DOS PROBLEMAS SOBRE NÚMEROS PRIMOS

DIANA ELENA LASSO ORDOÑEZ
KARINA MARIVEL YAZÁN ANRANGO

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2014

DOS PROBLEMAS SOBRE NÚMEROS PRIMOS

DIANA ELENA LASSO ORDOÑEZ
KARINA MARIVEL YAZÁN ANRANGO

Trabajo presentado como requisito parcial para optar al título de Licenciado en Matemáticas

Asesor
Prof. John Hermes Castillo Gómez

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

UNIVERSIDAD DE NARIÑO
SAN JUAN DE PASTO
2014

Nota de Responsabilidad

Todas las ideas y conclusiones aportadas en el siguiente trabajo son responsabilidad exclusiva de las autoras.

Artículo 1^{ro} del Acuerdo No. 324 de octubre 11 de 1966 emanado por el Honorable Consejo Directivo de la Universidad de Nariño.

San Juan de Pasto, Junio 11 de 2014

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____

_____

John Hermes Castillo Gómez
Presidente de Tesis

_____

Oscar Fernando Soto Agreda
Jurado

_____

Sergio Alexander Gómez
Jurado

Este trabajo está dedicado a:
Mi madre Elena Ordoñez y mi padre Rosendo Lasso quienes en vida me brindaron todo su apoyo y cariño para alcanzar siempre mis anhelos.
Diana

Este trabajo está dedicado a:
Mi madre Edilma Anrango, por ser la mayor razón para seguir siempre adelante.
Karina

Agradecimientos

Al término de este trabajo de grado es ineludible expresar los sentimientos de agradecimiento por aquellos que contribuyeron de manera incondicional en la realización de este aporte a nuestra formación matemática.

En primer lugar agradecemos a Dios por brindarnos su compañia y sabiduría en la realización de los aspectos de planificación y elaboración de este trabajo de grado.

A nuestras familias por su comprensión y confianza en el transcurso de estos arduos pero gratificantes meses.

A nuestra universidad por la formación académica y personal brindada.

Al grupo de profesores del departamento de Matemáticas, especialmente al futuro Dr. Wilson Mutis Cantero quien no solo nos brindó lo mejor de su conocimiento en Matemáticas, sino que también nos inculcó el amor por el estudio del álgebra y la teoría de números.

Al Mg. Sergio Gómez y Mg. Oscar Fernando Soto por la diligencia y sugerencias en la revisión de este trabajo.

Finalmente, a nuestro asesor Dr. John H. Castillo G., los más sinceros agradecimientos por su dedicación, orientación y sugerencias en el desarrollo de este trabajo de grado.

Diana Lasso
Karina Yazán

Universidad de Nariño
Mayo 30 de 2014.

Resumen

En este trabajo se realiza el estudio y análisis de dos problemas relevantes respecto a los números primos, el primero se refiere a la existencia de una fórmula o sucesión que genere todos los números primos y el segundo se refiere a establecer características que permitan determinar si un número es primo o compuesto cuando este es demasiado grande. En este estudio se analizan de manera detallada los conceptos fundamentales de la Teoría de números primos y se presentan algunos algoritmos con el fin de ejemplificar la teoría, mediante el uso de funciones del sistema de álgebra computacional GAP.

Abstract

In this we study and analyze two relevant problems concerning prime numbers, the first one refers to the existence of a formula or sequence that generates all the prime numbers and the second one is about to set characteristics to determine when a number is prime or composite if it is too large. This study analyzes in detail the fundamental concepts of the theory of prime numbers and some algorithms in order to illustrate the theory presented using system of computational algebra GAP.

Índice general

Introducción

En la teoría de números, los números primos han sido objeto de un arduo estudio tanto de matemáticos como de estudiosos del tema; alrededor de ellos se han planteado diferentes preguntas recurrentes que han hecho posible una caracterización cada vez más puntual. Este trabajo se ha enfocado específicamente a recopilar y organizar algunos resultados que han obtenido diferentes investigadores en el estudio de los dos siguientes interrogantes: ¿existe una fórmula general o sucesión con la que se pueda generar todos los números primos? y ¿cómo determinar si un número es primo o compuesto?

La dificultad para resolver el segundo problema parece incrementarse a medida que crece el número de digitos de un número sobre el cual se desea decidir su primalidad, sin embargo, en la búsqueda de métodos generales que permitan decidir la primalidad de un número dado n, se han planteado diferentes procedimientos (test de primalidad) utilizando algunas características propias de los números primos que permiten determinar si un número es primo o compuesto. Algunos números a pesar de ser compuestos cumplen dichos test de primalidad, estos son conocidos como pseudoprimos; entre ellos se destacan los pseudoprimos de Fermat y pseudoprimos fuertes base a, que aún siguen siendo el problema fundamental en la implementación de algoritmos de primalidad, a pesar de esto y en base a algunas propiedades y características de los números primos se ha podido restringir parcialmente el paso de estos números por dichos algoritmos.

En los capítulos 1 y 2 se presentan algunos resultados teóricos que serán necesarios para el entendimiento de los capítulos subsecuentes. Desafortunadamente o afortunadamente, en torno a estos dos problemas no se tienen respuestas determinantes o concretas que los solucionen, pero a través del análisis que han hecho diferentes investigadores se han podido establecer respuestas parciales que bajo ciertas condiciones cumplen con la primalidad de un número dado n; algunas partes de este análisis que son de interés para este trabajo se presentan en los capítulos 3 y 4. Dada la importancia de crear mecanismos eficientes y veraces para determinar si un número dado n es primo o no, finalmente en este trabajo se presentan algunos algoritmos de primalidad implementados en el sistema de álgebra computacional GAP (Groups, Algorithms, Programming - a System for Computational Discrete Algebra), algoritmos que pueden encontrarse en el Apéndice.

Capítulo 1

Preliminares

En este capítulo se presentan algunas definiciones y teoremas relacionados con los números primos como divisibilidad, congruencias, residuos cuadráticos; además de sucesiones, Topología y algunas propiedades de los grupos cíclicos las cuales se utilizan a lo largo de todo el trabajo. El objetivo es contribuir en la comprensión tanto de la caracterización de primalidad como de pseudoprimalidad y en particular en el desarrollo y evolución de algunos aspectos puntuales que se presentan en los siguientes capítulos.

Definición 1.1. Dado un número n que pertenece a un sistema de numeración, conjunto númerico o sucesión se llama sucesor de n al número que está inmediatamente después de él según el orden y se denota con n^+.

Definición 1.2. Para cada número natural n existe un y solo un número natural llamado el sucesor de x.

Teorema 1.1 (Principio de inducción matematica (PIM))**.** *Si S es un subconjunto de N tal que*

1. $0 \in S$,
2. $n^+ \in S$ *siempre que* $n \in S$.

Entonces $S = N$.

Teorema 1.2 (Principio de Inducción Matematica Generalizado (PIM2))**.** *Sea a un número natural y S un subconjunto de $\{k \in Z : k \geq a\}$. que satisface*

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

Entonces

$$S = \{k \in \mathbb{N} : k \geq a\}.$$

1.1. Divisibilidad

Definición 1.3. Sean a, b números enteros con $a \neq 0$. Decimos que a divide a b si existe un entero k tal que $b = ak$. En tal caso escribimos $a|b$. Decimos también que a es un divisor de b o que b es un múltiplo de a.

Para indicar que a no divide a b escribimos $a \not| b$. Es fácil verificar que para todo entero k, $1|k$ y si $k \neq 0$, $k|k$.

Teorema 1.3. *Supongamos que a, b y c son números enteros. Entonces*

1. *Si $a \neq 0$ entonces $a|0$, $a|a$, $a|(-a)$.*
2. *$1|a$, $(-1)|a$.*
3. *Si $a|b$ entonces $a|bc$.*
4. *Si $a|b$ y $b|c$ entonces $a|c$.*
5. *Si $a|b$ y $a|c$ entonces para todo $x, y \in Z$, $a|(bx + cy)$.*
6. *Si $a|b$ y $b \neq 0$ entonces $|a| \leq |b|$.*
7. *Si $a|b$ y $b|a$ entonces $a = b$ o $a = (-b)$.*

Definición 1.4 (Máximo Común Divisor (gcd))**.** Sean a y b dos enteros no ambos iguales a cero. m se denomina máximo común divisor de a y b si $m|a$, $m|b$ y para todo d tal que $d|a$ y $d|b$ se tiene que $d|m$.

Teorema 1.4. *Si $a = bq + r$ entonces $\gcd(a, b) = \gcd(b, r)$.*

Teorema 1.5. *Si $\gcd(a, b) = d$, entonces d es la mínima combinación lineal positiva entre a y b.*

Corolario 1.1. *Si $d = \gcd(a, b)$, entonces $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.*

Teorema 1.6. *Si $k \neq 0$ entonces $\gcd(ka, kb) = |k| \gcd(a, b)$.*

Definición 1.5. Si n es un entero positivo se define la función sigma como la suma de todos los divisores positivos de n y se denota como $\sigma(n)$.

Definición 1.6. (Ecuación Diofántica) Es Una ecuación de la forma $p(x_1, x_2, ..., x_n) = 0$ donde $p(x_1, x_2, ..., x_n)$ es un polinomio con coeficientes enteros y con las variables restringidas a tomar únicamente valores enteros.

1.2. Congruencias

Definición 1.7. Sean a y b enteros cualesquiera y n un entero positivo. Si $n|(a-b)$ se dice que a es congruente con b módulo n y se escribe,

$$a \equiv b \pmod{n}.$$

Si a no es congruente con b módulo n, se dice que $a \not\equiv b \pmod{n}$.

Lema 1.1. *Para todo par de enteros a y b, se tiene*

1. $a \equiv b \pmod{1}$.
2. *Si* $d|n$ *y* $a \equiv b \pmod{n}$ *entonces* $a \equiv b \pmod{d}$.

Teorema 1.7. *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces*

1. *Para todo par de enteros* r *y* s, $ar + cs \equiv br + ds \pmod{n}$.
2. $a + c \equiv b + d \pmod{n}$.
3. $a - c \equiv b - d \pmod{n}$.
4. $ac \equiv bd \pmod{n}$.
5. *Para todo entero* r, $a + r \equiv b + r \pmod{n}$.
6. *Para todo entero* r, $ar \equiv br \pmod{n}$.

1.3. Análisis

Definición 1.8. Progresión aritmética es toda sucesión en la cual cada término después del primero se obtiene sumándole al término anterior una constante llamada razón o diferencia.

Definición 1.9. Una topología en un espacio X es una colección $\mathcal{T}$ de subconjuntos de X con las siguientes propiedades.

1. $\varnothing \in \mathcal{T}$,X$\in \mathcal{T}$
2. $(O_1 \in \mathcal{T}, O_2 \in \mathcal{T}) \Rightarrow (O_1 \cap O_2 \in \mathcal{T})$
3. $\forall S \subset \mathcal{T}, \cup_{\mathcal{O}\in\mathcal{S}}\mathcal{O} \in \mathcal{T}$

Los conjuntos en $\mathcal{T}$ son llamados abiertos, sus complementos son llamados cerrados. Los conjuntos cerrados tienen las siguientes propiedades.

- X y $\varnothing$ son cerrados
- La unión finita de conjuntos cerrados es cerrada
- La intersección de un número arbitrario de conjuntos cerrados es cerrada

X es llamado un espacio topológico.

Definición 1.10. Dado un espacio X, una base para una topología X es una colección $\mathcal{B}$ de subconjuntos de X tales que

1. para todo $x \in X$, existe al menos una base B tal que $x \in B$.
2. si $x \in B_1 \cap B_2$ con B_1, B_2 bases, entonces existe una base B_3 tal que $x \in B_3 \subseteq B_1 \cap B_2$.

Definición 1.11 (Serie geométrica)**.** Sea r^n una sucesión. Se llama serie geométrica a la siguiente sumatoria

$$\Sigma_{n=1}^{\infty} r^n.$$

Considérese $S_n = \Sigma_{k=0}^{n} r^k = 1 + r + r^2 + \cdots + r^n$, luego

$$(11 + r + r^2 + \cdots + r^n)(1 - r) = 1 - r^{n+1},$$

de donde

$$S_n = \frac{1 - r^{n+1}}{1 - r}, r \neq 1.$$

Ahora

$$\lim_{n\to\infty} S_n = \lim_{n\to\infty} \frac{1 - r^{n+1}}{1 - r} = \begin{cases} \frac{1}{1-r} & \text{si } 0 \leq r < 1 \\ +\infty & \text{si } r > 1. \end{cases}$$

Así la serie $\Sigma_{n=1}^{\infty} r^n$ converge si $|r| < 1$ y en caso contrario diverge.

1.4. Residuos cuadráticos y reciprocidad

Definición 1.12. Sea p un primo impar y a un entero tal que $\gcd(a, p) = 1$. Si la congruencia

$$x^2 \equiv a \pmod{p}$$

tiene solución, decimos que *a es un residuo cuadrático módulo p.*

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

Definición 1.13. Si p es un primo impar, el *símbolo de Legendre* $\left(\frac{a}{p}\right)$ se define como

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \pmod{p}, \\ 1 & \text{si } a \text{ es un residuo cuadrático módulo } p, \\ -1 & \text{si } a \text{ no es un residuo cuadrático módulo } p. \end{cases}$$

Teorema 1.8. *Sea p un primo impar entonces,*

1. *Hay exactamente $\frac{p-1}{2}$ residuos cuadráticos módulo p incongruentes.*

Teorema 1.9 (Criterio de Euler)**.** *Si p es un primo impar y $\gcd(a,p) = 1$, entonces*

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

Teorema 1.10. *Sea p un primo impar y sean a y b enteros primos relativos con p. Entonces,*

1. *Si $a \equiv b \pmod{p}$ entonces $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. $\left(\frac{a^2}{p}\right) = 1$.
3. $\left(\frac{1}{p}\right) = 1$.
4. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.
5. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
6. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
7. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Corolario 1.2. *Para todo primo impar p se tiene la identidad*

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

La ley de reciprocidad cuadrática es uno de los resultados más notables de la Teoría de los Números, ya que permite calcular el valor de $\left(\frac{p}{q}\right)$ en muchos casos.

Teorema 1.11 (Ley de reciprocidad cuadrática)**.** *Sean p y q números primos impares distintos. Entonces se tiene*

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

1.5. Polinomios

Definición 1.14. Sea $p(x)$ un polinomio cuadrático $P(x) = ax^2 + bx + c$ entonces $\Delta = b^2 - 4ac$ se denomina discriminante del polinomio.

Teorema 1.12. *Sea $P(x) = ax2 + bx + c$ un polinomio cuadratico y $\Delta = b^2 - 4ac$. Dados los números reales a, b, c, se tiene*

- *Cuando $\Delta > 0$, $P(x)$ tiene dos raíces reales distintas $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, y su representación gráfica cruza el eje de las abscisas dos veces.*
- *Cuando $\Delta = 0$, $P(x)$ tiene dos raíces coincidentes reales $x_1 = x_2 = -\frac{b}{2a}$, y su representación gráfica es tangente al eje de abscisas.*
- *Cuando $\Delta < 0$, $P(x)$ no tiene raíces reales y su representación gráfica está estrictamente por encima o por debajo del eje de abscisas. En este caso, P(x) tiene dos raíces complejas distintas.*

Teorema 1.13. *El desarrollo de la potencia n-ésima de un binomio es una suma donde los exponentes b y c son números naturales con $b + c = n$, así,*

$$(x + y)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} x^{n-k} y^k$$

1.6. Teoría de Grupos

Definición 1.15. un grupo $(G, *)$ es un conjunto G, junto con una operación binaria $*$ en G, tal que satisface las siguientes acciones

- La operación binaria $*$ es asociativa.
- Existe un elemento e en G tal que $e * x = x * e = x$ para todas las x en G.
- Para cada a en G existe un elemento a' en G para el cual $a' * a = a * a' = e$.

Definición 1.16. Se dice que G es un grupo abeliano si se cumple la propiedad conmutativa para todo par de elementos en el grupo.

Definición 1.17. Sea G un grupo y $a \in G$. El orden de a en G es el menor numero n tal que $a^n = e$ en G, donde e es la identidad del grupo G.

Definición 1.18. El orden de un grupo es su cardinalidad, es decir, el número de elementos que tiene.

