UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS NATURALES Y MATEMÁTICA

ESCUELA DE MATEMÁTICA

"Una construcción recursiva del conjunto de los números primos".

Estudiante

Oscar Gustavo Carranza Tejada

CT07001

Para optar al grado de:

Licenciado en Matemática

Asesores

Lic. Mario Alexis Ruíz Mejía

Lic. Ernesto Américo Hidalgo Castellanos

Ciudad Universitaria, Octubre 2015

Índice general

Introducción

El documento se encuentra estructurado en tres capítulos, el primero de ellos es de Fundamentos Teóricos y está dedicado a exponer conceptos, resultados y procedimientos fundamentales del aritmética y teoría de números, esto para enmarcar teóricamente el contenido de los capítulos dos y tres.

En el segundo de los capítulos es sobre Números Primos, en la primera sección se citan algunas fórmulas conocidas que generan números primos, las siguientes secciones se dedican a estudiar resultados clásicos sobre la distribución de números primos, donde se enuncian algunos teoremas muy importantes, terminamos enunciando y demostrando el Postulado de Bertrand, el cual garantiza la veracidad de los argumentos escritos en las demostraciones del último capítulo.

Finalmente en el tercer capítulo se da una Formulación recursiva para el conjunto de los números primos, se comienza motivando la construcción y surgimiento de la fórmula, luego se enuncia y demuestra detalladamente para finalizar esbozando el método de demostración con dos ejemplos.

Este trabajo tiene un enfoque puramente teórico, esta fórmula garantiza que es posible construir el conjunto de los números primos y una manera de como calcularlos. Este método no es eficiente para calcular números primos, por este motivo expresamos que es un aporte teórico y no práctico.

1. Fundamentos teóricos

En este capítulo comenzamos en las primeras secciones definiendo algunos conceptos fundamentales en aritmética, luego en las siguientes secciones se dedican a exponer algunos procedimientos y resultados clásicos que servirán como preámbulo al estudio teórico y formal que se hará en los próximos capítulos. Las demostraciones las propiedades y resultados enunciados se refieren a [7] y [5].

1.1. Divisibilidad

Se dice que un entero $a \neq 0$ divide a un entero b, y se escribe $a \mid b$, si existe un entero k tal que $b = ak$. Por ejemplo $13 \mid 1001$ porque $13 \times 77 = 1001$. Algunas propiedades importantes de la divisibilidad son:

1. Si $a \mid b$ y c es un entero, entonces $a \mid bc$.
2. Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.
3. Si $a \mid b$ y $a \mid c$ y x y y son enteros cualesquiera, entonces podemos afirmar que $a \mid bx \pm cy$.
4. Si $m \mid (a - b)$ y $m \mid (c - d)$, entonces $m \mid (ac - bd)$.
5. Si $a \mid b$, $k \neq 0$ es un entero, entonces $ka \mid kb$.
6. Si $a \mid b$ y $c \mid d$, entonces $ac \mid bd$.

Las demostraciones no representan mayor dificultad y se deducen fácilmente de la definición.

Las propiedades anterior junto con los conceptos de Máximo Común Divisor (MCD) y Mínimo Común Múltiplo (MCM) se establecen algunos resultados clásicos muy útiles como el Lema de la División, el Algoritmo de Euclides y el Lema de Bezout.

Lema 1.1.1 (Lema de la División)**.** Para cada par de enteros $a \neq 0$ y b existe un único par de enteros q y r, satisfaciendo: $b = aq + r$ y $0 \leq r < |a|$.

A los enteros b, a, q y r se les conoce respectivamente como **dividendo**, **divisor**, **cociente** y **residuo** de la división entera de b por a.

Existen diversos métodos que permiten calcular el MCD de dos números enteros, estos métodos están fundamentados esencialmente en el Lema de División. Un método es el **Algoritmo de Euclides** consiste en una serie de divisiones sucesivas y el MCD se obtiene como uno de los residuos en el proceso de división. Además de dar un procedimiento para calcular el MCD, permite dar una comprobación de la existencia de éste.

Teorema 1.1.2 (Algoritmo de Euclides)**.** Dados a y b enteros positivos, hagamos

$$\begin{aligned} b &= aq_1 + r_1, & 0 \leq r_1 < a \\ a &= r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 & 0 \leq r_3 < r_2 \\ &\dots \\ r_n &= r_{n+1}q_{n+2} \end{aligned}$$

Entonces $(a : b) = r_{n+1}$.

Lema 1.1.3 (Lema de Bezout)**.** El MCD de dos enteros a y b siempre se puede expresar como combinación lineal de a y b. Es decir, existen enteros x y y tales que $(a : b) = ax + by$. A los enteros x y y se les conoce como **coeficientes de Bezout**.

El lema anterior asegura que en general haciendo las sustituciones sucesivas regresivamente siempre se pueden encontrar enteros x y y tales que $(a : b) = ax + by$.

1.2. Congruencias

La teoría de congruencias es un estudio formal del concepto de divisibilidad, que parte de una noción que se comporta de manera análoga a la igualdad. Como veremos, las congruencias cumplen propiedades importantes heredadas de a relación de divisibilidad que se exponen en esta sección.

Decimos que $a \equiv b \mod m$ (que se lee a es congruente con b módulo $m \in \mathbb{Z} \setminus \{\pm 1\}$) si y sólo si $m \mid (b - a)$.

Las siguientes expresiones son equivalentes:

- a es congruente con b módulo m. $a \equiv b \mod m$.
- El resto de a entre m es el mismo resto de b entre m. $a \mod m = b \mod m$.
- m divide exactamente a la diferencia de a y b. $m \mid a - b$.
- a se puede escribir como la suma de b y un múltiplo de m. $\exists k \in \mathbb{Z} : a = b + k \cdot m$.
- El término congruencia se utiliza además con dos sentidos ligeramente diferentes: por un lado con el sentido de identidad matemática, Por otro lado se utiliza en el sentido de ecuación, donde aparecen una o más incógnitas, y nos preguntamos si una congruencia tiene solución y en caso afirmativo cuáles son todas sus soluciones, por ejemplo la congruencia $x^2 - 5 \equiv 0 \mod 11$ tiene solución, y todas sus soluciones vienen dadas por $x \equiv 7 \mod 11$ y $x \equiv 4 \mod 11$. Es decir x puede ser cualquier entero de la forma: $11 \cdot k + 4$ y $11 \cdot k + 7$. Contrariamente la congruencia $x^2 - 2 \equiv 0 \mod 11$ no tiene solución.

Esta notación y terminología fueron introducidas por Carl Friedrich Gauss en su libro Disquisitiones Arithmeticae en 1801. Su uso se ha extendido a muchos otros entornos en los que podemos mencionar los polinomios con coeficientes en un cuerpo, a ideales de anillos de números algebraicos, etc.

1.2.1. Propiedades de las congruencias

La relación de congruencia hemos dicho que tiene muchas propiedades en común con la igualdad matemática:

- La congruencia para un módulo fijo m es una relación de equivalencia ya que se verifican las propiedades:
  1. reflexividad: $a \equiv a \mod m$.
  2. simetría: si $a \equiv b \mod m$ entonces también $b \equiv a \mod m$.
  3. transitividad: si $a \equiv b \mod m$ y $b \equiv c \mod m$ entonces también $a \equiv c \mod m$.
- Como la congruencia es una relación de equivalencia, determina en $\mathbb{Z}$ una partición que tiene tantas clases de equivalencia como unidades tiene el módulo m. Los elementos $x = m \cdot k + r$ están en la clase de resto r ; $0 \leq r < m$. Los múltiplos de m forman la clase de equivalencia del representante 0.
- Si a es coprimo con m y $a \equiv b \mod m$ entonces b también es coprimo con m.
- si $a \equiv b \mod m$ y k es un entero entonces también se cumple que:
  1. $a + k \equiv b + k \mod m$
  2. $k \cdot a \equiv k \cdot b \mod m$
  3. $\forall k > 0 : a^k \equiv b^k \mod m$
- Si además k es coprimo con m, entonces podemos encontrar un entero h^{-1} tal que $k \cdot h^{-1} \equiv 1 \mod m$ y entonces tiene sentido hablar de inversos y también es cierto que $\frac{a}{k} \equiv \frac{b}{k} \mod m$ donde por definición ponemos $\frac{a}{k} = a \cdot k^{-1}$.
- Como consecuencia de lo anterior, si tenemos dos congruencias con igual módulo: $c \equiv d \mod m$ y $a \equiv b \mod m$ podemos sumarlas, restarlas o multiplicarlas de forma que también se verifican las congruencias $a \pm c \equiv b \pm d \mod m$ y $a \cdot c \equiv b \cdot d \mod m$.
- $a \cdot r \equiv b \cdot r \mod m$ y $d = (m, r)$ entonces $a \equiv b \mod \frac{m}{d}$.

Propiedad sintetizadora

La posibilidad de sumar a ambos miembros de una congruencia el mismo número, multiplicarlos por el mismo número no nulo y elevar a la misma potencia entera positiva los enteros congruentes, puede fusionarse a través de la proposición siguiente:

Si $p(t)$ es un polinomio en t con coeficientes enteros, implica que de $a \equiv b \mod m$ se deduce que $p(a) \equiv p(b) \mod m$.

1.2.2. Teorema de Euler-Fermat

En teoría de números el teorema de Euler, también conocido como teorema de Euler-Fermat, es uno referente a números compuestos análogo al pequeño teorema de Fermat, y como tal afirma una proposición sobre la divisibilidad de los números enteros. El teorema establece que:

Teorema 1.2.1. Si a y n son enteros primos relativos, entonces $a^{\varphi(n)} \equiv 1 \mod m$, en donde $\varphi(n)$ es la función de Euler.

