Avances en el desarrollo de un método de factorización de enteros de complejidad polinomial

Hugo D. Scolnik[1] and Julia V. Picabea[2]

[1] Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina
hscolnik@gmail.com
[2] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina
picotea@hotmail.com

Resumen En este trabajo presentaremos diversos resultados conseguidos recientemente cuyo objetivo es lograr un método de factorización de enteros de complejidad polinomial. Se presentan resultados teóricos mientras que diversos algoritmos están en proceso de investigación.

1. Introducción

Hoy en día todavía se ignora si el problema de descomponer a un entero en sus factores primos tiene complejidad subexponencial o polinomial (usando computadoras *normales*, dejaremos las cuánticas para otro momento). Aparte del interés teórico, existe uno muy práctico: si se pudiese factorizar enteros *grandes* entonces se quebrarían las firmas digitales hechas con el algoritmo RSA.
El clásico método de Fermat para factorizar $n = p \cdot q$ partía de que $y = \frac{q+p}{2}$, $x = \frac{q-p}{2}$ son enteros entonces

$$n + x^2 = y^2 \Rightarrow p = mcd(n, (x - y)) \ , \ q = mcd(n, (x + y)) \tag{1}$$

salvo casos triviales. La idea es lograr una representación $n + x^2 = y^2$. Por lo general es casi imposible conseguir dicha representación. Maurice Kraitchik, un matemático ruso, planteó buscar las congruencias

$$x_i^2 \equiv y_i^2 \bmod n \tag{2}$$

Los métodos modernos mas eficientes (Quadratic Sieve, Number Field Sieve) tienen su origen en estas ideas, pero requieren definir polinomios adaptados a cada caso, y conducen a sistemas de ecuaciones módulo 2 con millones de incógnitas.Su complejidad es subexponencial.

2. Descripción del método

Las ideas básicas del método fueron expuestas anteriormente en [2].
Como trabajaremos con valores impares de n, la escritura anterior como diferencia de cuadrados siempre es posible. Aquí pretendemos mirar al método de Fermat desde otro punto de vista.
Para cualquier valor de c debe cumplirse que $x^2 \bmod c \in ROS_c$ donde
$ROS_c = \{a \bmod c \text{ con } a \in \mathbb{Z} \text{ tal que } \exists \alpha \in \mathbb{Z}_c \ a \equiv \alpha^2 \bmod c\}$. Además como $n + x^2 = y^2$ resulta que $n + x^2 \bmod c \in ROS_c$. Esto conduce a la siguiente definición

Definición 1. *Dados $n \in \mathbb{Z}$ impar, $c \in \mathbb{Z}$, $a \in ROS_c$. Si $b = (n + a) \in ROS_c$ se dice que (a, b, c) es un **target** para n. Si solo existe un par $a, b \in ROS_c$ tal que (a, b, c) resulta target, se denominará target único (TU) de n.*

Llamaremos también target único a c cuando existe una única terna (a, b, c) como en la definición.

$$\begin{array}{c} \text{Si } x^2 = a \bmod c \Rightarrow x^2 = a + c \cdot t \text{ para cierto valor de } t \\ y^2 = b \bmod c \Rightarrow y^2 = b + c \cdot u \text{ para cierto } u. \end{array} \tag{3}$$

Al obtenerse un TU, factorizar n es equivalente a hallar u y t que satisfagan

$$n + a + c \cdot t = b + c \cdot u \Longrightarrow \Delta = \frac{n + a - b}{c} = u - t \tag{4}$$

que además generen cuadrados para las ecuaciones 3.

Ejemplo 2. Si $n = 200902987$, algunos TU son

$$\begin{array}{c} a = 1,\ b = 0,\ c = 4 \\ a = 9,\ b = 4,\ c = 24 \\ a = 9,\ b = 16,\ c = 60 \\ a = 9,\ b = 36,\ c = 80 \end{array}$$

La última fila implica que $\Rightarrow x^2 = 9 + 80t$, $y^2 = 36 + 80u$.
Las soluciones son $x^2 = 510172569$, $y^2 = 711075556$ y la igualdad se cumple para $t = 6377157$, $u = 8888444$ y $\Delta = 2511287$

Hemos obtenido información acerca de x^2 e y^2 sin conocerlos explícitamente. Si se encontrase c suficientemente grande, se reduciría la complejidad del problema. Antes de continuar con esa idea se necesita garantizar la existencia de los TU, o en su defecto las condiciones de existencia.
Al observar varias salidas de TU para distintos valores de n, por ejemplo en el Cuadro 1 se encuentran valores de c que suelen repetirse en otras salidas. Algunos de ellos son

$$\text{c=3, 4, 5, 12, 45, 720}$$

Veremos bajo que hipótesis existen TU para un n dado.

Proposición 3. *Sea $n \in \mathbb{Z}$ impar tal que $n \not\equiv 0 \bmod 3$ entonces n tiene TU.*

Demostración. Resulta como corolario de las siguientes proposiciones.

Proposición 4. *Sea $n \in \mathbb{Z}$ impar entonces 4 es TU de n.*

Demostración. Los residuos cuadráticos módulo 4 son $ROS_4 = \{0, 1\}$.
Sean $a_1, b_1 \in ROS_4$, observar que si $a_1 = b_1$ entonces se tiene que

$$n + a_1 \equiv b_1 \bmod 4 \Rightarrow n \equiv a_1 - b_1 \bmod 4 \Rightarrow n \equiv 0 \bmod 4 \Rightarrow n \text{ es par}$$

lo cual contradice la hipótesis Entonces $a_1 \neq b_1$ si n es impar.

Para n impar se tienen dos casos

$$\begin{array}{l} n \equiv 1 \bmod 4 \Leftrightarrow n + 0 \equiv 1 \bmod 4 \\ n \equiv -1 \bmod 4 \Leftrightarrow n + 1 \equiv 0 \bmod 4 \end{array}$$

por lo tanto 4 es TU de n.

