Acta de Correcciones al Proyecto de Grado
Matemáticas Aplicadas

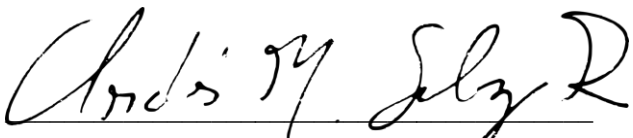
Fecha: junio 10 de 2021

Autores: CRISTHIAN ANDRÉS VALOR GARCÍA

Nombre del Proyecto de Grado: NÚMEROS PRIMOS EN LA SECUENCIA 6K ± 1

Director: ANDRÉS MAURICIO SALAZAR ROJAS

Como indica el artículo 2.27 de las Directrices de Trabajo de Grado, he verificado que los estudiantes indicados arriba han implementado todas las correcciones que los Jurados del Proyecto de Grado definieron que se efectuaran, como consta en el Acta de Calificación correspondiente.



Firma de Director(a) del Proyecto de Grado

Nota de Aceptación

Aprobado por el Comité de Trabajo de Grado en cumplimiento de los requisitos exigidos por la Pontificia Universidad Javeriana para optar el título de Profesional en Matemáticas Aplicadas.

Hernán Camilo Rocha Niño
Decano de la Facultad de Ingeniería y Ciencias

Diana Haidive Bueno Carreño
Directora Carrera de Matemáticas Aplicadas

Andrés Mauricio Salazar Rojas
Director(a) Trabajo

Diana Haidive Bueno Carreño
Jurado 1

Michell Andrés Gómez Leiva
Jurado 2

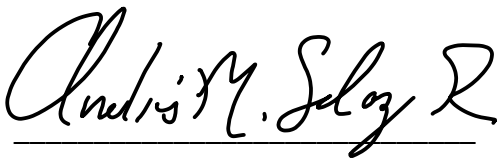
Santiago de Cali, abril 30 de 2021

Doctora
DIANA HAIDIVE BUENO
Directora de la carrera de Matemáticas Aplicadas
PONTIFICIA UNIVERSIDAD JAVERIANA CALI

Cordial saludo,

Por medio de la presente me permito informarle que el estudiante **CRISTHIAN ANDRÉS VALOR GARCÍA** con código **8936525,** trabajó y finalizó bajo mi dirección, el proyecto de grado denominado "**NÚMEROS PRIMOS EN LA SECUENCIA 6k ± 1"**, el cual considero se encuentra en condiciones para ser sometido a evaluación.

Atentamente



ANDRÉS MAURICIO SALAZAR ROJAS
Director del proyecto de grado
Departamento de Ciencias Naturales y Matemáticas

NÚMEROS PRIMOS EN LA SECUENCIA $6k \pm 1$

CRISTHIAN ANDRÉS VALOR GARCÍA

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA Y CIENCIAS
SANTIAGO DE CALI
2021

NÚMEROS PRIMOS EN LA SECUENCIA $6k \pm 1$

CRISTHIAN ANDRÉS VALOR GARCÍA

Trabajo de grado para optar por el título de profesional
en Matemáticas Aplicadas

PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERÍA Y CIENCIAS
SANTIAGO DE CALI
2021

Índice general

Resumen

En este trabajo se encuentra una fórmula explícita para determinar $\pi(n)$ a partir del cálculo de $\pi(n;6,1)$ y $\pi(n;6,5)$, empleando para ello el Principio de inclusión–exclusión a los conjuntos $\{6k+1\}$ y $\{6k+5\}$ al suprimir de estos el número de múltiplos de primos. También se encuentran dos identidades para los residuos entre Q^2 y $6Q$, al igual que para $5Q^2$ y $6Q$, siendo Q elementos de la forma, producto entre uno, dos o más primos menores o iguales que un cierto n.

Abstract

In this paper we find an explicit formula to determine $\pi(n)$ from the calculation of $\pi(n;6,1)$ and $\pi(n;6,5)$, employing for this purpose the Principle of inclusion–exclusion to the sets $\{6k+1\}$ and $\{6k+5\}$ by suppressing from these the number of multiples of primes. Two identities are also found for the residues between Q^2 and $6Q$, as well as for $5Q^2$ and $6Q$, with Q being elements of the form, product between one, two or more primes less than or equal to a certain n..

Introducción

Determinar el número de primos menores o iguales que un cierto n, en notación $\pi(n)$, plantea uno de los grandes desafíos de la matemática, esto debido a que no se conoce hasta la fecha una distribución precisa sobre los números primos, y es bien conocido que se pueden encontrar espacios de k enteros entre dos primos consecutivos, véase referencias [1] y [2].

Con este interesante y desafiante panorama matemático, en este trabajo se presenta una expresión para $\pi(n)$, y dos identidades que se desprenden de la misma.

El documento se ha divido en dos partes, en la primera se presentan algunos resultados clásicos de la teoría de números, como la existencia de soluciones de sistemas de ecuaciones modulares y el Teorema de Euler–Fermat. También se revisan algunos resultados sobre el comportamiento de los números primos en las secuencias $\{6k+1\}$ y $\{6k-1\}$.

En la segunda parte del documento, se presentan los resultados del trabajo de investigación, aquí se determina la fórmula explícita para $\pi(n)$ a partir del cálculo de $\pi(n;6,1)$ y $\pi(n;6,5)$, empleando para ello el Principio de inclusión–exclusión a los conjuntos $\{6k+1\}$ y $\{6k+5\}$, al suprimir de estos el número de múltiplos de primos. También se encuentran dos identidades para los residuos entre Q^2 y $6Q$, al igual que para $5Q^2$ y $6Q$, siendo Q elementos de la forma, producto entre uno, dos o más primos menores o iguales que un cierto n. Es importante mencionar que hasta donde se tiene información, los resultados reportados en el documento, no se han encontrado en la literatura.

