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

G. LEJEUNE-DIRICHLET

Démonstration de cette proposition : toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une infinité de nombres premiers

Journal de mathématiques pures et appliquées 1re série, tome 4 (1839), p. 393-422.
<http://www.numdam.org/item?id=JMPA_1839_1_4__393_0>

DÉMONSTRATION DE CETTE PROPOSITION :

Toute progression arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun, contient une infinité de nombres premiers;

PAR M. G. LEJEUNE-DIRICHLET.

(Lue à l'Académie des Sciences de Berlin, le 27 juillet 1837) (*).

Il suffit de considérer attentivement la suite naturelle des nombres premiers pour y découvrir, par voie d'induction, une foule de propriétés dont la généralité sera rendue d'autant plus probable que l'induction aura été poussée plus loin. Mais la démonstration rigoureuse de ces propriétés est ordinairement sujette aux plus grandes difficultés. Un des résultats les plus remarquables en ce genre est celui que l'on obtient en divisant chaque terme de la suite naturelle des nombres premiers par un même nombre quelconque. Exceptant les nombres premiers qui sont facteurs du diviseur, tous les autres laisseront des restes premiers à l'égard du diviseur. Or, on remarque d'abord que tout reste de cette espèce revient indéfiniment, et ensuite, prenant le rapport entre les nombres qui désignent combien de fois deux de ces restes ont reparu jusqu'à un terme quelconque de la suite, ce rapport a pour limite l'unité, la division étant continuée indéfiniment. Mettons de côté cette dernière circonstance, et ne faisons attention qu'au retour indéfini de chaque reste : alors le résultat de l'observation peut s'énoncer ainsi : toute progression

---

(*) Nous devons à l'obligeance de M. Terquem la traduction de cet excellent Mémoire imprimé en allemand dans le Recueil de l'Académie de Berlin. (J. L.)

arithmétique dont le premier terme et la raison sont des entiers sans diviseur commun contient une infinité de nombres premiers. Il n'existe pas de démonstration rigoureuse du théorème qui vient d'être énoncé ; et toutefois de nombreuses applications rendent une telle démonstration très désirable. Legendre est, que je sache, le seul analyste qui ait essayé de le démontrer. Ce théorème avait pour lui, outre l'attrait de la difficulté, un intérêt tout particulier, puisqu'il s'en était servi comme lemme dans ses travaux précédents (*). L'illustre géomètre fait dépendre sa démonstration de la solution de cette question : étant donnée une suite quelconque de nombres premiers impairs, trouver le plus grand nombre des termes consécutifs d'une progression arithmétique qui seraient divisibles par quelqu'un des nombres de la suite ; mais la solution qu'il donne n'est fondée que sur une induction. En essayant de prouver l'exactitude de cette solution, d'une simplicité si remarquable, on rencontre des difficultés qu'il m'a été impossible de surmonter. Ce n'est qu'après avoir abandonné cette voie, que je suis parvenu à la démonstration rigoureuse du théorème. Elle n'est pas purement *arithmétique*, puisqu'elle est fondée en partie sur la considération de grandeurs *continues*. A raison de la nouveauté des principes sur lesquels elle repose, j'ai cru, avant d'en venir au cas général, devoir considérer le cas particulier où la raison de la progression arithmétique est un nombre premier impair.

§ I^er^.

Soit p un nombre premier impair,
c une de ses racines primitives :

de sorte qu'en divisant par p la progression géométrique

$$c^0,\ c^1,\ c^2,\ c^3,\ \ldots . c^{p-2},$$

on trouve pour restes les nombres $1, 2, 3 \ldots . p-1$, dans un ordre quelconque.

(*) *Théorie des Nombres*, 4^e^ partie, § IX, p. 399, seconde édition.

Soit la congruence $c^\gamma \equiv n \pmod{p}$: γ étant supposé $< p-1$, nous l'appellerons, avec M. Gauss, l'indice du nombre n et nous le désignerons au besoin par γ_n. Le choix de la racine primitive est indifférent; mais une fois adoptée, on ne doit plus en changer. Cette définition de l'indice étant admise, on démontre facilement que l'indice d'un produit est égal au reste qu'on obtient en divisant par $p-1$ la somme des indices des facteurs. Observons de plus qu'on a toujours $\gamma_1 = 0$, $\gamma_{p-1} = \frac{p-1}{2}$, et que γ_n est pair ou impair, selon que n est ou n'est pas résidu quadratique de p, ou bien, en employant la notation de Legendre, selon qu'on aura

$$\left(\frac{n}{p}\right) = +1 \text{ ou } \left(\frac{n}{p}\right) = -1.$$

Soit maintenant q un nombre premier pair ou impair différent de p, et s un nombre positif plus grand que l'unité. Désignons par ω une racine de l'équation

$$\omega^{p-1} - 1 = 0, \qquad (1)$$

et formons la progression géométrique

$$\frac{1}{1 - \omega^\gamma \cdot \frac{1}{q^s}} = 1 + \omega^\gamma \cdot \frac{1}{q^s} + \omega^{2\gamma} \cdot \frac{1}{q^{2s}} + \omega^{3\gamma} \cdot \frac{1}{q^{3s}} + \ldots \qquad (2)$$

γ étant l'indice de q, en sorte que l'on a $c^\gamma \equiv q \pmod{p}$.

En donnant à q toutes les valeurs dont il est susceptible, et multipliant ensemble toutes les équations résultantes, le produit des seconds membres donne une série dont la loi est facile à trouver. En effet, soit $n = q'^{m'} \cdot q''^{m''} \ldots$, où q', q'', $\ldots$ désignent divers nombres premiers, alors le terme $n^{ième}$ aura la forme

$$\omega^{m'\gamma_{q'} + m''\gamma_{q''} + \cdots} \cdot \frac{1}{n^s};$$

mais on a

$$m'\gamma_{q'} + m''\gamma_{q''} + \ldots \equiv \gamma_n \pmod{p-1};$$

donc en vertu de l'équation (1),

$$\omega^{m'\gamma_{q'}+m''\gamma_{q''}+\cdots} = \omega^{\gamma_n}.$$

Ainsi, l'on a l'équation

$$\Pi.\frac{1}{1-\omega^{\gamma}.\frac{1}{q^s}} = \Sigma\omega^{\gamma}.\frac{1}{n^s} = \mathrm{L}. \qquad (3)$$

Le signe de multiplication Π s'étend à toutes les valeurs que peut prendre q, tandis que le signe sommatoire s'étend à tous les nombres entiers positifs n non divisibles par p. Dans le premier membre γ est l'indice de q ou γ_q; dans le second membre il désigne l'indice de n ou γ_n.

L'équation (3) renferme $p-1$ équations que l'on obtient en mettant pour ω ses $p-1$ valeurs. On sait que ces valeurs peuvent se représenter par les puissances d'une seule d'entre elles convenablement choisie. Soit Ω cette valeur; on aura donc

$$\Omega^0,\ \Omega^1,\ \Omega^2,\ \Omega^3 \ldots\ldots \Omega^{p-2},$$

pour les $p-1$ valeurs de ω; et nous désignerons les valeurs correspondantes de L par

$$\mathrm{L}_0,\ \mathrm{L}_1,\ \mathrm{L}_2,\ \ldots\ldots \mathrm{L}_{p-2}. \qquad (4)$$

Il est évident qne L_0 et $\mathrm{L}_{\frac{p-1}{2}}$ correspondent aux valeurs de $\omega = 1$, $\omega = -1$ et sont indépendantes de Ω.

Avant d'aller plus loin, il est nécessaire de dire pourquoi s doit être plus grande que l'unité. La nécessité de cette restriction est fondée sur la diversité qu'on remarque entre les séries infinies. En considérant les valeurs numériques des termes d'une série, ou les valeurs de leurs modules si les termes sont imaginaires, il peut se présenter deux cas : ou bien la somme d'un nombre quelconque de ces valeurs numériques reste toujours inférieure à une certaine limite finie, ou bien elle est susceptible de croître jusqu'à l'infini. Dans le premier cas, la série est convergente et a une somme complétement déterminée et indépendante de l'ordre des termes, soit qu'ils procèdent d'après une dimension, ou d'après une ou plusieurs dimen-

sions, et forment une suite simple, double ou multiple. Dans le second cas, la série *peut* encore être convergente; mais cette convergence, ainsi que la valeur de la somme, dépendent de l'ordre suivant lequel les termes se succèdent. Si la convergence a lieu pour un certain ordre de succession, elle peut cesser pour un ordre différent, ou bien la somme peut devenir autre. Ainsi, par exemple, les deux séries suivantes sont formées des mêmes termes :

$$1 - \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} - \frac{1}{\sqrt{4}} + \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{6}} + \ldots\ldots$$

$$1 + \frac{1}{\sqrt{3}} - \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{5}} + \frac{1}{\sqrt{7}} - \frac{1}{\sqrt{4}} + \ldots\ldots$$

La première est convergente, la seconde ne l'est pas; tandis que les deux séries

$$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \ldots\ldots,$$

$$1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \ldots\ldots,$$

quoique convergentes toutes deux, n'ont pas la même somme.

