Algorithmique des courbes hyperelliptiques et applications à la cryptologie

Pierrick Gaudry

École polytechnique

Mardi 12 décembre 2000

Plan

Motivations

I Définitions, loi de groupe

II Calcul de la cardinalité en genre 2

– Algorithme de Schoof
– Équations modulaires, motifs de factorisation

III Étude du log discret

– Notion de friabilité sur les Jacobiennes
– Algorithme pour les courbes hyperelliptiques de genre petit
– Conséquences

IV Perspectives

Motivations

Théorie algorithmique des nombres : manipuler sur ordinateur, efficacement des objets mathématiques abstraits (corps de nombres, courbes algébriques).

Courbes elliptiques : $\mathcal{E}\ :\ y^2 = x^3 + ax + b$ sur un corps fini $\mathbb{F}_q$, très étudiées ces dernières années.

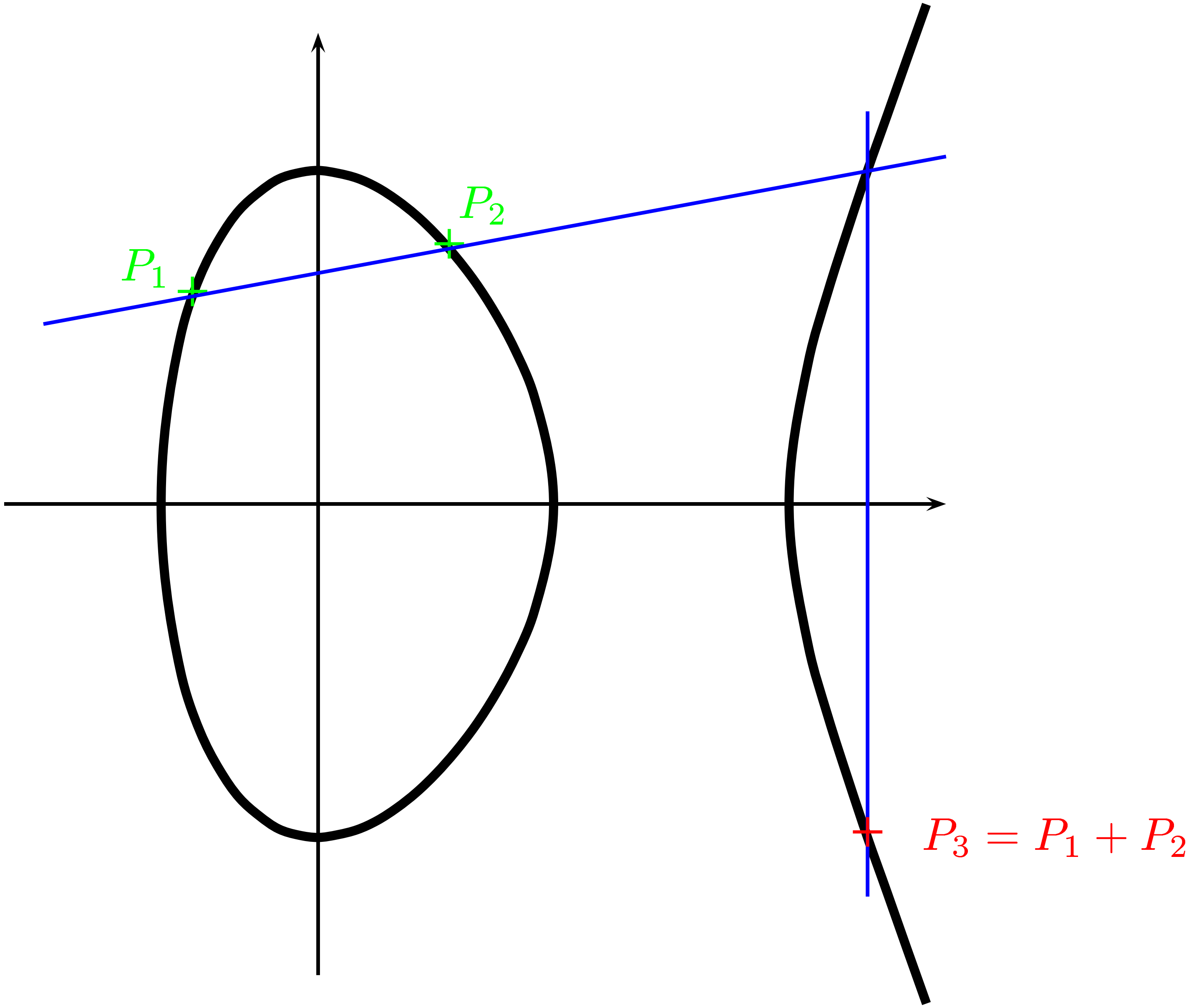
Les points forment un groupe abélien fini.

Algorithmes efficaces pour la loi de groupe et la calcul de la cardinalité.

Problème du logarithme discret : Soient $P_1 \in \mathcal{E}$ d'ordre n et $P_2 \in \langle P_1 \rangle$. Trouver λ tel que $P_2 = [\lambda]P_1$. Réputé difficile.

Application à la cryptographie : (groupe / log discret) primitive de base pour authentification, signature, chiffrement, ...

Avantage : Taille de clef petite ≈ 170 bits (i.e. groupe de cardinal $\approx 2^{170} \approx 10^{50}$)


P_1
P_2
$P_3 = P_1 + P_2$

Courbes plus générales

Les courbes sont classifiées par leur genre. ($g = 0$: coniques, $g = 1$: courbes elliptiques)

À partir du genre 2, la courbe n'est pas un groupe $\Longrightarrow$ nécessité de considérer la Jacobienne.

Motivations

- Étudier un cas plus général peut permettre de mieux comprendre un cas spécifique.
- En crypto : nécessité d'avoir des solutions de rechange.
- Même taille de clef, mais corps de base plus petit que les courbes elliptiques.

