CAPÍTULO 15

FACTORIZACIÓN DE NÚMEROS ENTEROS POLINOMIALES Y SUS ALGORITMOS

https://doi.org/10.22533/at.ed.5791125280215

Data de aceite: 22/12/2025

Ronald Cordero Méndez

RESUMEN: El método de factorización de Cordero se basa en un conjunto de teoremas y algoritmos que permiten la factorización de números enteros polinomiales, es decir, números enteros que pueden expresarse a través de fórmulas polinomiales específicas. A diferencia de los métodos tradicionales de factorización de números enteros que intentan descomponer cualquier número, este trabajo de investigación se centra en formas particulares de números enteros. El método proporciona fórmulas para descomponer ciertos números polinomiales en dos factores y que son la base matemática de los algoritmos, los cuales logra factorizar en forma completa estos dos números enteros obtenidos a través de las fórmulas.

PALABRAS CLAVES: Factorización, Números enteros, Algoritmos, Programas computacionales, Software, Teorema.

FACTORIZATION OF ENTERAL POLYNOMIAL NUMBERS AND THEIR ALGORITHMS

ABSTRACT: The Cordero factorization method is based on a set of theorems and algorithms that allow the factorization of polynomial integers, that is, integers that can be expressed through specific polynomial formulas. Unlike traditional integer factorization methods that attempt to decompose any number, this research focuses on particular forms of integers. The method provides formulas for decomposing certain polynomial numbers into two factors, which are the mathematical basis of the algorithms that completely factor these two integers obtained through the formulas.

KEYWORDS.: Factorization, Integers, Algorithms, Computer programs, Software, Theorem.

INTRODUCCIÓN

El método que aquí se plantea no es de propósito general para factorizar cualquier número entero, como lo es la Criba Cuadrática o la Criba del Cuerpo de Números. En su lugar, está diseñado para

trabajar con números que siguen ciertos patrones algebraicos específicos, como los son los números polinomiales de la forma $n^2 - nr + pr^2$, $2n^2 + pr^2$ o $n^2 + 2pr^2$.; El método de Cordero es una aproximación especializada a la factorización de números enteros, se limitada a números que se ajustan a fórmulas polinomiales específicas, y no a un método universal para todos los números enteros.

Tenemos claro que actualmente el principal reto en la factorización de los números enteros es la complejidad computacional que aumenta exponencialmente con el tamaño del número entero. A diferencia de la multiplicación, que es un problema relativamente sencillo y rápido de resolver, no se conoce un algoritmo eficiente para la factorización de números enteros grandes o muy grandes.

Los algoritmos actuales para números grandes, como la Criba del Cuerpo de Números (NFS), son muy lentos y requieren una enorme cantidad de recursos computacionales. Factores de cientos de dígitos pueden tardar años en ser resueltos incluso con la colaboración de miles de computadoras. Por ejemplo, el número RSA-250 (un número de 250 dígitos) fue factorizado en 2020 después de una gran cantidad de tiempo y esfuerzo. Este problema de la factorización hasta el momento no se ha clasificado formalmente en una clase de complejidad computacional simple (como P o NP). Se sabe que está en la clase NP y Co-NP, pero no se ha demostrado si pertenece a P o si es un problema NP-completo, lo que refleja su complejidad fundamental.

El mayor desafío a futuro es el algoritmo de Shor. Este algoritmo, diseñado para computadoras cuánticas, podría factorizar números enteros en un tiempo polinomial, lo que significaría que los números grandes se podrían factorizar de manera casi instantánea. Esto pondría en riesgo la seguridad de la criptografía actual. Aunque las computadoras cuánticas actuales aún no son lo suficientemente potentes para ejecutar el algoritmo de Shor a gran escala, su desarrollo representa un desafío teórico y práctico enorme para la criptografía moderna. Los avances más recientes en la factorización de números enteros se han centrado principalmente en la optimización de los algoritmos existentes para la computación clásica y en la investigación de nuevos enfoques teóricos. Esto se debe a la importancia de la factorización en la seguridad de la criptografía de clave pública, como el algoritmo RSA.

Los avances más notables en los últimos años han sido la factorización exitosa de números RSA de gran tamaño. Los esfuerzos se han concentrado en perfeccionar algoritmos como la NFS. Se han desarrollado variaciones, como el algoritmo GNFS-FFT, que buscan reducir el tiempo de ejecución y los recursos necesarios para la factorización. También han surgido investigaciones que reformulan el problema de la factorización desde diferentes ángulos matemáticos. Un ejemplo reciente es un enfoque que equipara la factorización con el problema de encontrar el perímetro de un rectángulo de área conocida, o con el cálculo de ciertas integrales.

Los teoremas y algoritmos de Cordero están diseñados para factorizar números polinomiales de formas particulares, como números de la forma: $n^2-nr+pr^2$, $2n^2+pr^2$ o n^2+2pr^2 donde p son números primos como $2, 3, 5, 11, 17, 29$ y 41 según el número polinomial con el que se esté trabajando, son números enteros con cierta estructura. Para estos números, sus métodos ofrecen un camino más directo que los algoritmos de propósito general. Esto es particularmente relevante en la teoría de números, donde el estudio de familias específicas de números pueden revelar propiedades y patrones importantes. La capacidad de factorizar números de estas formas de manera eficiente podría contribuir al conocimiento en este campo.

La factorización de números enteros grandes es la base de la seguridad de muchos sistemas criptográficos, como el algoritmo RSA. La dificultad de este problema es lo que los hace seguros. La propuesta de Cordero podría tener un impacto potencial en este campo, ya que, si sus algoritmos demuestran ser eficientes para factorizar un subconjunto de números enteros que se usan en criptografía, podría tener implicaciones para la seguridad de estos sistemas. Los teoremas y algoritmos de Cordero, junto con los programas computacionales que se han desarrollado para verificarlos, sirven como material de apoyo para la creación de software de factorización. Esto podría ayudar a construir herramientas más especializadas y eficientes para el cálculo de números primos muy grandes y la factorización de números enteros que cumplan con las condiciones de sus teoremas.

A diferencia de los métodos tradicionales de fuerza bruta o de criba, los trabajos de Cordero abordan la factorización desde una perspectiva diferente, utilizando propiedades polinomiales. Esta investigación fomenta el estudio de nuevos enfoques para resolver el problema de la factorización de números enteros, un problema para el cual no se tiene una solución eficiente y universalmente aplicable. Esto puede inspirar a otros investigadores a explorar caminos alternativos que, con el tiempo, podrían llevar a avances significativos en el campo.

FACTORIZACIÓN DE NÚMEROS POLINOMIALES DE LA FORMA:

$n^2-nr+pr^2$.

Consideremos números polinomiales que tienen la estructura $NP=n^2-nr+pr^2$ donde r es un número entero diferente de cero, p es un número afortunado de Euler, o sea $p\epsilon\{2, 3, 5, 11, 17, 41\}$ y n es un número entero. Si dados cuatro números enteros t_1, t_2, b_1, b_2, si se tiene que $n=p*b_1*b_2-t_1*t_2$ y $r=b_1*b_2-t_1*b_2-t_2*b_1$ entonces el NP es compuesto y dos de sus factores tienen la forma $t_1^2-t_1*b_1+pb_1^2$ y $t_2^2-t_2*b_2+pb_2^2$. Todo lo anterior se puede describir en el siguiente teorema.

Teorema polinomial de Cordero (1).

Sea $t_1,\ t_2,\ b_1,\ b_2\ \epsilon\ Z, b_1 \neq 0,\ b_2 \neq 0,\quad p \epsilon \{2,\ 3,\ 5,\ 11,\ 17,\ 41\}$.

Si $n = p*b_1*b_2 - t_1*t_2$ y $r = b_1*b_2 - t_1*b_2 - t_2*b_1 \neq 0$ entonces $NP = n^2 - nr + pr^2$ es compuesto y se factoriza como $NP = \left(t_1^{\,2} - t_1*b_1 + pb_1^{\,2}\right)\left(t_2^{\,2} - t_2*b_2 + pb_2^{\,2}\right)$.

Demostración.

Sea $NP = n^2 - nr + pr^2$, consideremos a $n = p*b_1*b_2 - t_1*t_2$ y $r = b_1*b_2 - t_1*b_2 - t_2*b_1 \neq 0$, $p \epsilon \{2,\ 3,\ 5,\ 11,\ 17,\ 41\}$.

