LAURENT

THÉORIE DES NOMBRES

THÉORIE
DES NOMBRES

ORDINAIRES ET ALGÉBRIQUES

THÉORIE

DES NOMBRES

ORDINAIRES ET ALGÉBRIQUES

PAR

H. LAURENT

Examinateur d'entrée à l'École Polytechnique.
Professeur à l'Institut agronomique,

PARIS
C. NAUD, ÉDITEUR
3, RUE RACINE, 3
—
1904

PRÉFACE

Ce petit traité d'arithmologie ne contient pas *toute* la théorie des nombres, il est destiné à combler une lacune qui existe dans les recherches arithmétiques de Gauss, dans la théorie des nombres de Legendre et dans le traité plus récent de M. Cahen. Ne voulant pas faire double emploi avec ces excellents ouvrages, j'ai dû limiter mon sujet et je me suis borné à étudier les questions relatives aux nombres premiers, laissant systématiquement de côté la théorie des formes fort bien exposées dans l'ouvrage de M. Cahen et dans la thèse tout à fait remarquable de M. Seguier (1894) publié chez G. Villars. C'est dans ce dernier ouvrage que l'on trouvera les recherches les plus récentes sur cette partie de la théorie des nombres.

Je me suis donc surtout attaché à traiter les questions relatives non seulement aux nombres premiers ordinaires, mais encore aussi aux nombres complexes algébriques.

J'ai donné en particulier une théorie analytique des nombres algébriques dans laquelle les nombres idéaux ont une existence réelle, sont de véritables nombres ordinaires.

J'ai essayé autant que possible, de substituer aux

méthodes synthétiques, les méthodes analytiques parfois plus longues, mais plus lumineuses ; c'est à mon avis, un manque d'égards pour le lecteur que de lui cacher la voie qui a conduit à un résultat, bien entendu, quand on connaît cette voie.

THÉORIE
DES
NOMBRES ORDINAIRES
ET ALGÉBRIQUES

INTRODUCTION

L'arithmologie, aussi appelée arithmétique supérieure, théorie des nombres, a pour but l'étude des propriétés des nombres entiers. Les mathématiques pures ont en général pour but l'étude des propriétés des quantités, qui sont représentées par les nombres, elles ont donc pour but la théorie des nombres.

Mais les nombres peuvent être considérés à deux points de vue, soit comme de simples auxiliaires visant surtout la quantité mesurée, soit comme symboles jouissant par eux-mêmes de propriétés indépendantes de la quantité. L'analyse algébrique se place au premier de ces points de vue, surtout utilitaire ; l'arithmologie se place au second point de vue. Mais l'arithmologie se passerait difficilement du concours de l'analyse algébrique, et si les deux parties de la théorie générale ont des buts distincts, elles se confondent en réalité souvent, et se prêtent un mutuel appui.

Je vais cependant essayer de donner une définition plus précise de l'arithmologie.

On sait que la numération a pour but de faire connaître des méthodes pour la représentation des nombres. Dans les traités élémentaires d'arithmétique, on n'enseigne qu'une méthode ; elle consiste, au fond, à représenter un nombre entier au moyen d'un polynôme entier tel que :

$$a_0 + a_1 x + a_2 x^2 + \ldots$$

dans lequel x désigne ce que l'on appelle la base, et a_0, a_1,

a_2... désignent les chiffres, c'est-à-dire des nombres positifs inférieurs à x. Dans la numération romaine, on suppose quelquefois les chiffres négatifs. Cauchy a également fait usage des chiffres négatifs. Ce qui permet de simplifier les calculs et de réduire le volume de la table de multiplication. Dans le système préconisé par Cauchy, les nombres successifs s'écrivent :

1, 2, 3, 4, 5, 15, 14, 13, 12, 11, 10, 11...

et $3\,\overline{1}\,\overline{4}$ par exemple représente 300-20-4 ou 276.

L'avantage des systèmes de numération, fondé sur l'emploi d'une base, consiste surtout en ce que tous les nombres entiers peuvent être représentés dans ces systèmes et d'une seule manière. Mais ce ne sont pas les seuls systèmes que l'on puisse adopter.

Ainsi la forme suivante :

$$x^2 + y^2 + z^2 + t^2$$

peut aussi représenter tous les nombres en donnant à x, y, z, t, des valeurs entières. Mais un même nombre pourrait être représenté de plusieurs manières différentes. D'autres formes ne représenteraient pas tous les entiers, ainsi $2n + 1$ ne représenterait que les nombres impairs, il y aurait dans l'emploi de ces systèmes des avantages et des inconvénients.

Il est facile de passer d'un système de numération fondé sur l'emploi d'une base à un système fondé sur l'emploi d'une base différente. Mais il n'est pas toujours facile d'écrire un nombre dans un système donné quand on sait l'écrire dans un autre, par exemple dans le système dont la base est 10. Ainsi bien que l'on sache que tout nombre peut se mettre sous la forme :

$$x^2 + y^2 + z^2 + t^2$$

il est très pénible de le mettre effectivement sous cette forme quand il dépasse mille.

Cela posé, je crois que l'on pourrait définir l'arithmologie en disant qu'elle a surtout en vue l'étude des systèmes de numération, ou pour employer un autre langage, l'étude des formes que peuvent affecter les nombres et la transformation de ces formes les unes dans les autres.

En analyse indéterminée par exemple, on cherche à mettre un nombre d sous la forme $ax + by$, $ax + by + cz...$, a, b, $c...$ désignant des entiers donnés. Ce même problème appartient aussi à la théorie des congruences.

Dans la théorie de la divisibilité, on cherche à mettre les nombres sous la forme $x\,y\,z...$, etc.

CHAPITRE PREMIER

FONCTIONS NUMÉRIQUES

1. — Valeur de $\Sigma\, n^p$

On a souvent besoin dans la théorie des nombres de considérer des fonctions définies pour des valeurs entières de la variable seulement ; ce sont des fonctions numériques. Telles seraient les fonctions de n.

$$1 + 2 + 3 \ldots + n ; \quad 1.2.3 \ldots n.$$

Interpoler une pareille fonction, c'est trouver une fonction définie pour toutes les valeurs de la variable et qui, pour des valeurs entières, coïncide avec la fonction numérique.

La formule de Newton donne

$$x^p = \frac{x}{1}\Delta 0^p + \frac{x(x-1)}{1.2}\Delta^2 0^p + \ldots \frac{x(x-1)\ldots(x-p+1)}{1.2\ldots p}\Delta^p 0^p ;$$

or on a

$$\sum_1^x x = \frac{x(x+1)}{1.2},$$

$$\sum_1^x \frac{x(x-1)}{1.2} = \frac{(x-1)x(x+1)}{1.2.3},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

donc

$$(1) \qquad \sum_1^x x^p = \frac{x(x+1)}{2}\Delta 0^p + \frac{(x-1)x(x+1)}{1.2.3}\Delta^2 0^p + \ldots$$
$$+ \frac{(x-p+1)\ldots x(x+1)}{1.2.3\ldots(p+1)}\Delta^p 0^p.$$

formule où

$$\Delta^k 0^p = k^p - \frac{k}{1}(k-1)^p + \frac{k(k-1)}{1.2}(k-2)^p \ldots$$

La formule (1) *interpole* la fonction numérique $\sum_1^n x^p$, et

cela d'une manière remarquable, car la fonction *interpolatrice* est entière.

Si l'on admet, ce qui sera démontré tout à l'heure, que $\frac{\Delta^p o^l}{p!}$ est un nombre entier, la formule (1) montre que $\sum_1^n x^p$ est divisible par $\frac{x(x+1)}{2}$, si $p < 4$ c'est-à-dire par $\sum_1^n x$, d'ailleurs on a, au moyen de la formule (1) :

$$\sum_1^x x = \frac{x(x+1)}{2},$$

$$\sum_1^x x^2 = \frac{x(x+1)(2x+1)}{6},$$

$$\sum_1^x x^3 = \left[\frac{x(x+1)}{2}\right]^2,$$

. . . . . .

Pour avoir la somme des puissances p de nombres en progression arithmétique a, $a + b$, $a + 2b$..., $a + nb$, on observera que cette somme est

$$\Sigma (a+nb)^p = a^p \sum_1^n x^0 + \frac{p}{1} a^{p-1} b \sum_1^n x + \frac{p(p-1)}{1.2} a^{p-2} b^2 \sum_1^n x^2$$

$$+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

elle dépend par conséquent des sommes que nous venons d'apprendre à calculer.

2. — Sur la fonction $\Delta^n o^p$

Considérons l'expression suivante, où α est entier et positif :

(1) $$P^\alpha x^\alpha e^x,$$

dans laquelle P désigne le symbole opératoire $\frac{d}{dx} x$. Il est facile de voir que cette expression (1) est le produit de e^x par un polynôme Q à coefficients *entiers*, l'opération $\frac{d}{dx} x$, n'introduisant jamais de dénominateurs. Or, on peut former l'expression (1) en partant de la formule

$$x^\alpha e^x = x^\alpha + \frac{x^{\alpha+1}}{1} + \frac{x^{\alpha+2}}{1.2} + \ldots,$$

et l'on a

$$\mathrm{P}x^n e^x = \frac{x^n(x+1)}{1} + \frac{x^{n+1}(x+2)}{1.2} + \ldots$$

$$\mathrm{P}^2 x^n e^x = \frac{x^n(x+1)^2}{1} + \frac{x^{n+1}(x+2)^2}{1.2} + \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mathrm{P}^n x^n e^x = \frac{x^n(x+1)^n}{1} + \frac{x^{n+1}(x+2)}{1.2} + \ldots;$$

multiplions par

$$e^{-x} = 1 - \frac{x}{1} + \frac{x^2}{1.2} - \ldots,$$

nous aurons le polynôme Q, à savoir :

$$Q = x^n \left[(x+1)^n + \frac{x}{1}[(x+2)^n - (x+1)^n] \ldots \right.$$

$$\left. + \frac{x^p}{p!}[(x+p+1)^n - \frac{p}{1}(x+p)^n + \frac{p(p-1)}{1.2}(x+p-1)^n \ldots \right]$$

ou

$$Q = x^n \left[(x+1)^n + \frac{x}{1}\Delta(x+1)^n \ldots + \frac{x^p}{p!}\Delta^p(x+1)^n + \ldots \right]$$

or, le polynôme Q est à coefficients entiers, donc

$$\frac{\Delta^p(x+1)^n}{p!} \text{ est entier.}$$

Dans la formule d'interpolation de Newton, tous les coefficients sont donc entiers, et plus généralement : *Si $f(x)$ est un polynôme à coefficients entiers, $\Delta^p f(x)$, pour toutes les valeurs entières de x sera divisible par p !*

3. — La fonction $\zeta(x)$ interpolant $\Sigma \frac{1}{n^x}$.

Si l'on pose avec Riemann

$$\zeta(x) = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \ldots \frac{1}{n^x} + \ldots,$$

la fonction $\zeta(x)$ ne sera déterminée que si la partie réelle de x est supérieure à l'unité, mais la fonction ζ ainsi définie,

peut être prolongée analytiquement et recevoir des valeurs bien déterminées, quel que soit x.

On a en supposant $x > 1$,

$$\frac{\Gamma(x)}{n^x} = \int_0^\infty z^{x-1} e^{-nz}\, dz ;$$

faisons $n = 1, 2\ldots$, en ajoutant on a

$$\Gamma(x)\, \zeta(x) = \int_0^\infty \frac{z^{x-1}\, dz}{e^z - 1}.$$

Or si l'on intègre $\frac{z^{x-1}\, dz}{e^z - 1}$ le long d'un lacet ayant son entrée au point $+\infty$ situé sur l'axe des x et le point o pour point critique, on a

$$\int \frac{z^{x-1}\, dz}{e^z - 1} = (e^{2\pi x\sqrt{-1}} - 1) \int_0^\infty \frac{z^{x-1}\, dz}{e^z - 1}$$

ou

$$\int \frac{z^{x-1}\, dz}{e^z - 1} = \zeta(x)\, \Gamma(x)\, (e^{2\pi x\sqrt{-1}} - 1),$$

et cette formule a pour premier membre une fonction bien définie quel que soit x, donc $\zeta(x)$ lui-même se trouve bien défini dans toute l'étendue du plan. Mais en déformant le lacet et son cercle et en rendant ses bords parallèles à l'axe des y sans lui faire franchir l'origine, on a

$$2\pi\sqrt{-1} \sum_{-\infty}^{+\infty} (2k\pi\sqrt{-1})^{x-1} = \zeta(x)\, \Gamma(x)\, (e^{2\pi x\sqrt{-1}} - 1),$$

le signe Σ étant pris en excluant la valeur $k = o$, cette formule revient à

$$2^x \pi^x [\sqrt{-1}^x + (-\sqrt{-1})^x]\, \zeta(1-x) = \zeta(x)\, \Gamma(x)\, (e^{2\pi x\sqrt{-1}} - 1).$$

Or $\sqrt{-1}^x = e^{\frac{\pi}{2} x\sqrt{-1}}$; divisant par $2e^{\pi x\sqrt{-1}}\sqrt{-1}$, on a

$$(1) \qquad 2^x \pi^x \sin\frac{\pi x}{2}\, \zeta(1-x) = \zeta(x)\, \Gamma(x) \sin \pi x.$$

Si l'on observe que

$$\Gamma(x)\, \Gamma(1-x) = \frac{\pi}{\sin \pi x}$$

on fait disparaître les sinus et l'on a

$$\frac{2^x\pi^x\zeta(1-x)}{\Gamma\left(\frac{x}{2}\right)\Gamma\left(1-\frac{x}{2}\right)} = \frac{\zeta(x)\,\Gamma(x)}{\Gamma(x)\,\Gamma(1-x)},$$

ou

$$2^x\pi^x\zeta(1-x)\,\Gamma(1-x) = \zeta(x)\,\Gamma\left(\frac{x}{2}\right)\,\Gamma\left(1-\frac{x}{2}\right)$$

Or, on a

$$\Gamma\left(1-\frac{x}{2}\right)\Gamma\left(\frac{1}{2}-\frac{x}{2}\right) = 2^x\sqrt{\pi}\,\Gamma(1-x),$$

alors la formule précédente devient

$$(2) \qquad \pi^{-\frac{x}{2}}\,\Gamma\left(\frac{x}{2}\right)\zeta(x) = \pi^{-\frac{1-x}{2}}\,\Gamma\left(\frac{1-x}{2}\right)\zeta(1-x).$$

On voit que la fonction

$$\pi^{-\frac{x}{2}}\,\Gamma\left(\frac{x}{2}\right)\zeta(x)$$

ne change pas quand on remplace x par $1-x$.

La formule (1) s'écrit :

$$\zeta(1-x) = 2^{-x}\pi^{-x}\zeta(x)\,\Gamma(x).\,2\cos\frac{\pi x}{2},$$

si l'on pose $\zeta(2) = s_2$, $\zeta(3) = s_3\ldots$, on a en posant $x = 2, 3\ldots$

$$\zeta(-1) = 2^{-1}\pi^{-2}s_2,$$
$$\zeta(-2) = 0,$$
$$\zeta(-3) = 2^{-3}\pi^{-3}s_3\,1\cdot2\cdot3,$$
$$\zeta(-4) = 0.$$
$$\ldots\ldots\ldots$$

La fonction $\xi(x)$

Reprenons la formule

$$\pi^{-\frac{x}{2}}\,\Gamma\left(\frac{x}{2}\right)\zeta(x) = \pi^{-\frac{1-x}{2}}\,\Gamma\left(\frac{1-x}{2}\right)\zeta(1-x),$$

multiplions les deux membres par $\frac{x}{2}(1-x)$, nous aurons

$$\pi^{-\frac{x}{2}}\Gamma\left(\frac{x}{2}+1\right)\zeta(x)(1-x)$$
$$=\pi^{-\frac{1-x}{2}}\Gamma\left(\frac{3-x}{2}\right)x\,\zeta(1-x);$$

si l'on pose

$$\xi(t)=\pi^{-\left(\frac{1}{2}+t\sqrt{-1}\right)}\Gamma\left(\frac{\frac{1}{2}+t\sqrt{-1}}{2}+1\right)$$
$$\zeta\left(\frac{1}{2}+t\sqrt{-1}\right)\left(\frac{1}{2}+t\sqrt{-1}-1\right),$$

la fonction $\xi(t)$ ne changera pas quand on changera t en $-t$.

