LES TRAVAUX DE M. BHARGAVA

par

Karim Belabas & Christophe Delaunay

Manjul Bhargava a reçu la médaille Fields au congrès international de Séoul «pour avoir développé de nouvelles méthodes en géométrie des nombres, qu'il a appliquées au comptage des anneaux de petit rang et pour borner le rang moyen de courbes elliptiques». Cet article est un survol d'une partie de ses travaux.

1. Lois de composition et comptages de discriminants

Commençons par rappeler une construction remontant aux *Disquisitiones*. Étant donnée une forme quadratique binaire $f(x, y) = ax^2 + bxy + cy^2$ à coefficients entiers, Gauss s'intéresse aux entiers représentables par cette forme, c'est-à-dire $\{f(\mathbf{v})\colon \mathbf{v} \in \mathbb{Z}^2\}$. Le célèbre exemple des entiers sommes de deux carrés correspond à $f(x, y) = x^2 + y^2$; il est résolu par Fermat puis Euler en se ramenant au cas des premiers représentables (2 et les premiers $p \equiv 1 \pmod 4$), à l'aide d'une propriété de multiplicativité (un produit de sommes de 2 carrés est somme de 2 carrés). Gauss remarque que, si $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ est une matrice entière de déterminant ± 1, alors $\mathbf{v} \mapsto \mathbf{v}\gamma$ est une bijection de $\mathbb{Z}^2$ et la forme $(\gamma \cdot f)$ définie par

$$(\gamma \cdot f)(\mathbf{v}) := f(\mathbf{v}\gamma)$$

représente les mêmes entiers que f. Le discriminant $D(f) = b^2 - 4ac$ de f est commun à tous les éléments de $\mathrm{GL}_2(\mathbb{Z}) \cdot f$ et il est tout aussi remarquable que, si l'on fixe un discriminant, il n'existe qu'un nombre *fini* d'orbites ; par exemple, pour $D = -4$, il n'y a qu'une seule orbite,

celle de x^2+y^2. À discriminant fixé, il n'y a donc qu'un nombre fini de problèmes de classification d'entiers représentables, un par orbite sous $\mathrm{GL}_2(\mathbb{Z})$.
Pour aller plus loin, il faut généraliser la multiplicativité des sommes de deux carrés. Gauss parvient à décrire toutes les identités de la forme

$$(a_1x_1^2+b_1x_1y_1+c_1y_1^2)(a_2x_2^2+b_2x_2y_2+c_2y_2^2)=(a_3x_3^2+b_3x_3y_3+c_3y_3^2),$$

où les trois formes quadratiques ont même discriminant et (x_3,y_3) sont deux fonctions bilinéaires à coefficients entiers de (x_1,y_1) et (x_2,y_2). Par exemple $(x_1^2+dy_1^2)(x_2^2+dy_2^2)=(x_3^2+dy_3^2)$, avec

$$(x_3,y_3):=(x_1x_2+dy_1y_2,\ x_1y_2-y_1x_2),$$

pour le discriminant $-4d$. Mais un nouveau phénomène apparaît : contrairement à l'exemple ci-dessus, l'identité obtenue mélange en général des formes de différentes orbites !

La théorie est plus riche en se limitant aux formes *primitives* [1], telles que $\mathrm{pgcd}(a,b,c)=1$, et en considérant plutôt les orbites pour le sous-groupe $\mathrm{SL}_2(\mathbb{Z})$ des matrices de déterminant 1. Voici le résultat :

***Théorème 1* (composition de Gauss).** — *Soit* $D\equiv 0,1 \pmod 4$. *L'ensemble des* $\mathrm{SL}_2(\mathbb{Z})$*-orbites de formes quadratiques binaires primitives de discriminant* D *possède une structure naturelle de* groupe abélien fini.

L'exemple qui précède le théorème conduit ainsi à décréter que la classe de x^2+dy^2 est l'élément neutre du groupe obtenu pour $D=-4d$.

La loi de groupe est explicite, donnée par des formules algébriques, mais reste obscure sous cette forme. Elle ne fut éclaircie qu'après réinterprétation par Dedekind, et en particulier l'introduction de la théorie des idéaux. En termes modernes, ce groupe est le groupe des classes (orientées) de l'anneau quadratique $Q(D)$ de discriminant D. Pour simplifier [2],

1. Cette propriété est invariante sous l'action de $\mathrm{GL}_2(\mathbb{Z})$.

2. En trahissant l'esprit de Bhargava, qui porte une grande attention aux cas dégénérés et évite justement ce type de réductions à un cadre générique ; ici en introduisant la notion d'orientation (ou, de façon équivalente, de classes au sens restreint), au prix de complications techniques. Pour les formes définies, la simplification est vénielle : le groupe des classes orientées est un produit de deux copies du sous-groupe d'indice 2 que nous considérons. Pour le cas général, voir [**Bha04a**].

restreignons nous au sous-ensemble formé des formes définies positives, de discriminant $D < 0$. Dans ce cas

$$Q(D) := \mathbb{Z}[x]/(x^2 - Dx + (D^2 - D)/4) \simeq \mathbb{Z}[(D + \sqrt{D})/2],$$

et soit $K = \mathbb{Q}(\sqrt{D})$ son corps des fractions. La multiplication de K induit sur l'ensemble des sous-Q-modules I de rang 1 de K (idéaux fractionnaires) une multiplication naturelle, de neutre Q ; s'il existe I' tel que $II' = Q$, I est dit inversible. Les isomorphismes de Q-modules partitionnent naturellement cet ensemble en classes (d'idéaux) : $I_1 \sim I_2$ s'il existe $\kappa \in K^*$ tel que $I_1 = \kappa I_2$.