Tenemos que:

$$NP = n^2 - nr + pr^2$$

$$NP = \left(p*b_1*b_2 - t_1*t_2\right)^2 - \left(p*b_1*b_2 - t_1*t_2\right)*\left(b_1*b_2 - t_1*b_2 - t_2*b_1\right) + p\left(b_1*b_2 - t_1*b_2 - t_2*b_1\right)^2$$

$$NP = p^2 b_1^{\,2} b_2^{\,2} - 2pb_1b_2t_1t_2 + t_1^{\,2}t_2^{\,2} - \left(b_1*b_2 - t_1*b_2 - t_2*b_1\right)*\left(p*b_1*b_2 - t_1*t_2 - pb_1*b_2 + pt_1*b_2 + pt_2*b_1\right)$$

$$NP = p^2 b_1^{\,2} b_2^{\,2} - 2pb_1b_2t_1t_2 + t_1^{\,2}t_2^{\,2} - \left(b_1*b_2 - t_1*b_2 - t_2*b_1\right)*\left(-t_1*t_2 + pt_1*b_2 + pt_2*b_1\right)$$

$$NP = p^2 b_1^{\,2} b_2^{\,2} - 2pb_1b_2t_1t_2 + t_1^{\,2}t_2^{\,2} + \left(b_1*b_2 - t_1*b_2 - t_2*b_1\right)*\left(t_1*t_2 - pt_1*b_2 - pt_2*b_1\right)$$

$$NP = p^2 b_1^{\,2} b_2^{\,2} - 2pb_1b_2t_1t_2 + t_1^{\,2}t_2^{\,2} + b_1b_2t_1t_2 - pt_1b_1b_2^{\,2} - pt_2b_2b_1^{\,2} - t_2b_2t_1^{\,2} + pt_1^{\,2}b_2^{\,2} + pt_1t_2b_1b_2 - b_1t_1t_2^{\,2} + pt_2b_1t_1b_2 + pb_1^{\,2}t_2^{\,2}$$

$$NP = p^2 b_1^{\,2} b_2^{\,2} + t_1^{\,2}t_2^{\,2} + b_1b_2t_1t_2 - pt_1b_1b_2^{\,2} - pt_2b_2b_1^{\,2} - t_2b_2t_1^{\,2} + pt_1^{\,2}b_2^{\,2} - b_1t_1t_2^{\,2} + pb_1^{\,2}t_2^{\,2}$$

$$NP = t_1^{\,2}t_2^{\,2} - t_2b_2t_1^{\,2} + pt_1^{\,2}b_2^{\,2} - b_1t_1t_2^{\,2} + b_1b_2t_1t_2 - pt_1b_1b_2^{\,2} + pb_1^{\,2}t_2^{\,2} - pt_2b_2b_1^{\,2} + p^2b_1^{\,2}b_2^{\,2}\ (*)$$

Por otro lado, tenemos:

$$\left(t_1^{\,2} - t_1b_1 + pb_1^{\,2}\right)\left(t_2^{\,2} - t_2b_2 + pb_2^{\,2}\right) = t_1^{\,2}t_2^{\,2} - t_1^{\,2}t_2b_2 + pb_2^{\,2}t_1^{\,2} - t_1b_1t_2^{\,2} + t_1b_1t_2b_2 - pb_2^{\,2}t_1b_1 + pb_1^{\,2}t_2^{\,2} - pb_1^{\,2}t_2b_2 + p^2b_1^{\,2}b_2^{\,2}\ (**)$$

De $(*)$ y $(**)$ obtenemos:

$$NP = n^2 - nr + pr^2 = \left(t_1^2 - t_1 b_1 + p b_1^2\right)\left(t_2^2 - t_2 b_2 + p b_2^2\right)$$

Queda demostrado el Teorema.

Algoritmo para factorizar completamente $\left(t_1^2 - t_1 b_1 + p b_1^2\right)\left(t_2^2 - t_2 b_2 + p b_2^2\right)$

El algoritmo $f(x) = \sqrt{(1-4p)x^2 + 2*(2t_1 - b_1)x + b_1^2}$, $x \epsilon Z$, $x \neq 0$ nos determina si el factor de NP $t_1^2 - t_1 * b_1 + p b_1^2$ (t_1 y b_1 *primos entre sí*) es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto. En caso de que t_1 y b_1 tengan divisores comunes, estos son factores de $t_1^2 - t_1 b_1 + p b_1^2$.

Sea el factor de NP, $t_1^2 - t_1 * b_1 + p b_1^2$ (t_1 y b_1 *primos entre sí*). Si existe al menos un $x \epsilon Z$, $x \neq 0$ tal que $f(x) = v$, entonces $t_1^2 - t_1 * b_1 + p b_1^2$ es un número compuesto, caso contrario, el número $t_1^2 - t_1 * b_1 + p b_1^2$ es primo.

En caso de que $t_1^2 - t_1 * b_1 + p b_1^2$ sea compuesto, entonces existe al menos un punto entero (x, v).

Luego $\frac{t}{b} = \frac{-b_1 + x \pm v}{2x}$ con $\frac{t}{b}$ fracción canónica, entonces $t^2 - tb + pb^2$ es un factor de $t_1^2 - t_1 * b_1 + p b_1^2$

El algoritmo $g(x) = \sqrt{(1-4p)x^2 + 2*(2t_2 - b_2)x + b_2^2}$ nos determina si el factor de NP $t_2^2 - t_2 * b_2 + p b_2^2$ (t_2 y b_2 *primos entre sí*) es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto. En caso de que t_2 y b_2 tengan divisores comunes, estos son factores de t_2 y b_2

Sea el factor de NP, $t_2^2 - t_2 * b_2 + p b_2^2$ (t_2 y b_2 *primos entre sí*). Si existe algún $x \epsilon Z$, $x \neq 0$ tal que $f(x) = v$, entonces $t_2^2 - t_2 * b_2 + p b_2^2$ es un número compuesto, caso contrario, el número $t_2^2 - t_2 * b_2 + p b_2^2$ es primo.

En caso de que $t_2^2 - t_2 * b_2 + p b_2^2$ sea compuesto, entonces existe el punto entero (x, v).

Luego $\frac{t}{b} = \frac{-b_1 + x \pm v}{2x}$ con $\frac{t}{b}$ fracción canónica, entonces $t^2 - tb + pb^2$ es un factor de $t_2^2 - t_2 * b_2 + p b_2^2$

➢Ejemplo de aplicación 1.

Sea $t_1 = 11$, $t_2 = 13$, $b_1 = -17$, $b_2 = 23$ y $p = 41$

$n = p * b_1 * b_2 - t_1 * t_2$

$$n = 41*(-17)*23 - 11*13 = -16174$$

$$r = b_1*b_2 - t_1*b_2 - t_2*b_1 = (-17)*23 - 11*23 - 13*(-17) = -423$$

El número polinomial que vamos a factorizar es:

$$NP = n^2 - n + pr^2 = (-16174)^2 - (-16174)*-423 + 41*(-423)^2 = 262092763$$

Por el teorema anterior podemos factorizar el número polinomial en los factores:

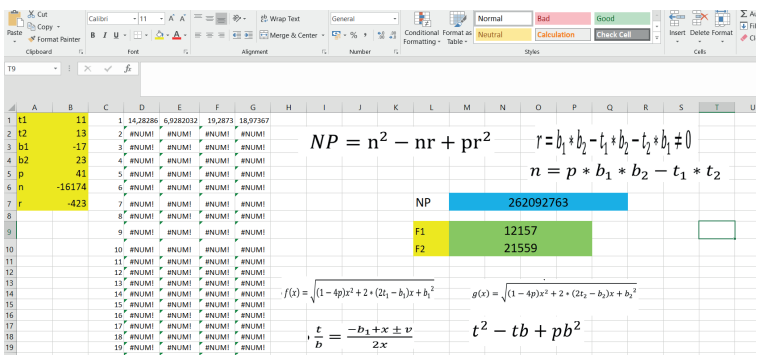
$$t_1^2 - t_1*b_1 + pb_1^2 = 11^2 - 11*(-17) + 41*(-17)^2 = 12157$$

$$t_2^2 - t_2*b_2 + pb_2^2 = 13^2 - 13*23 + 41*23^2 = 21559$$

Para encontrar la primalidad de los factores 12157 y 21559 o su factorización completa en caso de que sean compuestos debemos utilizar $g(x) = \sqrt{(1-4p)x^2 + 2*(2t_2 - b_2)x + b_2^2} = \sqrt{-163x^2 + 6x + 529}$

Y $g(x) = \sqrt{(1-4p)x^2 + 2*(2t_2 - b_2)x + b_2^2} = \sqrt{-163x^2 + 6x + 529}$

Utilizando Excel encontramos que: 21559



No hay pares ordenados donde la preimagen y la imagen sean cantidades enteras, o sea no hay puntos enteros. Obsérvese que los cálculos son muy pocos, para concluir que los números enteros 12157 y 21559 son ambos números primos.

Concluimos que la factorización completa de $262092763 = 12157*21559$

➢ Ejemplo de aplicación 2.

