Método de Factorización con Fracciones Continuas

David Antonio Garzón Avendaño, Esneider Fabian Sierra Alba, and Julio César Vásquez Arenas

Universidad Nacional de Colombia

Resumen Repasamos las ideas esenciales detrás del Algoritmo de Factorización con Fracciones Continuas a través de ejemplos. Primero recordando el algoritmo clásico de factorización (Trial Division) y el Algoritmo de Fermat que aprovecha el hecho de que cualquier factorización puede verse como una diferencia de cuadrados. Continuamos con el Método de Kraitchik que generaliza esa idea usando congruencias, el de Lehmar y Powers quienes proponen la utilización de fracciones continuas y el de Brilliart y Morrison quienes utilizan la eliminación gaussiana para hacer más eficiente al algoritmo.

Palabras claves: Algoritmo de Factorización · Factorización · Fracciones Continuas · Método de Kraitchik-Fermat · Factores · Método de Fermat · Trial Division

1. Trial Division

Cuando intentamos factorizar un número N siempre pensamos en encontrar dos o más factores no triviales de N, por lo que es natural pensar como primer método probar con números menores que N, y de hecho en esto consiste nuestro primer algoritmo, pero con algunas mejoras.

En un principio podríamos pensar en probar con todos los números menores que N, sin embargo conforme N se va volviendo cada vez más grande, hacer pruebas con $N-2$ números se va volviendo menos practico, tan solo piense en el número 1000001, hacer 999999 pruebas no suena nada practico. Por lo que se vuelve necesario pensar cómo reducir la cantidad de números con los que vamos a probar.

Teorema 1. *Sea $N \in \mathbb{N}$ con $N > 1$, si N es un número compuesto entonces N tiene al menos un factor primo p tal que $p \leq \sqrt{N}$.*

Demostración. (Por contradicción) Sea $N \in \mathbb{N}$ con $N > 1$. Supongamos que $N = pb$, con p el factor primo más pequeño de N y supongamos que $p > \sqrt{N}$. Como N no es primo entonces $b \neq 1$, además como p es el factor primo más pequeño de N entonces $p \leq b$, luego tenemos que $pb > \sqrt{N}\sqrt{N} = N$

Con el resultado anterior hemos reducido la cantidad de números con los que debemos probar, y en particular basta con probar con todos los números $n \leq \lfloor \sqrt{N} \rfloor$, he incluso si $\sqrt{N}$ es un número entero ya acabamos, debido a que N seria un cuadrado perfecto y una factorización no trivial seria $\sqrt{N}\sqrt{N}$. Sin embargo incluso con la cota anterior seguimos probando aún con demasiados números innecesarios, tan solo piense en los números pares en el caso en el que $2 \nmid N$, en este caso dividir por cualquier número par no tendría sentido, por esto veamos el siguiente teorema.

Teorema 2. *Teorema fundamental de la aritmética (TFA): Un número natural es primo o producto de números primos donde dicha descomposición es única salvo orden.*

Teorema 3. *Sea P un número primo y a, b números compuestos. Si b es un múltiplo de P (es decir $P \mid b$) y a no es un múltiplo de P, es decir ($P \nmid a$), entonces $b \nmid a$*

Demostración. Sean $b = p_0^{\alpha_0} p_1^{\alpha_1} \dots P^{\alpha_i} \dots p_n^{\alpha_n}$ y $a = j_0^{\beta_0} j_1^{\beta_1} \dots j_m^{\beta_m}$ las factorizaciones en números primos de a y b. Como $P \nmid a$ entonces $P \notin \{j_0, j_1, \dots, j_n\}$ conjunto de factores primos de a. Ahora veamos que no existe c tal que $bc = a$. Tomemos la factorización en números primos de $c = k_0^{\gamma_0} k_1^{\gamma_1} \dots k_r^{\gamma_r}$, luego para cualquier c tenemos que el producto entre c y b es $cb = k_0^{\gamma_0} k_1^{\gamma_1} \dots k_r^{\gamma_r} p_0^{\alpha_0} p_1^{\alpha_1} \dots P^{\alpha_i} \dots p_n^{\alpha_n}$, entonces $P \in \{k_0, k_1, \dots, k_r, p_0, p_1, \dots, P, \dots, p_n\}$ conjunto de factores primos de bc. Como P pertenece al conjunto de factores primos de bc pero no al conjunto de factores primos de a, usando el TFA tenemos que $bc \neq a$ debido a que la factorización de un número siempre es única salvo orden.