Les fonctions $\xi(t)$ et $\zeta(t)$ sont célèbres, elles font encore aujourd'hui l'objet des recherches de savants illustres, mais leurs propriétés qui, si elles étaient bien connues, donneraient la clef de la loi des nombres premiers, sont encore mal connues ou longues et difficiles à établir. Bornons-nous à constater que $\xi(t)$ est susceptible de se mettre sous la forme

$$A\left(1-\frac{t^2}{t_1^2}\right)\left(1-\frac{t^2}{t_2^2}\right)\cdots$$

A, t_1, t_2... désignant des constantes réelles (Hadamard, *Journal de Liouville* 1893). Mangoldt (*Journal de Crelle* XIV) a prouvé que les racines de $\zeta(x)=0$ étaient de la forme $\frac{1}{2}+t\sqrt{-1}$. Résultat entrevu par Riemann, mais non démontré par lui. Il nous est impossible de reproduire ces travaux, à cause de leur longueur. Peut-on espérer que cette théorie se simplifiera un jour?

4. — Nouvelle forme de $\zeta(x)$

On a évidemment

$$\zeta(x)=\mathcal{S}\frac{\pi}{z^x}\frac{\cos\pi z}{\sin\pi z}$$

le résidu étant relatif aux points 1, 2,... n,... mais il faut

supposer la partie réelle de x plus grande que un. On peut poser :

$$\zeta(x) = \frac{1}{2\sqrt{-1}} \int \frac{1}{z^x} \frac{\cos \pi z}{\sin \pi z}\, dz$$

et on peut supposer l'intégrale prise le long d'une parallèle à l'axe des y passant par le point $\frac{1}{2}$, alors

$$\zeta(x) = \frac{1}{2} \int_{-\infty}^{+\infty} \left(\frac{1}{2} + t\sqrt{-1}\right)^{-x} \frac{\sin \pi t \sqrt{-1}}{\cos \pi t \sqrt{-1}}\, dt$$

et si l'on intègre par parties

$$\zeta(x) = \frac{\pi}{2} \frac{1}{x-1} \int_{-\infty}^{+\infty} \left(\frac{1}{2} + t\sqrt{-1}\right)^{-x+1} \frac{dt}{(e^{\pi t} + e^{-\pi t})^2}$$

cette fois on peut supposer x quelconque et l'intégrale se développe quelque soit x suivant les puissances de $x - 1$. $\zeta(x)$ a donc un seul infini $x = 1$.

En prenant pour contour d'intégration la droite passant par le point $\frac{3}{2}$ et parallèle à l'axe des y on aurait eu

$$\zeta(x) - 1 = \frac{\pi}{2} \frac{1}{x-1} \int_{-\infty}^{+\infty} \left(\frac{3}{2} + t\sqrt{-1}\right)^{-x+1} \frac{dt}{(e^{\pi t} + e^{-\pi t})^2}$$

etc.

5. — Sur la fonction E (x)

On a souvent besoin de parler du plus grand entier contenu dans le nombre x, on le désigne par le symbole E(x) (égal à x si x est entier).

On a

$$\frac{1}{\pi} \int_{-\infty}^{+\infty} \frac{\sin at}{t}\, dt = \pm 1.$$

Pour $a > o$, on prend le signe $+$; pour $a < o$ le signe $-$, si l'on désigne par $\varphi(a)$ l'intégrale précédente, on a donc

$$\varphi(x) = \begin{cases} +1 \text{ si } x > 0; \\ -1 \text{ si } x < 0; \end{cases}$$

par suite

$$\varphi(x-1) = \begin{cases} 1 \text{ si } x - 1 > 0, x > 1, \\ -1 \text{ si } x - 1 < 0, x < 1, \end{cases}$$

$$\varphi(x-2) = \begin{cases} 1 \text{ si } x > 2. \\ -1 \text{ si } x < 2, \end{cases}$$

. . . . . .

Considérons alors la fonction

$$a_1\varphi(x-1)+a_2\varphi(x-2)\ldots+a_n\varphi(x-n)=f(x);$$

quand x varie de 0 à 1 elle est égale à

$$-(+a_1+a_2+\ldots a_n),$$

quand x varie de 1 à 2, elle est égale à

$$-(-a_1+a_2+a_3\ldots a_n),$$

. . . . . .

on aura donc $F(x)=E(x)$ entre les limites o et n si l'on pose

$$\begin{aligned}
&a_1+a_2+\ldots+a_n=0,\\
&a_1-a_2-\ldots-a_n=1,\\
&a_1+a_2-\ldots-a_n=2,\\
&\ldots\ldots\ldots\ldots\\
&a_1+a_2\ldots-a_n=n-1;
\end{aligned}$$

d'où l'on tire

$$a_1=\frac{1}{2},\quad a_2=\frac{1}{2}\ldots\quad a_{n-1}=\frac{1}{2},\quad a_n=-\frac{n-1}{2};$$

donc

$$E(x)=\frac{1}{2\pi}\int_{-\infty}^{+\infty}\frac{1}{t}\left[\sin(x-1)t+\sin(x-2)t\ldots+\sin(x-n+1)t-(n-1)\sin(x-nt)\right]dt,$$

ou en vertu d'une formule connue :

$$E(x)=\frac{1}{2\pi}\int_{-\infty}^{+\infty}\frac{1}{t}\left[\sin\left(x-\frac{n-1}{2}\right)\frac{\sin\frac{n-1}{2}t}{\sin\frac{t}{2}}-(n-1)\sin(x-nt)\right]dt.$$

et si l'on observe que

$$x=\frac{2}{\pi}\int_{-\infty}^{+\infty}\frac{\sin^2\frac{1}{2}tx}{t^2}\,dt,$$

la partie fractionnaire de x, (ou le reste de la division de p par q) sera

$$\frac{1}{\pi}\int_{-\infty}^{+\infty} dt \left[\frac{2\sin^2\frac{1}{2}tx}{t^2} + \frac{n-1}{2t}\sin(x-nt) - \frac{1}{2}\sin\left(x-\frac{n-1}{2}\right)t\,\frac{\sin\frac{n+1}{2}t}{t\sin\frac{t}{2}}\right],$$

$\left(\text{en remplaçant } x \text{ par } \frac{p}{q}\right)$

Voici une autre solution :

Considérons l'intégrale

$$\frac{1}{2\pi\sqrt{-1}}\int \frac{\pi\cos\pi z}{\sin\pi z}\,dz.$$

prise le long d'un cercle de rayon R décrit de l'origine comme centre. Elle est égale au nombre des racines de $\sin\pi x = o$ contenues dans ce cercle. Or si l'on suppose R compris entre les entiers n et $n+1$, il y aura $2n$ racines dans le cercle, donc la moitié de l'intégrale en question est le plus grand entier E (R) contenu dans R. Ainsi

$$E(R) = \frac{1}{4\sqrt{-1}}\int \frac{\cos\pi z}{\sin\pi z}\,dz,$$

ou

$$E(R) = \frac{1}{4}\int_0^{2\pi} \frac{\cos\pi Re^{\theta\sqrt{-1}}}{\sin\pi Re^{\theta\sqrt{-1}}} Re^{\theta\sqrt{-1}}\,d\theta.$$

Il est clair que l'on peut transformer l'intégrale en question de bien des manières.

6. — Sur la fonction $\varphi(N)$.

Nous désignerons par $\varphi(N)$ le nombre des entiers inférieurs et premiers à N, et nous ferons pour $N = 1$, $\varphi(1) = 1$.

Considérons l'équation indéterminée

$$y + x = N \qquad (1)$$

et ne considérons que les solutions positives et par suite inférieures à N, les N — 1 solutions sont évidemment

$$x = 1, 2, 3, \ldots, N - 1.$$
$$y = N - 1, N - 2, \ldots, 1.$$

soient a, b, c,... les facteurs premiers de N, et soit

$$N = a^{\alpha} b^{\beta} c^{\gamma} \ldots$$

cherchons le nombre des solutions de (1) dans lesquelles n'entre pas le facteur a, à cet effet cherchons d'abord celles dans lesquelles entre le facteur a et soit

$$x = ax', \; y = ay',$$

on aura

$$\frac{N}{a} = x' + y';$$

le nombre des solutions de cette équation est $\frac{N}{a} - 1$, il y a donc $N - \frac{N}{a} = N\left(1 - \frac{1}{a}\right)$ solutions de (1) ne contenant pas le facteur a. On verrait de même que le nombre des solutions ne renfermant pas le facteur b est $N\left(1 - \frac{1}{b}\right)$ et que le nombre des solutions ne renfermant pas ab est $N\left(1 - \frac{1}{ab}\right)$. Le nombre des solutions ne renfermant ni a, ni b, sera alors

$$N\left(1 - \frac{1}{a}\right) + N\left(1 - \frac{1}{b}\right) - N\left(1 - \frac{1}{ab}\right)$$

ou bien

$$N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right),$$

le nombre des solutions ne renfermant ni a, ni b, ni c sera

$$N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right) \text{ etc.}$$

or le nombre des solutions ne renfermant ni a, ni b, ni c,... est précisément $\varphi(N)$, on a donc

$$\varphi(N) = N\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\ldots$$

Corollaire 1°. Le nombre total des solutions de (1) est N. Or soit d un diviseur de N, $x' = \frac{x}{d}$, $y' = \frac{y}{d}$, on aura

$$\frac{N}{d} = x' + y'.$$

Le nombre des solutions de cette équation ne renfermant ni a, ni b,... est $\varphi\left(\frac{N}{d}\right)$; mais $\Sigma\ \varphi\left(\frac{N}{d}\right)$ est le nombre total des solutions de (1) et $\varphi\left(\frac{N}{d}\right) = \varphi(\delta)$, δ désignant le diviseur de N tel que $\delta d = N$, on a donc

$$\Sigma \varphi(\delta) = N.$$

δ désignant alors un diviseur quelconque de N.

Corollaire 2e. Si a, b, c... sont les facteurs de N premiers entre eux, on a

$$\varphi(N) = \varphi(abc...) = \varphi(a)\,\varphi(b)\,\varphi(c)...$$

cela résulte de la formule (2).

Voici une nouvelle méthode pour le calcul de $\varphi(n)$ que Cauchy appelle l'indicateur du nombre n.

Désignons par $J\frac{p}{q}$, 0 ou 1 suivant que $\frac{p}{q}$ est fractionnaire ou entier. On a évidemment

$$(1) \qquad E\left(\frac{n}{m}\right) = J\frac{1}{m} + J\frac{2}{m} + ... J\frac{n}{m},$$

$E\left(\frac{n}{m}\right)$ désignant l'entier contenu dans $\frac{n}{m}$, mais la formule suivante ou d_1, d_2... sont les diviseurs de x

$$n = \varphi(d_1) + \varphi(d_2) + ...$$

peut s'écrire

$$(2) \qquad n = J\frac{n}{1}\varphi(1) + J\frac{n}{2}\varphi(2) + J\frac{n}{3}\varphi(3)...,$$

Mais de (1) on tire

$$E\left(\frac{n}{m}\right) - E\left(\frac{n-1}{m}\right) = J\frac{n}{m},$$

donc (2) devient

$$n = \varphi(1)\left[\mathrm{E}\left(\frac{n}{1}\right) - \mathrm{E}\left(\frac{n-1}{1}\right)\right] + \varphi(2)\left[\mathrm{E}\left(\frac{n}{2}\right) - \mathrm{E}\left(\frac{n-1}{2}\right)\right] + \ldots$$

en faisant dans cette formule $n = 1, 2, 3\ldots$ on a des formules d'où l'on peut tirer $\varphi(n)$ sous forme de déterminant.

On peut aussi pour le même objet faire usage des formules telles que (2) et l'on a

$$\varphi(n) = \begin{vmatrix} 1 & 0 & 0 & \ldots & 1 \\ 1 & 1 & 0 & \ldots & 2 \\ 1 & 0 & 1 & \ldots & 3 \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{vmatrix}$$

Considérons le produit

$$(1 - x)(1 - x^2) \ldots (1 - x^{n-1}), = \mathrm{F}_n(x).$$

si α est racine primitive de $x^n - 1 = 0$, on aura

$$\begin{aligned} \mathrm{F}_n(\alpha) &= (1 - \alpha) \ldots (1 - \alpha^{n-1}) \\ &= (z - \alpha) \ldots (z - \alpha^{n-1}) \text{ pour } z = 1 \\ &= \frac{z^n - 1}{z - 1} \text{ pour } z = 1 \\ &= n \end{aligned}$$

si α n'est pas racine primitive, $\mathrm{F}_n(\alpha) = 0$; *or* $\varphi(n)$ est le nombre des racines primitives, donc

$$\frac{1}{n}\left[\mathrm{F}_n(\alpha) + \mathrm{F}_n(\alpha^2) \ldots + \mathrm{F}_n(\alpha^n)\right] = \varphi(n).$$

si α désigne une racine primitive.

Donc on peut mettre $\varphi(n)$ sous la forme

$$\frac{1}{2\pi\sqrt{-1}} \int \frac{1}{n} \mathrm{F}_n(z) \frac{nz^{n-1}}{z^n - 1} dz,$$

l'intégrale étant prise le long d'un cercle de rayon plus grand que 1 décrit de l'origine comme centre, ou

$$\varphi(n) = \frac{1}{2\pi\sqrt{-1}} \int \frac{(1 - z)\ldots(1 - z^{n-1}) z^{n-1} dz}{z^n - 1}$$

7. — Sur les diviseurs d'un nombre

Soit N un entier, a, b, c... ses facteurs premiers, en sorte que

$$N = a^{\alpha} b^{\beta} c^{\gamma} \ldots$$

les diviseurs de N sont a, b, c... ab, ac,... c'est-à-dire les termes du produit

$$(1) \qquad (1 + a + a^2 \ldots + a^{\alpha})(1 + b + \ldots b^{\beta}) \ldots$$

ou

$$\frac{a^{\alpha+1} - 1}{a - 1} \frac{b^{\beta+1} - 1}{b - 1} \frac{c^{\gamma+1} - 1}{c - 1} \ldots$$

Soient S_0, S_1... S_i... les sommes des puissances o, 1,... i... de ses diviseurs, les puissances i de ses diviseurs seront les termes du produit

$$(1 + a^i + \ldots a^{\alpha i})(1 + b^i + \ldots b^{\beta i}).$$

ou

$$\frac{a^{\alpha i + i} - 1}{a^i - 1} \frac{b^{\beta i + i} - 1}{b^i - 1} \ldots$$

on aura donc

$$S_i = \frac{a^{\alpha i + i} - 1}{a^i - 1} \frac{b^{\beta i + i} - 1}{b^i - 1} \ldots ;$$

en particulier la somme de ses diviseurs S_1 sera l'expression (1). Le nombre S_0 de ses diviseurs sera le nombre des termes du produit (1), on aura donc

$$S_0 = (\alpha + 1)(\beta + 1)(\gamma + 1) \ldots$$

Les formules de Newton permettront alors de calculer les fonctions symétriques $\Sigma a^i b^j$, $\Sigma a^i b^j c^k$... et même le produit abc... de tous les diviseurs. Mais on peut calculer ce produit directement comme il suit :

Le facteur a entre dans $(\beta + 1)(\gamma + 1)$... diviseurs, lesquels sont les diviseurs de $\frac{N}{a^{\alpha}}$ a le facteur a, le facteur a^2... y entrent le même nombre de fois, etc., donc dans le produit P

des diviseurs a entrera $(\beta+1)(\gamma+1)\ldots$ fois ; posant alors

$$p=(\alpha+1)(\beta+1)(\gamma+1)\ldots$$

a entrera dans le produit P avec l'exposant $\frac{p}{\alpha+1}$, a^2 avec le même exposant... on aura donc

$$P=a^{\frac{p}{\alpha+1}(1+2+\ldots\alpha)}\ldots$$

ou

$$P=a^{\frac{\alpha(\alpha+1)}{2}\frac{p}{\alpha+1}}\ldots=\sqrt{a^{p}b^{p}\ldots}$$

$$=(ab\ldots)^{\frac{p}{2}}=N^{\frac{p}{2}}.$$

Connaissant S_0, S_1... il ne serait pas difficile d'écrire un polynôme entier ayant pour racines les diviseurs de N.

Nous allons maintenant essayer d'interpoler la fonction numérique S_p en considérant N comme la variable.

Considérons la fonction

$$\frac{x}{1-x}+\frac{x^2}{1-x^2}\ldots+\frac{x^n}{1-x^n}+\ldots=\varphi(x),$$

définie pour toutes les valeurs de mod. $x<1$, on a

$$\begin{aligned}\varphi(x)=x&+x^2+x^3+x^4+\ldots\\&+x^2+x^4+x^6+x^8+\ldots\\&+x^3+x^6+x^9+x^{12}+.\\&\ldots\ldots\ldots\ldots\end{aligned}$$

le coefficient de x^N sera précisément le nombre S_0 des diviseurs de N. Le coefficient de x^N dans $\frac{d}{dx}x\,\varphi(x)$ sera S_1, le coefficient de x^N dans $\frac{d}{dx}x\frac{d}{dx}x\,\varphi(x)$ sera S_2 et ainsi de suite.

