\mathbb{Z}/(p))[x]$ es irreducible.

Ejemplo 2.1.1. El polinomio x^2+x+1 es irreducible en $(\mathbb{Z}/(2))[x]$ lo que permite construir un campo de cuatro elementos: $0,\ 1,\ x$ y $x+1$. Las operaciones en $\mathbb{Z}/(2)$ y la relación $x^2 = x+1$ definen las operaciones en este campo (se denotará $x+1$ por x')

$+$	**0**	**1**	**x**	**x′**
0	0	1	x	x'
1	1	0	x'	x
x	x	x'	0	1
x′	x'	x	1	0

$*$	**0**	**1**	**x**	**x′**
0	0	0	0	0
1	0	1	x	x'
x	0	x	x'	1
x′	0	x'	1	x

De hecho existen en $\mathbb{Z}/(p)[x]$ polinomios irreducibles de cualquier grado y todo campo finito puede ser construido de esta forma.

2.2. Ordenes Y Raíces Primitivas

Definición 2.2.1. Dados $a, n \in \mathbb{Z}$ con $n > 0$ y $(a, n) = 1$, se define el orden de a módulo n denotada por $ord_n\ a$, como el menor entero positivo t tal que $a^t \equiv 1(mod\ n)$. De igual forma si K es un campo finito y $a \in K,\ a \neq 0$, se define el orden de a en K, denotada por $ord_K\ a$, como el menor entero positivo t tal que $a^t = 1 \in K$; además $ord_p a = ord_{n/(p)} a$ donde p es primo.

Teorema 2.2.1. *$a^e \equiv a^{e'}(mod\ n)$ si y solo si $e \equiv e'(mod\ ord_n a)$*

Demostración: Supóngase que $ord_n\ a = t$, si $e \equiv e'(mod\ t)$ entonces $e = e' + tq$ para algún entero q y por lo tanto

$$a^e = a^{e'+tq} = a^{e'}(a^t)^q = a^{e'}(1)^q \equiv a^{e'}(mod\ n)$$

por que $a^t \equiv 1(mod\ n)$.
Recíprocamente, se supone que $a^e \equiv a^{e'}(mod\ n)$. Sin perder generalidad se puede asumir que $e \geq e'$. Como $(a, n) = 1$ se puede cancelar repetidamente a hasta obtener $a^{e-e'} \equiv 1(mod\ n)$, pero como $ord_n\ a = t$, entonces $t \mid (e - e')$ o sea $e \equiv e'(mod\ ord_n a)$. ■
Por el teorema de Euler, se tiene que $ord_n a \mid \Phi(n)$.

Definición 2.2.2. Se dice que a es una raíz primitiva módulo n si $ord_n a = \Phi(n)$. Análogamente, se dice que a es una raíz primitiva en K si $ord_K a = q - 1$ donde $q = |K|$ es el número de elementos de K.

Ejemplo 2.2.1. 2 es raíz primitiva módulo 5, ya que $2^4 \equiv 1(mod\ 5)$ $ord_5 2 = 4$, pero no es raíz primitiva módulo 7 porque $2^3 \equiv 1(mod\ 7)$, $ord_7 2 = 3$.

Se precisa una versión del pequeño teorema de Fermat para campos finitos:

Teorema 2.2.2. *Si K es un campo finito y $q = |K|$ entonces $a^q - a = 0$ para todo $a \in K$*

Demostración: Si $a = 0$ el teorema es cierto; se supone entonces $a \neq 0$. Sean $b_1, \ldots b_{q-1}$ los elementos no nulos de K. Los elementos $ab_1, \ldots ab_{q-1}$ son todos no nulos y distintos, luego son los mismos $b_1, \ldots b_{q-1}$ solo que en diferente orden. Así

$$\begin{aligned} b_1 \cdot b_2 \cdots b_{q-1} &= (ab_1)(ab_2)\cdots(ab_{q-1}) \\ &= a^{q-1}(b_1 \cdot b_2 \cdots b_{q-1}) \end{aligned}$$

luego $a^{q-1} = 1$, multiplicando por a se tiene $a^q = a$, entonces $a^q - a = 0$. ■
De este teorema se sigue que $ord_K a \mid q - 1$, análogo a lo que se sabía para $\mathbb{Z}/(n)$. A partir del Teorema 2.1.3 se tiene también que

$$x^q - x = x(x - b_1)\cdots(x - b_{q-1})$$

en $K[x]$.

2.3. Ley de Reciprocidad Cuadrática

La ley de Gauss de reciprocidad cuadrática afirma que si p y q son primos, hay una relación directa entre, p ser cuadrado módulo q y q ser cuadrado módulo p. Este teorema suministra un rápido algoritmo para determinar si a es cuadrado módulo p, donde a es un entero y p un número primo. Esta ley fué establecida por primera vez por Euler una forma muy complicada y fué redescubierta por Legendre, quien la demostró parcialmente en 1785. Gauss descubrió esta ley a la edad de 18 años en 1796 y presento su primera demostración completa.

Definición 2.3.1. Sea p un número primo impar y a un entero tal que $(a, p) = 1$. Si la congruencia

$$x^2 \equiv a(mod\ p)$$

tiene solución, se dice que a es un residuo cuadrático módulo p.

Ejemplo 2.3.1. Como los residuos cuadráticos módulo p, son precisamente los cuadrados módulo p, veamos que si $p = 7$, los residuos cuadráticos incongruentes módulo 7 son 1, 4 y 2 ya que,

$$1^2 \equiv 6^2 \equiv 1(mod\ 7),\ 2^2 \equiv 5^2 \equiv 4(mod\ 7)\ y\ 3^2 \equiv 4^2 \equiv 2(mod\ 7).$$

En general si $(a, p) = 1$, se sigue de la definición que a^2 es un residuo cuadrático módulo p.

Para facilitar el estudio de los residuos cuadráticos se introducirá el símbolo de Legendre mediante la siguiente definición.

Definición 2.3.2. Sea p un primo y a un entero donde $(a, p) = 1$. Se define el símbolo de Legendre $\left(\frac{a}{p}\right)$ por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático módulo } p \\ -1 & \text{si } a \text{ no es un residuo cuadrático módulo } p \end{cases}$$

Ejemplo 2.3.2.

(1) $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$

(2) $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$

Proposición 2.3.1. *Sea p un primo impar y a un entero tal que $p \nmid a$. Entonces*

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

Demostración: Se sabe que si $p \nmid a$ entonces $a^{p-1} \equiv 1(mod\ p)$, o sea, $X^{p-1} - 1$ tiene como raíces $1,\ 2, \ldots, p-1$ en $\mathbb{Z}/(p)$. Por otro lado,

$$X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1).$$

Si existe $b \in \mathbb{Z}$ tal que $a \equiv b^2 (mod\ p)$ entonces

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1(mod\ p);$$

o sea,

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

Como

$$X^2 \equiv Y^2 (mod\ p) \Longleftrightarrow X \equiv \pm Y (mod\ p),$$

hay por lo menos $\dfrac{p-1}{2}$ cuadrados en $(\mathbb{Z}/(p))^*$, luego los cuadrados son exactamente las raíces de $X^{\frac{p-1}{2}} - 1$ en $\mathbb{Z}/(p)$, donde los que no son cuadrados son exactamente las raíces de $X^{\frac{p-1}{2}} + 1$, o sea, si $\left(\dfrac{b}{p}\right) = -1$ entonces

$$b^{\frac{p-1}{2}} \equiv -1(mod\ p).$$

■

Lema 2.3.1 (Lema de Gauss). *Sea p un primo impar y sea a un entero tal que $(a, p) = 1$. Sea S el conjunto formado por los menores residuos positivos módulo p, de los números*

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a.$$

Si k representa el número de residuos que son mayores que $p/2$, entonces

$$\left(\frac{a}{p}\right) = (-1)^k.$$

Demostración: Se define t por $k + t = (p-1)/2$ y se representan los elementos de S por $a_1, a_2, \ldots, a_t, b_1, b_2, \ldots, b_k$ donde $a_i < p/2$ para cada i y $b_j > p/2$ para cada j.
Primero hay que probar que todos los elementos de S no son congruentes módulo p. De

hecho, si $m_1 \neq m_2$ $m_1 a \equiv m_2 a (mod\ p)$ entonces $p \mid (m_1 - m_2)a$ y como $(a, p) = 1$ entonces $p \mid (m_1 - m_2)$ lo cual es imposible porque $0 < m_1, m_2 \leq (p-1)/2$.
Lo segundo que hay que ver es que $a_i \neq p - b_j$ para todo i y para todo j. De hecho, si $a_i = p - b_j$, entonces $a_i + b_j \equiv 0 (mod\ p)$ y como $a_i = m_i a,\ b_j = m_j a$ para ciertos enteros m_i y m_j con $m_1 \neq m_2$, entonces se tendría $m_i a + m_j a \equiv 0 (mod\ p)$. Luego $p \mid (m_i + m_j)a$ y como $(a, p) = 1$ entonces $p \mid (m_i + m_j)$ lo que es imposible porque $2 < m_i + m_j \leq p - 1$.
Se tiene entonces que $a_1, a_2, \ldots, a_t, p - b_1, p - b_2, \ldots, p - b_k$ son todos diferentes, luego ellos son simplemente los números $1, 2, \ldots, (p-1)/2$ en algún orden, por lo tanto se tiene,

$$\begin{aligned} 1 \cdot 2 \cdots \frac{p-1}{2} &\equiv (p - b_1)(p - b_2) \cdots (p - b_k) a_1 a_2 \cdots a_t (mod\ p) \\ &\equiv (-b_1)(-b_2) \cdots (-b_k) a_1 a_2 \cdots a_t (mod\ p) \\ &\equiv (-1)^k b_1 b_2 \cdots b_k a_1 a_2 \cdots a_t (mod\ p), \end{aligned}$$

y como

$$b_1 b_2 \cdots b_k a_1 a_2 \cdots a_t = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot a^{\frac{p-1}{2}},$$

se tiene

$$\frac{p-1}{2}! \equiv (-1)^k \frac{p-1}{2}! a^{\frac{p-1}{2}} (mod\ p),$$

multiplicando por $(-1)^k$ y cancelando se obtiene

$$(-1)^k \equiv a^{\frac{p-1}{2}} (mod\ p),$$

que se puede escribir

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

Como $(-1)^k$ y (a/p) toman solo valores ± 1, se sigue de la congruencia anterior que

$$(-1)^k = \left(\frac{a}{p}\right).$$

■

Proposición 2.3.2. *Si p es primo impar y sea a un entero tal que $(a, p) = 1$. Sea*

$$M = [a/p] + [2a/p] + \cdots \left[\frac{1}{2}\frac{a(p-1)}{p}\right]$$

donde si $a = bq + r$ con $o \leq r < b$ se tiene que $[a/b] = q$ entonces

1. *Si a es impar, $(a/p) = (-1)^M$.*

2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \begin{cases} 1 & Si\ p \equiv \pm 1 (mod\ 8) \\ -1 & si\ p \equiv \pm 3 (mod\ 8) \end{cases}$

