BULLETIN DE LA S. M. F.

E. CAHEN

Sur la résolution exacte en nombres entiers des équations linéaires à coefficients quelconques

Bulletin de la S. M. F., tome 30 (1902), p. 234-242

<http://www.numdam.org/item?id=BSMF_1902__30__234_0>

SUR LA RÉSOLUTION EXACTE EN NOMBRES ENTIERS DES ÉQUATIONS LINÉAIRES A COEFFICIENTS QUELCONQUES;

Par M. E. Cahen.

1. Soit a un nombre > 0.

Nous appellerons *suite normale de valeurs approchées de ce nombre,* une suite infinie de fractions

$$\frac{m^{(1)}}{n^{(1)}}, \quad \frac{m^{(2)}}{n^{(2)}}, \quad \ldots,$$

jouissant de la propriété suivante : appelons $\frac{m}{n}$ le terme général; *en posant*

$$a = \frac{m}{n} + \frac{\varepsilon_n}{n},$$

ε_n *tend vers zéro lorsque le rang du terme* $\frac{m}{n}$ *augmente indéfiniment.* Comme nous allons le voir de suite, il existe de telles suites.

Distinguons deux cas suivant que a est incommensurable ou commensurable.

1° *a incommensurable.* — Comme exemple de suite normale, on peut citer les réduites successives du développement de a en fraction continue.

En effet, soit $\frac{m}{n}$ l'une de ces réduites.

On sait que

$$\left| a - \frac{m}{n} \right| < \frac{1}{n^2}.$$

Donc, en posant

$$a = \frac{m}{n} + \frac{\varepsilon_n}{n},$$

on a

$$|\varepsilon_n| < \frac{1}{n}.$$

Donc ε_n tend vers zéro.

2° *a commensurable.* — Soit $a = \frac{A}{B}$. Je dis que, dans ce cas, les termes d'une suite normale sont, à partir d'un certain rang, égaux à $\frac{A}{B}$. En effet, en posant

$$\frac{A}{B} = \frac{m}{n} + \frac{\varepsilon_n}{n},$$

on a

$$\varepsilon_n = \frac{nA - mB}{B}.$$

Si $\frac{m}{n}$ n'est pas égal à $\frac{A}{B}$, le numérateur de cette expression est au moins égal à 1 et l'on a

$$|\varepsilon_n| \geqq \frac{1}{B}.$$

Donc, ε_n ne peut tendre vers zéro, à moins qu'à partir d'un certain rang dans la suite, $\frac{m}{n}$ ne soit constamment égal à $\frac{A}{B}$. Alors, $\varepsilon_n = 0$.

Corollaire. — Soient $\frac{m}{n}$, $\frac{m'}{n'}$ deux termes quelconques d'une suite normale. La condition nécessaire et suffisante pour que α soit commensurable est que, à partir d'un certain rang, la quantité $m'n - mn'$ soit constamment nulle (1).

2. *Généralisation pour plusieurs nombres.*

Soient $a_1, a_2, \ldots, a_p$ des nombres.

Nous appellerons *suite normale de systèmes de valeurs approchées de ces nombres,* une suite de systèmes de p valeurs commensurables jouissant de la propriété suivante :

Appelons

$$\frac{m_1}{n}, \quad \frac{m_2}{n}, \quad \ldots, \quad \frac{m_p}{n},$$

un système de cette suite (toutes les fractions composant ce système sont supposées réduites au même dénominateur), en posant

$$a_1 = \frac{m_1}{n} + \frac{\varepsilon_n^{(1)}}{n}, \qquad a_2 = \frac{m_2}{n} + \frac{\varepsilon_n^{(2)}}{n}, \qquad \ldots, \qquad a_p = \frac{m_p}{n} + \frac{\varepsilon_n^{(p)}}{n},$$

les quantités $\varepsilon_n^{(1)}, \varepsilon_n^{(2)}, \ldots, \varepsilon_n^{(p)}$ tendent vers zéro quand le rang du système augmente indéfiniment.