Théorème 2 **(composition de Gauss, version 2)**
Il y a une bijection canonique entre les $\mathrm{SL}_2(\mathbb{Z})$*-orbites de formes quadratiques binaires définies positives et l'ensemble des classes d'isomorphismes de paires* (Q, I)*, où* Q *est un anneau quadratique de discriminant* < 0 *et* I *est une classe d'idéaux de* Q*.*
Les formes primitives *de discriminant* D *sont associées aux idéaux inversibles de* $Q(D)$ *et forment un groupe abélien.*

La bijection est explicite : si $I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z}$, où la $\mathbb{Z}$-base est orientée [3] telle que, dans le produit alterné $\wedge^2 Q \simeq \mathbb{Z}$,

$$\alpha_1 \wedge \alpha_2 = \lambda(1 \wedge \sqrt{D}), \quad \lambda \in \mathbb{Q}^+;$$

alors la classe de I a pour image la classe de la partie primitive de

$$N_{K/\mathbb{Q}}(\alpha_1 x + \alpha_2 y),$$

où on définit $N_{K/\mathbb{Q}}(a + b\sqrt{D}) := a^2 - Db^2$ pour $a, b \in \mathbb{Q}$. Mieux, chaque classe de forme quadratiques $ax^2 + bxy + cy^2$ contient une *unique* forme telle que $|b| \leq a \leq c$ et $b \geq 0$ si l'une des inégalités est une égalité. On peut donc choisir dans chaque classe de formes (ou d'idéaux) un représentant canonique, et manipuler ou compter des classes d'idéaux en calculant au moyen de formes quadratiques, vues comme points entiers dans ce domaine fondamental $\mathcal{F} \subset \mathbb{R}^3$. De plus, si on fixe $K = \mathbb{Q}(\sqrt{D})$ et que l'on choisit un anneau quadratique $Q \subset K$ maximal pour la relation

3. Sans ce choix d'orientation, la base serait définie modulo $\mathrm{GL}_2(\mathbb{Z})$ et non plus $\mathrm{SL}_2(\mathbb{Z})$, induisant une correspondance avec les classes de formes quadratiques binaires modulo $\mathrm{GL}_2(\mathbb{Z})$. Si (α_1, α_2) est une $\mathbb{Z}$-base arbitraire de I, alors (α_1, α_2) ou (α_2, α_1) est correctement orientée.

d'inclusion, par exemple si D est sans facteurs carrés [4], il se produit un petit miracle : tous les idéaux de Q sont inversibles (toutes les formes quadratiques de discriminant D sont primitives).

Les premiers travaux de Bhargava, dans sa thèse, sont consacrés à la généralisation de cette construction de Gauss. Plus précisément, on a vu apparaître un groupe arithmétique $G = \mathrm{SL}_2$, une représentation V définie sur $\mathbb{Z}$ (l'ensemble des formes quadratiques), tels que l'ensemble des orbites entières $G(\mathbb{Z}) \setminus V(\mathbb{Z})$ paramètre les classes d'idéaux des anneaux quadratiques. Bhargava a plus généralement cherché à paramétrer les *anneaux de rang n* (anneaux commutatifs, libres de rang n comme $\mathbb{Z}$-modules) et leurs idéaux.
Ces anneaux très simples forment un cadre naturel pour la définition usuelle du discriminant : si A est un anneau de rang n et $\alpha \in A$, on définit la trace de α, $\mathrm{Tr}(\alpha)$, comme étant la trace de la multiplication par α : $m_\alpha : A \to A$; on note $\mathrm{disc}(A)$ le déterminant $\det(\mathrm{Tr}(\alpha_i\alpha_j))$, pour une $\mathbb{Z}$-base $(\alpha_1, \ldots, \alpha_n)$ arbitraire de A. Les anneaux de discriminant 0 sont dits *dégénérés*. Dans le cas quadratique, on retrouve bien $\mathrm{disc}(Q(D)) = D$, et $\mathbb{Z}[x]/(x^2)$ est l'unique anneau dégénéré, à isomorphisme près.

Parmi ces anneaux, la théorie algébrique des nombres privilégie les anneaux de Dedekind (intègres, maximaux pour la relation d'inclusion dans leur corps des fractions), qui sont les bons analogues des entiers naturels dans leur corps des fractions ; en particulier le miracle vu plus haut se reproduit : tous les idéaux fractionnaires sont inversibles et forment donc un groupe. En fait, pour toute extension finie de corps $K/\mathbb{Q}$, $\dim_{\mathbb{Q}} K = n$, il existe un unique anneau de Dedekind $\mathbb{Z}_K \subset K$: le sous-anneau de nombre de rang n de K maximal pour l'inclusion, donc, et on notera $\mathrm{disc}\, K := \mathrm{disc}\, \mathbb{Z}_K$. De plus les classes d'idéaux fractionnaires (sous-$\mathbb{Z}_K$-modules de K de rang 1 modulo isomorphisme de $\mathbb{Z}_K$-modules) forment encore un groupe abélien fini, le groupe des classes de K, noté $\mathrm{Cl}(K)$.
Mais la classe des anneaux de petit rang contient tout aussi bien des anneaux comme $\mathbb{Z}[x]/(x^2)$ ou $\mathbb{Z}[x, y]/(x^2, xy, y^2)$ (respectivement de rangs 2 et 3, tous deux dégénérés), ou $\mathbb{Z}[x]/(x^2 + x)$ (non intègre), ou $\mathbb{Z}[\sqrt{5}]$ (non maximal dans son corps de fractions $\mathbb{Q}(\sqrt{5})$, puisqu'il est inclus

4. La condition nécessaire et suffisante est «$p^2 \nmid D$ pour p premier impair et $D \not\equiv 0, 4 \pmod{16}$».

dans $\mathbb{Z}[(1+\sqrt{5})/2]$). Il n'est pas nécessaire de se restreindre aux anneaux de Dedekind : les idéaux fractionnaires *inversibles* des anneaux non dégénérés ont de bonnes propriétés.

Où chercher d'autres couples (G, V) paramétrant ainsi des anneaux de petit rang ? Si possible tels que l'action de $G(\mathbb{Z})$ admette un invariant polynomial D, analogue au discriminant des formes quadratiques binaires ? Un cadre naturel est celui des *espaces vectoriels préhomogènes*, tels que l'action de $G(\mathbb{C})$ sur $V(\mathbb{C})$ admette une orbite Zariski-dense, c'est-à-dire dont le complémentaire S est un ensemble algébrique (par exemple une hypersurface $D = 0$). Heuristiquement, le lien est clair : après changement de base à $\mathbb{C}$, il ne doit plus rester qu'une orbite non dégénérée, puisqu'il n'existe qu'un seul anneau A de rang n non dégénéré et un seul A-module I inversible de rang 1 ($A = I = \mathbb{C}^n$) ; donc un seul objet à paramétrer.
Ces espaces, introduits par Sato dans les années 70 avec de toutes autres motivations, ont été classifiés par Sato et Kimura **[SK77]** modulo des transformations naturelles : il y en a essentiellement 36 types différents. Wright et Yukie **[WY92]** les avaient déjà étudiés sur un corps k dans le but explicite d'obtenir des paramétrisations et avaient montré que les $G(k)$-orbites non dégénérées de $(V - S)(k)$ paramétraient souvent des extensions de corps K/k ; et donc pourraient permettre de compter ces extensions (avec la restriction importante $[K : k] \leq 5$, imposée par la classification de Sato-Kimura). Bhargava a été le premier à s'intéresser systématiquement à leurs orbites entières, et à l'ensemble des objets, «dégénérés» ou non, qu'elles paramètrent. Ce qui lui permettra en particulier de réaliser le programme de compter les extensions $K/\mathbb{Q}$, $[K : \mathbb{Q}] \leq 5$, en s'inspirant du résultat connu pour les anneaux cubiques :