Note que la demostración anterior implica que solo es necesario probar con los números primos, ya que al estar probando con todos los números desde 2 hasta $\sqrt{N}$ estaremos probando con demasiados números innecesarios, por ejemplo, si $3 \nmid N$ por el teorema anterior ninguno de sus multiplos $(6, 9, 12, 15, ...)$ va a dividir a N. Gracias a los dos resultados anteriores podemos presentar el Algoritmo de Trial división.

Algoritmo de Trial Division Dado un número en $N \in \mathbb{N}$ con $N > 1$, este algoritmo encuentra una factorización no trivial de N si dicho número es compuesto. Para ello es necesario ir probando con cada uno de los posibles divisores de N. Como primer paso verificamos si la raíz de N es entera, ya que en dicho caso ya acabamos puesto que una factorización no trivial de N es $\sqrt{N}\sqrt{N}$, caso contrario usando los teoremas 1 y 2 podemos establecer que solo es necesario probar con i que toma valores primos desde 2 hasta $\lfloor \sqrt{N} \rfloor$.

Acá presentamos una implementación en Mathematica:

```
TrialDiv[N_] :=
 Module[{num = N, m = 0, n = 0},
  If[IntegerQ[Sqrt[num]], Return[{Sqrt[num]}]];
  For[i = 2, i < Floor[Sqrt[num]], i++,
   If[PrimeQ[i],
     If[Mod[num, i] == 0, m = i;
       n = num/m;
       Return[{m, n}]
       ];
     ];
   ];
  Return[{num}]]
```

2. Método de Fermat

El siguiente método para atacar el problema de factorizar un número se llama el Método de Fermat, este método parte de la idea de factorizar una diferencia de cuadrados $x^2 - y^2 = (x + y)(x - y)$, lo que resulta en una factorización no trivial de N siempre y cuando $(x - y) > 1$

Teorema 4. *Sea $N \in \mathbb{N}$ con con $N > 1$ un número impar positivo y compuesto, entonces N se puede escribir como diferencia de dos cuadrados:*

Demostración. Como N es compuesto e impar solo es necesario verificar la siguiente identidad

(Note que para que N sea un número impar, c, d deben ser números impares, luego $c + d$ y $c - d$ son divisibles entre 2)

$$\begin{aligned} N = cd &= \left(\frac{1}{2}(c+d)\right)^2 - \left(\frac{1}{2}(c-d)\right)^2 \\ &= \left(\frac{c^2 + 2cd + d^2}{4}\right) - \left(\frac{c^2 - 2cd + d^2}{4}\right) \\ &= \frac{4cd}{4} \\ &= cd. \end{aligned}$$

2.1. Algoritmo de Fermat

Dado un número en $N \in \mathbb{N}$ tal que $N > 1$, este algoritmo encuentra una factorización no trivial de N si dicho número es compuesto. Si N es par, nuestro algoritmo retorna la factorización $(2)(\frac{N}{2})$, Si N es impar este algoritmo parte de la idea de factorizar un número impar como diferencia de dos cuadrados,

por lo que para encontrar estos dos cuadrados debemos probar con enteros a desde $\lceil\sqrt{N}\rceil$ hasta $\lfloor\frac{N+9}{6}\rfloor$ (esta cota la probaremos más adelante), si $a^2 - N$ es un cuadrado perfecto entonces tenemos que una factorización no trivial es $((\sqrt{a^2-N}) - a)((\sqrt{a^2-N}) + a)$.

