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

LEJEUNE-DIRICHLET

Recherches sur la théorie des nombres complexes

Journal de mathématiques pures et appliquées 1re série, tome 9 (1844), p. 245-269.
<http://www.numdam.org/item?id=JMPA_1844_1_9__245_0>

RECHERCHES

SUR LA THÉORIE DES NOMBRES COMPLEXES;

PAR M. LEJEUNE-DIRICHLET.

(Lu à l'Académie des Sciences de Berlin le 27 mai 1841.)

(Extrait des Mémoires de l'Académie de Berlin. — Traduction de M. FAYE.)

Ce Mémoire n'est qu'une partie d'un travail considérable dans lequel je me propose d'étendre aux nombres complexes la plupart des solutions que j'ai déjà trouvées pour des questions relatives à la théorie des nombres entiers réels, en continuant à employer la méthode qui m'a servi dans les occasions que je viens de rappeler. J'ai été déterminé à donner cette extension à mon premier travail non-seulement à cause des nouveaux résultats qu'on en peut attendre, mais aussi, plutôt même, par le désir de soumettre ainsi à une épreuve mes nouvelles méthodes et d'examiner si leur succès doit être attribué à leur harmonie réelle avec la véritable nature des questions résolues, ou bien à ces circonstances favorables qui se présentent parfois dans les recherches mathématiques. C'est une épreuve que notre méthode a très-bien supportée; car pour l'adapter aux questions analogues de la théorie des nombres complexes, il a suffi de quelques modifications qui se déduisaient d'ailleurs naturellement du changement dans l'essence du sujet auquel elle était appliquée.

La majeure partie des nouvelles recherches dont je viens d'indiquer l'origine a pour objet la doctrine des formes quadratiques et paraîtra bientôt ailleurs. Je m'occuperai exclusivement, dans le présent Mémoire, de démontrer le théorème dont voici l'énoncé : « L'expression $kt + l$, » dans laquelle t désigne un nombre entier complexe indéterminé, et » où k, l représentent de semblables nombres donnés sans facteurs

» communs, contient toujours une infinité de nombres premiers. » Cette démonstration ressort, comme celle de la loi analogue pour les nombres réels, du théorème fondamental sur certaines propriétés de la forme quadratique des nombres complexes; aussi me bornerai-je, pour éviter les répétitions inutiles, à renvoyer le lecteur aux recherches déjà mentionnées [*].

§ I^er.

Nous avons déjà supposé que le lecteur connaît les propriétés élémentaires des nombres complexes; cependant il sera utile d'exposer ici brièvement quelques-unes de ces propriétés qui sont d'une importance particulière pour l'intelligence de ce qui va suivre.

Nous poserons, comme à l'ordinaire, $\sqrt{-1} = i$, et nous appellerons nombre entier complexe toute expression telle que $f + gi$, dans laquelle f et g représentent des nombres réels entiers. Le nombre positif $f^2 + g^2$, qui répond au nombre complexe $f + gi$, sera nommé la norme de celui-ci et sera désigné par $\mathrm{N}(f + gi)$. Quatre nombres complexes tels que

$$f + gi, \quad -g + fi, \quad -f - gi, \quad g - fi,$$

qui dépendent les uns des autres, de telle sorte que trois quelconques d'entre eux se déduisent du quatrième en le multipliant par -1, $\pm i$, seront nommés corrélatifs.

On peut toujours former, relativement à un module complexe donné m, une série de nombres qui possède cette double propriété: qu'il se trouve toujours parmi ses termes un nombre congru à un nombre

[*] Depuis que le présent Mémoire a été soumis à l'Académie, ces recherches ont été publiées dans le XXIV^e volume du Journal de M. Crelle, sous le titre de : « Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. » Ce Mémoire contient, outre l'objet indiqué par son titre, une brève exposition des éléments de la théorie des nombres complexes que j'ai limitée aux propositions nécessaires à l'intelligence de ce Traité. On trouvera une exposition plus complète de ces éléments dans le second Mémoire de M. Gauss sur les résidus biquadratiques; c'est dans cet ouvrage que ce grand géomètre a introduit pour la première fois dans la science la notion des nombres complexes; j'y renvoie le lecteur.

quelconque pour le module m, mais qu'il ne s'en trouve qu'un seul. Le nombre des termes ainsi incongrus entre eux est $\mathrm{N}(m)$.

On peut déterminer en général le nombre des termes d'un pareil système qui n'ont point de facteur commun avec m. Soit

$$m = i^{\mu} a^{\alpha} b^{\beta} c^{\gamma} \ldots, \tag{1}$$

où a, b, c,... représentent des nombres premiers dont aucun n'est égal ni corrélatif aux autres; et soient, en outre,

$$\mathrm{N}(a) = \mathrm{A}, \quad \mathrm{N}(b) = \mathrm{B}, \quad \mathrm{N}(c) = \mathrm{C}, \ldots;$$

alors le nombre cherché sera donné par l'équation

$$\psi(m) = (\mathrm{A} - 1)\,\mathrm{A}^{\alpha-1}.(\mathrm{B} - 1)\,\mathrm{B}^{\beta-1}.(\mathrm{C} - 1)\,\mathrm{C}^{\gamma-1}\ldots.$$

Soient

$$\mu,\ \mu',\ \mu'', \ldots \tag{2}$$

les termes dont le nombre est ainsi déterminé, et soit l un nombre qui n'ait aucun facteur commun avec m; on prouve facilement que les nombres

$$l\mu,\ l\mu',\ l\mu'', \ldots,$$

quand on les considère abstraction faite de leur ordre, sont congrus d'après le module m avec les nombres (2), et on en conclut aussitôt, comme dans la démonstration connue du théorème de Fermat pour les nombres réels, que l'on a toujours

$$l^{\psi m} \equiv 1 \pmod{m}. \tag{3}$$

Dans la théorie ordinaire des nombres on est obligé de considérer les nombres positifs comme primitifs, et les nombres négatifs comme dérivés des premiers en les multipliant par le facteur -1. De même, on simplifierait certaines considérations analogues sur les nombres complexes en choisissant, d'après un principe fixe, un des quatre nombres corrélatifs comme primitif ou *primaire*, dont les autres seraient les produits par -1, $\pm i$. La nécessité d'une telle distinction est surtout sensible quand il s'agit de nombres impairs, et, pour le choix à faire, on

peut se guider sur cette remarque que le produit de deux facteurs positifs devant être aussi positif, de même le produit de deux facteurs primaires devra être également un nombre primaire. Comme on le voit facilement, dans chaque groupe de nombres impairs corrélatifs il y en a toujours un, mais un seul, pour lequel f et g ont respectivement la forme $4\mu + 1$ et 2μ, de même qu'il y en a un seul pour lequel $f - 1$ et g sont contenus tous deux soit dans la forme 4μ, soit dans la forme $4\mu + 2$, et l'on peut facilement se convaincre que la condition énoncée ci-dessus est satisfaite quel que soit celui de ces nombres que l'on choisisse comme primaire, dans tous les groupes de nombres corrélatifs. Nous avons adopté la première définition dans le Mémoire cité plus haut, mais tout ce que nous avons dit reste encore vrai quand on choisit la deuxième. Or, comme la dernière définition est beaucoup plus convenable pour notre but actuel, nous considérerons désormais, dans ce Mémoire, comme primaire celui des quatre nombres impairs corrélatifs pour lequel $f - 1$ et g ont à la fois la forme 4μ, ou bien la forme $4\mu + 2$, en remarquant, toutefois, dans le seul but de faciliter l'emploi de cette définition, qu'elle se réduit évidemment à désigner comme primaire, dans chaque groupe de nombres impairs, celui qui est congru à l'unité positive d'après le module $2 + 2i$.

