Comptatge de punts de corbes sobre cossos finits

(Gaudin)

$\mathcal{C}$ corba projectiva, llisa, irreductible sobre un cos finit $\mathbb{F}_q$, $q=p^n$.

La funció Zeta,

$$Z(t) = \exp\left(\sum_{k\geq 1} \#\mathcal{C}(\mathbb{F}_{q^k}) \frac{t^k}{k}\right)$$

Thm (conjectura de Weil):

- $Z(t)$ és racional.
- Satisfà una equació funcional.
- Les seves arrels tenen mòdul $\frac{1}{\sqrt{q}}$.

De fet, $Z(t) = \frac{L(t)}{(1-t)(1-qt)}$ amb $L(t) \in \mathbb{Z}[t]$, $\deg L(t) = 2g$.

$P(t) := t^{2g} L\left(\frac{1}{t}\right)$ $\quad P(t) = t^{2g} - s_1 t^{2g-1} + s_2 t^{2g-2} + \cdots + (-1)^g s_g t^g + \cdots + q^g$

$\therefore$ $P(t)$ fa totes les arrels de mòdul $\sqrt{q}$

El que volem fer és, doncs, calcular $s_1, s_2, \ldots, s_g$.

El Jacobià de $\mathcal{C}$ serà el grup de classes de divisors.

- $\#\mathrm{Jac}(\mathcal{C})/_{\mathbb{F}_q} = P(1)$
- Cal. de Frobenius, $\pi : \overline{\mathbb{F}_q} \to \overline{\mathbb{F}_q}$, $x \longmapsto x^q$ s'estén a un automorfisme

$\mathrm{Jac}(\mathcal{C})/_{\mathbb{F}_q}$ - que fa $P(t)$ com a polinomi característic.

Algoritme:

Input: $\mathcal{C}/\mathbb{F}_q$ de gènere g. En general, la talla d'aquest objecte és $\approx (\log p)\cdot g$

Output: g enters de la talla $\approx g/2 \rightsquigarrow$ talla $= g^2 n \log p$.

Existeix un algoritme que calculi en temps polinomial en $g, n, \log p$?

De moment no se'n coneix cap.

Però:

- Si g és fitat o bé $\log p$ és fitat, llavors sí que és l'algoritme.

Per exemple, el cas pitjor: $n=1$, $g \to \infty$, $\log p \to \infty$ → mal és l'algoritme.

* Algoritmes

→ Schoof, Pila, Huang Ierardi, Adleman-Huang.

- polinomial en $\log q$.
- exponencial en g

→ Satoh + Mestre + —

- polinomial en np, però només funciona per $g=1,2,3$.

→ Kedlaya + Lauder-Wan + ..

- polinomial en $n g p$ (primer algoritme polinomial en g).

→ Hep: algoritme subexponencial, prog $\gg n \log p$.

Complexitat de les operacions aritmètiques:

$M(n)$: nombre d'operacions per multiplicar "objectes" de talla n.

- Naïf: $M(n) = O(n^2)$
- Karatsuba: $M(n) = O(n^{\log_2(3)})$
- FFT: $O(n \log n \log\log n)$ $(O(n^{1+\varepsilon}))$

Divisió, GCD, Resultant, Interpolació } es poden fer en $O(M(n))$ o $O(M(n)\log n)$

Schoof

A, varietat abeliana de dimensió g / $\mathbb{F}_q$. ℓ un primer.

Def: $A[\ell]$: punts de ℓ-torsió sobre $\overline{\mathbb{F}_q}$.

Teorema: $A[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ si $(\ell, p) = 1$

Fet: $\pi|_{A[\ell]}$ té un polinomi característic $P(t) \bmod \ell$.

Algoritme:

- Mentre no es té prou informació.
  - → escollir un nou ℓ, primer $\neq p$.
  - → calcular $A[\ell]$
  - → calcular l'acció de $\pi|_{A[\ell]}$
- Reconstruir $P(t)$ amb el CRT.

