Enrique R. Aznar García
eaznar@ugr.es

SUMA DE CUADRADOS

Si primo impar p con $p \equiv 1 \pmod 4$, se sabe desde la época de Euler que se puede poner como suma de dos cuadrados de forma única (salvo la conmutativa y el signo). O sea, existen enteros únicos $0 < a < b < p$ tales que

$$p = a^2 + b^2$$

Hay un método sencillo para su cálculo.

ALGORITMO DE SMITH. INICIACIÓN DEL MÉTODO

Primero se calcula un no residuo cuadrático módulo p. Como hay la mitad de residuos y no residuos. Se puede hacer por prueba y error, iterando un ciclo $i \in \{1, 2, \dots, p-1\}$ mientras el símbolo de Legendre $\left(\frac{i}{p}\right) = 1$. Así, se encuentra rápidamente un i tal que

$$\left(\frac{i}{p}\right) = -1 \equiv i^{(p-1)/2} \pmod p \Rightarrow x = i^{(p-1)/4}, \quad x^2 \equiv -1 \pmod p$$

Así, encontramos una raíz cuadrada x de -1 módulo p. Por ejemplo, para $p = 73$, el primer no residuo cuadrático módulo 73 que se encuentra es $i = 5$ y la raíz cuadrada de -1 módulo $p = 73$ entonces es

$$x = 5^{(73-1)/4} = 5^{18} \pmod{73} = 27$$

ALGORITMO DE EUCLIDES

A continuación se aplica el AEE a la pareja p, x, aunque en realidad sólo nos interesan los restos sucesivos, no hacen falta los coeficientes u, v ni tampoco hace falta llegar al mcd de ambos, que es 1. Basta terminar cuando encontremos un resto menor que $\sqrt{p}$.

Por ejemplo, para $p = 73, x = 27$, tenemos la siguiente sucesión de restos

$$\left.\begin{array}{rcl} 73 & = & 2 * 27 + 19 \\ 27 & = & 1 * 19 + 8 \\ 19 & = & 2 * 8 + 3 \end{array}\right\} \Rightarrow 73 - 3^2 = 64 = 8^2 \Leftrightarrow 73 = 3^2 + 8^2$$

donde hemos terminado al encontrar el primer resto $a = 3 \leq 8 = \lfloor\sqrt{73}\rfloor$ que es menor que $\sqrt{73}$.

OTRO EJEMPLO

Para $p = 27213649$, que es primo congruente con 1 módulo 4, el primer no residuo cuadrático módulo p que se encuentra es $i = 13$ y la raíz cuadrada de -1 módulo p entonces es

$$x = i^{(p-1)/4} = 13^{6803412} \pmod{73} = 13400700$$

A continuación aplicamos el AE a la pareja p, x, hasta encontrar un resto menor o igual que que $\lfloor\sqrt{p}\rfloor = 5216$. Por ejemplo, para $p = 27213649, x = 13400700$, tenemos la siguiente sucesión de restos

$$\left.\begin{array}{rcl} 27213649 & = & 2 * 13400700 + 412249 \\ 13400700 & = & 32 * 412249 + 208732 \\ 412249 & = & 1 * 208732 + 203517 \\ 208732 & = & 1 * 203517 + 5215 \end{array}\right\} \Rightarrow 27213649 - 5215^2 = 17424 = 132^2 \Leftrightarrow 27213649 =$$

ALGORITMO DE EUCLIDES COMO FRACCIÓN CONTINUA FINITA

Si aplicamos el AE a una pareja de números $a, b \geq 2$ obtenemos sucesivamente cocientes q_i y restos r_i tales que

$$r_{i-1} = q_i r_i + r_{i+1}, \quad 0 \leq r_{i+1} < r_i, \quad 0 \leq i \leq k$$

Como en cualquier FC, se pueden calcular los cociente sucesivos que llamamos sus **convergentes**.

$$\frac{A_i}{B_i} = [q_0, q_1, q_2, \dots, q_i] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_i}}}}$$

Estos numeradores y denominadores satisfacen la misma ecuación en recurrencia con distintos parámetros iniciales.

$$A_i = q_i A_{i-1} + A_{i-2}, \quad A_{-1} = 1, A_0 = q_0$$

$$B_i = q_i B_{i-1} + B_{i-2}, \quad B_{-1} = 0, B_0 = 1$$

Como se demuestra por inducción. Así, estos cálculos repetitivos se pueden tabular

$$\begin{array}{ccccccccc} & q_1 & q_2 & \cdots & q_{s-1} & q_s & q_{s+1} & & \cdots \\ \frac{1}{0} & \frac{q_0}{1} & \frac{q_1 q_0 + 1}{q_1 \cdot 1 + 0} & \cdots & \frac{A_{s-2}}{B_{s-2}} & \frac{A_{s-1}}{B_{s-1}} & \frac{q_s A_{s-1} + A_{s-2}}{q_s B_{s-1} + B_{s-2}} & & \cdots \end{array}$$

Para el primer ejemplo anterior, $a = 73, b = 27$. Sus cocientes y convergentes sucesivos son

$$\begin{array}{ccccccc} & 1 & 2 & 2 & 1 & 2 & 1 \\ \frac{1}{0} & \frac{2}{1} & \frac{3}{1} & \frac{8}{3} & \frac{19}{7} & \frac{27}{10} & \frac{73}{27} \end{array}$$

Observamos que el AE demuestra que una FC finita equivale a un número racional.
Además, como veremos todas las fórmulas anteriores tienen un análogo matricial.