Dans cette hypothèse, on a, pour chaque nombre impair primaire m,

$$m = a^{\alpha}.b^{\beta}.c^{\gamma}..., \tag{4}$$

où a, b, c,... désignent des nombres premiers primaires différents qui sont complétement déterminés par m, ainsi que leurs exposants.

§ II.

Avant de nous occuper de la question qui fait l'objet spécial de ce Mémoire, il faut que nous exposions quelques propriétés des résidus de diverses puissances pour les modules complexes.

Soient k et l deux nombres complexes sans facteur commun, et soit e le plus petit des exposants différents de zéro, pour lequel $l^e \equiv 1 \pmod{k}$; on dit alors que, pour le module k, l appartient à l'exposant e. Il est alors facile de se convaincre que

$$1,\ l,\ l^2,\ldots,\ l^{e-1},$$

sont incongrues d'après le module k; on voit aussi que si l'on prolonge la série, les mêmes résidus se reproduisent périodiquement, de telle sorte que les seules puissances qui soient congrues à l'unité sont celles dont les exposants sont des multiples de e. Puisque $l^{\psi(k)} \equiv 1 \pmod{k}$, e sera toujours un diviseur de $\psi(k)$. Dans le cas spécial où $\psi(k) = e$, les puissances

$$1,\ l,\ l^2,\ldots,\ l^{\psi(k)-1}$$

forment un système pareil à celui que nous avons considéré dans le paragraphe précédent, c'est-à-dire que ce système contient un terme, mais un seul, qui est congru d'après le module k, à un nombre arbitraire qui n'aurait aucun facteur commun avec k; et alors l est dit racine primitive de k. Si l'on connaît l'exposant e auquel l appartient, on pourra déterminer ensuite facilement l'exposant auquel appartient une puissance quelconque de l telle que l^s. On voit facilement que ce dernier exposant est $\frac{e}{\delta}$, où δ désigne le plus grand diviseur commun (positif) de s et de e.

1. Nous commencerons par le cas où le module est une puissance $(a + bi)^f$ d'un nombre premier impair à deux termes $a + bi$, de sorte que $\mathrm{N}(a + bi) = a^2 + b^2 = p$ est un nombre premier réel $4\mu + 1$. Il est facile, dans ce cas, de prouver l'existence d'une racine primitive. Si le nombre réel $\mathfrak{a}$ est une racine primitive pour le module p^f, il le sera aussi relativement au module $(a + bi)^f$. Or, dans la supposition que nous venons de faire,

$$1,\ \mathfrak{a},\ \mathfrak{a}^2,\ldots,\ \mathfrak{a}^{(p-1)p^{f-1}-1}$$

sont incongrus d'après le module p^f; ils auront donc la même propriété pour le module $(a + bi)^f$, et, d'un autre côté, on a

$$\psi[(a + bi)^f] = (p - 1)p^{f-1}.$$

Lorsqu'on a choisi une telle racine primitive $\mathfrak{a}$, alors l'exposant $\alpha_n < (p - 1)p^{f-1}$, pour lequel

$$\mathfrak{a}^{\alpha_n} \equiv n \,[\mathrm{mod.}\ (a + bi)^f],$$

se nommera l'indice du nombre arbitraire n non divisible par $a+bi$. Il suit immédiatement de cette définition, qu'on obtient l'indice d'un produit quand on retranche de la somme des indices des facteurs le plus grand multiple de $(p-1)p^{f-1}$ qui y soit contenu.

Le nombre a est toujours non-résidu quadratique de $a+bi$, puisque autrement chaque n devrait être résidu quadratique de $a+bi$. Il suit de là que α_n sera pair ou impair suivant que n sera résidu ou non-résidu quadratique de $a+bi$. On a ainsi, en employant le symbole introduit dans le Mémoire cité,

$$\left[\frac{n}{a+bi}\right] = (-1)^{\alpha_n}. \tag{5}$$

2. Le cas que nous allons maintenant traiter est celui d'un module de la forme r^g, où r désigne un nombre premier à un seul terme. Comme nous pouvons supposer que r est réel et positif, r est alors un nombre premier de la forme $4\mu+3$. Cette recherche exige la congruence suivante,

$$(b+zr)^{er^{g-2}} \equiv b^{er^{g-2}} + ezb^{er^{g-2}-1} r^{g-1} \pmod{r^g},$$

qui a déjà été employée dans les *Disquisitiones Arithmeticæ*, art. **86**. On y suppose, à la vérité, que b et z sont réels; mais la même démonstration est aussi applicable au cas où b et z sont des nombres complexes. Les nombres e et $g \gtreqless 2$ qui s'y trouvent en exposants sont naturellement positifs.

Il n'y a point de racine primitive pour le module r^g, excepté quand $g=1$, car on peut aisément déduire de la congruence précédente que le plus fort exposant auquel, pour ce module, un nombre puisse appartenir, est $(r^2-1)r^{g-1}$, tandis que $\psi(r^g) = (r^2-1)r^{2g-2}$. Mais on peut montrer, de la manière suivante, qu'il y a des nombres appartenant à l'exposant $(r^2-1)r^{g-1}$. L'assertion relative au cas où $g=1$ a déjà été prouvée (*Theor. res. biq.*, auct. C.-F. GAUSS, art. **53**). Soit b un nombre appartenant pour le module r à l'exposant r^2-1, c'est-à-dire une racine primitive de r. Dans cette supposition, $(b+zr)^e - 1$ ne sera divisible par r que si e est un multiple de r^2-1. Il suit de là que l'exposant auquel $b+zr$ appartient pour le module r^g doit être divi-

sible par $r^2 - 1$. Mais comme on a, d'autre part,

$$(b + zr)^{(r^2-1)r^{g-1}} \equiv 1 \pmod{r^g},$$

ce qui résulte de la congruence rapportée ci-dessus, quand on pose

$$(b + zr)^{r^2-1} = 1 + ur,$$

on voit que l'exposant en question doit être un diviseur de $(r^2 - 1)r^{g-1}$. D'après cela, on pourra trouver un nombre $b + zr$ appartenant à l'exposant $(r^2 - 1)r^{g-1}$ si l'on peut choisir z de telle sorte que la relation

$$(b + zr)^{(r^2-1)r^{g-2}} \equiv 1 \pmod{r^g}$$

ne soit point satisfaite.