1 Marco teórico

En el siguiente capítulo se presentan algunas definiciones y resultados clásicos de la teoría de números. Invitamos al lector interesado en profundizar sobre estos temas a consultar las referencias [1] y [2].

1.1 Números primos

A partir de este momento las letras minúsculas como a,b,c,d,k,m,n,p,q y r, representarán hasta que se diga lo contrario, números enteros.

1.1.1 Definición. Diremos que un número p divide a q, en notación $p|q$, si $q = kp$ para algún k. De no existir dicho entero k, diremos que p no divide a q, lo que se representa como $p \nmid q$.
Se puede comprobar que la divisibilidad es una relación reflexiva, transitiva y lineal, ésto último en el sentido de que

$$\text{Si } a|b \text{ y } a|c \text{ entonces } a|(pb + qc).$$

Si un número d divide a dos enteros a y b, entonces d recibe el nombre de divisor común de a y b. Para dos enteros arbitrarios siempre es posible encontrar al menos un divisor común. Esto se consigna en el siguiente Teorema.

1.1.2 Teorema. Dados dos enteros a y b, existe un divisor común de a y b de la forma

$$d = ax + by,$$

con x e y enteros.

Demostración. La demostración de este resultado se puede consultar en la referencia [1]. □

1.1.3 Corolario. Dados dos enteros a y b, existe un número d, y sólo uno, tal que d es un divisor común no negativo de a y b, que resulta ser el mayor divisor común de este par de números.

Demostración. De acuerdo con el Teorema 1.1.2, existe al menos un entero r que divide a a y b. Ahora bien, note que $-r$ también es un divisor de este par de números.
Representamos con D al conjunto de los divisores comunes de a y b. Es claro que este conjunto está acotado superiormente, entonces el elemento $d = \max D$, es el máximo común divisor de a y b. □

Emplearemos la notación (a, b) para representar al máximo común divisor del par de números a y b. En el caso en que $(a, b) = 1$ entonces diremos que a y b son primos entre sí.

1.1.4 Definición. Un entero positivo p mayor que 1 se llama primo si los únicos divisores positivos de p son 1 y p. Un número entero positivo que no es primo es llamado compuesto.

Es bien conocido que el conjunto de números primos es infinito, y que si n es un entero compuesto, entonces n admite un divisor primo menor o igual que $\sqrt{n}$, véase [1].
Se emplea la notación $\pi(x)$ para representar al número de primos menores o iguales que x, y puede probarse, ver referencia [3], que

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1, \tag{1.1}$$

resultado que se conoce como Teorema del número primo.
En la Figura 1.1 se presenta el gráfico de la función $\pi(x)$ tomando $x = 100 + 100k$ para $k = 0, \ldots, 9$.

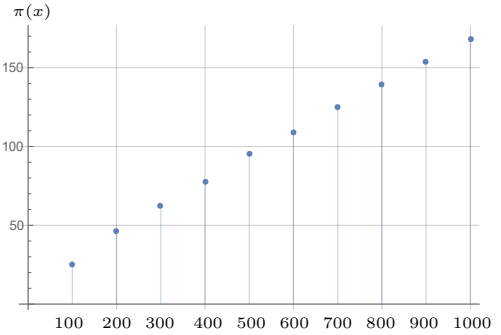


Figura 1.1. Gráfico de $\pi(x)$ tomando $x = 100 + 100k$ para $k = 0, \ldots, 9$.

Todo primo, excluyendo el 2, es un número impar, y es claro que esta afirmación es falsa en sentido contrario. Un dato curioso es que entre 1 y 100 existen 50 números impares, y en este mismo intervalo se pueden encontrar 25 números primos. Esta razón se reduce en la medida que se consideran conjuntos más grandes de números. Para ilustrar esto representemos con $H(n) = \{2k-1\}_{k=1}^{k=n}$ al conjunto de números impares en el intervalo $[1, 2n-1]$, e identifiquemos con $|H(n)|$ al cardinal de éste conjunto. En la Figura 1.2 se muestra el gráfico de $\pi(x)/|H(x/2)|$ tomando $x = 100+100k$ con $k = 0, \ldots, 9$. Note el comportamiento decreciente de la distribución de puntos

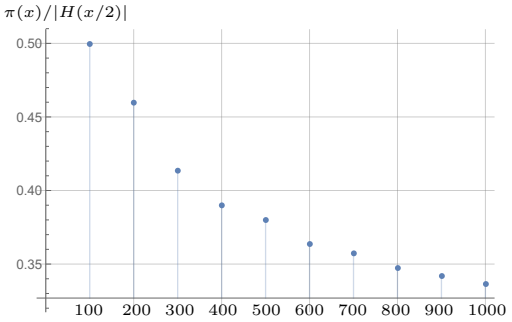


Figura 1.2. Gráfico de $\pi(x)/|H(x/2)|$ tomando $x = 100 + 100k$ para $k = 0, \ldots, 9$.

Lo anterior evidencia la existencia de espacios entre la secuencia de números primos. Esto se consigna en el siguiente Teorema.

1.1.5 Teorema. Dado cualquier entero positivo k, existen k enteros compuestos consecutivos.

Demostración. Sea k un entero positivo. Considere los siguientes números consecutivos

$$(k+1)!+2, (k+1)!+3, (k+1)!+4, \ldots, (k+1)!+k, (k+1)!+k+1.$$

Note que cada número es compuesto ya que $n|\,((k+1)!+n)$ para $2 \leq n \leq k+1$. □

1.1.6 Definición. La función totient de Euler, o función indicatriz de Euler, representada con la letra φ, indica el número de enteros positivos hasta un determinado entero n que son primos entre sí con n. Es decir,

$$\varphi(n) = |\{m \in \mathbb{N} | m \leq n \text{ y } (n, m) = 1\}|.$$

Es claro que si p es un número primo, entonces $\varphi(p) = p - 1$. En la Figura 1.3 se presentan los valores que toma $\varphi(n)$ con $n = 1, \ldots, 100$. Note que los puntos más altos en el gráfico coinciden con los números primos comprendidos en el intervalo $[1, 100]$.