És exponencial en g

- ℓ_{max} és de l'ordre de $g \log q$.
- Talla de $A[\ell]$: ℓ^{2g} punts de $\overline{\mathbb{F}_q}$ com a mínim $g(\log q)^{\ell^{2g}}$ ⇒ expo.
- Per les corbes el·líptiques (SEA):

Prop: Existeixen polinomis $\psi_\ell(x) \in \mathbb{F}_q[X]$ tals que $\forall P \in E(\overline{\mathbb{F}_q})$, $P = (x, y)$,

$$[\ell]P = 0 \iff \psi_\ell(x) = 0$$

$$\deg \psi_\ell = \frac{\ell^2 - 1}{2} \quad ; \quad \text{leadcoeff}(\psi_\ell(x)) = \ell.$$

Fet: es pot calcular $\psi_\ell(x)$ mitjançant fórmules de recurrència en $O(\log \ell \cdot M(\ell^2))$ operacions en $\mathbb{F}_q$.

Aleshores $E[\ell] \setminus \{0\}$ es pot representar com $B = \mathbb{F}_q[x,y] / (\psi_\ell(x), y^2 - (x^3 + ax + b))$

* Calcul de π en B:

$\pi(x,y) = (x^q, y^q)$ ← reduir mod $(\psi_\ell(x), y^2 - (x^3+ax+b))$.

calen $\log q$ operacions en B. $\Rightarrow \log q\ M(\ell^2 \log q)$.

Aleshores es calcula $s_n \in [0, \ell-1]$ tal que

$\pi^2(x,y) - [s_n]\pi(x,y) + [q](x,y) = 0$ dins de B.

* Complexitat total:

$(\log q) \cdot (\log q\ M(\ell^2 \log q)) = O(\log^{5+\varepsilon} q)$.

nombre de ℓ's $\quad O(\log q)$

* Millores d'Elkies: Atkin

$\Rightarrow$ Un factor de $\psi_\ell(x)$ és suficient.

Es construeix un factor de $\psi_\ell(x)$ que correspondrà a una "recta".

• Polinomi modular $\Phi_\ell(x,y)$.

Teorema: Sigui E ordinària sobre $\mathbb{F}_q$, $j \neq 0, 1728$. Sigui s_1 la traça d'E. Els graus dels factors irreductibles de $\Phi_\ell(x, j_E)$ són:

(E) i) $1, 1, r, \dots, r$ si $s_1^2 - 4q = \square$ en $\mathbb{F}_q^*$.

(A) ii) $r, r, \dots, r$ si $s_1^2 - 4q \neq \square$ en $\mathbb{F}_q^*$

(E') iii) $1, \ell$ si $s_1^2 - 4q = 0$ mod $\mathbb{F}_q$.
$1, \dots, 1$

En els casos i); ii) es diu que ℓ ~~és~~ és primer d'Elkies per E. Si no, es diu d'Atkin.

A més, r és el menor enter tal que $\forall P \in E[\ell]$, $\pi^r(P) \in \langle P \rangle$

A cada arrel j_1 de $\Phi_\ell(x, j_E)$; $j_1 \in \mathbb{F}_q^*$, se li pot associar $E \xrightarrow{\varphi} E_1 = E_{j_1}$ on φ és una isogènia de grau ℓ.

$\Rightarrow$ $\ker \varphi$ és una recta en $E[\ell] \Rightarrow$ se li pot associar un factor de ψ_ℓ de grau $\frac{\ell+1}{2}$ en $\mathbb{F}_q^k$; és a dir un factor de grau $k\frac{\ell-1}{2}$ en $\mathbb{F}_q[x]$.

Algoritme SEA:

- Calcular $\Phi_\ell(x,j)$
- Calcular la distribució de factors.
- Si és d'Elkies, sigui $j_1 \in \mathbb{F}_q$ una arrel.
  - calcular el factor $g_\ell(x)$ corresponent.
  - calcular a_ℓ mod ℓ.
- Si és d'Atkin.

Com que es treballa amb polinomis molt més petits, heurísticament es veu que la complexitat és $\mathcal{O}(\log^{4+\varepsilon} q)$.

Algoritme SWAMP (School With Algebraic Modular Polynomial).

→ Només es miren les abscisses:

$$B \simeq \mathbb{F}_q[x] / (\psi_\ell(x))$$

$P=(x,y)$

$[2]P = (\text{funció}(x), \ldots)$; $[k]P = (\text{funció}(x), \ldots)$

$[\ell]P = 0$, $h_{-k} = h_k \Rightarrow$ Hi ha $\frac{\ell-1}{2}$ valors diferents per $h_k(x)$.

Sigui $t \in B$, $t(x) = \sum_{k=1}^{\frac{\ell-1}{2}} h_k(x)$

Sigui $M(T)$ el polinomi minimal de t sobre $\mathbb{F}_q$.

