Dirección General de Cultura y Educación. Provincia de Buenos Aires
Instituto Superior Fundación Suzuki
D.I.P.R.E.G.E.P.: 3882

"MATEMÁTICA Y EL NÚMERO"

"LA CECA DE LOS NÚMEROS PRIMOS"

Tesina para optar al título de profesor de matemática

Autor: Bárbara Samanta Subidia
San Miguel, Buenos Aires
7 de marzo de 2009

Índice

Agradecimientos

- *Principalmente agradezco a Dios y María. Por guiar y alumbrar con su luz bendita el camino de mi vida.*
- *A mi familia, que me contuvo en las tormentas, truenos, aplazos, trabajos y parciales, y me acompañó en los momentos de mayor satisfacción y felicidad.*
- *A mis maestros, que con su sabiduría y humildad allanaron mi futuro.*
- *A mis compañeras del profesorado, quienes sábado a sábado reponían mis energías, con risas, mates y cariño.*
- *Y a todas las personas que en estos cuatro años comprendieron el inmenso valor que depositaba en la carrera y en mi superación personal.*

Desde lo más profundo de mi corazón

Muchas gracias, Samanta

ABRIL

Mi mejor creación

Aclaración del título:

Estudio de un campo numérico; los números primos, características, regularidad, uso y misterios.

Resumen:

A los niños les enseñan en el nivel primario el concepto de números primos y la búsqueda en los primeros cien unidades, sin profundizar en sus características e importancia. Los números primos representan un misterio fascinante el que nos enfrenta a una búsqueda de conocimiento. Su irregularidad, inexactitud, independencia son adjetivos inapropiados para los campos numéricos. Por esta razón se convierten en interesantes, desafiantes y misteriosos. En esta tesina trataremos de descubrir un poco más de su belleza.

Abstrac:

At the first levels of Elementary School children are taught about the concept of “números primos”and the searching on the first hundred units, without going deeper on their characteristics and importance. The “números primos” represent a fascinant mystey which face us to a seaching

of knowledge. Their irregularity, inexactitude and independence are unapropiate adjetives for the field of numbers. For this reason they become interesting, challenging and mysterious. Yn this thesis we will try to discover a little more of their beauty.

Descriptores:

Aritmética, Números primos, Criptografía, divisibilidad, inexactitud, irregularidad.

Introducción:

Hace un algunos de años cuando terminé el secundario sabía que comenzaría una etapa de estudio y esfuerzo, pero no podía decidir cual era mi camino. Realicé un test vocacional, el cual develaba mi inclinación y gusto por los NÚMEROS.

Hoy estoy terminando la carrera de Profesor de Matemáticas y me encuentro realizando un trabajo de investigación sobre aquel tema que siempre estuvo en mi mente y mi corazón.

La ciencia de los números, la exactitud, y la regularidad son sinónimos de matemática. Nuestra vida diaria esta signada por los números, ya sea como ciencia en sí o como herramienta para otras ciencias, para descubrir, admirar y desarrollar nuestro mundo.

En esta tesina voy a estudiar un campo numérico en especial, *Los números primos* ya que en ellos conviven misterios que me gustaría observar o simplemente tratar de descubrir sus usos y bellezas.

Fundamentación:

Los recovecos de la historia de las matemáticas han cimentado las bases de nuestra vida diaria y académica. Por esta razón existen contenidos que han quedado relegados arbitrariamente.

Han pasado los años y ellos están allí latentes, expectantes a que nuestra mente curiosa los estudien, a que nosotros los seres humanos amantes de las ciencias exactas descubramos sus matices y bellezas.

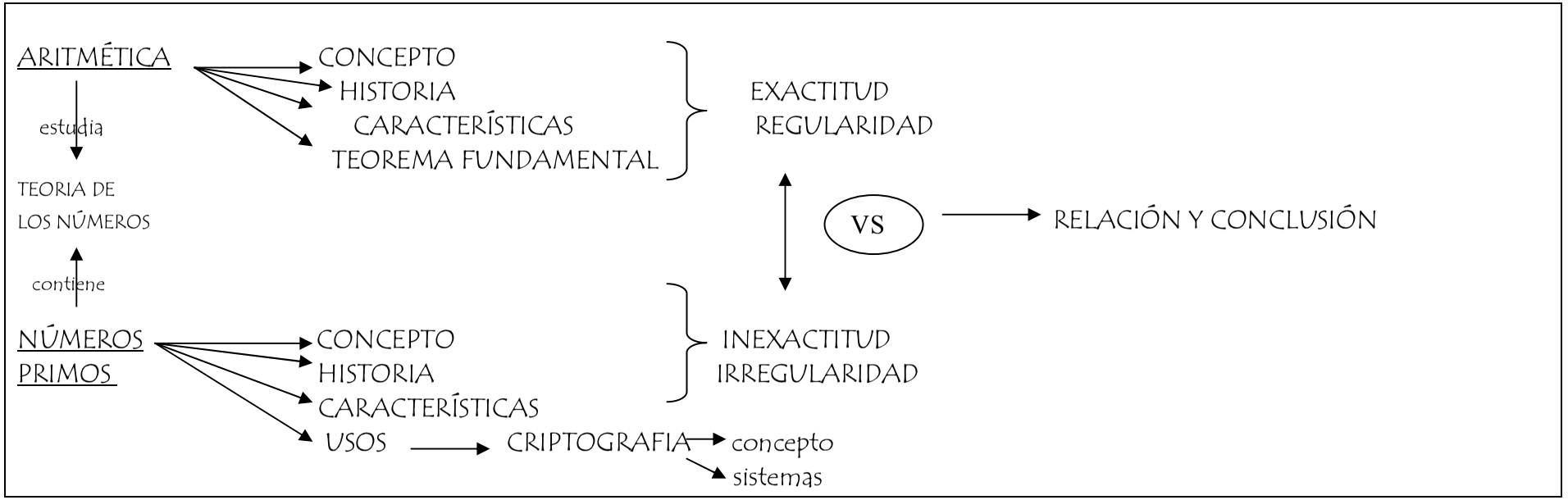
Es el caso de los números primos estudiados sólo por su concepto, aquí descubriremos su complejidad, importancia, incoherencias e irregularidad.

Supuestos y limitaciones:

- Suponemos que nos encontraremos con una basta información clásica de los números primos.
- Existen varios enfoques acerca de la naturaleza y características a lo largo de toda la historia.
- La información se limita a la descripción de los números primos y no a la investigación de sus usos.

