

Un método más rápido para la inversión generalizada de emparejamientos

Lael Cellier

lael.cellier@laposte.net

5 de octubre de 2026

Resumen

Satoh propuso recientemente un algoritmo para el problema de inversión generalizada de emparejamientos (GPI) que explota la estructura de la función de Miller en lugar de la búsqueda exhaustiva o de un oráculo con argumento fijo. Sobre una curva ordinaria, su coste esperado es del orden de $(q^k - 1)/\ell^2$ llamadas a una rutina de búsqueda de raíces de grado $\Omega(\ell)$, es decir $\tilde{O}((q^k - 1)/\ell)$ operaciones. Doy un método distinto para el mismo problema, válido para curvas ordinarias de grado de inmersión par $k > 2$ que admiten una torsión (*twist*) de grado par $e \geq 4$, cuyo coste esperado es de $q^{k/e}/2$ candidatos costando cada uno unos pocos emparejamientos: medida en multiplicaciones en $\mathbb{F}_{q^k}$, la mejora sobre el algoritmo de Satoh es un factor $q^{k-k/e}/\ell$ salvo constantes y logaritmos. El análisis utiliza un bucle de Miller de longitud múltiplo de ℓ , como en el emparejamiento de Tate, mientras que el bucle de Satoh tiene longitud $q^{k/2} \equiv -1 \pmod{\ell}$; el emparejamiento objetivo sólo interviene a través de un test final de pertenencia, de modo que el algoritmo resuelve GPI para el emparejamiento de Satoh directamente, sin conversión entre emparejamientos y sin logaritmo discreto en ninguna parte. El valor reducido del emparejamiento y la norma del valor bruto de Miller son coordenadas independientes, un hecho de restos chinos ya que $\gcd(\ell, q^{k/2} - 1) = 1$; el método es en consecuencia una búsqueda sobre pares de abscisas con un test final de emparejamiento, y no pretendo otra cosa: el núcleo técnico — una inversión en tiempo polinómico del valor bruto de Miller con ambos argumentos desconocidos — sirve para fijar ese espacio de búsqueda y para mostrar que nada en esta vía puede reducirlo. El test toma como entrada el valor bruto de Miller antes de la exponenciación final — la misma entrada que el propio algoritmo de inversión de Miller de Satoh, que ningún protocolo expone; pasar del valor reducido a ella es el paso de inversión de la exponenciación de Galbraith, Hess y Vercauteren, que las secciones 6–8 tratan por búsqueda y que la proposición 6.2 muestra imposible de atajar mediante la norma — y combina la relación de norma del trabajo anterior de Satoh sobre inversión de Miller con una proyección $\mathbb{F}_q$ -lineal que separa las dos abscisas desconocidas, las cuales viven en subespacios $\mathbb{F}_q$ -complementarios de $\mathbb{F}_{q^{k/2}}$; la explotación de esa estructura de subcuerpo se remonta a Akagi y Nogami, cuya reducción exige sin embargo que uno de los argumentos sea conocido. Sobre BN254 el coste esperado pasa de unos 2^{2800} a 2^{518} multiplicaciones en $\mathbb{F}_{q^k}$, sobre BLS12-381 de unos 2^{4325} a 2^{772} . Todas estas cifras permanecen muy por encima del coste del cálculo de índices en $\mathbb{F}_{q^k}$; el resultado es estructural, no criptoanalítico.

1 Introducción

Galbraith, Hess y Vercauteren [3] aislaron tres problemas de inversión para un emparejamiento bilineal $e: G_1 \times G_0 \rightarrow \mu_\ell$: los dos problemas con argumento fijo FAPI-1 y FAPI-2, en los que uno de los argumentos está dado, y el problema generalizado GPI, en el que sólo se da el objetivo z y cualquier par de preimágenes es admisible.

Satoh [7] observó que no se conocía ningún algoritmo que explotase la estructura matemática del cálculo del emparejamiento, en lugar de buscar en uno de los grupos, y dio uno: escribiendo la ℓ -ésima función de Miller como un sistema de factores, obtiene una descomposición del emparejamiento. Ate a partir de la cual una solución de GPI se ensambla mediante un paso de búsqueda de raíces. El

procedimiento resultante [7, Alg. 6.1] recorre $\gamma \in \mu_{\nu(s-1)}$, donde $s = q^{k/2}$ y $\nu = (s + 1)/N$, y en cada paso busca las raíces de una función φ de grado $(N - 1)/2$. Sobre una curva ordinaria, $\nu(s - 1) = (q^k - 1)/\ell$ y la probabilidad de éxito por paso es a lo sumo $(\ell - 1)/((s - 1)\nu)$ [7, Rem. 6.5], de modo que el coste esperado es del orden de $(q^k - 1)/\ell^2$ búsquedas de raíces de grado $\ell/2$, esto es $\tilde{O}((q^k - 1)/\ell)$ operaciones; Satoh describe este caso como «demasiado ineficiente incluso para experimentos numéricos con valores pequeños de q ».

Esta nota da un método distinto para el mismo problema, con menor coste esperado. Es, como el de Satoh, una búsqueda ciega con un test final de emparejamiento — aquí sobre pares de abscisas — y la proposición 6.2 muestra por qué nada construido sobre la norma del valor de Miller puede ser otra cosa: el valor reducido del emparejamiento y esa norma son coordenadas independientes. Dos puntos de encuadre son esenciales y se enuncian de entrada.

Longitud del bucle. El método toma la función de Miller $h_{d,A}$ en el argumento $\mathbb{F}_q$ -racional $A \in G_1$, evaluada en el argumento de traza nula $Q \in G_0$, con una longitud de bucle d múltiplo de ℓ — el marco de Tate. El algoritmo 6.1 de Satoh produce, en la notación de esta nota, $h_{q^{k/2}, -Q}(A)$ (sus letras A y Q son las inversas de las mías: su A está en G_0), con la función de Miller en el argumento de traza nula y un bucle de longitud $s = q^{k/2}$. La distinción que importa no es la orientación sino el residuo de la longitud del bucle módulo ℓ : la relación de norma en la que se apoya esta nota (proposición 3.1) da $(\xi(Q) - \xi(A))^d$ cuando $d \equiv 0 \pmod{\ell}$, y $(\xi(Q) - \xi(A))^{d-1}$ cuando $d \equiv -1 \pmod{\ell}$, que para $d = s$ vale idénticamente 1 (observación 3.2). El presente método, por tanto, *no* sustituye el paso interno de [7, Alg. 6.1], y no pretendo que lo haga. Lo que es cierto es que el emparejamiento objetivo sólo interviene en el método a través de un test final de pertenencia, de modo que puede tomarse igual al propio emparejamiento de Satoh (sección 6); ninguna conversión entre emparejamientos, y en particular ningún logaritmo discreto, interviene en ninguna parte.

Qué hay de nuevo. El núcleo del método es un procedimiento en tiempo polinómico que, a partir de un valor bruto de Tate–Miller $h_{d,A}(Q)$ con A y Q desconocidos, recupera A y Q (sección 5). Combina la relación de norma usada por Satoh en el marco de argumento fijo [6] con una proyección lineal que separa las dos abscisas desconocidas, las cuales viven en subespacios $\mathbb{F}_q$ -complementarios de $\mathbb{F}_{q^{k/2}}$ (sección 4). Esa estructura de subcuerpo fue explotada por primera vez por Akagi y Nogami [1], que reducen el problema de inversión de la exponenciación al exponente $q - 1$ para FAPI-2 formando el polinomio mínimo de la abscisa *dada*; su construcción requiere $\text{Tr}(\xi(Q)^3)$ y $N(\xi(Q))$ y no se traslada al caso en que Q es desconocido. El paso de «una incógnita, polinomio mínimo» a «dos incógnitas, proyección lineal» es la novedad técnica. En torno a él la nota añade la independencia del valor del emparejamiento y de la norma (proposición 6.2), que fija el espacio de búsqueda y muestra que no puede reducirse por esta vía; las formas cerradas de los valores de Miller de longitudes de bucle s y q como potencias del emparejamiento de Tate reducido (lema 3.3, observación 3.4), que permiten al algoritmo apuntar directamente a los emparejamientos de Satoh; y un recuento de la mejora sobre [7, Alg. 6.1] en cuatro factores, cada uno atribuido a uno de esos resultados (sección 10).

Anoto de paso que GPI no carece de consecuencias criptográficas: una prueba Groth16 [5] se acepta en cuanto se cumple una única ecuación producto de emparejamientos, y fijar su tercer elemento igual a $\mathcal{O}$ deja un valor objetivo calculable a partir sólo de la clave de verificación y de la entrada pública, de modo que cualquier solución de GPI proporciona una falsificación para un enunciado arbitrario. Como Groth16 sobre BN254 y BLS12-381 protege sistemas de criptomonedas en producción, tal falsificación sería un robo de fondos — fuera de todo alcance a los costes de la sección 10, pero una razón para vigilar GPI, y no sólo FAPI.

2 Marco y notación

Sea q una potencia de un primo impar y $E/\mathbb{F}_q$ una curva elíptica ordinaria con modelo de Weierstrass corto $Y^2 = X^3 + a_4X + a_6$. Sea ℓ un primo impar con $\ell \parallel \#E(\mathbb{F}_q)$ — divisibilidad exacta, $\ell \mid \#E(\mathbb{F}_q)$ y $\ell^2 \nmid \#E(\mathbb{F}_q)$, de modo que $h := \#E(\mathbb{F}_q)/\ell$ es primo con ℓ , lo que necesita el lema 6.1 — de grado de inmersión par $k > 2$; como $k = \text{ord}_\ell(q)$ divide a $\ell - 1$, se tiene $\ell \nmid k$ automáticamente. Siguiendo [7,

§5] pongo

$$s := q^{k/2}, \quad G_0 := \{P \in E[\ell] : \text{Fr}_q P = [q]P\}, \quad G_1 := E(\mathbb{F}_q) \cap E[\ell],$$

de modo que $G_0 \cong G_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, $G_0 \cap G_1 = \{\mathcal{O}\}$ y $E[\ell] = G_1 \oplus G_0$. Como $\ell \mid s + 1$, se tiene $\text{Fr}_q^{k/2} P = -P$ para $P \in G_0$; y como $\ell \nmid s - 1$, $\text{Fr}_q^{k/2}$ sólo tiene los valores propios 1 sobre G_1 y -1 sobre G_0 , de donde

$$E[\ell] \cap \ker(\text{Fr}_q^{k/2} - 1) = G_1, \quad E[\ell] \cap \ker(\text{Fr}_q^{k/2} + 1) = G_0. \quad (1)$$

ξ, η denotan las funciones coordenadas, $\tau := -\xi/\eta$ el uniformizante en $\mathcal{O}$, y $h_{n,A}$ la n -ésima función de Miller normalizada en A , es decir la función con $\text{div } h_{n,A} = n[A] - [nA] - (n-1)[\mathcal{O}]$ y $\text{lc}_{\mathcal{O}}(h_{n,A}) = 1$ respecto de τ .

