Cálculo de preimágenes del producto por enteros en curvas elípticas mediante álgebra lineal

Josep M. Miret, Jordi Pujolàs, Nicolas Thériault

Departament de Matemàtica, UdL

Departamento de Matemática y Ciencia de la Computación, USaCh

Proyecto "Nuevas herramientas criptográficas para la e-comunidad"
Programa Iberoamericano CyTeD
Lleida, miércoles 4 de mayo de 2022

k cuerpo, $char(k) \nmid 6, \quad \alpha_1, \alpha_2 \in k$

$$E : y^2 = x(x-\alpha_1)(x-\alpha_2) = x(x^2 + ax + b)$$

Producto por enteros $\begin{array}{ccc} \ell : E & \longrightarrow & E \\ P & \longmapsto & \ell P \end{array}$

Problema ($\ell = 2$): Dado $Q = (x_Q, y_Q) \in E(k)$, encontrar $\frac{1}{2}Q = \{P \in E(k) \mid 2P = Q\}$ "en términos de Q".

Formulas de adición:

$$a_2 = a,\ a_4 = b, a_6 = a_1 = a_3 = 0$$

$$b_2 = a_1^2 + 4a_2 = 4a,\ b_4 = 2a_4 + a_1 a_3 = 2b,$$

$$b_6 = a_3^2 + 4a_6 = 0,\ b_8 = \ldots = -b^2$$

$$x(2P) = \frac{x_P^4 - b_4 x_P^2 - 2b_6 x_P - b_8}{4x_P^3 + b_2 x_P^2 + 2b_4 x_P + b_6} =$$

$$\frac{x_P^4 - 2bx_P^2 + b^2}{4x_P^3 + 4ax_P^2 + 4bx_P} = \frac{(x_P^2 - b)^2}{4x_P(x_P^2 + ax_P + b)} =$$

$$= \left(\frac{x_P^2 - b}{2y_P}\right)^2 = x_Q \text{ es un cuadrado!!}$$

Recta $\overline{-PQ}$: $y = m(x - x_Q) + y_Q$

$$m = \frac{y_Q - y_{-P}}{x_Q - x_{-P}} = \frac{y_Q + y_P}{x_Q - x_P} = \frac{-f'(x_p)}{2y_P}$$

Proposición

$f(x) - (m(x - x_Q) + y_Q)^2 = (x - x_Q)(x - x_P)^2$

Proof.

La parte izquierda es un polinomio cúbico mónico. Raíces?

$$x = x_Q \Rightarrow f(x_Q) - (y_Q)^2 = 0$$

$$x = x_P \Longrightarrow f(x_P) - (-y_P)^2 = 0$$

x_P es una raíz doble:

$$f'(x_P) - 2(m(x_P - x_Q) + y_Q)m = f'(x_P) - 2(-y_Q - y_P + y_Q)m =$$

$$= f'(x_P) + 2y_P m = 0 \ \square$$

La identidad equivalente

$$\frac{f(x) - (m(x - x_Q) - y_Q)^2}{(x - x_Q)} = (x - x_P)^2$$

se interpreta con los algoritmos de Cantor: la izquierda son todas las 1as coordenadas no reducidas posibles que reducen a Q y la derecha es el representante no reducido de componer P con P. Evaluando $x = 0, \alpha_1, \alpha_2$ en

$$x - x_Q = \frac{f(x) - (m(x - x_Q) - y_Q)^2}{(x - x_P)^2}$$

vemos mas cuadrados y los sistemas lineales del título:

$$0 - x_Q = \frac{f(0) - (m(0 - x_Q) - y_Q)^2}{(0 - x_P)^2} = -w_0^2 \iff \frac{m(0 - x_Q) - y_Q}{x_P} = w_0$$

$$\alpha_1 - x_Q = \frac{f(\alpha_1) - (m(\alpha_1 - x_Q) - y_Q)^2}{(\alpha_1 - x_P)^2} = -w_1^2 \iff \frac{m(\alpha_1 - x_Q) - y_Q}{\alpha_1 - x_P} = w_1$$

$$\alpha_2 - x_Q = \frac{f(\alpha_2) - (m(\alpha_2 - x_Q) - y_Q)^2}{(\alpha_2 - x_P)^2} = -w_2^2 \iff \frac{m(\alpha_2 - x_Q) - y_Q}{\alpha_2 - x_P} = w_2$$

donde w_i son los "bisectores de Q"

$$w_0 = \sqrt{x_Q}, \quad w_1 = \sqrt{x_Q - \alpha_1}, \quad w_2 = \sqrt{x_Q - \alpha_2}$$

y cumplen $w_0, w_1, w_2 \in k \iff P \in E(k)$

Desarrollando

$$\begin{aligned}(x - x_P)^2 &= \frac{f(x) - (m(x - x_Q) - y_Q)^2}{x - x_Q} \\ &= x^2 + (a + x_Q - m^2)x + x_Q^2 + ax_Q + b + x_Q m^2 + 2y_Q m.\end{aligned}$$

e igualando coeficientes se obtiene

$$\begin{aligned} 2x_P &= m^2 - a - x_Q, \\ x_P^2 &= x_Q^2 + ax_Q + b + x_Q m^2 + 2y_Q m, \end{aligned}$$

y sustituyendo se concluye que el conjunto de m's satisface

$$\varphi_Q(m) = m^4 - 2(3x_Q + a)\, m^2 - 8y_Q\, m + (a^2 - 4b) - x_Q(3x_Q + 2a)$$

