

I. — Préliminaires.

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **19.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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 fermée¹. 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.
GAUSS¹.

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 GAUSS² en 1801, soient malheureusement encore vraies.

« On ne peut s'empêcher de convenir que toutes les méthodes 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 Arithmeticae*, 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*, 3^e 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 $\alpha\beta\dots\lambda$ de nombres premiers consécutifs $\alpha, \beta, \dots, \lambda$ à partir de 2 ;

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

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*

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

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 établies¹ 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. CXXI, 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 (1^{er} Août 1905; 2^e 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, n^o 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'abrégier 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

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

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 ÉLÉMENTS.

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 $k = \alpha$ 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 $k = \alpha + 1$, 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.