Universidad Distrital Francisco José De Caldas
Facultad De Ingeniería
Ingeniería De Sistemas

Monografía

Desarrollo de un algoritmo para encontrar factores de números enteros de gran cantidad de cifras mediante una modificación del Binomio de Newton

Jhonathan Henao Barbosa
Código: 20022020202

Director: Ing. César Augusto Suárez Parra

Bogotá, Colombia

22 de mayo de 2017

AGRADECIMIENTOS

Agradezco la ayuda brindada para la implementación y realización de pruebas del algoritmo al centro de cómputo de alto desempeño -CECAD- en particular al profesor Rodolfo Cáliz Ospino, la cual fue de vital importancia para poder evaluar números de gran cantidad de cifras y el manejo de concurrencia. También agradezco la colaboración en la realización del presente documento al profesor Ing. César Augusto Suárez Parra y la profesora Isabel Barrera.

TABLA DE CONTENIDO

Desarrollo de un algoritmo para encontrar factores de números enteros de gran cantidad de cifras mediante una modificación del Binomio de Newton

I. Introducción

Anteriormente solo a los matemáticos parecía interesarles la factorización de números enteros de gran cantidad de cifras, pero desde ya hace varios años éste tema ha suscitado el interés fuera de la comunidad matemática, ya que en la comunicación que se desarrolla en internet, al transmitirse datos algunos desean garantizar la integridad, privacidad o autenticidad de los mismos, por lo que utilizan diferentes sistemas de cifrado que generalmente basan su seguridad en la dificultad de factorizar números enteros de cifras desorbitantes considerando como grandes los números de más de 100 dígitos decimales. [1]

A pesar del aumento de la capacidad en los computadores y diferentes desarrollos algorítmicos que han generado mejoras en cuanto al tiempo para factorizar enteros, cuando se intenta factorizar un número entero demasiado grande, este es un problema para el cual no hay disponibles métodos sencillos de obtener factores. Esto ha persuadido a la banca y al comercio electrónico de que confíen la seguridad de sus transacciones financieras a los tiempos increíblemente largos que hasta el momento ello requiere.

Los avances logrados en factorización de enteros se deben principalmente a la introducción de nuevas ideas en teoría de números, a desarrollos algorítmicos y al aumento en la capacidad de los computadores.

Este documento muestra una forma de hallar factores de números enteros utilizando una modificación propuesta del Binomio de Newton, que podría ayudar en la búsqueda de generar estrategias computacionales para poder hallar factores de números enteros de muchas cifras desde un computador personal, sin ser necesaria la ayuda de computación distribuida o el uso de equipos de gran capacidad.

II. Estado Del Arte

A. Antecedentes

En el área de programación se muestra que para ejecutar algoritmos que encuentren factores de números enteros extremadamente grandes se requiere utilizar computación distribuida, tener mucho tiempo disponible de cómputo, extensa capacidad de memoria y aplicar algoritmos complejos, esta dificultad ha sido aprovechada para desarrollar algoritmos de cifrado de clave pública, donde la descomposición de números enteros de cientos hasta miles de dígitos decimales en su representación prima forma la base teórica de varios de ellos, como el algoritmo RSA.

En ciencias de la computación, un algoritmo es eficiente si existe un polinomio p_n tal que el algoritmo pueda resolver cualquier problema de tamaño n en un tiempo que esta en $O(p_n)$ y se dice que son algoritmos de tiempo polinómico, $O(p_n)$ es una de las notaciones implementadas en análisis de algoritmos al estudiar teoría de la complejidad algorítmica. Se consideran problemas "NP" aquellos en los que la máquina no puede dar respuesta a un problema en un tiempo finito y no se conoce su nivel de complejidad. Problemas "P", en cambio, son todos los problemas de decisión que pueden ser resueltos en tiempo polinomial. Problemas complementarios "Co-NP" son los problemas que no se pueden considerar como P o NP.

En el caso del problema de factorización de números enteros no se conoce exactamente las clases de complejidad que contienen, se sabe que tienen complejidad NP y Co-NP y se considera improbable resolverlos en tiempo polinomial. P versus NP es considerado uno de los siete problemas del milenio, es un problema central de las ciencias de la computación y de especial

importancia para los sistemas criptográficos utilizados en la actualidad, ya que desarrollos de algoritmos de factorización eficientes romperían esquemas de cifrado de clave pública, comúnmente utilizados para proteger transacciones financieras a través de internet.

Algunos registros históricos evidencian la dificultad que ha existido para factorizar números enteros grandes, es así como en 1874, W. Jevons Stanley un economista inglés, indicó que nadie sabría nunca los factores del entero de 10D (D hace referencia a la cantidad de dígitos decimales), en particular del número 8616460799. Sin embargo, Bancroft Brown, aproximadamente en 1925 lo pudo lograr, lo cual quedó registrado en un documento donde Brown explica cómo obtuvo la factorización de dicho número entero. [2]

En 1967, John Brillhart y John Selfridge declararon que: "... en general nada más que frustración se puede esperar en un ataque para factorizar un número de 25 dígitos o más, incluso con las velocidades disponibles en las computadoras modernas." Pero en 1970 Mike Morrison y John Brillhart lograron factorizar un número entero de 39D. De acuerdo con John Brillhart, la factorización de enteros, en los computadores de esa época, requería por lo general alrededor de una hora de tiempo de CPU, lo cual se ha valorado en 1 - 10 MIPS [3]; MIPS significa millones de instrucciones por segundo y MIPS-AÑO el número de instrucciones ejecutadas en un año de cómputo de un millón de Instrucciones por segundo.

La tabla I resume los avances que ocurrieron en la factorización de números enteros desde 1964 hasta 1994. [2]

TABLA I. RÉCORDS HISTÓRICOS EN LA FACTORIZACIÓN DE NÚMEROS ENTEROS

Año	Récord de Factorización
1964	20D
1974	45D
1984	71D
1994	129D

La tabla II muestra como aumentó la cantidad de potencia de cálculo disponible para factorización de enteros desde 1974 hasta 1994. [2]

TABLA II. PODER COMPUTACIONAL USADO PARA LOGRAR RECORDS EN FACTORIZACIÓN

Año	MIPS-AÑO
1974	0.001
1984	0.1
1994	5000

A pesar de las mejoras en ideas matemáticas, el aumento de potencia de cómputo, diferentes algoritmos utilizados y el respaldo de la computación distribuida, si se habla de factorizar enteros de centenas y más aún de miles de dígitos decimales aún hoy en día es computacionalmente complejo.

B. Algoritmos de Factorización

La descomposición de grandes números enteros es un problema difícil, debido a la imposibilidad de que exista un programa computacionalmente eficiente capaz de factorizar grandes números y a la aleatoriedad de la distribución de los números primos; no existe un procedimiento matemático que permita en un tiempo relativamente corto encontrar un número primo de una cantidad considerable de cifras, lo cual dificulta la descomposición en factores primos para números muy grandes. Uno de los casos más complicados de factorización se presenta cuando el número grande a factorizar es el producto de dos números primos grandes de aproximadamente el mismo tamaño.

Uno de los problemas del Milenio, según Landon T. Clay, se conoce como *P versus NP*, [4], muestra como la complejidad del problema de factorización de números enteros de muchas cifras se deriva en la cantidad de cálculos que son necesarios para hallar los factores de un número, de lo cual se plantea el siguiente interrogante: ¿existirá un método eficiente para realizar dicha búsqueda?

Con el aumento de la importancia comercial de los sistemas de cifrado que utilizan la dificultad de descomponer números en su factorización prima, surge el interés de la comunidad matemática sobre las implicaciones prácticas que tendría el descubrimiento de un método eficiente para encontrar los números primos de esta descomposición, ya que esto generaría un caos en las transacciones en línea. [5]

A continuación, se describen algunos métodos de factorización basados en avances algorítmicos y mejoras en la capacidad computacional, con los cuales se ha logrado factorizar números de muchas cifras, pero con un tiempo de ejecución muy grande.

1) Método p-1 de Pollard

El método p-1 de Pollard formalizó varias reglas que ya se conocían, este método se resume dados los siguientes pasos: [6]

1. El número *N* a hallarle los factores es un número perteneciente a los números naturales.
2. Su respuesta debe ser los divisores de *N* o el algoritmo no encontró factores.
3. Se toma una base de primos consecutivos $B = \{2,3,5, \dots q_t\}$.
4. Selecciona un número aleatorio *a* tal que $2 \leq a \leq N-1$, luego calcula $d = mcd(a,\ N)$, si $d \geq 2$, d es un factor de N.
5. Para cada q_i se calcula la parte entera $l = \left\lfloor \frac{lnN}{lnq_i} \right\rfloor$ con $i = 1,2, \dots, t$.
6. Calcular $d = mcd\ (a-1, N)$. Si $d = 1$ o $d = N$, entonces el algoritmo no encontró factores.

2) Método de Pollard-rho

El método de Pollard-rho, también conocido como el segundo método de factorizar de Pollard, se basa en ideas estadísticas. Los conceptos involucrados para encontrar el factor *p* del número *N* se describen a continuación: [7]

1. Construir una secuencia de números enteros $\{x_i\}$ que es periódicamente recurrente *mod p*. (Esto significa que la secuencia $\{x_i\}$ se repite periódicamente, excepto posiblemente para una parte al principio de la secuencia que puede variar, llamada parte aperiódica. A continuación, se presenta como ejemplo la secuencia Fibonacci *mod* 11, esta secuencia se define en (1):

$$x_i = x_{i-1} + x_{i-2} mod\ 11, con\ x_1 = x_2 = 1 \quad (1)$$

   a. Se obtienen los siguientes elementos de la secuencia:

$$1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, 2, 3, \dots mod\ 11$$

   b. Después de 10 elementos la secuencia se repite. Dado que esta secuencia particular se repite desde el principio, no tiene parte aperiódica.

2. Buscar el periodo de la secuencia y encontrar i y j tales que $x_i = x_j mod\ p$. Se debe tener en cuenta que generalmente encontrar esta secuencia involucra una gran cantidad de trabajo.
3. Identificar el factor *p* de *N*.

El método rho de Pollard se hizo aproximadamente un 25% más rápido por una modificación debido a Brent. Brent y Pollard en 1980 lograron descubrir el factor 1238926361552897 del número de Fermat F_8 El cálculo tomó un par de horas en un ordenador grande. [6]

3) Método de factorización de formas cuadráticas SQUFOF (Square Form factorization)

Otro de los métodos de factorización modernos es el método de Shanks o "factorización de formas cuadráticas" (SQUFOF). Gauss fue el primero en aplicar sistemáticamente la teoría de las formas cuadráticas binarias para encontrar factorizaciones de enteros (expresiones de la forma $Ax^2 + Bxy + Cy^2$).

El método SQUFOF de Shanks hace uso de la expansión de fracción continua regular de $\sqrt{N}$. La fórmula $A_{n-1}^2 = (-1)^n Q_n mod\ n$ se aplica para resolver la congruencia de Legendre $x^2 = y^2 mod\ N$. La idea de buscar un cuadrado en la expansión de la fracción continua de $\sqrt{N}$ es en realidad muy antigua, pero su uso en forma eficaz se debió a la llegada de las computadoras, por la dificultad de encontrar potencias cuadradas de números grandes. [7]

La tabla III muestra aproximadamente la equivalencia entre dígitos del número y los bits que ocupa ese número.

TABLA III. EQUIVALENCIA DE DÍGITOS DECIMALES DEL NÚMERO Y LOS BITS QUE EL NÚMERO OCUPA

Bits del número	Dígitos Decimales
330 Bits	100 dígitos aproximadamente
496 Bits	150 dígitos aproximadamente
512 Bits	155 dígitos aproximadamente
1024 Bits	309 dígitos aproximadamente
2048 Bits	617 dígitos aproximadamente

Fuente: El autor

Se han desarrollado estrategias bien equilibradas, basadas en una amplia experiencia informática, pero también se han cambiado cada vez que se introduce un nuevo método, por lo que cabe hacerse la pregunta ¿se podrían idear métodos de factorización mucho más rápidos que los que existen en la actualidad?

III. ALGORITMO PROPUESTO

A. Modificación del Binomio de Newton

Entendiendo la relación que tiene la fórmula del Binomio de Newton y la ecuación del cuadrado de la suma de dos cantidades, ésta última ecuación provee una plataforma natural a partir de la cual se desarrolla la metodología que se propone, uniendo diferentes definiciones existentes tanto en el álgebra como en la aritmética, se propone una forma diferente para hallar el cuadrado de la suma de dos cantidades de un número.

Para explicar el algoritmo se comienza con números menores a 100, luego se trabaja con números mayores a 100 y menores a 1000 y así sucesivamente hasta explicar la forma en la que se puede hallar la potencia cuadrada de un número de cualquier cantidad de cifras con el método propuesto.

Teniendo en cuenta que la ecuación del cuadrado de la suma de dos cantidades es un caso particular del Binomio de Newton, se propone una nueva forma para hallar cualquier potencia entera positiva a partir de una modificación del Binomio de Newton. [8]

En la siguiente sección se detalla el algoritmo para encontrar factores de números enteros de gran cantidad de cifras, que se desarrolló.

El Binomio de Newton es una fórmula que permite elevar un binomio a una potencia cualquiera entera y positiva [9], la cual se describe en la ecuación (3).

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \tag{3}$$

Un caso particular de esta fórmula, se presenta cuando el valor de la potencia n-ésima es igual a 2, que corresponde al desarrollo de la ecuación del cuadrado de la suma de dos cantidades, ver ecuación (4).

$$(x+y)^2 = \sum_{k=0}^{2} \binom{2}{k} x^{2-k} y^k$$

$$(x+y)^2 = \binom{2}{0} x^{2-0} y^0 + \binom{2}{1} x^{2-1} y^1 + \binom{2}{2} x^{2-2} y^2$$

$$(x+y)^2 = (1)(x)^2(1) + (2)(\mathrm{x})(\mathrm{y}) + (1)(1)(y)^2$$

$$(x+y)^2 = (x)^2 + 2(\mathrm{x})(\mathrm{y}) + (y)^2 \tag{4}$$

En la cual elevar al cuadrado $x + y$ equivale a multiplicar el binomio por sí mismo, dando por resultado el cuadrado de la primera cantidad más el duplo de la primera cantidad por la segunda cantidad más el cuadrado de la segunda cantidad. [8]

Visualizando la ecuación del cuadrado de la suma de dos cantidades como se muestra en (5).

$$(d+u)^2 = (d)^2 + 2(d)(u) + (u)^2 \tag{5}$$

Donde las variables *d* y *u* hacen referencia a decenas y unidades, segundo y primer orden en el estudio del sistema decimal. Hasta el momento se está hallando la potencia cuadrada de un número compuesto por dos cifras.

El siguiente cambio se visualiza gracias a la regla práctica para extraer la raíz cuadrada de un número mayor a 100. Se cambian los signos de operación de suma presentes en la ecuación por comillas dividiendo la ecuación en grupos.

Puede notarse que en la parte derecha de la igualdad ($= (d)^2 \ ' \ 2(d)(u) \ ' \ (u)^2$), quedan separados tres grupos, donde de derecha a izquierda el primer grupo sería el cuadrado de la unidad, $(u)^2$, el segundo grupo sería el duplo multiplicado por la decena multiplicado por la unidad, $2(d)(u)$, y el tercer grupo sería el cuadrado de la decena, $(d)^2$.

En la parte izquierda de la igualdad ($(d \ ' \ u)^2 =$), quedan separados dos grupos, donde de izquierda a derecha se separa con una comilla el orden superior del número, para éste caso la decena. El otro grupo son los órdenes inferiores faltantes del número, para éste caso, la unidad.

Lo dicho anteriormente se puede visualizar en (6)

$$(d \ ' \ u)^2 = (d)^2 \ ' \ 2(d)(u) \ ' \ (u)^2 \tag{6}$$

Se agrega ahora la definición aritmética de valor absoluto y relativo de cifra. Toda cifra tiene dos valores: absoluto y relativo; valor absoluto es el que tiene el número por su figura, y valor relativo es el que tiene el número por el lugar que ocupa [10]. Donde esté presente en la ecuación el orden superior del número, para éste caso la decena, se representará en valor absoluto de cifra, tomando la representación del número por su figura y no por el lugar que ocupa.

Los órdenes inferiores restantes, que para éste caso son las unidades, se representará en valor relativo de cifra, tomando la representación del número por el lugar que ocupa y no por su figura.

Los cambios propuestos anteriormente se pueden visualizar en (7) en color rojo

$$(d_{absoluto} + u_{relativo})^2 = (d_{absoluto})^2 + 2(d_{absoluto})(u_{relativo}) + (u_{relativo})^2 \quad (7)$$

Para el cálculo de la ecuación del cuadrado de la suma de dos cantidades visto de ésta manera, se implementan pasos presentes en el algoritmo de multiplicación.

