v. 5, n. 7, 2025

Journal of
Engineering
Research

FACTORIZATION OF POLYNOMIAL INTEGER NUMBERS AND THEIR ALGORITHMS

Ronald Cordero Méndez
Master's Degree

Acceptance date: 23/09/2025

Abstract: Cordero's 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 methods of integer factorization 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 factorize these two integers obtained through the formulas.
Keywords: Factorization, Integers, Algorithms, Computer programs, Software, Theorem.

INTRODUCTION

The method proposed here is not a general-purpose method for factoring any integer, such as the Quadratic Sieve or the Number Field Sieve. Instead, it is designed to work with numbers that follow certain specific algebraic patterns, such as polynomial numbers of the form; $n^2 + (r - 2)\, n + pr^2 - r + 1$, $2n^2 + pr^2$ o n^2+2pr^2.

Cordero's method is a specialized approach to the factorization of integers, limited to numbers that fit specific polynomial formulas, and not a universal method for all integers.

It is clear that currently the main challenge in integer factorization is the computational complexity that increases exponentially with the size of the integer. Unlike multiplication, which is a relatively simple and quick problem to solve, there is no known efficient algorithm for factorizing large or very large integers.

Current algorithms for large numbers, such as the Number Field Sieve (NFS), are very slow and require enormous computational resources. Factors with hundreds of digits can take years to solve, even with the collaboration of thousands of computers. For example, the number RSA-250 (a 250-digit number) was factored in 2020 after a great deal of time and effort. This factorization problem has not yet been formally classified into a simple computational complexity class (such as P or NP). It is known to be in the NP and Co-NP classes, but it has not been proven whether it belongs to P or is an NP-complete problem, reflecting its fundamental complexity.

The biggest challenge for the future is Shor's algorithm. This algorithm, designed for quantum computers, could factorize integers in polynomial time, which would mean that large numbers could be factorized almost instantaneously. This would jeopardize the security of current cryptography. Although current quantum computers are not yet powerful enough to run Shor's algorithm on a large scale, its development represents a huge theoretical and practical challenge for modern cryptography. The most recent advances in integer factorization have focused primarily on optimizing existing algorithms for classical computing and researching new theoretical approaches. This is due to the importance of factorization in the security of public-key cryptography, such as the RSA algorithm.

The most notable advances in recent years have been the successful factorization of large RSA numbers. Efforts have focused on refining algorithms such as NFS. Variations have been developed, such as the GNFS-FFT algorithm, which seek to reduce the execution time and resources required for factorization. Research has also emerged that reformulates the factorization problem from different mathematical angles. A recent example is an approach that equates factorization with the problem of finding the perimeter of a rectangle of known area, or with the calculation of certain integrals.

Cordero's theorems and algorithms are designed to factor polynomial numbers of particular forms, such as numbers of the form: $n^2 + (r - 2)\, n + pr^2 - r + 1$, $2n^2 + pr^2$ o n^2+2pr^2

where are prime numbers such as 2, 3, 5, 11, 17, 29 y 41 depending on the polynomial number being worked with, are integers with a certain structure. For these numbers, his methods offer a more direct path than general-purpose algorithms. This is particularly relevant in number theory, where the study of specific families of numbers can reveal important properties and patterns. The ability to factor numbers of these forms efficiently could contribute to knowledge in this field.

The factorization of large integers is the basis for the security of many cryptographic systems, such as the RSA algorithm. The difficulty of this problem is what makes them secure. Cordero's proposal could have a potential impact in this field, since if his algorithms prove to be efficient for factorizing a subset of integers used in cryptography, it could have implications for the security of these systems. Cordero's theorems and algorithms, together with the computer programs that have been developed to verify them, serve as supporting material for the creation of factorization software. This could help build more specialized and efficient tools for calculating very large prime numbers and factorizing integers that meet the conditions of his theorems.

Unlike traditional brute force or sieve methods, Cordero's work approaches factorization from a different perspective, using polynomial properties. This research encourages the study of new approaches to solving the problem of integer factorization, a problem for which there is no efficient and universally applicable solution. This may inspire other researchers to explore alternative paths that, over time, could lead to significant advances in the field.

FACTORIZATION OF POLYNOMIAL NUMBERS OF THE FORM: $N^2 + (R - 2) N + PR^2 - R + 1$

Let us consider polynomial numbers that have the structure $NP= n^2 + (r - 2) n + pr^2 - r + 1$ where r is an integer other than zero, p is a lucky Euler number, i.e. $p \in \{2, 3, 5, 11, 17, 41\}$, and n is an integer. If we are given four integers t_1, t_2, b_1, b_2 that are coprime, i.e., their greatest common divisor is one, and if we have that, $n = (p - 1) * b_1 * b_2 - t_1 * t_2 + ,t_1 * b_2 + t_2 * b_1 + 1$, and $r = b_1 * b_2 - t_1 * b_2 - t_2 * b_1$, then NP is composite and two of its factors have the form $t_1^2 - t_1 * b_1 + pb_1^2$ and $t_2^2 - t_2 * b_2 + pb_2^2$. All of the above can be described in the following theorem.

CORDERO'S POLYNOMIAL THEOREM (1)

Let $t_1, t_2, b_1, b_2 \in Z, b_1 \neq 0, b_2 \neq 0$, be relatively prime, $p \in \{2, 3, 5, 11, 17, 41\}$.

If $n = (p-1) * b_1 * b_2 - t_1 * t_2 + t_1 * b_2 + t_2 * b_1 + 1$ and $r = b_1 * b_2 - t_1 * b_2 - t_2 * b_1 \neq 0$ thenNP $= n^2 + (r-2) n + pr^2 - r + 1$ is composite and factors as $NP = (t_1^2 - t_1 * b_1 + pb_1^2) (t_2^2 - t_2 * b_2 + pb_2^2)$.

Proof.

Let $NP = n^2 + (r-2) n + pr^2 - r+1$. Considern $= (p-1) * b_1 * b_2 - t_1 * t_2 + ,t_1 * b_2 + t_2 * b_1 + 1$, and $r = b_1 * b_2 - t_1 * b_2 - t_2 * b_1 \neq 0$,$p \in \{2, 3, 5, 11, 17, 41\}$.

We have that:

$n = (p-1) * b_1 * b_2 - t_1 * t_2 + ,t_1 * b_2 + t_2 * b_1 + 1$

$n = pb_1 * b_2 - b_1 * b_2 - t_1 * t_2 + t_1 * b_2 + t_2 * b_1 + 1$

$n = pb_1 * b_2 - (b_1 * b_2 - t_1 * b_2 - t_2 * b_1) - t_1 * t_2 + 1$

$n = pb_1 * b_2 - r - t_1 * t_2 + 1$

Furthermore:

$NP = n_2 + (r - 2)n + pr^2 - r + 1$

$NP = n (n + r - 2) + pr2 - r + 1$

$NP=(pb_1*b_2-r-t_1*t_2+1pb_1*b_2-r-t_1*t_2+1+r-2)+pr^2-r+1$

$NP=(pb_1*b_2-r-t_1*t2+1)(pb_1*b_2-t_1*t_2-1)+pr^2-r+1$

$NP=p^2b_1^2b_2^2-pb_1b_2t_1t_2-pb_1b_2-prb_1b_2+rt_1t_2+r--pb_1b_2t_1t_2+t_1^2t_2^2+t_1t2+pb_1b_2-t_1t_2-1+pr^2-r+1$

