LOS TEOREMAS DE LA FACTORIZACIÓN DE CORDERO EN EL CONJUNTO DE LOS NÚMEROS ENTEROS

Data de aceite: 01/11/2023

Ronald Cordero Méndez
Universidad Internacional San Isidro Labrador. Costa Rica.

RESUMEN: Se presentan Los Teoremas de la Factorización de Cordero en el conjunto Z. Ejemplos de aplicación de estos teoremas. Utilidad en el cálculo de números primos muy grandes, así como en la factorización de números enteros muy grandes. Contribución a la Teoría de Números en un problema del que no se tiene una solución eficiente como es la factorización de números enteros y material de apoyo para la construcción de software que permitan el cálculo de números primos muy grandes necesarios en la criptografía.
PALABRAS CLAVE: Factorización, números primos, números afortunados de Euler, Teoremas.

ABSTRACT: The Cordero Factorization Theorems in the set Z are presented. Examples of application of these theorems. Useful in the calculation of very large prime numbers, as well as in the factorization of very large integers. Contribution to the Theory of Numbers in a problem for which there is no efficient solution, such as the factorization of integers and support material for the construction of software that allows the calculation of very large prime numbers necessary in cryptography.
KEYWORDS: Factorization, prime numbers, Euler's lucky numbers, Theorems.

1 | POLINOMIOS GENERADORES DE NÚMEROS PRIMOS Y COMPUESTOS.

Los números primos han sido tema de muchas investigaciones, muchas repetitivas que contribuyen poco al tema, lo que verifica la frase del gran matemático Leonhard Euler que dice**:** "Los matemáticos han intentado en vano, hasta la actualidad descubrir algún orden en la secuencia de números primos, y tenemos razones para creer que se trata de un misterio que la mente humana nunca resolverá" (Leonard Euler, 1707-1783, mencionado por Camacho y Camacho, 2020, p.85). Hasta el momento en el año 2022 este misterio no ha sido resuelto, por lo que creo que Euler puede estar en lo cierto. Leonhard Euler nació el 15 de abril de 1707 en

Basilea, Suiza y murió el 18 de septiembre de 1782 en San Petersburgo, Rusia (Aznar, 2007). Extraordinario matemático del siglo XVIII.

Otra frase que lo afirma dice:

> El encanto de los números primos consiste quizás en la imposibilidad de explicar en qué orden aparecen. Cada uno se dispersa a su antojo, cumpliendo la condición de no tener más divisores que el uno y él mismo. Aunque no cabe duda de que cuanto más grandes son, más difícil resulta encontrarlos, y es imposible predecir su aparición siguiendo ninguna regla… "La fórmula preferida del profesor (Ogawa, 2003, mencionadado por Frases y Pensamientos, s.f., párr. 4)

Nuestra pregunta ahora es cómo encontrar números primos, si no es posible encontrar una fórmula polinomial o de otro tipo que nos genere todos y cada uno de los números primos, o por lo menos una fórmula que genere solamente números primos aunque no sean consecutivos.

En algún momento dado aparecen los números compuestos que se mezclan con los números primos, por lo que me lleva a suponer que el cribado es una buena opción para encontrar números primos grandes.

Con ayuda de los polinomios $P(n) = n^2 + n + p$, donde p = 2, 3, 5, 11,17, 41 que resulta ser polinomios que generan números primos cuando n toma valores desde 0 h*asta* $n = p - 2$, y luego generan números compuestos y primos mezclados, por lo que el problema de encontrar una fórmula que genere solamente números primos no lo resuelve este tipo de polinomios. Pero encontrar una fórmula que genere los números compuestos que son generados por estos polinomios es el tema de la investigación además de buscar un procedimiento que ayude a cribar los números primos.

2 | POLINOMIOS DE LA FORMA $P(n) = n^2 + n + p$, DONDE $p = 2, 3, 5, 11, 17, 41$.

Los polinomios $P(n) = n^2 + n + p$, generan números primos, por ejemplo, se generan los números primos: 41, 43, 47, 53, 61, 71, 83, 97, 113, 181, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 707, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523,1601

cuando $P(n) = n^2 + n + 41$ y desde $n = 0$ h*asta* $n = 41 - 2 = 39$, en total 40 números primos, pero a partir de $n = 40$ se generan números compuestos y números primos. A este poliomio se le llama polinomio de Euler.

Otra forma de escribir el polinomio de Euler es $P(n) = n^2 - n + 41$, pero éste genera los números primos anteriores cuando, n toma valores desde 1 hasta 40.

Otro polinomio de esta forma que genera números primos es $P(n) = n^2 + n + 17$ desde $n = 0$ h*asta* $n = 17 - 2 = 15$, *el* cual fue descubierto por el matemático Adrien Marie Legendre:

> Legendre nació en París en el año 1752 en una familia rica. Recibió educación en el Collage Mazarin en París, y defendió su tesis en física y matemática en 1770. Murió en París en el año 1833, después de una larga y penosa enfermedad. Su viuda conservó cuidadosamente las pertenencias del matemático para preservar su memoria. El último lugar donde vivió fue en el pueblo de Auteuil en París, Francia (Fernández y Tamaro, 2004, párr.1)

3 | LOS NÚMEROS AFORTUNADOS DE EULER

Primero dejemos claro que Goldbach y Legendre demostraron que no es posible encontrar un polinomio que dé números primos para todo número natural, el primero lo demostró para coeficientes enteros y el segundo para funciones algebraicas racionales.