Sea $t_1 = 83,\ t_2 = 167,\ b_1 = 82\ ,\ b_2 = 105\ \ y\ \ p = 41$

$$n = p * b_1 * b_2 - t_1 * t_2$$

$$n = 41 * 82 * 105 - 83 * 167 = 339149$$

$$r = b_1 * b_2 - t_1 * b_2 - t_2 * b_1 = 82 * 105 - 83 * 105 - 167 * 82 = -13799$$

El número polinomial que vamos a factorizar es:

$$NP = n^2 - nr + p r^2 = (339149)^2 - (-13799) * 339149 + 41 * (-13799)^2 = 127508\ 869693$$

Por el teorema anterior podemos factorizar el número polinomial $127508\ 869693$ en los factores:

$$t_1^2 - t_1 * b_1 + p b_1^2 = 83^2 - 83 * 82 + 41 * 82^2 = 275767$$

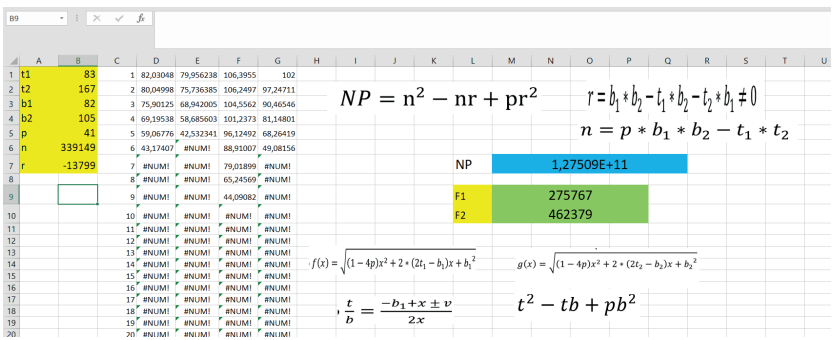
$$t_2^2 - t_2 * b_2 + p b_2^2 = 167^2 - 167 * 105 + 41 * 105^2 = 462379$$

Para encontrar la primalidad de los factores 275767 y 462379 o su factorización completa en caso de que sean compuestos debemos utilizar y

$$f(x) = \sqrt{(1-4p)x^2 + 2*(2t_1 - b_1)x + b_1^2} = \sqrt{-163x^2 + 168x + 6724}$$

$$g(x) = \sqrt{(1-4p)x^2 + 2*(2t_2 - b_2)x + b_2^2} = \sqrt{-163x^2 + 458x + 11025}$$

Utilizando Excel:



Por lo que 275767 es un número primo (le corresponde las dos primeras columnas, no hay puntos enteros) y 462379 es compuesto, existe el punto entero (-1,102).

Luego:

$$\frac{t}{b} = \frac{-105 - 1 + 102}{2*(-1)} = 2 \qquad entonces \quad 2^2 - 2*1 + 41*1^2 = 43$$

$$\frac{t}{b}=\frac{-105-1-102}{2*(-1)}=104 \quad entonces \quad 104^2-104*1+41*1^2=10753$$

Concluimos que:

$$127508\ \ 869693=43*10753*275767$$

FACTORIZACIÓN DE NÚMEROS POLINOMIALES DE LA FORMA: $2n^2+pr^2$

Consideremos números polinomiales que tienen la estructura $NP=2n^2+pr^2$ donde r es un número entero diferente de cero, $p\epsilon\{3, 5, 11, 29\}$ y n es un número entero . Si dados cuatro números enteros $t_1,\ t_2,\ b_1,\ b_2$, si se tiene que $n=pb_1b_2-t_1t_2$ y $r=2t_1b_2+t_2b_1$ entonces el NP es compuesto y dos de sus factores tienen la forma $2t_1^2+pb_1^2$ y $t_2^2+2pb_2^2$. Todo lo anterior se puede describir en el siguiente teorema.

Teorema polinomial de Cordero (2).

Sea $t_1,\ t_2,\ b_1,\ b_2\ \epsilon\ Z,\ b_1\neq 0,\ b_2\neq 0, p\epsilon\{3, 5, 11, 29\}$.

Si $n=pb_1b_2-t_1t_2$ y $r=2t_1b_2+t_2b_1\neq 0$ entonces $NP=2n^2+pr^2$ es compuesto y se factoriza como $NP=\left(2t_1^2+pb_1^2\right)\left(t_2^2+2pb_2^2\right)$.

Demostración.

Sea $NP=2n^2+pr^2$, consideremos $n=pb_1b_2-t_1t_2$ y $r=2t_1b_2+t_2b_1\neq 0$, $p\epsilon\{3, 5, 11, 29\}$.

Tenemos que:

$$NP=2n^2+pr^2$$

$$NP=2n^2+pr^2$$

$$NP=2\left(p^2b_1^2b_2^2-2pb_1b_2t_1t_2+t_1^2t_2^2\right)+p\left(4t_1^2b_2^2+4t_1b_2t_2b_1+t_2^2b_1^2\right)$$

$$NP=2p^2b_1^2b_2^2-4pb_1b_2t_1t_2+2t_1^2t_2^2+4pt_1^2b_2^2+4pt_1b_2t_2b_1+pt_2^2b_1^2$$

$$NP=2p^2b_1^2b_2^2+2t_1^2t_2^2+4pt_1^2b_2^2+pt_2^2b_1^2 \quad (*)$$

Por otro lado tenemos:

$$\left(2t_1^2+pb_1^2\right)\left(t_2^2+2pb_2^2\right)=2t_1^2t_2^2+4pt_1^2b_2^2+pb_1^2t_2^2+2p^2b_1^2b_2^2\,(**)$$

De $(*)\quad y\quad (**)$

$$NP=2n^2+pr^2=\left(2t_1^2+pb_1^2\right)\left(t_2^2+2pb_2^2\right)$$

Queda demostrado el Teorema.

Algoritmos para factorizar completamente a los factores $2t_1^2+pb_1^2$ y $t_2^2+2pb_2^2$

El algoritmo $f(x)=\sqrt{-8px^2+8*t_1x+b_1^2},\quad x\epsilon Z,\ x\neq 0$ nos determina si el factor de NP $2t_1^2+pb_1^2$ (t_1 y b_1 *números primos entre sí*) es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto. En caso de que t_1 y b_1 tengan divisores comunes, estos son factores de $2t_1^2+pb_1^2$.

Sea el factor de NP, $2t_1^2+pb_1^2$, (con t_1 y b_1 *números primos entre sí*). Si existe al menos un $x\epsilon Z,\ x\neq 0$ tal que $f(x)=v$, entonces $2t_1^2+pb_1^2$ es un número compuesto, caso contrario, el número $2t_1^2+pb_1^2$ es primo.

En caso de que $2t_1^2+pb_1^2$ sea compuesto, entonces existe al menos un punto entero $(x,\ v)$.

Luego $\frac{t}{b}=\frac{-b_1\ \pm\ v}{4x}$ con $\frac{t}{b}$ fracción canónica, entonces $2t^2+pb^2\quad o\quad \frac{2t^2+pb^2}{2}$ es un factor de $2t_1^2+pb_1^2$

El algoritmo $g(x)=\sqrt{-2px^2+2*t_2x+b_2^2}$ nos determina si el factor de NP $t_2^2+2pb_2^2$ (t_2 y b_2 *números primos entre sí*) es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto.

En caso de que t_2 y b_2 tengan divisores comunes, estos son factores de $2t_2^2+pb_2^2$.

Si existe algún $x\epsilon Z,\ x\neq 0$ tal que $f(x)=v$, $v\epsilon Z$ entonces $t_2^2+2pb_2^2$ (con t_2 y b_2 *primos entre sí.*) es un número compuesto, caso contrario, el número $t_2^2+2pb_2^2$ es primo.

En caso de $t_2^2+2pb_2^2$ que sea compuesto, entonces existe el punto entero $(x,\ v)$.

Luego $\frac{t}{b}=\frac{-b_2\ \pm\ v}{2x}$ con $\frac{t}{b}$ fracción canónica, entonces $2t^2+pb^2 \quad o \quad \frac{2t^2+pb^2}{2}$ es un factor de $t_2^2+2pb_2^2$

➢ Ejemplo de aplicación 1.

Sea $t_1=71,\quad t_2=11,\quad b_1=3\ ,\quad b_2=23 \quad y \quad p=29$

$n=pb_1b_2-t_1t_2$ y $r=2t_1b_2+t_2b_1$

$n=29*3*23-71*11=1220$

$r=2*71*23+11*3=3299$

El número polinomial que vamos a factorizar es:

$$NP=2n^2+pr^2=2*1220^2+29*3299^2=318595429$$

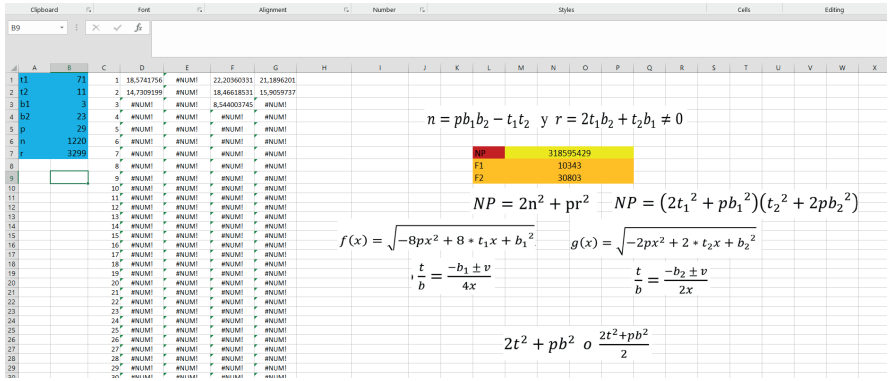
Por el teorema anterior podemos factorizar el número polinomial 318595429 en los factores:

$$2t_1^2+pb_1^2=2*71^2+29*3^2=10343$$
$$t_2^2+2pb_2^2=11^2+2*29*23^2=30803$$

Para encontrar la primalidad de los factores 10343 y 30803 o su factorización completa en caso de que sean compuestos debemos utilizar

$$f(x)=\sqrt{-2px^2+2*t_1x+b_1^2}=\sqrt{-58x^2+142x+9}$$
$$\text{Y}\ g(x)=\sqrt{-2px^2+2*t_2x+b_2^2}=\sqrt{-58x^2+11x+529}$$

Utilizando Excel encontramos que:



Por lo que 10343 y 30803 ambos son números primos. No hay puntos enteros al aplicar los algoritmos.