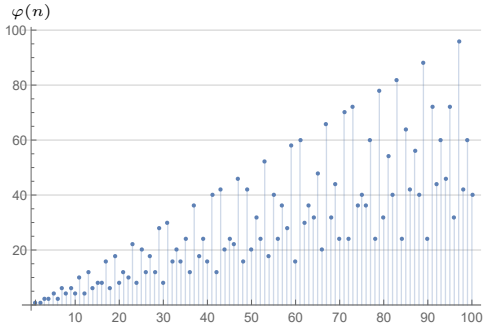


Figura 1.3. Gráfico de $\varphi(n)$ con $n = 1, \ldots 100$.

Empleando el Principio de inclusión–exclusión puede encontrarse una interesante expresión para $\varphi(n)$ que involucra los números primos divisores de n.

1.1.7 Teorema. Si $n \geq 1$, entonces

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

con p primo.

Demostración. Sean $\Omega = \{1, 2, ..., n\}$ y $p_1, p_2, \ldots p_r$ los divisores primos de n. Representemos con $\sigma(p_i)$ al conjunto

$$\sigma(p_i) = \{b \in \Omega : p_i | b\}.$$

Los elementos de Ω primos con n son aquellos que pertenecen al conjunto

$$\Omega - \bigcup_{i=1}^{r} \sigma(p_i).$$

De acuerdo con el Principio de inclusión–exclusión

$$\left|\Omega - \bigcup_{i=1}^{r} \sigma(p_i)\right| = |\Omega| - \sum_{1\le i\le r} |\sigma(p_i)| + \sum_{1\le i<j\le r} |\sigma(p_i)\cap\sigma(p_j)| - \sum_{1\le i<j<k\le r} |\sigma(p_i)\cap\sigma(p_j)\cap\sigma(p_k)| + \cdots \cdots + (-1)^r |\sigma(p_1)\cap\sigma(p_2)\cap\cdots\cap\sigma(p_r)|.$$

Ahora bien, si $p_i|n$ existen n/p_i múltiplos de p_i que pertenecen a Ω, con lo que

$$\begin{aligned} &|\sigma(p_i)| = \frac{n}{p_i}, \\ &|\sigma(p_i)\cap\sigma(p_j)| = \frac{n}{p_i p_j}, \\ &\vdots \\ &|\sigma(p_1)\cap\sigma(p_2)\cap\cdots\cap\sigma(p_r)| = \frac{n}{p_1 p_2 \dots p_r}. \end{aligned}$$

Se deduce

$$\begin{aligned} \varphi(n) &= n\left(1 - \sum_{1\le i\le r}\frac{1}{p_i} + \sum_{1\le i<j\le r}\frac{1}{p_i p_j} - \cdots + (-1)^r \frac{1}{p_1 p_2\dots p_r}\right) \\ &= n\prod_{p|n}\left(1-\frac{1}{p}\right) \end{aligned}$$

□

La función $\varphi(n)$ es fundamental en diversos campos del álgebra moderna y la teoría analítica de números.

1.1.8 Definición. Sean a, b y m con $m > 0$. Diremos que a es congruente con b módulo m, en notación

$$a \equiv b \pmod{m},$$

si $m|(a-b)$.

1.1.9 Lema. Sea m un entero positivo. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces

$$a + c \equiv b + d \pmod{m} \qquad \text{y} \qquad ac \equiv bd \pmod{m}$$

Demostración. La prueba de este resultado se puede consultar en la referencia [6]. □

1.1.10 Teorema (Euler–Fermat)**.** Si $(a, m) = 1$, entonces

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demostración. La prueba de este resultado se puede consultar en la referencia [1]. □

1.1.11 Teorema (Chino del resto)**.** Sean $m_1, m_2 .... m_n$ enteros positivos primos relativos dos a dos. El sistema

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_m}, \end{aligned}$$

tiene solución única módulo $m = m_1 m_2 \cdots m_n$. Esto significa que hay una solución x tal que $0 \leq x < m$ y todas las demás soluciones son congruentes módulo m con esta. Adicionalmente una solución es

$$x = \sum_{r=1}^{n} a_r y_r M_r,$$

en donde $M_r = \frac{m}{m_r}$ y y_r es tal que

$$M_r y_r \equiv 1 \pmod{m_r}.$$

Demostración. La prueba de este resultado se puede consultar en la referencia [6]. □

1.1.12 Lema. Sea $a = bq + r$, donde a,b, q y r son enteros. Entonces, $(a, b) = (b, r)$.

Demostración. La prueba de este resultado se puede consultar en la referencia [6]. □

1.2 Número de primos en las secuencias $6k+1$ y $6k-1$

En esta sección se revisan algunos resultados clásicos concernientes al número de primos en las secuencias aritméticas $\{6k+1\}$ y $\{6k-1\}$. El lector interesado en profundizar sobre estos aspectos puede consultar la referencia [1], capítulo 7, de donde se tomaron los fundamentos teóricos para la construcción de la prueba del Teorema 1.2.2, o revisar los apuntes y comentarios en [4], de donde se revisó y estudió la prueba del Teorema 1.2.3.

