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

J. BINET

Recherches sur la théorie des nombres entiers et sur la résolution de l'équation indéterminée du premier degré qui n'admet que des solutions entières

Journal de mathématiques pures et appliquées 1re série, tome 6 (1841), p. 449-494.
<http://www.numdam.org/item?id=JMPA_1841_1_6__449_0>

RECHERCHES

SUR

LA THÉORIE DES NOMBRES ENTIERS

ET

SUR LA RÉSOLUTION DE L'ÉQUATION INDÉTERMINÉE DU PREMIER DEGRÉ QUI N'ADMET QUE DES SOLUTIONS ENTIÈRES;

PAR M. J. BINET,

Professeur au Collége de France, ancien Inspecteur de l'École Polytechnique.

On trouvera dans la première partie de ce Mémoire quelques considérations sur les résidus des nombres, qui ont conduit à un procédé pour parvenir au plus grand diviseur de deux nombres entiers, que l'on croit nouveau. La marche de cette méthode permet de l'appliquer à la recherche du polynome qui divise à la fois deux polynomes donnés et que l'on nomme leur plus grand diviseur. Il n'était guère probable que, pour les nombres entiers, on pût rencontrer une méthode plus simple que le procédé que nous a transmis Euclide : nous devons reconnaître que la nouvelle méthode n'accroît pas ordinairement la facilité des opérations arithmétiques, et il en serait ainsi pour l'algèbre; mais elle conduit à des relations d'une simplicité digne de remarque, et qui peuvent être utiles. Elles m'ont fourni un théorème sur les nombres premiers qui n'a, peut-être, pas été remarqué.

Dans la seconde partie du Mémoire, on applique les diverses relations antérieurement obtenues à la résolution, en nombres entiers, de l'équation

$$ax - Ay = 1,$$

A et a étant des entiers donnés. Il en résulte un mode de solution

arithmétique, distinct de celui que l'on pratique ordinairement et qui fut donné en 1613 par Bachet de Méziriac. En ramenant cette méthode à l'algorithme régulier tiré des fractions continues, Lagrange observe qu'elle conserve, au fond, le même principe, et il ajoute « qu'il en est ainsi de toutes celles imaginées depuis Bachet. » (*Mémoires de l'Académie de Berlin*, 1768.)

J'ai publié en 1827 une méthode, à laquelle M. Libri était parvenu de son côté, et qui est fondée sur un principe différent de celui de Bachet : c'est le théorème de Fermat sur le résidu d'un entier, élevé à une puissance marquée par un nombre premier, qui fournit cette solution de la congruence du premier degré. (*Voyez* les Mémoires de M. Libri, et le *Journal de l'École Polytechnique*, XX^{e} cahier.) En employant un théorème d'Euler qui comprend celui de Fermat, M. Poinsot a donné à la solution une expression plus élégante, et plus simple à quelques égards, que la nôtre; et c'est à des considérations analogues que se rattachent de nouvelles recherches de M. Cauchy sur le même objet. (Voy. les *Nouveaux Exercices d'Analyse*, par M. Cauchy, tome II, 1841.) Ces diverses méthodes, curieuses sous le point de vue théorique, se prêtent péniblement au calcul arithmétique, lorsque les coefficients de l'équation donnée sont un peu grands : la méthode de Bachet conserve en ce cas tout l'avantage, et elle est véritablement alors la seule praticable. Celle que nous publions en ce moment nous paraît entraîner habituellement des calculs de même étendue, à peu près; dans quelques circonstances cependant elle est d'un emploi plus simple : c'est ce qui a lieu, par exemple, lorsque l'un des coefficients de l'équation est un nombre premier. Ce cas, auquel on peut ramener tous les autres, présente des facilités particulières dont la méthode de Bachet ne peut profiter.

Quoi qu'il en soit, les amateurs d'arithmétique verront peut-être avec intérêt le nouveau procédé qui leur est offert pour traiter la congruence du premier degré : on sait que cette congruence est la base de théories importantes dans la science des nombres entiers.

PREMIÈRE PARTIE.

[I]. Nous désignerons par A et a deux nombres entiers inégaux, et nous supposerons $A > a$; on pourra opérer la division de A par le diviseur a; soit p le quotient et a_1 le reste de la division. Le dividende A étant égal au produit ap ajouté au résidu a_1, on aura cette équation, provenant de la division exécutée,

$$A = ap + a_1 :$$

l'opération ayant été faite selon le mode habituel de l'arithmétique, fournira un reste a_1 positif et moindre que le diviseur a. Mais si l'on accroît le quotient p d'une unité, le produit $a(p + 1)$ sera supérieur au dividende A, et l'équation de la division pourra être ainsi écrite

$$A = a(p + 1) - a + a_1 = a(p + 1) - (a - a_1) ;$$

puisque a est $> a_1$ la différence $a - a_1$ est positive, et $-(a - a_1)$ est un résidu négatif qui résulte de la division où l'on admettrait un quotient $p + 1$, supérieur d'une unité au quotient p, qui est en usage dans l'arithmétique ordinaire. Lagrange nomme division *en dedans* l'opération usuelle qui exige un reste positif a_1 ; et il désigne par division *en dehors*, ou en excès, celle qui introduit un reste négatif. Dans les deux cas, le reste est de valeur numérique moindre que le diviseur ; et l'on voit que si une division a été exécutée en dedans, puis exécutée en dehors, les résidus a_1 et $a - a_1$ seront tels que leur somme $a_1 + \overline{a - a_1}$ composera le diviseur. Il s'ensuit que si a_1 est $> \frac{1}{2} a$, le résidu de la division en dehors, $a - a_1$, sera $< \frac{1}{2} a$, et réciproquement En employant le quotient p, ou le quotient $p + 1$, on peut donc amener le résidu, positif ou négatif, à une valeur numérique moindre que $\frac{a}{2}$.

Nous écrirons, en général, l'équation de la division sous la forme

$$A = ap \pm a_1,$$

p ayant la valeur convenable au signe admis pour le résidu dont la grandeur numérique a_1 sera toujours $< a$. D'après ce qui vient d'être dit, on poura réduire, si l'on veut, le reste a_1 à une valeur moindre que $\frac{a}{2}$, en lui donnant un signe convenable : il est souvent utile d'en user ainsi pour simplifier les calculs numériques.

Dans une seconde division de A nous allons employer le résidu a_1 comme diviseur ; l'équation provenant de cette division sera

$$A = a_1 p_1 \pm a_2 ;$$

p_1 est le quotient et $\pm a_2$ le résidu, positif ou négatif, de l'opération : on aura d'ailleurs

$$a_2 < a_1 < a.$$

Une troisième division du même A par a_2 amènera l'équation

$$A = a_2 p_2 \pm a_3 :$$

ces divisions de A pourront être continuées à l'aide des résidus subséquents a_4, a_5, . . . , tant que l'on n'aura pas rencontré un reste nul parmi les nombres décroissants $a_1 > a_2 > a_3 \ldots$; mais on parviendra nécessairement à une division qui se fera exactement et sans reste, après un certain nombre d'opérations : cette division sera représentée par l'équation

$$A = a_n p_n ;$$

a_n sera un entier supérieur à 1, ou simplement égal à 1. Il est clair que pour arriver à cette équation l'on aura exécuté un nombre de divisions marqué par $n + 1$, et dans chacune desquelles A aura été employé comme dividende.

[II]. Si toutes les divisions ont été faites de manière à fournir le

moindre résidu, tout au plus égal à la moitié du diviseur de l'opération, on aura

$$a > 2a_1, \quad a_1 > 2a_2, \quad a_2 > 2a_3, \ldots, \quad a_{n-1} > 2a_n,$$

et par conséquent

$$a > 2a_1 > 2^2a_2 > 2^3a_3 \ldots\ldots > 2^n a_n;$$

il s'ensuivrait

$$2^n < \frac{a}{a_n}:$$

Si l'on prend les logarithmes tabulaires des deux membres, on aura $n \log(2) < \log(a) - \log(a_n)$, ou bien $n < \frac{\log(a) - \log(a_n)}{\log(2)}$. Mais $\log(2) = 0{,}301030\ldots$ et la fraction $\frac{1}{\log(2)} = \frac{1}{0{,}301030\ldots} < \frac{10}{3}$; par suite

$$n < \frac{10}{3}[\log(a) - \log(a_n)] < \frac{10}{3}\log(a).$$

Le plus communément le nombre des divisions sera fort au-dessous de cette limite supérieure, quand a sera un peu grand. Si, par exemple, $a = 1000$, la limite supérieure sera $\frac{10}{3} \times 3 = 10$; c'est-à-dire que pour tout nombre qui ne surpassera pas 1000, le nombre des opérations qui amèneront le dernier résidu a_n et les quotients $p, p_1, p_2, \ldots, p_{n-1}$, ne peut s'élever au-dessus de 10 : généralement il sera beaucoup au-dessous de cette limite.

Il n'est pas inutile de remarquer que si l'on a été dans le cas d'effectuer un nombre considérable de divisions, le résidu a_n que l'on a en vue d'obtenir sera un petit nombre par rapport à a, et surtout quand on aura employé les moindres résidus dans toutes les divisions : pour que a_n ne fût pas une petite fraction de a, il faudrait que le nombre n des divisions fût très-petit; et encore il arrivera souvent qu'après peu de divisions, le résidu ne sera plus de quelques unités seulement, ou même l'unité.

La limite $\frac{\log a}{\log(2)}$ est aussi celle du dénombrement des divisions consécutives qu'exige la recherche du plus grand diviseur de A et a, lorsque, pour simplifier le calcul, on a soin d'admettre des résidus positifs ou négatifs, afin de n'employer que des diviseurs moindres que la moitié des dividendes correspondants, à partir de la seconde division. L'utilité de cette marche est manifeste, et je pense que l'on a dû en faire la remarque, quoique je ne la trouve dans aucun Traité. Alors les divisions seront représentées successivement par les formules

$$A = aq \pm \alpha_1, \quad a = \alpha_1 q \pm \alpha_2, \quad \alpha_1 = \alpha_2 q_2 \pm \alpha_3, \text{ etc.}, \quad \alpha_{n'-1} = \alpha_{n'} q_{n'},$$

$n' + 1$ étant le nombre des divisions; et d'après le décroissement des résidus, on aura

$$a > 2\alpha_1 > 2^2\alpha_2 > 2^3\alpha_3 \ldots > 2^{n'}\alpha_{n'}.$$

On tire de là, comme ci-dessus,

$$n' < \frac{\log(a) - \log(\alpha_n)}{\log(2)}.$$

On sait que cette série de divisions fournit les quotients, positifs ou négatifs, dont se composerait la fraction continue représentant la fraction numérique $\frac{a}{A}$. La fraction continue ainsi composée serait, en général, moins étendue que celle dont on fait ordinairement usage, et où l'on n'emploie que des quotients positifs. Au reste, Lagrange a recommandé l'usage des quotients négatifs pour la réduction en fraction continue, dans le cas où plusieurs quotients sont égaux à l'unité. (*Voy.* ses Additions à l'*Algèbre* d'Euler, etc.)

Dans les divisions de l'article précédent, la série des quotients, que nous dénotons par p, p_1, p_2, etc., sera ascendante; plusieurs termes consécutifs p_i, p_{i+1}, ... pourraient être égaux entre eux si l'on ne se servait pas des moindres résidus; mais quand on n'admettra que des résidus au plus égaux à la moitié des diviseurs respectifs,

les quotients augmenteront rapidement, et souvent p_{i+1} sera bien supérieur à $2p_i$.