- La información que se ha encontrado se limita a comentar el uso de los números primos en la criptografía, pero no detalla adecuadamente el algoritmo o procedimiento del funcionamiento en ese sistema.

CUADRO RESUMEN



Marco Histórico

Concepto e historia de la aritmética.

Aritmética: De origen griego *arriamos* (número) y *techne* (habilidad)

La aritmética es una rama de la matemática, su objetivo fundamental es contar y realizar cálculos científicos. También estudia ciertas operaciones con los números y las propiedades fundamentales.

Se realizará a continuación un resumen de los aportes generados por las diferentes civilizaciones a la aritmética.

EGIPCIOS: (aprox. 2.500 a.C.)

Su numeración era aditiva por ende su cálculos eran dificultosos y tenían problemas con la representación de fracciones. No fue mucho su contribución

BABILÓNICOS: (aprox. 2000 a.C.)

Su contribución fue sentar las bases para el punto de partida del álgebra y la aritmética. Poseían una base de 60y no existía el cero. La ventaja era conocer pocos símbolos y la desventaja era su lectura por orden y posición.

La matemática de los egipcios y babilónicos fue muy rudimentaria, lo hacían en forma inconciente. Los números surgen como herramientas no como ciencia.

PITAGÓRICOS (aprox. 500 a.C.)

Los pitagóricos reconocieron la matemática como ciencia. Realizaron mucos estudios sobre geometría y sobre los números. Pero para ellos esta ciencia era para pocos y secreta. No aceptaban las razones inconmensurables (números racionales).

ZENON (aprox. 500 a.C.)

Las paradojas de Zenón fueron precursores de la geometría y de aritmética en el caso del cálculo infinitesimal, límites e integrales.

HINDÚES (aprox. 200 al 1200 d. C.)

En el año 600 en la India se volvió a utilizar los símbolos del BRAHMI con notación posicional en base 10 la inclusión del cero y todas las reglas para las operaciones básicas actuales. También aceptaron a medias el uso de los números negativos. Los indios no apreciaban la importancia de sus propias aportaciones. No eran sensibles a los valoras de las matemáticas.

ÁRABES (aprox. 1000 al 1300 d.C.)

En aritmética, los árabes dieron un paso atrás. No realizaron muchos aportes. Ya que no disponían de ningún símbolo aunque estaban familiarizados con la idea de número negativo.

¿QUIÉNES ESTUDIARON ARITMÉTICA?

Como anteriormente se menciona, la aritmética es una rama de la matemática que estudia las relaciones con los números, y podemos afirmar que el primer ser humano que comenzó ha relacionar y prestar una rigurosidad a las relaciones y propiedades que se demostraban era el matemático griego DIOFANTO de ALEJANDRÍA en el siglo III d. C. Diofanto estudió la TEORÍA DE LOS NÚMEROS Y escribió trece libros (siete de los cuales se han perdido) dedicados a la resolución de ecuaciones

algebraicas, intentando dar métodos para encontrar sus soluciones enteras o racionales. Algunos ejemplos de los problemas que trataban en su libro son:

¿Qué números son suma de dos números al cuadrado? ¿Qué números son suma de tres números al cubo?

Números primos

Con respecto a los Números primos la historia nos cuenta lo siguiente.

Los números primos y sus propiedades fueron estudiados de manera exhaustiva por los matemáticos de la antigua Grecia.

Los matemáticos de la Escuela Pitagórica (500 a. C. a 300 a. C.) estaban interesados en los números por su misticismo y sus propiedades numerológicas. Ellos comprendían la idea de primalidad y estaban interesados en los números *perfectos* y *amigables*.

Para el momento en que los Elementos Euclidianos aparecieron por el 300 a. C., ya habían sido probados varios resultados importantes acerca de números primos. En el Libro IX de los Elementos, Euclides prueba que hay infinidad de números primos. Esta es una de las primeras demostraciones conocidas en la que se utiliza el *método del absurdo* para establecer el resultado. Euclides también demuestra el Teorema Fundamental de Aritmética.

Euclides: (330 a.C. - 275 a.C.)

Matemático griego. Poco se conoce a ciencia cierta de la biografía de Euclides, pese a ser el matemático más famoso de la Antigüedad.

Es probable que Euclides se educara en Atenas, lo que explicaría con su buen conocimiento de la geometría elaborada en la escuela de Platón, aunque no parece que estuviera familiarizado con las obras de Aristóteles. Enseñó en Alejandría, donde alcanzó un gran prestigio en el ejercicio de su magisterio durante el reinado de Tolomeo I Sóter; se cuenta que éste lo requirió para que le mostrara un procedimiento abreviado para acceder al conocimiento de las matemáticas, a lo que Euclides repuso que no existía una vía regia para llegar a la geometría (el epigrama, sin embargo, se atribuye también a Menecmo como réplica a una demanda similar por parte de Alejandro Magno).

La tradición ha conservado una imagen de Euclides como hombre de notable amabilidad y modestia, y ha transmitido así mismo una anécdota relativa a su enseñanza, recogida por Juan Estobeo: un joven principiante en el estudio de la geometría le preguntó qué ganaría con su aprendizaje; Euclides, tras explicarle que la adquisición de un conocimiento es siempre valiosa en sí misma, ordenó a su esclavo que diera unas monedas al muchacho, dado que éste tenía la pretensión de obtener algún provecho de sus estudios.

Euclides fue autor de diversos tratados, pero su nombre se asocia principalmente a uno de ellos, los Elementos, que rivaliza por su difusión con las obras más famosas de la literatura universal, como la Biblia o el Quijote. Se trata, en esencia, de una compilación de obras de autores .

Euclides también demostró que si el número $2^n - 1$ es primo, entonces el número 2^n-1 es un número perfecto. El matemático Euler (más tarde, en 1747) pudo demostrar que todos, aún los números perfectos, tienen esta forma. Hasta el día de hoy no se sabe si existe algún número perfecto que sea impar.

Cerca del 200 a. C. el Griego Eratóstenes ideó un algoritmo para calcular números primos llamado el *Tamiz de Eratóstenes*. (Desarrollado en el marco teórico)

Se da luego un gran vacío en la historia de los números primos que es usualmente llamado la Edad Obscura.

Pero en el siglo XVII , esa obra realizada por Diofanto fue un verdadero impulso para PIERRE DE FERMAT (1601-1665). Considerado el verdadero padre de la aritmética.