La factorización completa de $318595429 = 10343 * 30803$ o sea es un semiprimo.

➢ Ejemplo de aplicación 2.

Sea

$t_1 = 3,\ t_2 = 5,\ b_1 = 7\ ,\ b_2 = 11,\ k_1 = -13,\ k_2 = -19,\ l_1 = 41,\ l_2 = 23\ \ y\ \ p = 29$

Pero además: $t_* = p\,b_1 b_2 - t_1 t_2 = 29 * 7 * 11 - 3 * 5 = 2218$

$$t_{**} = p\,l_1 l_2 - 2k_1 k_2 = 29 * 41 * 23 - 2 * (-13) * (-19) = 26853$$

$$r_* = 2t_1 b_2 + t_2 b_1 = 2 * 3 * 11 + 5 * 7 = 101$$

$$r_{**} = k_1 l_2 + k_2 l_1 = (-13) * 23 + (-19) * 41 = -1078$$

$$n = p\,r_* r_{**} - t_* t_{**} = 29 * 101 * (-1078) - 2218 * 26853 = -62717416$$

$$n = p\,r_* r_{**} - t_* t_{**} = 29 * 101 * (-1078) - 2218 * 26853 = -62717416$$

Luego:

$$NP = 2n^2 + pr^2 = 2 * (-62717416)^2 + 29 * (-2069855)^2 = 7991193231343837$$

Sus factores son:

$$2{t_*}^2 + p{r_*}^2 = 2 * 2218^2 + 29 * 101^2 = 10134877$$

$${t_{**}}^2 + 2p{r_{**}}^2 = 26853^2 + 2 * 29 * (-1078)^2 = 788484481$$

O sea:

$$t_{**}^{\,2}+2\,p\,r_{**}^{\,2}=26853^2+2*29*\left(-1078\right)^2=788484481$$

Además estos factores se pueden factorizar:

$$2*t_1^{\,2}+p*b_1^{\,2}=2*3^2+29*7^2=1439$$

$$t_2^{\,2}+2\,p*b_2^{\,2}=5^2+58*11^2=7043$$

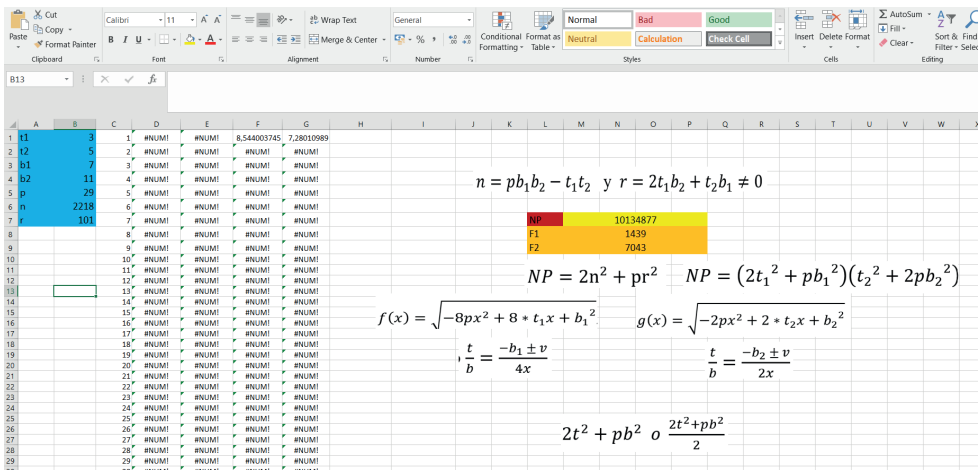
Y

$$2*k_1^{\,2}+p*l_1^{\,2}=2*\left(-13\right)^2+29*41^2=49087$$

$$2*k_2^{\,2}+p*l_2^{\,2}=2*\left(-19\right)^2+29*23^2=16063$$

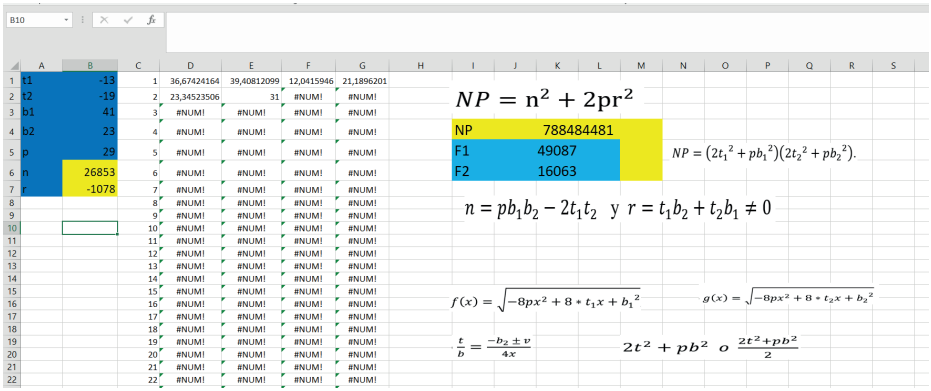
Por último para averiguar si estos cuatro factores son primos o compuestos se debe utilizar los algoritmos de Cordero.

a) Para los factores 1439 y 7043 se obtiene:



Ambos números enteros son primos, no hay puntos enteros.

b) Para el factor 49087 y 16063 se obtiene:



Se obtiene que 49087 es compuesto y 16063 es primo.

Tenemos el punto entero $(-2,31)$

$$\frac{t}{b}=\frac{-41+31}{4*(-2)}=\frac{5}{4} \quad entonces \quad \frac{2*5^2+29*4^2}{2}=257$$

$$\frac{t}{b}=\frac{-41-31}{4*(-2)}=9 \quad entonces \quad 2*9^2+29*1^2=191$$

Luego:

$$49087=257*191$$

La factorización completa de:

$$7991193231343837=191*257*1439*7043*16063$$

FACTORIZACIÓN DE NÚMEROS POLINOMIALES DE LA FORMA: n^2+2pr^2

Consideremos números polinomiales que tienen la estructura $NP=n^2+2pr^2$ donde r es un número entero diferente de cero, $p\epsilon\{3, 5, 11, 29\}$ y n es un número entero. Si dados cuatro números enteros t_1, t_2, b_1, b_2 primos entre sí, o sea el máximo común divisor entre ellos es el uno, si se tiene que $n=pb_1b_2-2t_1t_2$ y $r=t_1b_2+t_2b_1$ entonces el NP es compuesto y dos de sus factores tienen la forma $2t_1^2+pb_1^2$ y $2t_2^2+pb_2^2$. Todo lo anterior se puede describir en el siguiente teorema.

Teorema polinomial de Cordero (3).

Sea $t_1,\ t_2,\ b_1,\ b_2\ \epsilon\ Z, b_1\neq 0,\ b_2\neq 0$, $p\epsilon\{3,\ 5,\ 11,\ 29\}$.

Si $n=pb_1b_2-2t_1t_2$ y $r=t_1b_2+t_2b_1\neq 0$ entonces $NP=n^2+2pr^2$ es compuesto y se factoriza como $NP=\left(2t_1^{\,2}+pb_1^{\,2}\right)\left(2t_2^{\,2}+pb_2^{\,2}\right)$.

Demostración.

Sea $NP=n^2+2pr^2$, consideremos $n=pb_1b_2-2t_1t_2$ y $r=t_1b_2+t_2b_1\neq 0$, $p\epsilon\{3,\ 5,\ 11,\ 29\}$.

Tenemos que:

$$p\epsilon\{3,\ 5,\ 11,\ 29\}$$

$$NP=\left(pb_1b_2-2t_1t_2\right)^2+2p\left(t_1b_2+t_2b_1\right)^2$$

$$NP=\left(p^2b_1^{\,2}b_2^{\,2}-4pb_1b_2t_1t_2+4t_1^{\,2}t_2^{\,2}\right)+2p\left(t_1^{\,2}b_2^{\,2}+2t_1b_2t_2b_1+t_2^{\,2}b_1^{\,2}\right)$$

$$NP=p^2b_1^{\,2}b_2^{\,2}-4pb_1b_2t_1t_2+4t_1^{\,2}t_2^{\,2}+2pt_1^{\,2}b_2^{\,2}+4pt_1b_2t_2b_1+2pt_2^{\,2}b_1^{\,2}$$

$$NP=p^2b_1^{\,2}b_2^{\,2}+4t_1^{\,2}t_2^{\,2}+2pt_1^{\,2}b_2^{\,2}+2pt_2^{\,2}b_1^{\,2}\quad(*)$$

Por otro lado tenemos:

$$\left(2t_1^{\,2}+pb_1^{\,2}\right)\left(2t_2^{\,2}+pb_2^{\,2}\right)=4t_1^{\,2}t_2^{\,2}+2pt_1^{\,2}b_2^{\,2}+2pb_1^{\,2}t_2^{\,2}+p^2b_1^{\,2}b_2^{\,2}\quad(**)$$

De $(*)\quad y\quad (**)$

$$NP=n^2+2pr^2=\left(2t_1^{\,2}+pb_1^{\,2}\right)\left(2t_2^{\,2}+pb_2^{\,2}\right)$$

Queda demostrado el Teorema.