[III]. Rassemblons les équations des n divisions exécutées,

$$A = ap \pm a_1, \quad A = a_1 p_1 \pm a_2, \ldots, \quad A = a_{n-1} p_{n-1} \pm a_n, \quad (A)$$

où a_n est le dernier résidu, en sorte que $A = a_n p_n$, puisque nous admettons que cette $(n+1)^{ième}$ division s'exécute sans reste. Je désignerai par (A) ce groupe de n formules qui ont toutes A pour premier membre. J'indiquerai aussi quelquefois par le même signe (A) le système des n divisions représentées par ces formules, où les quantités $a, a_1, a_2, \ldots, a_n, p, p_1, \ldots, p_{n-1}$ sont censées des entiers positifs, puisque l'on a affecté explicitement du signe — ceux des résidus qui sont soustractifs.

Si toutes les divisions avaient été faites en dehors, ou avec des résidus négatifs, les équations (A) seraient

$$A = ap' - a'_1, \quad A = a'_1 p'_1 - a'_2, \ldots, \quad A = a'_{n'-1} p'_{n'-1} - a'_{n'-1} \quad (\overline{A}) :$$

Je dénoterai pareillement par $(\overline{A})$ ce groupe d'équations; les quotients $p', p'_1, p'_2, \ldots, p'_{n'-1}$ ayant été convenablement calculés, les résidus $a_1, a_2, a_3, \ldots, a_n$ seront des nombres décroissants $a > a_1 > a_2 \ldots > a_n$; mais plusieurs d'entre eux pourront être supérieurs à la moitié du résidu précédent. La forme des équations $(\overline{A})$ sera plus simple à traiter, et elle conduira à des relations plus régulières que le groupe (A), qui renferme des signes ambigus. Sous le rapport algébrique on voit facilement que ces formules (A) peuvent être remplacées par un groupe de la forme $(\overline{A})$, où l'on admettrait des nombres négatifs pour quelques-uns des résidus et des quotients; par exemple, si deux équations consécutives du premier groupe (A) sont

$$A = a_3 p_3 + a_4, \quad A = a_4 p_4 + a_5,$$

elles peuvent être présentées sous la forme

$$A = a_3 p_3 - (-a_4), \quad A = (-a_4)(-p_4) - (-a_5),$$

qui seront celles du groupe $(\overline{\mathrm{A}})$ si l'on pose

$$a'_4 = -a_4, \quad p'_4 = -p_4, \quad a'_5 = -a_5.$$

Ainsi, en supposant que les résidus du groupe $(\overline{\mathrm{A}})$ soient pris de manière que

$$a'_1 = \mp a_1, \quad a'_2 = \mp a_2, \quad a'_3 = \mp a_3, \ldots, \quad a'_n = \mp a_n;$$

et que, faisant correspondre les signes de cette ligne et de la suivante, l'on pose aussi

$$p'_1 = \mp p_1, \quad p'_2 = \mp p_2, \quad p'_3 = \mp p_3, \ldots, \quad p'_{n-1} = \mp p_{n-1};$$

le groupe $(\overline{\mathrm{A}})$ remplacera complétement le premier groupe (A), aux signes ambigus. Pour passer d'un groupe à l'autre, on devra simplement se rappeler que

$$a'_i p'_i = (\mp a_i)(\mp p_i) = a_i p_i.$$

Cette manière de présenter les équations (A) sous la forme plus régulière $(\overline{\mathrm{A}})$ n'est pas sans analogie avec le mode introduit par M. Sturm, dans les formules qui servent de base à son beau théorème sur les équations algébriques.

[IV]. Nous nous dispenserons ordinairement, pour plus de simplicité, d'écrire des accents supérieurs aux lettres $a'_1, a'_2, \ldots, a'_n$, $p'_1, p'_2, \ldots, p'_{n-1}$ dans les formules $(\overline{\mathrm{A}})$; et nous allons les considérer sous la forme

$$(\overline{\mathrm{A}}) \quad \begin{cases} \mathrm{A} = a\,p - a_1, \\ \mathrm{A} = a_1 p_1 - a_2, \\ \mathrm{A} = a_2 p_2 - a_3, \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ \mathrm{A} = a_{n-2} p_{n-2} - a_{n-1}, \\ \mathrm{A} = a_{n-1} p_{n-1} - a_n, \quad \text{et} \quad \mathrm{A} = a_n p_n. \end{cases}$$

Ce groupe d'égalités résulte donc de $n + 1$ divisions dans lesquelles un résidu a_i peut être négatif ou positif, sous la condition que le quotient de même indice p_i aura le signe de a_i : le décroissement des résidus $a_1, a_2, a_3, \ldots$ sera, si l'on veut, celui que donne le mode ordinaire de l'arithmétique, ou celui des moindres résidus, qui diminuent communément en raison plus que double, lorsqu'on passe de l'un des résidus au suivant.

La première de ces équations multipliée par p_1, et ajoutée à la seconde, donne

$$\mathrm{A}(1 + p_1) = a p_1 p - a_2;$$

celle-ci, multipliée par p_2 et ajoutée à la troisième équation du groupe, donne

$$\mathrm{A}(1 + p_2 + p_2 p_1) = a p_2 p_1 p - a_3;$$

en employant les i premières équations, on aura de la même manière

$$(1)\quad \begin{cases} \mathrm{A}(1 + p_{i-1} + p_{i-1} p_{i-2} + \text{etc.} + p_{i-1} p_{i-2} p_{i-3} \cdots p_2 p_1) \\ \qquad = a p_{i-1} p_{i-2} p_{i-3} \cdots p_2 p_1 p - a_i, \end{cases}$$

ou bien encore

$$a p_{i-1} p_{i-2} p_{i-3} \cdots p_1 p = a_i + \mathrm{A}(1 + p_{i-1} + p_{i-1} p_{i-2} + \text{etc.} + p_{i-1} p_{i-2} \cdots p_2 p_1);$$

et si l'on pose $i = n$, c'est-à-dire, si entre les n équations on a éliminé $a_1, a_2, a_3, \ldots, a_{n-1}$, on a ce résultat

$$(2)\quad a p p_1 p_2 \cdots p_{n-1} = a_n + \mathrm{A}(1 + p_{n-1} + p_{n-2} p_{n-1} + \text{etc.} + p_1 p_2 \cdots p_{n-1}).$$

On voit que cette formule s'obtient en ajoutant la $n^{ième}$ formule du groupe à la $(n-1)^{ième}$ multipliée par p_{n-1},

à la $(n-2)^{ième}$ multipliée par $p_{n-1}\, p_{n-2}$,

à la $(n-3)^{ième}$ multipliée par $p_{n-1}\, p_{n-2}\, p_{n-3}$,

et ainsi de suite jusqu'à la première, qui sera multipliée par $p_{n-1}\, p_{n-2}\, p_{n-3} \cdots p_2 p_1$.

Si l'on n'ajoute que les $n - i - 1$ premiers de ces produits, on aura éliminé les résidus $a_{n-1}, a_{n-2}, \ldots, a_{i-1}$, et l'équation résultante sera

$$(3)\quad \begin{cases} \mathrm{A}(1 + p_{n-1} + p_{n-1}p_{n-2} + \text{etc.} + p_{n-1}p_{n-2}\cdots p_{i+1}) \\ \qquad = a_i p_{n-1} p_{n-2} p_{n-3} \cdots p_{i+1} p_i - a_n, \end{cases}$$

ou bien

$$a_i p_i p_{i+1} p_{i+2} \cdots p_{n-2} p_{n-1} = a_n + \mathrm{A}(1 + p_{n-1} + \text{etc.} + p_{i+1} p_{i+2} \cdots p_{n-1}).$$

Il suit de cette formule que le produit

$$a_i p_i p_{i+1} p_{i+2} \cdots p_{n-2} p_{n-1},$$

étant divisé par A, donne a_n pour résidu, en sorte que les différents produits

$$\begin{aligned} a\ p\ p_1 p_2 p_3 \cdots p_{n-1}, \\ a_1 p_1 p_2 p_3 \cdots p_{n-1}, \\ a_2 p_2 p_3 \cdots p_{n-1}, \\ \cdots\cdots\cdots \\ \cdots\cdots\cdots \\ a_{n-1} p_{n-1}, \end{aligned}$$

sont des entiers congrus entre eux relativement au module A . tous ont a_n pour résidu commun. Ces entiers peuvent avoir des signes positifs ou négatifs, à cause des nombres $p_1, p_2, p_3, \ldots$ etc., qui entrent comme facteurs : il sera toujours facile de déterminer le signe du produit par les signes des facteurs.

On pourrait aisément déduire l'équation (2) d'une formule donnée autrefois par Lambert pour l'évaluation d'une fraction $\frac{a}{\mathrm{A}}$ au moyen de la somme d'un certain nombre de fractions ayant toutes pour numérateur commun l'unité. Cet objet a été traité depuis par Lagrange dans le V.e cahier du *Journal de l'École Polytechnique*. Pour retrouver la formule de Lambert, il suffirait de diviser la formule (2) par

$p, p_1, p_2, \ldots, p_{n-1}$ et par A ; mais l'objet de nos recherches exige que l'équation conserve la forme sous laquelle nous l'avons établie.

[V] Il est clair, par l'équation (1),

$$a\,p_{i-1}\,p_{i-2}\cdots p_2\,p_1\,p = a_i + \mathrm{A}\left\{\begin{matrix}1 + p_{i-1} + p_{i-1}\,p_{i-2} + \text{etc.}\\ + p_{i-1}\,p_{i-2}\cdots p_2\,p_1\end{matrix}\right\},$$

que tout diviseur commun à A et à a divise l'un quelconque des résidus a_i. Ainsi le plus grand diviseur Δ de a et A sera nécessairement facteur de chacun des résidus $a_1, a_2, \ldots, a_{n-1}, a_n$, et quand l'un de ces nombres sera premier il ne pourra y avoir de diviseur commun à a et à A ; mais un facteur de a_i qui diviserait A, pourrait ne pas diviser a, parce que l'équation (1) exige seulement qu'il divise le produit $a\,p_{i-1}\,p_{i-2}\cdots p_2\,p_1\,p$, et le diviseur en question pourra ne diviser que le produit $p_{i-1}\,p_{i-2}\cdots p_2\,p_1\,p$. Si l'on considère spécialement l'équation (2), on en conclura que le grand diviseur Δ doit être facteur du dernier résidu a_n, et ce grand diviseur sera a_n lui-même, si a_n divise a.

Ces conséquences pouvaient être tirées des équations (A) ou $(\overline{\mathrm{A}})$ avant d'en avoir déduit l'égalité (2) : en effet, par la première formule

$$\mathrm{A} = ap - a_1,$$

il est clair que tout diviseur de A et a divise a_1 ; mais un diviseur de A et a_1 est seulement obligé de diviser ap et il peut ne diviser que p sans diviser a ; il pourrait aussi avoir un de ses facteurs dans p et un autre facteur, complémentaire du premier, dans a. Quand on sera assuré que p n'a pas de diviseur commun avec A, il en résultera qu'un diviseur de A et a_1 divise a. Par la seconde formule

$$\mathrm{A} = a_1 p_1 - a_2,$$

on voit semblablement que tout diviseur de A et a_1 divise a_2 ; ainsi le grand diviseur Δ est parmi les facteurs de a_2 comme il était parmi ceux de a_1. On prouvera de la même manière qu'il est compris parmi les diviseurs de a_3, de a_4, ..., de a_{n-1} et de a_n : ainsi il ne peut surpasser a_n, et sera par conséquent le grand diviseur commun à a et a_n : or a_n

est beaucoup moindre que a dès que n est un nombre de quelques unités.