Autrement : considérons le produit

$$\frac{\sin\pi x}{\pi x}\cdot\frac{\sin\pi\frac{x}{2}}{\pi\frac{x}{2}}\ldots\frac{\sin\pi\frac{x}{n}}{\pi\frac{x}{n}}\ldots=\psi(x)$$

qui est évidemment convergent, il s'annule pour $x=n$, un

nombre de fois égal au nombre des diviseurs de n, donc en vertu du théorème de Cauchy sur les racines de $\varphi(x)$

$$S_p = \frac{1}{2\pi\sqrt{-1}} \int \frac{\psi'(x)}{\psi(x)} x^p \, dx.$$

l'intégrale étant prise le long d'un contour suffisamment petit enveloppant le point n.

8. — Intégrales et dérivés des fonctions numériques

Soient 1, d_1, d_2... n les diviseurs de n, posons

$$\varphi(n) = f(1) + f(d_1) + f(d_2) \ldots + f(n) \tag{1}$$

$\varphi(n)$ sera l'intégrale de f suivant les diviseurs de n et $f(n)$ sera la dérivée de $\varphi(n)$.

De (1) on tire

$$\begin{cases} \varphi(1) = f(1), \\ \varphi(2) = f(1) + f(2), \\ \varphi(3) = f(1) + f(3), \\ \varphi(4) = f(1) + f(2) + f(4), \\ \ldots\ldots\ldots\ldots \end{cases} \tag{2}$$

d'où l'on tire $f(1)$, $f(2)$,... en fonction de $\varphi(1)$, $\varphi(2)$... Pour résoudre ces équations, nous suivrons la marche suivante indiquée par M. Tchebychef.

Soit $F(n)$ une fonction nulle pour $n = 2, 3, 4\ldots$ et égale à 1 pour $n = 1$. Soient 1, d_1... n les diviseurs de n, on aura

$$F(1) = 1,$$
$$\Sigma F(d) = 1, \text{ pour } n > 1.$$

soit $\mu(n)$ la dérivée de $F(n)$ suivant les diviseurs de n. on aura

$$\mu(1) = 1, \tag{3}$$
$$\Sigma \mu(n) = 0. \tag{4}$$

Soit $n = a^\alpha b^\beta c^\gamma \ldots$ le nombre n décomposé en facteurs premiers, r le nombre des entiers a, b,...

Les diviseurs de n qui ne contiennent que des facteurs simples sont

$$1\,;\ a,\ b,\ldots\,;\ ab,\ ac\ldots\,;\ abc\ldots\ bcd\ldots\,;\ abc\ldots\ l,$$

leurs nombres sont

$$\begin{array}{rl} 1 & \text{facteur du degré 0,} \\ r & \text{—} \quad \text{—} \quad 1, \\ \dfrac{r(r-1)}{1.2} & \text{—} \quad \text{—} \quad 2, \\ \ldots\ldots\ldots\ldots & \end{array}$$

Les équations (3), (4) analogues à (2) déterminent complètement les quantités $\mu(1)$, $\mu(2)\ldots$ sans ambiguité, il suffit d'en trouver une solution.

Or je dis qu'on y satisfait en prenant $\mu(n) = 0$, quand n contient des facteurs premiers multiples, $\mu(n) = +1$ quand n ne contient que des facteurs premiers simples en nombre pair, et $\mu(n) = -1$, quand n n'a que des facteurs simples en nombre impair.

Or $\mu(n)$ lorsqu'il est nul et que n a des facteurs multiples n'introduit pas de termes dans la formule (4) le nombre des diviseurs fournissant la valeur 1 de μ est

$$1 + \frac{r(r-1)}{1.2} + \frac{r(r-1)\ (r-2)\ (r-3)}{1.2.3.4} \ldots$$

le nombre des diviseurs fournissant la valeur -1 de μ est

$$\frac{r}{1} + \frac{r(r-1)\ (r-2)}{1.2.3} + \ldots$$

il en résulte bien pour les valeurs de μ adoptées

$$\Sigma\mu(n) = 1 - \frac{r}{1} + \frac{r(r-1)}{1.2} - \ldots = (1-1)^r = 0.$$

Cela posé, pour résoudre le système (2), multiplions les équations de rang $1, d_1, d_2\ldots n$ par $\mu\left(\frac{n}{1}\right)$, $\mu\left(\frac{n}{d_1}\right)\ldots\ \mu(1)$ et ajoutons, le coefficient de $f(d)$ est, en désignant par δ un diviseur de $\frac{n}{d_i}$

$$\mu\left(\frac{n}{d_i}\right) + \mu\left(\frac{n}{d_i\,\delta}\right) + \ldots\ \mu(1) = \begin{cases} 1 \text{ si } d_i = n \\ 0 \text{ si } d_i < n \end{cases}$$

on en conclut :

$$(A) \qquad f(n) = \Sigma \mu\left(\frac{n}{d}\right) \varphi(d).$$

Les applications de cette formule sont nombreuses, considérons l'équation identique

$$\begin{aligned} f(1)\,\frac{x}{1-x} + f(2)\,\frac{x^2}{1-x^2} + f(3)\,\frac{x^3}{1-x^3} + \ldots \\ = f(1)\,(x + x^2 + x^3 + x^4 \ldots) \\ + f(2)\,(x^2 + x^4 + x^6 + \ldots) \\ + \ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Le coefficient de x^n dans le second nombre est $\Sigma f(d)$, d désignant un diviseur de n. On a donc

$$(B) \quad \left\{ \begin{array}{l} f(1)\,\dfrac{x}{1-x} + f(2)\,\dfrac{x^2}{1-x^2} + \ldots \\ = x f(1) + x^2 \ldots + x^n\,\Sigma f(d_n) + \ldots \end{array} \right.$$

d_n désignant un diviseur de n.

Or, en vertu de la formule (A) que nous venons de démontrer, on pourra aussi écrire

$$(C) \qquad \sum\left(\frac{x^n}{1-x^n}\sum \mu\left(\frac{n}{d}\right)\varphi(d)\right) = \sum x^n \varphi(n).$$

Si l'on prend $\varphi(n) = \mu(x)$ on a

$$x = \frac{x}{1-x} - \frac{x}{1-x^2} - \frac{x^3}{1-x^3} - \frac{x^5}{1-x^5} + \frac{x^6}{1-x^6} \ldots,$$

si $f(n) =$ quand n est carré et nul dans le cas contraire on a

$$x + x^4 + x^9 + \ldots = \frac{x}{1-x} - \frac{x^2}{1-x^2} - \frac{x^3}{1-x^3} + \frac{x^4}{1-x^4} \ldots$$

Si dans (B) on prend $f(n)$ égal à l'indicateur de n on a

$$f(1)\,\frac{x}{1-x} + f(2)\,\frac{x^2}{1-x^2} + \ldots = x + 2x^2 \ldots + nx^n + \ldots = \frac{x}{(1-x)^2}.$$

Il existe un grand nombre d'autres applications des for-

mules (B) et (C). Mais ces applications sont plus curieuses qu'utiles.

9. — Autres formules de M. Tchebychef

Supposons que l'on ait

$$f(x) = F(x) + F(2x) \ldots + F(nx) \ldots \tag{1}$$

proposons-nous de calculer F(1) et posons

$$F(1) = A_1 f(1) + A_2 f(2) \ldots + A_n f(n) + \ldots$$

pour déterminer A_1, A_2... remplaçons $f(1)$, $f(2)$... par leurs valeurs tirées de (1), nous aurons :

$$F(1) = A_1 [F(1) + F(2) + \ldots] + A_2 [F(2) + F(4) + \ldots] + \ldots \tag{2}$$

d'où l'on tire la solution

$$A_1 = 1,\ A_2 + 1 = 0,\ A_3 + 1 = 0,\ A^4 + A_2 + 1 = 0,$$

1° Si n est premier, $A_n + 1 = 0$, $A_n = -1$.

2° Si n est le produit de plusieurs nombres premiers tous différents $a, b, \ldots k, l$, le coefficient de $F(n)$ sera $A_\alpha + A_\beta + A_\gamma + \ldots + 1 = 0$, voyons ce que seront les nombres α, β... La formule (2) montre que $A_1 = 1$ est un terme des coefficients de $F(n)$, A_2 n'y entre que si n est divisible par 2,... A_α n'y entre que si n est divisible par α... donc α, β... sont les diviseurs de n. Parmi ces diviseurs considérons ceux qui ne contiennent pas l, soient α', β'... ces diviseurs on a

$$A_{\alpha'} + A_{\beta'} \ldots + 1 = 0,$$

il reste donc

$$\Sigma A_{\delta'} = 0,$$

δ' désignant un diviseur de $\frac{n}{l}$. Si le nombre des facteurs se réduit à deux k et l, la formule précédente donne

$$A_k + 1 = 0, \quad A_n = -1;$$

si le nombre des facteurs se réduit à trois j, k, l on a

$$A_{kl} + A_k + A_l = 0, \quad A_n = 1,$$

etc., donc A_n en général est égal à $(-1)^\varepsilon$, ε désignant le nombre des facteurs $a, b, \ldots l$.

3° Si $n = \alpha p^m$, p étant un nombre premier, on a

$$\Sigma A p^{m\delta} \delta = 0,$$

δ désignant un diviseur de α, si $\alpha = 1$, $A_n = 0$, donc il est nul pour $\alpha = 2, 3\ldots$ donc A_n est nul si n est divisible par des facteurs premiers multiples.

10. — Digression sur les nombres parfaits

Un nombre n est *parfait*, quand il est égal à la somme de ses diviseurs (non compris n, bien entendu). Il est *déficient* s'il est plus petit que la somme de ses diviseurs, *abondant* s'il est plus grand. Soit $\Sigma(n)$ la somme des diviseurs de n y compris n, si

$$n = a^\alpha b^\beta c \ldots$$

$a, b, c\ldots$ étant premiers, nous venons de voir que

$$(1) \qquad \Sigma(n) = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdots$$

Enfin on peut écrire (1) ainsi :

$$(2) \qquad \Sigma(n) = a^\alpha b^\beta \ldots \left[\frac{\left(a - \frac{1}{a^\alpha}\right)\left(b - \frac{1}{b^\beta}\right)\cdots}{(a-1)(b-1)} \right],$$

ou

$$\frac{n}{\Sigma(n)} = \frac{(a-1)(b-1)\ldots}{\left(a - \frac{1}{a^\alpha}\right)\left(b - \frac{1}{b^\beta}\right)\cdots},$$

donc

$$(3) \qquad \frac{n}{\Sigma(n)} > \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\cdots$$

On a encore en appelant $1, d_1, d_2, \ldots n$ les diviseurs de n

$$\Sigma(n) = 1 + d_1 + \ldots + d_n + n,$$

et

$$\frac{\Sigma(n)}{n} = \frac{1}{n} + \frac{d_1}{n} + \ldots \frac{d_n}{n} + 1.$$

mais les diviseurs pouvant être conjugués deux à deux de manière à ce que leur produit fasse n, on a aussi

$$\frac{\Sigma(n)}{n} = \frac{1}{n} + \frac{1}{d_1} + \frac{1}{d_2} \dots + \frac{1}{1}. \tag{4}$$

Théorème 1. — *Un nombre est abondant, parfait ou déficient, suivant que la somme des inverses de ses diviseurs est plus grande que 2, égale à 2 ou plus petite que 2.*

Cela résulte de la formule (4), en effet s'il est abondant $\Sigma(n) > 2\ n$ ou $\frac{\Sigma n}{n} > 2$, etc.

Théorème 2. — *Tout nombre qui est divisible par un nombre parfait ou abondant est abondant.*

Soit en effet p un diviseur parfait ou abondant de n, on a

$$\frac{\Sigma(p)}{p} \geq 2;$$

mais n admet p pour diviseur, donc la somme des inverses des diviseurs de n est plus grande que la somme des inverses des diviseurs de p, donc

$$\frac{\Sigma(n)}{n} > \frac{\Sigma(p)}{p},$$

et $\frac{\Sigma(n)}{n} > 2$, donc, etc. c. q. f. d.

Soient a, b,... l les facteurs premiers de n, on a [formule (3)]

$$\frac{n}{\Sigma(n)} > \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \dots \left(1 - \frac{1}{l}\right),$$

et par suite si n n'est pas deficient

$$\frac{1}{2} > \left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right) \dots \left(1 - \frac{1}{l}\right).$$

11. — Limites des nombres parfaits

Tout nombre de la forme p^α, p étant premier, est déficient.

En effet,

$$\Sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1};$$

or

$$2p^{\alpha} > \frac{p^{\alpha+1}-1}{p-1},$$

ou

$$2p^{\alpha+1} - 2p^{\alpha} > p^{\alpha+1} - 1,$$

si :

$$\alpha \geq 2$$

ou si $\alpha \leq 2$,

$$p^{\alpha+1} > 2p^{\alpha} - 1,$$

donc, etc.. c. q. f. d.

Tous les nombres parfaits ou abondants de la forme $a^{\alpha}b^{\beta}$ sont pairs, les nombres parfaits sont de la forme

$$2^n(2^{n+1}-1),$$

$2^{n+1}-1$ *étant premier.*

En effet l'inégalité

$$\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right) < \frac{1}{2}$$

n'est pas vérifiée pour $a = 3$, $b = 5$, ni *a fortiori*, pour des valeurs premières de a et b supérieures. Il reste à trouver les nombres parfaits de la forme $2^n a^{\alpha}$, or

$$\Sigma(2^n a^{\alpha}) = (2^{n+1}-1)\frac{a^{\alpha+1}-1}{a-1},$$

et pour que ce nombre ne soit pas déficient, il faut que

$$2^{n+1}a^{\alpha} \leq (2^{n+1}-1)\frac{a^{\alpha+1}-1}{a-1},$$

ou

$$a^{\alpha+1} - 2^{n+1}a^{\alpha} + 2^{n+1} - 1 \leq 0.$$

Considérons alors le polynôme

$$\varphi(x) = x^{\alpha+1} - 2^{n+1}x^{\alpha} + (2^{n+1}-1).$$

Ce polynôme n'a que deux variations, c'est-à-dire qu'il a au plus deux racines positives, l'une d'elles est évidemment

égale à 1 ; quant à l'autre il est facile de voir qu'elle est comprise entre $2^{n+1} - 1$ et 2^{n+1}.

Le nombre $2^n a^\alpha$ ne peut être parfait que si a est racine de $\varphi(x) = 0$, or a étant premier, on doit avoir $a = 2^{n+1} - 1$ et $\alpha = 1$. Les nombres parfaits de la forme $a^\alpha b^\beta$ sont donc de la forme

$$2^n (2^{n+1} - 1).$$

En second lieu soit $2^n \mu$ un nombre pair, μ n'étant plus divisible par 2, on aura :

$$\Sigma (2^n \mu) = \Sigma (2^n) \Sigma (\mu) = (2^{n+1} - 1) \Sigma (\mu);$$

pour que $2^n \mu$ soit parfait, il faut alors que

$$2^{n+1} \mu = (2^{n+1} - 1) \Sigma (\mu);$$

donc $2^{n+1} - 1$ doit être premier, car s'il admettait un diviseur, ce diviseur ne pouvant être 2, diviserait μ, $2^n \mu$ admettait le diviseur 2^n qui est abondant, et $2^n \mu$ serait lui-même abondant. $2^{n+1} - 1$ étant premier, divise μ, $2^n \mu$ admet alors le diviseur $2^n (2^{n+1} - 1)$ qui est parfait, $2^n \mu$ est donc égal à son diviseur $2^n \mu (2^{n+1} - 1)$, car tout nombre parfait n'a d'autre diviseur parfait que lui-même.

Les questions traitées dans les paragraphes précédents sont extraites d'un travail intéressant de M. Bourlet (*Nouvelles annales de mathématiques*, juillet 1896) on y trouve le théorème suivant :

Il n'existe aucun nombre parfait de la forme $a^\alpha b^\beta c^\gamma$; a, b, c étant premiers impairs.

CHAPITRE II

ANALYSE INDÉTERMINÉE DU PREMIER DEGRÉ

1. — Préliminaires

L'analyse indéterminée du premier degré a pour but la résolution en nombres entiers des équations du premier degré dont le nombre est inférieur à celui des inconnues.

