

MATHÉMATIQUES.

ANALYSE INDÉTERMINÉE DU PREMIER DEGRÉ. (1)

Un problème est, en général, indéterminé, lorsque le nombre des équations auxquelles il conduit est moindre que le nombre des inconnues. La partie de l'Algèbre, appelée *Analyse indéterminée*, a pour objet l'examen des conditions auxquelles doivent satisfaire les coefficients des équations, pour que les inconnues admettent des valeurs entières. Elle se propose aussi la recherche de ces valeurs, appelées *solutions entières*. Nous ne parlerons, ici, que de l'*Analyse indéterminée du premier degré*.

I. Généralités sur l'équation $ax + by = c$.

1. Considérons l'équation du premier degré, à deux inconnues,

$$ax + by = c, \quad (1)$$

dans laquelle on peut toujours supposer a, b, c entiers, premiers entre eux, et c positif.

2. Si les coefficients a, b ne sont pas premiers entre eux, l'équation n'admet aucune solution entière.

Soit m un facteur commun à ces coefficients, de manière que $a = ma', b = mb'$: l'équation peut être mise sous la forme $a'x + b'y = \frac{c}{m}$. Par hypothèse, c n'est pas divisible par m ; donc, si l'on remplaçait x et y par des valeurs entières, on aurait un nombre entier égal à une fraction.

3. Si a et b sont premiers entre eux, l'équation (1) admet des solutions entières.

Supposons d'abord a et b positifs, et $a < b$. L'équation, résolue par rapport à x , donne $x = \frac{c - by}{a}$. Or, si l'on divise par a

(1) Ce résumé d'une théorie importante est publié pour les jeunes gens qui se destinent aux Écoles spéciales. Peut-être sera-t-il suivi d'autres Notes sur l'Arithmétique, l'Algèbre, la Géométrie analytique, etc.

les $a - 1$ premiers multiples de b , aucune division ne se fait exactement; et les restes obtenus sont, dans un certain ordre, les nombres $1, 2, 3, \dots, a - 1$ (*). Un de ces restes est donc égal à celui que donne la division de c par a ; et la différence $c - by$ est divisible par a .

Si le coefficient a , par exemple, était négatif, il suffirait de changer x en $-x'$, et d'appliquer, à la nouvelle équation, la démonstration précédente. La proposition énoncée est donc générale.

4. Si $x = \alpha$, $y = \beta$ forment une solution de l'équation (1), toutes les solutions sont données par le système des formules

$$x = \alpha - b\theta, \quad y = \beta + a\theta; \quad (2)$$

dans lesquelles θ est un entier quelconque, positif, négatif ou nul.

L'équation (1) étant vérifiée par $x = \alpha$, $y = \beta$, on a, identiquement,

$$ax + by = c;$$

d'où, en éliminant c ,

$$a(x - \alpha) + b(y - \beta) = 0. \quad (3)$$

Cette équation donne

$$x - \alpha = -\frac{b(y - \beta)}{a}.$$

$x - \alpha$, $y - \beta$ doivent être entiers; et, par hypothèse, a , b sont premiers entre eux; donc, par un principe connu, a divise $y - \beta$ (*). Soit θ le quotient, de manière que $y - \beta = a\theta$; alors $x - \alpha = -b\theta$.

5. D'après cela, les valeurs de x et de y forment deux progressions par différence, ayant pour raisons b et $-a$, ou $-b$ et a .

6. Il suit aussi, de ce qui précède, que la résolution complète de l'équation (1) se réduit à la recherche d'une seule solution de cette équation.

II. Recherche d'une solution de $ax + by = c$.

7. D'après ce que l'on a vu ci-dessus (3), on pourrait trouver

(*) *Nouvelles Annales de Mathématiques*, tome I, p. 460.

(*) *Manuel d'Arithmétique et d'Algèbre*.

une solution en résolvant l'équation par rapport à l'inconnue x qui a le plus petit coefficient, et attribuant à y les valeurs 1, 2, 3, ... $a - 1$ (*). Ce tâtonnement ne peut être employé que si le coefficient a est fort petit. La méthode suivante est préférable (*).