Théorème 3 **(Levi [Lev14], Gan-Gross-Savin [GGS02])**
Il y a une bijection entre les ensembles suivants :
- *les classes d'isomorphismes d'anneaux cubiques,*
- *les formes cubiques binaires entières modulo l'action de* $\mathrm{GL}_2(\mathbb{Z})$.

Les analogues quartiques et quintiques sont donnés par les théorèmes suivants :

Théorème 4 **(Bhargava [Bha04c])**. — *Il y a une bijection entre les ensembles suivants :*
- *les paires de formes quadratiques entières en 3 variables modulo l'action de* $\mathrm{GL}_2(\mathbb{Z}) \times \mathrm{GL}_3(\mathbb{Z})$ *;*

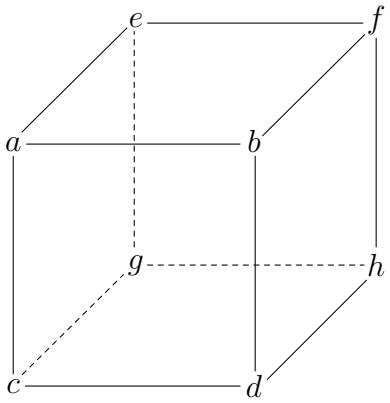
— *les classes d'isomorphismes de couples* (Q, R)*, où* Q *est un anneau quartique et* R *une résolvante cubique*[5] *de* Q*.*

Théorème 5 **(Bhargava [Bha10])**. — *Il y a une bijection entre les ensembles suivants :*

— *les quadruplets de 2-formes alternées entières de rang* 5 *(*$\mathbb{Z}^4 \otimes \Lambda^2\mathbb{Z}^5$*), entières modulo l'action de* $\mathrm{GL}_4(\mathbb{Z}) \times \mathrm{SL}_5(\mathbb{Z})$ *;*

— *les classes d'isomorphismes de couples* (Q, R)*, où* Q *est un anneau quintique et* R *une résolvante sextique*[6] *de* Q*.*

Ce sont les paramétrisations de ce type qui ont les conséquences les plus spectaculaires, mais Bhargava en obtient bien d'autres, pour quasiment tous les types de Sato-Kimura. Certaines admettent de nouvelles lois de composition comme la «loi du cube» : si on étiquette les 8 sommets d'un cube A par des entiers



on peut le partitioner en deux matrices 2×2 de trois façons différentes : $M_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, $N_1 = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)$, ou $M_2 = \left(\begin{smallmatrix} a & c \\ e & g \end{smallmatrix}\right)$, $N_2 = \left(\begin{smallmatrix} b & d \\ f & h \end{smallmatrix}\right)$, ou encore $M_3 = \left(\begin{smallmatrix} a & e \\ b & f \end{smallmatrix}\right)$, $N_3 = \left(\begin{smallmatrix} c & g \\ d & h \end{smallmatrix}\right)$; pour chacun de ces découpages, on construit une forme quadratique entière $Q_i(x, y) = -\det(M_i x + N_i y)$.

5. Une résolvante cubique de Q est un anneau cubique R muni d'une certaine application naturelle $Q \to R$; tous les anneaux quartiques admettent une résolvante cubique, les anneaux quartiques maximaux n'en admettent qu'une : dans ce cas on peut oublier la résolvante R.

6. Un anneau R de rang 6 muni d'une certaine application naturelle $Q \to \Lambda^2 R$; de nouveau, tous les anneaux quintiques admettent une telle résolvante et les anneaux maximaux n'en admettent qu'une.

***Théorème 6* (Bhargava [Bha04a]).** — *Si un cube A produit trois formes quadratiques primitives alors elles ont même discriminant et leur produit pour la composition de Gauss est le neutre. Réciproquement, si le produit de trois formes quadratiques primitives est le neutre, il existe un cube A permettant de les obtenir par la recette ci-dessus.*

Ce résultat est associé à la représentation standard $V(\mathbb{Z}) = \mathbb{Z}^2 \otimes \mathbb{Z}^2 \otimes \mathbb{Z}^2$ de $G(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$ et s'interprète lui aussi en termes de groupes de classes d'idéaux (inversibles) d'anneaux quadratiques. D'autres lois de composition sont associées aux pavés $2 \times 2 \times 3$ et aux groupes de classes d'anneaux cubiques [**Bha04b**]. On pourra trouver dans [**Bel05**] un survol plus détaillé de ces paramétrisations.

Outre l'intérêt algébrique intrinsèque de ces paramétrisations et lois de composition issues de représentations préhomogènes (G, V), on peut maintenant obtenir des résultats de comptage asymptotique des orbites non dégénérées de discriminant borné. On rentre dans un cadre classique en géométrie des nombres : le décompte de points entiers dans des domaines décrits par des inégalités polynomiales. L'analogue des conditions géométriques $|b| \leq a \leq c$ du domaine fondamental $\mathcal{F}$ de Gauss et des conditions de signe (formes définies positives) devient une étude des composantes connexes d'un domaine fondamental pour $G(\mathbb{Z}) \setminus (V - S)(\mathbb{R})$.

- Pour peu que les domaines fondamentaux obtenus soient suffisamment réguliers, et de volume euclidien fini, leur nombre de points entiers est bien approché par leur volume, avec un terme d'erreur dépendant de la régularité du bord. On sait déjà que leur bord n'est pas trop sauvage : ces ensembles sont définis par des inégalités polynomiales ; par contre, il ne faudrait pas qu'il y ait des «pointes» ou «tentacules» qui bien que de volume négligeable (ensembles de codimension > 0) contiendraient beaucoup de points entiers.
- Les conditions arithmétiques de primitivité, ou de restriction aux idéaux inversibles, deviennent des conditions de congruence. Ce qui devrait se traduire par l'apparition d'un produit eulérien de densités locales devant le terme volume. Typiquement, compter des n-uplets primitifs dans $\mathbb{Z}^n$ devrait se traduire par l'apparition d'un facteur $\prod_p (1 - p^{-n}) = \frac{1}{\zeta(n)}$. Pour peu que l'on maîtrise l'effet de ces conditions arithmétiques sur les termes d'erreur !

