Heuristiques à la Cohen-Lenstra, p-groupes abéliens finis et fonctions symétriques

Frédéric Jouhet

Institut Camille Jordan
Université Lyon 1

Journées CTN

Mardi 25 septembre 2012

u-moyennes

Pour p premier, $u \geq 0$ et h fonction à valeurs complexes définie sur les classes d'isomorphismes de p-groupes abéliens finis, Cohen-Lenstra (1984) ont défini la u-moyenne :

$$M_u(h) := \frac{\sum_{n\geq 1} p^{-nu} \sum_{H(p^n)} \frac{h(H)}{|Aut(H)|}}{\prod_{j\geq 1} \left(1 - p^{-u-j}\right)^{-1}},$$

où $\sum_{H(p^n)}$ porte sur toutes les classes d'isomorphismes des groupes abéliens finis d'ordre p^n.

Pour $h \equiv 1$ on a $M_u(1) = 1$, car par Hall (1938) :

$$\prod_{j\geq 1} \left(1 - p^{-u-j}\right)^{-1} = \sum_{n\geq 1} p^{-nu} \sum_{H(p^n)} \frac{1}{|Aut(H)|}$$

But : modèle heuristique pour donner de précises prédictions sur le comportement des groupes de classes de certaines familles de corps de nombres

Adaptation aux groupes de type S

Un p-groupe G est de type S si G est un p-groupe abélien fini doté d'une forme bilinéaire alternée non dégénérée $\beta\ :\ G \times G \to \mathbb{Q}/\mathbb{Z}$.
À isomorphisme près : G est un p-groupe de type $S \Leftrightarrow G \approx H \times H$
Un isomorphisme de groupes de type S préserve β, et le nombre $|Aut^s(G)|$ d'automorphismes de G respectant β, ne dépend pas de β.

Pour une fonction g définie sur les classes d'isomorphismes de groupes de type S, Delaunay (2001) défini :

$$M_u^S(g) = \frac{\displaystyle\sum_{n\geq 1} p^{-nu} \sum_{G(p^n)} \frac{|G|\, g(G)}{|Aut^S(G)|}}{\displaystyle\prod_{j\geq 1}\left(1 - p^{-2u-2j+1}\right)^{-1}},$$

où $\sum_{G(p^n)}$ porte sur toutes les classes d'isomorphismes des groupes G de type S et d'ordre p^n (la somme est vide si n impair).

Si $g \equiv 1$, alors $M_u^S(g) = 1$, car par Delaunay (2001) :

$$\prod_{j\geq 1}\left(1 - p^{-2u-2j+1}\right)^{-1} = \sum_{n\geq 1} p^{-nu} \sum_{G(p^n)} \frac{|G|}{|Aut^S(G)|} = \sum_{n\geq 1} p^{-2nu} \sum_{G(p^{2n})} \frac{|G|}{|Aut^S(G)|}$$

Groupe de Tate-Shafarevich d'une courbe elliptique

Si E est une courbe elliptique, définie sur $\mathbb{Q}$, d'équation $y^2 = ax^3 + bx + c$, alors $E(\mathbb{Q}) := \{\text{points rationnels de } E\}$ a une structure de groupe abélien.
Par Mordell-Weil (1928) : $E(\mathbb{Q})$ est de type fini, i.e.,

$$E(\mathbb{Q}) = \mathbb{Z}G_1 \oplus \mathbb{Z}G_2 \oplus \cdots \oplus \mathbb{Z}G_r \oplus E(\mathbb{Q})_{tors},$$

où $r \in \mathbb{N}$ est le rang, $G_i \in \mathbb{Q}$ et $E(\mathbb{Q})_{tors}$ sous-groupe fini.

On sait déterminer $E(\mathbb{Q})_{tors}$ (Mazur, 1978), mais pas r (conjecture de Birch-Swinnerton-Dyer) ni les générateurs G_i.
Le problème provient de l'apparition du groupe de Tate-Shafarevich $Ш(E)$, que l'on peut identifier par la suite exacte :

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to Sel_n(E) \to Ш(E)[n] \to 0,$$

où $Sel_n(E)$ est le n-ième groupe de Selmer de E, et $E(\mathbb{Q})/nE(\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^r$ lorsque n premier avec $|E(\mathbb{Q})_{tors}|$.