8. Soit, pour plus de régularité dans la notation,

$$ay + bx = A \quad (4)$$

l'équation proposée; et supposons $b < a$.

On a

$$x = \frac{A - ay}{b};$$

ou, en appelant Q, q, B, c les quotients et les restes que donnent A, a divisés par b :

$$x = Q - qy + \frac{B - cy}{b}.$$

Nous voulons que x et y soient entiers; nous devons donc attribuer à y une valeur qui rende entière la quantité $\frac{B - cy}{b}$.

Autrement dit, la résolution de l'équation (4) est ramenée à la résolution de

$$\frac{B - cy}{b} = z,$$

ou de

$$bz + cy = B. \quad (5)$$

Cette équation (5) est plus simple que la proposée; car c , reste de la division de a par b , est inférieur à b . Résolvons l'équation (5) par rapport à l'inconnue qui a le plus petit coefficient; nous aurons

(*) Je laisse de côté le cas particulier où c serait divisible par l'un des deux coefficients. Il est évident que si a divise c , il suffit, pour avoir une solution, de prendre

$$x = \frac{c}{a}, \quad y = 0;$$

etc.

(*) Elle est due à *Bachet de Méziriac*. (*Problèmes plaisants et délectables*. — 1624).

$$y = \frac{B - bz}{c} = Q' - q'z + \frac{C - dz}{c};$$

en représentant par Q' , q' les quotients entiers de B, b par c ; et par C, d les restes correspondants. Répétant le raisonnement ci-dessus, on verra que la valeur de z doit rendre entière la quantité $\frac{C - dz}{c}$, ou que l'équation (5) se réduit à celle-ci :

$$cr + dz = C; \quad (6)$$

dans laquelle les coefficients c, d sont respectivement inférieurs à b, c . À son tour, cette équation (6) en donne une encore plus simple; et ainsi de suite.

9. *Les coefficients c, d, e, \dots sont les restes successifs que donnerait l'opération du plus grand commun diviseur, effectuée sur a et b .*

Car c est le reste de la division de a par b ; de même, d est le reste de la division de b par c ; etc. Par hypothèse, a et b sont premiers entre eux; donc l'opération dont il s'agit conduira nécessairement à un dernier reste égal à l'unité. Ainsi, la résolution de l'équation (4) se réduit à celle d'une équation

$$u + gv = G,$$

dans laquelle le coefficient de l'une des inconnues est 1. Or, si l'on attribue à v une valeur entière quelconque, il en résulte, pour u , une valeur entière; et, en remontant successivement, on finira par déterminer les valeurs entières de x, y , correspondant à cette valeur de v .

10. On peut donner au calcul une marche régulière, qui le simplifie considérablement. (1)

Supposons

$$\begin{aligned} x &= \frac{A - ay}{b}, \quad y = \frac{B - bz}{c}, \quad z = \frac{C - cr}{d}, \quad r = \frac{D - ds}{e}, \\ s &= \frac{E - et}{f}, \quad t = \frac{F - fu}{g}, \quad u = \frac{G - gv}{h}, \dots \end{aligned} \quad (7)$$

Dans ces expressions, les quantités c, d, e, f, \dots sont, comme

(1) *L'algorithme* suivant, que je croyais nouveau en juillet 1832, a été trouvé, dès 1812, par M. *Piltate* (voir les *Annales de Mathématiques*, les *Nouvelles Annales* (1844), etc.).

nous l'avons dit, les restes successifs donnés par la recherche du plus grand commun diviseur entre a et b : admettons, pour fixer les idées, que le dernier de ces restes, égal à l'unité, soit h .

Relativement aux quantités B, C, D, \dots la loi de composition est bien simple : B est le reste de la division de A par b ; C est le reste de la division de B par c ; etc.

Le calcul de ces divers termes s'effectue comme l'indique le tableau ci dessous :

a	b	c	d	e	f	g	1
A	B	C	D	E	F	G	0

La ligne supérieure est la même que dans l'opération du plus grand commun (¹). Pour former la seconde ligne, on écrit A sous a ; puis l'on divise ce premier terme par b : on obtient ainsi un reste B , que l'on écrit au-dessous de b , etc. En général : *chaque terme de la ligne inférieure est le reste de la division du terme placé à gauche, par le terme placé au-dessus*. Il est visible que le dernier terme, correspondant au diviseur 1 , est 0 .