La factorización de φ_Q en $k(w_0)$ permite dar sus raíces como

$$M_Q = \{w_0 \pm (w_1 + w_2), -w_0 \pm (w_1 + w_2)\}$$

y por lo tanto nuestro objetivo

$$\frac{1}{2}Q = \left\{ \left(\frac{m^2 - a - x_Q}{2}, \frac{m^3 - ma - 3mx_Q - 2y_Q}{2} \right), \quad m \in M_Q \right\}$$

Caso $\ell = 3$

Problema:

Dado $Q = (x_Q, y_Q) \in E(k)$, encontrar $\frac{1}{3}Q = \{P \in E(k) \mid 3P = Q\}$.

Quién hace de α_1, α_2??

Modelo 3-torsion friendly: $a, b \in k, b \neq 0, b \neq a^3$

$$E : y^2 + 3axy + by = x^3,$$

$$(0,0) \in E[3](k)$$

Proposición

E es isomorfa al modelo de Weierstrass

$$\widehat{\mathrm{E}} : y^2 = x^3 + (3a\delta - 3\gamma^2)x + (2\gamma^3 + \delta^2 - 3a\gamma\delta)$$

si y solamete si $(\gamma, \delta) \in \widehat{\mathrm{E}}[3]$.

Corolario

En $E : y^2 + 3axy + by = x^3$, $(0,0) \in E[3]$.

Recurrencia habitual entre polinomios de división en E:

$$\Psi_1(x) = 1,$$
$$\Psi_2(x,y) = 2y + 3ax + b,$$
$$\Psi_3(x) = 3x^4 + 9a^2x^3 + 9abx^2 + 3b^2x,$$
$$\Psi_4(x,y) = \Psi_2(x,y) \cdot (2x^6 + 9a^2x^5 + 15abx^4 + 10b^2x^3 - 3ab^3x - b^4),$$
$$\Psi_5(x) = \Psi_4(x,y)\Psi_2^2(x,y) - \Psi_3^3(x),$$
$$\dots$$

$E[3]$

- $P=(x,y) \Rightarrow -P=(x,-y-3x-b), \quad -(0,0)=(0,-b)$
- $P+(0,0)=(-by/x^2,-b^2y/x^3), \quad P-(0,0)=(bx/y,-bx^3/y^2)$

Por lo tanto

$$\Psi_3(c)=0, c\neq 0 \Longrightarrow E[3]=\langle (c,d),(0,0)\rangle =$$

$$\left\{ \begin{array}{llll} (0,0), & (0,-b), & (-\frac{bd}{c^2},-\frac{b^2d}{c^3}), & (-\frac{bd}{c^2},\frac{b^2d}{c^3}+\frac{3abd}{c^2}-b), \\ (c,d), & (c,-d-3c-b), & (\frac{bc}{d},-\frac{bc^3}{d^2}), & (\frac{bc}{d},\frac{bc^3}{d^2}-\frac{3abc}{d}-b) \end{array} \right\}$$

Proposición

$\tilde{E}: y^2+3\tilde{a}xy+\tilde{b}y=x^3, \qquad E: y^2+3axy+by=x^3$

$$\tilde{E}\sim E \Leftrightarrow \tilde{a}=a+2m/3,\ \tilde{b}=b+2d+3ac$$

con $(c,d)\in E[3], \quad m=(3c^2+3ad)/(3ac+b+2d).$

Polinomios de 3-división

$$\Psi_3(x) = 3x^4 + 9a^2x^3 + 9abx^2 + 3b^2x \quad \text{en } E$$

$$\tilde{\Psi}_3(\tilde{x}) = 3\tilde{x}^4 + 9\tilde{a}^2\tilde{x}^3 + 9\tilde{a}\tilde{b}\tilde{x}^2 + 3\tilde{b}^2\tilde{x} \quad \text{en } \tilde{E}$$

$$\wr\ \varphi$$

$$3(x-c)^4 + (3a+2m)^2(x-c)^3 + 3(3a+2m)(3ac+b+2d)(x-c)^2$$
$$+3(3ac+b+2d)^2(x-c)$$

Si x es la 1a coordenada de un punto de E entonces

$$\tilde{\Psi}_3(\tilde{x}) = \Psi_3(x)$$

dado que a, b, c, d cumplen las condiciones necesarias para ello.

Miret, Moreno, Rio, Valls (2009) se dan cuenta de que

$$y_{[3]P} \in k^3$$

e identifican un segundo cubo involucrado en el cálculo de P.

Tenemos dos raíces cúbicas "independientes" explícitamente, mediante las que encontramos P.