Para poder hallar el cuadrado del número en la ecuación anterior se empiezan a realizar los cálculos de los grupos de derecha a izquierda en la parte derecha de la igualdad. Se empieza evaluando el primer grupo $(u_{relativo})^2$ y de dicho resultado se toman las unidades, que pasan a ser parte de la respuesta mientras las decenas son acarreadas. Ver Figura 1

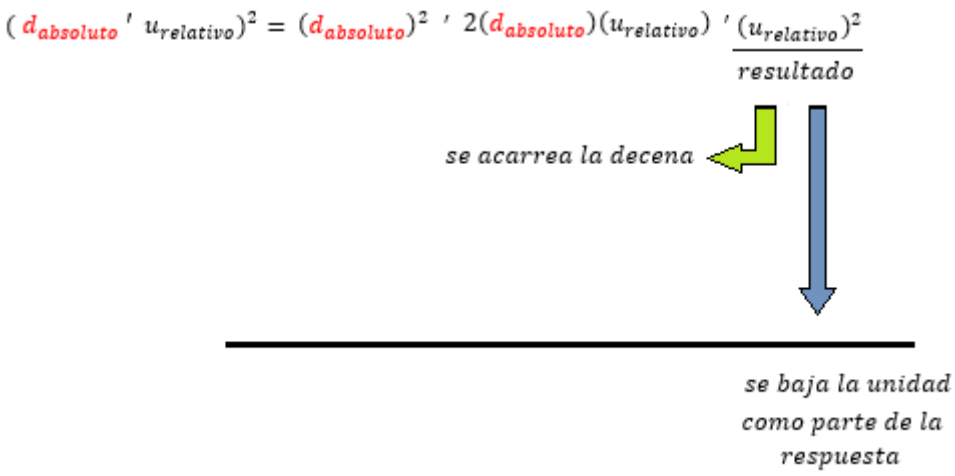


Figura 1: Evaluación del primer grupo de la modificación del cuadrado de la suma de dos cantidades para un número menor a 100.

Luego, se calcula el segundo grupo $2(d_{absoluto})(u_{relativo})$, y a ese resultado se le suma el acarreo proveniente del primer grupo. Del número que se obtiene de dicha suma, la unidad pasará a ser parte de la respuesta, mientras lo demás será utilizado como acarreo. Lo descrito anteriormente se puede visualizar en la Figura 2:

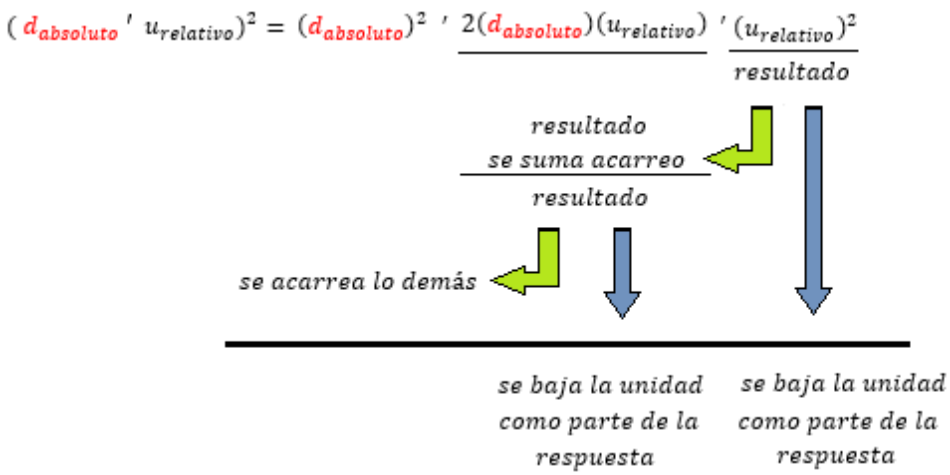


Figura 2: Evaluación del segundo grupo de la modificación del cuadrado de la suma de dos cantidades para un número menor a 100.

Para finalizar, se calcula el resultado del tercer grupo $(d_{absoluto})^2$, al cual se le suma el acarreo proveniente del segundo grupo; el número total resultante de esta suma se anexa como parte de la respuesta.

La Figura 3 muestra el proceso anteriormente descrito.

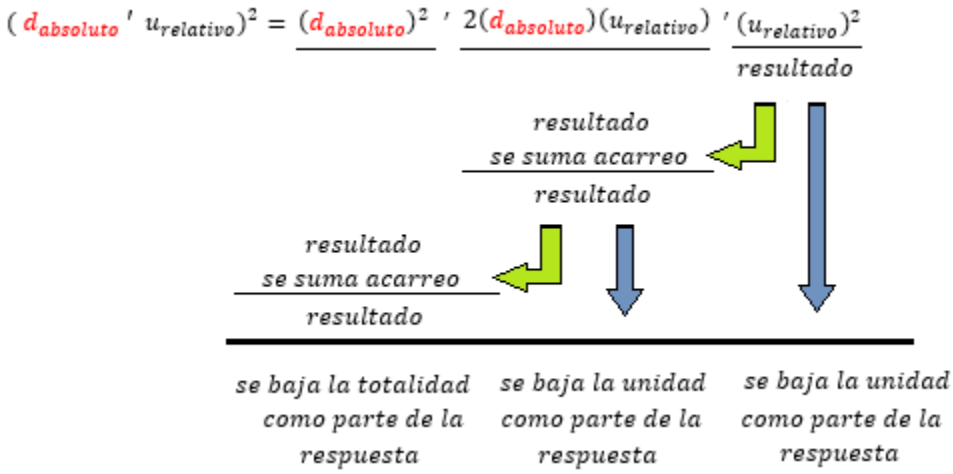


Figura 3: Evaluación del tercer grupo de la modificación del cuadrado de la suma de dos cantidades para un número menor a 100.

La concatenación de las tres respuestas conforma el cuadrado del número de dos cifras que se estaba evaluando.

Ejemplo 1:

Hallar $(37)^2$ utilizando el método propuesto. Como primer paso, escribir la ecuación del cuadrado de la suma de dos cantidades como se muestra en (8)

$$(30+7)^2 = (30)^2 + 2(30)(7) + (7)^2 \quad (8)$$

Dividir dicha ecuación en grupos, cambiando los signos de operación de suma por unas comillas, esto se observa en (9)

$$(30\ '\ 7)^2 = (30)^2\ '\ 2(30)(7)\ '\ (7)^2 \tag{9}$$

En donde esté presente en la ecuación el orden superior del número, representado para éste ejemplo como el número 30, tomar ahora su representación en valor absoluto de cifra. El número quedaría representado por su figura y no por el lugar que ocupa, convirtiéndose el número 30 en el número 3 como se observa en (10), en color rojo

$$(3\ '\ 7)^2 = (3)^2\ '\ 2(3)(7)\ '\ (7)^2 \tag{10}$$

En la ecuación se ubica al lado derecho de la igualdad empezando a realizar los cálculos de derecha a izquierda, evaluando entonces el primer grupo $(u_{relativo})^2$. Para éste ejemplo es $(7)^2 = 49$, del cual se toma la unidad como parte de la respuesta, el número 9, y se acarrea la decena, el número 4, para sumarlo con la evaluación del segundo grupo. En la Figura 4 se ilustra lo descrito anteriormente.

$$(d_{absoluto}\ '\ u_{relativo})^2 = (d_{absoluto})^2\ '\ 2(d_{absoluto})(u_{relativo})\ '\ (u_{relativo})^2$$

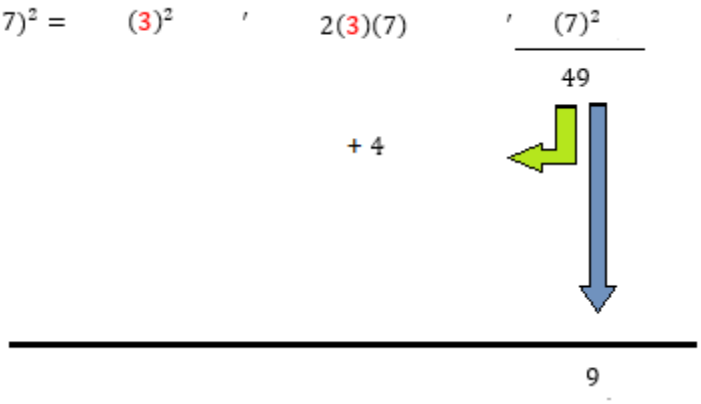


Figura 4: Evaluación del primer grupo de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por decenas y unidades.

Luego, se calcula el resultado del segundo grupo $2(d_{absoluto})(u_{relativo})$, que para el ejemplo es igual a $2(3)(7)=42$. A ese resultado se le suma el acarreo proveniente del primer grupo, el número 4, para formar el número 46, del que será parte de la respuesta la unidad, el número 6, y se acarrea el 4 para sumarlo a la evaluación del tercer grupo. Ver la Figura 5

$$(d_{absoluto}\ '\ u_{relativo})^2 = (d_{absoluto})^2\ '\ 2(d_{absoluto})(u_{relativo})\ '\ (u_{relativo})^2$$

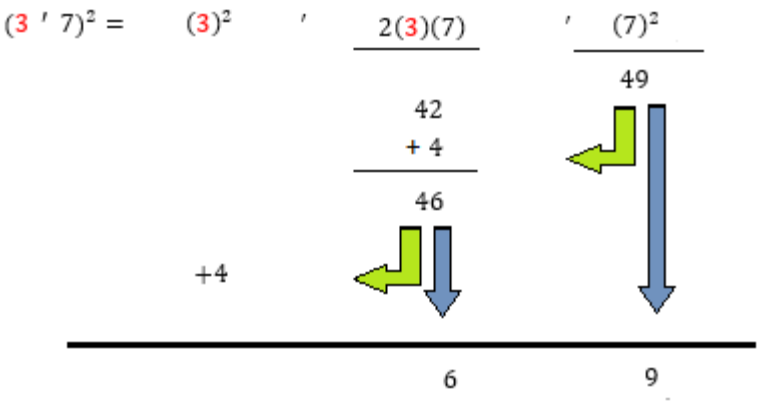


Figura 5: Evaluación del segundo grupo de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por decenas y unidades.

Por último, se evalúa el tercer grupo $(d_{absoluto})^2$, siendo para el ejemplo $(3)^2 = 9$, y se le suma el acarreo proveniente del segundo grupo, el número 4, dando como resultado el número 13 que baja en su totalidad a ser parte de la respuesta, como se presenta en la Figura 6.

$$(d_{absoluto}\ '\ u_{relativo})^2 = (d_{absoluto})^2\ '\ 2(d_{absoluto})(u_{relativo})\ '\ (u_{relativo})^2$$

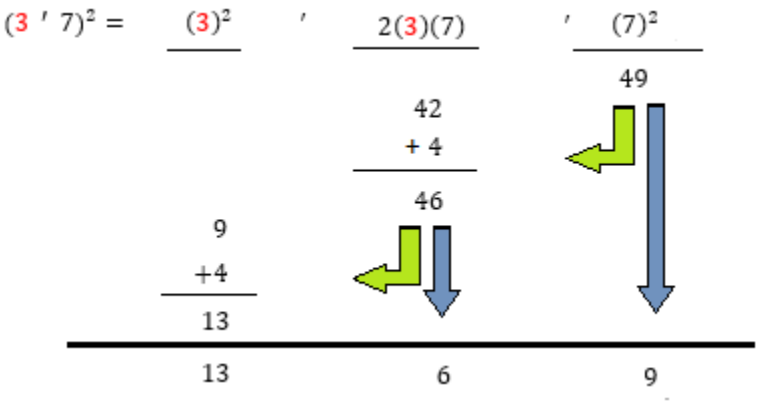


Figura 6: Evaluación del tercer grupo de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por decenas y unidades.

Las tres respuestas concatenadas forman el cuadrado del número 37 que es igual a 1369.

Si se evalúa la potencia cuadrada de números de más cifras, como por ejemplo uno conformado por centenas *c*, decenas y unidades *du*, en la parte izquierda de la igualdad la ecuación quedaría $((c\ '\ du)^2 =)$, separando el número en dos grupos, donde de izquierda a derecha se separa con una comilla el orden superior del número, para éste caso la centena. El otro grupo son los órdenes inferiores faltantes del número, para éste caso, la decena y la unidad.

En la parte derecha de la igualdad la ecuación quedaría $(= (c)^2 \prime 2(c)(du) \prime (du)^2)$, quedando nuevamente separados en tres grupos, donde de derecha a izquierda el primer grupo sería el cuadrado de la decena y la unidad, $(du)^2$, el segundo grupo sería el duplo multiplicado por la decena multiplicado por la unidad, $2(c)(du)$, y el tercer grupo sería el cuadrado de la decena, $(du)^2$.

El orden superior del número a hallarle el cuadrado se representa en valor absoluto de cifra, la centena, y las decenas y unidades toman su representación en valor relativo de cifra. Los cambios propuestos anteriormente para números compuestos por centenas *c*, decenas y unidades *du*, se pueden visualizar en (11), en color rojo

$$(c_{absoluto} \prime du_{relativo})^2 = (c_{absoluto})^2 \prime 2(c_{absoluto})(du_{relativo}) \prime (du_{relativo})^2 \quad (11)$$

Cambia la interpretación de cómo se escogen los números pertenecientes a las respuestas y a los acarreos, dependiendo la cantidad de cifras que tenga el número a hallarle la potencia cuadrada se tomarán la cantidad de cifras menos uno para las respuestas.

A manera de ejemplo, se desea calcular $(513)^2$ con el método propuesto. De forma análogo al ejemplo anterior, primero debe escribirse la ecuación del cuadrado de la suma de dos cantidades como se muestra en (12)

$$(500 + 13)^2 = (500)^2 + 2(500)(13) + (13)^2 \quad (12)$$

A continuación, dividir dicha ecuación en grupos, cambiando los signos de suma por unas comillas, como se ve en (13)

$$(500 \prime 13)^2 = (500)^2 \prime 2(500)(13) \prime (13)^2 \quad (13)$$

En donde esté presente en la ecuación el orden superior del número, representado para éste ejemplo como el número 500, tomar ahora su representación en valor absoluto de cifra. El número quedaría representado por su figura y no por el lugar que ocupa, convirtiéndose el número 500 en el número 5 como se muestra en (14), en color rojo

$$(5 \prime 13)^2 = (5)^2 \prime 2(5)(13) \prime (13)^2 \quad (14)$$

En la ecuación se ubica al lado derecho de la igualdad empezando a realizar los cálculos de derecha a izquierda, evaluando entonces el primer grupo $(13)^2 = 169$, del cual se toma la decena y la unidad como parte de la respuesta, el número 69, y se acarrea la centena, el número 1 para sumarlo con la evaluación del segundo grupo.

Para éste caso se toman de los resultados de la evaluación las decenas y las unidades como parte de la respuesta. La Figura 7 muestra este proceso

$$(c_{absoluto} \prime du_{relativo})^2 = (c_{absoluto})^2 \prime 2(c_{absoluto})(du_{relativo}) \prime (du_{relativo})^2$$

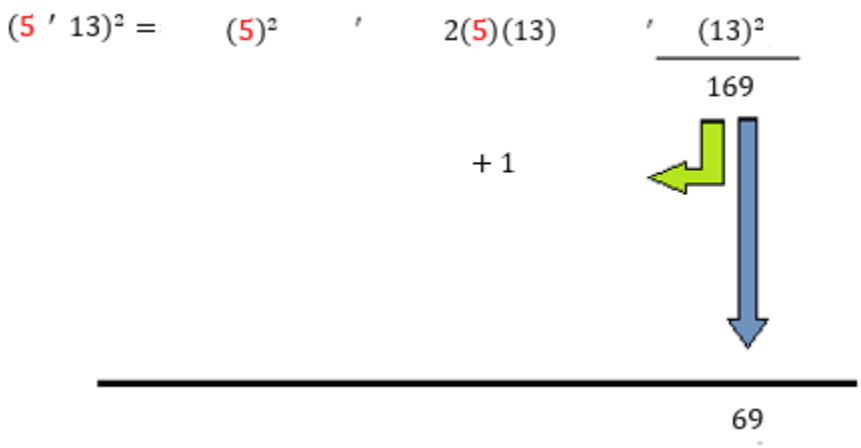


Figura 7: Evaluación del primer grupo de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por centenas, decenas y unidades.

Luego, se calcula el resultado del segundo grupo $2(5)(13) = 130$; a ese resultado se le suma el acarreo proveniente del primer grupo, el número 1, para formar el número 131, del que será parte de la respuesta la decena y la unidad, el número 31, y se acarrea el 1 para sumarlo a la evaluación del tercer grupo. Lo anteriormente descrito se observa en la Figura 8.

$$(c_{absoluto} \ ' \ du_{relativo})^2 = (c_{absoluto})^2 \ ' \ 2(c_{absoluto})(du_{relativo}) \ ' \ (du_{relativo})^2$$

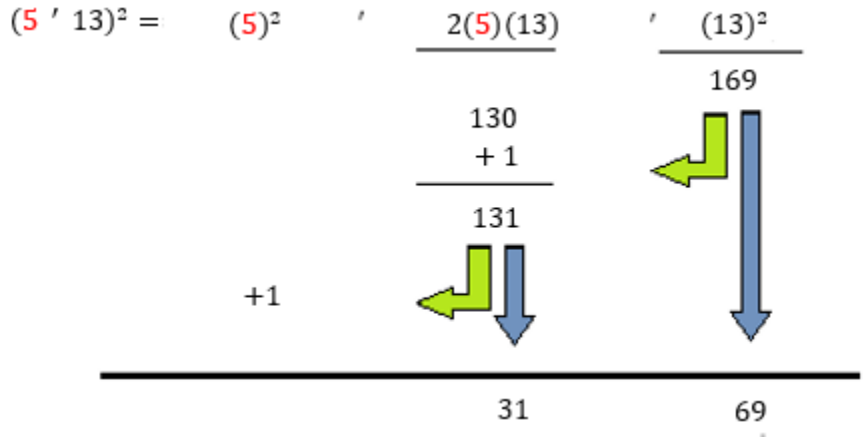


Figura 8: Evaluación del segundo grupo de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por centenas, decenas y unidades.