Definición 1.19. Sea G un grupo y sea S un subconjunto de G. Si para cada $a, b \in S$ el producto ab calculado en G tambien está en S, entonces S es cerrado bajo la operación de grupo de G.

Definición 1.20. Si H es un subconjunto de un grupo G cerrado bajo la operación de grupo de G y si H es un grupo bajo dicha operación, entonces H es un subgrupo de G. Se denotara por $H \leq G$ el hecho de que H es un subgrupo de G.

En la teoría de grupos, el teorema de Lagrange es un resultado importante que relaciona el orden de un grupo finito G con el orden de cualquiera de sus subgrupos.

Teorema 1.14. *(Teorema de Lagrange)Si G es un grupo finito y H es un subgrupo de G, entonces $|H|||G|$ donde $|G|$ y $|H|$ son el orden del grupo G y el orden del subgrupo H respectivamente.*

Definición 1.21. Sea $H \leq G$ y sea $a \in G$. La clase lateral izquierda aH de H es el conjunto $\{ah : h \in H\}$. La clase lateral derecha se define de manera similar.

Definición 1.22. Si G es un grupo y $a \in G$, entonces

$$H = \{a^n : n \in \mathbf{Z}\}$$

es un subgrupo de G. Este subgrupo es el subgrupo cíclico de G generado por a. Además, dado un grupo G y un elemento $a \in G$, si

$$G = \{a^n : n \in \mathbf{Z}\},$$

entonces a es un generador de G y el grupo G es cíclico. Si existe un conjunto finito de elementos a_i que genere G, entonces G es finitamente generado.

1.7. Teoría de Anillos

Definición 1.23. Un anillo R es una terna $(R, +, *)$ donde R es un conjunto no vacio y $+, *$ son dos operaciones binarias en R, llamadas suma y producto respectivamente, que cumplen las siguientes condiciones

- (R, +) es un grupo abeliano
- el producto cumple la propiedad asociativa
- Se cumplen las propiedades distributivas derecha e izquierda del producto con respecto a la suma

Definición 1.24. Sea R un anillo. Se dice que R tiene unitario si existe en R un elemento neutro para el producto.

Definición 1.25. Sea R un anillo conmutativo con unitario y sea $a \neq 0$ en R, se dice que a es una unidad en R si $a|1$, es decir, existe b en R tal que $ab = 1$.

Definición 1.26. Un anillo R con unitario es un anillo con división si todo elemento distinto de 0 en R es una unidad en R.

Definición 1.27. Un campo es un anillo conmutativo con división.

1.7.1. Ideales y Anillos Cocientes

Sea R un anillo y $(N, +)$ un subgrupo aditivo de $(R, +)$. Considérese el conjunto de clases laterales izquierdas módulo N, es decir,

$$R/N = \{a + N, a \in R\},$$

R/N con la suma de clases laterales es un grupo abeliano. Defínase en R/N la siguiente multiplicación

$$(a + N)(b + N) = ab + N$$

Teorema 1.15. *Sean R un anillo y N un subgrupo aditivo de R, la multiplicación de clases laterales en R/N está bien definida si y solo si para todo $r \in R$ se tiene*

$$rN = \{rn : n \in N\} \subseteq N \text{ y } Nr = \{nr : n \in N\} \subseteq N$$

.

Teorema 1.16. *Sea R un anillo y N un subgrupo aditivo de R. Si la multiplicación inducida en R/N está bien definida, entonces R/N es un anillo.*

Definición 1.28. Sea R un anillo, un subconjunto no vacio de R es un ideal de R si satisface las dos condiciones siguientes

- N es un subgrupo aditivo de R
- Para toda $r \in R$ y toda $n \in N$ se tiene rn, $nr \in N$

Teorema 1.17. *Sea R un anillo. R/N es un anillo si y solo si N es un ideal de R.*

Definición 1.29. Si N es un ideal de un anillo R, entonces el anillo R/N, con la suma y multiplicación de clases laterales se denomina anillo cociente o anillo factor.

Definición 1.30. Sea R un anillo conmutativo y $a \in R$. El ideal principal generado por a, se denota con $< a >$ y se define por

$$< a >= \{ar : r \in R\}.$$

Teorema 1.18. *Sea F un campo, si $p(x)$ es un polinomio irreducible en F, entonces $F[x]/ < p(x) >$ es un campo.*

Definición 1.31. Sean $R_!$ y R_2 dos anillos. Una funcion $f : R_1 \to R_2$ es un homomorfismo de anillos si satisface que para todo par de elementos $a, b \in R$ se satisfacen las dos condiciones siguientes

- $f(a + b) = f(a) + f(b)$
- $f(a.b) = f(a)f(b)$.

Si f es biyectiva entonces se dice que f es un isomorfismo de anillos y en tal caso se dice que R_1 y R_2 so anillos isomorfos.

Definición 1.32. Un grupo G es un grupo de torsión si todo elemento de G es de orden finito. G es libre de torsión si ningún otro elemento aparte de la identidad es de orden finito.

Lema 1.2. *Un grupo abeliano finito T es isomorfo a dos tipos diferentes de productos directos de grupos cíclicos, como sigue*

1. *T es isomorfo a un producto*

$$\mathbf{Z}_{(p_1)^{r_1}} \times \mathbf{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbf{Z}_{(p_n)^{r_n}}$$

   donde los p_i son primos no necesariamente distintos. Este producto directo de grupos cíclicos de orden la potencia de un primo isomorfo a T, es único excepto por un rearreglo de los factores.

2. *T es isomorfo a un producto directo*

$$\mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times \cdots \times \mathbf{Z}_{m_r}$$

   donde m_i divide a m_{i+1}. Los coeficientes de Torsión m_i de T son únicos.

Definición 1.33. El conjunto potencia de A (o conjunto de partes) es el conjunto $P(A)$ formado por todos los subconjuntos de A: $b \in \mathcal{P}(A)$ cuando $b \subseteq A$ y se denota con 2^A.

Capítulo 2

Conceptos básicos sobre números primos

En este capítulo se presentan algunas definiciones, teoremas y corolarios relacionados con la teoría de números y más específicamente con los números primos, que son las piezas centrales de dicha teoría y objeto fundamental de este trabajo.

Definición 2.1. Un entero $p > 1$ se denomina un número primo si tiene exactamente dos divisores positivos, es decir sus únicos divisores son 1 y p.

Un entero mayor que 1 que no es primo se denomina *compuesto*.

Definición 2.2. Si a y b son enteros no ambos iguales a cero tales que $\gcd(a, b) = 1$, se dice que a y b son primos relativos. Más generalmente si $a_1, a_2, ..., a_n$ son enteros tales que para todo i y para todo j con $i \neq j$, $1 \leq i, j \leq n$ se tiene $\gcd(a_i, a_j) = 1$, decimos que $a_1, a_2, ..., a_n$ son primos relativos dos a dos.

Teorema 2.1. *Si* $a|bc$ *y* $\gcd(a, b) = 1$, *entonces* $a|c$.

Demostración. Como $a|bc$ existe $k \in \mathbb{Z}$ tal que

$$bc = ak.$$

Como $\gcd(a, b) = 1$ existen enteros x, y tales que $ax + by = 1$.
Por lo tanto

$$\begin{aligned} c &= c(ax + by) \\ &= acx + bcy \\ &= acx + aky \\ &= a(cx + ky), \end{aligned}$$

es decir, $a|c$. ■

Como consecuencias del anterior resultado se obtienen los siguientes corolarios.

Corolario 2.1 (Euclides)**.** *Si p es primo y $p|ab$, entonces $p|a$ ó $p|b$.*

Demostración. Sí $p \nmid a$ entonces $\gcd(a, p) = 1$ y por el teorema $p|b$. ■

Corolario 2.2. *Si p es primo y $p|a_1a_2 \cdots a_n$, entonces $p|a_i$ para algún i, $1 \leq i \leq n$.*

Demostración. Por inducción sobre n.

Corolario 2.3. *Si p, $p_1, p_2, ..., p_n$ son números primos y $p|p_1p_2 \cdots p_n$, entonces $p = p_i$ para algún $i, 1 \leq i \leq n$.*

Demostración. Por hipótesis $p, p_1, p_2, ..., p_n$ son números primos y $p|p_1p_2 \cdots p_n$. Entonces por el resultado anterior $p|p_i$ para algún i, $1 \leq i \leq n$, pero $\gcd(p, p_i) = 1$ para todo $i = 1, 2, ..., n$. En consecuencia $p = p_i$. ■

Corolario 2.4. *Si $a_1, a_2, ..., a_n$ son enteros primos relativos dos a dos y para cada $i = 1, 2, ..., n$ $a_i|c$, entonces $a_1a_2 \cdots a_n|c$.*

Demostración. Por inducción sobre n.

Teorema 2.2 (Fermat)**.** *Sea p un número primo y a un entero primo relativo con p. Entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostración. Se sabe que $\mathbb{Z}_p^*$ constituye un grupo multiplicativo y dado que

$$|Z_p^*| = p - 1,$$

entonces por el Teorema de Lagrange para teoría de grupos se tiene $|a|_p|p - 1$ para todo $a \in Z_p^*$, luego existe $k \in \mathbb{Z}$ tal que $p - 1 = |a|_p k$. Pero por definición se tiene

$$a^{|a|_p} \equiv 1 \pmod{p}$$

entonces

$$(a^{|a|_p})^k \equiv (1)^k \pmod{p}$$

$$a^{|a|_p k} \equiv 1 \pmod{p}$$

por lo tanto

$$a^{p-1} \equiv 1 \pmod{p}$$

■

Como consecuencia inmediata del teorema anterior se tiene el siguiente corolario.

Corolario 2.5 (Pequeño Teorema de Fermat)**.** *Si p es un número primo, entonces*

$$a^p \equiv a \pmod{p}$$

para todo entero a.

Teorema 2.3 (Fundamental de la Aritmética, TFA)**.** *Todo entero $n > 1$ es primo o se puede factorizar como producto de primos, este producto es único salvo por el orden de los factores. Es decir,*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

donde los exponentes a_i son enteros positivos y $p_1 < p_2 < \cdots < p_k$ son primos.

Demostración. La prueba del teorema se divide en dos partes, la existencia de una descomposición en factores primos de n y su unicidad.
Sea S el conjunto de todos los números naturales que son primos o que pueden escribirse como producto de primos. Luego

$$S \subseteq \{k \in \mathbb{N} : k \geq 2\}.$$

Primero, dado que 2 es un número primo, entonces $2 \in S$. Ahora supóngase que $n > 2$ y que $k \in S$ para todo k tal que $2 \leq k < n$. Se debe probar que $n \in S$. Si n es primo entonces $n \in S$, con lo que termina la prueba. Si n no es primo existen r y t tales que $n = rt$ con $2 \leq r, t < n$. Pero por hipótesis r y t son primos o producto de primos. En consecuencia n es producto de primos, es decir $n \in S$. Por lo tanto por el Principio de Inducción Matemática Generalizado (PIM2)

$$S = \{k \in \mathbb{N} : k \geq 2\}.$$

Para probar la unicidad de la factorización salvo el orden se usará inducción sobre n. Para $n = 2$ claramente la representación es única. Supóngase ahora que para todo entero k con $2 \leq k < n$ la representación es única y que

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

donde p_i y q_i son primos con $p_1 \leq p_2 \leq \cdots \leq p_s$ y $q_1 \leq q_2 \leq \cdots \leq q_t$. Así, $p_1 | q_1 q_2 \cdots q_t$ en consecuencia $p_1 = q_j$ para algún j por lo que $q_1 \leq p_1$. Análogamente $q_1 | p_1 p_2 \cdots p_s$, entonces $q_1 = p_i$ para algún i, así $p_1 \leq q_1$, lo anterior demuestra que $p_1 = q_1$ luego

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

Como $\frac{n}{p_1} < n$ la hipótesis de inducción garantiza que estas dos representaciones de $\frac{n}{p_1}$ son idénticas (se ha escogido un orden), en consecuencia $s = t$ y para cada i, $p_i = q_i$. Luego por el Principio de Inducción Matemática (PIM) la prueba esta completa. ■

2.1. Infinitud de los números primos.

Teorema 2.4. *Existen infinitos números primos.*

En torno a este teorema existen varias pruebas realizadas por diferentes autores. En esta sección se presentan algunas de ellas. Más detalles y otras pruebas pueden encontrarse en [2], [8], [9] y [10].

2.1.1. Euclides

Sin duda uno de los más grandes matemáticos Griegos (325 - 265 a.c.), vivió en el siglo III a.c. Fue profesor de matemáticas en el Museo de Alejandría, la escuela del saber más brillante de su tiempo. Entre sus escritos más importantes se destaca la que podría llamarse la obra maestra de Euclides *" Los Elementos"* considerada la base de la geometría plana moderna. En dicha obra también se tratan aspectos importantes de la teoría de números como definiciones de número primo, número impar y número perfecto, además se plantea la pregunta de cuantos números primos existen y como respuesta se obtiene la que se conoce como la más elegante y clásica demostración de las matemáticas que corresponde a la proposición 20 del libro IX de Los Elementos.

Demostración 1 (Euclides)
Supóngase que el conjunto de números primos es finito y sea p el primo más grande. Considerese el producto de todos los primos más 1, así

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p + 1.$$

Luego n no puede ser divisible por ninguno de los primos de 2 hasta p, porque cualquiera de estas divisiones dejará como residuo 1, así existe un primo que no ha sido considerado. Pero se ha supuesto que los números hasta p incluyen todos los primos con lo que se llega a una contradicción. Por lo tanto, existen infinitos números primos. ■

2.1.2. Ernst Eduard Kummer

Matemático alemán (1810 - 1893), destacado por su gran capacidad para la matemática aplicada, realizó diversas e importantes contribuciones a la matemática en diferentes áreas. Por ejemplo en la codificación de algunas relaciones entre series hipergeométricas, también fueron objeto de su interés aspectos de la teoría de números como la infinitud de los números primos. A continuación se presenta la demostración realizada por Kummer en la que utiliza una idea similar a la desarrollada por Euclides.

Demostración 2 (Kummer)
Supóngase que existe solo un número finito de primos $p_1 < p_2 < \cdots < p_r$. Sea $N{=}p_1 \cdot p_2 \cdots p_r$. El

entero $N-1$, siendo un producto de primos, tiene un divisor primo, p_i en común con N; así, p_i divide a $N-(N-1)=1$, lo que es absurdo. ■

2.1.3. Hillel Fürstenberg

Matemático Americano-Israelí (1935 -), reconocido por la aplicación de métodos de teoría de probabilidades a otras áreas de las matemáticas, incluida la teoría de números. Furstenberg obtuvo reconocimiento muy tempranamente en su carrera gracias a una innovadora prueba de la infinitud de los números primos basada en topología.

Demostración 3 (Fürstenberg)
Defínase una topología $\mathcal{T}$ en $\mathbb{Z}$ usando las progresiones aritméticas (de $-\infty$ a $+\infty$) como una base. Se puede deducir que $\mathcal{T}$ es un espacio topológico, porque la intersección de dos progresiones aritméticas es una progresión aritmética. Los conjuntos abiertos de $\mathcal{T}$ son precisamente las uniones de progresiones aritméticas. En particular cualquier conjunto abierto es infinito ó vacío.

Ahora defínase para cada primo p el conjunto A_p cuyos elementos son todos los múltiplos de p, es decir,

$$A_p = \{pk : k \in \mathbf{Z}^+\}.$$

Las progresiones A_p son cerradas ya que su complemento es la unión de todas las otras progresiones aritméticas en $\mathcal{T}$, las cuales son conjuntos abiertos. Ahora sea A la unión de las progresiones A_p,

$$A = \cup_{p\in\mathbb{P}} A_p.$$

Si $\mathbb{P}$ es un conjunto finito, entonces A es una unión finita de conjuntos cerrados, así A es cerrado. Pero todos los enteros excepto -1 y 1 son múltiplos de algún primo, así el complemento de A es el conjunto $\{-1,1\}$, por lo tanto A debe ser abierto. Esto muestra que A no es una unión finita y así el conjunto $\mathbb{P}$ es infinito. ■

2.1.4. Christian Goldbach

Matemático germano (1690 - 1764), recordado por la conjetura que en honor a su nombre se conoce como la conjetura de Goldbach, la cual dice que *todo número par mayor que* 2 *puede escribirse como suma de dos números primos.*
Christian Goldbach demostró resultados importantes en la teoría de números, específicamente presentó una prueba acerca de la existencia de infinitos números primos utilizando los números de Fermat como una sucesión infinita de números naturales primos relativos dos a dos.

