

Sur le nombre d'invariants fondamentaux des formes binaires

Jacques DIXMIER, Paul ERDŐS et Jean-Louis NICOLAS

Résumé — Soient $d > 0$, V_d l'espace vectoriel des polynômes homogènes en x et y , de degré d , à coefficients complexes, $C[V_d]$ l'algèbre des fonctions polynomiales $V_d \rightarrow C$. Le groupe $G = SL(2, C)$ opère de manière naturelle dans V_d donc dans $C[V_d]$; soit A_d la sous-algèbre des éléments G -invariants dans $C[V_d]$; soit ω_d le cardinal de tout système générateur minimal de l'algèbre A_d (nombre d'invariants fondamentaux des formes binaires de degré d). Nous améliorons des minoration de ω_d dues à V. G. Kac et V. L. Popov.

On the number of fundamental invariants of binary forms

Abstract — Let $d > 0$ be an integer, V_d the vector space of homogeneous polynomials in x and y , of degree d , with complex coefficients, $C[V_d]$ the algebra of polynomial functions $V_d \rightarrow C$. The group $G = SL(2, C)$ operates in a natural way in V_d , and so in $C[V_d]$; let A_d be the subalgebra of G -invariant elements in $C[V_d]$; let ω_d be the number of elements in any minimal generating system of the algebra A_d (number of fundamental invariants for binary forms of degree d). We improve some minorations of ω_d obtained by V. G. Kac and V. L. Popov.

1. Soient n un entier > 0 , k un nombre réel. On notera $p(n)$ le nombre des partitions (avec répétitions) de n , et $p(n, k)$ le nombre des partitions de n dont les parts sont $\leq k$. Soit $f(n)$ une fonction tendant vers $+\infty$ quand $n \rightarrow +\infty$. Alors

$$p(n) \sim (1/4 \sqrt{3} n) \exp\left(\pi \sqrt{\frac{2}{3}} \sqrt{n}\right) \quad \text{quand } n \rightarrow +\infty \quad [2],$$

et

$$p(n, n^{1/2} \cdot (\log n) \cdot f(n)) / p(n) \rightarrow 1 \quad \text{quand } n \rightarrow +\infty \quad ([1], \text{ th. 1.1}).$$

2. Il est prouvé en [3], p. 105, que, pour d impair,

$$(1) \quad \omega_d \geq p(d-2) + \varphi(d-2) - 1$$

où φ est l'indicateur d'Euler. Nous allons prouver ceci :

PROPOSITION. — Pour d impair tendant vers $+\infty$, on a

$$\liminf \omega_d \cdot \left[\frac{d^{1/2}}{\log d \log \log d} p(d) \right]^{-1} > 0.$$

3. Soit n un entier > 0 . Considérons l'équation

$$(E_n) \quad x_1 + 2x_2 + \dots + (n-1)x_{n-1} \equiv 0 \pmod{n}$$

où x_1, \dots, x_{n-1} sont des entiers ≥ 0 non tous nuls. Une solution est dite indécomposable si elle n'est pas somme de 2 solutions. Il n'y a qu'un nombre fini $F(n)$ de solutions indécomposables. Il est prouvé en [3], p. 105 que, pour d impair, $\omega_d \geq F(d-2)$. Cela entraîne facilement (1). Nous allons améliorer la minoration de $F(n)$.

4. Soient n, k des entiers > 0 . Considérons l'équation

$$(E'_{n,k}) \quad x_1 + 2x_2 + \dots + (n-1)x_{n-1} = kn$$

où x_1, \dots, x_{n-1} sont des entiers ≥ 0 . Considérons la propriété suivante que peut posséder une solution (x_1, \dots, x_{n-1}) de $(E'_{n,k})$: $(P_{n,k})$: si x'_1, \dots, x'_{n-1} sont des entiers tels que

Note présentée par Alain CONNES.

$0 \leq x'_i \leq x_i$ pour tout i , alors $x'_1 + 2x'_2 + \dots + (n-1)x'_{n-1}$ est non divisible par n , sauf si $(x'_1, \dots, x'_{n-1}) = (0, \dots, 0)$ ou (x_1, \dots, x_{n-1}) .

Soit $G(n, k)$ le nombre de solutions de $(E'_{n, k})$ vérifiant $(P_{n, k})$. Une solution de $(E'_{n, k})$ est solution indécomposable de (E_n) si et seulement si elle vérifie $(P_{n, k})$. Donc

$$(2) \quad F(n) = \sum_{k \geq 1} G(n, k).$$

5. LEMME. — Supposons k premier à n . Soit $i = [(n-1)/k]$. Alors $G(n, k) \geq p(n, i)$. (On pose $[x] = \max_{n \in \mathbb{Z}, n \leq x}$)