Veamos el siguiente implementación en Mathematica:

```
FermatAlg[n_] := Module[{num = n, b, a},
  If[IntegerQ[Sqrt[num]], Return[{Sqrt[num]}]];
  If[Mod[num, 2] == 0, Return[{2, num/2}]];

  For[a = Ceiling[Sqrt[num]], a <= (num + 9)/6, a++,
   b =  Sqrt[a^2 - num];

   If[IntegerQ[b], Return[{a - b, a + b}]]
   ];
  Return[{num, 1}]
  ]
```

Este algoritmo es especialmente veloz cuando cuando tenemos que el número N que deseamos factorizar tiene como factores a dos números cuya distancia a $\sqrt{N}$ es relativamente pequeña, y a medida que crece la distancia entre estos factores, requerimos cada vez más iteraciones. Para mostrar esto de manera un poco más clara veamos qué pasa en el algoritmo.

Sea N un número compuesto impar y sea $u = \lceil\sqrt{N}\rceil$. por el Teorema 4 garantizamos la existencia de dos números a, b tal que $N = (a+b)(a-b)$, aplicando el algoritmo para encontrar los números a y b tenemos:

$$a_0 = u \longrightarrow \sqrt{u^2 - N} = b_0$$

En esta primera iteración tenemos los primeros candidatos para a y b, note que si $\sqrt{u^2 - N}$ no es un número entero, tenemos que pasar a la siguinete iteración, en donde:

$$a_1 = u + 1 \longrightarrow \sqrt{(u+1)^2 - N} = b_1$$

haciendo este mismo procedimiento $i - veces$ tenemos que:

$$a_i = u + i \longrightarrow \sqrt{(u+i)^2 - N} = b_i$$

Note que en cada iteración $a_i > a_{i-1}$ y $b_i > b_{i-1}$, por lo que $(a_i + b_i) > (a_{i-1} + b_{i-1})$ y $(a_i - b_i) < (a_{i-1} - b_{i-1})$, acá se puede evidenciar qué nuestro algoritmo arranca buscando factores cercanos a $\lceil\sqrt{N}\rceil$ y con cada iteración va buscando factores cada vez más lejanos a $\lceil\sqrt{N}\rceil$.

Otra pregunta natural es cómo se garantiza que este algoritmo termina, sin embargo, para esto solo basta con analizar el caso $a_i = \frac{N+1}{2}$, como N es impar a_i es un número entero. Veamos qué pasa con b_i:

$$\begin{aligned} b_i &= \sqrt{\left(\frac{N+1}{2}\right)^2 - N} \\ &= \sqrt{\left(\frac{N^2+2N+1}{4}\right) - N} \\ &= \sqrt{\frac{N^2+2N+1}{4} - \frac{4N}{4}} \\ &= \sqrt{\frac{N^2-2N+1}{4}} \\ &= \sqrt{\left(\frac{N-1}{2}\right)^2} \\ &= \frac{N-1}{2} \end{aligned}$$

Acá como N es impar b_i es un número entero, entonces como a_i y b_i son enteros, nuestro algoritmo para y $a_i = a$ y $b_i = b$. Ahora tomemos la diferencia de cuadrados $a^2 - b^2$ y factoricemos:

$$\begin{aligned} a^2 - b^2 &= \left(\frac{N+1}{2}\right)^2 - \left(\frac{N-1}{2}\right)^2 \\ &= \left(\frac{N+1}{2} + \frac{N-1}{2}\right)\left(\frac{N+1}{2} - \frac{N-1}{2}\right) \\ &= \left(\frac{2N}{2}\right)\left(\frac{2}{2}\right) \\ &= (N)(1) \end{aligned}$$

Lo anterior es una factorización trivial de N, sin embargo por la manera en la cual funciona nuestro algoritmo, en este punto ya se habrán descartado todos los candidatos a factor de N, por lo que este caso solo sucede cuando N es primo, más adelante introduciremos una mejor cota para las iteraciones del algoritmo.