Por último, se evalúa el tercer grupo $(5)^2 = 25$. Se le suma el acarreo proveniente del segundo grupo, el número 1, dando como resultado el número 26 que pasa en su totalidad a ser parte de la respuesta. Esto se muestra en la Figura 9.

$$(c_{absoluto} \ ' \ du_{relativo})^2 = (c_{absoluto})^2 \ ' \ 2(c_{absoluto})(du_{relativo}) \ ' \ (du_{relativo})^2$$

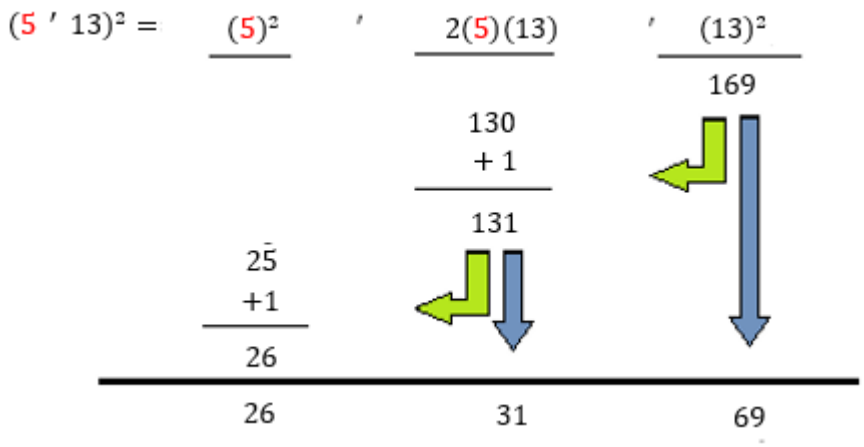


Figura 9: Evaluación del tercer grupo de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por centenas, decenas y unidades.

Las tres respuestas concatenadas forman el cuadrado del número 513 que es igual a 263169.

Dependiendo la cantidad de cifras que tenga el número a hallarle la potencia cuadrada se determina la cantidad de cifras que se escogen de los resultados para que sean parte de las respuestas. Cuando el número a hallarle la potencia está compuesto de dos cifras (decenas y unidades) se toma de los resultados la cantidad de cifras del número menos uno, es decir, se toma como parte de las respuestas solo las unidades. Si el número a hallarle la potencia estaba compuesto por tres cifras (centenas, decenas y unidades) se toma de los resultados la cantidad de cifras que tiene el número menos uno, es decir, se toma como parte de las respuestas solo las decenas y unidades. Este patrón se sigue utilizando así el número a hallarle la potencia cuadrada tenga más cifras.

Por ejemplo, al hallar la potencia cuadrada del número 8379 que está compuesto por unidades de mil, centena, decena y unidad, es decir cuatro cifras, se toman para formar las respuestas de los resultados 4 cifras menos uno, es decir, 3 cifras. En la Figura 10 se presenta el procedimiento en forma completa.

$$(m_{absoluto} \ ' \ cdu_{relativo})^2 = (m_{absoluto})^2 \ ' \ 2(m_{absoluto})(cdu_{relativo}) \ ' \ (cdu_{relativo})^2$$

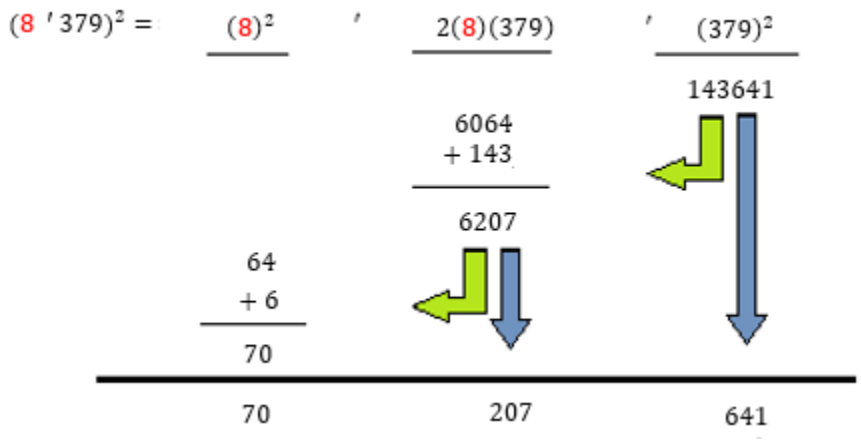


Figura 10: Evaluación completa de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por unidades de mil, centenas, decenas y unidades.

Entendiendo esta forma para hallar potencias cuadradas, se separa el número a hallarle la potencia cuadrada en dos partes. La primera parte es el orden superior del número representado en valor absoluto de cifra como la variable $x_{absoluto}$; la segunda parte son los órdenes inferiores faltantes del número representados en valor relativo de cifra como la variable $y_{relativo}$.

Dependiendo la cantidad de cifras que tenga $y_{relativo}$, se determinan los números pertenecientes a las respuestas y a los acarreos de los resultados, como se muestra en la Figura 11.

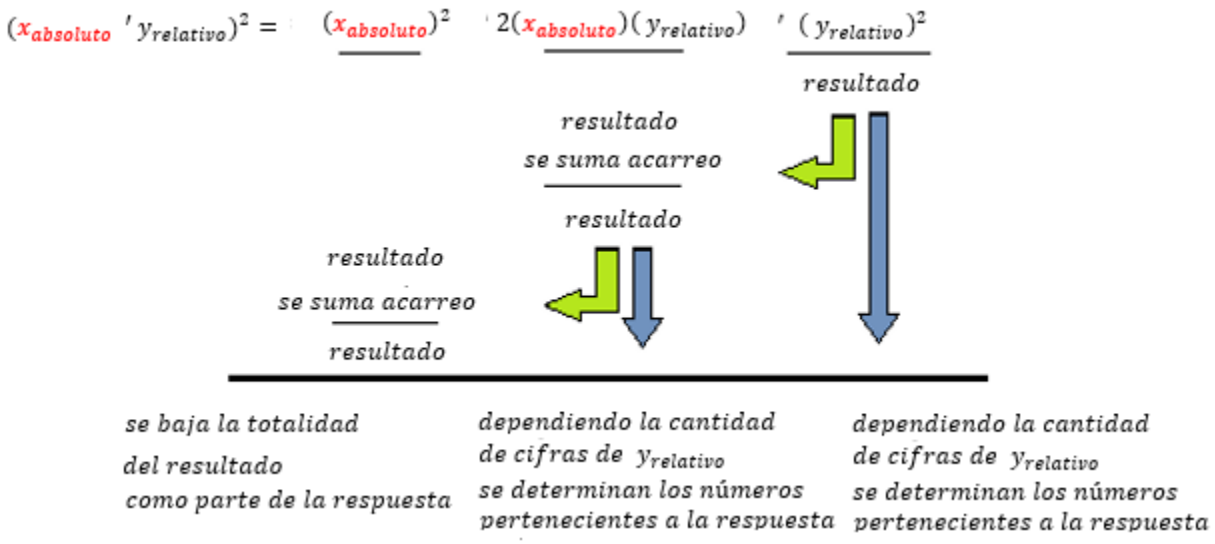


Figura 11: Evaluación completa de la modificación del cuadrado de la suma de dos cantidades para un número de cualquier cantidad de dígitos.

Por ejemplo, al hallar la potencia cuadrada del número 98379 que está compuesto por decenas de mil, unidades de mil, centena, decena y unidad, el valor de $x_{absoluto}$ es el orden superior del numero a hallarle la potencia cuadrada, las decenas de mil, representadas en valor absoluto de cifra $dm_{absoluto}$. Los órdenes inferiores faltantes (unidades de mil, centena, decena y unidad) serían $y_{relativo}$ representados en valor relativo de cifra $mcdu_{relativo}$. Dependiendo la cantidad de cifras de $y_{relativo} = mcdu_{relativo}$ se determinan los números pertenecientes a la respuesta. Como está compuesto por unidad de mil, centena, decena y unidad, se toman para formar las respuestas de los resultados cuatro cifras. Luego se forma con las tres respuestas unidas la potencia cuadrada del número 98379 que es igual a 9678427641. En la Figura 12 se ilustra todo el proceso.

$$= (dm_{absoluto}\ '\ mcdu_{relativo})^2 = (dm_{absoluto})^2\ '\ 2(dm_{absoluto})(mcdu_{relativo})\ '\ (mcdu_{relativo})^2$$

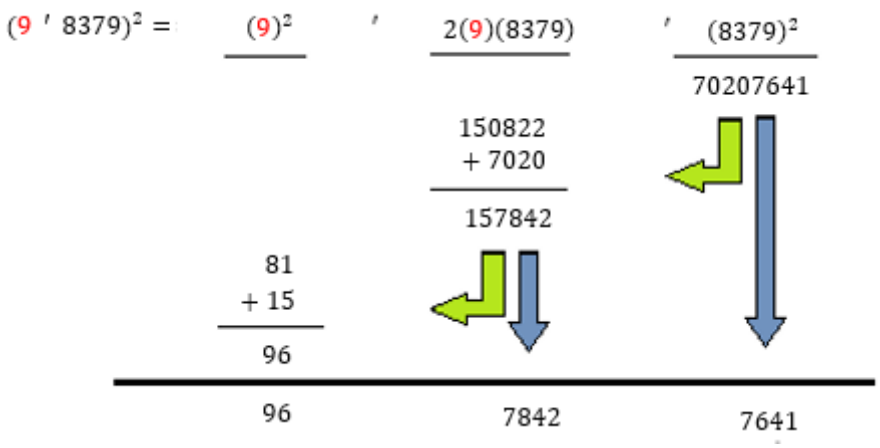


Figura 12: Evaluación completa de la modificación del cuadrado de la suma de dos cantidades para un número compuesto por decenas de mil, unidades de mil, centenas, decenas y unidades.

Esta es una variación de la ecuación del cuadrado de la suma de dos cantidades, y se recuerda que la ecuación del cuadrado de la suma de dos cantidades es un caso particular del Binomio de Newton. Se pretende establecer ahora cómo mediante los pasos definidos anteriormente se puede hallar cualquier potencia entera y positiva n mayor o igual a 2 mediante el siguiente mecanismo con x y y diferentes de 0, lo anteriormente descrito se visualiza en la ecuación (15)

$$(x_{absoluto}\ {}'\ y_{relativo})^n = (x_{absoluto})^n\ {}'\ (x_{absoluto})\left[\sum_{k=1}^{n-1}\binom{n}{k}(x_{relativo})^{n-1-k}\,(y_{relativo})^k\right]'\,(y_{relativo})^n \qquad (15)$$

En la parte izquierda de la igualdad ($(x_{absoluto}\ {}'\ y_{relativo})^n =$), de izquierda a derecha se sigue separando el número a hallarle la potencia enésima con comillas en dos partes; sigue la primera parte siendo el orden superior del número representado en valor absoluto de cifra como la variable $(x_{absoluto})$, mientras la segunda parte siguen siendo los órdenes inferiores faltantes del número como la variable $y_{relativo}$.

En la parte derecha de la igualdad ($= (x_{absoluto})^{n\prime}(x_{absoluto})\left[\sum_{k=1}^{n-1}\binom{n}{k}(x_{relativo})^{n-1-k}\,(y_{relativo})^k\right]'(y_{relativo})^n$) y

visualizando los grupos de derecha a izquierda, para el primer grupo sigue tomándose $y_{relativo}$ pero esta vez elevado a la potencia enésima. El segundo grupo contiene la variable $x_{absoluto}$ multiplicada por la sumatoria que va desde *k* igual a uno hasta *n* menos uno del coeficiente binomial de n sobre k multiplicado por la variable $x_{relativo}$ elevada a la *n* menos uno menos *k*, multiplicada por $y_{relativo}$ elevado a la *k*. El tercer grupo sigue siendo la variable $x_{absoluto}$ pero elevada a la enésima potencia.

Evaluando los grupos de derecha a izquierda, se evalúa el resultado del primer grupo $(y_{relativo})^n$, y dependiendo la cantidad de cifras que tenga $y_{relativo}$, se establece en los resultados los números pertenecientes a la respuesta y los que se acarrean.

Luego, se evalúa el segundo grupo $(x_{absoluto})\left[\sum_{k=1}^{n-1}\binom{n}{k}(x_{relativo})^{n-1-k}\,(y_{relativo})^k\right]$. A ese resultado se le suma el acarreo proveniente del primer grupo. Dependiendo la cantidad de dígitos que tenga $y_{relativo}$ multiplicado por $(n-1)$, se establecen de los resultados los números pertenecientes a la respuesta y los que se acarrean.

Por último, se halla el cálculo del tercer grupo $(x_{absoluto})^n$, se le suma el acarreo proveniente del segundo grupo y se toma la totalidad del resultado como parte de la respuesta. En la Figura 13 ilustra la descripción anterior.

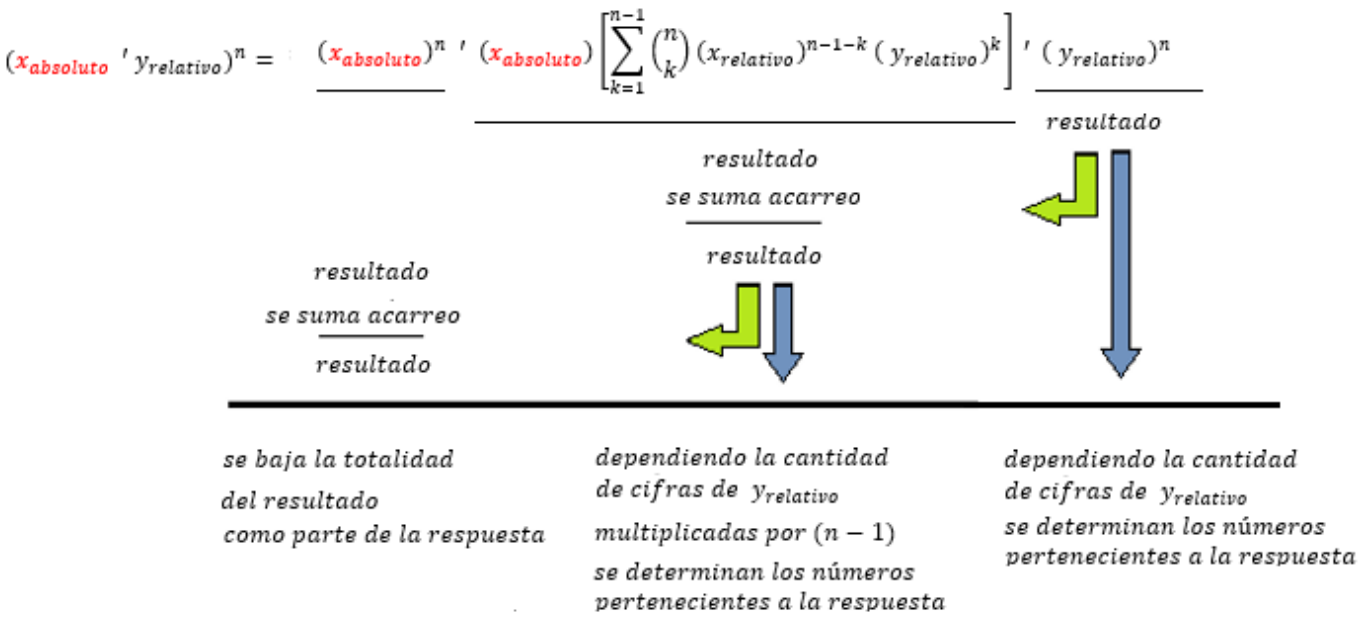


Figura 13: Evaluación completa de la modificación del Binomio de Newton.

Las tres respuestas concatenadas forman la potencia enésima del número.

Ejemplo 2:

Hallar $(379)^3$ utilizando el método propuesto.

Utilizando la ecuación descrita anteriormente en (13), se empiezan a evaluar los grupos de derecha a izquierda, empezando por $(y_{relativo})^n$, que es igual a $(79)^3 = 493039$; de este resultado se toman para la respuesta la cantidad de cifras que tenga $y_{relativo}$, es decir dos cifras, por lo que pasa a ser parte de la respuesta las decenas y las unidades, el número 39, y se la cifra restante, el número 4930. Esto se puede observar en la Figura 14.