$NP=p^2b_1^2b_2^2 - 2pb_1b_2t_1t_2 - prb_1b_2 + rt_1t_2 + t_1^2t_2^2 + pr^2$

$NP=p^2b_1^2b_2^2 - 2pb_1b_2t_1t_2 + r(t_1t_2 - pb_1b_2 + pr) + t_1^2t_2^2$

$NP=p^2b_1^2b_2^2 - 2pb_1b_2t_1t_2 + (b_1b_2-t_1b_2-t_2b_1)(t_1t_2-pt_1b_2+pt_2b_1), + t_1^2t_2^2$

$NP=p_2b_1^2b_2^2 - 2pb_1b_2t_1t_2 + b_1b_2t_1t_2 - pb_1b_2^2t_1 - pb_1^2b_2t_2 - t_1^2t_2b_2 + pt_1^2b_2^2 + pt_1b_2t_2b_1 - b_1t_1t_2^2+p-t_2b_1t_1b_2 + pt_2^2b_1^2+t_1^2t_2^2$

$NP = p_2b_1^2b_2^2 + b^1b^2t^1t^2 - pb_1b_2^2t_1 - pb_1^2b_2t_2 - t_1^2t_2b_2 + pt_1^2b_2^2 - b_1t_1t_2^2 + pt_2^2b_1^2 + t_1^2t_2^2$ (*)

On the other hand, we have:

$(t_1^2-t_1b_1+pb_1^2)(t_2^2-t_2b_2+pb_2^2)=t_1^2t_2^2-t_1^2t_2b_2+pb_2^2t_1^2-t_1b_1t_2^2+t_1b_1t_2b_2-pb_2^2t_1b_1+pb_1^2t_2^2-pb_1^2t_2b_2+p_2b_1^2b_2^2$(**)

From (*) y (**), we obtain:

$NP = n^2 + (r - 2)n + pr^2 - r + 1 = (t_1^2 - t_1b1 + pb_1^2)(t_2^2 - t_2b_2 + pb_2^2)$

The theorem is proven.

ALGORITHM FOR COMPLETE FACTORIZATION $(T_1^2-T_1B_1+PB_1^2)(T_2^2-T_2B_2+PB_2^2)$

The algorithm $f(x)=\sqrt{(1-4p)x^2+2*(2t_1-b_1)x+b_1^2},\ x\epsilon Z,\ x\neq 0$ determines whether the factor of NP $t_1^2-t_1*b_1+pb_1^2$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be $t_1^2-t_1*b_1+pb_1^2$. If there exists at least one $x\epsilon Z, x\neq 0$ such that $f(x) = v$,$v\epsilon Z$, then $t_1^2-t_1 * b_1 + pb_1^2$ is a composite number; otherwise, the number $t_1^2-t_1*b_1+pb_1^2$ is prime.

If $t_1^2-t_1 * b_1 + pb_1^2$ is composite, then there exists at least one integer point (x, v).

Then $\frac{t}{b} = \frac{-b_1+x\pm v}{2x}$ with $\frac{t}{b}$ canonical fraction, then $t^2-tb+pb^2$ is a factor of $t_1^2-t_1*b_1+pb_1^2$

The algorithm $g(x)=\sqrt{(1-4p)x^2+2*(2t_2-b_2)x+b_2^2}$ determines whether the factor of NP $t_2^2-t_2*b_2+pb_2^2$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be $t_2^2-t_2*b_2+pb_2^2$. If there exists an $x\epsilon Z, x\neq 0$ such that $f(x) =v$,$v\epsilon Z$, then $t_2^2-t_2*b_2+pb_2^2$ is a composite number; otherwise, the number $t_2^2-t_2*b_2+pb_2^2$ is prime.

If $t_2^2-t_2*b_2+pb_2^2$ is composite, then there exists an integer point (x, v).

Then $\frac{t}{b} = \frac{-b_1+x\pm v}{2x}$ with $\frac{t}{b}$ canonical fraction, then $t^2-tb+pb^2$ is a factor of $t_2^2-t_2*b_2+pb_2^2$

- Application example 1

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

$n= (p-1) * b_1*b_2-t_1*t_2+t_1*b_2+t_2*b_1+1$

$n = 40 *(-17) *23-11*13 +11*23+13*(-17)+1= -15750$

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

The polynomial number we are going to factor is:

$NP = n^2 + (r-2)n + pr^2 - r + 1 =(- 157502) + (-425)* - 15750 + 41*(-423^2)-(-423) + 1 = 262092763$

By the above theorem, we can factor the polynomial number 262092763 into the factors:

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

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

To find the primality of the factors 12157 and 21559 or their complete factorization in case they are composite, we must use

$$f(x) = \sqrt{(1-4p)x^2 + 2*(2t_1 - b_1)x + b_1^2} = \sqrt{-163x^2 + 78x + 289}$$

And

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

Using Excel, we find that:

	A	B	C	D	E	F	G	L	M
1	t1	11	1	14,28285686	6,92820323	19,28730152	18,97366596		
2	t2	13	2	#NUM!	#NUM!	#NUM!	#NUM!		
3	b1	-17	3	#NUM!	#NUM!	#NUM!	#NUM!		
4	b2	23	4	#NUM!	#NUM!	#NUM!	#NUM!		
5	p	41	5	#NUM!	#NUM!	#NUM!	#NUM!		
6	M	-31925	6	#NUM!	#NUM!	#NUM!	#NUM!		
7	r	-423	7	#NUM!	#NUM!	#NUM!	#NUM!	NP	262092763
8			8	#NUM!	#NUM!	#NUM!	#NUM!		
9			9	#NUM!	#NUM!	#NUM!	#NUM!	F1	12157
10			10	#NUM!	#NUM!	#NUM!	#NUM!	F2	21559
11			11	#NUM!	#NUM!	#NUM!	#NUM!		

There are no ordered pairs where the preimage and image are integers, i.e., there are no integer points. Note that very few calculations are needed to conclude that the integers 12157 and 21559 are both prime numbers.

We conclude that the complete factorization of 262092763 = 12157 * 21559

- Application example 2.

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

$n = (p-1) * b_1 * b_2 - t_1 * t_2 + t_1 * b_2 + t_2 * b_1 + 1$

$n = 40 * 82*105-83 * 167 + 83 * 105 + 167 * 82 + 1 = 352949$

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

The polynomial number we are going to factor is:

$NP = n^2+(r-2)n+pr^2 - r + 1 = (352949)^2 + (-13801) * 352949 + 41 * (-137992)^2 - (-13799) + 1 = 127508\ 869693$

By the above theorem, we can factor the polynomial number 127508 869693 into the factors:

$t_1^2 - t_1 * b_1 + pb_1^2 = 83^2 - 83 * 82 + 41 * 82^2 = 275767$

$t_2^2 - t_2 * b_2 + pb_2^2 = 167^2 - 167 * 105 + 41 * 105^2 = 462379$

To find the primality of the factors 275767 and 462379 or their complete factorization in case they are composite, we must use and

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

and

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

Using Excel:

	A	B	C	D	E	F	G	L	M
1	t1	83	1	82,03048214	79,956238	106,3954886	102		
2	t2	167	2	80,04998438	75,7363849	106,2497059	97,24710793		
3	b1	82	3	75,90125164	68,9420046	104,556205	90,46546302		
4	b2	105	4	69,19537557	58,685603	101,2373449	81,14801291		
5	p	41	5	59,0677577	42,5323406	96,12491873	68,26419266		
6	M	692097	6	43,17406629	#NUM!	88,91006692	49,08156477		
7	r	-13799	7	#NUM!	#NUM!	79,01898506	#NUM!	NP	1,27509E+11
8			8	#NUM!	#NUM!	65,24568951	#NUM!		
9			9	#NUM!	#NUM!	44,09081537	#NUM!	F1	275767
10			10	#NUM!	#NUM!	#NUM!	#NUM!	F2	462379
11			11	#NUM!	#NUM!	#NUM!	#NUM!		
12			12	#NUM!	#NUM!	#NUM!	#NUM!		

