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

ATHANASE DUPRÉ

Sur le nombre de divisions à effectuer pour trouver le plus grand commun diviseur entre deux nombres complexes de la forme $a + b\sqrt{-1}$, où a et b sont entiers

Journal de mathématiques pures et appliquées 1re série, tome 13 (1848), p. 333-343.
<http://www.numdam.org/item?id=JMPA_1848_1_13__333_0>

Sur le nombre de divisions à effectuer pour trouver le plus grand commun diviseur entre deux nombres complexes de la forme $a + b\sqrt{-1}$, *où* a *et* b *sont entiers;*

PAR M. ATHANASE DUPRÉ,

Professeur de Mathématiques appliquées à la Faculté des Sciences de Rennes.

Les opérations à effectuer pour trouver le plus grand commun diviseur entre deux nombres complexes ayant une grande analogie avec celles que l'on pratique pour le même but en arithmétique élémentaire, j'en ai fait l'objet d'un travail semblable à celui que M. Binet a bien voulu présenter de ma part à l'Académie des Sciences dans sa séance du 1er décembre 1845, et qui a été inséré dans le tome XI de ce Journal, page 41.

PREMIÈRE SECTION.

Soient $A = a + b\sqrt{-1}$ et $A_1 = a_1 + b_1\sqrt{-1}$ les deux nombres proposés ayant pour carrés de leurs modules

$$M = a^2 + b^2 \quad \text{et} \quad M_1 = a_1^2 + b_1^2 < M;$$

posons

$$\frac{a + b\sqrt{-1}}{a_1 + b_1\sqrt{-1}} = p + q\sqrt{-1}, \tag{1}$$

d'où

$$p = \frac{aa_1 + bb_1}{a_1^2 + b_1^2} \quad \text{et} \quad q = \frac{a_1 b - ab_1}{a_1^2 + b_1^2}.$$

Prenons pour quotient $p' + q'\sqrt{-1}$, p' et q' étant les entiers contenus dans p et q. De la sorte, on aura les équations

$$p = p' + \alpha, \quad q = q' + \beta,$$

où α et β désigneront les restes de mêmes signes que les parties entières.

En chassant le dénominateur dans l'équation (1) et mettant ces valeurs pour p et q, on trouve

$$(2)\qquad \begin{cases} a+b\sqrt{-1}=(p'+q'\sqrt{-1})\,(a_1+b_1\sqrt{-1}) \\ \qquad\qquad +(\alpha+\beta\sqrt{-1})\,(a_1+b_1\sqrt{-1}), \end{cases}$$

équation qui conduit, comme on sait, à remplacer dans la recherche du plus grand commun diviseur A et A_1, par A_1 et

$$(3)\qquad A_2=(\alpha+\beta\sqrt{-1})\,(a_1+b_1\sqrt{-1}).$$

Le module de A_2, élevé au carré, est

$$(4)\qquad M_2=(\alpha^2+\beta^2)\,M_1.$$

L'équation (1) donne d'ailleurs

$$(5)\qquad M=(p^2+q^2)\,M_1=[(p'+\alpha)^2+(q'+\beta)^2]\,M_1.$$

Il existe donc entre les produits MM_1 et M_1M_2 la relation

$$MM_1=\frac{(p'+\alpha)^2+(q'+\beta)^2}{\alpha^2+\beta^2}\,M_1M_2=\left(1+\frac{p'^2+q'^2+2p'\alpha+2q'\beta}{\alpha^2+\beta^2}\right)M_1M_2,$$

dans laquelle tous les termes peuvent être considérés comme positifs et où p' et q' ne sauraient être nuls en même temps à cause de $M>M_1$. Le cas le plus défavorable est celui où $p'=0$, $q'=1$, et l'on voit que, même alors, on aura

$$MM_1>2M_1M_2.$$

Ainsi le produit des carrés des modules des nombres à diviser l'un par l'autre, celui de plus grand module par celui de plus petit module, devient plus de moitié moindre à chaque nouvelle opération, et la recherche prendra fin après un nombre de divisions plus petit que l'exposant diminué d'une unité de la plus haute puissance de 2 contenue dans MM_1, ou, ce qui équivaut, plus petit que le nombre obtenu en divisant le logarithme de MM_1 par celui de 2 ou 0,301 03, et diminuant de 1 le résultat; ou encore, plus petit que $3{,}321\,93\,(i+i_1)-1$, i et i_1 désignant les nombres de chiffres de M et M_1.