Ces deux lignes étant calculées, on détermine les valeurs des inconnues u, t, s, r, z, y, x , au moyen des équations (7) ; c'est-à-dire que :

La valeur de chaque inconnue s'obtient en retranchant, d'un terme de la seconde ligne, le produit du terme écrit au-dessus par la valeur qu'on vient de calculer, et en divisant le reste par le terme placé à la droite du multiplicande.

11. Applications. 1^o Soit

$$89x + 162y = 209.$$

162	89	73	16	9	7	2	1
209	31	31	15	6	6	0	0

D'abord, 162 divisé par 89 donne 73 pour reste ; 89 divisé par 73 donne 16 pour reste ; etc.

(¹) On n'écrit pas les quotients,

En second lieu, 209 divisé par 89 donne 31 pour reste; 31 divisé par 73 donne 31 pour reste; etc.

Les deux lignes étant formées, nous avons, en prenant $v = 0$:

$$u = \frac{0 - 2.0}{1} = 0, \quad t = \frac{6 - 7.0}{2} = 3, \quad s = \frac{6 - 9.3}{7} = -3,$$

$$r = \frac{15 + 16.3}{9} = 7, \quad z = \frac{31 - 73.7}{16} = -30,$$

$$y = \frac{31 + 89.30}{73} = 37, \quad x = \frac{209 - 162.37}{89} = -65.$$

L'équation est donc vérifiée par $x = -65$, $y = 37$. Par suite, les valeurs générales de x et de y sont

$$x = -65 + 162\theta, \quad y = 37 - 89\theta.$$

2° Soit encore l'équation

$$29x - 47y = 112.$$

Elle donne

$$\begin{array}{c|c|c|c|c|c|c|c} -47 & 29 & -18 & 11 & -7 & 4 & -3 & 1 \\ \hline 112 & 25 & 7 & 7 & 0 & 0 & 0 & 0 \end{array}.$$

Puis

$$\frac{0 + 3.0}{1} = 0, \quad \frac{0 - 4.0}{-3} = 0, \quad \frac{0 + 7.0}{4} = 0, \quad \frac{7 - 11.0}{-7} = -1,$$

$$\frac{7 - 18.1}{11} = -1, \quad \frac{25 + 29.1}{-18} = -3, \quad \frac{112 - 47.3}{29} = -1;$$

donc

$$x = -1 + 49\theta, \quad y = -3 + 29\theta.$$

On peut remarquer, d'après cet exemple, que si la ligne inférieure est terminée par une suite de zéros, il est bon de commencer le calcul des inconnues à partir du terme qui précède le premier zéro.

12. *Emploi des fractions continues.* Nous venons d'expliquer le procédé le plus commode, propre à donner une solution de l'équation (1). La théorie des fractions continues peut être appliquée à cette recherche. En effet, si l'on réduit $\frac{a}{b}$ en fraction continue, et que $\frac{a'}{b'}$ soit l'avant-dernière réduite, on a

$$ab' - ba' = \pm 1;$$

d'où, en multipliant par $\pm c$:

$$\pm a.b'c \mp b.a'c = c.$$

Comparant cette identité à la proposée, on voit que celle-ci est vérifiée par

$$x = \pm b'c, \quad y = \mp a'c.$$

Cette méthode a l'inconvénient de donner, pour valeurs particulières de x , y , des multiples de c , lesquels peuvent être fort grands. Au contraire, l'algorithme indiqué ci-dessus conduit, presque toujours, à la solution la plus simple.

13. *Comparaison des deux méthodes.* Soit à trouver une solution de

$$47x + 89y = 508.$$

Le premier procédé conduit à

$$x = 43, \quad y = -17.$$

La réduction en fraction continue donne

$$x = 36.508 = 18\,288,$$

$$y = -19.508 = -9\,652.$$

14. *Application du théorème de Fermat.* Les divers procédés expliqués ci-dessus ne font pas connaître les valeurs des inconnues, en fonction *explicite* des quantités a , b , c . On pourrait se proposer, cependant, de *former immédiatement des valeurs satisfaisant à une équation proposée*. C'est à quoi l'on parvient, dans certains cas, par la méthode suivante, due à Binet ⁽¹⁾.