Generalment, el grau de $M(T)$ és $\ell+1$.

A aquest polinomi l'anomenarem "polinomi modular".

I el teorema d'E-A continua essent cert.

Sigui $t_0 \in \mathbb{F}_q$ una arrel de $M(T)$ (cas Elkies),

Aleshores $g(x) = \text{GFD}(\psi_\ell(x), t(x) - t_0)$ és un factor de $\psi_\ell(x)$ de grau $\frac{\ell-1}{2}$.

Complexitat: ℓ càlculs de polinomis $\sim \ell^2 \Rightarrow \mathcal{O}(\log^{5+\varepsilon} q)$. (no es millora School.)

* Genere superior:

Rep d'ALG:

Hipótesi: la corba és hiperelíptica.

Aleshores $A = Jac(\mathcal{C})$. Un punt genèric de A es pot representar amb $2g$ coordenades:

Aleshores: $A[\ell] = \{(x_1, \dots, x_{2g}) \in A : [\ell](x_1 \to x_{2g}) = 0\} \cup \{\text{punts excepcionals}\}$.

$$\Rightarrow \left(x_1^{(i)}, \dots, x_{2g}^{(i)}\right)_{i \in [1, \ell^2 - \varepsilon]} \quad \text{(nombre de punts excepcionals)}$$

L'ideal reduït de la variedat V es pot representar:

$$\begin{cases} P(x_1) = \prod_{i=1}^{\ell^2-\varepsilon} (x_1 - x_1^{(i)}) \\ x_2 - P_2(x_1) \\ \vdots \\ x_{2g} - P_{2g}(x_{2g}) \end{cases} \qquad \forall i, \forall k \quad x_k^{(i)} = P_k\left(x_1^{(i)}\right)$$

Aquesta representació és possible sobre x_1 és separant de V.

Pila: es força A dins una variedat projectiva $\rightsquigarrow \varepsilon = 0$.

Hollo, AdH:

- Randomitzacions.
- Quasi-Projectives ← perquè es busquen algoritmes deterministes.

• Algoritme d'Schoof per gènere 2.

Prenem $p > 2$ (i suficientment gran per evitar degeneracions)

$\mathcal{C}$ corba de gènere 2 sobre $\mathbb{F}_q$, donada per $y^2 = f(x)$

Hipòtesi: $\deg f = 5$ (model imaginari).

El Jacobià de $\mathcal{C}$: per Riemann Roch, tot element de $\mathrm{Jac}(\mathcal{C})$ es pot representar:

- $\mathcal{O}$
- pes 1: $D = (P) - (\infty)$ única placa a ∞.
- pes 2: $D = (P_1) + (P_2) - 2(\infty)$ (amb $P, P_1, P_2 \in \mathcal{C}$).

- Representació de Mumford:

$D = \langle u(x), v(x) \rangle$ amb $u, v \in \mathbb{F}_q[X]$, $u \mid v^2 - f$.

$u := \prod (X - x_i)$; v_i és tal que $y_i = v(x_i)$ (interpolant).
(x_i, y_i)

(i.e. les x_i son $D = \sum P_i - (\text{pes})(\infty)$)

$\deg u \leq g$; $\deg v < \deg u$.

Th (Algoritme de Cantor): permet efectuar la llei de grup en $\mathrm{Jac}(\mathcal{C})$ eficaçment, amb la representació Mumford.

Question: Com calcular $J[l]$.

Els divisors son generalment de pes 2.

Per tant, calcularem $J[l] \cap \{\text{div. de pes 2}\}$.

Un divisor de pes 2 es pot expressar com $\langle x^2 + u_1 x + u_0, v_1 x + v_0 \rangle$

$[l] D = 0 \iff$ [illegible] $\in \mathrm{Jac}(\mathcal{C})[l]$

Idea: calcular $[l]D$ amb Cantor (formulari).

S'obtenen equacions en 4 variables (u_1, u_0, v_1, v_0); es poden resoldre amb Bases de Gröbner (alg. de Buchberger). ← exponencial.

Idea 2: Utilitzar els polinomis de divisió de Cantor: multiplicar els divisors de pes 1: $[l]\langle x - x_P, y_P \rangle = \left\langle X^2 + \frac{d_1(x_P)}{d_2(x_P)} X + \frac{d_0(x_P)}{d_2(x_P)}, \frac{y_P}{e_0(x)} \left(e_1(x) X + e_2(x) \right) \right\rangle$

En les expressions anteriors, es pot provar que $\deg d_i, \deg e_i = \mathcal{O}(\ell^2)$.