Le seul cas qui puisse échapper à cette limite est celui où deux M

consécutifs sont égaux ; c'est ce qui arrive, par exemple, quand

$$A = 29 + 13\sqrt{-1}, \quad A_1 = 7 + 4\sqrt{-1},$$

on trouve

$$p' = 3, \quad q' = 0, \quad \alpha = \frac{60}{65}, \quad \beta = -\frac{25}{65}, \quad \alpha^2 + \beta^2 = 1,$$

et

$$A_2 = 8 + \sqrt{-1};$$

de sorte que l'on a

$$M_1 = M_2 = 65.$$

Alors la série des opérations devient infinie et les valeurs de A_1 et A_2 se reproduisent successivement.

Pour obvier à cet inconvénient, avant de continuer, on divise A_1 ou A_2 par $1 + \sqrt{-1}$ en ayant soin de tenir compte de ce facteur s'il est commun. Le quotient est $\frac{a_1+b_1}{2} + \frac{a_1-b_1}{2}\sqrt{-1}$, et l'on voit que le caractère de divisibilité consiste en ce que a_1 et b_1 doivent être tous deux pairs ou tous deux impairs. Si A_1 et A_2 n'admettent cela ni l'un ni l'autre, a_1 et b_1 sont l'un pair et l'autre impair; il en est de même de a_2 et b_2, et, de plus, si a_1 est le plus grand de ces quatre nombres, b_1 est nécessairement le plus petit. En multipliant, au besoin, par ± 1, $\pm\sqrt{-1}$, on peut toujours amener A_1 et A_2 aux formes

$$a_1 \pm b_1\sqrt{-1} \quad \text{et} \quad a_2 \pm b_2\sqrt{-1},$$

où a_1 est le plus grand des 4 nombres, b_1 le plus petit, et où les signes sont mis en évidence, les signes supérieurs ayant toujours lieu ensemble, ainsi que les inférieurs. On forme alors un nombre

$$A_1 - A_2 = (a_1 - a_2) \pm (b_2 - b_1)\sqrt{-1},$$

dans lequel figurent les différences arithmétiques $a_1 - a_2$ et $b_2 - b_1$, évidemment toutes deux paires ou toutes impaires; cela fait, on divise ce nouveau nombre par $1 + \sqrt{-1}$, et on l'emploie à la place de A_2 : il a un module moindre. En effet, l'équation

$$a_1^2 + b_1^2 = a_2^2 + b_2^2$$

donne

$$a_1 - a_2 = (b_2 - b_1)\frac{b_2 + b_1}{a_1 + a_2},$$

et, comme $a_2 > b_1$ et $a_1 > b_2$, on en conclut $a_1 - a_2 < b_2 - b_1 < b_2$; le carré du module de $A_1 - A_2$ est donc moindre que $2b_2^2$, et celui du nombre à employer moindre que b_2^2, à fortiori, moindre que $a_2^2 + b_2^2$.

Avec cette simple préparation, dans le cas très-rare où elle est nécessaire, rien ne peut entraver la marche des opérations ni diminuer la généralité de ce qui précède. Dans l'exemple numérique cité plus haut, on est conduit de la sorte à poursuivre la recherche en remplaçant A_2 par $A'_2 = 2 - \sqrt{-1}$ et $M_2 = 65$ par $M'_2 = 5$. A'_2 se trouve être une quantité première et le plus grand commun diviseur cherché, car il divise A_1 et donne pour quotient exact $2 + 3\sqrt{-1}$.