En todo lo que sigue, $A \in G_1$, $Q \in G_0$, y d es un entero con

$$\ell \mid d; \quad (2)$$

cuando haya que extraer una raíz d -ésima (lema 3.5) supongo además $d \mid s + 1$, la segunda condición de [6, Alg. 4.1]. El valor bruto de Miller es $v := h_{d,A}(Q) \in \mathbb{F}_{q^k}^\times$ y el emparejamiento de Tate reducido es $t(A, Q) := h_{\ell,A}(Q)^{(q^k-1)/\ell} \in \mu_\ell$, bilineal y no degenerado sobre $G_1 \times G_0$.

3 La relación de norma

Proposición 3.1. *Con la notación anterior, y usando sólo $\ell \mid d$,*

$$v^{s+1} = (-1)^d (\xi(Q) - \xi(A))^d. \quad (3)$$

En particular $v^{s+1} = -(\xi(Q) - \xi(A))^\ell$ para $d = \ell$.

Prueba. Como $\ell \mid d$ y $A \in E[\ell]$, $[d]A = \mathcal{O}$ y $\text{div } h_{d,A} = d([A] - [\mathcal{O}])$; igualmente $\text{div } h_{d,-A} = d([-A] - [\mathcal{O}])$. Luego $h_{d,A}h_{d,-A}$ y $(\xi - \xi(A))^d$ tienen el mismo divisor $d([A] + [-A] - 2[\mathcal{O}])$, y ambas tienen coeficiente director 1 en $\mathcal{O}$ puesto que $\xi = \tau^{-2} + \mathcal{O}(\tau^{-1})$; así

$$h_{d,A}h_{d,-A} = (\xi - \xi(A))^d. \quad (4)$$

A continuación, $h_{d,A} \circ [-1]$ y $h_{d,-A}$ tienen el mismo divisor; como $\tau \circ [-1] = -\tau$ para un modelo de Weierstrass corto y $\text{ord}_{\mathcal{O}} h_{d,A} = -d$, se tiene $\text{lc}_{\mathcal{O}}(h_{d,A} \circ [-1]) = (-1)^d$, de donde

$$h_{d,A} \circ [-1] = (-1)^d h_{d,-A}. \quad (5)$$

Por último $h_{d,A}$ está definida sobre $\mathbb{F}_q$ y $\text{Fr}_q^{k/2} Q = -Q$, luego $v^s = h_{d,A}(\text{Fr}_q^{k/2} Q) = h_{d,A}(-Q) = (-1)^d h_{d,-A}(Q)$ por (5), y $v^{s+1} = v \cdot v^s = (-1)^d (h_{d,A}h_{d,-A})(Q)$, que es (3) por (4). $\square$

El miembro derecho de (3) no contiene ningún valor de Miller. Compárese con la factorización $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$ que subyace a [6, Alg. 4.1]: allí el factor $h_{s,A}(Q)$ se elimina mediante una potencia $(s+1)$ -ésima. Su estructura exacta la da el lema 3.3: $h_{s,A}(Q) = -t(A, Q)^{-1/2}$, elemento de orden exactamente 2ℓ divisor de $s+1$, cuyo opuesto $-h_{s,A}(Q) = t(A, Q)^{-1/2}$ está en μ_ℓ ; con la función de Miller en el argumento de traza nula se obtiene en cambio $h_{s,Q}(A) = t(Q, A)^{-1/2} \in \mu_\ell$, que es el enunciado de [4] en este marco, con su forma cerrada. Es el fenómeno que Satoh describe como «(valor antes de la exponenciación final) = (función simple) $\times$ (otro emparejamiento)». Dos observaciones sobre la constante. Primera, es un signo conocido, no una cantidad que precalcular. Segunda, las implementaciones que no normalizan la función de Miller en $\mathcal{O}$ (el `lltatepairing` de PARI/GP es una) la sustituyen por otra constante; que sea de nuevo independiente de A y Q es una observación empírica sobre la normalización de las funciones de recta de PARI, hecha sobre la curva de juguete de la sección 9, y puede entonces leerse en un único par conocido.

Observación 3.2 (Longitud del bucle, no orientación). Para una longitud de bucle n arbitraria con $[n]P \neq \mathcal{O}$, el mismo cálculo de divisores da, exactamente y sin signo,

$$h_{n,P} h_{n,-P} = \frac{(\xi - \xi(P))^n}{\xi - \xi([n]P)}, \quad (6)$$

teniendo ambos miembros coeficiente director 1 en $\mathcal{O}$; (6) vale para P en cualquiera de los dos grupos. (El signo de (5) es $(-1)^{\text{ord}_{\mathcal{O}} h_{n,P}}$, esto es $(-1)^{n-1}$ cuando $[n]P \neq \mathcal{O}$ y $(-1)^n$ cuando $\ell \mid n$; sólo interviene si se evalúa $h_{n,P}$ en $-R$ en lugar de $h_{n,-P}$ en R .) Importan tres residuos de n módulo ℓ .

Si $n \equiv 0 \pmod{\ell}$, el denominador vale 1 y la relación de norma recupera $(\xi - \xi(P))^n$: es la proposición 3.1, y vale en *ambas* orientaciones. En la orientación Ate, $\text{Fr}_q^{k/2}$ actúa sobre los coeficientes de $h_{n,Q}$ y la envía a $h_{n,-Q}$, sin evaluación en un punto opuesto y por tanto sin signo, de modo que

$$h_{\ell,Q}(A)^{s+1} = (\xi(A) - \xi(Q))^\ell = -(\xi(Q) - \xi(A))^\ell = h_{\ell,A}(Q)^{s+1} \quad (Q \in G_0, A \in G_1) : \quad (7)$$

las dos normas coinciden.

Si $n \equiv -1 \pmod{\ell}$, entonces $[n]P = -P$ y (6) se convierte en $(\xi - \xi(P))^{n-1}$. Para $n = s$ el exponente $s - 1$ anula $\mathbb{F}_{q^{k/2}}^\times$, de modo que $h_{s,P}(R)^{s+1} = 1$ idénticamente y no sobrevive ninguna información sobre las abscisas; es el bucle que usa [7, Alg. 6.1] en el caso ordinario, y por eso ese algoritmo no puede alimentarse con el presente test. Para otros $n \equiv -1 \pmod{\ell}$, p. ej. $n = 2\ell - 1$, la norma no es trivial, pero determina ζ sólo salvo $\gcd(n-1, s-1)$ candidatos: 48 sobre la curva de juguete, y $48u \approx 2^{67,7}$ sobre BN254 (calculado para esa curva; en general $\gcd(2\ell - 2, s - 1)$ es un múltiplo de $\gcd(\ell - 1, q - 1) = 6u$, siendo coprimos los cofactores $6u^3 + 6u^2 + 3u + 1$ y $6u^3 + 6u^2 + 4u + 1$, y el factor 8 proviene de los demás factores de $s - 1$). La unicidad de la raíz es exactamente lo que compra $\ell \mid d \mid s + 1$ mediante $\gcd(d, s - 1) = \gcd(d, 2)$ (lema 3.5), y exactamente lo que pierde $n \equiv -1 \pmod{\ell}$.

Si $n \equiv q \pmod{\ell}$, como para el bucle Ate $T = t - 1$ con $P = Q \in G_0$, entonces $[n]Q = \text{Fr}_q Q$ y

$$h_{T,Q}(A)^{s+1} = \frac{(\xi(A) - \xi(Q))^T}{\xi(A) - \xi(Q)^q}, \quad (8)$$

de nuevo sin signo. Como $\xi(A) \in \mathbb{F}_q$, el denominador es $(\xi(A) - \xi(Q))^q$, de modo que (8) se reduce a $(\xi(A) - \xi(Q))^{T-q} = (\xi(A) - \xi(Q))^{-h\ell}$ con $h = \#E(\mathbb{F}_q)/\ell$: es la potencia $(-h)$ -ésima de (7) — sin signo, con una inversión — y lleva la misma información que la proposición 3.1 con $d = h\ell$, que sólo necesita $\ell \mid d$. (Coherentemente, $h_{q,Q} = h_{T,Q} h_{\ell,Q}^h$ como funciones normalizadas, y $h_{q,Q}(A)^{s+1} = 1$.) Todas las identidades de esta observación se comprobaron numéricamente (sección 9).

Lema 3.3. Para $P \in E[\ell]$, como funciones racionales,

$$h_{s,P}^\ell = \frac{h_{\ell,P}^s}{h_{\ell,-P}}. \quad (9)$$

Además, para $A \in G_1$ y $Q \in G_0$ no nulos, denotando $t(\cdot, \cdot)$ el emparejamiento de Tate reducido en cualquiera de los dos órdenes de argumentos,

$$t(A, Q) = h_{s,A}(Q)^{-2}, \quad t(Q, A) = h_{s,Q}(A)^{-2}, \quad (10)$$

de modo que $h_{s,A}(Q) = -t(A, Q)^{-1/2}$ y $h_{s,Q}(A) = t(Q, A)^{-1/2}$, siendo las raíces cuadradas las únicas en μ_ℓ . En particular $h_{s,Q}(A) \in \mu_\ell$ tiene orden exactamente ℓ , y $h_{s,A}(Q)$ tiene orden exactamente 2ℓ , con $2\ell \mid s + 1$.

Prueba. La regla de composición $h_{mn,P} = h_{m,P}^n h_{n,[m]P}$ (mismos divisores, ambos miembros normalizados) da, calculando $h_{\ell s,P}$ de dos maneras, $h_{\ell s,P}^\ell h_{\ell,[s]P} = h_{\ell,P}^s h_{s,[\ell]P}$; como $[s]P = -P$ y $h_{s,\mathcal{O}} = 1$, esto es (9). Evaluando: en la orientación Ate, $h_{\ell,Q}(A)^s = \text{Fr}_q^{k/2}(h_{\ell,Q}(A)) = h_{\ell,-Q}(A)$ por

conjugación de los coeficientes, luego $h_{s,Q}(A)^\ell = 1$; en la orientación Tate, $h_{\ell,A}(Q)^s = h_{\ell,A}(-Q) = -h_{\ell,-A}(Q)$ por (5) con ℓ impar, luego $h_{s,A}(Q)^\ell = -1$.

