Calcul de points rationnels sur une courbe elliptique de rang analytique 1

B. Allombert

IMB
CNRS/Université Bordeaux 1

03/02/2011

Lignes directrices

Introduction

Soit E une courbe elliptique définie sur $\mathbb{Q}$ de rang analytique 1.
Il s'agit de construire un générateur de la partie sans torsion de $E(\mathbb{Q})$.
L'exposé suit le preprint *Some remarks on Heegner point computation* de Mark Watkins (2006).

Lignes directrices

Nombre quadratiques imaginaires

Un nombre $\tau \in \mathbb{C}$ est un nombre quadratiques imaginaire si $\tau \notin \mathbb{R}$ et que $\dim_{\mathbb{Q}}(1, \tau, \tau^2) = 2$.
Nous associons plusieurs objets à τ.

1. Le polynôme minimal $P_\tau = a(x - \tau)(x - \overline{\tau})$, où a est l'unique entier tel que le contenu de P soit égal à 1.
2. Le réseau $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$.
3. L'ordre $\mathcal{O}_\tau = \{\alpha \in \mathbb{C} | \alpha\Lambda_\tau \subseteq \Lambda_\tau\} = \Lambda_\tau \cap \Lambda_{\frac{1}{\tau}}$. Λ_τ est un idéal fractionnaire de $\mathcal{O}_\tau$.
4. Le discriminant $\mathrm{Disc}(\tau) = \mathrm{Disc}(P_\tau) = \mathrm{Disc}(\mathcal{O}_\tau)$.

Lignes directrices

Trace et norme d'un idéal

Definition (trace d'un idéal)

Soit I est un idéal fractionnaire, l'ensemble $\{\mathrm{Tr}(\alpha) | \alpha \in I\}$ est un sous-$\mathbb{Z}$ module de $\mathbb{Q}$ monogène. On note $\mathrm{Tr}(I)$ son générateur positif.

Posons $P_\tau = ax^2 + bx + c$. Nous avons

- $\mathcal{N}(\Lambda_\tau) = \frac{1}{a}$
- $\mathrm{Tr}(\Lambda_\tau) \equiv -b/a \pmod 2$.

Lignes directrices

Points de Heegner

Un nombre quadratique imaginaire est un point de Heegner de niveau N si $\Im\tau > 0$ et $\mathrm{Disc}(\tau) = \mathrm{Disc}(N\tau)$.

Théorème

Soit $\mathcal{H}_N^D$ l'ensemble des point de Heegner de niveau N et de discriminant D, soit $S(D, N)$ l'ensemble des racines carrés modulo $2N$ de $D \pmod{4N}$, alors

$$\mathcal{H}_N^D/\Gamma_0(N) \cong S(D, N) \times \mathcal{C}\ell(\mathbb{Q}(\sqrt{D}))$$

. La première projection $t : \mathcal{H}_N^D/\Gamma_0(N) \mapsto S(D, N)$ est défini par

$$\Lambda_\tau \mapsto \mathrm{Tr}(\Lambda_\tau)/\mathcal{N}(\Lambda_\tau)$$

.

Lignes directrices

Soit E une coube elliptique défini sur $\mathbb{Q}$ modulaire de constante de Manin égale à 1, de niveau N. Soit Λ son réseau de période, $\wp$ la fonction de Weierstraß associé à E, on note $\mathcal{P}(z) = (\wp(z), \wp'(z))$ l'exponentielle elliptique de $\mathbb{C}/\Lambda \mapsto E(\mathbb{C})$. Soit

$$\phi(\tau) = \sum_{n \geq 1} \frac{a_n}{n} \exp(2i\pi n\tau)$$

.

Théorème

Soit $\tau \in \mathcal{H}_N^D$, alors $\mathcal{P}(\phi(\tau))$ appartient au corps de classe de Hilbert de $\mathbb{Q}(\sqrt(D))$.

Théorème

Soit $b \in S(D, N)$. On pose $H_N^D(b) = \{\tau \in H_N^D | t(\tau) = b\} \backslash \Gamma_0(N)$. Soit $P = \mathcal{P}(\sum_{\tau \in \mathcal{H}_N^D(b)} \phi(\tau))$, alors $P \in E(\mathbb{Q})$.