INTERPRETACIÓN MATRICIAL DEL AE

Las divisiones euclídeas equivalen a las igualdades matriciales siguientes

$$r_{i-1} = q_i r_i + r_{i+1} \iff \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$$

Análogamente, las igualdades recursivas de los numeradores y denominadores de los convergentes

$$\begin{matrix} B_i = q_i B_{i-1} + B_{i-2} \\ A_i = q_i A_{i-1} + A_{i-2} \end{matrix} \iff \begin{pmatrix} B_i & B_{i-1} \\ A_i & A_{i-1} \end{pmatrix} = \begin{pmatrix} B_{i-1} & B_{i-2} \\ A_{i-1} & A_{i-2} \end{pmatrix} \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$$

Tomamos $\begin{pmatrix} B_0 & B_{-1} \\ A_0 & A_{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, entonces $\begin{pmatrix} B_1 & B_0 \\ A_1 & A_0 \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}$ y por inducción finita tenemos

$$\begin{pmatrix} B_i & B_{i-1} \\ A_i & A_{i-1} \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}$$

Y los restos, también por inducción, dan lugar a

$$\begin{pmatrix} r_{-1} \\ r_0 \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} B_i & B_{i-1} \\ A_i & A_{i-1} \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$$

Como, $A_{-1} = 1, A_0 = 0$ y $B_{-1} = 0, B_0 = 1$, tenemos la igualdad

$$B_0 A_{-1} - B_{-1} A_0 = 1 - 0 = 1$$

y por inducción $B_i A_{i-1} - B_{i-1} A_i = (-1)^i$. Así, existe la matriz inversa

$$\begin{vmatrix} B_i & B_{i-1} \\ A_i & A_{i-1} \end{vmatrix} = (-1)^i \implies \begin{pmatrix} B_i & B_{i-1} \\ A_i & A_{i-1} \end{pmatrix}^{-1} = (-1)^i \begin{pmatrix} A_{i-1} & -B_{i-1} \\ -A_i & B_i \end{pmatrix}$$

y como $r_{-1} = a, r_0 = b$ podemos despejar en función de a, b

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = (-1)^i \begin{pmatrix} A_{i-1} & -B_{i-1} \\ -A_i & B_i \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \implies r_{i+1} = (-1)^i (bB_i - aA_i)$$

RELACIÓN CON EL AEE

El **AEE (algoritmo de Euclides extendido)**, aplicado a una pareja de enteros positivos a, b, no calcula A_i, B_i que son siempre positivos y crecen respectivamente hasta a y b. En su lugar, calcula $s_i = (-1)^{i+1}A_i$ y $t_i = (-1)^i B_i$ que por lo anterior, dan los restos sucesivos como combinación lineal de los dos enteros a y b.

$r_{i+1} = s_i a + t_i b$

y que satisfacen unas ecuaciones recursivas parecidas a las anteriores

$$\begin{array}{l} s_i = -q_i s_{i-1} + s_{i-2} \\ t_i = -q_i t_{i-1} + t_{i-2} \end{array} \iff \begin{pmatrix} t_i & t_{i-1} \\ s_i & s_{i-1} \end{pmatrix} = \begin{pmatrix} t_{i-1} & t_{i-2} \\ s_{i-1} & s_{i-2} \end{pmatrix} \begin{pmatrix} -q_i & 1 \\ 1 & 0 \end{pmatrix}$$

Como unos son los valores absolutos de los otros, **calcular los A_i, B_i equivale a calcular los s_i, t_i**.

EJEMPLO

Calculamos el mcd(73,27) extendido, en una tabla vertical con los 4 parámetros.

iter	q_i	r_{i+1}	s_i	t_i	A_i	B_i
-1		73	1	0	1	0
0	2	27	0	1	0	1
1	1	19	1	-2	1	2
2	2	8	-1	3	1	3
3	2	3	3	-8	3	8
4	1	2	-7	19	7	19
5	2	1	10	-27	10	27
6	-	0	-27	73	27	73

Observamos que los dos últimas columnas calculadas por sus ec. recursivas son los valores absolutos de las dos anteriores y que en la última fila que corresponde al resto cero se obtienen b y a.