Si $Ш$ est nul, alors $|Sel_n(E)|$ détermine r et en théorie les G_i.
Sinon, chaque point de $Sel_n(E)$ provient soit de $E(\mathbb{Q})$ (et contribue à l'augmentation du rang), soit d'un élément non nul de $Ш$.

Utilisation des heuristiques

Les groupes de Tate-Shafarevich sont conjecturalement finis. Dans ce cas, ils sont de type S, donc isomorphes à $H \times H$ et d'ordre un carré parfait.

Le principe heuristique stipule que si g est *raisonnable* :

$$\lim_{X \to \infty} \frac{\displaystyle\sum_{E \in \mathcal{F}_u,\, N_E \leq X} g(\text{Ш}(E))}{\displaystyle\sum_{E \in \mathcal{F}_u,\, N_E \leq X} 1} = M_u^S(g),$$

où $\mathcal{F}_u$ est l'ensemble des courbes elliptiques E de rang u définies sur $\mathbb{Q}$ et $N_E \in \mathbb{N}$ est le conducteur de la courbe E.

Pour G un p-groupe abélien de type S et $\ell \in \mathbb{N}$, soit $G[p^\ell]$ le sous-groupe des éléments de p^ℓ-torsion et $g_\ell : G \mapsto |G[p^\ell]|$. Alors, par Delaunay (2011) :

$$M_u^S(g_\ell) = 1 + \frac{1}{p^{2u-1}} + \cdots + \frac{1}{p^{\ell(2u-1)}}$$

En particulier $M_0^S(g_\ell) = M_1^S(g_\ell) \cdot p^\ell$

Généralisations

Question de Poonen : pour deux entiers positifs ℓ et m, si on pose $g(G) = |G[p^\ell]|^m$; a-t-on $M_0^S(g) = M_1^S(g)p^{\ell m}$?

Théorème (J-Delaunay, 2012)

Pour tout entier positif ℓ, soient ℓ entiers positifs ou nuls $m_1, \ldots, m_\ell$. Considérons la fonction g définie sur les classes d'isomorphismes des p-groupes abéliens de type S par : $g(G) := |G[p]|^{m_1}|G[p^2]|^{m_2} \cdots |G[p^\ell]|^{m_\ell}$, alors on a

$$M_0^S(g) = M_1^S(g)\, p^{m_1+2m_2+\cdots+\ell m_\ell}$$

Théorème (J-Delaunay, 2012)

Avec les mêmes notations, si on pose la partition d'entiers $\lambda = 1^{m_1} \cdots \ell^{m_\ell}$, alors

$$M_u^S(g) = \sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p^2)p^{-|\mu|(2u-1)},$$

où $C_{\lambda,\mu}$ est un polynôme explicite à coefficients entiers positifs.

Conséquence sur les groupes de Tate-Shafarevich

Conjecture (J-Delaunay, 2012)

Supposons $u \geq 0$ entier. Lorsque $E/\mathbb{Q}$, ordonnée par son conducteur, varie dans l'ensemble des courbes elliptiques de rang u, la moyenne de $|Ш(E)[p]|^{m_1}|Ш(E)[p^2]|^{m_2}\cdots|Ш(E)[p^\ell]|^{m_\ell}$ est égale à

$$\sum_{\mu\subseteq\lambda} C_{\lambda,\mu}(p^2)p^{-|\mu|(2u-1)}.$$

Pour $\ell = m_\ell = 1$, ce nombre vaut $1+p$ lorsque $u=0$, et $1+1/p$ lorsque $u=1$.

Conjecture du rang (rang de $E=0$ ou 1 avec probabilité $1/2$) et une conjecture de Bhargava-Shankar (2010) : en moyenne $|Ш(E)[p]| = 1+p$ (resp. $1+1/p$) pour les courbes de rang 0 (resp. 1).
Bhargava-Shankar (2010) : pour $p=2$ et $p=3$.

