Travaux de Manjul Bhargava

Isabelle Dubois

30 septembre 2014

Sommaire

Travaux de Manjul Bhargava

Isabelle Dubois

Sommaire

Biographie

Manjul Bhargava est un mathématicien indo-canado-américain, né en 1974.

Il soutient sa thèse en 2001, à l'université de Princeton (USA), sous la direction du célèbre Andrew Wiles (théorème de Fermat-Wiles).

Il est professeur à l'Université de Princeton depuis 2003.

Domaine de recherche - Prix

Son domaine de recherche est la théorie algébrique des nombres, en lien avec la théorie des représentations et la géométrie algébrique, tout en maîtrisant les outils analytiques de la théorie des nombres.

Il est lauréat de nombreux prix ou distinctions, dont la dernière en date est la médaille Fields, obtenue le 13 août 2014.
A noter qu'il a obtenu un prix français : le prix Fermat de recherches en Mathématiques décerné à Toulouse en 2011, pour sa contribution à la théorie des nombres.

Sommaire

Ce qu'en dit l'ICM

Texte d'introduction à la remise des prix :

Bhargava reçoit la médaille Fields "pour avoir développé des méthodes puissantes en géométrie des nombres, qu'il a appliquées au comptage des anneaux de petit rang et à la majoration du rang moyen des courbes elliptiques."

Plus précisément, "il a introduit dans sa thèse des lois de composition supérieures pour certaines formes binaires de degré au moins 3, grâce à une interprétation totalement nouvelle des travaux de Gauss sur les formes quadratiques binaires. Cette vision nouvelle lui a donné des outils de calcul effectif permettant de compter le nombre de corps de nombres de degré donné en fonction du discriminant."

Ce qu'en dit l'ICM

"Par ailleurs, il a donné une preuve simple des Théorèmes 15 et 290 de Conway sur la représentation des entiers par des formes quadratiques.

M. Bhargava a étudié ensuite certaines représentations de groupes arithmétiques intervenant dans les espaces de modules de courbes elliptiques. En collaboration avec Arul Shankar, il a alors établi que le rang des courbes elliptiques est borné en moyenne. Il a démontré la conjecture de Birch et Swinnerton-Dyer pour une proportion non nulle de courbes elliptiques sur $\mathbb{Q}$. En genre supérieur, il a aussi prouvé que la plupart des courbes hyperelliptiques de genre au moins 2 n'ont aucun point rationnel."

Sommaire

Théorèmes 15 et 290 : origines

Origines du problème :

Théorème des deux carrés (Fermat 1640-Euler 17..) :

Un entier naturel est somme de deux carrés d'entiers si et seulement si chacun de ses facteurs premiers de la forme $4k+3$ intervient à une puissance paire.

Théorème des trois carrés (Legendre 1798 - Gauss 1801) :

Un entier naturel est somme de trois carrés d'entiers si et seulement si il n'est pas de la forme $4^j(8k+7)$.

Théorème des quatre carrés (Lagrange 1770) :

Tout entier naturel est somme de quatre carrés d'entiers.

Théorèmes 15 et 290 : résultats

Généralisation : Quelles sont les formes quadratiques entières pouvant représenter tous les entiers naturels ?
(polynômes homogènes de degré 2, $\sum c_{ij}x_ix_j$, où $c, x \in \mathbb{Z}$)
Après les travaux de plusieurs mathématiciens, dont Ramanujan, on aboutit au résultat :

Théorème 15 (Conway-Schneeberger 1993, preuve non publiée - Bhargava 2000, preuve remaniée et raccourcie)

Si une forme quadratique définie positive, ayant une matrice associée à coefficients dans $\mathbb{Z}$, représente tous les entiers naturels jusqu'à 15, alors elle représente tous les entiers naturels.

Exemples : $x^2 + y^2 + z^2 + 2t^2$, $x^2 + y^2 + 2z^2 + 2t^2 + 2zt$ universelles, mais pas $x^2 + 2y^2 + 5z^2 + 5t^2$ (pas 15)
Remarque : On peut remplacer "tous les entiers naturels jusqu'à 15" par "les entiers $\{1, 2, 3, 5, 6, 7, 10, 14, 15\}$".

Théorèmes 15 et 290 : résultats

Théorème 290 (Bhargava-Hanke 2005, à paraître dans Inventiones Mathematicae - toujours non publié)

Si une forme quadratique définie positive à coefficients dans $\mathbb{Z}$ représente tous les entiers naturels jusqu'à 290, alors elle représente tous les entiers naturels.

Exemples : $x^2 + 2y^2 + 4z^2 + 31t^2 + yz - yt + 3zt$ universelle (1,5 jours de calculs), mais pas
$x^2 + 2y^2 + 4z^2 + 29t^2 + 145u^2 - xz - yz$ (pas 290)
Remarque : On peut remplacer "tous les entiers naturels jusqu'à 290" par "les entiers $\{1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290\}$".