El matemático Rabinowitz demostró que $P(n) = n^2 + n + p$ da números primos para $n = 0, \dots, p - 2$ si y solo si $1 - 4p$ es el negativo de un número de Heegner, que son los únicos números positivos k, que cumplen no ser cuadrados perfectos y que en el anillo de enteros del cuerpo $\mathbb{Q}(\sqrt{-k})$ es de factorización única.

Los números de Heegner son: 1,2,3,7,11,19,43, 67,163.

Además los números afortunados de Euler son los enteros positivos p, para los que $1 - 4p = -k$, siendo k un número de Heegner, y mediante comprobación obtenemos que los únicos posibles son 2, 3, 5, 11, 17, 41 y el número de Heegner asociado al 41 es el 163.

4 | PROBLEMÁTICA DE LA FACTORIZACIÓN DE LOS NÚMEROS ENTEROS.

No se ha encontrado un procedimiento eficiente para factorizar completamente (en sus factores primos) un número entero muy grande. Los números enteros muy grandes más difíciles de factorizar son aquellos que tienen solamente dos factores diferentes de uno y de aproximadamente el mismo tamaño.

En 1970 el límite era 20 dígitos, luego con el método de las fracciones continuas de Brillhart- Morrison se llegó a 50 dígitos en 1980. En el año 1994 se logra factorizar números de 100 dígitos por medio del método de la criba cuadrática de Carl Pomerance y luego se añaden métodos de factorización de números enteros como el de cuerpos algebraicos de Pollard y el método de Lenstra el cual utiliza curvas elípticas.

El algoritmo de criba cuadrática (QS), es un algoritmo de factorización de números enteros y en la práctica es el segundo método más rápido conocido superado en poco por la criba general del cuerpo de números. Es de propósito general, lo que significa que su tiempo de ejecución únicamente depende del tamaño del número entero y no sobre una estructura especial o de propiedades.

La factorización de curva elíptica de Lenstra o método de factorización de curva elíptica es un rápido algoritmo de tiempo de ejecución sub-exponencial para la factorización de enteros que utiliza curvas elípticas. Es el tercer método más rápido conocido de

factorización, superado por el algoritmo de la criba cuadrática (QS) y por la criba general del cuerpo de números.

El método de factorización de curva elíptica es de propósito especial y el más adecuado para encontrar factores pequeños, útil para encontrar divisores que no superen los 20 o 25 dígitos, así como su tiempo de ejecución está dominado por el tamaño del factor más pequeño, en lugar de por el tamaño del número a factorizar. Frecuentemente este método se utiliza para eliminar factores pequeños de un entero muy grande con muchos factores; si el entero resultante es todavía compuesto, entonces solo tiene factores grandes y es factorizado mediante el uso de técnicas de propósito general. El factor más grande encontrado con este método cuenta con 75 dígitos y fue descubierto el 2 de agosto del 2012 por Samuel Wagstaff. Incrementando el número de curvas probadas se mejoran las posibilidades de encontrar un factor. Hay consenso de que la factorización de números es un problema difícil, pero los avances nos dan una esperanza, quizás haya una solución muy pronto.

Hoy día la computación cuántica enfrenta el reto matemático de factorizar en números primos números enteros muy grandes. Investigadores de la Universidad Politécnica de Madrid en España han abordado el reto de factorizar números muy grandes en sus factores primos utilizando un dispositivo cuántico que simula la aritmética, en vez de calcular.

Pero la complejidad para factorizar un número muy grande se ha aprovechado para realizar algoritmos de criptografía que permiten mantener información privada segura. La criptografía es el estudio de las técnicas matemáticas relacionadas con los aspectos de seguridad informática tal como: la confidencialidad, la integridad de datos, la autenticidad y el no rechazo. Hay dos tipos de criptografía: criptografía simétrica o de clave privada y criptografía asimétrica o de clave pública. La principal aplicación de la criptografía es proteger la información para evitar que sea accesible a observadores no autorizados. Verificar que un mensaje no haya sido modificado a conveniencia por ejemplo. Es aquí donde la matemática juega un papel muy importante, y sobre todo los números primos muy grandes, puesto que los números primos muy grandes de más de 100 dígitos permiten formar semiprimos o biprimos que son el producto de dos números primos muy grandes y que sirven de códigos de seguridad, por su dificutad para ser factorizados.

La factorización de un número natural o entero necesita de más estudio, actualmente no se tiene un procedimiento 100% eficaz y eficiente, y esto no es producto de falta de investigación, puesto que en la historia de la matemática podemos considerar que valiosos genios de la humanidad trabajaron para encontrar una solución, como es el caso del francés Pierre de Fermat (1601-1665) y el Suizo Leonhard Euler (1707-1783).

