Séries L et courbes hyperelliptiques

Sylvain Duquesne

Université Montpellier 2

ANR Algol
Sorèze, 17 mars 2008

Institut de Mathématiques et de Modélisation de Montpellier (I3M)
Université Montpellier II – UMR CNRS 5149

Calcul des séries L associées aux courbes hyperelliptiques

Computing L-series of hyperelliptic curves

Papier présenté à ANTS 8
par Kedlaya et Sutherland

Contexte genres 1,2 ou 3

But Calculer les N premiers coefficients de la série L en passant par le produit Eulerien $L(C,s) = \prod_p L_p(p^{-s})$ ie par la fonction zeta

$$\frac{L_p(T)}{(1-T)(1+T)} = \exp\left(\sum_{k=1}^{\infty} N_k T^k/k\right)$$

où N_k est le nombre de points de C sur $\mathbb{F}_{p^k}$.On sait également que

$$L_p(T) = \prod_{i=1}^{2g}(1-\alpha_i T) = \sum_{i=0}^{2g} a_i T^i \text{ avec } a_{2g-i} = p^{g-i} a_i$$

$\Rightarrow$ il est suffisant de calculer $a_1, \cdots, a_g$

3 approches possibles

Énumération des points

Calcul de $N_1, \cdots, N_g$ et utilisation de $N_k = p^k + 1 - \sum_{i=1}^{2g} \alpha_i^k$

Utilisation de la structure de groupe

Calcul de $L_p(1) = \#J(C/\mathbb{F}_p)$ (pas de bébé, pas de géant)
$\Rightarrow L_p(T)$
Complexité en $O(p^{(2g-1)/4})$

Utilisation des méthodes p-adique

Algos de Kedlaya $\longrightarrow$ polynôme caractéristique du Frobenius
Complexité en $\tilde{O}(p^{1/2})$

Remarque : Complexité au mieux en $O(N)$
$\Rightarrow$ pas plus que 2^{40} en genre 1, 2^{28} en genre 2 et 2^{26} en genre 3

Stratégies

En genre 1

Stratégie 2 (BSGS) en $O(p^{1/4})$

En genre 2

- Mélange des stratégies 1 et 2 : énumération de $C(\mathbb{F}_p)$ en $O(p) \longrightarrow a_1$ connu et BSGS se fait alors en $O(p^{1/4})$
- Stratégie 2 (BSGS) en $O(p^{3/4})$
- Stratégie 3 (Kedlaya) en $\tilde{O}(p^{1/2})$

En genre 3

- Mélange des stratégies 1 et 2 : $O(p)$ (énumération) puis $O(p)$ (BSGS)
- Stratégie 3 (Kedlaya) en $\tilde{O}(p^{1/2})$

Finalement les constantes des O sont primordiales car $p < N$

Améliorations pour l'énumération

Quasi inutile en genre 1 (p très petit) mais utile en genre 2 et 3

Implémentation naïve

- Faire une table des résidus quadratiques de $\mathbb{F}_p$
- évaluer $f(x)$ et regarder si il est dans la table (d multiplications et d additions)

Utilisation des différences finies

$$(\Delta f)(x) = f(x+1) - f(x)$$

On peut alors énumérer toutes les valeurs de $f(x)$ par

$$f(x+1) = f(x) + (\Delta f)(x)$$

et Δf est de degré $d-1$
$\Rightarrow$ permet d'évaluer $f(x)$ en d additions seulement

Calcul de $|G|$

On suppose qu'on a

$$M_0 \leq |G| \leq M_1$$

Étape 1 : calcul de $\lambda(G)$ le ppcm des ordres des éléments de G

1. $E = 1$
2. Tirer α au hasard dans G
3. Calculer l'ordre de $\beta = \alpha^E$ en utilisant BSGS dans $[M_0/E, M_1/E]$
4. $E = |\beta|E$
5. Répeter les étapes 2,3,4 jusqu'à ce que soit
   - Il n'y ait qu'un seul multiple de E dans $[M_0, M_1]$ (et alors $|G|$ est ce multiple)
   - On ait fait c tirage (et alors $\lambda(G) = E$ avec probabilité $1 - 2^{2-c}$)