Algoritmos para factorizar completamente a

$$2t_1^{\,2}+pb_1^{\,2}\qquad y\qquad 2t_2^{\,2}+pb_2^{\,2}$$

El algoritmo $f(x)=\sqrt{-8px^2+8*t_1x+b_1^{\,2}},\quad x\epsilon Z,\ x\neq 0$ nos determina si el factor de NP $2t_1^{\,2}+pb_1^{\,2}$ (t_1 y b_1 *números primos entre sí*) es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto. En caso de que tengan divisores comunes, estos son factores de $2t_1^{\,2}+pb_1^{\,2}$.

Sea el factor de NP, $2t_1^2+pb_1^2$, $(\ t_1 y\ b_1\ números\ primos\ entre\ sí\ )$. Si existe al menos un $x\epsilon Z,\ x\neq 0$ tal que $f(x)=v$, entonces $2t_1^2+pb_1^2$es un número compuesto, caso contrario, el número $2t_1^2+pb_1^2$ es primo.

En caso de que $2t_1^2+pb_1^2$ sea compuesto, entonces existe al menos un punto entero $(x,\ v)$.

Luego $\frac{t}{b}=\frac{-b_1\ \pm\ v}{4x}$ con $\frac{t}{b}$ fracción canónica, entonces $2t^2+pb^2\quad o\quad \frac{2t^2+pb^2}{2}$ es un factor de $2^{t_1^2+pb_1^2}$

El algoritmo $g(x)=\sqrt{-8px^2+8*t_2x+b_2^2}$ nos determina si el factor de NP $2t_2^2+pb_2^2$ $(\ t_2\ y\ b_2\ números\ primos\ entre\ sí\ )$ es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto. En caso de que $t_2 y\ b_2$ tengan divisores comunes, estos son factores de $2t_2^2+pb_2^2$.

Sea el factor de NP, $2t_2^2+pb_2^2$, $(\ t_2 y\ b_2\ números\ primos\ entre\ sí\ )$. Si existe algún $x\epsilon Z,\ x\neq 0$ tal que $f(x)=v$, entonces es un número compuesto, caso contrario, el número $2t_2^2+pb_2^2$ es primo.

En caso de que $2t_2^2+pb_2^2$ sea compuesto, entonces existe el punto entero $(x,\ v)$.

Luego $\frac{t}{b}=\frac{-b_2\ \pm\ v}{4x}$ con fracción canónica, entonces $2t^2+pb^2\quad o\quad \frac{2t^2+pb^2}{2}$ es un factor de $2t_2^2+pb_2^2$

- Ejemplo de aplicación 1.

Sea $t_1=61,\ \ t_2=71,\ \ b_1=31\ ,\ \ b_2=23\quad y\quad p=11$

$n=pb_1b_2-2t_1t_2$ y $r=t_1b_2+t_2b_1$

$n=11*31*23-2*61*71=-819$

$r=61*23+71*31=3604$

El número polinomial que vamos a factorizar es:

$$r=61*23+71*31=3604$$

Por el teorema anterior podemos factorizar el número polinomial 286424713_{en} los factores:

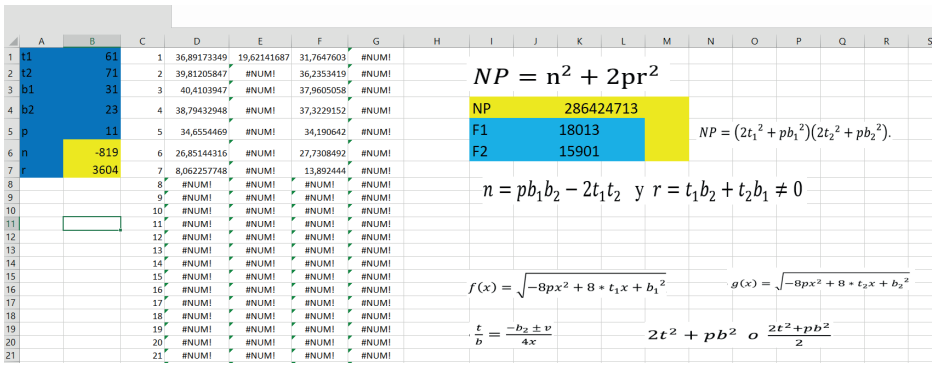
$$2t_1^2+pb_1^2=2*61^2+11*31^2=18013$$

$$2t_2^2+pb_2^2=2*71^2+11*23^2=15901$$

Para encontrar la primalidad de los factores 18013 y 15901 o su factorización completa en caso de que sean compuestos debemos utilizar $f(x)=\sqrt{-8px^2+8*t_1x+b_1^2}=\sqrt{-88x^2+488x+961}$

Y $g(x)=\sqrt{-8px^2+8*t_2x+b_2^2}=\sqrt{-88x^2+568x+529}$

Utilizando Excel encontramos que:



De la tabla en Excel obtenemos que 18013 y 15901 son ambos números primos. No hay puntos enteros.

➢ Ejemplo de aplicación 2.

Sea $t_1=31$, $t_2=17$, $b_1=7$, $b_2=11$, $k_1=-13$, $k_2=19$, $l_1=5$, $l_2=23$ y $p=29$

Pero además: $t_*=pb_1b_2-t_1t_2=29*7*11-31*17=1706$

$t_{**}=pl_1l_2-k_1k_2=29*5*23-(-13)*(19)=3582$

$$r_* = 2t_1b_2 + t_2b_1 = 2*31*11 + 17*7 = 801$$

$$r_{**} = 2k_1l_2 + k_2l_1 = 2*(-13)*23 + (19)*5 = -503$$

$$n = pr_*r_{**} - 2t_*t_{**} = 29*801*(-503) - 2*1706*3582 = -23905971$$

$$r = t_*r_{**} + t_{**}r_* = 1706*(-503) + 3582*801 = 2011064$$

Luego:

$$NP = n^2 + 2pr^2 = (-23905971)^2 + 2*29*(2011064)^2 = 806069397354409$$

Sus factores son:

$$2t_*^2 + pr_*^2 = 2*1706^2 + 29*801^2 = 24427301$$

$$2t_{**}^2 + pr_{**}^2 = 2*3582^2 + 29*(-503)^2 = 32998709$$

O sea:

$$806069397354409 = 24427301*32998709$$

Además estos factores se pueden factorizar:

$$2*t_1^2 + p*b_1^2 = 2*31^2 + 29*7^2 = 3343$$

$$t_2^2 + 2p*b_2^2 = 17^2 + 2*29*11^2 = 7307$$

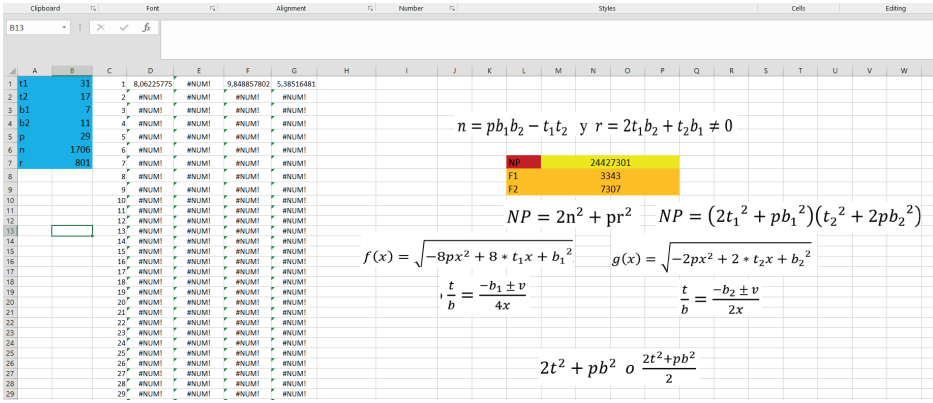
Y

$$2*k_1^2 + p*l_1^2 = 2*(-13)^2 + 29*5^2 = 1063$$

$$k_2^2 + 2p*l_2^2 = (19)^2 + 2*29*23^2 = 31043$$

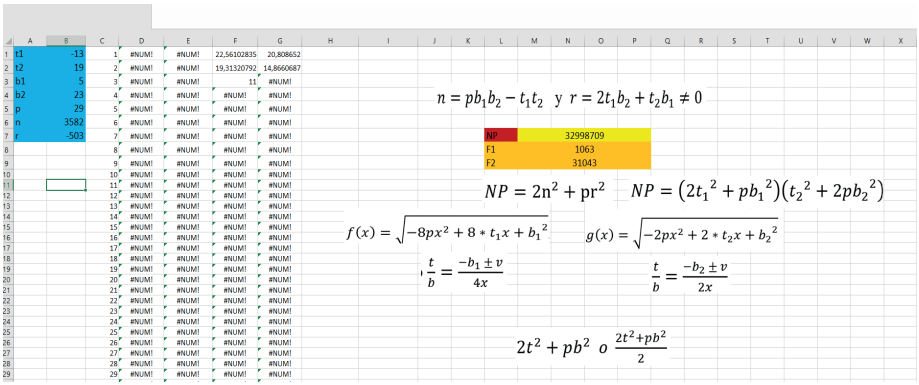
Por último para averiguar si estos cuatro factores son primos o compuestos se debe utilizar los algoritmos de Cordero.

a) Para los factores 3343 y 7307 se obtiene:



Ambos números enteros son primos, no hay puntos enteros.

b) Para los factores de y 31043 se obtiene:



Se obtiene que 1063 es primo y 31043 es compuesto.