Lignes directrices

Théorème de Gross-Zagier

Théorème (Gross-Zagier)

Soit $D < -4$ un discriminant fondamental tel que D et un carré inversible modulo $4N$, alors

$$h(P) = \frac{\sqrt{-D}}{4\Omega_{vol}} L'(E,1)L(E_D,1) \quad .$$

Conjecture (Gross-Hayashi)

Soit $D < 0$ un discriminant fondamental tel que D et un carré modulo $4N$, alors

$$h(P) = \frac{\sqrt{-D}}{4\Omega_{vol}} L'(E,1)L(E_D,1)2^{\omega(pgcd(D,N))}\frac{w(D)^2}{4} \quad .$$

Lignes directrices

Conjecture de Birch et Swinnerton-Dyer

Conjecture (Birch et Swinnerton-Dyer)

Soit G un générateur de la partie sans torsion de $E(\mathbb{Q})$, alors

$$L'(E,1) = \frac{\Omega_{re}\left(\prod_{p|N\infty} c_p\right)|Ш| h(G)}{E(\mathbb{Q})_{tors}{}^2} \quad .$$

Si $P = \ell G + T$ où T est de torsion, on a $h(P) = \ell^2 h(G)$ et donc

Conjecture

$$\frac{\ell^2}{|Ш|} = \frac{\sqrt{-D}\Omega_{re}\left(\prod_{p|N\infty} c_p\right)}{4\Omega_{vol} E(\mathbb{Q})_{tors}{}^2} L(E_D,1) 2^{\omega(pgcd(D,N))} \frac{w(D)^2}{4} \quad .$$

Conséquences

- P est de torsion si et seulement si $L(E_D, 1) = 0$.
- Le nombre $\ell' = \frac{\ell^2}{|\text{Ш}|}$ est calculable et $\mathcal{P}(\frac{\sum_{\tau \in \mathcal{H}_N^D(b)}}{\ell'}) = |\text{Ш}| G +$ torsion.

Procédé de Cremona-Silverman

Soit d le dénominateur de l'abscisse de P alors d est un carré et $d = h(P) - h_\infty(P) - \sum_{p|N} h_p(P)$.

Théorème (Procédé de Cremona-Silverman)

Les nombres h_p ne peuvent prendre qu'un nombre fini de valeur en fonction du type de Kodaira de E en p. Cela permet d'obtenir l'expression rationnelle des coordonnées de P à partir des valeurs réelles approchés.

On a besoin de 4 fois moins de précision par rapport aux fractions continues.

Lignes directrices

Calcul des séries

- Algorithmes pour le calcul de $L(E, 1)$ et $L'(E, 1)$ par Buhler-Gross, Womack, Roblot-Delaunay.
- $\phi(\tau)$ se calcule facilement à l'aide de Buhler-Gross et d'une méthode pas de bébé / pas de géant pour éviter le calcul des exponentielles.
- Plus la partie imaginaire de τ est grande, plus la série converge vite.
- Comme $\phi(\overline{\tau}) = \overline{\phi(\tau)}$, on peut éviter la moitié des calculs.

Choix des paramètres

L'algorithme dépend d'un choix de D tel que $L(E_D, 1) \neq 0$, de $b \in S(D, N)$ et pour chaque classes de $H_N^D(b)$, d'un représentant τ dont on doit maximiser la partie imaginaire.

Lignes directrices

Involution d'Atkin-Lehner

Soit $Q \| N$, et u, v telque $uQ^2 - vN = Q$. L'involution d'Atkin-Lehner W_Q est défini par $W_Q(\tau) = \frac{uQ\tau+v}{N\tau+Q}$.

Théorème

Méthode de Delaunay

$$\phi(\tau) = \epsilon_Q \phi(W_Q(\tau)) + \phi(W_Q(i\infty))$$

où $\epsilon_Q = \prod_{p|Q} \epsilon_p$. *De plus Soit* $\mathcal{P}(\sum_{\tau \in \mathcal{H}_N^D(b)} \phi(W_Q(\tau))) = P +$ *torsion.*

L'involution d'Atkin-Lehner permet d'obtenir de meilleur τ.

Lignes directrices

Algorithme de Watkins

Mark Watkins propose un algorithme pour optimiser le choix des représentants pour un discriminant donné.