1° Nous considérerons d'abord le système

$$ax = by = cz \ldots = dt.$$

Une solution est évidemment donnée par la formule

$$ax = by \ldots = dt = \mu$$

μ désignant le plus petit multiple de a. b, ... d, car μ doit être évidemment un multiple de a, b,... d ; les autres solutions s'obtiendront en prenant des multiples des valeurs trouvées pour celle-ci.

2° Si l'on considère le système

$$\frac{x}{a} = \frac{y}{b} = \ldots \frac{d}{t}$$

on le résoudra en posant :

$$x = \frac{a}{\Delta}, \quad y = \frac{b}{\Delta} \ldots \quad t = \frac{d}{\Delta},$$

Δ désignant le plus grand commun diviseur de a, b,... d, on aura les autres solutions en multipliant celles-ci par des nombres quelconques.

3° Si l'on considère $m - 1$ équations homogènes entre m inconnues

$$a_{11}x_1 + a_{12}x_2 \ldots a_{1m}x_m = 0,$$

. . . . . .

$$a_{m-1,1}x_1 + a_{m-1,2}x_2 \ldots a_{m-1,m}x_m = 0,$$

on les résoudra en les mettant sous la forme

$$\frac{x_1}{A_1} = \frac{x_2}{A_2} \cdots = \frac{x_m}{A_m}.$$

2. — Résolution de l'équation $a_1 x_2 + a_2 x_1 = b$.

L'équation du premier degré à deux inconnues peut se mettre sous la forme

(1) $$a_1 x_2 + a_2 x_1 = b,$$

a_1, a_2, b désignant des nombres n'ayant aucun facteur commun. Pour que cette équation admette des solutions entières il faut que a_1 et a_2 soient alors premiers entre eux ; car tout diviseur commun à a_1 et a_2 devrait diviser b. Nous supposerons donc a_1 et a_2 premiers entre eux.

Première solution. Soit $a_1 > a_2$: divisons a_1 par a_2, soit q_2 le quotient et a_3 le reste, nous aurons :

(1)' $$a_1 = a_2 q_2 + a_3$$

et alors (1) deviendra

$$(a_2 q_2 + a_3) x_2 + a_2 x_1 = b,$$

ou

(2) $$a_3 x_2 + a_2 x_3 = b,$$

en posant pour abréger

(1)'' $$x_3 = q_2 x_2 + x_1,$$

et l'équation (2) est de même forme que (1) ; mais elle a des coefficients plus petits ce qui est plus avantageux.

Divisant alors a_2 par a_3 on posera

(2)' $$a_2 = a_3 q_3 + a_4,$$

(2) deviendra

$$(a_3 q_3 + a_4) x_3 + a_3 x_2 = b,$$

ou bien

(3) $$a_3 x_4 + a_4 x_3 = b,$$

en posant

$$x_4 = q_3 x_3 + a_3 x_2, \tag{2}''$$

on fera alors

$$a_3 = a_4 q_4 + a_5, \tag{3}'$$

on aura

$$(a_4 q_4 + a_5) x_4 + a_4 x_3 = b,$$

ou

$$a_4 x_4 + a_5 x_4 = b, \tag{4}$$

et ainsi de suite. Les formules (1)', (2)', (3)'... montrent que a_1, a_2, a_3 ... sont les restes successifs que l'on rencontre dans la recherche du plus grand commun diviseur de a_1 et a_2, l'un d'eux finira donc par devenir nul, le précédent étant égal à l'unité, puisque a_1 et a_2 sont premiers entre eux. Supposons par exemple $a_5 = 1$, x_5 pourra être choisi arbitrairement, et l'on aura

$$x_4 = b - a_4 x_5.$$

L'équation (4) ayant fait connaître x_4 et x_5, l'équation (3) fera connaître x_3 à savoir :

$$x_3 = \frac{b - a_5 x_4}{a_4}$$

Cette valeur de x_3 est entière, pour s'en convaincre, il suffit de remplacer a_3 par sa valeur (3') et l'on a

$$x_3 = \frac{b - (a_4 q_4 + a_5) x_4}{a_4} = \frac{b - a_5 x_4}{a_4} - q_4 x_4,$$

ou en vertu de (4)

$$x_3 = a_4 x_5 - x_4 q_4.$$

l'équation (2) donnera x_2 et (1) fera connaître x_1 et l'on prouvera comme on l'a fait pour x_3 que x_2 et x_1 sont entiers.

Seconde solution. — Cette solution est identique au fond, à la précédente, mais elle l'explique; réduisons $\frac{a_1}{a_2}$ en fraction

continue ; comme a_1 et a_2 sont premiers entre eux, la dernière réduite sera $\frac{a_2}{a_1}$, en appelant $\frac{c_2}{c_1}$ l'avant-dernière on aura

$$a_2 c_1 - c_2 a_1 = \pm 1,$$

on en tire

$$a_2(\pm c_1 b) - (\pm c_2 b) a_1 = b ;$$

on satisfera donc à l'équation proposée en prenant

$$x_1 = \pm c_1 b \text{ et } x_2 = \mp c_2 b.$$

Nous ferons bientôt connaître d'autres moyens plus expéditifs pour résoudre l'équation (1). Nous voyons qu'elle admet toujours une solution quand a_1 et a_2 sont premiers entre eux, il reste à montrer comment d'une solution on peut déduire toutes les autres.

Soit : $x_1 = x_1^0$, $x_2 = x_2^0$ une solution, nous aurons :

$$a_2 x_1^0 + a_1 x_2^0 = b ;$$

de cette équation et de (1) on tire :

$$a_2(x_1 - x_1^0) + a_1(x_2 - x_2^0) = 0,$$

a_1 et a_2 étant premiers entre eux, a_1 doit diviser $x_1 - x^0$ donc il faut que l'on ait

$$x_1 - x_1^0 = k a_1,$$

k étant un entier et l'on a la solution générale

$$x_1 = x_1^0 + k a_1, \; x_2 = x_2^0 - k a_2 ;$$

les solutions forment donc des progressions arithmétiques, ayant pour raison a_1 et $- a_2$.

3. — Résolution des équations a plusieurs inconnues

Considérons d'abord un système de m équations à $m + 1$ inconnues, on pourra résoudre ce système par rapport à m des inconnues et il prendra la forme suivante :

$$\begin{aligned} a_1 x_1 &= A_1 t + z_1, \\ a_2 x_2 &= A_2 t + z_2, \\ &\cdots\cdots\cdots \\ a_m x_m &= A_m t + z_m, \end{aligned}$$

ou $a_1, a_2 \ldots A_1, A_2 \ldots \alpha_1, \alpha_2 \ldots$ sont des entiers connus et ou $x_1, x_2 \ldots x_m, t$ désignent les inconnues.

Pour résoudre le système on s'occupera d'abord de la première équation et l'on exprimera x_1 et t au moyen d'une variable auxiliaire t_1 (la variable k du paragraphe précédent) on remplacera t par sa valeur exprimée en t_1, et on n'aura plus que $m - 1$ équations à résoudre ; on procédera sur celles-ci comme sur le système complet et ainsi de suite.

Considérons en second lieu *une* équation de la forme

$$a_1x_1 + a_2x_2 + \ldots a_nx_n = b ; \tag{1}$$

on pourra simplifier cette équation comme il suit : Soit a_1 le plus petit coefficient, posons

$$a_2 = a_1q_2 + a'_2, \qquad a_3 = a_1q_3 + a'_3, \ldots \tag{1 bis}$$

q_2 , q_3 ... étant les quotients de la division de a_2 par a_1 , de a_3 par a_1 etc... la formule (1) s'écrira

$$a_1x_1 + (a_1q_2 + a'_2)\, x_2 \ldots\ldots (a_1q_n + a'_n)\, x_n = b$$

posons

$$x_1 + q_2x_2 + \ldots q_nx_n = x'_1 \tag{2}$$

nous aurons

$$a_1x'_1 + a'_2x_2 + \ldots a'_nx_n = b \tag{3}$$

Si cette équation est résolue, en vertu de (2) x_1 sera connue sous forme entière, or l'équation (3) est plus simple que (1), on la remplacera à son tour par une autre plus simple et ainsi de suite jusqu'à ce que l'un des coefficients prenne la valeur 1, l'inconnue correspondante s'en déduira sous forme entière en donnant aux autres des valeurs arbitraires.

Cette méthode tombera en défaut, si le coefficient d'une inconnue s'annule dans la suite des opérations avant de se réduire à 1. Voyons si ce cas peut se présenter.

On peut toujours supposer que les a n'ont pas de facteur commun, car il devrait diviser b et on peut supposer que l'on a supprimé ce facteur. Cela posé $a_1, a'_1, \ldots a'_3$ n'ont pas de facteur commun, car il devrait en vertu de (1 bis) diviser $a_1, a_2 \ldots a_n$; donc les transformées successives de (1) sont

telles que les coefficients des x n'ont pas de facteur commun ; en outre tous les a' ne peuvent être nuls sans quoi a_1 diviserait les autres a.

En résumé, si $a_1, \ldots a^n$ n'ont pas de diviseur commun, il restera au moins deux coefficients non nuls quand l'un d'eux sera égal à 1, donc l'équation (1), si les a sont premiers dans leur ensemble *admettra une solution où l'un des x sera fonction linéaire à coefficients entiers des autres*.

Supposons que l'on connaisse une solution de (1). Soit

$$x_1 = x_1^0,\ x_1 = x_2^0 \ldots x_n = x_n^0$$

cette solution, on aura

$$a_1 x_1^0 + \ldots a_n x_n^0 = b,$$

et en vertu de (1) :

$$a_1 (x_1 - x_1^0) + \ldots + a_n (x_n - x_n^0) = 0. \tag{4}$$

On satisfera à cette équation de la manière suivante : $b_1 \ldots c_1 \ldots$ désignant des entiers arbitraires, on posera

$$\Delta = \begin{vmatrix} a_1 a_2 \ldots a_n \\ b_1 b_2 \ldots b_n \\ \ldots\ldots \\ l_1 l_2 \ldots l_n \end{vmatrix}$$

il est clair que l'on pourra prendre

$$x_1 = x_1^0 + \frac{\partial \Delta}{\partial b_1},\ x_2 = x_2^0 + \frac{\partial \Delta}{\partial b_2} \ldots$$

ou

$$x_1 = x_1^0 + \frac{\partial \Delta}{\partial c_1},\ x_2 = x_2^0 + \frac{\partial \Delta}{\partial c_2} \ldots$$

Toutefois, il est bon d'observer que la solution générale de l'équation (1) dépend de $n - 1$ paramètres distincts seulement ; en effet nous avons vu que l'on pouvait remplacer (1) par une équation où le coefficient a_1 de x_1 pouvait être réduit à l'unité en remplaçant les inconnues par d'autres fonctions linéaires de celles-ci, mais alors si $a_1 = 1$ on pourra se donner tous les $x - x^0$, sauf $x_1 - x_1^0$ qui sera fonction linéaire des autres différences $x - x^0$. Ces solutions dépendront donc de $n - 1$ paramètres seulement.

Considérons enfin un système de m équations à $m + n$ inconnues, on pourra le résoudre par rapport à m inconnues $x_1 \dots x_m$ et le mettre sous la forme

$$a_1 x_1 = \gamma_{1,} t_1 + \dots \gamma_{1n} t_n + \gamma_{1,n+1}$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$a_m x_m = \gamma_{m1} t_1 + \dots \gamma_{mm} t_n + \gamma_{m,n+1}$$

les a et les x désignant des entiers et t désignant des inconnues.

On commencera par calculer les solutions de la première équation, qui seront fonctions linéaires de n indéterminées. comme on vient de le voir, on portera dans les autres équations à la place de t_1, t_2... leurs valeurs exprimées en fonction des indéterminées, on aura ainsi $m - 1$ équations que l'on traitera comme le système primitif jusqu'à ce que l'on parvienne à une seule équation.

En résumé :

Étant donné un système d'équations du premier degré à coefficients entiers, contenant plus d'inconnues que d'équations, s'il est possible de les résoudre en nombres entiers, les inconnues seront fonctions linéaires de paramètres auxquels on pourra donner des valeurs entières quelconques.

4. — Partition des nombres

La partition des nombres a pour but de trouver le nombre des solutions positives des équations indéterminées du premier degré ; c'est un problème facile à résoudre dans chaque cas particulier, abstraction faite de la longueur des calculs, mais difficile si l'on veut une solution algébrique.

Ainsi par exemple, le nombre des solutions positives et entières de :

$$a_1 x_1 + a_2 x_2 \dots + a_n x_n = b$$

est égal (en supposant bien entendu $a_1 \dots b$ entiers et positifs) au coefficient de z^b dans :

$$F(z) = (1 + z^{a_1} + z^{2a_1} + \dots)(1 + z^{a_2} + z^{2a_2} \dots) \dots$$

$$= \frac{1}{(1 - z^{a_1})(1 - z^{a_2})(1 - z^{a_3}) \dots}$$

on trouvera ce coefficient en décomposant $F(z)$ en éléments simples et en développant chaque élément.

De même pour trouver le nombre des solutions entières et positives de

$$a_1x_1 + a_2x_2 \ldots + a_nx_n = \alpha,$$
$$b_1x_1 + b_2x_2 \ldots + b_nx_n = \beta,$$
$$c_1x_1 + c_2x_2 \ldots + c_nx_n = \gamma.$$

il suffira de calculer le coefficient $u^\alpha v^\beta w^\gamma$ dans

$$\frac{1}{(1 - u^{a_1}v^{b_1}w^{c_1})(1 - u^{a_2}v^{b_2}w^{c_2})\ldots}$$

on trouverait d'une manière analogue le nombre des solutions de

$$a_1x + a_2x_2 \ldots + a_nx_n = \alpha$$

comprises entre des limites données; si a_1, $a_2 \ldots$ α n'étaient pas des nombres positifs, le coefficient de z^α dans l'expression

$$(z^{-l_1a_1} + z^{-(l_1+1)a_1} \ldots + z^{m_1a_1})(z^{-l_2a_2} + \ldots z^{m_2a_2}) \ldots$$

serait le nombre des solutions dans lesquelles on aurait

$$-l_1 < x_1 < m_1,$$
$$-l_2 < x_2 < m_2,$$
$$\ldots\ldots\ldots$$

et le calcul de ce coefficient se ramènerait à décomposer une fraction rationnelle en éléments simples.

Mais ces solutions fort simples en théorie, sont presque impossibles à réaliser dans la pratique. Nous verrons cependant qu'elles peuvent avoir leur utilité.

Reprenons l'équation à deux inconnues et mettons-la sous la forme

$$ax + by = c,$$

a, b, c étant des entiers donnés. Soient ξ, η une solution, en appelant t un entier, on aura :

$$x = \xi + at,\ y = \eta - at,$$

et pour que la solution η, ξ soit positive, il faudra que

$$\xi + bt > 0,\ \eta - at > 0,$$

et t devra satisfaire à la double condition

$$bt > -\zeta, \quad at < \tau_1,$$

si a et b sont positifs on aura

$$\frac{\tau_1}{a} > t > -\frac{\zeta}{b},$$

ou

$$\frac{\tau_1 b}{ab} > t > -\frac{\zeta a}{ab},$$

et t sera le plus grand entier contenu dans

$$\frac{\tau_1 b + a\zeta}{ab};$$

et comme $\tau_1 b + a\zeta = c$, ce sera le plus grand entier contenu dans $\frac{c}{ab}$, c'est le nombre cherché.

a et b ont été supposés positifs, si b par exemple était négatif on n'aurait plus $t > -\frac{\zeta}{b}$, mais $t < -\frac{\zeta}{b}$, mais on aurait toujours une limite $t > \frac{b}{\zeta}$ de t, avec $t < \frac{\tau_1}{a}$, mais la solution serait moins élégante.

La même méthode est encore applicable quel que soit le nombre des inconnues, bornons-nous à considérer l'équation

$$ax + by + cz = d.$$

soit ξ, τ_1, ζ une solution, si a', b', $c' = 1$ désignent trois arbitraires en réalité réduits à deux puisque $c' = 1$, on aura

$$x = \xi + (bc' - cb'),$$
$$y = \tau_1 + (ca' - ac'),$$
$$z = \zeta + (ab' - ba').$$

en écrivant que

$$\xi + (bc' - cb') > 0,$$
$$y + (ca' - ac') > 0,$$
$$\zeta + (ab' - ba') > 0,$$

on aura trois inégalités pour déterminer a' et b'.