El creciente desarrollo de la tecnología y la construcción de diferentes algoritmos matemáticos no han podido darle fin a la rapidez y eficiencia que debe tener un software que factorice números enteros, esto deja en evidencia el reto de los matemáticos actuales y futuros en el estudio de este tema.

5 | NÚMEROS COMPUESTOS Y PRIMOS GENERADOS POR POLINOMIOS.

¿Puede un polinomio no constante, de coeficientes enteros, tomar solamente valores primos?; la respuesta es no, ¿por qué?, debido al siguiente teorema.

Teorema.

Si $f(x) \in Z[x]$ *tiene grado positivo, entonces existe una cantidad infinita de números naturales n para los cuales* $f(n)$ *es un número compuesto.*

La otra pregunta que podemos hacernos es la siguiente:

¿Todo polinomio no constante f (x) ∈ Z[x] (conjunto de todos los polinomios de coeficientes enteros) puede generar infinita cantidad de números primos? Intrigante pregunta. Bouniakowsky y luego Schinzel y Sierpinski (1958) conjeturaron que si f (x) ∈ Z[x] irreducible, primitivo, es decir, el máximo común divisor de sus coeficientes enteros es igual a 1 y si más aún no hay ningún primo que divida a todos los valores de f(n) para enteros arbitrarios n, entonces este tipo de polinomios siempre generan números primos. (Revista Colombiana de Matemáticas. Vol XXI (1987). pág 263).

6 | EL TEOREMA PRINCIPAL.

TEOREMA.

Sea p un número primo y hagamos $f_p = n^2 + n + p$. Entonces las siguientes condiciones son equivalentes:

i. p=2,3,4,11,17,41

ii. $f_p(n)$ es un número primo para n=0,1,2,3,...,p-2

iii. $\mathbb{Q}\left(\sqrt{1-4p}\right)$ tiene número de clase igual a 1.

Tenemos que i. → ii., basta con sustituir p por 2,3,4,11,17,41 y verificar que en efecto se generan números primos desde n=0 hasta n=p-2.

La equivalencia de las condiciones ii.→ iii. fue demostrada por primera vez por Rabinovitch en 1912 y en 1936 es demostrada por Lehmer. Mientras que iii.→ ii. es demostrada por Szekeres en 1974 y por Ayoub y Chowla en 1981. (Revista Colombiana de Matemáticas. Vol XXI (1987). pág 281).

7 | IMPORTANCIA DE FACTORIZAR NÚMEROS ENTEROS GRANDES

Los algoritmos criptográficos se basan en un un problema computacionalmente difícil de resolver, la mayoría de los algoritmos empleados en criptografía de llave pública, tienen como problema a resolver la factorización prima de números grandes. El más usado en la actualidad es el algoritmo RSA, descubierto por Ron Rivest, Adi Shamir y Len Adleman, de ahí sus iniciales RSA. El RSA es el algoritmo de llave pública mas usado en el planeta, tanto para cifrado y descifrado como para fines digitales.

El algoritmo RSA es seguro mientras la llave privada solo la conozca el dueño. La

llave pública y privada se encuentran matemáticamente relacionadas de tal manera que a partir de la llave pública sea imposible generar la llave privada.

La fortaleza del algoritmo radica en la dificultad para factorizar números grandes, y lo cual hasta el momento no tiene una solución satisfactoria y definitiva.

8 | LOS TEOREMAS DE LA FACTORIZACIÓN DE CORDERO EN EL CONJUNTO DE LOS NÚMEROS ENTEROS.

Los teoremas aquí publicados, y sus aplicaciones, aunque no resuelven el difícil problema de factorizar completamente un número entero muy grande, son muy útiles para factorizar en dos factores un número entero, sin necesidad de recurrir a software, test de primalidad, o divisiones sucesivas. La factorización de estos números de forma polinomial cuadrática se puede encontrar utilizando fórmulas matemáticas descubiertas por el autor de este artículo.

8.1 Primer Teorema de la factorización de Cordero en Z

Teorema que permite factorizar en dos factores números de la forma $n^2 + n + p$ donde n ∈ $\mathbb{Z}$

Sea $r, s, x, k \in \mathbb{Z}\ y\ \ p \in \{2,3,5,11,17,41\}.$

1) Si $n = ((rs - r + 1)^2 \bullet x^2 - (rs - r + 1)(rs - r + 2s - 1) \bullet x + p \bullet (rs - r + 1)^2 + (rs + s + 1)(s - 2) + r + 2))(k - 1) + r(rs - r + 1) \bullet x^2 - (r(r + 2)(s - 2) + r^2 + 3r + 1)x + pr(rs - r + 1) + (r + 1)(s - 1)$

$entonces$: $n^2 + n + p$ es compuesto y dos de sus factores tienen la forma:

$$f_1 = (rs - r + 1)^2 \bullet x^2 - (rs - r + 1)(rs - r + 2s - 1) \bullet x + p \bullet (rs - r + 1)^2 + (rs + s + 1)(s - 2) + r + 2)$$

$$f_2 = \frac{n^2+n+p}{f_1} = f_1 * (k - 1)^2 + (2\beta + 1)(k - 1) + r^2x^2 - r(r + 2)x + pr^2 + r + 1$$