Thème de cette thèse : cas le plus simple après les courbes elliptiques : les courbes hyperelliptiques.

polynomial, rapide

exponentiel ou inconnu

polynomial théorique ou sous-exponentiel

	Courbes elliptiques	Courbes hyperelliptiques				Superelliptiques, C_{ab}			Autres
		$g=2$	3	4	$5,6,\ldots\to\infty$	$g=3$	4	$5,6,\ldots\to\infty$	
$+$				Cantor			G.P.S. Arita		?
$\#\mathrm{Jac}$	Schoof Satoh				Pila, Kampkötter, Huang–Ierardi				
L. D.					A.D.H.			G.P.S.	

Jacobiennes de courbes hyperelliptiques

Déf : Courbe hyperelliptique de genre g : courbe $\mathcal{C}$ admettant un modèle affine lisse

$$y^2 + h(x)y = f(x),$$

où $\deg f = 2g + 1$ et $\deg h \leqslant g$.

Déf : Diviseur : somme formelle finie de points de $\mathcal{C}$.

Si $D = \sum n_i P_i$, son degré est l'entier $\sum n_i$.

Déf : Diviseur principal : les n_i sont donnés par la valuation d'une fonction en P_i.

Ex : $\operatorname{div}(x - x_0) = (x_0, y_0) + (x_0, -y_0 - h(x_0)) - 2\infty$.

Prop : Les diviseurs principaux sont de degré 0.

Déf : Jacobienne : groupe quotient $\mathrm{Jac} \cong \mathrm{Div}^0/\mathrm{Princ}$.

Rem : Analogie avec le groupe de classes d'un corps de nombres.

Représentation de Mumford, algorithme de Cantor

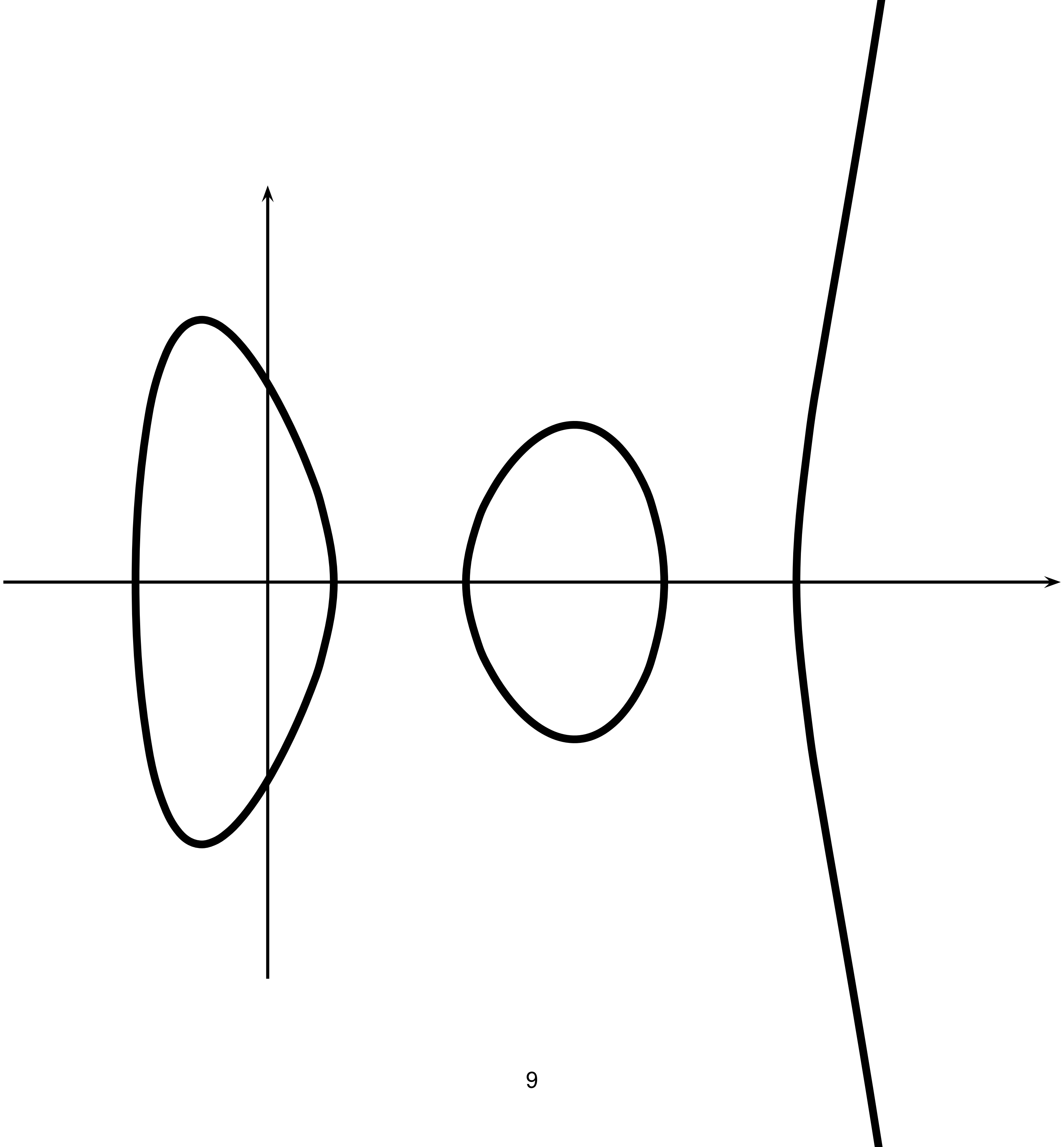
Rep de Mumford : On représente D par une paire de polynômes $\langle u(x), v(x) \rangle$, tels que