Swinnerton-Dyer (2008) et Kane (2011) : résultats pour $p=2$ et pour les tordues quadratiques E_d de certaines courbes $E/\mathbb{Q}$.
Avec la conjecture du rang : en moyenne $|Ш(E_d)[2]| = 3$ (resp. $3/2$) pour les courbes de rang 0 (resp. 1).

Conséquence sur les groupes de Selmer

Si $|E(\mathbb{Q})_{tors}| = 0$ et si le rang de $E = u$, alors $|Sel_n(E)| = n^u |Ш(E)[n]|$.

Conjecture (Poonen-Rains, 2012)

Pout tout entier $m \geq 0$, la valeur moyenne de $|Sel_p(E)|^m$ sur toutes les courbes $E/\mathbb{Q}$ est $\prod_{j=1}^{m}(1+p^j)$

Ceci suggère que les p-groupes de Selmer se comportent identiquement pour les rangs 0 et 1.

Conjecture (J-Delaunay, 2012)

Pout tous entiers $m \geq 0$ et $\ell \geq 0$, la valeur moyenne de $|Sel_{p^\ell}(E)|^m$ sur toutes les courbes $E/\mathbb{Q}$ est

$$\sum_{\mu \subseteq \ell^{\boldsymbol{m}}} C_{\ell^{\boldsymbol{m}},\mu}(p^2)p^{|\mu|}$$

Pour $\ell = 1$, on trouve

$$\sum_{\mu \subseteq 1^{\boldsymbol{m}}} C_{\lambda,\mu}(p^2)p^{|\mu|} = \sum_{k=0}^{m} \begin{bmatrix} m \\ k \end{bmatrix}_{p^2} p^k = \prod_{j=1}^{m}(1+p^j)$$

Notations combinatoires

Partition $\lambda := (\lambda_1 \geq \cdots \lambda_\ell > 0)$ de n : $|\lambda| := \sum_{i=1}^{\ell} \lambda_i = n$ et $\ell(\lambda) = \ell$.

Multiplicités : $m_i = m_i(\lambda) := \#\{j | \lambda_j = i\} \geq 0$
Notation : $\lambda = 1^{m_1} 2^{m_2} \ldots$ avec $n = m_1 + 2m_2 + \cdots$

Conjuguée : λ' telle que $\lambda'_i := \#\{j | \lambda_j \geq i\}$, pour $1 \leq i \leq \lambda_1$
Alors $|\lambda'| = |\lambda|$, $\ell(\lambda') = \lambda_1$, et $m_i(\lambda) = \lambda'_i - \lambda'_{i+1}$

Symbole de Pocchammer : $(a)_k \equiv (a; q)_k := (1 - a) \ldots (1 - aq^{k-1})$

Coefficient q-binomial : $\begin{bmatrix} n \\ k \end{bmatrix}_q := \dfrac{(q)_n}{(q)_k (q)_{n-k}} \in \mathbb{N}[q]$

Théorème q-binomial fini :

$$\sum_{k=0}^{n} (-1)^k z^k q^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q = (z)_n$$

Un polynôme multivarié

Soit $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots)$ telle que $\ell(\lambda') \leq \ell$.
Pour $x = \{x_1, \ldots, x_\ell\}$ et $t \in \mathbb{C}$, on pose $x^\lambda := x_1^{m_1} \ldots x_\ell^{m_\ell}$ et

$$R_\lambda(x;t) := \prod_{i=1}^{\ell} \prod_{j=\lambda'_{i+1}}^{\lambda'_i - 1} (x_i - t^j x_{i-1})$$

Théorème q-binomial $\Rightarrow R_\lambda(x;t)$ en fonction de x^μ. De plus :

Théorème (J-Delaunay, 2012)

Pour tout entier positif ℓ et toute partition $\lambda = 1^{m_1} 2^{m_2} \ldots \ell^{m_\ell}$, on a

$$x_1^{m_1} \ldots x_\ell^{m_\ell} = \sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(q)\, R_\mu(x;q),$$

où $C_{\lambda,\mu}(q) := q^{\sum_{i=1}^{\ell} \mu'_{i+1}(\lambda'_i - \mu'_i)} \prod_{i=1}^{\ell} \begin{bmatrix} \lambda'_i - \mu'_{i+1} \\ \lambda'_i - \mu'_i \end{bmatrix}_q \in \mathbb{N}[q]$