Para (10), la misma regla con $[\ell]A = [s+1]A = \mathcal{O}$ da $h_{\ell,A}^c = h_{\ell c,A}$ para todo c y $h_{(s+1)(s-1),A} = h_{s+1,A}^{s-1}$, mientras que los divisores dan $h_{s+1,A} = (\xi - \xi(A)) h_{s,A}$. Así, con $\zeta = \xi(Q) - \xi(A) \in \mathbb{F}_{q^{k/2}}^\times$,

$$\begin{aligned} t(A, Q) &= h_{\ell,A}(Q)^{(q^k-1)/\ell} = h_{q^k-1,A}(Q) = h_{s+1,A}(Q)^{s-1} \\ &= \zeta^{s-1} h_{s,A}(Q)^{s-1} = h_{s,A}(Q)^{s-1} = h_{s,A}(Q)^{-2}, \end{aligned}$$

el último paso porque $h_{s,A}(Q)^{2\ell} = 1$ y $2\ell \mid s+1$. El caso Ate es idéntico intercambiando A y Q . Como ℓ es impar, elevar al cuadrado es una biyección de μ_ℓ , lo que fija las raíces cuadradas; el signo de $h_{s,A}(Q)$ viene forzado por $h_{s,A}(Q)^\ell = -1$. Por último $t(A, Q) \neq 1$ por no degeneración, luego $h_{s,A}(Q)^2 \neq 1$ y el orden es exactamente 2ℓ , no 2; igualmente $h_{s,Q}(A) \neq 1$ y su orden es exactamente ℓ . $\square$

Cuatro consecuencias. Primera, el valor de Miller de longitud de bucle s es el emparejamiento de Tate reducido, al exponente $-1/2$ y sin exponenciación final: el «another pairing» de Satoh es literal. Es bilineal en ambos argumentos como valor bruto de Miller, lo que se comprobó directamente (sección 9). Segunda, el signo es una vez más el $(-1)^\ell$ de (5), el mecanismo de (7); (9) da en dos líneas el enunciado de [4] en orientación Ate. Tercera, la proposición 3.1 para $d = \ell$ es la misma identidad releída: $h_{\ell,A}(Q)^{s+1} = h_{s+1,A}(Q)^\ell = \zeta^\ell h_{s,A}(Q)^\ell = -\zeta^\ell$. Cuarta, la misma regla da el valor para la longitud de bucle q , observación 3.4.

Observación 3.4 (Longitud de bucle q). La misma regla de composición, aplicada a $h_{q^k,Q}$, da $h_{q^k,Q} = \prod_{i=0}^{k-1} h_{q,[q^i]Q}^{q^{k-1-i}}$, y como $[q^i]Q = \text{Fr}_q^i Q$ y A es racional, $h_{q,\text{Fr}_q^i Q}(A) = h_{q,Q}(A)^{q^i}$, luego $h_{q^k,Q}(A) = h_{q,Q}(A)^{kq^{k-1}}$. Por otro lado $\text{div } h_{q^k,Q} = (q^k - 1)([Q] - [\mathcal{O}]) = \text{div } h_{\ell,Q}^{(q^k-1)/\ell}$, luego $h_{q^k,Q}(A) = t(Q, A)$. Esto solo da $h_{q,Q}(A) \in \mu_{k\ell}$; que esté en μ_ℓ se sigue de la misma regla aplicada a $h_{q\ell,Q}$, $h_{q,Q}^\ell h_{\ell,[q]Q} = h_{\ell,Q}^q$, ya que $h_{\ell,Q}(A)^q = h_{\ell,\text{Fr}_q Q}(A)$ y $[q]Q = \text{Fr}_q Q$, de donde $h_{q,Q}(A)^\ell = 1$. Así, siendo la raíz única en μ_ℓ ,

$$h_{q,Q}(A) = t(Q, A)^{1/(kq^{k-1})} = t(Q, A)^{-1/(kq^{k/2-1})} \in \mu_\ell,$$

la última forma porque $q^{k-1} = sq^{k/2-1} \equiv -q^{k/2-1} \pmod{\ell}$ (y $\ell \nmid k$, sección 2). El objetivo de [7, Alg. 6.6], la envoltura de bucle q de su algoritmo 6.1, es $h_{q,-Q}(A) = t(Q, A)^{1/(kq^{k/2-1})}$ en la notación de esta nota ($h_{q,Q}(A)$ es bilineal en Q , por ser una potencia fija de t); un test final $t(Q, A) = z^{-kq^{k-1}}$ en la línea 15 de la sección 8 resuelve pues también ese problema directamente. (Comprobado numéricamente, sección 9.)

Lema 3.5. Sea $d \mid s+1$. Entonces $\gcd(d, s-1) = \gcd(d, 2)$, y para $u \in \mathbb{F}_{q^{k/2}}^\times$ la ecuación $\zeta^d = u$ o bien no tiene solución o bien tiene exactamente $\gcd(d, 2)$ soluciones en $\mathbb{F}_{q^{k/2}}^\times$. Cuando es resoluble:

1. si d es impar, la solución es única y vale $u^{d^{-1} \bmod (s-1)}$;
2. si d es par, las soluciones son $\pm \zeta_0$ para cualquier solución ζ_0 , que se obtiene escribiendo $d = 2^a d'$ con d' impar, poniendo $u_1 := u^{d'^{-1} \bmod (s-1)}$ y extrayendo a raíces cuadradas sucesivas de u_1 en $\mathbb{F}_{q^{k/2}}$ mediante cualquier algoritmo estándar.

Prueba. Estándar: s es impar, luego $\gcd(s+1, s-1) = 2$ y $\gcd(d, s-1) \mid 2$, y el resto es el recuento de soluciones de $\zeta^d = u$ en un grupo cíclico, como en la demostración de [6, Thm. 4.2]. Sólo el caso (i) se usa más abajo, pues d es impar en todo momento. $\square$

Para $d = \ell$ impar se aplica el caso (i). El caso (ii) es la ambigüedad de signo visible en [6, Alg. 4.1, pasos 3–4], donde se producen dos abscisas $\xi(A) \pm u$; duplica el coste y nada más.

4 El lema de separación

Supongamos que E admite una torsión E' de grado $e \mid k$, y pongamos $m := k/e$. Como k es par, $e \geq 3$ significa $e \in \{4, 6\}$: una torsión $e = 3$ fuerza $j(E) = 0$ y $6 \mid k$, luego una torsión séxtica, de modo que $e = 3$ nunca es el grado de torsión maximal y tomo e par en todo lo que sigue. La torsión está definida sobre $\mathbb{F}_{q^m}$ por un parámetro $\theta \in \mathbb{F}_{q^m}^\times$ cuya clase genera $\mathbb{F}_{q^m}^\times / (\mathbb{F}_{q^m}^\times)^e$, elegida entre las $\varphi(e)$ clases posibles como aquella para la que $\ell \mid \#E'(\mathbb{F}_{q^m})$ (la torsión de tipo D o de tipo M, en la terminología usual), y el isomorfismo de torsión $\psi: E' \rightarrow E$ envía (x', y') a $(\omega x', \omega^{3/2} y')$ con $\omega := \theta^{2/e}$. Como $G_0 = \psi(E'(\mathbb{F}_{q^m})[\ell])$,

$$\xi(P) \in W := \omega \mathbb{F}_{q^m} \quad \text{para todo } P \in G_0 \setminus \{\mathcal{O}\}, \quad (11)$$

un $\mathbb{F}_q$ -subespacio de dimensión $m = k/e$, contenido en $\mathbb{F}_{q^{k/2}}$ puesto que e es par. (Coherentemente, $\xi(P) \in \mathbb{F}_{q^{k/2}}$ porque ξ es par y $\text{Fr}_q^{k/2}$ actúa como $[-1]$ sobre G_0 , [7, Lem. 5.2].) Del otro lado, $\xi(A) \in \mathbb{F}_q$ para $A \in G_1$.

Lema 4.1 (Separación). *Supongamos $e \in \{4, 6\}$ y pongamos $\lambda := \omega^{q^m-1}$. Entonces $\omega \notin \mathbb{F}_{q^m}$, luego $\lambda \neq 1$ y $\mathbb{F}_q \cap W = \{0\}$; además $\lambda \in \mathbb{F}_{q^{k/2}}$, ya que $\lambda = \xi(Q_0)^{q^m} / \xi(Q_0)$ para cualquier $Q_0 \in G_0 \setminus \{\mathcal{O}\}$ y $\xi(Q_0) \in \mathbb{F}_{q^{k/2}}$, de modo que la aplicación $\mathbb{F}_q$ -lineal*

$$L: \mathbb{F}_{q^{k/2}} \longrightarrow \mathbb{F}_{q^{k/2}}, \quad L(u) := u^{q^m} - \lambda u$$

está bien definida, verifica $\ker L = W$ y $L|_{\mathbb{F}_q} = (1 - \lambda) \text{id}$; y para $\zeta := \xi(Q) - \xi(A)$ con $\xi(Q) \in W$, $\xi(A) \in \mathbb{F}_q$,

$$\xi(A) = \frac{L(\zeta)}{\lambda - 1}, \quad \xi(Q) = \zeta + \xi(A). \quad (12)$$

Prueba. Si $\omega \in \mathbb{F}_{q^m}$ entonces $\theta^2 = \omega^e \in (\mathbb{F}_{q^m}^\times)^e$, luego la clase de θ tiene orden divisor de 2 en un grupo cíclico de orden e en el que tiene orden e ; así $e \mid 2$, contra $e \geq 4$. Por tanto $\omega \notin \mathbb{F}_{q^m}$, es decir $\lambda \neq 1$. Si $a \in \mathbb{F}_q \cap W$ con $a \neq 0$ entonces $a = \omega x'$ con $x' \in \mathbb{F}_{q^m}^\times$ y $\omega = a/x' \in \mathbb{F}_{q^m}$, contradicción; luego $\mathbb{F}_q \cap W = \{0\}$. L es $\mathbb{F}_q$ -lineal porque $u \mapsto u^{q^m}$ lo es; para $u = \omega x' \in W$, $u^{q^m} = \omega^{q^m} x' = \lambda u$, luego $L(u) = 0$, es decir $W \subseteq \ker L$. Recíprocamente, $\omega^{e/2} = \theta$, y $X^{e/2} - \theta$ es irreducible sobre $\mathbb{F}_{q^m}$: su grado $e/2 \in \{2, 3\}$ es primo y θ no es una potencia $(e/2)$ -ésima, pues si no θ^2 sería una potencia e -ésima y la clase de θ tendría orden divisor de 2. Así $1, \omega, \dots, \omega^{e/2-1}$ es una $\mathbb{F}_{q^m}$ -base de $\mathbb{F}_{q^{k/2}}$ (nótese $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = e/2$), formada por vectores propios de $u \mapsto u^{q^m}$ con valores propios λ^j , $0 \leq j < e/2$, distintos dos a dos porque $\lambda \neq 1$ y $\lambda^{e/2} = \theta^{q^m-1} = 1$ con $e/2$ primo. Luego $u \mapsto u^{q^m}$ es diagonalizable y $\ker L$ es su espacio propio de λ , que es $\omega \mathbb{F}_{q^m} = W$. Para $a \in \mathbb{F}_q$, $a^{q^m} = a$, luego $L(a) = (1 - \lambda)a$. Aplicando L a ζ se obtiene $L(\zeta) = -(1 - \lambda)\xi(A)$, que es (12). $\square$

Observación 4.2. Para $e = 2$ se tiene $m = k/2$ y $W = \omega \mathbb{F}_{q^{k/2}} = \mathbb{F}_{q^{k/2}}$: la proyección degenera ($\lambda = 1$, $L = 0$), pero nada falla — $\xi(A) \in \mathbb{F}_q$ sigue teniendo sólo q valores posibles, de modo que el paso 3 del algoritmo 5.1 se convierte en un bucle sobre $x_A \in \mathbb{F}_q$ con $x_Q = \zeta + x_A$, al coste $O(q)$ en lugar de $O(1)$, y el algoritmo de la sección 8 recorre $\mathbb{F}_q \times \mathbb{F}_{q^{k/2}}$ al coste $q^{k/e}/2 = q^{k/2}/2$ de su fórmula general. La decodificación en $O(1)$ necesita por tanto torsiones cuárticas o séxticas — BN y BLS12 ($e = 6$), KSS16 ($e = 4$), las curvas de Brezing–Weng de [1] — y no las curvas que sólo tienen una torsión cuadrática.

