JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

CAMILLE JORDAN

Sur le nombre des solutions de la congruence $|a_{ik}| \equiv \text{AmodM}$

Journal de mathématiques pures et appliquées 6^e série, tome 7 (1911), p. 409-416.
<http://www.numdam.org/item?id=JMPA_1911_6_7__409_0>

Sur le nombre des solutions de la congruence $|a_{ik}| \equiv A \bmod M$;

PAR M. CAMILLE JORDAN.

Soient A, M deux entiers quelconques; $|a_{ik}|$ un déterminant à n colonnes, dont les n^2 éléments a_{ik} soient des entiers mod M.

Proposons-nous de calculer le nombre $\mathfrak{N}(n, A, M)$ des solutions de la congruence

$$|a_{ik}| \equiv A \bmod M. \tag{1}$$

Si $M = M'M''$, M' et M'' étant premiers entre eux, les nombres a_{ik}, A seront déterminés mod M si l'on connaît leurs restes a'_{ik}, A' par rapport à M' et leurs restes a''_{ik}, A'' par rapport à M''; et la congruence (1) équivaudra au système des deux suivantes :

$$|a'_{ik}| \equiv A' \bmod M', \qquad |a''_{ik}| = A'' \bmod M''.$$

On aura donc

$$\mathfrak{N}(n, A, M) = \mathfrak{N}(n, A', M')\,\mathfrak{N}(n, A'', M'').$$

Le problème est ainsi ramené au cas où M est une puissance d'un nombre premier.

Soit donc $M = p^\mu$, et supposons d'abord $A \gtrless 0 \bmod p^\mu$. Il sera de la forme cp^λ, λ étant un entier nul ou positif, mais $< \mu$; c un entier positif moindre que $p^{\mu-\lambda}$ et premier à p.

Soit $|a_{ik}|$ l'un des $\mathfrak{N}(n, cp^\lambda, p^\mu)$ déterminants cherchés qui satisfont à la congruence

$$|a_{ik}| \equiv cp^\lambda \bmod p^\mu. \tag{2}$$

Soient p^{λ_1} la plus haute puissance de p qui divise tous les éléments

de sa première ligne ; ... ; p^{λ_m} la plus haute puissance de p qui divise tous les déterminants formés avec les éléments de ses m premières lignes ; on aura évidemment

$$(3) \qquad 0 \leqq \lambda_1 \leqq \lambda_2 \ldots \leqq \lambda_{n-1} \leqq \lambda \qquad \text{et} \qquad \lambda_n = \lambda.$$

Désignons par

$$[n, \lambda_1, \lambda_2, \ldots, \lambda_{n-1}, cp^{\lambda}, \mu]$$

le nombre des solutions qui correspondent à un système déterminé de valeurs des exposants *caractéristiques* $\lambda_1, \ldots, \lambda_{n-1}, \lambda$; on aura

$$\mathfrak{N}(n, cp^{\lambda}, p^{\mu}) = \Sigma[n, \lambda_1, \ldots, \lambda_{n-1}, cp^{\lambda}, \mu],$$

la sommation s'étendant à tous les systèmes de valeurs de ces exposants qui satisfont aux relations (3).

Considérons une des $[n, \lambda_1, \ldots, \lambda_{n-1}, cp^{\lambda}, \mu]$ solutions à énumérer. Les éléments a_{1k} de la première ligne y seront de la forme $r_{1k}p^{\lambda_1}$, les r_{1k} étant $< p^{\mu-\lambda_1}$ et n'étant pas tous divisibles par p ; ceux des lignes suivantes, en nombre $n(n-1)$, peuvent être mis sous la forme

$$a_{ik} = q_{ik}\, p^{\mu-\lambda_1} + r_{ik},$$

q_{ik} étant $< p^{\lambda_1}$ et $r_{ik} < p^{\mu-\lambda_1}$. Les premiers termes peuvent être supprimés sans que le déterminant change de valeur mod p^{μ} ; ils sont également sans influence sur la valeur des exposants $\lambda_1, \ldots, \lambda_{n-1}, \lambda$. Cela fait, la congruence (2), divisée par p^{λ_1}, deviendra

$$(4) \qquad |r_{ik}| \equiv cp^{\lambda-\lambda_1} \bmod p^{\mu-\lambda_1},$$

et, dans ce nouveau déterminant, les exposants caractéristiques seront tous diminués de λ_1.

