ANNALES SCIENTIFIQUES DE L'É.N.S.

B.-I. CLASEN

Solutions entières de l'équation indéterminée $Ax + By = S$

Annales scientifiques de l'É.N.S. 1re série, tome 4 (1867), p. 347-354
<http://www.numdam.org/item?id=ASENS_1867_1_4__347_0>

SOLUTIONS ENTIÈRES

DE

L'ÉQUATION INDÉTERMINÉE

$$Ax + By = S,$$

PAR M. L'ABBÉ B.-I. CLASEN,
PROFESSEUR A LUXEMBOURG.

Nous supposerons A, B et S positifs et entiers; toutes les équations de ce genre se ramènent facilement à ce cas. Soit $A > B$, on trouve la solution la plus simple ou l'une des deux plus simples solutions en formant le tableau suivant :

	b	c	d	e	...	i	k	l	m	n	o	p	q
A	B	C	D	E	...	I	K	L	M	N	O	P	Q
$\pm\alpha$	$\mp\beta$	$\pm\gamma$	$\mp\delta$	$\pm\varepsilon$	...	$+\iota$	$-\varkappa$	$+\lambda$	$-\mu$	$+\nu$			
A′	B′	C′	D′	E′	...	I′	K′	L′	M′	o			

La deuxième ligne contient les différents diviseurs qu'on trouve en cherchant d'après la méthode ordinaire le plus grand commun diviseur de A et de B,

La première ligne contient les quotients correspondants à ces diviseurs, de sorte que

$$A = bB + C, \quad B = cC + D, \ldots.$$

Pour former la troisième ligne on décompose S en différentes parties, multiples chacune d'un des nombres A, B, C,..., c'est-à-dire qu'on satisfera à l'équation suivante en attribuant des valeurs entières à $\alpha, \beta, \gamma, \ldots$

$$S = \alpha A + \beta B + \gamma C + \ldots + \pi P + \chi Q.$$

De quelque manière qu'on choisisse les nombres $\alpha, \beta, \gamma, \ldots, \pi$, pourvu seulement que $S - \alpha A - \beta B - \gamma C - \ldots - \pi P$ ne soit pas négatif, χ sera entier et positif (ou zéro) si S est divisible par Q, et fractionnaire si S n'est pas divisible par Q, parce que les nombres A, B, C,..., P sont tous divisibles par Q, le plus grand commun diviseur de A et B. Pour que cette décomposition de S soit possible, il faut donc et il suffit que S soit divisible par Q. C'est, comme on sait, la condition même de la possibilité de notre problème. La justesse de notre méthode ne dépend pas de la manière dont on décompose S en multiples de A, B,.... En appliquant nos règles avec les précautions nécessaires on pourrait même attribuer à $\alpha, \beta, \ldots$ des valeurs négatives; mais pour trouver la plus simple solution et pour la trouver par les plus simples calculs, on décomposera S de préférence en multiples des plus grands nombres de la deuxième ligne, et l'on divisera par conséquent d'abord S par A, on désignera par α la partie entière du quotient de cette division, on en divisera le reste par B pour trouver de la même manière β et ainsi de suite. Généralement un certain nombre des facteurs $\alpha, \beta, \gamma, \ldots$ seront égaux à zéro. Soit ν le dernier de ceux qui ne sont pas nuls; nous pourrons négliger les suivants. Ces facteurs $\alpha, \beta, \gamma, \ldots, \nu$ formeront la troisième ligne et seront placés au-dessous des nombres A, B, C,..., N qu'ils multiplient dans l'expression de S. Nous donnerons au dernier de ces facteurs ν le signe $+$, à l'avant-dernier μ le signe $-$, à λ le signe $+$, et ainsi de suite, en faisant alterner dans la troisième ligne les signes $+$ et $-$.

Dans la quatrième ligne le nombre qui correspond au dernier nombre ν de la troisième ligne ainsi que les suivants sont égaux à zéro. La loi générale par laquelle chaque nombre de cette ligne se déduira de ceux qui le suivent et de ceux de la troisième ligne est donnée par la formule

$$C' = dD' + E' \mp \delta;$$

si E' ne figure pas au tableau ce nombre est censé être nul.

La solution cherchée sera alors

$$x = \pm B' + \alpha,$$
$$y = \mp A'.$$

Les signes $+$ ou $-$ qu'il faut choisir pour B′ et A′ sont les signes respectivement contraires à ceux de β et α du tableau.

Démonstration.