Les quantités désignées par α et β peuvent être mises sous la forme $\frac{K}{M_1}, \frac{K'}{M_1}$, K et K′ étant entiers; en substituant ces valeurs dans l'équation (4), on arrive à la relation

$$K^2 + K'^2 = M_1 M_2,$$

qui prouve que le produit de deux M consécutifs est décomposable en deux carrés parfaits, dont les racines sont les numérateurs de α et β.

DEUXIÈME SECTION.

Dans le *Compte rendu* de la séance de l'Académie des Sciences du 15 mars 1847, M. Wantzel (page 431) prend pour p' et q' les nombres entiers les plus voisins de p et q; de la sorte, α et β, au lieu d'être constamment moindres que 1, sont toujours moindres que $\frac{1}{2}$. Comme on l'a vu dans la première section, cela n'est pas nécessaire pour que les modules décroissent; mais, en opérant ainsi, on peut assigner au nombre des divisions à faire une limite plus restreinte. M. Wantzel fait voir que le nombre des opérations ne saurait surpasser le degré de la plus grande puissance de 2 contenue dans le carré du module le plus petit. Cette limite repose sur ce que $\alpha^2 + \beta^2$ est

une quantité inférieure à $\frac{1}{2}$, parce que α et β sont, chacun en particulier, inférieurs à $\frac{1}{2}$.

On peut aisément la remplacer par une limite plus restreinte, en considérant que s'il est possible, dans un cas déterminé, d'avoir $\alpha = \beta = \pm\frac{1}{2}$, cela ne saurait arriver dans plusieurs divisions consécutives. En effet, les équations (4) et (5) donnent

$$M = \frac{(p'+\alpha)^2+(q'+\beta)^2}{\alpha^2+\beta^2} M_2 = KM_2,$$

et, semblablement,

$$M_1 = \frac{(p''+\alpha')^2+(q''+\beta')^2}{\alpha'^2+\beta'^2} M_3 = K'M_3.$$

En ajoutant un accent à chaque lettre dans l'équation (5) et combinant cette équation avec l'équation (4), on trouve encore

$$(6) \qquad (p''+\alpha')^2+(q''+\beta')^2 = \frac{1}{\alpha^2+\beta^2};$$

de là il résulte $k \overset{=}{>} 5$, ce qui ne peut même avoir lieu deux fois consécutivement, de sorte que si $K' = 5$, on a nécessairement $K > 5$.

Pour prouver ces deux points, remarquons d'abord qu'il est permis de changer les signes des binômes $p'+\alpha$ et $q'+\beta$ dont les carrés entrent seuls dans K; ainsi on atteindra toutes les valeurs possibles de cette dernière quantité en donnant à p' et q' toutes les valeurs entières positives, et à α et β toutes les valeurs positives et négatives numériquement inférieures à $\frac{1}{2}$, ou égales à cette limite. De plus, K étant composé en p' et α comme en q' et β, on peut se dispenser de considérer les hypothèses réciproques; par exemple, après $p' = 0$, $q' = 1$, il est inutile de faire $p' = 1$, $q' = 0$. Cela posé, partons du cas particulier où $p' = 0$, $q' = 1$, $\alpha = \beta = \frac{1}{2}$, dans lequel

$$K = 1 + \frac{1+2\beta}{\alpha^2+\beta^2} = 5.$$

Si l'on fait décroître α, K augmente; si c'est β qui diminue de ε, le

numérateur décroît de 2ε, quantité plus grande que la diminution $2\varepsilon - \varepsilon^2$ subie par le dénominateur; on peut affirmer que le nombre fractionnaire augmente encore. β ne peut d'ailleurs être négatif dans ce cas, parce qu'il en résulterait

$$p = p' + \alpha = 0 + \alpha < 1 \quad \text{et} \quad q = q' + \beta = 1 + \beta < 1,$$