Demostración. Sea $A = \{r \in \{1, \ldots, n\} : (n, r) = 1\}$ es evidente que $|A| = \varphi(n)$.

Definamos ahora la siguiente aplicación $f : A \to \{1, \ldots, n\}$ tal que $f(r) = a \cdot r \mod n$

Es claro que por definición de f se tiene que para todo $r \in A : a \cdot r \equiv f(r) \mod n$

Luego puesto que $(a, n) = (r, n) = 1$ entonces $(a \cdot r, n) = 1$ por lo tanto puesto que $a \cdot r \equiv f(r) \mod n$ así se tiene que $(f(r), n) = 1$ por lo tanto se tiene que $\forall r \in A : f(r) \in A$ así entonces tenemos que $f(A) \subset A$.

Luego como $(a, n) = 1$, entonces existen enteros $x_1, x_2 \in \mathbb{Z}$ tales que $a \cdot x_1 + n \cdot x_2 = 1$, sea ahora $y_1 = x_1 \mod n$, es claro que $y_1 \in A$ luego como $a \cdot x_1 + n \cdot x_2 = 1$ entonces $a \cdot x_1 \equiv 1 \mod n$.

Es evidente que $y_1 \equiv x_1 \mod n$, por lo tanto tenemos que $a \cdot x_1 \equiv a \cdot y_1 \equiv 1 \mod n$. así entonces garantizamos que existe $y_1 \in A : a \cdot y_1 \equiv 1 \mod n$.

Sea ahora $s \in A$ cualquier elemento de A, entonces como $a \cdot y_1 \equiv 1 \mod n$ tenemos que $y_1 \cdot s \cdot a \equiv s \mod n$. Ahora sea $r_1 = (y_1 \cdot s) \mod n$, es claro que $r_1 \in A$ luego como $y_1 \in A \wedge s \in A$, entonces $(y_1, n) = (s, n) = 1$ luego esto implica que $(y_1 \cdot s, n) = 1$, luego como $y_1 \cdot s \cdot a \equiv s \mod n$ y $r_1 \equiv y_1 \cdot s \mod n$ entonces $a \cdot r_1 \equiv s \mod n$ entonces como $s \in \{1, \ldots, n\}$ garantizamos que $s = a \cdot r_1 \mod n = f(r_1)$ pues el resto de $a \cdot r_1$ es único por lo tanto así garantizamos que $\exists r_1 \in A : s = f(r_1)$ entonces tenemos que $s \in f(A)$ por lo tanto $A \subset f(A)$ así tenemos que $A = f(A)$.

Luego como $\forall r : a \cdot r \equiv f(r) \mod n$ esto implica que por las propiedades de congruencias, si

$P = \prod_{r \in A} r$ entonces, $\left(\prod_{r \in A} a \right) \cdot P \equiv \prod_{r \in A} f(r) \mod n$, es claro que $(n, P) = 1$ luego como $A = f(A)$ se tiene que $\prod_{r \in A} f(r) = \prod_{s \in f(A)} s = \prod_{s \in A} s = \prod_{r \in A} r = P$, así entonces garantizamos que $a^{\varphi(n)} \cdot P = a^{|A|} \cdot P = \left(\prod_{r \in A} a \right) \cdot P \equiv \prod_{r \in A} f(r) = P \mod n$ por lo tanto $a^{\varphi(n)} \equiv 1 \mod \frac{n}{(n, P)}$ por lo tanto

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

□

1.2.3. Pequeño Teorema de Fermat

Teorema 1.2.2 (Pequeño Teorema de Fermat)**.** Si p es un número primo, entonces, para cada número natural a coprimo con p, $a^{p-1} \equiv 1 \mod p$.

Demostración. Por el teorema de Euler-Fermat tenemos que $a^{\varphi(p)} \equiv 1 \mod p$ es claro que $\varphi(p) = p - 1$ y se tiene el resultado deseado. □

1.2.4. Teorema chino del resto

El teorema chino del resto es un resultado que da criterio y procedimientos de cálculo sobre las soluciones a sistemas de congruencias.

Teorema 1.2.3 (Teorema chino del resto)**.** Dados los números $m_1, m_2, \ldots, m_k \in \mathbb{Z} \setminus \{\pm 1\}$, primos relativos dos a dos, y b_1, b_2, ..., b_k enteros cualesquiera, el sistema de congruencias simultáneas

$$\begin{aligned} x &\equiv b_1 \mod m_1 \\ x &\equiv b_2 \mod m_2 \\ &\vdots \\ x &\equiv b_k \mod m_k \end{aligned}$$

siempre posee una única solución $\mod \prod_{i=1}^{k} m_i$.

Es decir, si x es tal solución, se verifica que $\bar{x}_{m_1} = \bar{x}_{m_2} = \ldots = \bar{x}_{m_k}$.

La forma original del teorema, escrita en un libro del siglo III por el matemático chino Sun Tzu y posteriormente publicado en 1247 por Qin Jiushao, es un enunciado sobre congruencias simultáneas.

Demostración. **Existencia de la solución**. Sea $M = \prod_{i=1}^{k} m_i$ y sea $\forall i = 1, \ldots, k : M_i = \dfrac{M}{m_i}$. Como todos los módulos m_j son coprimos entre sí, M_i y m_j son a su vez coprimos entre sí, luego por la Identidad de Bezout sabemos que $\exists r_i, s_i \in \mathbb{Z} : r_i \cdot m_i + s_i \cdot M_i = 1$. En tales condiciones, tomando las clases de equivalencia en ambos lados, se tiene por un lado y por

otro que: $s_i \cdot M_i \equiv 1 \mod m_i$ y $s_i \cdot M_i \equiv 0 \mod m_j$. Por tanto, definiendo $x = \sum_{i=1}^{k} b_i \cdot s_i \cdot M_i$ es claro que x es la solución buscada, debido que al tomar clases de equivalencia en cada m_i, todos los sumandos se anulan a excepción de $b_i \cdot s_i \cdot M_i$, y por tanto $\forall i = 1, \ldots, k : x \equiv b_i \mod m_i$. Así pues, queda probado que x es solución del sistema.

Unicidad de la solución. Como todos los m_i son coprimos, esa solución es la única existente en (mód M).

Para demostrarlo, supongamos que existiesen dos soluciones distintas: $\exists x_1, x_2 \in \mathbb{Z}$. Entonces: $\forall i = 1, \ldots, k : x_1 \equiv b_i \mod m_i$ y $\forall i = 1, \ldots, k : x_2 \equiv b_i \mod m_i$, por ser todos los m_j coprimos a pares, esto implica que el producto de lo módulos también divide a $x_1 - x_2$ es decir, $M \mid (x_1 - x_2)$, entonces $x_1 \equiv x_2 \mod M$. Por tanto, toda solución del sistema es congruente con x en (mód M), tal y como se había establecido previamente en el enunciado del Teorema. □

De manera más general, las congruencias simultáneas pueden ser resueltas si los m_j no son coprimos a pares. Una solución x existe si y sólo si: $\forall i, j : b_i \equiv b_j \mod (m_i, m_j)$.

Todas las soluciones x son entonces congruentes módulo el mínimo común múltiplo de los m_j.

Versiones del teorema chino del resto fueron también conocidas por Brahmagupta, y aparecen en el Liber Abaci de Fibonacci (1202).

1.3. La Criba de Eratóstenes

El método más práctico de obtener una lista de números primos es llamado **Criba de Eratóstenes**. La criba de Eratóstenes es un procedimiento que permite encontrar todos los primos menores que un entero positivo n mayor que dos. Se forma una tabla con todos los números naturales comprendidos entre 2 y n, y se van tachando los números que no

son primos de la siguiente manera: comenzando por el 2, se tachan todos sus múltiplos; comenzando de nuevo, cuando se encuentra un entero que no ha sido tachado, ese número es declarado primo, y se procede a tachar todos sus múltiplos, así sucesivamente. El proceso termina cuando el cuadrado del mayor número confirmado como primo es mayor que n.

A continuación ilustramos el método para encontrar los números primos mayores que 1 y menores que 100. Escribimos los números del 1 al 100:

1	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

Y luego de hacer el procedimiento explicado, la lista queda

~~1~~	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~~

Hasta aquí hemos encontrado (con la Criba de Eratóstenes) todos los primos que hay entre los primeros cien números, los cuales 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 y 97.

1.3.1. Refinamiento

Un refinamiento de la criba consiste en tachar los múltiplos del k-ésimo número primo p_k, comenzando por $(p_k)^2$ pues en los anteriores pasos se habían tachado los múltiplos de p_k correspondientes a todos los anteriores números primos, esto es $2 \cdot p_k, 3 \cdot p_k, 4 \cdot p_k, 5 \cdot p_k, \ldots, (p_k - 1) \cdot p_k$.

El algoritmo acabaría cuando $(p_k)^2 > n$ ya que no habría nada que tachar.

Otro refinamiento consiste en generar una lista sólo con números impares (pues los números pares distintos de 2 se sabe que no son primos), e ir tachando los múltiplos de los números primos mediante incrementos de $2 \cdot p$, es decir, los múltiplos impares $(2 \cdot k + 1) \cdot p$ de cada primo p. Esto aparece en el algoritmo original.

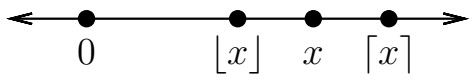
1.4. Funciones parte entera

En matemática, las funciones de parte entera son funciones: $f : \mathbb{R} \to \mathbb{Z}$ que toman un número real y devuelven un número entero más próximo, sea por exceso o por defecto.