— Si on désire compter les corps de nombres K ordonnés par discriminant, il suffit de compter leurs anneaux d'entiers $\mathbb{Z}_K$, c'est-à-dire des anneaux intègres et maximaux. La condition de maximalité est locale, analogue aux congruences du point précédent.
— Il faut espérer que les points entiers qui ne nous intéressent pas mais ne sont pas exclus par des conditions de congruence, par exemple associés à des anneaux non-intègres, soient en nombre négligeable dans ces domaines.

Un théorème de Minkowski énonce qu'à isomorphisme près le nombre de corps de nombres $N_n(X)$ de degré n et de discriminant borné par X est fini. Une conjecture du folklore prédit que, pour tout $n > 1$, il existe $c_n > 0$ tel que $N_n(X) \sim c_n X$, pour $X \to \infty$. (Des conjectures plus précises ont été proposées, remplaçant $\mathbb{Q}$ par une base plus générale, et fixant la clôture galoisienne ou des conditions locales.)
Le cas $n = 2$ est immédiat. Le cas $n = 3$, dû à Davenport et Heilbronn [**DH71**], est nettement plus ardu et nécessite déjà une paramétrisation des anneaux cubiques maximaux (mal comprise à l'époque) et une étude fine d'un domaine fondamental non compact dans $\mathbb{R}^4$.

Théorème 7. — *On a* $N_3(X) \sim \dfrac{X}{3\zeta(3)}$, *pour* $X \to \infty$.

(En collaboration avec Shankar et Tsimermann, Bhargava a précisé ce résultat dans [**BST13**] en donnant un second terme principal, démontrant une conjecture de Roberts.)
Entre 2004 et 2009, Bhargava à démontré cette conjecture pour les cas $n = 4$ et $n = 5$, les derniers qu'on pouvait espérer traiter par ces paramétrisations préhomogènes (d'après la classification de Sato-Kimura).

Théorème 8 **([Bha05, Bha10])**. — *Pour* $n = 4$ *ou* $n = 5$, *on a* $N_n(X) \sim c_n X$ *pour des constantes* c_4 *et* c_5 *explicites.*

Ces résultats sont des tours de forces techniques : les domaines fondamentaux à étudier vivent respectivement dans $\mathbb{R}^{12}$ et $\mathbb{R}^{40}$, et ont une géométrie compliquée, incluant de nombreuses «pointes» qu'il faut comprendre une à une : on ne peux pas estimer le nombre de leurs points entiers par leur volume. Il se passe plusieurs miracles à ce niveau : la majorité des pointes contient $o(X)$ points entiers ; à une exception près, les autres correspondent à des anneaux non intègres. L'exception se produit pour $n = 4$, où une pointe contient de l'ordre de X anneaux intègres dont le corps de fractions est de groupe de Galois D_4, le groupe dihédral

d'ordre 8, plus $o(X)$ autres points. Un résultat de Cohen, Diaz y Diaz et Olivier, obtenu par théorie du corps de classes, permet de compter indépendamment ces corps, et donc de ne pas tenir compte de cette dernière pointe !

2. Points rationnels sur les courbes (hyper)-elliptiques

Plus récemment, Bhargava, en collaboration avez Shankar, s'est détourné des représentations préhomogènes pour paramétrer et comprendre des structures ne se réduisant pas à un seul objet par changement de base sur $\mathbb{C}$. Ils ont obtenu des résultats très forts et remarquables sur le comportement du rang des courbes elliptiques. Une courbe elliptique E définie sur le corps des nombres rationnels $\mathbb{Q}$ est une courbe définie par une équation de la forme $E\colon y^2 = x^3 + ax + b$ où $a, b \in \mathbb{Q}$ sont fixés et vérifient $4a^3 + 27b^2 \neq 0$. Cette dernière inégalité est équivalente au fait que la courbe E est lisse et en particulier, qu'elle admet des tangentes en tous ses points. L'ensemble des points $\mathbb{Q}$-rationnels de E est alors

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \colon y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Le point $\mathcal{O}$, appelé « point à l'infini », provient naturellement de l'homogénéisation de l'équation vue dans l'espace projectif. Les courbes elliptiques font l'objet d'études intensives depuis de nombreuses décennies. Par exemple, il est particulièrement intéressant de chercher à comprendre l'ensemble de leurs points rationnels, i.e., les solutions des équations diophantiennes sous-jacentes. En effet, on classifie les courbes (lisses) suivant leur genre $g \in \mathbb{N}$. Ce nombre mesure en quelque sorte la complexité arithmétique de la courbe (pour les courbes définies sur $\mathbb{C}$, il s'agit du genre analytique qui compte le nombre de trous). Dans le cas du genre 0, on sait décrire explicitement l'ensemble de leurs points rationnels assez facilement. Pour $g \geq 2$, le théorème de Faltings affirme qu'il n'existe qu'un nombre fini de points rationnels sur les courbes de genre ≥ 2 (mais il peut être délicat de donner la liste de ces points). Pour le genre 1, toutes les situations peuvent arriver : aucun point, un nombre fini ou un nombre infini de points rationnels. Les courbes elliptiques sont en fait des courbes de genre 1 possédant au moins un point rationnel : on s'intéresse alors à cet ensemble non vide $E(\mathbb{Q})$.

D'autre part, les courbes elliptiques fournissent des exemples fondamentaux de groupes algébriques. Si $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ sont deux points de $E(\mathbb{Q})$, alors la droite (PQ) recoupe la courbe en un troisième

point $R = (x_R, y_R)$, on définit alors $P + Q$ comme l'opposé (pour la loi de groupe que l'on est en train de définir) du point R qui est le point $(x_R, -y_R)$. Pour doubler un point P, il suffit de prendre la tangente à la courbe en ce point qui recoupe la courbe en l'opposé de $2P = P + P$. Le fait remarquable est que cette opération munit $E(\mathbb{Q})$ d'une structure de groupe abélien dont le neutre est le point $\mathcal{O}$; trois points P, Q et R sur la courbe sont alignés si et seulement $P + Q + R = \mathcal{O}$ (ce qui a motivé la «loi du cube» vue en première partie). D'autre part, cette loi de groupe respecte le caractère algébrique des points : si P et Q ont des coordonnées rationnelles alors $P+Q$ a aussi des coordonnées rationnelles. Le théorème crucial suivant précise la structure de $E(\mathbb{Q})$.

