ANÁLISIS DEL COMPORTAMIENTO EN LA DISTRIBUCIÓN DE LOS NÚMEROS PRIMOS EN LOS NÚMEROS NATURALES.

Mauricio Moreno Vásquez

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

2017

ANÁLISIS DEL COMPORTAMIENTO EN LA DISTRIBUCIÓN DE LOS NÚMEROS PRIMOS EN LOS NÚMEROS NATURALES

Mauricio Moreno Vásquez

Julio Hernando Vargas Moreno

TRABAJO PARA OPTAR AL TÍTULO DE

MAGISTER EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

2017

Resumen

Este trabajo presenta una metodología para la búsqueda de números primos de forma determinista basada en una optimización de la famosa Criba de Eratóstenes, la cual permite de una manera sencilla encontrar los números primos desde 2 hasta *n*, siendo *n* un número natural dado, usando solo multiplicaciones, lo cual permite que este método pueda ser utilizado incluso por niños que no tengan un alto conocimiento en matemática, poniendo especial cuidado en no desperdiciar recursos de procesamiento, lo cual da pistas fundamentales para entender el porqué los números primos se encuentran distribuidos de una forma que parece aleatoria pero que no ha sido definida aun en los números naturales.

Haciendo un análisis de cómo es el comportamiento de dicha criba, se presenta además un algoritmo que permite calcular de manera exacta la distribución de los números primos en los números naturales y estudiando su comportamiento se hace una aproximación matemática a través de una fórmula que permite conocer como es dicha distribución, teniendo en cuenta que encontrarla es un problema que ha sido considerado desde hace mas de 2.000 años por los matemáticos más importantes del mundo como “El Santo Grial de las Matemáticas”.

Aprovechando el avance de los sistemas y la tecnología, se tiene una ventaja estratégica para poder abordar el problema y permite hacer pruebas más rigurosas de los resultados, para así aproximarse de una manera más exacta a los resultados esperados.

TABLA DE CONTENIDO

TABLA DE FIGURAS

1. Generalidades

Antecedentes y justificación

El estudio de los números primos es una parte importante de la teoría de números, estos se encuentran presentes en algunas conjeturas centenarias tales como la hipótesis de Riemann y la conjetura de Goldbach.

La distribución de los números primos es un tema recurrente de investigación en la teoría de números: si se consideran números individuales, los primos parecen estar distribuidos aleatoriamente, pero la distribución global de los números primos sigue leyes bien definidas.

La primera prueba indiscutible del conocimiento de los números primos se remonta a alrededor del año 300 A.C. y se encuentra en los Elementos de Euclides (tomos VII a IX). Euclides define los números primos, demuestra que hay infinitos de ellos, define el máximo común divisor y el mínimo común múltiplo y proporciona un método para determinarlos que hoy en día se conoce como el algoritmo de Euclides. Los Elementos contienen asimismo el teorema fundamental de la aritmética y la manera de construir un número perfecto a partir de un número primo de Mersenne. La criba de Eratóstenes, atribuida a Eratóstenes de Cirene, es un método sencillo que permite encontrar números primos.

Cabe anotar que uno de los mayores problemas matemáticos de todos los tiempos se refiere a la distribución de los números primos entre los números naturales. Muchos matemáticos famosos han pasado su vida tratando de resolverlo y han hecho avances significativos, como Gauss, Riemann y algunos otros. David Hilbert, en 1900 propuso 23 problemas pendientes de

solución para que los matemáticos del mundo trabajaran en ellos en el siglo XX, siendo el más significativo de ellos la solución a la hipótesis de Riemann, por su relación con la distribución de los números primos entre los números naturales.

Un siglo después, en el año 2000, el Instituto Clay de Matemáticas (Cambridge Massachusetts), seleccionó “los siete problemas del milenio” para resolver en el presente siglo y ofreció un millón de dólares por la solución de cada uno de ellos, clasificando nuevamente, como el más importante, solucionar la hipótesis de Riemann, también por su relación con la distribución de los números primos entre los números naturales.

La teoría de los números primos es una de las pocas áreas de la matemática pura que ha encontrado aplicación directa en el mundo real, concretamente en la criptografía. La criptografía estudia los métodos para cifrar mensajes secretos de manera que solo puedan ser descifrados por el receptor, y que nadie más pueda hacerlo.

Durante la década de los setenta, Whitfield Diffie y Martin Hellman se propusieron encontrar un proceso matemático que fuese fácil de llevar a término en una dirección, pero muy difícil de realizar en la dirección opuesta. Un proceso como este formaría la clave perfecta para los mensajes cifrados. Por ejemplo, se podría tener la clave dividida en dos partes y publicar la parte correspondiente al cifrado. Cualquiera podría enviarme mensajes cifrados, pero solo yo conocería la parte descifradora de la clave.

Durante mucho tiempo, se pensaba que la aplicación de los números primos era muy limitada fuera de la matemática pura. Esto cambió en los años 70 con el desarrollo de la criptografía de clave pública, en la que los números primos formaban la base de los primeros algoritmos tales como el algoritmo RSA. Publicado en 1977 por Ronald Rivest, Adi Shamir y

Leonard Adleman, un equipo de matemáticos y científicos informáticos del Massachusetts Institute of Technology, se dieron cuenta que los números primos eran la base ideal para un proceso de cifrado "computacionalmente fácil" y descifrado "computacionalmente difícil".

Identificación del problema

Por definición un número primo es un número natural que tiene únicamente dos divisores exactos distintos: sí mismo y la unidad.

Ahora bien, el problema de la distribución se refiere a la cantidad de números primos que pueden encontrarse en los números naturales hasta un número *N* determinado.

El modelado de la distribución de los números primos y su complejidad computacional son temas de investigación recurrentes entre los teóricos de números y estudiosos de los sistemas computacionales. La primalidad de un número concreto es (hasta ahora) impredecible a pesar de que existen leyes, como el teorema de los números primos y el postulado de Bertrand, que gobiernan su distribución a gran escala. Leonhard Euler comentó:

"Hasta el día de hoy, los matemáticos han intentado en vano encontrar algún orden en la sucesión de los números primos, y tenemos motivos para creer que es un misterio en el que la mente jamás penetrará."

En una conferencia de 1975, Don Zagier comentó: "Hay dos hechos sobre la distribución de los números primos de los que espero convencerles de forma tan incontestable que quedarán permanentemente grabados en sus corazones. El primero es que, a pesar de su definición simple y del papel que desempeñan como ladrillos con los que se construyen los números naturales, los números primos crecen como malas hierbas entre los números naturales, y no parecen obedecer

ninguna otra ley que la del azar, y nadie puede predecir dónde brotará el siguiente. El segundo hecho es aún más asombroso, ya que dice justo lo contrario: que los números primos muestran una regularidad pasmosa, que hay leyes que gobiernan su comportamiento, y que obedecen estas leyes con precisión casi militar."

Existen algoritmos de encriptación que se basan en el principio de que es computacionalmente imposible encontrar números primos "grandes" para brindar el nivel de confidencialidad de la información necesario, tal es el caso de los algoritmos de encriptación asimétricos o de clave publica desarrollados por la RSA.

Aportes del proyecto

El proyecto pretende aportar una metodología para encontrar números primos de forma determinista, a partir de ahí se pretende obtener un modelo matemático y un algoritmo que lo represente.

Objetivo general y objetivos específicos

Objetivo general.

Hacer un análisis del comportamiento de la distribución de los números primos en los números naturales por medio de un modelo determinista.

Objetivos específicos.

- Definir una metodología determinista, la cual no desperdicie ciclos de cómputo en el proceso de búsqueda de números primos.
- Hacer un estudio a partir de la metodología determinista para encontrar un patrón que rija la distribución de los números primos en los números naturales.
- Hacer una aplicación que permita visualizar la metodología propuesta y brinde información suficiente para poder llegar a conclusiones respecto a la distribución de los números primos entre los números naturales.
- Con los datos entregados por la aplicación inferir un modelo sobre el comportamiento de la aparición de los números primos en los números naturales.

Metodología

Se realizará una introducción al funcionamiento de los algoritmos y su respectiva representación en pseudocódigo; se hará una demostración de la veracidad de los resultados de los algoritmos; se mostrará una prueba de escritorio para entender el funcionamiento de los algoritmos.

Se pretende modelar desde el punto de vista algorítmico y matemático, la distribución de los números primos en los números naturales.

Se presentará una prueba de escritorio del modelo para compararla con la prueba anterior.

La investigación utiliza un método deductivo y analítico y se clasifica como de tipo descriptiva y explicativa.

Hipótesis.

Existe un patrón que rige la distribución de los números primos en los números naturales y puede ser representado a través de modelos algorítmicos.

Instrumentos de medición y toma de datos.

Para la medición y toma de datos se va a utilizar el programa MicroSoft Excel articulado con Visual Basic.

2. Estado Del Arte

Este capítulo pretende mostrar el estado del arte del tema de la distribución de los números primos en los números naturales comentando artículos y tesis relacionadas al tema y estableciendo el porqué estos artículos son importantes para la presente tesis.

MÉTODO GENERADOR DE NÚMEROS PRIMOS GRANDES BASADO EN NTL, TAO MENG, 2008

Resumen

"NTL (Number Theory Library) es una biblioteca de C++, que es desarrollada y sustentada por Victor Shoup de la Universidad de Nueva York. Ofrece una serie de algoritmos sobre la teoría de números y álgebra. Se presenta un método para la generación de números primos que se basa en NTL desde la importancia del generador, y da una prueba en tiempo real para satisfacer la actual exigencia aplicada sobre la base de este método." (Tao Meng, 2008)

El artículo ofrece información importante desde dos puntos de vista principalmente, los cuales son: la complejidad computacional del problema de hallar números primos de forma determinista y el método como tal que aporta para la solución a este problema.

La importancia de lo expuesto anteriormente para el proyecto, es ver la actualidad del problema siendo tan antiguo y mucho más si se observa que el problema se afronta desde el punto de vista de la Ingeniería de Sistemas y se utilizan las herramientas computacionales actuales para darle más relevancia al estudio del tema, más aun considerando que este es un problema originario de la matemática pura observado desde el punto de vista de la Ingeniería de Sistemas.

UNA ARQUITECTURA DE HARDWARE ESCALABLE PARA VALIDACIÓN DE NÚMEROS PRIMOS, CHEUNG, 2004

Resumen

"Este trabajo presenta una arquitectura escalable para la validación de números primos que se enfoca en hardware reconfigurable. La prueba de primalidad es crucial para los sistemas de seguridad, especialmente para la mayoría de los esquemas de clave pública. La fuerte prueba de Rabin-Miller para pseudoprimos ha sido mapeada en el hardware, que hace uso de un circuito para el cálculo de exponenciación modular de Montgomery para acelerar aún más la validación y para reducir el costo de hardware. Un generador de diseño ha sido desarrollado para generar una variedad de multiplicadores de Montgomery escalables y no escalables basados en parámetros definidos por el usuario. El uso de recursos y rendimiento de los diseños, implementados en dispositivos reconfigurables Xilinx, han explorado el uso de números primos muy grandes. Este trabajo demuestra la flexibilidad y soluciones de compromiso en el uso de la plataforma reconfigurable para la creación de prototipos de hardware criptográfico en sistemas embebidos. Se muestra que, por ejemplo, una prueba de primalidad 1024 bits se puede completar en menos de un segundo. Y un chip FPGA de bajo coste XC3S2000 puede acomodar una primalidad escalable de 32k bits con 64 elementos de procesamiento en paralelo." (Cheung, 2004)

Este artículo aborda el problema de la factorización de números naturales desde un punto de vista más amplio que el de otros artículos, ya que no piensa solo en la parte algorítmica de la solución sino que aborda el problema como un todo (software y Hardware) y como si esto no

fuera suficiente piensa en la actualidad y la economía de un modelo escalable y eficiente para solucionar el problema, más aun considerando que el problema crece de manera exponencial generalmente lo que hace de vital importancia la escalabilidad de la solución propuesta.