Según la forma de considerar el número entero más próximo a un número real dado, se pueden considerar varias funciones:

Definición 1.4.1 (de las funciones menor y mayor entero ($\lceil x \rceil$, $\lfloor x \rfloor$))**.** Las funciones **menor entero** y **mayor entero** de un número real x se denotan respectivamente por $\lceil x \rceil$, $\lfloor x \rfloor$ y se definen como sigue:

$$\lceil x \rceil := \text{ el } \textit{menor entero} \text{ que es mayor o igual a } x$$
$$\lfloor x \rfloor := \text{ el } \textit{mayor entero} \text{ que es menor o igual a } x.$$



La figura anterior justifica el nombre de las funciones $\lfloor x \rfloor$, $\lceil x \rceil$, sin embargo, se advierte que en la literatura también se les suele encontrar respectivamente como funciones *techo* y *piso*, a ésta última función (menor entero) con mucha frecuencia se suele llamar también función *parte entera* o *entero mayor* y denotar como $[\![x]\!]$.

La propiedad arquimediana de $\mathbb{R}$ asegura que existe un único número entero n tal que $n \leq x < n+1$. En este sentido las funciones

$$\begin{array}{rll} \lceil x \rceil : & \mathbb{R} \to \mathbb{Z} & \qquad\qquad \lfloor x \rfloor : \quad \mathbb{R} \to \mathbb{Z} \\ & x \mapsto n+1 & \qquad\qquad\qquad\quad x \mapsto n \end{array}$$

están bien definidas.

1.4.1. Función techo

La función techo se aplica a un número real x y devuelve el mínimo número entero k no inferior a x : $ceil(x) = \text{mín}\{k \in \mathbb{Z} : x \leq k\}$

Propiedades

- Para cualquier número real se cumple que $ceil(x) \geq x$.
- El número real x al que se aplica la función techo es un número entero si y sólo si la función techo de x tiene el mismo valor que x, es decir, $x \in \mathbb{Z}$ si y sólo si $ceil(x) = x$.
- La función techo tiene puntos de discontinuidad en los números enteros pero es diferenciable para el resto de puntos.

1.4.2. Función piso

La función piso se aplica a un número real x y devuelve el máximo número entero k no superior a x:

$\lfloor x \rfloor = \max\{k \in \mathbb{Z} : k \leq x\}$, Se conoce también como función máximo entero.

Propiedades

- El número real x al que se aplica la función piso es un número entero si y sólo si la función piso de x tiene el mismo valor que x. Es decir $x \in \mathbb{Z}$ si y sólo si $\lfloor x \rfloor = x$.
- Sea x con y números reales. En tal caso se cumple:

  1. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.
  2. $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ si m es entero.
  3. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
  4. $\lfloor x \rfloor + \lfloor -x \rfloor = 0$ si x es entero, en otro caso es -1.
  5. $x - \lfloor x \rfloor$ es la parte fraccionaria o mantisa de x.
  6. $ceil(x) = -\lfloor -x \rfloor$

Proposición 1.4.2. Un número m es racional si, sólo si existe un entero positivo h, tal que $\lfloor h \cdot m \rfloor = h \cdot m$.

2. Números primos

En este capítulo comenzamos recordando algunos conceptos fundamentales en aritmética, las siguientes secciones se dedican a exponer algunas fórmulas de números primos anteriormente conocidas y finalizamos con unos resultados clásicos sobre la distribución de los números primos. Todo esto inspirado en realizar una construcción muy teórica y formal en el siguiente capítulo.

Un número entero positivo p, se dice que es **número primo** (o simplemente primo) si p y 1 son los únicos divisores positivos distintos de p. Aquel número entero positivos que no es primo, se le llama **número compuesto** (o simplemente compuesto), a excepción del número 1 el cual no es primo ni compuesto.

Por ejemplo, todo número compuesto es de la forma $m = m_1 m_2$, donde $1 < m_1 < m$ y $1 < m_2 < m$, por ejemplo $6 = 2 \cdot 3$. Los números 2, 3, 5, 7 son todos números primos. Nótese que el único primo par es el 2 y todos los primos mayores que 2 son impares.

2.1. Fórmulas que generan números primos

Entenderemos fórmula de números primos, como una fórmula que genera exactamente los números primos, en orden y sin excepción alguna.

El famoso problema matemático es encontrar una fórmula de números primos explícita, en el estudio de este han surgido muchos y muy interesantes resultados, a los cuales hacemos referencia a continuación.

Funciones polinomiales

Se sabe que no existe una función polinomial no constante $P(n)$ que evalúe números primos para todos los enteros n La comprobación a esto es simple: Supongamos que dicho polinomio existe. Entonces $P(1)$ evaluaría al primo p entonces $P(1) \equiv 0 \mod p$.

Para cualquier k, $P(1+k\cdot p) \equiv 0 \mod p$. Así que $P(1+k\cdot p)$ no puede ser primo, si lo fuera, sería divisible por p a menos que fuera el mismo p. La única forma en que $P(1) = P(1+k\cdot p)$ para toda k si la función polinomial es constante y eso sería un absurdo, pues $P(n)$ no es constante.

Si se recurre a la teoría de números algebraicos, se puede demostrar un resultado aún más general: no existe una función polinomial no constante $P(n)$ que evalúe un número primo para casi todos los enteros n.

El polinomio cuadrático

$P(n) = n^2 + n + 41$ devuelve números primos para todos los enteros no negativos menores que 40. Los números primos para $n = 0, 1, 2, 3, \ldots$ son $41, 43, 47, 53, \ldots$ la diferencias entre los términos son $2, 4, 6, 8, 10, \ldots$ para $n = 40$ se obtiene $1681 = 41 \cdot 41$, el cual es un número cuadrado perfecto, el menor número compuesto para esta fórmula. De hecho si 41 divide a n, también divide a $P(n)$.

Basándonos en el Teorema de Dirichlet sobre las progresiones aritméticas se sabe que funciones lineales $f(x) = a \cdot x + b$ producen infinitos números primos siempre y cuando a y b sean primos relativos, aunque tal función no asumirá valores primos para cualquier x .

No se conoce si existe un polinomio de al menos grado mayor que 2 que genere una cantidad infinita de valores que sean números primos.

Fórmula basada en un sistema de ecuaciones diofánticas

En [8] se da una forma de generar números primos, mediante las soluciones a un sistema de ecuaciones diofánticas: Un conjunto de ecuaciones diofánticas en 26 variables puede ser usada para obtener números primos. Jones demostró que dado un número $k+2$ éste es primo si y solo si el sistema de 14 ecuaciones diofánticas tiene una solución en los números naturales.

Fórmula en términos de números factoriales que generan números primos

A lo largo de la historia, se han buscado numerosas fórmulas para generar números primos. El nivel más alto de exigencia para una fórmula así sería que asociara a cada número natural n el n-ésimo número primo. De forma más indulgente, se puede pedir una función f que asocie a cada número natural n un número primo de tal forma que cada uno de los valores tomados sólo aparezca una vez.

Además, se desea que la función se pueda calcular en la práctica. Por ejemplo, el teorema de Wilson asegura que p es un número primo si y sólo si $(p-1)! \equiv -1 \mod p$. Otro ejemplo: la función $f(n) = 2+(2\cdot n! \mod (n+1))$ genera todos los números primos, sólo los números primos, y sólo el valor 2 se toma más de una vez. Sin embargo, ambas fórmulas se basan en el cálculo de un factorial, lo que las hace computacionalmente "costosas", también se conoce una función en términos de números factoriales y función parte entera:

$$f(n) = 2 + (2 \cdot n - 1) \cdot (1 + \left\lfloor \frac{(2n)! + 1}{2 \cdot n + 1} \right\rfloor + \left\lfloor \frac{-(2n)! - 1}{2 \cdot n + 1} \right\rfloor)$$

El teorema de Wilson nos asegura también que esta fórmula genera solo números primos para todos los números naturales, pero al evaluar la fórmula para algunos números naturales n el lector puede darse cuenta del comportamiento de los valores. Esta fórmula no genera el conjunto de números primos en forma ordenada y además el número primo 2 se repite infinitas veces, en este trabajo se enuncia y demuestra una fórmula que construye al conjunto de los números primos en forma ordenada y sin repetir ningún elemento.

Una fórmula recursiva de los números primos anteriormente encontrada

Sea $\{p_n\}_{1,2,\ldots,n}$ la sucesión de los números primos entonces, se cumple que:

$$p_n = \left\lfloor 1 - \frac{1}{\log(2)} \cdot \log\left(\sum_{d|M_n} \left(\frac{\mu(d)}{2^d - 1} \right) - \frac{1}{2} \right) \right\rfloor .$$

donde $M_n = \prod_{j=1}^{n-1} p_j$ y μ es la función de Mobius.

Teóricamente hablando esta fórmula es una de las mejores encontradas para el conjunto de los números primos, pues los genera ordenadamente y sin repetir ningún elemento, sin embargo también lo hace en forma recursiva, esta es una fórmula que aparece en mucha de la literatura de texto e investigación sobre teoría de números, esta fórmula tiene mayor complejidad superior a la que se presenta en este trabajo, pues la fórmula utiliza la de Möbius en su definición.

Recordemos que la definición de la función de Möbius es 1 sobre los números naturales libres de cuadrados que tengan un número par de factores primos distintos, toma el valor -1 sobre los números naturales libres de cuadrados que tenga un número M_n impar de factores primos distintos y toma el valor de 0 sobre el número 0, esta función no es elemental pues no se conoce una forma sencilla para determinar cuántos factores primos va a tener un número natural.

La función de Möbius es complicada de evaluar pues no tiene una expresión explícita, eso la hace computacionalmente pesada. Además, como que si no fuera poco los índices del sumatorio se toman sobre un conjunto que no sigue un patrón lineal. El conjunto de los divisores de M_n es complicado de listar para valores grandes y su cardinalidad es orden exponencial.