2) Si $n = ((rs - r + 1)^2 \bullet x^2 - (rs - r + 1)(rs - r + 2s - 1) \bullet x + p \bullet (rs - r + 1)^2 + (rs + s + 1)(s - 2) + r + 2))(k + 1) - (r(rs - r + 1) \bullet x^2 - (r(r + 2)(s - 2) + r^2 + 3r + 1)x + pr(rs - r + 1) + (r + 1)(s - 1) + 1)$

$entonces$: $n^2 + n + p$ es compuesto y dos de sus factores tienen la forma:

$$f_1 = (rs - r + 1)^2 \bullet x^2 - (rs - r + 1)(rs - r + 2s - 1) \bullet x + p \bullet (rs - r + 1)^2 + (rs + s + 1)(s - 2) + r + 2)$$

$$f_2 = \frac{n^2+n+p}{f_1} = f_1 * (k + 1)^2 - (2\beta + 1)(k + 1) + r^2x^2 - r(r + 2)x + pr^2 + r + 1$$

Con $\beta = r(rs - r + 1) \bullet x^2 - (r(r + 2)(s - 2) + r^2 + 3r + 1)x + pr(rs - r + 1) + (r + 1)(s - 1)$

Nota: $r\ y\ s\ no\ pueden\ ser\ cero\ simultáneamente.$

También es importante aclarar que el teorema es válido en el conjunto de los

números reales y en el conjunto de los números complejos, es decir que las variables pueden ser sustituidos por números complejos y el Teorema se cumple.

8.1.1 Aplicaciones del Primer Teorema de La Factorización de Cordero en el Conjunto Z.

Si damos valores enteros a las variables que conforman las fórmulas del Primer Teorema de La Factorización de Cordero en los enteros, podemos encontrar la factorización en dos factores de los números de la forma $n^2 + n + p$ con $p \in \{2, 3, 5, 11, 17, 41\}$. Es importante aclarar que los cinco teoremas que aquí se publican son válidos en cualquier conjunto numérico, es decir las variables pueden ser sustituidas por números naturales, enteros, racionales, irracionales, reales o complejos y los teoremas se cumplen. Pero el objetivo de esta publicación es factorizar números naturales, por lo que nos limitaremos a dar solamente valores enteros a las variables que contienen las fórmulas.

Aplicación 1

Sea $r = 239, s = 678, x = 100\ ,\ k = 451\ y\ p = 41$ tenemos que:

$$\boldsymbol{rs\ -\ r\ +\ 1} = 239 * 678 - 239 + 1 = 161804$$

$$\boldsymbol{rs\ -\ r\ +\ 2s - 1} = 239 * 678 - 239 + 2 * 678 - 1 = 163158$$

$$\boldsymbol{rs + s\ +\ 1} = 239 * 678 + 678 + 1 = 162721$$

Luego:

$$f_1 = (\boldsymbol{rs\ -\ r\ +\ 1})^2 \bullet \boldsymbol{x^2} - (\boldsymbol{rs - r + 1})(\boldsymbol{rs - r + 2s - 1}) \bullet \boldsymbol{x} + \boldsymbol{p} \bullet (\boldsymbol{rs\ -\ r\ +\ 1})^2 + (\boldsymbol{rs + s} + \boldsymbol{1})(\boldsymbol{s - 2}) + \boldsymbol{r} + \boldsymbol{2})$$

$$f_1 = 161804^2 * 100^2 - 161804 * 163158 * 100 + 41 * 161804^2 + 162721 * 676 + 241 = 260238894367493$$

$$\beta = \boldsymbol{r}(\boldsymbol{rs - r + 1}) \bullet \boldsymbol{x^2} - (\boldsymbol{r}(\boldsymbol{r + 2})(\boldsymbol{s - 2}) + \boldsymbol{r^2} + \boldsymbol{3r} + \boldsymbol{1})\boldsymbol{x} + \boldsymbol{pr}(\boldsymbol{rs - r + 1}) + (\boldsymbol{r} + \boldsymbol{1})(\boldsymbol{s - 1})$$

$$\beta = 239 * 161804 * 100^2 - (239 * 241 * 676 + 239^2 + 3 * 239 + 1) * 100 + 41 * 239 * 161804 + 240 * 677 = 384397763576$$

$$n = f_1 * (k - 1) + \beta$$

$$n = 260238894367493 * 450 + 384397763576 = 117107886863135426$$

$$f_2 = \boldsymbol{f_1} * (k-1)^2 + (2\beta+1)(k-1) + \boldsymbol{r^2x^2} - \boldsymbol{r(r+2)x} + \boldsymbol{pr^2} + \boldsymbol{r} + \boldsymbol{1}$$

$$f_2 = 260238894367493 * 450^2 + (2 * 384397763576 + 1) * 450 + 239^2 * 100^2 - 239 * 241 * 100 + 41 * 239^2 + 239 + 1 = 52698722067972343651$$

Por el Primer Teorema de la Factorización de Cordero en los enteros,

$$117107886863135426^2 + 117107886863135426 + 41 = 260238894367493 * 52698722067972343651$$

Factorizado en sus factores primos es:

$$117107886863135426^2 + 117107886863135426 + 41 = 4943 * 150401 * 16\,419517 * 649\,305521 * 1730\,300293$$

Aunque el Teorema no logra la factorización completa, es muy útil porque logra factorizar el número en dos factores utilizando fórmulas matemáticas y sin necesidad de recurrir a test de primalidad, calculadoras factorizadoras de números, divisiones sucesivas o software.