Fermat (1601-1665)

Nacido de una familia de comerciantes, se formo como abogado en la ciudad de Toulouse, ganándose la vida con dicha profesión. Aunque las matemáticas eran una afición para Fermat, sólo podía dedicarles poco tiempo, contribuyó con resultados de primera importancia sobre la teoría de los números y al cálculo. La mayoría de los trabajos de Fermat eran conocidos por sus cartas a los amigos ya que publicó pocos artículos.

Fermat consideraba que se había descuidado la teoría de los números. Con la traducción de los libros de Diafanito realizados por Bachet, Fermat realizaba sus razonamientos y los escribía en los márgenes de las hojas.

Fermat anunció muchos teoremas sobre los números y en particular sobre los números primos. Como por ejemplo los siguientes:

*Método del descenso infinito.

*Estudios sobre los Números primos.

*Pequeño teorema de Fermat

*Gran teorema de Fermat o el último teorema de Fermat.

El próximo gran descubrimiento fue demostrar que la teoría de Albert Girard de que cada número primo de la forma $2^n + 1$ puede ser escrito de una manera única como la suma de 2 cuadrados y demostró como cualquier número puede ser escrito como la suma de cuatro cuadrados.

Ideó un nuevo método de factorización de números largos que demostró por medio de la factorización del número 2027651281 = 44021 × 46061.

Probó lo que se conoce como *El pequeño teorema de Fermat* (para distinguirlo del llamado *Ultimo Teorema*). Este establece que si *p* es un número primo entonces para cualquier entero *a* obtenemos que *ap* = *a* modulo *p*.

Esto prueba la mitad de lo que se ha llamado la Hipótesis China que data de unos 2000 años antes, y que dice que un entero *n* es primo si y solo si el número 2n - 2 es divisible por *n*. La otra mitad es falsa, ya que, por

ejemplo, 2341 - 2 es divisible por 341 aún cuando 341 = 31 × 11 es compuesto. El Pequeño Teorema de Fermat es la base de otros muchos resultados en la Teoría de Números y es la base de métodos de verificación de números primos que se utilizan aún hoy en ordenadores electrónicos.

Fermat mantuvo correspondencia con otros matemáticos de su época, y en particular con el monje Marín Mersenne. En una de sus cartas a Mersenne, él conjetura que los números $2^n + 1$ eran siempre primos si *n* es una potencia de 2. El había verificado esto para *n* = 1, 2, 4, 8 y 16 y sabía que si *n* no era una potencia de 2, el resultado fallaba. Los números de esta forma son llamados *Números de Fermat* y no fue hasta más de 100 años más tarde que Euler demostró que $2^{32}+1$ = 4294967297 es divisible por 641 y por tanto no es primo.

Leonhard Euler (nombre completo, **Leonhard Paúl Euler**)

Nació el 15 de abril de 1707 en Basilea, Suiza, y murió el 18 de septiembre de 1783 en San Petersburgo, Rusia. Fue un respetado matemático y físico, y está

considerado como el principal matemático del siglo XVIII y como uno de los más grandes de todos los tiempos.

Vivió en Rusia y Alemania la mayor parte de su vida y realizó importantes descubrimientos en áreas tan diversas como el cálculo o la teoría de grafos. También introdujo gran parte de la moderna terminología y notación matemática, particularmente para el área del análisis matemático, como por ejemplo la noción de función matemática. También se le conoce por sus trabajos en los campos de la mecánica, óptica y astronomía.

Euler ha sido uno de los matemáticos más prolíficos, y se calcula que sus obras completas reunidas podrían ocupar entre 60 y 80 volúmenes. Una afirmación atribuida a Pierre-Simon Laplace expresa la influencia de Euler en los matemáticos posteriores: «Lean a Euler, lean a Euler, él es el maestro de todos nosotros.»

En conmemoración suya, Euler ha aparecido en la serie sexta de los billetes de 10 francos suizos, así como en numerosos sellos postales tanto suizos como alemanes y rusos. El asteroide (2002) Euler recibió ese nombre en su honor.

Los números de la forma $2^n - 1$ también atrajeron la atención porque es muy fácil demostrar que a menos que *n* sea primo, este número será compuesto. A menudo éstos son llamados *Números primos de Mersenne* Mn, dado que Mersenne los estudió.

No todos los números de la forma $2^n - 1$ con *n* primo son primos.

Por ejemplo $2^{11} - 1 = 2047 = 23 \times 89$ es compuesto, aunque fue notado por primera vez en 1536.

Marin Mersenne

Nacido en una familia de campesinos cerca de Oizé (hoy Sarthe), en la provincia francesa de Maine, fue educado en Le Mans y en el colegio jesuita de La Flèche. Aunque en ocasiones se afirma que fue jesuita, lo cierto es que nunca llegó a ingresar en la Compañía de Jesús. El 17 de julio de 1611 se hizo miembro de los Mínimos dedicándose al estudio de la teología y el hebreo. Después de este período recibió la ordenación sacerdotal en París en 1613. Tras su consagración estuvo un tiempo enseñando filosofía y teología en Nevers, pero en 1619 regresó a París, siendo destinado al convento de L'Annonciade. En compañía de personajes como Étienne Pascal, Gilles de Robeval y Nicholas-Claude Fabri de Peiresc, estudió matemáticas y música. Tuvo una nutrida correspondencia con diversos eruditos de Francia, Italia, Inglaterra y Holanda, tales como Descartes, Pierre de Fermat, Galileo Galilei, Giovanni Doni y Constantijn Huygens. Durante la estancia de Descartes en Holanda, Mersenne fue su principal corresponsal y su intermediario con los sabios de la época. Desde 1620 hasta 1623 se dedicó exclusivamente a escribir en materia de filosofía y teología, y en 1623 publicó *Quaestiones celeberrimae in Genesim*, a la que rápidamente siguieron otras obras como *L'Impieté des déistes* (1624) y *La Vérité des sciences* (*La verdad en las ciencias*) (1624).

Visitó Italia en tres ocasiones, en 1640, 1641 y 1645.

Murió después de una serie de complicaciones que se derivaron de una intervención quirúrgica. En su testamento vital, pidió que su cuerpo fuera sometido a autopsia como último servicio al interés de la ciencia

Durante muchos años los números obtenidos de esta forma fueron los primos más largos conocidos. Cataldi probó que el número M19 es primo en 1588 y fue el primo más grande conocido por unos 200 años hasta que Euler probó que M31 es primo. Este marcó el récord por otra centuria hasta que Lucas demostró que M127 (el cual tiene 39 dígitos) es primo, tomando el récord hasta la era de la computadora electrónica.