Théorème 9 **(Théorème de Mordell-Weil)**. — *Le groupe $E(\mathbb{Q})$ est un groupe abélien de type fini, i.e., il existe $r \in \mathbb{N}$, il existe $G_1, \cdots, G_r \in E(\mathbb{Q})$ et il existe un sous-groupe fini $E(\mathbb{Q})_{\text{tors}}$ tels que :*

$$E(\mathbb{Q}) = \langle G_1 \rangle \oplus \cdots \oplus \langle G_r \rangle \oplus E(\mathbb{Q})_{\text{tors}}.$$

Résoudre l'équation diophantienne sous-jacente à E revient donc à déterminer le rang r, dit rang du groupe de Mordell-Weil, des générateurs et le sous-groupe de torsion $E(\mathbb{Q})_{\text{tors}}$. En particulier, $E(\mathbb{Q})$ peut être décrit à l'aide d'un nombre fini de points rationnels. À ce jour, il n'existe pas d'algorithme pour calculer l'entier r et trouver des générateurs en général. En revanche, la torsion d'une courbe elliptique est parfaitement bien comprise : elle s'explicite facilement et le théorème de Mazur affirme que le sous-groupe de torsion est toujours d'ordre inférieur à 16. Outre la résolution de l'équation diophantienne, il existe de nombreuses questions ouvertes sur les courbes elliptiques. Les travaux récents et tout à fait innovants de Bhargava et Shankar portent sur la question délicate du comportement du rang et ont des conséquences importantes sur certaines de ces questions ouvertes.

En fait, même s'il n'existe pas d'algorithme pour déterminer le rang et un système de générateurs d'une courbe elliptique, il existe un procédé théorique qui fonctionne assez bien en général. Pour cela, on associe à une courbe elliptique E définie sur $\mathbb{Q}$, son groupe de Tate-Shafarevich, $Ш(E)$. D'autre part, pour tout entier $n \in \mathbb{N}$, on peut définir le n-groupe de Selmer de E, $\text{Sel}_n(E)$; c'est un groupe fini et (théoriquement) calculable. On a alors la suite exacte suivante :

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \text{Sel}_n(E) \longrightarrow Ш(E)[n] \longrightarrow 0.$$

Il n'est pas question de donner une définition rigoureuse des groupes de Tate-Shafarevich et des n-groupes de Selmer. Intuitivement, le n-groupe de Selmer est constitué de certaines courbes $\mathcal{C}$ (de genre 1) qui possèdent des points partout localement i.e. qui possèdent un point défini sur $\mathbb{R}$ et un point défini sur les corps [7] $\mathbb{Q}_p$ pour tout nombre premier p. Les éléments de $Ш(E)[n]$ sont les courbes $\mathcal{C}$ de $\mathrm{Sel}_n(E)$ qui n'ont pas de point rationnel. Ainsi, le groupe $Ш(E)[n]$ mesure en quelque sorte l'obstruction à ce que les objets ayant des points partout localement aient un point global i.e. rationnel.
Si $Ш(E)[n] = \{0\}$ alors comme $\mathrm{Sel}_n(E)$ est calculable, on en déduit le rang (et un ensemble de générateurs). Cependant, il n'y a aucune raison d'avoir $Ш(E)[n] = \{0\}$ pour un n a priori mais on fait la conjecture suivante :

Conjecture 10 **(Cassels)**. — *Le groupe* $Ш(E)$ *est un groupe fini.*

Ceci dit, un contrôle du groupe de Selmer permet de majorer le rang puisque la suite exacte précédente implique que

$$r \leq \mathrm{rk}_p(\mathrm{Sel}_p(E)), \tag{1}$$

où p est un nombre premier et où $\mathrm{rk}_p(G)$ désigne le p-rang du groupe abélien fini G (i.e. la dimension sur $\mathbb{F}_p$ de G/pG). Pour $n \in \{2,3,4,5\}$, Bhargava et Shankar ont calculé la moyenne de $|\mathrm{Sel}_n(E)|$ pour l'ensemble des courbes elliptiques définies sur $\mathbb{Q}$. Afin d'énoncer correctement leurs résultats, nous devons être plus précis, en particulier pour ordonner les courbes elliptiques. Tout d'abord, on ne compte qu'une seule fois les courbes elliptiques dans une classe d'isomorphie. Deux équations $E\colon y^2 = x^3+ax+b$ et $E'\colon y^2 = x^3+a'x+b'$ sur $\mathbb{Q}$ définissent des courbes elliptiques isomorphes si et seulement si il existe $u \in \mathbb{Q}^*$ tel que $a' = u^4a$ et $b' = u^6b$. On passe alors de l'équation de E à celle de E' par le changement de variables $x \leftrightarrow u^2x$ et $y \leftrightarrow u^3y$. Ainsi, chaque classe d'isomorphie contient un unique représentant minimal, i.e., une courbe $E\colon y^2 = x^3 + ax + b$ tel que pour tout nombre premier p si p^4 divise a alors p^6 ne divise pas b. Pour une telle courbe, E, minimale, on définit la hauteur (naïve) de E par

$$\mathrm{ht}(E) = \max\{4|a|^3, 27b^2\}.$$

7. Si p est un nombre premier, le corps $\mathbb{Q}_p$ est le complété de $\mathbb{Q}$ pour la valeur absolue $|\cdot|_p = p^{-v_p(\cdot)}$, où $v_p(\cdot)$ désigne la valuation p-adique.