UNA ECUACIÓN DIOFÁNTICA

Si $p, d \geq 2$ son enteros primos entre si y la ecuación $x^2 + dy^2 = p$ tiene soluciones enteras, entonces
$x^2 + dy^2 = p \Longrightarrow -d \equiv (x/y)^2 \pmod{p}$
O sea, $-d$ es un residuo cuadrático módulo p. Si p es primo y $d = 1$ sabemos que el recíproco es cierto.

Para un natural arbitrario $d \in \mathbb{N}$, con $-d$ residuo cuadrático módulo p, veremos una condición constructiva, que llamamos algoritmo de Cornacchia-Smith, para la existencia de soluciones enteras $x, y \in \mathbb{Z}$ de la ecuación.

$$x^2 + dy^2 = p$$

Si $w \in \mathbb{N}$ satisface $w^2 \equiv -d \pmod{p}$, con p primo, entonces $\mathrm{mcd}(p, w) = 1$.
Los restos sucesivos entre p y w van disminuyendo hasta el máximo común divisor $r_k = 1$ y para todo $i < k$ se tiene

$$r_{i+1} = (-1)^{i+1}(pA_i - wB_i) \Longrightarrow r_{i+1}^2 = p^2A_i^2 - 2wpA_iB_i + w^2B_i^2 \Longrightarrow r_{i+1}^2 \equiv w^2B_i^2 \pmod{p}$$

O sea, para todo $i < k$,

$$r_{i+1}^2 + dB_i^2 \equiv (w^2 + d)B_i^2 \equiv 0 \pmod{p} \Longrightarrow r_{i+1}^2 + dB_i^2 = \lambda p$$

Vemos que si $\lambda = 1$ para algún índice i, se obtienen soluciones enteras a la ecuación diofántica $x^2 + dy^2 = p$.
Veremos que eso a veces es así para el primer resto $r_{\nu+1}$ que satisface

$$r_{\nu+1} < \sqrt{p} < r_\nu$$

Y demostraremos que, **si existe solución se encuentra necesariamente de esta forma**.

Comprobaremos el método de Cornacchia-Smith para el primo $p = 73$ con d igual a 1, 2 y 3 ya que la ecuación $w^2 \equiv -d \pmod{73}$ tiene solución para esos tres valores y se encuentran soluciones a $x^2 + dy^2 = p$.

EJEMPLO CON D = 3

Como -3 es un residuo cuadrático módulo 73 ya que $\left(\frac{-3}{73}\right) = 1$, existen dos soluciones a la ecuación $w^2 \equiv -3 \pmod{73}$, Cualquiera de las dos, $w = 17, 56$, nos sirve para el método de Cornacchia-Smith.
Calculamos el mcd(73,17) extendido, en una tabla vertical con los parámetros positivos.

iter	q_i	r_{i+1}	A_i	B_i	$r_{i+1}^2 + B_i^2$
-1		73	1	0	$73^2 + 3 * 0^2 = 73 * 73$
0	4	17	0	1	$17^2 + 3 * 1^2 = 4 * 73$
1	3	5	1	4	$5^2 + 3 * 4^2 = 1 * 73$
2	2	2	3	13	$2^2 + 3 * 13^2 = 7 * 73$
3	2	1	7	30	$1^2 + 3 * 30^2 = 37 * 73$

Observamos que las soluciones enteras a la ecuación diofántica $x^2 + 3y^2 = 73$ se obtienen en la iteración $i = 1$, con el primer resto, $r_2 = 5$ que es menor que $\sqrt{73} \approx 8.544$
$5^2 + 3 * 4^2 = 73$
También observamos que el menor múltiplo de $p = 73$ se obtiene en esa iteración
Como hemos demostrado antes, en todas las iteraciones se obtiene $x^2 + 3y^2 = \lambda p$ con $\lambda \geq 1$.

EJEMPLO CON D = 2

Como -2 es un residuo cuadrático módulo 73 ya que $\left(\frac{-2}{73}\right) = 1$, existen dos soluciones a la ecuación $w^2 \equiv -3 \pmod{73}$, Cualquiera de las dos, $w = 12, 61$, nos sirve para el método de Cornacchia-Smith.
Calculamos el mcd(73,61) extendido, en una tabla vertical con los parámetros positivos.

iter	q_i	r_{i+1}	A_i	B_i	$r_{i+1}^2 + B_i^2$
-1		73	1	0	$73^2 + 2 * 0^2 = 73 * 73$
0	1	61	0	1	$61^2 + 2 * 1^2 = 51 * 73$
1	5	12	1	1	$12^2 + 2 * 1^2 = 2 * 73$
2	12	1	5	6	$1^2 + 2 * 6^2 = 1 * 73$

Observamos que las soluciones enteras a la ecuación diofántica $x^2 + 2y^2 = 73$ se obtienen en la iteración $i = 2$, con el primer resto, $r_3 = 1$, que es menor que $\sqrt{73} \approx 8.544$
$1^2 + 2 * 6^2 = 73$
También observamos que el menor múltiplo de $p = 73$ se obtiene en esa iteración.
Como hemos demostrado antes, en todas las iteraciones se obtiene $x^2 + 2y^2 = \lambda p$ con $\lambda \geq 1$.