Revenant à la série infinie L, il est facile de voir qu'elle appartient aux séries de la première espèce en prenant $s > 1$. Faisons $L = \lambda + \mu\sqrt{-1}$; λ et μ seront des quantités finies déterminées. Quant au premier membre de l'équation (3), si l'on désigne par $f_m + g_m\sqrt{-1}$ le produit des m premiers facteurs de la forme $\frac{1}{1-\omega^{\gamma}\frac{1}{q^s}}$, ces facteurs étant pris dans un ordre quelconque, on pourra toujours prendre m assez grand pour que parmi les m premiers facteurs se trouvent tous ceux pour lesquels on a $q < h$, h désignant un nombre entier quelconque. Dès que m aura atteint ce degré de grandeur, chacune des deux différences $f_m - \lambda$, $q_m - \mu$, abstraction faite du signe, restera toujours plus petite que..... $\frac{1}{h^s} + \frac{1}{(h+1)^s} + \ldots\ldots$ quelque accroissement ultérieur que prenne m. Mais dans la supposition de $s > 1$, et dans celle-là seulement, la somme $\frac{1}{h^s} + \frac{1}{(h+1)^s} + \ldots$ devient plus petite qu'aucune quantité

donnée, en attribuant à h une valeur suffisamment grande. Il est donc démontré que le produit infini (3), quel que soit l'ordre des facteurs, est égal à la série infinie L; mais pour $s = 1$ ou < 1, cette démonstration cesse d'avoir lieu; en effet dans ce cas le produit infini n'a plus, en général, une valeur déterminée, indépendamment de l'ordre de multiplication. Lors même qu'on serait sûr que le produit infini a une valeur déterminée pour un certain ordre de multiplication, l'équation (3) ne serait d'aucune utilité pour trouver cette valeur, quoique, convenablement interprétée, elle subsistât toujours. Dans ce cas, q', q'', q''',... étant les valeurs de q correspondant à l'ordre adopté, il faudrait considérer L comme une série multiple composée d'abord des termes dans lesquels n ne contient que le facteur q', puis des termes où n contient seulement les facteurs q' et q'', et ainsi de suite. La nécessité de donner cette forme à la série rendrait sa sommation aussi pénible que la recherche directe du produit infini: la série ne présente de l'avantage sous le rapport de la simplicité, que lorsque l'ordre des termes peut être quelconque ou du moins ne dépend pas des facteurs premiers de n.

§ II.

Faisant donc $s = 1 + \rho$, quelque petite que soit la quantité positive ρ, l'équation (3) subsistera. Cherchons ce que devient la série L, lorsque ρ devient infiniment petit. Nous commencerons par le cas où $\omega = +1$, L étant alors $L_{(0)}$. Considérons la suite

$$S = \frac{1}{k^{1+\rho}} + \frac{1}{(k+1)^{1+\rho}} + \frac{1}{(k+2)^{1+\rho}} + \ldots,$$

dans laquelle k est une constante positive.

Si dans la formule connue

$$\int_0^1 x^{k-1} \log^\rho \left(\frac{1}{x}\right) dx = \frac{\Gamma(1+\rho)}{k^{1+\rho}},$$

on met pour k successivement k, $k+1$, $k+2$,... et qu'on ajoute les résultats, il vient

$$S = \frac{1}{\Gamma(1+\varepsilon)} \int_0^1 \log^\rho \left(\frac{1}{x}\right) \frac{x^{k-1}}{1-x}\, dx :$$

on a

$$\frac{1}{\varepsilon} = \frac{\Gamma\varepsilon}{\Gamma(1+\varepsilon)} = \frac{1}{\Gamma(1+\varepsilon)} \int_0^1 \log^{\rho-1} \left(\frac{1}{x}\right) dx ;$$

donc

$$S = \frac{1}{\varepsilon} + \frac{1}{\Gamma(1+\varepsilon)} \int_0^1 \left(\frac{x^{k-1}}{1-x} - \frac{1}{\log \frac{1}{x}} \right) \log^\rho \left(\frac{1}{x}\right) dx ,$$

et lorsque ρ devient infiniment petit, le second terme a pour limite finie

$$\int_0^1 \left(\frac{x^{k-1}}{1-x} - \frac{1}{\log \frac{1}{x}} \right) dx.$$

Considérons la suite plus générale

$$\frac{1}{b^{1+\rho}} + \frac{1}{(b+a)^{1+\rho}} + \frac{1}{(b+2a)^{1+\rho}} + \dots ,$$

contenant les deux constantes a et b ; mettant cette suite sous la forme

$$\frac{1}{a^{1+\rho}} \left[\frac{1}{\left(\frac{b}{a}\right)^{1+\rho}} + \frac{1}{\left(\frac{b}{a}+1\right)^{1+\rho}} + \frac{1}{\left(\frac{b}{a}+2\right)^{1+\rho}} + \dots \right],$$

et la comparant avec S, on voit immédiatement qu'elle est égale à une expression de cette forme

$$\frac{1}{a} \cdot \frac{1}{\varepsilon} + \varphi(\rho),$$

$\varphi(\rho)$ ayant une limite finie, pour ρ infiniment petit.

La suite $L_{(0)}$ est la réunion de $p-1$ suites partielles, que l'on obtient en mettant pour m les valeurs $1, 2, 3, \dots p-1$ dans la suite

$$\frac{1}{m^{1+\rho}} + \frac{1}{(p+m)^{1+\rho}} + \frac{1}{(2p+m)^{1+\rho}} + \dots :$$

$L_{(\omega)}$ a donc une valeur de la forme

$$L_{(\omega)} = \frac{p-1}{p} \cdot \frac{1}{\rho} + \varphi(\rho); \qquad (5)$$

ρ étant infiniment petit, $\varphi(\rho)$ a une limite finie, qu'on peut facilement, d'après ce qui précède, exprimer par une intégrale définie, ce qui toutefois n'est pas nécessaire pour notre but. L'équation (5) montre que pour ρ infiniment petit, $L_{(\omega)}$ est infiniment grand; mais que $L_{(\omega)} - \frac{p-1}{p} \frac{1}{\rho}$ a une valeur finie.

§ III.

Passons maintenant aux cas où ω a une valeur différente de l'unité. Quoique la valeur de la série L, pour $s>1$, ne dépende point de l'ordre de ses termes, il est toutefois avantageux dans notre recherche, d'adopter l'ordre où n va en croissant: dans cette supposition $\Sigma\omega^\gamma \frac{1}{n^s}$ est une fonction de s, qui conserve une valeur finie et continue pour toute valeur positive de s, de sorte qu'en faisant $s = 1 + \rho$ et ρ infiniment petit, la série a pour limite $\Sigma\omega^\gamma . \frac{1}{n}$; ce qui n'arrive pas nécessairement lorsque n ne suit pas un ordre ascendant, car alors $\Sigma\omega^\gamma \frac{1}{n}$ peut différer de $\Sigma\omega^\gamma \frac{1}{n^{1+\rho}}$ d'une quantité finie, ou même n'avoir aucune valeur déterminable. Pour démontrer cette dernière assertion, désignons par h un nombre entier positif; la somme des $h(p-1)$ premiers termes de la suite L est

$$\frac{1}{\Gamma(s)} \int_0^1 \frac{\frac{1}{x} f(x)}{1-x^p} \log^{s-1}\left(\frac{1}{x}\right) dx - \frac{1}{\Gamma(s)} \int_0^1 \frac{\frac{1}{x} f(x)}{1-x^p} \log^{s-1}\left(\frac{1}{x}\right) x^{hp} dx,$$

où pour abréger, l'on a mis

$$f(x) = \omega^{\gamma_1} x + \omega^{\gamma_2} x^2 + \omega^{\gamma_3} x^3 + \ldots \omega^{\gamma_{p-1}} x^{p-1}.$$