(1) Si l'on astreignait les termes d'une suite normale à être irréductibles, dans le cas de a commensurable, il n'y aurait qu'un nombre limité de termes dans la suite normale; l'un d'eux serait égal à a.

1° $a_1, a_2, \ldots, a_p$ *non tous commensurables.*

Comme exemple de suite normale, on peut citer les valeurs approchées successives découvertes par Hermite. Il a montré qu'on pouvait trouver une suite infinie de systèmes de fractions

$$\frac{m_1}{n}, \quad \frac{m_2}{n}, \quad \ldots, \quad \frac{m_p}{n},$$

telles que leurs différences respectives avec $a_1, a_2, \ldots, a_p$ soient en valeur absolue plus petites que $\frac{\lambda_p}{n\sqrt[p]{n}}$, λ_p étant un nombre fixe qui ne dépend que de p $\left(\lambda_p = \frac{p-1}{p}\right.$ d'après M. Minkowsky$\left.\right)$.

En posant donc

$$a_1 = \frac{m_1}{n} + \frac{\varepsilon_n^{(1)}}{n}, \qquad \ldots, \qquad a_p = \frac{m_p}{n} + \frac{\varepsilon_n^{(p)}}{n},$$

les quantités $\varepsilon_n^{(1)}, \ldots, \varepsilon_n^{(p)}$ sont toutes plus petites que $\frac{\lambda_p}{\sqrt[p]{n}}$ et, par suite, tendent vers zéro.

2° $a_1, a_2, \ldots, a_p$ *sont tous commensurables.*

Soit

$$a_1 = \frac{A_1}{B}, \qquad a_2 = \frac{A_2}{B}, \qquad \ldots, \qquad a_p = \frac{A_p}{B}.$$

Soit

$$\frac{m_1}{n}, \quad \frac{m_2}{n}, \quad \ldots, \quad \frac{m_p}{n},$$

un système de fractions non toutes égales respectivement à

$$\frac{A_1}{B}, \quad \frac{A_2}{B}, \quad \ldots, \quad \frac{A_p}{B};$$

on voit comme plus haut que certaines des quantités $\varepsilon_n^{(1)}, \varepsilon_n^{(2)}, \ldots, \varepsilon_n^{(p)}$ sont $\geqq \frac{1}{B}$.

Donc elles ne peuvent pas tendre toutes vers zéro, à moins qu'à partir d'un certain rang, $\frac{m_1}{n}, \frac{m_2}{n}, \ldots, \frac{m_p}{n}$ ne soient tous égaux respectivement à $\frac{A_1}{B}, \ldots, \frac{A_p}{B}$.

Alors tous les ε sont nuls.

Corollaire. — Soient

$$\frac{m_1}{n}, \quad \frac{m_2}{n}, \quad \ldots, \quad \frac{m_p}{n},$$
$$\frac{m'_1}{n'}, \quad \frac{m'_2}{n'}, \quad \ldots, \quad \frac{m'_p}{n'},$$

deux systèmes de la suite normale de systèmes.

La condition nécessaire et suffisante pour que $a_1, a_2, \ldots, a_p$ soient tous commensurables est que, à partir d'un certain rang, tous les déterminants du second ordre de la forme $m_h n' - m'_h n$ soient nuls, ou encore que tous les déterminants du second ordre extraits de la matrice

$$\left\| \begin{matrix} m_1, & m_2, & \ldots, & m_p, & n \\ m'_1, & m'_2, & \ldots, & m'_p, & n \end{matrix} \right\|$$

soint nuls.

3. *Propriété fondamentale des suites normales.*

Mais le cas où $a_1, a_2, \ldots. a_p$ sont tous commensurables n'est que le dernier d'une série d'autres cas que nous allons examiner maintenant.

Dire, en effet, que $a_1, a_2, \ldots, a_p$ sont égaux à $\frac{A_1}{B}, \frac{A_2}{B}, \ldots, \frac{A_p}{B}$, c'est-à-dire qu'on a

$$\begin{gathered} B a_1 - A_1 = 0, \\ B a_2 - A_2 = 0, \\ \ldots\ldots\ldots\ldots\ldots, \\ B a_p - A_p = 0, \end{gathered}$$

c'est donc dire qu'il existe entre $a_1, a_2, \ldots, a_p$, p relations linéaires distinctes à coefficients entiers.