Observación 4.3. Para $k = 2$, en particular para las curvas supersingulares de [7, §4] donde $t = 0$ fuerza $k \leq 2$, se tiene $s = q$ y ambas abscisas están en $\mathbb{F}_q$: ninguna aplicación $\mathbb{F}_q$ -lineal las separa. Ésta es, a mi juicio, la razón estructural por la que [6] (FAPI, un argumento conocido, tiempo polinómico) y [7] (GPI, ambos desconocidos, exponencial) tienen dominios de utilidad disjuntos.

Para una curva BN, $e = 6$, $m = 2$, $L(u) = u^{q^2} - \lambda u$ y $\lambda^3 = \theta^{q^2-1} = 1$: λ es una raíz cúbica primitiva de la unidad. En general $\lambda^{e/2} = 1$. Es una constante de la curva, obtenida a partir de cualquier generador conocido de G_0 .

Observación 4.4 (Test de Legendre para G_0). Para $x_Q \in \mathbb{F}_{q^{k/2}}$ con $\beta := x_Q^3 + a_4 x_Q + a_6 \neq 0$, sea $Q = (x_Q, y_Q)$ con $y_Q \in \mathbb{F}_{q^k}$, $y_Q^2 = \beta$. Entonces $\text{Fr}_q^{k/2} Q = -Q$ si y sólo si β es un no cuadrado en $\mathbb{F}_{q^{k/2}}$: en efecto $\text{Fr}_q^{k/2} Q = (x_Q, y_Q^s)$, y $y_Q^s = -y_Q$ si y sólo si $y_Q^{s-1} = \beta^{(s-1)/2} = -1$. La pertenencia de Q a $\ker(\text{Fr}_q^{k/2} + 1)$ se decide pues mediante un símbolo de Legendre en $\mathbb{F}_{q^{k/2}}$ *antes* de extraer ninguna raíz cuadrada, y aproximadamente la mitad de los $x_Q \in \mathbb{F}_{q^{k/2}}$ con $\beta \neq 0$ lo superan: el número de $x \in \mathbb{F}_{q^{k/2}}$ con $\beta(x)$ no cuadrado es $(s + t_s - N_0)/2$, donde t_s es la traza de Frobenius de E sobre $\mathbb{F}_{q^{k/2}}$ y $N_0 = \#\{\beta = 0\}$. Sobre el subespacio $W = \omega \mathbb{F}_{q^m}$ los dos grados de torsión se comportan de modo distinto. Para $e = 6$ ($a_4 = 0$), $\beta = \theta u^3 + a_6 \in \mathbb{F}_{q^m}$ para $x_Q = \omega u$, y como $[\mathbb{F}_{q^{k/2}} : \mathbb{F}_{q^m}] = 3$ es impar, β es no cuadrado en $\mathbb{F}_{q^{k/2}}$ si y sólo si lo es en $\mathbb{F}_{q^m}$: aproximadamente la mitad de los $x_Q \in W$ sobreviven, y el símbolo puede calcularse directamente en $\mathbb{F}_{q^m}$. Para $e = 4$ ($a_6 = 0$), $\beta = \omega u(\theta u^2 + a_4) \in \mathbb{F}_{q^m}$, cuadrado en la extensión cuadrática $\mathbb{F}_{q^{k/2}}$, mientras que ω es no cuadrado en $\mathbb{F}_{q^{k/2}}$ ($\omega^{(s-1)/2} = \theta^{(q^m-1)/2 \cdot (q^m+1)/2} = -1$, pues θ es no cuadrado en $\mathbb{F}_{q^m}$ y $(q^m + 1)/2$ es impar): *todo* $x_Q \in W$ con $\beta \neq 0$ sobrevive, el test es vacío, y $[\ell]Q = \mathcal{O}$ hace todo el filtrado. El símbolo no debe calcularse como una exponenciación de exponente de $\log_2 s$ bits, que costaría aproximadamente la mitad de lo que ahorra; como $\beta^{(s-1)/2} = N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2}$, cuesta $k/2 - 1$ Frobenius y $k/2 - 1$ multiplicaciones en $\mathbb{F}_{q^{k/2}}$ seguidos de un símbolo de Jacobi en $\mathbb{F}_q$, cuyo coste está muy por debajo de una multiplicación en $\mathbb{F}_{q^k}$. (Comprobado en la sección 9.)

5 Inversión de Miller con dos incógnitas

Esta sección contiene el resultado propiamente dicho: un procedimiento en tiempo polinómico que toma un valor bruto de Tate–Miller y devuelve sus dos argumentos. Es [6, Alg. 4.1], que invierte $h_{d,A}$ en un A conocido, con dos cambios: la orientación es Tate y no Ate, de modo que la norma da ζ^d y no ζ^2 (proposición 3.1 frente a [6, ec. (4.3)]) y la raíz d -ésima es única (lema 3.5); y su paso 3, $\xi(Q) = \xi(A) \pm u$, se sustituye por la proyección del lema 4.1. Los pasos 1–2 y 5–8 de abajo son suyos.

Algoritmo 5.1 Inversión de Miller, dos incógnitas

Entrada: $w \in \mathbb{F}_{q^k}^\times$; aquí $d \mid s + 1$; las constantes $\lambda, (\lambda - 1)^{-1}$ y la base del lema 4.1, precalculadas una vez por curva

Salida: $(A, Q) \in G_1 \times G_0$ con $h_{d,A}(Q) = w$, o $\perp$

- 1: $u \leftarrow (-1)^d w^{s+1}$
 - 2: $\zeta \leftarrow$ una raíz d -ésima de u en $\mathbb{F}_{q^{k/2}}^\times$ $\triangleright$ lema 3.5; $\perp$ si no hay ninguna, ambos signos si hay dos
 - 3: $x_A \leftarrow L(\zeta)/(\lambda - 1)$
si $x_A^q \neq x_A$ **entonces devolver** $\perp$
 - 4: $x_Q \leftarrow \zeta + x_A$ $\triangleright$ entonces $L(x_Q) = L(\zeta) + (1 - \lambda)x_A = 0$ automáticamente
 - 5: $\alpha \leftarrow x_A^3 + a_4 x_A + a_6$
si α no es un cuadrado en $\mathbb{F}_q$ **entonces devolver** $\perp$
 $A \leftarrow (x_A, \sqrt{\alpha})$
 - 6: $\beta \leftarrow x_Q^3 + a_4 x_Q + a_6$
si $N_{\mathbb{F}_{q^{k/2}}/\mathbb{F}_q}(\beta)^{(q-1)/2} \neq -1$ **entonces devolver** $\perp$ $\triangleright$ i.e. $\text{Fr}_q^{k/2} Q \neq -Q$, observación 4.4
 $Q \leftarrow (x_Q, y_Q)$ con $y_Q \in \mathbb{F}_{q^k}$, $y_Q^2 = \beta$
 - 7: **si** $[\ell]A \neq \mathcal{O}$ o $[\ell]Q \neq \mathcal{O}$ **entonces devolver** $\perp$
 - 8: $h \leftarrow h_{d,A}(Q)$
si $w = h$ **entonces devolver** (A, Q)
si $w = -h$ **entonces devolver** $(-A, -Q)$
si $w = h^s$ **entonces devolver** $(A, -Q)$
si $w = -h^s$ **entonces devolver** $(-A, Q)$
 - 9: **devolver** $\perp$
-

Proposición 5.1. *El algoritmo 5.1 es correcto y termina en $O((k \log q)^3)$ operaciones binarias.*

Prueba. Si $w = h_{d,A_0}(Q_0)$ para algún $(A_0, Q_0) \in G_1 \times G_0$, entonces por la proposición 3.1 $u = (\xi(Q_0) - \xi(A_0))^d$, luego $\zeta = \xi(Q_0) - \xi(A_0)$ (salvo el signo del caso (ii), que se prueba), y el lema 4.1 da $x_A = \xi(A_0)$, $x_Q = \xi(Q_0)$; los pasos 5–7 producen entonces $A = \pm A_0$, $Q = \pm Q_0$ con signos desconocidos. Por (5) y la demostración de la proposición 3.1, los cuatro valores brutos son $h_{d,A_0}(Q_0) = w$, $h_{d,-A_0}(-Q_0) = -w$, $h_{d,A_0}(-Q_0) = w^s$ y $h_{d,-A_0}(Q_0) = -w^s$ (para d impar), de modo que el paso 8 identifica los signos y devuelve un par cuyo valor de Miller es exactamente w . Recíprocamente, si el algoritmo devuelve un par entonces $A \in E(\mathbb{F}_q)[\ell] = G_1$ por los pasos 5 y 7, $Q \in E[\ell] \cap \ker(\text{Fr}_q^{k/2} + 1) = G_0$ por los pasos 6–7, la observación 4.4 y (1), y su valor de Miller es w por el paso 8. Sin el paso 8 el algoritmo podría devolver un par válido para un w que no es en absoluto un valor de Miller. Para el coste, contemos multiplicaciones en $\mathbb{F}_{q^k}$, cada una de $O((k \log q)^2)$ operaciones binarias con aritmética escolar, como en [6, Thm. 4.2]; una multiplicación en $\mathbb{F}_{q^{k/2}}$ o en $\mathbb{F}_q$ no cuesta más, y el exponente $d^{-1} \bmod (s-1)$, las constantes λ , $(\lambda-1)^{-1}$ y la base del lema 4.1 se calculan una vez por curva. Paso a paso:

1. $w^{s+1} = w^s \cdot w$: una potencia de Frobenius y una multiplicación, $O(k \log q)$ multiplicaciones, u $O(1)$ cuando $\mathbb{F}_{q^k}$ se presenta como extensión cuadrática de $\mathbb{F}_{q^{k/2}}$, en la que $w \mapsto w^s$ es la conjugación.
2. Una exponenciación en $\mathbb{F}_{q^{k/2}}$ con exponente menor que s : $O(k \log q)$ multiplicaciones.
3. ζ^{q^m} es una potencia de Frobenius ($O(k \log q)$ multiplicaciones, u $O(k^2)$ multiplicaciones en $\mathbb{F}_q$ con una matriz precalculada), seguida de una multiplicación; el test $x_A \in \mathbb{F}_q$ es gratuito en una $\mathbb{F}_q$ -base de $\mathbb{F}_{q^{k/2}}$ que contenga a 1.
4. Una suma.
5. Un símbolo de Legendre y una raíz cuadrada en $\mathbb{F}_q$: $O(\log q)$ multiplicaciones en $\mathbb{F}_q$.
6. El símbolo de Legendre en $\mathbb{F}_{q^{k/2}}$ a través de la norma, $k/2 - 1$ potencias de Frobenius y $k/2 - 1$ multiplicaciones en $\mathbb{F}_{q^{k/2}}$ y un símbolo de Jacobi en $\mathbb{F}_q$ (observación 4.4); una raíz cuadrada en $\mathbb{F}_{q^k}$, $O(k \log q)$ multiplicaciones — de hecho una raíz cuadrada en $\mathbb{F}_{q^{k/2}}$: una vez $\mathbb{F}_{q^k} = \mathbb{F}_{q^{k/2}}(\sqrt{\nu})$ con ν un no cuadrado de $\mathbb{F}_{q^{k/2}}$, el elemento β/ν es un cuadrado de $\mathbb{F}_{q^{k/2}}$ y $\sqrt{\beta} = \sqrt{\nu} \sqrt{\beta/\nu}$.
7. $[\ell]A$ en $E(\mathbb{F}_q)$ y $[\ell]Q$ en $E(\mathbb{F}_{q^k})$: $O(\log \ell) = O(\log q)$ operaciones de grupo cada uno, cada una un número acotado de multiplicaciones.
8. Un bucle de Miller de longitud $d \leq s+1$: $O(\log d) = O(k \log q)$ pasos de duplicación o suma de un número acotado de multiplicaciones cada uno, y cuatro comparaciones que cuestan una potencia de Frobenius.