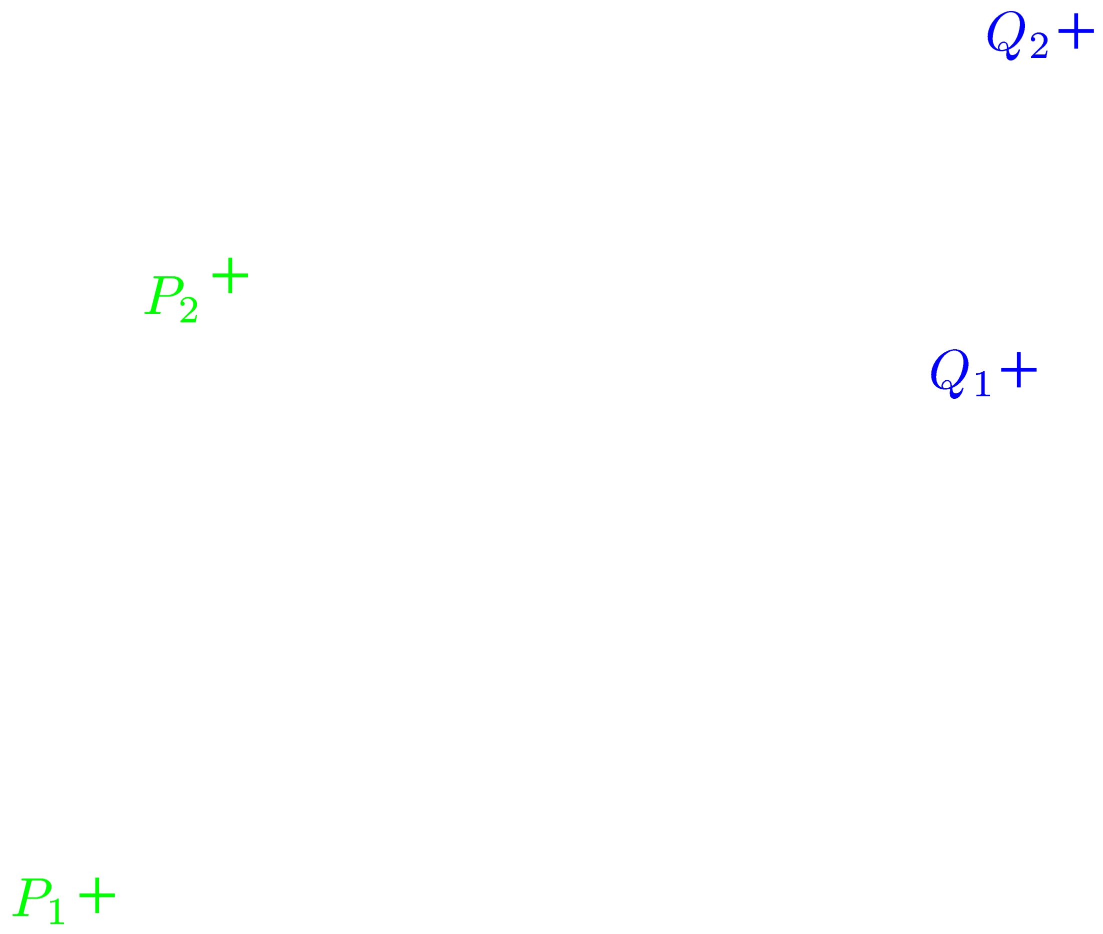
- $u(x)$ est de degré $r \leqslant g$ dont les racines sont notées x_i,
- $v(x)$ est de degré $< \deg u$, et $v(x_i) = y_i$, où $P_i = (x_i, y_i)$ est un point de la courbe.

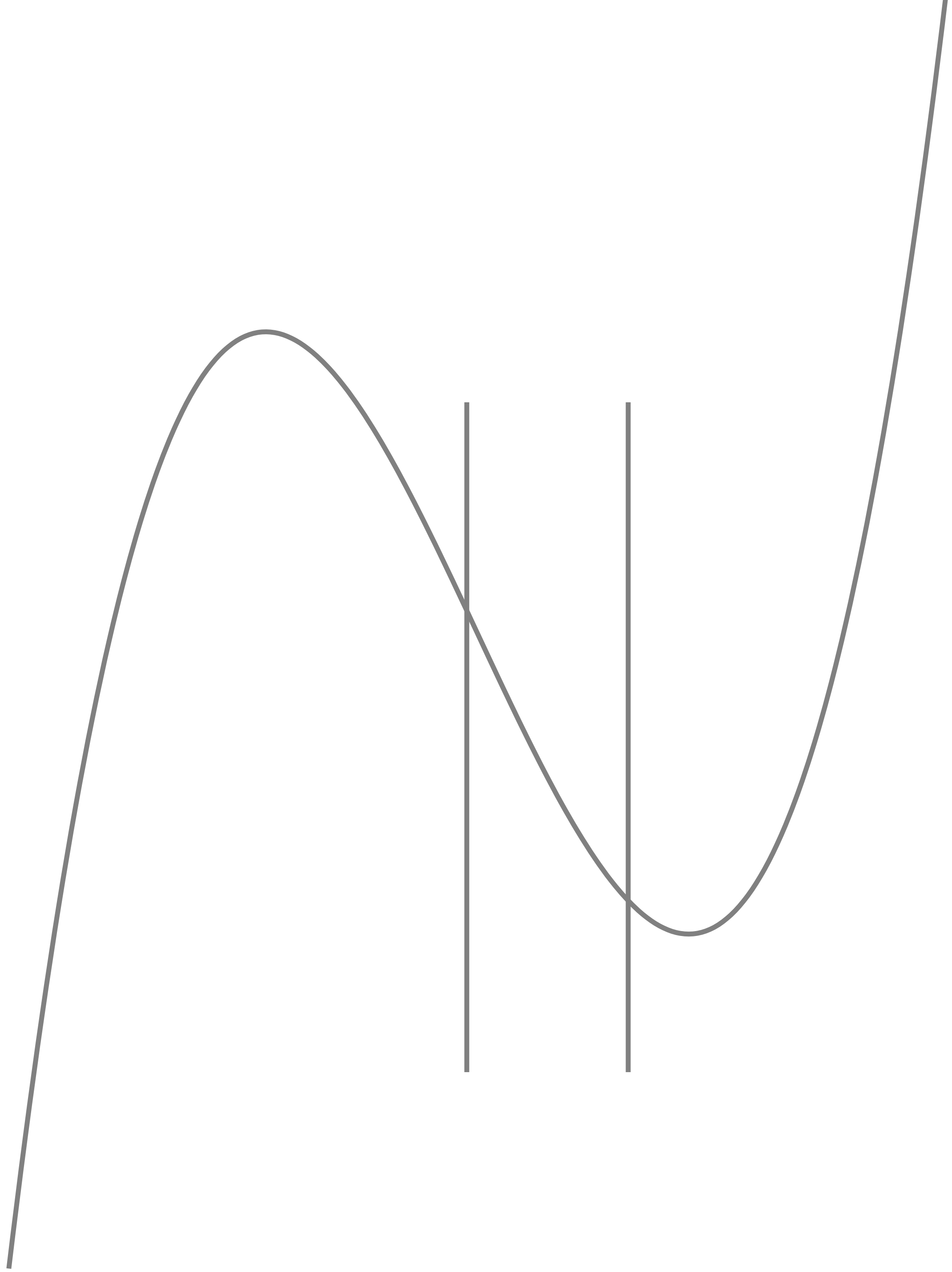
Loi de groupe : extension de la loi “corde et tangente” des courbes elliptiques.