El artículo es importante para la tesis ya que aporta la posibilidad de pensar en el problema desde todos los puntos de vista y permite una contextualización de la actualidad tecnológica y el costo ya no tan elevado de la capacidad alta de procesamiento necesaria para poder alcanzar la solución al problema.

UN ESTUDIO ESPECULATIVO DEL MODELADO DE RELAJACIÓN ANÓMALO PARA LA DISTRIBUCIÓN DE LOS NÚMEROS PRIMOS, WEN CHEN, 2010

Resumen

> "Hoy en día, muchos investigadores están desconcertados por los problemas sobre números primos, no sólo por sus características complejas y desconocidas, sino también porque es difícil construir un modelo para describir la relajación de la distribución de los números primos en el conjunto de todos los números naturales. Para el mejor conocimiento de los autores, aunque algunos métodos fenomenológicos, como la teoría de Riemann, pueden describir la distribución de los números primos con precisión, la ley para la distribución de los números primos no es clara y el modelo que los gobierna no ha sido fundamentado hasta ahora. En el presente estudio, por primera vez, contamos con el modelo de relajación anómala con el derivado fraccionario para obtener la distribución de los números primos. La comparación con la teoría de los números primos y la teoría de Riemann muestran que el nuevo modelo concuerda con los datos de los números primos." (Wen Chen, 2010)

Este artículo, aborda el problema desde el punto de vista netamente matemático y habla de la actualidad del problema para los investigadores, siendo un problema tan antiguo el hecho de que siga vigente parece ser extraordinario, aunque igualmente es desconcertante un problema que date de tanto tiempo no se haya resuelto aún.

La importancia del artículo para la tesis, radica en cómo el problema es abordado en la actualidad y se hacen pruebas para tratar de entenderlo pero aún no se ha propuesto algo que sea definitivo y aporte nuevas luces sobre el tema.

HARDWARE DIGITAL PARA LA GENERACIÓN DE NÚMEROS PRIMOS, SZECOWKA, P.M., 2012

Resumen

"El algoritmo de pruebas de los números primos se implementó en hardware digital especializado. El diseño fue codificado en VHDL, verificado, sintetizado y cargado en la FPGA, la interfaz propietaria Ethernet desarrollada fue integrada para proporcionar el control externo de la máquina de computación desde un ordenador común. Se añadió el protocolo de resolución de direcciones (ARP) para extender esta conexión más allá de la red de área local. El dispositivo puede probar un número único o generar una serie de números primos por encargo. El prototipo fue construido y probado experimentalmente. La Unidad de prueba de los números primos puede ser replicada para un mayor rendimiento y se utiliza para diversas tareas criptográficas." (Szecowka, P.M., 2012)

Este artículo es visto desde el punto de vista de la Ingeniería de Sistemas y se enfoca en un hardware de propósito especifico para encontrar números primos, con la interesante variante de que puede funcionar en red y así permite su escalabilidad no solo en calidad sino en cantidad, lo cual le da un "*plus*" al método considerando su complejidad computacional.

Desde el punto de vista de la metodología para resolver el problema, este artículo muestra la forma tradicional determinista, el aporte a la tesis está en la posibilidad de usar las redes de datos y el hardware para resolver problemas de este tipo, lo que permite que cualquier aporte en el campo con la ayuda de la Ingeniería de Sistemas se puede unir a distintas áreas y permitir acercarnos a la solución deseada del problema.

SOBRE LA DISTRIBUCIÓN DE LOS NÚMEROS PRIMOS, EL POSTULADO DE BERTRAND, PERAL ALONSO J.C., 2008

Resumen

> "El objetivo de este artículo es presentar brevemente algunos resultados y conjeturas sobre la Teoría de los Números, para centrarse de una manera especial en el famoso postulado de Bertrand. Son muchos los problemas que a lo largo de la historia se han planteado en relación con los números naturales y en particular con la distribución de los números primos. Algunos de ellos han originado una gran variedad de técnicas para poder resolverlos, especialmente en los campos del Álgebra y del Análisis, pero a pesar de toda la potencia matemática puesta en escena son muchos los enigmas por resolver." (Juan Carlos Peral Alonso, 2008)

El artículo da un recorrido histórico por las primeras incógnitas que surgieron sobre los números primos y cómo muchos de ellos aún están vigentes incluyendo el gran problema del comportamiento de la distribución de los números primos en los números naturales, eso si todo visto desde el punto de vista de la matemática pura.

El artículo muestra la forma tradicional como los matemáticos a través de la historia han afirmado su punto de vista sobre lo que consideran qué es la distribución de los números primos en los naturales, dando validez a la importancia del postulado de la tesis de que se puede encontrar un modelo que represente la forma en la que aparecen los números primos en los naturales y así poder entender de una mejor forma el problema en mención.

FORMULA PARA OBTENER EL SIGUIENTE NÚMERO PRIMO EN CUALQUIER SECUENCIA INCREMENTAL EN NÚMEROS NATURALES, RUIZ, S. M., 2004

Resumen

> "En este artículo se da una generalización de varias fórmulas para obtener el siguiente número primo, válida para cualquier sucesión creciente de números enteros positivos en el que sabemos que la expresión algebraica de su enésimo término." (Ruiz, S. M., 2004)

Este artículo recopila varias fórmulas para obtener números primos desde el punto de vista de la programación de computadores y muestra sus resultados.

Para este proyecto es importante ver cómo se afronta el problema desde el punto de vista de la programación de computadores y muestra lo actual de la problemática que encierran los números primos, bien sea solo para resolver un problema de programación.

GENERACIÓN DE GRANDES NÚMEROS PRIMOS DE MANERA ALEATORIA, SZECOWKA, P.M., 2012

Resumen

> "Los algoritmos de clave pública necesitan números primos. Cualquier red de tamaño razonable necesita un montón de ellos. Antes de hablar de las matemáticas de la generación de números primos, en el artículo es representada la Generación de los grandes números primos aleatorios. Nuevo algoritmo de generación de números primos grandes." (Szecowka, P.M., 2012)

El artículo habla de la mayor aplicación de los números primos en la actualidad y es en el cifrado de clave pública en donde es necesario tener números primos de tamaño "grande" y que sea generado de manera aleatoria para así preservar la seguridad de la información.

Este artículo es importante para este proyecto porque muestra una aplicación del problema de los números primos en la actualidad y así deja ver su importancia, dicho sea de paso se ve su importancia desde el punto de vista de la ingeniería de sistemas aplicada a solucionar problemas de la matemática pura.

REDES NEURONALES SIGUIENDO UN ENFOQUE BINARIO APLICADO AL PROBLEMA DE FACTORIZACIÓN DE UN NÚMERO PRIMO, JANSEN B., 2005

Resumen

"Hoy en día, el problema de factorización de un número primo tiene su aplicación a menudo en la criptografía moderna. Redes Neuronales Artificiales (RNAs) se han aplicado al problema de factorización de un número primo. Un número compuesto N es aplicado a las RNAs, y uno de sus factores primos p se obtiene como la salida. Anteriormente, se han propuesto redes neuronales que se ocupan de la entrada y datos de salida en un formato decimal. Sin embargo, la precisión no es suficiente. En este trabajo, se propone una red neuronal con un enfoque binario. La entrada N, así como la salida P deseada se expresaron en una forma binaria. Se espera que la red neuronal propuesta sea más estable, es decir, menos sensible a pequeños errores en las salidas de la red. Las simulaciones se han realizado y los resultados se compararon con los resultados presentados en el estudio anterior. El número de veces de búsqueda necesarios para el verdadero número primo puede ser bien reducido. Por otra parte, la función de densidad de probabilidad de los patrones de entrenamiento se investiga y la necesidad de diferentes técnicas de creación y/o selección de datos se muestra." (Jansen, B., 2005)

El artículo aborda el tema de la factorización de números naturales usando redes neuronales para solucionarlo de manera heurística y aprovechan para analizar los resultados obtenidos con el sistema para probar el poder del sistema experto.

En el artículo se habla de la distribución de los números primos como parte fundamental para poder resolver el problema abordado, todo esto lo hacen más desde un punto de vista de la

Ingeniería en Sistemas que desde el punto de vista matemático, lo cual habla de la importancia del problema en la Ingeniería de Sistemas y nos da luces sobre lo interrelacionados que se encuentran esos problemas entre sí.

SOBRE UNA PRUEBA DE PRIMALIDAD DE SOLOVAY Y STRASSEN, ATKIN, A. O. L. & LARSON, R. G., 1982

Resumen

"Solovay y Strassen proponen una prueba de primalidad basado en el hecho de que para primos **p > 2** tenemos **(a / p)** = a $^{(P-1)/2}$ (mod p), donde **(a / p)** es el símbolo de Jacobi. Se demuestra aquí que la prueba fuerte de pseudoprimo es mejor, en el sentido de que nunca se toma más tiempo, ni es menos eficaz y, a veces es más rápido o más eficaz. También se discute la probabilidad de error en la prueba fuerte pseudoprimo, y demostrar que nunca es mayor que 1/4." (Atkin, A. O. L., & Larson, R. G. 1982)

El artículo se refiere a un método para hacer un test de primalidad a un número natural específico y se trata de tener herramientas que nos permitan decidir si un test de primalidad es o no más eficiente que otro para así poder determinar cual usar.

Este artículo es importante para la tesis ya que desde ambos puntos de vista (el matemático y el de la Ingeniería de Sistemas) nos aporta una visión sobre la eficacia y rapidez de los métodos para saber si un número es primo o no, sin olvidarnos de un problema aparentemente mayor dificultad que es el de los pseudoprimos.

SOBRE PROBLEMAS DE CRIPTOGRAFÍA: PRUEBAS DE PRIMALIDAD Y FACTORIZACIÓN DE ENTEROS, POPE S., 2001

Resumen

"Esta tesis analiza los problemas clásicos de las pruebas de primalidad y factorización de enteros. Se discute un test de primalidad determinístico realizado por GL Miller, el cual bajo el supuesto de la Hipótesis de Riemann Extendida, se ejecuta en un tiempo polinomial.

También se discute un algoritmo de factorización de HW Lenstra, que asume algunas conjeturas no probadas pero plausibles, y se ejecuta en un tiempo subexponencial. Estos son problemas que tienen significativa relevancia en el mundo de la criptografía, y la complejidad inherente a estos problemas es de gran interés práctico y teórico.