D'après la manière dont notre tableau a été formé, nous avons

1° $$M' = 0n + 0 + \nu = \nu$$

et

(1) $$M'N = \nu N;$$

2° $$L = mM + N, \qquad LM' = mMM' + M'N,$$
$$L' = mM' + 0 - \mu, \quad L'M = mMM' - \mu M,$$

d'où l'on tire, en comparant avec l'équation (1),

(2) $$LM' - L'M = \mu M + \nu N \ (*);$$

3° $$K = lL + M, \qquad KL' = lLL' + ML',$$
$$K' = lL' + M' + \lambda, \quad K'L = lLL' + M'L + \lambda L,$$

d'où l'on tire, en comparant avec l'équation (2),

$$-KL' + K'L = \lambda L + \mu M + \nu N;$$

et en général si

(3) $$\pm CD' \mp C'D = \delta D + \varepsilon E + \ldots + \nu N;$$

on vérifie cette loi pour les nombres qui précèdent C, C′, D et D′, dans

(*) On fera bien d'observer que les signes des termes qui contiennent L′, M′ sont les signes contraires de λ et μ.

les deuxième et troisième lignes, car

$$\begin{aligned} B &= cC + D, & BC' &= cCC' + C'D, \\ B' &= cC' + D' \pm \gamma, & B'C &= cCC' + CD' \pm \gamma C, \end{aligned}$$

d'où l'on tire, en comparant avec l'équation (3) et en observant que les signes supérieur et inférieur de $\pm\gamma$ correspondent respectivement aux signes supérieurs et inférieurs de l'équation (3),

$$\mp BC' \pm B'C = \pm CD' \mp C'D + \gamma C = \gamma C + \delta D + \varepsilon E + \ldots + \nu N.$$

Cette loi étant vérifiée pour $LM' - L'M$ (2) doit par conséquent être générale et

$$\begin{aligned} &\pm AB' \mp A'B = \beta B + \gamma C + \ldots + \nu N. \\ &\pm AB' \mp A'B + \alpha A = S, \\ &A(\pm B' + \alpha) \mp BA' = S. \end{aligned}$$

Donc $x = \pm B' + \alpha$, $y = \mp A'$ est une solution de l'équation $Ax + By = S$.

Si S a été décomposé d'après la méthode que nous avons expliquée, 1° les nombres A', B', C' seront tous positifs, et 2° la solution qu'on trouvera sera l'une des deux solutions les plus simples.

1° Puisque $\delta D + \varepsilon E + \ldots + \nu N$ est le reste d'une division par C,

$$C > \delta D + \varepsilon E + \ldots + \nu N, \tag{4}$$

et, comme $C = dD + E$,

$$dD + E > \delta D + \varepsilon E + \ldots + \nu N.$$

Donc

$$d + \frac{E}{D} > \delta.$$

D n'est pas nul, sans quoi d et δ dont nous nous occupons ici n'existeraient pas. Si E est nul, c'est-à-dire si D est le dernier nombre de la deuxième ligne, alors

$$d > \delta. \tag{5}$$

En tout cas, comme $D > E$, il faut que l'on ait

$$d + 1 > \delta. \tag{6}$$

$M' = \nu$. Ce dernier nombre de la troisième ligne étant d'après nos règles affecté du signe $+$, il s'ensuit que $M' > o$.

$$L' = mM' - \mu,$$
$$K = mM + N,$$
$$K > \mu M + \nu N,$$

d'après l'inégalité (4); donc

$$mM + N > \mu M + \nu N,$$

et puisque $\nu = M'$,

$$mM + N > \mu M + NM',$$

$$m > \mu + \frac{N(M' - 1)}{M} \ (*),$$

$$mM' - \mu \quad \text{ou} \quad L' > \frac{NM'(M' - 1)}{M} + \mu(M' - 1),$$

M' étant entier et positif, il s'ensuit que $L' > o$.

Je dis maintenant qu'en général si $E' > o$ et $D' > o$, on aura aussi $C' > o$.

En effet

$$C' = dD' + E' \mp \delta,$$

et puisque δ est tout au plus égal à d, et que D' est entier et positif, C' est tout au moins égal à E' et par conséquent plus grand que zéro. A', B', C',... sont donc tous positifs parce que L' et M' le sont.

2° Je dis que $\frac{M}{Q} > M'$. N peut être le dernier nombre de la deuxième ligne. Alors Q, le plus grand commun diviseur de A et B, est ce même nombre N, et je dois prouver que $\frac{M}{N} > M'$.

Dans ce cas

$$M = nN, \quad \frac{M}{N} = n$$

et d'après l'inégalité (5)

$$n \quad \text{ou} \quad \frac{M}{N} > \nu \quad \text{ou} \quad M'.$$

(*) Inutile de rappeler que tous les nombres de la deuxième ligne, ainsi que $\alpha, \beta, \gamma, \ldots$, sont positifs et entiers.