Réciproquement, chaque solution de (4) donnera $p^{n(n-1)\lambda_1}$ solutions de (2) correspondant aux diverses valeurs possibles des q_{ik}. Nous obtenons ainsi une première formule de réduction

$$(5) \qquad \begin{aligned}[n, \lambda_1, \lambda_2, \ldots, \lambda_{n-1}, cp^{\lambda}, \mu] \\ = p^{n(n-1)\lambda_1}[n, 0, \lambda_2 - \lambda_1, \ldots, \lambda_{n-1} - \lambda_1, cp^{\lambda-\lambda_1}, \mu - \lambda_1].\end{aligned}$$

Reste à énumérer celles des solutions de la congruence (4) correspondant à la série d'exposants $0, \lambda_2 - \lambda_1, \ldots, \lambda - \lambda_1$. Dans chacune d'elles, l'un au moins des éléments r_{1k} de la première ligne n'est pas divisible par p. Considérons en particulier celles où le premier des

éléments non divisibles par p est $r_{1\alpha}$. Nous désignerons leur nombre par N_α et nous les grouperons en systèmes, en réunissant ensemble celles qui se déduisent de l'une d'elles par les opérations suivantes (lesquelles ne changent évidemment ni la valeur du déterminant, ni les constantes α, o, $\lambda_2-\lambda_1, \ldots, \lambda-\lambda_1$) :

1° Multiplication de la première ligne par l et de la deuxième par $l^{-1} \bmod p^{\mu-\lambda_1}$, l étant l'un des $p^{\mu-\lambda_1-1}(p-1)$ nombres premiers à p et $< p^{\mu-\lambda_1}$;

2° Addition, à l'une quelconque des $\alpha-1$ premières colonnes, de la $\alpha^{\text{ième}}$ colonne, multipliée par un des $p^{\mu-\lambda_1-1}$ multiples de p moindres que $p^{\mu-\lambda_1}$;

3° Addition, à l'une des $n-\alpha$ colonnes suivantes, de la $\alpha^{\text{ième}}$ colonne, multipliée par un nombre quelconque $< p^{\mu-\lambda_1}$;

4° Addition à l'une quelconque des $n-1$ lignes du déterminant, autre que la première, de celle-ci, multipliée par un nombre quelconque moindre que $p^{\mu-\lambda_1}$.

Chaque système ainsi formé contiendra

$$p^{\mu-\lambda_1-1}(p-1)\,p^{(\mu-\lambda_1-1)(\alpha-1)+(\mu-\lambda_1)(n-\alpha)+(\mu-\lambda_1)(n-1)} = p^{(\mu-\lambda_1)(2n-1)-\alpha}(p-1)$$

solutions évidemment distinctes, parmi lesquelles une solution *réduite*, dans laquelle $r_{1\alpha}$ est égal à 1, les autres éléments de la première ligne étant nuls, ainsi que ceux de la $\alpha^{\text{ième}}$ colonne. Dans cette solution réduite, le déterminant sera le produit de l'unité par un déterminant d'ordre $n-1$, ayant évidemment pour exposants caractéristiques $\lambda_2-\lambda_1, \ldots, \lambda-\lambda_1$. Le nombre des réduites distinctes sera celui des déterminants Δ de ce genre qui sont congrus à $cp^{\lambda-\lambda_1} \bmod p^{\mu-\lambda_1}$, soit $[n-1, \lambda_2-\lambda_1, \ldots, \lambda-\lambda_1, cp^{\lambda-\lambda_1}, \mu-\lambda_1]$. Chacune d'elles représentant un système de $p^{(\mu-\lambda_1)(2n-1)-\alpha}(p-1)$ solutions, on aura

$$N_\alpha = p^{(\mu-\lambda_1)(2n-1)-\alpha}(p-1)\,[n-1, \lambda_2-\lambda_1, \ldots, \lambda-\lambda_1, cp^{\lambda-\lambda_1}, \mu-\lambda_1],$$

et en faisant la sommation par rapport à α,

$$[n, o, \lambda_2-\lambda_1, \ldots, \lambda-\lambda_1, cp^{\lambda-\lambda_1}, \mu-\lambda_1]$$
$$= \sum_{\alpha=1}^{\alpha=n} N_\alpha = p^{(\mu-\lambda_1)(2n-1)-n}(p^n-1)\,[n-1, \lambda_2-\lambda_1, \ldots, \lambda-\lambda_1, cp^{\lambda-\lambda_1}, \mu-\lambda_1].$$