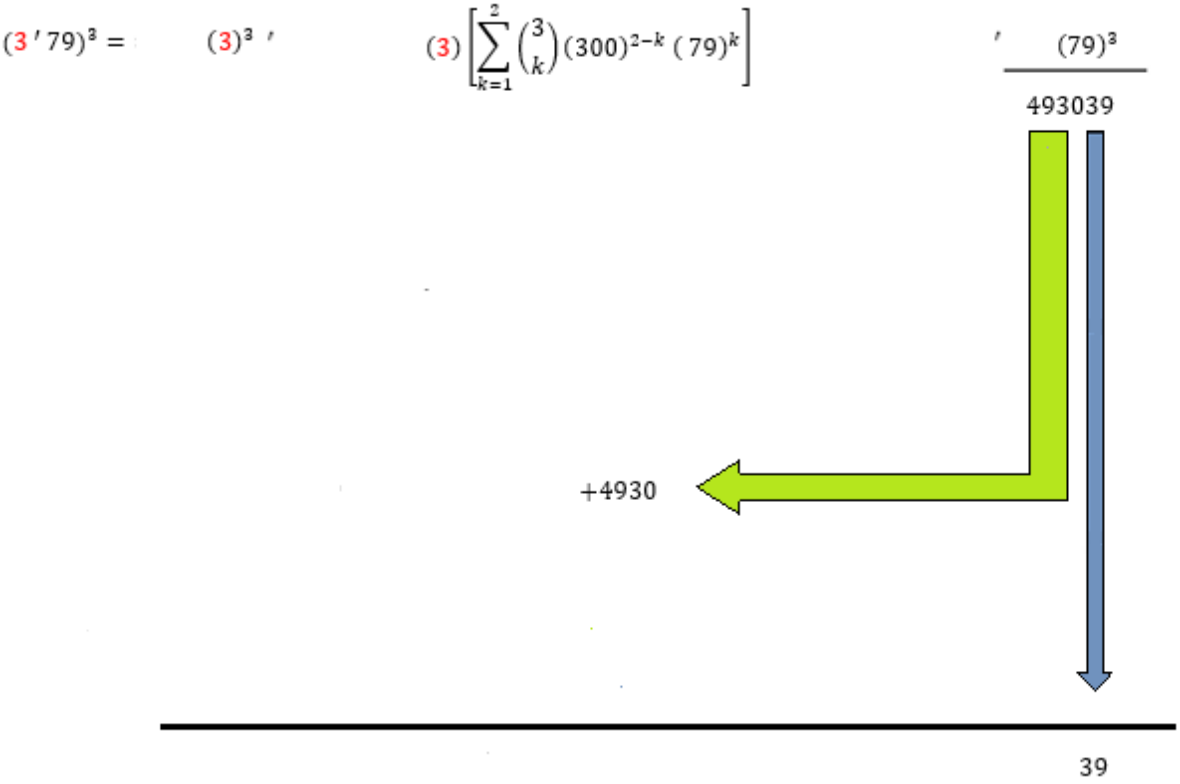


Figura 14: Evaluación del primer grupo de la modificación del Binomio de Newton para un número específico.

Luego se halla el resultado del segundo grupo $(3)\left[\sum_{k=1}^{2}\binom{3}{k}(300)^{2-k}\,(79)^k\right]$, que es igual a 269469; se le suma el acarreo proveniente del primer grupo, 4930, formando el resultado 274399.

De ese resultado los números que pertenecen a la respuesta se toman dependiendo de la cantidad de cifras de $y_{relativo}$ multiplicadas por $(n-1)$. Se toman entonces cuatro cifras de derecha a izquierda como parte de la respuesta, el número 4399 y se acarrea lo demás, el número 27. Lo dicho se ve en la Figura 15

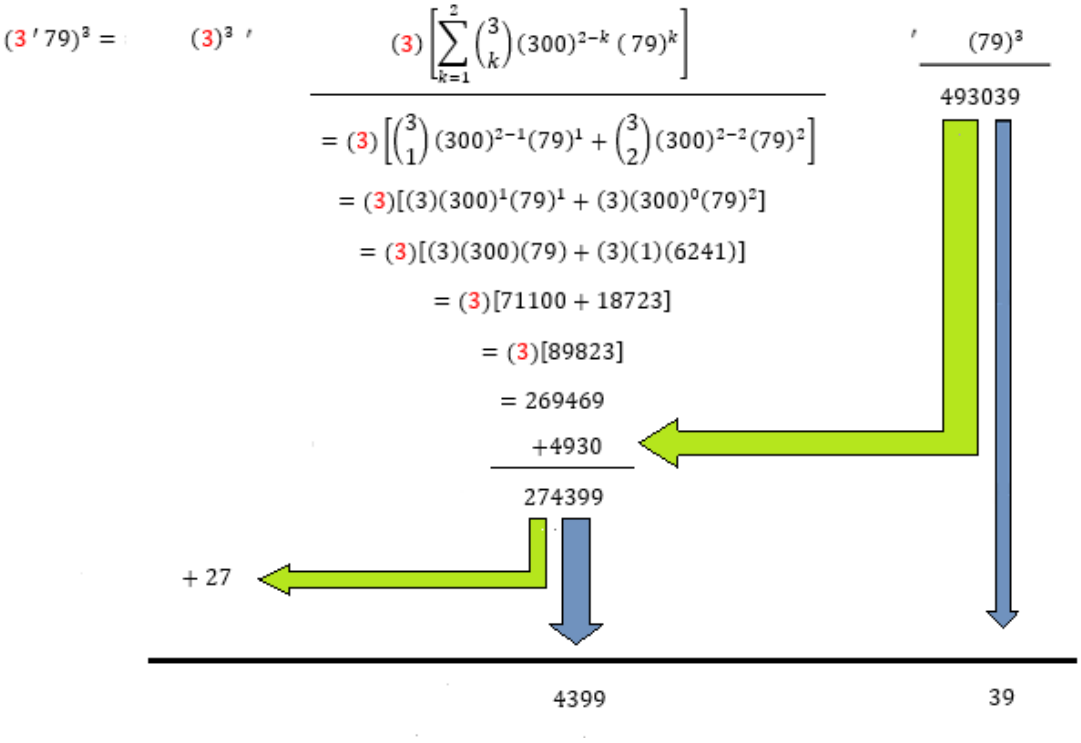


Figura 15: Evaluación del segundo grupo de la modificación del Binomio de Newton para un número específico.

Por último, se halla el cálculo del tercer grupo $(x_{absoluto})^n$, que es igual a $(3)^3 = 27$; se le suma el acarreo proveniente del segundo grupo, el número 27, dando por respuesta el número 54 el cual se toma en su totalidad como parte de la respuesta. El procedimiento completo se ilustra en la Figura 16.

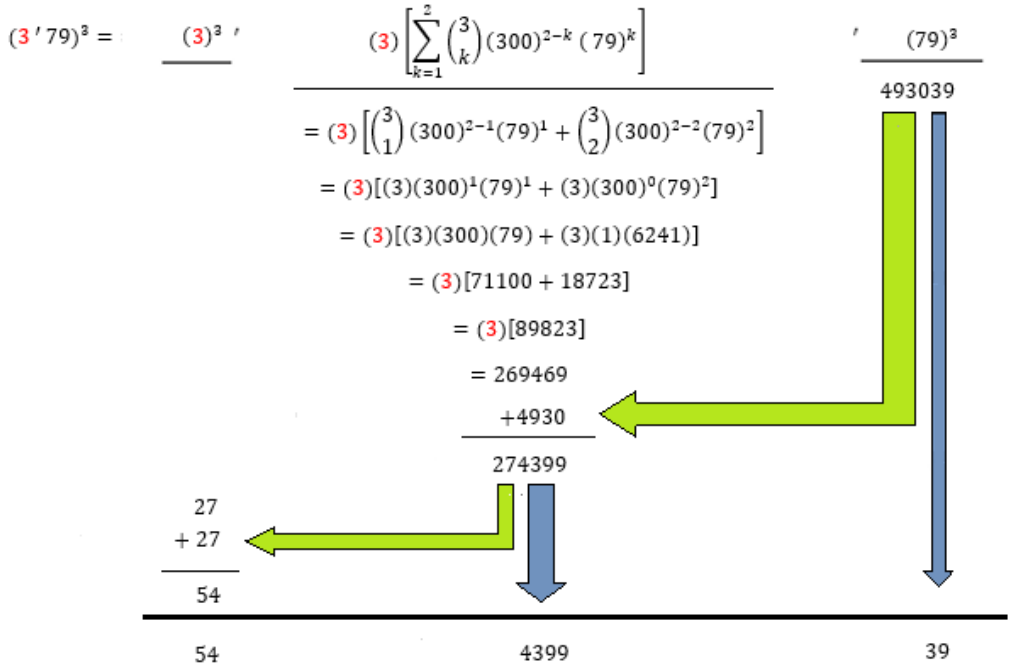


Figura 16: Evaluación del tercer grupo de la modificación del Binomio de Newton para un número específico.

Las tres respuestas concatenadas forman la potencia cúbica del número 379 que es igual a 54439939.

Ejemplo 3:

Hallar la cuarta potencia para el número 79 con el método propuesto. Utilizando la ecuación presente en (15). El proceso realizado se puede visualizar en la Figura 17.

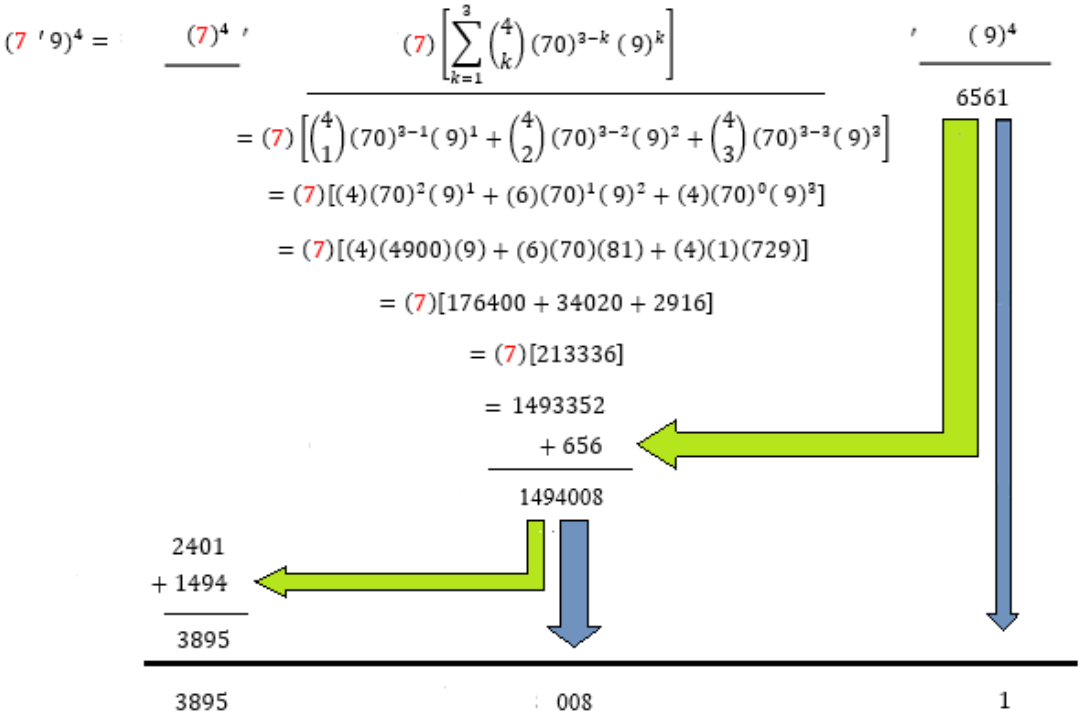


Figura 17: Evaluación del tercer grupo de la modificación del Binomio de Newton para un número específico.

Se conjetura entonces que para todos los x, y, n pertenecientes a los enteros positivos tales que la variable x y la variable y sean diferentes de 0 y la variable n sea mayor o igual a 2, la modificación del Binomio de Newton permite hallar potencias enésimas de un número. [8]

B. Mecanismo que permite conocer el factor de un número mediante la modificación del Binomio de Newton

En ésta sección se presenta la conjetura de como la modificación del Binomio de Newton permite dar a conocer el factor de un número.

Supóngase que desea hallar la potencia enésima de un número con la modificación del Binomio de Newton propuesta. Para tal propósito se toma nuevamente la ecuación descrita en (15)

Evaluando los grupos de derecha a izquierda, se evalúa el resultado del primer grupo $(y_{relativo})^n$, y dependiendo la cantidad de cifras que tenga $y_{relativo}$ se establece en los resultados los números pertenecientes a la respuesta y los que se acarrean. Ver Figura 18.

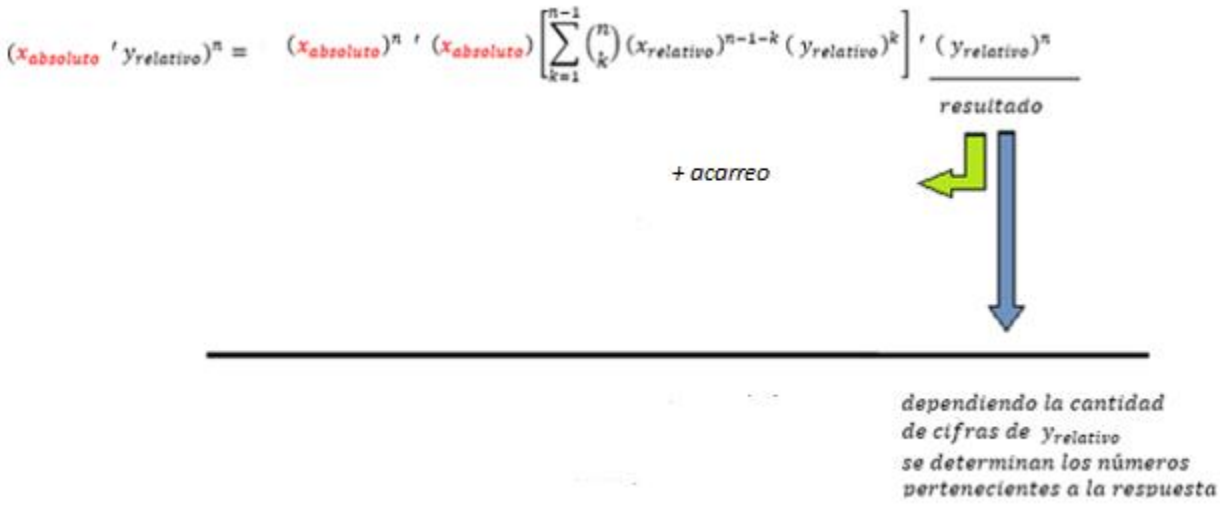


Figura 18: Evaluación del primer grupo de la modificación del Binomio de Newton.

Luego, se evalúa el segundo grupo $(x_{absoluto})\left[\sum_{k=1}^{n-1}\binom{n}{k}(x_{relativo})^{n-1-k}(y_{relativo})^k\right]$. A ese resultado se le suma el acarreo proveniente del primer grupo y se toma la totalidad del resultado.

La conjetura que se presenta es que al tomar la totalidad del resultado del segundo grupo y concatenarlo con la respuesta del resultado del primer grupo para formar un solo número, $y_{relativo}$ resulta ser factor de éste número formado. Lo anteriormente descrito se observa en la Figura 19.

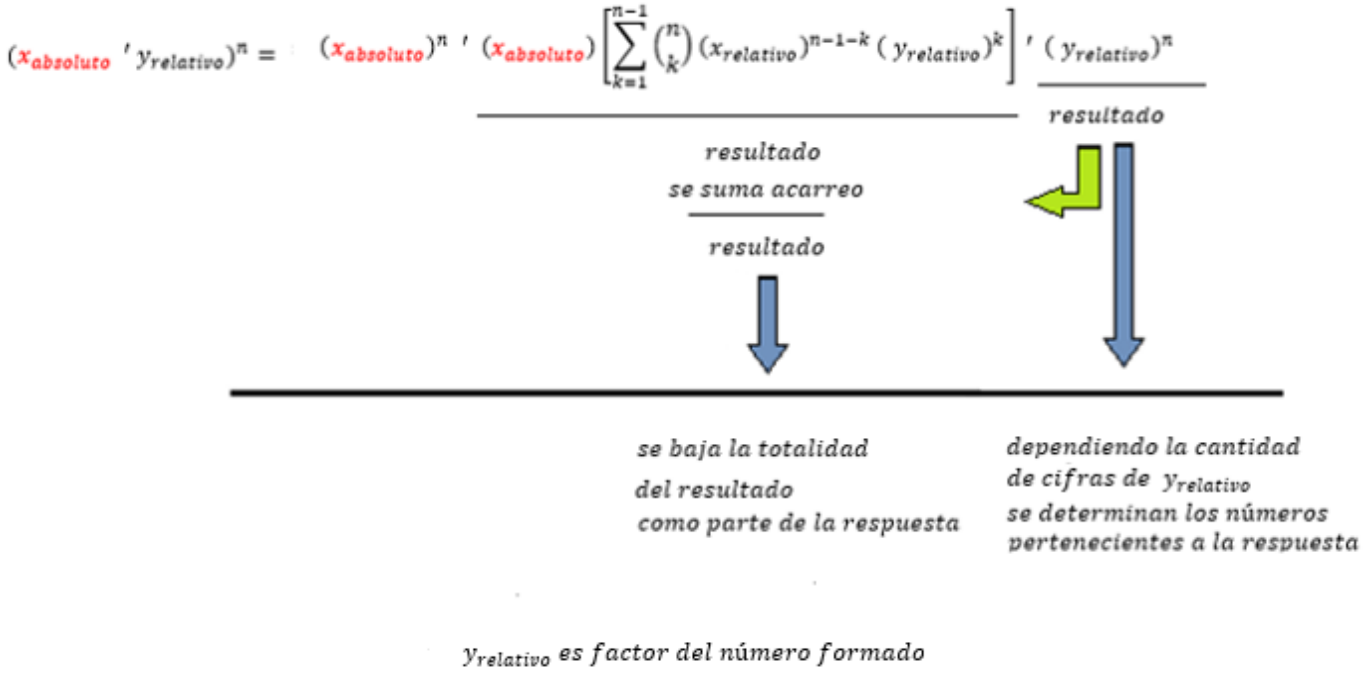


Figura 19: Evaluación del segundo grupo de la modificación del Binomio de Newton para un número específico especificando un factor del número formado.