ce qui entraînerait l'inégalité $M < M_1$, contraire à l'hypothèse. On peut donc affirmer qu'avec $p' = 0$, $q' = 1$ on a toujours $K > 5$, si ce n'est lorsque $\alpha = \pm\frac{1}{2}$ et $\beta = \frac{1}{2}$, ce qui donne $K = 5$. $p' = 0$ et $q' = 0$ ne peut se supposer, puisque cela donnerait $p^2 + q^2 < 1$; comme $p' = 0$, $q' = 1$ et β négatif. Si, maintenant, nous faisons croître q', le binôme $q' + \beta$ croîtra, hormis le cas où q' augmentant de 1, β passerait de $+\frac{1}{2}$ à $-\frac{1}{2}$, et alors même $q' + \beta$ ne diminuerait point; on peut en dire autant pour $p' + \alpha$. Ainsi K est constamment plus grand que 5, si ce n'est pour

$$p' = 0 \quad \text{avec} \quad \begin{cases} q' = 1, & \alpha = \pm\frac{1}{2}, & \beta = \frac{1}{2}, \\ q' = 2, & \alpha = \pm\frac{1}{2}, & \beta = -\frac{1}{2}; \end{cases}$$

$$p' = 1 \quad \text{avec} \quad \begin{cases} q' = 1, & \alpha = -\frac{1}{2}, & \beta = \frac{1}{2}, \\ q' = 2, & \alpha = -\frac{1}{2}, & \beta = -\frac{1}{2}; \end{cases}$$

et les hypothèses réciproques, cas dans lesquels on a

$$\alpha^2 + \beta^2 = \frac{1}{2}, \quad (p' + \alpha)^2 + (q' + \beta)^2 = \frac{5}{2}.$$

Lorsque $K' = 5$, K est plus grand que 5, puisque l'équation (6) donne

$$\frac{1}{\alpha^2 + \beta^2} = \frac{5}{2},$$

et, par suite,

$$\alpha^2 + \beta^2 = \frac{2}{5} < \frac{1}{2}.$$

De ces principes on déduit facilement la limite cherchée: soient,

comme précédemment,

$$M,\ M_1,\ M_2,\ldots,\ M_{n-2},\ M_{n-1},\ M_n,$$

les carrés des modules des nombres proposés et des restes successifs, y compris M_n qui est celui du plus grand commun diviseur au moins égal à 1. On aura

$$M \geqq 5M_2,\quad M_2 \geqq 5M_4,\ldots,\quad M_{n-2} \geqq 5M_n \geqq 5.$$

Combinant ces inégalités, on arrive de suite à la relation

$$M > 5^{\frac{n}{2}} = (\sqrt{5})^n, \tag{7}$$

où $\sqrt{5}$ remplace avec avantage le nombre 2 de M. Wantzel. Le cas de n impair n'altère pas la généralité de ce résultat, car alors on arrive de la même manière à

$$M > (\sqrt{5})^{n-3} M_{n-3};$$

et, d'ailleurs M_n est au moins 1, M_{n-1} au moins 2, M_{n-2} au moins 5 fois M_n ou 5, ce qui n'est pas compatible avec $M_{n-3} = 5$ fois M_{n-1} ou 10, et exige M_{n-3} au moins égal à 13, attendu que 11 et 12 ne sont pas décomposables en carrés parfaits : on peut donc poser l'inégalité

$$M_{n-3} \geqq 13 > (\sqrt{5})^3,$$

qui, combinée avec la précédente, redonne la relation (7), toujours vraie, si ce n'est pour n impair et < 3, c'est-à-dire $n = 1$. Dans ce cas, qui n'est pas compris dans la démonstration, il peut arriver, en effet, que $M = 2$, $M_n = M_1 = 1$, et il n'est pas vrai que l'on ait $M = 2 > \sqrt{5}$; mais alors le nombre des divisions à faire est nul. Le nombre des divisions étant évidemment $n - 1$, on peut toujours affirmer que la recherche du plus grand commun diviseur entre deux nombres complexes de la forme $a + b\sqrt{-1}$, où a et b sont entiers, exige un nombre d'opérations inférieur de plus d'une unité à l'exposant de la plus haute puissance de $\sqrt{5}$, contenue dans le carré du plus grand module, ou simplement inférieur à l'exposant de la plus haute

puissance de $\sqrt{5}$, contenue dans le carré du plus petit module; ce qui se démontrerait de même en partant de M_1 au lieu de M. Cet exposant n'est d'ailleurs autre chose que le quotient obtenu en divisant le logarithme du module carré par le logarithme de $\sqrt{5} = 0{,}349485$, et l'on peut substituer à cette division, quand on ne tient pas à une limite très-approchée, le produit du nombre des chiffres du carré, par 2,8614, et, à fortiori, par 3.