Mais les considérations développées au commencement de

ce paragraphe ne sont pas tout à fait inutiles, elles donnent facilement une solution approchée de la question, quand le second membre N de l'équation

$$a_1 x_1 + a_2 x_2 \ldots + a_n x_n = N$$

est un très grand nombre, en vertu de la remarque suivante due à Laguerre :

Si a_1, a_2... sont des entiers positifs, il faut, comme on l'a vu, trouver le coefficient de x^N dans

$$F(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2})\ldots}.$$

Or, si l'on décompose $F(z)$ en éléments simples, on aura des éléments de la forme

$$\frac{A}{z - \alpha};$$

et si les nombres a_1, a_2... sont premiers deux à deux des éléments de la forme

$$\frac{B}{(z-1)^p},$$

α désignant des racines de l'unité. Or le coefficient de z^N, dans la partie

$$\Sigma \frac{A}{z - \alpha_1}$$

donnera une quantité finie $\Sigma A \alpha^{-N-1}$, car le module de cette quantité est moindre que Σ mod. A, puisque le module de α est égal à 1. Si donc N est un grand nombre, on pourra se borner à calculer les quantités B.

Si les a n'étaient pas premiers entre eux deux à deux, on pourrait encore évidemment faire usage du même principe, mais il y aurait à calculer quelques coefficients A provenant de racines imaginaires qui pourraient être multiples.

5. — Sur les fractions

soit $\frac{a}{b}$ une fraction irréductible. Supposons b décomposé en deux facteurs p, q premiers entre eux et par suite avec a. Posons

$$\frac{a}{pq} = \frac{x}{p} + \frac{y}{q}$$

ou

$$a = qx + py$$

cette équation admettra des solutions entières. Si p et q admettent une décomposition en facteurs premiers entre eux, on pourra opérer sur $\frac{x}{p}$ et $\frac{y}{q}$ comme sur $\frac{a}{b}$, et ainsi de suite de sorte que si p^{α}, q^{β}, r^{γ}, s^{δ}... sont les facteurs premiers entre eux de b ; p, q... désignant des nombres premiers, on pourra mettre $\frac{a}{b}$ sous la forme

$$\frac{a}{b} = \pm \frac{A}{p^{\alpha}} \pm \frac{B}{q^{\beta}} \pm \frac{C}{r^{\gamma}} \dots$$

et cela d'ailleurs d'une infinité de manières. Si nous considérons la fraction $\frac{A}{p^{\alpha}}$ on pourra poser

$$A = p^{\alpha-1}P + P_1, \; P_1 < p^{\alpha-1},$$
$$P_1 = p^{\alpha-2}P_2 + P_3, \; P_3 < p^{\alpha-2},$$

alors on aura

$$A = p^{\alpha-1}P + p^{\alpha-2}P_2 + \dots$$

de sorte que l'on aura

$$\frac{a}{b} = \pm \left(\frac{P}{p} + \frac{P_2}{p^2} + \dots \frac{P_{2\alpha}}{p^{\alpha}} \right) \pm \dots,$$

Soit maintenant N un entier, p, q, r... ses facteurs premiers en sorte que

$$N = p^{\alpha} q^{\beta} r^{\gamma} \dots$$

posons

$$\frac{N'}{N} = \frac{\alpha}{p} + \frac{\beta}{q} + \frac{\gamma}{r} \dots$$

le nombre N′ est évidemment entier, on peut l'appeler le dérivé de N. On a alors les propriétés suivantes.

Le dérivé de MN *est* MN′ + NM′. En effet si

$$M = p^{a} q^{b} r^{c} \dots,$$
$$N = p^{\alpha} q^{\beta} r^{\gamma} \dots.$$

on a

$$MN = p^{a+\alpha} q^{b+\beta} \ldots,$$

et

$$\frac{(MN)'}{MN} = \frac{a+\alpha}{p} + \frac{b+\beta}{q} \ldots = \frac{M'}{M} + \frac{N'}{N};$$

d'où l'on tire $(MN)' = MN' + NM'$.
donc

$$(N^{\alpha})' = \alpha N^{\alpha-1} N'.$$

Si N *est premier on a* $N = 1$, *excepté si* $N = 1$, *alors* $N' = 0$.

Si $\frac{P}{Q}$ *est entier, ainsi que P et Q, on a*

$$\left(\frac{P}{Q}\right)' = \frac{P'Q - QP'}{Q^2}, \tag{1}$$

car en posant $\frac{P}{Q} = E$

$$P = EQ, \quad P' = EQ' + QE';$$

donc

$$E' = \frac{P' - EQ'}{Q} = \frac{P'Q - Q'P}{Q^2}.$$

On peut prendre la formule (1) pour définition[1] de $\left(\frac{P}{Q}\right)'$ quand $\frac{P}{Q}$ n'est pas entier ; alors si

$$P = a^{\alpha} b^{\beta} c^{\gamma} \ldots,$$
$$Q = p^{\mu} q^{\nu} r^{\rho} \ldots.$$

---

[1] Il est facile de constater que

$$\left(\frac{\varpi P}{\varpi Q}\right)' = \left(\frac{P}{Q}\right)'$$

car cela revient à

$$\frac{(\varpi P)' \varpi Q - (\varpi Q)' \varpi P}{\varpi^2 Q^2} = \frac{P'Q - Q'P}{Q^2},$$

ou à

$$\frac{(\varpi P' + \varpi' P) \varpi Q - (\varpi Q' + Q\varpi') \varpi P}{\varpi^2 Q^2} = \frac{P'Q - Q'P}{Q^2},$$

ce qui est une identité.

on aura

$$\left(\frac{P}{Q}\right)' = \frac{1}{p^{2\omega} q^{2\varepsilon} \ldots} \left[p^{\omega} q^{\varepsilon} \ldots \left(\frac{\alpha}{a} + \frac{\beta}{b} \ldots \right) - a^{\alpha} b^{\beta} \ldots \left(\frac{\omega}{p} + \frac{\varepsilon}{q} \ldots \right) \right].$$

on a donc

$$\left(\frac{P}{Q}\right)' : \frac{P}{Q} = \frac{P'}{P} - \frac{Q'}{Q}.$$

Il y a des nombres égaux à leurs dérivés, il est facile de voir que p, q, r... étant des nombres premiers, ils sont de la forme :

$$p^p, \quad \frac{p^p q^q}{r^r}, \ldots \quad \frac{p^p q^q r^r s^s}{t^t u^u v^v} \ldots$$

6. — Continuation du même sujet

Soient p, q, r... des nombres premiers, il ne saurait exister d'identité de la forme

$$\frac{A_\alpha}{p^\alpha} + \ldots + \frac{A_1}{p} + \frac{B_\beta}{q^\beta} + \ldots \frac{B_1}{q} + \ldots = 0,$$

$A_\alpha, \ldots A_1, \ldots B_\beta, \ldots B_1 \ldots$ désignant des entiers ainsi que α, β,... bien entendu on suppose toutes les fractions réduites à leur plus simple expression.

En effet on en déduirait

$$\frac{A_\alpha}{p} q^\beta r^\gamma \ldots + E = 0,$$

E désignant un entier, ce qui est absurde si A_α n'est pas nul, etc.

Le dérivé d'un nombre premier est 1, le dérivé d'un nombre non premier est évidemment supérieur à 1, s'il est entier; voyons si un nombre $\frac{P}{Q}$ fractionnaire peut avoir pour dérivé 1. En d'autres termes peut-on avoir :

$$P'Q - Q'P = Q^2.$$

Soit $P = a^\alpha b^\beta \ldots$ $Q = p^\omega q^\varepsilon \ldots$ les valeurs de P et Q décomposés en facteurs premiers, peut-on avoir ?

$$\frac{P'}{P} - \frac{Q'}{Q} = \frac{Q}{P},$$

ou

$$\frac{\alpha}{a}+\frac{\beta}{b}\ldots-\frac{\varpi}{p}-\frac{\varkappa}{q}\ldots=\frac{a^{\alpha}b^{\beta}\ldots}{p^{\varpi}q^{\varkappa}\ldots}.$$

le second membre est de la forme $\frac{A}{p^{\varpi}}+\frac{A'}{p^{\varpi-1}}+\ldots$, on devrait donc avoir une identité de la forme que nous venons de considérer, alors $\alpha=\beta=\ldots=0$, ce qui est absurde; il n'y a donc que les nombres premiers qui ont l'unité pour dérivé.

Le nombre 2 *n'est le dérivé d'aucun nombre entier.*

En effet si l'on pose

$$\frac{2}{N}=\frac{\alpha}{a}+\frac{\beta}{b}+\ldots$$

$$N=a^{\alpha}b^{\beta}\ldots$$

2 sera par définition le dérivé de N dont les facteurs premiers sont a, b,...

Si l'on suppose d'abord a, b,... au nombre de 1, on a

$$\frac{2}{N}=\frac{\alpha}{a},\qquad 2=\alpha a^{\alpha-1},$$

égalité impossible si a est au moins égal à 2.

Si l'on suppose les facteurs a, b au nombre de deux, on a

$$2=\alpha a^{\alpha-1}b^{\beta}+\beta a^{\alpha}b^{\beta-1}.$$

Cette formule est impossible, car a, b, α, β sont au moins égaux à 1, et l'égalité ne peut être satisfaite dans cette hypothèse, car a et b sont différents. A fortiori le nombre N ne saurait avoir plus de deux facteurs premiers, dont 2 ne saurait être un nombre dérivé. On verrait de même que :

3 *n'est le dérivé d'aucun entier;*

4 *est son propre dérivé, il n'est le dérivé d'aucun autre entier;*

5 *est le dérivé de* 6;

12 *est le dérivé de* 8.

Les propriétés des nombres dérivés semblent enveloppées d'un profond mystère, leur répartition paraît très irrégulière. Quand on prend les dérivés successifs d'un nombre, tantôt on obtient une suite qui finit par décroître et aboutir à l'unité,

tantôt on trouve une suite de nombres qui semblent rapidement croissants à l'infini. Il y a là une mine très riche à exploiter, mais elle est hérissée de difficultés.

7. — Médiation

Si l'on considère les fractions $\frac{a}{b}$ et $\frac{a'}{b'}$,

$$\frac{a+b'}{b+b'}$$

sera une moyenne entre $\frac{a}{b}$ et $\frac{a'}{b'}$, on lui donne le nom de *médiante*, et on donne le nom de *médiation* à l'opération qui consiste à former une médiante.

Considérons deux fractions $\frac{a}{b}$ et $\frac{a'}{b'}$ telles que

$$ab' - ba' = 1,$$

et par suite irréductibles, prenons les médiantes, ce qui donne la suite

$$\frac{a}{b}, \frac{a+a'}{b+b'}, \frac{a'}{b'},$$

entre chacun des intervalles $\frac{a}{b}$, $\frac{a+a'}{b+b'}$, $\frac{a'}{b'}$ intercalons des médiantes, nous aurons

$$\frac{a}{b}, \frac{2a+a'}{2b+b'}, \frac{a+a'}{b+b'}, \frac{a+2a'}{b+2b'}, \frac{a'}{b'};$$

dans chacun des nouveaux intervalles intercalons une médiante et ainsi de suite.

Si $\frac{a}{b} = \frac{0}{1}$ et $\frac{a'}{b'} = \frac{1}{1}$, les suites ainsi formées ont été appelées suites de Brocot.

Il est facile de voir que si

$$\frac{a}{b}\ \frac{a_1}{b_1} \cdots \frac{a_n}{b_n}\ \frac{a'}{b'}$$

sont des fractions telles que chacune d'elles est médiante entre la précédente et la suivante, et si l'on a

(1) $$ab' - ba' = 1,$$

on aura

$$a_i b_{i+1} - a_{i+1} b_i = 1. \qquad (2)$$

En effet il suffit de prouver que si l'on intercale une seule médiante, le théorème est vrai, il suffit donc de vérifier que

$$a(b+b') - b(a+a') = 1,$$

ce qui est facile, car cette formule se réduit à (1).

Toutes les fractions $\frac{a}{b}$, $\frac{a'}{b'}$ ... sont irréductibles, car si a_i et b_i avaient un facteur commun, en vertu de (2), il devrait diviser 1, ce qui est absurde.

On peut opérer la médiation en n'intercalant de médiantes qu'entre deux fractions dont la somme des dénominateurs est égale au rang de la suite qu'on forme ; la suite ainsi formée est la suite dite de Farey quand les fractions qui ont servi de point de départ sont $\frac{0}{1}$ et $\frac{1}{1}$.

On vérifie sans peine que les suites de Farey ne contiennent que des fractions irréductibles.

Si l'on range par ordre de grandeur toutes les fractions irréductibles comprises entre 0 et 1, dont le dénominateur ne surpasse pas n chacune d'elles sera médiante entre la précédente et la suivante.

CHAPITRE III

DES CONGRUENCES EN GÉNÉRAL

1. — Congruences

Deux nombres sont dits *congrus* suivant le module p, quand leur différence est divisible par p, ou quand, divisés par p, ils laissent les mêmes restes. On dit aussi qu'ils sont *résidus* l'un de l'autre par rapport à p; on exprime que a et b sont congrus suivant le module p, ainsi :

$$a \equiv b, \pmod{p}.$$

On appelle *résidu minimum* de a suivant le module p, le reste de la division de a par p.

On peut ajouter un même nombre aux deux membres d'une congruence, on peut multiplier ses deux membres par un même nombre sans qu'elle cesse d'avoir lieu. Mais on ne peut diviser les deux membres par un nombre μ : 1° que si les quotients sont entiers; 2° que si μ est premier avec le module. Enfin on peut toujours ajouter ou multiplier membre à membre des congruences de même module.

Soit F (x) un polynôme à coefficients entiers, la congruence F $(x) \equiv 0$, (mod. p) est du degré m, si F (x) est de degré m en x, x est l'inconnue; il y a des congruences telles que F $(z, y, z\ldots) \equiv 0$ (mod. p) à plusieurs inconnues, les valeurs *entières* de x, y, $z\ldots$ qui les rendent identiques sont les *racines*.

Soient a_1, a_2,... a_n, des entiers, x_1, x_2,... x_n des inconnues, une congruence du premier degré est de la forme

$$a_1x_1 + a_2x_2 \ldots + a_nx_n \equiv \alpha \pmod{a},$$

elle équivaut donc à l'équation indéterminée

$$ax + a_1x_1 + \ldots a_nx_n = \alpha,$$

qu'il faut résoudre en nombres entiers.

La congruence

$$a_1 x_1 \equiv \alpha \pmod{a} \tag{1}$$

équivaut ainsi à l'équation indéterminée

$$a_1 x_1 + a_2 x_2 = \alpha.$$

que nous avons appris à résoudre. On peut dire que si a_1 est premier avec a, *la congruence* (1) *admet toujours une solution et une seule, quand* a_1 *n'est pas congrue à zéro, pourvu que l'on considère comme ne formant pas des solutions distinctes les nombres congrus entre eux*[1].

Les congruences simultanées

$$a_{11} x_1 + a_{12} x_2 \ldots + a_{1n} x_n \equiv b_1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{n_1} x_1 + a_{n_2} x_2 \ldots + a_{nn} x_n \equiv b_n,$$

prises suivant le même module a se résoudront comme il suit : désignons par A_{11}, $A_{12}\ldots$, les coefficients de a_{11}, $a_{12}\ldots$ dans le déterminant

$$\begin{vmatrix} a_{11} & a_{12} \ldots & a_{1n} \\ a_{21} & a_{22} \ldots & a_{2n} \\ \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} \ldots & a_{2n} \end{vmatrix} = \Delta,$$

nous aurons :

$$\Delta x \equiv A_{11} b_1 + A_{21} b_2 \ldots A_{n_1} b_n,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\Delta x_n \equiv A_{2n} b_1 + A_{n_2} b_2 \ldots A_{nn} b_n.$$

ces congruences sont équivalentes aux congruences proposées et chacune d'elles se résoudra individuellement.

---

[1] (Voir le § intitulé théorème de Fermat, congruences binômes.) Ceci peut se prouver directement, en effet on sait que a, étant premier avec a, les nombres a_1, $2a_1\ldots$, $(a-1)\,a_1$ sont congrus à l'ordre près à 1, 2, 3... $a-1$ donc il existera un nombre x et un seul tel que $a_1 x \equiv \alpha$. On peut trouver ce nombre au moyen du théorème d'Euler en effet :

$$a_1^{\varphi(a)} \equiv 1 \pmod{a},$$

donc

$$a_1 x_1 \equiv \alpha a_1^{\varphi(a)},$$

revient à la congruence proposée (1), on en tire :

$$x_1 \equiv \alpha a_1^{\varphi(a)-1} \pmod{a}.$$

Remarque. — On simplifie quelquefois la résolution de la congruence $a_1 x_1 \equiv \alpha \pmod{a}$ quand a est un nombre composé. Soit $a = m m'$, il est clair que les solutions de $a_1 x_1 - \alpha \equiv o \pmod{a}$ sont des solutions communes de $a_1 x_1 - \alpha = 0 \pmod{m}$ et $\pmod{m}$. Si ξ est une solution de la congruence qui a pour module m, les solutions de la proposée, seront de la forme $\xi + m x_2$, donc

$$a_1 (\xi + m x_2) \equiv \alpha \pmod{m m'}.$$

donc $a_1 \xi - \alpha$ est divisible par m et l'on a en posant $\frac{a_1 \xi - \alpha}{m} = \mu$,

$$\mu + m x_2 \equiv 0 \pmod{m'}$$

ce qui donne x_2.