Ejemplo 4:

Encontrar un factor a partir de la quinta potencia del número 17.

Se empieza por utilizar la ecuación descrita en (13). Al empezar a evaluar de derecha a izquierda, se halla $(y_{relativo})^n = (7)^5 = 16807$. Dependiendo de la cantidad de cifras que tenga $y_{relativo}$ (para éste caso una cifra), se establece en los resultados los números pertenecientes a la respuesta y los que se acarrean, por lo que sería parte de la respuesta el número 7, y se acarrearía lo demás, el número 1680. Este procedimiento se puede observar en la Figura 20.

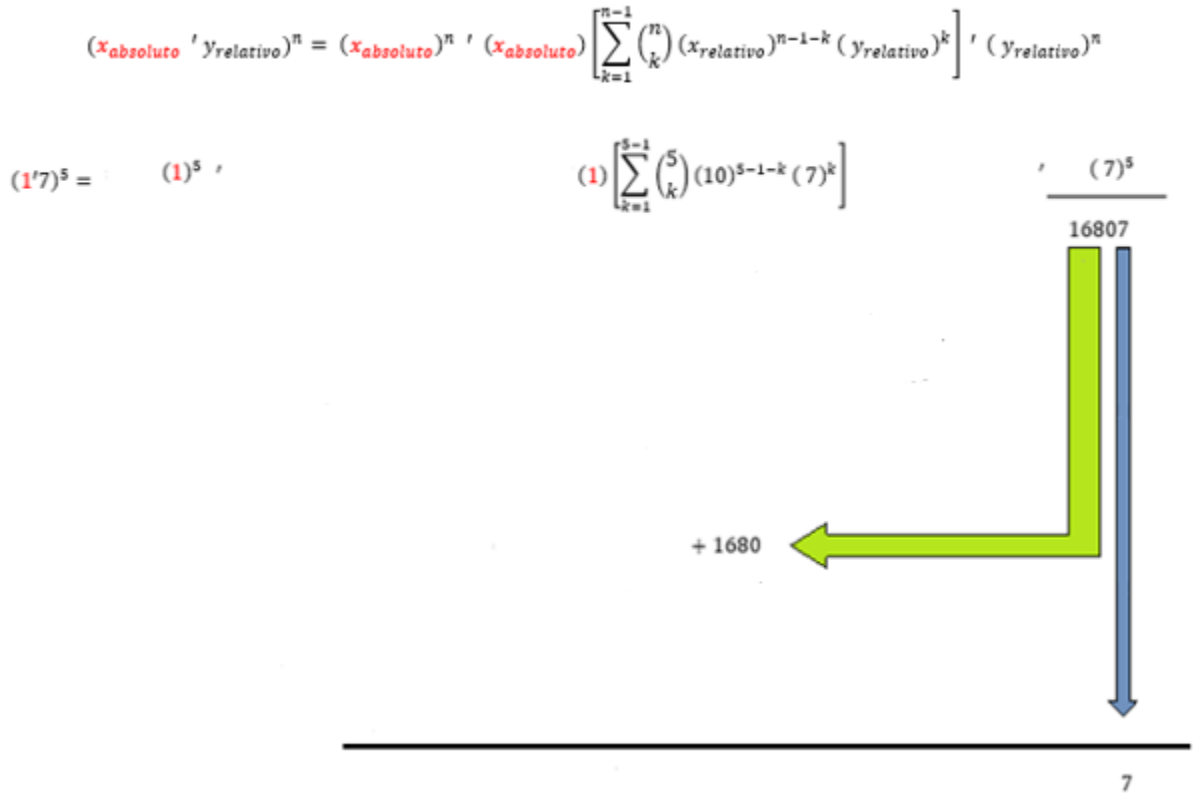


Figura 20: Evaluación del primer grupo de la modificación del Binomio de Newton para un número específico.

Luego, se evalúa el segundo grupo $(x_{absoluto})\left[\sum_{k=1}^{n-1}\binom{n}{k}(x_{relativo})^{n-1-k}(y_{relativo})^k\right] = (1)\sum_{k=1}^{4}\binom{5}{k}(10)^{4-k}(7)^k = 130305$. A ese resultado se le suma el acarreo proveniente del primer grupo, el valor 1680, quedando como resultado el número 131985. Al concatenar el resultado del segundo grupo con la respuesta del primer grupo se obtiene el número 1319857. A éste número se le puede hallar un factor, que resulta ser $(y_{relativo})$. Por lo tanto, el número 7 debe ser factor de 1319857, como se puede ver en la Figura 21.

$$(x_{absoluto}\ ' y_{relativo})^n = (x_{absoluto})^n\ '\ (x_{absoluto})\left[\sum_{k=1}^{n-1}\binom{n}{k}(x_{relativo})^{n-1-k}(y_{relativo})^k\right]'\ (y_{relativo})^n$$

$$(1'7)^5 = (1)^5\ ' \frac{(1)\left[\sum_{k=1}^{5-1}\binom{5}{k}(10)^{5-1-k}(7)^k\right]}{= (1)\left[\binom{5}{1}(10)^{4-1}(7)^1 + \binom{5}{2}(10)^{4-2}(7)^2 + \binom{5}{3}(10)^{4-3}(7)^3 + \binom{5}{4}(10)^{4-4}(7)^4\right]}\ ' \frac{(7)^5}{16807}$$

$$= (1)\left[\binom{5}{1}(10)^{4-1}(7)^1 + \binom{5}{2}(10)^{4-2}(7)^2 + \binom{5}{3}(10)^{4-3}(7)^3 + \binom{5}{4}(10)^{4-4}(7)^4\right]$$

$$= (1)[(5)(10)^3(7)^1 + (10)(10)^2(7)^2 + (10)(10)^1(7)^3 + (5)(10)^0(7)^4]$$

$$= (1)[(5)(1000)(7) + (10)(100)(49) + (10)(10)(343) + (5)(1)(2401)]$$

$$= (1)[35000 + 49000 + 34300 + 12005]$$

$$(1)[130305] = 130305$$

$$+ 1680$$

$$131985$$

131985 | 7

$$7\ es\ factor\ de\ 1319857$$

Figura 21: Evaluación del segundo grupo de la modificación del Binomio de Newton para un número indicando un factor para el número formado.

Al validar si 7 es un factor 1319857, se divide 1319857 entre 7 para constatar que el resultado de la división es un número entero, dando como respuesta el número 188551.

$$\frac{1319857}{7} = 188551$$

Ejemplo 5:

Hallar la potencia cúbica de 379 e indicar un número para el cual ($y_{relativo}$), el número 79, es factor. Ver Figura 22.

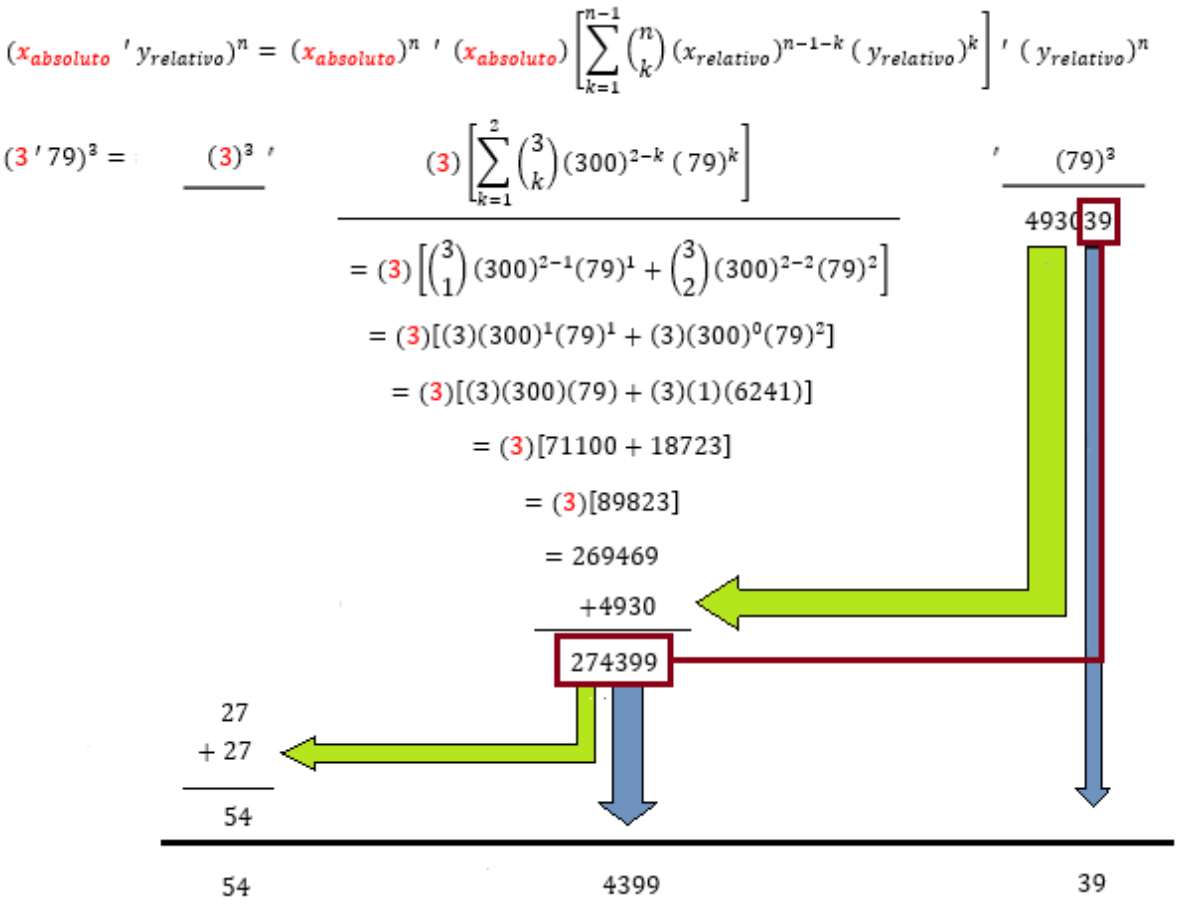


Figura 22: Evaluación completa de la modificación del Binomio de Newton para un número, indicando la potencia hallada y el factor de otro número.

Con lo presentado anteriormente se muestra cómo con la modificación del Binomio de Newton planteada se puede tanto conocer la potencia enésima de un número (en éste ejemplo la potencia cúbica de 379 da 54439939), como hallar también para otro número -resultado de la concatenación del acarreo y la respuesta del segundo grupo con la respuesta del resultado del primer grupo (números en los recuadros rojos)- un factor; que resulta ser $y_{relativo}$ (en éste ejemplo 79 es factor de 27439939).

Para comprobar si efectivamente 79 es factor de 27439939, se divide el número 27439939 entre 79 y luego se verifica que el resultado de la división es un número entero, el número 347341.

$$\frac{27439939}{79} = 347341$$

Hasta ahora se cuenta con una conjetura sobre un método para hallar factores, no se presenta una prueba formal matemática, pero se diseñaron y ejecutaron pruebas computacionales para determinar la validez de la conjetura para varios casos particulares.

IV. PRUEBAS

Basado en la modificación del Binomio de Newton se propone un mecanismo para obtener de forma computacionalmente eficiente potencias de un número entero de gran cantidad de cifras como también para hallar un factor de otro número entero de muchas cifras.

Las implementaciones de los algoritmos propuestos se realizaron en lenguaje de programación JAVA. En principio el lenguaje JAVA tiene ciertas limitaciones para evaluar números muy grandes debido a que los tipos de datos que utiliza para almacenar valores están restringidos. El tipo de dato DOUBLE, que es el más grande, es de máximo 64 bits y cuando se trata de almacenar un número mayor ocurre un desbordamiento.

Debido al problema descrito anteriormente se creía necesario implementar el código con ayuda de computación distribuida para poder evaluar números de gran tamaño, pero para solucionar éste inconveniente, se importa la librería Math y se utiliza la clase BigInteger, esta permite hacer cálculos con números enteros de muchas cifras decimales. Para salvar en una lista los valores de la combinatoria se importa la librería útil y se utilizan las clases LinkedList y List; y para paralelizar el programa y maximizar el poder de computo se importa también de la librería útil las clases concurrent.ExecutionException, concurrent.ExecutorService, concurrent.Executors y concurrent.Future.

Cuando se iniciaron las pruebas no se obtenía el resultado esperado ya que para el cálculo de algunas potencias (sobre todo para aquellos números que están compuestos de varios ceros), en algunas respuestas debía tomarse los ceros a la izquierda del número y no omitirlos, por lo que se añadió en el código una forma de hacer representativos los ceros a la izquierda del número. Para verificar la funcionalidad del algoritmo propuesto se realizaron más de 100 pruebas recurrentes utilizando simultáneamente el Binomio de Newton normal y la modificación del Binomio propuesta. Una vez verificada la funcionalidad del código se implementó en el centro de cómputo de alto desempeño (CECAD) para validar el alcance en cuanto a la cantidad de cifras de los números a los cuales se les pueden hallar factores.

Luego de asociar el código con tecnologías paralelas de programación, se paralelizó la sumatoria del segundo grupo de la modificación propuesta del Binomio de Newton y se validó su funcionalidad.

Para realizar los cálculos de forma paralela se calcula cada coeficiente binomial (dado que cada i-ésimo término de la sumatoria es independiente del i+1 o i-1 término). Luego todos los términos se suman.

¿Por qué se paralelizó? Porque se ahorra tiempo de cómputo y se utiliza mejor la máquina con éste enfoque, sobre todo si los exponentes son grandes (números mayores de 1000).

¿Cómo se paralelizó? Utilizando la clase Concurrent y empleando el método ExecutorService. El ServiceExecutor funciona como sigue: Se crea una instancia de una clase que sabe "mandar a hacer" tareas en paralelo. Este es el executor. El problema es que cada tarea paralela (en este caso el cálculo de los binomiales) puede tener tiempos de ejecución a otra similar. Entonces Funciona así:

Cada tarea a ejecutar en paralelo tiene un método que se llama "call". Este es como si fuera un "mini-main", es decir código que se ejecuta con cierta importancia, pero de forma paralela. Cada tarea paralela, para usar "call", debe implementar la interfaz "Callable". El ServiceExecutor invoca el método call() para cada tarea paralela que encuentre.

Cada tarea toma un tiempo diferente, y el Executor sabe que sólo en un Futuro (de ahí la interfaz Future) obtendrá el resultado del método call. Es decir, no sabe cuándo, pero sabe que el valor exacto va a estar disponible en un futuro. Por ello, el Executor lo que hace es esperar a que todos los resultados de las tareas que invocó con "call" estén disponibles. Mientras no los tenga todos, el programa principal no avanza.

De esta forma se podría concluir que el ServiceExecutor es el gestor de la concurrencia encargado de invocar las tareas paralelas y bloquear la aplicación hasta que estén todos los (sub) resultados de cada tarea.

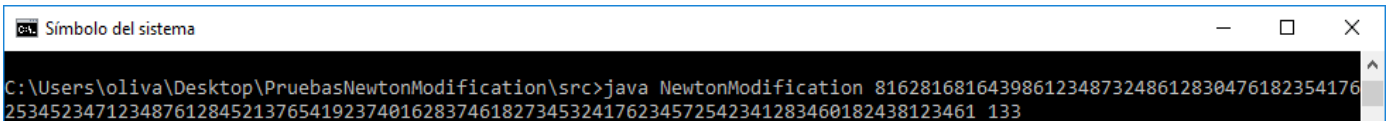
V. RESULTADOS

Al ejecutar la aplicación, los resultados se convierten en material de apoyo para el estudio de las conjeturas planteadas. Como se están manejando ejemplos con números de muchas cifras, los requerimientos de salida generan un modo de visualizar los resultados, pero serían demasiado largos para imprimirlos en este documento, por lo que se ha tomado solo un ejemplo de la ejecución.

La forma de realizar las pruebas es mediante el siguiente comando: java NewtonModification.