Ahora veamos cuál es el peor caso para números compuestos. Algo importante a remarcar es que nuestro algoritmo busca factores de un número, pero estos factores no necesariamente son primos. Entonces para construir el peor caso para números compuesto tenemos que buscar números los cuales todos sus factores no triviales posibles estén lo más alejados posible entre ellos y de la raíz de N para así maximizar la cantidad de ciclos. Lo anterior es posible con números de la forma $N = 3P$ con $P > 3$ un número primo, ya que como los únicos dos factores posibles de N son 3 y P entre más crezca P todos los factores no triviales de N van a estar más lejos entre ellos y de la raíz.

Teorema 5. *Sea N un número impar positivo, entonces el algoritmo de Fermat debe probar con números desde $\left\lceil \sqrt{N} \right\rceil$ hasta $\lfloor \frac{N+9}{6} \rfloor$.*

Demostración. Sea N un número impar, mayor que uno, y sea d el menor factor de N tal que $d > \sqrt{N}$. Note que el método de Fermat halla una factorización de la forma $N = d\frac{N}{d}$, la cual también podemos expresar como $N = (a+b)(a-b)$, entonces veamos que como d y N son enteros positivos podemos igualar ambas expresiones de la siguiente manera, $d = (a+b)$ y $\frac{N}{d} = (a-b)$. Ahora resolviendo este sistema para a tenemos:

$$a + b = d$$
$$a - b = \frac{N}{d}$$

sumando ambas ecuaciones y despejando para a tenemos:

$$a = \frac{1}{2}\left(d + \frac{N}{d}\right)$$

Además tenemos que el peor caso para nuestro algoritmo son los números de la forma $N = 3p$ y que $N = (a-b)(a+b)$ con a, b enteros positivos, por lo que no queda otra más que $(a-b) = 3$ y $(a+b) = p$. Entonces remplazando en la primera ecuación tenemos que:

$$a = \frac{1}{2}\left(d + \frac{N}{d}\right) \leq \frac{1}{2}\left(\frac{N}{3} + 3\right) = \frac{N+9}{6}$$

En particular como a es un número entero, basta con que nuestro algoritmo haga una búsqueda entre $\left\lceil \sqrt{N} \right\rceil$ hasta $\lfloor \frac{N+9}{6} \rfloor$ [1].

3. Método de Kraitchik-Fermat

El método de Kraitchik(1920) ofrece una generalización del método de Fermat. En lugar de encontrar dos enteros u y v tales que $u^2 - v^2 = N$, Kraitchik atacó el problema considerando u y v tales que $u^2 - v^2$ fuera un múltiplo de N, y si suponemos que $u \not\equiv \pm v \pmod{N}$ se tiene que $mcd(u-v, N)$ es un factor propio de N. Para encontrar (o construir) u y v primero consideramos la raíz del cuadrado mayor y más cercano a N, es decir $x_1 = \lceil \sqrt{N} \rceil$, luego consideramos la sucesión $\{x_{i+1} = x_i + 1 : 1 \leq i \leq k\}$,(por el momento k aumenta si no se puenden llegar a construir los elementos u y v) y con ella construimos la sucesión $\{F(x_i)\}$ donde $F(x) = x^2 \pmod{N}$. Ahora bien, si $v^2 = \prod_{i=1}^{k} F(x_i)$ y $u = \prod_{i=1}^{k} x_i$, entonces

$$u^2 = (\prod_{i=1}^{k} x_i)^2 = \prod_{i=1}^{k} (x_i)^2 \equiv \prod_{i=1}^{k} F(x_i) = v^2 \pmod{N}.$$

Una ayuda importante para construir v^2 es tomar la factorización de algunos elementos de $\{F(x_i)\}$, teniendo en cuenta que son "fáciles" de factorizar, y combinar elementos tales que la potencia de cada factor primo sea par. El inconveniente radica en que el máximo común divisor sea 1 o N, para ello consideremos los siguientes teoremas:

Teorema 6. *Dado $N \in \mathbb{Z}$ compuesto e impar y dados $x, y \in \mathbb{Z}$ tales que $x^2 \equiv y^2$ (mód N) donde $x \not\equiv \pm y$ (mód N), entonces $mcd(x+y, N)$ y $mcd(x-y, N)$ son factores propios de N.*

Demostración. Por hipótesis se tiene que $N \mid x^2 - y^2 = (x-y)(x+y)$ y por las incongruencias sabemos que $N \nmid (x-y)$ y $N \nmid (x+y)$ con lo cual $mcd(x+y, N) \neq N \neq mcd(x-y, N)$, y $mcd(x+y, N), mcd(x-y, N) > 1$ ya que si $mcd(N, x-y) = 1$ entonces $N \mid x+y$ lo que es una contradicción, de manera similar se llega a una contradicción si $mcd(N, x+y) = 1$.

Teorema 7. *Si N es un número entero positivo e impar con al menos dos factores primos distintos, y si x y y son enteros aleatorios sujetos a la condición $x^2 \equiv y^2$ (mód N), entonces, con probabilidad $\leq 1/2$, el $mcd(x-y, N)$ es un factor propio de N.*
(Esta demostración está como ejercicio en el Taller.)

Ejemplo 1. Para dejar en claro la idea de Kraitchik encontremos un factor propio de $N = 3427$. Primero tomamos $x_1 = \lceil \sqrt{N} \rceil = 59$ y con la sucesión

$$\{59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70\}$$

y mediante la función $F(x) = x^2 \pmod N$ obtenemos la sucesión

$$\{54, 173, 294, 417, 542, 669, 798, 929, 1062, 1197, 1334, 1473\}$$

donde

$59^2 \equiv 54 = 2^1 \cdot 3^3$ $\quad 60^2 \equiv 173 = 173^1$ $\quad 61^2 \equiv 294 = 2^1 \cdot 3^1 \cdot 7^2$
$62^2 \equiv 417 = 3^1 \cdot 139^1$ $\quad 63^2 \equiv 542 = 2^1 \cdot 271^1$ $\quad 64^2 \equiv 669 = 3^1 \cdot 223^1$
$65^2 \equiv 798 = 2^1 \cdot 3^1 \cdot 7^1 \cdot 19^1$ $\quad 66^2 \equiv 929 = 929^1$ $\quad 67^2 \equiv 1062 = 2^1 \cdot 3^2 \cdot 59^1$
$68^2 \equiv 1197 = 3^2 \cdot 7^1 \cdot 19^1$ $\quad 69^2 \equiv 1334 = 2^1 \cdot 23^1 \cdot 29^1$ $\quad 70^2 \equiv 1473 = 3^1 \cdot 491^1$

luego consideramos productos en donde la potencia de los factores primos sea par, las cuales pueden ser:

$$\text{Opción 1: } 54 \cdot 294 = 2^2 \cdot 3^4 \cdot 7^2 = (2 \cdot 3^2 \cdot 7)^2$$
$$\text{Opción 2: } 54 \cdot 798 \cdot 1197 = 2^2 \cdot 3^6 \cdot 19^2 = (2 \cdot 3^3 \cdot 19)^2$$

con lo cual, en la opción 1:

$$u = 59 \cdot 61 \equiv 172 \pmod{3427} \qquad v = 2^2 \cdot 3 \cdot 7 \equiv 126 \pmod{3427}$$

y en la opción 2:

$$u = 59 \cdot 65 \cdot 68 \equiv 328 \pmod{3427} \quad v = 2 \cdot 3^3 \cdot 7 \cdot 19 \equiv 328 \pmod{3427}.$$

Por tanto, solo consideramos la opción 1, de la cual obtenemos que $mcd(173 - 126, 3427) = 23$ (además $mcd(173 + 126, 3427) = 149$). De manera que $N = 3427 = 23 \cdot 149$.