[VI]. Cette considération peut conduire à une méthode nouvelle pour parvenir au plus grand diviseur Δ de deux entiers : elle sera également applicable aux polynomes algébriques entiers. Nous allons la développer pour les nombres.

On s'assurera, par la division, si a_n est diviseur de a, et nous venons de prouver qu'alors a_n sera le grand diviseur Δ des nombres A et a. Si la division ne se fait pas exactement, on nommera $-b_1$ et q le quotient de cette division, en sorte que

$$a = a_n q - b_1;$$

on divisera encore a par b_1. Soient q_1 le quotient et $-b_2$ le reste; on divisera a par b_2; soient q_2 le quotient et $-b_3$ le reste; cette suite de divisions semblables à celles qui ont été opérées sur A, amènera des résidus $b_1, b_2, \ldots, b_{n'}$ qui formeront une série fort décroissante : la dernière de ces divisions sera représentée par

$$a = b_{n'} q_{n'},$$

et la précédente par

$$a = b_{n'-1} q_{n'-1} - b_{n'}:$$

pour mieux nous faire comprendre, nous nommerons ce système d'opérations la seconde catégorie de divisions $(\overline{a})$: les n divisions où A a servi de dividende seront désignées sous le nom de première catégorie $(\overline{A})$. D'après la formule (2) établie ci-dessus, l'on aura cette relation résultant des n' divisions $(\overline{a})$,

$$(4) \quad \left\{ \begin{array}{l} a\,(1 + q_{n'-1} + q_{n'-1}\,q_{n'-2} \cdots + q_{n'-1}\,q_{n'-2} \cdots q_2\,q_1) \\ \qquad\qquad\qquad\qquad \cdot = a_n\,q_{n'-1}\,q_{n'-2} \cdots q_1\,q - b_{n'}\,: \end{array} \right.$$

Nous savons, par ce qui a été expliqué ci-dessus [V], que le grand diviseur de a et de a_n ne peut surpasser le résidu $b_{n'}$, et doit en être facteur; le plus communément (ou du moins bien souvent) pour des

nombres A et a qui ne seront pas immenses, on trouvera que $b_{n'}$ est diviseur de a_n, et alors il sera le grand diviseur cherché; si a_n n'est pas exactement divisible par $b_{n'}$, on opérera sur a_n et $b_{n'}$ comme on vient de faire avec a et a_n : en dénotant encore par $r, r_1, r_2, \ldots, r_{n''-1}$ les quotients, et par $-c_1, -c_2, -c_3, \ldots, -c_{n''-1}, -c_{n''}$ les restes des opérations, on aura la relation

$$(5)\quad \left\{ \begin{array}{l} a_n(1 + r_{n''-1} + r_{n''-1}\, r_{n''-2} + \text{etc.} + r_{n''-1}\, r_{n''-2} \ldots r_2\, r_1) \\ \qquad\qquad = b_n\, r_{n''-1}\, r_{n''-2} \ldots r_2\, r_1 r - c_{n''}. \end{array} \right.$$

On devra reconnaître si $c_{n''}$ divise exactement $b_{n'}$: alors $c_{n''}$ serait le diviseur Δ cherché; la même série d'opérations sera prolongée jusqu'à ce que l'on rencontre un résidu, tel que $c_{n''}$, qui divise exactement le dernier résidu $b_{n'}$ provenant d'une catégorie de n' divisions antérieures aux n'' divisions exécutées en dernier lieu : c'est ce qui ne peut manquer d'arriver puisque le premier reste a_n est beaucoup moindre que a; que $b_{n'}$ est beaucoup moindre que a_n; $c_{n''}$ beaucoup moindre que $b_{n'}$, et ainsi de suite. Que si, dans chacune des divisions, l'on a eu recours aux moindres résidus, en leur donnant des signes convenables, on aura, art. [II],

$$a > 2^n a_n, \quad a_n > 2^{n'} b_{n'}, \quad b_{n'} > 2^{n''} c_{n''},$$

et par suite

$$a > 2^{n+n'+n''} \times c_{n''}, \quad \text{et} \quad c_{n''} < \frac{a}{2^{n+n'+n''}},$$

et $c_{n''}$ sera généralement fort au-dessous de cette limite. On voit que si l'on détermine le nombre ν de manière que

$$2^{\nu-1} < a < 2^{\nu},$$

on aura

$$\frac{a}{2^{\nu}} < 1;$$

et que par conséquent le nombre $n+n'+n''+$ etc. de toutes les divisions exécutées sera moindre que ν qui est le nombre entier immédiatement supérieur à $\frac{\log(a)}{\log(2)}$.

[VII]. Nous avons déjà fait observer [III] que si l'on a pratiqué beaucoup de divisions dans la première catégorie, qui a donné le résidu a_n, ce reste est considérablement moindre que a : il arrivera même souvent que a_n se présentera assez faible après un petit nombre n d'opérations. Cette remarque convient aux autres catégories de divisions que l'on sera parfois amené à exécuter : elle fera concevoir que le calcul du grand diviseur par ce procédé, ordinairement moins simple que celui de la méthode d'Euclide, n'entraînera pourtant pas beaucoup plus de travail. Cette opération est une des plus parfaites de l'arithmétique, surtout quand on y introduit l'usage des résidus qui ne surpassent pas la moitié du diviseur de chaque division [art. II]; et si l'on n'avait pour but que de trouver le grand diviseur de deux entiers, je ne pourrais conseiller de lui substituer le nouveau procédé. On doit y employer A comme dividende n fois de suite; puis a sert de dividende n' fois de suite, avec différents diviseurs, etc. Dans la méthode d'Euclide on a l'avantage de voir le dividende et le diviseur décroître d'une division à la suivante. Mais le nouveau procédé conduit à des relations beaucoup moins compliquées que celles de la méthode d'Euclide, entre les entiers A et a, les divers résidus, et les quotients fournis par les divisions successives. La raison de cette plus grande simplicité tient à ce que, dans une même catégorie de nos divisions, la relation de deux résidus consécutifs est de la forme

$$\mathrm{A} = a_{i-1} p_{i-1} - a_i,$$

qui est une équation à différences finies du premier ordre; et dans la méthode d'Euclide on a, pour lier entre eux les résidus, une équation du second ordre

$$\alpha_{i-2} = \alpha_{i-1} g_{i-1} - \alpha_i.$$

Ce n'est qu'en passant d'une catégorie à l'autre de nos divisions, que l'on retrouve des relations de cette forme, ainsi qu'on le verra art. [IX]; mais ce passage ne peut avoir lieu qu'un petit nombre de fois, à moins qu'il ne s'agisse pour a d'un nombre immense, et dans ce cas toutes les méthodes vous exposent à de fort longs calculs.

[VIII]. Afin de donner une idée plus complète de ce procédé, on va l'appliquer à deux exemples : on comparera la nouvelle marche dans le second, qui emploie des nombres un peu grands, à celle d'Euclide.

Prenons d'abord $A = 1170$, $a = 705$; les divisions de la première catégorie, où A est constamment employé comme dividende, sont indiquées dans ce tableau :

A	a	$-a_1$	$-a_2$
1170	705	— 240	— 30
	2	— 5	— 39
	p	$-p_1$	$-p_2$

On voit que le premier résidu négatif $-a_1 = -240$; le second résidu de la division de A par a_1 est $-a_2 = -30$, celui-ci donne un quotient exact -39 : les deux autres quotients sont $p = 2$, $-p_1 = -5$. Pour s'assurer si $a_2 = 30$ est le grand diviseur et, dans tous les cas, pour le découvrir, on procède à une nouvelle catégorie de divisions, dans lesquelles $705 = a$ va servir de dividende :

a	a_2	b_1
705	30	15
	23	47
	q	q_1

Le résidu $15 = b_1$ divise 705, et donne 47 pour quotient : on n'a plus qu'à reconnaître s'il divise le résidu $a_2 = 30$ de la première catégorie : or cette division ayant lieu, il s'ensuit que 15 est le plus grand diviseur commun des nombres 1170 et 705 : toutes les divisions ont été effectuées de manière à fournir les moindres résidus.

Le second exemple offrira l'emploi de trois catégories de divisions : soient $A = 1292646$ et $a = 145145$; nous effectuerons encore les divisions de manière que les valeurs numériques des résidus n'excèdent pas

le demi-diviseur. Voici le tableau de la première catégorie de divisions où le dividende est constamment A = 1292646.

A	a	$-a_1$	$-a_2$	$-a_3$
1292646	145145	— 13659	— 4959	— 1653
	9	— 95	— 261	— 782
	p	$-p_1$	$-p_2$	$-p_3$

Les diviseurs a, a_1, a_2, a_3, fournissent les quotients 9, 95, 261, 782, qui croissent rapidement parce que chaque diviseur n'atteint pas la moitié du précédent : la division de A par a_3 donnant un quotient exact, le grand commun diviseur doit être facteur de 1653; pour le découvrir, on procède à une seconde catégorie de divisions :

a	a_3	$-b_1$
145145	1653	— 319
	88	— 455
	q	$-q_1$

Une seule division amène le résidu $b_1 = 319$, qui divise exactement $a = 145145$. On doit procéder à la troisième catégorie, où le dividende constant sera $a_2 = 1653$,

	b_1	c_1	c_2
1653	319	58	29
	5	28	57
	r	r_1	r_2

Elle conduit à un résidu $29 = c_2$ qui est exact diviseur de $316 = b_{17}$ car $319 = 29 \times 11$; et il en résulte que 29 est le plus grand diviseur des nombres proposés.

Je rapporterai ici le tableau des opérations de la méthode d'Euclide, à l'aide de divisions ordinaires :

1292646	145145	131486	13659	8555	5104	3451	1653	145	58	29
	8	1	9	1	1	1	2	11	2	2

En exécutant les divisions à l'aide de résidus moindres que les demi-diviseurs, on aura moins d'opérations. En voici le tableau :

1292646	145145	−13659	− 5104	− 1653	145	58	29
	9	− 11	3	2	− 11	2	2

Dans cet exemple, on voit que le nouveau procédé employé avec les moindres résidus, a entraîné 9 divisions; l'ancienne méthode en exige 10, et quand on y fait concourir les moindres résidus, 7 divisions suffisent pour faire connaître le grand diviseur 29.

[IX]. Nous ferons, pour abréger, dans l'équation (2),

$$\mathrm{P} = p\,p_1\,p_2 \cdots p_{n-2}\,p_{n-1},$$

$$\mathrm{P}_1 = p_1\,p_2\,p_3 \cdots p_{n-2}\,p_{n-1} + p_2 p_3 \cdots p_{n-1} + \text{etc.} + p_{n-2}\,p_{n-1} + p_{n-1} + 1;$$

elle deviendra

$$a_n = a\mathrm{P} - \mathrm{AP}_1;$$

dans les formules (4) et (5) nous écrirons pareillement

$$\mathrm{Q} = q\,q_1 q_2 \cdots q_{n'-2}\,q_{n'-1},$$

$$\mathrm{Q}_1 = q_1 q_2 \cdots q_{n'-2}\,q_{n'-1} + q_2\,q_3 \cdots q_{n'-1} + \text{etc.} + q_{n'-1} + 1,$$

$$\mathrm{R} = r\,r_1 r_2 \cdots r_{n''-2}\,r_{n''-1},$$

$$\mathrm{R}_1 = r_1 r_2 \cdots r_{n''-2}\,r_{n''-1} + \text{etc.} + r_{n''-1} + 1;$$

$$\mathrm{S} = s\,s_1 \cdots s_{n'''-1},$$

etc.;

l'on aura ainsi

$$a_n = aP - AP_1, \tag{4}$$

$$b_{n'} = a_n Q - aQ_1, \tag{5}$$

$$c_{n''} = b_{n'} R - a_n R_1, \tag{6}$$

$$d_{n'''} = c_{n''} S - b_{n'} S_1, \tag{7}$$

etc.