Proposición 5. *Sea n tal que $n \not\equiv 0 \bmod 3$ entonces 3 es TU de n.*

Demostración. La demostración resulta análoga a la anterior. Los residuos cuadráticos son $ROS_3 = \{0, 1\}$. Sean $a_1, b_1 \in ROS_3$, como $n \not\equiv 0 \bmod 3$, resulta que $a_1 \neq b_1$.
Los casos posibles son

$$\begin{array}{l} n \equiv 1 \bmod 3 \Leftrightarrow n + 0 \equiv 1 \bmod 3 \\ n \equiv -1 \bmod 3 \Leftrightarrow n + 1 \equiv 0 \bmod 3 \end{array} \tag{5}$$

Por lo tanto 3 es TU de n.

Cuadro 1. TU de 507527 ($p = 1009$, $q = 503$)

(a,b,c) =	1	0	3	Delta =	169176
(a,b,c) =	1	0	4	Delta =	126882
(a,b,c) =	4	1	5	Delta =	101506
(a,b,c) =	1	0	8	Delta =	63441
(a,b,c) =	1	0	9	Delta =	56392
(a,b,c) =	1	0	12	Delta =	42294
(a,b,c) =	4	6	15	Delta =	33835
(a,b,c) =	9	0	16	Delta =	31721
(a,b,c) =	9	16	20	Delta =	25376
(a,b,c) =	1	0	24	Delta =	21147
(a,b,c) =	1	0	36	Delta =	14098
(a,b,c) =	9	16	40	Delta =	12688
(a,b,c) =	19	36	45	Delta =	11278
(a,b,c) =	25	0	48	Delta =	10574
(a,b,c) =	49	36	60	Delta =	8459
(a,b,c) =	1	0	72	Delta =	7049
(a,b,c) =	9	16	80	Delta =	6344
(a,b,c) =	49	96	120	Delta =	4229
(a,b,c) =	73	0	144	Delta =	3525
(a,b,c) =	109	36	180	Delta =	2820
(a,b,c) =	169	96	240	Delta =	2115
(a,b,c) =	289	216	360	Delta =	1410
(a,b,c) =	649	576	720	Delta =	705

Las proposiciones anteriores garantizan que siempre existen TUs de n excepto cuando es divisible por 3 o por 4. Si este fuese el caso, se habrían encontrado factores de n.
Generalizando la idea de las demostraciones anteriores, se define:

$$f : ROS_c \times ROS_c \longrightarrow \mathbb{Z}_c$$
$$(a, b) \longrightarrow b - a \bmod c$$

Dado un target (a, b, c) de n entonces $n \equiv b - a \bmod c$. Por lo tanto buscar los targets de n módulo c es equivalente a encontrar el conjunto $f^{-1}(n)$.
Si $|ROS_c| \times (|ROS_c| - 1) > |\mathbb{Z}_c|$ entonces existe n para el cual c no es TU. Tomamos $|ROS_c| - 1$ porque si $a \equiv b \bmod c$ es un caso trivial donde c/n y se tiene uno de los factores.
Si c es impar entonces $\forall n_c \in \mathbb{Z}_c \quad \exists n \in \mathbb{Z}$ impar no primo tal que $n \equiv n_c \bmod c$, y por lo tanto puede escribirse como diferencia de cuadrados $n = y^2 - x^2$. Entonces $\exists a, b \in ROS_c$ tal que $n_c \equiv b - a \bmod c$ y resulta $Im(f) = \mathbb{Z}_c$. En el caso en que n sea par, cualquier $a \in \mathbb{Z}_c$ par conduce a valores pares de n que no necesariamente se pueden escribir como diferencia de cuadrados.

Existen valores de c que pueden ser TU o no, dependiendo del n que se quiere factorizar. Por ejemplo:
Sea $c = 5$ con $ROS_5 = \{0, 1, 4\}$.

$$|f^{-1}(4)| = 2 \text{ ya que } f(1, 0) = 4 \text{ y } f(0, 4) = 4$$
$$|f^{-1}(1)| = 2 \text{ con } f(0, 1) = 1 \text{ y } f(4, 0) = 1$$
$$|f^{-1}(2)| = 1 \text{ ya que solo } f(4, 1) = 2$$
$$|f^{-1}(3)| = 1 \text{ con } f(4, 1) = 3$$

Por lo tanto 5 no es TU para $n \equiv 4 \bmod 5$ ó $n \equiv 1 \bmod 5$. Pero si $n \equiv 2 \bmod 5$ ó $n \equiv 3 \bmod 5$ entonces 5 es TU. En el Cuadro 1 se tiene $n \equiv 2 \bmod 5$ y 5 es TU.

Definición 6. *Para cada $c \in \mathbb{N}$ se define* ***complejidad*** *como:*

$$complejidad(c) = max_{x \in \mathbb{Z}_c} \left\{ |f^{-1}(x)| \right\}$$

Si c es TU $\forall n$ entonces $complejidad(c) = 1$.
Se puede restringir $complejidad(c)$ a n de la siguiente forma

$$complejidad(c, n) = |f^{-1}(x)| \text{ con } x \equiv n \bmod c$$

donde se satisface que $complejidad(c, n) \leq complejidad(c)$. La desigualdad puede ser estricta, por ejemplo para c=5:

$$complejidad(5) = 2$$
Sin embargo $complejidad(5, 22) = 1$

ya que $22 \equiv 2 \bmod (5)$ y $2 \equiv 1 - 4 \bmod (5)$ es la única combinación posible de ROS.
Usando la definición de complejidad probaremos

Proposición 7. *$c = 8$ resulta TU $\forall n$ impar.*

Demostración. $ROS_8 = \{0, 1, 4\}$ y como n es impar, los targets que conducen a valores impares de n son

$$(0, 1, 8)$$
$$(1, 0, 8)$$
$$(1, 4, 8)$$
$$(4, 1, 8)$$

Cada uno de ellos conduce a una congruencia distinta $\{1, 7, 3, 5\}$ para n.