Therefore, 275767 is a prime number (it corresponds to the first two columns, there are no integer points) and 462379 is composite, there is an integer point (-1.102).

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

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

We conclude that:

127508 869693 = 43 * 10753 * 275767

- Application example 3

Let a = 83, b = 71, c = 97 , d = 107 y p = 41. How many polynomial numbers of the form $n^2 + (r-2)n + pr^2 - r+1$ can be obtained with these numbers, what are they, and find the complete factorization of each one?

Journal of Engineering Research ISSN 2764-1317 DOI https://doi.org/10.22533/at.ed.3175725170714

Solution:

$n = (p-1) * b_1 * b_2 - t_1 * t_2 + t_1 * b_2 + t_2 * b_1 + 1$
$r = b_1 * b_2 - t_1 * b_2 - t_2 * b_1$

In conclusion, we obtain 12 different polynomial numbers, namely $4P_2 = 12$.

FACTORIZATION OF POLYNOMIAL NUMBERS OF THE FORM $2N^2+PR^2$

Let us consider polynomial numbers that have the structure $NP=2n^2+pr^2$ where r is an integer other than zero, $p\epsilon \{3, 5, 11, 29\}$, and n is an integer. If we are given four integers t_1, t_2, b_1, b_2 that are relatively prime, that is, their greatest common divisor is one, and if we have that $n= pb_1b_2-t_1t_2$ and $2t_1b_2+t_2b_1$, then NP is composite and two of its factors have the form $2t_1^2+pb_1^2$ and $t_2^2+2pb_2^2$. All of the above can be described in the following theorem.

CORDERO'S POLYNOMIAL THEOREM (2)

Let $t_1, t_2, b_1, b_2 \epsilon Z, b_1\neq 0, b_2\neq 0$, be relatively prime, and $p\epsilon \{3, 5, 11, 29\}$.

If $n=pb_1b_2-t_1t_2$ and $r=2t_1b_2+t_2b_1\neq 0$, then-$NP=2n^2+pr^2$ is composite and factors as $NP = \left(2t_1^{\ 2} + pb_1^{\ 2}\right)\left(t_2^{\ 2} + 2pb_2^{\ 2}\right)$

Proof.

Let $NP=2n^2+pr^2$, considern $n = pb_1b_2-t_1t_2$ and $r=2t_1b_2+t_2b_1\neq 0$,$p\epsilon \{3, 5, 11, 29\}$

We have that:

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

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

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

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

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

On the other hand, we have:

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

From (*) y (**)

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

The theorem is proven.

ALGORITHMS FOR COMPLETELY FACTORING THE FACTORS $2T_1^{\ 2}+PB_1^{\ 2}$ Y $T^{22}+2PB_2^{\ 2}$

The algorithm $f(x) = \sqrt{-8px^2 + 8 * t_1x + b_1^{\ 2}}$, $x\epsilon Z$, $x\neq 0$ determines whether the factor of NP-$2t_1^{\ 2}+pb_1^{\ 2}$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be$2t_1^{\ 2}+pb_1^{\ 2}$. If there exists at least one $x\epsilon Z$, $x\neq 0$ such that $f(x)=v$,$v\epsilon Z$, then $2t_1^{\ 2}+pb_1^{\ 2}$ is a composite number; otherwise, the number $2t_1^{\ 2}+pb_1^{\ 2}$is prime.

If $2t_1^{\ 2}+pb_1^{\ 2}$is composite, then there exists at least one integer point (x, v).

Then $\frac{t}{b} = \frac{-b_1 \pm v}{4x}$with $\frac{t}{b}$canonical fraction, then $2t^2+pb^2$ o $\frac{2t^2+pb^2}{2}$ is a factor of $2t_1^{\ 2}+pb_1^{\ 2}$

The algorithm $g(x) = \sqrt{-2px^2 + 2 * t_2x + b_2^{\ 2}}$ determines whether the factor of NP $t_2^{\ 2}+2pb_2^{\ 2}$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be$t_2^{\ 2}+2pb_2^{\ 2}$. If there exists an $x\epsilon Z$, $x\neq 0$ such that $f(x) =v$,$v\epsilon Z$, ,then $t_2^{\ 2}+2pb_2^{\ 2}$ is a composite number; otherwise, the number $t_2^{\ 2}+2pb_2^{\ 2}$ is prime.

If $t_2^{\ 2}+2pb_2^{\ 2}$ is composite, then there exists an integer point (x, v).

Journal of Engineering Research ISSN 2764-1317 DOI https://doi.org/10.22533/at.ed.3175725170714

Permutations of a, b, c, and d 4!=24				n	r	NP	F1	F2	Factoring F1 (x, v) $\frac{t}{b}=\frac{-b_1\pm x+v}{2x}$ $t^2 - tb + pb^2$	Factorize F2 (x, v) $\frac{t}{b}=\frac{-b_2\pm x-v}{2x}$ $t^2 - tb + pb^2$
t1	t2	b1	b2			$n^2+(r-2)n$	$t_1^2 - t_1 * b_1 + pb_1^2$	$t_2^2 - t_2 * b_2 + pb_2^2$	Cordero's algorithm $f(x)=\sqrt{(1-4p)x^2+2*(2t_1-b_1)x+b_1^2}$ $g(x)=\sqrt{(1-4p)x^2+2*(2t_2-b_2)x+b_2^2}$	
83	71	97	107	425036	-5389	179554931771	384,607	466,853	(8,9) $\frac{t}{b}=\frac{-97+9\pm 8}{16}$ $\frac{t}{b}$ $=-5$ o $\frac{-49}{8}$ $5^2+5+41=71$ $49^2+49*8+41*8^2=5417$	Cousin
83	71	107	97	424,916	-5269	179452136891	467,417	383,923	Cousin	cousin
83	107	71	97	282,248	-8761	80337563003	207,677	386,839	(−5,4) $\frac{t}{b}=\frac{-71-5\pm 4}{-10}$ $\frac{t}{b}$ $=\frac{36}{5}$ o 8 $8^2-8+41=97$ $36^2-36*5+41*5^2=2141$	cousin
83	107	97	71	282,872	-9385	80972465531	384,607	210533	(8,9) $\frac{t}{b}=\frac{-97+9\pm 8}{16}$ $\frac{t}{b}$ $=-5$ o $\frac{-49}{8}$ $5^2+5+41=71$ $49^2+49*8+41*8^2=5417$	Cousin
83	97	107	71	312102	-8675	97785038651	467,417	209203	Cousin	Cousin
83	97	71	107	311598	-8171	97283391181	207,677	468,439	(−5,4) $\frac{t}{b}=\frac{-71-5\pm 4}{-10}$ $\frac{t}{b}$ $=\frac{36}{5}$ o 8 $8^2-8+41=97$ $36^2-36*5+41*5^2=2141$	cousin
71	83	97	107	424916	-5269	179452136891	383,923	467417	Cousin	Cousin
71	83	107	97	425036	-5389	179554931771	466,853	384,607	Cousin	(8,9) $\frac{t}{b}=\frac{-97+9\pm 8}{16}$ $\frac{t}{b}$ $=-5$ o $\frac{-49}{8}$ $5^2+5+41=71$ $49^2+49*8+41*8^2=5417$
71	107	83	97	330212	-7717	108932701883	281,597	386,839	(3,76) $\frac{t}{b}=\frac{-83+3\pm 76}{6}$ $\frac{t}{b}$ $=\frac{-2}{3}$ o -26 $26^2+26+41=743$ $2^2+2*3+41*3^2=379$	Cousin
71	107	97	83	330716	-8221	109424581691	383,923	285017	Cousin	(4,73) $\frac{t}{b}=\frac{-83+4\pm 73}{8}$ $\frac{t}{b}$ $=\frac{-3}{4}$ o -19 $3^2+3*4+41*4^2=677$ $19^2+19+41=421$
71	97	107	83	364,626	-7391	132496149371	466,853	283,807	cousin	cousin
71	97	83	107	364002	-6767	131911017083	281,597	468439	(3,76) $\frac{t}{b}=\frac{-83+3\pm 76}{6}$ $\frac{t}{b}$ $=\frac{-2}{3}$ o -26 $26^2+26+41=743$ $2^2+2*3+41*3^2=379$	Cousin
97	83	71	107	312102	-8675	97785038651	209,203	467,417	Cousin	Cousin
97	83	107	71	311598	-8171	97283391181	468,439	207677	Cousin	(−5,4) $\frac{t}{b}=\frac{-71-5\pm 4}{-10}$ $\frac{t}{b}$ $=\frac{36}{5}$ o 8 $8^2-8+41=97$ $36^2-36*5+41*5^2=2141$
97	107	83	71	241110	-9875	59750739131	283,807	210533	Cousin	cousin

