Un nuevo algoritmo para buscar valores pequeños no nulos de $|x^3 - y^2|$.

Ismael Jiménez, *C.S.I.C.*

Javier Herranz y Germán Sáez, *Universitat Politècnica de Catalunya.*

ijcalvo@terra.es, jherranz@mat.upc.es, german@mat.upc.es

Ecuación de Mordell:

$$k = x^3 - y^2.$$

- Si $x = t^2$ e $y = t^3$, $k = 0$.
- En los demás casos, la ecuación corresponde a una curva elíptica.
- ¿Como crece el valor mínimo de k en función de x?
- A. Baker (1967) y H. M. Stark (1973) probaron que

$$k \gg_\epsilon \log(x)^{1-\epsilon}.$$

Conjetura de Hall

M. Hall (1971): Para $x < 700.000$, $k > Cx^{1/2}$, $C = 1/5$.

Marshall Hall (1965, 1971):

$$\begin{aligned} f(t) &= \tfrac{t}{9}(t^9 + 6t^6 + 15t^3 + 12), \\ g(t) &= \tfrac{t^{15}}{27} + \tfrac{t^{12}+4t^9+8t^6}{3} + \tfrac{5t^3+1}{2}, \\ f^3(t) - g^2(t) &= -\tfrac{3t^6+14t^3+27}{108}, \quad k > x^{3/5}. \end{aligned}$$

Davenport (1965): "Si el grado de $f(t)$ es r, el grado de $f^3(t) - g^2(t) > r/2$".

L. V. Danilov (1982): Familia polinómica infinita del tipo,

$$(t^2+6t-11)^3-(t^2-5)^2\left((t-9)^2+4\right)=1728t-3456.$$

N. Elkies (1998):

$$(t^2+10t+5)^3-(t^2+4t-1)^2(t^2+22t+125)=1728t.$$

$$k<0.966\,x^{1/2}.$$

L. V. Danilov (1982): Familia polinómica infinita del tipo,

$$(t^2+6t-11)^3-(t^2-5)^2\left((t-9)^2+4\right)=1728t-3456.$$

N. Elkies (1998):

$$(t^2+10t+5)^3-(t^2+4t-1)^2(t^2+22t+125)=1728t.$$

$$k<0.966\,x^{1/2}.$$

CONJETURA DE HALL:

$$|x^3-y^2|\gg_\epsilon x^{1/2-\epsilon}.$$

Motivación y problemas afines

- Criptoanálisis RSA.

$$x^e \equiv c \pmod{m}.$$

- Puntos enteros en curvas.
- Puntos de un retículo cercanos a una curva.
- Algoritmos LLL de reducción de base.