Obsérvese que a pesar de que:

117107886863135426 2 + 117107886863135426 + 41 = 13714257165548927003249522479336943 es un número grande (36 dígitos) su factorización prima tiene solamente 5 factores,

Aplicación 2.

Sea $r = 139,\ s = 1608, x = -15\ ,\ k = -451\ y\ p = 11$ tenemos que:

$$\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{1} = 139 * 1608 - 139 + 1 = 223374$$

$$\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{2s} - \boldsymbol{1} = 139 * 1608 - 139 + 2 * 1608 - 1 = 226588$$

$$\boldsymbol{rs} + \boldsymbol{s} + \boldsymbol{1} = 139 * 1608 + 1608 + 1 = 225121$$

Luego:

$$f_1 = (\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{1})^2 \bullet \boldsymbol{x^2} - (\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{1})(\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{2s} - \boldsymbol{1}) \bullet \boldsymbol{x} + \boldsymbol{p} \bullet (\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{1})^2 + (\boldsymbol{rs} + \boldsymbol{s} + \boldsymbol{1})(\boldsymbol{s} - \boldsymbol{2}) + \boldsymbol{r} + \boldsymbol{2})$$

$$f_1 = 223374^2 * (-15)^2 - 223374 * 226588 * (-15) + 11 * 223374^2 + 225121 * 1606 + 141 = 12535012317883$$

$$\beta = \boldsymbol{r}(\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{1}) \bullet \boldsymbol{x^2} - (\boldsymbol{r}(\boldsymbol{r} + \boldsymbol{2})(\boldsymbol{s} - \boldsymbol{2}) + \boldsymbol{r^2} + \boldsymbol{3r} + \boldsymbol{1})\boldsymbol{x} + \boldsymbol{pr}(\boldsymbol{rs} - \boldsymbol{r} + \boldsymbol{1}) + (\boldsymbol{r} + \boldsymbol{1})(\boldsymbol{s} - \boldsymbol{1})$$

$$\beta = 139 * 223374 * (-15)^2 - (139 * 141 * 1606 + 139^2 + 3 * 139 + 1) * (-15) + 11 * 139 * 223374 + 140 * 1607 = 7800221671$$

$$n = f_1 * (k+1) - (\beta+1)$$

$$n = 12535012317883 * (-450) - 7800221672 = -5640763343269022$$

$$f_2 = \boldsymbol{f_1} * (k+1)^2 - (2\beta+1)(k+1) + \boldsymbol{r^2x^2} - \boldsymbol{r}(\boldsymbol{r}+\boldsymbol{2})\boldsymbol{x} + \boldsymbol{pr^2} + \boldsymbol{r} + \boldsymbol{1}$$

$$f_2 = 12535012317883 * (-450)^2 - (2 * 7800221671 + 1) * (-450) + 139^2 * (-15)^2 - 139 * 141 * (-15) + 11 * 139^2 + 139 + 1 = 2538347014575665731$$

Por el Primer Teorema de la Factorización de Cordero en los enteros,

$$(-5640763343269022)^2 + -5640763343269022 + 11 = 12535012317883 * 2538347014575665731$$

Factorizado en sus factores primos es:

$$(-5640763343269022)^2 + -5640763343269022 + 11 = 11\text{^}2 * 797 * 129\,981359 * 245\,154001 * 10354\,091731$$

Su factorización completa tiene 6 factores que son pocos, tomando en cuenta que el número a factorizar es grande. Utilizando calculadoras factorizadoras de números enteros, como la de Dario Alpern (véase, 4. Factorization using the Elliptic Curve Method) de https://www.alpertron.com.ar/ECM.HTM. Podemos factorizar números muy grandes con factores que sobrepasan los 100 dígitos, véase www.REVISTAELLABRADOR. Primer Teorema de La Factorización de Cordero en los números enteros.

8.2 Segundo Teorema de la factorización de Cordero en Z

Este teorema es la culminación de un resultado matemático (El teorema de la multiplicación de Cordero en Z), publicado por Ronald Cordero Méndez en: Memorias de Fimat 2020, que lo puede encontrar en: libro_memorias_fimat_concites_2020_c.pdf, página 104.