Cette expression de la somme est une conséquence de l'équation

donnée ci-dessus, et qui existe pour toute valeur positive de s,

$$\int_0^1 x^{n-1} \log^{s-1}\left(\frac{1}{x}\right) dx = \frac{\Gamma(s)}{n^s}.$$

Or l'on a

$$f(1) = \omega^{\gamma_1} + \omega^{\gamma_2} + \ldots \omega^{\gamma_{p-1}} = 1 + \omega + \ldots \omega^{p-2} = 0$$

lorsque ω n'est pas l'unité; donc le polynome $\frac{1}{x} f(x)$ sera divisible par $1 - x$; débarrassant la fraction qui est sous le signe d'intégration du facteur commun $1 - x$, cette fraction devient

$$\frac{t + u\sqrt{-1}}{1 + x + x^2 + \ldots x^{p-1}};$$

t et u sont des polynomes à coefficients réels. Si nous désignons par T et U, les valeurs maxima de t et u, dans l'intervalle de $x = 0$ à $x = 1$, alors les parties réelle et imaginaire de l'intégrale affectée du signe — seront respectivement plus petites que

$$\frac{T}{\Gamma(s)} \int_0^1 x^{hp} \log^{s-1}\left(\frac{1}{x}\right) dx = \frac{T}{(hp+1)^s},$$
$$\frac{U}{\Gamma(s)} \int_0^1 x^{hp} \log^{s-1}\left(\frac{1}{x}\right) dx = \frac{U}{(hp+1)^s};$$

ainsi cette seconde intégrale disparaît pour $h = \infty$; donc la série, en adoptant l'ordre croissant de n, est convergente, et l'on a

$$\sum \omega^{\gamma} \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^1 \frac{\frac{1}{x} f(x)}{1 - x^p} \log^{s-1}\left(\frac{1}{x}\right) dx.$$

Cette fonction de s, tant que l'on a $s > 0$, reste finie et continue, et cette propriété appartient même à son coefficient différentiel. Pour s'en assurer, il suffit de différentier par rapport à s, puis de faire attention que $\Gamma(s)$ et $\frac{d\Gamma(s)}{ds}$ sont également finies et continues, et que $\Gamma(s)$ ne peut devenir nulle tant que s est positive.

Faisant donc

$$\frac{1}{\Gamma(s)}\int_0^1 \frac{\frac{1}{x}f(x)}{1-x^p}\log^{s-1}\left(\frac{1}{x}\right)dx = \psi(s)+\chi(s)\sqrt{-1},$$

$\psi(s)$ et $\chi(s)$ étant des fonctions réelles, on aura pour $\rho > 0$, d'après un théorème connu,

$$(6)\quad \psi(1+\rho)=\psi(1)+\rho\psi'(1+\delta\rho),\quad \chi(1+\rho)=\chi(1)+\rho\chi'(1+\varepsilon\rho),$$

où δ et ε sont des fractions positives dépendant de ρ, et où

$$\psi'(s) = \frac{d\psi(s)}{ds},\quad \chi'(s) = \frac{d\chi(s)}{ds}.$$

Pour $\omega = -1$, on a évidemment $\chi(s) = 0$, et en passant d'une racine ω à sa conjuguée $\frac{1}{\omega}$, $\psi(s)$ conserve la même valeur, mais $\chi(s)$ prend une valeur de signe opposé.

§ IV.

Il nous reste à faire voir que la limite finie vers laquelle s'approche $\sum \omega^\nu \frac{1}{n^{1+\rho}}$, lorsque ρ devient infiniment petit et que ω n'est pas l'unité, ne se réduit pas à zéro. D'après le paragraphe précédent, cette limite est donnée par l'intégrale

$$\sum \omega^\nu \frac{1}{n} = -\int_0^1 \frac{\frac{1}{x}f(x)}{x^p-1}dx,$$

intégrale qui peut s'exprimer aisément en fonctions logarithmiques et circulaires. En effet, soit $x - e^{\frac{2m\pi}{p}\sqrt{-1}}$ un facteur linéaire du dénominateur $x^p - 1$; m est un des nombres de la suite $0, 1, 2, \ldots p-1$. Soit A_m le numérateur de la fraction partielle correspondant à ce facteur; on aura, d'après les formules connues

$$A_m = \frac{1}{p} f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right);$$

lorsque $m = 0$, $A = 0$; donc

$$\sum \omega^{\gamma} \frac{1}{n} = -\frac{1}{p} \sum f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right) \int_0^1 \frac{dx}{x - e^{\frac{2m\pi}{p}\sqrt{-1}}},$$

le signe $\sum$ dans le second membre s'étend de $m = 1$ à $m = p - 1$.

La fonction $f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right)$ est connue; c'est celle qu'on rencontre dans la division du cercle : elle se réduit facilement à la forme $f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)$. On a en effet

$$f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right) = \sum \omega^{\gamma_g} e^{gm\frac{2\pi}{p}\sqrt{-1}},$$

en prenant g depuis 1 jusqu'à $p - 1$. Soit h le reste de la division de gm par p; les diverses valeurs de h seront $1, 2 \ldots p - 1$; et à cause de la congruence $gm \equiv h \pmod{p}$, l'on a $\gamma_g \equiv \gamma_h - \gamma_m \pmod{p-1}$; si l'on remplace γ_g par $\gamma_h - \gamma_m$, ce qui est permis à cause de l'équation $\omega^{p-1} - 1 = 0$, il vient

$$f\left(e^{\frac{2m\pi}{p}\sqrt{-1}}\right) = \omega^{-\gamma_m} \sum \omega^{\gamma_h} e^{h\frac{2\pi}{p}\sqrt{-1}} = \omega^{-\gamma_m} f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right);$$

on a donc

$$\sum \omega^{\gamma} \cdot \frac{1}{n} = -\frac{1}{p} f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right) \sum \omega^{-\gamma_m} \int_0^1 \frac{dx}{x - e^{\frac{2m\pi}{p}\sqrt{-1}}};$$

mais α étant une fraction positive, on a

$$\int_0^1 \frac{dx}{x - e^{2\alpha\pi\sqrt{-1}}} = \log(2 \sin \alpha\pi) + \frac{\pi}{2}(1 - 2\alpha)\sqrt{-1};$$

par conséquent

$$\sum \omega^{\gamma} \cdot \frac{1}{n} = -\frac{1}{p} f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right) \sum \omega^{-\gamma_m} \left[\log\left(2 \sin \frac{m\pi}{p}\right) + \frac{\pi}{2}\left(1 - \frac{2m}{p}\right)\sqrt{-1}\right].$$

Quoique cette expression de $\sum \omega^{\gamma} \frac{1}{n}$ soit très simple, on ne peut pas en conclure en général, que cette quantité ne puisse devenir zéro. Il nous manque encore les principes nécessaires pour établir les conditions auxquelles doivent satisfaire des relations transcendantes, renfermant des nombres entiers indéterminés, pour pouvoir s'anéantir. Cependant, on peut montrer l'impossibilité de la réduction à zéro pour le cas où $\omega = -1$; mais le raisonnement n'est pas applicable aux valeurs imaginaires de ω pour lesquelles nous donnerons une démonstration spéciale dans le paragraphe suivant. Soit donc $\omega = -1$: en observant que γ_m est pair si $\left(\frac{m}{p}\right) = +1$, et impair si $\left(\frac{m}{p}\right) = -1$, on en conclut $(-1)^{-\gamma_m} = \left(\frac{m}{p}\right)$, $(-1)^{\gamma_n} = \left(\frac{n}{p}\right)$; donc pour ρ infiniment petit, la limite de L_{-1} sera

$$\sum \left(\frac{n}{p}\right)\frac{1}{n} = -\frac{1}{p} f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right) \sum \left(\frac{m}{p}\right)\left[\log\left(2\sin\frac{m\pi}{p}\right) + \frac{\pi}{2}\left(1 - \frac{2m}{p}\right)\sqrt{-1}\right],$$

ou, plus simplement

$$\sum \left(\frac{n}{p}\right)\frac{1}{n} = -\frac{1}{p} f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right) \sum \left(\frac{m}{p}\right)\left[\log\left(2\sin\frac{m\pi}{p}\right) - \frac{\pi}{p} m\sqrt{-1}\right];$$

car dans l'intervalle de $m = 1$ à $m = p - 1$, on a $\sum \left(\frac{n}{p}\right) = 0$.