2. — Carrés magiques

Considérons n^2 nombres

$$\begin{array}{c} x_{11}\, x_{12} \ldots x_{1n} \\ x_{21}\, x_{22} \ldots x_{2n} \\ \cdots\cdots\cdots \\ x_{n1}\, x_{n2} \ldots x_{nn} \end{array}$$

rangés comme les éléments d'un déterminant, ils forment un carré *magique* si l'on a

$$\begin{array}{l} x_{11} + x_{12} \ldots + x_{1n} = s, \\ x_{21} + x_{22} \ldots + x_{2n} = s, \\ \cdots\cdots\cdots\cdots\cdots \\ x_{n1} + x_{n2} \ldots + x_{nn} = s, \\ x_{11} + x_{21} \ldots + x_{n1} = s, \\ x_{12} + x_{22} \ldots + x_{n2} = s, \\ \cdots\cdots\cdots\cdots\cdots \\ x_{1n} + x_{2n} \ldots + x_{nn} = s, \end{array}$$

et encore

$$\begin{array}{l} x_{11} + x_{22} + \ldots x_{nn} = s, \\ x_{1n} + x_{2n-1} + \ldots x_{n1} = s. \end{array}$$

ces équations qui se réduisent à $2n + 1$ distinctes car les n

premières et les suivantes donnent toutes deux $\Sigma x_i = ns$, formant un système indéterminé du premier degré facile à résoudre au moins en théorie, si on laisse les x et les s complètement arbitraires.

La théorie des carrés magiques a été fort en honneur dans les derniers siècles, mais on ne comprend plus guère la faveur dont elle jouit aujourd'hui, puisque l'on sait à présent résoudre les équations indéterminées du premier degré. Voici d'ailleurs une manière assez simple de se procurer des carrés magiques à n^2 éléments quand n est premier.

Prenons :

$$x_{ij} = \text{résidu minimum } (ai + bj) + n \text{ résidu minimum } (a'i + b'j) \text{ (mod. } n).$$

a et b. a' et b' étant positifs et inférieurs à n, alors a, $2a$,... na, seront à l'ordre près égaux à 0, 1, 2,... $n - 1$, il en sera de même de $2b$, b,... nb et de a', $2a'$,... ainsi que de $2b'$, b'... nb', donc :

$$x_{ij} + x_{kj} \ldots + x_{mj} = \frac{n(n-1)}{2} + n\,\frac{n(n-1)}{2} = \frac{n(n^2-1)}{2}$$

car j étant constant, $a + bj$, $2a + bj$... fourniront tous les nombres comme a, $2a$,... il est clair que $x_{i1} + x_{i2} \ldots + x_{in}$ aura la même valeur.

En outre

$$x_{11} + x_{22} \ldots + x_{nn} = \frac{n(n-1)}{2} + n\,\frac{n-1}{2}.$$

Si $a + b$ est différent de n ainsi que $a' + b'$. Enfin

$$\begin{aligned} x_{n1} + x_{n-12} \ldots + x_{1n} &= \Sigma \text{ rés. } [ai + b(n-i)] \\ &\quad + n\,\Sigma \text{ rés. } [a'i + b'(n-i)] \\ &= \Sigma \text{ rés. } (a-b)i + n\,\Sigma \text{ rés. } (a'-b'); \end{aligned}$$

et cette somme sera encore la même si $a - b$ et $a' - b'$ sont différents de n.

Enfin il est clair que si les tableaux dont les éléments sont

les x_{ij} et les y_{ij} sont magiques, le carré dont l'élément général est $\alpha\, x_{ij} + \beta\, y_{ij} + \gamma$ est lui-même magique.

8	1	6
3	5	7
4	9	2

et

15	6	9	4
10	3	16	5
8	13	2	11
1	12	7	14

sont des carrés magiques dont tous les éléments sont distincts.

On a encore considéré des carrés *diaboliques*, qui sont des carrés magiques d'une nature particulière, car ils restent magiques quand on remplace par exemple les colonnes de rang $1, 2, .., p$ par celles de rang $p+1, p+2 \ldots 2p$ que l'on écrit les premières. On a enfin considéré des *cubes* magiques et des hypercubes magiques dans l'espace à plusieurs dimensions. Toutes ces questions dépendent de la théorie des congruences du premier degré. Elles sont regardées comme difficiles, mais la difficulté est ici dans la nature des choses, le problème à résoudre pour construire un carré magique dépendant en définitive d'un très grand nombre d'inconnues.

3. — Généralités sur les congruences d'ordre supérieur et de module premier

Soit $F(x)$ un polynôme en x, il est toujours possible de remplacer la congruence

$$F(x) \equiv 0 \pmod{p}$$

par une autre de même degré, et dont les coefficients soient inférieurs à p, sans en altérer les racines ; il suffit en effet de réduire les coefficients de $F(x)$ à leurs résidus minima relatifs à p[1].

[1] Quand deux nombres sont congrus on dit aussi qu'ils sont résidus ou restes l'un de l'autre par rapport au module, le résidu minimum d'un nombre est alors le reste de la division de ce nombre par le module.

Ceci posé, soit $F(x)$ un polynôme de degré m, $f(x)$ un polynôme de degré $n < m$. Je dis qu'il *existera toujours deux polynômes Q et R tels que l'on ait, en désignant par p un nombre premier.*

$$F(x) \equiv f(x)\varphi(x) + R(x), \pmod{p},$$

$R(x)$ étant de degré moindre que n. En effet soit :

$$F(x) = Ax^m + Bx^{m-1} + Cx^{m-2} + \ldots,$$
$$f(x) = ax^n + bx^{n-1} + Cx^{n-2} + \ldots,$$
$$\varphi(x) = \alpha x^r + \beta x^{r-1} + \gamma x^{r-2} + \ldots,$$
$$R(x) = A' x^{n-1} + B' x^{n-2} + \ldots,$$

pour déterminer Q et R, on aura les relations

$$A \equiv a\alpha,$$
$$B \equiv a\beta + b\alpha,$$
$$\ldots\ldots\ldots$$

toujours possibles si p est un nombre premier, et qui donnent α', β'... A' B'... sans ambiguïté.

$\varphi(x)$ et $R(x)$ sont ce que l'on appelle le *quotient* et le *reste* de la division de $F(x)$ par $f(x)$; quand R est nul on dit que *f divise* F.

Théorème premier. — *Si* $F(x)$ *est divisible par* $(x - a)$, *(mod. p) on a* $F(x) \equiv (x - a)\,Q(mod.\ p)$, *et cette formule a lieu si* $F(a)$ *est divisible par p.*

En effet on a en appelant Q le quotient et R le reste de la division de F par $x - a$;

$$F(x) = (x - a)\,Q + R;$$

soit $x = a$, on a

$$0 = R,$$

donc $F(x) \equiv (x - a)\,Q$.

$$F(x) = (x - a)\,Q.$$

Théorème 2e. — $F(x) \equiv 0$ *ne peut avoir plus de m racines*, *m désignant son degré*, à moins que l'on ait quel que soit x, $F(x) \equiv 0$.

Théorème 3e — *Si quelque soit* x, $F(x) \equiv 0$, *les coefficients de* $F(x)$ *sont congrus à o.*

Théorème 4e. — *Deux polynômes congrus ont leurs coefficients congrus.*

Tout polynôme $F(x)$ *est équivalent à un autre dans lequel le coefficient de la plus haute puissance de* x *serait* 1. En effet, il suffit de diviser tous les termes par le coefficient de la plus haute puissance a de x (cette division se fait suivant le module p). Cela revient à multiplier par le nombre a' tel que $a\,a' \equiv 1$.

Le *plus grand commun diviseur* de deux polynômes, suivant le module premier p est le polynôme du degré le plus élevé qui les divise tous deux.

La recherche du plus grand commun diviseur se fait comme en algèbre, à cette différence près que dans le cours de l'opération on peut toujours négliger les multiples de p.

Les nombres $f(1)$, $f(2)$,... $f(p)$, $f(p+1)$,... *se reproduisent périodiquement,* en effet on a

$$f(p+x) = f(x) + pf'(x) + \frac{p^2}{1.2} f''(x)$$

or les coefficients $f'(x)$, $\frac{f''(x)}{1.2}$ .... sont entiers donc

$$f(p+x) = f(x). \qquad \text{c.q.f.d.}$$

Une congruence $f(x) \equiv 0 \pmod{p}$, ne peut donc avoir pour racines que les nombres 0, 1, 2, 3,... $p-1$.

En général, on appelle polynômes irréductibles ceux qui n'ont pas de diviseurs entiers, et congruences irréductibles celles dont le premier membre est un polynôme irréductible.

Une congruence irréductible d'un degré supérieur au premier n'a pas de racines, car si elle avait une racine a, son premier membre serait divisible par $x - a$ et par suite ne serait pas irréductible.

4. — Théorème de Fermat et d'Euler

Théorème. — *La congruence suivante où p est premier*

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

admet pour racines tous les nombres non divisibles par p et par suite les p racines

$$1, 2, 3, \ldots, p-1.$$

En effet on a :

$$x^p + \frac{p}{1} x^{p-1} + \frac{p(p-1)}{1.2} x^{p-2} + \ldots + \frac{p}{1} x + 1 = (x+1)^p$$

or $\frac{p}{1}$, $\frac{p(p-1)}{1.2}$ ... sont divisibles par p, car, par exemple, $p \frac{p-1}{1.2}$ est un entier, donc $\frac{p-1}{2}$ est entier aussi puisque p est premier avec 1, 2, etc..., on aura donc

$$x^p + 1 \equiv (x+1)^p \pmod{p},$$

ou

$$(x+1)^p - x^p \equiv 1.$$

On en tire successivement

$$x^p - (x-1)^p \equiv 1,$$
$$(x-1)^p - (x-2)^p \equiv 1,$$
$$\ldots\ldots\ldots\ldots$$
$$2^p - 1^p \equiv 1$$

et en ajoutant

$$x^p - 1 \equiv x - 1,$$

ou

$$x^p \equiv x, \text{ ou : } (x^{p-1} - 1)\, x \equiv 0;$$

or si x ne divise pas p, on aura :

$$x^{p-1} - 1 \equiv 0.$$

c. q. f. d.

Ce théorème dû à Fermat a été généralisé comme il suit par Euler.

Théorème 2e. — La congruence

$$x^{\varphi(p)} - 1 \equiv 0, \pmod{p},$$

où p est quelconque et où $\varphi(p)$ désigne le nombre des entiers premiers et inférieurs à p, admet pour racines les nombres premiers avec p.

En effet soient p_1, p_2..., p_s les nombres premiers à p et inférieurs à p, si l'on considère la suite

$$x,\ p_1x,\ p_2x,\ \ldots\ldots,\ p_sx,$$

où x est premier avec p, je dis qu'elle se compose de nombres incongrus suivant le module p ; en effet si l'on avait

$$p_ix \equiv p_j\,x,$$

p et x étant premiers entre eux, on aurait

$$p_i = p_j,$$

ce qui est absurde, puisque p_i et p_j sont inférieurs à p, en second lieu $p_i\,x$ ne peut avoir pour résidu minimum qu'un des nombres $1, p_1, p_2 \ldots p_s$ premiers à p, car si l'on avait

$$p_ix = \alpha,$$

α désignant un nombre ayant un facteur commun avec p, on aurait $p_ix = \alpha + mp$, et l'un des facteurs de p appartiendrait à $p_i\,x$, ce qui ne peut être puisque x et p_i n'ont pas de facteurs communs avec p.

On aura donc :

$$x,\ xp_1,\ xp_2 \ldots xp_s \equiv 1,\ p_1,\ p_2 \ldots p_s$$

ou

$$x^{\varphi(p)} \equiv 1.$$

c. q. f. d.

5. — Conséquences des théorèmes de Fermat et d'Euler

Des congruences de module p premier

$$a^{p-1} - 1 \equiv 0,$$
$$b^{p-1} - 1 \equiv 0,$$

on tire

$$a^{p-1} - b^{p-1} \equiv 0\ ;$$

d'où une foule de théorèmes d'arithmétique par exemple : les 4^e puissances de deux nombres non divisibles par 5 sont divisibles par 5, etc.

On a :

$$a^p - a \equiv 0,\ b^p - b \equiv 0,$$

donc

$$a^p - b^p \equiv a - b.$$

On peut démontrer le théorème de Fermat comme il suit : formons la suite

$$a,\ 2a,\ 3a,\ \ldots.\ (p-1)a,$$

leurs résidus minima sont différents, et par suite à l'ordre près : 1, 2, 3..., $p-1$; en effet, si l'on avait

$$ia \equiv ja,$$

on en conclurait $(i-j)\,a \equiv 0$, or $i-j < p$ donc, on aurait $a = 0$, ce qui est absurde, donc :

$$a^{p-1}\,1.2.3...(p-1) \equiv 1.2.3...(p-1)$$

d'où

$$a^{p-1} \equiv 1.$$

Cette démonstration nous fait découvrir un autre théorème ; appelons restes complémentaires, ceux dont la somme est congrue à zéro. Les nombres

$$a,\ 2a,\ldots,\frac{p-1}{2}\,a$$

ne peuvent avoir parmi eux des restes complémentaires, car soit

$$ia + ja \equiv 0,$$

on aurait $i + j \equiv 0$, ce qui est absurde puisque i et j sont inférieurs ou au plus égaux à $\frac{p-1}{2}$.

Considérons les résidus minima de la suite

$$(1) \qquad a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}\,a,$$

soient $r_1, r_2 \ldots r_k$ ceux qui sont supérieurs à $\frac{p-1}{2}$
et $\rho_1, \rho_2 \ldots \rho_l$ les autres, on aura :

$$(2) \qquad r_1 r_2 \ldots r_k\,\rho_1 \rho_2 \ldots \rho_l \equiv 1.2.3.\,\frac{p-1}{2}\,a^{\frac{p-1}{2}};$$

mais si l'on fait $r_i = p - s_i$, s_i sera moindre que $\frac{p-1}{2}$ et l'on ne pourra avoir $s_i = \rho_i$, sans quoi on aurait

$$p_i - r_i = \rho_i$$

p_i et ρ_i seraient complémentaires, ce qui est absurde, donc

$$s_1 s_2 \ldots s_k \rho_1 \rho_2 \ldots \rho_k = 1.2.3 \ldots \frac{p-1}{2},$$

ou

$$(p - r_1)(p - r_2) \ldots \rho_1 \rho_2 \ldots = 1.2.3 \ldots \frac{p-1}{2},$$

ou

$$(-1)^k \rho_1 \rho_2 \ldots r_1 r_2 \ldots = 1.2.3 \ldots \frac{p-1}{2},$$

k désignant le nombre des résidus de la suite (1) supérieurs à $\frac{p-1}{2}$. Comparant avec (2) on a :

$$(-1)^k = a^{\frac{p-1}{2}} \text{ donc :}$$

Théorème. — *Soit k le nombre des résidus minima de la suite*

$$a, 2a, \ldots \frac{p-1}{2} a$$

supérieurs à $\frac{p-1}{2}$ on aura :

$$a^{\frac{p-1}{2}} = (-1)^k.$$

Ce théorème est de Gauss ; d'ailleurs le théorème de Fermat donne

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = 0.$$

Les racines de la congruence

$$x^{p-1} - 1 = 0$$

sont les nombres $1, 2, 3 \ldots p - 1$, donc

$$x^{p-1} - 1 = (x - 1)(x - 2) \ldots (x - p + 1);$$

en identifiant, on a

$$1.2.3 \ldots (p - 1)(-1)^{p-1} = -1 ;$$

si p est impair on a :

$$1.2.3...(p-1)+1 \equiv 0 \pmod{p.}$$

si $p = 2$ on a $1 \equiv 1$, d'où le

Théorème de Wilson. — *Si p est un nombre premier*

$$1.2.3...(p-1)+1 \equiv 0.$$

Le théorème d'Euler donne :

$$x^{\varphi(p)} - 1 \equiv 0 \pmod{p.}$$

soient $p_1, p_2..., p_k$ ses racines, on a

$$x^{\varphi(p)} - 1 = (x-p_i)Q + R.$$

pour $x = p_i$ on a $R \equiv 0$, donc

$$x^{\varphi(p)} - 1 \equiv (x-p_1)(x-p_2)...(x-p_k)$$

et par suite

$$p_1 p_2 ... p_k (-1)^{\varphi(p)} \equiv 1,$$

ou

$$p_1 p_2 ... p_k \equiv (-1)^{\varphi(p)}.$$

Ce qui donne le théorème de Wilson si p est premier. On pourrait évidemment trouver un grand nombre de théorèmes analogues. Par exemple

$$1+2+3...+p-1 \equiv 0.$$
$$1.2+1.3...+2.3+... \equiv 0, \text{ etc.}$$

qui sont évidents, car la première formule revient à

$$\frac{p(p-1)}{2} \equiv 0, \text{ etc.}$$

6. — Congruences binomes et racines primitives

On appelle congruences binômes les congruences de la forme

$$x^m \equiv a \pmod{M},$$

Nous considérerons d'abord les congruences de la forme

$$x^m \equiv 1 \pmod{M}, \tag{1}$$

dans lesquelles le second membre est égal à l'unité.