$D = P_1 + P_2 - 2\infty \in \mathrm{Jac}[\ell] \Leftrightarrow [\ell]D = \infty \hookrightarrow [\ell]P_1 = [\ell]P_2$.

Per tant, obtindrem un sistema més simple que el d'abans:

$$\begin{cases} E_1(x_1,x_2) = d_1(x_1)\,d_2(x_2) - d_1(x_2)\,d_2(x_1) \\ E_2(x_1,x_2) = d_0(x_1)\,d_2(x_2) - d_0(x_2)\,d_2(x_1) \\ P_1(x_1,x_2,y_1,y_2) = y_1\,e_1(x_1)\,e_0(x_2) + y_2\,e_1(x_2)\,e_0(x_1) \\ P_2(\text{---}) = \text{---} \end{cases} \quad \text{2 eq's en 2 incògnites}$$

Per obtenir una base de Gröbner, l'únic que cal és eliminar una de les dues variables de les primeres equacions:

En comptes de fer resultants bivariades, es fan unes quantes resultants univariades, i després s'interpolen els diferents valors.

S'acaba obtenint $\mathcal{O}(\ell^{6+\varepsilon})$ ops en $\mathbb{F}_q$. (molt aprox!!)

En total: $\mathcal{O}(\log^{8+\varepsilon} q)$ (si fem d'hora tot els càlculs previs i aplicar CRT).

L'algoritme SEA no es pot adaptar directament, però no es guanya gaire.
(perquè el cost està dominat pel càlcul de la ℓ-torsió).

El "record": $\ell = 29$. $\hookrightarrow$ manipula uns polinomis de grau 2,5 Milions.

- Càlcul del nombre de punts per aixecament canònic (SATOH).

Preliminars

- Extensions no ramificades de $\mathbb{Q}_p$.

$\mathbb{F}_{p^n} = \mathbb{F}_p[t]/(\bar{f}(t))$ amb $\bar{f}$ de grau n, irreductible.

Sigui $f(t)$ un polinomi en $\mathbb{Z}_p[t]$, de grau ℓ tal que $f \equiv \bar{f} \bmod p\mathbb{Z}_p[t]$.

$K = \mathbb{Q}_p[t]/(f(t))$ és una extensió no ramificada de $\mathbb{Q}_p$ (única llevat d'isomorfisme) (de grau n)

Notem: $q = p^n$; $\mathbb{F}_q$, $\mathbb{Z}_q$ (cos residual), $\mathbb{Q}_q$ (el cos p-àdic no ramificat).

$G = Gal(\mathbb{Q}_{p^n}/\mathbb{Q}_p) \cong Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma \rangle$ Frobenius : augmenta l'arrel σ pel Frobenius en G.

En els càlculs, un element de $\mathbb{Z}_{p^n}$ es representa com

$x = x_0 + x_1 t + \cdots + x_{n-1} t^{n-1}$ amb $x_i \in \mathbb{Z}/p^k\mathbb{Z}$ (precisió k (σp^k)).

La suma i producte són els usuals.

Per fer inversions: es fa per Newton: $x \leftarrow x - x(ax-1) \longrightarrow \frac{1}{a}$

• Aixecament canònic d'una corba el·líptica.

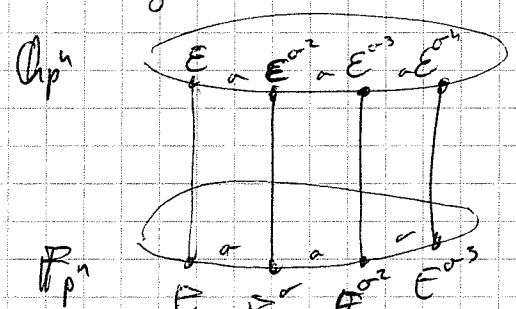
Sigui E una corba el·líptica $/\mathbb{F}_{p^n}$, ordinària.