La última parte está dedicada a algunos resultados de esfuerzos o intentos originales. En particular, se prueba el resultado de la complejidad que implica el problema de la factorización: bajo el supuesto de la hipótesis de Riemann Extendida se demuestra que la factorización reduce en un tiempo polinomial el problema de encontrar el orden de un elemento en un grupo finito." (Pope, S., 2001)

Este artículo hace una comparación entre varios métodos de testeo de primalidad deterministas y heurísticos y aborda el problema desde el punto de vista matemático haciendo un esfuerzo por convertir un problema de complejidad computacional exponencial en uno

polinomial tomando como referencia la hipótesis de Riemann extendida, lo cual no permite sacar conclusiones significativas sobre el problema.

El artículo es importante para la tesis ya que se refiere a la complejidad computacional de las soluciones a los problemas relacionados a los números primos y cómo se entrelazan con otros problemas que pueden ser considerados más importantes, como son la hipótesis de Riemann etc., todo esto desde el punto de vista matemático sin dejar de lado su complejidad computacional.

TEST DE PRIMALIDAD USANDO CURVAS ELÍPTICAS CON MULTIPLICACIÓN COMPLEJA POR $\mathbb{Q}(\sqrt{-7})$, WONG, A., 2013

Resumen

"En esta tesis, se da una prueba de primalidad determinista que probará el "compositeness" o primalidad de ciertas formas de números. Hacemos esto mediante curvas elípticas con multiplicación compleja por $\mathbb{Q}(\sqrt{-7})$. En particular, este método funciona en ciertas formas de números para los cuales el estándar de las pruebas de primalidad "n-1" y "n + 1" no son aplicables." (Wong, A., 2013)

Esta tesis aborda el tema de los test de primalidad desde un punto de vista matemático con una complejidad alta en su contenido y se centra en ciertos tipos de números especiales que se comportan de una manera particular.

Este artículo es importante para la tesis ya que da una idea sobre a qué nivel de profundidad y complejidad se puede llegar al abordar los problemas concernientes a los números primos y así ver que tan actuales y difíciles son las soluciones a estos tipos de problemas aun si se cuenta con la alta tecnología.

3. Recorrido histórico

Este capítulo pretende hacer un recorrido histórico del problema de la distribución de los números primos en los números naturales, además de identificar factores que repercuten en la historia de los algoritmos sobre números primos y de las soluciones para encontrarlos.

Durante más de 2000 años las mentes más maravillosas del mundo se han visto superadas por un problema matemático sin comparación, se trata de un problema tan difícil que ha atormentado a aquellos matemáticos que osaron resolverlo, algunos desistieron desesperados, otros enloquecieron con el tiempo e incluso unos cuantos intentaron suicidarse, no obstante, es un acertijo que desempeñó un papel crucial para la victoria de los aliados sobre la Alemania Nazi durante la segunda guerra mundial, la cual fue imprescindible para el nacimiento del computador y que arrojó una luz crucial para entender el comportamiento de los átomos. En la actualidad el mundo financiero que se desarrolla en Internet depende por completo de su naturaleza impenetrable; La solución al acertijo pondría por completo la economía del planeta a sus pies, por eso no debe sorprender que se haya establecido una recompensa de 1.000.000 de dólares a aquella persona que logre descifrarla, ahora bien ¿cuál es el Santo Grial de las matemáticas?, un misterio que lleva siglos atormentando a los matemáticos de todo el mundo, dicho misterio es conocido como el misterio de los números primos y es el problema matemático sin resolver más importante de la historia, así quien lo descifre alcanzará la inmortalidad.

¿Que son los números primos? y ¿por qué son tan importantes? a todos los niños se les enseñan los principios básicos “Un número primo, es un número que es divisible por sí mismo y 1 únicamente” pero lo que no les enseñan a los niños es el porqué estos números indivisibles son tan importantes y es el hecho de que son la base de las matemáticas, todos los números que no son primos se pueden construir multiplicando números primos, los números primos pueden ser considerados los átomos de las matemáticas.

Los primeros intentos de descifrar la importancia de los números primos, datan de la antigua Grecia, ellos establecieron los principios matemáticos sobre los que se ha trabajado desde entonces.

Las bibliotecas y academias de la Grecia Antigua, empezaron a llenarse de tablas que registraban números primos cada vez más altos, alrededor del año 3.000 a.C. Euclides, uno de los primeros grandes matemáticos de la historia descubrió que los números primos eran infinitos, demostrándolo de manera irrefutable y dicha demostración es una pieza clave del razonamiento matemático, sin embargo hubo algo que no fue capaz de entender, Euclides no podía predecir que números eran primos, no veía ningún patrón que le ayudara a entender donde encontrarlos.

Si se pudieran imaginar los números en fila, da la sensación de que los primos están colocados al azar; la pregunta es ¿existe el orden entre ellos? ¿hay alguna manera de entenderlos? ¿qué patrón siguen dentro de las matemáticas?

Al igual que las estrellas en el cielo infinito los números primos aparecen sin orden alguno en el universo de los números, algunos están cerca unos de otros, otros

mantienen la distancia, al parecer no hay ningún patrón que los defina, no tienen sentido y si hay algo que atormente a un matemático son los patrones y el sentido, las matemáticas consisten en buscar patrones que organicen el caos numérico que nos rodea, en encontrar la música que une a estos números y de todos ellos, los primos son los que más retos suponen para un buscador de patrones. El problema de este patrón o la aparente inexistencia del mismo, trajo de cabeza a todos los matemáticos del mundo desde la era de Euclides, los números primos se burlaron de las mentes matemáticas más importantes de los últimos 2.000 años.

El primer avance al respecto no llegaría hasta el siglo XVIII, el descubrimiento fue hecho por un joven alemán de 15 años que se convertiría más adelante en uno de los matemáticos más importantes de la historia, Carl Friedrich Gauss, de la noche a la mañana Gauss se convirtió en una estrella matemática gracias oportunamente a la astronomía, un planeta descubierto recientemente (Sirius) había desaparecido del cielo y se había escondido tras el resplandor del sol, los astrónomos se desesperaron pero Gauss logró encontrar un patrón matemático que explicara la ruta del planeta y señaló a los astrónomos donde encontrarlo, y tal como las matemáticas le indicaron, allí apareció aquel planeta juguetón.

Pero no eran las estrellas las que apasionaban a Gauss sino los números, fue un regalo que le hicieron por su decimoquinto cumpleaños lo que cambiaría el curso de la historia, un libro lleno de tablas con números; al final del mismo había una lista de números con la que Gauss se obsesionó desde el principio, eran números primos, y se pasaba horas escudriñando esos números para intentar descifrar sus secretos, al final hizo un descubrimiento memorable.

Por más que observaba esa lista de números primos, el joven Gauss al igual que numerosas generaciones de matemáticos anteriores no lograba encontrar un patrón para ellos y la manera de predecir donde están, dando la sensación de que los números primos se sucedían únicamente al azar, fue entonces cuando Gauss realizó uno de los movimientos más clásicos del arsenal de un matemático, cuando las cosas se complican demasiado pasemos al razonamiento lateral, intentemos plantear el problema de otra manera, hagámonos otra pregunta, en vez de intentar predecir exactamente que números son primos, Gauss se planteó cuantos números primos había.

Gauss solía contar cuantos números primos había en cada bloque de mil. Euclides había establecido que había un número infinito de números primos y Gauss empezó a contar cuantos exactamente había hasta el 10, había hasta el 100, cuantos hasta el 1.000 etc., a medida que contaba, los números primos parecían escasear cada vez mas pero ¿había algún modo de saber cómo?

Para Gauss, la manera en que disminuían los números primos era tan aleatorio como el juego de los dados, pero a medida que contaba los números se dio cuenta de que podía calcular la probabilidad de conseguir uno primo, por ejemplo entre el 1 y el 100 hay 25 números primos, lo que quiere decir que tenemos una probabilidad entre 4 de conseguir uno primo, pero entre el 1 y el 1.000 solo tenemos una probabilidad entre 6 de conseguir un número primo, a lo mejor la naturaleza escoge los números usando un dado de números primos. ¿Podría Gauss predecir el número de lados del dado? a medida que subían los números primos cuanto más contaba para calcular la probabilidad de encontrar un número primo, más se acercaba Gauss a un posible patrón, a pesar de la aleatoriedad

de los números primos, ante sus ojos se iba formando una regularidad asombrosa entre la niebla.

Cada vez que añadía un cero, Gauss comprobó que la proporción de números primos disminuía de forma regular con el 2 como clave, es decir, desde 10.000 hasta 100.000 y 1.000.000 la probabilidad de obtener un número primo descendía de 1 entre 8 a 1 entre 10 y 1 entre 12 respectivamente, si se quiere contar números primos hasta el 10.000 se necesitará un dado de 8 caras y si se quiere contar primos hasta el 1.000.000 entonces se necesitará uno de 12 caras; era como si la naturaleza escogiera los números primos con un dado cuyas caras crecieran de forma uniforme cuanto más grande eran los números primos.

Cuando Gauss unió todos los números primos en una grafica, el resultado mostraba una línea ascendente en una progresión dentada, una especie de escalera que saltaba cada vez que aparecía un número primo, pero se cansó de los escalones, con su dado de números primos, Gauss dibujó una segunda gráfica que calculaba los números primos de la escalera hasta el infinito y en vez de concentrarse en los detalles de cada peldaño individual, intentó predecir la tendencia general de los mismos, de ese modo dedujo que el número medio de números primos descendía siguiendo un hermoso patrón, esta era la primera prueba de que los números primos también seguían un patrón, las generaciones anteriores habían oído los números primos 1 a 1, nota a nota, incapaces de escuchar la melodía completa, pero echando un vistazo general a la partitura, Gauss logro identificar el tema musical que dominaba en la música de los números primos.

Gauss supo que su hallazgo no significaba más que un cálculo aproximado al número de primos existentes pero creía que había dado un gran paso adelante, sin embargo, no tenía pruebas que mostrar y para un matemático las pruebas lo son todo.

Gauss guardó sus descubrimientos hasta más tarde; entre sus discípulos se encontraba un joven matemático que se encargaría del siguiente gran descubrimiento sobre los números primos, Bernhard Riemann.

El director del colegio al que asistió Riemann, se dio cuenta que aquel niño introvertido poseía una habilidad nata e inusitada para las matemáticas, para animarlo ofreció al joven Riemann la posibilidad de disfrutar por completo de su biblioteca y de su magnífica colección de libros matemáticos, aquello supuso para Riemann un mundo nuevo lleno de posibilidades, un lugar en el que sentirse bajo control y como en casa, de repente frente a él surgió un mundo perfecto e idealizado lleno de números, que se convirtieron en sus mejores amigos, en uno de los libros de esta biblioteca el joven Riemann descubrió por primera vez el mundo de los números primos, cuentan que leyó unas 859 páginas en solo 6 días y que se lo devolvió a su profesor diciendo es un libro fantástico, me lo sé de memoria.