Substituons cette valeur dans la formule (5); celle-ci devient

$$(6)\quad [n, \lambda_1, \ldots, \lambda, cp^{\lambda}, \mu] = (p^n - 1)\, p^{(2n-1)\mu + [n(n-1)-(2n-1)]\lambda_1 - n} \times [n-1, \lambda_2 - \lambda_1, \ldots, \lambda_{n-1} - \lambda_1, cp^{\lambda - \lambda_1}, \mu - \lambda_1].$$

Par l'application réitérée de cette formule de réduction, on ramènera de même le calcul de

$$[n-1, \lambda_2 - \lambda_1, \ldots, \lambda_{n-1} - \lambda_1, cp^{\lambda-\lambda_1}, \mu - \lambda_1]$$

à celui de

$$[n-2, \lambda_3 - \lambda_2, \ldots, \lambda_{n-1} - \lambda_2, cp^{\lambda-\lambda_2}, \mu - \lambda_2],$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

et enfin à celui de

$$[1, cp^{\lambda - \lambda_{n-1}}, \mu - \lambda_{n-1}]$$

qui est évidemment égal à l'unité, car la congruence

$$a \equiv cp^{\lambda - \lambda_{n-1}} \bmod p^{\mu - \lambda_{n-1}}$$

n'a qu'une solution.

Le résultat final sera évidemment de la forme

$$[n, \lambda_1, \lambda_2, \ldots, \lambda, cp^{\lambda}, \mu] = (p^n - 1)(p^{n-1} - 1)\ldots(p^2 - 1)p^{\rho},$$

ρ étant une fonction linéaire de $\mu, \lambda_1, \ldots, \lambda_{n-1}$ qu'il est aisé de calculer.

Le terme constant dans cette fonction sera

$$-n - (n-1) - \ldots - 2 = 1 - \frac{n(n+1)}{2}.$$

Le coefficient de μ sera

$$(2n-1) + (2n-3) + \ldots + 3 = n^2 - 1.$$

Celui de λ_1 proviendra exclusivement des deux premières réductions : il est égal à

$$n(n-1) - (2n-1) - [(n-1)(n-2) - (2n-3)] - (2n-3) = -1.$$

Ceux de $\lambda_2, \ldots, \lambda_{n-2}$ s'en déduiraient en changeant n en $n-1$, $n-2, \ldots$. Ils sont donc aussi égaux à -1.

Enfin λ_{n-1} n'apparaît que dans la dernière réduction avec le coefficient

$$2(2-1) - (2.2-1) = -1.$$

On aura donc

$$\rho = 1 - \frac{n(n+1)}{2} + (n^2-1)\mu - (\lambda_1 + \lambda_2 + \ldots + \lambda_{n-1})$$

et, par suite,

$$(7) \quad \mathfrak{N}(n, cp^{\lambda}, p^{\mu}) = (p^n-1)\ldots(p^2-1)p^{1-n\frac{(n+1)}{2}+(n^2-1)\mu} \Sigma p^{-(\lambda_1+\lambda_2+\ldots+\lambda_{n-1})}$$

la sommation s'étendant à tous les systèmes de valeurs de $\lambda_1, \ldots, \lambda_{n-1}$ qui satisfont aux inégalités

$$\lambda_1 \leqq \lambda_2 \leqq \ldots \leqq \lambda_{n-1} \leqq \lambda.$$

Ce résultat est indépendant de c, comme il était aisé de le prévoir. Il resterait à calculer la somme

$$\Sigma p^{-(\lambda_1+\ldots+\lambda_{n-1})}.$$

Si λ est nul, $\lambda_1, \ldots, \lambda_{n-1}$ le seront également, et la somme se réduit à un seul terme, égal à l'unité.