Tenemos el punto entero $(3,11)$

$$\frac{t}{b}=\frac{-23+11}{2*3}=-2 \quad entonces \quad 2*(-2)^2+29*1^2=37$$

$$\frac{t}{b}=\frac{-23-11}{2*3}=\frac{-17}{3} \quad entonces \quad 2*(-17)^2+29*3^2=839$$

Luego:

$$31043=37*839$$

La factorización completa de:

$$806069397354409 = 37 * 839 * 1063 * 3343 * 7307$$

IDENTIDAD DE BRAHMAGUPTA-FIBONACCI

La identidad de Brahmagupta-Fibonacci, dice que:

$$(xu - nyv)^2 + n(xv + yu)^2 = (x^2 + n y^2)(u^2 + n v^2)$$

De otra forma:

$$(nyv - xu)^2 + n(xv + yu)^2 = (x^2 + n y^2)(u^2 + n v^2)$$

Se puede utilizar esta identidad para factorizar números polinomiales de la forma $(nyv - xu)^2 + n(xv + yu)^2 = (x^2 + n y^2)(u^2 + n v^2)$. Sustituyendo $n = 2p$, $y = b_1$, $v = b_2$, $x = t_1$, $u = t_2$, obtenemos:

Teorema polinomial de Cordero (4)(se deduce de la identidad de Brahmagupta-Fibonacci)

Sea $t_1,\ t_2,\ b_1,\ b_2 \in Z, t_1,\ t_2,\ b_1,\ b_2$, $p \epsilon \{3,\ 5,\ 11,\ 29\}$.

Si $n = 2pb_1b_2 - t_1t_2$ y $r = t_1b_2 + t_2b_1 \neq 0$ entonces $NP = n^2 + 2pr^2$ es compuesto y se factoriza como $NP = (t_1^2 + 2pb_1^2)(t_2^2 + 2pb_2^2)$.

Demostración.

Sea $NP = n^2 + 2pr^2$, consideremos $n = 2pb_1b_2 - t_1t_2$ y $r = t_1b_2 + t_2b_1 \neq 0$, $p \epsilon \{3,\ 5,\ 11,\ 29\}$.

Tenemos que:

$$NP = n^2 + 2pr^2$$

$$NP = (2pb_1b_2 - t_1t_2)^2 + 2p(t_1b_2 + t_2b_1)^2$$

$$NP = (4p^2b_1^2b_2^2 - 4pb_1b_2t_1t_2 + t_1^2t_2^2) + 2p(t_1^2b_2^2 + 2t_1b_2t_2b_1 + t_2^2b_1^2)$$

$$NP = 4p^2b_1^2b_2^2 - 4pb_1b_2t_1t_2 + t_1^2t_2^2 + 2pt_1^2b_2^2 + 4pt_1b_2t_2b_1 + 2pt_2^2b_1^2$$

$$NP = 4p^2b_1^2b_2^2 + t_1^2t_2^2 + 2pt_1^2b_2^2 + 2pt_2^2b_1^2 \quad (*)$$

Por otro lado tenemos:

$$\left(t_1^2+2pb_1^2\right)\left(t_2^2+2pb_2^2\right)=t_1^2t_2^2+2pt_1^2b_2^2+2pb_1^2t_2^2+4p^2b_1^2b_2^2\,(**)$$

De $(*)$ y $(**)$

$$NP=n^2+2pr^2=\left(t_1^2+2pb_1^2\right)\left(t_2^2+2pb_2^2\right)$$

Queda demostrado el Teorema.

Algoritmos para factorizar completamente a los factores

$$t_1^2+2pb_1^2 \qquad y \qquad t_2^2+2pb_2^2$$

El algoritmo $f(x)=\sqrt{-2px^2+2*t_1x+b_1^2},\ x\epsilon Z,\ x\neq 0$ nos determina si el factor de NP $f(x)=\sqrt{-2px^2+2*t_1x+b_1^2},\ x\epsilon Z,\ x\neq 0$ $(\ t_1 y\ b_1\ números\ primos\ entre\ sí\ )$ es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto. En caso de que $t_1 y\ b_1$ tengan divisores comunes, estos son factores de $t_1^2+2pb_1^2$.

Sea el factor de NP, $t_1^2+2pb_1^2$,. $(\ t_1 y\ b_1\ números\ primos\ entre\ sí\ )$ Si existe al menos un $x\epsilon Z,\ x\neq 0$ tal que $f(x)=v$, entonces $t_1^2+2pb_1^2$ es un número compuesto, caso contrario, el número $t_1^2+2pb_1^2$ es primo.

En caso de que $t_1^2+2pb_1^2$ sea compuesto, entonces existe al menos un punto entero $(x,\ v)$

Luego $\frac{t}{b}\ \frac{-b_1\ \pm\ v}{t_1^2+2pb_1^2}$ con $\frac{t}{b}$ fracción canónica, entonces $2t^2+pb^2$ o $\frac{2t^2+pb^2}{2}$ es un factor de

El algoritmo $g(x)=\sqrt{-2px^2+2*t_2x+b_2^2}$ nos determina si el factor de NP $t_2^2+2pb_2^2$ $(\ t_2\ y\ b_2\ números\ primos\ entre\ sí\ )$ es primo o compuesto y como deducir su factorización completa en caso de que sea compuesto. En caso de que $t_2 y\ b_2$ tengan divisores comunes, estos son factores de $t_2^2+2pb_2^2$.

Sea el factor de NP, $t_2^2+2pb_2^2$,. $(\ t_2 y\ b_2\ números\ primos\ entre\ sí\ )$ Si existe algún $x\epsilon Z,\ x\neq 0$ tal que , entonces es un número compuesto, caso contrario, el número es primo.

En caso de que $t_2^2+2pb_2^2$ sea compuesto, entonces existe el punto entero $(x,\ v)$.

Luego $\frac{t}{b}=\frac{-b_2 \pm v}{2x}$ con $\frac{t}{b}$ fracción canónica, entonces $2t^2+pb^2$ o $\frac{2t^2+pb^2}{2}$ es un factor de $t_2^{\,2}+2pb_2^{\,2}$

➢ Ejemplo de aplicación 1.

Sea $t_1=61,\quad t_2=71,\quad b_1=31\ ,\quad b_2=23\quad y\quad p=11$

$n=2pb_1b_2-t_1t_2$ y $r=t_1b_2+t_2b_1$

$n=2*11*31*23-61*71=11355$

$r=61*23+71*31=3604$

El número polinomial que vamos a factorizar es:

$$NP=n^2+2pr^2=(11355)^2+2*11*3604^2=414689977$$

Por el teorema anterior podemos factorizar el número polinomial 414689977 en los factores:

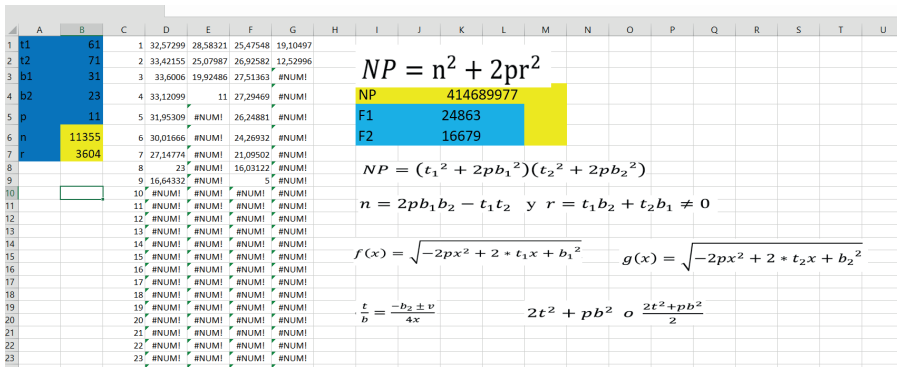
$$t_1^{\,2}+2pb_1^{\,2}=61^2+2*11*31^2=24863$$

$$t_2^{\,2}+2pb_2^{\,2}=71^2+2*11*23^2=16679$$

Para encontrar la primalidad de los factores 24863 y 16679 o su factorización completa en caso de que sean compuestos debemos utilizar $f(x)=\sqrt{-2px^2+2*t_1x+b_1^{\,2}}=\sqrt{-22x^2+122x+961}$

Y $g(x)=\sqrt{-2px^2+2*t_2x+b_2^{\,2}}=\sqrt{-22x^2+142x+529}$

Utilizando Excel encontramos que:



Por lo que 24863 y 16679 ambos son compuestos.