Lorsque a_n divisera exactement a, il sera le grand diviseur de a et de A ; son expression, donnée par la formule (4), sera

$$a_n = aP - AP_1,$$

et les équations suivantes n'auront pas lieu; mais si l'on reconnaît que $b_{n'}$ est le grand diviseur cherché, on aura les deux équations

$$b_{n'} = a_n Q - aQ_1, \quad \text{et} \quad a_n = aP - AP_1;$$

la dernière étant multipliée par Q, et ajoutée à la précédente donnera, en réunissant les termes affectés de a,

$$b_{n'} = a(PQ - Q_1) - AP_1 Q. \tag{8}$$

Souvent ces deux catégories de divisions auront suffi pour faire connaître le grand diviseur, qui sera alors $b_{n'}$: nous indiquerons plus bas quelques circonstances qui peuvent réduire la recherche à la première catégorie, ou aux deux premières, ou etc. Lorsque l'on devra recourir à la troisième catégorie de n'' divisions et que $c_{n''}$ sera reconnu le diviseur de $b_{n'}$, et par suite de A et a, les trois équations (4), (5), (6) existeront ensemble; des deux dernières on déduit, par l'élimination de $b_{n'}$,

$$c_{n''} = a_n(QR - R_1) - aQ_1 R,$$

qui ne diffère de l'équation que nous venons d'écrire qu'en ce que $c_{n''}$ remplace $b_{n'}$, a_n et a remplacent a et A, et enfin P, Q, P_1, Q_1 sont respectivement remplacés par Q, R, Q_1, R_1. Dans cette formule on substitue la valeur

$$a_n = aP - AP_1, \tag{4}$$

ou, ce qui revient au même, on multiplie cette équation (4) par $QR - R_1$ pour l'ajouter à la précédente égalité; il en résulte

$$(9) \qquad c_{n'} = a(PQR - PR_1 - RQ_1) - AP_1(QR - R_1).$$

Si l'on était obligé de recourir à une quatrième catégorie de divisions en nombre n''' pour atteindre le diviseur $d_{n'''}$, on déduirait des trois valeurs de $d_{n''}$, de $c_{n''}$, de $b_{n'}$, cette équation

$$d_{n'''} = a_n(QRS - QS_1 - SR_1) - aQ_1(RS - S_1):$$

cette équation, jointe à la première,

$$a_n = aP - AP_1,$$

donne, par l'élimination de a_n,

$$(10) \quad \begin{cases} d_{n'''} = a[PQRS - RSQ_1 - SPR_1 - PQS_1 + Q_1S_1] \\ \qquad - AP_1[QRS - SR_1 - QS_1]. \end{cases}$$

On continuerait de la même manière, si de nouvelles catégories de divisions avaient été nécessaires pour arriver au grand diviseur Δ : en admettant cette possibilité, je dirai cependant que je n'ai pas rencontré d'exemple qui exigeât plus de trois catégories, et ce dernier cas s'est même rarement présenté dans un assez grand nombre d'exemples.

On peut observer, dans ces formules, que le grand diviseur Δ, soit a_n, soit $b_{n'}$, soit $c_{n''}$, etc., se présente sous la forme $ax - Ay$, x et y étant des nombres entiers dont la composition est connue à l'aide des quotients $p, p_1, p_2, \ldots, p_{n-1}$; $q, q_1, q_2, \ldots, q_{n'-1}$; $r, r_1, r_2, \ldots, r_{n''-1}$; etc Dans ses *Nouveaux Exercices d'analyse*, M. Cauchy a remarqué que le grand diviseur de a et A est de cette forme [*voyez* tome II]; mais on n'avait pas aperçu la composition qui résulte des opérations que je viens d'indiquer.

[X]. Afin d'introduire dans ces diverses relations, et spécialement dans la formule (2), les quotients positifs tels qu'ils se sont présentés dans le premier groupe (A), nous rétablirons pour un instant des ac-

cents aux lettres $p', p'_1, p'_2, \ldots, p'_{n-1}$, $a'_1, a'_2, a'_3, \ldots, a'_{n-1}$, et nous reprendrons l'équation (2) sous la forme

$$a p' p'_1 p'_2 \ldots p'_{n-1} = a'_n + \mathrm{A}\left\{\begin{matrix} 1 + p'_{n-1} + p'_{n-1} p'_{n-2} + \text{etc.} \\ + p'_{n-1} p'_{n-2} \ldots p'_2 p'_1 \end{matrix}\right\} :$$

pour revenir du groupe $(\overline{\mathrm{A}})$ au premier (A), il faut se rappeler que chaque résidu $-a'_i = \pm a_i$ est accompagné de $p'_i = \mp p_i$. Le signe du produit $p' p'_1 p'_2 \ldots p'_{n-1}$ va donc dépendre des seuls quotients négatifs $p'_g = -p_g$, $p'_h = -p_h, \ldots$, et par conséquent du nombre des résidus *positifs* $+a_g = -a'_g$, $+a_h = -a'_h$, etc. Quant à sa grandeur numérique, elle est égale au produit $p p_1 p_2 \ldots p_{n-1}$. Nommons m le nombre des résidus positifs contenus dans la suite complète

$$\pm a_1, \ \pm a_2, \ \pm a_3, \ldots\ldots, \ \pm a_{n-1}, \ \pm a_n.$$

Deux cas sont à distinguer : le dernier résidu peut être $+a_n$, et alors, parmi les restes précédents, il ne s'en trouvera que $m-1$ affectés du signe positif, tels que

$$a_g = -a'_g, \quad a_h = -a'_h, \text{ etc.} :$$

à ces résidus négatifs a'_g, a'_h, répondent des quotients négatifs, et en nombre $m-1$,

$$p'_g = -p_g, \quad p'_h = -p_h, \text{ etc.}$$

Dans ce premier cas l'on aura donc pour le produit

$$p'_1 p'_2 p'_3 \ldots p'_{n-1} = p_1 p_2 p_3 \ldots p_{n-1} (-1)^{m-1};$$

l'équation (2) deviendra, d'après cela,

$$app_1 p_2 \ldots p_{n-1} (-1)^{m-1} = -a_n + \mathrm{A}\left\{\begin{matrix} p_1 p_2 \ldots p_{n-1} (-1)^{m-1} \pm p_2 p_3 \ldots p_{n-1} + \text{etc.} \\ \pm p_{n-2} p_{n-1} \pm p_{n-1} + 1 \end{matrix}\right\};$$

ou bien, après avoir multiplié par $(-1)^{m-1}$,

$$a p p_1 \ldots p_{n-1} = a_n (-1)^m + \mathrm{A}\left\{\begin{matrix} p_1 p_2 \ldots p_{n-1} \pm p_2 p_3 \ldots p_{n-1} + \text{etc.} \\ \pm p_{n-2} p_{n-1} \pm p_{n-1} + (-1)^{m-1} \end{matrix}\right\}.$$

Dans le second cas, où le dernier résidu $-a'_n = -a_n$, les m résidus positifs du groupe (A) sont compris parmi les $n-1$ précédents $\pm a_1$, $\pm a_2, \ldots, \pm a_{n-1}$, et alors les quotients négatifs

$$p'_g = -p_g, \quad p'_h = -p_h, \text{ etc.}$$

étant en nombre m, le produit

$$p'_1 p'_2 \cdots p'_{n-1} = p_1 p_2 \cdots p_{n-1} (-1)^m,$$

car l'on a toujours $p' = p$; ainsi l'équation (2'), après avoir été multipliée par $(-1)^m$, deviendra

$$a p p_1 p_2 \cdots p_{n-1} = a_n (-1)^m + \mathrm{A} \begin{Bmatrix} p_1 p_2 \cdots p_{n-1} \pm p_2 p_3 \cdots p_{n-1} \pm \text{etc.} \\ \pm p_{n-2} p_{n-1} \pm p_{n-1} + (-1)^m \end{Bmatrix}.$$

La partie non affectée du nombre entier A a la même forme dans les deux cas de $+a_n$ et de $-a_n$: les signes de la fonction multipliée par A seront faciles à déterminer, en ayant égard à la multiplication de $(-1)^{m-1}$ ou de $(-1)^m$ qui a lieu quand $a'_n = -a_n$, ou quand $a'_n = a_n$; et en introduisant dans chaque terme de la fonction

$$p'_1 p'_2 p'_3 \cdots p'_{n-1} + p'_2 p'_3 p'_4 \cdots p'_{n-1} + \text{etc.} + p'_{n-1} + 1,$$

les quotients négatifs $p'_g = -p_g$, $p'_h = -p_h$, etc.

Il est donc établi qu'en partant du groupe (A), où nous supposons un nombre m de résidus positifs $+a_g$, $+a_h$, etc., on obtient entre A, a, et le $n^{ième}$ résidu a_n, l'équation

$$a\mathrm{P} - \mathrm{A}\mathrm{P}_1 = a_n (-1)^n, \tag{11}$$

où

$$\mathrm{P} = p\, p_1 p_2 \cdots p_{n-1},$$

$$\mathrm{P}_1 = p_1 p_2 p_3 \cdots p_{n-1} \pm p_2 p_3 \cdots p_{n-1} + \text{etc.} \pm p_{n-1} \pm 1.$$

On eût obtenu évidemment un semblable résultat en n'employant que les i premières équations (A) entre A, a, a_1, $a_2, \ldots$, et a_i : il suffirait d'écrire dans l'équation (11), i à la place de n, et de remplacer m

par le nombre des résidus positifs renfermés dans la série

$$\pm a_1,\ \pm a_2,\ \pm a_3,\ \ldots,\ \pm a_i,$$

pour former cette relation.

Dans l'équation (11) les quotients $p, p_1, p_2, \ldots, p_{n-1}$, ainsi que a_n, sont maintenant censés des nombres positifs, parce qu'ils proviennent du premier groupe (A).

[XI]. Lorsque les entiers A et a n'ont pas de commun diviseur, et qu'ils ont été cependant soumis au système d'opérations qui produisent les quotients $p, p_1, \ldots, p_{n-1}, q, q_1, q_2, \ldots, q'_{n'-1}$, etc., le dernier des résidus, soit a_n, soit $b_{n'}$, soit $c_{n''}$, etc. qui devrait être le grand diviseur commun de A et a, s'il existait, se présentera sous la forme ± 1. Ce cas spécial, où A et a, sont premiers entre eux, mérite une attention particulière, en raison des relations qui s'ensuivent pour les deux nombres proposés A et a, d'après les équations de l'article [IX].

Si pour a_n on rencontre la valeur $a_n = \pm 1$, l'on aura, en vertu de l'équation (11), cette relation en a et A

$$aP - AP_1 = (-1)^m, \tag{12}$$

où m indique encore le dénombrement des résidus positifs introduits dans le premier groupe des divisions (A) : P a la même valeur $p\,p_1\,p_2 \ldots p_{n-1}$ que ci-dessus, et il en est ainsi de P_1 dont la forme en $p_1\,p_2 \ldots p_{n-1}$ est plus compliquée, mais connue.