Or on a, d'après le lemme précédent,

$$-1 + (b + zr)^{(r^2-1)r^{g-2}}$$
$$\equiv -1 + b^{(r^2-1)r^{g-2}} + (r^2 - 1)zb^{(r^2-1)r^{g-2}-1}r^{g-1} \pmod{r^g}.$$

Si maintenant on considère que

$$-1 + b^{(r^2-1)r^{g-2}} = Br^{g-1},$$

où B est un nombre entier, et si l'on pose, pour abréger,

$$(r^2 - 1)b^{(r^2-1)r^{g-2}-1} = C,$$

il est évident que la condition exigée sera remplie quand on aura choisi z de telle sorte que la congruence

$$Cz + B \equiv 0 \pmod{r}$$

n'ait pas lieu, ce qui peut toujours se faire, puisque C n'est point un multiple de r.

Le résultat qui vient d'être obtenu peut être complété, et l'on peut déterminer généralement combien de nombres différents, c'est-à-dire incongrus, appartiennent à l'exposant $(r^2 - 1)r^{g-1}$, ou, en général, à un quelconque de ses diviseurs. Soit er^ν un *de ces diviseurs* où l'on suppose e facteur de $r^2 - 1$ et $\nu \leqq g - 1$; le nombre demandé sera donné par l'expression $\varphi(e)\psi(r^\nu)$, où $\varphi(e)$ désigne le nombre des termes

qui, dans la série 0, 1, 2,..., $e-1$, n'ont aucun facteur commun avec e. Mais comme il est inutile de connaître ce nombre pour le but que nous nous proposons, nous ne nous arrêterons pas plus longtemps à cette détermination. La seule chose qui nous importe ici, c'est la forme du nombre qui appartient à l'exposant $r^{\varepsilon-1}$, et elle est très-facile à déterminer. Si φ appartient à cet exposant, de telle sorte que $\varphi^{r^{\varepsilon-1}}-1$ soit divisible par r^{ε}, et par conséquent aussi par r, alors $r^{\varepsilon-1}$ sera un multiple de l'exposant auquel φ appartient pour le module r. Comme le dernier exposant doit être, d'un autre côté, un diviseur de r^2-1, il doit avoir pour valeur 1, c'est-à-dire que φ est de la forme $1+zr$, et il ne reste plus à chercher que la condition à laquelle z doit être assujetti pour que $1+zr$ appartienne effectivement à l'exposant $r^{\varepsilon-1}$ pour le module r^{ε}. Dans ce but, on remarquera que, d'après le lemme précédent, $(1+zr)^{r^{\varepsilon-1}}-1$ est évidemment divisible par r^{ε}; ainsi l'exposant auquel $1+zr$ appartient divise $r^{\varepsilon-1}$, et par conséquent ne sera pas autre chose que $r^{\varepsilon-1}$ lui-même, pourvu que z soit tel que la congruence

$$(1+zr)^{r^{\varepsilon-2}} \equiv 1 \pmod{r^{\varepsilon}}$$

n'ait pas lieu. Si l'on donne à celle-ci la forme suivante, à l'aide du lemme,

$$zr^{\varepsilon-1} \equiv 0 \pmod{r^{\varepsilon}},$$

on voit que la condition nécessaire et suffisante pour que φ appartienne à l'exposant $r^{\varepsilon-1}$ consiste en ce que φ soit contenu dans l'expression $1+zr$ et que z ne soit point un multiple de r.

Cela étant supposé, il nous sera facile de démontrer que, β étant un nombre donné appartenant à l'exposant $(r^2-1)r^{\varepsilon-1}$, on pourra toujours trouver un second nombre $\varphi = 1+zr$ appartenant à l'exposant $r^{\varepsilon-1}$, qui sera de telle nature que la congruence

$$\beta^{\beta} = \varphi^{\gamma} \pmod{r^{\varepsilon}},$$

dans laquelle β et γ désignent des termes contenus dans la série

$$0, 1, 2, \ldots, (r^2-1)r^{g-1}-1; \quad 0, 1, \ldots, r^{g-1}-1,$$

ne puisse exister qu'à la condition de $\beta = 0$, $\gamma = 0$. Nous remarquerons aussitôt que l'une de ces deux équations $\beta = 0$, $\gamma = 0$, résulte évidemment de l'autre; ainsi il nous suffira de montrer que c peut être choisi de telle manière, que la congruence soit impossible quand β et γ sont tous deux différents de zéro. En deuxième lieu, il est facile de voir que la possibilité de la congruence suppose la divisibilité de β par r^2-1. Posons donc $\beta = (r^2-1)\beta'$, et ensuite $\beta^{r^{2-1}} = 1 + kr$, où k désigne un nombre donné qui n'est pas divisible par r. Notre congruence devient

$$(1 + kr)^{\beta'} \equiv (1 + zr)^{\gamma} \pmod{r^g},$$

et il suffit maintenant de disposer de z, de façon que cette congruence n'existe plus lorsque β' et γ sont pris tous les deux dans la série $1, 2, \ldots, r^{g-1}-1$. Comme $1 + kr$ et $1 + zr$ appartiennent à l'exposant r^{g-1}, et par suite $(1+kr)^{\beta'}$ et $(1 + zr)^{\gamma}$ aux exposants $r^{g-1-\lambda}$ et $r^{g-1-\mu}$, où r^{λ} et r^{μ} désignent les plus hautes puissances de r qui entrent dans β' et γ, il est évident que notre congruence exige que l'on ait $\lambda = \mu$, et elle devient, quand on pose $\beta' = r^{\lambda}\beta''$ et $\gamma = r^{\lambda}\gamma'$,

$$(1 + kr)^{\beta'' r^{\lambda}} \equiv (1 + zr)^{\gamma' r^{\lambda}} \pmod{r^g}.$$

Comme $\lambda \leqq g-2$, et comme cette dernière congruence est supposée juste pour $\lambda < g-2$, elle subsistera encore pour $\lambda = g-2$, et ainsi il nous reste seulement à prouver que, pour une valeur convenablement choisie pour z, la congruence

$$(1 + kr)^{\beta'' r^{g-2}} \equiv (1 + zr)^{\gamma' r^{g-2}} \pmod{r^g}$$

ne saurait avoir lieu.