1.2.1 Teorema. Si $p, q \in \{6k+1\}$ o $p, q \in \{6k-1\}$ entonces $pq \in \{6k+1\}$.

Demostración. Si $p, q \in \{6k+1\}$ entonces p es de la forma $p = 6x+1$ para algún entero x, y q es de la forma $q = 6y+1$ para algún entero y. Al hacer el producto pq obtenemos

$$pq = (6x+1)(6y+1) = 6(6xy+x+y)+1,$$

y por lo tanto $pq \in \{6k+1\}$.
La demostración para el caso en que $p, q \in \{6k-1\}$ es similar. □

1.2.2 Teorema. Existen infinitos primos de la forma $6k-1$.

Demostración. Supongamos que existen un número finito de primos de la forma $6k-1$, y sea p el mayor de ellos.
Consideremos el número $N = 6 \cdot 5 \cdot 7 \cdots p \ -1$. Note que N es de la forma $6k-1$ y ningún primo menor o igual que p divide a N, también es claro que $p < N$.
De acuerdo con lo anterior, si existe un primo que divida a N, este tiene que ser de la forma $6k+1$, véase Lema 2.1.1 en el siguiente capítulo. De acuerdo con el Teorema 1.2.1, el producto de este primo por otro del mismo tipo es de la forma $6k+1$. En consecuencia N es un primo mayor que p o debe admitir un divisor primo de la forma $6k-1$ mayor que p. □

1.2.3 Teorema. Existen infinitos primos de la forma $6k+1$.

Demostración. Supongamos que el conjunto de primos de la forma $6k+1$ es finito e identifiquemos con la letra P a dicho conjunto.
Sea N un número tal que $6p_i|N$ para todo $p_i \in P$ y considere el número $M = N^2 - N + 1$. Note que $M \equiv 1 \pmod 6$.

Al multiplicar M por $N+1$ obtenemos

$$M(N+1) = (N^2 - N + 1)(N+1) = N^3 + 1.$$

Si q es un divisor primo de M entonces $q|(N^3+1)$, es decir $N^3 \equiv -1 \pmod{q}$ y de acuerdo con el Lema 1.1.9 se tiene que $N^6 \equiv 1 \pmod{q}$.
Por otro lado, si $q|N$ tendríamos que $M \equiv 1 \pmod{q}$ lo cual no es posible ya que $q|M$, entonces $(N,q) = 1$ y de acuerdo con el Teorema 1.1.10

$$N^{q-1} \equiv 1 \pmod{q}. \tag{1.2}$$

Sea k el menor entero positivo tal que $N^k \equiv 1 \pmod{q}$, como $N^6 \equiv 1 \pmod{q}$, entonces k debe ser un divisor de 6 y por lo tanto k sería $1, 2, 3$ o 6.
Si $k = 1$ entonces $N \equiv 1 \pmod{q}$ y de acuerdo con el Teorema 1.1.9, se tiene que $N^3 \equiv 1 \pmod{q}$ lo cual no posible pues se ha probado que $N^3 \equiv (-1) \pmod{q}$. De acuerdo con esto, $k \neq 1$ y $k \neq 3$.
Si $k = 2$ entonces $N^2 \equiv 1 \pmod{q}$, esto quiere decir que existe un entero x tal que

$$(N-1)(N+1) = xq,$$

y como $N \not\equiv 1 \pmod{q}$ entonces $q|(N+1)$.
Note que $M = (N+1)(N-2) + 3$ y de acuerdo con el Lema 1.1.12

$$(M, N+1) = (N+1, 3) \leq q, \tag{1.3}$$

pero q no puede ser igual a 3, ya que debido a la construcción de N, 3 no divide a $N+1$. Esto indica que la desigualdad en (1.3) es estricta, y esto sería una contradicción con el hecho de que q es un divisor común de M y $N+1$.
De acuerdo con lo anterior, la única posibilidad es que $k = 6$ y se sigue de (1.2) que $6|(q-1)$, es decir $q \equiv 1 \pmod{6}$. Entonces habríamos encontrado un primo q de la forma $6k+1$ que no divide a N y que no pertenece al conjunto P. □

En relación con el número de primos en otras progresiones aritméticas, se conoce el siguiente resultado conocido como el Teorema de Dirichlet. El lector interesado en profundizar sobre estos aspectos puede consultar el capítulo 7 en [1], en particular el Teorema 7.9 y lemas precedentes.

1.2.4 Teorema. Si $r > 0$ y $(p, r) = 1$ entonces existe una infinidad de primos en la progresión aritmética $pk + r$, para $k = 0, 1, 2, \ldots$.

Demostración. La demostración de este resultado se puede consultar en [1]. □

Para $r > 0$ y $(p, r) = 1$ representaremos con $\pi(x; p, r)$ al número de primos q, menores o iguales que x, presentes en la progresión $pk + r$ para $k = 0, 1, 2, \ldots$. Es decir

$$\pi(x; p, r) = \sum_{\substack{q \leq x \\ q \equiv r \pmod{p}}} 1,$$

con q primo.
De manera equivalente como en (1.1), existe un resultado para la función $\pi(x; p, r)$, conocido como el Teorema del número primo para progresiones aritméticas, este afirma que

$$\pi(x; p, r) \sim \frac{\pi(x)}{\varphi(p)} \text{ cuando } x \to \infty.$$

Es importante mencionar que sigue siendo un problema abierto en Teoría analítica de números, el determinar cotas explícitas para la función $\pi(x; p, r)$. Por ejemplo, es conocido que

$$\pi(x; p, r) \ll \frac{1}{1 - \theta} \frac{x}{\varphi(p) \log x},$$

en donde $\theta < 1$, es una constante que depende de p y x. Este tipo de resultados se desprenden del Teorema de Brun–Titchmarsh, véase la referencia [5].