Si N n'est pas le plus grand commun diviseur de A et B, alors

$$M = nN + O,$$
$$\frac{M}{Q} = n\frac{N}{Q} + \frac{O}{Q},$$

Q étant alors moindre que N et pouvant tout au plus être égal à O, $\frac{M}{Q}$ est plus grand que $n + 1$ et par conséquent plus grand que ν (6) ou M'. Donc

$$\frac{M}{Q} > M'.$$

J'en tire

$$\frac{L}{Q} > L'.$$

$$L = mM + N,$$
$$\frac{L}{Q} = m\frac{M}{Q} + \frac{N}{Q},$$
$$L' = mM' + \mu.$$

Donc

$$\frac{L}{Q} > mM' + \frac{N}{Q} > L'.$$

Je dis maintenant qu'en général si $\frac{E}{Q} > E'$, $\frac{D}{Q} > D'$, on aura aussi $\frac{C}{Q} > C'$.

En effet

$$C = dD + E,$$
$$\frac{C}{Q} = d\frac{D}{Q} + \frac{E}{Q}.$$

$\frac{D}{Q}$, qui est par supposition plus grand que D' et entier parce que Q divise tous les nombres de la deuxième ligne, doit au moins être égal à $D' + 1$, et $\frac{C}{Q}$ est au moins égal à $dD' + \frac{E}{Q} + d$.

$$C' = dD' + E' \mp \delta,$$

d n'étant pas plus grand que δ (6) et $\frac{E}{Q}$ étant plus grand que E' par supposition, nous aurons $\frac{C}{Q} > C'$.

Nous venons de démontrer que $\frac{M}{Q} > M'$ et $\frac{L}{Q} > L'$, il faut donc que $\frac{K}{Q} > K'$, et de là on tire

$$\frac{I}{Q} > I', \ldots, \quad \frac{A}{Q} > A'.$$

La valeur générale entière de y est, comme on sait, en désignant par t un entier quelconque, $\mp\left(A' \pm \frac{A}{Q} t\right)$, le signe qui précède la parenthèse étant le signe contraire du α de notre tableau. Il suit de ce que $A' < \frac{A}{Q}$, que la plus petite valeur entière de y du signe contraire au α de notre tableau est $\mp A'$.

Exemple. $2072x + 427y = 27\,300$.

Si l'on commence la décomposition de 27 300 par le nombre 427, les calculs à faire se disposent de la manière suivante :

	4	1	5	1	3	2
2072	427	364	63	49	14	7
+0	−63	+1	−0	+0	−2	+1
4	14	11	2	1	1	0

$$y = -4, \quad x = +14.$$

Troisième ligne. — La division de 27 300 par 427 donne pour quotient 63;

Le reste de cette division, 399, divisé par 364 donne pour quotient 1;

Le reste de cette division, 35, divisé par 14 donne pour quotient 2;

Le reste de cette division, 7, divisé par 7 donne pour quotient 1.

La *quatrième ligne* a été formée par les opérations suivantes :

$$\begin{aligned}
2.0 &+ 0 + 1 = 1,\\
3.1 &+ 0 - 2 = 1,\\
1.1 &+ 1 + 0 = 2,\\
5.2 &+ 1 - 0 = 11,\\
1.11 &+ 2 + 1 = 14,\\
4.14 &+ 11 - 63 = 4.
\end{aligned}$$

Si l'on commence la décomposition de 27 300 par le nombre 2072, on trouve $27\,300 = 13.2072 + 1.364$ et le tableau devient

	4	
2072	427	364
+13	−0	+1
4	1	

$$y = -4, \quad x = 1 + 13 = 14.$$

Autre exemple. $45y + 65x = 3300$.

	1	2	4
65	45	20	5
−50	+1	−0	+1
4	3	1	

$$y = +4, \quad x = -3 + 50 = 47.$$

Si l'on avait à résoudre l'équation $45y - 65x = 3300$ on la ramènerait à ce cas en posant $x = -u$; l'équation deviendrait

$$45y + 65u = 3300, \quad y = 4, \quad u = 47, \quad x = -47.$$

Observation. — Pilatte avait indiqué dans les *Annales de Gergonne*, 1812, un algorithme pour trouver des solutions simples des équations indéterminées du premier degré. M. Catalan l'a publié et recommandé plusieurs fois (*Géomètre*, 1836; *Cours de Mathématiques*, de Blum; *Nouvelles Annales de Mathématiques*, t. III). Il a quelque analogie avec notre méthode. Celle-ci conduit cependant par des calculs beaucoup plus simples à des solutions souvent plus simples également, et elle a été trouvée par des considérations d'un ordre très-différent.

FIN DU TOME QUATRIÈME.