TABLE D'ÉLÉMENTS RELATIFS A LA BASE 30030 POUR LA RECHERCHE RAPIDE DES FACTEURS PREMIERS DES GRANDS NOMBRES

Autor(en): **Lebon, Ernest**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **9 (1907)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-10146

semble de lignes tel qu'il en passe une par deux points quelconques de l'espace comprend forcément des lignes s'étendant à l'infini. C'est ainsi que parmi les cercles orthogonaux à un plan, qui forment, comme on sait, un tel ensemble, figurent les droites parallèles à ce plan. On doit donc conclure que les métriques elliptiques archimédiennes n'ont pas d'existence géométrique, dans notre conception de l'espace. Mais ces métriques s'imposeraient, au contraire, si l'espace venait à être conçu, selon l'idée émise par Riemann, comme une variété numérique fermée[1]. On peut bien ajouter que rien ne permet d'affirmer que cette conception n'est pas celle de l'avenir.

G. COMBEBIAC (Bourges).

TABLE D'ÉLÉMENTS RELATIFS A LA BASE 30030 POUR LA RECHERCHE RAPIDE DES FACTEURS PREMIERS DES GRANDS NOMBRES

La dignité de la science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre.
GAUSS[1].

I. — PRÉLIMINAIRES.

1. Pour *reconnaître si un nombre donné est composé ou premier et trouver les facteurs premiers d'un nombre composé*, il n'existe ni de méthode générale, ni de procédé pratique ; on a, il est vrai, quelques procédés applicables à des nombres ayant des formes particulières ; mais il est regrettable de constater que l'on ne soit guère maintenant plus avancé qu'au début du XIX^me^ siècle et que les réflexions, suivantes publiées par GAUSS[2] en 1801, soient malheureusement encore vraies.

« On ne peut s'empêcher de convenir que toutes les mé-
« thodes proposées jusqu'à présent sont restreintes à des cas

[1] Ou mieux, si la *continuité géométrique* venait à être assimilée à celle d'une variété numérique fermée.

[2] *Disquisitiones Arithmeticæ*, Lipsiæ, 1801. N° 329. — Cet Ouvrage a été traduit par POULLET-DELISLE sous le titre *Recherches Arithmétiques*, Paris, 1807. P. 416.

« très particuliers, ou sont si longues et si pénibles, que « même pour ceux de ces nombres qui ne dépassent pas les « limites des Tables dont on est redevable à quelques mathé- « maticiens, c'est-à-dire pour les nombres à l'égard desquels « ces méthodes sont inutiles, elles fatiguent la patience du « calculateur le plus exercé, et qu'elles ne sont pour ainsi « dire pas applicables à de plus grands nombres. »

Notons que LEGENDRE [1] a écrit en 1830 des considérations analogues à celles de GAUSS et que E. LUCAS [2] a jugé nécessaire de reproduire en 1876 les réflexions précitées.

Par exemple, ce n'est qu'après des raisonnements et des calculs assez longs et compliqués que LEGENDRE arrive à montrer qu'il suffit d'essayer les nombres premiers 83, 107, 163, 401, 409, 467 et 509 pour conclure que le petit nombre 333667 est premier; que Th. PEPIN [3] trouve que le nombre 7444009 est égal à 53.140453. Ce dernier savant, en constatant qu'il trouve le facteur premier 53, ne peut s'empêcher d'ajouter : « On regrette de ne pas avoir employé la méthode des diviseurs ».

2. — C'est pour obvier à l'absence de méthode pratique que l'on s'est astreint à construire des Tables de diviseurs premiers des nombres. Mais il ne faut pas songer à continuer la publication de telles Tables dans le mode de disposition employé jusqu'ici, consistant à inscrire chaque nombre et son moindre diviseur premier : en effet, il a fallu, pour les 9 premiers millions, 9 volumes dont chacun contient 112 pages grand in-4°, les chiffres étant imprimés en petits caractères.