Il faut maintenant distinguer deux cas, selon que le nombre premier p est de la forme $4\mu + 3$ ou $4\mu + 1$; dans le premier cas, l'on a

$$\left(\frac{m}{p}\right) = -\left(\frac{p-m}{p}\right) \quad \text{et} \quad \sin\frac{m\pi}{p} = \sin\frac{(p-m)\pi}{p},$$

par conséquent la partie réelle de la somme disparaît. Et si l'on désigne par a les valeurs de m correspondant à $\left(\frac{m}{p}\right) = +1$ et par b celles qui répondent à $\left(\frac{m}{p}\right) = -1$, en d'autres termes si a et b sont

les résidus quadratiques et non quadratiques de p, plus petits que p, on aura

$$\sum\left(\frac{n}{p}\right)\frac{1}{n}=\frac{\pi}{p^2}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)(\Sigma a-\Sigma b)\sqrt{-1}.$$

Si $p=4\mu+1$, alors $\left(\frac{m}{p}\right)=\left(\frac{p-m}{p}\right)$; et la partie imaginaire disparaissant, l'on a

$$\sum\left(\frac{n}{p}\right)\frac{1}{n}=\frac{1}{p}f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)\log\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}};$$

le signe multiplicateur Π s'étend à toutes les valeurs de a et de b.

D'après des formules connues (*),

$$f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)=\sqrt{p}\,\sqrt{-1} \quad \text{si} \quad p=4\mu+3,$$
$$f\left(e^{\frac{2\pi}{p}\sqrt{-1}}\right)=\sqrt{p} \quad \text{si} \quad p=4\mu+1;$$

on obtient donc respectivement

$$\sum\left(\frac{n}{p}\right)\frac{1}{n}=\frac{\pi}{p\sqrt{p}}(\Sigma b-\Sigma a), \quad \sum\left(\frac{n}{p}\right)\frac{1}{n}=\frac{1}{\sqrt{p}}\log\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}},$$

suivant que $p=4\mu+3$ ou $=4\mu+1$.

Lorsque $p=4\mu+3$, on a $\Sigma a+\Sigma b=\frac{p(p-1)}{2}=$ un nombre impair; donc dans ce cas on ne peut avoir $\Sigma a=\Sigma b$; par conséquent $\sum\left(\frac{n}{p}\right)\frac{1}{n}$ ne peut pas devenir nulle.

Lorsque $p=4\mu+1$, on a recours à deux équations connues, et qu'on rencontre dans la division du cercle (**), savoir

$$2\Pi\left(x-e^{\frac{2a\pi}{p}\sqrt{-1}}\right)=Y-Z\sqrt{p}, \quad 2\Pi\left(x-e^{\frac{2b\pi}{p}\sqrt{-1}}\right)=Y+Z\sqrt{p},$$

(*) *Comment. Gotting. rec. vol.* I, ou *Mémoires de l'Académie de Berlin*, 1835.

(**) *Disq. arith.* art. 357.

où Y et Z représentent des polynomes à coefficients entiers : de ces deux équations, on déduit

$$4\cdot\frac{x^p-1}{x-1} = Y^2 - pZ^2;$$

si dans les trois équations précédentes, on fait $x=1$, et qu'on désigne par g et h les valeurs de Y et Z, on obtient, réduction faite,

$$2^{\frac{p+1}{2}}\,\Pi\sin\frac{a\pi}{p} = g - h\sqrt{p},$$

$$2^{\frac{p+1}{2}}\,\Pi\sin\frac{b\pi}{p} = g + h\sqrt{p},$$

$$g^2 - ph^2 = 4p.$$

Cette dernière équation montre que g est divisible par p; faisant donc $g=pk$, il vient

$$\frac{\Pi\sin\frac{b\pi}{p}}{\Pi\sin\frac{a\pi}{p}} = \frac{k\sqrt{p}+h}{k\sqrt{p}-h},\quad h^2 - pk^2 = -4:$$

la seconde de ces équations fait voir que h ne peut être égal à zéro; par conséquent, les deux membres de la première équation sont chacun différents de l'unité; d'où l'on conclut, d'après l'expression donnée ci-dessus, que $\sum\left(\frac{n}{p}\right)\frac{1}{n}$ ne peut avoir une valeur nulle. C. Q. F. D.

On peut ajouter à cela que $\sum\left(\frac{p}{n}\right)\frac{1}{n}$, étant pour ρ infiniment petit, la limite de $\Pi\frac{1}{1-\left(\frac{q}{p}\right)\frac{1}{q^{1+\rho}}}$, produit entièrement formé de facteurs positifs, ne peut devenir négative, et par conséquent a toujours une valeur positive.

De cette observation découlent immédiatement deux propositions importantes, et qu'il serait probablement très difficile de démontrer par une autre voie. Celle qui est relative au cas de $p=4\mu+3$ consiste en ce que pour les nombres premiers de cette forme, on a

toujours $\Sigma b > \Sigma a$. Toutefois, nous n'insisterons pas ici sur ces conséquences de notre méthode; nous nous proposons d'y revenir dans une autre occasion.

§ V.

Il nous reste à démontrer que la limite de L_m, pour ρ infiniment petit, est différente de zéro, lors même que l'on n'a pas $m = 0$ ou $m = \frac{p-1}{2}$. A cet effet, prenons le logarithme de $\Pi \frac{1}{1 - \omega^\gamma \frac{1}{q^{1+\rho}}}$, et développons le logarithme de chaque facteur, d'après la formule

$$-\log(1-x) = x + \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 + \ldots :$$

il vient ainsi

$$\Sigma\omega^\gamma \frac{1}{q^{1+\rho}} + \tfrac{1}{2}\Sigma\omega^{2\gamma}\frac{1}{(q^2)^{1+\rho}} + \tfrac{1}{3}\Sigma\omega^{3\gamma}\frac{1}{(q^3)^{1+\rho}} + \ldots = \log L;$$

le signe sommatoire est relatif à q, et γ est l'indice de q. Remplaçons ω successivement par ses valeurs $1, \Omega, \Omega^2, \ldots \Omega^{p-2}$, ajoutons tous les résultats et observons que la somme

$$1 + \Omega^{h\gamma} + \Omega^{2h\gamma} + \ldots + \Omega^{(p-2)h\gamma},$$

est nulle, excepté quand on a $h\gamma \equiv 0 \pmod{p-1}$, auquel cas cette somme devient égale à $p-1$; remarquons de plus que cette dernière congruence équivaut à celle-ci $q^h \equiv 1 \pmod{p}$; nous obtiendrons

$$(p-1)\left(\Sigma\frac{1}{q^{1+\rho}} + \tfrac{1}{2}\Sigma\frac{1}{q^{2+2\rho}} + \tfrac{1}{3}\Sigma\frac{1}{q^{3+3\rho}} + \ldots\right) = \log(L_0 L_1 \ldots L_{p-2}),$$

la sommation est relative aux valeurs de q dont la première, seconde... puissance est contenue dans la forme $Mp+1$. Le premier membre étant réel, il s'ensuit qu'il faut prendre dans le second membre, le logarithme *arithmétique* du produit $L_0 L_1 \ldots L_{p-2}$. Quelle que

soit la valeur de ρ, le premier membre est toujours positif; or nous allons démontrer que si l'on suppose une limite nulle à L_m pour ρ infiniment petit, le second membre devient $-\infty$, tandis que le premier reste toujours positif; donc la supposition est inadmissible. En effet, on peut donner au second membre cette forme

$$\log L_{(0)} + \log L_{\frac{p-1}{2}} + \log L_1 L_{p-2} + \log L_2 L_{p-3} + \dots$$