A éste comando se le asignan dos valores a evaluar, en este caso se evalúa el número

816281681643986123487324861283047618235417625345234712348761284521376541923740162837461827345324176234572542341283460182438123461 elevado a la potencia 133



La potencia se imprime con System.out.println(res.getAnswer()) y su resultado es:

188246416656231862627458024056397511197262813716622319429180746212531552365669173897187494688104074523824354304445651412769555413545516498143455411447734178108594095734953794535184345314151476886445945056728487072049914490006658694207756030336668179572264697415767753222888011944387698717725627050166730887862674484101515487545999146627207725811411700304470952405347417705004715950159184812022052060594989816853628217423930844726899645587879078618074080197883949715411946334497982047221690651236922083506318717037716264396367762526907152939023046803781727407917301311742247852258714416901539797231767692882093885547432590671517899235547859733349815567117558398078011022201628378850634935991182084996080454542424699429659115804083431992083408786544513870740294862648082021281982872842134630886889063892911373372379803667633185859451220352440151512900349780373195451278993946747505196220118351551755400782334536824588245095351232247527175932041470293079920679521786028307955330606315034958766539144885110198359241025037629127572309844107022220515843592505817265978134647504620324573146463339565781714234626879989748825241825107465722633540534791600600877950709345350803583013001955533591430384973784641032863290525464404083619324778738748933681330261299738114620045259418262567401572678537684213077876974791736126447926749420987897358845864464895194167286201343742829914814828518191622066110276206557882265566694969829463554143731951230918326002899387233350387201145809097968960243150475400492618799507564617870112490187477396127594068751603080324527184162503777592484889215122984394961179859318537489673549554446844602174965299796095182585026911148691321576866413829220642908597536547064660101854671553480807301135276159386213380462748212168068625320249166759809302337988929832062453463314881361850143052662203291260853504483555499393749699445080786485766136951581948129244887206574596495372627649876382254109549403632920981343333182979616955259757589962197518500483019722263949568797639025124802791950874072223961807229365755309154813181609611996806880667601433902008818557095663054346898566334261486040587677864141988074886088203200900178046593481527092859612814987850804639846111624279908217223941058218542681435308554120895035476744790800264934394117048042714320693583057080043852729442920154226832277872507815980648076469872482788399988869076767692203003334622722806093863385203959768969864362919671230830365413825021031426685232943112531651557579120034745784015747892285857493899036097314413279169064982365765222616825731747166589992567502530399472599384426591659327616505303237687928373539929857004978743106504391002730145634553656988039556013524391463835576676010044738842595885442162249043769372220102318751414690579494187882433908794325706432620949075401415224492055355067091543275285589099846716154598460309697171033546091747009348650211462357394104229657822588210965603867094462234869249930625583038959650746824759250818604047189646597642542176959530200490092767448617588395538941204517443365271854631304290947206920447279495493070222412527711043861852251061435477138097429382832654045991596885326863076440166689422269639082281221380979017461776184167140585273855342560845762649151615967838270019461689867364355417570298063007007159722275045148883385074909778870158637512838179234840501000494558152398182746483937327030292701484420856666873527542593225625419733319720647039738596408046871663648680376338585172532582535238227507247333882740475933352554078939495418640273394195082720918760559499341607809304701367809912436694917431598535083401095730466494803257230471531533569690779637625794784 16

380950202785742541788164359018534192531330703981036123884619363612214099470839102313701996956111098047678569267634188762979815651881327211874894923090812104632808550279205962228147586156366544086854294918807619075937386793595992520605038024426804448445378010644064516364535943131345617334472060420683687534450710051469138042970716049189661500686156993881542568149734275587621145787512567549691134491269291007577096868314594604871728072108883299064630481042834186293728971467304800659480730884470031943252952148792177059369242769098024711995118505369254884690821156980590317318741134814566954100478581013910666549108612554123913721668240467734671700786825461875763027425752599078097446900662623245773401468851137467655504994277244353259887082644277695074929606020178497668696685394863024929918012657006737656154224149281594504453354651344601469162600698383315833948429352007550407452342530451572730142994996163744520090310312027862452412164714561337750407918158537750848974507529333841989700114379347859152200849462111865868051326145489571306958337065403240561111665170714673739525222469181536092404830854144534275259623068936575109711639189263495904936449881138871473144836065911190461450631822817685318189446999627983698215877108477642600510872155533938997423858258215542301974635625739524727081606032688763268960010393939249692512012329586941077515437025032704800569619363255905358074985732910345299612056467080275033329930683699270144565317720386098473228101030678435649230576711798501445816638934617952922931597083664378692748730997686020271024005500430972649581003192365198185314974106277467232240639428617296791704946009524830117929763753366219146911223670780741204807502224476137367402700506539701148031627825515288643887751443250236439676521988733881508637293530929501637908633101967892092187533167982327867147659780109468736231270537740151538749534152969790620343142205704412597748939635923848545422027030099585343698135480011019501255379513705311140978356192027406678229515225080442776095902758516063520312771816604286648297619543396924826832897319916973060323172452843635000771820575284810885960129849044243559157698364515547496913131014206524507391894855304356142247571009869633075999735257664294397761261865002022185044802125485460040011830714885963339356887167709803384927071192752886593228601237871784350595940551799326510747164366465381035746222024185838853162204484397016229490057362426219980191919379268492822469217611750950629943381805322126245554783666206206622328171194883017414798483042489970013951916832232260598377258491119887945528183932698858253507271999176404080544013218875764381132475782272461574084778898270395997065336044361003328179290232624253360794581462546035325362230732070702761307205090892133253013832613612645225710195406292245365682359696783469311746786275162483849201780984916053689656398810196219321843602503894124600477677279056586951148882875079773181559156017643128235419081025084643862668559990646041732729175967827397835148558081821091416383707002331054908303509445517119987124136032039939474027059472509066992974007656440249056736267773945688778459066749937871142376409639224842486758787223007094228906481552423418040068781541903275239933374899564101843151246821115015278850623409117456384524507064277331439555889922028676851369411186487888001930693945321477843137950934763900870375232176162004002564198083462677893451239345809086999037835210436723899157993199798554318022826030873698821150612530761200406554207745136024783978795110312702130395338103454094083436209822477224731508705302627112845957133784440279575905789820137066072226713543166232237179708159414966517215487066858720302612486399908493719780061133371871688825194827971280192035487294626489164619838268948567071721842116665503099176983558497899917501034052616775286971412666001249537426553969804733798877927284449369917951116171436321692537418238035065577899142815613103592342394349827462348521153667743706636106174902638334071365702110278430618974448325924230937180870088702444846727758183326789320234269486319763810696375255464739523942600265859516121017858735196096701380152936859821876363070115616148438305246168616002324081530892816855577617324682827380900714519659716241671456164957538590627510344914451998113854405708588532594466517162610141919397699358881686235503521756826017350495788456267875257808631942114119790005145105261522649112706287113459263066126873027320776840895681032551287858392032253419445923532912682427733106184873029525508467912102734256329850939183348696523404034972675404331299861293673323563194656864505425696041375253642385033747045539811450179299058636960025043937786448830539779060995670018686083654473306313650729625565154615250097325233849758740845953292000957049660282382018763997496827620573803877182256241036347341152796961801682110350141502752864840776581959410005343875472717509652231824092782558338787449046709531745243308346390796841843765979419042255430405303189099195101759093198713510843649570779499857731260718466793283717931916102826799364564385354933178168069072135929413769379700263766022376368055405722001682373393824159955574740802039968100792639386374370504729932231319297306213399900111739108303003293524415856391521301476032448688261742771398934744239955027378260478849261942523834662848893980391960655987525616858191343974972695576174762066588948126346852700314104206120245870446976823752861434363913276209167554245607316719963500409685191280337744096168521630140965634210655791440065721814685435097535456976077127819814746566026105814752439738838093303065391079543587220538111053354195195457470797223843581171050121690458758235559189594223778860674430031520892511570570041765527694979557834570753022848736227813681351969636117759948104267201481066500542335150177185974574990056940383149512834666415

044672016828115162026943468152270101773827511061769086342237558765963204957122152578596897025629855299401359406429724803192640500726131778753091530300662294545295243812311797123939706435593255241721610730290499538266144965805605645865699505420792692544114713104170250979268141503253493498689762069862593200318155765710019406999500397975081215866627046000951086264545040621879335375936870075609970243507190940163899298075250980513283569601480214382328843664661221653432014038085337091569528613070783004811731581061019600794747178431165988605682595428018888907160901525952951065113304860056966740264985628419538583864862842961890369144655013930883293208957922751243375589617137111326438746855805764760777308267547180585720623401743058278322376444427977695318409161462975857243388036050353610843157910103528831255171938935002315165716185678987750114353214382786054939560695620456794172508435350798819360254150551231481724247560578031843675475979679718320179444734676398814294971481479990170126710355356694861132570393690851996288584765167283004862442909977174635120031149120319183587206405398947638236899586238706398990900118329522562747615262326086920610942542694132196316247540870491868917634041122134260991305800519049846660034309913331708320091463903716750799412725287656981279805323733853812180721491728805316199235745958104601560587937582460945474248464227371672552869432270524649292696754951751578678446653238940475362519360096258708795672225343222452198518133321424272711745817960061710598579439692788348462841083853800525474321236539659768871803818474391731006921534842223085809445002915862311183874096704844354900069631425622698047270764177668586760619563354563264898270784028758966315025599600965001872491077599148524647761253090171769365220994444455470753345937090083220046836164029891831224440437426985042843130754889279032731812642688937822396909853307029045106365778336302410502435345834434725822745646305468542557048316907686652919946578485637518242132754799428368310047860420147666940313127752737550452437709762149067001276889057235408918608412840672167321607393856183444255523614347175111773347240081381988078082118480724963661604851287463704992611925952589217735421439147237742728896781443547776853114735295610751213675895393760117126065456327782170975450087938889526639148592926768002731083096601028186679790556806760635084253707009849296006082801250793560571218949577721641456289969754266105372969508863726948008674061226574735925995699560978701818205234960347166645301025863881848559499603035720317092105565873107552431960283089381461792699067734114386024965859918810553986875873019108289139256765020073704641630494772295689992649891318884814765534839511248479592292340704203253961936329106583945669430578012066446831702972574681641710142651037199037300270664332562840219900442144728990352324349269181519098890514171126174871821835241151995380627541424225626554209315516221368543387286451193202989857563462545276604502656875091996502954617288731585536542038426690304050031396046059288641521626977023129950848685021588798663270646308277140403249339536320056232000012608624762824053452600189234795662114303206157812167850533090247617640601197319064129485935655330142229408408152215041828992578006305965841679190671209405839178424578567139421294720275254539221726280645284126773146370080998341719634789216610097147365043558328791890521955711977851893692028585016051632139649105127721594553979310200257297739055660019835326043074533517238225077679097100616051072078746038030479236370737106842794012479525110819075578406463661887933746059594019880613502248214276593225770790672319218098698247720324544901328930060870495640372672586505843503809690911760725722506855433059969472209960695108504765582928769839369889169597165110371659473764992911966766142653296724123126870678352488851284391049726333124426991059301536006111806520946864868409735476156365573133129602357318247987604016763945406562217370370973536581459853743161822302790492733984694847742773783721238301551798892700715365556313339030105871030496366962745419614269388561308004215272392652395472320540749873601739404499330719576684111116240485075305912673395907975169427917664533413167729285724587150709712746543996848719988044873973058650658947732950302999310380309423161593337337393172433017784611490112632367061245974773271824197908916438332420029867208258866939236355452630788008220931657708610536671194915228349828212036649123627334976537123474826962748500130543614322478076998948562661892591327062405685255394261092960016842607656832353612330018580173773554356482003730029107501852429035127495778429788486751716812611733524269713157481317000671096471872594614209626427387176028143196263859478628111113537611039928803665010729365073422032653414304711668523427892253279930294105760464323360708673427471054780201451449051762272905224919374625530986367599065688391151007697017046080740354215963354094071137091774164732761432390855554949146046108089788794895500874857980417396080392755645173502973028173011396341206748631436004734098845581392892913379315789478267428127680573508704149974108311849965665730352232746553971286573740923878588652821499190031976161201148795860530210486137828582358984676435339990051452739472137582433551498393045687189393991926651910048046069137181906507848021287389358835656472689808163593876411957052608378863589746043031624388486307689369047230157997178410959676874518063801114812089405526411011461470586710793896649632901717328038006384686841202428027306662274045082007928895616999413415829594817021499530392180422668177833963813507101955195740728536052223019387111235291699961626380183078860353750796361889834113100280777253886691950206036168399095505254147500352391088109709797035259024138194318884972598489607557887838554827847268993156846828265086950983435293529

598149969667930251801133689303410354648033730885127351661400491271469965650665663221144128734484994154961346650409146863630896168029966402380338308672845558880202325530083281899116048414010566226340336732681400509037581806632382229557762992731693993831636824257833867236824971700248504734031825809917092292504775669575350027409138531148349951094438582958103284235311358248566695113335355236026591743595462588963562825392240827173297864905987762136179464816051299546629970471930841008488857873366568658347477568480260958854808486251473968853490878897799418101473184318161108552615453882320178630912971611516663343372528496920573950213996907276452952672394744772415145341934764218760503858180780517557843128931095002941553134580442727296912034806515893139155116019946929948617250110808395582705809011050714073600301805691019029779137983626451426369225122079746152494789119385828372590365516677751615385101437559809788164528788647626542479048167084551333863154799365754368497163311819176419398462091733256226351444123594955603818419522209951452939377541952552125583097666087303233630212061143504370967435344292635490072248924928514458426145256090542802907475972847917751704137541219755821083904097266208112587631782014210415135879037799377485641448549943632422522144545618005145719714951524978996766174138679069994949411077107521749356234107470551644248634957961965652429182023580673582418713759150147132170499567261526643258734704085451849766962645083894586295278908629589494779263666059860032837482832595849974347782219394389166181239776950797183566658552184075333623499814156904935784432084937723695526466693199266637851645682413583285074677064566350839666353965397128946218769422914564227945199289495146265766570250773517742557629183756382674533007224809242186289969207456014207846415398580085646923264349055148977758263910102016266429041531272346307121672233521136940304760284170325219301070976540858619881276508717289525098642833286572887530429254573924131665833661348146849589256226948355224019634098 1

El múltiplo (número a hallarle el factor) se imprime en System.out.println(res.getMultiple()) ; su resultado es

175335167265797319679178428196382451825614284752476201865027449429828314255584967924039267921703385366644838444581913945889555413545516498143455411447734178108594095734953794535184345314151476886445945056728487072049914490006658694207756030336668179572264697415767753222888011944387698717725627050166730887862674484101515487545999146627207725811411700304470952405347417705004715950159184812022052060594989816853628217423930844726899645587879078618074080197883949715411946334497982047221690651236922083506318717037716264396367762526907152939023046803781727407917301311742247852258714416901539797231767692882093885547432590671517899235547859733349815567117558398078011022201628378850634935991182084996080454542424699429659115804083431992083408786544513870740294862648082021281982872842134630886889063892911373372379803667633185859451220352440151512900349780373195451278993946747505196220118351551755400782334536824588245095351232247527175932041470293079920679521786028307955330606315034958766539144885110198359241025037629127572309844107022220515843592505817265978134647504620324573146463339565781714234626879989748825241825107465722633540534791600600877950709345350803583013001955533591430384973784641032863290525464404083619324778738748933681330261299738114620045259418262567401572678537684213077876974791736126447926749420987897358845864464895194167286201343742829914814828518191622066110276206557882265566694969829463554143731951230918326002899387233350387201145809097968960243150475400492618799507564617870112490187477396127594068751603080324527184162503777592484889215122984394961179859318537489673549554446844602174965299796095182585026911148691321576866413829220642908597536547064660101854671553480807301135276159386213380462748212168068625320249166759809302337988929832062453463314881361850143052662203291260853504483555499393749699445080786485766136951581948129244887206574596495372627649876382254109549403632920981343333182979616955259757589962197518500483019722263949568797639025124802791950874072223961807229365755309154813181609611996806880660760143390200881855709566305434689856633426148604058767786414198807488608820320090017804659348152709285961281498780580463984611162427990821722394105821854268143530855412089503547674479080026493439411704804271432069358305708004385272944292015422683227787250781598064807646987248278839998886907676769220300333462272806093863385203959768969864362919671230830365413825021031426685232943112531651557591200347457840157478922858574938990360973144132791690649823657652226168257317471665899925675025303994725993844265916593276165053032376879283735399298570049787431065043910027301456345536569880395560135243914638355766760100447388425958854421622490437693722201023187514146905794941878824339087943257064326209490754014152244920553550670915432752855890998467161545984603096971710335460917470093486502114623573941042296578225882109656038670944622348692499306255830389596507468247592508186040471896465976425421769595302004900927674486175883955389412045174433652718546313042909472069204472794954930702224125277110438618522510614354771380974293828326540459915968853268630764401666894222696390822812213809790174617761841671405852738553425608457626491516159678382700194616898673643554175702980630070071597222750451488833850749097788701586375128381792348405010004945581523981827464839373270302927014844208566668735275425932256254197333197206470397385964080468 71