2 Resultados principales

En este capítulo se presentan los resultados del trabajo de investigación, con este propósito se ha divido en dos partes. En la primera se ilustra una técnica para determinar $\pi(n)$ a partir del número de primos en las secuencias $\{6k+1\}$ y $\{6k-1\}$. En la segunda se presentan dos resultados consecuencia del cómputo para $\pi(x;6,1)$ y $\pi(x;6,-1)$.
A partir de este momento denotaremos con $[q,p]$ al residuo de la división de q por p, e identificaremos a la secuencia $\{6k-1\}$ con $k=1,2,\ldots$ con su forma equivalente $\{6k+5\}$ con $k=0,2,3,\ldots$

2.1 Cálculo de $\pi(n)$ a partir de las secuencias $6k+1$ y $6k-1$

En la siguiente sección determinaremos el valor de $\pi(n)$ empleando las secuencias $\{6k+1\}$ y $\{6k-1\}$.

2.1.1 Lema. Si $p>3$ es un número primo, entonces p es de la forma $6k+1$ ó $6k+5$.

Demostración. Como p es primo, entonces no podría ser de la forma $6k$, $6k+2$, $6k+3$ ó $6k+4$ ya que estos números son compuestos, luego la única posibilidad para p es que sea la forma $6k+1$ ó $6k+5$. □

2.1.2 Lema. Si $(Q,6)=1$ entonces $\left[Q^2,6Q\right]$ es igual a Q o a $5Q$.

Demostración. Como $(Q,6)=1$ entonces existe un entero x tal que $Q=6x+r$ siendo $r=1$ o $r=5$. Al multiplicar esta última expresión por Q obtenemos $Q^2=6Qx+rQ$ y es claro que $0<rQ<6Q$, lo que finaliza la prueba. □

Del anterior lema se desprenden dos resultados que nos serán útiles para determinar el número de primos en las secuencias $\{6k+1\}$ y $\{6k+5\}$.

2.1.3 Corolario. Si Q es un primo de la forma $6k+1$, entonces $\left[Q^2, 6Q\right] = Q$ y $\left[5Q^2, 6Q\right]$ es compuesto. Si Q es un primo de la forma $6k+5$ entonces $\left[5Q^2, 6Q\right] = Q$ y $\left[Q^2, 6Q\right]$ es compuesto.

2.1.4 Corolario. Si $(Q, 6) = 1$ y $Q > n$, entonces $\left[Q^2, 6Q\right] > n$.

2.1.5 Definición. Sea P_n el conjunto de números primos menores o iguales que n y mayores que 3, note que $|P_n| = \pi(n) - 2$. Identificaremos con la letra $A(j)$ para $j = 0, 1, 2, \ldots$ a los siguientes conjuntos

$$A(j) = \begin{cases} \{1\} & \text{si } j = 0, \\ \left\{ \prod_{i=1}^{j} p_i \ : p_i \in P_n \right\} & \text{si } j = 1, 2, \ldots, |P_n|. \end{cases}$$

Emplearemos la letra Q para identificar a los elementos de los conjuntos $A(j)$. En particular, note que si $Q \in A(1)$, entonces $Q \in P_n$.

Identificaremos con $\beta(q)$ a la función

$$\beta(q) = \begin{cases} 0 & \text{si } q \text{ es primo o } 1, \\ 1 & \text{en otro caso.} \end{cases} \tag{2.1}$$

Podemos encontrar una expresión matemática para $\pi(n)$ utilizando las secuencias $\{6k+1\}$ y $\{6k+5\}$. Ilustraremos la técnica que vamos a emplear con el siguiente ejemplo.

2.1.6 Ejemplo (Cálculo de $\pi(100)$)**.** De acuerdo con el Lema 2.1.1, todos los números primos exceptuando el 2 y 3 están en las secuencias $\{6k+1\}$ y $\{6k+5\}$. Necesitamos determinar cuántos primos, menores o iguales a 100, hay en cada una de estas. Con este propósito centraremos nuestra atención primero en $\{6k+1\}$.
Representemos con $C = \{6k+1\}_{k=0}^{k=|C|-1}$ en donde

$$|C| = \left\lfloor \frac{100-1}{6} \right\rfloor + 1 = 17.$$

Es decir $|C|$ de número de elementos de la forma $6k+1$ desde 1 hasta 100.
El número de primos en C serán aquellos que no son múltiplos de primos, es decir, necesitamos eliminar de C todos aquellos números de la forma Qk para $Q \in A(1)$ y $k = 2, 3 \ldots$. Esto es

$$\pi(100; 6, 1) = \left| C \setminus \{1\} - \bigcup_{Q \in A(1)} \{Qk\}_{k=2}^{N} \right| \text{ en donde } N = \left\lfloor \frac{100}{Q} \right\rfloor. \tag{2.2}$$

De manera equivalente a como se demostró el Teorema 1.1.7 podemos emplear el Principio de inclusión - exclusión para calcular $\pi(100; 6, 1)$.
Vamos a eliminar de C todos aquellos números de la forma Qk con $Q \in A(1)$ presentes en $\{6k+1\}$. Después adicionaremos los números de la forma Qk con $Q \in A(2)$ presentes en $\{6k+1\}$. Después eliminaremos de C los números de la forma Qk con $Q \in A(3)$ presentes en $\{6k+1\}$ y de esta forma sucesivamente, hasta el caso Qk con $Q \in A(|P_{100}|)$ presentes en $\{6k+1\}$.
Para resolver cada uno de los casos antes mencionados, es necesario encontrar al menos una solución del siguiente sistema de ecuaciones modulares

$$\begin{cases} x \equiv 1 \pmod 6, \\ x \equiv 0 \pmod Q, \end{cases} \tag{2.3}$$

con $Q \in A(j)$ para $j = 1, 2, \ldots, |P_{100}|$. De acuerdo con el Teorema 1.1.11 el sistema admite solución, y una es Q^2, lo que indica que la secuencia

$$\left\{6Qk + \left[Q^2, 6Q\right]\right\}_{k=0}^{k=H-1} \tag{2.4}$$

con

$$H = \left\lfloor \frac{100 - \left[Q^2, 6Q\right]}{6Q} \right\rfloor + 1, \tag{2.5}$$