Demostración: Sean $r_1, r_2, \ldots r_{\frac{p-1}{2}}$ los menores residuos positivos modulo p de los números

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a.$$

se tiene entonces que

$$\begin{aligned} a &= p[a/p] + r_1 \\ 2a &= p[2a/p] + r_2 \\ &\vdots \\ \frac{p-1}{2}a &= p\left[\frac{1}{2}\frac{a(p-1)}{p}\right] + r_{\frac{p-1}{2}} \end{aligned}$$

sumando estas ecuaciones se obtiene

$$\begin{aligned} \left(1 + 2 + \cdots + \frac{p-1}{2}\right)a &= p\left([a/p] + [2a/p] + \cdots \left[\frac{1}{2}\frac{a(p-1)}{p}\right]\right) + r_1 + r_2 + \cdots + r_{\frac{p-1}{2}} \\ \frac{p^2-1}{8}a &= pM + r_1 + r_2 + \cdots + r_{\frac{p-1}{2}} \end{aligned}$$

Con las notaciones del lema de Gauss se puede escribir la ecuación anterior en la forma

$$\frac{p^2-1}{8}a = pM + (a_1 + a_2 + \cdots + a_t) + (b_1 + b_2 + \cdots + b_k). \tag{2.1}$$

En la demostración del lema de Gauss se vió que los números $p-b_1, p-b_2, \ldots, p-b_k, a_1, a_2 \ldots, a_t$ son simplemente los números $1, 2, \ldots, \frac{p-1}{2}$ en algún orden, por lo tanto

$$1 + 2 + \cdots + \frac{p-1}{2} = kp - b_1 - b_2 - \cdots - b_k + a_1 + a_2 + \cdots + a_t,$$

o sea

$$\frac{p^2-1}{8} = kp - b_1 - b_2 - \cdots - b_k + a_1 + a_2 + \cdots + a_t \tag{2.2}$$

restando (2.2) de (2.1) se obtiene

$$\frac{p^2-1}{8}(a-1) = p(M-k) + 2b_1 + 2b_2 + \cdots 2b_k$$

y como p es impar

$$\frac{p^2-1}{8}(a-1) \equiv (M-k)(mod\ 2).$$

Si a es impar, la congruencia anterior implica que $M \equiv k(mod\ 2)$ y por lo tanto por el lema de Gauss,

$$(-1)^M = (-1)^k = \left(\frac{a}{p}\right).$$

Ahora si $a = 2,\ M = 0$ puesto que $[2j/p] = 0$ para $1 \leq j \leq (p-1)/2$ ya que para estos casos $2 \leq 2j < p$, se tiene que

$$\frac{p^2-1}{8}(a-1) \equiv -k \equiv k(mod\ 2),$$

y por el lema de Gauss

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

por otro lado, se tienen dos posibilidades, la primera es que $\frac{p^2-1}{8}$ sea par, luego

$$\begin{aligned} \frac{p^2-1}{8} = 2k &\Rightarrow 8 \mid p^2-1 = (p-1)(p+1) \\ &\Rightarrow 8 \mid (p-1)\ o\ 8 \mid (p+1) \\ &\Rightarrow p \equiv \pm 1(mod\ 8) \end{aligned}$$

entonces $\left(\frac{2}{p}\right) = 1$ si $p \equiv \pm 1(mod\ 8)$. La segunda posibilidad es que $\frac{p^2-1}{8}$ sea impar, luego

$$\begin{aligned} \frac{p^2-1}{8} &= 2k+1 \\ p^2-1 &= 8(2k)+8 \\ p^2-9 &= 8(2k) \\ (p-3)(p+3) &= 8(2k) \Rightarrow 8 \mid (p-3)\ o\ 8 \mid (p+3) \Rightarrow p \equiv \pm 3(mod\ 8) \end{aligned}$$

entonces $\left(\frac{2}{p}\right) = -1$ si $p \equiv \pm 3(mod\ 8)$. ■

Teorema 2.3.1 (Ley de Reciprocidad Cuadrática). *Sean p y q primos impares diferentes. Entonces,*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2(q-1)/2}.$$

Demostración: Sean

$$M = [q/p] + [2q/p] + \cdots \left[\frac{1}{2}\frac{q(p-1)}{p}\right]$$

y

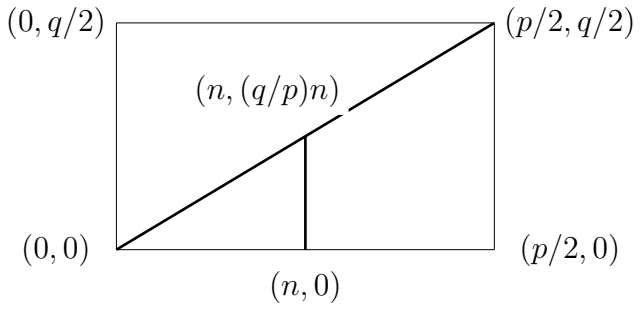
$$N = [p/q] + [2p/q] + \cdots \left[\frac{1}{2}\frac{p(q-1)}{q}\right]$$

por el teorema anterior se tiene que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^M(-1)^N = (-1)^{M+N}$$

y es suficiente demostrar que $M + N = (p-1)/2(q-1)/2$.

Consideremos el rectángulo R en el plano cuyos vértices son $(0,0),\ (p/2,0),\ (0,q/2),\ (p/2,q/2)$ sin incluir su frontera.



Si se llama *punto reticular* a un punto (x, y) que tiene ambas coordenadas enteras, se ve que el rectángulo contiene $(p-1)/2(q-1)/2$ puntos reticulares. También hay que observar que sobre la diagonal que une $(0,0)$ con $(p/2, q/2)$ no hay puntos reticulares. De hecho, como la ecuación de la recta que une estos puntos es $py = qx$, si hubiera un punto reticular sobre la recta se tendría que $p \mid qx$ y como $(p,q) = 1$ entonces $p \mid x$, pero esto es imposible porque $x < p/2$.

Por otra parte, para todo entero positivo n, el número d puntos reticulares sobre la recta vertical que pasa por $(n,0)$ y que se encuentran por debajo de la diagonal es $[nq/p]$. Por lo tanto, el número de puntos reticulares en el rectángulo R que están por debajo e la diagonal es precisamente M. Similarmente, el número de puntos reticulares en el rectángulo R que están por encima de la diagonal es N, y por lo tanto

$$M + N = \frac{(p-1)}{2}\frac{(q-1)}{2}.$$

■

Como $(q/p) = \pm 1$, entonces $(q/p)^2 = 1$ y se puede expresar la ley de reciprocidad cuadrática en la forma

$$\left(\frac{p}{q}\right) = (-1)^{(p-1)/2(q-1)/2}\left(\frac{q}{p}\right)$$

que es más conveniente para estudiar el carácter cuadrático de un entero.

Ejemplo 2.3.3. Determinemos si 60 es un residuo cuadrático módulo 239.
Como $60 = 2^2 \cdot 3 \cdot 5$, entonces

$$\left(\frac{60}{239}\right) = \left(\frac{2}{239}\right)^2 \left(\frac{3}{239}\right)\left(\frac{5}{239}\right)$$

ahora

$$\begin{aligned}\left(\frac{2}{239}\right)^2 &= 1\\ \left(\frac{3}{239}\right) &= (-1)^{\frac{1}{2}(238)\frac{1}{2}(2)}\left(\frac{239}{3}\right) = (-1)\left(\frac{239}{3}\right)\end{aligned}$$

multiplicando, hallando el residuo al dividir por tres y aplicando 2.3.2, se tiene:

$$\begin{aligned}\left(\frac{3}{239}\right) &= -\left(\frac{2}{3}\right)\\ &= -(-1) = 1.\end{aligned}$$

y

$$\begin{aligned}\left(\frac{5}{239}\right) &= (-1)^{\frac{1}{2}(238)\frac{1}{2}(4)}\left(\frac{239}{5}\right) = \left(\frac{239}{5}\right)\\ &= \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1\end{aligned}$$

Por lo tanto, $(60/239) = 1$ y así, 60 es un residuo cuadrático módulo 239.

2.4. Extensiones Cuadráticas de Campos Finitos

Sean p primo y d un entero que no sea cuadrado perfecto. El anillo $(\mathbb{Z}/(p))[\sqrt{d}]$ es el conjunto

$$\{a + b\sqrt{d},\ a, b \in \mathbb{Z}/(p)\}$$

donde la adición y la multiplicación se definen como,

$$\begin{aligned}(a + b\sqrt{d}) + (a' + b'\sqrt{d}) &= (a + a') + (b + b')\sqrt{d},\\ (a + b\sqrt{d})(a' + b'\sqrt{d}) &= (aa' + dbb') + (ab' + a'b)\sqrt{d}.\end{aligned}$$

Por definición,

$$a + b\sqrt{d} = a' + b'\sqrt{d} \Longleftrightarrow a = a',\ b = b'.$$

Como grupo aditivo, $(\mathbb{Z}/(p))[\sqrt{d}] = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$. Se va a investigar una estructura multiplicativa de $(\mathbb{Z}/(p))[\sqrt{d}]$. Obsérvese inicialmente que, si d es un cuadrado módulo p entonces $(\mathbb{Z}/(p))[\sqrt{d}]$ no puede ser un campo, pues si $a^2 = d$ en $\mathbb{Z}/(p)$ entonces $(a + \sqrt{d})(a - \sqrt{d}) = a^2 - d = 0$ en $(\mathbb{Z}/(p))[\sqrt{d}]$. La siguiente proposición es el recíproco de este hecho.