Un aixecament canònic de E és una corba $\mathcal{E}$ sobre $\mathbb{Q}_{p^n}$ que es redueix a E mod p, i tal que $End(E) \cong End(\mathcal{E})$

Th (Serre-Tate): Un aixecament canònic existeix i és únic llevat d'isomorfisme.

donat per: $\Phi_p(J, J^\sigma) = 0$: J es redueix a $j(E)$. ($J(E)$ és l'invariant j de E)

• Cicle d'isogènies:



$\Phi_p\left(j(\mathcal{E}^{\sigma^i}), j(\mathcal{E}^{\sigma^{i+1}})\right) = 0$

Es equacions algebraiques, on n incògnites (els invariants dels lifts).

Algoritme de Satoh:

Aplicar l'algoritme de Newton per aixecar una solució del sistema.

(tenim una solució $j(E^{\sigma^i})$ mod p^n ( ).

per a això va bé per $p = 2$.

Per aixecar a precisió k, $\mathcal{O}\left((n^2 k)^{1+\varepsilon}\right)$ (però és exponencial en p!)

Lema: Si J és tal que $J \equiv j(\mathcal{E}) \bmod p^k$ i J' és tal que $\begin{cases} \Phi_p(J,J') = 0 \\ J' \equiv J^p \bmod p \end{cases}$ Aleshores, $J' \equiv j(\mathcal{E}^\sigma) \bmod p^{k+1}$

Prova: Desenvolupament de Taylor més Kronecker: $\Phi_p(x,y) \equiv (x^p - y)(x - y^p) \bmod p$

Algoritme AGM (per $p=2$) (Mestre).

Si $y^2 = x(x-a^2)(x-b^2)$ amb $a, b \in \mathbb{F}_{2^n}$, $\frac{a}{b} \equiv 1 \bmod 8$. Aleshores $\sqrt{\frac{a}{b}}$ existeix, i es pot prendre $\equiv 1 \bmod 4$.

$\begin{cases} a' = \frac{a+b}{2} \\ b' = b\sqrt{\frac{a}{b}} \quad (= \sqrt{ab}) \end{cases}$ La corba $y^2 = x(x-a'^2)(x-b'^2)$ és 2-isògena a $\mathcal{E}$.

A més a més, $j(\mathcal{E}') \equiv j(\mathcal{E})^2 \bmod 2$, i per tant, pel lema previ es guanya un bit de precisió.

Inicialització: Si $\mathcal{E}: y^2 + xy = x^3 + a_6$ en $\mathbb{F}_{2^n}$. $(a_6 \neq 0)$.

Fem $\begin{cases} a_0 = 1 + 7a_6 \bmod 16 \\ b_0 = 1 \bmod 16 \end{cases}$ $\begin{cases} a_{i+1} = \frac{a_i + b_i}{2} \\ b_{i+1} = \sqrt{a_i b_i} \end{cases}$

Aquests successors són aproximacions successives a l'aritmètic canònic.

La complexitat teòrica és $\mathcal{O}\left((n^* k)^{1+\varepsilon}\right)$

Algoritme quasi-optimal (Kim et al, Lercier-Lubicz, Harley).

Calcula el aritmètic canònic en temps quasi-lineal en la talla de la sortida $\left(\mathcal{O}((nk)^{1+\varepsilon})\right)$.

S'intenta resoldre $\Phi_p(J, J^\sigma) = 0$.

Hipòtesi: calcular σ és "fàcil" (cost d'una multiplicació).

Sigui X una aproximació de J amb precisió k.

$$0 = \Phi\left(\underbrace{J}_{X+p^k E}, \underbrace{J^\sigma}_{X^\sigma + p^k E^\sigma}\right) = \Phi_p(X, X^\sigma) + p^k E \frac{\partial \Phi_p}{\partial x}(X, X^\sigma) + p^k E^\sigma \frac{\partial \Phi_p}{\partial y}(X, X^\sigma) + p^{2k}(\cdots)$$

(Taylor)

$\Phi_p(X, X^\sigma) \equiv 0 \bmod p^k$ (lema simple). $\Rightarrow \Phi_p(X, X^\sigma) = p^k V$.

Per tant, $p^k\left(V + \epsilon \frac{\partial\phi_p}{\partial x}(x,x^\sigma) + \epsilon^\sigma \frac{\partial\phi_p}{\partial x}(x,x^\sigma)\right) \equiv 0 \mod p^{2k} \Rightarrow$

$\Rightarrow V + \boxed{\epsilon} \frac{\partial\phi}{\partial x}(x,x^\sigma) + \boxed{\epsilon^\sigma} \frac{\partial\phi}{\partial x}(x,x^\sigma) \equiv 0 \mod p^k$.