6636486803763385851725325825352382275072473338827404759333525540789394954186402733941950827209187605594
9934160780930470136780991243669491743159853508340109573046649480325723047153153356969077963762579478416
3809502027857425417881643590185341925313307039810361238846193636122140994708391023137019969561110980476
7856926763418876297981565188132721187489492309081210463280855027920596222814758615636654408685429491880
7619075937386793595992520605038024426804448445378010644064516364535943131345617334472060420683687534450
7100514691380429707160491896615006861569938815425681497342755876211457875125675496911344912692910075770
9686831459460487172807210888329906463048104283418629372897146730480065948073088447003194325295214879217
7059369242769098024711995118505369254884690821156980590317318741134814566954100478581013910666549108612
5541239137216682404677346717007868254618757630274257525990780974469006626232457734014688511374676555049
9427724435325988708264427769507492960602017849766869668539486302492991801265700673765615422414928159450
4453354651344601469162600698383315833948429352007550407452342530451572723014299499616374452009031031202
7862452412164714561337750407918158537750848974507529333841989700114379347859152200849462111865868051326
1454895713069583370654032405611116651707146737395252224691815360924048308541445342752596230689365751097
1163918926349590493644988113887147314483606591119046145063182281768531818944699962798369821587710847764
2600510872155533938997423858258215542301974635625739524727081606032688763268960010393939249692512012329
5869410775154370250327048005696193632559053580749857329103452996120564670802750333329930683699270144565
3177203860984732281010306784356492305767117985014458166389346179529229315970836643786927487309976860202
7102400550043097264958100319236519818531497410627746723224063942861729679170494600952483011792976375336
6219146911223670780741204807520224476137367402700506539701148031627825515288643887751443250236439676521
9887338815086372935309295016379086331019678920921875331679823278671476597801094687362312705377401515387
4953415296979062034314220570441259774893963592384854542202703009958534369813548001101950125537951370531
1140978356192027406678229515225080442776095902758516063520312771816604286648297619543396924826832897319
9169730603231724528436350007718205752848108859601298490442435591576983645155474969131310142065245073918
9485530435614224757100986963307599973525766429439776126186500202218504480212548546004001183071488596333
9356887167709803384927071192752886593228601237871784350595940551799326510747164366465381035746222024185
8388531622044843970162294900573624262199801919193792684928224692176117509506299433818053221262455547836
6620620662232817119488301741479848304248997001395191683223226059837725849111988794552818393269885825350
7271999176404080544013218875764381132475782272461574084778898270395997065336044361003328179290232624253
3607945814625460353253622307320707027613072050908921332530138326136126452257101954062922453656823596967
8346931174678627516248384920178098491605368965639881019621932184360250389412460047767279056586951148888
2875079773181559156017643128235419081025084643862668559990646041732729175967827397835148558081821091416
3837070023310549083035094455171199871241360320399394740270594725090669929740076564402490567362677739456
8877845906674993787114237640963922484248675878722300709422890648155242341804006878154190327523993337489
9564101843151246821115015278850623409117456384524507064277331439555889922028676851369411186487888001930
6939453214778431379509347639008703752321761620040025641980834626778934512393458090869990378352104367238
9915799319979855431802282603087369882115061253076120040655420774513602478397879511031270213039533810345
4094083436209822477224731508705302627112845957133784440279575905789820137066072226713543166232237179708
1594149665172154870668587203026124863999084937197800611333718716888251948279712801920354872946264891646
1983826894856707172184211666550309917698355849789991750103405261677528697141266600124953742655396980473
3798877927284449369917951116171436321692537418238035065577899142815613103592342394349827462348521153667
7437066361061749026383340713657021102784306189744832592423093718087008870244484672775818332678932023 42
6948631976381069637525546473952394260026585951612101785873519609670138015293685982187636307011561614843
8305246168616002324081530892816855577617324682827380900714519659716241671456164957538590627510344914451
9981138544057085885325944665171626101411919397699358881686235503521756826017350495788456267875257808631 9
4211411979000514510526152264911270628711345926306612687302732077684089568103255128785839203225341944592
3532912682427733106184873029525508467912102734256329850939183348696523404034972675404331299861293673323
5631946568645054256960413752536423850337470455398114501792990586369600250439377864488305397790609956700
1868608365447330631365072962556515461525009732523384975874084595329200095704966028238201876399749682762
0573803877182256241036347341152796961801682110350141502752864840776581959410005343875472717509652231824
0927825583387874490467095317452433083463907968418437659794190422554304053031890991951017590931987135108
4364957077949985773126071846679328371793191610282679936456438535493317816806907213592941376937970026376
6022376368055405722001682373393824159555747408020399681007926393863743705047299322313192973062133999 00
1117391083030032935244158563915213014760324486882617427713989347442399550273782604788492619425238346628
4889398039196065598752561685819134397497269557617476206658894812634685270031410420612024587044697682375
2861434363913276209167554245607316719963500409685191280337744096168521630140965634210655791440065721814
6854350975354569760771278198147465660261058147524397388380933030653910795435872205381110533541951954574

70797223843581171050121690458758233559189594223778860674430031520892511570570041765527694979557834570753022848736227813681351969636117759948104267201481066500542335150177185974574990056940383149512834666641504467201682811516202694346815227010177382751106176908634223755876596320495712215257859689702562985529940135940642972480319264050072613177875309153030066229454529524381231179712393970643559325524172161073029049953826614496580560564586569950542079269254411471310417025097926814150325349349868976206986259320031815576571001940699950039797508121586662704600095108626454504062187933537593687007560997024350719094016389929807525098051328356960148021438232884366466122165343201403808533709156952861307078300481173158106101960079474717843116598860568259542801888890716090152959295106511330486005696674026498562841953858386486284296189036914465501393088329320895792275124337558961713711132643874685580576476077308267547180585720623401743058278322376444427977695318409161462975857243388036050353610843157910103528831255171938935002315165716185678987750114353214382786054939560695620456794172508435350798819360254150551231481724247560578031843675475979679718320179444734676398814294971481479990170126710355356694861132570393690851996288584765167283004862442909977174635120031149120319183587206405398947638236899586238706398990900118329522562747615262326086920610942542694132196316247540870491868917634041122134260991305800519049846660034309913331708320091463903716750799412725287656981279805323733853812180721491728805316199235745958104601560587937582460945474248464227371672552869432270524649292696754951751578678446653238940475362519360096258708795672225343222452198518133321424272711745817960061710598579439692788348462841083853800525474321236539659768871803818474391731006921534842223085809445002915862311183874096704844354900069631425622698047270764177668586760619563354563264898270784028758966315025599600965001872491077599148524647761253090171769365220994444455470753345937090083220046836164029891831224440437426985042843130754889279032731812642688937822396909853307029045106365778336302410502435345834434725822745646305468542557048316907686652919946578485637518242132754799428368310047860420147666940313127752737550452437709762149067001276889057235408918608412840672167321607393856183444255523614347175111773347240081381988078082118480724963661604851287463704992611925952589217735421439147237742728896781443547776853114735295610751213675895393760117126065456327782170975450087938889526639148592926768002731083096601028186679790556806760635084253707009849296060828012507935605712189495777216414562899697542661053729695088637269480086740612265747359259956995609787018182052349603471666453010258638818485594996030357203170921055658731075524319602830893814617926990677341143860249658599188105539868758730191082891392567650200737046416304947722956899926498913188848147655348395112484795922923407042032539619363291065839456694305780120664468317029725746816417101426510371990373002706643325628402199004421447289903523243492691815190988905141711261748718218352411519953806275414242256265542093155162213685433872864511932029898575634625452766045026568750919965029546172887315855365420384266903040500313960460592886415216269770231299508486850215887986632706463082771404032493395363200562320000126086247628240534526001892347956621143032061578121678505330902476176406011973190641294859356533014222940840815221504182899257800630596584167919067120940583917842457856713942129472027525453922172628064528412677314637008099834171963478921661009714736504355832879189052195571197785189369202858501605163213964910512772159455397931020025729773905566001983532604307453351723822507767909710061605107207874603803047923637073710684279401247952511081907557840646366188793374605959401988061350224821427659322577079067231921809869824772032454490132893006087049564037267258650584350380969091176072572250685543305996947220996069510850476558292876983936988916959716511037165947376499291196676614265329672412312687067835248885128439104972633312442699105930153600611180652094686486840973547615636557313312960235731824798760401676394540656221737037097353658145985374316182230279049273398469484774277378372123830155179889270071536555631333903010587103049636696274541961426938856130800421527239265239547232054074987360173940449933071957668411111624048507530591267339590797516942791766453341316772928572458715070971274654399684871998804487397305865065894773295030299931038030942316159333733739317243301778461149011263236706124597477327182419790891643833242002986720825886693923635545263078800822093165770861053667119491522834982821203664912362733497653712347482696274850013054361432247807699894856266189259132706240568525539426109296001684260765683235361233001858017377355435648200373002910750185242903512749577842978848675171681261173352426971315748131700067109647187259461420962642738717602814319626385947862811111353761103992880366501072936507342203265341430471166852342789225327993029410576046432336070867342747105478020145144905176227290522491937462553098636759906568839115100769701704608074035421596335409407113709177416473276143239085555494914604610808978879489550087485798041739608039275564517350297302817301139634120674863143600473409884558139289291337931578947826742812768057350870414997410831184996566573035223274655397128657374092387858865282149919003197616120114879586053021048613782858235898467643533999005145273947213758243355149839304568718939399192665191004804606913718190650784802128738935883565647268980816359387641195705260837886358974604303162438848630768936904723015799717841095967687451806380111481208940552641101146147058671079389664963290171732803800638468684120242802730666227404508200792889561699941341582959481702149953039218042266817783396381350710195519574072853605222 3

019387111235291699961626380183078860353750796361889834113100280777253886691950206036168399095505254147500352391088109709797035259024138194318884972598489607557887838554827847268993156846828265086950983435295981499696679302518011336893034103546480337308851273516614004912714699656506656632211441287344849941549613466504091468636308961680299664023803383086728455588802023255300832818991160484140105662263403367326814005090375818066323822295577629927316939938316368242578338672368249717002485047340318258099170922925047756695753500274091385311483499510944385829581032842353113582485666951133353552360265917435954625889635628253922408271732978649059877621361794648160512995466299704719308410084888578733665686583474775684802609588548084862514739688534908788977994181014731843181611085526154538823201786309129716115166633433725284969205739502139969072764529526723947447724151453419347642187605038581807805175578431289310950029415531345804427272969120348065158931391551160199469299486172501108083955827058090110507140736003018056910190297791379836264514263692251220797461524947891193858283725903655166777516153851014375598097881645287886476265424790481670845513338631547993657543684971633118191764193984620917332562263514441235949556038184195222099514529393775419525521255830976660873032336302120611435043709674353442926354900722489249285144584261452560905428029074759728479177517041375412197558210839040972662081125876317820142104151358790377997748564144854994363242252214454561800514571971495152497899676617413867906999494941107710752174935623410747055164424863495796196565242918202358067358241871375915014713217049956726152664325873470408545184976696264508389458629527890862958949477926366605986003283748283259584997434778221939438916618123977695079718356665855218407533362349981415690493578443208493772369552646669319926663785164568241358328507467706456635083966635396539712894621876942291456422794519928949514626576657025077351774255762918375638267453300722480924218628996920745601420784641539858008564692326434905514897775826391010201626642904153127234630712167223352113694030476028417032521930107097654085861988127650871728952509864283328657288753042925457392413166583366134814684958925622694835522401963409812816816439861234873248612830476182354176253452347123487612845213765419237401628374618273453241762345725423412834601824381234612831047618235417625345234712348761284521376541923740162837461827345324176234572542341283460182438123461

Un factor de 128 dígitos decimales. La división entre múltiplo y factor es

107688610488560879219227465272178274288283446512859705614672069811408156062850112367883987339713744397830545223616837758184681753162965480813295809463143231626596800306225227166112483083890463997584578936128170022964658207703246304442516101546891344839462163460262956734419769705802840387855857350814594696242700145134730622168792547108729610007971812324004629170275151388955617193086705443072168360268162844578680302335711333640713707446437864997190736367334698821989133418940706779845807896910234568547259089266794638516282097371408603755971231715742464661789298864820086599625454655336947719511284778710107983922098763675300913704834208574243089572776474024985040073872255796996017141859488770132413996829877078101624684284609282590117649069048954131491587698170606353869071248119939268675121545097250913510976345560655116574564824496049613083949788634411214873308930982527734835497535746500327230235159782640890809517750442835928532620844263797527321208757052347581309978959108713378634379610969880269799368828630517147301370183624659860194023418989433613546796475981217092519239499183432882467084927985336023982113982573389540832669133729512315015968987481672949736566036511092761718104633050016054322327253180657334440138976115455363008000268833623081104685618758475118318521673226597394989371409462734457114058728098117735645984639005506501199915122480170225858452754666880012813181438303360471296858506415227357294499480723290359704501888132200434426406376756262284604837071219388855014579411442024548339623156178211332169654812965676875099324535548783658245990233573642815591513794173958471298986342323656669197681109237195918876348419495065597529212140114779918656183997734643910112302356162432552935268205558760092321499152902866076211854723904490634890541933551704843295374589274735794370777213688269406846664305061630356574688656780891724141360458822542682531813914864479412094948785484535882889274600856844957985412118223452964339548767213178547092005096648795982576768278058488242068619255567441099545699630402606617005230019810745940435952954620259814083292059059092699701510957125151914271939073233751995388623447268942554920711465158969494682450282518474379816969186770787591285450220596656335283620106266495952591262549734793445540905144037077105199013211364447962107895809481407170625632675712959219635083338690091175164634739078089831993454899622600097256625283958606790079314784986513040048412870330573516921674272610535849590140881695521041182964403701943867583756236269108397821716528056966401918074319459866726808931897132748520845570515174593847110802302579115452253338158516186424683800520450541186022185951118631704791995663666205335183097802351213

93607458992896685155630580810262728789653341331776805703323169612357941734777649045979912996196331782678725483710535046065139090761565301334239094283634665038216739230277342494686059368561741179017361469900119609439282569374887173495164036812956974474081751325237027170890788440242845886676444794724901787036856610712153572161480022699830732401559203654980487972510566354973770643499714740561830259904426278127959550989375364023554319178316080710752848953102279001290653682469036382012022402895989901426595188918674705659197294352643318844955351210159523522263255959107510471059954961364485739753139315186612795383892681715855913796242557873383733256802372115281559710929948669954474789079861784790899234492831565516530320769240355547564115012856368235251415526204589747919487320278589000233462620870551854973073987014370130653824223054087761675861201250559527877444750558129241614110775765132254380807832752190935475215060785886494252002467519258808568937896365805530154026157158288039230681542587770349512446614360848388112876570844844655452694485870796946339748671655417925487890019948301558129719266703613757461492096382942859232520474978496081499613526960360405603548261104871922731826183463930241341161878429045038179730033608832334227571090179484875728528584273005356678327873349178027373844968200966503772747451894520267264102719683968322887094101587843458061968590048453570652865331848845025643778569011458712315661858568814113948078300099848723298188757417043184353863065307515073134335634416962353722238501833921831530763994120103741944396103989476852143527785946469424569383292815655484987100911935811417725627434926280116002073988284889273891124728237454018224743800408233993813345665166520235227658002328217582780171075042850986743914059469411686106919741341212304393664020391828525675742647611663677360703703979431120785028505388592460490781017153468281007305321170979752702320990717492754686776105488876610857790171380442541270581461018527117929201662392090966579890646227974791851768379429662623711963843423613426463568214310459070590390787662488687643319748157188283003004490896563487753757358206841178357153901105138212368519958871988076088737379435030267320606627480968443486147891994311844570556150621034492917017787477960769684202071211117455036704206120403258092453082486335160324554854562888377103771993309261223936110528964322154875205149932141975806678041175359553702068874738631152481813366736288483258503674141589662520444030892964068286636648779110077443088748031110389067862439121165337642372844522916815237050746915628929630293804790255821081988329261756157643428394639618222811255019592687208866777843046762182202756355881554216691939388579822634794335684762921210813250885897429509695384797463610146674234553355297972231889722129433963113979225208730007814615264752615898966290332007147113093302880597420155326501729293703478241894330238817427718378758852678558996046790022279853081061428720218104515542431789033521927169225237378392568091057345386997012778579451091889854118483514107555516939885979066137292806831597830925694702274501837810019893960762489856667020761112223796964484993796908848873088018486344784724208857115352223009606326868656285378413765089932010933039232064656261106470109459534049777495095740634742612291249949057167436498627525145767788330025616812936223610928028149440243939141581675234695459588769349482340640925231493044445476507847520844796671122492404003355429053875874774183328179239079065108895465862768687070433698238549520008772397002557703856071811613655360993706915500694780292328466342234017256172876441053817200047266094789880816092642385978701694667415705368327708805236233422926572914839185060539670655372508716689571862682365729558398009998897199566493888107610056451499553724638436548400892569536782856169956486797634383355826151770009499525202090692067838201847235841548271878513537678322181580063456623793136400260104072877125474663112724157359773318174435716236519042096921266246217449389333296670155076312070930289930668315452788693643474568848894677485184014857831826640289261947298049382883849767619386111131913007033844944236201269486730514451145208592906735983645383512089618268665906861834476684882357842978550350958817778175598116950711479142221065844064211985072839477473283671316596584753396647846894128356402224512699714439157498389598594073080828358686401191286357051482454440448635622894391926335584757010589203166953592420876934016778581763248738253204738081925037352572966614146403588870888496146471571685798008551019674766288581856847359251505399519629629152654621180478299159228222547462030238760395315142766537331614945736659230058549259273705041359493208347008415442319487436749514569564642353497432679717747862474114296965980242041159716458935498894635832838435745503484497557261898699728757741732682121194145814060102032845941604805906056700032554322822367296986387317064523051745609179830568407438109024901033211365211758700133320039829970654685440201884755470561508863466431586398971802324703251192505385872417173216424622509638336889971900711535549500511419309713567766552949819704912927468033605707914002049859933587499070501189208460684836627056438959389723044415635525790834809011828133928205922802526251715956129353469859973648996431311097636728960879118746563882208193811513888347168967200307654390586952351672005026499753967977939953004458896458851231481761944614040179017439527528367561258732682526700318307109839200013912853486863200810859282021733128158082401249014653200596610390879438492691330412298122052930230416083044984694357829516764015600208069397472496075120047762327765487857476535122485321145681042316446867882446054377867231141169455994386262966512137919655256594123890289620193174327389308835092527220439758419150614763833245641219562357747343