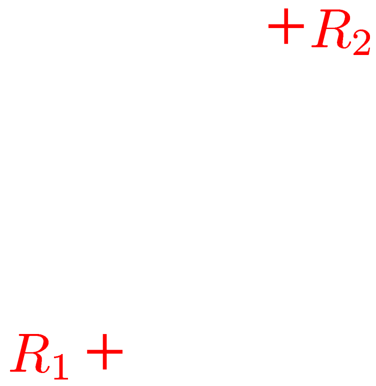
Algorithme de Cantor : calculer avec la rep. de Mumford

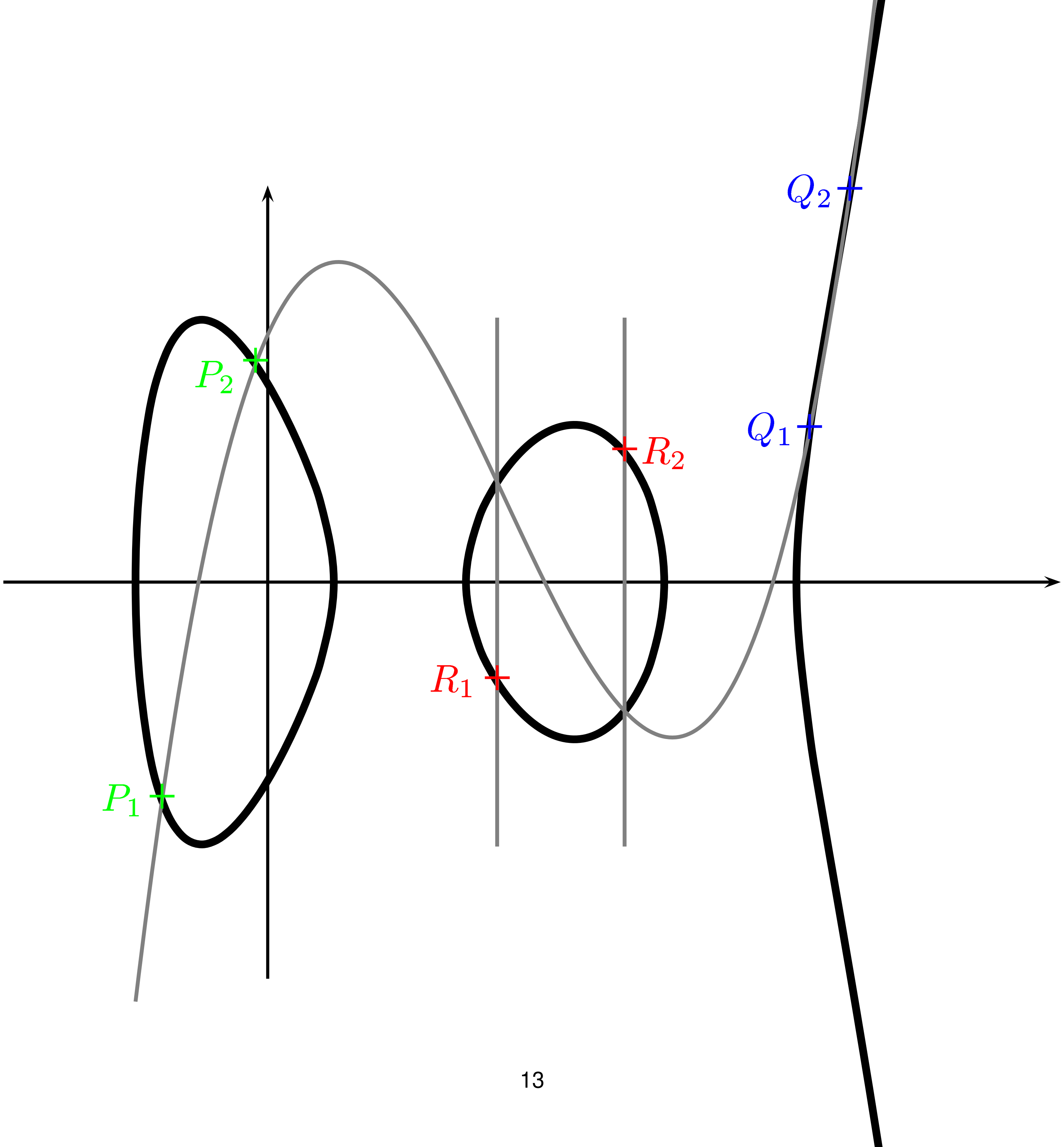
- mime la composition / réduction des formes quadratiques imaginaires,
- efficace, déroulé pour le genre 2 (Spallek, Harley) cf aussi Nagao.