Nous ferons voir que cette relation a souvent lieu entre deux nombres a et A; il sera prouvé ci-dessous qu'elle existe nécessairement lorsque $A > a$ est un nombre premier.

Quand a_n ne sera pas égal à ± 1, et qu'après avoir formé la seconde catégorie de divisions, où a est employé comme dividende constant selon la règle de l'art. [VI], l'on rencontrera $b_{n'} = \pm 1$, l'équation (5) deviendra

$$a_n Q - aQ_1 = (-1)^{m'},$$

où m' dénote le nombre des résidus positifs introduits dans la seconde catégorie des divisions, Q étant le produit $q\,q_1\,q_2 \ldots q_{n-1}$ et Q_1 un

nombre entier connu à l'aide des quotients $q_1, q_2, \ldots, q_{n-1}$, ou par l'équation elle-même quand on connaît a_n, Q, et a. On a d'ailleurs, dans tous les cas,

$$aP - AP_1 = a_n(-1)^m.$$

On peut écrire cette formule et la précédente ainsi :

$$\begin{aligned} a\ P(-1)^m - AP_1(-1)^m &= a_n, \\ a_n Q(-1)^{m'} - aQ_1(-1)^{m'} &= 1. \end{aligned}$$

Ces deux formules ne diffèrent des équations (4) et (5) qu'en ce que P et P_1 sont multipliés par $(-1)^m$, Q et A_1 le sont par $(-1)^{m'}$, et b_n est ici égal à 1 ; éliminant entre elles le résidu a_n, on aura à la place de l'équation (8) cette égalité

$$a[PQ(-1)^{m+m'} - Q_1(-1)^{m'}] - AP_1Q(-1)^{m+m'} = 1 ; \tag{13}$$

on l'écrira plus simplement en la multipliant par $(-1)^{m+m'}$: on aura de cette manière

$$a[PQ - Q_1(-1)^m] - AP_1Q = (-1)^{m+m'}. \tag{14}$$

Lorsque l'on ne trouvera pas $b_n = \pm 1$, mais que b_n sera > 1, on devra passer à une troisième catégorie de divisions pour rencontrer un résidu $c_n = \pm 1$; si l'on nomme m'' le nombre des résidus positifs de ces nouvelles divisions, on aura, à la place des équations (4), (5), (6), trois équations que nous écrirons ainsi :

$$\begin{aligned} a\ P(-1)^m - AP_1(-1)^m &= a_n, \\ a_n Q(-1)^{m'} - aQ_1(-1)^{m'} &= b_{n'}, \\ b_{n'} R(-1)^{m''} - a_n R_1(-1)^{m'} &= 1, \end{aligned}$$

et l'élimination de a_n et $b_{n'}$ entre ces égalités conduira à une formule semblable à l'équation (9) : on pourra la multiplier par $(-1)^{m+m'+m''}$, et alors elle sera

$$a[PQR - PR_1(-1)^{m'} - RQ_1(-1)^m] - AP_1[QR - R_1(-1)^{m'}] = (-1)^{m+m'+m''}.$$

Un résultat semblable aurait encore lieu, alors même qu'il faudrait poursuivre dans un plus grand nombre de catégories la recherche du dernier résidu ± 1 qui doit, en ce cas, remplacer le diviseur de a et A : c'est ce que prouvent les équations (9), ou (10), ou etc., dans lesquelles le dernier résidu sera toujours exprimé par une somme ou une différence de la forme $ax \pm Ay$, x et y étant des entiers. Ainsi, dans le cas que nous examinons, de a et A premiers entre eux, on arrivera à une équation de la forme

$$aM - AP_1M_1 = \pm 1,$$

dans laquelle les entiers M et $P_1 M_1$ seront assez simplement déterminés à l'aide de P, P_1, Q, Q_1, R, R_1, etc., qui eux-mêmes ne dépendent que des quotients p, p_1, p_2, etc., q, q_1, q_2, etc., r, r_1, r_2, etc. Les nombres M et P_1M_1 seront nécessairement hétérogènes, car s'ils admettaient un facteur commun, il devrait diviser ± 1, ce qui est impossible. Par la même raison, A est premier à M, et a l'est aussi à $P_1 M_1$.

[XII]. Nous avons déjà constaté par l'équation (1)

$$a\,p\,p_1\,p_2 \ldots p_{i-1} = a_i + A\,(1 + p_{i-1} + p_{i-1}\,p_{i-2} + \text{etc.}),$$

que tout diviseur de a et A est aussi facteur de a_i. Admettons que a soit hétérogène à A, comme dans l'art. [XI], et que de plus il en soit ainsi de chacun des quotients p, p_1, p_2, ..., p_{i-1} à l'égard du même A ; en ce cas, a_i sera sans diviseur commun avec A, et c'est ce que l'on a déduit des équations $(\overline{A})$ considérées successivement art. [V]. Réciproquement si a_i, a_{i-1}, a_{i-2}, ..., a_2, a_1, et a sont des entiers hétérogènes à A, il s'ensuivra que les quotients p, p_1, p_2, ..., p_{i-1} seront aussi hétérogènes à A.

Quand la série complète des quotients p, p_1, p_2, ..., p_{n-1} sera composée de nombres hétérogènes à A, et que a sera lui-même premier à A ; la suite des résidus a_1, a_2, ..., a_{n-1}, a_n ne renfermera encore que des nombres hétérogènes à A : or le dernier reste a_n devant diviser exactement A, en vertu de sa définition [II], ce nombre ne peut être que ± 1 : ainsi la dernière des équations (A) sera

$$A = a_{n-1}\,p_{n-1} \pm 1 ;$$

et l'on pourra écrire $a_n = 1$, en ne considérant que la valeur numérique, le signe étant réservé. Dans le cas dont il s'agit, la formule (11) devient

$$(15) \qquad a\,p\,p_1\,p_2\,p_3 \cdots p_{n-2}\,p_{n-1} = (-1)^m + \mathrm{AP}_1 :$$

elle montre que le nombre entier résultant de la formule

$$a\,p\,p_1\,p_2 \cdots p_{n-2}\,p_{n-1} + (-1)^{m+1}$$

est toujours divisible par A, qui est premier à a, ainsi qu'à tous les quotients $p, p_1, p_2, \ldots, p_{n-1}$, lesquels dérivent de A et de a, d'après les règles indiquées antérieurement art. [I].

Si toutes les divisions représentées par le groupe (A) ont été exécutées en dedans et avec des restes positifs $+a_1, +a_2, \ldots, +a_{n-1}, +a_n$ on aura $m = n$, et le nombre divisible par A sera

$$a\,p\,p_1\,p_2 \cdots p_{n-1} + (-1)^{n+1} ;$$

alors le multiplicateur P_1 de A, ou le quotient de la division par A, aura cette forme simple, où les termes ne présentent que des variations de signes,

$$\mathrm{P}_1 = p_1\,p_2\,p_3 \cdots p_{n-1} - p_2\,p_3 \cdots p_{n-1} + p_3\,p_4 \cdots p_{n-1} \pm \text{etc.}$$
$$\pm p_{n-2}\,p_{n-1} \mp p_{n-1} \pm 1.$$

Si toutes les divisions ont été exécutées en dehors ou avec des résidus négatifs, le nombre $m = 0$, et l'on aura

$$(15') \qquad a\,p\,p_1\,p_2 \cdots p_{n-1} - 1 = \mathrm{AP}_1 ;$$

alors tous les signes de P_1 seront positifs et sa valeur sera

$$\mathrm{P}_1 = p_1\,p_2\,p_3 \cdots p_{n-1} + p_2\,p_3 \cdots p_{n-1} + \text{etc.} + p_{n-1} + 1.$$

On devra ne pas oublier que les conditions de ces formules de A premier à a et à $p, p_1, p_2, \ldots, p_{n-1}$, reviennent à celles de A premier à a ainsi qu'aux résidus $a_1, a_2, \ldots, a_n$.

Dans le cas dont nous nous occupons, on met facilement en évidence la proposition exprimée par la formule (15), en écrivant les équations du groupe $(\overline{A})$ sous cette forme

$$\begin{aligned}
A + a_1 &= a\,p,\\
A + a_2 &= a_1\,p_1,\\
A + a_3 &= a_2\,p_2,\\
&\cdots\cdots\cdots\\
&\cdots\cdots\cdots\\
&\cdots\cdots\cdots\\
A + a_{n-1} &= a_{n-2}\,p_{n-2},\\
A \pm 1 &= a_{n-1}\,p_{n-1}:
\end{aligned}$$

nous écrivons dans la dernière $A \pm 1$, parce qu'il a été établi ci-dessus que $a_n = \mp 1$. Si l'on forme le produit de ces égalités, le premier membre se composera de

$$(A + a_1)\,(A + a_2)\;\ldots(A + a_{n-1})\,(A \pm 1),$$

et après avoir développé les multiplications, on aura une classe de termes affectés de A, et un produit

$$\pm\, a_1\, a_2\, a_3 \ldots a_{n-1}.$$

Ce produit pourra être transporté dans le second membre où se trouve déjà $a\,p\,p_1\,p_2 \ldots p_{n-1} \times a_1\,a_2\,a_3 \ldots a_{n-1}$; l'on aura donc cette formule

$$AM = (a\,p\,p_1\,p_2 \ldots p_{n-1} \mp 1)\,a_1\,a_2\,a_3 \ldots a_{n-1}:$$

les nombres $a_1, a_2, a_3, \ldots, a_{n-1}$, étant premiers à A, par hypothèse, il en résulte que l'autre facteur du second membre de l'équation, savoir,

$$a\,p\,p_1\,p_2 \ldots p_{n-1} \mp 1$$

doit être divisible par A. Quand les formules $(\overline{A})$ proviennent du premier groupe (A), et que, dans ce groupe, il se trouve un nombre m

de restes positifs, on retrouve aisément les conditions de la formule (15), en introduisant dans le produit $p_1 p_2 p_3 \cdots p_{n-1}$ un nombre m ou un nombre $m - 1$ de quotients négatifs, conformément à ce que nous avons expliqué art. [X]. La formule (15) a l'avantage de montrer la composition du multiplicateur de A, ce que l'on ne trouverait pas aussi facilement par le procédé actuel.

[XIII]. Prenons pour exemple $A = 77 = 7 \times 11$, et $a = 50$, on pourra disposer les divisions ainsi que l'indique ce tableau, où toutes les opérations ont été faites à la manière ordinaire de l'arithmétique et avec des restes positifs.

77	50	27	23	8	5	2	1
	1	2	3	9	15	38	

Les quotients $p, p_1, p_2, p_3, p_4, p_5$, sont

$$1, 2, 3, 9, 15, 38,$$

et ils n'ont pas de diviseurs communs avec $A = 7 \times 11$; les restes positifs, au nombre de $6 = m = n$, sont

$$27, 23, 8, 5, 2, 1,$$

et ils ont servi tour à tour de diviseur au même dividende 77 : d'après le théorème (15), le produit

$$50.1.2.3.9.15.38$$

étant divisé par 77, doit donner $(-1)^6 = 1$ pour reste; c'est-à-dire que le nombre

$$50.2.3.9.15.38 - 1$$

doit être divisible par 77 : ce nombre est 1538 999, qui égale, en effet, 77×19987.