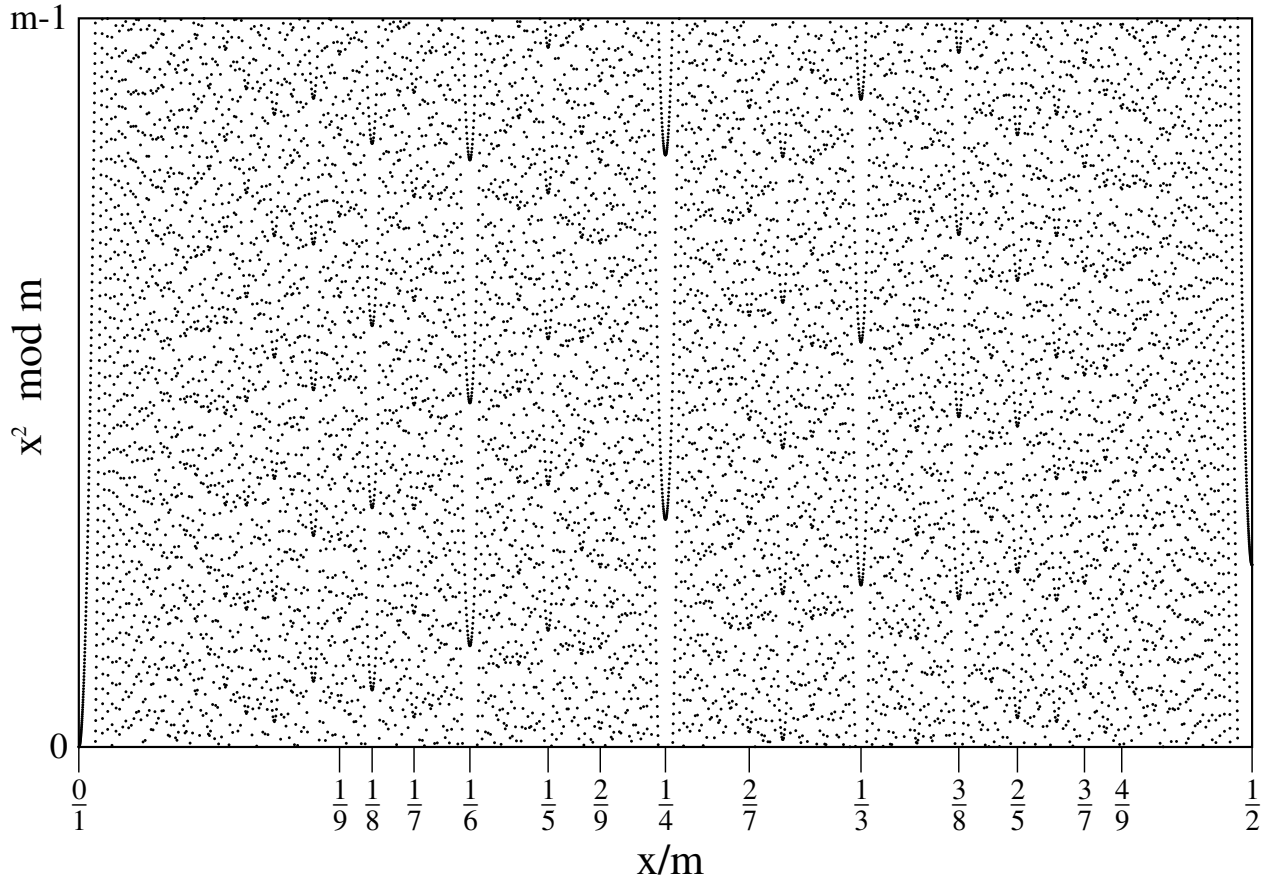

Figure 1: Residuos cuadráticos

Geometría de $k(x)$

$$k(x) = x^3 - \left\lfloor x^{3/2} \right\rfloor^2,$$

$$t = a/b, \quad \alpha \equiv a^2 \pmod{b^2}, \qquad x_0 = \lfloor t^2 \rfloor = \frac{a^2 - \alpha}{b^2}.$$

$$k(x_0 + i) = (x_0 + i)^3 - y^2, \quad y = \left\lfloor (x_0 + i)^{3/2} \right\rfloor.$$

$$k(x_0+i) =$$

$$\frac{-2Ca^3+\frac{3}{4}(b^2i-\alpha)^2a^2-3(b^2i-\alpha)Ca-C^2+(b^2i-\alpha)^3}{b^6},$$

donde los valores de C e i deben cumplir

$$2a^3+3(b^2i-\alpha)a+2C\equiv 0 \pmod{2b^3}.$$

$$P_j(x) = x^3 - (\frac{3}{2}t)^2x^2 + (\frac{3}{2}t^4 - \frac{3C}{b^3}t)x + \frac{C}{b^3}t^3 - \frac{C^2}{b^6} - \frac{1}{4}t^6.$$