On a, d'après l'équation (5),

$$\log L_{(0)} = \log\left(\frac{p-1}{p} \cdot \frac{1}{\varepsilon} + \varphi(\rho)\right) = \log\frac{1}{\varepsilon} + \log\left(\frac{p-1}{p} + \rho\varphi(\rho)\right),$$

le second terme du second membre a pour limite la quantité finie $\log\left(\frac{p-1}{p}\right)$; $\log L_{\frac{p-1}{2}}$ reste aussi une quantité finie, car, d'après le paragraphe 4, la limite de $L_{\frac{p-1}{2}}$ est une quantité différente de zéro. Or, d'après le paragraphe 3, l'on a

$$\log L_m L_{p-1-m} = \log[\psi^2(1+\rho) + \chi^2(1+\rho)];$$

si pour ρ infiniment petit, L_m et par conséquent L_{p-1-m} devenait nul, on devrait donc avoir $\psi(1)=0$ et $\chi(1)=0$, et alors d'après les equations (6) il viendrait

$$\log L_m L_{p-1-m} = \log\varepsilon^2[\psi'^2(1+\delta\varepsilon)+\psi'^2(1+\varepsilon\varepsilon)] = -2\log\frac{1}{\varepsilon} + \log[\psi'^2(1+\delta\varepsilon)+\chi'^2(1+\varepsilon\varepsilon)]$$

Si l'on ajoute le terme $-2\log\frac{1}{\varepsilon}$, au premier terme de $\log L_{(0)}$, on a $-\log\left(\frac{1}{\varepsilon}\right)$, qui devient $-\infty$ pour ρ infiniment petit, et il est evident que cette valeur négative infinie ne sera pas détruite par l'expression $\log[\psi'^2(1+\delta\rho)+\chi'^2(1+\varepsilon\rho)]$; car cette expression reste finie, ou bien devient elle-même $-\infty$ si l'on a simultanément $\psi'^2(1)=0$ et $\chi'^2(1)=0$. Il est tout aussi clair, qu'en considérant comme devenant nuls d'autres couples que L_m et L_{p-1-m}, la contradiction n'en sera que plus forte. Il est donc démontré que la li-

mite de L_m est finie et différente de zéro pour $m > 0$, et que dans le cas où $m = 0$, cette limite devient infinie; ainsi la suite

$$\sum \omega^{\gamma} \frac{1}{q^{1+\rho}} + \frac{1}{2} \sum \omega^{2\gamma} \frac{1}{q^{2+2\rho}} + \frac{1}{3} \sum \omega^{3\gamma} \frac{1}{q^{3+3\rho}} + \ldots = \log L \quad (7)$$

s'approche toujours, lorsque ω n'est pas $= 1$, d'une limite finie, et devient infinie pour $\omega = 1$ et ρ infiniment petit.

Si l'on voulait avoir cette limite, dont la connaissance d'ailleurs n'est pas nécessaire pour notre but, sa détermination au moyen de l'expression $\log [\psi(1) + \chi(1)\sqrt{-1}]$, serait sujette à une ambiguité qu'on peut faire facilement disparaître dans chaque cas particulier, c'est-à-dire lorsque p et ω sont donnés numériquement: soit

$$\log L = u + v\sqrt{-1} = \log [\psi(1+\rho) + \sqrt{-1}\,\chi(1+\rho)],$$

on en tire

$$u = \frac{1}{2} \log [\psi^2(1+\rho) + \chi^2(1+\rho)],$$

$$\cos v = \frac{\psi(1+\varepsilon)}{\sqrt{\psi^2(1+\varepsilon) + \chi^2(1+\varepsilon)}}, \quad \sin v = \frac{\chi(1+\varepsilon)}{\sqrt{\psi^2(1+\varepsilon) + \chi^2(1+\varepsilon)}},$$

et par conséquent la limite de u est sans aucune ambiguité

$$= \frac{1}{2} \log [\psi^2(1) + \chi^2(1)]:$$

pour avoir celle de v, il faut remarquer que la suite (7), quelle que soit la petitesse de ρ, varie d'une manière continue avec cette grandeur, ce qui est facile à démontrer; donc v est aussi une fonction continue de ρ. Comme $\psi(1)$ et $\chi(1)$ ne peuvent s'anéantir simultanément, on pourra au moyen des expressions de $\psi(1+\rho)$ et $\chi(1+\rho)$, données ci-dessus sous forme d'intégrales définies, déduire une valeur finie positive R, telle que pour toutes les valeurs de ρ plus petites que R l'une au moins des deux fonctions ne change pas de signe. Dès que ρ sera devenu plus petit que R, $\cos v$ ou $\sin v$ ne changera plus de signe, et par conséquent l'arc variable v ne pourra plus croître ou décroître que d'une quantité $< \pi$. La série (7) pour toute valeur finie de ρ appartient à la première espèce, dont il a été question au paragraphe 1er; sa

somme a donc toujours une valeur déterminée. Si l'on calcule numériquement au moyen de cette série la valeur de v qui correspond à $\rho = R$, et qu'on désigne cette valeur par V, la limite v_0 de v sera complétement déterminée au moyen des deux équations

$$\cos v_0 = \frac{\psi(1)}{\sqrt{\psi^2(1)+\chi^2(1)}}, \quad \sin v_0 = \frac{\chi(1)}{\sqrt{\psi^2(1)+\chi^2(1)}},$$

en se rappelant qu'on doit avoir $V - v_0 < \pi$, abstraction faite du signe.

§ VI.

Nous sommes maintenant en état de démontrer que toute progression arithmétique dont la raison est le nombre premier p, et dont le premier terme est un entier non divisible par p, renferme une infinité de nombres premiers, ou en d'autres termes, qu'il existe une infinité de nombres premiers de la forme $\mu p + m$, où μ est un nombre entier indéterminé, et m l'un des nombres de la suite $1, 2, 3, \ldots p-1$. En effet, l'équation (7) représente $p-1$ équations, correspondant aux racines $1, \Omega, \Omega^2, \Omega^3, \ldots \Omega^{p-2}$; si l'on multiplie la première de ces équations par 1, la seconde par $\Omega^{-\gamma_m}$, la troisième par $\Omega^{-2\gamma_m}\ldots$, la dernière par $\Omega^{-(p-2)\gamma_m}$, et qu'on ajoute ensuite leurs premiers membres, il vient

$$\begin{aligned}
&\sum\left[1+\Omega^{\gamma-\gamma_m}+\Omega^{2(\gamma-\gamma_m)}+\ldots+\Omega^{(p-2)(\gamma-\gamma_m)}\right]\frac{1}{q^{1+\rho}}\\
&+\frac{1}{2}\sum\left[1+\Omega^{2\gamma-\gamma_m}+\Omega^{2(2\gamma-\gamma_m)}+\ldots+\Omega^{(p-2)(2\gamma-\gamma_m)}\right]\frac{1}{q^{2+2\rho}}\\
&+\frac{1}{3}\sum\left[1+\Omega^{3\gamma-\gamma_m}+\Omega^{2(3\gamma-\gamma_m)}+\ldots+\Omega^{(p-2)(3\gamma-\gamma_m)}\right]\frac{1}{q^{3+3\rho}}\\
&+\ldots,
\end{aligned}$$

où les sommations sont relatives à q, γ étant l'indice de q.

Mais chacune des sommes entre parenthèses est nulle, excepté lorsqu'on a $h\gamma - \gamma_m \equiv 0 \pmod{p-1}$; alors la somme est égale à $p-1$:

cette congruence équivaut à celle-ci $q^k \equiv m \pmod{p}$; on a donc l'équation

$$\sum \frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \frac{1}{q^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{q^{3+3\rho}} + \ldots$$

$$= \frac{1}{p-1}\left[\log L_0 + \Omega^{-\gamma_m}\log L_1 + \Omega^{-2\gamma_m}\log L_2 + \ldots \Omega^{-(p-2)\gamma_m}\log L_{p-2}\right],$$

où la première sommation est relative à tous les nombres premiers q de la forme $\mu p + m$; la seconde sommation est relative aux nombres premiers dont le carré est de cette forme; la troisième aux nombres premiers dont le cube est de cette forme, et ainsi de suite. Lorsque ρ s'approche d'être nul, le second membre, à raison de $L_{(0)}$ qu'il contient, devient infiniment grand; donc le premier doit aussi devenir infiniment grand. Or on sait que la somme

$$\frac{1}{2}\sum \frac{1}{q^2} + \frac{1}{3}\sum \frac{1}{q^3} + \ldots$$

reste une quantité finie, lors même qu'on prend pour q tous les nombres entiers qui sont > 1; *à fortiori* restera-t-elle finie lorsqu'on ne prend pour q que les nombres premiers; conséquemment c'est la suite $\sum \frac{1}{q^{1+\rho}}$ qui doit dépasser une quantité positive quelconque; elle doit donc renfermer une infinité de termes, c'est-à-dire qu'il y a une infinité de nombres premiers de la forme $\mu p + m$. C. Q. F. D.