On peut opérer les divisions en excès, et en introduisant des résidus négatifs à toutes les divisions ; on aura ainsi

77	50	— 23	— 15	— 13	— 1
	2	— 4	— 6	— 6	

Tous les restes étant négatifs, on a $m = 0$, et d'après la formule (12), le nombre

$$50.2\ 4.6.6 - 1 = 14399$$

doit être divisible par 77 : ce nombre est en effet le produit de 77×187.

En effectuant les divisions sous la condition d'avoir des restes moindres chacun que la moitié du précédent résidu, les opérations seront représentées dans ce tableau.

77	50	— 23	8	— 3	— 1
	2	— 3	10	— 26	

Les résidus 23, 8, 3, 1 décroissent en raison plus que double ; et pour remplir cette condition on a admis trois résidus négatifs — 23, — 3, — 1, et un seul positif, 8 : on a donc ici $m = 1$, et d'après la formule (12), le nombre

$$50 \times 2.3.10.26 + 1$$

doit être divisible par 77 : ce nombre est $78001 = 77 \times 1013$.

Si en posant toujours $A = 77$, on eût pris $a = 21$, les conditions de la formule (12) ne se fussent plus trouvées remplies. Voici les divisions en dedans.

77	21	14	7
	3	5	11

On se fût trouvé alors dans le cas de la formule (11). on eût eu

$p = 3$, $p_1 = 5$; $a_1 = 14$, $a_2 = 7$, $m = 2$; ainsi le nombre

$$21.3.5 - 7 = 308$$

doit être divisible par 77: ce nombre $= 77 \times 4$. Ici se présente le diviseur commun 7 des nombres 21 et 77.

[XIV]. Les conditions exigées par la formule (15),

$$a p p_1 p_2 \cdots p_{n-1} + (-1)^{m+1} = \mathrm{AP}_1,$$

c'est-à-dire pour que le nombre entier

$$a p p_1 p_2 \cdots p_{n-1} + (-1)^{m+1}$$

soit exactement divisible par A, peuvent être nombreuses; car il faut que A soit hétérogène à a et aux quotients $p, p_1, p_2, \ldots, p_{n-1}$, fournis par une série de n divisions où A sert de dividende constant [I]. Néanmoins ces conditions seront remplies toutes les fois que l'on prendra pour A un nombre premier $\alpha > a$. Alors, en effet, les résidus décroissants $a_1, a_2, a_3, \ldots, a_n$, tous moindres que a, et par conséquent que α, seront sans diviseurs communs avec α, que l'on suppose premier; et il a été démontré antérieurement [XII] qu'alors les quotients $p, p_1, p_2, \ldots, p_{n-1}$, sont eux-mêmes sans diviseurs communs avec $\mathrm{A} = \alpha$: ce sont d'ailleurs des entiers moindres que le nombre premier, et cela suffisait pour dispenser de toute preuve. Il en résulte ce théorème, pour un nombre premier quelconque α:

divisez α par a; soit p le quotient et a_1 le reste;
divisez α par a_1; soit p_1 le quotient et a_2 le reste;
divisez α par a_2; soit p_2 le quotient et a_3 le reste;

par ces opérations consécutives vous arriverez à un reste $a_n = 1$, si vous avez exécuté toutes les divisions selon le mode ordinaire qui donne des restes positifs; cela posé, le nombre entier ainsi formé

$$a p p_1 p_2 \cdots p_{n-1} + (-1)^{n+1} = \alpha \mathrm{P}_1, \tag{16}$$

sera nécessairement divisible par le nombre premier α, en sorte que dans cette formule P_1 sera un entier.

Si vous avez exécuté seulement m divisions en dedans, art. [I], et les $n - m$ autres divisions en dehors ou avec des résidus négatifs; que les quotients positifs des divisions soient encore dénotés par $p, p_1, p_2, \ldots, p_{n-1}$; vous arriverez à un dernier résidu qui sera $+1$ ou -1, et le nombre entier

$$(16) \qquad a p p_1 p_2 \ldots p_{n-1} + (-1)^{m+1} = \alpha P_1$$

sera exactement divisible par α : ici les nombres p, p_1, p_2, etc., ainsi que P_1 et n, désignent des entiers différents de ceux du premier cas, où les résidus étaient tous positifs.

Si l'on a rendu tous les résidus négatifs, en exécutant les divisions en dehors, la formule (15) prendra cette expression plus simple

$$a p p_1 p_2 \ldots p_{n-1} - 1 = \alpha P_1,$$

car alors on doit prendre $m = 0$, m étant le nombre des opérations à résidus positifs.

Le théorème de Wilson établit que le nombre $2.3.4\ldots(\alpha-2)(\alpha-1)+1$, ne sera divisible par α, que sous la condition de α premier. Le produit $2.3.4\ldots(\alpha-1)$ devient d'une grandeur énorme dès que α n'est plus un petit nombre entier : cette difficulté d'arithmétique pratique rend assez rare l'emploi de cette belle propriété. Notre théorème montre qu'en prenant à volonté, un entier a dans la série $2.3.4\ldots(\alpha-1)$, on peut facilement trouver les facteurs $p, p_1, p_2, \ldots, p_{n-1}$, qui doivent lui être associés, pour fournir la quantité $a p p_1 p_2 \ldots p_{n-1} \pm 1$ divisible par α; et le nombre n de ces facteurs sera non-seulement moindre que $\alpha - 2$, mais considérablement au-dessous de $a < \alpha$, quand a sera un peu grand [II].

Cette propriété, qui convient à tous les nombres premiers α, peut recevoir d'utiles applications. Nous avons déjà dit qu'elle n'est pas, comme le théorème de Wilson, un caractère exclusif du nombre premier, et c'est, d'ailleurs, ce que nous allons établir dans un instant. On connaît d'autres propriétés qui appartiennent aux nombres premiers et qui n'appartiennent pas à eux seuls : tel est le théorème de Fermat, selon lequel $a^{\alpha-1} - 1$ est divisible par α premier, quand a n'est

pas divisible par le même α : Euler a découvert que A étant un nombre composé et A′ étant le dénombrement des entiers moindres que A et premiers avec lui, le nombre entier $a^{A'} - 1$ est divisible par A, pourvu que a soit premier avec A.

[XV]. Voici d'autres cas généraux où les conditions de la formule (15) seront remplies : soit $A = \alpha^h$, α étant premier et h entier positif; si α est supérieur à a, les conditions dont il s'agit pour la formule (15) auront également lieu ; car α étant $> a$, et $a > a_1 > a_2 > a_3, \ldots$, ces entiers, tous moindres que α, seront premiers avec $A = \alpha^h$, puisqu'ils le seront avec α, qui est premier; par suite les entiers $p, p_1, p_2, \ldots, p_{n-1}$ seront premiers à A, d'après ce qui a été prouvé art. [XII], et c'est tout ce qu'exige la formule (15).

Si $A = \alpha . A_1$, A_1 étant un entier qui n'ait aucun facteur premier inférieur à α, et si l'on suppose $\alpha > a$, on en conclura sur-le-champ que les restes $a_1, a_2, \ldots$, tous moindres que α, ne peuvent avoir aucun facteur commun avec lui ni avec A_1, parce que les diviseurs premiers de A_1 ne sont pas moindres que α, par hypothèse; en ce cas, qui comprend les précédents, les conditions du théorème seront remplies, et le nombre

$$a p p_1 p_2 \ldots p_{n-1} + (-1)^{m+1}$$

sera un entier divisible par $A = \alpha A_1$.

α étant encore le moindre diviseur premier de $A = \alpha A_1$, supposons $a > \alpha$: après avoir formé les restes $\pm a_1, \pm a_2, \ldots, \pm a_i$ des premières divisions de A par $a, a_1, a_2, \ldots, a_{i-1}$, si l'on a rencontré pour tous ces restes des nombres hétérogènes à A, et que a_i soit actuellement moindre que α, tous les autres résidus $\pm a_{i+1}$, etc., jusqu'au dernier a_n, seront premiers à A, puisqu'ils seront au-dessous de son plus petit diviseur α : dans ce cas tous les quotients seront aussi premiers à A, et les conditions de l'équation (15) seront assurées.

Ceci suffit pour montrer que la formule (15) et la proposition qu'elle exprime seront souvent applicables.

SECONDE PARTIE.

Application à la résolution de l'équation du premier degré en nombres entiers.

[XVII]. L'analyse précédente s'applique aisément à la détermination des entiers x et y propres à satisfaire à l'équation

$$ax - Ay = 1,$$

à laquelle on ramène la résolution de l'égalité $ax_1 - Ay_1 = B$ en posant

$$x_1 = Bx, \quad y_1 = By:$$

après avoir substitué, on pourra diviser par B, et l'on n'aura plus à traiter que l'équation

$$ax - Ay = 1, \tag{17}$$

où les entiers A et a devront être premiers entre eux.

On sait que, si l'on peut connaître d'une manière quelconque deux valeurs particulières x_0 et y_0 qui satisfassent à cette égalité, en sorte que

$$ax_0 - Ay_0 = 1,$$

on obtiendra sur-le-champ, pour les valeurs générales x, y,

$$x = x_0 + \lambda.A,$$
$$y = y_0 + \lambda.a,$$

λ étant un entier pris à volonté, positif ou non. Si l'on parvient à calculer facilement l'un des nombres x_0 ou y_0, on aura l'autre sans difficulté, puisque la valeur y_0, par exemple, est $y_0 = \frac{ax_0 - 1}{A}$: elle n'exigera qu'une multiplication et une division, dès que x_0 sera exactement connu comme nous le supposons.

Quand A est un nombre premier $\alpha > a$, l'équation étant

$$ax - \alpha y = 1, \tag{18}$$

on arrive immédiatement à une valeur de x_0 à l'aide du théorème que nous avons établi [XIV]. En conservant les notations de cet article, nous avons reconnu, par l'équation (16), que

$$a\,p\,p_1\,p_2 \ldots p_{n-1} - \alpha P_1 = (-1)^m;$$

ou bien, en représentant encore par P le produit $p\,p_1\,p_2 \ldots p_{n-1}$, et en multipliant l'équation par $(-1)^m$,

$$a\mathrm{P}\,(-1)^m - \alpha \mathrm{P}_1\,(-1)^m = 1 : \tag{16}$$

cette relation, où $\mathrm{P}\,(-1)^m$, $\mathrm{P}_1\,(-1)^m$ sont des entiers composés d'éléments numériques connus, autorise à prendre pour x_0 et y_0 les valeurs

$$x_0 = \mathrm{P}(-1)^m, \quad y_0 = \mathrm{P}_1(-1)^m;$$

on aura, par suite, ces valeurs générales de x et y,

$$x = \mathrm{P}(-1)^m + \lambda.\mathrm{A}, \quad y = \mathrm{P}_1(-1)^m + \lambda a, \tag{19}$$

λ étant un entier quelconque à volonté.