Proposición 8. *Dado n, sean c_1, c_2 TU de n coprimos. Entonces $c = c_1 \cdot c_2$ es TU de n.*

Demostración. Supongamos que $\exists a_1, a_2, b_1, b_2 \in ROS_c$ tales que

$$n + a_1 \equiv b_1 \bmod c$$
$$n + a_2 \equiv b_2 \bmod c$$

Tomando congruencias módulo c_1, c_2 las igualdades se mantienen obteniéndose
para c_1

$$n + a_1 \equiv b_1 \bmod c_1$$
$$n + a_2 \equiv b_2 \bmod c_1$$

para c_2

$$n + a_1 \equiv b_1 \bmod c_2$$
$$n + a_2 \equiv b_2 \bmod c_2$$

Al empezar se supuso que c_1, c_2 eran targets únicos entonces

$$a_1 \equiv a_2 \bmod c_1$$
$$b_1 \equiv b_2 \bmod c_1$$

y

$$c_1 \mid (a_1 - a_2)$$
$$c_1 \mid (b_1 - b_2)$$

Análogamente para c_2

$$c_2 \mid (a_1 - a_2)$$
$$c_2 \mid (b_1 - b_2)$$

Como c_1, c_2 eran coprimos entonces

$$c \mid (a_1 - a_2) \rightarrow a_1 \equiv a_2 \bmod c$$
$$c \mid (b_1 - b_2) \rightarrow b_1 \equiv b_2 \bmod c$$

Por lo tanto $c = c_1 \cdot c_2$ es TU.

De aquí se concluye que como 3, 4 y 8 son TU $\forall n \not\equiv 0 \bmod 3$ impar entonces 12 y 24 son TU de dichos n.
La última proposición se puede traducir en que al agregar un nuevo primo a los targets únicos, la cantidad de TU crece al doble. Se vió que hay números que siempre resultan targets únicos. También existen casos que nunca lo son.

Proposición 9. *Sea $c \in \mathbb{Z}$ primo tal que $c > 3 \Rightarrow \exists n$ tal que c no es TU de n.*

Demostración. Basta ver que $\forall c$ primo tal que $c > 3$ se cumple que
$|ROS_c| \times (|ROS_c| - 1) > |\mathbb{Z}_c|$

$$|\mathbb{Z}_c| = c \text{ y } |ROS_c| = \frac{c+1}{2}$$

$$|ROS_c| \times (|ROS_c| - 1) = (\frac{c+1}{2}) \cdot (\frac{c-1}{2}) = \frac{c^2-1}{4}$$

$$\frac{c^2-1}{4} \overset{?}{>} c$$
$$\Leftrightarrow c^2 - 4c - 1 > 0 \Leftrightarrow c > 4$$

A continuación definiremos

Definición 10. *Diremos que c es un un target doble de n si $\exists$ únicos $a, a', b, b' \in ROS_c$ $a \neq a'$ y $b \neq b'$ tales que (a, b, c) y (a', b', c) son ambos targets de n.*

Como vimos antes para $c = 5$ y $n \equiv 4 \bmod 5$, tanto $(1, 0, 5)$ como $(0, 4, 5)$ resultan targets de n. En algunos casos los targets dobles se pueden reducir combinándolos con los TU. Cuando $c = 2$ siempre es target doble, sin embargo al combinarlo con el TU $\overline{c} = 4$ se puede identificar cual es el correcto. Este ejemplo resulta trivial, ya que el caso $c = 2$ solo aporta información acerca de la paridad de x^2 é y^2 que ya se tenía gracias a $\overline{c} = 4$.
De manera análoga a 10 se pueden definir targets triples, cuádruples y de mayor orden.

3. Targets de segundo nivel

Sea n entero impar y (a, b, c) TU de n.
Para $\Delta = \frac{n+a-b}{c}$ se puede repetir el procedimiento (si Δ es par se lo divide por 2^k tal que $\Delta/2^k$ sea impar y se modifican las fórmulas en forma obvia), y calcular los TU $(a_\Delta, b_\Delta, c_\Delta)$ para Δ. Se intentará hallar una forma de combinar estos targets con los de primer nivel y así conocer más del n que se intenta factorizar.
De la expresión del TU para Δ y reemplazando por su expresión original se obtiene

$$\Delta + a_\Delta + c_\Delta \cdot t_\Delta = b_\Delta + c_\Delta \cdot u_\Delta \Longrightarrow \frac{n+a-b}{c} + a_\Delta + c_\Delta \cdot t_\Delta = b_\Delta + c_\Delta \cdot u_\Delta \tag{6}$$

Reordenando los términos

$$n + a + a_\Delta \cdot c + c \cdot c_\Delta \cdot t_\Delta = b + b_\Delta \cdot c + c \cdot c_\Delta \cdot u_\Delta \tag{7}$$

$(a + a_\Delta \cdot c, b + b_\Delta \cdot c, c \cdot c_\Delta)$ es un posible nuevo target para n que llamaremos (aa, bb, cc). Por construcción

$$n + aa = bb \bmod cc \tag{8}$$

No necesariamente ocurre que $aa, bb \in ROS_{cc}$. Por lo tanto lo primero que se hará es descartar estos casos, que no resultan interesantes para el análisis. A los nuevos targets encontrados se les aplicarán el siguiente filtro

FILTRO 1

$$aa \in ROS_{cc} \text{ y } bb \in ROS_{cc}$$

Definición 11. *Sea n entero impar y (aa, bb, cc) contruídos como antes. Entonces (aa, bb, cc) se llama target de segundo nivel de n cuando pasa el Filtro 1, es decir cuando $aa, bb \in ROS_{cc}$.*

Ejemplo 12. Sea $n = 507527$, $(9, 16, 20)$ TU de n entonces $\Delta = 25376$.
Un target de Δ es $(4, 0, 9)$.

$$(9 + 4 \cdot 20, 16 + 0 \cdot 20, 20 \cdot 9) = (89, 16, 180)$$

Para que sea target de n debe pasar el Filtro1. Sin embargo

$$89 \notin ROS_{180} \ ^{3}$$

Por lo tanto $(89, 16, 180)$ no es target de segundo nivel de n.

A pesar de pasar el Filtro1 (aa, bb, cc) podría no ser TU de n. Por lo tanto aún cuando la igualdad (7) se cumpla, no necesariamente

$$x^2 \equiv a + a_\Delta \cdot c \bmod c \cdot c_\Delta \tag{9}$$

ni

$$y^2 \equiv b + b_\Delta \cdot c \bmod c \cdot c_\Delta \tag{10}$$

En este caso diremos que aún cuando (aa, bb, cc) es target de segundo nivel, no es correcto ya que las expresiones anteriores no son correctas.