Lo que Riemann había aprendido, terminaría floreciendo de una manera espectacular unos años más tarde, atraído por la presencia de Gauss, Riemann entro a estudiar en 1846 en la universidad de Gotinga, esta pequeña ciudad medieval donde los hermanos Grimm escribieron la mayoría de sus cuentos infantiles, no ha cambiado mucho desde la época de Riemann, pero Gotinga estaba a punto de vivir una revolución matemática.

Las matemáticas tradicionalmente se han visto como una herramienta para el cálculo, un sirviente para otras ciencias, en Paris, los matemáticos construían barcos y cañones pero en Alemania el tema iba más allá del reconocimiento, los matemáticos estaban entrando en un mundo mucho más abstracto y creativo lleno de formas nuevas y extrañas de figuras geométricas y números.

Riemann se sumergió por completo en la revolución matemática de Gotinga, su doctorado introdujo una nueva teoría sobre la geometría abstracta y desde entonces ha sido considerada como uno de los aportes más importantes a las matemáticas, pero a pesar de su éxito académico, Riemann prefería mantenerse al margen de todo. Era un hipocondriaco susceptible de sufrir brotes depresivos que decidía esconderse del mundo en su trabajo y detrás de una poblada barba negra, fue su carácter introvertido lo que lo convirtió en el sucesor de Gauss, cuando realizó uno de los descubrimientos que transformarían la historia de los números primos, Riemann se dio cuenta de repente de algo crucial mientras trabajaba con una formula llamada función Z, Riemann se dio cuenta de que podía usar esa función Z para construir un escenario matemático tridimensional, como si de un espejo mágico se tratara, la función lo llevo de un universo de números estancados a un número nuevo de geometría, Riemann contempló ese espejo mágico, tomo aire y se adentro en él.

Al principio, Riemann desconocía que la función Z estuviera relacionada con los números primos, pero al otro lado del espejo, empezó a darse cuenta de que los contornos del paisaje creados por la fórmula, podrían descifrar los secretos de estos números, hacia el Este se extendía una amplia meseta, pero cuando Riemann miró hacia el Oeste descubrió una gran cordillera, una de las montañas ascendía al infinito, sin embargo lo

verdaderamente importante no era la altura de las cumbres, sino que fue en la profundidad de los valles donde encontró lo que llevaba tiempo buscando, en unos puntos clave, la superficie de este grafico tridimensional se hundía hasta la altura 0 al igual que aquellos puntos geográficos que se encuentran al nivel del mar, los matemáticos los llaman puntos cero, Riemann se dio cuenta de la importancia de estos puntos cuando descubrió que mantenían una conexión inesperada con la distribución de números primos, una conexión que todos los matemáticos que siguieron a Riemann hasta el otro lado del espejo, describieron como fascinante, se necesitó un gran salto imaginativo para establecer ese punto de conexión entre el universo de los números y el mundo de la geometría, pero el descubrimiento de Riemann le permitió mejorar de forma considerable el enfoque que Gauss había realizado anteriormente, Gauss se había valido del dado de los números primos, para intentar adivinar cuantos primos había en el universo de los números, pero el cálculo final, no era más que una aproximación y a los matemáticos les gustan las cosas exactas, Riemann descubrió que la ubicación precisa de cada cero se podía usar para corregir el intento de Gauss, como si cada cero constituyera una nota musical cuyas vibraciones perturbaran el intento de Gauss para acercarse más a la escalera real de los números primos y la combinación de todas esas notas la que origina la melodía musical que mejora la teoría de Gauss dando el número exacto de primos a medida que contamos y contamos, uno de los apuntes más relevantes del descubrimiento de Riemann es que los ceros que al principio no parecían tener relación alguna con los números primos se podían utilizar para entender como están distribuidos estos últimos.

El descubrimiento de Riemann supuso un hito matemático de igual importancia a la teoría de Einstein sobre la equivalencia entre masa y energía, en este caso los números

primos se convierten en música, Riemann descubrió el mapa del tesoro que escondía los secretos de los primos, estos puntos al nivel del mar o ceros, servían para orientarnos, fue entonces cuando Riemann se dio cuenta de algo aun mas importante, a medida que registraba la ubicación de los 10 primeros ceros, noto que surgía un patrón, estos ceros no se encontraban dispersos al azar, sino que estaban perfectamente alineados a lo largo de todo el paisaje, Riemann no quiso creer que el hecho de que los primeros 10 ceros se encontraran en fila fuese una coincidencia y asumió que todos los ceros por infinitos que fueran se encontraban en esa misma línea, una línea recta.

Su conjetura es hoy en día conocida como la hipótesis de Riemann, ¿qué implicaciones tenía ese patrón en los números primos? si bien Riemann estaba en lo cierto y los ceros se encontraban perfectamente alineados, el intento de Gauss habría sido mucho más certero de lo que él mismo habría imaginado, significaría que el dado de los números primos los distribuía equitativamente por todo el universo de los números, el descubrimiento de Riemann nos muestra la belleza de la música de los números primos.

Si todos los ceros se encontraban alineados, tal y como Riemann sugería, entonces existiría un equilibrio delicado entre todas las notas musicales que eran emanadas de los ceros pero si Riemann se equivocaba y al final había algún cero descolocado, lo que ocurriría sería que un músico aparte estaría arruinando la función.

Riemann no creía en esa posibilidad, él estaba convencido de que no importaba cuanto contáramos, cuanto viajáramos por ese paisaje tridimensional, todos los ceros estarían en fila, demostrando que la teoría de Gauss se acercaba mucho al número real de números primos.

El espejo mágico de Riemann transformó nuestra visión de los primos, conectando 2 ámbitos diferentes de las matemáticas, los ceros del paisaje con los números primos dando con una de esas conexiones inesperadas siendo uno de los momentos más grandes para los matemáticos.

Riemann publicó su descubrimiento en un documento de 9 páginas en 1.859, a pesar de la naturaleza revolucionaria de su nueva teoría, Riemann intentó restarle importancia añadiendo que era muy posible que todos los puntos cero se encontraran en la misma línea, el problema era que no tenía ninguna prueba irrefutable, no obstante la falta de demostraciones plausibles no evitó que el nombre de Riemann cobrara fama, en la universidad de Gotinga lo ascendieron a jefe del departamento de matemáticas, exactamente el mismo puesto que antes había ocupado su predecesor Gauss.

Riemann no vivió lo suficiente para saborear su éxito, la guerra abierta entre Rusia y Hannover invadió las calles de Gotinga, Riemann huyo a Italia convencido que si se quedaba una bala acabaría con su vida en algún fuego cruzado, pero lo peor lo esperaba allá, a las 3 semanas de su llegada a Italia moriría de Tuberculosis, tenía solo 39 años.

No tardaron en reconocerlo como uno de los matemáticos mas grandes de la historia, sin embargo su reputación podría haber llegado a mas de no haber sido por su efectiva ama de llaves, que al ver la cantidad de papeles que Riemann había dejado en su habitación, la mujer quemó gran parte de los manuscritos aún inéditos, ya nunca sabremos qué tan cerca estaba Riemann de probar su hipótesis, sin embargo sus ideas sirvieron de testigo a generaciones futuras de matemáticos cuyo sueño ha sido desde

entonces y hasta ahora demostrar que Riemann estaba en lo cierto sobre la ubicación de los ceros.

A principios del siglo XX, la hipótesis de Riemann se había convertido en uno de los misterios matemáticos más maravillosos del mundo, todavía nadie había logrado demostrarla; pero poco después de la primera guerra mundial, llego el siguiente gran descubrimiento, pero no tuvo lugar en Gotinga sino al otro lado de Europa.

Al principio del siglo XX, Inglaterra se había convertido en algo así como un estanque matemático, las grandes universidades inglesas se habían mantenido al margen de la revolución matemática que se extendió por los 5 continentes durante el siglo XIX, por eso resultó aun más sorprendente que la siguiente pieza del problema de los números primos saliera de Cambridge.

El hombre que despertó a Inglaterra de su modorra matemática se llamaba Godfrey Harold Hardy y estaba obsesionado con los números primos.

En una ocasión llegó a afirmar que los números primos eran mejor para leer que los resúmenes de futbol durante el desayuno. La mayor aportación de Hardy al enigma de los números primos, no tardaría en llegar.

Riemann había dicho que había tantos puntos cero en la línea que era muy probable que todos estuvieran en ella, Hardy demostró que había al menos infinitos puntos cero en esa línea, de ese modo reivindicaba cierta veracidad en la hipótesis de Riemann, aquel descubrimiento sonaba como si Hardy hubiera demostrado realmente la hipótesis de Riemann, pero infinito es una palabra trampa, es posible demostrar que hay

infinitos puntos cero en la línea y aun así, habrá infinitos puntos cero que no hemos comprobado o lo que es peor, infinitos puntos cero que pudieran estar fuera de la línea.

Si se imaginase que se estuviera en un hotel con infinitas habitaciones, se pudiera comprobar todas las habitaciones pares para ver si están ocupadas, pero a pesar de haber comprobado un número infinito de habitaciones, aún quedarían las infinitas habitaciones impares sin mirar, en el caso de Hardy en vez de comprobar si las habitaciones estaban ocupadas o libres, comprobaba si los puntos cero estaban o no sobre la línea, por desgracia Hardy ni siquiera había conseguido demostrar aun, si la mitad de los ceros estaban en la línea, su descubrimiento era extraordinario, pero quedaba demasiado camino por delante.

Una mañana de 1913 Hardy encontró sobre su escritorio una carta recién llegada que contenía teoremas fantásticos sobre los números primos, el autor de la misiva afirmaba poseer una fórmula que calculaba el número de primos entre 1 y 1.000.000.000 con un margen de error minúsculo, de ser verdad sería un gran paso adelante, Hardy estuvo a punto de tirar la carta a la basura, al fin y al cabo las matemáticas atraen a un gran número de excéntricos, pero aquella misma noche comprobó que los teoremas funcionaban de verdad, la carta que había recibido Hardy, la habría escrito otro gran genio y por si eso fuera poco venía del otro lado del mundo.

El autor de aquel teorema se llamaba Srinivasa Ramanujan, un chico de 23 años que trabajaba para la autoridad portuaria de Madras por 20 rupias al mes, al igual que Hardy él estaba obsesionado con los números primos, en su puesto de trabajo en vez de aburrirse contando los barcos que entraban y salían, se pasaba la jornada laboral anotando

cálculos y cálculos sobre números primos, después del trabajo él se dirigía a caminar descalzo por la playa mientras seguía pensando en los números primos, era imposible que estuviera al tanto de los avances matemáticos de occidente y aun así fue capaz de redescubrir por si solo la mayoría de los resultados a los que había llegado Riemann 50 años antes.

Lo que convierte a esta historia en algo aun más singular es el hecho de que Ramanujan era prácticamente autodidacta, en la escuela primaria, mostró su precocidad matemática pero su arrogancia sobre cualquier otra asignatura, impidió que tuviera acceso a la universidad.

Ajeno a las convenciones habituales de las matemáticas, Ramanujan se adentró en el problema de los números primos con el entusiasmo de un niño, fue precisamente su ingenuidad al respecto lo que lo convirtió en uno de los grandes.

