NOUVELLES ANNALES DE MATHÉMATIQUES

E. LIONNET

Note sur la limite du nombre des divisions à faire pour trouver le plus grand commun diviseur de deux nombres entiers

Nouvelles annales de mathématiques 1re série, tome 4 (1845), p. 617-626

<http://www.numdam.org/item?id=NAM_1845_1_4__617_0>

NOTE

Sur la limite du nombre des divisions à faire pour trouver le plus grand commun diviseur de deux nombres entiers ;

PAR M. E. LIONNET,

Professeur de mathématiques au collége royal Louis-le-Grand (*).

Dans cette note, j'indique, pour le nombre des divisions à faire lorsqu'on cherche le plus grand commun diviseur de deux nombres entiers, des limites qui conviennent a tous les systèmes de numération et qui comprennent les limites déjà données par MM. Binet et La[illegible]. De plus, je montre comment on obtient, quel que soit le mode de division, la limite la plus approchée entre toutes celles qui dépendent seulement du plus petit des deux nombres proposés. Les démonstrations dont je fais usage paraîtront, je l'espère, aussi élémentaires que le comporte la nature de la question.

I. Soient A et B les deux nombres proposés, D leur plus grand commun diviseur. Si l'on divise A et B par D et qu'on cherche le plus grand commun diviseur des quotients ainsi obtenus, on effectuera le même nombre de divisions que pour trouver celui des nombres A et B; or ces quotients sont premiers entre eux, donc, dans la recherche d'une limite du nombre de ces divisions, on peut supposer que le plus grand commun diviseur D est égal à l'unité. Cela posé, soient

$$B\ldots\ldots D_5, D_4, D_3, D_2, 1,$$

(*) Un extrait de cette note a été présenté, le 1er décembre dernier, par M. Binet, à l'Académie des sciences.

tous les nombres qui ont servi successivement de diviseurs. Si l'on considère trois diviseurs consécutifs tels que D_5, D_4, D_3, le troisième sera le reste de la division du premier par le second ; donc le premier est au moins égal à la somme des deux autres : mais, D_2 est au moins égal à 2, donc D_3 est au moins égal à 3 ; pareillement, D_4 est au moins égal à 5, D_5 au moins égal à 8, D_6 au moins égal à 13 et D_7 au moins égal à 21 ; donc on a

$$(1)\ D_6 > 10 \text{ et } D_7 > 10 \times 2 ;$$

d'où l'on déduit

$$D_8 > 10 \times 3,\ D_9 > 10 \times 5,\ D_{10} > 10 \times 8,$$
$$D_{11} > 10 \times 13,\ D_{12} > 10 \times 21,$$

et, à plus forte raison,

$$(2)\ D_{11} > 10^2,\ D_{12} > 10^2 \times 2 :$$

Or, de même que les inégalités (1) ont conduit aux inégalités (2), celles-ci conduiront à

$$(3)\ D_{16} > 10^3,\ D_{17} > 10^3 \times 2,$$

ou à

$$D_{3.5+1} > 10^3,\ D_{3.5+2} > 10^3 \times 2,$$

et, ainsi de suite, en supposant que le nombre des diviseurs intermédiaires soit constamment égal à 3 : donc on a généralement

$$D_{5n+1} > 10^n ;$$

mais, 10 étant la base du système dans lequel on opère, 10^n contient $n+1$ chiffres ; d'ailleurs $5n+1$ est le nombre total des divisions effectuées, lorsqu'on prend D_{5n+1} pour premier diviseur ou pour le plus petit B des deux nombres proposés ; donc, lorsqu'on effectue plus de $5n$ divisions, B contient plus de n chiffres, ou autrement, *le nombre des divisions effectuées ne peut excéder cinq fois le nombre des*

chiffres de B. Telle est la limite donnée par M. Lamé (*).

II. En observant que, dans la démonstration précédente, la seule particularité relative à la base 10 consiste en ce qu'on a supposé que le sixième et le septième des nombres 1, 2, 3, 5, 8, 13, 21 contiennent l'un la base et l'autre le double de la base, on voit que des raisonnements analogues sont applicables à une base quelconque, et l'on peut établir cette règle générale : *Pour avoir une limite du nombre de divisons à faire dans la recherche du plus grand commun diviseur de deux nombres entiers, en opérant dans un système dont la base est* b, *on écrit la suite des nombres*

(1) 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144....

dont chacun, à partir du troisième, est égal à la somme des deux qui le précèdent immédiatement, jusqu'à ce qu'on ait obtenu deux termes consécutifs dont l'un contienne la base et l'autre le double de la base; le nombre des termes précédents multiplié par le nombre des chiffres du plus petit des deux nombres proposés est la limite demandée.