representa el número de términos de la forma Qk presentes en la secuencia $\{6k+1\}$ comprendidos entre 1 y 100.
Digamos que $Q = 7$, entonces para este caso las ecuaciones (2.4) y (2.5) serían respectivamente

$$\{42k + 7\}_{k=0}^{k=H-1} \text{ con } H = 3.$$

Note que los números 7, 49 y 91 son los múltiplos de 7 presentes en la secuencia $\{6k+1\}$.
Como se ha visto, si $Q \in A(1)$ existe la posibilidad de que el residuo $\left[Q^2, 6Q\right] = Q$ y entonces se trataría de un número primo que no deseamos eliminar de los existentes en la secuencia $\{6k+1\}$.
Por otro lado, es fácil probar que si $Q \in A(j)$ con $j > 1$ entonces el residuo $\left[Q^2, 6Q\right]$ es un número compuesto.
De acuerdo con esto, los números de la forma Qk con $Q \in A(j)$ presentes en $\{6k+1\}$ entre 1 y 100, factibles para ser eliminados o agregados al conjunto C, son

$$\left\lfloor \frac{100 - \left[Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\left(\left[Q^2, 6Q\right]\right) \tag{2.6}$$

Digamos que $Q = 7 \cdot 13 = 91 \in A(2)$, entonces, de acuerdo con (2.4), la secuencia que involucra los números de la forma $91k$ presentes en $\{6k+1\}$ es la secuencia $\{546k + 91\}$, y se desprende de (2.6) que el número de términos factibles para ser eliminados o agregados al conjunto C es 1, que en este caso se refiere al número 91.
Si Q es un número compuesto tal que $Q > 100$, entonces de acuerdo con el Corolario 2.1.4 se tiene que $\left[Q^2, 6Q\right] > 100$ y en este caso

$$\left\lfloor \frac{100 - \left[Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\big(\left[Q^2, 6Q\right]\big) = -1 + 1 = 0.$$

Digamos que $Q = 5 \cdot 7 = 35 \in A(2)$, entonces la secuencia que involucra los números de la forma $35k$ presentes en $\{6k+1\}$ es la secuencia $\{35k+175\}$, y en este caso no existen términos en esa secuencia de la forma $6k + 1$ comprendidos entre 1 y 100.
Por último, note que si $Q \in A(0)$ entonces $Q = 1$ y en este caso $\left[Q^2, 6Q\right] = 1$ y de acuerdo con (2.6), obtendríamos $\left\lfloor \frac{100-1}{6} \right\rfloor$ términos factibles para iniciar nuestro conteo de primos, sin incluir el número 1 en la secuencia $\{6k + 1\}$, es decir $|C \setminus \{1\}|$, como se pudo apreciar en (2.2).
De acuerdo con lo anterior, el número de primos presente en la secuencia $\{6k + 1\}$, desde 1 hasta 100, está dado por la expresión

$$\pi(100; 6, 1) = \sum_{j=0}^{|P_{100}|} (-1)^j \sum_{Q \in A(j)} M\left(100, \left[Q^2, 6Q\right]\right) \tag{2.7}$$

en donde

$$M\left(100, \left[Q^2, 6Q\right]\right) = \left\lfloor \frac{100 - \left[Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\left(\left[Q^2, 6Q\right]\right).$$

Note que si $j \geq 3$, entonces $Q > 100$ y de acuerdo con el Corolario 2.1.4

$$\sum_{Q \in A(j)} \left(\left\lfloor \frac{100 - \left[Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\left(\left[Q^2, 6Q\right]\right) \right) = 0.$$

Esto indica que (2.7) puede reducirse a

$$\pi(100; 6, 1) = \sum_{j=0}^{3} (-1)^j \sum_{Q \in A(j)} \left(\left\lfloor \frac{100 - \left[Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\left(\left[Q^2, 6Q\right]\right) \right)$$

en donde cada uno de los términos es fácilmente computable, dando como resultado que $\pi(100;6,1)=11$.
De manera equivalente, se puede determinar $\pi(100;6,5)$, la diferencia consiste en que se debe contar el primer término de $\{6k+5\}$ a partir de $k=0$, pues 5 es primo, y también cambiar $\left[Q^2,6Q\right]$ por $\left[5Q^2,6Q\right]$ ya que el sistema modular que debemos resolver en este caso es

$$\begin{cases} x\equiv 5 \pmod 6, \\ x\equiv 0 \pmod Q. \end{cases} \tag{2.8}$$

De acuerdo con lo anterior

$$\pi(100;6,5)=\sum_{j=0}^{|P_{100}|}(-1)^j\sum_{Q\in A(j)}M\left(100,\left[5Q^2,6Q\right]\right)+1 \tag{2.9}$$

en donde

$$M\left(100,\left[5Q^2,6Q\right]\right)=\left\lfloor\frac{100-\left[5Q^2,6Q\right]}{6Q}\right\rfloor+\beta\left(\left[5Q^2,6Q\right]\right).$$

Debido a que los conjuntos de números primos en las secuencias $\{6k+1\}$ y $\{6k+5\}$ son disjuntos, entonces, el total de primos menores o iguales que 100 exceptuando el 2 y el 3, es decir $\pi(100)-2$ esta dado por

$$\pi(100)-2=\pi(100;6,1)+\pi(100;6,5)=23.$$

El análisis anterior se puede concretar en el siguiente Teorema.