En 1952 Robinson probó que los números primos de Mersenne M521, M607, M1279, M2203 y M2281 son primos utilizando un modelo temprano de ordenador comenzando así la era electrónica.

Para el 2005 habían sido encontrados un total de 42 primos de Mersenne. El más grande es M25964951, el cual tiene 7816230 dígitos decimales.

El trabajo de Euler tuvo un gran impacto en la teoría numérica en general y sobre la de primos en particular.

Él amplió el Teorema Pequeño de Fermat e introdujo la función φ de Euler. Como mencionamos antes, factorizó el 5o número Fermat 232 + 1, y encontró 60 pares de números amigables a los que nos referimos anteriormente, y estableció (pero no pudo demostrar) lo que se conoce como la Ley de Reciprocidad Cuadrática.

Aún quedan abiertas muchas preguntas (algunas de ellas datan de hace más de cien años) relacionadas a los números primos.

Criptografía

Los números primos tienen como utilidad, en la actualidad, un uso relevante. Se puede observar el la criptografía. El desarrollo de este tema se visualiza en el marco teórico, pero la historia se detalla a continuación.

La historia de la criptografía es larga y abunda en anécdotas. Ya las primeras civilizaciones desarrollaron técnicas para enviar mensajes durante las campañas militares de forma que si el mensajero era interceptado la información que portaba no corriera el peligro de caer en manos del

enemigo. Posiblemente, el primer criptosistema que se conoce fuera documentado por el historiador griego Polibio: un sistema de sustitución basado en la posición de las letras en una tabla. También los romanos utilizaron sistemas de sustitución, siendo el método actualmente conocido como César, porque supuestamente Julio César lo utilizó en sus campañas, uno de los más conocidos en la literatura (según algunos autores, en realidad Julio César no utilizaba este sistema de sustitución, pero la atribución tiene tanto arraigo que el nombre de éste método de sustitución ha quedado para los anales de la historia). Otro de los métodos criptográficos utilizados por los griegos fue la escitala espartana, un método de trasposición basado en un cilindro que servía como clave en el que se enrollaba el mensaje para poder cifrar y descifrar.

En 1465 el italiano León Battista Alberti inventó un nuevo sistema de sustitución polialfabética que supuso un gran avance de la época. Otro de los criptógrafos más importantes del siglo XVI fue el francés Blaise de Vigenere que escribió un importante tratado sobre "la escritura secreta" y que diseñó una cifra que ha llegado a nuestros días asociada a su nombre. A Selenus se le debe la obra criptográfica "Cryptomenytices et Cryptographiae" (Lüneburg, 1624). Durante los siglos XVII, XVIII y XIX, el interés de los monarcas por la criptografía fue notable. Las huestes de Felipe II utilizaron durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos que los matemáticos del rey consideraban inexpugnable. Cuando el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, a la sazón Enrique IV, el

conocimiento mostrado por el rey francés impulsó una queja de la corte española ante del papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a sus ejércitos. Por su parte, la reina María Estuardo, reina de los Escoceses, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un criptoanálisis exitoso por parte de los matemáticos de Isabel.

La máquina *Enigma* utilizada por los alemanes durante la II Guerra Mundial

Desde el siglo XIX y hasta la Segunda Guerra Mundial las figuras más importantes fueron la del holandés Auguste Kerckhoffs y la del prusiano Friedrich Kasiski. Pero es en el siglo XX cuando la historia de la criptografía vuelve a presentar importantes avances. En especial durante las dos contiendas bélicas que marcaron al siglo: la Gran Guerra y la Segunda Guerra Mundial. A partir del siglo XX, la criptografía usa una nueva herramienta que permitirá conseguir mejores y más seguras cifras: las máquinas de cálculo. La más conocida de las máquinas de cifrado, posiblemente sea la máquina alemana Enigma: una máquina de rotores que

automatizaba considerablemente los cálculos que era necesario realizar para las operaciones de cifrado y descifrado de mensajes. Para vencer al ingenio alemán, fue necesario el concurso de los mejores matemáticos de la época y un gran esfuerzo computacional. No en vano, los mayores avances tanto en el campo de la criptografía como en el del criptoanálisis no empezaron hasta entonces.

Tras la conclusión de la Segunda Guerra Mundial, la criptografía tiene un desarrollo teórico importante; siendo Claude Shannon y sus investigaciones sobre teoría de la información esenciales hitos en dicho desarrollo. Además, los avances en computación automática suponen tanto una amenaza para los sistemas existentes como una oportunidad para el desarrollo de nuevos sistemas. A mediados de los años 70 el Departamento de Normas y Estándares norteamericano publica el primer diseño lógico de un cifrador que estaría llamado a ser el principal sistema criptográfico de finales de siglo: el Estándar de Cifrado de Datos o DES. En esas mismas

fechas ya se empezaba a gestar lo que sería la, hasta ahora, última revolución de la criptografía teórica y práctica: los sistemas asimétricos. Estos sistemas supusieron un salto cualitativo importante ya que permitieron introducir la criptografía en otros campos que hoy día son esenciales, como el de la firma digital.

Marco teórico:

Un *número perfecto:*

Es aquel que la suma de sus divisores propios da como resultado el número en si mismo. Por ejemplo, el número 6 tiene como divisores propios al 1, 2 y al 3 y 1 + 2 + 3 = 6, 28 tiene divisores 1, 2, 4, 7 y 14 y 1 + 2 + 4 + 7 + 14 = 28.

Divisibilidad

Un número a se puede dividir por otro número b (o también, a es divisible por b), cuando con el número de unidades que indique el número a se puedan hacer tantos números como indique el número b, teniendo todos estos grupos el mismo número de unidades.

Ej: 12 se puede dividir por 3.

Existen diferentes criterios de divisibilidad que se encuantran en la planificación aúlica.

Un *par de números amigables*:

Es un par como 220 y 284 tal que los divisores propios de un número suman el otro y viceversa.