Proposición 2.4.1. *Si* $\left(\frac{d}{p}\right) = -1$ *entonces* $(\mathbb{Z}/(p))[\sqrt{d}]$ *es un campo.*

Demostración: Para esta demostración solo se probará la existencia del inverso ya que las demás propiedades se verifican con facilidad teniendo en cuenta como se definieron las operaciones, entonces si $(a, b) \neq (0, 0)$, $(a + b\sqrt{d})^{-1} = (a - b\sqrt{d})/(a^2 - db^2)$. Se tiene que $a^2 - db^2 \in (\mathbb{Z}/(p))^*$ pues d no es cuadrado módulo p. Para probar que el inverso siempre existe basta con mostrar que $a^2 - db^2 \neq 0$.

1. Si $b \neq 0$, y $a^2 - db^2 = 0$, que equivale a $d = (a/b)^2$, se tendría una contradicción.

2. Si $b = 0$, $a^2 - db^2 = a^2 \neq 0$ pues $(a, b) \neq (0, 0) \Rightarrow a \neq 0 \Rightarrow a^2 \neq 0$.

entonces el inverso siempre existe. ■

Capítulo 3

Primos de Mersenne y Pruebas de Primalidad.

Varias fórmulas han sido propuestas para generar números primos arbitrariamente grandes, Fermat, por ejemplo, conjeturó que todo número de la forma $2^{2^n}+1$ es primo, lo que fué desmentido por Euler ($2^{2^5}+1 = 641 \cdot 6700417$ es compuesto). A pesar de los esfuerzos, no se conoce ninguna fórmula simple para generar primos arbitrariamente grandes y la mayoría de los matemáticos creen que no existe una fórmula de este tipo.
Existen algunas fórmulas que generan familias interesantes de primos. La fórmula de este tipo que más interesa es $M_p = 2^p - 1$, llamados números de Mersenne. Cuando M_p es primo, se dirá que M_p es un primo de Mersenne. Parte de la razón por la cuál los números de esta forma son interesantes es que a pesar de que M_p no siempre es primo es relativamente fácil probar para un exponente p dado, incluso bastante grande, si M_p es primo o compuesto. En gran parte por este motivo los diez mayores primos conocidos hasta hoy son primos de Mersenne y a lo largo de la historia el mayor primo conocido casi siempre fué un primo de Mersenne.

3.1. Fórmulas para Primos y Pruebas de Primalidad.

Se mencionó en la introducción de este capítulo que no se conoce ninguna fórmula simple para generar primos arbitrariamente grandes. Existen fórmulas que generan números primos pero que son tan complicadas que no ayudan mucho a generar números primos explícitamente ni a responder preguntas teóricas sobre la distribución de los primos. Un ejemplo de fórmulas

para p_n, el enésimo primo es

$$p_n = \left\lfloor 1 - \frac{1}{\ln 2} \ln \left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor,$$

donde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$.

Ejemplo 3.1.1. Vamos a calcular p_4, tenemos que $p_{4-1} = p_3 = 2 \cdot 3 \cdot 5 = 30$, primero calculemos la sumatoria:

$$\begin{aligned}
\sum_{d|30} \frac{\mu(d)}{2^d - 1} &= \left(\frac{1}{2-1} + \frac{-1}{2^2-1} + \frac{-1}{2^3-1} + \frac{-1}{2^5-1} + \frac{1}{2^6-1} + \frac{1}{2^{10}-1} + \frac{1}{2^{15}-1} + \frac{-1}{2^{30}-1} \right) \\
&= \left(1 - \frac{1}{3} - \frac{1}{7} - \frac{1}{31} + \frac{1}{63} + \frac{1}{1023} + \frac{1}{32767} - \frac{1}{1073741823} \right) \\
&= 0,508432509851113436604955640253 57
\end{aligned}$$

ahora reemplazando en la fórmula

$$\begin{aligned}
p_4 &= \left\lfloor 1 - \frac{1}{\ln 2} \ln \left(-\frac{1}{2} + (0,508432509851113436604955640253 57) \right) \right\rfloor \\
&= \left\lfloor 1 - \frac{1}{\ln 2} (-4,775660822797495487190874194900 8) \right\rfloor \\
&= \lfloor 7,889822186017653381222020791826 3 \rfloor \\
&= 7
\end{aligned}$$

Otra fórmula es

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

donde

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0,0203000500000007\ldots$$

La inutilidad de esta última fórmula viene del hecho que para calcular c se debe encontrar todos los primos; la fórmula se tornaría mas interesante si existiera otra interpretación para el número real c, lo que parece muy improbable. Por otro lado, existe un número real $a > 1$ tal que $\lfloor a^{3^n} \rfloor$ es siempre primo.

Algo relacionado con generar números primos es el de probar si un determinado número es primo. Existe un algoritmo bastante simple para probar si cualquier entero positivo n es primo: calcular el residuo de la división de n por cada entero m con $2 \leq m \leq \sqrt{n}$. Si el residuo es cero en algún caso entonces n es compuesto y se encuentra un divisor; si esto

nunca ocurre, n es primo. El inconveniente de este algoritmo es que es muy lento: incluso para un entero de 200 dígitos se tendrían que hacer aproximadamente 10^{100} divisiones lo que por el momento está fuera del alcance de nuestra tecnología para lograrlo rápidamente.
Algunos teoremas de teoría de números pueden ser usados para probar la primalidad de un entero positivo n. Por el teorema de Wilson, por ejemplo, se puede probar la primalidad de n calculando $(n-1)!\ mod\ n$, infelizmente, esta operación parece ser tan difícil de efectuar como la búsqueda de los divisores del algoritmo anterior, claro que no esta excluida la posibilidad de que alguien invente un algoritmo rápido para calcular $(n-1)!\ mod\ n$.
Una idea mejor es la de usar el pequeño teorema de Fermat, se toma $a,\ 1 < a < n$ y se calcula $a^{n-1}\ mod\ n$. Si n es primo se tiene $a^{n-1} \equiv 1(mod\ n)$; cualquier otro resultado indica que n es compuesto incluso se encontró un factor de n.
Si $a^{n-1} \equiv 1(mod\ n)$, por otro lado, no se demostró que n es primo; si n es compuesto satisfaciendo $a^{n-1} \equiv 1(mod\ n)$ se dirá que n es un pseudoprimo de a. Los pseudoprimos existen pero son raros: el menor pseudoprimo de 2 es $341 = 11 \cdot 31$ y existen apenas 21853 pseudoprimos de 2 menores que $2,5 \cdot 10^{10}$ (contra 1091987405 primos). Pomerance (mejorando un resultado anterior de Erdös) probó que si $P\pi_a(x)$ es el número de pseudoprimos hasta x de a se tiene que

$$P\pi_a(x) \leq x \cdot e^{-\frac{\ln x \ln\ln\ln x}{2 \ln\ln x}}$$

para x suficientemente grande. La siguiente proposición exhibe una familia infinita de pseudoprimos de a (para cualquier $a > 1$ dado); así la simple verificación de $a^{n-1} \equiv 1(mod\ n)$ no demuestra la primalidad de n.

Proposición 3.1.1. *Sea $a > 1$ y p primo, $p > 2$. Entonces*

$$n = \frac{a^{2p}-1}{a^2-1} = \frac{a^p-1}{a-1} \cdot \frac{a^p+1}{a+1}$$

es un pseudoprimo de a.

Demostración: Por el pequeño teorema de Fermat,

$$\frac{a^p-1}{a-1} \equiv \frac{a^p+1}{a+1} \equiv 1(mod\ p)$$

primero se probara que estos números son impares,

$$\frac{a^p-1}{a-1} = a^{p-1} + a^{p-2} + a^{p-3} + \cdots a + 1$$

1. Si a es par, a^r es par y como $\underbrace{a^{p-1}+a^{p-2}+a^{p-3}+\cdots a}$ tiene una cantidad par de números, entonces su suma es par y al sumarle 1 el resultado da impar.

2. Si a es impar, a^r es impar y como $\underbrace{a^{p-1}+a^{p-2}+a^{p-3}+\cdots a}$ tiene una cantidad par de elementos entonces su suma es par y al sumarle 1 el resultado da impar.

para $\frac{a^p+1}{a+1}$ se realiza un razonamiento similar, entonces se tiene que $n \equiv 1(mod\ 2p)$ o $n = 2kp+1$ para k entero. Así, como $a^{2p} \equiv 1(mod\ n)$ se tiene que $a^n = a^{2kp+1} = (a^{2p})^k \cdot a \equiv a(mod\ n)$, entonces $a^n \equiv a(mod\ n)$ lo que concluye la demostración. ■

Una idea natural es la de probar varios valores de a. Si $(a,n) > 1$, se tiene que $a^{n-1} \not\equiv 1(mod\ n)$; mientras que, si n es un producto de pocos primos grandes, los valores de a para los cuales $(a,n) > 1$ son extraños y obligan a encontrar un valor tal de a que el progreso sería muy poco en relación a los primeros algoritmos. De hecho, una vez encontrado a con $(a,n) > 1$ es fácil encontrar (a,n) por el algoritmo de Euclides, lo que da una factorización (parcial) de n. Es un hecho interesante que existen algunos números compuestos extraños n, llamados *números de Carmichael*, con la propiedad que si $0 < a < n$ y $(a,n) = 1$ entonces $a^{n-1} \equiv 1(mod\ n)$. Un hecho demostrado por Alford, Granville y Pomerance es que si $CN(x)$ es la cantidad de números de Carmichael menores que x entonces $CN(x) \geq x^{2/7}$ para x suficientemente grande, lo que implica la existencia de infinitos números de Carmichael. Hay apenas 2163 números de Carmichael menores que $2,5 \cdot 10^{10}$ y los primeros son 561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 y 75361.