Méthode : utilisation d'une inversion de matrices ℓ-dimensionnelles due à Schlosser (2007)

Coefficients $C_{\lambda,\,\mu}$ et fonctions symétriques

Par Lascoux (2005) : $C_{\lambda,\,\mu}(1/q) = q^{n(\mu)-n(\lambda)} Q'_{\lambda/\mu}(\mathbf{1}; q)$,
où $Q'_\lambda(x_1, \ldots, x_\ell; q)$ est le polynôme de Hall-Littlewood modifié.

Pour p premier, $C_{\lambda,\,\mu}(p)$ compte le nombre de sous-groupes de type μ dans un p-groupe abélien fini de type λ (Delsarte, 1948).
Ceci était le point de départ de la construction de l'algèbre de Hall, puis des polynômes de Hall-Littlewood.

Okounkov (1999) : définition du coefficient (q, t)-binomial $\begin{bmatrix}\lambda \\ \mu\end{bmatrix}_{q,t}$ comme quotient de valeurs spéciales des polynômes d'interpolation de Macdonald. On a en fait

$$C_{\lambda,\mu}(1/q) = \begin{bmatrix}\lambda \\ \mu\end{bmatrix}_{0,q}$$

Le théorème précédent s'avère être un cas limite d'une formule d'inversion des coefficients (q, t)-binomiaux due à Okounkov.

Propriété miroir pour $C_{\lambda,\mu}$

Par la dualité de Pontryagin, on a pour m et k entier, et λ partition de m :

$$\sum_{\substack{|\mu|=k \\ \mu\subseteq\lambda}} C_{\lambda,\,\mu}(q) = \sum_{\substack{|\mu|=m-k \\ \mu\subseteq\lambda}} C_{\lambda,\,\mu}(q).$$

Se prouve aussi en spécialisant une formule de sommation de polynômes de Hall-Littlewood due à Lascoux (2005) :

$$\sum_{\lambda}\sum_{\mu\subseteq\lambda} P_\lambda(x;q)P_\mu(y;q)b_\lambda(q)Q'_{\lambda/\mu}(\mathbf{1};q) = \prod_{i\geq 1}\frac{1}{1-x_i}\prod_{j\geq 1}\frac{1-qx_iy_j}{1-x_iy_j}$$

Généralisation par Lascoux-Rains-Warnaar (2009), dans le contexte des polynômes d'interpolation non symétriques de Macdonald :

$$\sum_{|\mu|=k}\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_{q,t}\begin{bmatrix}\mu\\ \nu\end{bmatrix}_{q,t} = \sum_{|\mu|=|\lambda|+|\nu|-k}\begin{bmatrix}\lambda\\ \mu\end{bmatrix}_{q,t}\begin{bmatrix}\mu\\ \nu\end{bmatrix}_{q,t}$$

Lien avec les heuristiques (1)

À $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ on associe le p-groupe abélien fini :

$$H_\lambda := (\mathbb{Z}/p\mathbb{Z})^{m_1} \oplus \left(\mathbb{Z}/p^2\mathbb{Z}\right)^{m_2} \oplus \cdots \oplus \left(\mathbb{Z}/p^\ell\mathbb{Z}\right)^{m_\ell}$$

Cohen-Lenstra (1984) : si $|\lambda| = m$, alors

$$\sum_{H(p^n)} \frac{|Hom_{inj}(H_\lambda, H)|}{|Aut(H)|} = \frac{1}{p^{n-m}(1/p;1/p)_{n-m}},$$

où $|Hom_{inj}(H_\lambda, H)|$ est le nombre d'homomorphismes injectifs de H_λ dans H.