Sea $s, x, T \in \boldsymbol{Z}, s \neq 0,\ \ p \in \{2, 3, 5, 11, 17, 41\}$

1) Si $n = (s^2x^2 + s(s-2)x + ps^2 - s + 1) * T + sx^2 + (s-1)x + ps - 1$ entonces $n^2 + n + p$ es compuesto y dos de sus factores tienen la forma:

$$f_1 = s^2x^2 + s(s-2)x + ps^2 - s + 1$$

$$f_2 = \frac{n^2+n+p}{f_1} = f_1T^2 + (2\beta+1)T + x^2 + x + p \quad \text{con } \beta = sx^2 + (s-1)x + sp - 1$$

2) Si $n = (s^2x^2 + s(s-2)x + ps^2 - s + 1) * T - (sx^2 + (s-1)x + ps)$ entonces $n^2 + n + p$ es compuesto y dos de sus factores tienen la forma:

$$f_1 = s^2x^2 + s(s-2)x + ps^2 - s + 1$$

$$f_2 = \frac{n^2+n+p}{f_1} = f_1T^2 - (2\beta+1)T + x^2 + x + p \quad \text{con } \beta = sx^2 + (s-1)x + sp - 1$$

Este Teorema al igual que el primer teorema, su objetivo es encontrar una factorización en dos factores de números de la forma $n^2 + n + p$ con $p \in \{2, 3,5,11,17,41\}$.

8.2.1 Aplicaciones del Segundo Teorema de la Factorización de Cordero en los números enteros.

Aplicación 1

Sea $s = 678, x = -80,\ T = 12\ \ y\ p = 41$ tenemos que:

$$f_1 = s^2x^2 + s(s-2)x + ps^2 - s + 1$$

$$f_1 = 678^2(-80)^2 + 678 * 676 * (-80) + 41 * (678)^2 - 678 + 1$$

$$f_1 = 2924157727$$

$$\beta = sx^2 + (s-1)x + sp - 1$$

$$\beta = 678 * (-80)^2 + 677 * (-80) + 678 * 41 - 1 = 4312837$$

Calculemos los dos valores para

$$n_1 = (s^2x^2 + s(s-2)x + ps^2 - s + 1) * T + sx^2 + (s-1)x + ps - 1$$

$$n_1 = 2924157727 * 12 + 4312837 = 35094205561$$

$$n_2 = (s^2x^2 + s(s-2)x + ps^2 - s + 1) * T - (sx^2 + (s-1)x + ps)$$

$$n_2 = 2924157727 * 12 - 4312838 = 35085579886$$

Luego:

Primer caso:

$$f_2 = f_1T^2 + (2\beta + 1)T + \boldsymbol{x^2} + \boldsymbol{x} + \boldsymbol{p}$$

$$f_2 = 2924157727 * 12^2 + (2 * 4312837 + 1) * 12 + (-80)^2 - 80 + 41$$
$$= 421182\ 227149$$

Así:

$$(n_1)^2 + n_1 + p = f_1 * f_2$$

$$(35094205561)^2 + 35094205561 + 41 = 2924157727 * 421182227149$$

Su factorización completa es:

$$(35094205561)^2 + 35094205561 + 41 = 563\ *\ 748\ 103423\ *\ 2924\ 157727$$

Segundo caso:

$$f_2 = f_1T^2 - (2\beta + 1)T + x^2 + x + p$$

$$f_2 = 2924157727 * 12^2 - (2 * 4312837 + 1) * 12 + (-80)^2 - 80 + 41$$
$$=\ 420975\ 210949$$

Así;

$$(n_2)^2 + n_2 + p = f_1 * f_2$$

$$(35085579886)^2 + 35085579886 + 41 = 2924157727 * 420975210949$$

Y esta es su factorización completa, o sea es un biprimo.

8.3 Tercer Teorema de la factorización de Cordero en Z

Este teorema se utiliza en la factorización de los números de la forma $4n^2 + 4p - 1$ con p ∈ {2,3,5,11,17,41}. Al igual que el primer y segundo teoremas de la factorización de Cordero en el conjunto de los números enteros, su factorización es de dos factores, y estos pueden ser compuestos, uno primo y el otro compuesto o los dos factores pueden dar números primos.

Sea $s, x, T \in \boldsymbol{Z}, s \neq 0,\ p \in \{2,3,5,11,17,41\}$

1) Si $n = \frac{x^2 - x + p - 1}{2}$ entonces $4n^2 + 4p - 1$ es un número compuesto y dos de sus factores tienen la forma:

$$f_1 = x^2 - 3x + p + 2 \quad y \quad f_2 = x^2 + x + p$$

2) Si $n = [s^2x^2 + s(s-2)x + ps^2 - s + 1] * T \pm \left[\frac{s(3s-2)x^2 + (3s^2 - 8s + 2)x + ps(3s-2) - 3s + 4}{2}\right]$ entonces $4n^2 + 4p - 1$ es un número compuesto y dos de sus factores tienen la forma:

$$f_1 = s^2x^2 + s(s-2)x + ps^2 - s + 1 \quad y$$

$$f_2 = 4f_1T^2 \pm 8T\beta + (3s-2)^2x^2 + (3s-2)(3s-8)x + \frac{(3s^2 - 8s + 2)^2 + (3s-2)[3s^3(p-1) - s^2(2p-11) - 13s + 2]}{s^2}$$

Donde $\beta = \left[\frac{s(3s-2)x^2 + (3s^2 - 8s + 2)x + ps(3s-2) - 3s + 4}{2}\right]$