Ejemplo 13. Sea $n = 67381$ con $(36, 25, 96)$ un TU, $\Delta = 702$ y $(4, 1, 5)$ TU de Δ. Entonces

$$(aa, bb, cc) = (420, 121, 480) \tag{11}$$

Como $420, 121 \in ROS_{480}$ entonces resulta target de segundo nivel.
En este caso $x^2 = 580644$ pero $580644 \neq 420 + 480 \cdot t$ para $t \in \mathbb{Z}$. Esto ocurre porque $c = 480$ no es TU de n, es target doble y la solución es $(324, 25, 480)$.

También se puede usar la información de los targets no únicos (dobles, triples, etc) para descartar casos erróneos.
Varios filtros se han implementado para detectar ramas que no son correctas. Todavía existen casos ambiguos que no se filtran, en donde sin conocer la factorización de n no se sabe si conducen o no a una solución.

El Cuadro 2 muestra la salida de un programa desarrollado por Martín Degrati, que calcula los targets de segundo nivel para $n = 507527$. Los casos que figuran OK conducen a expresiones que son verdaderas para x^2 e y^2 y los filtrados no resultan targets para n. Los casos que no dicen nada se refieren a targets que no son verdaderos para x^2 e y^2 pero que no se pueden identificar como erróneos con lo hecho hasta ahora sin conocer los valores reales de x^2 e y^2.

Definición 14. *Si c es un target de n que es a su vez target de Δ lo vamos a denominar Target Simétrico, es decir (a_1, b_1, c_1) TU de n es simétrico sii*

$$\Delta + a_1 \equiv b_1 \bmod c_1$$

Como es la misma ecuación que cumple n se deduce que $\Delta \equiv n \bmod c_1$

Hasta ahora no hemos podido probar que siempre existan targets simétricos.

[3] $ROS_{180} = \{0, 1, 4, 9, 16, 25, 36, 40, 45, 49, 61, 64, 76, 81, 85, 100, 109, 121, 124, 136, 144, 145, 160, 169\}$

Cuadro 2. Targets de segundo nivel para 507527

(a,b,c)=(	1,	0,	3):	Δ=	169176						
(a,b,c)=(	1,	0,	4):	Δ=	126882						
$(a_\Delta,b_\Delta,c_\Delta)$=(	4,	1,	5):	(aa,	bb,	cc) = (	17,	4,	20)	Filtrado.	
(a,b,c)=(	4,	1,	5):	Δ	= 101506						
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	3):	(aa,	bb,	cc) = (	4,	6,	15)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	4,	9):	(aa,	bb,	cc) = (	4,	21,	45)	Filtrado.	
(a,b,c)=(	1,	0,	8):	Δ=	63441						
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	4):	(aa,	bb,	cc) = (	1,	8,	32)	Filtrado.	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	8):	(aa,	bb,	cc) = (	1,	8,	64)	Filtrado.	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	16):	(aa,	bb,	cc) = (	1,	8,	128)	Filtrado.	
	⋮	⋮	⋮	⋮	⋮						
(a,b,c)=(	9,	0,	16):	Δ=	31721						
$(a_\Delta,b_\Delta,c_\Delta)$=(	1,	0,	3):	(aa,	bb,	cc) = (	25,	0,	48)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	4):	(aa,	bb,	cc) = (	9,	16,	64)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	8):	(aa,	bb,	cc) = (	9,	16,	128)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	4,	0,	9):	(aa,	bb,	cc) = (	73,	0,	144)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	4,	9,	12):	(aa,	bb,	cc) = (	73,	144,	192)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	9,	16):	(aa,	bb,	cc) = (	9,	144,	256)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	16,	9,	24):	(aa,	bb,	cc) = (	265,	144,	384)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	4,	9,	36):	(aa,	bb,	cc) = (	73,	144,	576)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	16,	9,	48):	(aa,	bb,	cc) = (	265,	144,	768)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	40,	9,	72):	(aa,	bb,	cc) = (	649,	144,	1152)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	112,	9,	144):	(aa,	bb,	cc) = (	1801,	144,	2304)	OK	
	⋮	⋮	⋮	⋮	⋮						
(a,b,c)=(	169,	96,	240):	Δ=	2115						
$(a_\Delta,b_\Delta,c_\Delta)$=(	1,	0,	4):	(aa,	bb,	cc) = (	409,	96,	960)	Filtrado.	
$(a_\Delta,b_\Delta,c_\Delta)$=(	1,	4,	8):	(aa,	bb,	cc) = (	409,	1056,	1920)	Filtrado.	
$(a_\Delta,b_\Delta,c_\Delta)$=(	1,	4,	16):	(aa,	bb,	cc) = (	409,	1056,	3840)	Filtrado.	
$(a_\Delta,b_\Delta,c_\Delta)$=(	1,	4,	32):	(aa,	bb,	cc) = (	409,	1056,	7680)	Filtrado.	
(a,b,c)=(	289,	216,	360):	Δ=	1410						
(a,b,c)=(	649,	576,	720):	Δ=	705						
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	4):	(aa,	bb,	cc) = (	649,	1296,	2880)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	8):	(aa,	bb,	cc) = (	649,	1296,	5760)	OK	
$(a_\Delta,b_\Delta,c_\Delta)$=(	0,	1,	16):	(aa,	bb,	cc) = (	649,	1296,	11520).		

3.1. Targets de mayores niveles

Sea n entero impar, (a, b, c) TU de n, $\Delta = \frac{n+a-b}{c}$ y $(a_\Delta, b_\Delta, c_\Delta)$ TU para Δ. Sea (aa, bb, cc) target de segundo nivel.
Si definimos $\Delta^{(2)} = \frac{n+aa-bb}{cc}$, se pueden calcular los targets $(a_{\Delta^{(2)}}, b_{\Delta^{(2)}}, c_{\Delta^{(2)}})$ para $\Delta^{(2)}$ y construir $(a_3, b_3, c_3) = (aa + a_{\Delta^{(2)}} \cdot cc, bb + b_{\Delta^{(2)}} \cdot cc, cc \cdot c_{\Delta^{(2)}})$.