On note alors $\mathcal{F}$ l'ensemble des courbes $E\colon y^2 = x^3 + ax + b$ minimales et pour $x \in \mathbb{R}$, on pose $\mathcal{F}(x) = \{E \in \mathcal{F}\colon \mathrm{ht}(E) \leq x\}$. Enfin, si $f\colon \mathcal{F} \to \mathbb{R}$ est une fonction, la moyenne de f sur l'ensemble des courbes elliptiques ordonnées par la hauteur est

$$M(f) = \lim_{x\to\infty} \frac{\sum_{E\in\mathcal{F}(x)} f(E)}{\sum_{E\in\mathcal{F}(x)} 1},$$

si la limite existe. Si f est la fonction caractéristique d'une propriété P, on parle de la probabilité (ou de la densité) de l'ensemble des courbes elliptiques vérifiant P. Avec ces définitions, les résultats de Bhargava et Shankar sont les suivants :

Théorème 11. — *On a :*

- $M(|\operatorname{Sel}_2|) = 3$ *(*[**BS13c**]*)* ;
- $M(|\operatorname{Sel}_3|) = 4$ *(*[**BS13d**]*)* ;
- $M(|\operatorname{Sel}_4|) = 7$ *(*[**BS13a**]*)* ;
- $M(|\operatorname{Sel}_5|) = 6$ *(*[**BS13b**]*)* ;

On obtient les mêmes moyennes lorsqu'on considère des sous-familles de courbes elliptiques de $\mathcal{F}$ définies par un nombre fini de congruences sur les coefficients a et b.

La conjecture générale formulée par Bhargava et Shankar est la suivante :

Conjecture 12. — *Pour $n \in \mathbb{N}$, on a $M(|\operatorname{Sel}_n|) = \sigma(n)$, où $\sigma(n)$ désigne la somme des diviseurs de n.*

Cette conjecture se retrouve aussi dans les travaux modélisant le comportement des groupes de Selmer et de Tate-Shafarevich ([**?**], [**?**], [**?**]).
Les moyennes calculées par Bhargava et Shankar entraînent des résultats sur le rang général des courbes elliptiques. En effet, l'équation (1) et $M(|\operatorname{Sel}_2|) = 3$ impliquent que la moyenne des rangs des courbes elliptiques est majorée par $3/2$ ([**BS13c**]). Lorsque Bhargava et Shankar ont annoncé cette majoration, c'était le premier résultat inconditionnel montrant que le rang moyen était borné. Le meilleur résultat antérieur était dû à Young ([**You06**]) sous l'hypothèse de Riemann généralisée et sous la conjecture de Birch et Swinnerton-Dyer avec une majoration de $25/14$ donc moins bonne que le $3/2$ que Bhargava et Shankar obtiennent sans conjecture ! Il convient à ce point de donner une explication sur la conjecture de Birch et Swinnerton-Dyer qui est centrale en théorie des

nombres. On sait associer à une courbe elliptique E définie sur $\mathbb{Q}$ une série L :

$$L(E,s)=\sum_{n\geq 1} a_n n^{-s}=\prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})},$$

où les produit porte sur tous les nombres premiers p. On a $a_p=\alpha_p+\beta_p$ et pour tous p sauf un nombre fini, le nombre a_p est en fait défini par

$$a_p=p+1-\sharp E(\mathbb{F}_p),$$

où $\sharp E(\mathbb{F}_p)$ est le nombre de points de la courbe elliptique vue dans le corps fini à p éléments, $\mathbb{F}_p$. Le théorème de Hasse affirme que $|a_p|\leq 2\sqrt{p}$ ce qui permet d'obtenir la convergence absolue de $L(E,s)$ pour $\Re e(s)>3/2$ et de montrer qu'elle définit une fonction entière dans ce demi-plan. Les fameux travaux de Wiles complétés par Taylor-Wiles et Breuil-Conrad-Diamond-Taylor entraînent que $L(E,s)$ admet un prolongement analytique à tout le plan complexe et qu'elle satisfait une équation fonctionnelle qui relit la valeur $L(E,s)$ à celle de $L(E,2-s)$. Le point $s=1$ est une valeur centrale pour $L(E,s)$ et la conjecture de Birch et Swinnerton-Dyer (BSD) prédit un lien entre $L(E,1)$ et certains invariants arithmétiques de E.

Conjecture 13 **(Birch et Swinnerton-Dyer)**. — *On note $r_{an}\in\mathbb{N}$ l'ordre d'annulation de $L(E,s)$ en $s=1$. On a*

$$r_{an}=r \text{ (forme faible de la conjecture BSD).}$$

Plus précisément

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\Omega(E)c(E)\frac{R(E)|Ш(E)|}{(\sharp E(\mathbb{Q})_{\text{tors}})^2},$$

où $\Omega(E)\in\mathbb{R}_+$ est la période réelle [8]*, $c(E)\in\mathbb{N}$ est le produit des nombres de Tamagawa, $R(E)\in\mathbb{R}_+$ est le régulateur de E (intuitivement, il donne une mesure de la complexité d'un système de générateurs de $E(\mathbb{Q})$) et où $Ш(E)$ est supposé être un groupe fini (i.e. on suppose que la conjecture de Cassels est vérifiée pour énoncer cette conjecture).*

Les travaux de Kolyvagin et de Gross-Zagier entraînent en particulier que si $r_{an}\leq 1$ alors $r=r_{an}$ et le groupe $Ш(E)$ est fini. La conjecture BSD est à la base de nombreuses autres conjectures en théorie des nombres.

8. Il n'est pas nécessaire ici de définir précisément les invariants arithmétiques impliqués dans l'égalité de la conjecture de Birch et Swinnerton-Dyer.

Les travaux de Young établissent, avec des outils analytiques (formules explicites, etc.) une majoration de l'ordre d'annulation moyen en $s = 1$ des fonctions $L(E, s)$ lorsque E parcourt les courbes elliptiques définies sur $\mathbb{Q}$. Pour obtenir son résultat, Young a également besoin de faire des hypothèses sur les zéros de fonctions L (les fonctions $L(E, s)$ des courbes elliptiques mais également d'autres fonctions L) d'où l'utilisation de l'hypothèse de Riemann généralisée.

En utilisant leur résultat sur le 5-groupe de Selmer et les travaux de T. Dokchitser et V. Dokchitser ([**DD10**]) sur la parité des p-groupes de Selmer, Bhargava et Shankar obtiennent

Théorème 14 **([BS13b])**. — *La moyenne des rangs des courbes elliptiques est majorée par* 0.885.

Ce résultat très fort est à mettre en parallèle avec les conjectures classiques du domaine qui prédisent que la moyenne du rang, $M(r)$ est égale à $1/2$. Plus précisément, on fait la conjecture suivante :

Conjecture 15. — *Le rang des courbes elliptiques est en moyenne 0 ou 1 avec une probabilité de 1/2 pour chaque cas.*

Toujours dans [**BS13b**], les auteurs déduisent de la moyenne du 5-groupe de Selmer qu'une densité d'au moins 20,62% des courbes elliptiques ont un rang égal 0 et, si on admet la conjecture 10 qu'une densité d'au moins 26,12% des courbes elliptiques ont un rang égal à 1. Pour le dernier point, Bhargava et C. Skinner ([**BS14**]) obtiennent un résultat inconditionnel en montrant qu'il existe une densité positive de courbes elliptiques de rang 1. C'est le premier résultat donnant une borne inférieure sur le rang moyen.