§ VII.

Pour étendre la démonstration précédente à une progression arithmétique où la raison n'est pas un nombre premier, il est nécessaire d'avoir recours à quelques propositions fondées sur la théorie des restes; nous réunissons ici ces propositions succinctement, afin de pouvoir plus facilement en faire usage: on en trouvera la démonstration dans la troisième section de l'ouvrage de M. Gauss (*Disq. arith.*) où ce sujet est traité à fond.

I. L'existence des racines primitives n'est pas bornée aux nombres premiers impairs, mais ces racines ont aussi lieu pour la puissance p^π

de ces nombres. Ainsi, c étant une racine primitive pour le module p^π, les restes des puissances

$$c^0,\ c^1,\ c^2,\ \ldots\ c^{(p-1)p^{\pi-1}-1},$$

pris d'après ce module, sont tous différents entre eux, et coïncident avec les nombres $< p^\pi$ et premiers à p^π. Si l'on a un nombre n, non divisible par p, alors l'exposant $\gamma_n < (p-1)p^{\pi-1}$, qui correspond à la congruence

$$c^{\gamma_n} \equiv n \pmod{p^\pi},$$

sera complétement déterminé, et nous le nommerons l'*indice* de n. On démontre encore ici facilement que l'indice d'un produit est égal au reste de la division de la somme des indices des facteurs par $(p-1)p^{\pi-1}$ et que γ_n est pair ou impair selon qu'on a $\left(\frac{n}{p}\right)$ égal à $+1$ ou à -1.

II. Dans la théorie des racines primitives, le nombre premier 2 se comporte tout autrement que les nombres premiers impairs; ce nombre premier 2 donne lieu aux observations suivantes, en faisant abstraction de la première puissance de 2, qu'il n'est pas nécessaire de considérer ici.

(1). Au module 2^2 correspond la racine primitive -1. Soit n un nombre impair quelconque et α_n son indice, de sorte que l'on ait $(-1)^{\alpha_n} \equiv n \pmod 4$; selon que n sera de la forme $4\mu+1$ ou $4\mu+3$, α_n sera $=0$ ou $=1$; l'on obtient l'indice d'un produit, en prenant le reste de la division par 2 de la somme des indices des facteurs.

(2). Si le module est de la forme 2^λ où $\lambda \geqq 3$, il n'existe plus de racine primitive, c'est-à-dire il n'existe pas de nombre, dont la période des restes, d'après le diviseur 2^λ, donne tous les nombres impairs $< 2^\lambda$; mais on peut représenter ainsi la moitié de ces nombres: en effet, soit un nombre de la forme $8\mu+5$ ou simplement 5; si l'on divise par 2^λ la suite des puissances

$$5^0,\ 5^1,\ 5^2,\ \ldots\ 5^{2^{\lambda-2}-1},$$

on aura $2^{\lambda-2}$ restes différents, tous de la forme $4\mu+1$ et $<2^\lambda$. Ainsi si n est de la forme $4\mu+1$, on peut toujours satisfaire à la congruence

$$5^{\beta_n} \equiv n \pmod 2,$$

l'indice β_n devant être $<2^{\lambda-2}$; mais si n est de la forme $4\mu+3$, la congruence est impossible; dans cette dernière supposition $-n$ étant de la forme $4\mu+1$, on a donc la double congruence

$$5^{\beta_n} \equiv \pm n \pmod{2^\lambda}:$$

nous appellerons d'une manière générale l'indice du nombre impair n, l'exposant $\beta_n<2^{\lambda-2}$, qui satisfait à cette double congruence. D'après ce double signe, le reste de n divisé par 2^λ, n'est pas complétement déterminé par l'indice β_n auquel correspondent deux restes complémentaires, relativement à 2^λ. Il est évident que les propositions ci-dessus citées sont également applicables aux indices ainsi définis, savoir, que l'indice d'un produit est égal au reste qu'on obtient en divisant la somme des indices des facteurs par $2^{\lambda-2}$, et que β_n est pair ou impair selon que n est de la forme $8m\pm1$ ou $8m\pm5$. Pour faire disparaître l'ambiguité, il suffit de considérer à la fois les deux congruences $(-1)^{\alpha_n} \equiv n \pmod 4$ et $5^{\beta_n} \equiv \pm n \pmod{2^\lambda}$; si $\alpha_n=0$, on prend le signe supérieur, et si $\alpha_n=1$, on prend le signe inférieur; on peut réunir les deux indices en cette unique congruence

$$(-1)^{\alpha_n}.5^{\beta_n} \equiv n \pmod{2^\lambda},$$

qui détermine complétement le reste de la division de n par 2^λ.

III. Soit $k=2^\lambda.p^\pi.p'^{\pi'}\ldots$ et $\lambda \overset{=}{>} 3$; $p, p', \ldots$ sont des nombres premiers impairs; soit n un nombre premier avec $2, p, p', \ldots$: si nous représentons par $\alpha_n, \beta_n, \gamma_n, \gamma'_n, \ldots$ les indices correspondants respectivement aux racines primitives $-1, 5, c, c', \ldots$

et aux modules 4, 2^λ, p^π, $p'^{\pi'}$, ... on aura les congruences

$$(-1)^{\alpha_n} \equiv n \pmod 4,\quad 5^{\beta_n} \equiv \pm n \pmod{2^\lambda},\quad c^{\gamma_n} \equiv n \pmod{p^\pi},$$
$$c^{\gamma'_n} \equiv n \pmod{p'^{\pi'}},\ldots$$

D'après des théorèmes connus, l'ensemble de ces congruences suffit pour déterminer le reste de la division de n par k, en observant que le signe de la seconde congruence est fixé par la première.

Nous appellerons les indices α_n, β_n, γ_n, γ'_n, ... ou simplement les indices α, β, γ, γ', ... le *système des indices*, relativement au nombre n. Or α est susceptible de deux valeurs, β de $2^{\lambda-2}$ valeurs, γ de $(p-1)p^{\pi-1}$ valeurs, etc.; ainsi le nombre total des systèmes d'indices est

$$2.2^{\lambda-2}.(p-1)p^{\pi-1}.(p'-1)p'^{\pi'-1}\ldots = k\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\ldots = K, \quad (8)$$

ce qui coïncide avec le théorème connu où K exprime combien il existe de nombres entiers plus petits que k et premiers à k.

§ VIII.

Venant maintenant à notre démonstration générale du théorème sur les progressions arithmétiques, nous ferons observer qu'on ne restreint pas cette généralité en admettant que la raison k de la progression est divisible par 8, et qu'elle est par conséquent comprise dans la forme de k du paragraphe précédent; car il est évident que si le théorème existe dans cette supposition, à plus forte raison existera-t-il lorsque k est impair ou divisible seulement par 2 ou 4.

Soit donc θ, φ, ω, ω', ... une racine quelconque des équations

$$\theta^2-1=0;\quad \varphi^{2^{\lambda-2}}-1=0,\quad \omega^{(p-1)p^{\pi-1}}-1=0,\quad \omega'^{(p'-1)p'^{\pi'-1}}-1=0,\ldots \quad (9)$$

et q un nombre premier différent de 2, p, p', ...; formons l'équation

$$\frac{1}{1-\theta^\alpha\varphi^\beta\omega^\gamma\omega'^{\gamma'}\ldots\frac{1}{q^i}} = 1+\theta^\alpha\varphi^\beta\omega^\gamma\omega'^{\gamma'}\ldots\frac{1}{q^i}+\theta^{2\alpha}\varphi^{2\beta}\omega^{2\gamma}\omega'^{2\gamma'}\ldots\frac{1}{q^{2i}}+\ldots,$$

dans laquelle $s > 1$, et où le système des indices est relatif à q; si l'on met pour q toutes les valeurs dont il est susceptible, et si l'on multiplie ensemble toutes les équations résultantes, en ayant égard aux propriétés des indices énoncées ci-dessus, et aux équations (9), on aura

$$\Pi \cdot \frac{1}{1 - \theta^{\alpha} \varphi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \frac{1}{q^s}} = \Sigma \theta^{\alpha} \varphi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots \frac{1}{n^s} = \mathrm{L}; \qquad (10)$$