Método del absurdo:

Es un método de demostración (a menudo usado por Aristóteles como un argumento lógico) en el que asumimos una hipótesis y obtenemos un resultado absurdo, por lo que concluimos que la hipótesis de partida ha de ser falsa. Este método es también conocido como **prueba por contradicción** o prueba **ad absurdum**. Parte de la base es el cumplimiento de la ley de exclusión de intermedios: una afirmación que no puede ser falsa, ha de ser consecuentemente verdadera. Supongamos que se desea demostrar la proposición *P*. El procedimiento consiste en demostrar que asumiendo como cierta la falsedad de *P* (o sea, *P negada*) conduce a una contradicción lógica. Esta *P* no puede ser falsa, por lo que ha de ser verdadera.Por ejemplo, consideremos la proposición "no existe un número racional mínimo mayor que cero". En una *reducción al absurdo*, comenzaríamos

por asumir lo contario que existe un mínimo número racional y que es mayor que cero; llamémoslo r_0.
Ahora, hagamos $x = r_0/2$. Por lo tanto, x es un número racional mayor que cero; y x es más pequeño que r_0. Pero eso es absurdo, contradice nuestra hipótesis de partida de que r_0 era el número racional mínimo. Por lo tanto, debemos concluir que la proposición que asumimos como cierta: "hay un número racional mínimo mayor que cero" es falsa.
No es inusual utilizar este tipo de razonamiento con proposiciones como la indicada, acerca de la inexistencia de cierto elemento matemático. Se asume que ese elemento existe y se prueba que eso conduce a una contradicción; por lo tanto, ese objeto no existe. Por ejemplo, se puede probar de esta manera que la raíz cuadrada de 2 es irracional.
La **demostración por reducción al absurdo** es un tipo de argumento lógico muy empleado en las demostraciones matemáticas. Consiste en demostrar una proposición matemática probando que el que no lo sea conduce a una contradicción.
Un ejemplo es la demostración de que la raíz cuadrada de 2 es un número irracional. La afirmación inicial es la contraria: imagínese que es un número racional, es decir, que
$\sqrt{2} = \frac{p}{q}$, donde p y q son números enteros, y que q es distinto de 0. Sin pérdida de generalidad, se puede suponer que p y q son positivos (si los dos son negativos, basta con multiplicarlos por -1), y que son primos entre sí, es decir, que no comparten ningún factor común (en caso contrario, basta con dividirlos entre su máximo común divisor).
Elevando al cuadrado:
$2 = \frac{p^2}{q^2}$
Multiplicando por q^2 se tiene:
$2q^2 = p^2$ La expresión es un número par, así que también lo es. Eso implica que p es par, porque, de no serlo, no sería par, con lo que no se podría cumplir la igualdad. Sea, donde n es un número entero. Así, la expresión queda:
$2q^2 = (2n)^2 = 4n^2$

Simplificando, se tiene:
$q^2 = 2n^2$

Por el mismo razonamiento de antes, $2n^2$ es un número par, así es que q^2 también es par, y q también es par.

Como p y q son los dos pares, eso quiere decir que tienen al menos un factor común, que es 2. Esto entra en contradicción con la forma en que se han elegido los números p y q para que no tuvieran ningún factor común. Como esta elección de p y q se hizo sin pérdida de generalidad y el razonamiento posterior es correcto, eso quiere decir que la premisa inicial de que $\sqrt{2}$ era racional es falsa.
Luego $\sqrt{2}$ es irracional.

Teoría de los números

Teoría elemental de números

En la teoría elemental de números, se estudian los números enteros sin emplear técnicas procedentes de otros campos de las matemáticas. Pertenecen a la teoría elemental de números las cuestiones de divisibilidad, el algoritmo de Euclides para calcular el máximo común divisor, la factorización de los enteros como producto de números primos, la búsqueda de los números perfectos y las congruencias. Son enunciados típicos el pequeño teorema de Fermat y el teorema de Euler que lo extiende, el teorema chino del resto y la ley de reciprocidad cuadrática.

En esta rama se investigan las propiedades de las funciones multiplicativas como la función de Möbius y la función φ de Euler; así como las sucesiones de números enteros como los factoriales y los números de Fibonacci.

Diversos cuestionamientos dentro de la teoría elemental de números parecen simples, pero requieren consideraciones muy profundas y nuevas aproximaciones, incluyendo las siguientes:

- Conjetura de Goldbach sobre que todos los números pares (a partir de 4) son la suma de dos números primos.
- Conjetura de los números primos gemelos sobre la infinitud de los llamados números primos gemelos
- Último teorema de Fermat (demostrado en 1995)
- Hipótesis de Riemann sobre la distribución de los ceros de la función zeta de Riemann, íntimamente conectada con el problema de la distribución de los números primos.

Teorema Fundamental de Aritmética:

Todo entero puede ser escrito como un producto único de primos.

Números primos:

Un número primo[1] es un número entero mayor que cero, que tiene exactamente dos divisores positivos. También podemos definirlo como aquel número entero positivo que no puede expresarse como producto de dos números enteros positivos más pequeños que él, o bien, como producto de dos enteros positivos de más de una forma. Conviene observar que con cualquiera de las dos definiciones el 1 queda excluido del conjunto de los números primos.

[1] El término primo no significa que sean parientes de alguien. Deriva del latín "primus" que significa primero (πρωτος, protos en griego). El teorema fundamental de la aritmética afirma que todo número entero se expresa de forma única como producto de números primos. Por eso se les considera los "primeros", porque a partir de ellos obtenemos todos los demás números enteros. (El 15 se obtiene multiplicando los primos 3 y 5.

Ejemplos: a) El 7 es primo. Sus únicos divisores son 1 y 7. Sólo puede expresarse como producto de 7·1.

b) El 15 no es primo. Sus divisores son 1, 3, 5 y 15. Puede expresarse como 3·5. (Y también como 15·1)

Tamiz de Eratóstenes:

Tabla realizada por Erastóstenes para descubrir o encontrar los primeros números primos en diez decenas. El método consiste en graficar una cuadricula de cien números.

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

El 1 no cuenta y luego se tachan los múltiplos de 2, 3, 5, 7. Luego quedarán al descubierto los números primos.

Características

Números primos gemelos

Dos números primos (p, q) son números primos gemelos si están separados por una distancia de 2, es decir, si $q = p + 2$.

Los primeros números primos gemelos son:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43),
(59, 61), (71, 73), (101, 103), (107, 109), (137, 139), (149, 151),
(179, 181), (191, 193), (197, 199), (227, 229), (239, 241), (269, 271),
(281, 283), (311, 313), (347, 349), (419, 421), (431, 433), (461, 463),
(521, 523), (569, 571), (599, 601), (617, 619), (641, 643), (659, 661),
(809, 811), (821, 823), (827, 829), (857, 859), (881, 883).

Lagunas de primos:

Son aquellas tiras de números compuestos que no son primos. Por ejemplo 20, 21, 22.