Tous les travaux précédents ont aussi des applications sur les courbes elliptiques qui vérifient la (forme faible de la) conjecture de Birch et Swinnrton-Dyer. En effet, Bhargava, Skinner et Zhang obtiennent le théorème suivant :

Théorème 16. — [**?**] *Au moins 66,48% des courbes elliptiques vérifient la forme faible de la conjecture de Birch et Swinnerton-Dyer et vérifie la conjecture de Cassels.*

La démonstration de $M(|\operatorname{Sel}_2|) = 3$ ([**BS13c**]) repose sur l'étude et le comptage des formes quartiques binaires définies sur $\mathbb{Q}$. Soit V l'espace vectoriel de ces formes [9], i.e.

$$V(\mathbb{Q}) = \{f(x_1, x_2) = ax_1^4 + bx_1^3x_2 + cx_1^2x_2^2 + dx_1x_2^3 + ex_2^4 \colon a, b, c, d, e \in \mathbb{Q}\}.$$

Si f est une forme quadratique binaire, on lui associe deux invariants :

$$\begin{aligned} I = I(f) &= 12ae - 3bd + c^2 \\ J = J(f) &= 72ace + 9bcd - 27ad^2 - 27b^2e - 2c^3. \end{aligned}$$

On définit aussi la hauteur de f par $\operatorname{ht}(f) = \frac{4}{27}\max\{|I|^3, J^2/4\}$. Le groupe $\mathrm{PGL}_2(\mathbb{Q})$ agit naturellement sur $V(\mathbb{Q})$: pour $g \in \mathrm{PGL}_2(\mathbb{Q})$ et $f \in V(\mathbb{Q})$, on pose

$$(g \cdot f)(x_1, x_2) = (\det(g))^{-2} f((x_1, x_2) \cdot g),$$

de telle sorte que $I(g \cdot f) = I(f)$ et $J(g \cdot f) = J(f)$. On dit que $f \in V(\mathbb{Q})$ a des solutions partout localement si l'équation $y^2 = f(x_1, x_2)$ a des solutions (non-triviales) dans $\mathbb{R}$ et dans tous les complétés $\mathbb{Q}_p$ de $\mathbb{Q}$ pour tout nombre premier p. On note $V(\mathbb{Q})^{\mathrm{sl}}$ le sous-ensemble [10] de $V(\mathbb{Q})$ constitué des formes f qui ont des solutions partout localement. L'action de $\mathrm{PGL}_2(\mathbb{Q})$ préserve $V(\mathbb{Q})^{\mathrm{sl}}$. Maintenant si $[f] \in \mathrm{PGL}_2(\mathbb{Q})\backslash V(\mathbb{Q})^{\mathrm{sl}}$ alors la classe $[f]$ peut être identifiée à un élément de $\operatorname{Sel}_2(E)$ où E est la courbe définie par $y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$. En faisant varier les coefficients I et J et en ne gardant qu'une courbe elliptique dans la classe d'isomorphie (cela correspond à ne garder qu'un représentant de $[f]$ modulo $\mathbb{Q}^\times$ sur les formes quartiques binaires via l'action $\gamma \cdot f := \gamma^2 f$, $\gamma \in \mathbb{Q}^\times$), on obtient une correspondance bijective

$$(\mathrm{PGL}_2(\mathbb{Q}) \times \mathbb{Q}^\times)\backslash V(\mathbb{Q})^{\mathrm{sl}} \leftrightarrow \{(E, c) \colon E \text{ courbe elliptique}, c \in \operatorname{Sel}_2(E)\}/\sim .$$

Pour obtenir le résultat sur la moyenne du 2-groupe de Selmer, tout le tour de force de Bhargava et Shankar revient à compter le nombre de classes d'équivalence des formes quartiques binaires dans $V(\mathbb{Q})^{\mathrm{sl}}$ dont la hauteur est inférieure à x. Plusieurs résultats généraux et intéressants en eux-mêmes sont nécessaires. Il s'agit d'abord d'arriver à compter, comme dans la première partie et via la théorie géométrique des nombres, les classes d'équivalence modulo $\mathrm{PGL}_2(\mathbb{Z})$ des formes quartiques binaires à coefficients entiers, $V(\mathbb{Z})$. Il faut alors trouver un représentant entier

9. Cet ensemble, noté également V n'a aucun rapport avec l'ensemble V donné dans la première partie de ce texte.

10. L'idée est de paramétrer ainsi les 2-groupes de Selmer.

pour les classes de $V(\mathbb{Q})^{\mathrm{sl}}$ modulo $(\mathrm{PGL}_2(\mathbb{Q}) \times \mathbb{Q}^\times)$ ayant des invariants entiers et enfin faire intervenir la condition d'avoir des solutions partout localement. Outre l'article [**BS13c**], on pourra trouver dans [**Ho14**] ou dans [**Poo13**] une présentation beaucoup plus détaillée de toutes ces étapes.

La stratégie précédente se généralise à d'autres couples (G, V) où V est une représentation du groupe G pour lesquels l'espace des invariants est un anneau engendré par deux polynômes : on parle alors de représentations corégulières. Et, en effet, en adaptant leur méthode sur d'autres espaces, Bhargava et Shankar parviennent à calculer la moyenne des 3-4-5-groupes de Selmer (par exemple, pour les 3-groupes de Selmer, l'espace V est celui des formes formes cubiques ternaires et G est le groupe SL_3).