Para 24863 tenemos los puntos enteros: $(8,23)\ \ y\ \ (-4,11).$

Luego:

$\frac{t}{b}=\frac{-31+23}{16}=\frac{-1}{2}$ entonces $\frac{2*(-1)^2+11*2^2}{2}=23$ es un factor de 24863.

$\frac{t}{b}=\frac{-31-23}{16}=\frac{-27}{8}$ entonces $\frac{2*(-27)^2+11*8^2}{2}=1081$ es un factor de 24863.

$\frac{t}{b}=\frac{-31+11}{-8}=\frac{5}{2}$ entonces $\frac{2*(5)^2+11*2^2}{2}=47$ es un factor de 24863.

$\frac{t}{b}=\frac{-31-11}{-8}=\frac{21}{4}$ entonces $\frac{2*(21)^2+11*4^2}{2}=529$ es un factor de 24863.

La factorización completa de 24863=23*47*23 (se toman los dos factores más pequeños y el tercero se obtiene por división).

Para 16679 tenemos el punto entero : $(9,5).$

Luego:

$\frac{t}{b}=\frac{-23+5}{18}=-1$ entonces $2*(-1)^2+11*1^2=13$ es un factor de 16679.

$\frac{t}{b}=\frac{-23-5}{18}=\frac{-14}{9}$ entonces $2*(-14)^2+11*9^2=1283$ es un factor de 16679.

La factorización completa de 16679=13*1283

Luego la factorización completa de:

$$414689977=13*23*23*47*1283$$

IDENTIDADES QUE SE DEDUCEN DE LOS TEOREMAS.

La expresión $NP=N^2+(r-2)N+pr^2-r+1=\frac{(2N+r-2)^2+(4p-1)r^2}{4}$

Sea $a,\ b,\ c,\ d\ \ y\ \ n=4p-1$ con $N=pab-ab-cd+cb+da+1\quad y\quad r=ab-cb-da$

$$NP=\frac{(2N+r-2)^2+(4p-1)r^2}{4}=\frac{\left(\left(\frac{n+1}{2}\right)ab-2ab-2cd+2cb+2da+2+ab-cb-da-2\right)^2+n(ab-cb-da)^2}{4}$$

$$=\frac{\left(\frac{nab+ab-4ab-4cd+4cb+4da+2ab-2cb-2da}{2}\right)^2+n(ab-cb-da)^2}{4}$$

$$=\frac{(nab+ab-4ab-4cd+4cb+4da+2ab-2cb-2da)^2+4n(ab-cb-da)^2}{16}$$

$$=\frac{(nab-ab-4cd+4cb+2da-2cb)^2+4n(ab-cb-da)^2}{16}$$

Por el Teorema Polinomial de Cordero(1)

$$NP=(c^2-ca+pa^2)(d^2-db+pb^2)$$

$$=\left(c^2-ca+\left(\frac{n+1}{4}\right)a^2\right)\left(d^2-db+\left(\frac{n+1}{4}\right)b^2\right)$$

$$=\left(c^2-ca+\left(\frac{n+1}{4}\right)a^2\right)\left(d^2-db+\left(\frac{n+1}{4}\right)b^2\right)$$

$$=\frac{(4c^2-4ca+a^2+na^2)(4d^2-4db+b^2+nb^2)}{16}$$

Luego:

$$(nab-ab-4cd+4cb+2da-2cb)^2+4n(ab-cb-da)^2=(4c^2-4ca+a^2+na^2)(4d^2-4db+b^2+nb^2)$$

I.Primera Identidad de Cordero

$$(nab-ab-4cd+\ 2cb+2da)^2+4n(ab-cb-da)^2=(4c^2-4ca+a^2+na^2)(4d^2-4db+b^2+nb^2))$$

II. Segunda Identidad de Cordero

$$2(nab-cd)^2+n(2cb+da)^2=(2c^2+na^2)(d^2+2nb^2)$$

Comprobación:

$$2(nab-cd)^2+n(2cb+da)^2=2(n^2a^2b^2-2nabcd+c^2d^2)+n(4c^2b^2+4abcd+d^2a^2)$$
$$=2n^2a^2b^2-4nabcd+2c^2d^2+4nc^2b^2+4nabcd+nd^2a^2$$

$$=2n^2a^2b^2+2c^2d^2+4nc^2b^2+nd^2a^2(*)$$

Por otro lado:

$$(2c^2+na^2)(d^2+2nb^2)=2c^2d^2+4nb^2c^2+na^2d^2+2n^2a^2b^2(**)$$

De (*) y (**) obtenemos que:

$$2(nab-cd)^2+n(2cb+da)^2=(2c^2+na^2)(d^2+2nb^2)$$

III. Tercera Identidad de Cordero.

$$(nab-2cd)^2+2n(cb+da)^2=(2c^2+na^2)(2d^2+nb^2)$$

Comprobación:

$$(nab-2cd)^2+2n(cb+da)^2=(n^2a^2b^2-4nabcd+4c^2d^2)+2n(c^2b^2+2abcd+d^2a^2$$

$$=n^2a^2b^2-4nabcd+4c^2d^2+2nc^2b^2+4nabcd+2nd^2a^2$$

$$=n^2a^2b^2+4c^2d^2+2nc^2b^2+2nd^2a^2(*)$$

Por otro lado:

$$(2c^2+na^2)(2d^2+nb^2)=4c^2d^2+2nb^2c^2+2na^2d^2+n^2a^2b^2(**)$$

De (*) y (**) obtenemos que:

$$(nab-2cd)^2+2n(cb+da)^2=(2c^2+na^2)(2d^2+nb^2)$$

IV. Identidad de Brahmagupta-Fibonacci.

$$(nab-cd)^2+n(cb+da)^2=(c^2+na^2)(d^2+nb^2)$$

Comprobación:

$$(nab-cd)^2+n(cb+da)^2=(n^2a^2b^2-2nabcd+c^2d^2)+n(c^2b^2+2abcd+d^2a^2)$$

$$= n^2a^2b^2 - 2nabcd + c^2d^2 + nc^2b^2 + 2nabcd + nd^2a^2$$
$$= n^2a^2b^2 + c^2d^2 + nc^2b^2 + nd^2a^2 \quad (*)$$

Por otro lado:

$$(c^2 + na^2)(d^2 + nb^2) = c^2d^2 + nb^2c^2 + na^2d^2 + n^2a^2b^2 \quad (**)$$

De (*) y (**) obtenemos que:

$$(nab - cd)^2 + n(cb + da)^2 = (c^2 + na^2)(d^2 + nb^2)$$

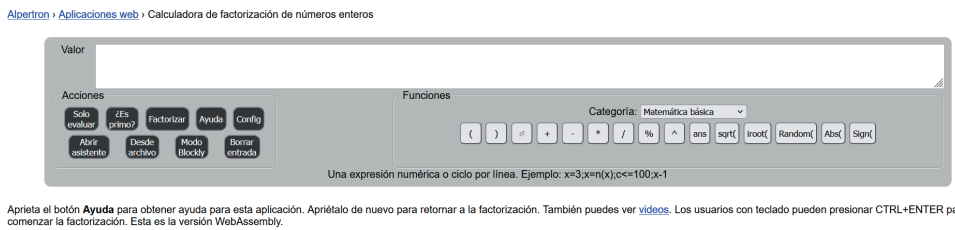
GENERADOR DE NÚMEROS PRIMOS DE MÁS DE 100 DÍGITOS.

La expresión algebraica $(c-a)^2 + (p-1)a^2$ es generadora de números primos. Tiene siempre pocos factores y ellos crecen rápidamente en su cantidad de dígitos.

Si le damos valores grandes a las variables c y a, con p un número afortunado de Euler, $p \in \{2, 3, 5, 11, 17, 41\}$

podemos encontrar números primos de más de 100 dígitos. Para tal efecto se utiliza la Calculadora de Darío Alpern.

Calculadora de factorización de números enteros

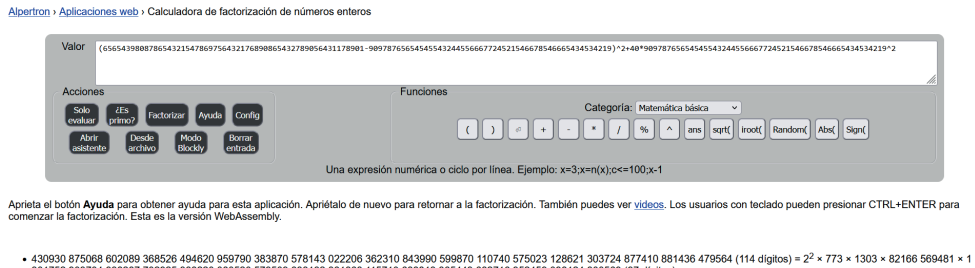


Para empezar sea:

$$c = 65654398087865432154786975643217689086543278905643117890 1$$

$$a = 90978765654545543244556667724521546678546665434534219$$

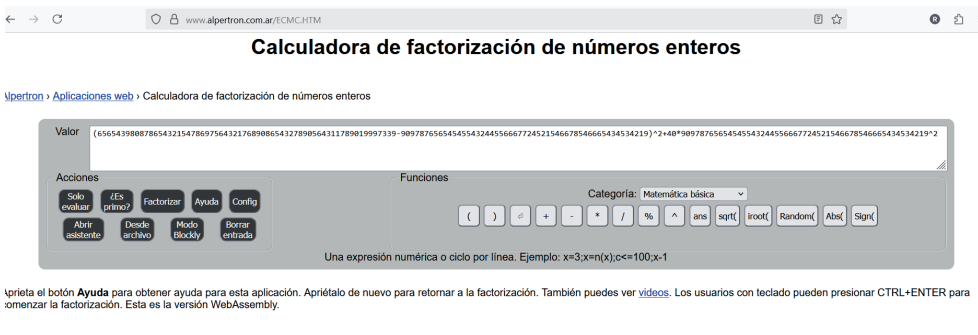
Los cuales son números al azar con $p=41$. Calculando $(c-a)^2+(p-1)a^2$ obtenemos:



Lo cual en primera instancia genera el número primo:

1 301752 903704 938287 702925 388220 080520 573509 838132 881863 115710 688813 365443 682716 952459 098124 300569 (97 dígitos)

Si agregamos más dígitos a , de tal forma que el cálculo no se pase más allá de los números primos de 20 dígitos, obtenemos más números primos grandes.