Una fórmula de representación para los números primos

Sea $\{p_n\}_{1,2,\ldots,n}$ la sucesión de los números primos entonces, aseguramos que:

$$p_n = \left\lfloor 10^{2^n} \cdot c \right\rfloor - 10^{2^{n-1}} \cdot \left\lfloor 10^{2^{n-1}} \cdot c \right\rfloor, \text{ donde } c = \sum_{n=1}^{\infty} \left(\frac{p_n}{10^{2^n}} \right) = 0{,}0203000500000007\ldots$$

Esta fórmula es de representación, en el sentido que el valor de la constante c que no se conoce exactamente (no se conocen todos los números primos), lo que podemos decir es que aunque esta igualdad ha sido presentada como fórmula, realmente se queda a nivel de relación la cual la cumplen los números primos.

2.2. Teorema de Mills

El teorema de Mills afirma que existe una constante θ tal que $\left\lfloor \theta^{3 \cdot n} \right\rfloor$ es un número primo para todos los números naturales $n \geq 1$.

Donde θ indica una constante matemática llamada constante de Mills y $\left\lfloor \theta^{3 \cdot n} \right\rfloor$ indica la función parte entera de $\theta^{3 \cdot n}$. El teorema fue demostrado en 1947 por Mills, quien sin embargo, no determinó el valor de θ, ni propuso ninguna aproximación. Sucesivamente el valor de la constante fue calculado de forma más precisa. A día de hoy, se desconoce su valor exacto, pero si es cierta la hipótesis de Reimann, la constante vale aproximadamente $\theta \approx 1{,}30637788386308069046\ldots$

Esta fórmula no puede generar todos los primos ya que obviamente crece muy rápido.

2.3. Primos en la progresión aritmética $p^a k + 1$ con p primo.

Dada una progresión aritmética $c \cdot k + b$, una pregunta interesante que nos podemos hacer es ¿para qué valores de c y b la progresión contiene infinitos números primos?

Es claro que si el máximo común divisor entre c y b es $(c, b) = d > 1$, entonces la progresión no contiene números primos ya que para todo k, $c \cdot k + b = d \cdot \left(\frac{c}{d} \cdot k + \frac{b}{d} \right)$ es compuesto pues $\frac{c}{d}, \frac{b}{d}$ son números naturales. De ahí se sigue que una condición necesaria para que existan infinitos números primos en la progresión aritmética $c \cdot k + b$ es que $(c, b) = 1$.

En 1837, Lejeune Dirichlet demostró que ésta es tambiéen una condición suficiente. La demostración de Dirichlet no es elemental, ya que usa argumentos de la teoría analítica de números y del análisis. Aquí nos restringimos a demostrar el teorema de Dirichlet de una manera elemental para el caso en que $c = p^a$ y $b = 1$.

En primer lugar mostraremos que, si para todo a existe un número primo de la forma $p^a k + 1$, entonces existen infinitos números primos de la forma $p^a k + 1$. Para ello, procedamos por contradicción. Supongamos que para todo a existe un número primo de la forma $p^a k + 1$. Si hubiera un conjunto finito de números primos de la forma $M = p^a k + 1$, existiera un k máximo tal que M es un número primo. Sea β tal que $p^\beta > M$. Por hipótesis existe un l tal que $p^\beta l + 1$ es primo. Pero $p^\beta l + 1 = p^a (p^{\beta - a} l) + 1$ lo que contradice la suposición de que M sea el mayor primo de esta forma.

Con lo anterior, es suficiente demostrar que la progresión $p^a k + 1$ contiene al menos un número primo. Sean $c = 2^{p^{a-1}}$ y q un divisor primo de $c^{p-1} + c^{p-2} + \ldots + c + 1$. Por el teorema de Fermat sabemos que $2^p \equiv 2 \mod p$ y así $2^{p^a} \equiv 2 \mod p$, $2^{p^a} \equiv 1 \mod q$, de donde $p \neq q$.

Por otra parte q no divide $c - 1$, ya que si $c \equiv 1 \mod q$, entonces $c^{p-1} + c^{p-2} + \ldots + c + 1 \equiv p \equiv 0 \mod q$, lo cual que implica que $p = q$. Por lo tanto, $q \nmid 2^{p^{a-1}} - 1$, así el orden de 2 módulo q es p^a. Aplicando de nuevo el teorema de Fermat, tenemos que $2^{q-1} \equiv 1 \mod q$, Luego $p^a \mid q - 1$, que implica que $q = p^a k + 1$. es un primo de la forma deseada.

2.4. Distribución de primos

Dado un primo $p < n$ es obvio que $p \mid n!$, pero no sabemos de inmediato cuál es la mayor potencia de p que divide a $n!$.

Para calcular tal potencia veamos que para cada i, p^i aparece en el producto $n! = n \times (n-1) \times \cdots \times 2 \times 1$ en los factores $p^i, 2p^i, \ldots, \left\lfloor \frac{n}{p^i} \right\rfloor p^i$. De ahí se sigue que p^i aparece como un divisor de exactamente $\left\lfloor \frac{n}{p^i} \right\rfloor$ números de la lista $1, 2, \ldots, n$. Entonces, si α es la mayor potencia de p que divide a $n!$, tenemos que $\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$, pues cada múltiplo de p^i aporta un factor de p en cada uno de los sumandos $\left\lfloor \frac{n}{p} \right\rfloor, \left\lfloor \frac{n}{p^2} \right\rfloor, \ldots, \left\lfloor \frac{n}{p^i} \right\rfloor$. Notemos que la suma es finita, pues si $k > \log_p(n)$, entonces $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. De esta forma,

$$\alpha = \sum_{i=0}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{i=0}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Teorema 2.4.1 (Teorema de Chebyshev)**.** Para todo entero $m \geq 2$ se cumple que $\prod_{p_j \leq m} p_j < 4^m$.

Demostración. Notemos primero que para m pequeño se comprueba fácilmente tal desigualdad. Además si se demuestra para $m = 2l + 1$ entonces para $m = 2l + 2$ se cumplirá también porque no se agregan primos al producto. Luego, supongamos por hipótesis de inducción que, para todo $k < 2l + 1$, la desigualdad se tiene.

Dado que todo primo p, tal que $l + 1 < p \leq 2l + 1$, se tiene que p divide $(2l + 1)!$ pero no divide $(l + 1)!$, se sigue que

$$\prod_{l+1 < p_j \leq 2l+1} p_j < \binom{2l+1}{l+1} = \binom{2l}{l+1} + \binom{2l}{l} < (1+1)^{2l} = 4^l.$$

Combinando esta desigualdad con la hipótesis de inducción tenemos que

$$\prod_{p_j \leq 2l+1} p_j = \prod_{p_j \leq l+1} p_j \prod_{l+1 < p_j \leq 2l+1} p_j < 4^{l+1} 4^l = 4^{2l+1},$$

que es lo que queríamos demostrar. □

Existen otros resultados sobre la distribución de primos, pero su demostración necesita teoría que está fuera de los objetivos de este trabajo.

Teorema 2.4.2 (Teorema del número primo)**.** Sea $\pi(n)$ el número de primos menores o iguales a n. Entonces la sucesión $\left\{ \frac{\pi(n)\log(n)}{n} \right\}_{n \in \mathbb{N}}$ converge a 1.

En particular este teorema nos está diciendo que podemos acotar la función $\pi(n)$ con la función $\frac{n}{\log(n)}$, es decir que, existen constantes c y C tales que $c\frac{n}{\log(n)} < \pi(n) < C\frac{n}{\log(n)}$.

El Teorema de los números primos es un caso particular de un resultado conocido como Teorema de Dirichlet.

Teorema 2.4.3 (Teorema de Dirichlet)**.** Sean a y b enteros con $(a, b) = 1$ y $\pi_{a,b}(x)$ la función con dominio los reales positivos definida como el número de primos de la forma $a + kb$ con $k \in \mathbb{N}$, dentro del intervalo $[2, x]$. Entonces la sucesión $\left\{ \frac{\pi_{a,b}(n)\log(n)}{n} \right\}_{n \in \mathbb{N}}$ converge $\frac{1}{\phi(b)}$, donde ϕ es la función de Euler.

2.5. Postulado de Bertrand

Dedicamos esta sección a un resultado fundamental en la demostración de la fórmula en el siguiente capítulo, el Postulado de Bertrand permite una mejor comprensión sobre la distribución de los números primos, tener una idea del comportamiento irregular de estos números es una cuestión muy compleja, sin embargo el postulado de Bertrand que se enuncia y demuestra a continuación proporciona una relación entre un primo y su primo antecesor,

dicha regla es que todo primo mayor que 2 es menor que el doble de su primo antecesor, este postulado insinúa que el conjunto de los números primos puede ser construido recursivamente.

En otras palabras el Postulado de Bertrand establece que dado $n \in \mathbb{N}, n \geq 2$, entre n y $2 \cdot n$ siempre hay un número primo. Equivalentemente se tiene que si p es primo entonces el siguiente primo q de p satisface $q < 2 \cdot p$. Para ser capaces de dar una demostración del postulado de Bertrand, necesitamos la siguiente función aritmética.

Definición 2.5.1. Sea $\vartheta : (0, \infty) \to \mathbb{R}, \vartheta(x) = \sum_{p \leqslant x,\, p \text{ primo}} \log(p) = \log\left(\prod_{p \leqslant x} p\right)$.

Para probar esta identidad necesitamos:

Proposición 2.5.2. Se tiene que $\forall n \geq 1 : \vartheta(n) < 2 \cdot n \cdot \log(2)$.