2.1.7 Teorema. Si $n\geq 5$ entonces

$$\pi(n)=2+\sum_{j=0}^{|P_n|}(-1)^j\sum_{Q\in A(j)}M^*(n,j,Q) \tag{2.10}$$

donde

$$M^*(n,j,Q)=\left\lfloor\frac{n-\left[Q^2,6Q\right]}{6Q}\right\rfloor+\left\lfloor\frac{n-\left[5Q^2,6Q\right]}{6Q}\right\rfloor+\beta^*(j)$$

siendo β^* la función definida como

$$\beta^*(j)=\begin{cases}1 \text{ si } j=0,1,\\ 2 \text{ si } j\geq 2.\end{cases}$$

Demostración. Del conjunto $\{6k+1\}\cup\{6k+5\}$ iniciando en 1 y 5 hasta todos aquellos números menores o iguales que n; eliminaremos el número de múltiplos de primos, y de acuerdo con el Principio de inclusión – exclusión, adicionaremos el número de múltiplos dos a dos de primos, sustraeremos el número de múltiplos tres a tres de primos, y de esta forma todos aquellos productos de primos presentes en $\{6k+1\}\cup\{6k+5\}$. Con este propósito, para $Q \in A(j)$ con $j \geq 1$, resolvemos los sistemas de ecuaciones modulares,

$$\begin{cases} x \equiv 1 \pmod 6, \\ x \equiv 0 \pmod Q, \end{cases} \quad \begin{cases} x \equiv 5 \pmod 6, \\ x \equiv 0 \pmod Q, \end{cases} \tag{2.11}$$

que de acuerdo con el Teorema 1.1.11 admiten solución, y la secuencia asociada a cada uno de estos conjuntos solución es respectivamente,

$$\{6Qk + \left[Q^2, 6Q\right]\} \quad \text{y} \quad \{6Qk + \left[5Q^2, 6Q\right]\},$$

contando con

$$\left\lfloor \frac{n - \left[Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\left(\left[Q^2, 6Q\right]\right) \quad \text{y} \quad \left\lfloor \frac{n - \left[5Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\left(\left[5Q^2, 6Q\right]\right)$$

número de términos para ser adicionados o eliminados de acuerdo con la elección de $Q \in A(j)$.
Como no nos interesa incluir el 1 en nuestra cuenta inicial, pero el 5 sí, definimos $\beta^*(0) = 1$. Por otro lado, de acuerdo con el Corolario 2.1.3 para $Q \in A(1)$ se tiene que

$$\beta\left(\left[Q^2, 6Q\right]\right) + \beta\left(\left[5Q^2, 6Q\right]\right) = 1.$$

Por otro lado, teniendo en cuenta que para $Q \in A(j)$ con $j \geq 2$, los residuos $\left[Q^2, 6Q\right]$ y $\left[5Q^2, 6Q\right]$ son compuestos, entonces para este caso

$$\beta\left(\left[Q^2, 6Q\right]\right) + \beta\left(\left[5Q^2, 6Q\right]\right) = 2,$$

situación equivalente cuando $Q > n$, pues de acuerdo con el Corolario 2.1.3, si $Q > n$ entonces $\left[Q^2, 6Q\right] > n$ y también $\left[5Q^2, 6Q\right] > n$.
En el caso de que alguno de los residuos supere el valor de n, la parte entera tomaría el valor de -1, pero igualmente al sumar 1 o 2 según sea la situación, se tendría el valor de 0 o 1, que sería el número de términos para adicionar o quitar del conjunto $\{6k+1\}\cup\{6k+5\}$. □

Es claro que aunque el Teorema anterior nos permite determinar el número de primos menores o iguales que un cierto n, el cómputo de (2.1.7) puede ser bastante dispendioso, esto debido a que los conjuntos $A(j)$ dependiendo del valor de n pueden tener un tamaño considerable, esto se verá con más detalle en la siguiente sección.

2.2 Identidades para $[Q^2, 6Q]$ y $[5Q^2, 6Q]$

A continuación se presentan dos identidades subyacentes a las expresiones para $\pi(n;6,1)$ y $\pi(n;6,5)$.

2.2.1 Teorema. Si $n \geq 5$ entonces

$$\sum_{j=0}^{|P_n|}(-1)^j \sum_{Q\in A(j)} \left\lfloor \frac{n-[Q^2;6Q]}{6Q} \right\rfloor = 1 \tag{2.12}$$

Demostración. De acuerdo con (2.7), para un cualquier n se tiene que

$$\pi(n;6,1) = \sum_{j=0}^{|P_n|}(-1)^j \sum_{Q\in A(j)} M\left(n, \left[Q^2, 6Q\right]\right) \tag{2.13}$$

en donde

$$M\left(n, \left[Q^2, 6Q\right]\right) = \left\lfloor \frac{n-\left[Q^2, 6Q\right]}{6Q} \right\rfloor + \beta\left(\left[Q^2, 6Q\right]\right).$$

Note que para $Q \in A(1)$, $\beta\left(\left[Q^2, 6Q\right]\right)$ toma el valor de 0 cuando $\left[Q^2, 6Q\right] = Q$, un primo de la forma $6k+1$, o es igual a 1, y toma el valor de 1 cuando $\left[Q^2, 6Q\right]$ es compuesto. De acuerdo con esto

$$\sum_{Q\in A(1)} \beta\left([Q^2; 6Q]\right) = \pi(n) - 2 - \pi(n, 6, 1).$$

Por otro lado, para $Q \in A(j)$ con $j \geq 2$, se tiene que $\beta\left(\left[Q^2, 6Q\right]\right) = 1$, y si identificamos con

$$\binom{|P_n|}{j},$$

al número de productos de j distintos primos que se pueden escoger de los $|P_n|$ elementos, entonces obtenemos que

$$\sum_{j=2}^{|P_n|}(-1)^j \sum_{Q\in A(j)} \beta\left(\left[Q^2, 6Q\right]\right) = \binom{|P_n|}{2} - \binom{|P_n|}{3} + \ldots + (-1)^{|P_n|}\binom{|P_n|}{|P_n|},$$

y de acuerdo con el Teorema del binomio,

$$\binom{|P_n|}{0} - \binom{|P_n|}{1} + \sum_{j=2}^{|P_n|}(-1)^j \sum_{Q\in A(j)} \beta\left(\left[Q^2, 6Q\right]\right) = (1-1)^{|P_n|} = 0.$$

o de manera equivalente,

$$\sum_{j=2}^{|P_n|}(-1)^j \sum_{Q\in A(j)} \beta\left(\left[Q^2, 6Q\right]\right) = -1 + |P_n| = -3 + \pi(n)$$