le signe de multiplication Π s'étend à tous les nombres premiers autres que 2, p, p',... et le signe sommatoire à tous les nombres entiers positifs, non divisibles par 2, p, p'.....; dans le premier membre le système des indices α, β, γ,... se rapporte au nombre q et dans le second membre au nombre n. L'équation générale (10), où les diverses racines θ, φ, ω, ω',... peuvent être combinées entre elles d'une manière quelconque, contient évidemment K équations particulières. Afin de pouvoir désigner commodément les diverses suites L, correspondant à ces combinaisons, il faut concevoir les racines des équations (9), comme étant les puissances de l'une d'entre elles Θ, Φ, Ω, Ω',..... où $\Theta = -1$; on aura ainsi

$$\theta = \Theta^{a}, \quad \varphi = \Phi^{b}, \quad \omega = \Omega^{c}, \quad \omega' = \Omega^{c'}, \ldots$$

où

$$a < 2, \quad b < (p-1)p^{\pi-1}, \quad c < (p'-1)p'^{\pi'-1}, \ldots$$

et la suite L correspondant à ces valeurs sera désignée par

$$\mathrm{L}_{a, b, c, c', \ldots} \qquad (11)$$

La nécessité de la restriction $s > 1$ dans l'équation (10) repose sur les raisons déjà développées dans le premier paragraphe.

§ IX.

On peut diviser en trois *classes* les suites L, au nombre de K, produites par les combinaisons des racines $\theta, \varphi, \omega, \omega' \ldots$: la *première* classe ne contient qu'une série, savoir $L_{0,\,0,\,0,\,0,\ldots}$ pour laquelle on a

$$\theta = 1, \quad \varphi = 1, \quad \omega = 1, \quad \omega' = 1 \ldots.$$

La *seconde* classe contient toutes les suites où il ne se présente que des racines *réelles* des équations (3), de sorte qu'on a

$$\theta = \pm 1, \quad \varphi = \pm 1, \quad \omega = \pm 1, \quad \omega' = \pm 1 \ldots;$$

on combinera ces racines de toutes les manières possibles, en exceptant seulement la combinaison qui constitue la première classe. Enfin la *troisième* classe renferme toutes les suites où l'une au moins des racines $\varphi, \omega, \omega', \ldots$ est imaginaire. Il est évident que les suites de cette classe sont conjuguées par couples; car les combinaisons des racines

$$\theta, \varphi, \omega, \omega' \ldots, \quad \text{et} \quad \frac{1}{\theta}, \frac{1}{\varphi}, \frac{1}{\omega}, \frac{1}{\omega'}, \ldots$$

donnent des résultats différents, dans l'hypothèse qu'au moins une racine est imaginaire.

Nous avons maintenant à chercher ce que deviennent ces séries, lorsqu'on y fait $s = 1 + \rho$ et que la quantité positive ρ devient infiniment petite. Occupons-nous d'abord de la première classe : il est évident que cette série peut être considérée comme composée de K séries partielles dont chacune a la forme

$$\frac{1}{m^{1+\rho}} + \frac{1}{(k+m)^{1+\rho}} + \frac{1}{(2k+m)^{1+\rho}} + \ldots,$$

où m est $< k$ et premier à k; par conséquent d'après le paragraphe II, cette série a pour expression

$$\frac{K}{k}\frac{1}{\rho} + \varphi(\rho), \qquad (12)$$

$\varphi(\rho)$ conservant une valeur finie, pour ρ infiniment petit.

En concevant les séries de la seconde et troisième classe ordonnées suivant l'ordre ascendant de n, et se rappelant que $s > 0$, on obtient pour elles l'équation

$$\sum \theta^{\alpha} \varphi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots \frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^1 \frac{\Sigma \theta^{\alpha} \varphi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots x^{n-1}}{1-x^k} \log^{s-1}\left(\frac{1}{x}\right) dx : \quad (13)$$

le signe Σ du second membre s'étend à toutes les valeurs positives de n plus petites que k et premières à k; α, β, γ, γ', ... est un système d'indice relatif à n; on démontre facilement que le second membre a une valeur finie. En effet, le polynome $\Sigma\theta\, \varphi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots . x^{n-1}$ renferme le facteur $1-x$; car, en faisant $x = 1$, ce polynome se change dans le produit

$$(1+\theta)\left[1+\varphi+\ldots+\varphi^{2^{\lambda-2}-1}\right]\left[1+\omega+\ldots+\omega^{(p-1)p^{\pi-1}-1}\right]\left[1+\omega'+\ldots\omega'^{(p-1)p'^{\pi'-1}-1}\right]\ldots$$

dont un au moins des facteurs s'anéantit, puisque la combinaison

$$\theta = 1, \quad \varphi = 1, \quad \omega = 1, \quad \omega' = 1, \ldots$$

est exclue, comme appartenant à la première classe.

On se convaincra, d'une manière aussi facile, que le second membre de l'équation (13), et son coefficient différentiel pris par rapport à s, sont des fonctions continues de s; de là on conclut que chaque série de la deuxième et troisième classe, pour des valeurs de ρ infiniment petites, a une limite finie, exprimée par

$$\sum \theta^{\alpha} \varphi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots \frac{1}{n} = \int_0^1 \frac{\Sigma \theta^{\alpha} \varphi^{\beta} \omega^{\gamma} \omega'^{\gamma'} \ldots x^{n-1}}{1-x^k} dx; \quad (14)$$

il reste à démontrer que cette limite n'est jamais nulle.

§ X.

La limite de L pour la deuxième et troisième classe peut bien s'exprimer facilement, par la méthode du paragraphe 4, en fonctions logarithmiques et circulaires; mais cette expression n'est d'au-

cune utilité pour notre but, même pour le cas de la seconde classe, quoique ce cas ait une grande analogie avec celui qu'on a traité dans la seconde moitié du quatrième paragraphe. Regardons la propriété dont nous nous occupons comme démontrée pour les séries de la seconde classe (c'est-à-dire admettons que les limites de ces séries ne sont pas nulles), et nous allons faire voir qu'elle existe aussi dans la troisième classe : à cet effet développons les logarithmes des deux membres de l'équation (10); nous obtiendrons

$$\Sigma\theta^{\alpha}\varphi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\ldots\frac{1}{q^{1+\rho}}+\frac{1}{2}\Sigma\theta^{2\alpha}\varphi^{2\beta}\omega^{2\gamma}\omega'^{2\gamma'}\ldots\frac{1}{q^{2+2\rho}}+\ldots=\log L:$$

les indices $\alpha, \beta, \gamma, \gamma', \ldots$ et le signe Σ se rapportent à q. Si l'on représente les racines $\theta, \varphi, \omega, \omega', \ldots$ comme il a été dit à la fin du paragraphe 8, le terme général du premier membre devient

$$\frac{1}{h}\Sigma\Theta^{h\alpha a}\Phi^{h\beta b}\Omega^{h\gamma c}\Omega'^{h\gamma' c'}\ldots\frac{1}{q^{h+h\rho}},$$

tandis que, d'après la formule (11), le second membre devient

$$\log L_{a,b,c,c',\ldots}$$

Soit maintenant m un nombre entier $<k$ et n'ayant aucun facteur commun avec k. Si l'on multiple les deux membres par

$$\Theta^{-\alpha_m a}\Phi^{-\beta_m b}\Omega^{-\gamma_m c}\Omega'^{-\gamma'_m c'}\ldots;$$

et si, pour abréger, on écrit seulement le terme général du premier membre, il vient

$$\ldots\frac{1}{h}\Sigma\Theta^{(h\alpha-\alpha_m)a}\Phi^{(h\beta-\beta_m)b}\Omega^{(h\gamma-\gamma_m)c}\Omega'^{(h\gamma'-\gamma'_m)c'}\ldots\frac{1}{q^{h+h\rho}}+\ldots$$
$$=\Theta^{-\alpha_m a}\Phi^{-\beta_m b}\Omega^{-\gamma_m c}\Omega'^{-\gamma_m c'}\ldots\log L_{a,b,c,c',\ldots},$$

si l'on somme, pour embrasser toutes les combinaisons des racines, depuis $a=0$, $b=0$, $c=0$, $c'=0,\ldots$ jusqu'à $a=1,\ldots$, $b=2^{\lambda-2}-1$, $c=(p-1)p^{\pi-1}-1$, $c'=(p'-1)p'^{\pi'-1}-1\ldots$,