4. Factorización con Fracciones Continuas

Un problema del método de Kraitchik consiste en que las combinaciones de las potencias no siempre dan como resultado una congruencia $u^2 \equiv v^2 \pmod{N}$ con $u \not\equiv v \pmod{N}$ y además encontrar dicha combinación puede requerir de un número considerable de elementos en la sucesión $\{x_i : 1 \leq i \leq k\}$, para resolver este problema Henry Lehmer y Ralph Powers en 1931, en lugar de considerar la función $F(x) = x^2 \pmod{N}$, consideraron usar convergentes de la fracción continua de $\sqrt{N}$.

Si A_n/B_n es la n-ésima convergente de $\sqrt{N}$ y sea

$$Q_n = A_n^2 - NB_n^2,$$

entonces $Q_n \equiv A_n^2 \pmod{N}$. De manera que podemos considerar las sucesiones $\{A_i\}$, $\{Q_i\}$ para construir u y v teniendo en cuenta la eliminación Gaussiana. La razón por la cual se usan convergentes de las fracciones continuas es debido a que los elementos x_i del método de Kraitchik son mayores que $\sqrt{N}$ mientras que los elementos Q_i cumplen la desigualdad $|Q_i| < 2\sqrt{N}$, así, los Q_i son menores, en valor absoluto, que los x_i y por tanto son "fáciles" de factorizar.

Aunque el uso de fracciones parciales permite encontrar factorizaciones generalmente pequeñas para buscar las combinaciones lineales que ayudan a construir los cuadrados perfectos, no resulta muy eficiente buscarlas por prueba y error. Una estrategia para encontrar estas combinaciones fue descrita por John Brilliart y Michael Morrison usando ideas simples del álgebra lineal.

A cada exponente se le puede asociar un vector de exponentes de la siguiente forma: sea $N = \prod_i^m p_i^{\alpha_i}$ donde p_i es el i-ésimo primo y p_m el mayor primo que divide a N. En esta formulación debemos considerar todos los $p < p_m$ incluso si su exponente correspondiente es 0. El vector de exponentes asociado a N sería $(\alpha_1, \alpha_2, ...\alpha_m)$. Por ejemplo, para $4680 = 2^3 \cdot 3^2 \cdot 5 \cdot 13$, su vector de exponentes asociado sería $(3, 2, 1, 0, 0, 1)$.

Teorema 8. *N es un cuadrado perfecto si y sólo si todos los exponentes de su factorización en números primos son pares.*

Gracias al anterior teorema podemos simplificar el problema. Realmente no nos interesan los exponentes concretos de una factorización particular, basta con obtener una combinación de números cuya suma de sus vectores de exponentes asociados módulo 2 sea el vector nulo.

La estrategia consiste en elegir un subconjunto de números primos, que llamaremos una base, sobre la cual descomponer por medio de Trial Division los números encontrados mediante el método de las fracciones continuas, es decir, se deben descartar aquellos números que no pueden descomponerse en dicha base. Sea n la longitud de la base. Si elegimos m números factorizables en dicha base con $m > n$, podemos construir una matriz de $m \times n$ donde cada fila corresponda con el vector de exponentes módulo 2 asociado a cada número seleccionado.

Teorema 9. *Si una matriz tiene más filas que columnas, alguna de sus filas es combinación lineal de las demás.*

Gracias al anterior teorema podremos encontrar una fila que sea combinación lineal de las demás, equivalentemente, podemos encontrar una combinación lineal cuya suma dé el vector nulo, que es justamente lo que estamos buscando. Esto se puede hacer fácilmente mediante el Método de Reducción de Gauss. Adicionalmente, si adjuntamos una matriz identidad de tamaño $n \times n$ y le aplicamos las mismas transformaciones que se realizan sobre la matriz anteriormente construida, bastará con chequear las filas de ceros en dicha matriz y la matriz adjunta nos mostrará la combinación lineal que hace que dicha suma dé 0.

Resulta conveniente incluir el -1 entre los números que conforman la base con el objetivo de poder factorizar también números negativos. Adicionalmente hay que notar que la igualdad $A^2 - NB^2 = Q$ muestra que para un p primo tal que $p|Q$ se cumple que $(\frac{A}{B})^2 \equiv N \mod p$, es decir, N es un residuo cuadrático módulo p. Por tal motivo la base sólo debería incluir primos p para los cuales N sea un residuo cuadrático.