Si le nombre a est racine de la congruence (1) et s'il n'est racine d'aucune autre congruence de la forme :

$$x^\mu \equiv 1 \pmod{M},$$

dans laquelle $\mu < m$, on dit que a est une *racine primitive* de la congruence (1) et que a *appartient* à l'exposant m.

Théorème 1er. — *L'exposant auquel appartient un nombre a, premier avec* M *suivant le module* M *est un diviseur de* $\varphi(M)$.

En effet, supposons que a appartienne à l'exposant m, s'il est premier avec M on aura

$$a^m \equiv 1, \quad a^{2m} \equiv 1, \ldots \quad a^{\mu m} \equiv 1, \pmod{M}$$

et réciproquement si l'on a $a^\nu \equiv 1$, il faut que ν soit multiple de m, en effet soit $\nu > m$, faisons alors $\nu = mq + r$ on aura

$$a^{mq+r} \equiv 1 \quad \text{et} \quad a^r \equiv 1,$$

ce qui exige que $r = 0$ si $r < m$, or on a

$$a^{\varphi(M)} \equiv 1,$$

donc $\varphi(M)$ est multiple de m. c.q.f.d.

On appelle *racines primitives d'un nombre* M les nombres qui appartiennent à l'exposant $\varphi(M)$ suivant le module M, autrement dit :

Si pour un nombre $m < \varphi(M)$ on n'a jamais

$$a^m \equiv 1 \pmod{M},$$

et si cette formule a lieu pour $m = \varphi(M)$, a sera racine primitive de M.

Théorème 2e. — *Il n'existe de racines primitives de* M *que si* M *est premier impair, ou une puissance de nombre premier impair, ou au double d'une puissance de nombre premier impair, ou enfin si* $M = 4$.

Soient $a, b, c, \ldots$ les facteurs premiers de M et :

$$M = a^\alpha b^\beta c \ldots$$

soit g un nombre premier avec M, on aura

$$g^{\varphi(a^\alpha)} \equiv 1,\ g^{\varphi(b^\beta)} \equiv 1,\ldots$$

les modules de ces congruences étant a^α, b^β,... soit s le plus petit multiple de $\varphi(a^\alpha)$, $\varphi(b^\beta)$... on aura

$$g^s \equiv 1,$$

suivant les modules a^α, b^β,... et par suite

$$g^s \equiv 1 \pmod{M}.$$

Je dis que $s < \varphi(M)$, en effet on sait que

$$\varphi(M) = \varphi(a^\alpha)\,\varphi(b^\beta)\ldots$$

or s est le plus petit multiple de $\varphi(a^\alpha)$, $\varphi(b^\beta)$... le fait en question sera donc établi si l'on prouve que $\varphi(a^\alpha)$, $\varphi(b^\beta)$... ont un facteur commun. Or, on a :

$$\varphi(a^\alpha) = a^\alpha\left(1 - \frac{1}{a}\right) = a^\alpha - a^{\alpha-1},$$

donc si a est impair et si $\alpha > 1$, $\varphi(a^\alpha)$ est divisible par 2; donc en général les nombres $\varphi(a^\alpha)$, (b^β)... auront le facteur commun 2 et $s < \varphi(M)$, et il n'y aura pas de racine primitive; les seules exceptions à cette règle sont relatives au cas où il n'y aurait dans M qu'un seul facteur premier impair, ainsi il ne pourra exister de racines primitives que si :

$$M = 2a^\alpha, \text{ ou : } a^\alpha, \text{ ou : } 2^n.$$

Or, je dis que si $M = 2^n$, il n'y a pas de racines primitives, excepté si $M = 4$, en effet, tout nombre a premier avec M est impair et de la forme $4k \pm 1$, or, on a alors

$$a^2 = 2^3 k' + 1,$$
$$a^{2^2} = 2^4 k'' + 1,$$
$$\ldots\ldots\ldots$$
$$a^{2^{n-3}} = 2^n K + 1.$$

Cette dernière formule donne

$$a^{\frac{M}{2}} = 1 \text{ ou : } a^{\frac{2M}{2}} = 1,$$

a n'est donc pas racine primitive, si $M > 4$.

Lorsque le module M *est premier,* $\varphi(M)$ *est égal à* M — 1 *et un nombre a est racine primitive s'il appartient à l'exposant* M — 1 *; en d'autres termes si l'on a*

$$a^{M-1} - 1 \equiv 0,$$

et si s étant moindre que M — 1 *on n'a jamais*

$$a^s - 1 \equiv 0,$$

les racines primitives d'un nombre premier p, sont donc les racines primitives de la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}.$$

7. — Étude du cas où le module est premier

Théorème 1er. — *La congruence*

$$x^m - 1 \equiv 0 \pmod{p}, \tag{1}$$

dans laquelle p est premier admet pour racines réelles les δ *racines de la congruence*

$$x^\delta - 1 \equiv 0 \pmod{p}, \tag{2}$$

dans laquelle δ *est le plus grand commun diviseur de m et de p — 1.*

En effet $x^\delta - 1$ est le plus grand commun diviseur de $x^{p-1} - 1$, et $x^m - 1$, donc les racines réelles de (1) sont les racines de $x^\delta - 1 \equiv 0$, mais les racines de $x^{p-1} - 1 \equiv 0$, en vertu du théorème de Fermat sont 1, 2, 3,..., $p - 1$. Or $(x^p - 1) : (x^\delta - 1) \equiv 0$ a au plus $p - 1 - \delta$ racines donc $x^\delta - 1 \equiv 0$ en a au moins δ, donc enfin (1) a δ racines réelles à savoir les racines (2). c.q.f.d.

Théorème 2e. — *Si a, b, c... sont racines de*

$$x^m \equiv 1, \tag{1}$$

les quantités a, a^2,..., b, b^2,... et en général $a^\alpha b^\beta c^\gamma$... seront également racines de la même congruence.

(Nous supposerons dans ce paragraphe que toutes les congruences sont relatives au module premier p.).

En effet de la congruence

$$x^m - 1 \equiv 0 \quad \text{ou} \quad x^m \equiv 1,$$

on conclut

$$a^{2m} \equiv 1, \quad a^{3m} \equiv 1, \ldots$$

c'est-à-dire

$$(a^2)^m \equiv 1, \quad (a^3)^m \equiv 1, \ldots$$

de même on a

$$(a^\alpha)^m \equiv 1, \quad (b^\beta)^m \equiv 1, \ldots$$

et par conséquent

$$(a^\alpha b^\beta c^\gamma \ldots)^m \equiv 1,$$

ce qui prouve que $a^\alpha b^\beta c^\gamma \ldots$ est racine de (1). c q f.d.

Théorème 3e. — *Si a est racine primitive de*

$$x^m - 1 \equiv 0, \tag{1}$$

m désignant un diviseur de $p - 1$, *les autres racines seront* $a^2, a^3, \ldots, a^m$.

En effet $a, a^2 \ldots, a^m$ sont racines, la congruence (1) a m racines, si donc nous prouvons que $a, a^2, \ldots$ sont incongrus le théorème sera démontré.

Or si l'on pouvait avoir i et $j < m + 1$,

$$a^i \equiv a^j,$$

on aurait

$$a^i (a^{j-i} - 1) \equiv 0;$$

or a^i n'est pas nul, $a^{j-i} - 1$ ne peut pas l'être non plus puisque a est racine primitive de (1) donc, etc. c.q.f.d.

Théorème 4e. — *Si a n'est pas racine primitive du diviseur m de* $p - 1$, *a n'appartiendra pas à l'exposant m, mais bien à un exposant inférieur* 0 *qui sera un diviseur de m.*

En effet, supposons que a appartienne à l'exposant 0 on aura $a^{\theta+1} \equiv a$, $a^{\theta+2} \equiv a^2 \ldots$ $a^{2\theta} \equiv a^\theta \equiv a$ etc. Les puissances de a formeront donc une période.

De plus pour $i < \theta$ et $j < \theta$, on n'aura jamais $a^i \equiv a^j$ sans quoi on aurait $(a^{j-i} - 1)\, a^i \equiv 0$ or a^{j-i} ne peut être congru à 1 puisque a appartient à l'exposant 0.

a^m fera donc partie de la série $a^\theta, a^{2\theta}, \ldots$ et 0 sera un diviseur de m.

Théorème 5e. — *Si m est un diviseur premier de* $p - 1$,

toutes les racines de $x^m - 1 \equiv 0$ *sont primitives (abstraction faite de l'unité).*

Soit en effet $a^m - 1 \equiv 0$, a désignant une racine de $x^m - 1 \equiv 0$; $x^m - 1 \equiv 0$ et $x^{m'} - 1 \equiv 0$ ayant une racine commune a, cette racine appartient à leur plus grand commun diviseur $x - 1$, donc 1 est la seule racine non primitive.

Théorème 6. — *Si m est un diviseur de $p - 1$ de la forme q^α, q étant premier, le nombre des racines primitives de* $x^m - 1 \equiv 0$ *sera* $\varphi(m)$.

En effet, les racines non primitives satisfont à $x^\delta - 1 \equiv 0$ ou $\delta < m$ ou $< q^\alpha$, alors δ divisera m car $x^\delta - 1 \equiv 0$ et $x^m - 1 \equiv 0$ ayant une racine commune, elle appartiendra au plus grand commun diviseur de $x^\delta - 1$ et $x^{q^\alpha} - 1$, soit $x^\delta - 1$ ce plus grand commun diviseur, δ sera un diviseur de q^α et même de $q^{\alpha-1}$, de sorte que si a est une racine non primitive elle satisfait à $x^{q^{\alpha-1}} - 1 \equiv 0$. Cette congruence a $q^{\alpha-1}$ racines, la congruence $x^{q^\alpha} - 1 \equiv 0$ a donc $q^\alpha - q^{\alpha-1} = \varphi(q^\alpha)$ racines primitives.

Théorème 7e. — *Soit a une racine de $x^{q^\alpha} - 1 \equiv 0$, b une racine de $x^{r^\beta} - 1 \equiv 0$,..., q, r,..., désignant des nombres premiers, soit $q^\alpha r^\beta \ldots = m$, $a\,b\,c\ldots$ sera racine de*

$$x^m - 1 \equiv 0$$

et réciproquement toutes les racines de $x^m - 1 \equiv 0$ *seront de cette forme.*

En effet :

$$a^{q^\alpha} \equiv 1 \quad \text{donc} \quad a^{q^\alpha r^\beta \ldots} \equiv 1, \quad b^{q^\alpha r^\beta \ldots} \equiv 1 \ldots,$$

donc

$$(a\,b\,c\ldots)^{q^\alpha r^\beta \ldots} \equiv 1.$$

réciproquement $a\,b\,c\ldots$ a $q^\alpha r^\beta \ldots = m$ valeurs, si on prouve qu'elles sont distinctes, tout sera prouvé. Soient a', b', c',... des valeurs de a, b, c..., si l'on avait

$$a\,b\,c\ldots = a'\,b'\,c'\ldots$$

on en conclurait en supposant : a différent de a' mod. $\wp$.

$$(a\,b\,c\ldots)^{r^\beta s^\gamma \ldots} = (a'\,b'\ldots)^{r^\beta s^\gamma \ldots},$$

ou

$$a^{\alpha\beta\gamma\ldots} \equiv a'^{\alpha\beta\gamma\ldots},$$

ou

$$a^{\omega} \equiv a'^{\omega}$$

soit ε une racine primitive de $x^{q^\alpha} - 1 \equiv 0$, alors on aura

$$a \equiv \varepsilon^i, \quad a' \equiv \varepsilon^{i'},$$

donc

$$\varepsilon^{i\omega} \equiv \varepsilon^{i'\omega},$$

ou

$$(\varepsilon^{(i-i')\omega} - 1)\,\varepsilon^{i'\omega} \equiv 0.$$

$\varepsilon^{i'\omega}$ n'est pas congru à zéro, donc $\varepsilon^{(i-i')\omega} - 1 \equiv 0$, donc $(i - i')\omega$ devrait être multiple de q^α ce qui est impossible, car $i - i' < q^\alpha$ ne peut contenir le facteur q^α et ω ne contient que les facteurs r, s... donc les m valeurs de $abc\ldots$ sont distinctes et représentent les racines de $x^m - 1 \equiv 0$.

Théorème 8e. — *Les mêmes choses étant posées que dans le théorème précédent, si a, b, c,... sont des racines primitives de* $x^{q^\alpha} - 1 \equiv 0$, $x^{r^\beta} - 1 \equiv 0$,... *abc... sera racine primitive de* $x^m - 1 \equiv 0$.

En effet, si $abc\ldots$ n'est pas racine primitive de $x^m - 1 \equiv 0$ on aura par exemple $(abc\ldots)^\theta \equiv 1$, et $x^\theta - 1 \equiv 0$ et $x^m - 1 \equiv 0$ auront une racine commune $abc\ldots$ satisfaisant à $x^\delta - 1 \equiv 0$, δ étant le pl. gr. c. diviseur de m et θ, on a donc

$$a^{q^\alpha - 1}\, b^{r^\beta}\, c^{\ldots} \ldots \equiv 1,$$

si l'on suppose que $\delta < q^\alpha r^\beta \ldots$ ne contienne pas α fois le facteur q, ou en ôtant les facteurs congrus à un

$$a^{q^\alpha - 1} - 1 \equiv 0,$$

donc a ne serait pas racine primitive de $a^{q^\alpha} - 1 \equiv 0$.

Théorème 9e. — *Si a, b, c... ne sont pas tous racines primitives de* $x^{q^\alpha} - 1 \equiv 0$, $x^{r^\beta} - 1 \equiv 0$,..., *abc... ne sera pas racine primitive de* $x^m - 1 \equiv 0$.

En effet, si par exemple a n'est pas racine primitive de $a^{q^\alpha} - 1 \equiv 0$, il satisfera à $x^{q^\alpha - 1} - 1 \equiv 0$ et l'on aura :

$$a^{q^\alpha - 1}\, b^{r^\beta}\, c^{\ldots} \ldots \equiv 1, \text{ donc, etc.}$$

Théorème 10e. — *Le nombre de racines primitives de* $x^m - 1 \equiv 0$, *ou m est un diviseur de* $p - 1$ *quelconque est* $\varphi(m)$.

En effet, le nombre de ces racines primitives est égal au produit des nombres des racines primitives des équations

$$x^{q^\alpha} - 1 \equiv 0, \qquad x^{r^\beta} - 1 \equiv 0, \ldots,$$

q^α, r^β,... étant les facteurs premiers avec leurs exposants de de m donc : le nombre cherché est $\varphi(p^\alpha)\,\varphi(p^\beta)\ldots = \varphi(m)$.

c.q.f.d.

8. — Recherche des racines primitives des nombres premiers

La recherche des racines primitives des nombres premiers repose sur le théorème suivant.

Théorème. — *Le résidu suivant le module premier p d'une puissance, ne saurait être racine primitive de p ou de la congruence*

$$x^{p-1} - 1 \equiv 0 \pmod{p.} \tag{1}$$

ce qui est la même chose.

En effet supposons

$$a \equiv z^\delta,$$

je dis que a n'est pas racine primitive de (1), en effet on tire de là

$$a^{\frac{p-1}{\delta}} \equiv z^{p-1}$$

et en vertu du théorème de Fermat $z^{p-1} \equiv 1$, donc :

$$a^{\frac{p-1}{\delta}} \equiv 1$$

et a n'est pas racine primitive (bien entendu l'hypothèse $z \equiv 0$ est écartée).