Demostración 4 (Goldbach)
Para esta prueba es necesario presentar el siguiente lema.

Lema 2.1. *Los números de Fermat $F_n = 2^{2^n} + 1$ son primos relativos dos a dos.*

Demostración. Primero se demuestra por inducción que $F_m - 2 = F_0 \cdot F_1 \cdots F_{m-1}$.
Así.
verifiquemos para $m = 2$

$$\begin{aligned} F_2 - 2 &= 2^{2^2} + 1 - 2 \\ &= 2^4 - 1 \\ &= (2^2 - 1)(2^2 + 1) \\ &= 3 \cdot 5 \\ &= (2^{2^0} + 1)(2^{2^1} + 1) \\ &= F_0 \cdot F_1. \end{aligned}$$

Ahora supóngase que se cumple para m. *(hipotesis inductiva)*
Entonces veamos para $m + 1$.

Como $F_{m+1} = 2^{2^{m+1}} + 1$, luego

$$\begin{aligned} F_{m+1} - 2 &= 2^{2^{m+1}} - 1 \\ &= (2^{2^m} - 1)(2^{2^m} + 1) \\ &= (F_m - 2)F_m = F_0 \cdot F_1 \cdots F_{m-1} \cdot F_m \end{aligned}$$

Por lo tanto $F_m - 2 = F_0 \cdot F_1 \cdots F_{m-1}$. Esto significa que si d divide a ambos a F_n y F_m (con $n < m$), entonces d también divide a $F_m - 2$; así d divide a 2. Pero cada número de Fermat es impar, luego d es 1. ■

Con ayuda del anterior resultado, se puede demostrar la infinitud de $\mathbb{P}$. En efecto, como existen infinitos números de Fermat y son primos relativos dos a dos, esto implica que existen infinitos números primos. ■
Cualquier sucesión infinita de primos relativos dos a dos funciona en esta prueba. Una forma de definir este tipo de sucesiones es la siguiente, sean a y b enteros positivos primos relativos, se define la sucesión como sigue,

$$a_1 = a,$$

$$a_n = \prod_{i=1}^{n-1} a_i + b, \quad \text{para todo } n > 1,$$

los números de Fermat (con $a = 1$, $b = 2$) y de la misma forma la sucesión de Sylvester,

$$a_1 = 2 \text{ y } a_{n+1} = (a_n)^2 - a_n + 1.$$

2.1.5. Peter Schorn

Fue uno de los muchos autores que presentaron una prueba de la infinitud de los numeros primos. Sin embargo su atencion se ha centrado en otros aspectos, tales como la informatica, la prueba realizada por él se puede encontrar en su pagina personal http://www.schorn.ch/.

Demostración 5 (Schorn)

Lema 2.2. *Si* $1 \leq i < j \leq n$, *entonces*

$$gcd((n!)i + 1, (n!)j + 1) = 1.$$

Demostración. En efecto, como $j = i + d$, para algún $1 \leq d < n$, entonces

$$\begin{aligned} \gcd((n!)i + 1, (n!)j + 1) &= \gcd((n!)i + 1, (n!)i + (n!)d + 1) \\ &= \gcd((n!)i + 1, (n!)d). \end{aligned}$$

Sea $e = \gcd((n!)i + 1, (n!)d)$, luego $e|(n!)d$.
Si $e|d$, entonces

$$e|(n!).$$

Así $e|(n!)i$. Pero $e|(n!)i + 1$, luego $e|1$. Por lo tanto $e = 1$ ■

Ahora probemos la infinitud de los primos. Supóngase que existen solo m números primos; sea $n = m + 1$. La anterior observación nos dice que los n enteros $(n!)i + 1$, para $i = 1, 2, ..., n$ son primos relativos dos a dos. Si p_i es un primo que divide a $(n!)i + 1$, entonces $p_1, p_2, ..., p_n$ son primos distintos, con $n = m + 1$, que contradice la suposición inicial. ■

2.1.6. Saidak

Esta demostración de la infinitud de los números primos fué presentada en el año 2006, apareció en un artículo de Filip Saidak con el título "A new Proof of Euclid's theorem" en American Mathematical Monthly.

Demostración 6 (Saidak)
Sea $n > 1$ un entero positivo. Como n y $n + 1$ son enteros consecutivos, ellos deben ser primos

relativos, y así el número $N_2 = n(n+1)$ debe tener al menos dos factores primos diferentes. Similarmente, como los enteros $n(n+1)$ y $n(n+1)+1$ son consecutivos, por lo tanto primos relativos, el número $N_3 = n(n+1)[n(n+1)+1]$ debe tener al menos tres factores primos diferentes. Este proceso puede continuar indefinidamente. ■

2.1.7. Thomas Joannes Stieltjes

Matemático holandés (1856 - 1894). Fue profesor de cálculo diferencial e integral en la Universidad de Toulouse; trabajó en casi todas las ramas del análisis, fracciones continuas y teoría de números, es conocido como *" el padre de las fracciones continuas"*.

Demostración 7 (Stieltjes)
Supóngase que $p_1, p_2, ..., p_r$ son los únicos primos existentes. Ahora sea $N = p_1 \cdot p_2 \cdots p_r$ y sea $N = mn$ cualquier factorización de N, con $1 \leq m, n$. Cada primo p_i divide a m ó a n, pero no a ambos, entonces $m+n$ no es divisible por cualquiera de los primos existentes, lo que es absurdo ya que $m + n \neq 1$. ■

2.1.8. Leonhard Euler

Matemático suizo (1707 - 1783), considerado el matemático más destacado del siglo XVIII y uno de los más grandes matemáticos de todos los tiempos. Realizó descubrimientos importantes en campos tan diversos como el cálculo infinitesimal y teoría de gráfos. Euler llegó a descubrir relaciones sorprendentes entre la teoría de números y el análisis. Demostró que la divergencia de la serie armónica implica la existencia de infinitos números primos. La demostración es por reducción al absurdo, se basa en el Teorema Fundamental de la Aritmética y en la divergencia de la serie armónica.

Demostración 8 (Euler)
La idea
Euler mostró que deben existir infinitos primos porque una cierta expresión formada por todos los primos es infinita. Si p es cualquier primo, entonces $1/p < 1$; por tanto la suma de las serie geométrica es

$$\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-(1/p)}.$$

Similarmente, si q es otro primo, entonces

$$\sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1-(1/q)}.$$

Multiplicando estas igualdades:

$$1+\frac{1}{p}+\frac{1}{q}+\frac{1}{p^2}+\frac{1}{pq}+\frac{1}{q^2}+\cdots=\frac{1}{1-(1/p)}\times\frac{1}{1-(1/q)}.$$

Explícitamente el lado izquierdo es la suma de los inversos de todos los números de la forma $p^h q^k (h,k\geq 0)$, cada uno contado sólo una vez, porque cada número natural tiene una factorización única como producto de primos. Esta idea es la base de la siguiente prueba.

Demostración
Supóngase que $p_1, p_2, ..., p_n$ son todos los primos. Para cada $i = 1, 2, ..., n$,

$$\sum_{k=o}^{\infty}\frac{1}{{p_i}^k}=\frac{1}{1-(1/p_i)}.$$

Multiplicando estas n ecuaciones, se obtiene

$$\prod_{i=1}^{n}\left(\sum_{k=o}^{\infty}\frac{1}{{p_i}^k}\right)=\prod_{i=1}^{n}\frac{1}{1-(1/p_i)},$$

donde el lado izquierdo es la suma do los inversos de todos los números naturales, cada uno contado una vez, esto se sigue del Teorema Fundamental de la Aritmética que todo número natural es igual, en una forma única, al producto de primos. Pero la serie $\sum_{j=1}^{\infty}\frac{1}{j}$ es divergente; siendo una serie de términos positivos, así el lado izquierdo es infinito, mientras el lado derecho es claramente finito, esto es absurdo. ■

2.1.9. Axel Thue

Matemático noruego (1863 - 1992), reconocido por su original trabajo en aproximación diofántica y combinatorias. El declaró en 1914 el llamado problema de las palabras para semigrupos o problema de Thue. A continuacion se presenta la prueba de Thue acerca de existencia de infinitos números primos en la que utiliza unicamente el Teorema Fundamental de la Aritmetica.

Demostración 9 (Thue)
Sean $n, k \geq 1$ enteros que satisfacen $(1+n)^k < 2^n$, la anterior desigualdad se cumple para $k = 1$ y para todo $n > 1$. Sean $p_1 = 2, p_2 = 3, ..., p_r$ todos los primos menores o iguales que 2^n. Supóngase que $r \leq k$. Por el Teorema Fundamental de la Aritmética, todo entero $m, 1 \leq m \leq 2^n$, puede ser escrito de forma única como

$$m = 2^{e_1}\cdot 3^{e_2}\cdots p_r^{e_r},$$

donde $0 \leq e_1 < n, 0 \leq e_2 < n, ..., 0 \leq e_r < n$.
Como el número de valores que pueden tomar los exponentes $e_1, e_2, ..., e_r$ es a lo mas $(n+1)^r$, se

sigue que $2^n \leq (n+1)n^{r-1} < (n+1)^r \leq (n+1)^k < 2^n$, lo que es absurdo. Así $r \geq k+1$.
Ahora supóngase que $n = 2k^2$, donde k es un entero positivo cualquiera y dado que $1 + 2k^2 < 2^{2k}$ para cada $k \geq 1$ se sigue que

$$(1 + 2k^2)^k < 2^{2k^2} = 4^{k^2}.$$

Así, existen al menos $k+1$ primos menores que 4^{k^2}.
Como k puede tomarse arbitrariamente grande, esto muestra que existen infinitos primos y que $k+1$ es realmente un límite inferior para el número de primos menores que 4^{k^2}. ■

Al parecer las pruebas realizadas por Perott, Auric y Metrod no tuvieron mayor trascendencia. De hecho dichas pruebas se conocen gracias al libro *History of the theory of numbers vol 1* de Dickson.

2.1.10. Perott

Esta prueba se conoce como la prueba olvidada de Perott, es una prueba de 1881 y aparece en [9]. Esta prueba consiste en contar los enteros menores que un entero dado que no son divisibles por un cuadrado, contando aquellos que son divisibles por cada cuadrado. No se pudo encontrar información específica sobre el autor.

Demostración 10 (Perott)
Se sabe que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} < 2,$$

ver [6]. Ahora considérese

$$\delta = 2 - \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

Supóngase que solo existen r números primos $p_1 < p_2 < \cdots < p_r$. Sea N cualquier entero tal que $p_1 \cdot p_2 \cdots p_r < N$. El número de enteros menores o iguales que N que no son divisibles por un cuadrado es por lo tanto 2^r (que es el número de todos los posibles subconjuntos distintos de $\mathbb{P}$), porque todo entero se puede expresar de forma única como producto de números primos. El número de enteros menores o iguales que N divisibles por p_i^2 es a lo sumo N/p_i^2; así el número de enteros menores o iguales que N y divisibles por algún cuadrado es como máximo $\sum_{i=1}^{r} N/p_i^2$. Por lo tanto

$$N \leq 2^r + \sum_{i=1}^{r} \frac{N}{p_i^2} < 2^r + N\left(\sum_{n=1}^{\infty} \frac{1}{n^2} - 1\right) = 2^r + N(1-\delta). \tag{2.1.1}$$

Como $2^r < p_1 \cdot p_2 \cdots p_r < N \leq N\delta$, de la desigualdad (2.1.1)
se tiene que

$$N < N\delta + N(1-\delta) = N.$$

Luego $N < N$, lo que es absurdo. Por lo tanto existen infinitos números primos ■
La anterior demostracion fue generalizada por L. J. P. Kilford. (Ver *An infinitude of proofs of the infinitude of primes*).

2.1.11. Auric

Esta es otra prueba considerada como olvidada y lastimosamente tampoco se ha encontrado información sobre su autor. Ver [9].

Demostración 11 (Auric)
Supóngase que existen solo r números primos $p_1 < p_2 < \cdots < p_r$. Sean $t \geq 1$ un entero cualquiera y $N = p_r^t$. Por el Teorema Fundamental de la Aritmética cada entero $m, 1 \leq m \leq N$, se puede escribir de forma única como $m = p_1^{f_1} \cdot p_2^{f_2} \cdots p_r^{f_r}$ y la sucesión $\{f_1, f_2, ..., f_r\}$, con cada $f_i \geq 0$ se define de forma única. Notese también que $p_1^{f_i} \leq m \leq N = p_r^t$. Sea $E = (\log p_r)/(\log p_1)$, entonces $f_i \leq tE$. Así, el número de enteros positivos menores o iguales que N es a lo más igual al número de sucesiones $\{f_1, f_2, ..., f_r\}$; es decir, $p_r^t = N \leq (tE+1)^r \leq t^r(E+1)^r$. Pero si t es suficientemente grande, esta desigualdad no se puede cumplir, una vez que la función exponencial p_r^t crece más rápido que la función $t^r(E+1)^r$. Lo cual muestra que el número de primos debe ser infinito. ■

2.1.12. Métrod

Al igual que las dos anteriores pruebas también se considera como una prueba olvidada sobre la infinitud de los números primos. Lastimosamente tampoco se puede encontrar información sobre su autor. Ver [9].

Demostración 12 (Métrod)
Supóngase que existen solo r números primos $p_1 < p_2 < \cdots < p_r$. Sea $N = p_1 \cdot p_2 \cdots p_r$, y para cada $i = 1, 2..., r$, sea $Q_i = N/p_i$. Note que p_i no divide a Q_i, mientras p_i divide a Q_j, para todo $j \neq i$. Sea $S = \sum_{i=1}^{r} Q_i$. Si q es cualquier primo que divide a S entonces $q \neq p_i$ porque p_i divide a Q_j (para $j \neq i$) pero p_i no divide a Q_i. Así deben existir otros primos. ■

El siguiente resultado también sirve como una prueba de la infinitud de los números primos, pero es más general pues demuestra que existen infinitos números primos en una determinada sucesión. La demostración puede encontrarse en [4].

Teorema 2.5 (Dirichlet)**.** *Si* $\gcd(a, d) = 1$ *con* a *y* d *enteros positivos, entonces hay un número infinito de primos de la forma* $a + kd$.

Mas adelante se enuncia el denominado *Teorema de los Números Primos*, uno de los más famosos de la teoría avanzada de números, que proporciona una estimación sobre la distribución de los primos en el conjunto de los números naturales. Definamos primero la función $\pi(x)$ que asigna a cada entero positivo x el número de primos menores o iguales a x, $\pi(1) = 0, \pi(2) = 1, \pi(3) = 2, \pi(10) = 4$. Otros valores pueden encontrarse en la Tabla 2.1.
El siguiente teorema fue demostrado a mitad del siglo XIX por P. Chebyshev, en el se estableció el verdadero orden de magnitud para la función conteo de primos $\pi(x)$.

Teorema 2.6 (Chebyshev)**.** *Existen números positivos A, B tales que para todo $x > 2$,*

$$\frac{Ax}{\ln x} < \pi(x) < \frac{Bx}{\ln x}$$

Como ya se ha observado que la distribución de los primos es muy irregular, no existe una fórmula sencilla que defina $\pi(x)$. Sin embargo *El Teorema de los Números Primos* establece una aproximación asintótica de $\pi(x)$.

Teorema 2.7 (Teorema de los Números Primos, TNP)**.**

$$\lim_{x\to\infty} \frac{\pi(x)}{(\frac{x}{\log(x)})} = 1.$$

La afirmación del teorema fue conjeturada de manera independiente por Gauss en 1792 y por Legendre en 1798 pero sólo hasta 1896 J. Hadamard y C. De la Vallee Poussin demostraron el Teorema por primera vez utilizando teoría de funciones de variable compleja. En 1949 A. Selberg y P. Erdös dieron una demostración más elemental sin usar análisis complejo pero aún muy difícil para presentarla en estas notas. En 1997, D. Zagier presentó una prueba más corta, dada por Newmann. Ver demostración en [5].

x	$\pi(x)$
10^2	25
10^3	168
10^4	1229
10^6	78498
10^8	5761455
10^{12}	37607912018
10^{16}	279238341033925
10^{17}	2623557157654233
10^{18}	24739954287740860
10^{19}	234057667276344607
10^{20}	2220819602560918840
10^{21}	21127269486018731928
10^{22}	201467286689315906290
$4 \cdot 10^{22}$	783964159847056303858

Tabla 2.1: Valores de la función $\pi(x)$.