Para entender en más detalle cómo funciona la eliminación Gaussiana, volvamos a buscar un factor no trivial de $N = 3427$ usando la base $B = \{-1, 2, 3, 7\}$. En primer lugar debemos calcular las convergentes de $\sqrt{3427}$, las cuales son $\{58, 59, \frac{117}{2}, \frac{644}{11}, \frac{761}{13}, \frac{1405}{24}, \frac{2166}{37}, \frac{36061}{616}, ...\}$. Para cada convergente debemos calcular su Q correspondiente, tomando el numerador como A y el denominador como B, mediante la fórmula $Q = A^2 - NB^2$, para la primera convergente tendríamos $Q = 58^2 - 3427 \cdot 1^2 = -63$, obteniendo la congruencia 58^2 mód $3427 \equiv -63 = -1 \cdot 3^2 \cdot 7^1$. Como nuestra Base tiene 4 números debemos repetir el mismo ejercicio con el resto de convergentes por lo menos hasta encontrar 5 Qs factorizables en nuestra base. Esta factorización se realiza mediante el clásico algoritmo de Trial Division.

$58^2 \equiv -63 = -1 \cdot 3^2 \cdot 7^1$ $\quad 59^2 \equiv 54 = 2^1 \cdot 3^2$ $\quad 117^2 \equiv -19 = -1 \cdot 19^1$

$644^2 \equiv 69 = 3^1 \cdot 23^1$ $\quad 761^2 \equiv -42 = -1 \cdot 2^1 \cdot 3^1 \cdot 7^1$ $\quad 1405^2 \equiv 73 = 73^1$

$2166^2 \equiv -7 = -1 \cdot 7^1$ $\quad 36061^2 \equiv 9 = 3^2$

Así los Qs factorizables en la base $\{-1, 2, 3, 7\}$ forman el siguiente conjunto $F = \{-63, 54, -42, -7, 9\}$ y sus vectores de exponentes son los siguientes:

$$-63 = (1,0,2,1) \qquad 54 = (0,1,3,0) \qquad -42 = (1,1,1,1)$$
$$-7 = (1,0,0,1) \qquad 9 = (0,0,2,0)$$

A estos vectores se les aplica módulo 2 y construimos una matriz en la cual a cada fila le corresponde uno de los vectores de exponentes módulo 2 de los números en F. Adicionalmente le adjuntamos una matriz identidad de tamaño 5×5.

$$\begin{pmatrix} 1&0&0&1 \\ 0&1&1&0 \\ 1&1&1&1 \\ 1&0&0&1 \\ 0&0&0&0 \end{pmatrix} \begin{pmatrix} 1&0&0&0&0 \\ 0&1&0&0&0 \\ 0&0&1&0&0 \\ 0&0&0&1&0 \\ 0&0&0&0&1 \end{pmatrix}$$

A ambas matrices les aplicamos la reducción de Gauss, obteniendo

$$\begin{pmatrix} 1&0&0&1 \\ 0&1&1&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \end{pmatrix} \begin{pmatrix} 0&0&0&1&0 \\ 0&0&1&1&0 \\ 1&0&0&1&0 \\ 0&1&1&1&0 \\ 0&0&0&0&1 \end{pmatrix}$$

Finalmente buscaremos en la matriz de la izquierda las filas de ceros, estas filas representan combinaciones lineales de los vectores de exponentes de los números en F que hacen que el producto de ellos sea un cuadrado perfecto. Por ejemplo para la quinta fila tenemos que $F_2F_3F_4 = (54)(-42)(-7) = (2 \cdot 3^3)(-1 \cdot 2 \cdot 3 \cdot 7)(-1 \cdot 7) = (2^2 \cdot 3^4 \cdot 7^2) = 126^2$ es un cuadrado perfecto. Además $126^2 \equiv (59^2 \cdot 761^2 \cdot 2166^2) = (59 \cdot 761 \cdot 2166)^2 \equiv (-172)^2$, es decir, $126^2 \equiv (-172)^2$ mód 3427, pero $126 \not\equiv \pm 172 \mod 3427$, con lo cual $\gcd(126 + 172, 3427) = 23$ es un factor propio de 3427.