Irregularidad e inexactitud

¿Cuántos números primos hay?

Una de las primeras preguntas que podemos hacernos es si la cantidad de números primos es finita o infinita. Euclides de Alejandría demostró que hay infinitos.

Demostración de Euclides

Supongamos que existe solamente un número finito de primos:

Sea C = {p1, p_2,... $P_{.D.}$ } el conjunto formado por todos ellos.

Consideremos ahora el número M = $p_1 sp_a \times ... P_{.D.}+1$. Como cada primo $p_{i.}$ Es mayor que 1, M es un número mayor que cualquiera de los $p_{i.}$; es decir, M no está en el conjunto C y por tanto es compuesto.

Admitirá entonces una descomposición como producto de factores primos (por el teorema fundamental de la aritmética).

Por hipótesis, estos factores sólo pueden estar entre los primos que aparecen en el conjunto C.

Por tanto, existirá un primo q del conjunto C, tal que q | M y obviamente, q | $p_1 sp_a \times ... p_n$. Por consiguiente, q divide a la diferencia M - $p_1 \times p_2 \times ... \times p_n$ (que es 1). Pero ningún número primo divide a 1, y q es un número primo que divide a 1 (Contradicción). Concluimos entonces que el conjunto de los números primos no puede ser finito.

Utilización

En la actualidad donde se puede observar la utilización de los números primos.
Hace poco tiempo un equipo de investigadores de la compañía Cray, fabricante de supercomputadoras, fue capaz de hallar un número primo de 258.716 dígitos. Para escribir el número completo con todos sus dígitos se necesitarían unas cuantas páginas de esa revisa. Esta noticia, que para muchos puede resultar algo extraña y, para decir lo menos, hasta absurda, dio la vuelta al mundo en los titulares de los periódicos.

En la escuela todos aprendemos lo que son los números primos: un número n es primo si sólo es divisible entre 1 y n mismo. Por ejemplo, 31 es primo, y 99 no lo es. Además, muy posiblemente todos recordemos también un método para determinar si un número dado es o no es primo. La forma más obvia de hacerlo es la siguiente. Dado un número n, vemos si es divisible entre 2, después si es divisible entre 3, etc.. , continuando así hasta llegar a la raíz cuadrada de n. Si no encontramos ningún divisor, podemos afirmar que es primo.

Nada más sencillo. El problema es que este método es muy ineficiente cuando n es un número muy grande, Por ejemplo, para saber si 123456789012345677 es primo tendríamos que hacer aproximadamente mil millones de divisiones. Trate el lector de determinar por este método si el número 2^{859433}-1 es primo (esto es, 2 elevado a la potencia 859433, que es un número par, menos 1). Este, precisamente, es el primo hallado por los matemáticos de Cray.

Determinar si un número dado es o no es primo es uno de los problemas más interesantes de la aritmética. La historia de las matemáticas está salpicada, a través de los siglos, de desarrollos de métodos para determinar

primalidad, y en la actualidad, la investigación destinada a producir métodos eficientes para hacerlo es un campo sumamente activo.

Un problema relacionado es el de factorizar un número dado en factores primos. Si probar que un determinado número n muy grande es primo es un problema complicado, hallar los factores primos de n, aún teniendo la seguridad de que o no es primo, es, en general, un problema más difícil todavía que requiere más tiempo de cálculo.

¿Qué importancia puede tener saber que 2^{859433}-1 es primo? Se trata de algo que va mucho más allá de una mera curiosidad intelectual o de un alarde de virtuosismo aritmético. Resulta que en los años recientes se han hecho grandes avances en criptografía mediante el uso de resultados de la teoría de números y, en particular mediante el uso de números primos muy grandes.

La criptografía es el estudio de los sistemas de codificación para la transmisión de mensajes en forma secreta. Un sistema criptográfico funciona usualmente de este modo. El mensaje que se desea trasmitir es codificado mediante una clave secreta, y esta codificación sólo podrá ser descifrada por quien conozca la clave.

Otra definición:

La criptografía (del griego κρύπτω krypto, «oculto», y γράφω graphos, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

Sin embargo, como es bien sabido, con mucho ingenio y tiempo suficiente, ha sido posible burlar códigos secretos y descifrar mensajes

trasmitidos usando sistemas de codificación muy sofisticados. La historia de la Segunda Guerra Mundial abunda en anécdotas de este tipo.

Usando números primos muy grandes se ha podido desarrollar sistemas criptográficos llamados de clave pública.

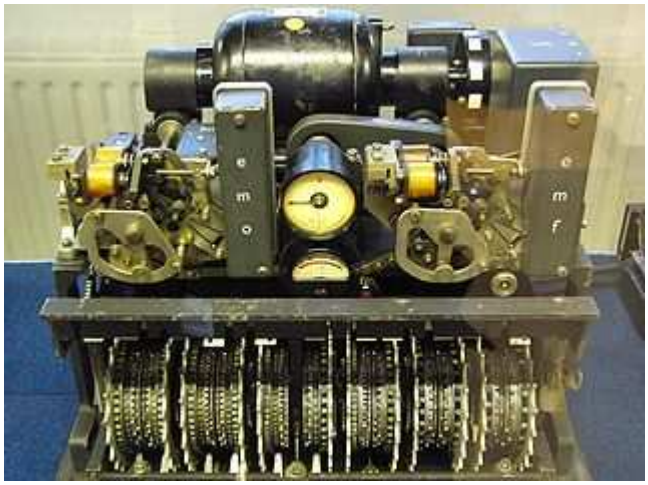
Mediante estos sistemas de codificación, dos personas se pueden transmitir datos con gran seguridad de que un tercero no podrá descifrar los mensajes. El sistema de codificación se basa en conocer un par de números primos muy grandes; el producto de estos números primos se utiliza para codificar la información a ser trasmitida, y la codificación se hace de tal modo que hallar la clave resulta tan difícil como hallar la factorización de ese producto de primos, es decir, hallar los dos números primos grandes usados en la codificación, y esto, como hemos mencionado anteriormente, resulta una labor extremadamente difícil, por no decir imposible, si los números involucrados son muy grandes.

En los sistemas de clave pública se usa una clave para codificar y otra clave para descifrar, y también se puede usar varias claves para cada una de estas operaciones. Así, se puede dar a conocer las claves de codificación (claves públicas) manteniendo secretas las claves para descifrar.