8.3.1 Aplicaciones del Tercer Teorema de la Factorización de Cordero en el Conjunto de los números enteros.

Aplicación 1

Sea $x = 90.\ p = 17,\ \ n = \frac{x^2 - x + p - 1}{2} = \frac{90^2 - 90 + 17 - 1}{2} = 4013$

$$f_1 = x^2 - 3x + p + 2 = 90^2 - 3 * 90 + 17 + 2 = 7849$$

$$f_2 = x^2 + x + p = 90^2 + 90 + 17 = 8207$$

Luego: $4n^2 + 67 = 4 * 4013^2 + 67 = 7849 * 8207$

Aplicación 2

Sea $s = 54, x = -24, p = 11,\ T = 13$

$$f_1 = s^2x^2 + s(s-2)x + ps^2 - s + 1$$
$$= 2916 * 576 + 54 * 52 * (-24) + 11 * 2916 - 54 + 1 = 1644247$$

$$\beta = \frac{s(3s-2)x^2 + (3s^2 - 8s + 2)x + ps(3s-2) - 3s + 4}{2}$$
$$= \frac{54 * 160 * 576 + 8318 * (-24) + 11 * 54 * 160 - 162 + 4}{2}$$
$$= 2435945$$

$$f_2$$
$$= 4f_1T^2 \pm 8T\beta + (3s-2)^2x^2 + (3s-2)(3s-8)x$$
$$+ \frac{(3s^2 - 8s + 2)^2 + (3s-2)[3s^3(p-1) - s^2(2p-11) - 13s + 2]}{s^2}$$
$$= 4 * 1644247 * 169 \pm 8 * 13 * 2435945 + 160^2 * 576 + 160 * 154 * (-24)$$
$$+ \frac{69189124 + 160 * (472392 * 10 - 2916 * 11 - 13 * 54 + 2)}{2916}$$

$$f_2 = 4 * 1644247 * 169 + 8 * 13 * 2435945 + 160^2 * 576 + 160 * 154 * (-24) + 281129$$

$$f_2 = 1379284621$$

ó

$$f_2 = 4 * 1644247 * 169 - 8 * 13 * 2435945 + 160^2 * 576 + 160 * 154 * (-24) + 2811 = 872608061$$

Luego:

$$n = [s^2x^2 + s(s-2)x + ps^2 - s + 1] * T$$
$$\pm \left[\frac{s(3s-2)x^2 + (3s^2 - 8s + 2)x + ps(3s-2) - 3s + 4}{2}\right]$$

$$n = 1644247 * 13 + 2435945 = 23811156$$

ó

$$n = 1644247 * 13 + 2435945 = 23811156$$

Así:

$$4n^2 + 4p - 1$$

$$4 * 23811156^2 + 43 = 1644247 * 1379284621$$

ó

$$4 * 18939266^2 + 43 = 1644247 * 872608061$$

8.4 Cuarto Teorema de la factorización de Cordero en Z

Factorizar números enteros en sus factores primos utilizando fórmulas matemáticas no ha sido posible hasta el momento. Las fórmulas aquí publicadas permiten factorizar en dos factores algunos números enteros que tienen forma polinomial. El Cuarto Teorema de la Factorización de Cordero al igual que los anteriores permite factorizar en dos factores que pueden ser: primos los dos factores, uno primo y el otro compuesto o los dos compuestos.

Sea $s, x, T \in \mathbb{Z}, s \neq 0 \;\; y \; p \in \{3,5,11,29\}$

1) Si $n = (4s^2x^2 + 4sx + 2ps^2 + 1) * T \pm (2sx^2 + x + sp)$

entonces: $2n^2 + p$ es compuesto y dos de sus factores tienen la forma:

$$f_1 = 4s^2x^2 + 4sx + 2ps^2 + 1$$

$$f_2 = \frac{2n^2+p}{f_1} = 2f_1T^2 \pm 4\beta T + 2x^2 + p$$

Con $\beta = 2sx^2 + x + sp$

2) Si $n = (2x^2 + p) * T \pm (2sx^2 + x + sp)$

entonces: $2n^2 + p$ es compuesto y dos de sus factores tienen la forma:

$$f_1 = 2x^2 + p$$

$$f_2 = \frac{2n^2+p}{f_1} = 2f_1T^2 \pm 4\beta T + 2f_1s^2 + 4sx + 1$$

Con $\beta = 2sx^2 + x + sp$

8.4.1 Aplicaciones del Cuarto Teorema de la Factorización de Cordero en los números enteros.

Aplicación 1.

Sea $s = 48, x = 23, p = 29, T = 12$

$$f_1 = 4s^2x^2 - 4sx + 2ps^2 + 1$$

$$f_1 = 4 * (48)^2(23)^2 - 4 * 48 * 23 + 2 * 29 * 48^2 + 1 = 5004481$$

$$n = (4s^2x^2 - 4sx + 2ps^2 + 1) * T \pm (2sx^2 - x + sp)$$

$$n = 5004481 * 12 + (2 * 48 * 23^2 - 23 + 48 * 29) = 60105925$$

Ó

$$n = 5004481 * 12 - (2 * 48 * 23^2 - 23 + 48 * 29) = 60001619$$

$$f_2 = \frac{2n^2+p}{f_1} = 2f_1T^2 \pm 4\beta T + 2x^2 + p$$

$$f_2 = 2 * 5004481 * 144 + 4 * 52153 * 12 + 2 * 23^2 + 29 = 1443794959$$

Ó

$$f_2 = 2 * 5004481 * 144 - 4 * 52153 * 12 + 2 * 23^2 + 29 = 1438788271$$

Luego:

$$2 * 60105925^2 + 29 = 5004481 * 1443794959$$

Ó

$$2 * 60001619^2 + 29 = 5004481 * 1438788271$$

Aplicación 2.