(sabut; coneguts; incògnites; conegut)

Volem resoldre una equació de la forma $X^\sigma + AX + B = 0$ a $\mathbb{Q}_{p^n}$ amb $A \equiv 0 \mod p$ (gràcies a la relació de Kronecker, això es pot garantir en el nostre cas).

Aquesta equació s'anomena "d'Artin Schreider". Es fa amb Newton.

Sigui X la solució que busquem i $x \equiv X \mod p^k$ (ull al camí de retorn).

$$\begin{cases} X = x + p^k e \\ X^\sigma = x^\sigma + p^k e^\sigma \end{cases} \Leftrightarrow \underbrace{(x^\sigma + Ax + B)}_{p^k B'} + p^k(e^\sigma + Ae) = 0 \Rightarrow e^\sigma + Ae + B' = 0$$

Tornem a trobar-nos amb la mateixa equació!

<u>Algo AS</u> (A,B,k) retorna x t.q. $X^\sigma + AX + B \equiv 0 \mod p^k$.

- Si $k=1$, retornar $\sqrt[p]{-B} \mod p$.
- $X \leftarrow AS(A,B,k/2)$ (x conegut amb prec. $k/2$)
- $X \leftarrow$ lift arbitrari de $X \mod p^k$
- $B' \leftarrow (X^\sigma + Ax + B)/(p^{k/2})$ (B' conegut amb precisió $k/2$)
- $e \leftarrow AS(A, B', k/2)$ (e conegut amb precisió $k/2$.
- Retornar $X + p^{k/2}e$ (amb precisió k)

<u>Complexitat</u>.

$C(k) = 2C\left(\frac{k}{2}\right) + 5M(nk) = 5M(nk) + 5\cdot 2\, M(n\tfrac{k}{2}) + 5\cdot 4\, M(n\tfrac{k}{4}) = O($

$= O(\log k \cdot M(nk))$.

<u>Càlcul del Frobenius</u>:

- Si $1 + x + \cdots + x^n$ és irreductible en $\mathbb{F}_p[X]$, es pren aquest polinomi per definir l'extensió $\mathbb{Q}_{p^n} = \mathbb{Q}_p[\alpha]$. Com $\alpha^{n+1} = 1$, $\alpha^\sigma = \alpha^p$.
- Si no, es pren $f(x) \mid x^{p^n-1} - 1$ en $\mathbb{Q}_{p^n}$. El generador és una arrel de f. Calcular $f(x)$ es pot fer per Newton sense utilitzar σ!! ($p=2$: $f(x^2) = f(x)f(-x)$)

• Com deduir la corbaldat en l'aixecament canònic.

Suposem que ja hem "aixecat" la corba E:

El polinomi característic del Frobenius total (potència q) dóna el numerador de Zeta.

$$\mathcal{E} \xrightarrow{\varphi_0} \mathcal{E}^\sigma$$

φ_0 és una isogènia que aixeca el Frobenius. Ens volem calcular (p.ex. amb Vélu).

Quan tenim φ_0, podem deduir l'acció de φ_0 sobre la forma $\frac{dx}{y}$:

$$\varphi_0^*\left(\frac{dx}{y}\right) = \lambda \frac{dX}{Y} \text{ en } \mathcal{E}$$
$$\text{en } \mathcal{E}^\sigma$$

$\mathcal{E} \xrightarrow{\varphi_0} \mathcal{E}^\sigma \xrightarrow{\varphi_1} \mathcal{E}^{\sigma^2} \Rightarrow$ l'acció de $\varphi_1 = \varphi_0^\sigma$ sobre les formes diferencials ve donada per λ^σ.

Per tant, $\psi = \varphi_{n-1} \circ \varphi_{n-2} \circ \cdots \circ \varphi_1 \circ \varphi_0 \Rightarrow$ ve donat per $N(\lambda)$.

(↖ aixecament de Frob)

$\psi\left(\frac{dx}{y}\right) = N(\lambda)\left(\frac{dx}{y}\right)$. L'altre VAP és $\frac{q}{N(\lambda)}$. Per tant, $Tr(\bar{E}) = N(\lambda) + \frac{q}{N(\lambda)}$

Ex: corba el·líptica / $\mathbb{F}_{2^n}$. Si el diferencial és $y^2 = x(x-1)(x-k)$, $k = 1 + 8\gamma$. Aleshores, $Tr(\bar{E}) = t + \frac{q}{t}$, on $t = N(\lambda) = N\left(\frac{1}{1+4\gamma}\right)$

Per calcular la norma de x en $\mathbb{Q}_{p^n}/\mathbb{Q}_p$,

Si $\mathbb{Q}_{p^n} = \mathbb{Q}_p[X]/(f(t))$, i $x = c(t)$, aleshores $N(x) = \text{Res}(c(t), f(t))$ en cert sentit.