Q_2
P_2
Q_1
P_1




R_2
R_1



Q_2
P_2
Q_1
R_2
R_1
P_1

II Cardinalité, généralités

On se place sur un corps fini $\mathbb{F}_q$, où $q = p^n$.

Déf : Endomorphisme de Frobenius : automorphisme $\pi \ : \ x \mapsto x^q$, défini sur $\overline{\mathbb{F}_q}$, étendu aux points de $\mathcal{C}$, puis à $\mathrm{Jac}(\mathcal{C})$.

Thm : (Weil) Le polynôme caractéristique de π sur $\mathrm{Jac}(\mathcal{C})$ est de la forme

$$\chi(t) = t^{2g} - s_1 t^{2g-1} + s_2 t^{2g-2} + \cdots - s_1 q^{g-1} t + q^g,$$

où s_i entier lié à $\#\mathcal{C}/\mathbb{F}_{q^i}$, et racines de module $\sqrt{q}$.

De plus $\quad \#\mathrm{Jac}(\mathcal{C}) = \chi(1)$.

$\Longrightarrow \ (\sqrt{q} - 1)^{2g} \leqslant \#\mathrm{Jac} \leqslant (\sqrt{q} + 1)^{2g}$, *i.e.* $\#\mathrm{Jac} = q^g + O(q^{g-\frac{1}{2}})$.

Algorithmes : • naïf, en $O(q^g)$ opérations ;

- en racine carrée (Shanks, Pollard) : $O(q^{(2g-1)/4})$ opérations ;
- cas particuliers : courbes à multiplication complexe, réelle, courbes de Koblitz.

Algorithme de Schoof pour les courbes hyperelliptiques

Principe général : Calculer $\chi(t)$ modulo de petits nombres premiers ℓ, à l'aide des éléments de ℓ-torsion du groupe. Puis, théorème Chinois.

Thm : Si $(\ell, p) = 1$, la ℓ-torsion est de la forme $\mathrm{Jac}(\mathcal{C})[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$.

Thm : Le polynôme caractéristique de π restreint à $\mathrm{Jac}(\mathcal{C})[\ell]$ est $\chi(t) \bmod \ell$.

Appartenance de $D = \langle x^g + u_{g-1}x + \cdots + u_0, v_{g-1}x^{g-1} + \cdots + v_0\rangle$ à $\mathrm{Jac}(\mathcal{C})[\ell]$ décrite par un idéal de division, noté I_ℓ :

- I_ℓ est radical, de dimension zéro, de degré $\ell^{2g} - 1$,
- possibilité de manipuler formellement un élément de $\mathrm{Jac}(\mathcal{C})[\ell]$ en travaillant modulo I_ℓ,

$\Longrightarrow$ on teste toutes les valeurs possibles de $\chi(t) \bmod \ell$: algorithme en temps polynomial.

Pila (1990), Kampkötter (1991), Huang–Ierardi (1998) : algorithmes théoriques.

Genre 2 : utilisation des polynômes de division de Cantor

Changement de variables :

$$D = \langle x^2+u_1x+u_0, v_1x+v_0\rangle = P_1+P_2-2\infty = (x_1,y_1)+(x_2,y_2)-2\infty.$$

On a $[\ell]D = 0 \iff [\ell]P_1 = -[\ell]P_2$,

Cantor (1994) donne des formules explicites pour $[\ell]P$.

$\Longrightarrow$ système de la forme

$$\left\{\begin{array}{ccccc} E_1(x_1,x_2) & = & d_1(x_1)d_2(x_2)-d_1(x_2)d_2(x_1) & = & 0, \\ E_2(x_1,x_2) & = & d_0(x_1)d_2(x_2)-d_0(x_2)d_2(x_1) & = & 0, \\ F_1(x_1,x_2,y_1,y_2) & = & y_1e_1(x_1)e_0(x_2)+y_2e_1(x_2)e_0(x_1) & = & 0, \\ F_2(x_1,x_2,y_1,y_2) & = & y_1e_2(x_1)e_0(x_2)+y_2e_2(x_2)e_0(x_1) & = & 0, \end{array}\right.$$

où les d_i et e_i sont de degré $O(\ell^2)$ et calculés par récurrence.

Résolution du système : Résultant des deux premières équations, puis propagation de la solution.

$\Longrightarrow$ obtention d'un diviseur de ℓ-torsion.

Puis, détermination de $\#\mathrm{Jac} = \chi(1) \bmod \ell$ à l'aide de ce diviseur.

Détails de l'algorithme :

- Gestion des solutions parasites
- Calcul rapide du résultant par évaluation / interpolation $\Longrightarrow$ on ne manipule que des polynômes univariés, degré $O(\ell^4)$.

Implantation : effectuée en Magma. Possible de traiter jusqu'à $\ell = 13$.

Combinaison avec d'autres méthodes :

- Division par deux dans la Jacobienne (G.–Harley–Schost)
- Algorithme "paradoxe des anniversaires" (Harley)

Ex : $p \approx 10^{19}$, courbe aléatoire $\Longrightarrow$ $\#\mathrm{Jac}(\mathcal{C}) \approx 10^{38}$. (ANTS–IV)

	Courbes elliptiques	Courbes hyperelliptiques				Superelliptiques, C_{ab}			Autres
		$g{=}2$	3	4	$5,6,\ldots\to\infty$	$g{=}3$	4	$5,6,\ldots\to\infty$	
$+$									
$\#\mathrm{Jac}$									
L. D.									