Calcul de $|G|$

Étape 2 : Déduire $|G|$ de $\lambda(G)$ en $O(|G|^{1/4})$

On suppose cette fois que $M_0 \leq |G| \leq 2M_0$ et on calcule les ordres des p-Sylow de G pour $p|\lambda(G)$

Optimisation dans le cas des jacobiennes

Définition

Un polynôme symplectique unitaire est un polynôme réel de degré pair dont les racines sont sur le cercle unité et groupées en paires conjuguées

Hypothèse de Riemann pour les courbes (théorème de Weil)

$L_p(zp^{-\frac{1}{2}}) = \sum a_i z_i$ est un polynôme unitaire symplectique et

$$|a_i| \leq \binom{2g}{i}$$

On en déduit

$$(\sqrt{q}-1)^{2g} \leq \#J(C/\mathbb{F}_p) \leq (\sqrt{q}+1)^{2g}$$

Optimisation dans le cas des jacobiennes

Amélioration de la borne pour a_2

Soit $\sum_{i=1}^{2g} a_i z^i$ un polynôme symplectique unitaire, alors

$$-g + 2 + (a_1^2 - \delta^2)/2 \leq a_2 \leq g + \left(\frac{g-1}{2g}\right) a_1^2$$

Exemple en genre 3 $\longrightarrow$ intervalle de longueur 6 au lieu de 30

Utilisation des probabilités

On suppose que ce qu'on cherche $(|G|,\ a_1,\ a_2)$ est une variable aléatoire X avec un certaine distribution dans $[M_0, M_1]$.
On fait un BSGS en partant de la médiane M de X et avec une taille de pas de $\sqrt{2E}$ où E est l'écart à la médiane.
Reste à connaître M et E

Lien avec les matrices aléatoires

P polynôme symplectique unitaire $\leftrightarrow$ classe de conjugaison des matrices symplectiques unitaires de taille $2g$ ayant P comme polynôme caractéristique.

Théorie des matrices aléatoires

$\longrightarrow$ distribution des valeurs propres

$\longrightarrow$ distribution des coefficients de P

$$\Rightarrow M \text{ et } E$$

Pour a_1

écart à la médiane en genre 1 : .85 au lieu de 1
écart à la médiane en genre 2 : .79 au lieu de 2
écart à la médiane en genre 3 : .80 au lieu de 3

Question : P se comporte t'il comme un polynôme aléatoire ?

Finalement

- Gain d'un facteur 4 à 8 en genre 1 par rapport à GP
- Détermination des stratégies à utiliser en genre 2 et 3 suivant N

BSD en genre 2

très peu de littérature

Empirical evidence for the BSD conjecture for modular Jacobians of genus 2 curves

Flynn, Leprévost, Schaeffer, Stein, Stoll et Wetherell en 2000

BSD

2 conjectures

- le rang de la jacobienne est égal à l'ordre d'annulation de la série L en 1
- $\lim_{s \to 1} (s-1)^{-r} L(J,s) = \ldots$

Calculs effectués

Jacobiennes modulaires

La séries L est convergente pour $\Re e(s) > 3/2$. Il faut donc qu'elle se prolonge pour que BSD ait un sens.

Pour les Jacobiennes modulaires (quotients de $J_0(N)$), c'est vrai.

En plus on en connait

Jacobiennes traitées

- Quotient de $X_0(N)$ par un sous groupe d'Atkin-Lehner
  $\longrightarrow$ pas toutes traitées
- Quotient optimaux (le noyau de la réduction est connexe)

Toutes de rang 0 ou 1 $\longrightarrow$ seconde conjecture seulement

Pour aller plus loin ?

- Continuer leurs calculs
- Autres familles de courbes modulaires
- Tordues ?
- Cas du rang 2 (première conjecture)
- Courbes non modulaires ?

Exemple de courbes non modulaires

$y^2 = x^5 + A$

Etudiée par Stoll et Yang en 2003
Il existe une forme modulaire de Hilbert h_A telle que

$$L(s, J_A) = L(s, h_A) \text{ sur } \mathbb{Q}(\sqrt{5})$$

$\Rightarrow$ expression explicite de $L(1, J_A)$