Cada paso cuesta $O(k \log q)$ multiplicaciones en $\mathbb{F}_{q^k}$, es decir $O((k \log q)^3)$ operaciones binarias, y los pasos 1, 2, 6 y 8 alcanzan esa cota. Las raíces cuadradas son deterministas bajo el precálculo supuesto en [6], un generador del 2-Sylow, y de tiempo esperado con el algoritmo de Cipolla en caso contrario. $\square$

Dos rasgos merecen comentario. Primero, ningún test sobre u solo es discriminante: w^{s+1} es una norma, luego está en $\mathbb{F}_{q^{k/2}}$ para *todo* w , y todo elemento de $\mathbb{F}_{q^{k/2}}$ es un cuadrado en $\mathbb{F}_{q^k}$; por eso el paso 6 comprueba β en $\mathbb{F}_{q^{k/2}}$ y no en $\mathbb{F}_{q^k}$ — la condición útil es que β sea un *no* cuadrado en $\mathbb{F}_{q^{k/2}}$, observación 4.4 —, por eso el paso 4 es una mera asignación (una vez $x_A \in \mathbb{F}_q$, $L(x_Q) = L(\zeta) + (1 - \lambda)x_A = 0$ automáticamente), y por eso los tests de los pasos 3, 6 y 7 cargan con todo el peso. Sobre la curva de juguete de la sección 9, 3000 raíces ℓ -ésimas aleatorias de un objetivo fijo pasaron todas las condiciones de norma y de cuadrado y fueron todas rechazadas en el paso 3. Segundo, el procedimiento devuelve ambos argumentos; no es un oráculo de pertenencia seguido de una búsqueda. Es el punto en que la presente nota va más allá de [1]: su ecuación (8) es exactamente (3) con los papeles de A y Q intercambiados, y su reducción posterior usa el polinomio mínimo del $\xi(Q)$ conocido, que aquí no está disponible.

6 De la inversión de Miller a GPI

Sea e un emparejamiento bilineal no degenerado cualquiera sobre $G_1 \times G_0$ o sobre $G_0 \times G_1$ con valores en μ_ℓ — el emparejamiento de Tate reducido t en cualquiera de los dos órdenes de argumentos, o el emparejamiento de Satoh — y sea $z \in \mu_\ell \setminus \{1\}$ un objetivo GPI para e .

El valor bruto de Tate–Miller v con $v^{(q^k-1)/\ell} = t(A, Q)$ queda determinado por el valor reducido sólo salvo un elemento del núcleo de $x \mapsto x^{(q^k-1)/\ell}$, subgrupo de orden $(q^k - 1)/\ell = (s - 1)\nu$ donde $\nu := (s + 1)/\ell$. Esto es demasiado grande para enumerarlo, y no es lo que necesita el algoritmo 5.1: lo que necesita es ζ , y la proposición 6.2 más abajo muestra que cuando v recorre esa clase, ζ recorre todo $\mathbb{F}_{q^{k/2}}^\times$ — es decir, el objetivo no restringe ζ en absoluto. El algoritmo GPI recorre por tanto directamente los pares de abscisas $(x_A, x_Q) \in \mathbb{F}_q \times W$ (sección 8) o, de forma equivalente pero más lenta, $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ decodificado mediante los pasos 3–4 del algoritmo 5.1 (observación 8.1); en ambos casos cada par se contrasta con z , y la raíz d -ésima del paso 2 nunca es necesaria.

El punto esencial para lo que sigue es que ninguno de los dos bucles evalúa un emparejamiento antes de su test final: e sólo interviene en el test final, y sólo a través de la pregunta de si $e(A, Q) \in \{z, z^{-1}\}$. En consecuencia:

- el algoritmo resuelve GPI para el emparejamiento e , cualquiera que sea, evaluado en el test final, y la proposición 7.1 se aplica tal cual a todo e de ese tipo, ya que su argumento de recuento sólo usa la bilinealidad y la no degeneración;
- en particular, tomando $e(A, Q) := h_{s,-Q}(A)$ — que es $h_{q^{k/2},-A}(Q)$ en las letras de Satoh, la condición de salida de [7, Alg. 6.1] — el algoritmo resuelve *directamente* el problema GPI de Satoh. Por el lema 3.3 este e vale $t(Q, A)^{1/2}$, bilineal y no degenerado, de modo que el test final puede ser equivalentemente $t(Q, A) \in \{z^2, z^{-2}\}$, más barato que un bucle de Miller de longitud s ; igualmente el objetivo de bucle q , $h_{q,-Q}(A)$, de [7, Alg. 6.6] es $t(Q, A)^{1/(kq^{k/2-1})}$ por la observación 3.4, comprobado como $t(Q, A) \in \{z^{\pm kq^{k-1}}\}$;
- nunca se calcula una relación entre dos emparejamientos distintos, y ninguna requeriría un logaritmo discreto si se calculase. La constante κ' con $t(Q, A) = t(A, Q)^{\kappa'}$, por ejemplo, tiene la forma cerrada

$$\kappa' = \frac{kh}{kh - c(q - 1)} \bmod \ell, \quad c := \frac{q^k - 1}{\ell}, \quad h := \frac{\#E(\mathbb{F}_q)}{\ell}, \quad (13)$$

que se sigue de la expresión de Frey–Rück del emparejamiento de Tate mediante el de Weil (lema 6.1); vale 15 sobre la curva de juguete de la sección 9. El método no la usa, y ningún logaritmo discreto aparece en ninguna parte de la nota.

Lema 6.1. *Sea e_ℓ el emparejamiento de Weil, dado por la fórmula de Miller $e_\ell(A, Q) = (-1)^\ell h_{\ell,A}(Q)/h_{\ell,Q}(A)$, y sean c, h como en (13), con $\rho := kh/(q - 1) \bmod \ell$. Entonces para $A \in G_1, Q \in G_0$,*

$$t(A, Q) = e_\ell(A, Q)^{c-\rho}, \quad t(Q, A) = e_\ell(A, Q)^{-\rho},$$

de donde (13). La no degeneración de $t(Q, A)$ es $\rho \neq 0$, es decir $\ell \nmid kh$: aquí $\ell \nmid k$ porque $k = \text{ord}_\ell(q)$ divide a $\ell - 1$, y $\ell \nmid h$ porque $\ell \parallel \#E(\mathbb{F}_q)$. La no degeneración de $t(A, Q)$ es $\rho \neq c$, que es exactamente la no anulación del denominador $kh - c(q - 1) = (q - 1)(\rho - c)$ de (13).

Prueba. La identidad $t(P, R) = e_\ell(P, \sigma S - S)$, donde $[\ell]S = R$ y $\sigma = \text{Fr}_q^k$, es la forma de Lichtenbaum del emparejamiento de Tate [2]; es clásica, y aquí sólo se calculan los exponentes. Como $\pi^k - 1$ anula $E[\ell]$, se factoriza como $\ell\phi$ en $\text{End}(E)$, luego $\sigma S - S = \phi(R)$, y ϕ actúa sobre las dos rectas propias de π en el módulo de Tate $T_\ell E$ como $(\alpha^k - 1)/\ell$ y $(\beta^k - 1)/\ell$, donde $\alpha \equiv 1, \beta \equiv q \pmod{\ell}$ son los valores propios. Escribamos $\alpha = 1 + \ell a, \beta = q + \ell b$; entonces $\alpha + \beta = t = q + 1 - \ell h$ da $a + b = -h$, y $\alpha\beta = q$ da $b \equiv -qa$, luego $a \equiv h/(q - 1)$ y $(\alpha^k - 1)/\ell \equiv ka, (\beta^k - 1)/\ell \equiv c + kq^{k-1}b \equiv c - ka \pmod{\ell}$.

Así $\phi(Q) = [c - \rho]Q$ para $Q \in G_0$ y $\phi(A) = [\rho]A$ para $A \in G_1$, lo que da $t(A, Q) = e_\ell(A, Q)^{c-\rho}$ y $t(Q, A) = e_\ell(Q, A)^\rho = e_\ell(A, Q)^{-\rho}$ por antisimetría. $\square$

Proposición 6.2 (Independencia del valor del emparejamiento y de la norma). *Como $\gcd(\ell, s - 1) = 1$, la aplicación*

$$\mathbb{F}_{q^k}^\times \longrightarrow \mu_\ell \times \mathbb{F}_{q^{k/2}}^\times, \quad v \longmapsto (v^{(q^k-1)/\ell}, v^{s+1})$$

es un homomorfismo suprayectivo con núcleo de orden $\nu = (s + 1)/\ell$. El valor reducido del emparejamiento y la norma de un valor bruto de Miller son por tanto coordenadas independientes: fijar la primera deja la segunda uniformemente distribuida sobre $\mathbb{F}_{q^{k/2}}^\times$, y ningún procedimiento que lea v sólo a través de v^{s+1} — en particular ninguno construido sobre la proposición 3.1 — recibe información alguna sobre el objetivo.

Prueba. $\mathbb{F}_{q^k}^\times$ es cíclico de orden $(s - 1)(s + 1)$. El núcleo consta de los v de orden divisor de $\gcd((s - 1)(s + 1)/\ell, s + 1) = \nu \gcd(s - 1, \ell) = \nu$, luego la imagen tiene orden $(q^k - 1)/\nu = \ell(s - 1) = |\mu_\ell \times \mathbb{F}_{q^{k/2}}^\times|$. $\square$

Éste es el contenido de la proposición 7.1 de abajo, enunciado de una vez por todas: la vía de la norma descarta el objetivo por completo, y lo que queda es una búsqueda sobre pares de abscisas con un test final de emparejamiento. (Comprobado sobre la curva de juguete de la sección 9: la imagen tiene el orden predicho $\ell(s - 1)$.)