97	107	71	83	240,990	-9755	596,264,11451	209,203	285,017	cousin	(4,73) $\frac{t}{b}=\frac{-83+4\pm 73}{8}$ $\frac{t}{b}$ $=\frac{-3}{4}$ o -19 $3^2+3*4+41*4^2=677$ $19^2+19+41=421$
97	71	107	83	364002	-6767	131911017083	468439	281,597	Cousin	(3,76) $\frac{t}{b}=\frac{-83+3\pm 76}{6}$ $\frac{t}{b}$ $=\frac{-2}{3}$ o -26 $26^2+26+41=743$ $2^2+2*3+41*3^2=379$
97	71	83	107	364,626	-7391	132,496,149,371	283,807	466,853	cousin	Cousin
107	83	71	97	282872	-9385	80972465531	210,533	384607	Cousin	(8,9) $\frac{t}{b}=\frac{-97+9\pm 8}{16}$ $\frac{t}{b}$ $=-5$ o $\frac{-49}{8}$ $5^2+5+41=71$ $49^2+49*8+41*8^2=5417$
107	83	97	71	282,248	-8761	80337563003	386,839	207677	Cousin	(−5,4) $\frac{t}{b}=\frac{-71-5\pm 4}{-10}$ $\frac{t}{b}$ $=\frac{36}{5}$ o 8 $8^2-8+41=97$ $36^2-36*5+41*5^2=2141$
107	97	83	71	240,990	-9755	596,264,11451	285,017	209203	(4,73) $\frac{t}{b}=\frac{-83+4\pm 73}{8}$ $\frac{t}{b}$ $=\frac{-3}{4}$ o -19 $3^2+3*4+41*4^2=677$ $19^2+19+41=421$	Cousin
107	97	71	83	241110	-9875	59750739131	210533	283807	Cousin	Cousin
107	71	97	83	330212	-7717	108932701883	386,839	281597	Cousin	(3,76) $\frac{t}{b}=\frac{-83+3\pm 76}{6}$ $\frac{t}{b}$ $=\frac{-2}{3}$ o -26 $26^2+26+41=743$ $2^2+2*3+41*3^2=379$
107	71	83	97	330716	-8221	109424581691	285,017	383923	(4,73) $\frac{t}{b}=\frac{-83+4\pm 73}{8}$ $\frac{t}{b}$ $=\frac{-3}{4}$ o -19 $3^2+3*4+41*4^2=677$ $19^2+19+41=421$	Prime

Then $\frac{t}{b}=\frac{-b_2\pm v}{2x}$ with $\frac{t}{b}$ canonical fraction, then i $2t^2+pb^2$ $\frac{2t^2+pb^2}{2}$ o s a factor of $t_2^2+2pb_2^2$

➢ Application example 1.

Let $t_1=71$, $t_2=11$, $b_1=3$, $b_2=23$ y $p=29$

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

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

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

The polynomial number we are going to factor is:

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

By the above theorem, we can factor the polynomial number into the factors:

$2t_1^2+pb_1^2=2 * 71^2 + 29 * 3^2 =10343$

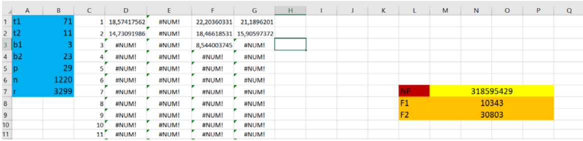
$t_2^2+2pb_2^2=11^2 + 2 * 29 * 23^2 = 30803$

To find the primality of the factors 10343 and or their complete factorization in case they are composite, we must use

$$f(x)=\sqrt{-2px^2+2*t_1x+b_1^2}=\sqrt{-58x^2+142x+9}$$

And $$g(x)=\sqrt{-2px^2+2*t_2x+b_2^2}=\sqrt{-58x^2+11x+529}$$

Using Excel, we find that:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	t1	71	1	18,57417562	#NUM!	22,20360331	21,1896201										
2	t2	11	2	14,73091986	#NUM!	18,46618531	15,90597372										
3	b1	3	3	#NUM!	#NUM!	8,544003745	#NUM!										
4	b2	23	4	#NUM!	#NUM!	#NUM!	#NUM!										
5	p	29	5	#NUM!	#NUM!	#NUM!	#NUM!										
6	n	1220	6	#NUM!	#NUM!	#NUM!	#NUM!										
7	r	3299	7	#NUM!	#NUM!	#NUM!	#NUM!					NP		318595429			
8			8	#NUM!	#NUM!	#NUM!	#NUM!					F1		10343			
9			9	#NUM!	#NUM!	#NUM!	#NUM!					F2		30803			
10			10	#NUM!	#NUM!	#NUM!	#NUM!										
11			11	#NUM!	#NUM!	#NUM!	#NUM!										

Therefore,10343 and30803 are both prime numbers. There are no integer points when applying the algorithms.

The complete factorization of 318595429 = 10343 * 30803 , that is, it is a semiprime.

- Application example 2.

Let 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

But, in addition: $t * = pb_1b_2 - t_1t_2 = 29 * 7 *11 - 3 * 5 = 2218$

$t^{**}=pl_1l_2 - 2k_1k_2 = 29 * 41 * 23 - 2 * (-13) * (-19) = 26853$

$r * = 2t_1b_2 + t_2b_1 = 2 * 3 * 11 + 5*7 = 101$

$r^{**}=k_1l_2+k_2l_1=(-13) * 23+(-19) * 41=-1078$

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

$r=2t_*r_{**}+t_{**}r_* = 2* 2218 * (-1078) + 26853 * 101 = -2069855$

Then:

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

Its factors are:

$2t_*^2+pr_*^2 = 2 * 2218^2 + 29 * 101^2 = 10134877$

$t_{**}^2 + 2pr_{**}^2 = 26853^2+ 2 * 29 * (-1078)^2 = 78848448$

That is:

$7991193231343837 = 10134877 * 788484481$

Furthermore, these factors can be factored:

$2 * t_1^2+p*b_1^2 = 2 * 3^2 + 29 * 72 = 1439$

$t_2^2 + 2p*b_2^2=5^2 + 58 * 11^2 = 7043$

And

$2 * k_1^2 + p * l_1^2 = 2 *(-13)^2 + 29 * 41^2 = 49087$

$2 * k_2^2 + p * l_2^2 = 2 *(-19)^2 +29 * 23^2 =16063$

Finally, to find out if these four factors are prime or composite, Cordero's algorithms must be used.