Supposons que, dans l'équation (1), a soit un nombre premier absolu ⁽²⁾. Posons $x = cx'$, $y = cy'$; d'où $ax' + by' = 1$; puis

$$x' = -\frac{by' - 1}{a}$$

(1) *Journal de l'École polytechnique*, 20^e Cahier.

(2) On peut toujours supposer a , b , c positifs; en changeant, s'il est nécessaire, x en $-x$, y en $-y$; etc.

Il s'agit de rendre entière la quantité $\frac{by' - 1}{a}$: or, d'après le *théorème de Fermat* ⁽¹⁾, $\frac{b^{a-1} - 1}{a}$ est un nombre entier. Si donc nous prenons $y' = b^{a-2}$, la valeur correspondante de x' sera entière; et nous aurons, généralement,

$$x = - \left(c \frac{b^{a-1} - 1}{a} + b\theta \right), \quad y = cb^{a-2} + a\theta.$$

15. *Généralisation.* Si aucun des coefficients a, b n'est premier, désignons par k le nombre des entiers inférieurs et premiers à a : la quantité $b^k - 1$ est divisible par a ⁽²⁾. Donc, en prenant $y' = b^k - 1$, nous aurons $x' = -\frac{b^k - 1}{a}$, valeur entière puis

$$x = - \left(c \frac{b^k - 1}{a} + b\theta \right); \quad y = cb^{k-1} + a\theta. \quad (3)$$

III. Solutions positives.

16. Dans l'équation (1), les coefficients a, b peuvent être positifs ou négatifs; donc, en mettant les signes en évidence, on a ces trois cas distincts :

$$ax - by = c, \quad ax + by = c, \quad ax + by = -c.$$

La dernière équation ne peut, évidemment, admettre aucun système de valeurs positives. Quant à la première, si $x = \alpha, y = \beta$ forment une solution, on a généralement

$$x = \alpha + b\theta, \quad y = \beta + a\theta.$$

Conséquemment, cette équation admet une infinité de solutions positives. Reste à considérer

$$ax + by = c, \quad (1)$$

en supposant a, b, c positifs.

(1) *Nouvelles Annales de Mathématiques*, tome I, p. 463.

(2) *Nouvelles Annales*, tome I, p. 463.

(3) Ces formules sont plus simples que celles de Binet.

17. Représentons toujours par α, β des valeurs particulières de x, y , positives ou négatives : les valeurs générales sont

$$x = \alpha - b\theta, \quad y = \beta + a\theta.$$

Si nous voulons que x, y soient positifs, nous devons prendre l'entier θ de manière qu'il satisfasse aux conditions

$$\theta < \frac{\alpha}{b}, \quad \theta > -\frac{\beta}{a}.$$

Si les limites $\frac{\alpha}{b}, -\frac{\beta}{a}$ ne comprennent entre elles aucun entier, l'équation (1) n'admet aucune solution positive. Dans tous les cas, elle n'en admettra qu'un nombre limité : cherchons quel peut être ce nombre de solutions.

18. Pour cela, représentons par A l'entier immédiatement inférieur à $-\frac{\beta}{a}$, et par B l'entier immédiatement inférieur à $\frac{\alpha}{b}$ (1) : nous ne pouvons attribuer à θ que les valeurs $A + 1, A + 2, \dots, B$, lesquelles sont en nombre $B - A$. D'ailleurs, la différence entre les limites de θ étant $\frac{\alpha}{b} + \frac{\beta}{a} = \frac{c}{ab}$, si l'on appelle q le plus grand nombre entier contenu dans $\frac{c}{ab}$, on a $B - A$ égale q ou $q + 1$. Ainsi, le nombre des solutions positives de $ax + by = c$ est égal à l'un des deux quotients entiers de c par ab (2).