Si $\lambda = 1$, un certain nombre des quantités $\lambda_1, \ldots$ pourront être nulles, les suivantes étant égales à 1. Si l est le nombre de ces dernières, on aura un terme égal à p^{-l}; la somme cherchée sera donc

$$\Sigma_0^{n-1} p^{-l} = \frac{p^{-nl}-1}{p^{-1}-1}.$$

Si λ est plus grand que 1 la somme contiendra un nombre considérable de termes, dont beaucoup seront semblables. Mais on peut la transformer comme il suit :

Débarrassons-nous d'abord des puissances négatives de p en posant

$$\lambda_1 = \lambda - \alpha_1, \quad \ldots \quad \lambda_{n-1} = \lambda - \alpha_{n-1}.$$

Il viendra

$$\Sigma p^{-(\lambda_1+\ldots+\lambda_{n-1})} = p^{-(n-1)\lambda} \Sigma p^{\alpha_1+\ldots+\alpha_{n-1}}$$

avec les conditions

$$0 \leqq \alpha_{n-1} \leqq \alpha_{n-2} \leqq \ldots \leqq \alpha_1 \leqq \lambda.$$

Or, si nous désignons par m un entier quelconque, on aura

$$(8) \qquad \Sigma_0^{\alpha_{k-1}} p^{m\alpha_k} = \frac{p^{m(\alpha_{k-1}+1)}-1}{p^m-1} = c_m p^{m\alpha_{k-1}} + d_m,$$

en posant pour abréger

$$c_m = \frac{p^m}{p^m - 1}, \qquad d_m = \frac{-1}{p^m - 1}.$$

On aura de même

$$\Sigma_0^{\lambda} p^{m\alpha_1} = c_m p^{m\lambda} + d_m.$$

Multiplions la formule (8) par $p^{\alpha_1+\ldots+\alpha_{k-1}}$ et sommons par rapport à α_k. Il viendra

$$\Pi p^{\alpha_1+\ldots+\alpha_{k-1}+m\alpha_k} = c_m \Sigma p^{\alpha_1+\ldots+(m+1)\alpha_{k-1}} + d_m \Sigma p^{\alpha_1+\ldots+\alpha_{k-1}}.$$

L'application répétée de cette formule de réduction donnera successivement

$$\begin{aligned}\Sigma p^{\alpha_1+\ldots+\alpha_{n-1}} = {} & c_1 \Sigma p^{\alpha_1+\ldots+2\alpha_{n-2}} + d_1 \Sigma p^{\alpha_1+\ldots+\alpha_{n-1}} \\ = {} & c_1 c_2 \Sigma p^{\alpha_1+\ldots+3\alpha_{n-3}} + c_1 d_2 \Sigma p^{\alpha_1+\ldots+\alpha_{n-2}} \\ & + d_1 c_1 \Sigma p^{\alpha_1+\ldots+2\alpha_{n-2}} + d_1 d_2 \Sigma p^{\alpha_1+\ldots+\alpha_{n-2}} \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

On arrivera finalement à une somme de 2^{n-1} termes dont chacun sera de la forme

$$B p^{l\lambda},$$

l étant l'un des entiers $0, 1, \ldots, \lambda - 1$ et B un produit de $n - 1$ facteurs des espèces c et d, et jouissant des propriétés suivantes :

Chaque facteur d_m (s'il n'est pas le dernier) est suivi dans B par l'un des deux facteurs c_1 ou d_1 ; et chaque facteur c_m (s'il n'est pas le dernier) est suivi de c_{m+1} ou de d_{m+1}.

Si le dernier facteur de B est un d, l sera nul, et B sera un produit de facteurs successifs ayant chacun l'une des formes suivantes :

$$(9) \qquad d_1, \quad (c_1 d_2), \quad (c_1 c_2 d_3), \quad \ldots.$$

Soient $k_1, k_2, k_3, \ldots$ les nombres de facteurs de ces diverses sortes ; on aura

$$(10) \qquad n - 1 = k_1 + 2k_2 + 3k_3 + \ldots.$$

D'ailleurs, en permutant ces facteurs, on obtiendra $\frac{(n-1)!}{k_1! k_2! k_3! \ldots}$ termes semblables, dont chacun sera égal à

$$d_1^{k_1}(c_1 d_2)^{k_2}(c_1 c_2 d_3)^{k_3} \ldots = (-1)^{k_1+k_2+\ldots} \frac{p^{k_2+3k_3+\ldots+\frac{\nu(\nu-1)}{2}k_\nu+\ldots}}{(p-1)^{k_1+k_2+\ldots}(p^2-1)^{k_2+\ldots}\ldots}.$$

L'ensemble des termes de la somme où $l = 0$ sera donc la somme

$$\Sigma(-1)^{k_1+k_2+\dots}\frac{(n-1)!}{k_1!\,k_2!\dots}\,\frac{p^{k_2+3k_3+\dots+\frac{\nu(\nu-1)}{2}k_\nu+\dots}}{(p-1)^{k_1+k_2+\dots}(p^2-1)^{k_2+\dots}\dots}$$

étendue à toutes les valeurs de $k_1, k_2, \dots$ qui satisfont à la condition (10). Cette somme est une fonction de $n-1$, que nous désignerons par S^0_{n-1}.