For the factor 1439 , and 7043, we obtain:

	A	B	C	D	E	F	G	L	M
1	t1	3	1	#NUM!	#NUM!	8,544003745	7,28010989		
2	t2	5	2	#NUM!	#NUM!	#NUM!	#NUM!		
3	b1	7	3	#NUM!	#NUM!	#NUM!	#NUM!		
4	b2	11	4	#NUM!	#NUM!	#NUM!	#NUM!		
5	p	29	5	#NUM!	#NUM!	#NUM!	#NUM!		
6	n	2218	6	#NUM!	#NUM!	#NUM!	#NUM!		
7	r	101	7	#NUM!	#NUM!	#NUM!	#NUM!	NP	10134877
8			8	#NUM!	#NUM!	#NUM!	#NUM!	F1	1439
9			9	#NUM!	#NUM!	#NUM!	#NUM!	F2	7043
10			10	#NUM!	#NUM!	#NUM!	#NUM!		
11			11	#NUM!	#NUM!	#NUM!	#NUM!		
12			12	#NUM!	#NUM!	#NUM!	#NUM!		

Both integers are prime, there are no integer points.

For the factors 49087 , and 16063, we obtain:

	A	B	C	D	E	F	G	J	L
1	t1	-13	1	39,63584237	40,92676386	19,8746069	23,3880311		
2	t2	-19	2	36,67424164	39,40812099	12,0415946	21,1896201		
3	b1	41	3	31,67017524	36,26292873	#NUM!	15,3297097		
4	b2	23	4	23,34523506	31	#NUM!	#NUM!	NP	788484481
5	p	29	5	#NUM!	22,15851981	#NUM!	#NUM!	F1	49087
6	n	26853	6	#NUM!	#NUM!	#NUM!	#NUM!	F2	16063
7	r	-1078	7	#NUM!	#NUM!	#NUM!	#NUM!		
8			8	#NUM!	#NUM!	#NUM!	#NUM!		

We obtain that 49087 is composite and 16063 is prime.

We have the integer point (- 4,31)

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

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

Then:

$$49087 = 257 * 191$$

The complete factorization of:

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

FACTORIZATION OF POLYNOMIAL NUMBERS OF THE FORM N^2+2PR^2

Let us consider polynomial numbers that have the structure $NP = n^2+2pr^2$ where r is an integer other than zero, p∊ {3, 5, 11, 29}, and n is an integer. If we are given four integers that are prime to each other, that is, the greatest common divisor between them is one, if we have that $tn=pb_1b_2-2t_1t_2$, and $r=t_1b_2+t_2b_1$, then the NP is composite and two of its factors have the form $2t_1^2+pb_1^2$, and $2t_2^2+pb_2^2$. All of the above can be described in the following theorem.

CORDERO'S POLYNOMIAL THEOREM (3).

Let $t_1, t_2, b_1, b_2 \in Z, b_1\neq 0, b_2\neq 0$, be relatively prime, and p∊ {3, 5, 11, 29 }.

If $n = pb_1b_2 - 2t_1t_2$ and $r = t_1b_2 + t_2b_1 \neq 0$, then $NP = n^2 + 2pr^2$ is composite and factors as $NP=(2t_1^2+pb_1^2)(2t_2^2+pb_2^2)$

Proof.

Let $NP=n^2 + 2pr^2$, considern$=pb_1b_2-2t_1t_2$ and $r=t_1b_2 + t_2b_1 \neq 0$,p∊ {3, 5, 11, 29 }.

We have that:

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

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

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

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

$NP = p^2b_12b_2^2 + 4t_1^2t_2^2 + 2pt_1^2b_2^2 + 2pt_2^2b_1^2$ (*)

On the other hand, we have:

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

From (*) y (**)

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

The theorem is proven.

ALGORITHMS FOR COMPLETELY FACTORING A $2T_1^2+PB_1^2$ Y $2T_2^2+PB_2^2$

The algorithm $f(x) = \sqrt{-2px^2 + 4 * t_1x + b_1^2}$ x ∊ Z, x≠0 determines whether the factor of NP-$2t_1^2+pb_1^2$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be $2t_1^2+pb_1^2$. If there exists at least one x ∊ Z, x≠0 such that f(x) = v ,v∊Z , then $2t_1^2+pb_1^2$ is a composite number; otherwise, the number $2t_1^2+pb_1^2$ is prime.

If $2t_1^2+pb_1^2$ is composite, then there exists at least one integer point (x, v).

Then $\frac{t}{b} = \frac{-b_1 \pm v}{2x}$ with $\frac{t}{b}$ canonical fraction, then is a factor of $2t_1^2+pb_1^2$

The algorithm $g(x) = \sqrt{-2px^2 + 4 * t_2x + b_2^2}$ determines whether the factor of NP $2t_2^2+pb_2^2$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be $2t_2^2+pb_2^2$. If there exists some x ∊ Z, x≠0 such that , , then is a composite number; otherwise, the number is prime.

If i $2t_2^2+pb_2^2$ s composite, then there exists an integer point (x, v).

Then $\frac{t}{b} = \frac{-b_2 \pm v}{2x}$ with $\frac{t}{b}$ canonical fraction, then is a factor of $2t^2+pb^2$ o $\frac{2t^2+pb^2}{2}$

- Application example 1

Let $t_1=61$, $t_2=71$, $b_1=31$, $b_2=23$ y $p=11$

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

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

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

The polynomial number we are going to factor is:

$NP = n^2 + 2pr^2 = (-819)^2 + 2 * 11 * 3604^2 = 286424713$

By the above theorem, we can factor the polynomial number into the factors:

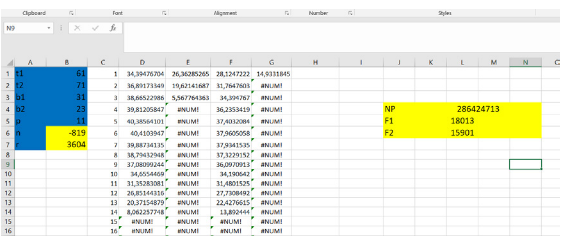
$2t_1^2 + pb_1^2 = 2 * 61^2 + 11 * 31^2 = 18013$
$2t_2^2 + pb_2^2 = 2 * 71^2 + 11 * 23^2 = 15901$

To find the primality of the factors 18013 and 15901 or their complete factorization in case they are composite, we must use

$$f(x) = \sqrt{-2px^2 + 4 * t_1 x + b_1^2} = \sqrt{-22x^2 + 244x + 961}$$

And $$g(x) = \sqrt{-2px^2 + 4 * t_2 x + b_2^2} = \sqrt{-22x^2 + 284x + 529}$$

Using Excel, we find that:



	A	B	C	D	E	F	G	J	L
1	t1	61	1	34,39476704	26,36285265	28,1247222	14,9331845		
2	t2	71	2	36,89173349	19,62141687	31,7647603	#NUM!		
3	b1	31	3	38,66522986	5,567764363	34,394767	#NUM!		
4	b2	23	4	39,81205847	#NUM!	36,2353419	#NUM!	NP	286424713
5	p	11	5	40,38564101	#NUM!	37,4032084	#NUM!	F1	18013
6	n	-819	6	40,4103947	#NUM!	37,9605058	#NUM!	F2	15901
7	r	3604	7	39,88734135	#NUM!	37,9341535	#NUM!		
8			8	38,79432948	#NUM!	37,3229152	#NUM!		
9			9	37,08099244	#NUM!	36,0970913	#NUM!		
10			10	34,6554469	#NUM!	34,190642	#NUM!		
11			11	31,35283081	#NUM!	31,4801525	#NUM!		
12			12	26,85144316	#NUM!	27,7308492	#NUM!		
13			13	20,37154879	#NUM!	22,4276615	#NUM!		
14			14	8,062257748	#NUM!	13,892444	#NUM!		
15			15	#NUM!	#NUM!	#NUM!	#NUM!		
16			16	#NUM!	#NUM!	#NUM!	#NUM!		