La Table dont je propose l'emploi pour résoudre le double problème en question, dont la construction repose sur d'élégantes propriétés non encore signalées de certaines progressions arithmétiques, n'exige que de rapides comparaisons de nombres et occupe une surface petite relativement à l'importance des résultats qu'elle donne. Son emploi constitue une méthode uniforme applicable aux grands nombres.

---

[1] *Théorie des Nombres*, 3e édit., Paris, 1830. N° 256. N° 260.

[2] Compte rendu de la Session tenue à Clermont-Ferrand en 1876 par l'Association Française pour l'Avancement des Sciences. P. 61.

[3] *Extension de la Méthode d'Euler pour la décomposition des grands nombres en facteurs premiers*. Memorie della Pontificia Accademia dei nuovi Lincei, vol. IV, Roma, 1893. P. 72.

3. — Soient :

B le produit $\alpha\beta...\lambda$ de nombres premiers consécutifs $\alpha,\beta,...,\lambda$ à partir de 2 ;

P le produit $(\alpha - 1)(\beta - 1)\ldots(\lambda - 1)$;

I l'un quelconque des P nombres premiers à B et inférieurs à B ;

K un nombre successivement égal aux entiers positifs, à partir de 0.

On reconnaît aisément que : *Chacun des systèmes des* P *progressions arithmétiques de terme général* BK+I *renferme tous les nombres premiers autres que ceux qui forment* B.

On peut dire que B est la *base* du système considéré et que I est l'*indicateur* d'un terme de ce système.

Deux indicateurs sont dits *complémentaires* lorsque leur somme est égale à la base.

4. — Soient N, D et M des nombres d'un système de progressions de base B.

Il est évident que : *Le nombre* N *est ou n'est pas divisible par le diviseur* D *selon que* K *et* M *sont ou ne sont pas tels que l'équation*

$$(a) \qquad BK + I = MD$$

soit satisfaite, B, I *et* D *étant connus.*

Soient k et m les valeurs *minima* de K et M satisfaisant à l'équation (a). Les nombres k se nomment *caractéristiques.*

Nous dirons que la caractéristique k et l'indicateur I sont les *éléments* du nombre N par rapport à un diviseur D.

5. — Le lecteur est supposé connaître les propriétés que j'ai établies [1] pour calculer les éléments k et I. La construction

[1] Mon premier travail sur ce sujet a été signalé à l'Académie des Sciences de Paris, dans la séance du 3 Juillet 1905 (*Comptes Rendus,* T. CXLI, Paris, 1905, P. 78). Mes principaux Mémoires se trouvent dans le *Jornal de Sciencias Mathematicas, Physicas e Naturaes* publié par l'Académie Royale des Sciences de Lisbonne (1er Août 1905; 2e série, T. VII, Lisbonne, 1906); dans les *Rendiconti* de l'Académie Royale des Lincei (Vol. XV, Roma; Nota presentata dal Socio V. VOLTERRA nella Seduta del 22 Aprile 1906); dans le *Bulletin* de la Société Philomathique de Paris (28 Avril 1906, Paris, à la Sorbonne, 1906); dans le *Bulletin* de la Société Mathématique Américaine (May 1906, New York, 1906); dans les *Comptes Rendus* du Congrès tenu à Lyon en août 1906 par l'Association Française pour l'Avancement des Sciences; dans *Il Pitagora, Giornale di Matematica* di GAETANO FAZZARI (Anno XIII, 1906-1907, Palermo, nº 6-7, 1907). Ce Journal contient une Table de base 30030 donnant, pour les nombres inférieurs à 510510, les caractéristiques relatives aux diviseurs premiers de 17 à 709, le multiplicateur correspondant à la première valeur de l'indicateur pour chaque caractéristique et cette première valeur, et permettant, par suite, d'abréger notablement la recherche des facteurs premiers de ces nombres.

de la Table dont je propose l'emploi dépend principalement de la propriété suivante :

Lorsque deux nombres N *et* N_1, $N > N_1$, *admettent le même diviseur* D *et la même caractéristique* k, *la différence de leurs indicateurs* I *et* I_1 *est multiple de* D.