Ramanujan cruzó los mares desde Madras hasta Inglaterra a donde llegó en 1914, poco antes de la irrupción de la primera guerra mundial, Ramanujan y Hardy trabajaron conjuntamente en diversos proyectos matemáticos, entre ambos lograron tener éxito, juntos alcanzaron soluciones brillantes a numerosos retos, pero el enigma de los números primos aún lo seguía siendo.

Hardy ya había advertido de la malicia de estos números y ellos se negaron a revelar sus secretos, es probable que el genio de Ramanujan hubiera logrado vencerlos al fin de no ser por una depresión que acabó con su estado de salud. Ramanujan murió tan solo a los 33 años de edad.

El problema que planteaba la hipótesis de Riemann seguía obsesionando a Hardy pero con el tiempo fue perdiendo la ilusión porque cada vez se sentía más incapaz de hallar la solución al igual que alguna vez lo hizo Ramanujan, Hardy intentó suicidarse sin éxito; sin duda la hipótesis de Riemann ponía a prueba a los más fuertes.

El 8 de junio de 1.954, uno de los matemáticos mas importantes del mundo se quitó la vida, se envenenó con cianuro, aquel matemático se llamaba Alan Turing, fue un autentico erudito, suele ser llamado el padre de la informática, Turing saltó a la fama como uno de los matemáticos que logró descifrar el código secreto alemán, lo que no llegó a saberse tanto es que la hipótesis de Riemann desempeñó un papel fundamental en el proceso de descifrado.

Durante la segunda guerra mundial enviaron un grupo de matemáticos a Bletchley Park para que intentaran descifrar los mensajes alemanes que se habían interceptado, para Turing y sus compañeros, Bletchley era como estar en Cambridge, aquí descifraban mensajes secretos a diario, una especie de pasatiempo del que dependían muchas vidas.

Cuando no se encontraba ocupado descifrando mensajes, la mente de Turing se volvía de nuevo hacia el problema matemático en el que tanto tiempo había estado trabajando antes de estallar la guerra, un problema que le había planteado uno de los tutores de Cambridge, GH Hardy, era claro está, el de la hipótesis de Riemann.

El enfoque de Turing se diferenció del de los demás matemáticos en 2 aspectos vitales, el primero, que empezó a considerar que la hipótesis de Riemann fuera en realidad falsa y el segundo, que decidió demostrar que era falsa con una táctica completamente revolucionaria.

Turing construyó una máquina, aquella máquina exploraría el paisaje tridimensional de Riemann intentando demostrar que la hipótesis era falsa, para ello buscaría puntos cero que estuvieran fuera de la línea.

A finales de los años 30 la habitación que tenía Turing en Cambridge había desaparecido bajo numerosas ruedas y dispositivos de engranaje, pero la guerra interrumpió su trabajo, fue entonces cuando lo destinaron a Bletchley Park, aunque no había logrado terminar la máquina, el trabajo que si había realizado constituiría uno de los cimientos de una máquina nueva que lograría descifrar los códigos enemigos secretos.

La máquina de Turing alcanzó un éxito mundial, rebajo la duración de la guerra en al menos 2 años y salvó numerosas vidas, quizás no sea aventurarse demasiado si se afirma que el trabajo que Turing había realizado sobre la máquina de Riemann antes de la guerra, fue lo que facilitó al final la victoria sobre los nazis.

Después de la guerra, Turing siguió usando máquinas para resolver problemas, pero su experiencia en Bletchley le enseñó que sería mucho más útil construir una que se pudiera programar para hacer mas de una tarea, con tubos de rayos catódicos y tambores magnéticos, Turing creó el prototipo del ordenador moderno.

Una de las primeras misiones en las que se embarcó Turing con su computadora, fue la de buscar los ceros de Riemann y obviamente se encontró con que todos estaban sobre aquella línea recta.

La máquina nueva de Turing logró ubicar los primeros 1.104 ceros todos ellos en la línea y después se rompió, pero no fue la máquina lo único que se le estropeó a Turing,

su propia vida empezaba también a sufrir desajustes a tal límite que lo llevaron al suicidio.

Pero las nociones de informática de Turing siguieron hacia adelante, él había iniciado una marcha hacia la era moderna, una era en la que los ordenadores mejorarían el alcance humano en el cómputo de los números primos, en 1.952 un ordenador descubrió el primer número primo que estaba más allá de la capacidad de cálculo del ser humano.

Hasta el año 2.006, el número primo más grande que se había encontrado tenía más de 7.800.000 dígitos.

Tal y como había propuesto Turing, las computadoras se podían usar para explorar partes del paisaje de Riemann que hasta entonces habían permanecido inexpugnables, en el 2.005 se publicó un informe que afirmaba que los primeros tres trillones de ceros estaban todos en la famosa línea recta, puede parecer excesivo llegar a semejante número de cálculos lo cual le da validez al problema de Riemann.

Si se considerara que la línea de Riemann parte de Gotinga, se podría decir que Riemann la llevó a las afueras de la ciudad con sus cálculos, Turing entonces la habría acercado a la luna y gracias al ordenador, se ha podido viajar a 100 años luz del punto inicial, como si de una nave espacial se tratara los ordenadores envían mensajes desde puntos extremadamente lejanos en el universo de los números y aun así todos los ceros que en él se encuentran confirman la hipótesis de Riemann. A medida que avanzaba el siglo XX, los matemáticos empezaban a reconocer que se habían atascado y entonces en los años 70 se produjo un nuevo descubrimiento crucial sobre el enigma de los números primos, un descubrimiento llegado del lugar más inesperado.

El instituto de estudios avanzados de Princeton es el paraíso para los cerebros más brillantes del mundo matemático y científico, la cultura matemática alemana no logró sobrevivir a la violencia de la segunda guerra mundial y muchos de los matemáticos judíos más eruditos de la época huyeron a América en busca de asilo, entre ellos Albert Einstein.

Desde la segunda guerra mundial, Princeton se ha postulado como la institución matemática más importante del planeta.

En 1972 un joven matemático norteamericano llamado Hugh Montgomery se pasaba el día debatiendo sus nuevas ideas en el instituto, pero a diferencia de sus predecesores, Montgomery decidió no mirar a si, sino a cómo estaban distribuidos los ceros que Riemann había colocado sobre la línea.

Lo que descubrió, revolucionaría de nuevo las matemáticas, el patrón que se apreciaba era el de números relativamente poco cercanos.

Todos los días a las 3 en punto, los académicos se reunían en la sala común para uno de los rituales más importantes de todos los departamentos matemáticos, el té de la tarde, aquel día a Montgomery le presentaron a un famoso físico Freeman Dyson, el cual no dudo en relacionar la teoría de los ceros con los valores de energía de su teoría de las matrices aleatorias.

Lo que descubrieron Montgomery y Dyson fue que el comportamiento primario de los átomos, que son los cimientos básicos de la materia se correspondía considerablemente con el comportamiento primario de los números primos, los cimientos básicos de las matemáticas.

Se trataba de una conexión inesperada que abría las puertas hacia un nuevo enfoque sobre la hipótesis de Riemann.

A pesar de los grandes descubrimientos, a los matemáticos todavía se les resiste hallar una prueba que demuestre la hipótesis de Riemann; los números primos mantienen su halo místico, hasta hace unos pocos años solo los matemáticos parecían interesarse realmente por estos números misteriosos, pero un cambio de planes de última hora colocó a los números primos en el eje central de un mundo duro y sucio, la comunicación electrónica.

Cada vez que se realiza una transacción Online, se están utilizando números primos para codificar los detalles de la tarjeta de crédito, la seguridad del sistema se basa en la dificultad que entraña desmenuzar un número hasta los primos que lo constituyen.

El sistema es completamente seguro porque todavía no se entiende los números primos, si se lograra demostrar la hipótesis de Riemann, se aprendería mucho más sobre el comportamiento de los números primos, quizás incluso se podría ser capaz de averiguar los números primos que conforman cifras muy elevadas, un descubrimiento de ese tipo colapsaría el sistema financiero electrónico a nivel mundial.

No resulta especialmente sorprendente que un empresario haya estipulado una recompensa de un millón de dólares para quien logre descifrar la hipótesis de Riemann, pero a los matemáticos no les interesa el dinero, la solución a esa hipótesis tendría consecuencias tan interesantes para el ámbito de las matemáticas que la mayoría vendería su alma por una prueba.

3.000 años después, el enigma de los números primos sigue derrotando a generaciones de matemáticos, a pesar de las emocionantes conexiones que se han encontrado con la física, la criptografía y los ordenadores, a los matemáticos aún les queda mucho para dar con el resultado final, un resultado que puede llegar en cualquier momento y en cualquier lugar, pero lo que sí es seguro es que aquella persona que logre demostrar la hipótesis de Riemann se le recordará para siempre como el matemático que hizo cantar a los números primos. (Du Satoy, M. 2005)

4. Solución del problema

Este capítulo explica el porqué se escogió este tema, que fue lo que se hizo a nivel conceptual y de programación y aclara cuáles son los insumos necesarios para abordar el tema tratado en este trabajo, la forma en que se utilizaron dichos insumos y además mostrar los resultados obtenidos al finalizar la investigación.

Motivación

La inquietud investigativa en la que se basó para elegir el tema de la distribución de los números primos en los números naturales surgió al conocer cómo la RSA (empresa encargada de la seguridad de la información a nivel mundial) basaba toda la seguridad del comercio electrónico del mundo en el problema de factorizar números naturales de gran tamaño, los cuales constaban de solo 2 factores primos relativamente grandes también y además distantes entre sí.

El origen del problema puede ser explicado a través de una anécdota muy interesante en la que John McCarthy (inventor del lenguaje LISP y teórico de la inteligencia artificial) propuso un problema que resolvió Michael Rabin (conocido por ser el creador de interesantes algoritmos informáticos).

El problema es el siguiente: disponemos de un puñado de espías dispuestos a entrar en el territorio enemigo. Deseamos evitar que sean atacados cuando traten de regresar a territorio propio y también la infiltración de espías enemigos. Así, cada espía ha de presentar una contraseña a nuestros guardias fronterizos, que éstos comprobarán. Aunque tenemos confianza en nuestros espías y en la lealtad de los guardias, existe el temor de que éstos puedan revelar el

secreto. ¿Qué información habrían de recibir los guardias, y de qué modo han de presentar los espías sus contraseñas, de manera que sólo los agentes propios puedan pasar, y nadie más?

La solución que dió Michael Rabin fue: el espía selecciona al azar dos números primos muy grandes y facilita a los guardias fronterizos sólo el producto de ambos. A su regreso, el espía le da al guardia los dos números; el guardia los multiplica y comprueba que su producto coincide con el que le fue dado al salir. Incluso aunque el guardia revelase el producto, no habría forma práctica de que los adversarios determinasen los factores primos, si éstos son lo suficientemente grandes.

Este principio, por cierto, es en el que se basan los algoritmos de encriptación que utiliza la RSA con el fin de garantizar la seguridad de su sistema de encriptamiento asimétrico o de clave pública, basado en la complejidad computacional que implica el factorizar números grandes múltiplos de dos primos.

La RSA con el fin de probar que su sistema funciona publicó entre otros, el reto de factorización, el cual consistió en dar a conocer a los interesados una serie de números, para que ellos intentaran encontrar sus factores primos, todo esto incentivado por una retribución económica para quien hubiera podido encontrar la solución.