De acuerdo con lo anterior, (2.13) toma la siguiente forma

$$\pi(n;6,1) = \left\lfloor \frac{n-1}{6} \right\rfloor - \sum_{Q\in A(1)} \left\lfloor \frac{n-[Q^2,6Q]}{6Q} \right\rfloor - \pi(n) + 2 + \pi(n;6,1) + \\ + \sum_{j=2}^{\alpha}(-1)^j \sum_{Q\in A(j)} \left\lfloor \frac{n-[Q^2,6Q]}{6Q} \right\rfloor - 3 + \pi(n),$$

de donde se concluye que

$$\sum_{j=0}^{|P_n|}(-1)^j \sum_{Q\in A(j)} \left\lfloor \frac{n-[Q^2,6Q]}{6Q} \right\rfloor = 1$$

□

Note que $\binom{|P_n|}{j}$, dependiendo del valor de n puede tomar valores muy grandes, esta es la razón de que el cómputo de (2.1.7) pueda ser bastante dispendioso, como se mencionó al final de la sección anterior.

2.2.2 Teorema. Si $n \geq 5$ entonces

$$\sum_{j=0}^{|P_n|}(-1)^j \sum_{Q\in A(j)} \left\lfloor \frac{n-[5Q^2,6Q]}{6Q} \right\rfloor = 0 \tag{2.14}$$

Demostración. De acuerdo con (2.9), para un cualquier n se tiene que

$$\pi(n;6,5) = \sum_{j=0}^{|P_n|}(-1)^j \sum_{Q\in A(j)} M\left(n, \left[5Q^2, 6Q\right]\right) + 1 \tag{2.15}$$

en donde

$$M\left(n,\left[5Q^2,6Q\right]\right)=\left\lfloor\frac{n-\left[5Q^2,6Q\right]}{6Q}\right\rfloor+\beta\left(\left[5Q^2,6Q\right]\right).$$

Note que para $Q\in A(1)$, $\beta\left(\left[5Q^2,6Q\right]\right)$ toma el valor de 0 cuando $\left[5Q^2,6Q\right]=Q$, un primo de la forma $6k+5$ y toma el valor de 1 cuando $\left[5Q^2,6Q\right]$ es compuesto. De acuerdo con esto

$$\sum_{Q\in A(1)}\beta\left([5Q^2,6Q]\right)=\pi(n)-2-\pi(n;6,5).$$

Por otro lado, para $Q\in A(j)$ con $j\geq 2$, se tiene que $\beta\left(\left[5Q^2,6Q\right]\right)=1$, y como vimos en la prueba del teorema anterior al ser $\beta\left(\left[5Q^2,6Q\right]\right)=1$, vamos a obtener que

$$\sum_{j=2}^{|P_n|}(-1)^j\sum_{Q\in A(j)}\beta\left(\left[5Q^2,6Q\right]\right)=-1+|P_n|=-3+\pi(n)$$

De acuerdo con lo anterior, (2.15) toma la siguiente forma

$$\pi(n;6,5)=\left\lfloor\frac{n-5}{6}\right\rfloor+1-\sum_{Q\in A(1)}\left\lfloor\frac{n-[5Q^2,6Q]}{6Q}\right\rfloor-\pi(n)+2+$$
$$+\pi(n;6,5)+\sum_{j=2}^{|P_n|}(-1)^j\sum_{Q\in A(j)}\left\lfloor\frac{n-[5Q^2,6Q]}{6Q}\right\rfloor-3+\pi(n),$$

de donde se concluye que

$$\sum_{j=0}^{|P_n|}(-1)^j\sum_{Q\in A(j)}\left\lfloor\frac{n-[5Q^2,6Q]}{6Q}\right\rfloor=0$$

□

3 Conclusiones

Se ha encontrado una fórmula explícita de $\pi(n)$ empleando el Principio de inclusión–exclusión al conjunto $\{6k+1\} \cup \{6k-1\}$, al suprimir de este los múltiplos de números primos. Es necesario mencionar que el cómputo de dicha fórmula puede llegar a ser dispendiosa, sin embargo en su estructura se ha podido revelar dos identidades para los residuos entre Q^2 y $6Q$, al igual que para $5Q^2$ y $6Q$, en notación $[Q^2, 6Q]$ y $[5Q^2, 6Q]$, siendo Q elementos de la forma, producto entre uno, dos o más primos menores o iguales que un cierto n.
Como un trabajo futuro se espera poder generalizar el Teorema 2.2.1 para cualquier secuecia $\{pk+r\}$ con $(p, r) = 1$.

Bibliografía

[1] T. M. Apostol. *Introducción a la teoría analítica números*. Edición 1. Reverté, 1984

[2] Niven, Ivan, Herbert S. Zuckerman, y José Hernán Pérez Castellanos. Introducción a la teoría de los números. 1969.

[3] A. Selberg. "An elementary proof of the prime-number theorem". *Annals of Mathematics*, pp. 305-313, 1949.

[4] David Radcliffe. "Primes of the form 6k+1", 2013. [En línea]. Disponible en: https://mathblag.wordpress.com/2013/08/30/primes-of-the-form-6k1/. [Accedido: 05-abr-2021]

[5] Thorner, Jesse, and Asif Zaman. "A Chebotarev variant of the Brun–Titchmarsh theorem and bounds for the lang-trotter conjectures." International Mathematics Research Notices 2018.16 (2018): 4991-5027.

[6] K. Rosen, *Matemáticas discretas y sus aplicaciones*. Quinta edición. Concepción Fernández, 2004.