Les valeurs des M sont d'ailleurs nécessairement toutes comprises dans la formule $x^2 + y^2$ où x et y sont des entiers incomplexes, et même on ne peut avoir $M_n = 1$ qu'autant que les deux nombres proposés sont premiers entre eux. Alors M_{n-1} peut être 2; M_{n-2} ne peut être 5, à moins que M_{n-2} ne soit M; car $2 \times 5 = 10 = 3^2 + 1^2$ donnerait pour α ou β la valeur $\pm \frac{3}{5}$, numériquement plus grande que $\frac{1}{2}$. M_{n-1} étant pair, M_{n-2} ne peut être 8, car $1 + \sqrt{-1}$ serait diviseur commun, et M_n serait > 1. Ainsi, en remontant la série des M, on voit que, après 1 et 2, on arrive à 9 au moins. En continuant cette discussion, calculant α et β à l'avance au moyen de l'équation (3), et s'aidant, pour abréger, de l'équation (2), où les seules indéterminées sont p' et q', qui représentent des nombres entiers, on voit que M_{n-3} est au moins 32, et M_{n-4} au moins 121 : les M croissent donc beaucoup plus rapidement encore que ne l'indique la limite trouvée plus haut; en conséquence, elle pourrait être plus approchée. Elle ne jouit pas de la propriété de ne pouvoir être remplacée par une meilleure, comme cela a lieu pour la plupart des diverses limites que j'ai données, au sujet du plus grand commun diviseur en arithmétique élémentaire, lorsqu'on ne les simplifie pas en remplaçant le logarithme du plus petit des nombres proposés par le nombre de ses chiffres.

TROISIÈME SECTION.

Nous avons vu précédemmment comment on peut, dans la recherche du plus grand commun diviseur, remplacer les deux nombres proposés par d'autres dont les modules sont de plus en plus petits à mesure que l'on avance dans la série des opérations. On peut aussi se proposer de trouver deux nombres ayant le même plus grand commun

diviseur que les nombres proposés et présentant certaines particularités; tels, par exemple, que l'un d'eux soit incomplexe.

Soient m, n, m', n' des indéterminées entières incomplexes, et posons

$$\begin{aligned} A' &= m(a + b\sqrt{-1}) + n(a_1 + b_1\sqrt{-1}) \\ &= (ma + na_1) + (mb + nb_1)\sqrt{-1}, \\ A'_1 &= m'(a + b\sqrt{-1}) + n'(a_1 + b_1\sqrt{-1}) \\ &= (m'a + n'a_1) + (m'b + n'b_1)\sqrt{-1}; \end{aligned}$$

le plus grand commun diviseur entre A et A_1 divisera évidemment A' et A'_1. Posons, en outre,

$$LA' + L'A'_1 = A, \quad HA' + H'A'_1 = A_1,$$

c'est-à-dire

$$(8) \quad \begin{cases} [(Lm + L'm')a + (Ln + L'n')a_1] \\ + [(Lm + L'm')b + (Ln + L'n')b_1]\sqrt{-1} = a + b\sqrt{-1}, \end{cases}$$

$$(9) \quad \begin{cases} [(Hm + H'm')a + (Hn + H'n')a_1] \\ + [(Hm + H'm')b + (Hn + H'n')b_1]\sqrt{-1} = a_1 + b_1\sqrt{-1}, \end{cases}$$