Sea $s = 8, x = 5, p = 29, T = 11$

$$f_1 = 2x^2 + p = 2 * 25 + 29 = 79$$

$$\beta = 2sx^2 + x + sp = 2 * 8 * 25 + 5 + 8 * 29 = 637$$

$$n = (2x^2 + p) * T + (2sx^2 + x + sp) = 79 * 11 + 637 = 1506$$

ó

$$n = (2x^2 + p) * T - (2sx^2 + x + sp) = 79 * 11 - 637 = 232$$

Luego:

$$f_2 = 2f_1T^2 + 4\beta T + 2f_1s^2 + 4sx + 1 =$$

$$2 * 79 * 121 + 4 * 637 * 11 + 2 * 79 * 64 + 4 * 8 * 5 + 1 = 57419$$

$$f_2 = 2f_1T^2 - 4\beta T + 2f_1s^2 + 4sx + 1 =$$

$$2 * 79 * 121 - 4 * 637 * 11 + 2 * 79 * 64 + 4 * 8 * 5 + 1 = 1363$$

Tenemos:

$$2 * 1506^2 + 29 = 79 * 57419$$

$$2 * 232^2 + 29 = 79 * 136$$

8.5 Quinto Teorema de la Factorización de Cordero en Z

Sea $s, x, T, r \in \mathbb{Z},\ s, r \neq 0\ y\ p \in \{2, 3, 5, 11, 17, 41\}$

Si $n = (s^2x^2 + sx + p)(r * T + 1) - r(sx + 1) + 1$ entonces

$n^2 + (r - 2)n + pr^2 - r + 1$ es un número compuesto y dos de sus factores tienen la forma:

$$f_1 = s^2x^2 + sx + p$$

$$f_2 = f_1(r * T + 1)^2 - r(2sx + 1)(r * T + 1) + r^2$$

8.5.1 Aplicaciones del Quinto Teorema de la Factorización de Cordero en el Conjunto de los números enteros.

Aplicación 1

Sea $s = -8, \quad r = 11, \; x = 6, \; T = -4, \; p = 41$

$$p(n) = n^2 + 9n + 4951$$

$$n = (64 * 36 - 8 * 6 + 41) * (-43) - 11 * (-8 * 6 + 1) + 1$$

$$n = 2297 * (-43) + 11 * 47 + 1$$

Donde:

$$f_1 = 2297 \quad y \quad n = -98253$$

$$f_2 = 2297 * (-43)^2 - 11 * 43 * 95 + 121 = 4202339$$

Entonces:

$$(-98253)^2 + 9 * (-98253) + 4951 = 9652772683 = 2297 * 4202339$$

Y ambos factores son números primos.

REFERENCIAS

Aznar, E. (2007). *Leonhard Euler Matemático (1707 Basilea. Suiza, 1783 San Petesburgo, Rusia*). https://www.ugr.es/eaznar/euler.htm

Camacho, J. y Camacho, O. (2020). *Dos Científicos Bajo Un Fresno: Un Viaje A La Ciencia. En Doce Escritos.* Google Books.

Fernández, T. y Tamaro, E. (2004). *Adrien-Marie Legendre.* https://www.biografíasyvidas.com/biografía/l/legendre.htm

Frases y pensamientos. (s.f.). *Frases de números primos*. https://www.frasesypensamientos.com.ar/frases-de-numeros-primos.html

Ayoub, R. and Chowla, S., *On Euler's polynomial.* J. Nb. Th., 13, 1981.

Borevish, Z. I. and Shafarevich, I. R. , *Number Theory.* Academic press, New York, 1966.

Cohn, H., *Advanced Number Theory.* Dover Publ., New York, 1962.

Goldfeld, D., *Gauss' class number problem for imaginary quadratic fields.* Bull. Amer. Math. Soc., 13, 1985.

Lehmer, D.H., *On the function* . Sphinx 6, 1936.

Paulo Ribenboim. *Revista Colombiana de matemáticas. Vol. XXI (1987).* Queen University. Kingston, Ontario, Canadá.

R. Balister, B. Bollobás, R. Morris, *The sharp threshold for making squares*, Ann. Math. **188** (2018) 49-143.

C. Pomerance, *A Tale of Two Sieves,* Notices Amer. Math. Soc. **43** nº 12 (1996) 1473-1485.

Memorias de FIMAT. 2020. XII Festival Internacional de Matemáticas - XXII Congreso Nacional de Ciencias, Tecnología y Sociedad. Pàgs. 104-106

Biografìas y Vidas.com