Demostración. Sea $m \in \mathbb{N} \cup \{0\}$

$$M = \binom{2 \cdot m + 1}{m} = \frac{(2 \cdot m + 1)!}{m! \cdot (m+1)!} = \frac{(2 \cdot m + 1) \cdots (m+2)}{m!} \in \mathbb{N}.$$

Ahora $(1+1)^{2 \cdot m + 1} = \sum_{n=0}^{2 \cdot m + 1} \binom{2 \cdot m + 1}{n} > \binom{2 \cdot m + 1}{m} + \binom{2 \cdot m + 1}{m+1} = 2 \cdot M$. Por lo tanto se tiene $M < 2^{2 \cdot m}$. Si $m + 1 < p \leq 2 \cdot m + 1 \Rightarrow p \mid ((2 \cdot m + 1) \cdots (m+2)) \wedge p \nmid m!$ Por lo que $\left(\prod_{m+1 < p \leqslant 2 \cdot m + 1} p\right) \mid M$ y

$$\vartheta(2 \cdot m + 1) - \vartheta(m+1) = \sum_{m+1 < p \leqslant 2 \cdot m + 1} \log(p) \leqslant \log(M) < 2 \cdot m \cdot \log(2).$$

Para $n = 1, 2$ el resultado es trivial. Supongamos cierto el resultado para $n \leqslant n_0 - 1$.

- Si n_0 es par:

$$\vartheta(n_0) = \vartheta(n_0 - 1) < 2 \cdot (n_0 - 1) \cdot \log(2) < 2 \cdot n_0 \cdot \log(2).$$

- Si n_0 es impar, $n_0 = 2 \cdot m + 1$,

$$\begin{aligned}\vartheta(n_0) = \vartheta(2 \cdot m + 1) &= \vartheta(2 \cdot m + 1) - \vartheta(m+1) + \vartheta(m+1) \\ &< 2 \cdot m \cdot \log(2) + 2 \cdot (m+1) \cdot \log(2) \\ &= 2 \cdot (2 \cdot m + 1) \cdot \log(2) = 2 \cdot n_0 \cdot \log(2)\end{aligned}$$

puesto que $m + 1 \leq n$.

En ambos casos $\vartheta(n_0) < 2 \cdot n_0 \cdot \log(2)$. Por lo tanto $\forall n \geq 1 : \vartheta(n) < 2 \cdot n \cdot \log(2)$. □

Teorema 2.5.3 (Postulado de Bertrand)**.** Si $n \geq 1$, entonces existe al menos un número primo p tal que $n < p \leq 2 \cdot n$, esto es, si p_r es el r-ésimo primo, $\forall r \geq 1 : p_{r+1} < 2 \cdot p_r$.

Demostración. Para $n \leqslant 2^9 = 512$, cada primo de los siguientes 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631 es menor que dos veces su predecesor. Por lo tanto podemos tomar $n > 2^9$. Ahora si $p^{\alpha(p)} \mid n!$, $p^{\alpha(p)+1} \nmid n!$, entonces $\alpha(p) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$ pues los números $1, 2, \ldots, n$ incluyen exactamente $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p, $\left\lfloor \frac{n}{p^2} \right\rfloor$ múltiplos de $p^2, \ldots,$ $\left\lfloor \frac{n}{p^i} \right\rfloor$ múltiplos de p^i.

Sea $N = \frac{(2 \cdot n)!}{(n!)^2} = \prod_{p \leqslant 2 \cdot n} p^{k_p}$. Por lo tanto tenemos que $k_p = \sum_{m=1}^{\infty} \left(\left\lfloor \frac{2 \cdot n}{p^m} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^m} \right\rfloor \right)$. Sea p un factor primo de N. Por lo tanto $k_p \geqslant 1$.

Supongamos que no hay ningún primo satisfaciendo $n < p \leq 2 \cdot n$. Entonces $p \leq n$.

Si $\frac{2}{3} \cdot n < p \leq n \Rightarrow 2 \cdot p \leq 2 \cdot n < 3 \cdot pyp^2 > \frac{4}{9} \cdot n^2 > 2 \cdot n$. Se sigue que $k_p = \left\lfloor \frac{2 \cdot n}{p} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p} \right\rfloor = 2 - 2 = 0$, lo cual es una contradicción. Por lo tanto $\forall p \mid N : p \leq \frac{2}{3} \cdot n$. De esta forma obtenemos que

$$\sum_{p \mid N} \log(p) \leq \sum_{p \leq \frac{2}{3} \cdot n} \log(p) = \vartheta\left(\frac{2}{3} \cdot n\right) \leq \frac{4}{3} \cdot n \cdot \log(2) \text{ (Proposición 2.5.2).}$$

Si $k_p \geq 2 \Rightarrow k_p = \sum_{m=1}^{\infty} \left(\left\lfloor \frac{2 \cdot n}{p^m} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^m} \right\rfloor \right)$. Cada término de la suma $\left(\left\lfloor \frac{2 \cdot n}{p^m} \right\rfloor - 2 \cdot \left\lfloor \frac{n}{p^m} \right\rfloor \right)$ es 0 ó 1 correspondientemente en el caso que $\left\lfloor \frac{2 \cdot n}{p^m} \right\rfloor$ sea par o impar. Para $p^m > 2 \cdot n$ el término es 0. Se tiene

$$k_p \leq \sum_{\substack{p^m \leq 2 \cdot n \\ m \cdot \log(p) \leq \log(2 \cdot n)}} 1 \leq \left\lfloor \frac{\log(2 \cdot n)}{\log(p)} \right\rfloor$$

Por lo tanto $2 \cdot \log(p) \leq k_p \cdot \log(p) \leq \log(2 \cdot n) \Rightarrow p \leq \sqrt{2 \cdot n}$. Esto implica que hay a lo más $\sqrt{2 \cdot n}$ valores de p. Ahora se sigue que $\sum_{k_p \geq 2} k_p \cdot \log(p) \leq \left(\sqrt{2 \cdot n} \right) \cdot (\log(2 \cdot n))$. Por lo tanto

$$\begin{aligned} \log(N) &\leq \sum_{k_p=1} \log(p) + \sum_{k_p \geq 2} k_p \cdot \log(p) \\ &\leq \sum_{p|N} \log(p) + \left(\sqrt{2 \cdot n} \right) \cdot (\log(2 \cdot n)) \\ &\leq \frac{4}{3} \cdot n \cdot \log(2) + \left(\sqrt{2 \cdot n} \right) \cdot (\log(2 \cdot n)) . \end{aligned}$$

Ahora $(1+1)^{2 \cdot n} = \sum_{j=0}^{2 \cdot n} \binom{2 \cdot n}{j}$ y $\forall 0 \leq j \leq n : \binom{2 \cdot n}{2 \cdot n - j} = \binom{2 \cdot n}{j} \leq \binom{2 \cdot n}{n} = N$. Por lo tanto $2^{2 \cdot n} \leq 2 \cdot n \cdot N \Rightarrow 2 \cdot n \cdot \log(2) \leq \log(2 \cdot n) + \log(N) \leq \frac{4}{3} \cdot n \cdot \log(2) + \left(1 + \sqrt{2 \cdot n} \right) \cdot (\log(2 \cdot n))$. Se sigue que $\frac{2}{3} \cdot n \cdot \log(2) \leq \left(1 + \sqrt{2 \cdot n} \right) \cdot (\log(2 \cdot n))$ lo cual implica $2 \cdot n \cdot \log(2) \leq 3 \cdot \left(1 + \sqrt{2 \cdot n} \right) \cdot (\log(2 \cdot n))$.

Sea $\xi = \frac{\log(n/512)}{10 \cdot \log(2)} > 0$ lo cual implica $\xi = \frac{\log\left((2 \cdot n)/\left(2^{10}\right)\right)}{\log\left(2^{10}\right)} = \frac{\log(2 \cdot n)}{\log\left(2^{10}\right)} - 1$ por lo tanto

$\xi + 1 = \dfrac{\log(2 \cdot n)}{\log\left(2^{10}\right)} \Rightarrow \log\left(2^{10 \cdot (\xi+1)}\right) = \log(2 \cdot n)$ de donde se sigue $2 \cdot n = 2^{10 \cdot (1+\xi)}$.

Por lo tanto $2 \cdot n \cdot \log(2) \leq 3 \cdot \left(1 + \sqrt{2 \cdot n}\right) \cdot (\log(2 \cdot n))$ toma la forma $2^{10 \cdot (1+\xi)} \leq 30 \cdot (1 + \xi) \cdot \left(1 + 2^{5 \cdot (1+\xi)}\right)$.

Se sigue que $2^{5 \cdot \xi} = 2^{10 \cdot (1+\xi)} \cdot 2^{-5 \cdot \xi} \cdot 2^{-10} \leq 30 \cdot 2^{-5} \cdot (1 + \xi) \cdot \left(2^{-5-5 \cdot \xi} + 1\right)$.

Puesto que $30 \cdot 2^{-5} = \dfrac{30}{32} < 1 - 2^{-5} = 1 - \dfrac{1}{32}$ y $2^{-5-5 \cdot \xi} + 1 < 1 + 2^{-5}$, entonces

$2^{5 \cdot \xi} < \left(1 - 2^{-5}\right) \cdot \left(1 + 2^{-5}\right) \cdot (1 + \xi) = \left(1 - 2^{-10}\right) \cdot (1 + \xi) < 1 + \xi$. Por lo tanto $2^{5 \cdot \xi} < 1 + \xi$.

Por otro lado $2^{5 \cdot \xi} = 2^{5 \cdot \xi \cdot \log(2)} > 1 + 5 \cdot \xi \cdot \log(2) > 1 + \xi$, lo cual es un absurdo.