Il en résulte que, si m et m_1 sont les multiplicateurs de D tels que $N = Dm$, $N_1 = Dm_1$, on a la formule

$$(b) \qquad m = m_1 + \frac{I - I_1}{D} .$$

Pour trouver les facteurs premiers de m ou reconnaître que m est premier, on cherche si m se trouve parmi les indicateurs des groupes 0 dans les Tableaux D, de 17 à 173, ou bien on se sert de la *Table de caractéristiques relatives à la base 2310* (1).

II. — Disposition des Eléments.

6. — Au point de vue de la moindre surface occupée par la Table de base 30030, je vais donner une disposition des éléments plus avantageuse que celle que j'ai proposée au Congrès des Sociétés Savantes en avril 1906.

7. — Pour chaque diviseur premier D, ces diviseurs étant considérés en ordre croissant à partir de 17, on forme un Tableau de la manière suivante :

La caractéristique la plus faible $k = \varkappa$ correspond au carré du diviseur premier considéré δ. On écrit cette caractéristique, puis le multiplicateur $m_1 = \delta$, ensuite l'indicateur I_1 relatif à δ^2, enfin les indicateurs I relatifs aux produits de δ par les multiplicateurs m non divisibles par les nombres premiers inférieurs à δ. On écrit la caractéristique $k = \varkappa + 1$, puis le premier multiplicateur m_1 non divisible par les nombres premiers inférieurs à δ, ensuite l'indicateur I_1 relatif au produit δm_1, enfin les indicateurs I relatifs aux produits de δ par les multiplicateurs m non divisibles par les nombres premiers inférieurs à δ. On continue à écrire ainsi les valeurs successives de k, de m_1, de I_1, des indicateurs I, jusqu'à et y compris la caractéristique $k = \delta - 1$.

---

1 Paris, Delalain Frères, 1906.

Comme les valeurs des multiplicateurs m vont en croissant, il en est de même des valeurs des indicateurs relatifs à une même caractéristique.

8. — La Table sera donc formée d'autant de *Tableaux* D qu'elle contiendra de diviseurs premiers D. Chaque Tableau D contiendra autant de *groupes* d'indicateurs que de caractéristiques inscrites.

De D = 17 à D = 173, les Tableaux D commencent à la caractéristique 0; à partir de D = 179, de D = 251, de D = 307,..., les Tableaux D commencent respectivement aux caractéristiques 1, 2, 3,.....

III. — Mode d'emploi de la Table.

9. — Soit N un nombre non divisible par les facteurs premiers 2, 3, 5, 7, 11 et 13 de la base 30030. En divisant N par 30030, ce qui est rapide, on trouve pour quotient le nombre K et pour reste l'indicateur I.

10. — Par rapport aux caractéristiques k d'un Tableau D, le nombre K peut être inférieur à D — 1, égal à D — 1, supérieur à D — 1.

Si K > D — 1, soient $\mathscr{Q}$ et $\mathscr{R}$ respectivement le quotient et le reste obtenus en divisant K par D. On est alors ramené à se servir de $\mathscr{R}$ de la même manière dont on se sert de K, lorsque K $\leq$ D — 1.

11. — Supposons que l'on ait reconnu que N admet le facteur premier D.

Si K $\leq$ D — 1, la formule (*b*) donne le multiplicateur m de D.

Si K > D, le multiplicateur de D est un nombre M inférieur à N et ayant la forme BK + I. Alors, on trouve la formule

$$(c) \qquad M = B\mathscr{Q} + \left(m_1 + \frac{I - I_1}{D}\right).$$

12. — Selon que I se trouve ou ne se trouve pas, dans le Tableau 17, parmi les indicateurs soit du groupe $k = K$, soit du groupe $k = \mathscr{R}$, N est ou n'est pas divisible par 17.