Proposition (J-Delaunay, 2012)

Pour $\ell \in \mathbb{N}$, soit $\lambda = 1^{m_1} 2^{m_2} \cdots \ell^{m_\ell}$ et H un p-groupe abélien fini. Alors

$$|Hom_{inj}(H_\lambda, H)| = \prod_{i=1}^{\ell} \prod_{j=\lambda'_{i+1}}^{\lambda'_i - 1} \left(|H[p^i]| - p^j |H[p^{i-1}]|\right) := R_\lambda(H;p)$$

Lien avec les heuristiques (2)

Corollaire

Soient m entier et $|\lambda| = m$*. Alors* $\displaystyle\sum_{\mu} \frac{R_\lambda(H_\mu;p)}{|Aut H_\mu|} z^{|\mu|} = \frac{z^m}{(z/p;1/p)_\infty}$

(avec $|\mu| = n \leftrightarrow$ (H_μ d'ordre p^n) et une sommation due à Euler)

Théorème (J-Delaunay, 2012)

Pour $\ell \in \mathbb{N}$*, soit* $\lambda = 1^{m_1} \cdots \ell^{m_\ell}$ *et* $z \in \mathbb{C}$*. Alors*

$$\sum_{\mu} \frac{|H_\mu[p]|^{m_1} \cdots |H_\mu[p^\ell]|^{m_\ell}}{|Aut H_\mu|} z^{|\mu|} = \frac{1}{(z/p;1/p)_\infty} \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(p)\, z^{|\nu|} \qquad (1)$$

Théorème (J-Delaunay, 2012)

Pour $\ell \in \mathbb{N}$*, soit* $\lambda = 1^{m_1} \cdots \ell^{m_\ell}$*. Alors la u-moyenne de la fonction* $g_\lambda : H \mapsto |H[p]|^{m_1} \cdots |H[p^\ell]|^{m_\ell}$ *vaut :* $M_u(g_\lambda) = \displaystyle\sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p) p^{-|\mu| u}$*, et sa u-moyenne au sens des groupes de type S vaut :*

$$M_u^S(g_\lambda) = \sum_{\mu \subseteq \lambda} C_{\lambda,\mu}(p^2) p^{-|\mu|(2u-1)}$$

Énumération

Rappelons que $H_\lambda := (\mathbb{Z}/p\mathbb{Z})^{m_1} \oplus (\mathbb{Z}/p^2\mathbb{Z})^{m_2} \oplus \cdots \oplus (\mathbb{Z}/p^\ell\mathbb{Z})^{m_\ell}$

Cohen-Lenstra(1984) : $|Aut(H_\lambda)| = p^{\lambda_1'^2+\cdots+\lambda_\ell'^2} \prod_{j=1}^{\ell} (1/p; 1/p)_{m_j}$

Delaunay (2011) : si $G_\lambda \simeq H_\lambda \times H_\lambda$ de type S,

$$|Aut^S(G_\lambda)| = p^{2(\lambda_1'^2+\cdots+\lambda_\ell'^2)+|\lambda|} \prod_{j=1}^{\ell} (1/p^2; 1/p^2)_{m_j}$$

De plus

$H_\lambda[p^k] \simeq (\mathbb{Z}/p\mathbb{Z})^{m_1} \oplus \cdots \oplus (\mathbb{Z}/p^{k-1}\mathbb{Z})^{m_{k-1}} \oplus (\mathbb{Z}/p^k\mathbb{Z})^{\lambda_k'} \Rightarrow |H_\lambda[p^k]| = p^{\lambda_1'+\cdots+\lambda_k'}$

Donc on déduit de (1) :

$$\sum_{\mu} \frac{q^{\sum_{i\geq 1}\mu_i^2}\, q^{-m_1\mu_1-\cdots-m_\ell(\mu_1+\cdots+\mu_\ell)}}{\prod_{i\geq 1}(q)_{\mu_i'-\mu_{i+1}'}} z^{|\mu|} = \frac{1}{(zq)_\infty} \sum_{\nu\subseteq\lambda} C_{\lambda,\nu}(1/q)\, z^{|\nu|}$$