El tema de investigación entonces es abordado desde un nuevo punto de vista, el cual busca encontrar los números primos de forma tal que no se desperdicie ningún ciclo, como sí lo hace por ejemplo la criba de Eratóstenes al ser programada.

Después del análisis de cómo funciona la criba de Eratóstenes, la cual puede considerarse vigente aun en nuestros días, se hace una mejora para que no se desperdicien recursos y se

realizó una prueba que permitió encontrar algo interesante que daría inicio al estudio de este tema y más tarde concluiría en aportes interesantes respecto al mismo.

Con base en lo anterior se decide hacer una tesis completa hablando de la relación de la Criba y el problema de la distribución de los números primos en los naturales, cabe anotar que este problema es considerado “El Santo Grial de las matemáticas” y fue de gran importancia para el desarrollo de la informática tal y como la conocemos en la actualidad.

Insumos

Se va a explicar de manera sintética cuáles son los insumos qué se necesitan para abordar el tema a continuación.

Algo importante es el hecho de que la parte matemática necesaria es muy sencilla ya que no es necesario utilizar, por ejemplo, el concepto de raíces cuadradas como en la mayoría de los métodos que se conocen para hallar números primos; a nivel de programación no se manejan residuos como podría pensarse para resolver el problema, de hecho solo se necesita saber multiplicar y hacer unas cuantas divisiones, teniendo en cuenta solo la parte entera por estar hablando de números naturales.

Desde el punto de vista de programación, con la utilización de una herramienta como Visual Basic de Excel, se muestra la sencillez de los cálculos y la poca necesidad e importancia de utilizar herramientas especializadas para la solución y estudio del problema.

Con la utilización de vectores (arreglos) a nivel de programación para la solución del problema, se da un salto importante para disminuir la complejidad computacional del problema, ya que permite hacer uso de la criba para la eliminación de números no primos.

Ya definidos los insumos necesarios, es importante explicar cómo fueron estos usados y a nivel conceptual entender qué fue lo que se hizo con ellos.

Lo primero que se hizo fue hacer un programa en Visual Basic que permitiera encontrar los números primos hasta un número dado y los mostrara de una forma que se pudieran comprobar en una hoja de cálculo.

Después se procedió a hacer lo mismo para la distribución y hacer las respectivas pruebas de los algoritmos.

Ya sabiendo la forma cómo se usaron estos insumos y de saber qué fue lo que se hizo a nivel conceptual, se procede a explicar qué fue lo que se hizo a nivel de programación.

La Criba

La criba utilizada para el estudio, es un algoritmo que permite hallar todos los números primos menores que un número natural dado *n*.

Aunque existen actualmente una buena cantidad de métodos para encontrar los números primos, surge la inquietud de que debe existir una forma de encontrar una criba similar a la de Eratóstenes que se comporte de una forma en la que no se desperdicie ningún ciclo y solo marque los números primos sin repetir, de esta forma tratar de encontrar un patrón que permita

definir el comportamiento de la distribución de los números primos en los números naturales, el cual es el problema que realmente se quiere abordar.

Desde el punto de vista de la complejidad computacional de la criba, se aclara que el objetivo no es encontrar el método más rápido de encontrar los números primos. Sino encontrar una criba eficiente que permita visualizar un patrón en el comportamiento de los números primos en los números naturales.

La criba consiste en formar una lista con todos los números naturales comprendidos entre 2 y *n*, y a continuación se van tachando los números que no son primos de la siguiente manera: se efectúa una división entre *n* y el primer número no tachado, se hace un ciclo que empieza desde la parte entera de esta división y va disminuyendo hasta llegar al número que en primer lugar no estaba tachado, en cada iteración se tachan las multiplicaciones entre ellos siempre y cuando el número no haya sido tachado anteriormente; comenzando de nuevo desde el siguiente número no tachado en la lista, cuando se encuentra un número entero que no ha sido tachado, ese número es declarado primo, y se procede a repetir el ciclo anterior, así sucesivamente. El proceso termina cuando la división entre n y el número primo es menor que el siguiente número no tachado y a partir de este momento se infiere que todos los números no tachados son primos.

Pseudocódigo

Algoritmo Criba de Eratóstenes Optimizada

Entrada: Un número natural *n*

Salida: El conjunto de números primos menores o iguales a *n*

Escriba todos los números naturales desde *2* hasta *n*

Para *i* desde *2* hasta *i* > *n* / *i* **haga lo siguiente:**

    Si *i* no ha sido marcado **entonces:**

        Para *j* desde $\lfloor n/i \rfloor$ hasta *i* (descendiendo) **haga lo siguiente:**

            Si *j* no ha sido marcado **entonces:**

                Ponga una marca en *i* * *j*

El resultado es: Todos los números sin marca son primos

Acerca de la notación:

$\lfloor x \rfloor$ es la función parte entera de *x*

a / *b* es el cociente de dividir *a* entre *b*

a * *b* es la multiplicación de *a* por *b*

Para su implementación, se maneja un vector de tipo lógico con *n* elementos. De esta manera, la posición *i* contiene el valor **Verdadero** como representación de que *i* ha sido marcado y **Falso** en otro caso.

Para demostrar el algoritmo de la criba se debe comprobar que ningún número primo es eliminado: El algoritmo solo tacha números que son producto de dos factores mayores que uno.

Todo número compuesto k, $2 < k \leq n$

K = p * q p primo $p < q \leq \lfloor n/p \rfloor$

Demostración: Por el teorema fundamental de la aritmética

$k = p_1^{n_1}$

$p_m^{n_m} = p_1 * \left(p_1^{n_1 - 1} * \ldots * p_m^{n_m}\right) \rightarrow representa\ q$

Por contradicción:

$Si\ q > \frac{n}{p};\ p_1^{n_1 - 1};\ p_m^{n_m} > \frac{n}{p} \Longrightarrow k > n$

Por lo tanto el algoritmo elimina todo número compuesto entre 2 y n.

A continuación se presenta una prueba de escritorio del algoritmo, la cual permite entender el funcionamiento de la Criba y su relación con la distribución de los números primos en los naturales.

Se define n = 120.

Se genera una lista de números desde 1 hasta 120

Ilustración 1

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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Se inicializa i en 2

Como 2 no es mayor que 120 sobre 2

Se define j = 120 / i = 120 / 2 = 60

Se multiplica 2 por j y el resultado se marca para efecto de la prueba con amarillo, y se va disminuyendo j hasta llegar a i, en este caso 2, siempre y cuando no se encuentre marcado j. Es importante entender que es diferente hacer el ciclo desde j disminuyendo hasta i, en este caso 2; que hacerlo de la forma tradicional desde 2 hasta j, ya que esto permite que no se eliminen números intermedios que son necesarios para que la criba funcione correctamente.

Ilustración 2

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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

En su orden se marcan con amarillo los números: 120, 118, 116, 114, 112, 110, 108, 106, 104, 102, 100, 98, 96, 94, 92, 90, 88, 86, 84, 82, 80, 78, 76, 74, 72, 70, 68, 66, 64, 62, 60, 58, 56, 54, 52, 50, 48, 46, 44, 42, 40, 38, 36, 34, 32, 30, 28, 26, 24, 22, 20, 18, 16, 14, 12, 10, 8, 6 y 4.

Cabe notar que para i = 2 se marcaron (120 / 2) – 2 + 1 = 59 números.

Se busca el siguiente número no tachado, que en este caso es 3.

Como 3 no es mayor que 120 sobre 3

Se define j = (120 / i) = (120 / 3) = 40

Se multiplica 3 por j y el resultado se marca en este caso con azul y se va disminuyendo j hasta llegar a i, en este caso 3, siempre y cuando no se encuentre marcado j.

Ilustración 3

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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

En su orden se marcan con azul los números: 117, 111, 105, 99, 93, 87, 81, 75, 69, 63, 57, 51, 45, 39, 33, 27, 21, 15 y 9.

Cabe notar que para i = 3 se marcaron ((120 / 3) – 3 + 1) * (1 – (1 / 2)) = 19 números.

Se busca el siguiente número no tachado, que en este caso es 5.

Como 5 no es mayor que 120 sobre 5

Se define j = (120 / i) = (120 / 5) = 24

Se multiplica 5 por j y el resultado se marca con rojo y se va disminuyendo j hasta llegar a i, en este caso 5, siempre y cuando no se encuentre marcado j.

Ilustración 4

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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

En su orden se marcan en este caso con rojo los números: 115, 95, 85, 65, 55, 35 y 25.

Cabe notar que para i = 5 se marcaron ((120 / 5) – 5 + 1) * (1 – (1 / 2) – (1 / (2 * 3))) = 7 números.

Se busca el siguiente número no tachado, que en este caso es 7.

Como 7 no es mayor que 120 sobre 7

Se define j = (120 / i) = (120 / 7) = 17

Se multiplica 7 por j y el resultado en este caso se marca con verde y se va disminuyendo j hasta llegar a i, en este caso 7, siempre y cuando no se encuentre marcado j.

Ilustración 5

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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

En su orden se marcan con verde los números: 119, 91, 77 y 49.

Cabe notar que para i = 7 se marcaron

((120 / 7) – 7 + 1) * (1 – (1 / 2) – (1 / (2 * 3)) – (1 / (2 * 3 * 5))) = 4 números.

Se busca el siguiente número no tachado, que en este caso es 11.

Como 11 es mayor que 120 sobre 11 se finaliza el ciclo y los números no marcados entre 2 y 120 son primos.

Para este ejemplo el resultado es: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109 y 113.

Algoritmo de Distribución

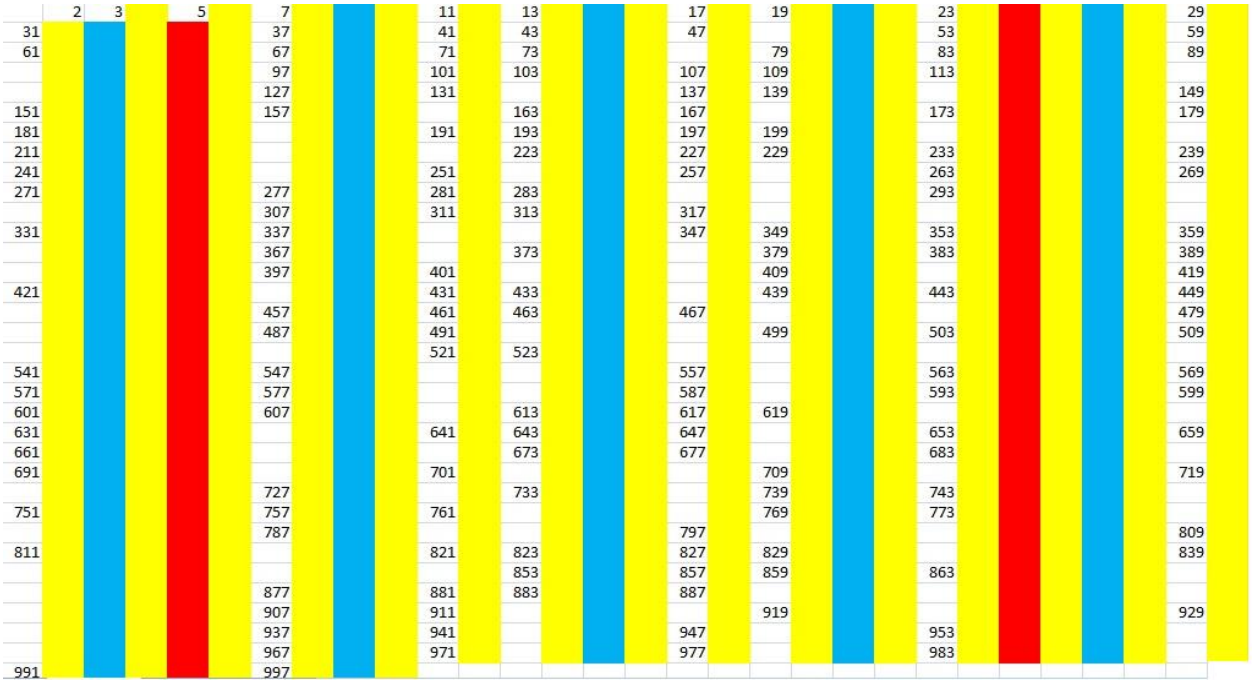
El algoritmo de distribución permite hallar la cantidad de números primos que se encuentran hasta un número natural dado n.