D'après le lemme précédent, cette congruence est identique à celle-ci,

$$(\gamma' z - \beta'' k) r^{g-1} \equiv 0 \pmod{r^g},$$

ou, ce qui revient au même, à celle-ci,

$$\gamma' z \equiv \beta'' k \pmod{r}.$$

Qu'on remarque maintenant que, les nombres γ' et β'', non divisibles par r, étant réels, on pourra toujours déterminer un nombre réel δ évidemment non-divisible par r, qui soit tel que

$$\beta'' \equiv \gamma' \delta \pmod{r};$$

ce qui transforme la dernière congruence en

$$z \equiv k\delta \pmod{r}.$$

Or δ, et par suite $k\delta$, ne peut recevoir que $r-1$ valeurs incongrues d'après le module r, tandis que z, qui est assujetti à l'unique condition de ne point être divisible par r, peut prendre r^2-1 valeurs différentes; on voit donc qu'il existe pour z,

$$r^2 - 1 - (r-1) = r(r-1)$$

valeurs incongrues qui jouissent de la propriété de rendre impossible la dernière congruence. *C. Q. F. D.*

Nous venons de démontrer que pour les bases $\mathfrak{b}$ et $\mathfrak{c}$ déterminées de la manière indiquée et appartenant aux exposants $(r^2-1)r^{g-1}$ et r^{g-1}, la congruence

$$\mathfrak{b}^{\beta} = \mathfrak{c}^{\gamma} \pmod{r^g},$$

dans laquelle β et γ sont des nombres de ces séries

$$0, 1, 2, \ldots, (r^2-1)r^{g-1} - 1; \quad 0, 1, 2, \ldots, r^{g-1} - 1,$$

ne peut subsister que dans le cas où $\beta = \gamma = 0$; ce résultat peut s'exprimer d'une manière un peu différente, et l'on se convaincra sans difficulté qu'on en peut déduire que l'expression

$$\mathfrak{b}^{\beta}\,\mathfrak{c}^{\gamma}$$

donne, pour toutes les combinaisons β, γ dont le nombre

$$(r^2-1)r^{g-1}.r^{g-1} = (r^2-1)r^{2g-2} = \psi(r^g),$$

des nombres incongrus d'après le module r^g, c'est-à-dire deviendra congru une seule fois à chaque nombre n non divisible par r. Les valeurs de β et de γ, pour lesquelles cela a lieu, seront nommées indices de n et seront désignées par β_n et γ_n. Il est évident que les nombres congrus ont mêmes indices, et l'on voit aisément comment les indices d'un produit se déduisent des indices de ses facteurs. Comme

$$c \equiv 1 \pmod{r},$$

de $\mathfrak{b}^{\beta_n} c^{\gamma_n} \equiv n \pmod{r^g}$ il suit aussitôt

$$\mathfrak{b}^{\beta_n} \equiv n \pmod{r},$$

et par conséquent, $\mathfrak{b}$ étant évidemment non-résidu quadratique de r, β_n sera pair ou impair, suivant que r sera résidu ou non-résidu quadratique de r; ou bien, en employant les symboles adoptés plus haut,

$$\left[\frac{n}{r}\right] = (-1)^{\beta_n}. \tag{6}$$

3. Il nous reste encore à examiner le cas où le module est une puissance de $1 + i$.

Soient x et e deux nombres positifs dont le second est impair; soit, en outre, t un nombre complexe arbitraire, mais impair. Puisque

$$[1 + t(1 + i)^x]^e = 1 + et(1 + i)^x + \ldots,$$

dont les termes, à partir du troisième inclusivement, sont évidemment divisibles par $(1 + i)^{x+1}$, il s'ensuit que $[1 + t(1 + i)^x]^e$ aura la forme $1 + t'(1 + i)^x$, où t' est aussi impair. En outre, si l'on suppose $x \overset{=}{>} 3$,

$$[1 + t(1 + i)^x]^2 = 1 + t'(1 + i)^{x+2},$$

où t' est aussi impair. Si l'on combine ces deux résultats, on trouve sans difficulté que, dans la supposition de $x \overset{=}{>} 3$, on a toujours

$$[1 + t(1 + i)^x]^\varrho = 1 + t'(1 + i)^{2x+2\rho},$$

où t' est impair ainsi que t, et où ρ est l'exposant de la plus forte puissance de 2 qui entre dans θ.

Il suffit à l'objet que nous avons en vue que l'exposant de la puissance de $1+i$ que l'on prend pour module soit impair et $\geqq 7$. Soit donc le module $=(1+i)^{3+2h}$, de telle sorte que $h \geqq 2$. Qu'on fasse $x=3$, ou $=4$ dans le résultat précédemment obtenu, et l'on verra aussitôt que $1+t(1+i)^x$ appartient à l'exposant 2^h pour le module $(1+i)^{3+2h}$. Cela étant supposé, il est facile de se convaincre que les deux nombres appartenant à l'exposant 2^h, savoir, $1+t(1+i)^3$ et $1+u(1+i)^4$, dans lesquels t et u sont impairs, possèdent toujours la propriété de rendre impossible, pour tout autre cas que celui où $\delta = \varepsilon = 0$, la congruence

$$[1+t(1+i)^3]^\delta \equiv [1+u(1+i)^4]^\varepsilon \,[\text{mod. } (1+i)^{3+2h}],$$

dans laquelle δ et ε sont des termes de la série

$$0, 1, 2, \ldots, 2^h - 1.$$

Dans le fait, puisque chacune de ces deux suppositions $\delta = 0$, $\varepsilon = 0$, entraîne nécessairement l'autre comme conséquence, il nous suffira de montrer que notre congruence devient impossible quand δ et ε sont tous deux différents de zéro. Désignons les plus hautes puissances de 2, qui entrent respectivement dans δ et dans ε, par 2^ρ et 2^σ, où $\rho < h$, $\sigma < h$, les deux membres seront respectivement contenus dans les deux formes

$$1+t'(1+i)^{3+2\rho}, \quad 1+u'(1+i)^{4+2\sigma},$$

où t' et u' représentent des nombres impairs. Substituons ces valeurs, il vient

$$t'(1+i)^{3+2\rho} \equiv u'(1+i)^{4+2\sigma} \,[\text{mod. } (1+i)^{3+2h}];$$

cette congruence est évidemment impossible, puisque les deux exposants $3+2\rho$ et $4+2\sigma$ sont inégaux et tous deux moindres que $3+2h$.

Posons, comme cas particulier, $t=1$, $u=-1$; alors la congruence

$$(-1+2i)^\delta \equiv 5^\varepsilon \,[\text{mod. } (1+i)^{3+2h}]$$

ne peut subsister que dans le cas où l'on supposerait $\delta = \varepsilon = 0$, ou bien, ce qui revient au même, comme il est facile de s'en convaincre, l'expression