També es pot fer $N(x) = \exp(\log N(x)) = \exp(Tr(\log x))$.

La resultant és fàcil de calcular amb l'alg. d'Euclides recurs.

Gènere superior:

Teorema: es pot aixecar una var. abeliana ordinària i fonda si hi ha polarització.

Però en general no es pot aixecar la corba.

En gènere 2, tota v.ab. principalment polaritzada és el jacobià d'una corba hiperelíptica.

En gènere 3: molt semblant, però la corba no serà hiperel·líptica.

Per gènere ≥ 3 no podem treballar amb la corba ($g=3$ millor que no ho fem).

Ens calen les fórmules explícites per descriure una isogènia.

Es pot fer mitjançant:

* equacions modulars
* fórmules semblants a Vélu.

Mestre: per $g=2$, $p=2$ es tenen fórmules: Richelot.

per $g>2$, $p=2$: fórmules de duplicació de les funcions Θ (mitjana de Borchardt).

Amb aquestes fórmules es pot aplicar un algorisme d'aixecament (AGM - Mestre).

Estan implementats per Lercier i Lubicz.

- Càlcul del polinomi característic:

* $g=2$ (Richelot).

$J(\mathcal{C}) \xrightarrow[\text{aixecament}]{\varphi} J(\mathcal{C}^0)$ on φ és l'aixecament de l'isogènia de Richelot.

$\varphi^*\begin{pmatrix} \frac{dx}{y} \\ \frac{x\,dx}{y} \end{pmatrix} = M_\varphi \begin{pmatrix} \frac{dX}{Y} \\ \frac{X\,dX}{Y} \end{pmatrix}$ on M_φ és completament explícita gràcies a les fórmules de Richelot.

D'aquí se'n dedueix l'acció de $\Psi = \varphi_{n-1} \circ \cdots \circ \varphi_1 \circ \varphi_0$ sobre la forma diferencial de $\mathcal{C}$: $M_\Psi = M_\varphi^{\sigma^{n-1}} \cdot M_\varphi^{\sigma^{n-2}} \cdots M_\varphi^{\sigma} \cdot M_\varphi$ = "Norma de M_φ".

* $g \geq 3$ (Borchardt):

S'utilitzen les fórmules de Thome (1870) $\rightsquigarrow$ la norma d'un escalar $\in \mathbb{Q}_{2^m}$ dóna el producte de VAPs de Frobenius que són enters en $\mathbb{Q}_{2^m}$

Utilitzant LLL es pot deduir el polinomi.

L'aixecament canònic és MOLT eficaç per $g=1$ i p petit, o per $g=2,3$ i $p=2$.

Algoritme de Kedlaya.

És un algoritme polinomial en g!!

Objectiu: utilitzar el teorema de les traces de Lefschetz per la cohomologia de Monsky-Washnitzer.

Sigui $\mathcal{C}$ una corba afí sobre $\mathbb{F}_q$, llisa; A = anell de coordenades.

$$\#\mathcal{C}/\mathbb{F}_q = \mathrm{Tr}\left(\Phi_q^{-1} \mid H^0(A/K)\right) - \mathrm{Tr}\left(\Phi_q^{-1} \mid H^1(A/K)\right).$$

$\mathcal{C}$ ve donada per una equació $f(x,y)=0$ en $\mathbb{F}_q$. I $A = \mathbb{F}_q[x,y]/(f(x,y))$

$A := \mathbb{Q}_q[x,y]/(f(x,y))$ on $f(x,y)$ és un aixecament arbitrari de $f(x,y)$.
llis.

Si es vol poder aixecar el Frobenius $x \mapsto x^q$ de $\mathbb{F}_q$ a A, cal completar A: $A^\infty := \mathbb{Q}_q[[x,y]]/(f)$

Problema: d'aquesta manera obtindríem H^i de dimensió infinita.

El que es fa és considerar només aquelles sèries que convergeixen "ràpid":

$\sum_{i,j} a_{ij} x^i y^j$ i és demana que $\mathrm{val}_p(a_{ij})$ creixi almenys linealment en $i+j$

Aleshores s'obté l'espai $A^\dagger$.