7 Densidad del conjunto de soluciones

Proposición 7.1. *Supongamos $e \in \{4, 6\}$, $k > 2$, d impar con $d \mid s + 1$, y fijemos $z \in \mu_\ell \setminus \{1\}$. Cuando v recorre $\{v : v^{(q^k-1)/\ell} = z\}$, la cantidad $\zeta = ((-1)^d v^{s+1})^{1/d}$ recorre todo $\mathbb{F}_{q^{k/2}}^\times$, alcanzando cada valor el mismo número de veces (proposición 6.2 y lema 3.5). Sea e un emparejamiento bilineal no degenerado sobre $G_1 \times G_0$ o $G_0 \times G_1$ con valores en μ_ℓ . Entre los $s - 1$ valores de ζ , exactamente $(\ell - 1)/2$ son decodificados por los pasos 3–7 del algoritmo 5.1 en un par (A, Q) con $e(A, Q) = z^{\pm 1}$. Luego el número esperado de candidatos que examinar es*

$$\frac{1}{\pi_z} = \frac{2(s - 1)}{\ell - 1} \approx \frac{2q^{k/2}}{\ell} = 2\nu. \quad (14)$$

Prueba. La primera afirmación es la proposición 6.2 (la norma es uniforme sobre $\mathbb{F}_{q^{k/2}}^\times$ sobre la fibra de z) junto con la biyectividad de $\zeta \mapsto \zeta^d$ sobre $\mathbb{F}_{q^{k/2}}^\times$ (lema 3.5, d impar). Para la segunda, por el lema 4.1 la aplicación $(\xi(A), \xi(Q)) \mapsto \xi(Q) - \xi(A)$ es inyectiva sobre $\mathbb{F}_q \times W$. Los pares $(A, Q) \in (G_1 \setminus \{\mathcal{O}\}) \times (G_0 \setminus \{\mathcal{O}\})$ con $e(A, Q) \in \{z, z^{-1}\}$ son $2(\ell - 1)$ por bilinealidad y no degeneración (para cada A , un Q para cada uno de los dos valores); se permutan en órbitas de tamaño 4 por $(A, Q) \mapsto (\pm A, \pm Q)$, que conserva ambas abscisas y dentro de las cuales e toma cada uno de los dos valores dos veces, y dan por tanto $(\ell - 1)/2$ valores distintos de ζ . $\square$

Los ζ exitosos están todos en el subespacio $\mathbb{F}_q \oplus W$, de dimensión $1 + k/e$, de modo que el algoritmo de la sección 8 recorre ese subespacio ($q^{1+k/e}$ elementos, 2^{761} para BN254) en lugar de $\mathbb{F}_{q^{k/2}}^\times$. El recuento (14) es para este último; para el primero, en el orden natural por bloques (x_A fuera, x_Q dentro), el trabajo es de $q^{k/e}/2$ candidatos en el primer bloque válido, la mitad de ellos caros para $e = 6$ y todos para $e = 4$ (observación 4.4), sea cual sea ℓ (secciones 8 y 9).

8 El algoritmo completo

Por el lema 4.1, los valores ζ decodificados por los pasos 3–4 del algoritmo 5.1 son exactamente $\zeta = x_Q - x_A$ con $(x_A, x_Q) \in \mathbb{F}_q \times W$, y por la proposición 6.2 el objetivo no restringe ζ . El algoritmo GPI recorre por tanto directamente los pares (x_A, x_Q) ; la norma y la proyección L no se evalúan en absoluto. El análisis de las secciones 4–7 interviene sólo por lo que demuestra: que éste es el espacio de búsqueda, y que nada en la vía de la norma puede reducirlo (la sección 10 enumera las reducciones y lo que justifica cada una).

Algoritmo 8.1 GPI, bucle de longitud ℓ

Entrada: q ; $E : Y^2 = X^3 + a_4X + a_6$ ordinaria sobre $\mathbb{F}_q$; un primo impar $\ell \parallel \#E(\mathbb{F}_q)$ de grado de inmersión par $k > 2$; un grado de torsión par $e \geq 4$ con $e \mid k$; un emparejamiento bilineal no degenerado e sobre $G_1 \times G_0$, p. ej. $t(A, Q)$, $t(Q, A)$, o el de Satoh $h_{s,-Q}(A) = t(Q, A)^{1/2}$; un objetivo $z \in \mu_\ell \setminus \{1\}$.

Salida: $(A, Q) \in G_1 \times G_0$ con $e(A, Q) = z$, o $\perp$.

1: **Precálculo** (independiente de z):

2: $s \leftarrow q^{k/2}$; $m \leftarrow k/e$

3: elegir $Q_0 \in G_0 \setminus \{\mathcal{O}\}$; $W \leftarrow \xi(Q_0) \mathbb{F}_{q^m}$, con $\mathbb{F}_q$ -base $\xi(Q_0) \cdot \{1, \gamma, \dots, \gamma^{m-1}\}$ para γ generador de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$

4: **Bucle principal:**

5: **para** $x_A \in \mathbb{F}_q$ **hacer**

6: $\alpha \leftarrow x_A^3 + a_4x_A + a_6$

7: **si** α es un cuadrado en $\mathbb{F}_q$ **entonces**

8: $A \leftarrow (x_A, \sqrt{\alpha})$

9: **si** $[\ell]A = \mathcal{O}$ **entonces**

10: **para** $x_Q \in W$ **hacer**

11: $\beta \leftarrow x_Q^3 + a_4x_Q + a_6$

12: **si** $N_{\mathbb{F}_{q^{k/2}/\mathbb{F}_q}}(\beta)^{(q-1)/2} = -1$ **entonces** ▷ i.e. $\text{Fr}_q^{k/2}Q = -Q$, observación 4.4

13: $Q \leftarrow (x_Q, y_Q)$ con $y_Q \in \mathbb{F}_{q^k}$, $y_Q^2 = \beta$

14: **si** $[\ell]Q = \mathcal{O}$ **entonces**

15: $\chi \leftarrow e(A, Q)$

16: **si** $\chi = z$ **entonces**

17: **devolver** (A, Q)

18: **si** $\chi = z^{-1}$ **entonces**

19: **devolver** $(-A, Q)$

20: **devolver** $\perp$

El emparejamiento e sólo se evalúa en la línea 15, y el objetivo z sólo interviene en las líneas 15–19. La línea 18 usa $e(-A, Q) = e(A, Q)^{-1}$, de modo que un único par exitoso da la respuesta tras a lo sumo dos elecciones de signo; esto está contabilizado en el recuento $(\ell - 1)/2$ de la proposición 7.1. Toda abscisa de G_1 tiene exactamente una abscisa pareja en G_0 , de modo que el bucle se detiene dentro del bloque del primer x_A que pasa las líneas 7 y 9, tras recorrer aproximadamente la mitad de W ; para estas esperanzas los dos bucles se toman en orden uniformemente aleatorio, como en la sección 9 (el orden fijo escrito arriba encuentra siempre el mismo primer x_A). El trabajo esperado es de $(q - n)/(n + 1)$ x_A rechazados, $n = (\ell - 1)/2$, cada uno al coste de un símbolo de Legendre en $\mathbb{F}_q$ y, cuando $h > 1$, para la mitad que lo supera, de un $[\ell]A$ (para $h = 1$ ningún x_A rechazado supera el símbolo), seguidos de $q^{k/e}/2$ candidatos x_Q , la mitad de ellos caros para $e = 6$ y todos para $e = 4$ (observación 4.4).

Relación con el algoritmo 5.1. El algoritmo 5.1 no es llamado por el algoritmo 8.1, y ello es deliberado. Sus pasos 1–4 (norma, raíz d -ésima, proyección) decodifican un valor bruto candidato w en un par de abscisas, y la proposición 6.2 muestra que, cuando w recorre la fibra de z , producen cada par de $\mathbb{F}_q \times W$ con igual frecuencia: ejecutarlos sería recorrer $\mathbb{F}_q \times W$ dando un rodeo por $\mathbb{F}_{q^{k/2}}^\times$, cuyo coste da la observación 8.1. El algoritmo 8.1 recorre los pares directamente y conserva la segunda mitad del algoritmo 5.1 línea por línea: las líneas 6–8 y 11–13 son sus pasos 5 y 6 (raíces cuadradas y tests de Legendre), las líneas 9 y 14 su paso 7 (comprobaciones de orden), y las líneas 15–19 sustituyen su paso 8 — la comparación del valor bruto $h_{d,A}(Q)$ con w salvo los cuatro signos — por la comparación del valor reducido $e(A, Q)$ con $z^{\pm 1}$. Lo que el algoritmo 5.1 aporta no es, pues, una subrutina sino un teorema: que $\mathbb{F}_q \times W$ es el espacio de búsqueda, y que ninguna decodificación basada en la norma puede reducirlo.

Observación 8.1 (El bucle sobre $\mathbb{F}_{q^{k/2}}^\times$). También puede recorrerse $\zeta \in \mathbb{F}_{q^{k/2}}^\times$ — digamos $\zeta \leftarrow g\zeta$ para un elemento g de orden grande, que a diferencia de un generador no exige factorizar $s - 1$, reiniciando desde un nuevo ζ_0 cuando la clase $\zeta_0 \langle g \rangle$ se agota, o simplemente eligiendo ζ al azar — y decodificar cada ζ por los pasos 3–4 del algoritmo 5.1 antes de proseguir como arriba; ζ^{q^m} se actualiza con una multiplicación por paso y el test $x_A \in \mathbb{F}_q$ es gratuito en una base que contiene 1. Este bucle visita $q^{k/2-1-k/e}$ elementos de $\mathbb{F}_{q^{k/2}}$ por cada par (x_A, x_Q) que acaba decodificando, a unas pocas multiplicaciones en $\mathbb{F}_{q^{k/2}}$ cada uno; su coste esperado es de $\frac{2(s-1)}{\ell-1}$ pasos así, unos $2^{1271}M$ sobre BN254 y $2^{2032}M$ sobre BLS12-381 en la unidad de la sección 10, gastados por completo en localizar los pares que el bucle directo de arriba enumera gratis. Está dominado y sólo se consigna porque es la forma en que aparece la decodificación del algoritmo 5.1.