Réciproquement, si, entre $a_1, a_2, \ldots. a_p$, il existe p relations linéaires distinctes à coefficients entiers, en résolvant ces p relations, on voit que $a_1, a_2, \ldots, a_p$ sont commensurables. Alors on voit que ce cas n'est qu'un cas particulier de celui où il existe r de ces relations ($r \leqq p$).

Il faut donc examiner ces cas. Pour cela, nous démontrons le théorème suivant qui peut être considéré comme la propriété fondamentale des systèmes normaux et qui est une généralisation de celle du n° 1.

Si, entre des nombres a_1, a_2 ..., a_p, il existe une relation linéaire à coefficients entiers

$$(1) \qquad A_1 a_1 + A_2 a_2 + \ldots + A_p a_p + B = 0,$$

la même relation existe entre les fractions d'un système normal

$$A_1 \frac{m_1}{n} + A_2 \frac{m_2}{n} + \ldots + A_p \frac{m_p}{n} + B = 0,$$

pourvu que le dénominateur du système dépasse une certaine limite.

En effet, on peut poser

$$a_1 = \frac{m_1}{n} + \frac{\varepsilon_n^{(1)}}{n},$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$a_p = \frac{m_p}{n} + \frac{\varepsilon_n^{(p)}}{n},$$

les ε tendant vers zéro.

L'égalité (1) devient alors

$$A_1\left(\frac{m_1}{n} + \frac{\varepsilon_n^{(1)}}{n}\right) + A_2\left(\frac{m_2}{n} + \frac{\varepsilon_n^{(2)}}{n}\right) + \ldots + A_p\left(\frac{m_p}{n} + \frac{\varepsilon_n^{(p)}}{n}\right) + B = 0,$$

d'où

$$(2) \quad A_1 m_1 + A_2 m_2 + \ldots + A_p m_p + B n = -\left(A_1 \varepsilon_n^{(1)} + A_2 \varepsilon_n^{(2)} + \ldots + A_p \varepsilon_n^{(p)}\right).$$

Comme le premier membre de cette égalité est entier, et que le second membre tend vers zéro, il arrivera, à partir d'un certain rang, que ces deux membres seront nuls. On a alors

$$(3) \qquad A_1 m_1 + A_2 m_2 + \ldots + A_p m_p + B n = 0,$$

$$(4) \qquad A_1 \frac{m_1}{n} + A_2 \frac{m_2}{n} + \ldots + A_p \frac{m_p}{n} + B = 0.$$

Réciproquement. — Si la relation (4) a lieu à partir d'un certain rang, la relation (3) a lieu aussi. Alors, le premier membre de l'égalité (2) est nul, et, comme le second tend vers zéro, on voit, en passant à la limite, que l'égalité (1) est vérifiée.

Le théorème du n° 1 se généralise de la façon suivante :

Soient

$$\begin{array}{cccc}
\dfrac{m_1}{n}, & \dfrac{m_2}{n}, & \ldots, & \dfrac{m_p}{n}, \\
\dfrac{m_1^{(1)}}{n_1}, & \dfrac{m_2^{(1)}}{n_1}, & \ldots, & \dfrac{m_p^{(1)}}{n_1}, \\
\ldots & \ldots & \ldots & \ldots, \\
\dfrac{m_1^{(p)}}{n_p}, & \dfrac{m_2^{(p)}}{n_p}, & \ldots, & \dfrac{m_p^{(p)}}{n_p},
\end{array}$$

$(p+1)$ termes quelconques d'une suite normale relative à des nombres a_1, a_2. ..., a_p.