	Courbes elliptiques	Courbes hyperelliptiques				Superelliptiques, C_{ab}			Autres
		$g=2$	3	4	$5,6,\ldots\to\infty$	$g=3$	4	$5,6,\ldots\to\infty$	
$+$									
#Jac									
L. D.									

Équations modulaires en genre 2

Idée : Mimer les techniques d'Atkin–Elkies qui fonctionnent pour les courbes elliptiques. Utilisation d'équations modulaires afin de fabriquer un facteur du polynôme de division.

$$\begin{aligned}\Phi_2(X,Y) &= X^3+Y^3-X^2Y^2+1488XY(X+Y)-162000(X^2+Y^2)+40773375XY \\ &\quad +8748000000(X+Y)-157464000000000.\end{aligned}$$

Première approche : Construire un système d'équations reliant les invariants d'Igusa (j_1, j_2, j_3) de deux courbes dont les Jacobiennes sont (ℓ,ℓ)-isogènes.

- utilisation de formes modulaires de Siegel : manipulation de séries en trois variables,
- action du groupe symplectique $\mathrm{Sp}_4(\mathbb{Z})$, classes d'un sous-groupe de congruences $\Gamma_0(\ell)$,
- système énorme, même pour $\ell = 2$.

Rem : Reste d'actualité pour étendre au genre 2 l'algorithme de Satoh.

Deuxième approche : purement algébrique (G.–Schost)

Thm : Soit $\mathcal{C}\ :\ y^2 = x^5 + f_3x^3 + f_2x^2 + f_1x + f_0$. Il existe un polynôme $\Xi_\ell(T, f_i)$ tel que

- son degré en T est $\ell^3 + \ell^2 + \ell + 1$,
- ses racines sont en bijection avec les sous-groupes d'ordre ℓ de $\mathrm{Jac}(\mathcal{C})$,
- son motif de factorisation est en lien avec le degré des extensions où sont définis ces sous-groupes d'ordre ℓ, et donc avec $\#\mathrm{Jac}(\mathcal{C}) \bmod \ell$.

Construction théorique : partant d'une courbe générique, on exprime formellement l'idéal de ℓ-division. On considère le polynôme minimal d'un élément séparant de cet idéal. On définit ensuite une action sur les racines de ce polynômes, correspondant à se déplacer dans le sous-groupe engendré par un diviseur. Le polynôme $\Xi_\ell(T)$ est une résolvante pour cette action.

Rem : Construction analogue de celle de Charlap–Coley–Robbins (1991) pour les courbes elliptiques.

Construction pratique : instanciation / interpolation

Mieux : (Schost, thèse) instanciation / relèvement(s) de Newton.

Problème : Nombre de monômes du résultat est en $O(\ell^{12})$.

Calculé pour $\ell = 3$, calcul pour $\ell = 5$ à la limite de ce qui est possible actuellement ($>$250 000 monômes).

$\Xi_3(T, f_0, f_1, f_2, f_3) =$
$T^{40} + 312 f_3 T^{38} - 7904 f_2 T^{37} + (-16344 f_3^2 + 183488 f_1) T^{36} + (337536 f_3 f_2 - 4179456 f_0) T^{35} +$
$(345456 f_3^3 + 464064 f_3 f_1 - 2381088 f_2^2) T^{34} + (-6044256 f_3^2 f_2 - 196322688 f_3 f_0 + 33608832 f_2 f_1) T^{33} +$
$(-3966084 f_3^4 - 58451616 f_3^2 f_1 + 52440768 f_3 f_2^2 + 1324005696 f_2 f_0 - 364387392 f_1^2) T^{32} +$
$(57911232 f_3^3 f_2 + 280858752 f_3^2 f_0 + 591085824 f_3 f_2 f_1 - 241107200 f_2^3 - 1357926912 f_1 f_0) T^{31} +$
$(26487216 f_3^5 + 388684800 f_3^3 f_1 - 378838944 f_3^2 f_2^2 + 8135750592 f_3 f_2 f_0 - 8711658240 f_3 f_1^2 +$
$1407612480 f_2^2 f_1 - 30436734528 f_0^2) T^{30} + (-308962080 f_3^4 f_2 + 15709314816 f_3^3 f_0 - 7039348992 f_3^2 f_2 f_1 +$
$1847884416 f_3 f_2^3 - 21546021888 f_3 f_1 f_0 - 4295003904 f_2^2 f_0 + 7496418816 f_2 f_1^2) T^{29} + (-97855128 f_3^6 +$
$717110304 f_3^4 f_1 + 731068032 f_3^3 f_2^2 - 75564061056 f_3^2 f_2 f_0 - 47621349504 f_3^2 f_1^2 + 55550744448 f_3 f_2^2 f_1 +$
$141450046848 f_3 f_0^2 - 8868753152 f_2^4 - 240969913344 f_2 f_1 f_0 + 76579431936 f_1^3) T^{28} + (815181696 f_3^5 f_2 -$
$7457389056 f_3^4 f_0 - 11717124096 f_3^3 f_2 f_1 + 4346795520 f_3^2 f_2^3 + 144606394368 f_3^2 f_1 f_0 -$
$71162772480 f_3 f_2^2 f_0 + 16981051392 f_3 f_2 f_1^2 - 11416397824 f_2^3 f_1 + 131172009984 f_2 f_0^2 -$
$150350708736 f_1^2 f_0) T^{27} + (140091120 f_3^7 - 9497570112 f_3^5 f_1 + 1617994080 f_3^4 f_2^2 -$
$202079060352 f_3^3 f_2 f_0 - 85220137728 f_3^3 f_1^2 + 146302604928 f_3^2 f_2^2 f_1 + 357349905792 f_3^2 f_0^2 -$
$35760872448 f_3 f_2^4 - 857345121792 f_3 f_2 f_1 f_0 + 254363526144 f_3 f_1^3 + 16342396416 f_2^3 f_0 +$
$4166138880 f_2^2 f_1^2 + 1294107121152 f_1 f_0^2) T^{26} + \cdots$ (30 fois plus de termes)