Soient y_1, \dots, y_i des entiers ≥ 0 tels que $y_1 + 2y_2 + \dots + iy_i = n$. Définissons x_1, \dots, x_{n-1} ainsi : $x_l = 0$ si k ne divise pas l , et $x_{km} = y_m$ pour $m = 1, 2, \dots, i$. Alors (x_1, \dots, x_{n-1}) est solution de $(E'_{n, k})$. Soient x'_1, \dots, x'_{n-1} des entiers tels que $0 \leq x'_i \leq x_i$ pour tout i , et que n divise $x'_1 + 2x'_2 + \dots + (n-1)x'_{n-1}$. Alors $x'_i = 0$ si k ne divise pas i , et n divise $kx'_k + 2kx'_{2k} + \dots + ikx'_{ik} = k(x'_k + 2x'_{2k} + \dots + ix'_{ik})$, donc n divise $x'_k + 2x'_{2k} + \dots + ix'_{ik} \leq y_1 + 2y_2 + \dots + iy_i = n$. Donc $(x'_k, \dots, x'_{ik}) = (0, \dots, 0)$ ou (y_1, \dots, y_i) . Ainsi, (x_1, \dots, x_{n-1}) vérifie $(P_{n, k})$.

6. LEMME. — Soient k, n des entiers > 0 . Soit $d(n)$ le nombre des diviseurs de n . Le nombre des entiers > 0 premiers à n et $\leq k$ est de la forme

$$\frac{\varphi(n)}{n} k + \theta d(n) \quad \text{avec} \quad |\theta| \leq 1.$$

Soit μ la fonction de Möbius. On a

$$\begin{aligned} \sum_{i \leq k, (i, n) = 1} 1 &= \sum_{i \leq k} \sum_{j|i, j|n} \mu(j) = \sum_{j|n} \mu(j) \sum_{i \leq k, j|i} 1 = \sum_{j|n} \mu(j) \left[\frac{k}{j} \right] \\ &= \sum_{j|n} \frac{\mu(j)}{j} k + R = k \prod_{p \text{ premier}, p|n} \left(1 - \frac{1}{p} \right) + R \end{aligned}$$

avec $|R| \leq \sum_{j|n} |\mu(j)| \leq d(n)$.

7. Par ailleurs, rappelons que $d(n) \leq cn^{0.3}$ ([4], p. 489) et que

$$\frac{\varphi(n)}{n} \geq \frac{c'}{\log \log n} \quad \text{pour} \quad n \geq 3 \quad [7]$$

où $c, c' > 0$ sont des constantes absolues.

8. LEMME. — On a, quand $n \rightarrow +\infty$,

$$\liminf F(n) \cdot \left[\frac{n^{1/2}}{\log n \cdot \log \log n} p(n) \right]^{-1} > 0.$$

Soit $n \mapsto f(n)$ une fonction tendant vers $+\infty$. On a, en utilisant (2) et le lemme 5,

$$F(n) \geq \sum_{(k, n) = 1, 1 \leq k \leq n^{1/2}/\log n \cdot f(n)} G(n, k) \geq \sum_{(k, n) = 1, 1 \leq k \leq n^{1/2}/\log n \cdot f(n)} p\left(n, \left[\frac{n-1}{k} \right] \right).$$

Or, si $1 \leq k \leq n^{1/2}/\log n \cdot f(n)$, on a

$$\left[\frac{n-1}{k} \right] \geq \frac{n-1}{n^{1/2}} \log n \cdot f(n) = n^{1/2} (\log n) f(n) \left(1 - \frac{1}{n} \right),$$

donc

$$p\left(n, \left[\frac{n-1}{k}\right]\right) \geq (1-o(1)) p(n)$$

uniformément en k (d'après [1]). Compte tenu de 6 et 7, le nombre des entiers premiers à n et $\leq n^{1/2}/\log n \cdot f(n)$ majore

$$\frac{c}{\log \log n} \frac{n^{1/2}}{\log n \cdot f(n)}$$

où c est une constante absolue. Donc

$$F(n) \geq \frac{cn^{1/2}}{f(n) \log n \log \log n} (1-o(1)) p(n).$$

Vu l'arbitraire de la fonction f , on en déduit le lemme, et la proposition 2.

9. Supposons maintenant $d=2c$ avec c impair.

PROPOSITION. — Soit $\varepsilon > 0$. Pour $d \equiv 2 \pmod{4}$ et $d \rightarrow +\infty$, on a

$$\liminf \omega_d \left[e^{((n/\sqrt{3})-\varepsilon) (\log \log d/\log d)} d^{1/2} p\left(\frac{d}{2}\right) \right]^{-1} > 0.$$

D'après [5], p. 165, ω_d majore le nombre S_c de solutions indécomposables de l'équation

$$(3) \quad 2x_2 + 3x_3 + \dots + cx_c = 2y_2 + 3y_3 + \dots + cy_c$$

où x_2, \dots, y_c sont des entiers ≥ 0 . Posons

$$C = \pi \sqrt{\frac{2}{3}}, \quad q = \left[\frac{C c^{1/2}}{\log c} \right], \quad r = [c^{1/2}].$$

Dans chacun des intervalles $]c-q, c]$, $]c-2q, c-q]$, \dots , $]c-(r+q)q, c-(r+q-1)q]$, il existe un nombre congru à 1 modulo q ; soit E l'ensemble de nombres ainsi défini; il a $r+q$ éléments. Soit $\{i_1, i_2, \dots, i_q\}$ une partie à q éléments de E . On a

$$i_1 + \dots + i_q \geq q(c - (r+q)q) \geq q(c - 2rq) \geq q\left(c - \frac{2Cc}{\log c}\right).$$