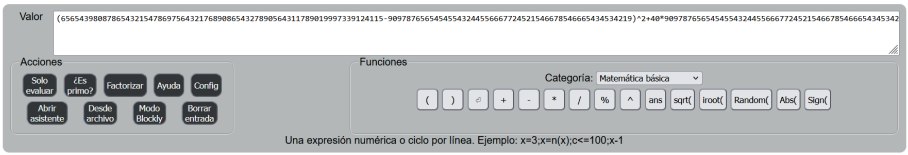


Agregando dígitos a $c=\ldots 9997339$ se genera el número primo.

2288 367454 838097 963404 301630 837236 389495 056486 818353 822358 291908 172297 961014 517108 605156 381149 672655 597618 282454 951613 (118 dígitos)

Si se continúa agregándole dígitos a $c=\ldots 124115$

Alpertron › Aplicaciones web › Calculadora de factorización de números enteros



Aprieta el botón **Ayuda** para obtener ayuda para esta aplicación. Apriétalo de nuevo para retornar a la factorización. También puedes ver videos. Los usuarios con teclado pueden presionar CTRL+ENTER para comenzar la factorización. Esta es la versión WebAssembly.

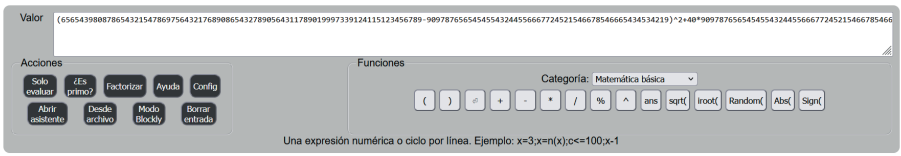
- 43 104999 882799 079945 219756 194167 039168 003319 160165 309250 721750 551406 218084 093637 395597 396581 828242 575974 381041 180183 541097 837580 331222 889256 (140 dígitos) = 2^3 × 823 × 186103 × 411241 × 8 283161 × 1 885598 156677 × 5477 000715 384580 494996 202126 711962 091427 531918 772899 077448 176579 347270 269995 010409 441260 357873 441409 155089 (106 dígitos)

Se obtiene el número primo:

5477 000715 384580 494996 202126 711962 091427 531918 772899 077448 176579 347270 269995 010409 441260 357873 441409 155089 (106 dígitos)

De nuevo agregando más dígitos a $c = \ldots 123456789$

Alpertron › Aplicaciones web › Calculadora de factorización de números enteros



Aprieta el botón **Ayuda** para obtener ayuda para esta aplicación. Apriétalo de nuevo para retornar a la factorización. También puedes ver videos. Los usuarios con teclado pueden presionar CTRL+ENTER para comenzar la factorización. Esta es la versión WebAssembly.

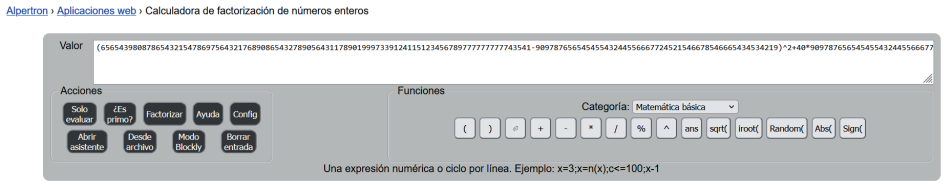
- 43 104999 882799 081139 850974 564765 913530 219024 980265 226493 628029 971940 048098 994526 176007 275343 416160 689380 335209 421573 979476 350338 160983 188567 192032 466733 003340 (158 dígitos) = 2^2 × 5 × 22637 × 50767 × 5 146927 × 1071 802889 × 33271 499126 352881 × 10 217907 813762 213791 050870 769943 953270 963923 595964 281635 014438 401039 829316 278741 175524 090484 510234 040227 646455 280011 (116 dígitos)

Se obtiene el número primo:

10 217907 813762 213791 050870 769943 953270 963923 595964 281635 014438 401039 829316 278741 175524 090484 510234 040227 646455 280011 (116 dígitos)

De nuevo si agregamos más dígitos al valor de $c = \ldots 777777777743541$

Calculadora de factorización de números enteros



Aprieta el botón **Ayuda** para obtener ayuda para esta aplicación. Apriétalo de nuevo para retornar a la factorización. También puedes ver videos. Los usuarios con teclado pueden presionar CTRL+ENTER para comenzar la factorización. Esta es la versión WebAssembly.

- 43 104999 882799 081139 850975 759397 133095 448263 639059 262024 086195 369452 726405 742412 028779 138496 329823 260911 434073 666326 523132 567494 827600 370741 746087 490838 558194 755834 752231 206615 065985 298124 (188 dígitos) = $2^2 \times 1091 \times 16649 \times 13664\,788260\,996343 \times 43\,416203\,723888\,433417\,890261\,272856\,760764\,281962\,459273\,531699\,170675\,760224\,282527\,438117\,082830\,403180\,072988\,511913\,790772\,523621\,470280\,848385\,381572\,585954\,114958\,450924\,508602\,996863$ (164 dígitos)

Se obtiene el número primo:

43 416203 723888 433417 890261 272856 760764 281962 459273 531699 170675 760224 282527 438117 082830 403180 072988 511913 790772 523621 470280 848385 381572 585954 114958 450924 508602 996863 (164 dígitos)

El proceso se puede continuar hasta donde la tecnología soporte. El procedimiento permite obtener rápidamente números primos de más de 100 dígitos, utilizando la Calculadora de Darío Alpern y la fórmula del matemático Ronald Cordero Méndez. Durante el proceso se puede variar el valor de , siendo los más eficientes para generar número primos grandes el 11, 17 y 41.

Utilizando otros valores de c y a con $p=41$ se pueden generar números primos como:

a) 759050 592899 752060 564706 105636 755615 085360 293660 512843 479011 292689 078293 297564 877805 521191 685447 243892 767273 779189 181165 662587 405612 236299 255057 777886 692385 706935 077225 377505 628104 152900 149210 462923 120141 394908 326235 314576 431484 838010 390019 (240 dígitos)

b) 27772 055806 634340 962756 711851 152269 996007 223579 086286 185457 849489 675713 282309 006044 632725 239539 363213 753111 928233 682929 492266 157153 366618 749626 642629 767338 834017 403223 964589 010842 813198 258542 954790 226204 957917 091984 539721 667418 119862 393651 000711 537525 900400 539899 (263 dígitos)

CONCLUSIONES

I.Los teoremas y algoritmos de cordero buscan superar las limitaciones de los métodos tradicionales en términos de velocidad y eficiencia.

II. La investigación de Cordero no se limita a solamente la teoría; se extiende a la aplicación práctica, como es el caso de construcción de software basado en sus algoritmos para encontrar números primos y factorizar números compuestos de gran tamaño.

III. La investigación tiene implicaciones en la búsqueda de números primos, incluso de más de cien dígitos.

IV. La investigación es una contribución a la teoría de números que se enfoca en la creación de herramientas algorítmicas y computacionales para abordar uno de los problemas más antiguos y complejos de las matemáticas: la factorización de números enteros.

REFERENCIA

Abel, U. y Siebert, H."Secuencias con un gran número de valores primos". Soy. Matemáticas. Mensual 100, 167-169, 1993.

Boston, N. y Greenwood, M. L. "Cuadráticas que representan números primos". América. Matemáticas. Mensual 102,595-599, 1995

Dudley, U. "Historia de la fórmula de los números primos". América. Matemáticas. Mensual 76, 23-28, 1969.

Garrison, B. "Polinomios con un gran número de valores primos". América. Matemáticas. Mensual 97, 316-317, 1990.

Hardy, G. H. y Wright, E. M. "Introducción a la Teoría de Números", 5° ed. Oxford, Inglaterra: Clarendon Press, 1979.

Pregg, E. Jr. "Concursos de programación de Al Zimmermann: polinomios generadores de primos". 13 de marzo de 2006. https:// www.recmath.org/contest/description.php.