Motifs de factorisation de Ξ_3

$\deg \Xi_3(T) = 40$ (au lieu de 80)

$p \equiv 2 \bmod 3$	
motif	$\#\mathrm{Jac}(\mathcal{C}) \bmod 3$
$(10)^4$	2
$(2)^2(6)^6$	1
$(4)(12)^3$	1
$(2)^{20}$	1
$(1)^2(2)(4)(8)^4$	0
$(1)^2(2)(3)^2(6)^5$	0
$(1)^8(2)^{16}$	0
$(1)^5(2)^4(3)(6)^4$	0
$(4)^{10}$	$1, 2$

$p \equiv 1 \bmod 3$	
motif	$\#\mathrm{Jac}(\mathcal{C}) \bmod 3$
$(5)^8$	$1, 2$
$(1)(2)^2(3)(4)^2(12)^2$	$0, 2$
$(1)^4(2)^2(4)^8$	$0, 2$
$(1)(3)^4(9)^3$	$0, 1$
$(1)^4(3)^{12}$	$0, 1$
$(1)^{40}$	$0, 1$
$(4)^{10}$	2
$(2)^2(6)^6$	1
$(2)^{20}$	1
$(1)^4(3)^{12}$	0
$(1)^2(2)(3)^2(6)^5$	0
$(1)^5(2)^4(3)(6)^4$	0
$(1)^8(2)^{16}$	0

Vérification expérimentale :

- choix d'une courbe aléatoire sur un petit corps premier,
- calcul de son nombre de points par une méthode naïve,
- calcul du motif de factorisation de $\Xi_3(T)$ pour cette courbe,
- vérification avec les tables.

Le polynôme modulaire $\Xi_\ell(T)$ est un objet qui a bien les propriétés attendues pour une extension Elkies–Atkin, mais il ne peut pas être utilisé tel quel.

III Logarithme discret dans les Jacobiennes

Soit $\mathcal{C}$ une courbe hyperelliptique de genre g sur $\mathbb{F}_q$.

Problème du log discret : Étant donnés D_1 d'ordre (premier) n, et D_2 dans le sous-groupe engendré par D_1, trouver un entier λ modulo n tel que $D_2 = [\lambda]D_1$.

Algorithme naïf : $O(q^g)$ opérations

Algorithme de Pollard-Rho : $O(q^{g/2})$ opérations

Lorsque le genre est "grand" (*i.e.* $g \gg \log q$), il existe un algorithme en temps sous-exponentiel $L_{q^g}\left(\frac{1}{2},\ c\right)$

- Adleman–Demarrais–Huang (94) : algorithme heuristique
- Flassenberg–Paulus (99) : expériences pour expliciter le "genre grand"
- Müller–Stein–Thiel, Enge (99) : versions prouvées de l'algorithme

Rem : $L_N(a, c) = \exp(c(\log N)^a(\log\log N)^{1-a})$.

Notion de friabilité (ADH) sur la Jacobienne

Déf : Un diviseur est premier si son polynôme $u(x)$ est irréductible sur $\mathbb{F}_q$.

Prop : Un diviseur $D = \langle u(x), v(x) \rangle$ est égal à la somme des diviseurs premiers $\langle u_i(x), v_i(x) \rangle$, où les $u_i(x)$ sont les facteurs irréductibles de $u(x)$.

$\Longrightarrow$ $\mathrm{Div}(\mathcal{C})$ hérite du “théorème de factorisation unique” des polynômes.

Déf : Un diviseur sur $\mathbb{F}_q$ est dit 1-friable si son polynôme $u(x)$ a tous ses facteurs irréductibles de degré 1 sur $\mathbb{F}_q$.

Rem : De manière équivalente, les points qui forment D sont eux-mêmes définis sur $\mathbb{F}_q$.

Principe du calcul d’index : se servir de la décomposition des éléments friables pour se ramener à un problème d’algèbre linéaire.

Déf : Base de facteurs, notée $\mathcal{F}$: ensemble des diviseurs $\langle x - x_0, y_0 \rangle$ où $(x_0, y_0) \in \mathcal{C}$.

Algorithme : calcul d'index en genre petit

1. Construire la base de facteurs $\mathcal{F} = \{P_j = \langle x - x_j, y_j \rangle$, où $(x_j, y_j) \in \mathcal{C}\}$.
2. Initialiser une marche pseudo-aléatoire similaire à celle utilisée dans la méthode Rho. Partir d'un diviseur R_0, calculer R_{i+1} à partir de R_i en ajoutant un diviseur selectionné parmi 20 diviseurs précalculés : $R_{i+1} = R_i + T^{(\mathcal{H}(R_i))}$, où $\mathcal{H}$ est une fonction de hachage. (cf Sattler–Schnorr, Teske)
   Maintenir une représentation $R_i = \alpha_i D_1 + \beta_i D_2$.
3. Ne garder que les diviseurs R_i friables, et les stocker dans une matrice $M = (m_{ji})$ de taille $\#\mathcal{F} \times (\#\mathcal{F} + 1)$, chaque colonne étant définie par
   $$R_i = \sum m_{ji} P_j.$$
4. Calculer un vecteur non nul $(\gamma_i) \in \mathrm{Ker}(M)$.
5. Retourner $\lambda = -\left(\sum \alpha_i \gamma_i\right) / \left(\sum \beta_i \gamma_i\right) \bmod n$.