Los sistemas criptográficos a clave pública permiten la trasmisión secreta de mensajes entre varias personas, de modo que la persona A puede enviar un mensaje que sólo puede ser descifrado por la persona B, y otro mensaje que sólo puede ser descifrado por la persona C, cada una de las cuales conoce su propia clave secreta para descifrar. Es más, quien recibe el mensaje puede determinar si quien lo envió fue en realidad la persona A o fue un impostor.

Hacia 1940, el matemático inglés G. H. Hardy se regocijaba pensando que al menos un área de la ciencia (la teoría de números), se mantuviese remotamente alejada de las actividades humanas ordinarias, ya que de esta forma esta ciencia se podía mantener limpia. Cuál no sería su sorpresa si se enterase de que organismos de seguridad del Gobierno de los EE.UU. han intentado controlar la publicación de artículos de investigación sobre teoría

de números que contengan información sobre números primos muy grandes. Afortunadamente la American Mathematical Society logro que esta prohibición no fuese establecida, al menos por ahora.



La máquina alemana de cifrado de Lorenz, usada en la Segunda Guerra Mundial para el cifrado de los mensajes para los generales de muy alto rango

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía es auténtica en un doble sentido: que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido .Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca

asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

En la Jerga de la criptografía, la información original que debe protegerse se denomina *texto en claro*. El ***cifrado*** es el proceso de convertir el *texto plano* en un galimatías ilegible, denominado *texto cifrado* o *criptograma*. Por lo general, la aplicación concreta del *algoritmo de cifrado* (también llamado *cifra*[2]) se basa en la existencia de una *clave*: información secreta que adapta el *algoritmo de cifrado* para cada uso distinto.

Las dos técnicas más sencillas de *cifrado*, en la criptografía clásica, son la *sustitución* (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la *trasposición* (que supone una reordenación de los mismos); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas.

El ***descifrado*** es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la *clave*. El *protocolo criptográfico* especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de *protocolos*, *algoritmos de cifrado*, procesos de gestión de claves y actuaciones de los usuarios, en conjunto es lo que constituyen un *criptosistema*, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de *cifras*: los algoritmos que utilizan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado*, y los que utilizan una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*.

*Los primeros se denominan *cifras simétricas*, de *clave simétrica* o de *clave privada* y son la base de los algoritmos de cifrado clásico.

[2] *Cifra es una antigua palabra arábiga para designar el número cero; en la antigüedad cuando Europa empezaba a cambiar del sistema de numeración romano al arábigo, se desconocía el cero por lo que este resultaba misterioso, de ahí probablemente que cifrado signifique misterioso*

* Los segundos se denominan *cifras asimétricas*, de *clave asimétrica* o de *clave pública* y forman el núcleo de las técnicas de cifrado modernas.

La **criptografía asimétrica** es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma

persona a la que se ha enviado el mensaje. Una clave es *pública* y se puede entregar a cualquier persona, la otra clave es *privada* y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la *confidencialidad* del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Si el propietario del par de claves usa su clave privada para cifrar el mensaje, cualquiera puede descifrarlo utilizando su clave pública. En este caso se consigue por tanto la *identificación* y *autenticación* del remitente, ya que se sabe que sólo pudo haber sido él quien utilizó su clave privada (salvo que alguien se la hubiese podido robar). Esta idea es el fundamento de la firma electrónica.

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un solo sentido que aprovechan propiedades particulares, por ejemplo de los números primos. Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil. Por ejemplo, es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos. Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza

de la información, sería fácil computar el inverso. Por ejemplo, *si tenemos un número compuesto por dos factores primos y conocemos uno de los factores, es fácil computar el segundo*.

Dado un cifrado de clave pública basado en factorización de números primos, la clave pública contiene un número compuesto de dos factores primos grandes, y el algoritmo de cifrado usa ese compuesto para cifrar el mensaje. El algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos, para que el descifrado sea fácil si poseemos la clave privada que contiene uno de los factores, pero extremadamente difícil en caso contrario.

Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que 10^{100}) elegidos al azar para conformar la clave de descifrado.

La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

Relación

Como observamos en la parte teórica de esta tesina podemos establecer algunos núcleos que se relacionan. Por ejemplo que la aritmética es el estudio de los números y sus relaciones, que la teoría de de los números trata de establecer relaciones con ellos y que la teoría fundamental de la aritmética, la cual se basa en que cualquier número compuesto se puede escribir como un producto de números primos.

Pero en contra posición podemos también observar que los números primos, los cuales son base para lo anterior mencionado, no se rigen con las reglas que las matemáticas dictan. Ellos no tienen un patrón de aparición, no se sabe cuantos hay, ni cuando van a parecer. Los números primos son exactamente el contra ejemplo de la exactitud que caracteriza a la ciencia que fundan. ESTA CARACTERISTICA LOS CONVIERTEN EN ESPECIALES.

Conclusión:

Luego de un estudio más profundo sobre el campo numérico de los números primos puedo afirmar que ellos son el ejemplo en la cual se sustenta, que las matemáticas y en especial los números primos forman parte de nuestra vida.

Las ciencias en donde los conceptos están rígidos e indiscutidos es una ciencia seca y muerta. Los números primos tienen INDEPENDENCIA Y MISTERIO. Como lo observamos en esta investigación, éstos no tienen regularidad y hasta el momento no existe, matemático que pueda establecer un patrón general para hallarlos y por lo tanto no dependen de ninguna expresión, por lo tanto son independientes.

Los contenidos de las ciencias exactas están expectantes a que nosotros los amantes de las matemáticas descubramos su belleza.

No todo en esta ciencia, que algunos la creen muerta, está descubierto.

Planificación del trabajo aúlico

Objetivos

- Que el alumno logre encontrar números primos.
- Que el alumno logre experimentar la búsqueda del nuevo conocimiento.
- Que el alumno logre familiarizarse con expresiones algebraicas distintas a las vistas habitualmente.

Para comenzar la clase el docente comentará el tema de los números primos y recordarán sus características.

A continuación les contará un poco de la historia de estos números y conocerán la vida de Marín Mersenne. Luego en el pizarrón tendrán escrito una afirmación del matemático.

> Los números primos de la forma $2^n - 1$ también atrajeron la atención porque es muy fácil demostrar que a menos que *n* sea primo, este número será compuesto. A menudo éstos son llamados *Números primos de Mersenne* Mn.

Entre todos buscarán números en el pizarrón y en las carpetas. Con los alumnos verificarán la afirmación.