Capítulo 3

Generación de primos

Diferentes matemáticos han planteado con frecuencia problemas relacionados con los números primos con el fin de establecer una caracterización de ellos. En este capítulo se presentará uno de los interrogantes más recurrentes en el estudio de los números primos, ¿existe una función elemental f tal que $f(n)$ sea primo para todo n? Dicho interrogante busca encontrar expresiones sencillas a partir de las cuales se obtengan solamente números primos.
En el intento por dar respuesta a la pregunta, Euler probó que la función $f(n) = n^2 + n + 41$ es un número primo para cada asignación de n entre 1 y 39; sin embargo para $n = 40$ resulta

$$f(40) = 40^2 + 40 + 41 = 40^2 + 2(40) + 1 = (40 + 1)^2,$$

que obviamente es un número compuesto.
De hecho el siguiente resultado muestra que ningún polinomio en una variable con coeficientes enteros sirve para alcanzar el objetivo planteado.

Teorema 3.1. *Si $f(n)$ es un polinomio no constante con coeficientes enteros, entonces $f(n)$ es un número compuesto para infinitos valores enteros de n.*

Demostración. Si $f(n)$ es compuesto para todo $n \geq 1$, entonces claramente el teorema está probado. Ahora supóngase el caso que $f(n)$ es primo en algún momento, es decir, existe $n_0 \geq 1$ tal que $f(n_0) = p$, con p primo.
Dado que el $\lim_{n\to\infty} |f(n)| = \infty$, existe $n_1 \in \mathbb{Z}$ tal que si $n \geq n_1$, entonces $|f(n)| > p$.
Sea h tal que $n_0 + ph \geq n_1$, entonces

$$\begin{aligned} f(n_0 + ph) &= f(n_0) + (\text{múltiplos de } p) \\ &= p + (\text{múltiplos de } p) \\ &= Y \cdot p. \end{aligned}$$

Como $|f(n_0 + ph)| = |Y| \cdot p > p$. Así $f(n_0 + ph)$ es compuesto. ■

No se conoce si existe un polinomio en una sola variable de al menos grado mayor que 2 capaz de generar un número infinito de valores que sean primos.

Otro resultado está basado en la solución de ecuaciones Diofánticas, llamadas así en honor al matemático griego Diofanto de Alejandría quien las estudió detalladamente por primera vez.
James P. Jones et al. [7] demostraron que se pueden encontrar números primos a partir de un sistema de ecuaciones diofánticas con 26 variables. Más específicamente probaron que un número $k+2$ es primo si y sólo si el siguiente sistema de catorce ecuaciones diofánticas tiene una solución en los números naturales;

$$\begin{aligned}
wz + h + j - q &= 0 \\
(gk + 2g + k + 1)(h + j) + h - z &= 0 \\
16(k+1)^3(k+2)(n+1)^2 + 1 - f^2 &= 0 \\
2n + p + q + z - e &= 0 \\
e^3(e+2)(a+1)^2 + 1 - o^2 &= 0 \\
(a^2-1)y^2 + 1 - x^2 &= 0 \\
16r^2y^4(a^2-1) + 1 - u^2 &= 0 \\
n + l + v - y &= 0 \\
(a^2-1)l^2 + 1 - m^2 &= 0 \\
ai + k + 1 - l - i &= 0 \\
((a + u^2(u^2-a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2 &= 0 \\
p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m &= 0 \\
q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x &= 0 \\
z + pl(a - p) + t(2ap - p^2 - 1) - pm &= 0
\end{aligned}$$

Este sistema puede ser usado para encontrar un polinomio P en varias variables con coeficientes enteros, tal que el conjunto de valores positivos de P corresponde al conjunto de los números primos. Reducir el número de variables del polinomio aún es un problema abierto, sin embargo según [7] el mejor resultado obtenido se trata de un polinomio en 12 variables conocido por Yuri Matijasevi $\check{c}$ al parecer desde 1973.

En el estudio de los números primos es importante destacar aquellos que tienen una forma especial, con esto nos referimos a primos p que pueden obtenerse a partir de expresiones particulares. Por ejemplo los números de Mersenne M_n y los números de Fermat F_n definidos por

$$M_n = 2^n - 1 \text{ y } F_n = 2^{2^n} + 1,$$

que en algunas ocasiones resultan ser números primos.
Los primos de forma especial han sido de continuo interes por sí mismos y por su historia, en particular los números de Mersenne que se definen así.

Definición 3.1 (Números de Mersenne)**.** Son aquellos números de la forma $M_n = 2^n - 1$ con $n \in \mathbb{Z}^+$. Los números de Mersenne que son primos se denominan *Primos de Mersenne.*

Teniendo en cuenta algunas restricciones del exponente n, los números de Mersenne pueden ser números primos, como lo demuestra el siguiente teorema.

Teorema 3.2. *Si $M_n = 2^n - 1$ es primo, entonces n es primo.*

Demostración. Si n es compuesto, entonces $n = dk$ con $1 < d, k < n$; así $2^n - 1 = (2^d - 1)((2^d)^{k-1} + (2^d)^{k-2} + \cdots + 2^d + 1)$ es compuesto. ■

Esto significa que la búsqueda de primos de Mersenne se puede reducir a los exponentes primos n. Además nótese que el recíproco del teorema es falso, es decir, que si n es primo M_n puede no serlo. Por ejemplo para $n = 11$, $2^{11} - 1 = 23 \cdot 89$ no es primo aunque 11 si lo es. La parte práctica del teorema es que se puede descartar un gran número de exponentes, considerando solamente exponentes primos durante la búsqueda de primos de Mersenne. Aún más, se pueden descartar otros números de Mersenne compuestos, con ayuda del siguiente resultado el cual caracteriza como son los factores primos de M_n.

Teorema 3.3 (Euler)**.** *Para todo primo $q > 2$, cualquier factor primo de $M_q = 2^q - 1$ debe ser congruente con* $1 \pmod q$ *y además debe ser congruente con* $\pm 1 \pmod 8$.

Demostración. Sea r un factor primo de $2^q - 1$, con q primo, $q > 2$. Entonces $2^q \equiv 1 \pmod r$ y como q es primo, el menor exponente positivo h tal que $2^h \equiv 1 \pmod r$ debe ser q. Así, en el grupo multiplicativo de residuos no cero módulo r, el cual es de orden $r-1$, el residuo 2 tiene orden q. Esto implica que $r \equiv 1 \pmod q$, ya que el orden de un elemento en un grupo divide al orden del grupo. Como $2^q \equiv 1 \pmod r$, entonces $2^{q+1} \equiv 2 \pmod r$, de esta forma $2^{(q+1)/2}$ es una raíz cuadrada de 2 módulo q. Por la ley de la reciprocidad cuadrática, cualquier módulo primo del cual 2 es un resíduo cuadrático es congruente con $\pm 1 \pmod 8$, ver Capítulo 1. Luego $r \equiv \pm 1 \pmod 8$. ■

Así la búsqueda de primos de Mersenne recorre algún conjunto Q de exponentes primos, quitando candidatos $q \in Q$ verificando si $2^q \equiv 1 \pmod r$ para varios primos pequeños $r \equiv 1 \pmod q$ y $r \equiv \pm 1 \pmod 8$.
Los primos de Mersenne conocidos se presentan en la Tabla 3.1, en la cual además del primo de Mersenne se encuentra el número de dígitos que tiene y cuando fue encontrado.
Existen muchos problemas abiertos e interesantes entorno a los primos de Mersenne. Por ejemplo, no se ha demostrado si existen infinitos de estos primos e incluso no se sabe si infinitos números

Primos	Dígitos	Descubrimiento	Primos	Dígitos	Descubrimiento
2^2-1	1	antiguedad	$2^{21701}-1$	6533	30-10-1978
2^3-1	1	antiguedad	$2^{23209}-1$	6987	09-02-1979
2^5-1	2	antiguedad	$2^{44497}-1$	13395	08-04-1979
2^7-1	3	antiguedad	$2^{86243}-1$	25962	25-09-1982
$2^{13}-1$	4	1456	$2^{110503}-1$	33265	28-01-1988
$2^{17}-1$	6	1588	$2^{132049}-1$	39751	20-09-1983
$2^{19}-1$	6	1588	$2^{216091}-1$	65050	06-09-1985
$2^{31}-1$	10	1772	$2^{756839}-1$	227832	19-02-1992
$2^{61}-1$	19	1883	$2^{859433}-1$	258716	10-01-1994
$2^{89}-1$	27	1911	$2^{1257787}-1$	378632	03-09-1996
$2^{107}-1$	33	1914	$2^{1398269}-1$	420921	13-11-1996
$2^{127}-1$	39	1876	$2^{2976221}-1$	895932	24-08-1997
$2^{521}-1$	157	30-01-1952	$2^{3021377}-1$	909526	27-01-1998
$2^{607}-1$	183	30-01-1952	$2^{6972593}-1$	2098960	01-06-1999
$2^{1279}-1$	386	25-06-1952	$2^{13466917}-1$	4053946	14-11-2001
$2^{2203}-1$	664	07-10-1952	$2^{20996011}-1$	6320430	17-11-2003
$2^{2281}-1$	687	09-10-1952	$2^{24036583}-1$	7235733	15-05-2004
$2^{3217}-1$	969	08-09-1957	$2^{25964951}-1$	7816230	18-02-2005
$2^{4253}-1$	1281	03-11-1961	$2^{30402457}-1$	9152052	15-12-2005
$2^{4423}-1$	1332	03-11-1961	$2^{32582657}-1$	9808358	04-09-2006
$2^{9869}-1$	2917	11-05-1963	$2^{37156667}-1$	11185272	06-09-2008
$2^{9941}-1$	2993	16-05-1963	$2^{42643801}-1$	12837064	12-04-2009
$2^{11213}-1$	3376	02-06-1963	$2^{43112609}-1$	12978189	23-08-2008
$2^{19937}-1$	6002	04-03-1971	$2^{57885161}-1$	17425170	25-01-2013

Tabla 3.1: Primos de Mersenne conocidos

de Mersenne M_n con n primo son compuestos. Para determinar la primalidad de los números de Mersenne se utilizó el Test de Lucas-Lehmer del cual se hablará más adelante. Ver Capítulo 4. Los números de Mersenne están estrechamente relacionados con los números perfectos que se definen como se sigue.

Definición 3.2 (Números perfectos)**.** Un entero positivo n es llamado un número perfecto si este es igual a la suma de todos sus divisores positivos, excluyendo al mismo n. Luego $\sigma(n) = 2n$.

Por ejemplo, 6 es el primer número perfecto porque $6 = 1 + 2 + 3$. Euclides, muchos siglos antes que Mersenne ya conocía estos números y encontró una fuerte relación entre ellos y los números perfectos. Si M es un número primo de Mersenne, entonces $M \cdot (M+1)/2$ es un número perfecto. Asi mismo, Euler demostró en el siglo $XVIII$ que todos los números perfectos pares son de la forma $M \cdot (M+1)/2$. No se conocen en la actualidad números perfectos impares, se sospecha que no existe ninguno. Las anotaciones anteriores se pueden resumir en el siguiente resultado.

Teorema 3.4. *Un número par n es perfeto si y sólo si es de la forma*

$$n = 2^{q-1}M_q,$$

donde $M_q = 2^q - 1$ es un primo de Mersenne.

Demostración. Supóngase que $n = 2^a m$ es un número par, donde m es el mayor divisor impar de n. Los divisores de n son de la forma $2^j d$, donde $0 \leq j \leq a$ y $d|m$. Sea D la suma de los divisores de m excluyendo a m y sea $M = 2^{a+1} - 1 = 2^0 + 2^1 + ... + 2^a$. Así la suma de todos los divisores de n es $M(D + m)$. Si M es primo y $M = m$, entonces $D = 1$ y la suma de todos los divisores de n es $M(1 + m) = 2n$, por lo tanto n es perfecto.
Ahora supóngase que $n = 2^a m$ es perfecto. Entonces $M(D + m) = 2n = 2^{a+1}m = (M + 1)m$, de donde

$$m = MD.$$

Si $D > 1$, entonces D y 1 son divisores distintos de m menores que m, contradiciendo la definición de D, Así $D = 1$, por lo tanto m es primo y $m = M = 2^{a+1} - 1$. ■

Definición 3.3 (Números de Fermat)**.** Son aquellos números de la forma $F_n = 2^{2^n} + 1$ con $n \in \mathbb{Z}$ no negativos. Los números de Fermat que son primos se denominan *Primos de Fermat.*

Los famosos números de Fermat, como los números de Mersenne, han sido objeto de una ardua investigación. En 1637 Fermat declaró que los números F_n son siempre primos, en efecto los primeros cinco hasta $F_4 = 65537$ son primos. Sin embargo, este es uno de los pocos casos donde Fermat estuvo equivocado. Cada número de Fermat para el que se ha podido decidir su primalidad ha resultado compuesto; el primero de estos compuestos $F_5 = 4294967297$ fue factorizado por Euler.

Teorema 3.5. *Si $p = 2^m + 1$ es un primo impar, entonces m es una potencia de 2.*

Demostración. Supóngase que $m = ab$, donde a es el mayor divisor impar de m. Como

$$2^{ab} + 1 = (2^b + 1)(2^{(a-1)b} - 2^{(a-2)b} + 2^{(a-3)b} - \cdots - 2^b + 1),$$

entonces $2^b + 1$ es un factor de p. Pero p es primo, por lo tanto necesariamente $p = 2^b + 1$; esto es, $a = 1$ y $m = b$ es una potencia de 2. ■

El siguiente resultado es útil ya que restringe los posibles factores primos de un número de Fermat.

Teorema 3.6 (Euler, Lucas)**.** *Para todo $n \geq 2$, cada factor primo p de $F_n = 2^{2^n} + 1$ debe cumplir* $p \equiv 1 \pmod{2^{n+2}}$.

Demostración. Sea r un factor primo de F_n y sea h el menor entero positivo con $2^h \equiv 1 \pmod{r}$. Entonces, como $2^{2^n} \equiv -1 \pmod{r}$, tenemos $h = 2^{n+1}$. Así 2^{n+1} divide a $r-1$. Como $n \geq 2$, tenemos que $r \equiv 1 \pmod{8}$, luego por la ley de reciprocidad cuadratica 2 es un residuo cuadratico módulo r, así $h = 2^{n+1}$ divide a $\frac{r-1}{2}$, de donde $r \equiv 1 \pmod{2^{n+2}}$ para todo factor primo r de n. ■

Fue este resultado el que le permitió a Euler encontrar el factor 641 de F_5 y por lo tanto ser el primero en refutar la afirmación de Fermat. En la actualidad, el resultado anterior es útil en la búsqueda de factores en números de Fermat muy grandes.
Gracias a la combinación de varios métodos, incluyendo el test Pepin o en muchos casos los más nuevos algoritmos de factorización disponibles, varios números de Fermat han sido factorizados ya sea parcial o completamente o en su defecto se ha determinado que son compuestos. La situación actual para todo F_n, con $n \leq 24$ es la siguiente.