EJEMPLO CON D = 1

Como -1 es un residuo cuadrático módulo 73 ya que $\left(\frac{-1}{73}\right) = 1$, existen dos soluciones a la ecuación $w^2 \equiv -1 \pmod{73}$, $w = 27, 46$. Cualquiera de las dos nos sirve para el método de Cornacchia-Smith. Calculamos el mcd(73,27), con los parámetros positivos y añadiendo la última fila correspondiente al resto cero.

iter	q_i	r_{i+1}	A_i	B_i	$r_{i+1}^2 + B_i^2$
-1		73	1	0	$73^2 + 0^2 = 73 * 73$
0	2	27	0	1	$27^2 + 1^2 = 10 * 73$
1	1	19	1	2	$19^2 + 2^2 = 5 * 73$
2	2	8	1	3	$8^2 + 3^2 = 1 * 73$
3	2	3	3	8	$3^2 + 8^2 = 1 * 73$
4	1	2	7	19	$2^2 + 19^2 = 5 * 73$
5	2	1	10	27	$1^2 + 27^2 = 10 * 73$
6	-	0	27	73	$0^2 + 73^2 = 73 * 73$

Observamos que las soluciones enteras a la ecuación diofántica $x^2 + y^2 = p = 73$ se obtienen en la iteración $i = 2$, $8^2 + 3^2 = 73$, con el primer resto, $r_3 = 8$ que es menor que $\sqrt{73} \approx 8.544$. Como hemos demostrado antes, en todas las iteraciones se obtiene una igualdad del tipo $x^2 + y^2 = \lambda p$ con $\lambda \geq 1$.

También observamos que los B_i como satisfacen, $B_i = q_i B_{i-1} + B_{i-2}$, son los restos sucesivos de dividir los dos últimos de ellos. Leyendo su columna de abajo arriba, coincide con la tercera columna porque el último es siempre $a = p$ y el penúltimo coincide con b cuando éste es, $b = w < p/2$, una raíz cuadrada de -1 módulo p. Por tanto,

Si $b = w < a/2$ una raíz cuadrada de -1 módulo a, la columna de los cocientes es simétrica. O sea, es la misma leída de arriba abajo que de abajo arriba.

UNA DESIGUALDAD IMPORTANTE

Aunque los numeradores y denominadores de los convergentes crecen respectivamente hasta los enteros $a, b \geq 2$, los restos r_λ permiten acotar los denominadores. Así, si r_λ es uno de los restos de la pareja a, b y P y $Q \neq 0$

$$|aQ - bP| < r_\lambda \Longrightarrow B_\lambda \leq |Q|$$

Para la demostración de la implicación, usaremos un cambio de variables debido a Legendre (1798).

$$\left.\begin{array}{l} P = MA_\lambda - NA_{\lambda-1} \\ Q = MB_\lambda - NB_{\lambda-1} \end{array}\right\} \Longleftrightarrow \begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} A_\lambda & -A_{\lambda-1} \\ B_\lambda & -B_{\lambda-1} \end{pmatrix} \begin{pmatrix} M \\ N \end{pmatrix}$$

como la matriz del cambio tiene determinante $(-1)^\lambda \neq 0$, las variables se pueden despejar

$$\begin{pmatrix} M \\ N \end{pmatrix} = (-1)^\lambda \begin{pmatrix} -B_{\lambda-1} & A_{\lambda-1} \\ -B_\lambda & A_\lambda \end{pmatrix} \begin{pmatrix} P \\ Q \end{pmatrix} \Longleftrightarrow \left\{\begin{array}{l} M = (-1)^\lambda (QA_{\lambda-1} - PB_{\lambda-1}) \\ N = (-1)^\lambda (QA_\lambda - PB_\lambda) \end{array}\right.$$

O sea, existe una correspondencia biunívoca entre ambas parejas de enteros.
Ahora, sustituyendo P y Q, tenemos

$$aQ - bP = M(aB_\lambda - bA_\lambda) - N(aB_{\lambda-1} - bA_{\lambda-1}) = (-1)^\lambda (Mr_{\lambda+1} + Nr_\lambda)$$

Ahora, si $MN > 0$, entonces $|aQ - bP| = |M| r_{\lambda+1} + |N| r_\lambda \geq r_\lambda$ contrario a la hipótesis.

Si $M = 0$, entonces $|aQ - bP| = |N| r_\lambda \geq r_\lambda$ también contrario a la hipótesis.