3.2. Pruebas Basadas en Factorizaciones de $n-1$

Proposición 3.2.1. *Sea $n > 1$. Si para cada factor primo q de $n-1$ existe un entero a_q tal que $a_q^{n-1} \equiv 1(mod\ n)$ y $a_q^{(n-1)/q} \not\equiv 1(mod\ n)$ entonces n es primo.*

Demostración: Sea q^{k_q} la mayor potencia de q que divide $n-1$. Como $a_q^{(n-1)/q} \not\equiv 1(mod\ n)$ el orden de a_q en $(\mathbb{Z}/(n))^*$ es un múltiplo de q^{k_q}, ahora como $\Phi(n)$ es múltiplo del orden de a_q, entonces $\Phi(n)$ es múltiplo de q^{k_q}. Como esto vale para todo factor primo q de $n-1$, $\Phi(n)$ es un múltiplo de $n-1$ entonces n es primo. ■

Proposición 3.2.2 (Pocklington). *Si $n-1 = q^k R$ donde q es primo y existe un entero a tal que $a^{n-1} \equiv 1(mod\ n)$ y $(a^{(n-1)/q} - 1,\ n) = 1$ entonces cualquier factor primo de n es congruente a 1 módulo q^k.*

Demostración: Si p es un factor primo de n y como $a^{n-1} \equiv 1(mod\ n)$ se tiene que $a^{n-1} \equiv 1(mod\ p)$ además $(a^{(n-1)/q} - 1,\ n) = 1$ entonces p no divide a $a^{(n-1)/q} - 1$, luego el $ord_p a$, divide a $n-1$ pero no divide a $(n-1)/q$. Así, $q^k | ord_p a | p-1$, entonces $p \equiv 1(mod\ q^k)$. ■

Corolario 3.2.1. *Si $n-1 = FR$, con $F > R$ y para todo factor primo q de F existe $a > 1$ tal que $a^{n-1} \equiv 1(mod\ n)$ y $(a^{(n-1)/q} - 1,\ n) = 1$ entonces n es primo.*

Demostración: Sea q un factor primo de F y q^k la mayor potencia de q que divide F; por la proposición anterior, todo factor primo de n debe ser congruente a 1 módulo q^k. Como esto vale para cualquier factor primo de F, se sigue que cualquier factor primo de n debe ser congruente a 1 módulo F. Como $F > \sqrt{n}$, esto implica que n es primo. ■

De hecho, basta conocer un conjunto de factores primos cuyo producto sea mayor que $(n-1)^{1/3}$ para, usando el resultado de de Pocklington, intentar demostrar la primalidad de n. Los siguientes criterios clásicos son consecuencias directas de las proposiciones de arriba.

Fermat conjeturó que todo número de la forma $F_n = 2^{2^n} + 1$ es primo y verificó la conjetura para $n \leq 4$. Euler mostró más tarde que F_5 no es primo ($F_5 = 4294967297 = 641 \cdot 6700417$) y ya se demostró que F_n es compuesto para varios valores de n, ningún otro primo de la forma $F_n = 2^{2^n} + 1$ es conocido, pero se conocen muchos primos (algunos bastante grandes) de la forma $a^{2^n} + 1$ que son conocidos como primos de Fermat generalizados. La prueba que sigue muestra como probar eficientemente la primalidad de F_n

Corolario 3.2.2 (Prueba de Pépin). *Sea $F_n = 2^{2^n} + 1$; F_n es primo si y solamente si $3^{(F_n-1)/2} \equiv -1(mod\ F_n)$.*

Demostración: $\Rrightarrow$] Si F_n es primo por la proposición 2.4.1 se tiene que

$$\left(\frac{3}{F_n}\right) \equiv 3^{(F_n-1)/2}(mod\ F_n)$$

ahora aplicando la ley de reciprocidad cuadrática

$$\begin{aligned}
\left(\frac{3}{F_n}\right) &= (-1)^{(3-1)(F_n-1)/4}\left(\frac{F_n}{3}\right) \\
&= (-1)^{(2)(2^{2^n}+1-1)/4}\left(\frac{F_n}{3}\right) \\
&= (-1)^{2(2^{2^n})/4}\left(\frac{F_n}{3}\right) \\
&= \left(\frac{F_n}{3}\right) = -1
\end{aligned}$$

ya que $F_n \equiv -1(mod\ 3)$, luego

$$-1 \equiv 3^{(F_n-1)/2}(mod\ F_n)$$

entonces

$$3^{(F_n-1)/2} \equiv -1(mod\ F_n)$$

$\Leftarrow]$ Si $3^{(F_n-1)/2} \equiv -1(mod\ F_n)$, tenemos que $3^{(F_n-1)} \equiv 1(mod\ F_n)$ y $3^{(F_n-1)/2} \not\equiv 1(mod\ F_n)$, luego por la proposición 3.2.1, F_n es primo. ■

Corolario 3.2.3 (Teorema de Proth; 1878). *Sea $n = h \cdot 2^k + 1$ con $2^k > h$. Entonces n es primo si y solamente si existe un entero a con $a^{(n-1)/2} \equiv -1(mod\ n)$.*

Demostración: $\Rightarrow]$Si n es primo, se puede tomar un a cualquiera tal que no sea un cuadrado módulo n es decir $(\frac{a}{n}) = -1$; la mitad de los enteros entre 1 y $n-1$ sirven como a. Por la proposición 2.4.1 se tiene que

$$-1 = \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}(mod\ n)$$

entonces, $a^{\frac{n-1}{2}} \equiv -1(mod\ n)$.
$\Leftarrow]$ Si hacemos $F = 2^k$ tenemos que $n - 1 = h \cdot F$ donde $F > h$, además como $a^{(n-1)/2} \equiv -1(mod\ n)$ entonces $a^{(n-1)} \equiv 1(mod\ n)$ y $(a^{(n-1)/2} - 1,\ n) = 1$; utilizando el corolario 3.2.1 la prueba queda terminada. ■

Corolario 3.2.4. *Si $n = h \cdot q^k + 1$ con q primo y $q^k > h$. Entonces n es primo si y solamente si existe un entero a con $a^{(n-1)/2} \equiv 1(mod\ n)$ y $(a^{(n-1)/q} - 1,\ n) = 1$.*

Demostración: $\Rightarrow]$ Si n es primo, se puede tomar un a cualesquiera tal que $(\frac{a}{n}) = 1$ o sea que sea un cuadrado módulo n. Por la proposición 2.4.1 se tiene que

$$1 = \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}}(mod\ n)$$

entonces, $a^{\frac{n-1}{2}} \equiv 1(mod\ n)$.
$\Leftarrow]$ Si hacemos $F = q^k$ tenemos que $n - 1 = h \cdot F$ donde $F > h$, además como $a^{(n-1)/2} \equiv 1(mod\ n)$ entonces $a^{(n-1)} \equiv 1(mod\ n)$ y por hipótesis $(a^{(n-1)/q} - 1,\ n) = 1$; utilizando el corolario 3.2.1 la prueba queda terminada. ■

Una gran mayoría de los 100 primos más grandes conocidos cumplen las condiciones del Teorema de Proth. Esto se debe al hecho que los primos de esta forma son frecuentes y que su primalidad es fácilmente demostrada usando este resultado.

3.3. Primos de Mersenne

Se debe recordar que un número de Mersenne es un número de la forma $M_p = 2^p - 1$. Se verá primero que $2^p - 1$ solo es primo cuando p es primo.

Proposición 3.3.1. *Si $2^n - 1$ es primo entonces n es primo.*

Demostración: Supóngase que n es compuesto, es decir si $n = ab$ con $a,\ b \geq 2$ entonces $1 < 2^a - 1 < 2^n - 1$ y $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$ por otro lado

$$\begin{aligned} 2^a &\equiv 1 (mod\ 2^a - 1) \\ (2^a)^b &\equiv 1^b (mod\ 2^a - 1) \\ (2^a)^b - 1 &\equiv 0 (mod\ 2^a - 1) \end{aligned}$$

por lo tanto $2^n - 1$ es compuesto, lo que contradice que $2^n - 1$ es primo, entonces n es primo.■
Por otro lado, no se sabe demostrar que existen infinitos primos de Mersenne ni que existen primos p para los cuales M_p es compuesto. Se conjetura, entretanto, que existen infinitos primos p para los cuales M_p es primo y que, si p_n es el enésimo primo de este tipo, se tiene que

$$0 < A < \frac{\ln p_n}{n} < B < +\infty$$

para ciertas constantes A y B. Existen algunas conjeturas más precisas en cuanto al valor de $\lim_{n\to\infty} \sqrt[n]{p_n}$; Eberhart conjeturó que este límite existe y es igual a 3/2; Wagstaff por otro lado conjeturó que el límite es

$$2^{e^{-\gamma}} \approx 1{,}4757613971$$

donde γ la ya mencionada constante de Euler-Mascheroni.(final capítulo 1)
Los primos de Mersenne son interesantes también por causa de los *números perfectos*.
Dado $n \in \mathbb{N}^*$, se define

$$\sigma(n) = \sum_{d|n} d,$$

la suma de los divisores (positivos) de n. Por el teorema fundamental de la aritmética se tiene que si

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},$$

con $p_1 < p_2 < \cdots < p_m$ entonces

$$\begin{aligned} \sigma(n) &= (1 + p_1 + \cdots p_1^{e_1}) \cdots (1 + p_m + \cdots p_m^{e_m}) \\ &= \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_m^{e_m+1} - 1}{p_m - 1}. \end{aligned}$$

En particular, si $(a,b) = 1$ entonces $\sigma(ab) = \sigma(a)\sigma(b)$. Un entero positivo n es llamado perfecto si $\sigma(n) = 2n$; los primeros números perfectos son $6, 28, 496, 8128, 33550336$ que se pueden factorizar de la siguiente manera

$$\begin{aligned} 6 &= 2(2^2-1) \\ 28 &= 2^2(2^3-1) \\ 496 &= 2^4(2^5-1) \\ 8128 &= 2^6(2^7-1) \\ 33550336 &= 2^{12}(2^{13}-1) \end{aligned}$$

El próximo resultado caracteriza los números perfectos pares.