Théorèmes 15 et 290 : idées

Les preuves des ces deux théorèmes reposent sur les éléments suivant :

- Théorème 15, preuve assez élémentaire :
  Notions de réseaux (associés à une forme), de nombre "absent", du procédé d'"escalade de réseaux" consistant à construire un réseau à partir d'un réseau non universel et d'un vecteur dont la norme est un nombre "absent". Ces chaînes de réseaux sont en nombre fini (à isométrie près) et s'arrêtent à la dimension 5 (5 variables au plus pour la forme associée). Notion de genre d'une forme quadratique (classes d'équivalence de formes sur $\mathbb{Z}_p$).

  Il existe 201 formes quaternaires universelles à matrice entière.

Théorèmes 15 et 290 : idées

- Théorème 290, mêmes idées de départ que pour 15 mais preuve plus complexe, outils analytiques supplémentaires : entiers représentables localement par une forme (c'est-à-dire mod p^α pour tout α), bornes effectives pour les coefficients de la forme modulaire associée à une forme quadratique (fonction théta), calculs plus longs et plus complexes, on s'arrête à la dimension 7.

  Il existe 6436 formes quaternaires universelles.

Lois de composition supérieures : origines

Loi de composition de Gauss, Disquisitiones Arithmeticae, 1801 :

Objets : formes quadratiques binaires entières et primitives, $f(x, y) = ax^2 + bxy + cy^2$, $a, b, c \in \mathbb{Z}$, $pgcd(a, b, c) = 1$.
Action du groupe $SL_2(\mathbb{Z})$: $(Af)(x, y) = f((x, y)A)$.
On définit une loi de composition $f_1 * f_2$ lorsque f_1 et f_2 ont même discriminant Δ.
Cette loi est une loi de groupe abélien fini sur l'ensemble $\mathcal{C}l(\Delta)$ des classes d'équivalence de formes de même discriminant.

En langage moderne : On obtient une bijection entre les orbites de formes quadratiques munies d'une loi de groupe, $\mathcal{C}l(\Delta)$, et le groupe de classes restreint de l'unique anneau quadratique $O(\Delta)$ de discriminant Δ, $\mathcal{C}l^+(O(\Delta))$.

Lois de composition supérieures : résultats

Bhargava propose une nouvelle vision de la loi de composition de Gauss, conduisant à des généralisations, appelées lois de composition supérieures.
Première étape de généralisation : généralisation de la loi de composition de Gauss à des lois de composition sur des espaces de cubes, dont les groupes sont reliés à des groupes de classes d'anneaux quadratiques.
Deuxième étape de généralisation : généralisation à des lois de composition sur d'autres espaces de formes, dont les groupes sont reliés à des groupes de classes d'anneaux de rang supérieur (jusqu'au rang 5).

Lois de composition supérieures : résultats

Lois de composition supérieures de Bhargava, Higher composition laws I à IV, 2001 à 2008 (V ?) :

Objets d'étude : $V_{\mathbb{Z}}$, espaces de formes (k-iques n-aires) ou plus généraux,
Action de groupe : $G_{\mathbb{Z}} = SL_2(\mathbb{Z})$, ou produit de tels groupes, ou plus général,
Paramétrisation des formes suivant des invariants polynômiaux : discriminant ou ses généralisations,
Groupes étudiés : orbites $G_{\mathbb{Z}} \backslash V_{\mathbb{Z}}$, loi de groupe : loi de composition supérieure,
Bijections : ces groupes sont reliés à des anneaux de nombres algébriques.

Lois de composition supérieures : résultats

Bhargava définit ainsi 14 lois de composition supérieures (dont celle de Gauss).

Exemple : $V =$ ensemble des paires (A, B) de formes quadratiques ternaires entières, $G = GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$,
les orbites sont en bijection avec les classes d'isomorphismes de paires (Q, R) où Q est un anneau quartique et R un anneau cubique associé à Q,
Invariant :
$Disc(A, B) := Disc(4Det(Ax + By)) = Disc(Q) = Disc(R)$.

Toutes les lois, ici.

Lois de composition supérieures : idée de départ

Pour la petite histoire, Bhargava se serait inspiré du Rubik's cube pour retrouver la loi de composition de Gauss, et en déduire ses généralisations.

"The story of the cube", ici.