En consecuencia, $MN \leq 0$, con $M \neq 0$ y entonces

$$|Q| = |M| B_\lambda + |N| B_{\lambda-1} \geq B_\lambda$$

como queríamos demostrar.

EL TEOREMA DE CORNACCHIA-SMITH

Si $p, d \geq 2$ son enteros primos entre si y la ecuación $x^2 + dy^2 = p$ tiene soluciones enteras, entonces
$x^2 + dy^2 = p \Longrightarrow -d \equiv (x/y)^2 \pmod p$
$-d$ es un residuo cuadrático módulo p. Si p primo, $\mathbb{Z}_p$ es cuerpo y existen exactamente dos enteros distintos módulo p tal que $w^2 \equiv -d \pmod p$. Uno, $0 < w < p/2$ y otro $p/2 < w_1 = p - w < p$ y ambos son primos con p.

Si $4 < p$, entonces $\sqrt{p} < p/2 < w_1$ y como los restos sucesivos entre p y w_1 van disminuyendo hasta su máximo común divisor $r_k = 1$ existe el primer resto $r_{\nu+1}$ que satisface

$r_{\nu+1} < \sqrt{p} < r_\nu$
Como la primera división es $p = 1 * w_1 + w$, su resto es $r_2 = w$ y los sucesivos entre p y w coinciden con los siguientes entre p y w_1. Y da igual aplicar el AEE entre p y w que entre p y w_1 ya que se encuentra el mismo $r_{\nu+1}$.

Por lo razonado antes, para todo $i < k$, se tiene una pareja de enteros tales que
$r_{i+1}^2 + dB_i^2 = \lambda p$
Si para algún índice i, $\lambda = 1$, encontramos soluciones a la ecuación diofántica $x^2 + dy^2 = p$.

Pero si existen soluciones enteras x, y, entonces se tiene
$x^2 + dy^2 = p \Rightarrow x^2 \equiv -dy^2 \equiv w^2 y^2 \pmod p \Longleftrightarrow (x + wy)(x - wy) \equiv 0 \pmod p$

Cuando p es primo, se tiene que $x \pm wy \equiv 0 \pmod p \Longrightarrow x = wQ - pP$, con $|Q| = |y| \neq 0$.
Como además, $x^2 = p - dy^2 < p \Longrightarrow |wQ - pP| = |x| < \sqrt{p} < r_\nu \Longrightarrow B_\nu < |Q| = |y|$.

Entonces, $B_\nu^2 < y^2 \Longrightarrow dB_\nu^2 < dy^2 = p - x^2 < p \Longrightarrow \lambda p = r_{\nu+1}^2 + dB_\nu^2 < p + p = 2p \Longrightarrow \lambda = 1$
Y hemos demostrado el **teorema de Cornacchia-Smith: Si existen soluciones se encuentran con el resto $\boldsymbol{\nu + 1}$**.
$r_{\nu+1}^2 + dB_\nu^2 = p$

EJEMPLO CON D = 19

Vamos a comprobar que el método de Cornacchia-Smith para el primo $p = 73$ con $d = 19$ no encuentra soluciones a la ecuación $x^2 + 19y^2 = p$. O sea, el método no asegura la existencia de soluciones.
Salvo para $d = 1$, ya que un teorema clásico demostrado por Euler lo asegura.

Como -19 es un residuo cuadrático módulo 73 ya que $\left(\frac{-19}{73}\right) = 1$, existen dos soluciones a la ecuación $w^2 \equiv -19 \pmod{73}$, Cualquiera de las dos, $w = 28, 45$, nos sirve para el método de Cornacchia-Smith.
Calculamos el mcd(73,28) extendido, en una tabla vertical con sólo los parámetros positivos.

iter	q_i	r_{i+1}	A_i	B_i	$r_{i+1}^2 + B_i^2$
-1		73	1	0	$73^2 + 19 * 0^2 = 73 * 73$
0	2	28	0	1	$28^2 + 19 * 1^2 = 11 * 73$
1	1	17	1	2	$17^2 + 19 * 2^2 = 5 * 73$
2	1	11	1	3	$11^2 + 19 * 3^2 = 4 * 73$
3	1	6	2	5	$6^2 + 19 * 5^2 = 7 * 73$
4	1	5	3	8	$5^2 + 19 * 8^2 = 17 * 73$
5	5	1	5	13	$1^2 + 19 * 13^2 = 44 * 73$

Observamos que el método de Cornacchia-Smith **no** encuentra soluciones enteras a la ecuación diofántica $x^2 + 19y^2 = p$. Ya que en todas las iteraciones se obtiene una igualdad del tipo $x^2 + 3y^2 = \lambda p$ con $\lambda > 1$.