Lorsque les deux termes auxquels on s'est arrêté sont précédés immédiatement d'un terme qui contient la base, ainsi que cela arrive pour les bases 2, 3, 5, 7, 8, 11, 12, 13, on reconnaît facilement que la limite peut être diminuée d'une unité. Ainsi, en désignant par c le nombre des chiffres de B, et par l la limite correspondante à la base b, on aura les résultats suivants :

$b =$	2,	3,	4,	5,	6,	7,	8,	9,
$l =$	$2c-1$,	$3c-1$,	$3c$,	$4c-1$,	$4c$,	$5c-1$,	$5c-1$,	$5c$,

$b =$	10,	11,	12,	13.
$l =$	$5c$,	$6c-1$,	$6c-1$,	$6c-1$.

(*) Comptes rendus de l'Académie, 28 octobre 1844.

III. La forme des limites $2c-1$, $3c-1$, $3c\ldots$ varie avec la base b; de plus, si l'on considère, par exemple le nombre 13, écrit dans le système décimal, et le même nombre 21 écrit dans le système dont la base est 6, et qu'on fasse successivement $B=13$ et $B=21$, les limites $5c$ et $4c$ correspondantes à ces bases donneront $l=10$ et $l=8$. Ainsi ces limites varient en général de forme et de grandeur avec la base du système dans lequel on opère, quoique le nombre des divisions à faire soit indépendant de cette base Proposons-nous de déterminer une limite qui convienne à tous les systèmes.

Soient, comme précédemment, A et B les deux nombres dont on cherche le plus grand commun diviseur et R le reste de la division de A par B. En supposant que R ne soit pas contenu exactement dans B, on aura $R > \frac{1}{2}B$ ou $R < \frac{1}{2}B$; dans le premier cas, si l'on divise B par R, on obtiendra le reste $B-R < \frac{1}{2}B$: donc deux divisions au plus sont nécessaires pour obtenir un reste $R_1 < \frac{1}{2}B$; par la même raison deux divisions au plus sont nécessaires pour obtenir un nouveau reste $R_2 < \frac{1}{2}R_1$. En supposant que la même nécessité continue de se présenter jusqu'à ce qu'on ait obtenu le plus grand commun diviseur R_n, on aura la suite d'inégalités $2R_1 < B$, $2R_2 < R_1$, $2R_3 < R_2 \ldots 2R_{n-1} < 2R_{n-2}$, $2R_n < R_{n-1}$ d'où l'on conclut immédiatement

$$2^n \times R_n < B \text{ ou } 2^n < B,$$

en supposant $R_n = 1$. Mais on a fait au plus $2n$ divisions pour obtenir R_n; donc, en comptant la dernière, *on en a fait au plus* $1+2n$, n *étant l'exposant de la plus grande puissance de* 2 *contenue dans le plus petit* B *des deux nombres proposés.* M. Binet a trouvé, par une démonstration analogue, la limite plus simple $1+n$ (*), mais en considérant la division sous un

(*) Journal de M. Liouville, tome VI, 1841.

autre point de vue. Il n'est peut-être pas sans intérêt de montrer que cette limite $1+2n$ est une conséquence immédiate de la limite $2c-1$ que nous avons déterminée précédemment et qui correspond au cas où le nombre B est écrit dans le système binaire.

En effet 2 étant la base du système et c le nombre des chiffres de B, on a $B = \text{ou} > 2^{c-1}$ et $B < 2^c$; donc $c-1$ est égal à l'exposant n de la plus grande puissance de 2 contenue dans B; donc $c = 1 + n$ et, par suite, $2c - 1 = 1 + 2n$.

IV. Considérons la suite des nombres

(1) 1, 2, 3, 5, 8, 13, 21, 34, 55, 89.....

auxquels on reconnaît immédiatement cette propriété, que si l'on cherche le plus grand commun diviseur de deux termes consécutifs, tels que 34 et 21, on obtiendra successivement pour restes les nombres précédents 13, 8, 5, 3, 2, 1 et le dernier reste 0; d'où il résulte que le nombre des divisions effectuées est égal au nombre des termes qui précèdent le plus grand 34 des deux nombres qu'on a pris dans la série.

Pour obtenir la limite $5c$, nous avons supposé seulement que les sixième et septième termes de cette série contiennent l'un la base 10 et l'autre le double de cette base, sans tenir aucun compte de l'excès 3 de 13 sur 10 ni de l'excès 1 de 21 sur 10×2; il est donc présumable qu'en ayant égard à ces différences nous pourrons trouver une limite plus approchée.