Problema 2.5.1. Sean n y k enteros positivos tales $n > 2^k$. Demostrar que los primeros k números que son mayores que n y primos relativos con $n!$ son primos.

Solución. Como $n > 2^k$ se sigue que $n^2 > 2^k n$. Entonces por el postulado de Bertrand tenemos que entre cada dos términos consecutivos de la sucesión $n, 2n, 4n, \ldots, 2^k n$ existe al menos un primo. Así entre n y n^2 existen al menos k primos. En Particular, los k menores números que son mayores que n y que son primos relativos con $n!$ están entre n y n^2 .Si uno de tales números no fuese primo, digamos$l = ab$, y suponiendo que $a \leq b$, tendríamos que $a^2 \leq l \leq n^2$. Luego $a < n$, lo que contradice el hecho de que $n!$ y l son primos relativos. □

□

3. Formulación recursiva para el conjunto de los números primos

En este capítulo se enuncia y demuestra una construcción recursiva del conjunto de los números primos.

Esta fórmula nace con una idea muy intuitiva e inductiva: Conocemos los primeros números primos 2, 3, ..., supongamos que podemos conocer el $m-$ésimo primos p_m, entonces qué cantidad g_m debemos sumar a p_m para obtener el siguiente número primo, i.e. ¿Quién es g_m tal que $p_{m+1} = p_m + g_m$?

En este trabajo exhibimos una fórmula que teóricamente permite calcular para todo número natural m a g_m, dándonos así una construcción recursiva del conjunto de los números primos, esta fórmula es una directa aplicación del postulado de Bertrand. Este Postulado en la mayoría de textos de teoría de números simplemente se enuncia y demuestra, pero en la literatura clásica rara vez se ve su aplicación, aquí tratamos de utilizar su fuerza para cumplir nuestros objetivos, en este sentido la idea es enunciar y demostrar la fórmula que proponemos como una clara y aplicación directa de este postulado.

El interés propio que tiene este postulado en nuestro trabajo es sorprendente, pues es la herramienta fundamental para linealizar el conjunto de los números primos utilizando el aritmética modular. Esta linealización es un procedimiento común en matemática, por ejemplo, el conjunto funciones pueden ser linealizadas localmente por medio de la derivada, la idea de conjunto puede ser linealizada por medio de los espacios vectoriales, también muchas ecuaciones diferenciales pueden ser resueltas mediante una combinación lineal infinita de funciones más suaves, y muchos más objetos pueden ser mejor estudiados cuando se linealizan, así pues, la linealización extrae de lo caótico en los objetos las propiedades mejor estudiables.

La fórmula que se propone no es otra cosa más que el mínimo de una función lineal por tramos sobre un hiperparalelepípedo tomando en cuenta sus puntos reticulares, la idea de número primo también se puede linealizar, como veremos a continuación.

3.1. Fórmula recursiva de los números primos

En este sesión vamos a exponer y formular los dos teoremas que nos permiten definir una fórmula de los números primos

Teorema 3.1.1 (Criba de Eratóstenes)**.** Sea $p \in \mathbb{N}, r \in \mathbb{R}$ tal que $r \geq \sqrt{p}$ entonces, p es primo si y solo si el conjunto $\{q \text{ primo} : q \mid p, q \neq p \wedge q \leq r\} = \emptyset$.

Demostración. "$\Rightarrow$" Sea $A = \{q \text{ primo} : q \mid p, q \neq p \wedge q \leq r\}$, tenemos que p es primo. A fines de contradicción supongamos que $A \neq \emptyset$, entonces $\exists q \in P : q \mid p, q \neq p \wedge q \leq r$. Luego como p es primo que divide a q y q es primo también, entonces se debe tener que $q = p$, pero esto es un absurdo pues $q \neq p$, así entonces tenemos que $A = \emptyset$.

"$\Leftarrow$" Ahora tenemos que $A = \emptyset$. A fines de contradicción supongamos que p no es primo, entonces $\exists q \in P : q \mid p \wedge 1 < q < p$, luego como $A = \emptyset$ se debe tener que $q \notin A$, esto implica que $q > r \geq \sqrt{p}$, entonces $q > \sqrt{p}$ por lo tanto $q^2 > p$. Luego como $q \mid p \wedge 1 < q < p$, entonces existe $d \in \mathbb{Z} : 1 < d < p \wedge p = q \cdot d$, entonces $q = \dfrac{p}{d}$, esto implica que $\dfrac{p^2}{d^2} > p$, así tenemos entonces que $p > d^2$, por lo tanto $\sqrt{p} > d > 1$, luego como $d > 1$, entonces $\exists p_0 \in P : p_0 \mid d$, entonces $p_0 \leq d < \sqrt{p} \leq r$, luego como $d \mid p \wedge p_0 \mid d$, entonces $p_0 \mid p$, luego como $d < p$, esto implica que $p_0 < p$, entonces $p_0 \neq p$ por lo tanto así garantizamos que $p_0 \in A = \emptyset$ y esto es un absurdo. Por lo tanto así concluimos que p es primo.

Y así probamos el teorema. □

Teorema 3.1.2. Sea $\{p_n\}_{n\in\mathbb{N}}$ la sucesión de los números primos entonces,

$$p_1 = 2,$$

$$p_2 = 3,$$

$$\forall n \in \mathbb{N}, n \geq 2 : p_{n+1} = \min_{(t_1,\ldots,t_n)\in D} \left(\sum_{j=1}^{n} \left(\left(\frac{M}{p_j} \right)^{p_j - 1} \cdot t_j \right) - M \cdot \left\lfloor \frac{\sum_{j=1}^{n} \left(\left(\frac{M}{p_j} \right)^{p_j-1} \cdot t_j \right) - p_n}{M} \right\rfloor \right),$$

En donde:

$$M = \prod_{i=1}^{n} p_i;$$

$$D = \{(t_1, \ldots, t_n) \in \mathbb{N}^n \text{ tal que } \forall i = 1, \ldots, n : 1 \leq t_i \leq p_i - 1\};$$

$$\lfloor \bullet \rfloor : \mathbb{R} \to \mathbb{Z} \text{ tal que } \lfloor x \rfloor = \text{máx}\{k \in \mathbb{Z} : k \leq x\}$$

3.2. Demostración de la existencia de una fórmula que construye recursivamente a los primos

Basta con probar el teorema para demostrar la existencia de dicha fórmula.

Demostración de . Sea $f : D \to \mathbb{Z}$ tal que

$$f(t_1, \ldots, t_n) = \sum_{j=1}^{n} \left(\left(\frac{M}{p_j} \right)^{p_j - 1} \cdot t_j \right) - M \cdot \left\lfloor \frac{\sum_{j=1}^{n} \left(\left(\frac{M}{p_j} \right)^{p_j-1} \cdot t_j \right) - p_n}{M} \right\rfloor$$

Definimos un conjunto B tal que $B := f(D)$. Observamos que $|D| = \prod_{i=1}^{n} (p_i - 1) < \infty$, por lo tanto $|B| = |f(D)| \leq |D| < \infty$, por lo tanto el conjunto B es finito y no vacío, así entonces aseguramos que B tiene un mínimo valor, es decir $\exists z \in \mathbb{Z} : z = \min B$. Por lo tanto

debemos probar que $\forall n \in \mathbb{N}, n \geq 2 : p_{n+1} = z = \min B$, para ello haremos lo siguiente:

Sea $n \in \mathbb{N}$ tal que $n \geq 2$, Por el teorema 3.1.1 tenemos que

$$\forall r \geq \sqrt{(p_{n+1})} : A(r) = \{q \text{ primo} : q \mid p_{n+1}, q \neq p_{n+1} \wedge q \leq r\} = \emptyset.$$

Por el postulado de Bertrand podemos garantizar que

$$p_{n+1} < 2 \cdot p_n \Rightarrow \sqrt{(p_{n+1})} < \sqrt{(2 \cdot p_n)} \leq \sqrt{(p_n \cdot p_n)} = \sqrt{\left((p_n)^2\right)} = p_n,$$

así entonces tenemos que $p_n \geq \sqrt{(p_{n+1})}$. Luego tomando $r = p_n$ se tiene que el conjunto $A(p_n) = \{q \text{ primo} : q \mid p_{n+1}, q \neq p_{n+1} \wedge q \leq p_n\} = \emptyset$, luego esto nos garantiza que $\forall j = 1, \ldots, n : p_j \nmid p_{n+1}$.

Por lo tanto $\exists \left(t_1^0, \ldots, t_n^0\right) \in D$ tal que

$$\begin{aligned} p_{n+1} &\equiv t_1^0 \mod p_1 \\ &\vdots \\ p_{n+1} &\equiv t_n^0 \mod p_n \end{aligned}.$$

Luego por el teorema chino del resto tenemos que:

$$p_{n+1} \equiv \sum_{j=1}^{n} \left(t_j^0 \cdot b_j \cdot \left(\frac{M}{p_j} \right) \right) \mod M$$

para todo $b_j \in \mathbb{Z}$ tal que $\forall j = 1, \ldots, n : b_j \cdot \left(\frac{M}{P_j} \right) \equiv 1 \mod p_j$.

Puesto que $\forall j = 1, \ldots, n : \left(\frac{M}{p_j}, p_j \right) = 1$ el pequeño teorema de Fermat nos garantiza que

$\forall j = 1, \ldots, n : \left(\frac{M}{p_j}\right)^{p_j - 1} \equiv 1 \mod p_j$ por lo tanto $\forall j = 1, \ldots, n : \left(\frac{M}{p_j}\right)^{p_j - 2} \cdot \left(\frac{M}{p_j}\right) \equiv 1$ mód p_j.