$$(-1+2i)^{\delta}\,5^{\varepsilon}$$

ne donne que des nombres incongrus d'après le module $(1+i)^{3+2h}$ pour toutes les combinaisons δ, ε, dont le nombre est évidemment 2^{2h}. Tous ces nombres sont primaires, c'est-à-dire $\equiv 1\,[\mathrm{mod.}\,(1+i)^3]$, puisque $-1+2i$ et 5 possèdent eux-mêmes cette propriété. Remarquons actuellement que pour chaque module divisible par $(1+i)^3$, deux nombres impairs congrus sont à la fois primaires ou à la fois non primaires, et que, par suite, notre expression ne peut devenir congrue qu'aux nombres primaires; en outre, il est facile de voir que, pour le module $(1+i)^{3+2h}$, il n'existe que $\frac{1}{4}\psi\,[(1+i)^{3+2h}] = 2^{2h}$ nombres impairs primaires incongrus entre eux; on voit donc que l'expression précédente devient congrue une fois, mais une fois seulement, à chaque nombre primaire impair n. Les exposants δ_n, ε_n, pour lesquels cela arrive, seront nommés, à leur tour, les indices de n, et il est évident qu'on obtiendra le premier ou le second indice d'un produit, si, de la somme des premiers ou des seconds indices des facteurs, on supprime le plus grand multiple de 2^h qui y soit contenu. Les indices δ_n, ε_n possèdent, en outre, des propriétés analogues à celles dont nous avons fait mention dans les conclusions des deux numéros précédents et qui sont, comme celles-ci, relatives à la théorie des résidus quadratiques. Posons

$$(-1+2i)^{\delta_n}\,5^{\varepsilon_n} = \lambda' + \nu' i,$$

où λ' et ν' sont respectivement pairs et impairs; on a, d'après les équations (e) et (f), démontrées dans le § VIII du Mémoire cité,

$$(-1)^{\frac{\lambda'^2+\nu'^2-1}{4}} = \left[\frac{i}{\lambda'+\nu' i}\right] = \left[\frac{i}{-1+2i}\right]^{\delta_n}\left(\frac{i}{5}\right)^{\varepsilon_n},$$

$$(-1)^{\frac{(\lambda'+\nu')^2-1}{8}} = \left[\frac{1+i}{\lambda'+\nu' i}\right] = \left[\frac{1+i}{-1+2i}\right]^{\delta_n}\left[\frac{1+i}{5}\right]^{\varepsilon_n};$$

et par conséquent, puisque

$$\left[\frac{i}{-1+2i}\right]=-1,\quad \left[\frac{i}{5}\right]=1,\quad \left[\frac{1+i}{-1+2i}\right]=1,\quad \left[\frac{1+i}{5}\right]=-1,$$

$$(-1)^{\frac{\lambda'^2+\nu'^2-1}{4}}=(-1)^{\delta_n},\qquad (-1)^{\frac{(\lambda'+\nu')^2-1}{8}}=(-1)^{\varepsilon_n}.$$

Posons maintenant $n=\lambda+\nu i$; remarquons ensuite que, en vertu de la congruence

$$\lambda+\nu i\equiv\lambda'+\nu' i\ (\text{mod. } 8),$$

résultant de ce que 8 est un facteur de $(1+i)^{3+2h}$, λ et ν ne diffèrent respectivement de λ' et de ν' que d'un multiple de 8; on voit donc que l'on peut remplacer λ', ν' par λ, ν dans les équations que nous venons d'obtenir, et l'on trouve

$$(7)\quad n=\lambda+\nu i,\quad (-1)^{\frac{\lambda^2+\nu^2-1}{4}}=(-1)^{\delta_n},\quad (-1)^{\frac{(\lambda+\nu)^2-1}{8}}=(-1)^{\varepsilon_n}.$$

4. Nous sommes maintenant en état de pouvoir considérer un nombre quelconque k comme module; cependant, pour éviter toute prolixité inutile, nous nous bornerons au cas où k est pair, la plus haute puissance de $1+i$ qui y entre ayant la forme $3+2h$, et h étant $\geqq 2$. Soit le nombre k, abstraction faite du facteur i^μ égal au produit des puissances des nombres premiers

$$(8)\qquad (a+bi)^f,\quad (a'+b'i)^{f'},\ldots;\quad r^g,\ r'^{g'},\ldots;\quad (1+i)^{3+2h}.$$

Les nombres premiers impairs et à deux termes $a+bi$, $a'+b'i$,..., que nous supposerons primaires pour plus de simplicité, sont inégaux, et r, r',... sont des nombres premiers à un terme, positifs et différents les uns des autres. Que l'on choisisse maintenant d'après les prescriptions des trois numéros précédents, pour chacun des modules (8), une ou deux bases

$$(9)\qquad \mathfrak{a},\ \mathfrak{a}',\ldots;\quad \mathfrak{b},\ \mathfrak{c},\ \mathfrak{b}',\ \mathfrak{c}',\ldots;\quad -1+2i,\ 5,$$

et l'on obtiendra pour chaque n, nombre premier relatif à k, et en

même temps primaire, une série d'indices

$$(10) \qquad \alpha_n, \alpha'_n, \ldots; \quad \beta_n, \gamma_n, \beta'_n, \gamma'_n, \ldots; \quad \delta_n, \varepsilon_n,$$

que l'on devra appeler le système des indices de n, et qui est complétement déterminée si l'on choisit les bases une fois pour toutes. Il est clair que les nombres congrus n et n' ont même système d'indices, et l'inverse de cette loi a également lieu, parce que, dans la supposition de l'identité de système pour deux nombres n et n', on a la congruence $n \equiv n'$ pour chacun des modules (8), et par conséquent aussi pour le module k. Si l'on considère le nombre des valeurs qui peuvent être attribuées à chacun des indices (10) en particulier, on voit aussitôt que le nombre des systèmes différents (10) sera exprimé par le produit

$$(p-1)p^{f-1}.(p'-1)p'^{f'-1}\ldots \times (r^2-1)r^{2g-2}.(r'^2-1)r'^{2g'-2}\ldots \times 2^{2h},$$

c'est-à-dire par $\frac{1}{4}\psi(k)$, comme cela doit être en effet, puisque $\frac{1}{4}\psi(k)$ coïncide évidemment avec le nombre de tous les nombres incongrus d'après le module k, qui n'ont avec k aucun facteur commun, et qui sont, en outre, primaires.

Comme nous aurons souvent à considérer, dans les paragraphes suivants, une série de nombres jouissant de la propriété dont nous venons de parler, c'est-à-dire une série qui ne contient qu'un seul terme qui soit congru, d'après le module k, avec tout nombre premier avec k et, en outre, primaire, nous conviendrons de désigner par

$$(11) \qquad l$$

le terme général d'une pareille série de nombres composée de $\frac{1}{4}\psi(k)$ termes.

§ III.

Revenons actuellement au théorème que nous avons désigné, dans l'introduction, comme l'objet de ce Mémoire, théorème d'après lequel la formule

$$kt + l$$

contient un nombre infini de nombres premiers, lorsque les nombres

donnés k et l n'ont point de diviseur commun, et observons qu'on peut évidemment, sans restreindre la généralité, considérer k comme divisible par $1+i$, et regarder comme impair et $\geqq 7$ l'exposant de la plus haute puissance de $1+i$ qui entre dans k; de la sorte, k devient de la forme supposée dans le paragraphe précédent, art. 4. Rappelons, en outre, que quatre nombres corrélatifs sont toujours à la fois premiers ou non premiers, et il devient évident que l peut être considéré comme nombre primaire, et que cette lettre peut recevoir la signification qui lui a été donnée par l'équation (11).