Proposición 3.3.2. *Si M_p es un primo de Mersenne entonces $2^{p-1}M_p$ es perfecto.*

Demostración: Sea $n = 2^{p-1}M_p = 2^{p-1}(2^p-1)$ donde (2^p-1) es primo. Entonces

$$\sigma(n) = \sigma(2^{p-1}(2^p-1))$$

como $(2^{p-1}, 2^p-1) = 1$ se tiene que

$$\begin{aligned} \sigma(n) &= \sigma(2^{p-1})\sigma(2^p-1) \\ &= \frac{2^p-1}{2-1}(2^p-1+1) \\ &= 2^p(2^p-1) \\ &= 2n, \end{aligned}$$

por lo tanto, n es un número perfecto. ■

Ahora se demostrará el recíproco de la proposición anterior

Proposición 3.3.3. *Si n es un número perfecto par, entonces n es de la forma $2^{p-1}M_p$, donde M_p es un primo de Mersenne.*

Demostración: Como n es un número perfecto, se puede escribir $n = 2^{p-1}r$ con $p > 1$ y r impar positivo. Como n es perfecto se tiene

$$\begin{aligned} 2n = 2^p r &= \sigma(n) \\ &= \sigma(2^{p-1})\sigma(r) \\ &= \frac{2^p-1}{2-1}\sigma(r) \\ &= 2^p - 1\sigma(r). \end{aligned}$$

por lo tanto

$$\sigma(r) = \frac{2^p r}{2^p - 1} = r + \frac{r}{2^p - 1}.$$

Como $2^p r = 2^p - 1\sigma(r)$, entonces $2^p - 1 \mid 2^p r$, y ya que $(2^p - 1, 2^p) = 1$ se tiene que $(2^p - 1) \mid r$ y como consecuencia $\frac{r}{2^p-1} \mid r$. Ahora r tiene solo dos divisores ya que $\sigma(r)$ es la suma de los divisores, entonces

$$\frac{r}{2^p - 1} = 1.$$

Luego $r = 2^p - 1$ es primo y n es de la forma $2^{p-1}(2^p - 1) = 2^{p-1}M_p$. ■

Por otro lado uno de los problemas sin resolver más antiguos de la matemática es el de la existencia de números perfectos impares. Solo se sabe que si existe un número perfecto impar, debe ser muy grande (mas de 300 dígitos) y satisfacer varias condiciones complicadas.

Conjetura 3.3.1. *No existe ningún número perfecto impar.*

El siguiente resultado es el criterio de Lucas-Lehmer, la base de los algoritmos que prueban para grandes valores de p si $2^p - 1$ es o no primo.

Teorema 3.3.1. *Sea S la secuencia definida por $S_0 = 4$, $S_{k+1} = S_k^2 - 2$ para todo natural k. Sea $n > 2$; $M_n = 2^n - 1$ es primo si y solamente si S_{n-2} es múltiplo de M_n.*

Demostración: Obsérvese inicialmente que

$$S_n = (2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}$$

para todo natural n.
La demostración es hecha por inducción, $S_0 = 4 = (2 + \sqrt{3})^{2^0} + (2 - \sqrt{3})^{2^0}$ y

$$\begin{aligned}
S_{k+1} &= S_k^2 - 2 \\
&= \left((2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k}\right)^2 - 2 \\
&= \left((2 + \sqrt{3})^{2^k}\right)^2 + 2 \cdot (2 + \sqrt{3})^{2^k} \cdot (2 - \sqrt{3})^{2^k} + \left((2 - \sqrt{3})^{2^k}\right)^2 - 2 \\
&= \left((2 + \sqrt{3})^{2^k}\right)^2 + 2 \cdot (4 - 3)^{2^k} + \left((2 - \sqrt{3})^{2^k}\right)^2 - 2 \\
&= (2 + \sqrt{3})^{2^{k+1}} + (2 - \sqrt{3})^{2^{k+1}}.
\end{aligned}$$

Si M_n es primo, $n > 2$. Hay que recordar que n es un primo impar. Por reciprocidad

cuadrática se tiene que

$$\begin{aligned}\left(\frac{3}{M_n}\right) &= (-1)^{(3-1)(M_n-1)/4}\left(\frac{M_n}{3}\right)\\ &= (-1)^{(2)(2^n-1-1)/4}\left(\frac{M_n}{3}\right)\\ &= (-1)^{(2)(2^n-2)/4}\left(\frac{M_n}{3}\right)\\ &= (-1)^{(4)(2^{n-1}-1)/4}\left(\frac{M_n}{3}\right)\\ &= (-1)^{(2^{n-1}-1)}\left(\frac{M_n}{3}\right) = -1\end{aligned}$$

pues $2^{n-1}-1$ es impar y

$$\begin{aligned}2 &\equiv -1(mod\ 3)\\ 2^n &\equiv -1(mod\ 3)\\ 2^n-1 &\equiv -2 \equiv 1(mod\ 3)\\ 2^n-1 &\equiv 1(mod\ 3)\end{aligned}$$

Así, 3 no es un cuadrado en $\mathbb{Z}/(M_p)$ y $K = (\mathbb{Z}/(M_p)[\sqrt{3}])^*$ es un campo de orden M_n^2. Se quiere probar que

$$(2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0(mod\ M_p),$$

o sea, que es igual a 0 en K. Esto equivale a demostrar que $(2+\sqrt{3})^{2^{n-2}} = -(2-\sqrt{3})^{2^{n-2}}$ en K, lo que puede se puede reescribir como

$$\begin{aligned}(2+\sqrt{3})^{2^{n-2}}\cdot(2+\sqrt{3})^{2^{n-2}} &= -(2-\sqrt{3})^{2^{n-2}}\cdot(2+\sqrt{3})^{2^{n-2}}\\ (2+\sqrt{3})^{2^{n-2}+2^{n-2}} &= -1\\ (2+\sqrt{3})^{2\cdot 2^{n-2}} &= -1\\ \left((2+\sqrt{3})^{2^{n-1}}\right)^2 &= (-1)^2\\ (2+\sqrt{3})^{2^n} &= 1\end{aligned}$$

así, es claro que el orden de $2+\sqrt{3}$ es un divisor de 2^n se debe por lo tanto probar que el orden de $2+\sqrt{3}$ es exactamente 2^n

Como K tiene $M_n^2-1 = 2^{n+1}(2^{n-1}-1)$ elementos, se debe probar que $2+\sqrt{3}$ no es una cuarta

potencia en K. Nótese que $(2+\sqrt{3})^{2^n}=1$ demuestra que $2+\sqrt{3}$ es un cuadrado, lo que de hecho puede ser visto más directamente: $2+\sqrt{3}=(1+\sqrt{3})^2/2$ y $2=2^{n+1}=2^{(n+1)^2}$ es una cuarta potencia em K. Falta demostrar que $\pm(1+\sqrt{3})$ no son cuadrados en K. Supóngase por absurdo que

$$\epsilon(1+\sqrt{3})=(a+b\sqrt{3})^2,\ \epsilon=\pm 1; \tag{3.1}$$

se tiene

$$\epsilon(1-\sqrt{3})=(a-b\sqrt{3})^2, \tag{3.2}$$

multiplicando (3.1) y (3.2)

$$-2=(a^2-3b^2)^2$$

lo que significa que -2 es un cuadrado módulo M_n (pues a y b son enteros). Esto, es falso:

$$\left(\frac{-2}{M_n}\right)=\left(\frac{-1}{M_n}\right)\left(\frac{2}{M_n}\right)=-1\cdot 1=-1,$$

pues $M_n\equiv 3(mod\ 4)$ y ya se vio que 2 es un cuadrado módulo M_p esto concluye la demostración.

Ahora supóngase por absurdo que $M_n|S_{n-2}$, donde

$$S_{n-2}=(2+\sqrt{3})^{2^{n-2}}+(2-\sqrt{3})^{2^{n-2}}$$

y que M_n es compuesto, con un factor primo q con $q^2<M_n$. Se tiene

$$(2+\sqrt{3})^{2^{n-2}}+(2-\sqrt{3})^{2^{n-2}}\equiv 0(mod\ q),$$

luego, en el grupo multiplicativo $G=(\mathbb{Z}/(q)[\sqrt{3}])^*$, se tiene

$$(2+\sqrt{3})^{2^{n-2}}=-(2-\sqrt{3})^{2^{n-2}}.$$

Como $2-\sqrt{3}=(2+\sqrt{3})^{-1}$ esta ecuación puede ser reescrita

$$\begin{aligned}
(2+\sqrt{3})^{2^{n-2}}\cdot(2+\sqrt{3})^{2^{n-2}} &= -(2-\sqrt{3})^{2^{n-2}}\cdot(2+\sqrt{3})^{2^{n-2}}\\
(2+\sqrt{3})^{2^{n-2}+2^{n-2}} &= -1\\
(2+\sqrt{3})^{2\cdot 2^{n-2}} &= -1\\
\left((2+\sqrt{3})^{2^{n-1}}\right)^2 &= (-1)^2\\
(2+\sqrt{3})^{2^n} &= 1
\end{aligned}$$

lo que significa que el orden de $2+\sqrt{3}$ en G es 2^n. Esto es un absurdo, pues el número de elementos de G es apenas $q^2-1<2^n$. Queda por lo tanto demostrado que si S_{n-2} es múltiplo de M_n entonces M_n es primo. ■

Cuando M_p no es primo, se puede garantizar que sus factores primos son de ciertas formas especiales. Esto es muy útil cuando se buscan primos de Mersenne, pues se puede eliminar algunos exponentes encontrando factores primos de M_p. Esto también puede ser útil para conjeturar cual es la probabilidad de que M_p es primo, o mas precisamente, cual es la relación en la distribución de los primos de Mersenne.