From the Excel table, we obtain that 18013 and 15901 are both prime numbers. There are no integer points.

➢ Application example 2

Let

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

But, in addition: $t_* = pb_1b_2 - t_1t_2 = 29 * 7 * 11 - 31 * 17 = 1706$

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

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

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

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

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

Then:

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

Its factors are:

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

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

That is:

$806069397354409 = 24427301 * 32998709$

Furthermore, these factors can be factored:

$2_*t_1^2 + p^*b_1^2 = 2 * 31^2 + 29 * 7^2 = 3343$
$t_2^2 + 2p^*b_2^2 = 17^2 + 2 * 29 * 11^2 = 7307$

And

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

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

Finally, to find out whether these four factors are prime or composite, Cordero's algorithms must be used.

For the factors 3343 , and 7307, we obtain:

Journal of Engineering Research ISSN 2764-1317 DOI https://doi.org/10.22533/at.ed.3175725170714

	A	B	C	D	E	F	G	L	M
1	t1	31	1	8,06225775	#NUM!	9,848857802	5,38516481		
2	t2	17	2	#NUM!	#NUM!	#NUM!	#NUM!		
3	b1	7	3	#NUM!	#NUM!	#NUM!	#NUM!		
4	b2	11	4	#NUM!	#NUM!	#NUM!	#NUM!		
5	p	29	5	#NUM!	#NUM!	#NUM!	#NUM!		
6	n	1706	6	#NUM!	#NUM!	#NUM!	#NUM!		
7	r	801	7	#NUM!	#NUM!	#NUM!	#NUM!	NP	24427301
8			8	#NUM!	#NUM!	#NUM!	#NUM!	F1	3343
9			9	#NUM!	#NUM!	#NUM!	#NUM!	F2	7307
10			10	#NUM!	#NUM!	#NUM!	#NUM!		
11			11	#NUM!	#NUM!	#NUM!	#NUM!		

Both integers are prime; there are no integer points.

For the factors 1063 , and 31043, we obtain:

	A	B	C	D	E	F	G	L	M
1	t1	-13	1	#NUM!	#NUM!	22,56102835	20,808652		
2	t2	19	2	#NUM!	#NUM!	19,31320792	14,8660687		
3	b1	5	3	#NUM!	#NUM!	11	#NUM!		
4	b2	23	4	#NUM!	#NUM!	#NUM!	#NUM!		
5	p	29	5	#NUM!	#NUM!	#NUM!	#NUM!		
6	n	3582	6	#NUM!	#NUM!	#NUM!	#NUM!		
7	r	-503	7	#NUM!	#NUM!	#NUM!	#NUM!	NP	32998709
8			8	#NUM!	#NUM!	#NUM!	#NUM!	F1	1063
9			9	#NUM!	#NUM!	#NUM!	#NUM!	F2	31043
10			10	#NUM!	#NUM!	#NUM!	#NUM!		

We obtain that 1063 is prime and 31043 is composite.

We have the integer point (3,11)

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

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

Then:

31043 = 37 * 839

The complete factorization of:

806069397354409 = 37 * 839 * 1063 * 3343 * 7307

BRAHMAGUPTA-FIBONACCI IDENTITY

The Brahmagupta-Fibonacci identity states that:

$(xu-nyv)^2 + n(xv + yu)^2 = (x^2 + ny^2)(u^2 + nv^2)$.

In other words:

$(nyv-xu)^2 + n(xv + yu)^2 = (x^2 + ny^2)(u^2 + nv^2)$

This identity can be used to factor polynomial numbers of the form n^2+2pr^2.

Substituting $n=2p$, $y=b_1$, $v=b_2$, $x=t_1$, $u=t_2$, we obtain:

CORDERO'S POLYNOMIAL THEOREM (4) (DEDUCED FROM THE BRAHMAGUPTA-FIBONACCI IDENTITY)

Let $t_1, t_2, b_1, b_2 \in Z, b_1 \neq 0, b_2 \neq 0$, be relatively prime, and $p \in \{3, 5, 11, 29\}$.

If $n = 2pb_1b_2 - t_1t_2$ and $r = t_1b_2 + t_2b_1 \neq 0$, then $NP = n^2 + 2pr^2$ is composite and factors as $NP = (t_1^2+2pb_1^2)(t_2^2+2pb_2^2)$.

Proof.

Let $NP = n^2 + 2pr^2$. Consider $n = 2pb_1b_2 - t_1t_2$ and $r = t_1b_2 + t_2b_1 \neq 0$,$p \in \{3, 5, 11, 29\}$.

We have that:

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

$NP = (2pb1b2 - t1t2)^2 + 2p(t1b2 + t2b1)^2$

$NP = (4p^2b_1^2b_2^2 - 4pb_1b_2t_1t_2+t_12t_2^2) + (2pt_1^2b_2^2+2t_1b_2t_2b_1+t_2^2b_1^2)$

$NP=4p^2b_1^2b_2^2-4pb_1b_2t_1t_2+t_12t_2^2+2pt_1^2b_2^2 + 4pt_1b_2t_2b_1+2pt_2^2b_1^2$

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

On the other hand, we have:

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

From(*) y (**)

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

The theorem is proven.

Journal of Engineering Research ISSN 2764-1317 DOI https://doi.org/10.22533/at.ed.3175725170714

ALGORITHMS FOR COMPLETELY FACTORING THE FACTORS $T_1^2+2PB_1^2$ Y $T_2^2+2PB_2^2$

The algorithm $f(x)=\sqrt{-2px^2+2*t_1x+b_1^2}$, $x\epsilon Z$, $x\neq 0$ determines whether the factor of NP $t_1^2+2pb_1^2$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be $t_1^2+2pb_1^2$. If there exists at least one such that $f(x) = v$,$v\epsilon Z$, , then $t_1^2+2pb_1^2$ is a composite number; otherwise, the number is prime.

If $t_1^2+2pb_1^2$ is composite, then there is at least one integer point (x, v).

Then $\frac{t}{b}=\frac{-b_1\pm v}{2x}$ with $\frac{t}{b}$ canonical fraction, then $2t^2+pb^2$ o $\frac{2t^2+pb^2}{2}$ is a factor of $t_1^2+2pb_1^2$

The algorithm $g(x)=\sqrt{-2px^2+2*t_2x+b_2^2}$ determines whether the factor of NP $t_2^2+2pb_2^2$ is prime or composite and how to deduce its complete factorization if it is composite.

Let the factor of NP be $t_2^2+2pb_2^2$. If there exists some $x\epsilon Z$, $x\neq 0$ such that $f(x) = v$,$v\epsilon Z$, , then $t_2^2+2pb_2^2$ is a composite number; otherwise, the number $t_2^2+2pb_2^2$ is prime.

If $t_2^2+2pb_2^2$ is composite, then there exists an integer point (x, v).