$$x = x_0 + j + b'\omega,$$

$$0 \leq j < b', b' = 2b/\gcd(3a, 2b)$$

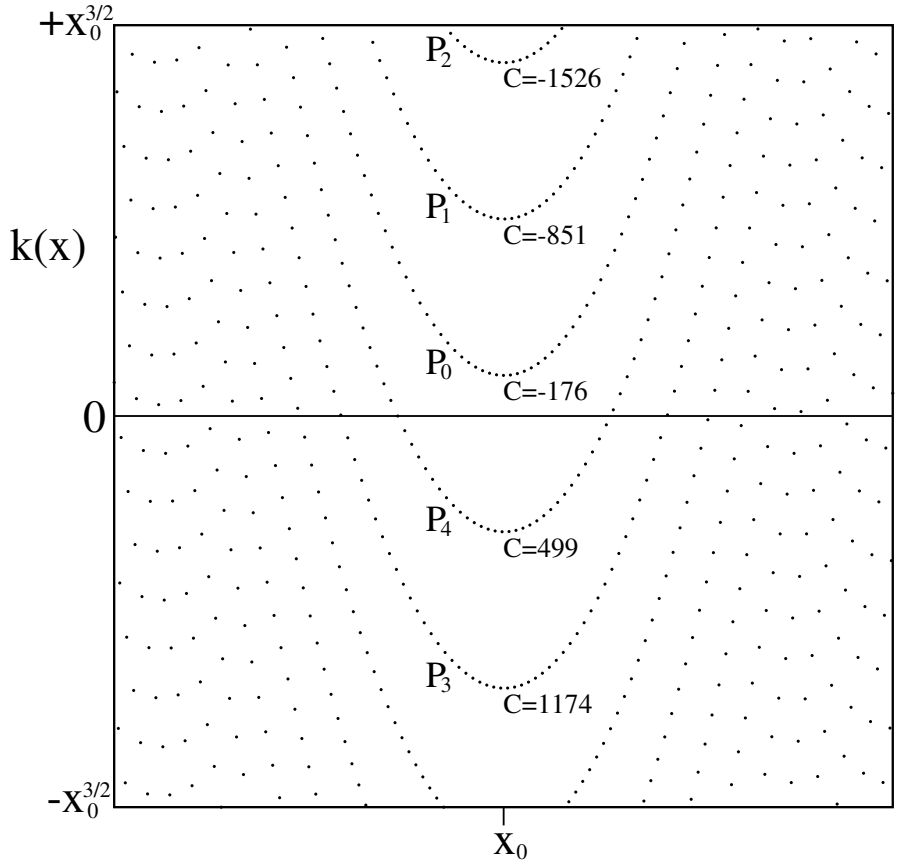

Figure 2: Polinomios para $t = 222272/15$

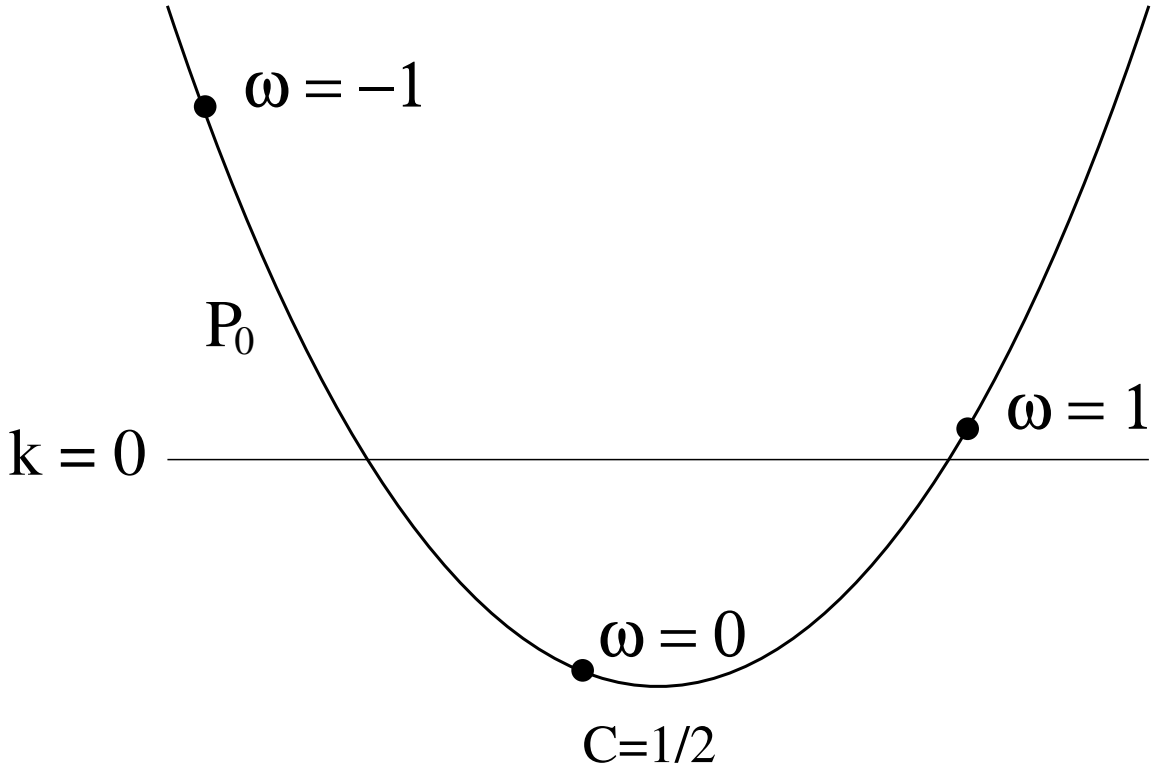

Figure 3: Mejor polinomio: P_0, $\omega = 0, \pm 1$

El nuevo algoritmo

$$2a^3 + 3(b^2 j - \alpha)a + 2C \equiv 0 \pmod{2b^3}.$$

$$a \equiv (2C)^{1/3} \pmod{b^2}.$$

C. Padró and G. Sáez, *Taking cube roots on* $\mathbb{Z}_m$*.*
Appl. Math. Lett. **15** (2002), 703–708.

Casos con $k < \sqrt{x}$.

#	x	k	$\lvert k\rvert/\sqrt{x}$	Comentarios
1	2	-1	0.72	-
2	5234	17	0.23	H, GPZ
3	8158	24	0.27	H. GPZ
4	93844	-297	0.97	H, GPZ
5	367806	207	0.34	H, GPZ
6	421351	-618	0.95	H, GPZ
7	720114	-225	0.27	H, GPZ
8	939787	307	0.32	H, GPZ
9	28187351	307	0.32	H, GPZ
10	110781386	-8569	0.81	H, GPZ
11	154319269	-11492	0.93	H, GPZ
12	384242766	-14668	0.75	H, GPZ
13	390620082	-14857	0.75	H, GPZ
14	3790689201	-28024	0.46	GPZ
15	65589428378	-117073	0.46	E
16	952764389446	852135	0.87	E
17	12438517260105	2767769	0.78	E
18	35495694227489	5190544	0.87	E
19	53197086958290	-4401169	0.60	E
20	5853886516781223	1641843	0.021	E!
21	12813608766102806	-87002345	0.77	E
22	23415546067124892	105077952	0.69	E
23	38115991067861271	30032270	0.15	E
24	322001299796379844	548147655	0.97	E
25	471477085999389882	-497218657	0.72	E
26	810574762403977064	-193234265	0.21	E
27	9870884617163518770	1651035656	0.53	JHS
28	42532374580189966073	1878790553	0.29	JHS
29	51698891432429706382	4101044247	0.57	JHS
30	44648329463517920535	-3732472441	0.56	JHS
31	231411667627225650649	-4103440667	0.27	JHS
32	601724682280310364065	13027681441	0.53	JHS
33	4996798823245299750533	-32544033652	0.46	JHS
34	14038790674256691230847	93061667259	0.79	JHS
35	77148032713960680268604	-27285673040	0.098	JB!
36	18017900429510584966881 8	75183236932	0.18	JB
37	372193377967238474960883	-460298021013	0.75	JHS
38	20288713731858925006361 55	-1246491276481	0.88	JB