Definición 15. *Se dirá que (a_3, b_3, c_3) es un target de tercer nivel para n si cumple que $a_3, b_3 \in ROS_{c_3}$*

Esta idea se puede generalizar inductivamente para mayores niveles de la siguiente manera:
Sea $i \geq 2$ (a_i, b_i, c_i) target del i-ésimo nivel.
Sea $\Delta^{(i)} = \frac{n+a_i-b_i}{c_i}$ y $(a_{\Delta^{(i)}}, b_{\Delta^{(i)}}, c_{\Delta^{(i)}})$ TU de $\Delta^{(i)}$. Se construye

$$(a_{i+1}, b_{i+1}, c_{i+1}) = (a_i + a_{\Delta^{(i)}} \cdot c_i, b_i + b_{\Delta^{(i)}} \cdot c_i, c_i \cdot c_{\Delta^{(i)}}) \tag{12}$$

Si $a_{i+1}, b_{i+1} \in ROS_{c_{i+1}}$ entonces se dirá que $(a_{i+1}, b_{i+1}, c_{i+1})$ es target del $(i+1)$-ésimo nivel.

4. Deltas de corrección

Sea n entero impar, (a, b, c) TU de n. Sea $\Delta = \frac{n+a-b}{c}$ y $(a_\Delta, b_\Delta, c_\Delta)$ TU de Δ.
Del TU se tiene que $x^2 = a + c \cdot t$
Para el segundo nivel se obtuvo la siguiente expresión que no se sabe si es correcta $x^2 = a + c \cdot (a_\Delta + c_\Delta \cdot t_\Delta)$
Si el target de segundo nivel no es correcto, entonces agregaremos un factor de corrección δ_x y veremos que forma debe tener

$$x^2 = a + c \cdot (a_\Delta + c_\Delta \cdot t_\Delta) + \delta_x = a + c \cdot t$$
$$c \cdot (a_\Delta + c_\Delta \cdot t_\Delta) + \delta_x = c \cdot t \Rightarrow \delta_x = c \cdot (t - a_\Delta - c_\Delta \cdot t_\Delta)$$

Análogamente para $y^2 = b + c \cdot u$ y la expresión del segundo nivel $y^2 = b + c \cdot (b_\Delta + c_\Delta \cdot u_\Delta)$, se obtiene que

$$\delta_y = c \cdot (u - b_\Delta - c_\Delta \cdot u_\Delta) \tag{13}$$

Queremos ver también que relación existe entre δ_x y δ_y:

$$n + a + c \cdot (a_\Delta + c_\Delta \cdot t_\Delta) + \delta_x = b + c \cdot (b_\Delta + c_\Delta \cdot u_\Delta) + \delta_y \tag{14}$$

Tomando módulo $c \cdot c_\Delta$ se obtiene que $\delta_x \equiv \delta_y \bmod c \cdot c_\Delta$.
Por lo tanto los deltas de corrección cumplen las siguientes ecuaciones

$$\delta_x \equiv 0 \bmod c$$
$$\delta_y \equiv 0 \bmod c$$
$$\delta_x \equiv \delta_y \bmod c \cdot c_\Delta$$

Qué ocurre con los factores de corrección si seguimos avanzando de nivel?
Existen dos posibles casos:

1. Cuando el nivel anterior es verdadero, es decir no necesita un delta de corrección.
2. Cuando el nivel anterior no es verdadero, por lo tanto es necesario un delta de corrección.

Veremos que ocurre en cada uno de estos casos en el tercer nivel para luego generalizar la idea en niveles mayores.
Se tienen las ecuaciones del primer y segundo nivel, asumiendo que no es necesario un delta de corrección

$$x^2 = a + c \cdot t \tag{15}$$

$$x^2 = a + c \cdot (a_\Delta + c_\Delta \cdot t_\Delta) \tag{16}$$

Avanzando un nivel mas se obtiene $\Delta^{(2)} = \frac{n+aa-bb}{cc}$ y $(a_{\Delta^{(2)}}, b_{\Delta^{(2)}}, c_{\Delta^{(2)}})$

$$x^2 = a + c \cdot (a_\Delta + c_\Delta \cdot (a_{\Delta^{(2)}} + c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}})) \tag{17}$$

Para que la ecuación anterior sea válida y por lo tanto igual a (15) y (16) se agrega un factor de corrección.

$$\begin{gathered} a + c \cdot a_\Delta + c \cdot c_\Delta \cdot t_\Delta = a + c \cdot a_\Delta + c \cdot c_\Delta \cdot a_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}} + \delta_x^3 \\ c \cdot c_\Delta \cdot t_\Delta = c \cdot c_\Delta \cdot a_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}} + \delta_x^3 \\ c \cdot c_\Delta \cdot (t_\Delta - a_{\Delta^{(2)}} - c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}}) = \delta_x^3 \end{gathered}$$

Análogamente para y^2 se tiene

$$\begin{gathered} b + c \cdot b_\Delta + c \cdot c_\Delta \cdot u_\Delta = b + c \cdot b_\Delta + c \cdot c_\Delta \cdot b_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot u_{\Delta^{(2)}} + \delta_y^3 \\ c \cdot c_\Delta \cdot u_\Delta = c \cdot c_\Delta \cdot b_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot u_{\Delta^{(2)}} + \delta_y^3 \\ c \cdot c_\Delta \cdot (u_\Delta - b_{\Delta^{(2)}} - c_{\Delta^{(2)}} \cdot u_{\Delta^{(2)}}) = \delta_y^3 \end{gathered}$$

Entonces los deltas del tercer nivel cumplen

$$\begin{gathered} \delta_x^3 \equiv 0 \bmod c \cdot c_\Delta \\ \delta_y^3 \equiv 0 \bmod c \cdot c_\Delta \end{gathered}$$

Además vale que

$$n + a + c \cdot a_\Delta + c \cdot c_\Delta \cdot a_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}} + \delta_x^3 = b + c \cdot b_\Delta + c \cdot c_\Delta \cdot b_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot u_{\Delta^{(2)}} + \delta_y^3$$

Tomando módulo $c \cdot c_\Delta \cdot c_{\Delta^{(2)}}$ resulta que

$$\delta_x^3 \equiv \delta_y^3 \bmod c \cdot c_\Delta \cdot c_{\Delta^{(2)}}$$

¿Qué pasa si (16) necesita un delta de corrección? La ecuación se transforma en

$$\begin{gathered} a + c \cdot a_\Delta + c \cdot c_\Delta \cdot t_\Delta + \delta_x^2 = a + c \cdot a_\Delta + c \cdot c_\Delta \cdot a_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}} + \delta_x^3 \\ c \cdot c_\Delta \cdot t_\Delta + \delta_x^2 = c \cdot c_\Delta \cdot a_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}} + \delta_x^3 \\ c \cdot c_\Delta \cdot (t_\Delta - a_{\Delta^{(2)}} - c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}}) = \delta_x^3 - \delta_x^2 \end{gathered}$$