Cela étant, formons, en conservant toutes les désignations employées dans le § II, art. 4, les équations binômes suivantes, qui répondent aux bases de l'équation (9), d'après la série,

$$(12)\quad \begin{cases} \varphi^{(p-1)p^{f-1}} = 1,\ \varphi'^{(p'-1)p'^{f'-1}} = 1,\ldots; \\ \psi^{(r^2-1)r^{g-1}} = 1, \quad \chi^{rg-1} = 1, \quad \psi'^{(r'^2-1)r'^{g'-1}} = 1, \quad \chi'^{r'g'-1} = 1,\ldots; \\ \theta^{2^h} = 1, \quad \eta^{2^h} = 1. \end{cases}$$

Posons, en outre, pour abréger,

$$\Omega_n = \varphi^{\alpha_n}\varphi'^{\alpha'_n}\ldots \times \psi^{\beta_n}\chi^{\gamma_n}\psi'^{\beta'_n}\chi'^{\gamma'_n}\ldots \times \theta^{\delta_n}\eta^{\varepsilon_n}.$$

Ce produit, ainsi formé, possède plusieurs propriétés très-faciles à démontrer et importantes pour ce qui va suivre; ce sont elles qui vont nous occuper avant tout. Si l'on se représente les racines de l'unité contenues dans Ω comme constantes, on a évidemment

$$(13)\qquad \Omega_{nn'} = \Omega_n \Omega_{n'},$$

et si l'on admet que $n' \equiv n \pmod{k}$,

$$(13')\qquad \Omega_{n'} = \Omega_n.$$

En continuant toujours de supposer qu'on ne change point les racines de l'unité contenues dans Ω, et en étendant le symbole $\sum$ à toutes les valeurs de l définies en l'équation (11),

$$(14)\qquad \sum \Omega_l = 0, \quad \text{ou} \quad \sum \Omega_l = \tfrac{1}{4}\psi(k),$$

selon qu'il se trouve parmi les racines $\varphi, \varphi', \ldots; \psi, \chi, \psi', \chi', \ldots; \theta, \eta,$ au moins une qui diffère de l'unité positive, ou que toutes ces racines lui sont égales. Dans le fait, puisqu'à tous les l répondent tous les systèmes possibles de l'équation (10), notre somme peut se décomposer facilement en facteurs dont chacun ne contiendrait qu'une seule des racines indiquées plus haut. Celui de ces facteurs où φ se présente est évidemment

$$1 + \varphi + \varphi^2 + \ldots + \varphi^{(p-1)p^{f-1}-1},$$

et par conséquent

$$= 0, \quad \text{ou} \quad = (p-1)\,p^{f-1},$$

suivant que φ est différent de l'unité positive ou lui est égal ; et comme on en peut dire autant de toutes les autres, notre assertion se trouve démontrée.

Si nous nous servons dès à présent, comme nous le ferons partout dans la suite, du signe S pour désigner une sommation qui s'étend à toutes les combinaisons des racines des équations (12), racines dont le nombre est évidemment $= \frac{1}{4}\psi(k)$, on a enfin

$$\text{(15)} \qquad S\Omega_n = \tfrac{1}{4}\psi(k), \quad \text{ou} \quad S\Omega_n = 0,$$

suivant que la congruence $n \equiv 1 \pmod{k}$ existe ou n'existe pas. Le premier résultat découle évidemment de ce que tous les indices (10) s'évanouissent pour $n \equiv 1$. Quant au second, pour se convaincre de sa justesse, il suffira de remarquer que $S\Omega_n$ peut être décomposé en facteurs dont chacun ne contient que les racines d'une des équations (12), et que celui de ces facteurs qui est relatif à la première n'est pas autre chose que la somme des racines de cette équation élevée à la puissance α_n. Ce facteur s'évanouira toujours pour cette raison et à cause de $\alpha_n < (p-1)\,p^{f-1}$, excepté lorsque l'on a $\alpha_n = 0$. Ce résultat, ainsi que les considérations analogues qui ont lieu pour les autres facteurs, ont pour conséquence immédiate la deuxième des équations (15), si l'on considère que, dans le cas où $n \equiv 1 \pmod{k}$ n'aurait pas lieu, un des indices (10), au moins, serait différent de zéro.

Cette introduction nous conduit à une démonstration facile de l'é-

quation

$$(16) \qquad \Pi \frac{1}{1 - \Omega_q \frac{1}{(Nq)^s}} = \sum \Omega_n \frac{1}{(Nn)^s} = L.$$

Dans cette équation, s désigne une grandeur arbitraire positive dépassant l'unité; quant au signe de la multiplication Π et à celui de la sommation $\sum$, le premier s'étend à tous les nombres premiers primaires q qui n'entrent point dans k, tandis que le second s'applique à tous les nombres primaires qui n'ont aucun diviseur commun avec k. Les racines φ, φ',... qui entrent dans Ω peuvent être choisies arbitrairement, mais doivent être les mêmes dans chaque Ω, de telle sorte que notre équation générale $\frac{1}{4}\psi(k)$ représente les équations particulières répondant aux diverses combinaisons de racines. Pour nous convaincre de l'exactitude de cette équation, développons dans le premier membre le facteur général en ayant égard à l'équation (13). On obtient ainsi

$$\frac{1}{1 - \Omega_q \frac{1}{(Nq)^s}} = 1 + \Omega_q \frac{1}{(Nq)^s} + \Omega_{q^2} \frac{1}{(N.q^2)^s} + \text{etc....}$$

Qu'on exécute maintenant la multiplication indiquée, qu'on se souvienne que, d'après l'équation (4), chaque nombre n ne peut être représenté comme produit de puissances de nombres premiers primaires que d'une seule façon, et le premier membre de notre équation se transforme dans le second. *C. Q. F. D.*

§ IV.

Nous allons maintenant considérer de plus près la série générale L, équation (16), qui a évidemment une valeur finie et indépendante de la manière dont les termes se suivent aussi longtemps que $s > 1$, et nous chercherons, en particulier, à déterminer comment cette valeur varie lorsqu'en posant $s = 1 + \rho$, on fait la variable positive ρ infiniment petite. La série L, but de nos recherches actuelles, se décompose en $\frac{1}{4}\psi(k)$ séries partielles dont chacune contient tous les termes où n est congru selon le module k au même nombre l, équation (11). Une

quelconque de ces séries partielles devient

$$W = \sum \frac{1}{N(kt+l)^{1+\rho}},$$

lorsqu'on y supprime dans tous ses termes le facteur commun Ω; là le signe $\sum$ comprend tous les nombres entiers complexes t. Nous avons montré, dans le Mémoire intitulé *Rech. sur les form.*, § XVIII, art. 3, que cette dernière série devient égale à l'expression $\frac{\pi}{N(k)}\frac{1}{\rho}$ lorsque ρ devient infiniment petit. Ce résultat peut être complété à l'aide des considérations développées au lieu cité, et l'on prouve facilement que

$$W = \frac{\pi}{N(k)}\frac{1}{\rho} + A + \rho F(\rho),$$

où A désigne une constante réelle, et $F(\rho)$ une fonction réelle de ρ qui tend vers une limite finie quand ρ devient infiniment petit. Il s'ensuit immédiatement, en tenant compte de l'équation (14), que

$$(17) \qquad L = \frac{\pi\psi(k)}{4N(k)}\frac{1}{\rho} + F(\rho), \quad \text{ou} \quad L = A + A'i + \rho[\Phi(\varphi) + i\Phi'(\rho)],$$

suivant que les racines de l'unité contenues dans L sont toutes égales aux racines positives de l'unité, ou que l'une d'elles au moins est différente de celles-ci. A et A′ sont des constantes réelles, et $F(\rho)$, $\Phi(\rho)$, $\Phi'(\rho)$ sont des fonctions réelles de ρ qui tendent vers des limites finies pour des valeurs infiniment petites de la variable positive ρ.