Proposición 3.3.4. *Sean p y q primos con q un divisor de M_p y $p>2$. Entonces $q\equiv 1(mod\ p)$ y $q\equiv\pm 1(mod\ 8)$.*

Demostración: Si q divide a M_p entonces $2^p\equiv 1(mod\ q)$, lo que significa que el orden de 2 módulo q es p (pues p es primo). Esto quiere decir que p es un divisor de $q-1$ ya que $2^{q-1}\equiv 1(mod\ q)$, o sea, que $q\equiv 1(mod\ p)$. Por otro lado, $2\equiv 2^{p+1}=(2^{(p+1)/2})^2(mod\ q)$, lo que quiere decir que 2 es un cuadrado modulo q, entonces $(\frac{2}{q})=1$, lo que significa que $q\equiv\pm 1(mod\ 8)$. ■

Los valores de p para los cuales la primalidad de M_p ha sido probada, sugieren que para una amplia mayoría de valores de p, M_p no es primo. Esto es apenas una conjetura: no se sabe demostrar siquiera que existen infinitos primos p para los cuales M_p es compuesto. La siguiente proposición sirve para garantizar que para ciertos valores especiales de p, algunos muy grandes, M_p no es primo.

Proposición 3.3.5. *Sea p primo, con $p\equiv 3(mod\ 4)$. Entonces $2p+1$ es primo si y solo si $2p+1$ divide a M_p*

Demostración: $\Rightarrow$] Sea $q=2p+1$, si es primo entonces,

$$M_p=2^p-1=2^{(q-1)/2}-1\equiv\left(\frac{2}{q}\right)-1(mod\ q).$$

Pero p es de la forma $4t+3$ lo que significa que

$$\begin{aligned} q &= 2(4t+3)+1\\ &= 8t+7 \end{aligned}$$

entonces $q\equiv 7(mod\ 8)$, luego $\left(\frac{2}{q}\right)=1$. Entonces, $M_p\equiv 0(mod\ q)$, o sea $2p+1$ divide a M_p.
$\Leftarrow$] Supongamos que $2p+1$ no es primo, luego tiene factores primos r con $r\not\equiv 1(mod\ p)$ (pues

$r < p$). Si $2p+1$ divide a M_p, r sería un factor primo de M_p contradiciendo la proposición 3.3.4. ■

Los primos p para los cuales $2p+1$ es primo son llamados primos de Sophie Germain. Algunos primos de Sophie Germain bastante grandes son conocidos como $p_0 = 18458709 \cdot 2^{32611} - 1$, así, por la proposición anterior, M_{p_0} es compuesto. Se sabe también que si $\pi_{SG}(x)$ denota el número de primos de Sophie Germain menores que x entonces existe C tal que para todo x

$$\pi_{SG}(x) < C\frac{x}{(\ln x)^2}.$$

Se cree que $\pi_{SG}(x)$ es asintótico a $Cx/(\ln x)^2$ para alguna $C > 0$ mas no se sabe demostrar, aún, que existen infinitos primos de Sophie Germain.

3.4. Pruebas Basadas en Factorizaciones de $n+1$

Supóngase $n > 1$ y P, Q enteros tales que $D = P^2 - 4Q$ no es un cuadrado módulo n. Sea

$$\alpha = \frac{P + \sqrt{D}}{2},$$

raíz de la ecuación $X^2 - PX + Q = 0$, y para todo natural m U_m y V_m son definidos recursivamente por

$$\begin{aligned} U_0 &= 0,\ U_1 = 1,\ U_{m+2} = PU_{m+1} - QU_m, \\ V_0 &= 2,\ V_1 = P,\ V_{m+2} = PV_{m+1} - QV_m. \end{aligned}$$

Se probará por inducción que

$$\alpha^m = \frac{V_m + U_m\sqrt{D}}{2},$$

para $m+1$ se tiene que

$$\begin{aligned}
\frac{V_{m+1}+U_{m+1}\sqrt{d}}{2} &= \frac{PV_m - QV_{m-1} + (PU_m - QU_{m-1})\sqrt{D}}{2} \\
&= \frac{P(V_m + U_m\sqrt{D} - Q(V_{m-1} + U_{m-1}\sqrt{D})}{2} \\
&= \frac{P(V_m + U_m\sqrt{D}}{2} - \frac{Q(V_{m-1} + U_{m-1}\sqrt{D})}{2} \\
&= P\alpha^m - Q\alpha^{m-1} \\
&= \alpha^{m-1}(P\alpha - Q) \\
&= \alpha^{m-1}\left(P\left(\frac{P+\sqrt{D}}{2}\right) - Q\right) \\
&= \alpha^{m-1}\left(\frac{P^2 + P\sqrt{D}}{2} - Q\right) \\
&= \alpha^{m-1}\left(\frac{P^2 + P\sqrt{D} - 2Q}{2}\right)
\end{aligned}$$

por otro lado

$$\alpha = \frac{P+\sqrt{D}}{2} \Rightarrow \alpha^2 = \frac{P^2 + 2P\sqrt{D} + D}{4}$$

reemplazando D se tiene

$$\begin{aligned}
\alpha^2 &= \frac{P^2 + 2P\sqrt{D} + P^2 - 4Q}{4} \\
&= \frac{2P^2 + 2P\sqrt{D} - 4Q}{4} \\
&= \frac{P^2 + P\sqrt{D} - 2Q}{2}
\end{aligned}$$

entonces reemplazando tenemos

$$\alpha^{m-1}\left(\frac{P^2 + P\sqrt{D} - 2Q}{2}\right) = \alpha^{m-1}\cdot\alpha^2 = \alpha^{m+1}$$

Si

$$\overline{\alpha} = \frac{P-\sqrt{D}}{2},$$

es la segunda raíz de la ecuación $X^2 - PX + Q = 0$, se puede probar utilizando un razonamiento similar al de arriba que

$$\overline{\alpha^m} = \frac{V_m - U_m\sqrt{D}}{2},$$

también se puede escribir

$$U_m = \frac{\alpha^m - \overline{\alpha}^m}{\sqrt{D}},\ V_m = \alpha^m + \overline{\alpha}^m,$$

las cuales se demuestran por inducción.
Para $m+1$ se tiene que

$$\begin{aligned}
\frac{\alpha^{m+1} - \overline{\alpha}^{m+1}}{\sqrt{D}} &= \frac{\frac{V_{m+1}+U_{m+1}\sqrt{D}}{2} - \frac{V_{m+1}-U_{m+1}\sqrt{D}}{2}}{\sqrt{D}} \\
&= \frac{V_{m+1} + U_{m+1}\sqrt{D} - V_{m+1} + U_{m+1}\sqrt{D}}{2\sqrt{D}} \\
&= \frac{2U_{m+1}\sqrt{D}}{2\sqrt{D}} \\
&= U_{m+1}
\end{aligned}$$

De igual forma para $V_m = \alpha^m + \overline{\alpha}^m$, se tiene por inducción para $m+1$

$$\begin{aligned}
\alpha^{m+1} + \overline{\alpha}^{m+1} &= \frac{V_{m+1} + U_{m+1}\sqrt{D}}{2} + \frac{V_{m+1} - U_{m+1}\sqrt{D}}{2} \\
&= \frac{V_{m+1} + U_{m+1}\sqrt{D} + V_{m+1} - U_{m+1}\sqrt{D}}{2} \\
&= \frac{2V_{m+1}}{2} = V_{m+1}
\end{aligned}$$

De estas fórmulas se sigue que

$$U_{n+1} = \frac{PU_n + V_n}{2},\ V_{n+1} = \frac{DU_n + PV_n}{2}$$

donde la demostración por inducción para U_{n+1} es

$$\begin{aligned}
\frac{PU_{n+1} + V_{n+1}}{2} &= \frac{P(PU_n - QU_{n-1}) + PV_n - QV_n}{2} \\
&= \frac{P^2U_n - PQU_{n-1}) + PV_n - QV_n}{2} \\
&= \frac{P(PU_n + V_n) - Q(PU_{n-1} + V_{n-1})}{2} \\
&= P\left(\frac{PU_n + V_n}{2}\right) - Q\left(\frac{PU_{n-1} + V_{n-1}}{2}\right)
\end{aligned}$$

utilizando la hipótesis de inducción se tiene

$$\begin{aligned} &= PU_{n+1} - QU_n \\ &= U_{n+2}, \end{aligned}$$

para V_{n+1} se hace un razonamiento similar, otras fórmulas que también se desprenden de las anteriores son

$$U_{2m} = U_m V_m,\ V_{2m} = V_m^2 - 2Q^m.$$

Éstas fórmulas permiten calcular U_m y V_m módulo n. Recordemos del capítulo anterior que si $p > 2$ es primo y d no es un cuadrado módulo p entonces $K = (\mathbb{Z}/(p))[\sqrt{d}]$ es un campo con p^2 elementos.

Proposición 3.4.1. *Si n es primo y D no es un cuadrado módulo n entonces $\alpha^n = \overline{\alpha}$ en $K = (\mathbb{Z}/(n))[\sqrt{D}]$.*

Demostración: Supóngase que n es primo. En K se tiene la siguiente identidad

$$(X + Y)^n = X^n + Y^n$$

dado que del binomio de Newton tenemos que

$$\binom{n}{m} = \frac{n!}{m!(m-n)!}$$

es múltiplo de n si $0 < m < n$. Aplicando esta identidad a α se tiene

$$\alpha^n = \frac{P^n + D^{(n-1)/2}\sqrt{D}}{2^n} = \frac{P - \sqrt{D}}{2} = \overline{\alpha}.$$

pues $P^n \equiv P(mod\ n),\ 2^n \equiv 2(mod\ n)$ y $D^{(n-1)/2} \equiv -1(mod\ n)$, ya que D no es un cuadrado módulo n. ■

Análogamente, si n es primo, se tiene que $\overline{\alpha}^n = \alpha$ en K. Así, todavía en K, $\alpha^{n+1} = \overline{\alpha}^{n+1} = \alpha\overline{\alpha}$. De la fórmula para U_m se sigue que $U_{n+1} \equiv 0(mod\ n)$. Con esto queda demostrada la siguiente proposición.

Proposición 3.4.2. *Si n es primo impar, $\left(\frac{D}{n}\right) = -1$ y las secuencias U_m, V_m son definidas por las recurrencias*

$$\begin{aligned} U_0 &= 0,\ U_1 = 1,\ U_{m+2} = PU_{m+1} - QU_m, \\ V_0 &= 2,\ V_1 = P,\ V_{m+2} = PV_{m+1} - QV_m, \end{aligned}$$

entonces $U_{n+1} \equiv 0(mod\ n)$.