Lorsqu'un nombre N n'est divisible par aucun des diviseurs

premiers inférieurs à un diviseur $D = \delta$, le Tableau δ indique de même que N est ou n'est pas divisible par δ.

13. — Soit à résoudre, avec la Table de base 30030, le double problème en question.

On consulte le Tableau **17**. Si l'on reconnaît que N est divisible par 17, on calcule le multiplicateur m ou M ; on cherche si m ou M est divisible par 17 ; etc., jusqu'à un multiplicateur m ou M non divisible par 17. On est alors ramené à résoudre, pour le multiplicateur M le problème que l'on va résoudre quand on a reconnu que N n'est pas divisible par 17.

Sachant que N n'est pas divisible par 17, on voit si N est divisible par 19 en consultant le Tableau **19**. Si l'on reconnaît que N est divisible par 19, on calcule le multiplicateur m ou M ; on cherche si m ou M est divisible par 19 ; etc., etc.

Si l'on arrive à un Tableau Δ tel que $I = I_1$, on en conclut que $N = \Delta^2$.

Sinon, on est averti que l'on a essayé tous les diviseurs premiers de 17 au nombre premier Δ immédiatement inférieur à $\sqrt{N}$, lorsque l'on arrive à un diviseur premier Δ' tel que $I < I_1$.

Avant de consulter les Tableaux D en ordre croissant à partir du Tableau **17**, on regarde s'il y a un Tableau Δ tel que $I = I_1$ sinon on cherche le Tableau Δ' tel que $I < I_1$. Alors, on consulte d'abord tous les Tableaux D où il existe une caractéristique $k = K$. Etc.

IV. — Remarques.

14. — Si les indicateurs inscrits étaient remplacés par des nombres égaux à $\frac{I-1}{2}$ ou à $\frac{I-15015}{2}$, selon que l'indicateur est supérieur ou inférieur à 15015, la Table serait encore moins étendue.

15. — Comme, pour le diviseur premier 17, il n'y a aucun indicateur supprimé, on peut diminuer de moitié l'étendue du Tableau **17** en faisant correspondre à chaque caractéristique seulement les indicateurs inférieurs à 15015. Alors, si l'on trouve $I > 15015$, on cherche le complément de I dans les indicateurs inscrits à la caractéristique $16-k$.

16. — Si l'on formait les autres Tableaux D en ne supprimant aucun indicateur, on pourrait aussi n'y inscrire que les indicateurs inférieurs à 15015, et opérer de même quand on a $I > 15015$.

17. — Se plaçant toujours au point de vue de faire occuper à la Table le moins possible de surface, on pourrait, pour un certain nombre des diviseurs premiers D les plus petits, n'inscrire, à chaque caractéristique de 0 à $D - 1$, que les indicateurs inférieurs à 15015, mais en ne supprimant pas les indicateurs venant d'un produit Dm divisible par les nombres premiers inférieurs à D. Alors, quand N donnera le quotient K et l'indicateur I supérieur à 15015, on regardera si le complément de I se trouve parmi les indicateurs qui correspondent soit à $k = D - 1 - K$, soit à $k = D - 1 - \mathcal{R}$.

18. — On peut prendre pour nombres directeurs des Tableaux les caractéristiques k, des groupes les facteurs premiers D. Alors, on consulte d'abord le tableau $k = K$. Lorsque I se trouve parmi les indicateurs d'un groupe D', N est divisible par D' ; s'il n'en est pas ainsi, il y a deux cas. 1° Quand $K < 17$, N est premier. 2° Quand $K \geqq 17$, on consulte le groupe 17 du Tableau $k = \mathcal{R}_{17}$: si I se trouve dans ce groupe, N est divisible par 17 ; sinon, N n'admet pas le facteur 17 et il faut consulter le groupe 19 du Tableau $K = \mathcal{R}_{19}$; etc ; N est premier lorsque l'on est conduit à un diviseur premier D supérieur à K.

Paris, Février 1907.

ERNEST LEBON.