Les séries L peuvent se partager en trois classes, d'après les différentes combinaisons de racines qu'elles contiennent. La première de ces classes consiste dans la série unique où toutes les racines de l'unité ont pour valeur 1, et qui est relative à la première des équations (17). La seconde classe embrasse toutes les autres séries où il n'y a que des racines réelles. Remarquons maintenant que les seules équations où les exposants soient impairs sont celles dont les racines sont désignées par χ, χ',..., et l'on verra que, pour représenter toutes les séries de la seconde classe, il faut combiner de toutes les manières possibles les doubles signes de

$$\varphi = \pm 1,\ \varphi' = \pm 1,\ldots;\quad \psi = \pm 1,\ \chi = \pm 1,\ \psi' = \pm 1,\ \chi' = \pm 1,\ldots;$$
$$\theta = \pm 1,\ \eta = \pm 1;$$

mais de toutes ces combinaisons il faut exclure celle qui répond aux signes supérieurs tous ensemble; cette combinaison unique forme la première classe. Enfin, la troisième classe comprend toutes les séries qui présentent au moins une racine imaginaire de l'unité, et l'on voit facilement que les séries de cette classe sont toujours ordonnées par couples, puisque, dans la supposition énoncée, les deux combinaisons de racines

$$\varphi,\ \varphi',\ldots;\quad \psi,\ \chi,\ \psi',\ \chi',\ldots;\quad \theta,\ \eta,$$

et

$$\frac{1}{\varphi},\ \frac{1}{\varphi'},\ldots;\quad \frac{1}{\psi},\ \frac{1}{\psi'},\ \frac{1}{\chi},\ \frac{1}{\chi'},\ldots;\quad \frac{1}{\theta},\ \frac{1}{\eta},$$

sont évidemment différentes l'une de l'autre. Dans ces séries la transition de l'une à celle qui lui est coordonnée a lieu en changeant i en $-i$ dans la deuxième équation (17), tandis que les termes imaginaires de cette équation disparaissent pour les séries de la seconde classe, auxquelles l'équation citée appartient également.

Quand ρ devient infiniment petit, la valeur de la série qui constitue la première classe croît par-delà toute limite positive, tandis que les valeurs de toutes les autres séries tendent vers des limites finies, comme on peut s'en convaincre d'après l'équation (17). Cela n'est cependant pas suffisant pour le but que nous nous proposons, et il nous faut encore faire voir que toutes ces limites sont différentes de zéro, c'est-à-dire qu'on n'a pas à la fois $A = 0$, $A' = 0$ dans la seconde des équations (17). Admettons un instant que cette preuve soit faite pour toutes les séries de la seconde classe. Cette supposition admise, nous montrerons, dans le paragraphe suivant, que cette assertion est vraie pour la troisième classe, et nous en déduirons aussitôt la loi posée au commencement du § III, en sorte qu'il ne nous restera plus qu'à démontrer, à la fin de ce Traité, la propriété supposée à l'égard des séries de la seconde classe.

§ V.

Prenons les logarithmes népériens des deux membres de l'équation (16) et développons, il vient

$$\ldots + \frac{1}{\mu}\sum \Omega_{q^\mu}\,\frac{1}{(\mathrm{N}q)^{\mu+\mu\rho}} + \ldots = \log \mathrm{L}.$$

Dans cette équation nous nous sommes bornés, pour abréger, à écrire le terme général dans lequel on doit attribuer successivement à μ toutes les valeurs depuis $\mu = 1$ jusqu'à $\mu = \infty$; de plus, le signe de la sommation s'y rapporte à tous les nombres q. Soit maintenant l un nombre déterminé quelconque parmi ceux qui ont été définis sous le numéro (11), et posons

$$ll' \equiv 1 \pmod{k},$$

où l' est, comme l, un nombre primaire et premier avec k. Multiplions notre équation par Ω_l, et faisons la sommation d'après toutes les combinaisons possibles de racines, il vient

$$\ldots + \frac{1}{\mu} \sum (S\Omega_{l'q^\mu}) \frac{1}{(Nq)^{\mu+\mu\rho}} + \ldots = S\Omega_{l'} \log L.$$

Maintenant, d'après l'équation (15),

$$S\Omega_{l'q^\mu} = 0,$$

excepté quand

$$l'q^\mu \equiv 1,$$

ou bien, ce qui revient au même, excepté quand

$$q^\mu \equiv l \pmod{k},$$

auquel cas la valeur de la somme devient $\frac{1}{4}\psi(k)$. L'équation devient ainsi

$$(18) \qquad \sum \frac{1}{(Nq)^{1+\rho}} + \frac{1}{2} \sum \frac{1}{(Nq)^{2+2\rho}} + \ldots = \frac{4}{\psi(k)} S\Omega_{l'} \log L,$$

où le signe $\sum$ s'étend dans le premier, le deuxième,... terme respectivement, aux nombres premiers q dont les premières, deuxièmes,... puissances sont

$$\equiv l \pmod{k}.$$

Posons spécialement

$$l \equiv 1,$$

alors on a

$$l' \equiv 1 \pmod{k}, \quad \Omega_{l'} = 1,$$

et le résultat général se transforme en

$$\sum \frac{1}{(Nq)^{1+\rho}} + \frac{1}{2}\sum \frac{1}{(Nq)^{2+2\rho}} + \ldots = \frac{4}{\psi(k)}\,S.\log L.$$

Considérons actuellement la somme S log L pour le cas où ρ devient infiniment petit. Les termes correspondants aux séries de la deuxième classe tendent ensemble vers des limites finies; au contraire, le terme correspondant à la première classe prend alors une valeur positive infiniment grande, puisque ce terme peut être mis, d'après l'équation (17), sous la forme

$$\log\left(\frac{1}{\rho}\right) + \log\left(\frac{\pi\psi(k)}{4N(k)} + \rho F(\rho)\right),$$

dont la première partie devient infinie tandis que la seconde tend vers une limite finie. Supposons maintenant que la limite finie d'une série de la troisième classe soit égale à zéro, c'est-à-dire supposons que l'on ait, dans l'équation (17),

$$A = 0, \quad A' = 0;$$

alors de la réunion des deux membres qui, dans notre somme, répondent à cette série et à celle qui lui est coordonnée, résultera l'expression suivante :

$$-2\log\left(\frac{1}{\rho}\right) + \log[\varphi(\rho)^2 + \varphi'(\rho)^2].$$