Al ser $\delta_x^2 \equiv 0 \bmod c$

$$\begin{gathered} \delta_x^3 \equiv 0 \bmod c \\ \delta_x^3 \equiv \delta_x^2 \bmod c \cdot c_\Delta \end{gathered}$$

Análogamente

$$\begin{gathered} \delta_y^3 \equiv 0 \bmod c \\ \delta_y^3 \equiv \delta_y^2 \bmod c \cdot c_\Delta \end{gathered}$$

Ejemplo 16. Sea $n = 507527 = y^2 - x^2 = 571536 - 64009$.
Tomamos el TU de n $(73, 0, 144)$ del cual se obtiene $\Delta = 3525$. Un TU de este delta es $(4, 9, 16)$. Entonces

$$(aa, bb, cc) = (649, 1296, 2304)$$

Como $649, 1296 \in ROS_{2304}$ entonces es target de segundo nivel. Pero no es solución ya que

$$\frac{x^2 - 649}{2304} = 27{,}5$$

Los posibles targets para $c = 2304$ son

$$\begin{gathered} (1657, 0, 2304) \\ (1801, 144, 2304) \\ (2233, 576, 2304) \\ (649, 1296, 2304) \end{gathered}$$

Como en este caso sabemos que $x^2 = 64009$ entonces

$$x^2 \equiv 1801 \bmod (2304) \Longrightarrow 1801 = 649 + 8 \cdot c_1 \text{ donde } c_1 = 144$$

Análogamente como $y^2 = 571536$ se tiene que

$$y^2 \equiv 144 \bmod (2304) \Longrightarrow 144 = 1296 - 8 \cdot c_1$$

Los deltas de corrección son $\delta_x^2 = 8 \cdot c_1$ y $\delta_y^2 = -8 \cdot c_1$.

Todavía es necesaria mas información para poder reconocer que δ_x^2 y δ_y^2 son los correctos y en que casos son requeridas dichas correcciones.
Por inducción, se generaliza más allá del tercer nivel, obteniéndose

$$\begin{array}{l} \delta_x^r \equiv 0 \bmod \prod_0^{r-2} c_{\Delta^{(i)}} \\ \delta_y^r \equiv 0 \bmod \prod_0^{r-2} c_{\Delta^{(i)}} \end{array} \tag{18}$$

donde $\Delta^{(0)} = n.$.
Cuando para el nivel $r-1$ también es necesario un delta de corrección, resulta

$$\begin{array}{l} \delta_x^{r-1} \equiv \delta_x^r \bmod \prod_0^{r-2} c_{\Delta^{(i)}} \\ \delta_y^{r-1} \equiv \delta_y^r \bmod \prod_0^{r-2} c_{\Delta^{(i)}} \end{array}$$

Al elegir una rama incorrecta, si se avanza por ese camino, ¿es posible que la misma llegue a corregirse?
Suponiendo que se tiene $(aa, bb, cc) = (a + c \cdot a_\Delta, b + c \cdot b_\Delta, c \cdot c_\Delta)$ el target de segundo nivel. Avanzando un paso más en la rama tenemos $(a_{\Delta^{(2)}}, b_{\Delta^{(2)}}, c_{\Delta^{(2)}})$ que construye el target $(a + c \cdot a_\Delta + c \cdot c_\Delta \cdot a_{\Delta^{(2)}}, b + c \cdot b_\Delta + c \cdot c_\Delta \cdot b_{\Delta^{(2)}}, c \cdot c_\Delta \cdot c_{\Delta^{(2)}})$
Si fuese correcto se tendría que

$$\begin{cases} x^2 = a + c \cdot a_\Delta + c \cdot c_\Delta \cdot a_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot t_{\Delta^{(2)}} \\ y^2 = b + c \cdot b_\Delta + c \cdot c_\Delta \cdot b_{\Delta^{(2)}} + c \cdot c_\Delta \cdot c_{\Delta^{(2)}} \cdot u_{\Delta^{(2)}} \end{cases}$$

Reduciendo módulo $c \cdot c_\Delta$

$$\begin{cases} x^2 \equiv a + c \cdot a_\Delta \bmod c \cdot c_\Delta \\ y^2 \equiv b + c \cdot b_\Delta \bmod c \cdot c_\Delta \end{cases} \tag{19}$$

De la expresión se deduce que el target de segundo nivel (aa, bb, cc) era correcto.
Por lo tanto una vez tomada una rama equivocada no es posible volver a un caso bueno y son necesarias correcciones. Si se tuviera alguna forma de descartar las ramas incorrectas, la factorización de n podría bajar su complejidad. Hemos encontrado ramas incorrectas que no parecen llegar a ningún absurdo y que admiten una corrección (cuyo delta es múltiplo del c del paso anterior) que llevaría al caso correcto para dicho target. Sin embargo en otros casos la rama elegida llega a un punto en el que no se admiten este tipo de correcciones.

Ejemplo 17. Tomando $n = 3784751$ se obtiene $(785, 576, 1280)$ target de segundo nivel y $(1, 0, 3)$ TU para $\Delta^{(2)}$

$$(785, 576, 1280) + {}^4(1, 0, 3) \Rightarrow (2065, 576, 3840)$$

que no es solución. Para este caso no existe ninguna corrección como las que describimos anteriormente. La solución es $(3025, 1536, 3840) = (2065 + 960, 576 + 960, 3840)$

$$\begin{cases} \delta_x^2 \not\equiv 0 \bmod 1280 \\ \delta_y^2 \not\equiv 0 \bmod 1280 \end{cases} \tag{20}$$

Pero resulta $960 \equiv 0 \bmod 16$ es múltiplo de $c = 16$ del TU inicial.