Lois de composition supérieures : applications

Quelques applications obtenues (moyennant également des techniques de comptage de la géométrie des nombres) :

- Preuve de l'heuristique de Cohen-Martinet : estimation de la taille moyenne du sous-groupe de 2-torsion du groupe de classes de corps cubiques.
- Généralisation des estimations de Davenport-Heilbronn : nombre moyen de corps de nombres de degré n ayant pour groupe de Galois S_n (clôture galoisienne) :
  $c_n = \lim_{X \to +\infty} \frac{\#\{S_n\text{−corps de nombres de deg } n, \text{ de disc} \leq X\}}{X}$
  Résultats déjà connus : n=1,2,3. Bhargava : n=4, n=5.
  Par exemple,
  $c_4 = \frac{5\zeta(2)^2\zeta(3)}{24\zeta(5)} = \frac{5}{24}\prod_p(1 + p^{-2} - p^{-3} - p^{-4}) \simeq 0.253\ldots$

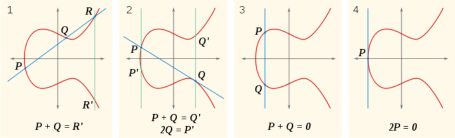
Quelques perspectives : liens avec groupes de Lie exceptionnels, paramétrisations d'anneaux commutatifs de rang >5, extensions aux anneaux non commutatifs.

Rang de courbes elliptiques : origines

Origines du problème :

Soit E une courbe elliptique sur $\mathbb{Q}$, donnée par l'équation $y^2 = x^3 + Ax + B$, avec $4A^3 + 27B^2 \neq 0$.

On définit sur E une loi de groupe par la méthode des sécantes-tangentes, conservant les points rationnels :



Théorème de Mordell (1922-23) :

Le groupe $E(\mathbb{Q})$ des points rationnels sur une courbe elliptique est un groupe abélien de type fini.

Ainsi $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$, où r est le rang de E et T son sous-groupe (fini) de torsion.

Rang de courbes elliptiques : origines

Il est très difficile de connaître le rang d'une courbe elliptique en général, même s'il existe des algorithmes qui fonctionnent si A et B sont de taille modérée.
Que peut valoir le rang en moyenne ? D'ailleurs, cette "moyenne" existe-t-elle ?

Résultats, sous les conjectures GRH et BSD :

Le rang moyen de toutes les courbes elliptiques, ordonnées suivant leur hauteur, est fini et borné par :
2.3 (Brumer 1992), 2 (Heath-Brown 2004), 1.79 (Young 2006)

Conjecture de Birch et Swinnerton-Dyer (1965), "Millennium Problem" du Clay Institute :

$$r = r_{an} := ord_{s=1} L(E, s)$$

Rang de courbes elliptiques : résultats

Théorème (Bhargava-Shankar 24/12/2013) :

Le rang moyen de toutes les courbes elliptiques, ordonnées suivant leur hauteur, est au plus égal à 1.5.

Théorème (Bhargava-Shankar 25/12/2013) :

Les courbes elliptiques étant ordonnées suivant leur hauteur, une proportion strictement positive d'entre elles :

- ont un rang nul.
- ont un rang analytique nul.
- satisfont la conjecture BSD.

Remarques : Les deux derniers résultats reposent sur un travail récent de Skinner et Urban sur la Conjecture principale d'Iwasawa pour GL_2. Le 31/12/2013, il est prouvé que le rang moyen est < 0.885.

Rang de courbes elliptiques : résultats

Derniers résultats connus !

Théorème (Bhargava-Skinner-Zhang 18/07/2014) :

Les courbes elliptiques étant ordonnées suivant leur hauteur :

- au moins 66.48% satisfont la conjecture BSD.
- au moins 16.5% (resp. 20.68%) ont un rang algébrique et analytique égal à 0 (resp. 1).
- le rang moyen est au moins égal à 0.2068.

Rang de courbes elliptiques : idées

Voici quelques éléments intervenant dans les démonstrations du premier théorème :

- On étudie le 2-groupe de Selmer, fini d'ordre 2^s, défini par :

$$0 \to \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to Sel_2(E) \to Ш_E[2] \to 0$$

- A chaque élément de $Sel_2(E)$ on associe une forme quartique binaire entière d'invariants $(I, J) = (-48A, -1728B)$ (Birch et Swinnerton-Dyer),
- On compte en moyenne le nombre de classes de formes quartiques binaires d'invariants (I, J) sous l'action du groupe $GL_2(\mathbb{Z})$ (est fonction de $\zeta(2)$),
- On en déduit qu'en moyenne le cardinal de $Sel_2(E)$ est égal à 3, et donc que s est en moyenne au plus égal à 1.5.

Rang de courbes elliptiques : idées

A noter que l'on retrouve aussi le comptage des orbites de paires de formes quadratiques ternaires sous l'action de $GL_2(\mathbb{Z}) \times SL_3(\mathbb{Z})$.

Les résultats suivants s'appuient sur l'étude des p-groupes de Selmer pour $p = 3$ et 5 et font intervenir les formes cubiques ternaires ($p = 3$) et des quintuples de formes alternées quinaires ($p = 5$).

D'autre part, comme pour les applications au comptage de corps de nombres, Bhargava utilise des techniques de la géométrie des nombres, à savoir le comptage de points entiers dans diverses composantes de domaines fondamentaux en termes de volumes. Et ces méthodes sont au coeur des démonstrations !

Le mot de la fin

Merci de votre attention !