Esta proposición nos brinda otro algoritmo para probar la primalidad de n.

Proposición 3.4.3. *Si $n \neq 2$ es primo, $n \nmid Q$, $n \nmid D$ y D es cuadrado módulo n entonces $U_{n-1} \equiv 0(mod\ n)$.*

Demostración: En el anillo $K = \mathbb{Z}/(n)[\sqrt{D}]$, se tiene que

$$\alpha^n = \frac{P^n + D^{(n-1)/2}\sqrt{D}}{2^n} = \frac{P + \sqrt{D}}{2} = \alpha$$

pues $P^n \equiv P(mod\ n)$, $2^n \equiv 2(mod\ n)$ y $D^{(n-1)/2} \equiv 1(mod\ n)$, ya que D es un cuadrado módulo n, entonces $\alpha^{n-1} = 1$ en K, pues α es invertible en K; de hecho $\alpha\overline{\alpha} = Q$,

$$\begin{aligned} \alpha\overline{\alpha} &= \left(\frac{P + \sqrt{D}}{2}\right)\left(\frac{P - \sqrt{D}}{2}\right) \\ &= \frac{P^2 - 4Q}{4} \end{aligned}$$

por otro lado

$$\begin{aligned} D &= P^2 - 4Q \\ Q &= \frac{P^2 - D}{4} \Rightarrow \alpha\overline{\alpha} = Q \end{aligned}$$

que es invertible en K. Del mismo modo, $\overline{\alpha}^{n-1} = 1$ en K y por lo tanto se tiene, en K

$$U_{n-1} = \frac{\alpha^{n-1} - \overline{\alpha^{n-1}}}{\sqrt{D}} = \frac{1-1}{\sqrt{D}}0$$

o sea, $U_{n-1} \equiv 0(mod\ n)$. ■

En general, si $n \neq 2$ es primo, $n \nmid Q$, $n \nmid D$ entonces $U_{n-(\frac{D}{n})}$ es múltiplo de n, lo que se debe al hecho de que α^m es igual $\overline{\alpha}^m$ si $m = n - (\frac{D}{n})$ en el anillo $K = \mathbb{Z}/(n)[\sqrt{D}]$. Obsérvese ahora que si $\alpha^m = \overline{\alpha}^m$ en K entonces existe un entero r tal que

$$\alpha^m = \overline{\alpha}^n + nr\sqrt{D}$$

pues $\frac{\alpha^m - \overline{\alpha}^m}{\sqrt{D}} \in \mathbb{Z}$. Este hecho se usa para probar por inducción el siguiente resultado.

Proposición 3.4.4. *Si $n \neq 2$ es primo, $n \nmid Q$, $n \nmid D$ entonces para todo natural $k \geq 1$, $U_{m \cdot n^{k-1}}$ es múltiplo de n^k, donde $m = n - (\frac{D}{n})$.*

Demostración: Supóngase, por hipótesis de inducción, que

$$\alpha^{m\cdot n^{k-1}} = \overline{\alpha}^{m\cdot n^{k-1}} + n^k r_k\sqrt{D},\ r_k \in \mathbb{Z}.$$

Elevando los dos lados de la ecuación a la n-ésima potencia se tiene

$$\alpha^{m\cdot n^k} = \left(\overline{\alpha}^{m\cdot n^{k-1}} + n^k r_k\sqrt{D}\right)^n = \overline{\alpha}^{m\cdot n^k} + n^{k+1} r_{k+1}\sqrt{D}$$

donde r_{k+1} pertenece a $\mathbb{Z}[\sqrt{D}]$ por un lado, y por otro

$$\begin{aligned} \alpha^{m\cdot n^k} &= \overline{\alpha}^{m\cdot n^k} + n^{k+1} r_{k+1}\sqrt{D} \\ \frac{\alpha^{m\cdot n^k} - \overline{\alpha}^{m\cdot n^k}}{\sqrt{D}} &= n^{k+1} r_{k+1} \end{aligned}$$

entonces $n^{k+1} r_{k+1} = U_{m\cdot n^k}$ es un entero, lo que implica que $r_{k+1} \in \mathbb{Q} \cap \mathbb{Z}[\sqrt{D}]$ y por lo tanto es entero, lo que concluye la prueba. ■

Apéndice A

Tablas

En esta última sección presentaremos algunas tablas indicando los mayores primos conocidos hasta el momento.

Los diez mayores primos conocidos

Primo	**Nº de dígitos**	**Descubridor**	**Fecha**
$2^{25964951}-1$	7816230	$Martin\ Nowak.(GIMPS)$	2005
$2^{24036583}-1$	7235733	$Josh\ Findley.(GIMPS)$	2004
$2^{20996011}-1$	6320430	$Michael\ Shaker.(GIMPS)$	2003
$2^{13466917}-1$	4053946	$Michael\ Cameron.(GIMPS)$	2001
$2^{6972543}-1$	2098960	$Nayan\ Hajratwala.(GIMPS)$	1999
$2^{3021377}-1$	909526	$Clarkson,\ Woltman.(GIMPS)$	1998
$2^{2976221}-1$	895932	$Spence,\ Woltman.(GIMPS)$	1997
$2^{1398269}-1$	420921	$Armengaud,\ Woltman.(GIMPS)$	1996
$2^{1257787}-1$	378632	$Slowinski,\ Gage$	1996
$2^{859433}-1$	258716	$Slowinski,\ Gage$	1994

Recordemos que cuando p y $p+2$ son ambos primos, se dice que ellos son primos gemelos.

Los diez mayores pares de primos gemelos conocidos

Primo	Nº de dígitos	Descubridor	Fecha
$361700055 \cdot 2^{39020} \pm 1$	11755	*Henri Lifchitz*	1999
$835335 \cdot 2^{39014} \pm 1$	11751	*Bellinger y Gallot*	1998
$242206083 \cdot 2^{38880} \pm 1$	11713	*Jarai e Indlekofer*	1995
$40883037 \cdot 2^{23456} \pm 1$	7069	*Lifchitz y Gallot*	1998
$843753 \cdot 2^{22222} \pm 1$	6696	*Rivera y Gallot*	1997
$7485 \cdot 2^{20023} \pm 1$	6032	*Buddenhagen y Gallot*	1998
$8182815 \cdot 2^{17838} \pm 1$	5377	*Smith y Gallot*	1998
$570918348 \cdot 10^{5120} \pm 1$	5129	*Harvey Dubner*	1995
$697053813 \cdot 2^{16352} \pm 1$	4932	*Jarai e Indlekofer*	1995
$37442007 \cdot 2^{15440} \pm 1$	4656	*Hanson y Gallot*	1999

Sea $n\sharp$, llamado el *primorial de* n el producto de todos los números primos menores o iguales a n. Se usa también la notación $n!!\ldots!!$, con k puntos de admiración, para simbolizar el producto de $n(n-k)(n-2k)\ldots$ de los enteros positivos menores o iguales a n y congruentes a n módulo k. Un primo de la forma $n\sharp \pm 1$ es llamado primorial y un primo de la forma $n!!\ldots!!$ es llamado multifactorial.

Los diez mayores primos multifactoriales y primoriales conocidos

Primo	Nº de dígitos	Descubridor	Fecha
$6917! - 1$	23560	*Cladwell y Gallot*	1998
$6380! + 1$	21507	*Cladwell y Gallot*	1998
$42209\sharp + 1$	18241	*Cladwell y PrimeForm*	1999
$14614!!!! + 1$	13632	*Charles F. Kerchner III*	1998
$10830!!! + 1$	13000	*Charles F. Kerchner III*	1998
$3610! - 1$	11277	*Cris Caldwell*	1993
$3507! - 1$	10912	*Cris Caldwell*	1992
$24029\sharp + 1$	10387	*Cris Caldwell*	1993
$23801\sharp + 1$	10273	*Cris Caldwell*	1993
$11915!!!!! + 1$	11277	*Charles F. Kerchner III*	1998

Recordemos que p es llamado un primo de Sophie Germain si $2p + 1$ también es primo y que M_p es compuesto para los valores de p es los que $p \equiv 3(mod\ 4)$. Este nombre es usado porque Sophie Germain probó el primer caso del último teorema de Fermat (recientemente

demostrado por Wiles) para primos de esta forma.

Los diez mayores primos de Sophie Germain conocidos

Primo	Nº de dígitos	Descubridor	Fecha
$18458709 \cdot 2^{32611} - 1$	9825	*Kerchner y Gallot*	1999
$14516877 \cdot 2^{24176} - 1$	7285	*Kerchner y Gallot*	1999
$72021 \cdot 2^{23630} - 1$	7119	*Yves Gallot*	1999
$2375063906985 \cdot 2^{19380} - 1$	5847	*Jarai e Indlekofer*	1999
$276311 \cdot 2^{19003} + 1$	5726	*Ballinger y Gallot*	1998
$92305 \cdot 2^{16998} + 1$	5122	*Kerchner y Gallot*	1998
$8069496135 \cdot 10^{5072} - 1$	5082	*Harvey Dubner*	1995
$470943129 \cdot 2^{16352} - 1$	4932	*Jarai e Indlekofer*	1995
$157324389 \cdot 2^{16352} - 1$	4931	*Jarai e Indlekofer*	1995
$5415312903 \cdot 10^{4526} - 1$	4536	*Harvey Dubner*	1994

EL mayor primo conocido a traves de la história

Primo	Nº de dígitos	Descubridor	Fecha
$2^{17} - 1$	6	*Cataldi*	1588
$2^{19} - 1$	6	*Cataldi*	1588
$2^{31} - 1$	10	*Euler*	1772
999999000001	12	*Loof*	1851
$(2^{59} - 1)/179951$	13	*Landry*	1867
$(2^{53} + 1)/(3 \cdot 107)$	14	*Landry*	1867
$2^{127} - 1$	39	*Lucas*	1876
$(2^{148} + 1)/17$	44	*Ferrier*	1951
$180(2^{127} - 1)^2 + 1$	79	*Miller y Wheeler*	1951
$2^{521} - 1$	157	*Robinson*	1952