Then $\frac{t}{b}=\frac{-b_2\pm v}{2x}$ with $\frac{t}{b}$ canonical fraction, $2t^2+pb^2$ o $\frac{2t^2+pb^2}{2}$ then is a factor of $t_2^2+2pb_2^2$

- Application example 1

Let $t_1=61$, $t_2=71$, $b_1=31$, $b_2=23$ y $p=11$

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

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

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

The polynomial number we are going to factor is:

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

By the above theorem, we can factor the polynomial number into the factors:

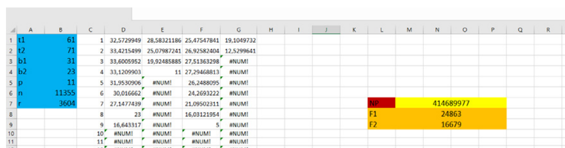
$t_1^2+2pb_1^2 = 61^2 + 2 * 11 * 31^2 = 24863$
$t_2^2 + 2pb_2^2 = 71^2 + 2 * 11 * 23^2 = 16679$

To find the primality of the factors 24863 and or their complete factorization in case they are composite, we must use

$f(x)=\sqrt{-2px^2+2*t_1x+b_1^2}=\sqrt{-22x^2+122x+961}$

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

Using Excel, we find that:



	A	B	C	D	E	F	G	L	N
1	t1	61	1	32,5729949	28,58321186	25,47547841	19,1049732		
2	t2	71	2	33,4215499	25,07987241	26,92582404	12,5299641		
3	b1	31	3	33,6005952	19,92485885	27,51363298	#NUM!		
4	b2	23	4	33,1209903	11	27,29468813	#NUM!		
5	p	11	5	31,9530906	#NUM!	26,2488095	#NUM!		
6	n	11355	6	30,016662	#NUM!	24,2693222	#NUM!		
7	r	3604	7	27,1477439	#NUM!	21,09502311	#NUM!	NP	414689977
8			8	23	#NUM!	16,03121954	#NUM!	F1	24863
9			9	16,643317	#NUM!	5	#NUM!	F2	16679
10			10	#NUM!	#NUM!	#NUM!	#NUM!		
11			11	#NUM!	#NUM!	#NUM!	#NUM!		

Therefore, 24863 y 16679 are both composite.

For 24863, we have the integer points: (8,23) y (-4,11).

Then:

$\frac{t}{b}=\frac{-31+23}{16}=\frac{-1}{2}$ $\frac{2*(-1)^2+11*2^2}{2}=23$ is a factor of 24863.

$\frac{t}{b}=\frac{-31-23}{16}=\frac{-27}{8}$ then $\frac{2*(-27)^2+11*8^2}{2}=1081$ is a factor of 24863.

$\frac{t}{b}=\frac{-31+11}{-8}=\frac{5}{2}$ then $\frac{2*(5)^2+11*2^2}{2}=47$ is a factor of 24863.

$\frac{t}{b}=\frac{-31-11}{-8}=\frac{21}{4}$ then $\frac{2*(21)^2+11*4^2}{2}=529$ is a factor of 24863.

The complete factorization of 24863 = 23*47*23 (the two smallest factors are taken and the third is obtained by division).

For 16679, we have the integer point: (9 ,5).

Then:

$\frac{t}{b} = \frac{-23+5}{18} = -1$ then $2 * (-1)^2 + 11 * 1^2 = 13$ is a factor of 16679.
$\frac{t}{b} = \frac{-23-5}{18} = \frac{-14}{9}$ then $2 * (-14)^2 + 11 * 9^2 = 1283$ is a factor of 16679.

The complete factorization of 16679=13*1283

Then the complete factorization of:

414689977 = 13 * 23 * 23 * 47 * 1283

IDENTITIES DERIVED FROM THEOREMS

The expression NP=N2+r-2N+pr2-r+1= $\frac{(2N+r-2)^2+(4p-1)r^2}{4}$

Let a, b, c, d y n = 4p-1 with
N = pab - ab - cd + cb + da + 1 y r = ab - cb - da

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

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

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

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

By Cordero's Polynomial Theorem(1)

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

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

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

Then:

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

I. First Cordero Identity

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

II. Second Identity of Lamb

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

Verification:

2(nab-cd)²+n(2cb+da)²=2(n2a2b2-2nabcd+c2d2)+n(4c2b2+4abcd+d2a2)
$=2n^2a^2b^2 - 4nabcd + 2c^2d^2 + 4nc^2b^2 + 4nabcd + nd^2a^2$
$=2n^2a^2b^2+2c^2d^2+4nc^2b^2+nd^2a^2$(*)

On the other hand:
$(2c^2+na^2)(d^2+2nb^2)=2c^2d^2 + 4nb^2c^2+na^2d^2+2n^2a^2b^2$(**)
From (*) and (**) we obtain that:

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

III. Third Cordero Identity

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

Verification:

$(nab-2cd)^2 + 2n(cb+da)^2 = (n^2a^2b^2-4nabcd+4c^2d^2)+2n(c^2b^2+2abcd+d^2a^2)$
=n2a2b2-4nabcd+4c2d2+2nc2b2+4nabcd+2nd2a2
$=n^2a^2b^2 + 4c^2d^2 + 2nc^2b^2 + 2nd^2a^2$(*)

On the other hand:

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

From (*) and (**) we obtain that:

$(nab-2cd)^2 + 2n(cb+da)^2 = (2c2 + na2)(2d^2 + nb^2)$

From (*) and (**) we obtain that:

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

IV. Brahmagupta-Fibonacci identity

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

$(nab-cd)^2+n(cb+da)^2 = (n^2a^2b^2-2nabcd+-c^2d^2) + n(c^2b^2+2abcd+d^2a^2)$
$=n^2a^2b^2-2nabcd+c^2d^2+nc^2b^2+2nabcd+n-d^2a^2$
$=n^2a^2b^2+c^2d^2+nc^2b^2+nd^2a^2$(*)
On the other hand:

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

From (*) and (**) we obtain that:

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

PRIME NUMBER GENERATOR WITH MORE THAN 100 DIGITS

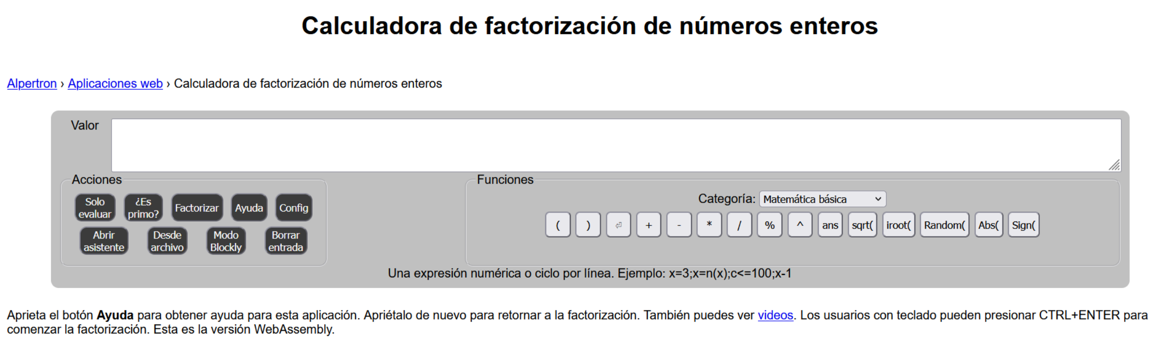
By Cordero's Polynomial Theorem (1)

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

If we take the factor:

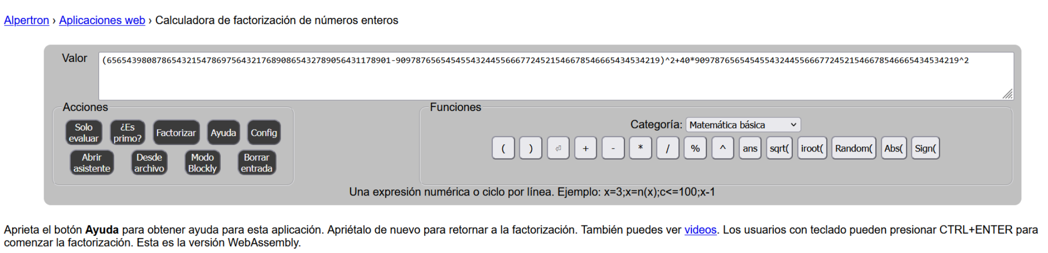
$(c^2 - ca + pa^2) = (c - a)^2+(p-1)a^2$

If we give large values to the variables c y a, *con p un número afortunado de Euler* , p$\in${2, 3, 5, 11, 17, 41}
We can find prime numbers with more than 100 digits, because the expression has few factors and these grow rapidly in the number of digits.
For this purpose, we use Darío Alpern's Calculator.



To begin with, let:
c = 65654398087865432154786975643217689 0865432789056431178901 = 90978765654545543 244556667724521546678546665434534219

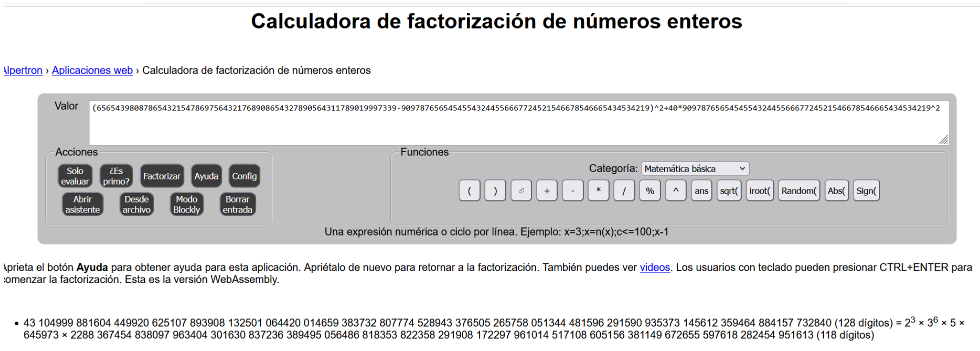
These are random numbers with p =41 . Calculating $(c-a)^2+(p-1)a^2$, we obtain:



Which initially generates the prime number:

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

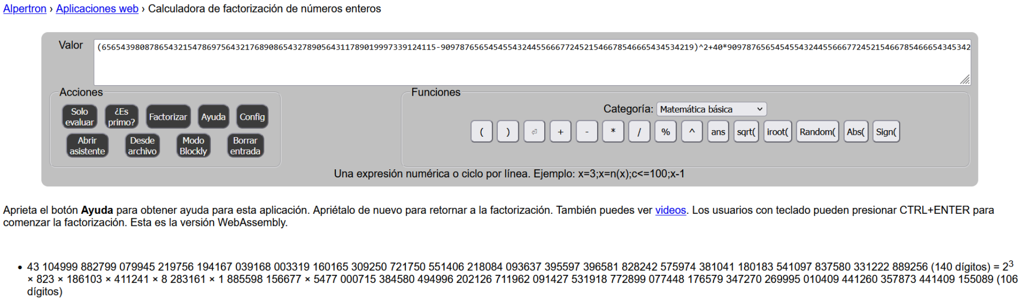
If we add more digits to c, so that the calculation does not go beyond 20-digit prime numbers, we obtain more large prime numbers.



Adding digits to c=…9997339 generates the prime number.

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

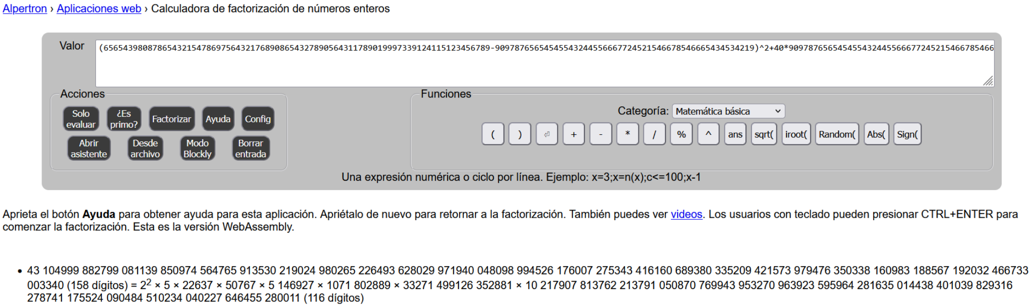
If you continue adding digits to c=…124115



You get the prime number:

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

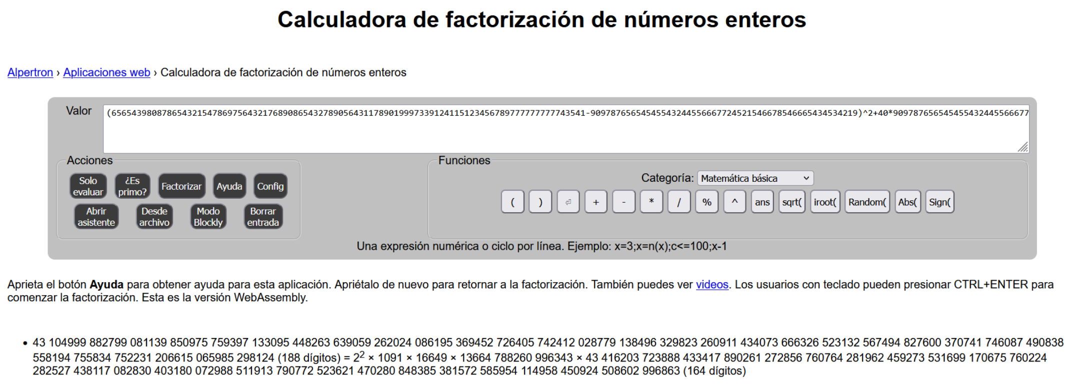
Again, adding more digits to



The prime number is obtained:

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

Again, if we add more digits to the value of c=…77777777743541



We obtain the prime number:

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 digits)

The process can be continued as far as the technology allows. The procedure makes it possible to quickly obtain prime numbers with more than 100 digits, using Darío Alpern's calculator and mathematician Ronald Cordero Méndez's formula. During the process, the value of can be varied, with 11, 17, and 41 being the most efficient for generating large prime numbers.

Using other values of c y a with p=41, prime numbers such as the following can be generated:

a) 759,050 592,899 752,060 564,706 105,636 755,615 85,360 293,660 512,843 479,011 292,689 78,293 297,564 877,805 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 digits)

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 964589,010,842 813,198 258,542 954,790 226,204 957,917 091,984 539,721 667,418 119,862 393,651 000,711 537,525 900,400 539899 (263 digits)

CONCLUSIONS

I. Cordero's theorems and algorithms seek to overcome the limitations of traditional methods in terms of speed and efficiency.

II. Cordero's research is not limited to theory alone; it extends to practical applications, such as the construction of software based on his algorithms to find prime numbers and factorize large composite numbers.

III. The research has implications for the search for prime numbers, even those with more than 100 digits.

IV. The research is a contribution to number theory that focuses on the creation of algorithmic and computational tools to address one of the oldest and most complex problems in mathematics: the factorization of integers.

REFERENCES

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.