Con n compuesto

$n = 8$	$n = 6$	$n = 4$
$2^8 - 1 = 255$	$2^6 - 1 = 63$	$2^4 - 1 = 15$

Con n primo

$n = 2$	$n = 3$	$n = 5$
$2^2 - 1 = 3$	$2^3 - 1 = 7$	$2^5 - 1 = 31$

Pero el docente pretenderá con esta actividad que un alumno, por la experimentación, contraponga la afirmación.

Luego surge una nueva afirmación que extiende lo anterior dicho. También resuelto por el autor

No todos los números de la forma $2^n - 1$ con n primo son primos.

Por ejemplo $2^{11} - 1 = 2047 = 23 \times 89$ es compuesto, aunque fue notado por primera vez en 1536. Buscan más ejemplos.

También para comprobar si es compuesto, debo saber si es divisible por mas de un número. La tabla con los criterios de divisibilidad nos pueden ayudar.

Criterios de divisibilidad

Los siguientes criterios nos permiten averiguar si un número es divisible por otro de una forma sencilla, sin necesidad de realizar una división:

Número	Criterio	Ejemplo
2	El número termina en cero o cifra par.	378: porque "8" es par.
3	La suma de sus cifras es un múltiplo de 3.	480: porque 4+ 8+ 0 = 12 es múltiplo de 3.
4	El número formado por las dos últimas cifras es 00 ó múltiplo de 4.	7324: porque 24 es múltiplo de 4.

5	La última cifra es 0 ó 5.	485: porque acaba en 5.
6	El número es divisible por 2 y por 3.	24: Ver criterios anteriores.
7	Para números de 3 cifras: Al número formado por las dos primeras cifras se le resta la última multiplicada por 2. Si el resultado es múltiplo de 7, el número original también lo es.	469: porque 46-(9*2)= 28 que es múltiplo de 7.
	Para números de más de 3 cifras: Dividir en grupos de 3 cifras y aplicar el criterio de arriba a cada grupo. Sumar y restar alternativamente el resultado obtenido en cada grupo y comprobar si el resultado final es un múltiplo de 7.	52176376: porque (37-12) - (17-12) + (5-4)= 25-5+1= 21 es múltiplo de 7.
8	El número formado por las tres últimas cifras es 000 ó múltiplo de 8.	27280: porque 280 es múltiplo de 8.
9	La suma de sus cifras es múltiplo de 9.	3744: porque 3+7+4+4= 18 es múltiplo de 9.
10	La última cifra es 0.	470: La última cifra es 0.
11	Sumando las cifras (del número) en posición impar por un lado y las de posición par por otro. Luego se resta el resultado de ambas sumas obtenidas. si el resultado es cero (0) o un múltiplo de 11, el número es divisible por éste.	42702: 4+7+2=13 · 2+0=2 · 13-2=11 → 11 es múltiplo de 11
12	El número es divisible por 3 y 4.	528: Ver criterios anteriores.
13	Para números de 3 cifras: Al número formado por las dos primeras cifras se le suma la última multiplicada por 4. Si el resultado es	364: porque 36+4·4= 52 es múltiplo de 13.

	múltiplo de 13, el número original también lo es.	
	Para números de más de 3 cifras: Dividir en grupos de 3 cifras, sumar y restar alternativamente los grupos de derecha a izquierda y aplicar el criterio de arriba al resultado obtenido. Si es múltiplo de 13, el número original también lo es.	432549: porque 549-432 = 117 y luego 11 + 4·7 = 39 es múltiplo de 13.
14	El número es divisible por 2 y por 7.	224: Ver criterios anteriores
15	El número es divisible por 3 y por 5.	255: Ver criterios anteriores
16	El número formado por las cuatro últimas cifras es múltiplo de 16.	254176: porque 4176 es múltiplo de 16.
17	Al número obtenido al suprimir la última cifra, se le resta esta última cifra multiplicada por 5, y se comprueba si el resultado es múltiplo de 17.	493: porque 49-5·3 = 34 es múltiplo de 17.
18	El número es divisible por 2 y por 9.	576: Ver criterios anteriores
19	Al número obtenido al suprimir la última cifra, se le suma esta última cifra multiplicada por 2, y se comprueba si el resultado es múltiplo de 19.	323: porque 32+3·2 = 38 es múltiplo de 19.
20	El número acaba en cero y la penúltima cifra es par.	480: porque acaba en 0 y 8 es par.
21	El número es divisible por 3 y por 7.	231: Ver criterios anteriores

22	El número es divisible por 2 y por 11.	220: Ver criterios anteriores
24	El número es divisible por 3 y por 8.	480: Ver criterios anteriores
25	Las dos últimas cifras son 00 ó múltiplo de 25.	9325: porque acaba en 25
26	El número es divisible por 2 y por 13.	234: Ver criterios anteriores
28	El número es divisible por 4 y por 7.	336: Ver criterios anteriores
30	El número acaba en cero y la suma de sus cifras es un múltiplo de 3.	690: porque acaba en cero y 6+9+0 = 15 es múltiplo de 3

Realizamos experimentación en el pizarrón, para corroborar, errar y acertar. Así encontrar más números para afirmar o refutar tal afirmación.

Conversamos de la importancia que tienen los números primos en la aritmética y la experimentación del ensayo y error para encontrar resultados y generalizaciones. Para continuar aprendiendo.

En forma individual

1. Buscan 5 números compuestos con n primo y colocan la factorización correspondiente.
2. Realizan la misma actividad, esta vez en forma individual, con la siguiente afirmación de Fermat.

Los números $2^n + 1$ eran siempre primos si n es una potencia de 2.

Verifica para n= 1, 2, 4, 8, 16 y 32. lo cumple?

Evaluación:

- Recorrido del docente por los bancos.
- Compartir los resultados con el compañero de banco.
- Puesta en común en el pizarrón.

Bibliografía

- Morris Kline,"*El pensamiento matemático desde la antigüedad hasta nuestros días*", Ed: Alianza. Madrid, España, 1992.
- Adrián Paenza "Matemática…¿estás ahí?"Sobre números, personajes, problemas y curisidades, Ed.: Siglo veintiuno editores. Buenos Aires, Argentina. 2005.
- http://es.wikipedia.org/wiki/N%C3%BAmero_primo
- http://es.wikipedia.org/wiki/Criptograf%C3%ADa
- http://ili-2008.wikispaces.com/file/view/marcus+du+sautoy.doc
- Du Sautoy Marcos "La música de los números primos", ED.: El Acantilado.