Así que en particular si $\forall j = 1, \ldots, n : b_j = \left(\frac{M}{p_j}\right)^{p_j - 2}$ entonces, de nuevo el teorema chino del resto nos asegura que:

$$p_{n+1} \equiv \sum_{j=1}^{n} \left(t_j^0 \cdot \left(\frac{M}{p_j}\right)^{p_j - 2} \cdot \left(\frac{M}{p_j}\right) \right) = \sum_{j=1}^{n} \left(t_j^0 \cdot \left(\frac{M}{p_j}\right)^{p_j - 1} \right) \mod M.$$

Así entonces garantizamos que $\exists \left(t_1^0, \ldots, t_n^0\right) \in D$ y un entero $k \in \mathbb{Z}$ tales que

$$p_{n+1} = \sum_{j=1}^{n} \left(t_j^0 \cdot \left(\frac{M}{p_j}\right)^{p_j - 1} \right) + M \cdot k.$$

Sea ahora $Q = \sum_{j=1}^{n} \left(t_j^0 \cdot \left(\frac{M}{p_j}\right)^{p_j - 1} \right)$. El postulado de Bertrand nos garantiza que:

$$\begin{aligned} p_n < p_{n+1} < 2 \cdot p_n &\Rightarrow p_n < Q + M \cdot k < 2 \cdot p_n \\ &\Rightarrow p_n - Q < M \cdot k < 2 \cdot p_n - Q \\ &\Rightarrow \frac{p_n - Q}{M} < k < \frac{2 \cdot p_n - Q}{M}. \end{aligned}$$

Por lo tanto así aseguramos que $ceil\left(\frac{p_n - Q}{M}\right) \leq k \leq \left\lfloor \frac{2 \cdot p_n - Q}{M} \right\rfloor$.

Así entonces tenemos que $ceil\left(\frac{p_n - Q}{M}\right) \leq \left\lfloor \frac{2 \cdot p_n - Q}{M} \right\rfloor$.

Ahora aplicando las propiedades de las funciones parte entera mencionadas en el capítulo 1

tenemos que

$$\begin{aligned}\left\lfloor \frac{2\cdot p_n - Q}{M} \right\rfloor - ceil\left(\frac{p_n - Q}{M}\right) &= \left\lfloor \frac{2\cdot p_n - Q}{M} \right\rfloor - \left(-\left\lfloor \frac{Q - p_n}{M} \right\rfloor\right) \\ &= \left\lfloor \frac{2\cdot p_n - Q}{M} \right\rfloor + \left\lfloor \frac{Q - p_n}{M} \right\rfloor \leq \left\lfloor \frac{2\cdot p_n - Q}{M} + \frac{Q - p_n}{M} \right\rfloor \\ &= \left\lfloor \frac{2\cdot p_n - Q + Q - p_n}{M} \right\rfloor = \left\lfloor \frac{p_n}{M} \right\rfloor \\ &= 0 \text{ pues } \forall n \in \mathbb{N}, n \geq 2 : p_n < M.\end{aligned}$$

Así entonces garantizamos que $\left\lfloor \frac{2\cdot p_n - Q}{M} \right\rfloor - ceil\left(\frac{p_n - Q}{M}\right) \leq 0$, lo que es equivalente que $\left\lfloor \frac{2\cdot p_n - Q}{M} \right\rfloor \leq ceil\left(\frac{p_n - Q}{M}\right)$.

Así que por lo tanto se concluye que

$$\left\lfloor \frac{2\cdot p_n - Q}{M} \right\rfloor = ceil\left(\frac{p_n - Q}{M}\right).$$

Luego esto nos asegura que $k = ceil\left(\frac{p_n - Q}{M}\right) = -\left\lfloor \frac{Q - p_n}{M} \right\rfloor$.

Por lo tanto tenemos que

$$\begin{aligned}p_{n+1} &= Q - M \cdot \left\lfloor \frac{Q - p_n}{M} \right\rfloor \\ &= \sum_{j=1}^{n} \left(\left(\frac{M}{p_j}\right)^{p_j - 1} \cdot t_j^0 \right) - M \cdot \left\lfloor \frac{\sum_{j=1}^{n} \left(\left(\frac{M}{p_j}\right)^{p_j - 1} \cdot t_j^0 \right) - p_n}{M} \right\rfloor \\ &= f\left(t_1^0, \ldots, t_n^0\right) \in f(D) = B.\end{aligned}$$

Por lo tanto $p_{n+1} \in B$, entonces así tenemos que $p_{n+1} \geq z = \min B$.

Ahora supongamos a fines de contradicción que $p_{n+1} > z = \min B$. Esto que implica que p_{n+1} no puede ser una cota inferior del conjunto $f(D)$. Por lo tanto existe $(t_1^1, \ldots, t_n^1) \in D$

tal que

$$p_{n+1} > f\left(t_1^1, \ldots, t_n^1\right) = H - M \cdot \left\lfloor \frac{H - p_n}{M} \right\rfloor, \text{ donde } H = \sum_{j=1}^{n} \left(t_j^1 \cdot \left(\frac{M}{p_j} \right)^{p_j - 1} \right).$$

Luego como $\left\lfloor \frac{H - p_n}{M} \right\rfloor \leq \frac{H - p_n}{M}$ entonces esto implica que

$$H - M \cdot \left\lfloor \frac{H - p_n}{M} \right\rfloor \geq H - M \cdot \left(\frac{H - p_n}{M} \right) = H - (H - p_n) = p_n.$$

Así entonces garantizamos $p_{n+1} > f\left(t_1^1, \ldots, t_n^1\right) = H - M \cdot \left\lfloor \frac{H - p_n}{M} \right\rfloor \geq p_n$.

Ahora probaremos que $f\left(t_1^1, \ldots, t_n^1\right)$ que es un número primo, para ello supondremos lo contrario.

Supongamos que $f\left(t_1^1, \ldots, t_n^1\right)$ no es primo,ahora por el postulado de Bertrand tenemos que

$$\sqrt{\left(f\left(t_1^1, \ldots, t_n^1\right)\right)} < \sqrt{(p_{n+1})} < \sqrt{(2 \cdot p_n)} \leq \sqrt{(p_n \cdot p_n)} = \sqrt{\left((p_n)^2\right)} = p_n.$$

Luego por el teorema 3.1.1 garantizamos que

$$\left\{ q \text{ primo} : q \mid f\left(t_1^1, \ldots, t_n^1\right), q \neq f\left(t_1^1, \ldots, t_n^1\right) \wedge q \leq p_n \right\} \neq \emptyset.$$

Luego esto nos asegura que existe un primo $q \in \{p_1, \ldots, p_n\}$:

$$q \mid f\left(t_1^1, \ldots, t_n^1\right) \wedge q \neq f\left(t_1^1, \ldots, t_n^1\right).$$

Por lo tanto $q \mid f\left(t_1^1, \ldots, t_n^1\right) = H - M \cdot \left\lfloor \frac{H - p_n}{M} \right\rfloor$.

Ahora como $q \in \{p_1, \ldots, p_n\}$ entonces esto implica que $q \mid M$.

Por lo tanto tenemos que $q \mid H = \sum_{j=1}^{n} \left(t_j^1 \cdot \left(\frac{M}{p_j} \right)^{p_j - 1} \right)$.

Ya que $q \in \{p_1, \ldots, p_n\}$ entonces esto nos garantiza que existe $s \in \{1, \ldots, n\} : q = p_s$. Es claro que $\forall j \neq s, j = 1, \ldots, n : p_s = q \mid \left(t_j^1 \cdot \left(\frac{M}{p_j} \right)^{p_j - 1} \right)$ y $\left(\left(\frac{M}{p_s} \right), p_s \right) = 1$. Luego como $q \mid H$ esto nos garantiza que

$$p_s = q \mid \left(t_s^1 \cdot \left(\frac{M}{p_s} \right)^{p_s - 1} \right).$$

El pequeño teorema de Fermat nos asegura que $\left(\frac{M}{p_s} \right)^{p_s - 1} \equiv 1 \mod p_s$.

Por lo tanto $\left(\frac{M}{p_s} \right)^{p_s - 1} \cdot t_s^1 \equiv t_s^1 \mod p_s$, luego como $p_s = q \mid \left(t_s^1 \cdot \left(\frac{M}{p_s} \right)^{p_s - 1} \right)$, entonces esto nos asegura que $p_s \mid t_s^1$. Pero esto es un absurdo porque $1 \leq t_s^1 \leq p_s - 1$.

Así entonces garantizamos que justamente $f\left(t_1^1, \ldots, t_n^1\right)$ es un número primo.

Luego como $p_{n+1} > f\left(t_1^1, \ldots, t_n^1\right) = H - M \cdot \left\lfloor \frac{H - p_n}{M} \right\rfloor \geq p_n$, entonces esto implica que

$f\left(t_1^1, \ldots, t_n^1\right) = p_n$ por lo tanto $p_n \mid f\left(t_1^1, \ldots, t_n^1\right) = H - M \cdot \left\lfloor \frac{H - p_n}{M} \right\rfloor$. Ahora como $p_n \in \{p_1, \ldots, p_n\}$ entonces esto implica que $p_n \mid M$.

Por lo tanto tenemos que

$$p_n \mid H = \sum_{j=1}^{n} \left(t_j^1 \cdot \left(\frac{M}{p_j} \right)^{p_j - 1} \right).$$

Es claro que $\forall j \neq n, j = 1, \ldots, n : p_n \mid \left(t_j^1 \cdot \left(\frac{M}{p_j} \right)^{p_j - 1} \right)$ y $\left(\left(\frac{M}{p_n} \right), p_n \right) = 1$.

Luego como $p_n \mid H$ esto nos garantiza que $p_n \mid \left(t_n^1 \cdot \left(\frac{M}{p_n} \right)^{p_n - 1} \right)$.