Analyse, conséquences

Thm : Sous des hypothèses raisonnables, le temps moyen d'exécution de l'algorithme est en $O(g!q + q^2)$ opérations polynomiales.

- $1/g!$: probabilité de friabilité
- $g!q$: temps de construction de la matrice
- gq^2 : temps de l'algèbre linéaire creuse par l'algorithme de Lanczos

Si l'on suppose que le genre est petit, fixé (i.e. $g \leqslant 9$), alors la complexité est en $O(q^2)$, à comparer avec $O(q^{g/2})$ pour la méthode Rho.

g	1	2	3	4	5	6	7
Rho	$q^{1/2}$	q	$q^{3/2}$	q^2	$q^{5/2}$	q^3	$q^{7/2}$
Index	q^2	q^2	q^2	q^2	q^2	q^2	q^2

Raffinements, extensions, applications :

- En genre 2, algèbre linéaire en temps linéaire $\Longrightarrow$ complexité $O(q)$,
identique à celle de la méthode Rho.

- En genre 4, complexité en $O(q^{8/5})$.

- En genre grand, $g \gg \theta \log q$ (Enge–G.) Amélioration de la meilleure
complexité sous-exponentielle prouvée : $L_{q^g}(1/2, \sqrt{2})$.

- Application à la descente de Weil : (Frey, Galbraith–Smart, G.–Heß–Smart)
courbes elliptiques sur une extension composée en caractéristique 2 peu sûres.

- Cet algorithme s'étend aux courbes superelliptiques et C_{ab} (Arita).

Expériences pratiques : Implanté en Magma et en C (ZEN, Bignum, GMP).
Recherche de relations en parallèle sur une grappe de PC, algèbre linéaire sur un
seul PC. Tirer profit des automorphismes.

- Courbe de genre 6 (proposée par Koblitz), sur $\mathbb{F}_p$ avec $p \approx 5 \times 10^6$

- Courbe de genre 4 (avec Heß et Smart) sur $\mathbb{F}_{2^{21}}$.

corps	$\mathbb{F}_{5026243}$
équation	$y^2 + y = x^{13}$
genre	6
$\#J$	$\approx 10^{40}$

cardinal de la base de facteurs	$193,485$
temps pour construire la base	1638 sec
nombre de pas aléatoires	$201,426,284$
nombre de "early abort" par Swan	$100,721,873$
nombre de relations calculées	$281,200$
proportion d'éléments friables $(g!)$	716.3 (720)
temps total pour recueillir les relations	$513,870$ sec $=$ **6 jours**
temps pour écrire les relations sur la base	$8,822$ sec
temps pour prétraiter la matrice	1218 sec
taille de la matrice	$165,778 \times 165,779$
temps total pour Lanczos	$780,268$ sec $=$ **9 jours**

Temps sur un Pentium II 450 MHz

Auteur	Équation de la courbe	Corps	Automorphismes	m
Koblitz	$Y^2+Y=X^5+X^3$	$\mathbb{F}_{2^n}$	Frob + $\begin{cases} X \mapsto X+1 \\ Y \mapsto Y+X^2 \end{cases}$	$4n$
	$Y^2+Y=X^5+X^3+X$	$\mathbb{F}_{2^n}$	Frobenius	$2n$
	$Y^2+Y=X^{2g+1}+X$	$\mathbb{F}_{2^n}$	Frobenius	$2n$
	$Y^2+Y=X^{2g+1}$	$\mathbb{F}_{2^n}$	Frobenius	$2n$
Buhler–Koblitz Chao et al.	$Y^2+Y=X^{2g+1}$ (et ses twists)	$\mathbb{F}_p$ avec $p \equiv 1\ (2g+1)$	multiplication par ζ_{2g+1}	$2(2g+1)$
Sakai–Sakurai Smart	$Y^2+Y=X^{13}+X^{11}+X^9+X^5+1$	$\mathbb{F}_{2^{29}}$	Frob + $\begin{cases} X \mapsto X+1 \\ Y \mapsto Y+X^6+X^5+X^4+X^3+X^2 \end{cases}$	4×29
Duursma–Sakurai	$Y^2=X^p-X+1$	$\mathbb{F}_{p^n}$	Frob + $\begin{cases} X \mapsto X+1 \\ Y \mapsto Y \end{cases}$	$2np$

Pour un usage cryptographique, il est préférable d'utiliser les courbes de genre 1, 2, 3.

Le corps de base des courbes elliptiques doit être un corps premier ou une extension de degré premier.

	Courbes elliptiques	Courbes hyperelliptiques				Superelliptiques, C_{ab}			Autres
		$g=2$	3	4	$5,6,\ldots\to\infty$	$g=3$	4	$5,6,\ldots\to\infty$	
$+$									
$\#\mathrm{Jac}$									
L. D.									

	Courbes elliptiques	Courbes hyperelliptiques				Superelliptiques, C_{ab}			Autres
		$g=2$	3	4	$5,6,\ldots\to\infty$	$g=3$	4	$5,6,\ldots\to\infty$	
$+$									
$\#\mathrm{Jac}$									
L. D.									

Perspectives

1 Courbes de genre 2

– Poursuivre la construction de l'analogue Elkies–Atkin

– Étendre l'algorithme de Satoh

2 Courbes hyperelliptiques de genre 3

– Adapter l'algorithme de Schoof (Elkies–Atkin ?)

– Étudier le calcul d'index : l'algèbre linéaire peut-elle être faite en temps meilleur que $O(q^{3/2})$?

3 Courbes plus générales (superelliptiques, C_{ab})

– Étudier la loi de groupe (Galbraith–Paulus–Smart, Arita), le calcul de la cardinalité

– S'attaquer au logarithme discret (plus facile qu'hyperelliptique ?)