9 Verificación experimental

Todos los enunciados se comprobaron en PARI/GP 2.15.4 (núcleo GMP 6.3.0, 64 bits) bajo Ubuntu 24.04.4 LTS, Linux 6.18, en una máquina virtual en la nube de un solo núcleo que reporta un Intel Xeon a 2,10 GHz con 3,9 GiB de RAM; $\mathbb{F}_{q^k}$ se representa mediante un único polinomio irreducible de grado 12 (ffgen de PARI), no como torre. La curva es la curva BN de parámetro $u = 1$ ($u = -1$ da una más pequeña, $q = 19$, $\ell = 13$, con sólo seis abscisas en cada grupo, demasiado pequeña para que los recuentos de abajo signifiquen algo): $q = 103$, $\ell = 97$, $E : Y^2 = X^3 + 5$, $\#E(\mathbb{F}_q) = \ell$, $\mathbb{F}_{q^k} \simeq \mathbb{F}_{103^{12}}$ de 80 bits; aquí $e = 6$, $m = 2$, y λ resultó ser de orden 3. El signo $(-1)^d = -1$ de la proposición 3.1 se confirmó con una función de Miller normalizada en $\mathcal{O}$; con `elltatepairing` de PARI, que no lo está, la constante bruta es otro elemento de $\mathbb{F}_q^\times$, independiente de (A, Q) , y el emparejamiento reducido no se ve afectado puesto que $(q - 1) \mid (q^k - 1)/\ell$.

comprobación	resultado
$\xi(Q) \in \mathbb{F}_{q^{k/2}}$ para $Q \in G_0$	sí
$\lambda = \xi(Q)^{q^m} / \xi(Q)$ independiente de Q , $\text{ord}(\lambda) = 3$	sí
$L(u) = 0$ para todo $u \in W$; $\mathbb{F}_q \cap W = \{0\}$ (todos los $a \in \mathbb{F}_q^\times$)	sí
Prop. 3.1 con Miller normalizado: $v^{s+1} = -\zeta^\ell$	sí
Alg. 5.1 recupera $(\xi(A), \xi(Q))$ exactamente, 30 pares aleatorios	30/30
3000 raíces ℓ -ésimas aleatorias de un objetivo aceptadas	0
Prop. 7.1: 48^2 pares de abscisas, 96 pares con $t = z$, 48 valores de ζ	sí
Obs. 3.2: (6) exacta para $n = 5, 11, 13$; (7); $h_{s,A}(Q)^{s+1} = 1$; $h_{2\ell-1,A}(Q)^{s+1} = \zeta^{2\ell-2}$; (8) con $T = 6$	sí
Lema 3.3: (9) en ambas orientaciones; (10); $-h_{s,A}(Q) = t(A, Q)^{48}$, $48 \equiv -1/2$; $\text{ord}(h_{s,A}(Q)) = 194 = 2\ell$	sí
$h_{s,Q}(A)$ bilineal en Q y en A sin exponenciación final; $h_{s,-Q}(A) = t(Q, A)^{1/2}$	sí
Lema 6.1: $e_\ell \in \mu_\ell$; $t(A, Q) = e_\ell^{c-\rho}$, $t(Q, A) = e_\ell^{-\rho}$ ($c \equiv 10$, $\rho \equiv 80 \pmod{\ell}$); (13) da 15, y $t(Q, A) = t(A, Q)^{15}$	sí
$\gcd(2\ell - 2, s - 1) = 48$ sobre la curva de juguete, $= 48u$ sobre BN254	sí
Los cuatro valores $w, -w, w^s, -w^s$ de la prop. 5.1	sí
Prop. 6.2: imagen de $v \mapsto (v^{(q^k-1)/\ell}, v^{s+1})$ de orden $\ell(s-1)$	sí
Obs. 3.2: $h_{T,Q}(A)^{s+1} = (\xi(A) - \xi(Q))^{-h\ell}$; $h_{q,Q}(A)^{s+1} = 1$; $h_{3\ell,A}(Q)^{s+1} = -\zeta^{3\ell}$ con $3\ell \nmid s+1$	sí
Obs. 3.4: $h_{q,Q}(A)^\ell = 1$; $h_{q,Q}(A) = t(Q, A)^{49}$, $49 \equiv -1/(kq^{k/2-1})$; $h_{q,-Q}(A) = t(Q, A)^{48}$	sí
Obs. 4.4: β no cuadrado en $\mathbb{F}_{q^{k/2}} \iff \text{Fr}_q^{k/2}Q = -Q$ sobre 2000 $x_Q \in W$ aleatorios (1001 no cuadrados, $e = 6$); β no cuadrado para 30 puntos de G_0	sí
$1/\pi_z = (s-1)/48 = 2,49 \cdot 10^{10}$ frente a $2s/\ell = 2,46 \cdot 10^{10}$ predicho	sí

Una inversión completa de un emparejamiento bilineal. El algoritmo de la sección 8 se ejecutó hasta el final: los candidatos son los pares $(a, x_Q) \in \mathbb{F}_q \times W$ con $W = \xi(Q_0)\mathbb{F}_{q^2}$, es decir $\zeta = x_Q - a$, $q^3 = 1\,092\,727$ candidatos en total, para los cuales $x_A = a$ y x_Q se leen directamente y no hace falta ninguna proyección. El objetivo fue $z = t(A^*, Q^*)$ para un par uniformemente aleatorio $(A^*, Q^*) \in G_1 \times G_0$, luego olvidado; el test final fue $t(A, Q) \in \{z, z^{-1}\}$, el emparejamiento de Tate totalmente reducido, totalmente bilineal. Para que los recuentos sean significativos, a se enumeró en un orden uniformemente aleatorio de $\mathbb{F}_q$ y, para cada a , x_Q en un orden uniformemente aleatorio de W ; el tiempo de reloj de pared es `getwalltime`.

Toda abscisa a de G_1 admite exactamente una abscisa en G_0 que la completa en una solución, de modo que la ejecución se detiene dentro del bloque del *primer* a válido que encuentra: salta los a inválidos (cada uno al coste de un símbolo de Legendre, contado como un bloque saltado de q^2), luego recorre W en busca de las 48 abscisas de G_0 , evaluando un emparejamiento de Tate en cada una, hasta encontrar la correcta. En efecto, la ejecución fija A en la primera abscisa válida y busca en W su pareja. En este orden por bloques el trabajo esperado es de $(q-n)/(n+1)$ bloques saltados, $n = (\ell-1)/2$, cada uno al coste de un símbolo de Legendre en $\mathbb{F}_q$ y, cuando $h > 1$, de una multiplicación escalar $[\ell]A$ para la mitad de ellos aceptada por ese símbolo, seguidos de $q^{k/e}/2$ candidatos, la mitad de ellos caros, en el primer bloque válido (1,1 bloques y 5 304 candidatos sobre la curva de juguete); para un orden uniforme sobre $\mathbb{F}_q \times W$ el recuento correspondiente sería $2q^{1+k/e}/\ell$ por el argumento de recuento de la proposición 7.1, que coincide con él sólo salvo una constante, y sólo porque $\ell \approx q$ sobre una curva BN. Sobre 12 objetivos independientes: 12 éxitos, estando el par devuelto en $G_1 \times G_0$ con $t(A, Q) = z$ exactamente, 11 valores distintos de $\xi(A)$ (nunca el par de origen); de 0 a 4 a inválidos saltados (media 1,3); posición del x_Q correcto en el recorrido de W entre 1 022 y 10 350 de 10 609 (media 5 896), compatible con la uniforme; de 3 a 48 emparejamientos de Tate evaluados; tiempo de

reloj de pared entre 0,37 s y 1,92 s, dominado por las raíces cuadradas en $\mathbb{F}_{q^k}$ y las multiplicaciones escalares por ℓ del recorrido, no por los emparejamientos. Las ejecuciones aquí reportadas son anteriores a la observación 4.4 y comprobaban $\text{Fr}_q^{k/2} Q = -Q$ tras la raíz cuadrada; con el test de Legendre primero, calculado mediante la norma, se ahorra aproximadamente la mitad de las raíces cuadradas y multiplicaciones escalares al coste de $k/2 - 1$ multiplicaciones. La misma ejecución con el test final $t(Q, A) \in \{z_S^2, z_S^{-2}\}$, $z_S = h_{s,-Q^*}(A^*) = t(Q^*, A^*)^{1/2}$ — el propio emparejamiento de Satoh — tiene éxito de forma idéntica. Así que el problema GPI completo, para un emparejamiento con exponenciación final, queda resuelto de principio a fin, al coste que predice la sección 7.

Dos curvas más. La curva de juguete de arriba tiene $h = 1$, de modo que la línea 9 de la sección 8 ($[\ell]A = \mathcal{O}$) nunca se ejercita, y sólo $e = 6$. Las mismas comprobaciones se hicieron sobre dos curvas con cofactor: $q = 53$, $E : Y^2 = X^3 + X$, $\ell = 17$, $\#E(\mathbb{F}_q) = 68$, $h = 4$, $k = 8$, $e = 4$, $m = 2$ ($j = 1728$, torsión cuártica); y $q = 103$, $E : Y^2 = X^3 + 4$, $\ell = 37$, $\#E(\mathbb{F}_q) = 111$, $h = 3$, $k = 12$, $e = 6$, $m = 2$. Sobre ambas: λ tiene orden exactamente $e/2$; $1, \omega, \dots, \omega^{e/2-1}$ son vectores propios de $u \mapsto u^{q^m}$ con valores propios λ^j y $\ker L = W$ (lema 4.1); la proposición 3.1 se cumple con signo -1 ; el algoritmo 5.1 recupera $(\xi(A), \xi(Q))$ en 30/30 pares aleatorios; las formas cerradas del lema 3.3 y de la observación 3.4 se cumplen, con $\text{ord}(h_{s,A}(Q)) = 2\ell$; el κ' de (13) vale 3 y 8 respectivamente y $t(Q, A) = t(A, Q)^{\kappa'}$; la imagen de la aplicación de la proposición 6.2 tiene orden $\ell(s-1)$; y el algoritmo de la sección 8, en orden aleatorio, tuvo éxito en 5/5 objetivos aleatorios en cada curva, verificándose el par devuelto contra z . La línea 9 se ejercita ahora: en la curva $e = 4$, de los x_A que superan el símbolo de Legendre, 4/5, 2/3, 12/13, 6/7 y 1/2 fueron rechazados por $[\ell]A \neq \mathcal{O}$ en las cinco ejecuciones ($|\xi(G_1)| = 8$ entre las 33 abscisas de $E(\mathbb{F}_q)$); en la curva $e = 6$, 0/1, 2/3, 1/2, 0/1 y 3/4 (18 entre 55).

La curva $e = 4$ revela un hecho estructural que los ejemplos $e = 6$ ocultan: 400/400 de los $x_Q \in W$ con $\beta \neq 0$ tenían β no cuadrado en $\mathbb{F}_{q^{k/2}}$, frente a 203/399 en la curva $e = 6$. Es la observación 4.4 en sus dos casos: para $e = 4$ el test de Legendre es vacío y $[\ell]Q = \mathcal{O}$ hace todo el filtrado; para $e = 6$ rechaza aproximadamente la mitad.