Posons :

$$(4) \quad c' = \left[c - \frac{2Cc}{\log c} \right].$$

Comme $i_1 + \dots + i_q$ est divisible par q , on a $i_1 + \dots + i_q = qM$ avec un entier $M \geq c'$. Considérons les solutions de

$$2x_2 + 3x_3 + \dots + cx_c = i_1 + \dots + i_q (= qM)$$

où $x_i = 0$ quand i n'est pas divisible par q . Si $q > 1$, le nombre de ces solutions est

$$p(M, c/q) \geq p\left(c', \frac{1}{C} c^{1/2} \log c\right) \geq p\left(c', \frac{1}{C} c'^{1/2} \log c'\right) \geq \alpha p(c')$$

où α est une constante absolue (d'après [1], th. 1.1). Or

$$p(c') = \frac{1}{4\sqrt{3}c'} \exp(C\sqrt{c'}) (1+o(1)) \quad (\text{cf. § 1})$$

$$= \frac{1}{4\sqrt{3}c} \exp\left(C\left(c - \frac{2Cc}{\log c}\right)^{1/2}\right) (1+o(1)) \quad \text{d'après (4)}$$

$$\begin{aligned}
&= \frac{1}{4\sqrt{3}c} \exp(Cc^{1/2}) \exp\left(-\frac{C^2 c^{1/2}}{\log c}(1+o(1))\right)(1+o(1)) \\
&= p(c) \exp\left(-\frac{C^2 c^{1/2}}{\log c}(1+o(1))\right)(1+o(1)).
\end{aligned}$$

D'autre part, toute somme partielle extraite de $i_1 + \dots + i_q$, distincte de 0 et qM , est non divisible par q d'après le choix de i_1, \dots, i_q . Ainsi,

$$S_c \geq \alpha p(c) \exp\left(-\frac{C^2 c^{1/2}}{\log c}(1+o(1))\right) N$$

où N est le nombre de parties de E à q éléments, c'est-à-dire

$$\binom{r+q}{q} \geq \frac{r^q}{q^q} = \exp(q \log(r/q)) = \exp\left(\frac{C c^{1/2}}{\log c} \log \log c(1+o(1))\right).$$

Donc

$$\begin{aligned}
S_c &\geq \alpha p(c) \exp\left(-\frac{C^2 c^{1/2}}{\log c}(1+o(1)) + \frac{C c^{1/2}}{\log c}(\log \log c)(1+o(1))\right)(1+o(1)) \\
&= \alpha p(c) \exp\left(C c^{1/2} \frac{\log \log c}{\log c}(1+o(1))\right)(1+o(1)) \\
&= \alpha p\left(\frac{d}{2}\right) \exp\left(\frac{C}{\sqrt{2}} d^{1/2} \frac{\log \log d}{\log d}(1+o(1))\right)(1+o(1)).
\end{aligned}$$

10. Soit maintenant $d=4c$, avec c entier. D'après [6], p. 526-527, ω_d majore le nombre de solutions indécomposables de (E_c) , donc

$$\liminf \omega_d \cdot \left[\frac{d^{1/2}}{\log d \log \log d} p\left(\frac{d}{4}\right) \right]^{-1} > 0.$$

Note reçue le 15 juin 1987, acceptée le 26 juin 1987.

RÉFÉRENCES BIBLIOGRAPHIQUES

- [1] P. ERDÖS et J. LEHNER, The distribution of the number of summands in the partitions of a positive integer, *Duke Math. J.*, 8, 1941, p. 335-345.
- [2] G. H. HARDY et S. RAMANUJAN, Asymptotic formulae in combinatory analysis, *Proc. London Math. Soc.*, 17, 1918, p. 75-115.
- [3] V. G. KAC, Root systems, representations of quivers and invariant theory, *Springer Lecture Notes in Math.*, n° 996, 1983, p. 75-108.
- [4] J.-L. NICOLAS et G. ROBIN, Majorations explicites pour le nombre de diviseurs de N , *Canad. Math. Bull.*, 26, 1983, p. 485-492.
- [5] V. L. POPOV, Homological dimension of algebras of invariants, *J. für die reine und angew. Math.*, 341, 1983, p. 157-173.
- [6] V. L. POPOV, Syzygies in the theory of invariants, *Math. U.S.S.R. Izvestiya*, 47, 1983, p. 544-622.
- [7] J. B. ROSSER et L. SCHOENFELD, Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, 6, 1962, p. 64-94.

J. D. : 7, résidence Clos-de-Bures, 91440 Bures-sur-Yvette;

P. E. : Magyar Tudományok Akadémia, Matematikai Kutató Intézet, Reáltanoda u. 13-15, Pf 127, H-1364 Budapest, Hongrie;

J.-L. N. : Mathématiques, Université de Limoges, 123, avenue Albert-Thomas, 87060 Limoges Cedex.