Se forma una tabla con todos los números naturales comprendidos entre 1 y *n* / 7, y se van tachando los números que no son primos de la siguiente manera: se efectúa una división

entre *n* séptimos y el primer número no tachado, se hace un ciclo que empieza desde la parte entera de esta división y va disminuyendo hasta el número en el que empezó el ciclo, en cada iteración se tachan las multiplicaciones entre ellos siempre y cuando el número no haya sido tachado anteriormente; comenzando de nuevo desde el siguiente número no tachado, cuando se encuentra un número entero que no ha sido tachado, ese número es declarado primo, y se procede a repetir el ciclo anterior, así sucesivamente. El proceso termina cuando el contador es igual a 5, esto se puede considerar análogo a la criba de Eratóstenes ejecutada hasta 5.

Se define una variable *Dist*, la cual se inicializa como la parte entera de 4 veces *n* dividido entre 15 mas 2, esto se concluye al aplicar la criba hasta 5, se elimina esta cantidad de números tal y como se muestra en la siguiente figura ya que de 30 columnas se eliminan 22 columnas dejando solo 8 columnas con posibles primos excepto el 2, el 3 y el 5 y quitándole el 1 que no se considera primo, hay que aumentar 2 unidades a las 8 columnas de 30 lo cual nos da un valor inicial para la variable Dist; como se muestra en la siguiente gráfica.

Ilustración 6



Cabe anotar que esta variable inicial puede variar dependiendo de hasta donde se aplique la criba inicial y de esta manera se puede disminuir de una forma considerable el tiempo de ejecución de los algoritmos para encontrar la distribución de los números primos en los números naturales.

Esta proporción aplica para cualquier *n*, en este caso se muestra hasta *n*=1000, cabe anotar que esta característica es interesante teniendo en cuenta que aplica para cualquier *n* y en este caso puede permitir que la complejidad computacional disminuya, al saberse que nunca en estas columnas hacia abajo se va a encontrar un número primo, lo cual puede permitir la eliminación de una parte significativa de los números no primos.

Por el principio de inclusión exclusión se demuestra el número con el cual se inicializa la variable Dist:

$$\left(\frac{n}{2}-1\right)+\left(\frac{n}{3}-1\right)+\left(\frac{n}{5}-1\right)-\frac{n}{6}-\frac{n}{10}-\frac{n}{15}+\frac{n}{30}=\frac{11n}{15}-3$$

$$\left(\frac{11n}{15}-3\right)+\left(\frac{4n}{15}+2\right)=n-1$$

A continuación se inicia un ciclo desde que contador sea igual a 7 ya que anteriormente se aplicó la criba para 2, 3 y 5 respectivamente; hasta que *n* sobre *contador* sea menor que *contador* y se cuentan los posibles primos desde *contador* hasta *n* sobre *contador* y se los resto a la variable *Dist*.

Ahora se procede a eliminar algunos no primos necesarios para tener la exactitud deseada, lo cual se hace encontrando el siguiente primo y multiplicándolo con el actual para hacer una división de *n* sobre la multiplicación de los 2 primos, y se marca la multiplicación de los primos hasta este número.

Pseudocódigo

Algoritmo Distribución Primos en Naturales

Entrada: Un número natural *n*

Salida: La cantidad de números primos menores o iguales a *n*

Escriba todos los números naturales desde *2* hasta *n / 7*

Para *i* desde *2* hasta *5* **haga lo siguiente:**

Si *i* no ha sido marcado **entonces:**

Para *j* desde $\lfloor n/(7*i) \rfloor$ hasta *i* (descendiendo) **haga lo siguiente:**

Si *j* no ha sido marcado **entonces:**

Ponga una marca en *i * j*

*Dist := 4 * n / 15 + 2*

Para *i* desde 7 hasta *n / i < i* **haga lo siguiente:**

Si *i* no ha sido marcado **entonces:**

Dist := Dist - 1

Encuentro el siguiente primo j

Si *n / (i * j)* > i

Para k desde i hasta *n / (i * j)* **haga lo siguiente:**

Si k no ha sido marcado **entonces:**

Ponga una marca en *i* * *k*

i := *j* - *1*

El resultado es: Dist es la cantidad los números primos que existen desde 1 hasta n

Acerca de la notación:

$\lfloor x \rfloor$ es la función parte entera de *x*

a / *b* es el cociente de dividir *a* entre *b*

a * *b* es la multiplicación de *a* por *b*

:= es la asignación de un valor a una variable

A continuación se presenta una prueba de escritorio del algoritmo, la cual permite entender el funcionamiento de la distribución de los números primos en los naturales.

Se define n = 2310.

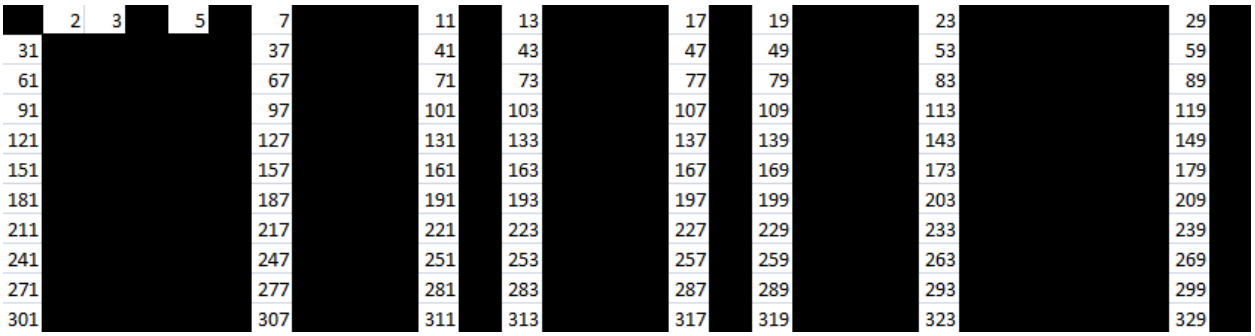
Se genera una lista de números desde 1 hasta *n* / 7 = 2310 / 7 = 330

Ilustración 7

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	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210
211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270
271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300
301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330

Se procede a eliminar los múltiplos de 2, 3 y 5 por medio de la criba

Ilustración 8



	2	3		5		7				11		13				17		19				23				29
31						37				41		43				47		49				53				59
61						67				71		73				77		79				83				89
91						97				101		103				107		109				113				119
121						127				131		133				137		139				143				149
151						157				161		163				167		169				173				179
181						187				191		193				197		199				203				209
211						217				221		223				227		229				233				239
241						247				251		253				257		259				263				269
271						277				281		283				287		289				293				299
301						307				311		313				317		319				323				329

Se inicializa Dist en 4 * n / 15 + 2 = 4 * 2310 / 15 + 2 = 618.

Como i < n / i, es 7 < (2310 / 7 = 330)

Se hace un conteo desde i = 7 hasta n / i = (2310 /7 = 330) de los no marcados, en este caso 87.

Se asigna Dist := Dist – 87 = 616 – 87 = 531.

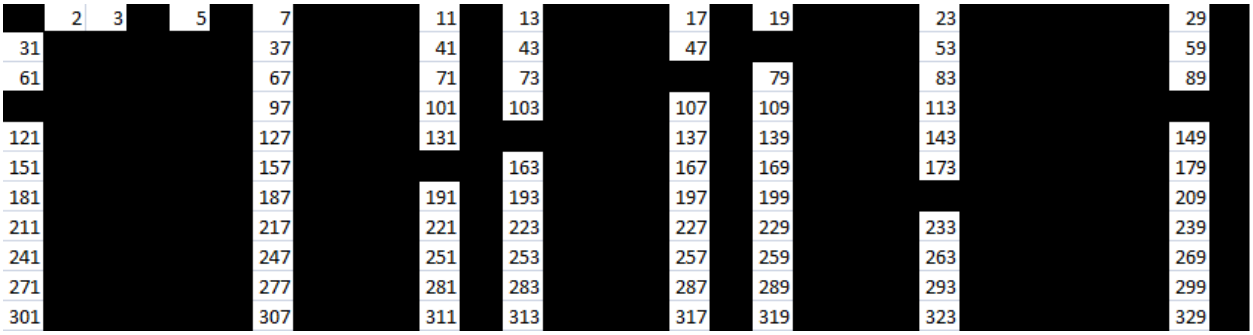
Se encuentra el siguiente primo j = 11.

Se inicializa k := n / (i * j) = 2310 / (7 * 11) = 30 > i = 7

Se marcan a continuación los números:

7 * 7 = 49, 7 * 11 = 77, 7 * 13 = 91, 7 * 17 = 119, 7 * 23 = 161 y 7 * 29 = 203.

Ilustración 9



	2	3		5		7				11		13				17		19				23						29	
31						37				41		43				47						53						59	
61						67				71		73						79				83						89	
						97				101		103				107		109				113							
121						127				131						137		139				143						149	
151						157						163				167		169				173						179	
181						187				191		193				197		199										209	
211						217				221		223				227		229				233						239	
241						247				251		253				257		259				263						269	
271						277				281		283				287		289				293						299	
301						307				311		313				317		319				323						329	

Se asigna i = j = 11.

Como i < n / i, es 11 < 2310 / 11 = 210

Se hace un conteo desde i = 11 hasta n / 11 = 210 de los no marcados en este caso 47.

Se asigna Dist := Dist – 47 = 531 – 47 = 484.