Un autre résultat de Bhargava issu d'une stratégie similaire porte sur l'existence de points rationnels sur les courbes en général. Comme dit précédemment, on classifie les courbes (lisses) suivant leur genre $g \in \mathbb{N}$. Les courbes elliptiques sont des courbes de genre 1 ayant au moins un point rationnel et le rang donne une mesure de « l'abondance » des points rationnels sur la courbe (par exemple, un nombre fini si le rang est nul, une infinité si le rang est ≥ 1). Dans ce contexte, il est naturel de se demander si une courbe aléatoire définie sur $\mathbb{Q}$ possède ou non un point rationnel. Cette question a été étudiée par plusieurs auteurs et les travaux remarquables de Bhargava dans ce domaine apportent une réponse précise dans le cas particulier et important des courbes hyperelliptiques. Une telle courbe de genre g peut se ramener à une équation de la forme :

$$C\colon y^2 = f_0 x^n + f_1 x^{n-1} y + \cdots + f_{n-1} x y^{n-1} + f_n y^n,$$

où $n = 2g + 2$ et où le polynôme homogène $f(x, y) = f_0 x^n + f_1 x^{n-1} y + \cdots + f_{n-1} x y^{n-1} + f_n y^n \in \mathbb{Z}[x, y]$ n'a pas de facteurs carrés non-triviaux dans $\bar{\mathbb{Q}}[x, y]$. En définissant la hauteur de la courbe C par

$$H(C) = \max_{0 \leq i \leq n} (|f_i|),$$

on peut définir la limite inférieure de la densité des courbes hyperelliptiques définies sur $\mathbb{Q}$ qui ne possèdent pas de point rationnel. On note ρ_g cette limité inférieure. Bhargava démontre le théorème suivant :

Théorème 17 **([Bha13])**. — *On a* $\rho_g = 1 + o(2^{-g})$, $g \to \infty$.

La stratégie de la preuve de ce théorème rejoint celle du calcul de la moyenne du 2-groupe de Selmer. À un point rationnel sur C, Bhargava

associe une orbite entière de l'action du groupe $G(\mathbb{Z}) = \mathrm{GL}_n(\mathbb{Z})$ sur un certain espace $V(\mathbb{Z})$ de telle sorte que le couple (G, V) est une certaine représentation corégulière beaucoup plus technique à traiter que celles mentionnées précédemment. Bhargava parvient néammoins à compter ces orbites entières et à en déduire le théorème. Ce résultat a des conséquences spectaculaires sur la philosophie « local-global ». En particulier, lorsque $g \to \infty$, 100% des courbes hyperelliptiques définies sur $\mathbb{Q}$ ayant des points dans tous les complétés de $\mathbb{Q}$ n'ont, en fait, pas de point rationnel.

Outre ces travaux majeurs en théorie algébrique des nombres et en géométrie arithmétiques, M. Bhargava a obtenu de nombreuses contributions originales et importantes en théorie des nombres citons simplement par exemple ses travaux sur la généralisation de la fonction factorielle et ses travaux autour des théorèmes "15" et "290" sur les valeurs prises par les formes quadratiques définies positives.

Références

[Bel05] Karim Belabas. Paramétrisation de structures algébriques et densités de discriminants [d'après Bhargava]. *Astérisque*, (299) :267–299, 2005. Séminaire Bourbaki. Vol. 2003/2004.

[Bha04a] Manjul Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1) :217–250, 2004.

[Bha04b] Manjul Bhargava. Higher composition laws. II. On cubic analogues of Gauss composition. *Ann. of Math. (2)*, 159(2) :865–886, 2004.

[Bha04c] Manjul Bhargava. Higher composition laws. III. The parametrization of quartic rings. *Ann. of Math. (2)*, 159(3) :1329–1360, 2004.

[Bha05] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Ann. of Math. (2)*, 162(2) :1031–1063, 2005.

[Bha10] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Ann. of Math. (2)*, 172(3) :1559–1591, 2010.

[Bha13] Manjul Bhargava. Most hyperelliptic curves over $\mathbb{Q}$ have no rational points. *Preprint available on arXiv :1308.0395v1*, 2013.

[BS13a] Manjul Bhargava and Arul Shankar. The average number of elements in the 4-selmer groups of elliptic curves is 7. *Preprint available on arXiv :1312.7333v1*, 2013.

[BS13b] Manjul Bhargava and Arul Shankar. The average size of the 5-selmer groups of elliptic curves is 6, and the average rank is less than 1. *Preprint available on arXiv :1312.7859v1*, 2013.

[BS13c] Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Preprint available on arXiv :1006.1002v3*, 2013.

[BS13d] Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Preprint available on arXiv :1007.0052v2*, 2013.

[BS14] Manjul Bhargava and Christopher Skinner. A positive proportion of elliptic curves over $\mathbf{Q}$ have rank one. *Preprint available on arXiv :1401.0233v1*, 2014.

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2) :439–499, 2013.

[DD10] Tim Dokchitser and Vladimir Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math. (2)*, 172(1) :567–596, 2010.

[DH71] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields (ii). *Proc. Roy. Soc. Lond. A*, 322 :405–420, 1971.

[GGS02] Wee Teck Gan, Benedict Gross, and Gordan Savin. Fourier coefficients of modular forms on G_2. *Duke Math. J.*, 115(1) :105–169, 2002.

[Ho14] Wei Ho. How many rational points does a random curve have ? *Bull. Amer. Math. Soc. (N.S.)*, 51(1) :27–52, 2014.

[Lev14] F. Levi. Kubische Zahlkörper und binäre kubische Formenklassen. *Leipz. Ber (Berichte über die Verhandlungen der Königl. Sächsischen Gesellschaft der Wissenschaften zu Leipzig. Math.-phys. Klasse)*, (66) :26–37, 1914.

[Poo13] Bjorn Poonen. Average rank of elliptic curves [after Manjul Bhargava and Arul Shankar]. *Astérisque*, (352) :Exp. No. 1049, viii, 187–204, 2013. Séminaire Bourbaki. Vol. 2011/2012. Exposés 1043–1058.

[SK77] M. Sato and T. Kimura. A classification of irreducible prehomogeneous vector spaces and their relative invariants. *Nagoya Math. J.*, 65 :1–155, 1977.

[WY92] David J. Wright and Akihiko Yukie. Prehomogeneous vector spaces and field extensions. *Invent. Math.*, 110(2) :283–314, 1992.

[You06] Matthew P. Young. Low-lying zeros of families of elliptic curves. *J. Amer. Math. Soc.*, 19(1) :205–250, 2006.

Karim Belabas, Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France., CNRS, IMB, UMR 5251, F-33400 Talence, France., INRIA, F-33400 Talence, France. • *E-mail :* Karim.Belabas@math.u-bordeaux.fr

Christophe Delaunay, Laboratoire de Mathématiques de Besançon, Facultés des sciences et techniques, CNRS, UMR 6623, 16 route de Gray, 25030 Besançon, France • *E-mail :* Christophe.Delaunay@univ-fcomte.fr