911906977130953011995249870467751891471887360842131847369384535999423650712877827906379906979952760953863181392021408600211162102320706498218017205934729718801060740114053681272579386560720370000925834181166051141689752735311790618997676762479079421257803853143932918487146461746505718562292120546965967521161494207467504657601734871556105404722686908773796244205185518097748013923874801842794753280631364738643856985825442576310858641996028906399833838149236109531788214073463263340047856134273561291677641599623176662482382600214993707393669889431897401018451415172024543179193534684181873536180093341886469585226021050148156630189263739219928314032010183556076253151075299532281767924399546034674496767136285017639838938026077256692693540972063722276919086165875122162434732522161533470135023802443877451738219798177147150231234684435905756852433648777657316056408914138952594243897009506173586393321081275079300496303804633008631499140436639089407798919415878680852715976233805840106136793601433963625992664635852909085744059193040073796788472774050545520348199680473610707783470141795312721749460385857395681708239201198839147998183592704190368750278979654666505679570738835899683354478292233208527159213966052606047438744302526228219788410398918029962473274602013376740232402097717402845518753833812968652113472870500147698160171986567385427762991766625156020143583445306195037896020053513281028069482425502437836383315874114077802709631170199939669553675132846393241428947283688572738080105221296277160940294885034491185362457175031169542394199786315801973613974779736625778126316938639437301885976737692873310017868018489121662282956706071775621171822802967580493157173467892602229924184426722760137500841463861347201205664988825039252723803046298523568556378231370592497921914477745782682599265093822356445335943138061429829232512125332815422146149300369639618212214119650464069340997212527885902848536432764242878458381694343084745049818331429337112154906361057891257924481991690991690222798106097692063721746299657744085429221966367979537728011793874795172654422375006512636255107136502967487336325123747929971718645991329747410256786182999742898934284902963668830774786686226452644371258824257641326582032240749677909660932398024458686130288550038066104015919346152164677041397323380488609724250115683573755539800672849245564349764299416672313914829122412560902013784303226647696452366265368390864032968389549675791412770156087366564195604212066212291917000074146688825367353039698759481529661801985254622276206592480259612316793327872741762436845430548225048957254614785206976972027939563999374585367777989944376866331768871932022467666272791559360617126752287969018490102735904383526421626341241360501193672680996979559512014340283713968427816258408418870922309220024726080810992084460090402677785667621777741703590931696796465444599649532976162299177635920563792939045678167706628581223853981598710143713545974111027796530012261694742276316598439152861643547799059525477026962611524602184529175064064192374185837350225261597455652344640491971042664059476338054306172702376333033075348308993915436782014451249053802538072414501458266570355116444360360475981409690001776609017476412965635213455369556636644012868782717420249826553987885111840621161144095839554474268658729330209465293870748426681634828995557298873189926442841876840060270703305910419802019463690378721872404832053319725762890293519524955634258417536142683588536851288641887685999984814946222306988970844462733371081968470270993277095858246935717944239929315300270003590928442037406332197038086529036756438685883572814948501021149461629189902643400170441405167625134544593827783038582995519072912979430987533503239424129956158021635582179435493287457551180167565789355390515112787622771825741287971374999834143709283241791195637316757750751234331855830456001975083147064745353263444585028202575581821787586482141831174091024560223212887661870104570747749376453987980256571206785293188054935248208953324868864732582772457698215139488705105731651555918732271977152504304988099697378767607355793317859957198545367479676842649069317877041072386506880061512110545910714492994456363933488463911021634382466976839461990931305281511445317906068970745942165030181518196949868050652701381746936887919687844375666734995019727375367341959703900407715406026329803481590039439238999489436462157106537229831440265121478051802607671267427599023966079929573141431276567458756715530472281096229374970603100770652070393210059524064141380277898909430991537148472266519603559082105926702226962616412982448572098305362479766648739095851185497904345072863344715796342496840952902725707985772107631956202838636699602834912991129668391629924641136127272075571887002694411435118315444567113224187967625945904475104558603735700738907190577351809545025607393411278143241800330924486346351868644557041832031769965646663843117606033957502570595091550041979976870530848662414888120281822941669237373105525152964236259694271876752654206589898471257458488995846126289150289764549177676951981243741848286293003960896299218436989776596965144805519524416212315986311501035318628995927208060750802233616519243148988391695978504966309236415860787710380568574950676368046354325508541213135892169355605606336031690179177181815551168184669667635699386790355198838656461158216487135807663718406714307273104647947017014534984092035837501790410849052363123254900277762823463604564701901440577855978550843383145200028191674526859120336466462841451952706093574679517094153644781286490159851256318612659865719509772531721599256477986936357372754552206104263192890156595348031249903129528823064306755197046007451305274488601231505558112235378227126690244544314662154773903863176897958901971308791483865584608622688510473340147438960710908623

0148970412724875847980070547656945318512706209802499169786506074928088061344951676594652957232798698023
4324835192224065183049668330745088496559789260262334556550165020537757643972563902541135695010096495489
1438178547748406132982691239838391413366568563405763679709118298608214808182228823104018568288488379511
9078566192532440242570639701914277522937963126038344817255496794250973214061210878137545290246733837139
9659393714197685084997642636719790388459436748256157525183373072375680109682129429854659140046073632783
1592307382722774349075688803897198943351152562212117085604915063436295867014971667121783377869459302966
0621093230220328065730379822755774921193167342596935626221931010688588274500427377099132942395445630028
6287240774603056703876241501830252685518704072391159732456721693377959115430547747428438566437427900679
8223932257807115112610568070876553730869087713504650686722607691499315494710957462701085594226287359791
0296012666449361852165065980834427689204237322291521140848495940008866853992649183880821182846570395485
5839603220231858542091955593377873769930880882395492364496409602881811218682665842412975865795187863357
0231715992342235831566631791844417799704184940676810870091655016573623307834200874981231995416921502988
3819265098263612408776395331564639738201750856852025698996502521002458551146222359699984762047974430629
5910585763527432203715112865533846233499531681751760419078530945274577266391815659620656254520776933720
1080115496816026116420178370569520471592261751762260688110267117442441886809032494642839364513029858623
9195495085598289455563701446135640502223406312235393977349974367520493505309929141437536002101380742682
6678494605534407190456189341277003432739317854538245567001354467695832168204954728170085935227504983321
7655431986535959012480919684340712656395689392601868141448907289917138195517355709297611085475906795398
2945861641377932195095464624595227823532369192024088666176953371697612004328442100053869060368353503564
4356534473215668778664506887862248228984154559330449765458234009572934781547518416538858028513595059484
7477501135512094395012573184413043736466011136520345803980279762271345018667696238034947931583547694765
7088304806874603919990318575011047151174318138972103470116477303834509743047407176053047855871551509537
1696493634659251102061133273635516191709393775363551586635166760138061875843253338601600872699960213292
9957444309644762448018804267707813250071060380369446534926834535094431051726711066761599292559860552318
7206855107901787721452391232797235781046358205355036536069051482962448662929949877375501874313458974204
8012001318614339675773820681066371653867657832391330711784448536790430585855449743292224470205689613140
6497040230893953472534082437003317908175937644713403628462442075626843015456578599294186067676976231392
9742892163688568981103 21

VII. TRABAJO FUTURO

Se considera que a partir del método expuesto se podría generar una criba que ayude en el proceso de factorización de números enteros.

VIII. ANEXOS

El lenguaje de programación elegido para hacer la implementación de los códigos es el lenguaje Java. A continuación, se muestra el código implementado sobre la modificación del Binomio de Newton y como halla el factor de otro número.

```
import java.math.BigInteger;
import java.util.LinkedList;
import java.util.List;
import java.util.concurrent.ExecutionException;
import java.util.concurrent.ExecutorService;
import java.util.concurrent.Executors;
import java.util.concurrent.Future;

public class NewtonModification {

    public static NewtonModificationExecutionResult power( String number, int n ) throws IllegalArgumentException{

        if( n < 2 || number.length() < 2){
            throw new IllegalArgumentException();
        }

        int numberOfDigits = number.length();        // Get number of digits in the number

        int digitsPendingToProcess = number.length();
        int digitsProcessed = 0;

        String ansFactor = "";

        // Trivial case: 2 digits in yr

        digitsProcessed = 2;
        String numberToProcess = number.substring( numberOfDigits - digitsProcessed );  // Get 2-digit number in String representation

        BigInteger yr = new BigInteger( numberToProcess );  // Convert String to BigInteger for arithmethic operations
        BigInteger yr_n = yr.pow( n );                      // Calculate yr^n

        String ans = yr_n.toString();                       // Final Answer. String format.

        digitsPendingToProcess = numberOfDigits - digitsProcessed;

        // Non-trivial case. Number with more than 2 digits

        while( digitsPendingToProcess != 0 ){               // More digits to process?
```

```
            numberToProcess = number.substring( numberOfDigits - digitsProcessed - 1);  // Update numberToProcess with new digit.

            // First term to calculate: d_{t}^n

            BigInteger dt = new BigInteger( numberToProcess.substring(0, 1) );  // Get number's left-most digit.

            // It may happen dt == 0. Handle two different cases

            if( dt.compareTo( BigInteger.ZERO ) != 0 ){ // dt != 0

                  BigInteger dt_n = dt.pow( n );

                  yr = new BigInteger( numberToProcess.substring(1) );    // yr holds first part of the answer.

                   // Second term to calculate

                  // Calculate yr_k from yr_{1} to yr_{n-1}.
                  // This can be done in 2 ways

                  // Approach 1)
                  // As yr_n is known, calculate yr_k just dividing and saving in a list.
                  // It is better to do this that recalculate every yr_k
                  // The problem with this is that for large numbers the program runs out of space

                  // Approach 2)
                  // Do not save every yr_k. Just pass yr and yr_n to BinomialTermCalculator and there calculate yr_k but not store other values.
                  // Problems: Too much recalculation of yr_k.

                  // Second approach selected.

                  ExecutorService executor = Executors.newFixedThreadPool(n);

                  List<BinomialTermCalculator> terms = new LinkedList<BinomialTermCalculator>();

                  for( int k = 1; k < n; k++ ){
                        terms.add( new BinomialTermCalculator( n, k, digitsProcessed + 1, dt, yr, yr_n )  );
                  }

                  List<Future<BigInteger>> tasks = null;

                  try {
                         tasks = executor.invokeAll(terms);
                  } catch (InterruptedException e) {
                        // TODO Auto-generated catch block
                        e.printStackTrace();
                  }

                  List<BigInteger> binomialTerms = new LinkedList<BigInteger>();

                  for( Future<BigInteger> t : tasks ){
                        try {
                                    binomialTerms.add( t.get() );
                        } catch (InterruptedException | ExecutionException e) {
                              // TODO Auto-generated catch block
```

```
            e.printStackTrace();
        }
}

executor.shutdown();

//System.out.println("List of binomial terms ... " + binomialTerms);

// Sum and multiply

BigInteger secondTerm = BigInteger.ZERO;

for( BigInteger term : binomialTerms ){
        secondTerm = secondTerm.add(term);
}

secondTerm = secondTerm.multiply( dt );

// Third term to calculate already known and stored in yr_n

// Ensemble answer

// Take numberToProcess.length()  digitsProcessed digits from yr_n

String yrNAsString = yr_n.toString();
int yrNLength = yrNAsString.length();

int numberLength = numberToProcess.length();

int digitsToTake = numberLength - 1;

//System.out.println("Digits to take for term 3 => " + digitsToTake );

String ans3 = "";
String toAdd = "";

if( yrNLength >= digitsToTake  ){

        // Split yr_n into last part of the answer and part to add

        ans3 = yrNAsString.substring( yrNLength - digitsToTake );
        toAdd = yrNAsString.substring( 0, yrNLength - digitsToTake  );

}else{

          // Fill ans3 with zeroes at left

        for( int i = 0; i < digitsProcessed - yrNLength; i++ ){
                ans3 = ans3 + "0";
        }

        ans3 += yrNAsString ;

        toAdd = "0";
}
```

```
            // Sum term2 with toAdd

            secondTerm = secondTerm.add( new BigInteger( toAdd ) );

            // Take (n-1)*numberToProcess.length() digits from secondTerm

            String secondTermAsString = secondTerm.toString();

            int size2 = secondTermAsString.length();

            digitsToTake = (n-1)*(numberLength - 1);

            String ans2 = "";

            if( size2 >= digitsToTake ){
                  ans2 = secondTermAsString.substring( size2 - digitsToTake );
                  toAdd = secondTermAsString.substring(0,size2 - digitsToTake ) ;
            }else{

                    // Fill ans2 with zeroes at left

                  for( int i = 0; i < digitsToTake - size2; i++ ){
                        ans2 = ans2 + "0";
                  }

                  ans2 += secondTermAsString ; // Concatenate second term

                  toAdd = "0";
            }


            if( toAdd.equals("")){
                  toAdd = "0";
            }

            // Add dt_n with toAdd

            dt_n = dt_n.add( new BigInteger( toAdd ) );
            String ans1 = dt_n.toString();

            ans = ans1 + ans2 + ans3;
            ansFactor = secondTerm + ans3;

            yr_n = new BigInteger( ans );

      }

      // Advance iteration

      digitsProcessed++;
      digitsPendingToProcess--;

}

// Create answer
```

```
            NewtonModificationExecutionResult result = new NewtonModificationExecutionResult( ans, ansFactor, yr.toString()
);
            return result;
        }

        public static void main ( String[] args ){

            NewtonModificationExecutionResult res = NewtonModification.power( args[0], Integer.parseInt( args[1]) );

            System.out.println( res.getAnswer() );
            System.out.println( res.getMultiple() ) ;
            System.out.println( res.getFactor() ) ;
        }
}
```

IX. REFERENCIAS

[1] D. L. Hostalot, "Ataque de factorización a RSA," [Online]. pp. 50-58-52-56-59. Disponible en: http://www.researchgate.net/...Ataque...RSA

[2] A. M. Odlyzko, "The future of integer factorization," AT&T Bell Laboratories, Murray Hill, NJ 07974, Jul 1995, [Online]. pp. 4-9-9. Disponible en: http://http://www.dtc.umn.edu/~odlyzko/doc/future.of.factoring.pdf

[3] J. Brillhart and J. L. Selfridge, "Some factorizations of $2^n \pm 1$ and related results", *Math. Comp.*, 1967, pp. 87-96.

[4] S. Cook, "The P versus NP problem" Clay Mathematics Institute, Disponible en www.claymath.org.

[5] M. Du Sautoy "La música de los números primos", Editorial Acantilado, ISBN 978-84-96489-83-7, Séptima Edición, Disponible en: www.librosmaravillosos.com/index.html.

[6] L. S. Carrasco Pérez "factorización de enteros", Universidad Autónoma Metropolitana, México, 20 de julio de 2012, tesís de maestría en ciencias matemáticas aplicadas e industriles.

[7] H. Riesel "Números primos y métodos computacionales de factorización", 2da Edición, editorial Birkhäuser.

[8] J. Henao Barbosa, "Un método para hallar potencias enésimas de un número" Colombia, Dirección Nacional De Derecho De Autor, Libro 10 Tomo 492 Partida 405.

[9] A. Baldor, *Álgebra*, edición de 1988, México: Compañía Cultural Editora y Distribuidora de Textos Americanos, S.A. (CCEDTA), Edición Códice América, S.A. ISBN 84-357-0062-3 y Publicaciones cultural s.a. de C.V ISBN 968-439-211-7, 1988, p. 97.

[10] A. Baldor, *Aritmética*, Décima reimpresión, México: Compañía Cultural Editora y Distribuidora de Textos Americanos, S.A. (CCEDTA), Edición Códice América, S.A. ISBN 84-357-0062-3 y Publicaciones cultural s.a. de C.V ISBN 968-439-211-7, 1995, pp. 31-375.