Aunque basta comprobar en la iteración con el primer resto $r_{\nu+1}$ que satisface $r_{\nu+1} < \sqrt{p} < r_\nu$. En este ejemplo, basta comprobarlo con $r_4 = 6$ ya que este es el primer resto menor que $\sqrt{73} \approx 8.544$.

OTRA ECUACIÓN DIOFÁNTICA

Si $p, d \geq 2$ son enteros primos entre si y la ecuación $x^2 + dy^2 = 4p$ tiene soluciones enteras, entonces
$x^2 + dy^2 = 4p \Longrightarrow -d \equiv (x/y)^2 \pmod{4} p$
O sea, $-d$ es un residuo cuadrático módulo $4p$.

Para un natural $d \in \mathbb{N}$, tal que $-d$ sea congruente con 1 módulo 4 (implica que es el discriminate de un cuerpo cuadrático) con $-d$ residuo cuadrático módulo $4p$, veremos una condición constructiva, que llamamos **algoritmo de Cornacchia-Smith modificado**, para la existencia de soluciones enteras $x, y \in \mathbb{Z}$ de la ecuación $x^2 + dy^2 = 4p$.

$$x^2 + dy^2 = 4p \Leftrightarrow p = \left(\frac{x + y\sqrt{-d}}{2}\right)\left(\frac{x - y\sqrt{-d}}{2}\right) \text{ p escinde en el anillo de enteros cuadráticos}$$

Si $w \in \mathbb{N}$ satisface $w^2 \equiv -d \pmod{4p}$, con p primo, entonces $\operatorname{mcd}(2p, w) = 1$.
La condición $w^2 \equiv -d \pmod{4p}$ es equivalente a que $w^2 \equiv -d \pmod{p}$ y $w \equiv -d \pmod{2}$.
Los restos sucesivos entre $2p$ y w van disminuyendo hasta el máximo común divisor $r_k = 1$ y para todo $i < k$

$$r_{i+1} = (-1)^{i+1}(2pA_i - wB_i) \Longrightarrow r_{i+1}^2 = 4p^2A_i^2 - 4wpA_iB_i + w^2B_i^2 \Longrightarrow r_{i+1}^2 \equiv w^2B_i^2 \pmod{4p}$$

O sea, para todo $i < k$,

$$r_{i+1}^2 + dB_i^2 \equiv (w^2 + d)B_i^2 \equiv 0 \pmod{4p} \Longrightarrow r_{i+1}^2 + dB_i^2 = \lambda 4p$$

Vemos que si $\lambda = 1$ para algún índice i, se obtienen soluciones enteras a la ecuación diofántica $x^2 + dy^2 = 4p$.
Veremos que eso a veces es así para el primer resto $r_{\nu+1}$ que satisface

$$r_{\nu+1} < 2\sqrt{p} < r_\nu$$

Y demostraremos que, **si existe solución se encuentra necesariamente de esta forma**.

CORNACCHIA-SMITH MODIFICADO

Si $-d \equiv 1 \pmod 4$ y la ecuación $x^2 + dy^2 = p$ no tiene soluciones enteras, a veces la ecuación $x^2 + dy^2 = 4p$ si tiene soluciones. En ese caso,

$$x^2 + dy^2 = 4p \Longrightarrow -d \equiv (x/y)^2 \pmod{4p}$$

Así, $-d$ es un residuo cuadrático módulo p y también es un residuo cuadrático módulo 2. Si p primo, $\mathbb{Z}_p$ es cuerpo y existen exactamente dos enteros distintos módulo p, $w^2 \equiv -d \pmod p$. Uno de ellos, $w < p$ y el otro $w_1 = p - w < p$. Como p es un primo impar, uno de los dos w o w_1 es impar y tiene la misma paridad que $-d$. Si w impar, entonces $w^2 = (2k+1)^2 \equiv 1 \equiv -d \pmod 4$, y como p y 4 son primos entre si

$$\left.\begin{array}{l} w^2 \equiv -d \pmod 4 \\ w^2 \equiv -d \pmod p \end{array}\right\} \Longrightarrow w^2 \equiv -d \pmod{4p}$$

O sea, basta que el símbolo de Legendre $\left(\frac{-d}{p}\right) = 1$ para que exista w impar tal que $w^2 \equiv -d \pmod{4p}$.

Como los restos sucesivos entre $2p$ y w van disminuyendo hasta su máximo común divisor $r_k = 1$ existe el primer resto $r_{\nu+1}$ que satisface $r_{\nu+1} < 2\sqrt{p} < r_\nu$.

Por lo razonado antes, para todo $i < k$, se tiene una pareja de enteros tales que $r_{i+1}^2 + dB_i^2 = \lambda 4p$. Si para algún índice i, $\lambda = 1$, encontramos soluciones a la ecuación diofántica $x^2 + dy^2 = 4p$.