On a vu précédemment que D_2 est au moins égal à 2 ou, autrement, que lorsqu'on fait deux divisions pour trouver le plus grand commun diviseur des nombres A et B, le plus petit nombre B est au moins égal à 2; pareillement, quand on fait trois divisions, B est au moins égal à 3; quand on fait 4 divisions, B est au moins égal à 5, et, en général, quand

on fait n divisions, B est au moins égal au n^e terme de la série (1). Cela étant, supposons qu'on demande une limite du nombre des divisions à faire, lorsqu'on a, par exemple, $B = 17$: si l'on cherche dans la série (1) le premier terme $21 > 17$, le nombre 6 des termes précédents sera la limite demandée ; car si l'on était obligé de faire plus de 6 divisions, B serait au moins égal à 21, ce qui est contraire à l'hypothèse. Je dis de plus qu'aucune autre limite, dépendant seulement de B, ne donnera pour maximum du nombre des divisions un nombre inférieur à 6. Car, si cela était, cette même limite appliquée au nombre $13 < 17$ donnerait encore un maximum inférieur à 6; et l'on vient de voir qu'en supposant $A = 21$ et $B = 13$ le nombre des divisions à faire était égal à 6. On peut donc établir cette règle générale : *Pour avoir la limite la plus approchée du nombre des divisions à faire dans la recherche du plus grand commun diviseur de deux nombres entiers* A *et* B, *on écrit les termes de la série* (1) *jusqu'au premier terme supérieur à* B ; *le nombre des termes précédents est la limite demandée.*

V. Chaque fois qu'une division conduirait à un reste plus grand que la moitié du diviseur correspondant, on peut ajouter une unité au quotient et soustraire le dividende du produit du diviseur par le quotient, ce qui conduit à un reste moindre que la moitié du diviseur. En réduisant ainsi deux divisions à une seule, on conçoit qu'on puisse trouver des limites moindres que celles qu'on vient d'obtenir. Supposons donc qu'on apporte cette modification à la recherche du plus grand commun diviseur des nombres A et B, et soient, comme précédemment,

$$B \ldots \ldots D_5,\ D_4,\ D_3,\ D_2,\ 1,$$

tous les nombres qui ont servi de diviseurs. Si l'on considère trois diviseurs consécutifs tels que D_5, D_4, D_3, le troisième

sera le reste de la division du premier par le second ; donc, suivant qu'on aura pris le quotient par excès ou par défaut, afin d'obtenir un reste $D_3 < \frac{1}{2} D_4$, on aura

$$D_5 = \text{ou} > 3D_4 - D_3 \text{ ou } D_5 = \text{ou} > 2D_4 + D_3.$$

Désignant par K l'excès de D_4 sur $2D_3$, on trouve

$$3D_4 - D_3 = 5D_3 + 3K \text{ et } 2D_4 + D_3 = 5D_3 + 2K,$$

d'où l'on conclut

$$2D_4 + D_3 < 3D_4 - D_3.$$

Donc, quel que soit le mode de division, on aura toujours

$$D_5 = \text{ou} > 2D_4 + D_3 :$$

mais D_3 est au moins égal à 2, donc D_3 est au moins égal à 5 ; pareillement, D_4 est au moins égal à 12, D_5 au moins égal à 29 et ainsi de suite ; donc on a

$$(4) \qquad D_4 > 10 \text{ et } D_5 > 10 \times 2.$$

Or, de même que les inégalités (1) ont conduit à

$$D_{5n+1} > 10^n$$

Les inégalités (4) conduiront, par des raisonnements analogues, à

$$D_{3n+1} > 10^n$$

d'où l'on conclut que *le nombre des divisions à faire ne peut excéder trois fois le nombre des chiffres de* B. M. Binet a donné la limite moins approchée $1 + \frac{10}{3} c$ (*).

On reconnaît aisément que la série

$$(2) \qquad 1, 2, 5, 12, 29 \ldots\ldots$$

(*) Journal de M. Liouville, tome VI, 1841, et comptes rendus de l'Académie, 4 novembre 1844.

dans laquelle 3 termes consécutifs sont tels que le 3^e est égal au double du 2^e augmenté du 1^{er}, donne lieu à des conséquences analogues à celles qu'on a déduites de la série (1). Aussi nous contenterons-nous de les énoncer :

1° *Pour avoir une limite* l' *du nombre de divisions à faire dans la recherche du plus grand commun diviseur de deux nombres entiers* A *et* B, *on écrit les termes de la série* (2) *jusqu'au premier qui contienne la base du système dans lequel on opère, le nombre des termes précédents multiplié par le nombre des chiffres du plus petit* B *des deux nombres proposés est la limite demandée.* On trouve ainsi les résultats suivants :

$$b = 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10, 11, 12, 13$$
$$l' = c,\ 2c,\ 2c,\ 2c,\ 3c,\ 3c,\ 3c,\ 3c,\ 3c,\ 3c,\ 3c,\ 4c$$