La valeur $x_0 = \mathrm{P}(-1)^m$ sera d'un calcul plus simple que celle de $y_0 = \mathrm{P}_1\,(-1)^m$, parce que P_1 serait composé d'un certain nombre de termes à évaluer séparément. On devra pour cette raison déduire, ainsi que nous l'avons dit pour y_0, la valeur de P_1 de l'équation

$$a\mathrm{P} - \alpha \mathrm{P}_1 = (-1)^m,$$

qui donne

$$\mathrm{P}_1 = \frac{a\mathrm{P} - (-1)^m}{\alpha}.$$

[XVIII]. Lorsque les quotients $p, p_1, p_2, \ldots, p_{n-1}$ seront en petit nombre, le calcul de P sera facile; mais dans le cas où n serait un peu grand, et où ces quotients, qui servent maintenant de facteurs, seraient des nombres considérables, P deviendrait un fort grand nombre, pénible

à calculer. Mais on doit observer que, relativement à l'usage de P pour obtenir x, tout multiple de α renfermé dans P est sans utilité, et doit être négligé, parce qu'on peut le regarder comme compris dans la partie $\alpha\lambda$, qui est un multiple entier arbitraire de α. Soit $P_\alpha < \alpha$ le résidu positif ou négatif de P, selon le module α, et soit M le quotient de la division, en sorte que

$$P = P_\alpha + \alpha M;$$

la valeur de x_0 sera

$$x_0 = P_\alpha (-1)^m + \alpha M (-1)^m,$$

et celle de x est

$$x = P_\alpha (-1)^m + \alpha [\lambda + M (-1)^m],$$

ou bien encore

$$x = P_\alpha (-1)^m + \alpha\lambda_1,$$

λ_1 étant un entier pris à volonté : on indiquera dans l'article suivant comment on peut obtenir P_α sans être obligé de calculer complétement le produit P.

D'après la formule (16), on a

$$P_1 = \frac{aP_\alpha + a\alpha M - (-1)^m}{\alpha} = \frac{aP_\alpha - (-1)^m}{\alpha} + aM,$$

ainsi $\frac{aP_\alpha - (-1)^m}{\alpha}$ est un entier.

La valeur de P_1 substituée dans celle de y donne

$$y = \frac{aP_\alpha (-1)^m - 1}{\alpha} + a[\lambda + M (-1)^m],$$

et, en remplaçant par λ_1 le multiplicateur de a, elle est simplement

$$y = \frac{aP_\alpha (-1)^m - 1}{\alpha} + a\lambda_1,$$

que l'on eût formée en portant le valeur de x dans l'équation

$$ax - \alpha y = 1.$$

Ce couple (x, y) ne diffère de celui que nous avions en premier lieu, qu'en ce que le résidu $P_\alpha < \alpha$ remplace le produit P, d'où il tire son origine au moyen de la division de P par α, car λ_1 est un entier arbitraire comme l'était λ; on doit remarquer que le nombre M disparaît et est enveloppé dans λ_1. En posant $\lambda_1 = 0$, on aura simplement ce couple (x, y), que je dénote encore par x_0, y_0,

$$x_0 = P_\alpha (-1)^m,$$
$$y_0 = \frac{a P_\alpha (-1)^m - 1}{\alpha}.$$

Ces nombres seront respectivement au-dessous de α, et a, pour leurs grandeurs numériques : si x_0 est positif, on aura la plus simple solution en nombres positifs de l'équation proposée; mais si $P_\alpha (-1)^m$ était négatif, au lieu de prendre $\lambda_1 = 0$, on poserait $\lambda_1 = 1$, et alors les valeurs

$$x_0 = P_\alpha (-1)^m + \alpha,$$
$$y_0 = \frac{a [P_\alpha (-1)^m + \alpha] - 1}{\alpha},$$

seraient des nombres positifs et moindres que α et a respectivement; les inconnues déterminées sous cette condition résolvent le problème des nombres associés d'Euler (*Opusc. analyt.*); on sait qu'il a nommé associé du nombre entier $a < \alpha$, un nombre entier $x < \alpha$ et tel que le produit ax étant divisé par α, donne l'unité pour résidu ou reste de division; en sorte que x doit satisfaire à l'équation

$$ax = 1 + \alpha y,$$

que nous venons de traiter, et de plus il doit être $< \alpha$.

[XIX]. Cette solution repose entièrement sur le théorème (16), et, quant au calcul arithmétique, sur la détermination du résidu P_α du produit P. On peut obtenir ce résidu sans être obligé de calculer préalablement la valeur complète du produit P : en supposant P composé d'un certain nombre de facteurs considérables par leur grandeur, on pourra choisir les plus gros facteurs p_{n-1}, p_{n-2}, et si leur produit effec-

tué surpasse α, on le divisera par α, afin d'en tirer un résidu ρ relatif à ce module; on multipliera ce résidu ρ par p_{n-3}, et l'on prendra le résidu ρ_1 de ce nouveau produit partiel, toujours pour le même module α; ρ_1 sera lui-même multiplié par p_{n-4}, et l'on cherchera encore, par la division, le résidu du produit $\rho_1 p_{n-4}$: en continuant ainsi à multiplier le dernier résidu formé par un nouveau facteur de P, et poussant la série de ces opérations jusqu'au dernier facteur p, on parviendra évidemment au résidu cherché P_α. Les résidus partiels $\rho, \rho_1, \rho_2, \ldots$ seront tous moindres que α, et il en est ainsi de $p_{n-1}, p_{n-2}, \ldots$: ainsi les produits successivement formés n'atteindront pas α^2. Nous montrerons, dans un exemple, comment on peut faire concourir les divisions qui ont fourni les $p, p_1, p_2, \ldots, p_{n-1}$ à simplifier ces calculs. Cette recherche du résidu P_α n'est pas particulière au cas de α premier; elle sera utile pour d'autres applications; nous avons cru devoir en rappeler la marche, bien connue des personnes qui se sont occupées de la théorie des nombres entiers.

[XX]. Nous avons admis que a était moindre que le nombre premier α; s'il en était autrement et que l'équation fût

$$a'x - \alpha y = 1,$$

a' étant supérieur à α, on pourrait diviser le nombre a' par α; soient h le quotient de la division et $a < \alpha$ le reste, on aurait

$$a' = h.\alpha + a;$$

en mettant cette valeur de a' dans l'équation à résoudre, elle devient

$$(h\alpha + a)\,x - \alpha y = 1,$$

ou bien

$$ax - \alpha(y - hx) = 1.$$

En posant $y - hx = y'$, l'équation se change en

$$ax - \alpha y' = 1,$$

où $a < \alpha$; et cette congruence peut être traitée maintenant par la méthode qui vient d'être expliquée : elle fera connaître les valeurs de x et de y'; or $y = y' + hx$, et partant y sera connu quand on aura x et y'.

[XXI]. Pour premier exemple, nous prendrons l'équation

$$887\,x - 1103\,y = 1,$$

où 1103 est un nombre premier; voici le tableau des divisions exécutées selon la règle de l'article [I] et de manière que les résidus soient moindres que les demi-diviseurs :

		a_1	a_2	a_3
1103	887	216	23	-1
	1	5	48	
	p	p_1	p_2	

Dans chaque division 1103 a servi de dividende : les quotients sont 1, 5, 48; les résidus sont 216, 23 et -1; ainsi deux résidus sont positifs, et le nombre dénoté par $m = 2$; $n = 3$, puisqu'il y a trois divisions opérées avant de rencontrer le résidu ± 1. D'après cela, la valeur de x est, selon la formule (19),

$$(-1)^2 x = 1.5.48 + 1103.\lambda.$$

La valeur positive de $x < 1103$ est donc $5.48 = 240$; celle de y qui lui correspond sera donnée en mettant 240 à la place de x dans

$$y = \frac{887.x - 1}{1103} = \frac{887.240 - 1}{1103} = 193.$$

On a donc pour les valeurs générales de x et y,

$$x = 240 + 1103.\lambda,$$
$$y = 193 + 887.\lambda.$$

Cet exemple n'a exigé que des calculs fort simples, parce que les coefficients 1103 et 887 sont peu considérables. Par la méthode de Lagrange, il faut réduire en fraction continue la fraction $\frac{887}{1103}$: il a trouvé (*Algèbre* d'Euler)

$$\frac{887}{1103} = \cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{9+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\frac{1}{4}}}}}}}$$

les fractions convergentes que l'on doit calculer, par les règles ordinaires, sont

$$\frac{0}{1},\ \frac{1}{1},\ \frac{4}{5},\ \frac{37}{46},\ \frac{78}{97},\ \frac{115}{143},\ \frac{193}{240},\ \frac{887}{1103};$$

la méthode dont il s'agit enseigne que la fraction $\frac{193}{240}$ fournit des valeurs de x et de y, savoir, $x_0 = 240$, $y_0 = 193$, nombres que nous venons d'obtenir.

Nous donnerons un second exemple, où nous choisissons pour coefficients des nombres plus considérables : nous y expliquerons la manière de faire concourir les divisions qui auront fourni les quotients $p, p_1, p_2, \ldots$, à simplifier le calcul du résidu P_α du produit $P = p p_1 p_2 \cdots p_{n-1}$. Le nombre $\alpha = 785809$ est premier d'après la table des diviseurs des nombres de Burckhardt : nous dirons, en passant, que cette table peut être utilement consultée pour des calculs de ce genre, et dans beaucoup d'autres occasions.

Soit donc l'équation

$$4598.x - 785809.y = 1 :$$

on cherchera, selon les règles des art. [I] et [XIV], les quotients

$p, p_1, p_2, \ldots$ Le tableau suivant présente les divisions effectuées avec les moindres résidus positifs ou négatifs.

α	a	$-a_1$	a_2	$-a_3$	a_4
785809	4598	-449	59	-12	1
	171	-1750	13319	-65484	
	p	$-p_1$	p_2	$-p_3$	

Quatre divisions ont été faites, en employant α comme dividende, pour parvenir au résidu $a_4 = 1$: deux résidus, 59 et 1, sont positifs; ainsi $m = 2$, et par suite $(-1)^m = 1$, on aura donc, d'après la formule (19), cette valeur générale de x, pour l'équation donnée,

$$x = 171 \times 1750 \times 13319 \times 65484 - \lambda.\alpha.$$

Avec cette valeur de x on obtiendra celle de y, par l'équation même qui donne

$$y = \frac{ax - 1}{\alpha},$$

elle n'exigera plus qu'une multiplication et une division.

Cette valeur de x exigerait la formation du produit

$$P = 171 \times 1750 \times 13319 \times 65484,$$

qui renfermerait 15 chiffres; l'on a ordinairement besoin de solutions plus simples, et dont la valeur numérique ne dépasse pas α.