Primo	Nº de dígitos	Fecha	Comentario
$2^{607}-1$	183	*Robinson*	1952
$2^{1279}-1$	386	*Robinson*	1952
$2^{2203}-1$	664	*Robinson*	1952
$2^{2281}-1$	687	*Robinson*	1952
$2^{3217}-1$	969	*Riesel*	1957
$2^{4423}-1$	1332	*Hurwitz*	1961
$2^{9689}-1$	2917	*Gillies*	1963
$2^{9941}-1$	2993	*Gillies*	1963
$2^{11213}-1$	3376	*Gillies*	1963
$2^{19937}-1$	6002	*Tuckerman*	1971
$2^{21701}-1$	6533	*Noll y Nickel*	1978
$2^{23209}-1$	6987	*Noll*	1979
$2^{44497}-1$	13395	*Nelson y Slowinski*	1979
$2^{86243}-1$	25962	*Slowinski*	1982
$2^{132049}-1$	39751	*Slowinski*	1983
$2^{216091}-1$	65050	*Slowinski*	1985
$91581\cdot 2^{216193}-1$	65087	*Amdahl Six*	1989
$2^{756839}-1$	227832	*Slowinski y Gage*	1992
$2^{859433}-1$	258716	*Slowinski y Gage*	1994
$2^{1257787}-1$	378632	*Slowinski y Gage*	1996
$2^{1398269}-1$	420921	*Armengaud, Woltman, (GIMPS)*	1996
$2^{2976221}-1$	895932	*Spence, Woltman (GIMPS)*	1997
$2^{3021377}-1$	909526	*Clarkson, Woltman.(GIMPS)*	1998
$2^{6972543}-1$	2098960	*Nayan Hajratwala.(GIMPS)*	1999
$2^{13466917}-1$	4053946	*Michael Cameron.(GIMPS)*	2001
$2^{20996011}-1$	6320430	*Michael Shaker.(GIMPS)*	2003
$2^{24036583}-1$	7235733	*Josh Findley.(GIMPS)*	2004
$2^{25964951}-1$	7816230	*Martin Nowak.(GIMPS)*	2005

Los cien mayores primos conocidos

	Primo	Nº de dígitos	Fecha	Comentario
1	$2^{25964951}-1$	7816230	2005	*Mersenne* 42
2	$2^{24036583}-1$	7235733	2004	*Mersenne* 41
3	$2^{20996011}-1$	6320430	2003	*Mersenne* 40
4	$2^{13466917}-1$	4053946	2001	*Mersenne* 39
5	$2^{6972543}-1$	2098960	1999	*Mersenne* 38
6	$2^{3021377}-1$	909526	1998	*Mersenne* 37
7	$2^{2976221}-1$	895932	1997	*Mersenne* 36
8	$2^{1398269}-1$	420921	1996	*Mersenne* 35
9	$2^{1257787}-1$	378632	1996	*Mersenne* 34
10	$2^{859433}-1$	258716	1994	*Mersenne* 33
11	$2^{756839}-1$	227832	1992	*Mersenne* 32
12	$302627325\cdot 2^{530101}+1$	159585	1999	
13	$481899\cdot 2^{481899}+1$	145072	1998	*Cullen*
14	$361275\cdot 2^{361275}+1$	108761	1998	*Cullen*
15	$302442855\cdot 2^{336211}+1$	101219	1998	
16	$9\cdot 2^{304607}+1$	91697	1998	
17	$3\cdot 2^{303093}+1$	91241	1998	
18	$7\cdot 2^{283034}+1$	85203	1998	
19	$27253\cdot 2^{272347}-1$	81990	1998	
20	$67234^{16384}+1$	79096	1999	*Fermat generalizado*
21	$262419\cdot 2^{262419}+1$	79002	1998	*Cullen*
22	$9183\cdot 2^{262112}+1$	78908	1997	
23	$111113277\cdot 2^{250132}+1$	75306	1998	
24	$22695\cdot 2^{247131}+1$	74399	1999	
25	$217807\cdot 2^{243537}-1$	73318	1999	
26	$5\cdot 2^{240937}+1$	72530	1997	
27	$982451707\cdot 2^{239848}+1$	72211	1998	
28	$25229\cdot 2^{238652}-1$	71846	1998	

	Primo	Nº de dígitos	Fecha	Comentario
29	$73 \cdot 2^{227334} + 1$	68437	1999	
30	$127 \cdot 2^{220417} - 1$	66355	1999	
31	$29 \cdot 2^{219317} + 1$	66023	1999	
32	$391581 \cdot 2^{216193} - 1$	65087	1989	
33	$2^{216081} - 1$	65050	1985	*Mersenne* 31
34	$3 \cdot 2^{213321} + 1$	64217	1997	
35	$5 \cdot 2^{209787} + 1$	63153	1997	
36	$7 \cdot 2^{207084} + 1$	62340	1998	
37	$132599 \cdot 2^{206032} - 1$	62027	1999	
38	$331139 \cdot 2^{201240} - 1$	60585	1999	
39	$281143 \cdot 2^{187639} - 1$	56491	1999	
40	$81 \cdot 2^{185745} + 1$	55917	1999	
41	$15 \cdot 2^{184290} + 1$	55478	1998	
42	$60541 \cdot 2^{176340} + 1$	53089	1997	
43	$39781 \cdot 2^{176088} + 1$	53013	1997	
44	$73 \cdot 2^{171854} + 1$	51736	1998	
45	$127 \cdot 2^{170393} - 1$	51296	1999	
46	$159821 \cdot 2^{168770} - 1$	50811	1999	
47	$48833 \cdot 2^{167897} + 1$	50547	1999	
48	$74269 \cdot 2^{167546} + 1$	50442	1999	
49	$2 \cdot 3^{105106} + 1$	50149	1999	
50	$285 \cdot 2^{165957} + 1$	49961	1998	
51	$111253 \cdot 2^{165379} - 1$	49790	1999	
52	$21 \cdot 2^{164901} + 1$	49642	1999	
53	$1002774^{8192} + 1$	49162	1999	*Fermat generaizado*
54	$27423 \cdot 2^{158625} + 1$	47756	1997	
55	$3 \cdot 2^{157169} + 1$	47314	1995	
56	$325859 \cdot 2^{156148} - 1$	47011	1999	
57	$285 \cdot 2^{155637} + 1$	46854	1998	

	Primo	Nº de dígitos	Fecha	Comentario
58	$111763 \cdot 2^{155551} - 1$	46831	1998	
59	$291 \cdot 2^{154544} + 1$	46525	1999	
60	$151023 \cdot 2^{151023} - 1$	45468	1998	*Woodall*
61	$16 \cdot 2^{149146} + 1$	44899	1998	
62	$9 \cdot 2^{149143} + 1$	44898	1995	
63	$185767 \cdot 2^{149009} - 1$	44862	1999	
64	$256267 \cdot 2^{148941} - 1$	444842	1999	
65	$165 \cdot 2^{147953} + 1$	44541	1991	
66	$29 \cdot 2^{147316} - 1$	44348	1999	
67	$9 \cdot 2^{147073} + 1$	44275	1995	
68	$9 \cdot 2^{145247} + 1$	43725	1995	
69	$29 \cdot 2^{144937} + 1$	43632	1999	
70	$178747 \cdot 2^{144789} - 1$	43592	1999	
71	$231 \cdot 2^{143949} + 1$	43336	1998	
72	$165 \cdot 2^{143437} + 1$	43182	1998	
73	$180924^{8192} + 1$	43070	1999	*Fermat generalizado*
74	$143018 \cdot 2^{143018} - 1$	43058	1998	*Woodall*
75	$333 \cdot 2^{142307} - 1$	42842	1998	
76	$190229 \cdot 2^{141576} - 1$	42624	1999	
77	$63 \cdot 2^{141497} + 1$	42597	1999	
78	$203 \cdot 2^{141477} + 1$	42592	1999	
79	$285 \cdot 2^{141253} + 1$	42524	1998	
80	$150152^{8192} + 1$	42407	1999	*Fermat generalizado*
81	$288759 \cdot 2^{140001} + 1$	42150	1999	
82	$165 \cdot 2^{139459} + 1$	41984	1998	
83	$1263080^{8192} + 1$	41791	1999	*Fermat generalizado*
84	$81 \cdot 2^{138239} + 1$	41616	1998	
85	$122463 \cdot 2^{137552} + 1$	41473	1998	
86	$111850^{8192} + 1$	41359	1999	*Fermat generaliado*

	Primo	Nº de dígitos	Fecha	Comentario
87	$245 \cdot 2^{136993} + 1$	41242	1999	
88	$130297 \cdot 2^{136645} - 1$	41140	1999	
89	$70175 \cdot 2^{135753} + 1$	40871	1998	
90	$438523 \cdot 2^{135415} - 1$	40770	1999	
91	$203 \cdot 2^{135125} + 1$	40679	1999	
92	$105 \cdot 2^{133443} + 1$	49173	1998	
93	$71852^{8192} + 1$	39784	1999	*Fermat generalizado*
94	$2^{132049} - 1$	39751	1983	*Mersenne* 30
95	$63 \cdot 2^{131325} + 1$	39535	1999	
96	$2 \cdot 3^{82780} + 1$	39497	1999	
97	$10038165 \cdot 2^{131040} + 1$	39454	1997	
98	$5581 \cdot 2^{131000} + 1$	39439	1999	
99	$577294575 \cdot 2^{130639} + 1$	39336	1999	
100	$195 \cdot 2^{130388} + 1$	39253	1998	

Un primo se llama de Cullen si es de la forma $n \cdot 2^n + 1$, de Woodall si es de la forma $n \cdot 2^n - 1$ y de Fermat generalizado si es de la forma $a^{2^n} + 1$.

BIBLIOGRAFÍA

[1] JIMÉNEZ BECERRA, Luis, et al. *Teoría de números para principiantes*. Bogotá: Unibiblos. 1999.

[2] ISAACS, R. *Números enteros. Teoría, algoritmos y divertimientos*. Bucaramanga: UIS. 1992.

[3] MOREIRA, Carlos y SALDANHA, Nicolau. *Vigésimo segundo seminario brasilero de matemática*. Río de Janeiro: IMPA. 1999.

[4] PETTOFREZZO, A. *Introducción a la teoría de números*. México: Prentice-Hall. 1972