El pequeño teorema de Fermat nos asegura que $\left(\frac{M}{p_n} \right)^{p_n - 1} \equiv 1 \mod p_n$.

Por lo tanto $\left(\frac{M}{p_n} \right)^{p_n - 1} \cdot t_n^1 \equiv t_n^1 \mod p_n$, luego como $p_n \mid \left(t_n^1 \cdot \left(\frac{M}{p_n} \right)^{p_n - 1} \right)$, entonces esto nos asegura que $p_n \mid t_n^1$. Pero esto es un absurdo porque $1 \leq t_n^1 \leq p_n - 1$ .Así entonces garantizamos que no debe suceder que $p_{n+1} > z = \min B$, por lo tanto aseguramos que $p_{n+1} = \min f(D)$. □

Esto prueba el resultado principal de este trabajo y concluimos que:

Si $\{p_n\}_{n \in \mathbb{N}}$ la sucesión de los números primos entonces,

$$
\begin{aligned}
p_1 &= 2, \\
p_2 &= 3, \\
\forall n \in \mathbb{N}, n \geq 2 : p_{n+1} &= \min_{(t_1, \ldots, t_n) \in D} \left(\sum_{j=1}^{n} \left(\left(\frac{M}{p_j} \right)^{p_j - 1} \cdot t_j \right) - M \cdot \left\lfloor \frac{\sum_{j=1}^{n} \left(\left(\frac{M}{p_j} \right)^{p_j - 1} \cdot t_j \right) - p_n}{M} \right\rfloor \right),
\end{aligned}
$$

En donde:

$$
\begin{aligned}
M &= \prod_{i=1}^{n} p_i; \\
D &= \{ (t_1, \ldots, t_n) \in \mathbb{N}^n \text{ tal que } \forall i = 1, \ldots, n : 1 \leq t_i \leq p_i - 1 \}; \\
\lfloor \bullet \rfloor &: \mathbb{R} \to \mathbb{Z} \text{ tal que } \lfloor x \rfloor = \max\{ k \in \mathbb{Z} : k \leq x \}
\end{aligned}
$$

3.3. Ejemplos

Ejemplo 3.3.1. Tenemos que $p_1 = 2$, $p_2 = 3$, usaremos nuestro resultado para encontrar p_3. En este caso tenemos que $M = 2 \cdot 3 = 6$; $D = \left\{(t_1, t_2) \in \mathbb{N}^2 : 1 \leq t_1 \leq 1, 1 \leq t_2 \leq 2\right\} = \{(1,1), (1,2)\}$;

$$f(t_1, t_2) = \sum_{j=1}^{2} \left(\left(\frac{6}{p_j} \right)^{p_j - 1} \cdot t_j \right) - 6 \cdot \left\lfloor \frac{\sum_{j=1}^{2} \left(\left(\frac{6}{p_j} \right)^{p_j - 1} \cdot t_j \right) - 3}{6} \right\rfloor = 3 \cdot t_1 + 4 \cdot t_2 - 6 \cdot \left\lfloor \frac{3 \cdot t_1 + 4 \cdot t_2 - 3}{6} \right\rfloor$$ por lo tanto tenemos que $f(D) = \{f(1,1), f(1,2)\}$, haciendo los cálculos tenemos que:

$f(1,1) = 7 - 6 \cdot \left\lfloor \frac{4}{6} \right\rfloor = 7 - 0 = 7$; $f(1,2) = 11 - 6 \cdot \left\lfloor \frac{8}{6} \right\rfloor = 11 - 6 \cdot 1 = 5$, Así por lo tanto tenemos que

$f(D) = \{7, 5\}$. Por lo tanto aplicando nuestro resultado tenemos que

$p_3 = \text{mín}\, f(D) = \text{mín}\{7, 5\} = 5$, Así concluimos que $p_3 = 5$.

Ejemplo 3.3.2. Ahora encontraremos p_4.Tenemos que $p_1 = 2$, $p_2 = 3$, $p_3 = 5$; $M = 2 \cdot 3 \cdot 5 = 30$;

$D = \left\{(t_1, t_2, t_3) \in \mathbb{N}^3 : 1 \leq t_1 \leq 1, 1 \leq t_2 \leq 2, 1 \leq t_3 \leq 4\right\}$. Por lo tanto se va a tener que

$$D = \{(1,1,1), (1,1,2), (1,1,3), (1,1,4), (1,2,1), (1,2,2), (1,2,3), (1,2,4)\};$$

$$f(t_1,t_2,t_3) = \sum_{j=1}^{3}\left(\left(\frac{30}{p_j}\right)^{p_j-1}\cdot t_j\right) - 30\cdot\left\lfloor\frac{\sum_{j=1}^{3}\left(\left(\frac{30}{p_j}\right)^{p_j-1}\cdot t_j\right)-5}{30}\right\rfloor$$
$$= 15\cdot t_1 + 100\cdot t_2 + 1296\cdot t_3 - 30\cdot\left\lfloor\frac{15\cdot t_1+100\cdot t_2+1296\cdot t_3-5}{30}\right\rfloor.$$

Por lo tanto

$$f(D) = \{f(1,1,1), f(1,1,2), f(1,1,3), f(1,1,4), f(1,2,1), f(1,2,2), f(1,2,3), f(1,2,4)\}.$$

Haciendo los cálculos se tiene que:

$$f(1,1,1) = 1411 - 30\cdot\left\lfloor\frac{1406}{30}\right\rfloor = 1411 - 30\cdot 46 = 31;$$
$$f(1,1,2) = 2707 - 30\cdot\left\lfloor\frac{2702}{30}\right\rfloor = 2707 - 30\cdot 90 = 7;$$
$$f(1,1,3) = 4003 - 30\cdot\left\lfloor\frac{3998}{30}\right\rfloor = 4003 - 30\cdot 133 = 13;$$
$$f(1,1,4) = 5299 - 30\cdot\left\lfloor\frac{5294}{30}\right\rfloor = 5299 - 30\cdot 176 = 19;$$
$$f(1,2,1) = 1511 - 30\cdot\left\lfloor\frac{1506}{30}\right\rfloor = 1511 - 30\cdot 50 = 11;$$
$$f(1,2,2) = 2807 - 30\cdot\left\lfloor\frac{2802}{30}\right\rfloor = 2807 - 30\cdot 93 = 17;$$
$$f(1,2,3) = 4103 - 30\cdot\left\lfloor\frac{4098}{30}\right\rfloor = 4103 - 30\cdot 136 = 23;$$
$$f(1,2,4) = 5399 - 30\cdot\left\lfloor\frac{5394}{30}\right\rfloor = 5399 - 30\cdot 179 = 29.$$

Así entonces tenemos que $f(D) = \{31, 7, 13, 19, 11, 17, 23, 29\}$.

Por lo tanto aplicando nuestro resultado tenemos que $p_4 = \text{mín}\, f(D) = 7$.

Conclusiones y Recomendaciones

En base a la teoría expuesta en la investigación desarrollada, puede concluirse que:

- Se lograron los objetivos planteados: encontrar una fórmula recursiva de los números primos, mostrar mediante esta teoría desarrollada lo profundo de la teoría de las congruencias mediante el empleo del teorema chino del resto y dar una aplicación del postulado de Bertrand, efectivamente la fórmula es una aplicación de dicho postulado.
- Exponer la importancia que se tendría conocer los métodos de optimización para tratar más a fondo la fórmula, pues el problema se trata de encontrar un mínimo valor de una función. La fórmula por si sola dice eso.
- Haber elaborado un recurso bibliográfico de apoyo y consulta disponible a todos los estudiantes al cual puedan recurrir y extraer información que consideren pertinente según sus necesidades académicas.

En esta obra se expone una forma de construir recursivamente la sucesión de los números primos.

Se ha estudiado la teoría básica de números y el postulado de Bertrand como parte de ella para poder comprender el procedimiento que se hizo para encontrar la fórmula de los números primos.

También se hacen las siguientes recomendaciones y consideraciones:

- Se recomienda al lector interesado en este escrito comprender cada uno de los resultados

y técnicas expuestas para poder darse cuenta de lo maravillosa que es la fórmula encontrada en esta obra y así motivarlo más a mejorarla.

- Seguir estudiando esta línea de trabajo y dar continuidad a esta investigación: por ejemplo estudiar los métodos de optimización para poder encontrar más generalmente el mínimo valor de la función definida en la demostración del teorema principal de esta obra.

Bibliografía

[1] Selberg. Atle. *An elementary proof of the prime number theorem.* Langesund, Noruega, 1949.

[2] Chris Caldwell. *Proof of fermat little theorem. The primes page.* Massachusetts, USA: Harvard Colleg., 1994.

[3] Weisstein EricW. *Congruences.* Bloomington, Indiana,USA: math world wolfram reserch, 1989.

[4] Samuel Horsley. *The sieve of eratosthenes. Being a Account of his method of finding all the prime numbers.* Billerica, Massachusetts, USA, 1772.

[5] Fabio E. Brochero Martínez & Juan Ignacio Restrepo Lozano. *un recorrido por la teoría de números: 25 años de olimpiadas colombianas de matemáticas.* Colombia, Universidad Antonio Nariño, 2006.

[6] Koblitz Neal. *A course in number theory and criptography.* New York, USA: University Week, 1998.

[7] Mario A. Ruiz. *Apuntes Teoría de Números.* El Salvador, Universidad de El Salvador, 2014.

[8] James P. Jones & Daihachiro Sato & Hideo Wada & Douglas Wiens. *Diophantine representation of the set of prime numbers.* v. 83, págs. 449 - 464. American Mathematical Monthly 83. The Official Journal of the Mathematical Association of America, 1976.