A continuación incluimos un código en Mathematica que implementa el algoritmo aquí expuesto.

```
(*Fatoriza un Numero entero usando el método de las
Fracciones Parciales sobreuna Base de primos,
calculando nc número de convergentes de la Fracción Parcial
y con ad filas adicionales en la matriz con respecto al
número de elementos en la Base*)

Factorizacion[Numero_,Base_,nc_,ad_]:=Module[{A,B,Cs,Q,V,M,M1,M2,x,y,i,j,
            exponentes,modulos,cuadrados},
    Cs=Convergents[Sqrt[Numero],nc];
    exponentes=Table[None,Length[Base]+ad];
    modulos=Table[None,Length[Base]+ad];
    cuadrados=Table[None,Length[Base]+ad];
```

```
(*Se encuentran los vectores de exponentes de los números
hallados por medio de las convergentes de raíz de n que pueden
ser factorizados en la Base dada*)

    For[i=1;j=1,i<=Length[exponentes],i++,
        V=None;
        While[j<=Length[Cs]&&V==None,
            A=Numerator[Cs[[j]]];B=Denominator[Cs[[j]]];
            Q=A^2-Numero B^2;V=Factorizable[Q,Base];j++
        ];
        If[j>Length[Cs],Return[Factorizacion[Numero,Base,2nc,ad]]];
        exponentes[[i]]=V;modulos[[i]]=Mod[V,2];cuadrados[[i]]=A;
    ];

(*Se construye y reduce la matriz con los vectores
 anteriormente encontrados*)
    M=Join[Join[modulos],IdentityMatrix[Length[Base]+ad],2];
    M=RowReduce[M,Modulus->2];
    M1=M[[;,1;;Length[Base]]];
    M2=M[[;,Length[Base]+1;;2Length[Base]+ad]];

    (*Se buscan las combinaciones lineales que producen filas de
    ceros en la matriz por medio de una matriz adjunta*)
    For[i=Length[M],i>0&&M1[[i]]==Table[0,Length[Base]],i--,
        x=1;y=1;V=Table[0,Length[Base]];
        For[j=1,j<=Length[Base]+ad,j++,
            If[M2[[i]][[j]]==1,
                V=V+exponentes[[j]];
                y=Mod[y cuadrados[[j]],Numero];
            ];
        ];
        For[j=1,j<=Length[Base],j++,
            x=Mod[x PowerMod[Base[[j]],V[[j]]/2,Numero],Numero];
        ];
        If[x!=y&&x!=Numero-y&&Numero-x!=y,Return[GCD[x-y,Numero]]];
    ];
    Return[None];
];
```

A modo de nota podemos mencionar que el método de fracciones parciales tiene una complejidad $\mathcal{O}(N^{\epsilon(N)})$ donde $\epsilon(N) \approx 2\sqrt{\frac{ln(lnN)}{lnN}}$.

Referencias

1. Martin,G.: Favtorization Upper Bound. Mathematics Stack Exchange(2016).
2. Bressoud, D., Wagon, S.: A Course In ComputationaI Number Theory. John Wiley & Sons, Hoboken, New Jersey (2000).
3. Crandall, R., Pomerance, C.: Prime Numbers A Computational Perspective. Springer, New York, New York (2005).
4. Morrison, M.A., Brillhart, J.: A Method of Factoring and the Factorization of F7. MATHEMATICS OF COMPUTATION. 29(129), 183–205 (1975).
5. Pomerance, C.: A Tale of Two Sieves. NOTICES OF THE AMS. 4(12), 1473–1485 (1996).
6. Wagstaff, S.S.: The Joy of Factoring. American Mathematical Society, Providence, Rhode Island (2013).