IV. Résolution de l'équation $ax + by + cz = d$.

19. Pour que cette équation, dans laquelle a, b, c, d sont entiers et premiers entre eux, admette des solutions entières, il faut et il suffit que a, b, c , soient premiers entre eux.

On verra, comme au n° 2, que si les coefficients a, b, c , ne sont pas premiers entre eux, l'équation est impossible. La seconde partie de la proposition résultera de ce qui suit.

(1) Comme c n'est supposé divisible ni par a ni par b , aucune des limites $\frac{\alpha}{b}, -\frac{\beta}{a}$ n'est entière.

(2) Ce petit théorème, que je trouve dans mes notes de 1839, est souvent attribué à M. Hermite.

20. Si, parmi les coefficients a , b , c il en est deux qui soient premiers entre eux, on peut exprimer les valeurs des inconnues correspondantes, en fonction de la troisième inconnue et d'une indéterminée.

Dans

$$ax + by + cz = d, \quad (8)$$

supposons a , b premiers entre eux, et transposons cz , nous aurons, en représentant $d - cz$ par t :

$$ax + by = t. \quad (9)$$

Pour satisfaire à cette nouvelle équation, posons $x = tx'$, $y = ty'$; d'où résulte

$$ax' + by' = 1. \quad (10)$$

Si nous pouvons déterminer un système de valeurs numériques vérifiant l'équation (10), ces valeurs, multipliées par t , nous donneront une solution de l'équation (9). Or, a et b sont premiers entre eux; donc au moyen d'une des méthodes ci-dessus exposées, nous pourrons calculer des valeurs $x' = \alpha$, $y' = \beta$, satisfaisant à l'équation (10); et nous aurons, comme solution générale de l'équation (8):

$$x = \alpha (d - cz) - b\theta, \quad y = \beta (d - cz) + a\theta; \quad (11)$$

z et θ restant arbitraires.

21. Si, au contraire, deux quelconques des coefficients a , b , c ne sont pas premiers entre eux, les valeurs des inconnues sont fonctions de deux indéterminées.

Soit m le plus grand commun diviseur des coefficients a , b ; nous pouvons mettre l'équation (8) sous la forme

$$a'x + b'y = \frac{d - cz}{m}; \quad (12)$$

a' , b' étant les quotients de a , b par m : ces quotients sont premiers entre eux.

Représentons par t le second membre de l'équation (12), lequel doit être entier: les inconnues z , t doivent satisfaire à la condition

$$cz + mt = d. \quad (13)$$

Or, a , b , c sont premiers entre eux; donc c , m sont aussi

premiers entre eux; et l'équation (13) admet des solutions entières, données par les formules

$$z = \gamma - m\theta, \quad t = \mu + c\theta; \quad (14)$$

γ, μ étant des valeurs particulières de z, t .

Actuellement, l'équation (12) devient

$$a'x + b'y = t; \quad (15)$$

et comme a', b' sont premiers entre eux, nous retombons sur le cas traité précédemment (20).

Si donc α, β sont des valeurs entières de x', y' vérifiant l'équation auxiliaire

$$a'x' + b'y' = 1, \quad (16)$$

les valeurs générales de x, y, z sont

$$\left. \begin{aligned} x &= \alpha t - b'\theta' = \alpha (\mu + c\theta) - b'\theta', \\ y &= \beta t + a'\theta' = \beta (\mu + c\theta) + a'\theta', \\ z &= \gamma - m\theta. \end{aligned} \right\} (17)$$

22. *Application.* Soit l'équation

$$6x + 10y + 15z = 1\ 841. \quad (18)$$

Elle donne

$$3x + 5y = \frac{1841 - 15z}{2}, \quad 15z + 2t = 1\ 841.$$

Celle-ci est vérifiée par $z = 1, t = 913$; donc les formules (14) deviennent

$$z = 1 - 2\theta, \quad t = 913 + 15\theta.$$

D'autre part, l'équation $3x + 5y = t$ est vérifiée par $x = 2t, y = -t$: les valeurs générales de x, y, z , sont donc

$$\left. \begin{aligned} x &= 2(913 + 15\theta) - 5\theta', \quad y = -(913 + 15\theta) + 3\theta', \\ z &= 1 - 2\theta. \end{aligned} \right\} (19).$$

V. Solutions positives.

23. Pour montrer la marche à suivre, il suffit de considérer un cas particulier; par exemple, celui que nous venons de traiter. D'après la valeur de z , l'indéterminée θ doit être *nulle*

$$\begin{aligned}x &= -2(609 - 43z) + 5t, \\y &= -11(609 - 43z) + 27t;\end{aligned}$$

t étant un entier quelconque.