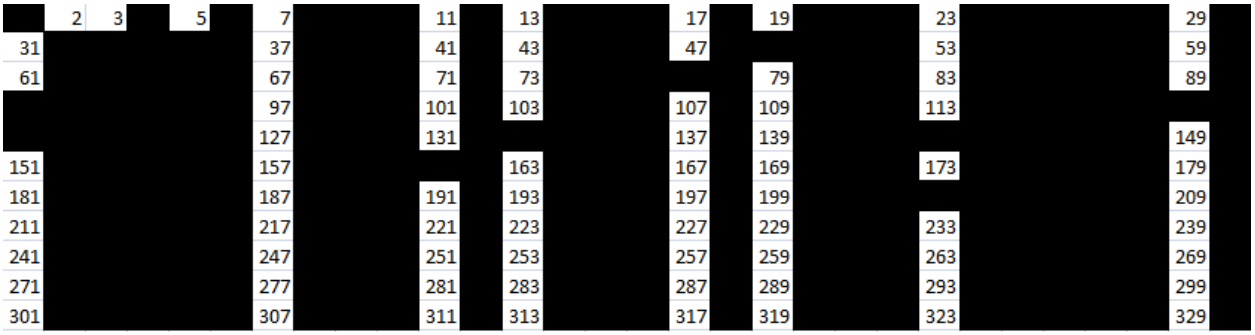
Se encuentra el siguiente primo j = 13.

Como n / (i * j) = 2310 / (11 * 13) = 16 > i = 11

Se marcan a continuación los números:

11 * 11= 121, 11 * 13 = 143

Ilustración 10



	2	3		5		7				11		13				17		19				23						29	
31						37				41		43				47						53						59	
61						67				71		73						79				83						89	
						97				101		103				107		109				113							
						127				131						137		139										149	
151						157						163				167		169				173						179	
181						187				191		193				197		199										209	
211						217				221		223				227		229				233						239	
241						247				251		253				257		259				263						269	
271						277				281		283				287		289				293						299	
301						307				311		313				317		319				323						329	

Se asigna i = j = 13.

Como i < n / i, es 13 < 2310 / 13 = 178

Se hace un conteo desde i = 13 hasta n / 11 = 178 de los no marcados en este caso 36.

Se asigna Dist := Dist – 36 = 484 – 36 = 448.

Se encuentra el siguiente primo j = 17.

Como n / (i * j) = 2310 / (13 * 17) = 10 < i= 13

Ya no se marcan más números.

Se asigna i = j = 17.

Como i < n / i, es 17 < 2310 / 17 = 136

Se hace un conteo desde i = 17 hasta n / 17 = 136 de los no marcados en este caso 26.

Se asigna Dist := Dist – 26 = 448 – 26 = 422.

Se encuentra el siguiente primo j = 19.

Se asigna i = j = 19.

Como i < n / i, es 19 < 2310 / 19 = 122

Se hace un conteo desde i = 19 hasta n / 19 = 122 de los no marcados en este caso 23.

Se asigna Dist := Dist – 23 = 422 – 23 = 399.

Se encuentra el siguiente primo j = 23.

Se asigna i = j = 23.

Como i < n / i, es 23 < 2310 / 23 = 100

Se hace un conteo desde i = 23 hasta n / 23 = 100 de los no marcados en este caso 17.

Se asigna Dist := Dist – 17 = 399 – 17 = 382.

Se encuentra el siguiente primo j = 29.

Como i < n / i, es 29 < 2310 / 29 = 80

Se hace un conteo desde i = 29 hasta n / 29 = 80 de los no marcados en este caso 13.

Se asigna Dist := Dist – 13 = 382 – 13 = 369.

Se encuentra el siguiente primo j = 31.

Como i < n / i, es 31 < 2310 / 31 = 75

Se hace un conteo desde i = 31 hasta n / 31 = 75 de los no marcados en este caso 11.

Se asigna Dist := Dist – 11 = 369 – 11 = 358.

Se encuentra el siguiente primo j = 37.

Como i < n / i, es 37 < 2310 / 37 = 62

Se hace un conteo desde i = 37 hasta n / 37 = 62 de los no marcados en este caso 7.

Se asigna Dist := Dist – 7 = 358 – 7 = 351.

Se encuentra el siguiente primo j = 41.

Como i < n / i, es 41 < 2310 / 41 = 56

Se hace un conteo desde i = 41 hasta n / 41 = 56 de los no marcados en este caso 4.

Se asigna Dist := Dist – 4 = 351 – 4 = 347.

Se encuentra el siguiente primo j = 43.

Como i < n / i, es 43 < 2310 / 43 = 54

Se hace un conteo desde i = 43 hasta n / 43 = 54 de los no marcados en este caso 3.

Se asigna Dist := Dist – 3 = 347 – 3 = 344.

Se encuentra el siguiente primo j = 47.

Como i < n / i, es 47 < 2310 / 47 = 49

Se hace un conteo desde i = 47 hasta n / 47 = 49 de los no marcados en este caso 1.

Se asigna Dist := Dist – 1 = 344 – 1 = 343.

Se encuentra el siguiente primo j = 53.

Como i > n / i, es 53 > 2310 / 53 = 44

Se da por terminado el algoritmo con un resultado de Dist = 343.

Después de explicado a nivel de programación los algoritmos aportados en esta tesis, se pretende dar una explicación de a qué resultados se llegaron.

Se hace un estudio detallado de la Criba y el algoritmo de la distribución de los números primos en los naturales programados en Visual Basic para Excel.

Aproximación Matemática de la Distribución

Se presente la siguiente fórmula matemática para la distribución de los números primos en los naturales, la cual es sustentada por el comportamiento de la Criba.

$$D = \frac{{}^{n}/_{2} - \sum_{i=2}^{p(i)*p(i)>n} \left({}^{n}/_{p(i)} - p(i) + 1\right) * \left(j := j - \left(k := \left({}^{k}/_{(p(i-1))}\right)\right)\right)}{n}$$

Donde:

D es la distribución de los números primos en los naturales

n es el numero al cual se le va a aplicar la formula

p(i) es un arreglo con los números primos

j es una variable que empieza en 1

k es una variable que empieza en 1

:= se refiere a asignar un valor a una variable

$\sum$ va desde $p(2)=3$ hasta $p(i)*p(i) > n$

Para la fórmula anterior, haciendo una definición desde un punto de vista matemático más formal, se tiene la siguiente función recursiva.

$$D = \frac{{}^{n}/_{2} - \sum_{i=2}^{p(i)*p(i)>n} \left({}^{n}/_{p(i)} - p(i) + 1\right) * (a(i-1))}{n}$$

$$b(1) = \frac{1}{p(1)}$$

$$b(n) = b(n-1) * \frac{1}{p(n)}, n \geq 2, n \in \mathbb{Z}^+$$

$$a(1) = 1 - b(1)$$

$$a(n) = a(n-1) - b(n), n \geq 2, n \in \mathbb{Z}^+$$

A continuación se presenta una prueba de escritorio de la fórmula con n = 120 con el fin de hacer una comparación entre la formula de la distribución y la prueba de escritorio que se hizo a la criba para ver la forma en que se eliminan los números no primos de la lista.

$$D = \frac{\frac{120}{2} + 1 - \left(\frac{120}{3} - 2\right) \times \frac{1}{2} - \left(\frac{120}{5} - 4\right) \times \left(\frac{1}{2} - \frac{1}{2 \times 3}\right) - \left(\frac{120}{7} - 6\right) \times \left(\frac{1}{2} - \frac{1}{2 \times 3} - \frac{1}{2 \times 3 \times 5}\right)}{120}$$

Lo cual es acorde con el comportamiento de la Criba ya que se puede comparar cada parte de la formula con cada ejecución de un ciclo en la Criba.

5. Conclusiones

- Al finalizar el proyecto se realizó un estudio que permite tener una aproximación formal sobre el comportamiento de la complejidad computacional del problema de encontrar los números primos de forma determinista.
- Se definió un procedimiento o metodología determinista, el cual demostró ser eficiente para encontrar números primos, al no desperdiciar ningún ciclo de programación y además, permitió crear un algoritmo para el estudio de la distribución de los números primos en los números naturales.
- Estos algoritmos permitieron hacer una extrapolación de la metodología definida que permita de una forma “eficiente” encontrar números primos de mayor tamaño y la cual siga siendo determinista a través de la reutilización de vectores.
- Se diseñó una aplicación que permite visualizar la Criba y el algoritmo de distribución y brinda información necesaria para poder llegar a conclusiones importantes respecto a la distribución de los números primos entre los números naturales y su complejidad computacional.
- Con los datos entregados por la aplicación se infiere una fórmula matemática y un modelo sobre el comportamiento de la aparición de los números primos en los números naturales.

6. Recomendaciones

Los resultados de esta investigación servirán entre otras cosas para inferir métodos más eficientes para encontrar números primos de tamaño mayor a lo predefinido por las Unidades Aritmético Lógicas de los computadores.

Al manifestar que los números primos no aparecen de manera aleatoria sino que siguen una modelable regularidad, se puede entender y explicar cuál es su relación con la hipótesis de Riemann y otros comportamientos con los que ha sido asociado.

La criba puede ser un método de enseñanza para los niños del mundo de cómo hallar números primos y permitir que estos hagan sus propias conclusiones sobre la distribución de los números primos en los números naturales.

El algoritmo para hallar la distribución de los números primos en los números naturales permite tener una visión algorítmica de una fórmula matemática en la actualidad informática ya que se puede abordar un nuevo tipo de fórmulas que probablemente no hayan sido tenidas en cuenta por los matemáticos que puedan haberse mantenido al margen del tema de la programación de computadores.

Es posible en la actualidad con la ayuda de los sistemas encontrar patrones que no se habían descubierto en problemas de alta importancia independientemente del medio.

7. Referencias

Atkin, A.O.(1982). On a primality test of Solovay and Strassen. SIAM Journal on Computing, DOI: 10.1137/0211064

Chen, W. A (2010) Speculative study of anomalous relaxation modeling for the distribution of prime numbers. Mechatronics and Embedded Systems and Applications (MESA), DOI:10.1109/MESA.2010.5552005

Cheung, P. (2004) A Scalable Hardware Architecture for Prime Numbre Validation. Field-Programmable Technology. DOI:10.1109/FPT.2004.1393266

Du Satoy, M. (2005) La música de los números primos. (Videos) History Channel, BBC & Open University.

Jansen B. (2005) Neural networks following a binary approach applied to the integer prime-factorization problem. Neural Networks (Montreal). DOI:10.1109/IJCNN.2005.1556309

Meng, T. (2008) A Method of Big Prime Number Generator based on NTL. Intelligent Information Hiding and Multimedia Signal Processing, (Harbin). DOI:10.1109/IIH-MSP.2008.191

Peral, J. C. (2008) Sobre la distribución de los números primos el postulado de Bertrand. Sigma 33, 209.

Pope, S. (2001). On problems of cryptography: Primality testing and factoring integers. ProQuest Dissertations and Theses, 85.

Ruiz, S. M. (2004). Formula to obtain the next prime number in any increasing sequence of positive integer numbers. Smarandache Notions Journal.

Shahabi, M. (2012). The distribution of the classical error terms of prime number theory. University of Lethbridge (Canada). ProQuest Dissertations and Theses, 129.

Szecowka, P.M. (2012) Digital hardware for prime numbers generation. Mixed Design of Integrated Circuits and Systems (Warsaw).

Szecowka, P.M (2012) Generation of the large random prime numbers. Mixed Design of Integrated Circuits and Systems (Warsaw).

Wong, A. (2013). Primality test using elliptic curves with complex multiplication by Q-7. ProQuest Dissertations and Theses, 71.