$F_0 = 3 = P$
$F_1 = 5 = P$
$F_2 = 17 = P$
$F_3 = 257 = P$
$F_4 = 65,537 = P$
$F_5 = 641 \cdot 6700,417$
$F_6 = 274,177 \cdot 67,280,421,310,721$
$F_7 = 59,649,589,127,497,217 \cdot 5,704,689,200,685,129,054,721$
$F_8 = 1,238,926,361,552,897 \cdot 93,461,639,715,357,977,769,163,558,199,606,896,$
$584,051,237,541,638,188,580,280,321$
$F_9 = 2,424,833 \cdot 7,455,602,825,647,884,208,337,395,736,200,454,918,783,366,$
$342,657 \cdot 741,640,062,627,530,801,524,787,141,901,937,474,059,940,781,097,$
$519,023,905,821,316,144,415,759,504,705,008,092,818,711,693,940,737$
$F_{10} = 45,592,577 \cdot 6,487,031,809 \cdot 4,659,775,785,220,018,543,264,560,743,076,$
$778,192,897 \cdot 130,439,874,405,488,189,727,484,768,796,509,903,946,608,530,$
$841,611,892,186,895,295,776,832,416,251,471,863,574,140,227,977,573,104,$
$895,898,783,928,842,923,844,831,149,032,913,798,729,088,601,617,946,094,$
$119,449,010,595,906,710,130,531,906,171,018,354,491,609,619,193,912,488,$
$538,116,080,712,299,672,322,806,217,820,753,127,014,424,577$
$F_{11} = 319,489 \cdot 974,849 \cdot 167,988,556,341,760,475,137 \cdot 3,560,841,906,445,833,$
$920,513 \cdot 173,462,447,179,147,555,430,258,970,864,309,778,377,421,844,723,$
$664,084,649,347,019,061,363,579,192,879,108,857,591,038,330,408,837,177,$
$983,810,868,451,546,421,940,712,978,306,134,189,864,280,826,014,542,758,$
$708,589,243,873,685,563,973,118,948,869,399,158,545,506,611,147,420,216,$
$132,557,017,260,564,139,394,366,945,793,220,968,665,108,959,685,482,705,$

$388,072,645,828,554,151,936,401,912,464,931,182,546,092,879,815,733,057,$
$795,573,358,504,982,279,280,090,942,872,567,591,518,912,118,622,751,714,$
$319,229,788,100,979,251,036,035,496,917,279,912,663,527,358,783,236,647,$
$193,154,777,091,427,745,377,038,294,584,918,917,590,325,110,939,381,322,$
$486,044,298,573,971,650,711,059,244,462,177,542,540,706,913,047,034,664,$
$643,603,491,382,441,723,306,598,834,177$
$F_{12} = 114,689 \cdot 26,017,793 \cdot 63,766,529 \cdot 190,274,191,361 \cdot 1,256,132,134,125,$
$569 \cdot C$
$F_{13} = 2,710,954,639,361 \cdot 2,663,848,877,152,141,313 \cdot 3,603,109,844,542,291,$
$969 \cdot 319,546,020,820,551,643,220,672,513 \cdot C$
$F_{14} = C$
$F_{15} = 1,214,251,009 \cdot 2,327,042,503,868,417 \cdot 168,768,817,029,516,972,383,$
$024,127,016,961 \cdot C$
$F_{16} = 825,753,601 \cdot 188,981,757,975,021,318,420,037,633 \cdot C$
$F_{17} = 31,065,037,602,817 \cdot C$
$F_{18} = 13,631,489 \cdot 81,274,690,703,860,512,587,777 \cdot C$
$F_{19} = 70,525,124,609 \cdot 646,730,219,521 \cdot C$
$F_{20} = C$
$F_{21} = 4,485,296,422,913 \cdot C$
$F_{22} = C$
$F_{23} = 167,772,161 \cdot C$
$F_{24} = C$

Donde C es un compuesto y todos los factores escritos explícitamente son primos. Así los únicos números de Fermat factorizados completamente van de F_1 hasta F_{11} y no se conocen factores para F_{20} y F_{24}. El número de Fermat compuesto más grande que se conoce es $F_{2747497}$ y su factor primo $57 \times 2^{2747499} + 1$ fue descubierto por Marshall Bishop in Prime Grid's Proth Prime Search el 13 de mayo de 2013; el número de Fermat más pequeño de carácter desconocido es F_{33}.

Para determinar la primalidad de los números de Fermat fue usado el Test de Pepin, el cual describe en el Capítulo 4.

Definición 3.4 (Primos gemelos)**.** Son aquellos que distan dos unidades.

Ejemplos de primos gemelos son las parejas (29, 31); (17, 19) y (341, 343). No se conoce si existen finitas o infinitas de estas parejas.

El siguiente resultado ha sido de gran ayuda en la búsqueda de nuevos pares de primos gemelos, su demostración puede encontrarse en [9].

Teorema 3.7 (Clement, 1949)**.** *Los enteros $n, n+2$, son primos gemelos si y sólo si*

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

Algunos de los primos gemelos recientemente encontrados se presentan en la Tabla 3.2

Primos	**Dígitos**	**Descubrimiento**
$318032361 \cdot 2^{107001} \pm 1$	32220	Dic-2011
$1765199373 \cdot 2^{107520} \pm 1$	32376	Ago.2009
$108615 \cdot 2^{110342} \pm 1$	33222	Ene-2997
$5558745 \cdot 10^{33334} \pm 1$	33341	Jun-2007
$60194061 \cdot 2^{114689} \pm 1$	34533	Jun-2006
$307259241 \cdot 2^{115599} \pm 1$	34808	Sep-2005
$598899 \cdot 2^{118987} \pm 1$	35825	Sep-2002
$8151728061 \cdot 2^{125987} \pm 1$	37936	Nov-2010
$23272426305 \cdot 2^{140001} \pm 1$	42155	Feb-2012
$12378188145 \cdot 2^{140002} \pm 1$	42155	Abr-2012
$84966861 \cdot 2^{140219} \pm 1$	42219	Dic-2010
$1679081223 \cdot 2^{151618} \pm 1$	45651	Dic-2010
$22835841624 \cdot 7^{54321} \pm 1$	45917	May-2010
$33218925 \cdot 2^{169690} \pm 1$	51090	Abr-2010
$16869987339975 \cdot 2^{171960} \pm 1$	51779	Ene-2009
$100314512544015 \cdot 2^{171960} \pm 1$	51780	Nov-2002
$194772106074315 \cdot 2^{171960} \pm 1$	51780	Abr-2011
$2003663613 \cdot 2^{195000} \pm 1$	58711	Jun-2008
$65516468355 \cdot 2^{333333} \pm 1$	100355	Oct-2002
$3756801695685 \cdot 2^{666669} \pm 1$	200700	May-2001

Tabla 3.2: Primos gemelos conocidos

Capítulo 4

Reconociendo Primos

Como se ha podido observar los números primos son fundamentales en la Teoría de Números y en las matemáticas en general, razón por la cual surge la necesidad de crear o encontrar métodos eficientes que permitan determinar rápidamente si un entero positivo es o no un número primo. Desafortunada o afortunadamente no se han encontrado métodos generales que permitan decidir si un entero positivo es o no primo.

La criba de Eratóstenes llamada así en honor al matemático griego Eratóstenes (276 - 194 a.C.) es un método eficiente para encontrar todos los primos menores o iguales a un entero n dado. Este procedimiento se fundamenta en la siguiente propiedad de los números compuestos. Si un entero $n > 1$ es compuesto, entonces se puede escribir como $n = bc$, donde $1 < b < n$ y $1 < c < n$. Supóngase que $b \leq c$, entonces $b^2 \leq bc = n$ y así $b \leq \sqrt{n}$. Como $b > 1$, entonces b tiene al menos un factor primo p. De esta forma

$$p \leq b \leq \sqrt{n}$$

Adicionalmente como $p|b$ y $b|n$, entonces $p|n$. En consecuencia un número compuesto n siempre tiene un divisor primo p, tal que $p \leq \sqrt{n}$. Usando esta observación se puede llevar a cabo la criba de Eratóstenes, como sigue. Se escriben todos los números entre 2 y n, primero se marcan todos los números pares mayores que 2, al terminar, el primer número no tachado distinto de 2 es 3 que es un número primo; luego tachamos todos los múltiplos de 3 mayores que 3; al terminar, el menor número no tachado mayor que 3 es 5 que es un número primo; tachamos seguidamente todos los múltiplos de 5 mayores que 5 y continuamos el proceso hasta tachar todos los múltiplos de p mayores que p para todo primo $p \leq \sqrt{n}$. Luego los enteros no tachados al finalizar este procedimiento son precisamente los números primos menores o iguales a n. En la Tabla 4.1 se muestra la criba Eratóstenes para $n = 100$.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Tabla 4.1: Números primos entre 2 y 100.

Nótese entonces que los números primos menores o iguales que 100 son: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. Una observación detenida de la criba permite ver que la distribución de los primos decrece de manera constante, lo que podría inducir a pensar que el número de primos es finito. Sin embargo ya se demostró en el Capítulo 2 que el número de primos es infinito.

4.1. Pseudoprimos

Sea S una declaración aritmética fácilmente comprobable y supóngase que se tiene un teorema del tipo, si n es primo entonces n satisface S. Así si se tiene un entero grande n y se desea decidir si es primo o compuesto, se prueba si n realmente satisface S, si n no cumple S ya se ha demostrado que n es compuesto, si n cumple S puede ocurrir que n sea primo ó que n sea compuesto. Así un pseudoprimo es un entero compuesto que verifica la propiedad S.
Por ejemplo, si S es la afirmación n es 2 o un número impar, se tiene una declaración fácilmente comprobable para cualquier entero n. El concepto de pseudoprimo es de gran utilidad para restringir los conjuntos donde se pueda encontrar números primos. Sin embargo este test no es una fuerte evidencia de primalidad ya que existen muchos más pseudoprimos alrededor de este test que primos verdaderos.
El teorema de Fermat es un medio fundamental para distinguir entre primos y compuestos, como consecuencia de esto se tiene la siguiente definición.

Definición 4.1 (Pseudoprimos de Fermat)**.** Un número compuesto n es un pseudoprimo de Fermat base a si

$$a^n \equiv a \pmod{n}, a \in Z. \tag{4.1.1}$$

Cuando $\gcd(a, n) = 1$, se puede multiplicar a ambos lados por el inverso multiplicativo de a módulo n para obtener

$$a^{n-1} \equiv 1 \pmod{n}. \tag{4.1.2}$$

Por ejemplo, $n = 91$ es un pseudoprimo de Fermat base 3 ya que $n = 91$ es compuesto y $3^{91} \equiv 3$ (mód 91). De manera similar 341 es un pseudoprimo de Fermat base 2. La base 1 no es interesante ya que todo número compuesto es un pseudoprimo base 1, supóngase entonces de aquí en adelante que $a \geq 2$. El siguiente resultado, cuya demostración se puede encontrar en [3] muestra que los pseudprimos de Fermat son escasos comparados con los primos.

Teorema 4.1. *Para cada entero fijo $a \geq 2$, el número de pseudoprimos de Fermat base a que son menores o iguales a x es $o(\pi(x))$ cuando $x \to \infty$, es decir, los pseudoprimos de Fermat son escasos comparados con los primos.*

Los números impares n satisfacen la congruencia $a^{n-1} \equiv 1 \pmod{n}$ para $a = n - 1$, así la congruencia no dice mucho de n en este caso. Si $a^{n-1} \equiv 1 \pmod{n}$ se cumple para un par (a, n), donde $1 < a < n - 1$, entonces n es un probable primo base a. Así si n es un primo, entonces n es un probable primo base a para cada entero a, con $1 < a < n - 1$. El resultado anterior afirma que para una selección fija a, la mayoría de probables primos base a en realidad son primos. De esta forma se tiene un test simple para distinguir entre miembros de un conjunto que contiene un conjunto escaso de números compuestos y todos los primos que exceden a $a + 1$ y los números compuestos restantes que exceden a $a + 1$.

En el siguiente algoritmo se usará el Teorema de Fermat para determinar si un número es compuesto o es un probable primo.

4.1.1. Algoritmo (Test probable primo)

Dados dos enteros a, n con $n > 3$ y $2 \leq a \leq n - 2$, el algoritmo retorna o bien " n es probable primo base a" o " n es compuesto".

```
probprimo:=function(n,a)
          local b;
          b:=a^n mod n;
          if b<>a then
          return [n,"es compuesto"];
          fi;
          return [n,"es probable primo base", a];
end;
```

Teorema 4.2. *Para cada entero $a \geq 2$ existen infinitos pseudoprimos de Fermat base a.*

Demostración. Se prueba que si p es cualquier primo impar que no divide a $a^2 - 1$, entonces $n = (a^{2p} - 1)/(a^2 - 1)$ es un pseudoprimo base a. Por ejemplo si $a = 2$ y $p = 5$, entonces se tiene $n = 341$.

Primero nótese que

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

así que n es compuesto. Como $a^p \equiv a \pmod{p}$, al elevar al cuadrado ambos lados se obtiene que $a^{2p} \equiv a^2 \pmod{p}$. Luego p divide a $a^{2p} - a^2$. Pero p no divide a $a^2 - 1$ por hipótesis, además

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

de donde

$$(n - 1)(a^2 - 1) = a^{2p} - a^2.$$

Luego p divide a $n - 1$. Se puede concluir algo más de $n - 1$, usando la identidad

$$n - 1 \equiv a^{2p-2} + a^{2p-4} + \cdots + a^2,$$

obsérvese que $n - 1$ es la suma de un número par de términos de la misma paridad, de esta forma $n - 1$ debe ser par. Hasta ahora se tiene que 2 y p son divisores de $n - 1$, así que $2p$ debe igualmente ser un divisor. Entonces $a^{2p} - 1$ es un divisor de $a^{n-1} - 1$. Pero $a^{2p} - 1$ es un múltiplo de n, luego $a^{n-1} \equiv 1 \pmod{n}$. ■

Una categoría de números relacionados estrechamente con los pseudoprimos de Fermat es la siguiente.

4.2. Números de Carmichael

En la búsqueda de un método simple y rápido para distinguir números primos de números compuestos, se puede considerar la combinación de pseudoprimos de Fermat para varias bases a. Por ejemplo, aunque 341 es un pseudoprimo base 2 este no es un pseudoprimo base 3 y al contrario 91 es un pseudoprimo base 3 pero no base 2. Parece que no hay pseudoprimos que sean simultáneamente base 2 y 3, o si tales compuestos existen parece que no existe algún conjunto finito de bases tal que existan pseudoprimos en todas las bases en el conjunto. Si esto fuese cierto sería muy útil ya que probar primalidad se reduciría a una sencilla cuestion de cálculo.
Sin embargo, el número $561 = 3 \cdot 11 \cdot 17$ no es solo un pseudoprimo de Fermat en ambas bases 2 y 3, también es un pseudoprimo para toda base a. Los pseudoprimos pueden ser fácilmente reconocidos por su factorización prima.

Definición 4.2. Un entero compuesto n, con $a^n \equiv a \pmod{n}$ para todo entero a se denomina *número de Carmichael.*

Teorema 4.3 (Criterio de Korselt)**.** *Un entero n es un número de Carmichael si y sólo si n es positivo, compuesto, libre de cuadrados y para cada primo p que divide a n se tiene que $p - 1$ divide a $n - 1$.*

Demostración. Supóngase que n es un número de Carmichael, entonces n es compuesto. Sea p un factor primo de n. Por el Teorema de Fermat

$$a^n \equiv a \pmod{n}$$

particularmente

$$p^n \equiv p \pmod{n}.$$

Nótese que p^2 no divide a n, ya que si $p^2|n$, entonces

$$p^2|p^n - p$$

$$p^2|p(p^{n-1} - 1)$$

$$p^2|p^{n-1} - 1$$

pero $p^2|p^{n-1}$ porque $n > 3$, luego p^2 divide a cualquier combinación lineal de $p^{n-1} - 1$ y p^{n-1}, en particular,

$$p^2|p^{n-1} - (p^{n-1} - 1)$$

de donde $p|1$ lo cual es imposible; así n es libre de cuadrados. Sea a una raíz primitiva módulo p. Como $a^n \equiv a \pmod{n}$, se tiene $a^n \equiv a \pmod{p}$, de donde $a^{n-1} \equiv 1 \pmod{p}$. Pero $a \pmod{p}$ tiene orden $p - 1$, así $p - 1$ divide a $n - 1$.

Ahora, supóngase que n es compuesto, libre de cuadrados y que para cada primo p que divide a n, se tiene que $p - 1$ divide a $n - 1$. Se debe mostrar $a^n \equiv a \pmod{n}$ para todo entero a. Como n es libre de cuadrados, es suficiente mostrar que $a^n \equiv a \pmod{p}$ para cada entero a y cada primo p que divide a n.