L, L', H, H' désignant encore des entiers incomplexes: on pourra affirmer que le plus grand commun diviseur entre A' et A'_1 divise A et A_1, et, par suite, qu'il est le même que le plus grand commun diviseur cherché. Mais il faudra vérifier les équations (8) et (9) pour des valeurs quelconques de a, b, a_1, b_1, ce qui exige

$$(10) \quad Lm + L'm' = 1,$$

$$(11) \quad Ln + L'n' = 0;$$

$$(12) \quad Hm + H'm' = 0,$$

$$(13) \quad Hn + H'n' = 1.$$

L'équation (13) montre que n et n' sont des quantités premières entre elles; et, cela étant, l'équation (11) prouve que L est un multiple de n', $L = n't$, et L' un multiple de n, $L' = -nt$; ce qui change l'équation (10) en

$$mn' - m'n = \frac{1}{t},$$

et fait voir que t n'admet que les valeurs $+1$ et -1, et que m, n, m', n' doivent vérifier l'équation

$$mn' - m'n = \pm 1. \tag{14}$$

A cause de la symétrie des calculs, l'équation (12) n'amène pas d'autre condition. m et n peuvent donc être pris arbitrairement parmi les quantités premières entre elles, pourvu qu'on déduise ensuite m' et n' de l'équation (14). Veut-on, par exemple, que A′ soit incomplexe et égal à $ma + na_1$; on posera

$$mb + nb_1 = 0 = m\mathrm{B} + n\mathrm{B}_1,$$

B et B_1 étant les quotients de b et b_1 par leur plus grand commun diviseur, et on prendra $m = \mathrm{B}_1$, $n = -\mathrm{B}$: de la sorte, m et n seront des quantités premières entre elles, et on aura

$$\mathrm{A}' = a\mathrm{B}_1 - a_1\mathrm{B}, \quad \mathrm{A}'_1 = (m'a + n'a_1) \pm \mathrm{D}\sqrt{-1},$$

D étant le plus grand commun diviseur de b et b_1; m' et n' étant deux des valeurs que fournit l'équation

$$\mathrm{B}_1 n' + \mathrm{B}m' = \pm 1.$$

A_1 et A'_1, comparés à A et A_1, offrent certains avantages : le plus grand commun diviseur de A′ et du carré M'_1 du module de A'_1 est le carré du module du plus grand commun diviseur cherché, ce que l'on ne peut affirmer pour A et A′. Cela permet de s'assurer plus promptement si les nombres sont premiers entre eux.

Soient, par exemple,

$$\mathrm{A}_1 = 141 + 106\sqrt{-1} \quad \text{et} \quad \mathrm{A} = 154 - 153\sqrt{-1},$$
$$\mathrm{M}_1 = 31117 \quad \text{et} \quad \mathrm{M} = 47125,$$

b et b_1 étant évidemment premiers entre eux; on a pour valeur de A′, abstraction faite du signe,

$$\mathrm{A}' = 141 \times 153 + 106 \times 154 = 37897.$$

On peut en avoir facilement une moindre. Il suffit, pour que A′ soit une différence arithmétique au lieu d'une somme, de multiplier A

par $\sqrt{-1}$, et de prendre

$$A_1 = 141 + 106\sqrt{-1} \quad \text{et} \quad A = 153 + 154\sqrt{-1};$$

alors

$$B_1 = 53, \quad B = 77, \quad D = 2,$$

et

$$A' = 141 \times 77 - 53 \times 153 = 2748.$$

L'équation (13) devient

$$77n' + 53m' = \pm 1;$$

elle donne $n' = 11$, $m' = -16$ avec le signe inférieur, et, par suite, on a

$$A'_1 = 573 + 2\sqrt{-1}, \quad M'_1 = 328333,$$

en changeant le signe de A'_1, ce qui est permis. M'_1 et A' n'ont pas de commun diviseur, et l'on est assuré que les nombres proposés sont premiers entre eux. M et M_1 ont, au contraire, pour plus grand commun diviseur, 29, ce qui laisse la question indécise.

On peut aussi profiter des indéterminées pour se procurer deux nombres dont l'un ait un module beaucoup plus petit que M_1, ce qui abrége la recherche. Dans l'exemple précédent, $m = n = 1 = n'$ et $m' = 0$ conduisent à remplacer A et A_1 par A_1 et $12 + 48\sqrt{-1}$, dont le module 2448 est plus petit que 31117.