Teorema

$E : y^2 + 3axy + by = x^3, \quad P = (x, y) \in E(k) \setminus E[3]$. Entonces

$$y_{[3]P} = \left(\frac{(x^3 - 3abx - 2b^2)y - (4bx^3 + 9a^2bx^2 + 6ab^2x + b^3)}{\Psi_3(x)} \right)^3$$

Demostración: Por propiedades de los $\Psi_j(x)$ se tiene $y_{[3]P} =$

$$\frac{\frac{1}{2}\left(\Psi_5(P)\Psi_2(P) - \Psi_4(P)\Psi_4^*(P) - 3ax_P\Psi_3(P)^3 + 3a\Psi_2(P)\Psi_3(P)\Psi_4(P) - b\Psi_3(P)^3\right)}{\Psi_3(P)^3}$$

Simplificando $y^2 \leftrightarrow x^3 - 3axy - by$ y tomando

$$\begin{aligned} \mu_{a,b}(x) &= x^3 - 3abx - 2b^2 \\ \nu_{a,b}(x) &= -(4bx^3 + 9a^2bx^2 + 6ab^2x + b^3) \end{aligned}$$

entonces el numerador de $y_{[3]P}$ tiene la forma

$$\left(\mu_{a,b}(x)\cdot y+\nu_{a,b}(x)\right)^3+k(x,y)\cdot\underbrace{(y^2+3axy+by-x^3)}_{=0}(x^3-3abx-2b^2)^2,$$

$$\begin{aligned} k(x,y) = \quad & y(x^3-3abx-2b^2)-(3ax-9a^3+13b)\Psi_3^*(x) \\ & +3a^2(10b-9a^3)x^2+3ab(11b-9a^3)x+3b^2(4b-3a^3) \end{aligned}$$

Corolario

$y_Q \notin k^3 \Longrightarrow Q \notin [3]E(k)$

Corolario

$E: y^2+3axy+by=x^3$, $(c,d)\in E[3]$, $c\neq 0$,
$m=(3c^2+3ad)/(3ac+b+2d)$, $Q=(x_Q,y_Q)\in[3]E(k)$,
$y_Q-d-m(x_Q-c)\notin k^3 \Longrightarrow Q\notin[3]E(k)$

Teorema

$Q=(x_Q,y_Q)\in[3]E(k)\setminus E[3] \Longrightarrow y_Q,\ y_Q-d-m(x_Q-c)\in k^3$

Trisectores

Los *trisectores* de $Q \in E(k)$ son

$$\omega_1(Q) = \sqrt[3]{y_Q} \quad , \quad \omega_2(Q) = \sqrt[3]{y_Q - d - m(x_Q - c)}$$

$$Q \in [3]E(k) \leftrightarrow 9 \text{ pares } \{\omega_1(Q), \omega_2(Q)\} \subset k \times k$$

Pregunta: Cada par corresponde a una trisección $P \in \frac{1}{3}Q$ de Q?

Dado $Q \in [3]E(k)$ y un par de trisectores $\{\omega_1, \omega_2\}$ la trisección P correspondiente es la solución del sistema

$$\begin{cases} \omega_1 \Psi_3(x_P) = \mu_{a,b}(x_P) \cdot y + \nu_{a,b}(x_P) \\ \omega_2 \Psi_3(x_P) = \tilde{\mu}_{a,b}(x_P) \cdot y + \tilde{\mu}_{a,b}(x_P) \end{cases}$$

x_P se encuentra con el gcd de las dos resultantes de cada equación respecto de y.

Funciones de trisecado:

$$\omega_1(x,y) = \frac{\mu_{a,b}(x)\cdot y + \nu_{a,b}(x)}{\Psi_3(x)}$$

$$\omega_2(x,y) = \frac{\tilde{\mu}_{\tilde{a},\tilde{b}}(\tilde{x})\cdot \tilde{y} + \tilde{\nu}_{\tilde{a},\tilde{b}}(\tilde{x})}{\widetilde{\Psi}_3(\tilde{x})}$$

Teorema

Para todo $P=(x,y)\in E(k)\setminus E[3]$, las funciones de trisecado $\omega_1(P),\omega_2(P)$ cumplen

$$\begin{array}{rrcl} i) & \omega_1(P+(0,0)) & = & \omega_1(P), \\ ii) & \omega_2(P+(0,0)) & = & \zeta_2\cdot\omega_2(P), \\ iii) & \omega_1(P+(c,d)) & = & \zeta_1\cdot\omega_1(P), \\ iv) & \omega_2(P+(c,d)) & = & \omega_2(P). \end{array}$$

con $\zeta_1,\zeta_2\in k$ raíces cúbicas de la unidad.

En el caso general $\ell P = Q$, suponiendo

$$E[\ell] = \langle W_1,\ W_2 \rangle$$

entonces las funciones $h_1,\ h_2,\ g_P$ definidas por

$$div(h_i) = \ell W_i - \ell \mathcal{O}$$

$$div(g_P) = \ell P + (-Q) - (\ell + 1)\mathcal{O}$$

cumplen

$$\Big(g_P(W_i)\Big)^{\ell} = h_i(-Q) \cdot \Big(h_i(P)\Big)^{\ell}$$

por lo tanto $h_i(-Q)$ es una potencia ℓ.

Gracias por su atención