La substitution dans la dernière équation la transforme en

$$-147(609 - 43z) + 362t - 7u = 85;$$

d'où l'on conclut

$$t = 3 + 7t', \quad u = -21(609 - 43z) + 143 + 362t'.$$

Ainsi l'entier t n'est plus arbitraire; et l'on doit prendre, au lieu des valeurs précédentes de x, y :

$$\begin{aligned}x &= -2(609 - 43z) + 5(3 + 7t'), \\y &= -11(609 - 43z) + 27(3 + 7t').\end{aligned}$$

Substituant dans la troisième équation, on la change en

$$230z + 101t' = 3\,355.$$

Par suite,

$$z = 8 - 101\theta, \quad t' = 15 + 230\theta;$$

θ étant un entier quelconque.

Enfin

$$\begin{aligned}x &= 10 - 636\theta, \\y &= 1 - 4304\theta, \\u &= 8 - 7943\theta; \\z &= 8 - 101\theta.\end{aligned}$$

avec

Nous avons eu égard, successivement, à toutes les équations données; donc ces dernières valeurs sont les solutions générales cherchées.

VII. Application arithmétique.

25. PROBLÈME. *Quelles sont les valeurs entières de x , les plus générales, qui rendent entières les fractions*

$$\frac{37x + 26}{100}, \quad \frac{53x + 38}{72}, \quad \frac{19x + 22}{12}, \quad \frac{107x + 26}{120}?$$

En décomposant chaque dénominateur en facteurs premiers entre eux, nous pouvons remplacer ces fractions par les suivantes :

$$\frac{37x + 26}{4}, \frac{37x + 26}{25}, \frac{53x + 38}{8}, \frac{53x + 38}{9}, \frac{19x + 22}{3},$$

$$\frac{19x + 22}{4}, \frac{107x + 26}{3}, \frac{107x + 26}{5}, \frac{107x + 26}{8},$$

ou bien, en rejetant la partie entière de chaque fraction :

$$\frac{x + 2}{4}, \frac{12x + 1}{25}, \frac{5x + 6}{8}, \frac{8x + 2}{9}, \frac{x + 1}{3}, \frac{3x + 2}{4},$$

$$\frac{2x + 2}{3}, \frac{2x + 1}{5}, \frac{3x + 2}{8}.$$

Pour rendre entière la fraction $\frac{5x + 6}{8}$, il suffit de rendre entière $\frac{-3x + 6}{8} = \frac{-3(x - 2)}{8}$. Et comme 8 et 3 sont premiers entre eux, la condition donnée se réduit à $\frac{x - 2}{8} = \text{entier}$.

Des simplifications analogues à celle-là se rencontrent dans les fractions $\frac{8x + 2}{9}, \frac{3x + 2}{4}, \frac{2x + 2}{3}$; en sorte qu'on peut les remplacer par $\frac{4x + 1}{9}, \frac{x - 2}{4}, \frac{x + 1}{3}$.

Le problème proposé revient donc à rendre entières les fractions

$$\frac{x + 2}{4}, \frac{12x + 1}{25}, \frac{x - 2}{8}, \frac{4x + 1}{9}, \frac{x + 1}{3}, \frac{x - 2}{4}, \frac{x + 1}{3},$$

$$\frac{2x + 1}{3}, \frac{3x + 2}{8};$$

ou, plus simplement, les fractions

$$\frac{x - 2}{25}, \frac{x - 2}{8}, \frac{x - 2}{9}.$$

Le numérateur commun devant être divisible par 25, 8 et 9, il est visible que

$$x = 2 + 1800\theta,$$

θ étant un entier quelconque.

E. CATALAN.

Liège, 16 octobre 1873.