La condition nécessaire et suffisante pour qu'entre ces nombres il y ait r relations linéaires, distinctes, à coefficients entiers (ou simplement commensurables) est que les déterminants d'ordre $p+2-r$ extraits du Tableau

$$\begin{array}{ccccc}
m_1, & m_2, & \ldots, & m_p, & n, \\
m_1^{(1)}, & m_2^1, & \ldots, & m_p^1, & n_1, \\
\ldots & \ldots, & \ldots, & \ldots, & \ldots, \\
m_1^{(p)}, & \ldots, & \ldots, & \ldots, & n_p,
\end{array}$$

soient, à partir d'un certain rang dans ce Tableau, tous nuls.

En effet, il faudra qu'à partir d'un certain rang les équations telles que

$$(5) \qquad m_1^{(h)} A_1 + m_2^{(h)} A_2 + \ldots + m_p^{(h)} A_p + n^{(h)} B = 0$$

et toutes les suivantes soient satisfaites par r systèmes indépendants de valeurs des inconnues $A_1, A_2, \ldots, A_p, B$ non toutes nulles.

Par conséquent il faudra que les déterminants de l'énoncé soient nuls.

Réciproquement, s'ils le sont, les équations en nombre infini (5) se réduisent à $p+1-r$ d'entre elles. Ce sont des équations homogènes à $p+1$ inconnues. Elles auront donc r systèmes de solutions indépendantes. Comme les coefficients des équations sont entiers, on peut supposer les solutions commensurables et par suite entières.

On trouve ainsi r relations linéaires à coefficients entiers entre les valeurs

$$\frac{m_1^{(h)}}{n}, \quad \frac{m_2^{(h)}}{n}, \quad \ldots, \quad \frac{m_p^{(h)}}{n}$$

et, par suite aussi, entre

$$a_1, \quad a_2, \quad \ldots, \quad a_p \quad (^1).$$

4. La question précédente intervient dans la *solution approchée en nombres entiers des équations linéaires* (²). La première chose à faire est en effet de découvrir les relations *linéaires exactes* à coefficients entiers qui existent entre les coefficients. Autrement dit on est amené à la question de la *résolution exacte en nombres entiers des équations linéaires à coefficients quelconques*.

S'il s'agit d'une équation homogène, soit $p+1$ le nombre d'inconnues. Après avoir divisé par le coefficient de x_{p+1} on peut écrire l'équation

$$a_1 x_1 + a_2 x_2 + \ldots + a_p x_p + x_{p+1} = 0.$$

La question ne dffère pas de celle qu'on vient de traiter. Les valeurs des inconnues $x_1, x_2, \ldots, x_{p+1}$ sont les nombres que nous avons appelés plus haut $A_1, A_2, \ldots, A_p$, B.

Considérons maintenant une équation non homogène. On peut la diviser par le terme qui ne contient pas d'inconnue et l'écrire

$$a_1 x_1 + \ldots + a_p x_p + 1 = 0.$$

Pour qu'elle soit possible il faut que la suivante

$$a_1 x_1 + a_2 x_2 + \ldots + a_p x_p + x_{p+1} = 0$$

le soit. Il faudra donc d'abord que les déterminants d'ordre $p+1$

(¹) Il est bien évident que la condition énoncée ne peut servir à constater par un simple calcul numérique l'existence de relations entre des incommensurables. Car, si loin qu'on pousse le Tableau précédent, si la condition n'est pas satisfaite, elle le sera peut-être plus loin. Inversement, si elle l'est elle cessera peut-être de l'être plus loin. Mais cela est dans la nature des choses. Pour un seul nombre déjà, il ne suffit pas de savoir calculer ses chiffres décimaux l'un à la suite de l'autre, pour savoir s'il est commensurable ou non.

(²) L. Kronecker, *Monatsber. der K. P. Ak. d. Wiss. zu Berlin,* 1884, p. 1179, 1193, 1271, 1299. Werke 3¹, p. 49, 109.

extraits du Tableau des systèmes de valeurs normales relatives aux nombres $a_1, a_2, \ldots, a_p$ soient tous nuls à partir d'un certain rang.