Supóngase que $p|n$ y a es un entero. Si $p|a$

$$a \equiv 0 \pmod{p}$$

además

$$a^p \equiv a \pmod{p}$$

de donde

$$a^p \equiv 0 \pmod{p}$$

como $p|n$, $n = pk$, para algún k en los enteros

$$(a^p)^k \equiv (0)^k \pmod{p}$$

$$a^n \equiv 0 \pmod{p}$$

por todo esto

$$a^n \equiv a \pmod{p}$$

Ahora si $p \nmid a$ se tiene

$$a^{p-1} \equiv 1 \pmod{p}$$

pero $p-1|n-1$; así, $a^{n-1} \equiv 1 \pmod{p}$. Luego

$$a^n \equiv a \pmod{p}.$$

Por lo tanto la congruencia claramente se cumple para todo a. ■

Alrededor de los números de Carmichael surge la siguiente pregunta. ¿Existen infinitos números de Carmichael? De nuevo, infortunadamente para los test de primalidad la respuesta es afirmativa. P. Erdös en 1956 presentó un argumento heurístico para mostrar que no solamente existen infinitos números de Carmichael, sino que estos no son tan raros como se podría pensar; pero fueron W.R. Alford, Andrew Granville y Carl Pomerance quienes en 1994 probaron por primera vez que existen infinitos números de Carmichael. El resultado se presenta a continuación, la prueba puede encontrarse en [1]..

Teorema 4.4 (Alford, Granville, Pomerance)**.** *Existen infinitos números de Carmichael. En particular, para x suficientemente grande, el número $C(x)$ de numeros de Carmichael que no exceden a x satisface $C(x) > x^{2/7}$.*

El concepto de pseudoprimos de Fermat es muy bueno, ya que es fácil de comprobar y por cada base $a > 1$ existen pocos pseudoprimos comparados con los primos. Sin embargo, existen compuestos como los números de Carmichael, para los que la congruencia $a^n \equiv a \pmod{n}$ es inútil como medio para reconocer compuestos.
Lo ideal sería un test simple para el cual los pseudoprimos sean reconocidos como compuestos.

Teorema 4.5. *Sea n un primo impar y $n-1 = 2^s t$, donde t es impar. Si $n \nmid a$ entonces*

$$\begin{cases} a^t \equiv 1 \pmod{n}, & \text{ó} \\ a^{2^i t} \equiv -1 \pmod{n}, & \text{para algún } 0 \leq i \leq s-1 \end{cases} \tag{4.2.1}$$

Definición 4.3. Un probable primo fuerte base a es un entero $n > 3$ impar que satisface 4.2.1 con $1 < a < n-1$.

Lema 4.1. *Sea n un probable primo fuerte base a, entonces n es un probable primo base a.*

Demostración. Supóngase que n es un probable primo fuerte base a, así $n-1 = 2^s t$, donde t es impar entonces $a^t \equiv 1 \pmod{n}$ ó $a^{2^i t} \equiv -1 \pmod{n}$, para algún $0 \leq i \leq s-1$, donde $n \nmid a$ y $1 < a < n-1$.
Si $a^t \equiv 1 \pmod{n}$, entonces

$$(a^t)^{2^s} \equiv (1)^{2^s} \pmod{n}$$

$$a^{2^s t} \equiv 1 \pmod{n}$$

$$a^{n-1} \equiv 1 \pmod{n}.$$

Ahora si $a^{2^i t} \equiv -1 \pmod{n}$, entonces

$$(a^{2^i t})^{2^{s-i}} \equiv (-1)^{2^{s-i}} \pmod{n}$$

$$a^{2^s t} \equiv 1 \pmod{n}$$

$$a^{n-1} \equiv 1 \pmod{n},$$

por lo tanto n es un probable primo base a. ■

Luego, como todo primo mayor que $a+1$ es un probable primo fuerte base a, la única diferencia entre los dos conceptos es que posiblemente menos compuestos pasen el test probable primo fuerte.

4.2.1. Algoritmo (Test probable primo fuerte)

Dado un número impar $n > 3$ y un entero a con $1 < a < n-1$. Este algoritmo retorna o bien "n es un probable primo fuerte base a" o "n es compuesto".

```
Exponente:= function(n)
            local s,x,t,R;
            s:=0;
            x:=n-1;
            while x mod 2=0 do
            s:=s+1;
            x:=x/2;
            od;
            t:=(n-1)/(2^s);
            R:=[s,t];
            return (R);
end;

Probprimofuerte:=function(n,a)
                local F,i,m,D,t,s;
                D:=Exponente(n);
                s:=D[1];
                t:=D[2];
                F:=Gcd(a,n);
```

```
                if F=1 then
                if a^t mod n =1 then
                return [n,"es probable primo fuerte base", a];
                fi;
                for i in [0 .. (s-1)] do
                m:=a^((2^i)*t) mod n;
                if m=n-1 then
                return [n,"es probable primo fuerte base", a];
                fi;
                od;
                else return [a, "y", n,"no son primos relativos"];
                fi;
                return [n,"es compuesto"];
end;
```

Nótese que para $n = 91$ y $a = 10$ se tiene $90 = 2^1 \cdot 45$ y $10^{45} \equiv -1 \pmod{91}$. Así 4.2.1 se cumple, es decir, 91 es un probable primo fuerte base 10.
Ahora considérese la posibilidad de mostrar que un número impar n es compuesto mediante el no cumplimiento de la ecuación 4.2.1 para un número particular a. Por ejemplo, 341 es un pseudoprimo para la base 2. En efecto la ecuación 4.2.1 no se cumple para $n = 341$ y $a = 2$. De hecho, se tiene $340 = 2^2 \cdot 85$, $2^{85} \equiv 32 \pmod{341}$ y $2^{170} \equiv 1 \pmod{341}$.
J. Selfridge propuso utilizar el Teorema 4.5 como un test para pseudoprimos a principios de 1970 y fué él quien acuñó el termino de "pseudoprimo fuerte".

Definición 4.4. Un entero n es un pseudoprimo fuerte base a si n es un compuesto impar, $n-1 = 2^s t$, con t impar y 4.2.1 se cumple.

Así, 341 no es un pseudoprimo fuerte para la base 2, mientras 91 es un pseudoprimo fuerte para la base 10.
Si n es un pseudoprimo fuerte para la base a, entonces n es un pseudoprimo para la base a. El ejemplo $n = 341$ y $a = 2$ muestra que el recíproco es falso.
Ya se han discutido métodos para reconocer rápidamente números compuestos. Si un número dado no es declarado compuesto por dicho test, este es primo o no se ha logrado probar que el número es compuesto. A pesar de estar casi seguros de que el número es primo, no tenemos una prueba, más bien es una conjetura sostenida por los experimentos numéricos. Sin embargo ahora se tratará el tema de como se podría realmente probar que dicho número es primo.

A continuación se presentan algunos tests con el objeto de Probar primalidad.

4.3. El test $n-1$

Puede probarse primalidad para números pequeños usando la criba de Eratóstenes, pero para números grandes existen mejores métodos, uno de estos esta basado en el Pequeño Teorema de Fermat como la más simple de todas la pruebas de primalidad, conocido como el test $n-1$, el método sugiere no factorizar n, pero si $n-1$.

En el siguiente teorema se presenta la idea considerada por Lucas en 1876.

Teorema 4.6 (Teorema de Lucas)**.** *Si a, n son enteros con $n > 1$ y*

$$a^{n-1} \equiv 1 \pmod{n}, \text{ pero } a^{(n-1)/q} \not\equiv 1 \pmod{n} \text{ para todo primo } q|n-1, \tag{4.3.1}$$

entonces n es primo.

Demostración. La primera condición implica que el orden de a en $\mathbb{Z}_n^*$ es un divisor de $n-1$, mientras la segunda condición implica que el orden de a no es un divisor propio de $n-1$, es decir, este es igual a $n-1$. Pero el orden de a es también un divisor de $\varphi(n)$ por el Teorema de Euler, así

$$n - 1 \leq \varphi(n).$$

Supóngase que n es compuesto y tiene un factor primo p, entonces p y n son enteros en $\{1, 2, ..., n\}$ que no son primos relativos con n, luego por la definición de la función de Euler, se tiene

$$\varphi(n) \leq n - 2.$$

Esto es una contradicción, por lo tanto n debe ser primo. ■

La primera condición del teorema de Lucas no es vacía para números primos; tal número a es llamado una raíz primitiva módulo n y todos los primos la tienen, es decir si n es primo, el grupo multiplicativo $\mathbb{Z}_n^*$ es cíclico. Ver Capítulo 1.
Aunque no se conoce un algoritmo determinístico en tiempo polinomial para encontrar una raíz primitiva para un número primo, el obstáculo principal llevando a cabo el teorema de Lucas como un test de primalidad no es la búsqueda de una raíz primitiva a, sino encontrar la factorización prima completa de $n-1$. Como ya sabemos la factorización en la práctica es difícil para muchos números. Pero no es difícil para todo número. Por ejemplo, considere la búsqueda para primos que son 1 más que una potencia de 2. Como se observó en el Teorema 3.5 tal primo debe ser de la forma $F_k = 2^{2^k} + 1$, esta sucesión de números corresponde a los números de Fermat ya mencionados.
Pepin en 1877 dió un criterio similar al siguiente para la primalidad de un número de Fermat.

Teorema 4.7 (Test de Pepin)**.** *Para $k \geq 1$, el numero $F_k = 2^{2^k} + 1$ es primo si y sólo si $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$.*

Demostración. Supóngase que F_k es primo. Como 2^k es par, se sigue que $2^{2^k} \equiv 1 \pmod 3$, así $F_k \equiv 2 \pmod 3$, es decir, $F_k \equiv -1 \pmod 3$. Pero también $F_k \equiv 1 \pmod 4$ luego el símbolo de Legendre $(\frac{3}{F_k}) = -1$, en consecuencia 3 no es un residuo cuadrático $\pmod{F_k}$. Ahora por el criterio de Euler se tiene

$$\left(\frac{3}{F_k}\right) \equiv 3^{(F_k-1)/2} \pmod{F_k},$$

luego

$$3^{(F_k-1)/2} \equiv -1 \pmod{F_k}.$$

Ahora supóngase que

$$3^{(F_k-1)/2} \equiv -1 \pmod{F_k},$$

entonces para la base 3

$$3^{F_k-1} \equiv 1 \pmod{F_k}, \text{ pero } 3^{F_K-1/q} \not\equiv 1 \pmod{F_k} \text{ para todo primo } q|F_k - 1,$$

así por el Teorema de Lucas F_k es primo. ■

El F_k más grande para el cual el test de Pepin se ha usado es F_{24}. Como se discutió anteriormente este número es compuesto, de hecho todos los números de Fermat mayores que F_4 para los cuales se ha podido determinar su primalidad son compuestos.

4.4. Factorización parcial

El paso más difícil en general, en la implementación del Teorema de Lucas como un test de primalidad es la factorización prima completa de $n-1$, podría preguntarse si puede hacerse cualquier uso de una factorización parcial de $n-1$. En particular, sea

$$n - 1 = FR, \text{ donde la factorización prima completa de } F \text{ es conocida} \tag{4.4.1}$$

Si F es bastante grande como una función de n, se puede formar una prueba de primalidad de n con ayuda del Teorema de Lucas, si en efecto n es primo. El siguiente resultado permite deducir alguna información sobre la factorización prima de n.

Teorema 4.8 (Pocklington)**.** *Supóngase que $n-1 = FR$, donde la factorización prima completa de F es conocida y a es tal que*

$$a^{n-1} \equiv 1 \pmod n \text{ y } gcd(a^{(n-1)/q} - 1, n) = 1 \text{ para todo primo } q|F. \tag{4.4.2}$$

Entonces todo factor primo de n es congruente con $1 \pmod F$.

Demostración. Sea p un factor primo de n. De $a^{n-1} \equiv 1 \pmod{n}$ se tiene que el orden de a^R en $\mathbb{Z}_p^*$ es un divisor de $(n-1)/R = F$. De $\gcd(a^{(n-1)/q} - 1, n) = 1$, $|a^R|_p$ no es un divisor propio de F, luego $|a^R|_p$ es igual a F. Por lo tanto F divide al orden de $\mathbb{Z}_p^*$, que es $p-1$, de donde

$$p \equiv 1 \pmod{F}.$$

■

Corolario 4.1. *Supóngase que $n-1 = FR$, donde la factorización prima completa de F es conocida y a es tal que $a^{n-1} \equiv 1 \pmod{n}$ y $\gcd(a^{(n-1)/q} - 1, n) = 1$ para todo primo $q|F$ y $F \geq \sqrt{n}$, entonces n es primo.*

Demostración. El teorema anterior implica que cada factor primo de n es congruente con $1 \pmod{F}$, así cada factor primo de n excede a F. Pero $F \geq \sqrt{n}$, luego cada factor primo de n excede a $\sqrt{n}$, lo que es absurdo. Por lo tanto n debe ser primo. ■

El siguiente resultado permite considerar un valor de F más pequeño.

Teorema 4.9 (Brillhart, Lehmer, y Selfridge.)**.** *Supóngase que $n-1 = FR$, donde la factorización prima completa de F es conocida y a es tal que $a^{n-1} \equiv 1 \pmod{n}$ y $\gcd(a^{(n-1)/q} - 1, n) = 1$ para todo primo $q|F$ y que $n^{1/3} \leq F < n^{1/2}$. Considere la representación de n en base F, es decir $n = c_2F^2 + c_1F + 1$, donde c_1, c_2 son enteros en $[0, ..., F-1]$. Entonces n es primo si y solo si $c_1^2 - 4c_2$ no es un cuadrado.*

Demostración. Como $n \equiv 1 \pmod{F}$ se sigue que el dígito unidad en base F de n es 1. Así n tiene su representación en base F en la forma $c_2F^2 + c_1F + 1$ como se declaro. Supóngase que n es compuesto. Del teorema anterior todos los factores primos de n son congruentes con $1 \pmod{F}$, así deben exceder a $n^{1/3}$. Por lo tanto n tiene exactamente dos factores primos.

$$n = pq,\ p = aF + 1,\ q = bF + 1,\ a \leq b.$$

Luego

$$c_2F^2 + c_1F + 1 = n = (aF+1)(bF+1) = abF^2 + (a+b)F + 1.$$

El objetivo es mostrar que se debe tener $c_2 = ab$ y $c_1 = a + b$, para obtener que $c_1^2 - 4c_2$ es un cuadrado. Primero obsérvese que $F^3 \geq n > abF^2$, luego $ab \leq F - 1$. Se sigue que $a + b \leq F - 1$ o $a = 1$, $b = F - 1$. En el último caso, $n = (F+1)((F-1)F + 1) = F^3 + 1$, contradiciendo que $F \geq n^{1/3}$. Por lo tanto ambos ab y $a + b$ son enteros positivos menores que F. De la unicidad de la representación de un número en base F se tiene $c_2 = ab$ y $c_1 = a + b$ como se declaro, así $c_1^2 - 4c_2$ es un cuadrado.

Ahora para el recíproco, supóngase que $c_1^2 - 4c_2$ es un cuadrado, es decir $c_1^2 - 4c_2 = u^2$. Entonces

$$\begin{aligned} n &= c_2F^2 + c_1F + 1 \\ &= \frac{4c_2}{4}F^2 + \frac{2c_1F}{2} + 1 \\ &= \frac{c_1^2 - u^2}{4}F^2 + \frac{c_1F + uF + c_1F - uF}{2} + 1 \\ &= \frac{(c_1+u)(c_1-u)}{4}F^2 + \frac{c_1+u}{2}F + \frac{c_1-u}{2}F + 1 \\ &= \left(\frac{c_1+u}{2}F\right)\left(\frac{c_1-u}{2}F + 1\right) + \frac{c_1-u}{2}F + 1 \\ &= \left(\frac{c_1+u}{2}F + 1\right)\left(\frac{c_1-u}{2}F + 1\right) \end{aligned}$$

como $c_1 \equiv u \pmod 2$ las dos fracciones son enteras. Además esta factorización es no trivial y como $c_2 > 0$ se sigue que $|u| < c_1$, En consecuencia n es compuesto. ■

Nótese que para obtener una aplicación eficiente del teorema anterior como un test de primalidad se hace importante encontrar un método rápido que sirva para verificar si el entero $c_1^2 - 4c_2$ es un cuadrado.

4.5. El test $n + 1$

La dificultad principal de aplicar el test $n - 1$ para probar que n es primo está en encontrar un divisor de $n - 1$ suficientemente grande completamente factorizado. Para algunos valores de n esto no es problema, tal como con los números de Fermat para los cuales se tiene el test de Pepin, ver seccion 4.3. Para otras clases de números tales como los números de Mersenne, la factorización prima de 1 más que el número, se presenta el siguiente método.