Lien avec les poynômes de Hall-Littlewood

Cette dernière identité peut s'écrire :

$$\sum_{\mu} q^{|\mu|+n(\mu)-(\lambda'|\mu')} P_\mu(z, zq\ldots; q) = \frac{1}{(zq)_\infty} \sum_{\nu\subseteq\lambda} C_{\lambda,\nu}(1/q)\, z^{|\nu|}$$

qui se démontre aussi par un cas particulier de la formule de Lascoux, originellement dû à Warnaar (2006) :

$$\sum_{\lambda,\,\mu} q^{n(\lambda)+n(\mu)-(\lambda'|\mu')} P_\lambda(x;q) P_\mu(y;q) = \prod_{i\geq 1} \frac{1}{(1-x_i)(1-y_i)} \prod_{i,j\geq 1} \frac{1-x_i y_j}{1-x_i y_j/q}$$

Cette sommation de Warnaar est une identité de type A_2 pour les fonctions de Hall-Littlewood, et fortement liée aux identités de Rogers-Ramanujan pour l'algèbre de Lie A_2, dues à Andrews-Schilling-Warnaar (1999).

Une identité combinatoire

Du résultat général sur les u-moyennes, on déduit :

Théorème (J-Delaunay, 2012)

Pour $\ell \in \mathbb{N}$, soient $\lambda = 1^{m_1} \cdots \ell^{m_\ell}$ telle que $\lambda_1 \leq \ell$, et $z \in \mathbb{C}$. Alors

$$\sum_{\mu_1 \leq \ell} \frac{z^{|\mu|} q^{2n(\mu)+|\mu|-(\lambda'|\mu')}}{\prod_{i\geq 1}(q)_{\mu'_i-\mu'_{i+1}}} (zq^{\mu'_\ell+1})_\infty = \sum_{\nu \subseteq \lambda} C_{\lambda,\nu}(1/q) z^{|\nu|} \tag{2}$$

Pour $m_1 = \cdots = m_{\ell-1} = 0$ et $m_\ell = 1$ (i.e., $\lambda = (\ell)$, partition ligne), on retrouve un résultat de Delaunay (2011) :

$$\sum_{\mu_1 \leq \ell} \frac{z^{|\mu|} q^{2n(\mu)}}{\prod_{i\geq 1}(q)_{\mu'_i-\mu'_{i+1}}} (zq^{\mu'_\ell+1})_\infty = \frac{1-z^{\ell+1}}{1-z} \tag{3}$$

Sommes-nous capables de prouver (2) via les polynômes symétriques ?

Sommation finie de polynômes de Hall-Littlewood

La réponse est oui pour (3), et non pour (2).

Théorème (J-Delaunay, 2012)

Soit $n \in \mathbb{N}^*$, et $x = \{x_1, \dots, x_n\}$ un ensemble de n variables. Alors pour tout $a \in \mathbb{C}$ tout $k \in \mathbb{N}^*$, on a

$$\sum_{\lambda \subseteq (k^n)} q^{n(\lambda)} (a; q^{-1})_{\ell(\lambda)} (a; q^{-1})_{n - m_k(\lambda)} P_\lambda(x; q)$$

$$= \sum_{I \subseteq [n]} q^{k\binom{|I|}{2}} (a; q^{-1})_{|I|} (a; q^{-1})_{n-|I|} \prod_{i \in I} x_i^k$$

$$\times \prod_{i \in I} \frac{1 - a x_i^{-1} q^{1-n}}{1 - x_i^{-1} q^{1-|I|}} \prod_{j \notin I} \frac{1 - a x_j}{1 - x_j q^{|I|}} \prod_{i \in I, j \notin I} \frac{x_i - q x_j}{x_i - x_j},$$

où la somme à gauche porte sur les partitions λ telles que $\lambda_1 \leq k$ et $\ell(\lambda) \leq n$ et $[n] := \{1, \dots, n\}$.

C'est une version finie du théorème q-binomial pour les fonctions de Hall-Littlewood, dû à Macdonald (1979) :

$$\sum_{\lambda} q^{n(\lambda)} (a; q^{-1})_{\ell(\lambda)} P_\lambda(x; q) = \prod_{i \geq 1} \frac{1 - a x_i}{1 - x_i}$$