alors on a pour le terme général du premier membre

$$\frac{1}{h}\Sigma W\frac{1}{q^{h+h\rho}};$$

le signe Σ est relatif à q, W est le produit des sommes,

$$\Sigma\Theta^{(h\alpha-\alpha_m)a},\quad \Sigma\Phi^{(h\beta-\beta_m)b},\quad \Sigma\Omega^{(h\gamma-\gamma_m)c},\quad \Sigma\Omega^{(h\gamma'-\gamma'_m)c'},\ldots$$

les sommes étant prises par rapport aux racines a, b, c, c',... et entre les limites ci-dessus énoncées. Maintenant, en se rappelant les propositions du paragraphe 7, il est facile de voir : 1° que la première somme est 2 ou zéro, selon qu'on a ou qu'on n'a pas la congruence $h\alpha-\alpha_m\equiv 0\,(\text{mod. }2)$, ou, ce qui revient au même, selon qu'on a ou qu'on n'a pas la congruence $q^h\equiv m\,(\text{mod. }4)$; 2° que la seconde somme se réduit à $2^{\lambda-2}$ ou à 0, selon qu'on a ou qu'on n'a pas la congruence $h\beta-\beta_m\equiv 0\,(\text{mod. }2^{\lambda-2})$, ou bien selon qu'on a ou non la congruence $q^h\equiv\pm m\,(\text{mod. }2^\lambda)$, 3° que la troisième somme se réduit à $(p-1)p^{\pi-1}$ ou à 0, selon que la congruence $h\gamma-\gamma_m\equiv 0$ $[\text{mod. }(p-1)p^{\pi-1}]$ a lieu ou non, ou ce qui revient au même, selon que la congruence $q^h\equiv m\,(\text{mod. }p^\pi)$ a lieu ou non; et ainsi de suite. Il s'ensuit que W est toujours nulle, excepté lorsqu'on a simultanément les congruences $q^h\equiv m$, pour les modules $2^\lambda, p^\pi, p'^{\pi'};\ldots$ ou ce qui revient au même, lorsqu'on a la congruence $q^h\equiv m\,(\text{mod. }k)$, et dans ce cas $W=K$; ainsi notre équation devient

$$\left.\begin{aligned}&\Sigma\frac{1}{q^{1+\rho}}+\frac{1}{2}\Sigma\frac{1}{q^{2+2\rho}}+\frac{1}{3}\Sigma\frac{1}{q^{3+3\rho}}+\ldots\\&\qquad=\frac{1}{K}\Sigma\Theta^{-\alpha_m a}\Phi^{-\beta_m b}\Omega^{-\gamma_m c}\Omega'^{-\gamma'_m c'}\ldots\log L_{a,b,c,c',\ldots}\end{aligned}\right\}(15)$$

où les sommations dans le premier membre sont relatives à tous les nombres premiers dont la première, ou la seconde, ou la troisième puissance, etc., est de la forme $\mu k+m$, tandis que la sommation dans le second membre se rapporte aux racines a, b, c, c',... prises entre les limites indiquées. Si l'on fait spécialement $m=1$, alors

$\alpha_m = 0$, $\beta_m = 0$, $\gamma_m = 0$, $\gamma'_m = 0$;... et le second membre se réduit à

$$\frac{1}{K} \Sigma \log . L_{a, b, c, c', \ldots}$$

Le terme de cette somme qui correspond à la série L de la première classe ou à $L_{0, 0, 0, 0, \ldots}$ contiendra (d'après la formule 12) $\log \frac{1}{\rho}$. D'après l'hypothèse ci-dessus énoncée, les termes qui répondent aux diverses séries L de la seconde classe restent finis pour des valeurs de ρ infiniment petites. Maintenant, si la valeur de la limite pour une série L de la troisième classe pouvait devenir nulle, alors, en raisonnant comme dans le paragraphe V, l'expression (13) donnerait pour le logarithme de cette série L, combinée avec l'autre série L qui lui est conjuguée, le terme $-2 \log \left(\frac{1}{\rho}\right)$, lequel s'ajouterait à $\log \left(\frac{1}{\rho}\right)$, fourni par $L_{0, 0, 0, 0, \ldots}$; il resterait ainsi $-\log \left(\frac{1}{\rho}\right)$ qui devient infini négatif, pour ρ infiniment petit, tandis que le premier membre de l'équation (15), ne contient que des termes positifs; ainsi aucune série L de la troisième classe ne peut avoir zéro pour valeur de sa limite, et nous sommes en possession de ce résultat (sous la réserve d'une démonstration à donner pour les séries de la deuxième classe), que

$$\log L_{a, b, c, c', \ldots}$$

pour une valeur de ρ infiniment petite, conserve toujours une limite finie, excepté, lorsqu'on a simultanément $a = 0$, $b = 0$, $c = 0$, $c' = 0, \ldots$ dans lequel cas, ce logarithme acquiert une valeur infiniment grande. Si l'on applique ce résultat à l'équation générale (15), on voit de suite que le second membre devient infini pour ρ infiniment petit, et cela par le terme $\frac{1}{K} \log L_{0, 0, 0, 0, \ldots}$ qui croît au-delà de toute limite, tandis que les autres termes restent finis. Il faut donc aussi que le premier membre dépasse toute grandeur finie; d'où il suit, comme au paragraphe VI, que la série

$\sum \frac{1}{q^{1+t}}$ contient un nombre infini de termes, ou ce qui revient au même, qu'il existe un nombre infini de nombres premiers de la forme $k\mu + m$, où μ est un nombre entier indéterminé, et m est un nombre n'ayant aucun facteur commun avec k. C. Q. F. D.

§ XI.

Pour compléter cette démonstration, il reste à montrer d'après la valeur de la limite des séries L de la seconde classe donnée par l'équation (14), que pour une combinaison des racines de la forme ± 1, ± 1, ± 1, ± 1,... en n'exceptant que la forme $+1$, $+1$, $+1$, $+1$,..., que pour une telle combinaison, dis-je, la somme

$$\Sigma(\pm 1)^{\alpha}(\pm 1)^{\beta}(\pm 1)^{\gamma}(\pm 1)^{\gamma'} \ldots \frac{1}{n}, \qquad (16)$$

a toujours une valeur différente de zéro, α, β, γ, γ',... étant un système d'indices relatif à n pour lequel il faut prendre, suivant leur ordre de grandeur, tous les nombres entiers positifs et non divisibles par les nombres premiers $2, p, p' \ldots$. Dans le Mémoire que j'ai eu l'honneur de soumettre en premier lieu à l'Académie, j'avais démontré cette propriété par des considérations indirectes, et assez compliquées. Depuis, je me suis assuré qu'on peut arriver au même but par un chemin plus court.

Les principes dont j'ai fait usage s'appliquent en effet à d'autres problèmes dont on ne soupçonnerait pas d'abord la connexion avec celui qui est l'objet de ce Mémoire. On résout nommément à l'aide de ces principes cette question intéressante : trouver le nombre de formes quadratiques qui répondent à un *déterminant* donné soit positif, soit négatif; et l'on prouve que ce nombre (ce qui toutefois n'est pas la forme finale de cette recherche) peut être représenté par le produit de deux facteurs, dont l'un est une fonction très simple du déterminant et conserve une valeur finie pour chaque déterminant, et dont l'autre est une suite qui coïncide avec la suite (16) donnée ci-dessus. Il suit immédiatement de ce résultat, que la somme (16) ne peut jamais devenir nulle; car, si cela pouvait avoir

lieu, le nombre des formes quadratiques relatives au déterminant correspondant serait aussi zéro, ce qui est impossible, puisque ce nombre est toujours $\geqq 1$.

Par ce motif j'ai supprimé ici ma première démonstration relative à la propriété énoncée de la suite (16); et je renvoie pour cet objet à mes recherches sur les formes quadratiques, qui paraîtront incessamment (*), et d'où découle, comme un simple corollaire, la proposition nécessaire pour compléter le présent Mémoire.

(*) Ces recherches ont paru dans le Journal de M. Crelle, tome XIX : voir aussi, dans le même Journal (tome XVIII, une notice préliminaire sur le même objet, écrite en français, sous ce titre : *sur l'usage des séries infinies dans la théorie des nombres* (J. L.)