[4] Al hablar de suma de targets se hace referencia a la manera de combinar los TU con los de Δ para obtener los del siguiente nivel. Es decir $(a, b, c) + (a_\Delta, b_\Delta, c_\Delta) = (a + a_\Delta \cdot c, b + b_\Delta \cdot c, c \cdot c_\Delta)$

5. Conclusión

Conocemos ciertas expresiones que son correctas para x^2 e y^2 pero al tener un cc tan pequeño no aportan mucha información acerca de ellos. Al avanzar por una rama cc se hace mas grande, pero hasta no poder detectar si el camino es correcto o no se corre el riesgo de perder mucho tiempo con ecuaciones que no conducen a ningún lado. Hasta ahora se ha hecho hincapié en los TU, sin embargo al trabajar con números tan grandes la información que proviene de ellos no permite avanzar mas rápido hacia la factorización de n. Algunas páginas atrás, se definió la complejidad de un target, la cual estaba sujeta tanto a c como a n. También se puede concentrar el estudio en buscar valores de c suficientemente grandes con bajas complejidades y así obtener una serie de ecuaciones siendo una de ellas la correcta.
Actualmente estamos desarrollando diversos algoritmos basados en los resultados expuestos.

Referencias

1. http://video.google.es/videoplay?docid=-5894352876163776594#
2. http://campus.usal.es/~xrecsi/Imagenes/conferenciantes/Scolnik.pdf

Apéndice:
Cálculo de raíces cuadradas modulares.

Patricia L. Quattrini

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina
pquattri@dm.uba.ar

Supongamos que tenemos un target único (a, b, c) para n, entonces sabemos que $n + x^2 = y^2$, $x^2 \equiv a \mod c$, $y^2 \equiv b \mod c$ y $n + a \equiv b \mod c$.
Si $x^2 \equiv a \mod c$, tenemos que x será congruente módulo c a *alguna* de las raíces cuadradas de a módulo c. Recordemos que no estamos pidiendo que a y c sean coprimos, y que por raíz cuadrada de a (módulo c) entendemos cualquier entero $0 \leq r \leq c-1$ tal que $r^2 \equiv a \mod c$.
Así, si $x \equiv r \mod c$, tendremos que $x^2 = (r + ct)^2$ para algún $t \in \mathbb{Z}$. Análogamente para y^2.
En este apéndice veremos cómo calcular las *parábolas* $u = (r + ct)^2$. Esto equivale a hallar todas las raíces r de $a \mod c$. Éstas parábolas serán utilizadas para generar filtros.

Como hallar raíces cuadradas módulo c.

Problema: Dados $a > 0$ y c enteros, con a cuadrado módulo c, queremos calcular *todas* las raíces cuadradas de a módulo c, es decir todos los enteros $0 \leq r < c$ tales que $r^2 \equiv a \mod c$. Podemos suponer que $0 \leq a < c$ ya que si esto no ocurre cambiamos a por $a \mod c$.

Algunas observaciones:

- No vamos a suponer que a y c son coprimos, ni c libre de cuadrados. De hecho, nos interesa el caso absolutamente general. Algunos casos particulares, como $(a, c) = 1$ o hallar *una* raíz cuando $c = p^k$ con p primo impar, se encuentran en la literatura. Por falta de referencias para el caso general, lo desarrollaremos aquí.
- El procedimiento general es: factorizamos c, recordar que c es muy pequeño en relación a n y esto es factible. Si $c = p_1^{e_1} \cdots p_s^{e_s}$, buscamos las raíces cuadradas de a módulo cada $p_i^{e_i}$. Luego, las vamos *levantando* de a pares con el teorema chino del resto. Nos ocuparemos aquí de hallar raíces módulo cada potencia de primo.
- No nos ocupamos acá de cómo calcular la raíz cuadrada de a módulo p con p primo y a coprimo con p. Esto figura en muchos textos (ver, por ejemplo, [1]) y suele estar implementado en muchos paquetes matemáticos.

Cálculo de las raíces de $a \mod p^e$, para a y p coprimos, $p \neq 2$.

Se calcula una raíz cuadrada de a módulo p: la llamamos r_0. *Todas* las raíces de $a \mod p$ serán r_0 y $-r_0$ ya que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo y la ecuación $x^2 - a$ no puede tener más de dos soluciones en un cuerpo cualquiera.
El lema de Hensel nos dice que cada raíz r se levanta a una única raíz módulo p^e, y éstan son *todas* las raíces módulo p^e (ver [2], o [3] para una versión más sencilla del lema de Hensel).
El procedimiento general para ir levantando raíces es:
si r_i es es raíz de a módulo p^{2^i}, $r_{i+1} = r + \frac{a - r_i^2}{2r_i} \mod p^{2^i}$ es una raíz de a módulo $p^{2^{i+1}}$ (la división por $2r_i$ es en $\mathbb{Z}/p^{2^{i+1}}\mathbb{Z}$).

Así, iterando, obtenemos las dos raíces de a módulo p^e: r y $-r$.

Cálculo de las raíces de a mód p^e, para a y p no coprimos, p primo impar.

Observación: Si $r^2 \equiv a \mod p^e$, entonces lo mismo vale para $-r$. De cada par $r, -r$, uno y sólo uno de éstos valores se encuentra en el intervalo $[0, \frac{1}{2}p^e)$. Luego, basta buscar las raíces r en ese intervalo.

- Caso $a = 0$.
  En este caso tenemos que ver cuándo $(\alpha p^t)^2 \equiv 0 \mod p^e$ y $0 \leq \alpha p^t < \frac{1}{2}p^e$. Esto da $t \geq e/2$. Ponemos $T = \lceil e/2 \rceil$ y $r = \alpha p^T$ con $\alpha \in \mathbb{Z}$ y $0 \leq \alpha \leq \frac{1}{2}p^{\lfloor e/2 \rfloor}$.
- Caso $a \neq 0$.
  Ponemos $a = a_1 p^m$. Recordemos que $a < p^e$, y por lo tanto $m < e$. Se puede ver que si a es un cuadrado módulo p^e y $r = r_1 p^t$ es una raíz, entonces $t = m/2$ y r_1 es raíz de a_1 módulo p^{e-m}. Y recíprocamente.
  ¿Cómo encuentro *todas* las raíces?
  Recordar que a_1 es coprimo con p y por lo tanto tiene exactamente dos raices $\pm\widetilde{r}$ módulo p^{e-m}. Luego $r_1 = \pm\widetilde{r} + \alpha p^{e-m}$ y tenemos que ver qué valores puede y debe tomar α para recorrer *todos* los enteros de la forma

$$r = \pm\widetilde{r}p^{m/2} + \alpha p^{e-m/2} \tag{1}$$

  módulo p^e y *no congruentes entre sí.* y en el intervalo $(0, \frac{1}{2}p^{m/2})$. Observar que toda expresión de la forma (1) es una raíz cuadrada de a módulo p^e. No es difícil ver que α se mueve entre 0 y $\lfloor \frac{1}{2}p^{m/2} - \widetilde{r}p^{m-e} \rfloor$. Análogamente para $-\widetilde{r}$.