Teorema (M.W): Es pot aixecar el Frobenius en $A^\dagger$ i $\dim H^i < \infty$.

És pren el complex de deRham:

$$0 \longrightarrow \underbrace{D^0(A^\dagger)}_{A^\dagger} \xrightarrow{d_0} \underbrace{D^1(A^\dagger)}_{(A^\dagger dx + A^\dagger dy)/\left(\frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy\right)} \xrightarrow{d_1} \underbrace{D^2(A^\dagger)}_{0} \xrightarrow{d_2} \cdots \quad \leftarrow \text{no és exacte!!}$$

$$H^i := \mathrm{Ker}\, d_i / \mathrm{Im}\, d_{i+1} = \begin{cases} H^0 \text{ és de dimensió } 1. \\ H^1 \longrightarrow \text{porta tota la informació.} \\ H^i = 0 \quad \forall i \geq 2 \end{cases}$$

- Algorisme

- Aixecar Frob a $A^\dagger$
- Calcular l'acció sobre una base de H^1 { → Calcular l'acció en $\mathcal{D}^\dagger(A^\dagger)$ (sobre la base de H^1!) ; → Reduir mòdul els diferencials exactes.
- Deduir-ne el polinomi característic.

Exemple (cas de corbes hiperel·líptiques) $p>2$:

$y^2 = f(x)$ (deg $f = 2g+1$) en $\mathbb{F}_{p^m}$. En el cas en què ens trobem, es pot aixecar σ (el petit Frobenius), de manera que $\sigma(x) = x^p$ (m no és $\equiv$ mod p!).

Es fa gràcies a construir $\mathcal{C}$ per $\mathcal{C} - \{y=0\} =: \mathcal{C}'$.

$A^\dagger$ és construït per $A^{\dagger\prime} = \mathbb{Q}_{p^m}\langle\langle x, y, y^{-1}\rangle\rangle / (y^2 = f(x))$ ← preserven només les sèries que convergeixen ràpida.

- Càlcul de $\frac{1}{y^\sigma}$

$$(y^\sigma)^2 = (f(x))^\sigma \Rightarrow \frac{1}{y^\sigma} = \frac{1}{y^p}\cdot y^p \cdot (f(x)^\sigma)^{-1/2} = \frac{1}{y^p}\left(y^{-2p} f(x)^\sigma\right)^{-1/2} =$$

$$= \frac{1}{y^p}\left(\frac{f(x)^\sigma}{f(x)^p}\right)^{-1/2} = \frac{1}{y^p}\left(1 + \frac{f(x)^\sigma - f(x)^p}{y^{2p}}\right)^{-1/2}.$$

Desenvolupant en sèrie de potències $(1+t)^{-1/2}$, s'obté una sèrie convergent ràpidament en $\frac{1}{y}$.

H^1 es descomposa en $H^1_+ \oplus H^1_-$ ($\dim \deg f = \dim 2g$) si estable per l'involució $\begin{cases} x \mapsto x \\ y \mapsto -y \end{cases}$.

Una base de H^1_+ és $\left\{\frac{x^i dx}{y},\ i \in [0, \frac{d}{2g} - 1]\right\}$

En $H^1_- = \left\{\frac{x^i dx}{y},\ i \in [0, 2g-1]\right\}$. ← teorema de Kedlaya.

La prova del th. Kedlaya és el propi algorisme.

Es comença amb una forma diferencial en H^1: $\frac{x^i dx}{y}$ o bé $\frac{x^i dx}{y^2}$

L'algorisme redueix aquesta forma en la base.

Lema tècnic: la reducció no comporta la convergència ràpida.

En H^1_-:

$$\omega_i = \frac{x^i dx}{y} \rightsquigarrow \omega_i^\sigma = \frac{x^{ip} p x^{p-1} dx}{y^p} = \sum_{k \geq 0} Q_k(x) \left(\frac{1}{y^{2k}}\right) \frac{dx}{y}$$

($\deg Q_k(x) \leq 2g$, excepte $Q_0(x)$?; $\frac{1}{y^{2k}} \to \tau^k$)

Per $k>0$, escriure $Q_k(x)\tau^k \frac{dx}{y}$ en $\cdots (x)\tau^{k-1}\frac{dx}{y}$ — — — .