4.5.1. EL test de Lucas-Lehmer

Sea $f(x) = x^2 - ax + b$, con $a, b \in \mathbb{Z}$ y $\Delta = a^2 - 4b$ no un cuadrado. Considérese las sucesiones de Lucas así,

$$U_k = \frac{x^k - (a-x)^k}{x - (a-x)} \pmod{f(x)},\ V_k = x^k + (a-x)^k \pmod{f(x)}. \tag{4.5.1}$$

Las sucesiones U_j, V_j satisfacen la siguiente recurrencia para el polinomio $x^2 - ax + b$ con $j \geq 2$

$$U_j = aU_{j-1} - bU_{j-2},\ V_j = aV_{j-1} - bV_{j-2}.$$

En efecto, como

$$\begin{aligned} x^2 &\equiv ax - b \pmod{f(x)} \\ x^2(x^{j-2}) &\equiv ax(x^{j-2}) - b(x^{j-2}) \pmod{f(x)} \\ x^j &\equiv ax^{j-1} - bx^{j-2} \pmod{f(x)} \end{aligned}$$

además

$$\begin{aligned} x^2 - ax &\equiv -b \pmod{f(x)} \\ a^2 - 2ax + x^2 &\equiv a^2 - ax - b \pmod{f(x)} \\ (a-x)^2 &\equiv a(a-x) - b \pmod{f(x)} \\ (a-x)^2(a-x)^{j-2} &\equiv a(a-x)(a-x)^{j-2} - b(a-x)^{j-2} \pmod{f(x)} \\ (a-x)^j &\equiv a(a-x)^{j-1} - b(a-x)^{j-2} \pmod{f(x)}. \end{aligned}$$

Luego

$$\begin{aligned} x^j - (a-x)^j &\equiv ax^{j-1} - bx^{j-2} - (a(a-x)^{j-1} - b(a-x)^{j-2}) \pmod{f(x)} \\ x^j - (a-x)^j &\equiv a(x^{j-1} - (a-x)^{j-1}) - b(x^{j-2} - (a-x)^{j-2}) \pmod{f(x)} \\ \frac{x^j - (a-x)^j}{x - (a-x)} &\equiv \frac{a(x^{j-1} - (a-x)^{j-1})}{x - (a-x)} - \frac{b(x^{j-2} - (a-x)^{j-2}}{x - (a-x)} \pmod{f(x)} \\ U_j &\equiv aU_{j-1} - bU_{j-2} \pmod{f(x)}. \end{aligned}$$

Por otro lado

$$\begin{aligned} x^j + (a-x)^j &\equiv ax^{j-1} - bx^{j-2} + (a(a-x)^{j-1} - b(a-x)^{j-2}) \pmod{f(x)} \\ x^j + (a-x)^j &\equiv a(x^{j-1} + (a-x)^{j-1}) - b(x^{j-2} + (a-x)^{j-2}) \pmod{f(x)} \\ V_j &\equiv aV_{j-1} - bV_{j-2} \pmod{f(x)}. \end{aligned}$$

Dados los valores iniciales

$$U_0 = 0, U_1 = 1,\ V_0 = 2, V_1 = a$$

se puede observar que los polinomios U_k, V_k no tienen grado positivo; es decir, estos son enteros.

Teorema 4.10. *Sean a, b, Δ tal que $f(x) = x^2 - ax + b$, $\Delta = a^2 - 4b$ no un cuadrado y sean*

$$U_j = \frac{x^j - (a-x)^j}{x - (a-x)} \pmod{f(x)},\ V_j = x^j + (a-x)^j \pmod{f(x)}.$$

Si p es primo con $\gcd(p, 2b\Delta) = 1$, *entonces*

$$U_{p-\left(\frac{\Delta}{p}\right)} \equiv 0 \pmod{p}. \tag{4.5.2}$$

Definición 4.5. Un número compuesto n con $\gcd(n, 2b\Delta) = 1$ es un pseudoprimo de Lucas con respecto a $x^2 - ax + b$ si $U_{n-\left(\frac{\Delta}{n}\right)} \equiv 0 \pmod{n}$.

Ahora se presentaran algunas herramientas necesarias para la demostración del Teorema 4.11

Como la sucesión (U_j) es construida por reducción de polinomios módulo $x^2 - ax + b$, y como el Teorema 4.11 y la Definición 4.5 se refieren a la sucesión reducida módulo n, realmente se está tratando con polinomios en el anillo $R = \mathbf{Z}_n[x]/ < x^2 - ax + b >$. A continuación se presenta un listado de clases laterales

$$\{i + jx : i, j \text{ son enteros con } 0 \leq i, j \leq n - 1\}.$$

Las clases laterales se suman como vectores módulo n y se multiplican via $x^2 = ax - b$. Así, se tiene

$$\begin{aligned}(i_1 + j_1 x) + (i_2 + j_2 x) &= i_3 + j_3 x \\ (i_1 + j_1 x)(i_2 + j_2 x) &= i_4 + j_4 x\end{aligned}$$

donde

$$\begin{aligned} i_3 = i_1 + i_2 \pmod{n},\ j_3 = j_1 + j_2 \pmod{n} \\ i_4 = i_1 i_2 - b j_1 j_2 \pmod{n},\ j_4 = i_1 j_2 + i_2 j_1 + a j_1 j_2 \pmod{n}.\end{aligned}$$

Ahora probemos el Teorema 4.11

Demostración. Supóngase que p es un primo impar con $\left(\frac{\Delta}{p}\right) = -1$. Entonces Δ no es un residuo cuadrático en $\mathbf{Z}_p$, así que el polinomio $x^2 - ax + b$, que tiene discriminante Δ, es irreducible en $\mathbf{Z}_p$. Así, $R = \mathbf{Z}_p[x]/ < x^2 - ax + b >$ es un campo isomórfo al campo finito $\mathbf{F}_{p^2}$ con p^2 elementos, ver Capitulo 1. El subcampo $\mathbf{Z}_p (= \mathbf{F}_p)$ es reconocido como aquellas clases laterales $i + jx$ con $j = 0$.

En $\mathbf{F}_{p^2}$ la función σ que toma un elemento a su p-ésima potencia tiene las siguientes propiedades que son derivadas del Teorema Binomial 1.13 y del Pequeño Teorema de Fermat 2.5,

- $\sigma(u + v) = \sigma(u) + \sigma(v)$
- $\sigma(uv) = \sigma(u)\sigma(v)$
- $\sigma(u) = u$ si y solo si u esta en el subcampo $\mathbf{Z}_p$.

Se ha creado el campo $\mathbf{F}_{p^2}$ para proporcionar raíces para $x^2 - ax + b$, que no se encontraban en $\mathbf{Z}_p$. Las clases laterales $i + jx$ que son raíces son x, y $a - x = a + (p-1)x$. Como x y $a - x$ no están en $\mathbf{Z}_p$ y σ debe permutar las raíces de $f(x) = x^2 - ax + b$, se tiene

$$\text{en el caso } \left(\frac{\Delta}{p}\right) = -1 : \begin{cases} x^p \equiv a - x \pmod{(f(x), p)} \\ (a-x)^p \equiv x \pmod{(f(x), p)} \end{cases} \tag{4.5.3}$$

Entonces $x^{p+1} - (a-x)^{p+1} \equiv x(a-x) - (a-x)x \equiv 0 \pmod{(f(x), p)}$, luego

$$x^{p+1} - (a-x)^{p+1} \equiv 0 \pmod{(f(x).p)}$$

$$\frac{x^{p+1} - (a-x)^{p+1}}{x - (a-x)} \equiv 0 \pmod{(f(x), p)}$$

$$U_{p+1} \equiv 0 \pmod{p}$$

Ahora, sea p primo con $(\frac{\Delta}{p}) = 1$. En este caso se tiene que $x^2 - ax + b$ tiene dos raíces en $\mathbf{Z}_p$, así que el anillo $R = \mathbf{Z}_p[x]/ < x^2 - ax + b >$ no es un campo finito, más bien este es isomórfo a $\mathbf{Z}_p \times \mathbf{Z}_p$, ver 1 y cada elemento a la p-ésima potencia es el mismo. Así,

$$\text{en el caso } \left(\frac{\Delta}{p}\right) = 1 : \begin{cases} x^p \equiv x \pmod{(f(x), p)} \\ (a-x)^p \equiv a - x \pmod{(f(x), p)} \end{cases} \tag{4.5.4}$$

Nótese, también que la suposición que $\gcd(p, b) = 1$ implica que x y $a - x$ son invertibles en R, puesto que $x(a-x) \equiv b \pmod{f(x)}$. Por tanto $x^{p-1} = (a-x)^{p-1} = 1$ en R. Entonces

$$x^{p-1} - (a-x)^{p-1} \equiv 0 \pmod{(f(x), p)}$$

$$x^{p-1} - (a-x)^{p-1} \equiv 0 \pmod{p}$$

por lo tanto

$$U_{p-1} \equiv 0 \pmod{p}$$

. ■

Definición 4.6. Si n es un entero positivo con $\gcd(n, 2b\Delta) = 1$ el rango de apariencia de n denotado por $r_f(n)$ es el menor entero positivo r con $U_r \equiv 0 \pmod{n}$.

U_k es una "sucesión de divisibilidad", lo cual se puede observar en el siguiente resultado.

Lema 4.2. *si $k|j$ entonces $U_k|U_j$.*

Demostración. Considérese la identidad

$$x^s - b^s = (x-b)(x^{s-1} + x^{s-2}b + \cdots + xb^{s-2} + b^{s-1}).$$

Supóngase que $k|j$, es decir que $j = ks$ para algun $s \in \mathbb{Z}$. Entonces remplazando x por x^k y b por b^k se tiene

$$x^{ks} - b^{ks} = (x^k - b^k)(x^{k(s-1)} + x^{k(s-2)}b + \cdots + xb^{k(s-2)} + b^{k(s-1)}),$$

es decir,

$$x^j - b^j = (x^k - b^k)(x^{k(s-1)} + x^{k(s-2)}b + \cdots + xb^{k(s-2)} + b^{k(s-1)}).$$

Remplazando b por $a - x$ se obtiene

$$x^j - (a-x)^j = (x^k - (a-x)^k)(x^{k(s-1)} + x^{k(s-2)}(a-x) + \cdots + x(a-x)^{k(s-2)} + (a-x)^{k(s-1)}).$$

Por lo tanto $(x^k - (a-x)^k)|(x^j - (a-x)^j)$, es decir $U_k|U_j$. ■

También se considera la posibilidad de que $U_k = U_j = 0$. Luego se obtiene el siguiente lema.

Lema 4.3. *Si* $\gcd(n, 2b\Delta) = 1$, *entonces* $U_j \equiv 0 \pmod{n}$ *si y sólo si* $j \equiv 0 \pmod{r_f(n)}$.

Demostración. Sea $r = r_f(n)$. Supóngase que

$$U_j = \frac{x^j - (a-x)^j}{x - (a-x)} \equiv 0 \pmod{n}$$

luego $x^j - (a-x)^j \equiv 0 \pmod{n}$, es decir, $x^j \equiv (a-x)^j \pmod{n}$, y $j = qr + s$, con $0 \leq s < r$, entonces

$$\begin{aligned} x^{qr+s} &\equiv (a-x)^{qr+s} \pmod{n} \\ x^{qr}x^s &\equiv (a-x)^{qr}(a-x)^s \pmod{n}. \end{aligned}$$

como

$$\begin{aligned} U_r &\equiv 0 \pmod{n} \\ x^r - (a-x)^r &\equiv 0 \pmod{n} \\ x^r &\equiv (a-x)^r \pmod{n} \\ x^{qr} &\equiv (a-x)^{qr} \pmod{n}. \end{aligned}$$

Luego $x^{qr}x^s \equiv x^{qr}(a-x)^s \pmod{n}$, es decir,

$$n|x^{qr}x^s - x^{qr}(a-x)^s$$

$$n|x^{qr}(x^s - (a-x)^s)$$

así n divide a $x^s - (a-x)^s$ y esto implica

$$U_s \equiv 0 \pmod{n}.$$

Por la definición de $r_f(n)$ se tiene que $s = 0$. así, $j \equiv 0 \pmod{r}$.

Ahora supóngase que $j \equiv 0 \pmod{r}$, luego $U_r | U_j$; pero $n | U_r$. De esta forma $n | U_j$, es decir,

$$U_j \equiv 0 \pmod{n}$$

■

En base al teorema 4.11 se tiene el siguiente resultado.

Teorema 4.11. *Sean f, Δ tal que $f(x) = x^2 - ax + b$, $\Delta = a^2 - 4b$ y p un primo tal que $\gcd(p, 2b\Delta) = 1$, entonces $r_f(p) | p - (\frac{\Delta}{p})$.*

Demostración. Sea $r = r_f(p)$, luego

$$U_r \equiv 0 \pmod{p}$$

pero p es primo, entonces por el Teorema 4.11

$$U_{p-(\frac{\Delta}{p})} \equiv 0 \pmod{p}.$$

Por lo tanto $r | p - (\frac{\Delta}{p})$. ■

En analogia al Teorema 4.8 se tiene el siguiente resultado.

Teorema 4.12 (Morrison)**.** *Sean f, Δ tal que $f(x) = x^2 - ax + b$, $\Delta = a^2 - 4b$ y sea n un entero positivo con $\gcd(n, 2b) = 1$, $(\frac{\Delta}{n}) = -1$. Si F es un divisor de $n+1$ y*

$$U_{n+1} \equiv 0 \pmod{n}, \ \ \gcd(U_{(n+1)/q}, n) = 1 \text{ para todo primo } q | F, \tag{4.5.5}$$

entonces todo primo p que divide a n satisface $p \equiv (\frac{\Delta}{p}) \pmod{F}$. En particular, si $F > \sqrt{n} + 1$, entonces n es primo.

Demostración. Supóngase que $n + 1 = RF$, donde $F = \prod_{i=1}^{l} q_i^{\alpha_i}$. Sea p un factor primo de n. Como $U_{n+1} \equiv 0 \pmod{n}$, entonces $U_{n+1} \equiv 0 \pmod{p}$, luego por el Lema 4.3 se tiene que

$$r_f(p) | n + 1.$$

Además $r_f(p)$ no divide a $\frac{n+1}{q_i}$ para cada $1 \leq i \leq l$, porque si lo dividiera se tendría $p | \gcd(U_{(n+1)/q}, n) = 1$, lo que es absurdo. Esto implica que para cualquier $i, q_i | r_f(p)$, es más $q_i^{\alpha_i} | r_f(p)$ y así $F | r_f(p)$, luego $F | p - (\frac{\Delta}{p})$, por tanto $p \equiv (\frac{\Delta}{p}) \pmod{F}$. Si además se tiene $F > \sqrt{n} + 1$, entonces para cada factor primo p de n se tiene

$$p \geq F - 1 > \sqrt{n},$$

así n es primo. ■

Para poder usar el Teorema 4.12 como un test de primalidad, se necesita encotrar un polinomio $f(x)$ apropiado, para esto se pude escoger a, b al azar

Teorema 4.13. *Sean f, Δ tal que $f(x) = x^2 - ax + b$, $\Delta = a^2 - 4b$ y sea n un entero positivo con $\gcd(n, 2b) = 1$ y $(\frac{\Delta}{n}) = -1$. Si F es un divisor par de $n+1$ y*

$$V_{F/2} \equiv 0 \pmod{n}, \ \gcd(V_{F/2q}, n) = 1 \text{ para todo primo } q|F \tag{4.5.6}$$

entonces todo primo p que divide a n satisface $p \equiv (\frac{\Delta}{p}) \pmod{F}$. En particular, si $F > \sqrt{n} + 1$, entonces n es primo.