Considérons maintenant un terme $Bp^{l\lambda}$ où l soit différent de zéro. Les l derniers facteurs de B seront nécessairement $c_1\, c_2 \dots c_l$.

Les $n-1-l$ facteurs précédents pourront être groupés en facteurs des formes (9). La somme S'_{n-1} des coefficients des termes en $p^{l\lambda}$ sera donc

$$c_1 c_2 \dots c_l S^0_{n-1-l} = \frac{p^{\frac{l(l+1)}{2}}}{(p-1)\dots(p^l-1)} S^0_{n-1-l}.$$

Les coefficients S'_{n-1} étant ainsi définis, on aura

$$\sum p^{-(\lambda_1+\dots+\lambda_{n-1})} = p^{-(n-1)\lambda}\sum p^{\alpha_1+\dots+\alpha_{n-1}} = p^{-(n-1)\lambda}\sum_{l=0}^{l=n-1} S'_{n-1}\,p^{l\lambda}.$$

Nous avons dans tout ce qui précède cherché à déterminer le nombre $\mathfrak{N}(n, A, p^\mu)$ des solutions de la congruence

$$|a_{ik}| \equiv A \bmod p^\mu,$$

en supposant que $A = cp^\mu$ est différent de zéro.

Si A était nul, la méthode que nous avons suivie exigerait quelques modifications, pour tenir compte des solutions dans lesquelles tous les coefficients de la première ligne seraient nuls soit dans le déterminant primitif, soit dans l'un des déterminants successifs d'ordre $n-1$, $n-2, \dots$ auxquels conduit la méthode de réduction. (Ces solutions n'existent pas si le déterminant n'est pas nul.)

Au lieu de reprendre les calculs, il est plus simple de déterminer le nombre $\mathfrak{N}(n, 0, p^\mu)$ par différence, en remarquant que le nombre total des hypothèses possibles sur les valeurs des éléments a_{ik} étant $p^{n^2\mu}$, on doit avoir

$$\sum_{A=0}^{A=p^\mu-1} \mathfrak{N}(n, A, p^\mu) = p^{n^2\mu},$$

d'où

$$\mathfrak{N}(n, 0, p^\mu) = p^{n\cdot\mu} - \sum_{c,\lambda} \mathfrak{N}(n, cp^\lambda, p^\mu), \tag{11}$$

où c parcourt la suite des $p^{\mu-\lambda-1}(p-1)$ nombres premiers à p et moindres que $p^{\mu-\lambda}$, et λ la suite des nombres $0, 1, \ldots, \mu-1$.

La sommation par rapport à c est immédiate, car nous avons vu que $\mathfrak{N}(n, cp^\lambda, p^\mu)$ est indépendant de c. On aura donc

$$\sum_{c,\lambda} \mathfrak{N}(n, cp^\lambda, p^\mu) = p^{\mu-\lambda-1}(p-1) \sum_{\lambda} \mathfrak{N}(n, cp^\lambda, p^\mu).$$

Substituant dans (11) et remplaçant $\mathfrak{N}(n, cp^\lambda, p^\mu)$ par sa valeur (7) il vient

$$\mathfrak{N}(n, 0, p^\mu) = p^{n\cdot\mu}\left[1 - (p^n-1)\ldots(p-1)p^{-\frac{n(n+1)}{2}}\Sigma p^{-(\lambda_1+\ldots+\lambda_{n-1}+\lambda)}\right],$$

la sommation étant étendue à toutes les valeurs de $\lambda_1, \ldots, \lambda$ qui satisfont aux relations

$$0 \leqq \lambda_1 \leqq \ldots \leqq \lambda \leqq \mu - 1.$$

Cette somme, dont la forme est toute semblable à celle de la somme $\Sigma p^{-(\lambda_1+\ldots+\lambda_{n-1})}$ étudiée plus haut, est susceptible de la même transformation.