EL TEOREMA DE CORNACCHIA-SMITH MODIFICADO

Pero si existen soluciones enteras x, y, entonces se tiene

$$x^2 + dy^2 = 4p \Rightarrow x^2 \equiv -dy^2 \equiv w^2 y^2 \pmod{4p} \Longrightarrow (x+wy)(x-wy) \equiv 0 \pmod{p}$$

Pero x, y tienen que ser ambos impares ya que en caso contrario ambos serían necesariamente pares y la ecuación $x^2 + dy^2 = p$ tendría soluciones enteras contra la hipótesis inicial. Como w lo tomamos impar, tenemos que ambos factores $x + wy$ y $x - wy$ son pares y entonces uno de ellos será congruente con cero módulo $2p$. Entonces,

$$x \pm wy \equiv 0 \pmod{2p} \Longrightarrow x = wQ - 2pP, \text{ con } |Q| = |y| \neq 0$$

Además,

$$x^2 = 4p - dy^2 < 4p \Longrightarrow |wQ - 2pP| = |x| < 2\sqrt{p} < r_\nu \Longrightarrow B_\nu < |Q| = |y|$$

Pero entonces,

$$B_\nu^2 < y^2 \Longrightarrow dB_\nu^2 < dy^2 = 4p - x^2 < 4p \Longrightarrow \lambda 4p = r_{\nu+1}^2 + dB_\nu^2 < 4p + 4p = 8p \Longrightarrow \lambda = 1$$

Y hemos demostrado el **teorema de Cornacchia-Smith modificado**:

Si existen soluciones $x^2 + dy^2 = 4p$ pero no $x^2 + dy^2 = p$, con $-d \equiv 1 \pmod{p}$, se encuentran con el resto $\nu + 1$, entre $2p$ y w impar tal que $w^2 \equiv -d \pmod{p}$, que satisface $r_{\nu+1} < 2\sqrt{p} < r_\nu$.

$$r_{\nu+1}^2 + dB_\nu^2 = 4p$$

EJEMPLO DE CORNACCHIA-SMITH MODIFICADO

Para $d = 19, p = 73$ hemos visto que la ecuación diofántica $x^2 + dy^2 = p$ no tiene soluciones enteras con el método de Cornacchia-Smith (como veremos eso implica que no existen soluciones enteras).

Sin embargo, para los mismos $d = 19, p = 73$, la ecuación diofántica $x^2 + dy^2 = 4p$ **si** tiene soluciones enteras.
Y se encuentran con el **método de Cornacchia-Smith modificado**.

Como -19 es un residuo cuadrático módulo 73 ya que $\left(\frac{-19}{73}\right) = 1$, existen dos soluciones a la ecuación $w^2 \equiv -19 \pmod{73}$, Una de ellas, $w = 45$, tiene la misma paridad que $d = 19$ y nos sirve para el método de Cornacchia-Smith modificado:
Calculamos el mcd de $(2p, w) = (2 * 73, 45) = (146, 45)$ extendido con sólo los parámetros positivos.

iter	q_i	r_{i+1}	A_i	B_i	$r_{i+1}^2 + B_i^2$
-1		146	1	0	$146^2 + 19 * 0^2 = 146 * 146$
0	3	45	0	1	$45^2 + 19 * 1^2 = 7 * 146$
1	4	11	1	3	$11^2 + 19 * 3^2 = 1 * 146$
2	11	1	4	13	$1^2 + 19 * 13^2 = 11 * 146$

Observamos que las soluciones enteras a la ecuación diofántica $x^2 + dy^2 = 4p = 146$ se obtienen en la iteración $i = 1$, con el primer resto $r_2 = 11$, que es menor que $2\sqrt{73} \approx 17.088$
$11^2 + 19 * 3^2 = 146$
También observamos que el menor múltiplo de $4p = 146$ se obtiene en esa iteración y que en todas las iteraciones se obtiene una igualdad del tipo $x^2 + dy^2 = \lambda 4p$ con $\lambda > 1$.

LA FUNCIÓN CONTINUANTE

Dados enteros positivos a, b, sus restos sucesivos satisfacen
$r_{i-1} = q_i r_i + r_{i+1}$
Cuando son primos entre si, el último resto distinto de cero es $r_n = 1$, entonces algunos anteriores son

$$\begin{cases} r_{n-1} = q_n r_n + r_{n+1} = q_n \\ r_{n-2} = q_{n-1} r_{n-1} + r_n = q_{n-1} q_n + 1 \\ r_{n-3} = q_{n-2} r_{n-2} + r_{n-1} = q_{n-2}(q_{n-1} q_n + 1) + q_n = q_{n-2} q_{n-1} q_n + q_{n-2} + q_n \\ r_{n-4} = q_{n-3} r_{n-3} + r_{n-2} = q_{n-3} q_{n-2} q_{n-1} q_n + q_{n-3} q_{n-2} + q_{n-3} q_n + q_{n-1} q_n + 1 \end{cases}$$

Observamos que por inducción, cada resto r_i es función de los cocientes que le siguen.
Esta función la llamamos **continuante** y la denotamos por
$r_i = Q(q_{i+1}, \dots, q_n)$

Más precisamente, se puede definir esta función por recursión

$$Q(q_1, \dots, q_k) = q_1 Q(q_2, \dots, q_k) + Q(q_3, \dots, q_k)$$

con los valores iniciales $Q(\emptyset) = 1$ y $Q(q) = q$.