Demostración. Supóngase que p es un primo impar que divide a U_m y V_m a la vez. Entonces la definición de las sucesiones de Lucas implica

$$x^m \equiv (a - x)^m \pmod{(f(x), p)} \text{ y } x^m \equiv -(a - x)^m \pmod{(f(x), p)}$$

así que $x^m \equiv 0 \pmod{(f(x), p)}$. Entonces $b^m \equiv (x(a - x))^m \equiv 0 \pmod{(f(x), p)}$; es decir, $p|b$. Sea $U_m = dk_1$ y $V_m = dk_2$, donde $d = \gcd(U_m, V_m)$ y ya que $U_{2m} = U_m V_m$, se tiene

$$\gcd(U_{2m}, n) = \gcd(dk_1 \cdot dk_2, n)$$

como $p|U_m$ y $p|V_m$, entonces $p|d$, además $p|b$, luego $p|\gcd(d, 2b)$ pero $\gcd(n, 2b) = 1$, luego $\gcd(n, d) = 1$. Así,

$$\begin{aligned} \gcd(dk_1 dk_2, n) &= \gcd(k_1 k_2, n) \\ &= \gcd(k_1, n) \cdot \gcd(k_2, n) \\ &= \gcd(dk_1, n) \cdot \gcd(dk_2, n) \\ &= \gcd(U_m, n) \cdot \gcd(V_m, n). \end{aligned}$$

Así, $V_{F/2} \equiv 0 \pmod{n}$ implica $U_F \equiv 0 \pmod{n}$ y $\gcd(U_{F/2}, n) = 1$. Ahora supóngase que q es un factor primo impar de F. Así, $U_{F/q} = U_{F/2q} V_{F/2q}$, como $U_{F/2q} | U_{F/2}$ se tiene que $\gcd(U_{F/2q}, n) = 1$, pero $\gcd(V_{F/2q}, n) = 1$, luego $\gcd(U_{F/q}, n) = 1$. Así, por el Teorema 4.12 $F|r_f(p)$, luego por el Teorema 4.11 $F|p - (\frac{\Delta}{p})$, es decir

$$p \equiv (\frac{\Delta}{p}) \pmod{p}$$

Como $F > \sqrt{n} + 1$ se tiene que n es primo. ■

Así como el test $n - 1$ se satisface particularmente bien para los números de Fermat, el test $n + 1$ es una prueba específicamente rápida para los números de Mersenne.

Teorema 4.14 (Test Lucas-Lehmer para primos de Mersenne)**.** *Considérese la sucesión v_k para $k = 0, 1, ...,$ definida recursivamente por $v_0 = 4$ y $v_{k+1} = v_k^2 - 2$. Sea p un primo impar. Entonces $M_p = 2^p - 1$ es primo si y sólo si $v_{p-2} \equiv 0 \pmod{M_p}$.*

Demostración. Sea $f(x) = x^2 - 4x + 1$, así $\Delta = 4^2 - 4(1) = 16 - 4 = 12$.Por el Teorema 1.10 se tiene,

$$\left(\frac{12}{M_p}\right) = \left(\frac{3}{M_p}\right)\left(\frac{4}{M_p}\right)$$

donde $\left(\frac{2}{M_p}\right) = (-1)^{({M_p}^2-1)/8} = 1$, luego $\left(\frac{4}{M_p}\right) = \left(\frac{2}{M_p}\right)\left(\frac{2}{M_p}\right) = 1$, por otro lado $\left(\frac{3}{M_p}\right)\left(\frac{M_p}{3}\right) = (-1)^{(M_p-1)(3-1)/4} = (-1)^{(M_p-1)/2} = -1$, pero $M_p \equiv 1 \pmod 3$, es decir, $\left(\frac{M_p}{3}\right) \equiv 1 \pmod 3$, luego $\left(\frac{3}{M_p}\right) = -1$.

Por lo tanto

$$\left(\frac{12}{M_p}\right) = -1.$$

Sea $F = 2^{p-1}$ un divisor par de $M_p + 1$,

$$F = 2^{p-1} = \frac{M_p + 1}{2}$$

luego $\frac{M_p+1}{2} > \sqrt{M_p} + 1$, entonces por el Teorema 4.13 es necesario probar solamente que

$$V_{2^{p-2}} \equiv 0 \pmod{M_p}.$$

Como

$$\begin{aligned} V_{2m} &\equiv x^{2m} + (4-x)^{2m} \\ &= (x^m + (4-x)^m)^2 - 2x^m(4-x)^m \\ &= (V_m)^2 - 2(x(4-x))^m \end{aligned}$$

pero $x(4-x) \equiv 1 \pmod{f(x)}$, entonces

$$V_{2m} \equiv V_m^2 - 2 \pmod{f(x)}$$

Además $V_1 = x + (4-x) = 4$. Así

$$V_{2^k} = v_k$$

por hipótesis $v_{p-2} \equiv 0 \pmod{M_p}$, es decir

$$V_{2^{p-2}} \equiv 0 \pmod{M_p}$$

por lo tanto M_p es primo.

Para la segunda parte de la demostración, supóngase que $M = M_p$ es primo. Como $\left(\frac{\Delta}{M}\right) = -1$, donde $\Delta = 12$ es el discriminante de $f(x) = x^2 - 4x + 1$, entonces $f(x)$ es irreducible sobre $\mathbb{Z}_M$, Así $\mathbb{Z}_M[x]/ < x^2 - 4x + 1 >$ es isomorfo a F_{M^2} con M^2 elementos donde las raices para el polinomio $f(x)$ son x y $4 - x$, luego

$$\begin{cases} x^M \equiv 4 - x \pmod{(f(x), M)} \\ (4-x)^M \equiv x \pmod{(f(x), M)}. \end{cases}$$

considérese $(x-1)^{M+1}$ de dos formas,
como $(x-1)^2 \equiv 2x \pmod{(f(x), M)}$, por el criterio de Euler se tiene

$$\begin{aligned} 2^{(M-1)/2} &\equiv \left(\frac{2}{M}\right) \pmod{M} \\ 2^{(M-1)/2} &\equiv 1 \pmod{M} \end{aligned}$$

así

$$\begin{aligned} ((x-1)^2)^{(M+1)/2} &\equiv (2x)^{(M+1)/2} \pmod{(f(x), M)} \\ (x-1)^{M+1} &\equiv (2x)^{(M+1)/2} \pmod{(f(x), M)} \\ &= 2 \cdot 2^{(M-1)/2} \cdot x^{(M+1)/2} \\ &\equiv 2x^{(M+1)/2} \pmod{(f(x), M)}. \end{aligned}$$

Por otro lado,

$$(x-1)^{M+1} = (x-1)(x-1)^M \equiv (x-1)(x^M - 1) \equiv (x-1)(3-x) \equiv -2 \pmod{(f(x), M)}.$$

Así

$$\begin{aligned} 2x^{(M+1)/2} &\equiv -2 \pmod{(f(x), M)} \\ x^{(M+1)/2} &\equiv -1 \pmod{(f(x), M)}, \end{aligned}$$

es decir,

$$x^{2^{p-1}} \equiv -1 \pmod{(f(x), M)}.$$

Como $(4 - x) \equiv x^M \pmod{(f(x), M)}$, se tiene

$$\begin{aligned} (4-x)^{(M+1)/2} &\equiv (x^M)^{(M+1)/2} \pmod{(f(x), M)} \\ (4-x)^{(M+1)/2} &\equiv (x^{(M+1)/2})^M \pmod{(f(x), M)} \\ (4-x)^{(M+1)/2} &\equiv (-1)^M \pmod{(f(x), M)}, \end{aligned}$$

como M es un primo mayor que 2, entonces

$$(4-x)^{(M+1)/2} \equiv -1 \pmod{(f(x), M)}$$

luego

$$\begin{aligned} x^{2^{p-1}} - (4-x)^{(M+1)/2} &\equiv 0 \pmod{(f(x), M)} \\ \frac{x^{2^{p-1}} - (4-x)^{2^{p-1}}}{x-(4-x)} &\equiv 0 \pmod{(f(x), M)} \end{aligned}$$

esto es,

$$U_{2^{p-1}} \equiv 0 \pmod{M}.$$

Si $U_{2^{p-2}} \equiv 0 \pmod{M}$, entonces

$$x^{2^{p-2}} \equiv (4-x)^{2^{p-2}} \pmod{(f(x), M)}$$

así
$-1 \equiv x^{2^{p-1}} \equiv x^{2^{p-2}} x^{2^{p-2}} \equiv x^{2^{p-2}}(4-x)^{2^{p-2}} \equiv (x(4-x))^{2^{p-2}} \equiv 1^{2^{p-2}} \equiv 1 \pmod{(f(x), M)}$. Lo que es absurdo. Como $U_{2^{p-1}} = U_{2^{p-2}} V_{2^{p-2}}$, se tiene $V_{2^{p-2}} \equiv 0 \pmod{M}$. Pero $V_{2^{p-2}} = v_{p-2}$, por lo tanto

$$v_{p-2} \equiv 0 \pmod{M}.$$

■

Conclusiones

- En este trabajo se recopilaron algunos resultados que permiten estudiar dos problemas clásicos en el estudio de los números primos. Aunque no se conoce si existe una fórmula o sucesión con la que se pueda generar todos los números primos, en este trabajo se presentaron algunos resultados con los que se pueden dar expresiones particulares en este sentido. Entre ellas se estudiaron los números de Mersenne y los números de Fermat, el objetivo fue encontrar generalidades de dichos números que posibiliten obtener al menos secuencias finitas de números que sean primos.

- Por otra parte, respecto al problema de como determinar si un número es primo o no, especialmente cuando este es demasiado grande, desafortunadamente o afortunadamente tampoco se tiene una respuesta concreta; hasta hoy no hay un teorema, definición o propiedad matemática que permita determinar con eficiencia si un número es primo o compuesto. En este trabajo se presentaron algunos resultados que ayudan a decidir sobre la primalidad de un número dado. En particular en el apéndice se presenta la implementación de algunos procedimientos que ayudan a resolver este problema para ciertos números y con los cuales se puede ejemplificar la teoría estudiada.

- Los problemas estudiados en este trabajo son problemas abiertos y la comunidad matemática aún continua trabajando en sus posibles soluciones. De esta forma este es un campo en el cual se pueden desarrollar futuras investigaciones.

Apéndice

En este Apéndice se presentan algunos algoritmos implementados en el desarrollo de este trabajo.

A.1. Algoritmo (Test probable primo)

Dados dos enteros a, n con $n > 3$ y $2 \leq a \leq n-2$, usando el Pequeño Teorema de Fermat 2.5 el algoritmo retorna o bien " n es probable primo base a" o " n es compuesto".

```
probprimo:=function(n,a)
          local b;
          b:=a^n mod n;
          if b<>a then
          return [n,"es compuesto"];
          fi;
          return [n,"es probable primo base", a];
end;
```

A.2. Algoritmo (Test probable primo fuerte)

Dado un número impar $n > 3$ y un entero a con $1 < a < n-1$; el algoritmo probable primo fuerte inicialmente encuentra la representación de $n = 1 + 2^s t$, donde t es impar, luego utilizando las congruencias del Teorema 4.5 retorna o bien "n es un probable primo fuerte base a" o "n es compuesto". ´´

```
Exponente:= function(n)
            local s,x,t,R;
            s:=0;
            x:=n-1;
            while x mod 2=0 do
            s:=s+1;
            x:=x/2;
            od;
            t:=(n-1)/(2^s);
            R:=[s,t];
            return (R);
end;
```

```
Probprimofuerte:=function(n,a)
                local F,i,m,D,t,s;
                D:=Exponente(n);
                s:=D[1];
                t:=D[2];
                F:=Gcd(a,n);
                if F=1 then
                if a^t mod n =1 then
                return [n,"es probable primo fuerte base", a];
                fi;
                for i in [0 .. (s-1)] do
                m:=a^((2^i)*t) mod n;
                if m=n-1 then
                return [n,"es probable primo fuerte base", a];
                fi;
                od;
                else return [a, "y", n,"no son primos relativos"];
                fi;
                return [n,"es compuesto"];
end;
```

A.3. Algoritmo n-1

Teniendo en cuenta las condiciones del Teorema de Pocklinton 4.8, el corolario 4.1 y el Teorema de Brillhart, Lehmer y Selfridgede 4.9. Dado un entero positivo $n > 3$, este algoritmo retorna o bien " n es primo" o " n es compuesto".

```
base:= function(n,b)
       local L,m,q,k;
       q:=n;
       k:=0;
       L:=[];
       while q<>0 do
       Add(L,q mod b);
       q:=Int (q/b);
       k:=k+1;
       od;
       return (L);
end;

Pock:= function(n)
       local a,l,F,p,P,g,R,r1,r;
       a:=Random([2..n-2]);
       if a^(n-1) mod n <>1 then
```

```
        return [n,"es compuesto"];
        fi;
        l:=DivisorsInt(n-1);
        F:=Random(l);
        P:=PrimeDivisors(F);
        for p in P do
        g:=Gcd((a^((n-1)/p) mod n)-1,n);
        if g in [2..n-1] then
        return [n,"es compuesto"];
        fi;
        if g=n then return Pock(n);
        fi;
        od;
        if F>=RootInt(n) then
        return [n,"es primo"];
        fi;
        if RootInt(n,3)<=F and F<RootInt(n) then
        R:=base(n,F);
        r:=R[2]^2-4*R[3];
        r1:=RootInt(r);
        if r1^2<>r then
        return [n,"es primo"];
        else
        return [n,"es compuesto"];
        fi;
        fi;
        if F<RootInt(n,3) then
        return Pock(n);
        fi;
end;
```

A.4. Algoritmo n+1 (Morrison)

El siguiente algoritmo utiliza el Teorema de Morrison 4.12 para determinar la primalidad de un número dado $n > 2$. El algoritmo inicialmente toma dos variables locales a y b que corresponden a los coeficientes del polinomio $f(x) = x^2 - ax + b$ y calcula el discriminante correspondiente al polinomio, luego usará la secuencia de Lucas U_k como lo indica el Teorema. El algoritmo retorna o bien " n es primo" o " n es compuesto".

```
Morrison:=function(n)
         local D,L,F,q,P,p,g,l,j,a,b;
         a:=Random([0..n-1]);
         if a=0 then
         b:=Random([1..n-1]);
```

```
        else
        b:=Random([0..n-1]);
        fi;
        D:=a^2-4*b;
        if  Gcd(n,2*b)=1 and Legendre(D,n)=-1 then
        L:=DivisorsInt(n+1);
        F:=Random(L);
        while F<=RootInt(n)+1 do
        F:=Random(L);
        od;
        if Lucas(a,b,n+1)[1] mod n <> 0 then
        return [n,"es compuesto"];
        fi;
        P:=PrimeDivisors(F);
        for q in P do
        g:=Gcd(Lucas(a,b,(n+1)/q)[1],n);
        if g<>1 then
        return Morrison (n);
        fi;
        od;
        return  [n,"es primo"];
        else
        return Morrison (n);
        fi;
end;
```

A.5. Algoritmo (Primos de Mersenne)

El siguiente algoritmo usa el Teorema 4.14 Test Lucas-Lehmer para primos de Mersenne, para determinar la primalidad de un número de Mersenne. Así dado un primo p impar el algoritmo retorna o bien " Mp es primo" o "Mp es compuesto".

```
PrimosMp:=function(p)
        local Mq,k,v1;
        Mq:=(2^p)-1;
        v:=4;
        for  k in [1..p-2] do
        v:=(v^2)-2;
        v1:=v mod Mq;
        od;
        if v1=0 then
        return ["2^",p,"-1 es primo "];
        else
```

```
        Print("2^",p,"-1 es compuesto ");
        fi;
end;
```

Bibliografía

[1] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Ann. of Math. (2)*, 139(3):703–722, 1994.

[2] A. Bhattacharya. Infinitude of primes: Remembering previous works and also proofs by forgotten mathematicians. consulta: mayo de 2014.

[3] R. Crandall and C. Pomerance. *Prime numbers: A computational perspective*. Springer, New York, second edition, 2005.

[4] F. A. G. de la Hoz. Teoría de números entrega 4: Teorema de dirichlet. page 12, mayo 2003.

[5] J. R. Gaytan. El teorema de los números primos. *Instituto de Matemáticas, UNAM-Morelia*, 2003.

[6] G. Grabinsky. Euler, el prestidigitador de las series. *Miscelánea Matemática*, 45:55–66, 2007.

[7] J. P. Jones, D. Sato, H. Wada, and D. Wiens. Diophantine representation of the set of prime numbers. *Amer. Math. Monthly*, 83(6):449–464, 1976.

[8] J. Rengel Rojo. Recopilación de diversas demostraciones de la infinitud de los números primos. Master's thesis, Universidad de la Rioja, 2013.

[9] P. Ribenboim. *The new book of prime number records*. Springer-Verlag, New York, 1996.

[10] V. Vicario García. Las demostraciones alternativas como recurso científico y didáctico. el caso de la infinitud de los números primos. *Revista OIM*, (33):1–14, noviembre–diciembre 2008.