Recuento de operaciones. No se hace ninguna comparación de tiempos: a esta escala los tiempos miden el intérprete GP, y los dos costes tienen asintóticas distintas en ℓ . En el algoritmo de la sección 8, cada x_A cuesta un símbolo de Legendre en $\mathbb{F}_q$ y, para la mitad que lo supera, una raíz cuadrada en $\mathbb{F}_q$ y un $[\ell]A$; cada x_Q cuesta un símbolo de Legendre en $\mathbb{F}_{q^{k/2}}$ calculado mediante la norma como en la observación 4.4 ($k/2 - 1$ Frobenius y $k/2 - 1$ multiplicaciones en $\mathbb{F}_{q^{k/2}}$, luego un símbolo de Jacobi en $\mathbb{F}_q$ de coste muy inferior a $1M$), que rechaza aproximadamente la mitad para $e = 6$ y nada para $e = 4$ (observación 4.4), y para los supervivientes una raíz cuadrada en $\mathbb{F}_{q^k}$ y un $[\ell]Q$ sobre $E(\mathbb{F}_{q^k})$ — unas 2^{12} multiplicaciones en $\mathbb{F}_{q^k}$ por x_Q en promedio para $e = 6$ a los tamaños de la sección 10, es decir aproximadamente cuatro emparejamientos de Tate, y el doble para $e = 4$. En el bucle de la observación 8.1, cada ζ cuesta además una multiplicación para actualizar ζ^{q^m} , tres o cuatro para la decodificación y un test de pertenencia gratuito en una base que contiene 1, alcanzándose lo anterior sólo para la fracción $q^{1+k/e-k/2}$ de los ζ . El paso interno de [7, Alg. 6.1] es, para ℓ impar, la búsqueda de raíces de $g(T) = \gamma$ sobre $\mathbb{F}_{q^k}$ con $\deg g = (\ell-1)/2$, aquí 48 ($\varphi = g(\xi)$; la forma $g(T)^2(T^3+b) - \gamma^2$ de grado 99 es [7, ec. (6.1)] para ℓ par).

10 Comparación con [7]

La proposición 6.2 hace explícito el factor de mejora, término a término. En [7, Alg. 6.1] la variable del bucle γ recorre $\gamma_0 \mu_{(s-1)\nu}$, de modo que γ^ν recorre la clase $z^{-1} \mathbb{F}_{q^{k/2}}^\times$, cada valor ν veces, con una búsqueda de raíces de grado $(\ell-1)/2$ en cada paso. Ese bucle es ya un recorrido ciego de una coordenada $\mathbb{F}_{q^{k/2}}^\times$: por [7, Thm. 5.3(ii)–(iii)], en sus letras ($A \in G_0$, P racional), $\varphi(A+P)^\nu h_{s,-A}(P) \in \mathbb{F}_{q^{k/2}}^\times$, de modo que $\varphi(A+P)^\nu$ es el producto de $h_{s,-A}(P)^{-1} \in \mu_\ell$ y de un elemento $c_{A,P} \in \mathbb{F}_{q^{k/2}}^\times$ — la escisión $\mu_{\ell(s-1)} \cong \mu_\ell \times \mu_{s-1}$ de la proposición 6.2, aplicada a $\varphi(A+P)^\nu$ en lugar de v . Su c es la componente

μ_{s-1} , y el bucle sobre γ con $\varphi(kR)^\nu = c/z$ fija la componente μ_ℓ en z^{-1} y recorre la otra, que no lleva información alguna sobre z . El presente método (i) elimina la redundancia ν , tomando la propia coordenada como variable del bucle, dentro de la cual la raíz d -ésima es única (lema 3.5); (ii) elimina la búsqueda de raíces, ya que la decodificación de la coordenada en las dos abscisas es polinómica (algoritmo 5.1); (iii) reduce la coordenada de $\mathbb{F}_{q^{k/2}}^\times$ a $\mathbb{F}_q \oplus W$ mediante la torsión (lema 4.1); y (iv) comprueba la pertenencia de x_A a $\xi(G_1)$ con un símbolo de Legendre antes de tocar W , que es el orden por bloques de la sección 8. Los cuatro factores son $\nu \approx s/\ell$, $\tilde{O}(\ell)$, $q^{k/2-1-k/e}$ y unos q/ℓ ; su producto es $q^{k-k/e}/\ell$ salvo constantes y logaritmos, el cociente de las dos primeras columnas de abajo. Buscar en G_0 por múltiplos de un generador en lugar de recorrer W reduce la coordenada una vez más, a ℓ puntos, y es la última columna. Nada en esta cadena usa z antes del test final, y por la proposición 6.2 nada en esta vía podría hacerlo.

Lo que hace la vía de la norma puede pues enunciarse con precisión. En la orientación Tate con $\ell \mid d$, la ambigüedad del valor bruto de Miller — una clase de tamaño $(s-1)\nu$ — se reduce en el factor ν al pasar a la norma; la decodificación de ζ en las dos abscisas se vuelve polinómica incluso con ambas desconocidas (lema 4.1); y la coordenada residual es independiente del objetivo (proposición 6.2), de modo que el bucle de la sección 8, o el dominado de la observación 8.1, la recorre sin guía.

La comparación con [7, Alg. 6.1] debe hacerse con la misma convención, esperanza contra esperanza. Para [7, Alg. 6.1] sobre una curva ordinaria, la probabilidad de éxito por iteración es a lo sumo $(\ell-1)/((s-1)\nu)$ [7, Rem. 6.5], y cada iteración es una búsqueda de raíces de grado $(\ell-1)/2$ sobre $\mathbb{F}_{q^k}$; el coste esperado es por tanto al menos $\frac{(s-1)\nu}{\ell-1} \cdot \tilde{O}(\ell) \approx \tilde{O}((q^k-1)/\ell)$. Para el algoritmo de la sección 8 el número esperado de candidatos es $q^{k/e}/2$, costando cada uno aproximadamente cuatro emparejamientos en promedio para $e = 6$ — la mitad cara unos ocho — y unos ocho para $e = 4$ (sección 9); para el bucle sobre $\mathbb{F}_{q^{k/2}}^\times$ de la observación 8.1 es $\frac{2(s-1)}{\ell-1}$ pasos de unas pocas multiplicaciones en $\mathbb{F}_{q^{k/2}}$. Para comparar lo comparable, la tabla de abajo está en una única unidad, M : una multiplicación en $\mathbb{F}_{q^k}$. Las conversiones usadas son: una raíz cuadrada en $\mathbb{F}_{q^k}$ y una multiplicación escalar por ℓ sobre $E(\mathbb{F}_{q^k})$ valen cada una $\approx 2^{12}M$ a estos tamaños; un emparejamiento de Tate de longitud de bucle ℓ con $A \in E(\mathbb{F}_q)$, con funciones de recta dispersas y exponenciación final ciclotómica, $\approx 2^{10}M$; una multiplicación en $\mathbb{F}_{q^{k/2}} \approx 1M$; el símbolo de Legendre de la observación 4.4 $\approx k/2 M$, siendo despreciable el símbolo de Jacobi en $\mathbb{F}_q$; una búsqueda de raíces de grado d sobre $\mathbb{F}_{q^k} \approx d \log_2(q^k) M$. Todas las entradas son esperanzas, y son ilustrativas más que medidas: cada conversión anterior es exacta sólo salvo un factor pequeño, y los exponentes heredan esa holgura. Lo robusto es la razón entre las columnas, $q^{k-k/e}/\ell$ salvo constantes y logaritmos, no los valores absolutos.

curva	[7, Alg. 6.1]	esta nota (sección 8)	observación 8.1	búsqueda exhaustiva
BN254 (alt_bn128)	$2^{2800}M$	$2^{518}M$	$2^{1271}M$	$2^{263}M$
BLS12-381	$2^{4325}M$	$2^{772}M$	$2^{2032}M$	$2^{264}M$

Dos salvedades. La cota sobre la probabilidad de Satoh es una cota superior, luego su coste esperado real puede ser mayor, lo cual sólo ensancha la brecha. Y la comparación es legítima porque, con $e := h_{s,-Q}(A)$ en la línea 15, el algoritmo resuelve el mismísimo problema de [7, Alg. 6.1] — como la sección 9 demuestra sobre la curva de juguete — no porque una rutina sustituya a otra.

11 Limitaciones

1. El método exige un grado de torsión par $e \geq 4$ (observación 4.2) y $k > 2$ (observación 4.3). No se aplica por tanto a las curvas supersingulares sobre las que [7] obtiene un número constante de iteraciones; se aplica precisamente al régimen que [7] identifica como sin esperanza.
2. Buscar directamente en G_0 para un A fijo cuesta $\ell/2$ evaluaciones del emparejamiento en esperanza, unos $2^{263}M$ y $2^{264}M$ sobre las dos curvas: menos que el algoritmo de la sección 8

en unas $4q^{k/e}/\ell$, es decir 2^{256} y 2^{509} ; un logaritmo discreto en μ_ℓ ($\approx 2^{100}$ y $\approx 2^{126}$ por TNFS especial) es más barato aún. Satoh hace la misma observación sobre su propio algoritmo. La mejora estrecha una brecha sin cerrarla.

3. La explotación de $\xi(G_0) \subset \mathbb{F}_{q^{k/2}}$ por la traza y la norma se debe a [1], cuya reducción al exponente $q-1$ es más fuerte que todo lo obtenido aquí en el marco de argumento fijo. La novedad reivindicada en este punto es que el mecanismo sobrevive al paso a dos argumentos desconocidos; las demás contribuciones se enumeran en la introducción.
4. El bucle usa z sólo en su test final, y la proposición 6.2 dice por qué: nada construido sobre la norma puede hacer otra cosa. La relación (8) para el verdadero bucle $\text{Ate } T = t - 1$ tampoco es una salida, puesto que se reduce a la proposición 3.1 con $d = h\ell$ (observación 3.2). La propia descomposición de Satoh no es una excepción: la constante $c \in \mathbb{F}_{q^{k/2}}^\times$ de [7, Thm. 5.5] es la componente μ_{s-1} de $\varphi(A+P)^\nu$ en la misma escisión de restos chinos (sección 10) — no de v , cuya norma vale 1 para su longitud de bucle (observación 3.2); incidentalmente $(\varphi(A+P)^\nu)^{s+1} = c_{A,P}^2$. Es independiente de z por la misma razón, de la que $\mu_\ell \cap \mathbb{F}_{q^{k/2}}^\times = \{1\}$, el hecho que invoca su demostración del teorema 5.5(iii), es el corolario; de modo que su bucle sobre c tampoco recibe nada de z . No conozco ninguna descomposición del valor bruto que evite la coordenada; si existe alguna es la cuestión que queda abierta.

Referencias

- [1] S. Akagi and Y. Nogami. *Exponentiation inversion problem reduced from fixed argument pairing inversion on twistable Ate pairing and its difficulty*. IWSEC 2014, LNCS 8639, pp. 240–249, Springer, 2014.
- [2] G. Frey and H.-G. Rück. *A remark concerning m -divisibility and the discrete logarithm in the divisor class group of curves*. Math. Comp. 62(206), pp. 865–874, 1994.
- [3] S. Galbraith, F. Hess and F. Vercauteren. *Aspects of pairing inversion*. IEEE Trans. Inform. Theory 54(12), pp. 5719–5728, 2008.
- [4] R. Granger, F. Hess, R. Oyono, N. Thériault and F. Vercauteren. *Ate pairing on hyperelliptic curves*. EUROCRYPT 2007, LNCS 4515, pp. 430–447, Springer, 2007.
- [5] J. Groth. *On the size of pairing-based non-interactive arguments*. EUROCRYPT 2016, LNCS 9666, pp. 305–326, Springer, 2016.
- [6] T. Satoh. *Miller inversion is easy for the reduced Tate pairing of embedding degree greater than one*. IACR Cryptology ePrint Archive, Report 2019/385, revised 2025.
- [7] T. Satoh. *Decomposition of the Ate pairing and its relation to generalized pairing inversion*. IACR Cryptology ePrint Archive, Report 2026/1049.