PROPIEDADES DE LA FUNCIÓN CONTINUANTE

Demostraremos que la función continuante coincide con la función, $f(q_1, \ldots, q_k)$, definida como

La suma de todos los productos comenzando con $q_1 \cdots q_k$ y eliminando recursiva y sucesivamente todos los productos de pares adjacentes.

Si q_1 no aparece en uno de los productos tampoco está q_2 ya que es su adyacente. Por tanto, la suma de los que no contienen q_1 es exactamente $f(q_3, \ldots, q_k)$. Y en los productos que contienen a q_1, si le sacamos factor común queda $q_1 f(q_2, \ldots, q_k)$. Como los productos se clasifican en estas dos clases, hemos demostrado que

$$f(q_1, \ldots, q_k) = q_1 f(q_2, \ldots, q_k) + f(q_3, \ldots, q_k)$$

Como las dos funciones iniciales son las mismas, por inducción se tiene $Q(q_1, \ldots, q_k) = f(q_1, \ldots, q_k)$. Equivalentemente, si coinciden en los valores iniciales una función recursiva es única.

OTRAS PROPIEDADES

Ahora, como el producto de enteros es asociativo y conmutativo, se tiene que la función continuante es simétrica

$$Q(q_1, \ldots, q_k) = Q(q_k, \ldots, q_1)$$

Y también, para cada natural $i \leq n$, se verifica la desigualdad

$$Q(q_1 \ldots, q_i) Q(q_{i+1} \ldots, q_n) \leq Q(q_1 \ldots, q_n)$$

ya que cada producto que aparece sumando en la izquierda aparece también sumando en la derecha.

EL TEOREMA DE SMITH

Particularizando para $d = 1$, el teorema de Cornacchia-Smith dice que si existen soluciones enteras para $x^2 + y^2 = p$ estas se encuentran aplicando el AE a p y w con $w^2 \equiv -1 \pmod{p}$. Como $x^2 \equiv -1 \pmod{p}$ tiene solución si y sólo si $(-1)^{(p-1)/4} = \left(\frac{-1}{p}\right) = 1$. Existe w si y sólo si p es congruente con 1 módulo 4.

Por tanto, una condición necesaria para que $x^2 + y^2 = p$ tenga solución es que p sea congruente con 1 módulo 4. Pero un teorema de Fermat, demostrado por Euler da la siguiente caracterización:

Un número primo p es expresable como suma de dos cuadrados si y sólo si p = 2 ó es congruente con 1 módulo 4.

Este teorema de Fermat implica que si $p \equiv 1 \pmod{4}$ el método de Cornacchia-Smith siempre encuentra soluciones. Pero se puede dar una nueva demostración del teorema de Fermat, razonando que $B_\nu^2 < p$ y por tanto

$$r_{\nu+1}^2 + B_\nu^2 = \lambda p < 2p \Longrightarrow r_{\nu+1}^2 + B_\nu^2 = p$$

Para eso necesitamos la función continuante que revierte el AE. O sea, dados los cocientes sucesivos obtiene el primer resto. Si $q_1 \ldots, q_n$ es la sucesión de cocientes obtenida al aplicar el AE a p, w, como la función continuante verifica la desiguladad $Q(q_1 \ldots, q_n) \geq Q(q_1 \ldots, q_\nu)Q(q_{\nu+1} \ldots, q_n)$, finalmente se tiene

$$\left.\begin{array}{l} p = Q(q_1 \ldots, q_n) \\ r_\nu = Q(q_{\nu+1} \ldots, q_n) > \sqrt{p} \\ |B_\nu| = Q(q_\nu \ldots, q_1) = Q(q_1 \ldots, q_\nu) \end{array}\right\} \Rightarrow p \geq r_\nu |B_\nu| > \sqrt{p}|B_\nu| \Rightarrow \sqrt{p} > |B_\nu| \Leftrightarrow B_\nu^2 < p$$

Notaremos que la igualdad $|B_\nu| = Q(q_\nu \ldots, q_1)$ sólo es cierta cuando w es una raíz cuadrada de -1 módulo p.

O sea, hemos demostrado el **teorema de Smith**.
Si p es congruente con 1 módulo 4, el método de Cornacchia-Smith descompone p como suma de cuadrados.

Enrique R. Aznar García
eaznar@ugr.es