Cette condition étant remplie, les équations

$$m_1^{(h)} x_1 + m_2^{(h)} x_2 + \ldots + m_p^{(h)} x_p + n^{(h)} x_{p+1} = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

se réduiront à r d'entre elles. Il restera à exprimer qu'elles ont un ou des systèmes de solutions ou $x_{p+1} = 1$, autrement dit que les r équations à coefficients entiers

$$m_1^{(h)} x_1 + m_2^{(h)} x_2 + \ldots + m_p^{(h)} x_p + n^{(h)} = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

sont possibles en nombres entiers. La condition est connue et l'on sait trouver la solution générale (¹).

Considérons enfin un système d'équations. On peut voir si chaque équation prise à part est possible et en trouver la solution générale. On sait que cette solution générale est une expression linéaire à coefficients entiers de variables entières. La question de savoir si le système a une solution, c'est-à-dire si les solutions des différentes équations peuvent coïncider, est donc ramenée à une question d'analyse indéterminée du premier degré que l'on sait résoudre.

5. On peut simplifier la méthode donnée pour la résolution de l'équation

$$a_1 x_1 + \ldots + a_p x_p + b = 0. \tag{6}$$

Celle donnée plus haut exige la connaissance d'une suite normale pour p nombres; cette suite peut se trouver par l'algorithme d'Hermite relatif à p nombres.

La simplification en question consiste à n'appliquer que l'algorithme relatif à $p - 1$ nombres. C'est une généralisation de la méthode donnée par Hermite lui-même dans le cas de $p = 2$ (²).

(¹) Voir par exemple : STIELTJES, *Essai sur la théorie des nombres* (*Annales de la Faculté des Sciences de Toulouse*), t. IV, 1890.

(²) HERMITE, *Journal für Mathematik*, t. XL, 1850, p. 261, et t. LXXXVIII, 1880, p. 12.

L'équation peut s'écrire

$$\frac{a_1}{a_p} x_1 + \frac{a_2}{a_p} x_2 + \ldots + \frac{a_{p-1}}{a_p} x_{p-1} + x_p + \frac{b_p}{a_p} = 0.$$

ou en posant, d'après l'algorithme en question,

$$\frac{a_1}{a_p} = \frac{m_1}{n} + \frac{\varepsilon_1}{n\sqrt[p-1]{n}}, \quad \ldots, \quad \frac{a_{p-1}}{a_p} = \frac{m_{p-1}}{n} + \frac{\varepsilon_{p-1}}{n\sqrt[p-1]{n}},$$

puis, multipliant toute l'équation par n,

$$\left(m_1 + \frac{\varepsilon_1}{\sqrt[p-1]{n}}\right) x_1 + \left(m_2 + \frac{\varepsilon_2}{\sqrt[p-1]{n}}\right) x_2 + \ldots$$
$$+ \left(m_{p-1} + \frac{\varepsilon_{p-1}}{\sqrt[p-1]{n}}\right) x_{p-1} + n x_p + \frac{n b_p}{a_p} = 0.$$

Soit A_n le nombre entier le plus voisin de $\frac{n b_p}{a}$; on a

$$\frac{n b_p}{a_p} = A_n + r_n \qquad |r_n| \leqq \frac{1}{2}.$$

L'équation s'écrit alors

$$m_1 x_1 + m_2 x_2 + \ldots + m_{p-1} x_{p-1} + n x_p + A_n$$
$$= -\left(\frac{\varepsilon_1 x_1 + \varepsilon_2 x_2 + \ldots + \varepsilon_{p-1} x_{p-1}}{\sqrt[p-1]{n}}\right) - r_n.$$

Or, n croissant indéfiniment, le second membre devient plus petit que 1, et, comme le premier membre est entier, c'est que les deux membres sont nuls. On a donc

$$m_1 x_1 + m_2 x_2 + \ldots + m_{p-1} x_{p-1} + n x_p + A_n = 0.$$

Faisons croître n; nous aurons un certain nombre d'équations de cette forme, dont on pourra trouver la solution générale. Il restera à savoir si cette solution satisfait à l'équation (6).