On peut éviter, ainsi que nous l'avons dit, de calculer complétement ce produit, et arriver au résidu que fournirait la division de P_α par α. Pour cela on prendra d'abord les deux facteurs

$$13319 \times 65484 :$$

on divise 13319 par $a = 12$, cela donne

$$13319 = 12 \times 1109 + 11 = 12 \times 1110 - 1;$$

multipliant par $p_3 = 65484$, on aura

$$133_{19} \times 65484 = 1110 \times 12 \times 65484 - 65484 :$$

mais par la quatrième division on a

$$12 \times 65484 = 785890 - 1 = \alpha - 1 ;$$

on aura donc

$$133_{19} \times 65484 = 1110(\alpha - 1) - 65484.$$

On négligera la partie qui est multiple de $\alpha = 785809$, et l'on ne prendra que le résidu de ce produit

$$- 1110 - 65484 = - 66594.$$

Ce nombre doit être encore multiplié par les facteurs 171×1750 : on pourra semblablement employer l'une ou l'autre des divisions qui ont amené les quotients $p = 171$, ou $p_2 = 1750$, et l'on trouvera pour résidu du produit P, le nombre négatif $P_\alpha = - 138260$; enfin, ajoutant $\alpha = 785809$, on a

$$875809 - 138260 = 647549 :$$

ce sera la valeur positive de x moindre que α; c'est le nombre associé de 4598 relativement au nombre premier α. Cette valeur de x étant connue, on obtiendra par la division celle de

$$y = \frac{4558 \times 647549 - 1}{\alpha} = 3789.$$

On aura donc encore pour solution générale de l'équation proposée

$$x = 647549 + 785809.\lambda,$$
$$y = 3789 + 4598.\lambda.$$

Afin de faciliter la comparaison de cette solution à celle que donne l'algorithme des fractions continues, je vais rapporter les quotients qui entrent comme dénominateurs des fractions intégrantes, dans la

fraction continue égale à $\frac{a}{\alpha}$: ces quotients sont

$$170,\ 1,\ 9,\ 4,\ 6,\ 2,\ 1,\ 5;$$

en sorte que

$$\frac{a}{\alpha} = \cfrac{1}{170 + \cfrac{1}{1 + \cfrac{1}{9 + \text{etc.}}}};$$

les fractions convergentes à calculer successivement sont

$$\frac{1}{170},\ \frac{1}{171},\ \frac{10}{1709},\ \frac{41}{7007},\ \frac{256}{43751},\ \frac{553}{94509},\ \frac{809}{138260},$$

et la fraction suivante serait

$$\frac{4598}{785809} = \frac{a}{\alpha}.$$

On aura, d'après le procédé de Lagrange,

$$x = -\ 138260,\quad y = -\ 809.$$

Pour déduire de ces valeurs négatives des solutions positives, on ajoutera $\alpha = 785809$ à x, et $a = 4598$ à y; il vient ainsi

$$x = 647549,\quad y = 3789;$$

ce sont les nombres qui ont été trouvés par l'autre méthode. On aurait pu simplifier un peu ce dernier calcul en procédant, pour la formation des quotients de la fraction continue, de manière à amener les moindres restes dans chaque division; mais cela n'aurait pas suffi, ce nous semble, pour compenser la plus grande longueur du calcul numérique.

[XXII]. La résolution de l'équation

$$aX - AY = 1,$$

où A est un nombre composé $\alpha.A_1$, se ramène facilement à celle de deux équations de la forme

$$ax - \alpha y = 1,$$
$$ax_1 - A_1 y_1 = 1;$$

car on tire de celles-ci

$$ax - 1 = \alpha y,$$
$$ax_1 - 1 = A_1 y_1,$$

et par la multiplication

$$(ax - 1)(ax_1 - 1) = \alpha A_1 y y_1,$$

ou bien

$$1 - (ax - 1)(ax_1 - 1) + A y y_1 = 1.$$

Si l'on compare cette équation à la proposée

$$aX - AY = 1,$$

on voit que celle-ci sera satisfaite en posant

$$aX = 1 - (ax - 1)(ay_1 - 1), \quad AY = - A y y_1,$$

ce qui donne les valeurs entières

$$X = x + x_1 - axx_1, \quad Y = - y y_1 :$$

ainsi Y et X seront deux nombres connus si x, x_1, y, y_1 ont été préalablement déterminés. Si α et A_1 sont des nombres premiers, on pourra employer la méthode précédente pour traiter séparément les deux équations en x et y, en x_1 et y_1; si A_1 était encore un nombre composé égal à α_1, α_2,..., on pourrait joindre à l'équation

$$ax - \alpha y = 1$$

les suivantes

$$ax_1 - \alpha_1 y_1 = 1,$$
$$ax_{11} - \alpha_{11} y_{11} = 1,$$
etc.,

d'où

$$(ax - 1)(ax_1 - 1)(ax_{11} - 1) \ldots = \alpha \alpha_1 \alpha_{11} \ldots y y_1 y_{11} \ldots$$

Soit i le nombre de ces facteurs simples α, α_1, α_{11},..., égaux ou inégaux de A; on aurait

$$(ax - 1)(ax_1 - 1)(ax_{11} - 1) \ldots + (-1)^{i-1} - A y y_1 y_{11} \ldots = (-1)^{i-1};$$

en multipliant par $(-1)^{i-1}$ cette formule, on aura

$$1-(1-ax)(1-ax_1)(1-ax_{11})\ldots-A(-1)^{i-1}yy_1y_{11}\ldots=1.$$

Celle-ci étant comparée à l'équation à resoudre

$$aX-AY=1,$$

permet de prendre pour valeurs entières de Y et X,

$$Y=(-1)^{i-1}yy_1y_{11}\ldots\ldots\ldots+\lambda a,$$
$$X=\frac{1-(1-ax)(1-ax_1)(1-ax_{11})\ldots}{a}+\lambda A,$$

λ étant toujours un entier arbitraire positif ou non. Pour le calcul de ces nombres, il convient de s'occuper d'abord de Y: il est donné par le produit des $y, y_1, y_{11},\ldots$ qui sont des nombres connus; quant à X, il le sera par l'équation même lorsque Y aura été obtenu.

Comme la valeur de Y pourra être un grand nombre, on en écartera, si l'on veut, tous les multiples de a selon la marche indiquée [XVIII] pour réduire cette valeur à son résidu selon le module a.

Il existe d'autres procédés pour ramener la congruence $aX-AY=1$ à la résolution des congruences $ax-\alpha y=0$, $ax-\alpha_1y_1=1$, etc. (*Voyez* les *Disquisitiones arithm.* de M. Gauss, ou la traduction française de M. Delille, seconde section, art. 30). Celui que nous venons d'employer est assez simple dans sa marche; mais nous allons exposer une méthode qui dispense, comme celle de Bachet ou de Lagrange, de décomposer A dans ses facteurs premiers α, α_1, etc.

[XXIII]. La méthode de l'art. [XVI] supposait α premier; elle s'applique néanmoins, sans aucune modification, à l'équation

$$ax-Ay=1,$$

où a et A seraient des nombres composés, toutes les fois qu'en procédant sur les entiers $a<A$ qui sont premiers entre eux, comme si l'on voulait déterminer leur commun diviseur, à l'aide du procédé de l'art. [VI], on arrive, par une seule catégorie de divisions, à un dernier résidu ±1 : nous avons indiqué plusieurs cas généraux, dans l'art. [XIV],

où cette circonstance doit se présenter; alors on a, entre les nombres a, A et les quotients $p, p_1, p_2, \ldots, p_{n-1}$, la relation (12)

$$aP - AP_1 = (-1)^m,$$

où $P = p\,p_1\,p_2 \ldots p_{n-1}$: il est clair qu'en appliquant cette formule de la même manière que dans le cas de $A = \alpha$, nombre premier, on arrivera à la valeur de x, savoir,

$$x = P(-1)^m + \lambda.A;$$

et quand x sera connu, on en déduira y par l'équation proposée

$$ax - Ay = 1.$$

Si le produit $P = p\,p_1\,p_2 \ldots p_{n-1}$ est composé de beaucoup de facteurs, on devra procéder à son égard, ainsi que nous l'avons expliqué [XIX], pour arriver à son résidu P_A, relatif au diviseur ou module A.

Cette marche revient encore à celle qui a été expliquée [art. XVIII] : après avoir déterminé le résidu P_A de la division du produit $P = p\,p_1\,p_2 \ldots p_{n-1}$ par A, en sorte que l'on puisse poser

$$P = P_A + M.A,$$

si l'on substitue cette valeur de P dans l'équation (12), elle devient

$$a(P_A + MA) - AP_1 = (-1)^m,$$

ou bien

$$aP_A - (-1)^m = A(P_1 - aM),$$

et par la division on aura

$$P_1 - aM = \frac{aP_A - (-1)^m}{A};$$

soit $P_{1,a}$ le quotient entier fourni au second membre; il sera évidemment au-dessous de a, car $\frac{P_A}{A}$ est moindre que l'unité, P_A étant un résidu qui provient du module A. Avec cette quantité entière $P_{1,a}$, on a l'équation

$$aP_A - AP_{1,a} = (-1)^n,$$

où les nombres P_A et $P_{1,a}$ sont respectivement inférieurs à A et à a: on doit remarquer que la valeur de M n'a pas été calculée: elle dépend du nombre P que l'on a voulu se dispenser d'évaluer.

Lorsque l'on aura rencontré pour dernier résidu a_n de la première catégorie des divisions un nombre différent de ± 1, la formule (12) n'aura plus lieu; en ce cas, on aura la relation générale (11),

$$aP - AP_1 = a_n(-1)^m.$$

On devra passer à la seconde catégorie, où a va servir de dividende constant, a_n de premier diviseur, et l'on trouvera, ainsi qu'il a été expliqué [art. VI], une suite de résidus $\pm b_1$, $\pm b_2, \ldots, \pm b_{n'}$: si le dernier de ces nombres $b_{n'} = 1$, on aura, d'après la formule (13),

$$a[PQ - Q_1(-1)^m] - AP_1Q = (-1)^{m+m'}.$$

En combinant cette formule avec l'équation proposée, ainsi que nous l'avons fait pour le premier cas, et après avoir mis l'équation donnée sous la forme

$$ax(-1)^{m+m'} - Ay(-1)^{m+m'} = (-1)^{m+m'},$$

on en conclura, pour déterminer les valeurs générales des nombres x et y,

$$x(-1)^{m+m'} = PQ - Q_1(-1)^m - \lambda.A,$$
$$y(-1)^{m+m'} = P_1Q - \lambda.a.$$

Les formules

$$(11) \qquad \begin{cases} aP - AP_1 = (-1)^m a_n, \\ a_nQ - aQ_1 = (-1)^{m'}, \end{cases}$$

permettront de simplifier le calcul, s'il se présentait avec trop de complication, en raison de la grandeur des nombres. En effet, au moyen de la relation (11) entre P et P_1, a_n étant un résidu calculé, a et A étant des nombres donnés, on pourra réduire le produit P à son résidu P_A selon A, en négligeant le multiple de A que P renfermera : on calculera ensuite une valeur $P_{1,a}$ par l'équation

$$aP_A - P_{1,a}A = (-1)^m.a_n,$$

qui n'est que l'équation (11) où P est remplacé par P_A; il en résulte

$$P_{1,a} = \frac{aP_A - (-1)^m a_n}{A}.$$

$P_{1,a}$ sera un entier : il différera de P_1 par un multiple de a qui sera le même que le multiple de A par lequel P_A diffère de P. On réduira aussi le produit Q à son résidu Q_a relatif au diviseur a, et dans y on remplacera P_1 et Q par leurs résidus $P_{1,a}$ et Q_a : on pourra même ne prendre à la place du produit P_1Q que son résidu σ relatif à a; on aura ainsi

$$y = \sigma(-1)^{m+m'} + \lambda_1 a;$$

à cette valeur de y on adjoindra la valeur correspondante de x, fournie par l'équation

$$ax - Ay = 1.$$

Le cas que nous venons de traiter où $b_{n'} = \pm 1$, aura nécessairement lieu toutes les fois que $a < A$, sera un nombre premier; il se présentera encore lorsque le plus petit des diviseurs de a surpassera le résidu a_n trouvé à la fin de la première catégorie de divisions [XIV].

Il est facile de voir que si le résidu $b_{n'}$ n'était pas ± 1, comme nous venons de le supposer, il faudrait passer à une nouvelle catégorie de divisions, qui amènerait à employer la relation (14), ou même les relations subséquentes, si l'on était obligé de poursuivre la recherche du dernier résidu qui doit nécessairement prendre la grandeur ± 1, puisque A et a ont été supposés premiers entre eux. Nous répétons qu'il sera très-rare que l'on ait à employer plus de deux catégories de divisions pour parvenir à reconnaître, par le résidu ± 1, que les nombres A et a sont premiers entre eux.