On voit que la limite $3c$ est commune à 7 bases différentes et que, *pour trouver le plus grand commun diviseur de deux nombres écrits dans le système dont la base est* 2, *le nombre des divisions à faire ne peut excéder le nombre des chiffres du plus petit* B *des deux nombres proposés.*

Remarque. Le nombre B étant écrit dans le système dont la base est 2, on a $B = \text{ou} > 2^{c-1}$ et $B < 2^c$; donc $c - 1$ est égal à l'exposant n de la plus grande puissance de 2 contenue dans B; donc $c = 1 + n$. Telle est la limite donnée par M. Binet.

2° *Pour avoir la limite la plus approchée du nombre de divisions à faire, dans la recherche du plus grand commun diviseur de deux nombres entiers* A *et* B, *on écrit les termes de la série* (2) *jusqu'au premier terme supérieur à* B, *le nombre des termes précédents est la limite demandée.*

VI. Lorsqu'on connaît le plus grand commun diviseur de A et B, ou plus généralement un facteur D commun à ces deux nombres, on substitue à B, dans le calcul des limites

précédentes, le quotient $\frac{B}{D}$, ou seulement au nombre des chiffres de B celui des chiffres de ce quotient, ce qui donne ordinairement des limites plus approchées.

Prenons pour exemple les nombres 2904 et 1122 écrits dans le système décimal, et dont le plus grand commun diviseur s'obtient en effectuant 5 ou 4 divisions selon la manière d'opérer. Les limites $5c$ et $3c$ appliquées à 1122 donnent $l = 20$, $l' = 12$: l'emploi des séries (1) et (2) donnent les limites plus approchées $l = 15$, $l' = 9$. Mais les nombres 2904 et 1122, étant divisibles par 2, par 3, et par 11, sont divisibles par le produit $2 \times 3 \times 11 = 66$ et, sans effectuer la division de 1122 par 66, on voit que le quotient de cette division contient deux chiffres; ce qui réduit les limites $5c$ et $3c$ à $l = 10$, $l' = 6$. Enfin si l'on divise 1122 par 66 et qu'on emploie les séries (1) et (2) en substituant le quotient 17 à 1122, on aura les limites encore plus approchées $l = 6$, $l' = 4$.

VII. Supposons qu'en cherchant le plus grand commun diviseur de A et B, on ait pris tous les quotients par excès afin d'obtenir des restes moindres que la moitié des diviseurs correspondants, et soient, dans cette nouvelle hypothèse,

$$B.... \; D_5, \; D_4, \; D_3, \; D_2, \; 1,$$

tous les nombres employés comme diviseurs. Si l'on considère trois diviseurs consécutifs, tels que D_5, D_4, D_3, on aura

$$D_5 = \text{ou} > 3\,D_4 - D_3.$$

Or D_2 est au moins egal à 2, donc D_3 est au moins égal à 5, D_4 au moins égal à 13, D_5 au moins égal à 34, etc. On est ainsi conduit à la suite des nombres

(3) $\qquad 1, \; 2, \; 5, \; 13, \; 34, \; 89, \; 233....$

dans laquelle trois termes consécutifs sont tels que le troi-

sième est égal au triple du second moins le premier. Cette série donnerait lieu à des conséquences analogues à celles qu'on a déduites des séries (1) et (2) : mais, comme les termes qui la composent sont l'unité et tous les termes de rang pair de la série (1), on voit qu'étant donnée une limite l déduite de la série (1) et relative au mode ordinaire de division, on obtiendra une limite l'' relative au cas actuel, en faisant $l''=1+\frac{1}{2}l$. Ainsi, par exemple, la limite $l=5c$ donnera $l''=1+\frac{5}{2}c$, c'est-à-dire que, lorsqu'en opérant dans le système décimal on a pris tous les quotients par excès, afin d'obtenir des restes moindres que la moitié des diviseurs correspondants, *le nombre des divisions effectuées ne peut excéder l'unité augmentée de cinq fois la moitié du nombre des chiffres du plus petit* B *des deux nombres proposés.*

Nota. La limite dite de M. Binet, relative aux quotients le plus approchés, est déjà ancienne et depuis longtemps du domaine public. La limite de M. Lamé, relative aux quotients ordinaires, est nouvelle, M. Finck en a donné une démonstration dans ce volume (p. 71); le beau travail qu'on vient de lire complète et simplifie la théorie. Le lecteur attentif aura remarqué l'erreur qui nous a échappé dans un travail analogue (p. 569); on n'a $n < 3k$ que lorsque k est moindre que 3. Tm.