Cálculo de las raíces de a mód 2^e, para a impar y a un cuadrado módulo 2^e.

- Si $e = 1$, hay una única raíz $r = 1$.
- Si $e = 2$, hay dos raíces $\pm 1 \mod 4$.
- Si $e \geq 3$, entonces a tiene 4 raíces: si r es una raíz cualquiera, $\pm r$ y $\pm r + 2^{e-1}$ son todas las raíces de $a \mod 2^e$.
  Para ver esto basta ver que si $r^2 \equiv a \mod 2^k$ y $k \geq 3$ entonces r se levanta a una única raíz de $a \mod 2^{k+1}$.
  Ponemos $r_1 = r + t2^{k-1}$ y definimos t según

$$\begin{cases} \frac{a-r^2}{2^k} \text{ impar} & t = 1 \\ \frac{a-r^2}{2^k} \text{ par} & t = 0 \end{cases}$$

  r_1 será una raíz de a módulo 2^{k+1}. *Todas* las raíces módulo 2^{k+1} serán $\pm r_1, \pm r_1 + 2^k$.

Cálculo de las raíces de a mód 2^e, para a par y a un cuadrado módulo 2^e.

Observación: Si $r^2 \equiv a \mod 2^e$, entonces lo mismo vale para $-r$ y $\pm r + 2^{e-1}$. Si a es impar, de estos cuatro valores, hay exactamente dos en el intervalo $[0, 2^{e-1})$. Luego, basta buscar las raíces r en ese intervalo.

- Caso $a = 0$.
  En este caso tenemos que ver cuándo $(\alpha 2^t)^2 \equiv 0 \mod 2^e$ y $0 \leq \alpha 2^t \leq 2^{e-1}$. Igual que para $p \neq 2$, esto da $t \geq e/2$. Ponemos $T = \lceil e/2 \rceil$ y $r = \alpha 2^T$ con $\alpha \in \mathbb{Z}$ y $0 \leq \alpha \leq 2^{\lfloor e/2 \rfloor - 1}$.
  Observación: tanto 0 como 2^{e-1} son raíces de $a = 0$ e iguales a su inversa aditiva, o sea, al tomar $-r$ tenemos la misma raíz.

- Caso $a \neq 0$.
  Ponemos $a = a_1 2^m$. Igual que para $p \neq 2$ se ve que si $r = r_1 2^t$ es una raíz, entonces: $2t = m$ y $r_1^2 \equiv a_1(2^{e-m})$.
  Así, $r = r_1 2^{m/2}$ con r_1 raíz de a_1 módulo 2^{e-m}. Y recíprocamente.
  ¿Cuáles son *todas* las raíces?
  Supongamos que $e - m \geq 3$. Por lo tanto a_1 tiene exactamente cuatro raices $\pm\widetilde{r}$ y $\pm\widetilde{r} + 2^{e-m-1}$ módulo 2^{e-m}. Entonces $r_1 = \pm\widetilde{r} + s2^{e-m-1} + \alpha 2^{e-m}$, con $s = 0, 1$. Multiplicando por $2^{m/2}$, r es de la forma

$$r = \pm\widetilde{r}2^{m/2} + s2^{e-m/2-1} + \alpha 2^{e-m/2} \tag{2}$$

  módulo 2^e ($\alpha \in \mathbb{Z}, s = 0, 1$). Igual que antes, queremos *todas* las soluciones *no congruentes entre sí.* Observar que toda expresión de la forma (2) es una raíz cuadrada de a módulo 2^e.

  - Ponemos $\mu = \widetilde{r}p^{m-e}$, $\nu = m/2 - 1$. Recordar que $0 < \widetilde{r} < 2^{e-m} \Rightarrow 0 < \mu = \widetilde{r}p^{m-e} < 1$. Planteando que $r < 2^{e-1}$, obtenemos las distintas raíces:
  $r = \widetilde{r}2^{m/2} + \alpha 2^{e-m/2}$ con $0 \leq \alpha \leq \lfloor 2^\nu - \mu \rfloor$
  $r = -\widetilde{r}2^{m/2} + \alpha 2^{e-m/2}$ con $1 \leq \alpha \leq \lfloor 2^\nu + \mu \rfloor$
  $r = \widetilde{r}2^{m/2} + 2^{e-m/2-1} + \alpha 2^{e-m/2}$ con $\lceil -\mu - 1/2 \rceil \leq \alpha \leq \lfloor 2^\nu - \mu - 1/2 \rfloor$
  $r = -\widetilde{r}2^{m/2} + 2^{e-m/2-1} + \alpha 2^{e-m/2}$ con $\lceil +\mu - 1/2 \rceil \leq \alpha \leq \lfloor 2^\nu + \mu - 1/2 \rfloor$

Levantar raíces usando el teorema chino del resto

Para $c = p_1^{e_1} \cdots p_s^{e_s}$ tendremos, para cada $p_i^{e_i}$ una lista de raíces: v Para cada par de listas de raíces $[r_{i1}, \cdots, r_{ik_i}]$ módulo $p_i^{e_i}$. Esta lista representa la mitad de las raíces módulo $p_i^{e_i}$. Usando el teorema chino del resto, levantamos cada raíz de la primer lista con $\pm$ cada raíz de la segunda lista y obtenemos (la mitad de) las raíces de a módulo $p_1^{e_1} p_2^{e_2}$. Iteramos el procedimiento hasta obtener la lista de raíces módulo c.

Referencias

[1] Henri Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer, 1996, Cap. 1.5.
[2] M. Ram Murty *Introduction to p-adic Analytic Number Theory*, Studies in Advanced Mathematics, Vol. 27, AMS-International Press, 2002, Cap. 4.
[3] `http://mathforum.org/library/drmath/view/70474.html`.