Après avoir combiné cette expression avec la précédente, la somme contiendra le terme $-\log\left(\frac{1}{\rho}\right)$ qui prend une valeur négative infiniment grande, et qui ne peut être détruit par $\log[\varphi(\rho^2) + \varphi'(\rho^2)]$, puisque ce dernier logarithme peut seulement avoir une limite finie, ou bien prendre lui-même une valeur négative infiniment grande. Ce résultat est en contradiction avec notre équation précédente, dont le premier membre ne contient que des termes positifs, et cette contradiction serait encore évidemment renforcée si l'on voulait considérer comme évanouissantes les valeurs des limites pour plus d'un couple de séries coordonnées de la troisième classe. Il est ainsi prouvé, réserve faite de la démonstration qu'il nous reste à donner pour les séries de

deuxième classe, que log L tend toujours vers une limite finie, excepté dans le seul cas où L désigne la série de la première classe, car alors notre logarithme peut devenir plus grand que tout nombre donné positif.

Revenons à présent à l'équation générale (18); nous voyons que le deuxième membre, et par conséquent aussi le premier membre, devient infini quand ρ devient infiniment petit. Mais, maintenant, la somme de toutes les séries qui se trouvent dans le premier membre, à partir de la seconde inclusivement, reste finie, puisque

$$\frac{1}{2}\sum\frac{1}{(Nq)^2}+\frac{1}{3}\sum\frac{1}{(Nq)^3}+\ldots$$

est encore finie même lorsqu'on ne borne point les sommations, comme nous le faisons ici, à certains nombres premiers q, et qu'on l'étend à tous les nombres entiers dont la norme surpasse l'unité. Il faut donc que ce soit la somme $\sum\frac{1}{(Nq)^{1+\rho}}$ qui croisse au delà de toute limite finie, ce qui exige que le nombre de ses termes soit infini; elle donnera donc alors un nombre infini de nombres premiers tous contenus dans la forme $kt+l$. *C. Q. F. D.*

§ VI.

Afin de compléter la démonstration que nous venons d'exposer, il faut encore faire voir que, pour chaque série de deuxième classe, la limite correspondante à une valeur infiniment petite de ρ est différente de zéro. Une série de ce genre contient une combinaison de racines de la forme

$$\varphi=\pm 1,\ \varphi'=\pm 1,\ldots;\quad \psi=\pm 1,\ \chi=1,\ \psi'=\pm 1,\ \chi'=1,\ldots;$$
$$\theta=\pm 1,\ \eta=\pm 1.$$

Formons le produit de ceux d'entre les nombres premiers

$$a+bi,\quad a'+b'i,\ldots;\quad r,\ r',\ldots,$$

auxquels, dans cette combinaison de racines, répond une racine égale à l'unité négative, à savoir, $\varphi, \varphi',\ldots; \psi, \psi',\ldots$, et désignons le

produit de ces nombres premiers par Q, et par V le produit de tous les autres (il va sans dire que si, dans un de ces groupes, il ne se trouve point de nombre premier, on remplacera Q ou V par l'unité); alors l'expression Ω_n, contenue dans le terme général de la série, pourra prendre la forme suivante, d'après les résultats obtenus en l'équation (5) et en l'équation (6):

$$\Omega_n = \left[\frac{n}{Q}\right] \theta^{\delta_n} \eta^{\varepsilon_n}.$$

Posons, en outre, comme plus haut,

$$n = \lambda + \nu i,$$

il vient

$$\theta^{\delta_n} = \theta^{\frac{\lambda^2+\nu^2-1}{4}}, \quad \eta^{\varepsilon_n} = \eta^{\frac{(\lambda+\nu)^2-1}{8}}.$$

Si $\theta = 1$, la première de ces équations est évidente; si, au contraire, $\theta = -1$, elle coïncide avec une des équations désignées par la formule (7), et il en arrive autant de la seconde.

La limite d'une série quelconque de la deuxième classe est par conséquent

$$\sum \theta^{\frac{\lambda^2+\nu^2-1}{4}} \eta^{\frac{(\lambda+\nu)^2-1}{8}} \left[\frac{\lambda+\nu i}{Q}\right] \frac{1}{(\lambda^2+\nu^2)^{1+\rho}},$$

où ρ est supposé infiniment petit; le signe $\sum$ s'étend à tous les nombres impairs primaires $\lambda + \nu i$ qui n'ont aucun facteur commun avec k, ou avec QV, ce qui revient au même; remarquons encore qu'on ne peut avoir simultanément

$$Q = 1, \quad \theta = 1, \quad \eta = 1,$$

car, dans cette supposition, la combinaison des racines considérée plus haut répondrait à la série L de la première classe. Mais maintenant notre série est, avec cette restriction, toujours contenue dans la série générale qui, comme nous l'avons montré dans le Mémoire déjà souvent cité, exprime, abstraction faite d'un facteur fini, le nombre des classes comprenant toutes les formes quadratiques pour un déterminant arbitraire non quadratique. Que l'on compare avec la série ci-dessus celle que nous avons trouvée dans l'ouvrage cité, § XVIII,

équation (18), pour l'expression de ce nombre, et l'on verra que la première est relative aux quatre déterminants

$$QV^2, \quad iQV^2, \quad (1+i)QV^2, \quad i(1+i)QV^2,$$

d'après les quatre combinaisons respectives de racines qui peuvent s'y présenter,

$$\theta=1,\ \eta=1; \quad \theta=-1,\ \eta=1; \quad \theta=1,\ \eta=-1; \quad \theta=-1,\ \eta=-1.$$

De là résulte immédiatement la propriété qu'il s'agit de démontrer; car, si notre série se réduisait à zéro, alors le nombre des classes des formes quadratiques deviendrait aussi nul pour le déterminant correspondant, ce qui est impossible, puisque ce nombre est toujours au moins égal à l'unité.

Nous terminerons par une remarque destinée à éclaircir la comparaison que nous avons précédemment indiquée; cette remarque consiste en ce qu'on peut, sans changer la valeur de la série trouvée à l'endroit cité, étendre la sommation dans cette série à tous les nombres impairs primaires $\lambda + \nu i$ sans facteurs communs avec le déterminant, auxquels cette dénomination est applicable dans le sens adopté dans le présent Mémoire. Cela résulte immédiatement de ce que, pour un groupe quelconque de nombres impairs assemblés, le nombre considéré comme primaire d'après une définition, est évidemment égal ou opposé à celui qui lui correspond dans l'autre définition, et que, de plus, un terme quelconque de la série reste invariable quand on y change $-\lambda+\nu i$ en $-\lambda-\nu i$.