Si alors on veut trouver les racines primitives d'un nombre premier p, on ôtera des nombres 1, 2, 3,..., $p-1$, les résidus de puissances; les racines primitives cherchées se trouveront

parmi les nombres restants ; je dis que *les nombres qui ne sont pas résidus de puissances, sont racines primitives de p.*

En effet supposons que l'on ait

$$a^\delta - 1 \equiv 0$$

δ étant moindre que $p - 1$, a ne sera pas racine primitive de p, on en conclut quelque soit x

$$x^{p-1} - a^\delta \equiv x^{p-1} - 1.$$

le premier membre de cette congruence peut s'écrire $\left(x^{\frac{p-1}{\delta}}\right)^\delta - a^\delta$, il est donc divisible par $x^{\frac{p-1}{\delta}} - a$, il doit en être demême de $x^{p-1} - 1$, et la congruence $x^{\frac{p-1}{\delta}} - a$ doit avoir $\frac{p-1}{\delta}$ racines, donc enfin si a n'est pas racine primitive, cette quantité sera résidu de quelque puissance. Les racines primitives doivent donc bien être les nombres restants parmi 1, 2, 3,..., $p - 1$ quand on en a ôté les résidus de puissances.

Veut-on avoir les racines primitives de 7 on ôtera de la suite

1, 2, 3, 4, 5, 6

les nombres 1, 4, 2 qui sont résidus de carrés, 6 qui est résidu de cube et il restera 3 et 5 qui sont racines primitives puisqu'il doit y avoir $\varphi(7) = 2$ racines primitives pour le nombre 7.

9. — Indices ou logarithmes modulaires

Considérons la congruence :

$$x^{p-1} \equiv 1 \pmod{p} \tag{1}$$

où p désigne un nombre premier, elle a $p - 1$ solutions qui sont 1, 2,... $p - 1$. On sait d'ailleurs que si a n'est pas congru à p; a, a^2,... a^{p-1} seront solutions distinctes de (1) car a est alors une racine primitive.

Si l'on considère la congruence suivante où $a < p$

$$a^n \equiv N \pmod{p}$$

elle aura une solution n et une seule si N n'est pas congru à 0. On dit alors que n est l'indice de N dans la base a, et on écrit

$$n = \text{ind. N} \pmod{p}$$

Les indices jouissent de toutes les propriétés des logarithmes, ainsi dans une même base a, on a

$$\text{ind. N} + \text{ind. N}' = \text{ind. NN}' \pmod{p}$$

En effet par définition

$$N \equiv a^{\text{ind. N}} \pmod{p}$$
$$N' \equiv a^{\text{ind. N}} \pmod{p}$$

donc

$$NN' \equiv a^{\text{ind. N} + \text{ind. N}'}$$

ce qui revient à la formule que nous voulions démontrer. On a donc aussi

$$\text{Ind. N} + \text{ind. N}' + \text{ind. N}'' \ldots = \text{ind. NN}'\text{N}'' \ldots,$$
$$\text{Ind. N} - \text{ind. N}' = \text{Ind.} \frac{N}{N'}$$
$$\text{Ind. N}^h = h \text{ ind. N.}$$

Lorsque l'on a une table d'indices, on peut résoudre la congruence

$$x^m \equiv a \pmod{p}$$

car elle revient à

$$m \text{ ind. } x \equiv \text{ind. } a \pmod{p}$$

on est ainsi ramené à une congruence du premier degré que l'inconnue soit x ou qu'elle soit m.

Les indices, à cause de leurs propriétés sont appelés logarithmes modulaires.

10. — Modules composés

Nous avons vu qu'un nombre M n'a de racines primitives que s'il est premier, cas étudié précédemment, ou que s'il

est une puissance de nombre premier impair ou le double d'une telle puissance, enfin 4 est la seule puissance de 2 admettant des racines primitives.

Considérons alors un module de la forme p^{k+2}, $k > 0$, ou p est premier, Soit h un entier, on aura

$$(1) \qquad (1 + hp^k)^p \equiv 1 + hp^{k+1}, \text{ (mod. } p^{k+2}),$$

car si l'on développe le premier membre par la formule du binôme, on a

$$1 + hp^{k+1} + \frac{p-1}{1.2} h^2 p^{2k+1} + \ldots$$

et en négligeant les multiples de p^{k+2}, on a bien $1 + h\,p^{k+1}$.

Cela posé supposons qu'il existe une racine primitive pour le module p^{k+1}, et soit g cette racine, supposons que l'on ait $g^\delta \equiv 1 \pmod{p^k}$ ou :

$$g^\delta = 1 + hp^k.$$

En vertu de (1), on aura

$$g^{\delta p} = (1 + hp^k)^p \equiv 1 + hp^{k+1}, \text{ (mod. } p^{k+2}),$$

ou

$$g^{\delta p} \equiv 1 \text{ (mod. } p^{k+1}).$$

or, par hypothèse g est racine primitive de p^{k+1}, donc δp doit être divisible par $\varphi(p^{k+1}) = (p-1)\,p^k$ (p. 57), donc δ doit être divisible par $(p-1)\,p^{k-1}$, Mais g appartient à l'exposant δ relativement au module p^k, donc

$$\varphi(p^k) = (p-1)\,p^{k-1}$$

est divisible par δ, donc

$$\delta = \varphi(p^k);$$

donc g est aussi racine primitive de p^k. Donc dans la formule

$$g^{(p-1)p^{k-1}} \equiv 1 + hp^k,$$

h ne peut être divisible par p, sans quoi on aurait

$$g^{(p-1)p^{k-1}} \equiv 1 \text{ (mod. } p^{k+1}),$$

g ne peut donc être racine primitive de p^{k+1}.

Donc *les racines primitives d'une puissance d'un nombre premier p, sont racines primitives de p lui-même.*

Réciproquement, soit g une racine primitive de p^k et supposons que dans la formule

$$g^{p-1}p^{k-1} = 1 + hp^k$$

h ne soit pas divisible par p. Soit δ l'exposant auquel appartient g relativement au module p^{k+1}, on aura

$$g^\delta \equiv 1, \pmod{p^{k+1}}$$

et

$$g^\delta \equiv 1 \pmod{p^k},$$

δ sera divisible par $\varphi(p^k)$. Mais δ est un diviseur de $\varphi(p^{k+1}) = p\,\varphi(p^k)$, donc

$$\delta = \varphi(p^k) \text{ ou } \delta = \varphi(p^{k+1});$$

Mais la première formule ne peut avoir lieu, puisque h n'est pas divisible par p, donc :

$$\delta = \varphi(p^{k+1});$$

alors comme on a

$$g^{p-1}p^k = (1 + hp^k)^p = 1 + hp^{k+1} \pmod{p^{k+2}}$$

il en résulte

$$g^{p-1}p^k = 1 + h'p^{k+1},$$

h' n'étant pas divisible par p, donc :

Si g est racine primitive de $p > 2$ et si $g^{p-1} - 1$ n'est pas divisible par p^2, g est racine primitive des puissances de p.

Si g' est une racine primitive de p, $g' + pl$ sera encore une racine primitive de p, car

$$g^p = (g' + pl)^p = g'^p + \frac{p}{1} plg'^{p-1} + \ldots,$$

ou

$$g^p \equiv g'^p \pmod{p^2};$$

et si l'on pose

$$g'^p = g + g''p, \pmod{p^2},$$

on aura :

$$g^p - g = p(g'' - l) \pmod{p^2}$$

et $g = g' + pl$ est une racine primitive des puissances de p, excepté, si $l \equiv g''$ (mod. p), ainsi :

$$g' + pl \equiv g'^{p} \text{ (mod. } p^2\text{)}.$$

Or il y a $\varphi(p-1)$ nombres incongrus (mod. p), et chaque nombre g' fournit $p-1$ nombres g de la forme $g' + pl$ tels que $g^{p-1} - 1$ n'est pas divisible par p^2, donc :

Les racines primitives des puissances de p, sont les $(p-1)\varphi(p-1)$ *nombres incongrus entre eux suivant le module* p^2.

On peut alors généraliser comme il suit la notion d'indice :

Soit :

$$\varphi(p^k) = a$$

alors :

$$1,\ g,\ g^2 \ldots g^{a-1}$$

sont incongrus suivant le module p^k, à la condition d'exclure les multiples de p, il existe alors des nombres congrus entre eux suivant le module a et tels que

$$n \equiv g^{\alpha} \text{ (mod. } a\text{)}.$$

on posera alors

$$\alpha \equiv \text{ind. } n \text{ (mod. } a\text{)}.$$

le calcul de ces nouveaux indices est le même que celui des indices relatifs aux nombres premiers. On a du reste

$$\text{ind. } 1 = 0,\ \text{ind. } (-1) \equiv \frac{a}{2} \text{ (mod. } a\text{)}$$

et n est congru ou non à un carré suivant que n est pair ou impair;

on a :

$$n \equiv g^{\text{ind. } n} \text{ (mod. } p^k\text{)},$$
$$n^s \equiv g^{s \text{ ind. } n} \text{ (mod. } p^k\text{)}$$

et si $n^s \equiv 1$, s ind. n est divisible par a, s doit alors être un multiple de $\frac{a}{\delta}$. δ désignant le plus grand commun diviseur de a et de ind. n. Le plus petit des nombres s, où l'exposant auquel appartient n est $\frac{a}{\delta}$; donc :

La condition nécessaire et suffisante pour que n soit racine primitive de p^k est que n soit premier avec a.

Étude du module 4

Nous avons vu qu'il existe des racines primitives pour le module 4.

Au module 4 correspond la racine primitive -1. Si n est un nombre impair et α son indice.

$$(-1)^\alpha \equiv n \pmod 4$$

Si n est de la forme $4\nu + 1$, on aura $\alpha = 0$, si n est de la forme $4\nu + 3$, on aura $\alpha = 1$.

A un nombre de la forme 2^λ ou $\lambda > 2$, ne correspond plus de racine primitive. Mais si l'on considère les nombres

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

on aura $2^{\lambda-2}$ résidus correspondants tous différents de la forme $4\nu + 1$, donc si n est de la forme $4\nu + 1$, on peut satisfaire à la congruence

$$5^\beta \equiv n \pmod 2;$$

tandis que si n est de la forme $4\nu + 3$, cette congruence est impossible ; dans cette dernière hypothèse si $-n$ est de la forme $4\nu + 1$, on a :

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

on appellera *indice* du nombre impair n l'exposant β qui satisfait à cette congruence. β est pair ou impair, selon que n est de la forme $8\nu \pm 1$ ou $8\mu \pm 5$. La congruence

$$(-1)^\alpha 5^\beta \equiv n \pmod{2^\lambda}$$

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

11. — Congruences binomes générales

La congruence

$$x^m \equiv \omega \pmod n.$$

peut se résoudre en observant que si a, b, c... sont des nombres premiers entre eux, la congruence

$$f(x) \equiv 0 \bmod (abc\ldots)$$

ne pourra avoir lieu que si l'on a à la fois

$$f(x) \equiv 0 \pmod{a}, \qquad f(x) \equiv 0 \pmod{b}\ldots$$

supposons que α soit une racine de la première de ces congruences, β une racine de la seconde, etc., on posera :

$$x \equiv \alpha \pmod{a}, \qquad x \equiv \beta \pmod{b}\ldots$$

alors on aura si x satisfait à ces formules :

$$f(x) \equiv f(\alpha) \equiv 0 \pmod{a},$$
$$f(x) \equiv f(\beta) \equiv 0 \pmod{b},$$
$$\ldots\ldots\ldots\ldots$$

et par suite $a, b,\ldots$ étant premiers entre eux

$$f(x) \equiv 0 \pmod{abc\ldots}$$

12. — Résidus quadratiques

On appelle résidus quadratiques du nombre p, les nombres q qui satisfont à la relation :

$$x^2 \equiv q \pmod{p},$$

ou qui sont congrus à un carré.

Résidus relatifs au module 2, les résidus quadratiques de 2 satisfont à la relation

$$q = x^2 + 2n.$$

si donc q est pair cette égalité sera impossible, elle sera au contraire toujours possible si q est impair. (Il faut observer que les nombres pairs sont congrus à zéro et que 0 n'est pas compté.)

Résidus relatifs à un module premier impair p, formons la suite $1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$, tous ces nombres sont incongrus en effet si l'on avait :

$$s^2 \equiv s'^2 \quad \text{ou} \quad (s - s')(s + s') \equiv 0,$$

il faudrait que $s \equiv s'$ ou $s \equiv -s'$, or ni la somme ni la différence de deux nombres inférieurs à $\frac{p-1}{2}$ ne peut être

supérieure à $p - 1$ et par suite ne peut être divisible par p.

Mais $(p - s)^2 \equiv s^2$, donc les nombres

$$1^2, 2^2, \ldots (p-2)^2, (p-1)^2,$$

sont congrus deux à deux, *donc il n'existera que* $\frac{p-1}{2}$ *résidus quadratiques de* p, *mais il en existera bien* $\frac{p-1}{2}$; *soit* q *un résidu quadrique de* p, *on aura*

$$q^{\frac{p-1}{2}} \equiv 1.$$

En effet, on a

$$q \equiv x^2, \quad \text{d'où} \quad q^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1,$$

d'après le théorème de Fermat.

Soit s *un non-résidu, on aura :*

$$s^{\frac{p-1}{2}} \equiv -1.$$

En effet, d'après le théorème de Fermat, on a

$$s^{p-1} - 1 \equiv 0 \quad \text{ou} \quad \left(s^{\frac{p-1}{2}} - 1\right)\left(s^{\frac{p-1}{2}} + 1\right) \equiv 0,$$

donc $s^{\frac{p-1}{2}} \equiv \pm 1$; mais l'équation $x^{\frac{p-1}{2}} - 1 \equiv 0$, a $\frac{p-1}{2}$ racines, à savoir les $\frac{p-1}{2}$ résidus quadriques de p, donc $x^{\frac{p-1}{2}} + 1 = 0$ doit avoir $\frac{p-1}{2}$ autres racines réelles, ce sont les non-résidus, donc on a bien

$$s^{\frac{p-1}{2}} \equiv -1. \qquad \text{c. q. f. d.}$$

Legendre désigne par $\left(\frac{q}{p}\right)$ le résidu minimum de $q^{\frac{p-1}{2}}$ en sorte que $\left(\frac{q}{p}\right) = +1$ si q est résidu de p et -1 s'il est non résidu. On a alors :

1° $$\left(\frac{q}{p}\right)^2 = 1,$$

2° $$q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p},$$

3° $$\left(\frac{q}{p}\right)\left(\frac{q'}{p}\right)\ldots = \left(\frac{qq'\ldots}{p}\right),$$

En effet

$$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \cdot \left(\frac{q'}{p}\right) \equiv q'^{\frac{p-1}{2}} \cdots,$$

donc

$$\left(\frac{q}{p}\right)\left(\frac{q'}{p}\right)\cdots \equiv (q\,q'\cdots)^{\frac{p-1}{2}} \equiv \left(\frac{qq'\cdots}{p}\right)$$

D'où l'on conclut que le produit de deux résidus ou de deux non-résidus est un résidu et que le produit d'un résidu par un non-résidu est un non-résidu.

13. — Démonstration d'un lemme

Soit p un nombre premier qui ne divise pas q, si l'on prend les résidus minima compris entre $-\frac{p-1}{2}$ et $+\frac{p-1}{2}$ des nombres q, $2q$,... $\frac{p-1}{2}q$ et si l'on désigne par μ le nombre de ceux qui sont négatifs. on aura :

$$\left(\frac{q}{p}\right) = (-1)^{\mu}.$$

En effet : soient a_1, a_2,... a_λ les résidus positifs de la suite en question, $-b_1$, $-b_2$,... $-b_\mu$ les résidus négatifs. Je dis que l'on ne saurait avoir

$$b_m = a_m;$$

en effet, soit $-b_m \equiv \beta q$, $a_m \equiv \alpha q$, on aurait :

$$\beta q \equiv -\alpha q \text{ ou } (\beta + \alpha)\, q \equiv 0,$$

ce qui est impossible, puisque α et β sont au plus égaux à $\frac{p-1}{2}$. Il résulte de là que les a et les b sont aux signes près les nombres 1, 2,... $\frac{p-1}{2}$, on a donc

$$(-1)^{\mu} a_1 \cdots a_\lambda b_1 b_2 \cdots b_\mu \equiv q.2q \cdots \frac{p-1}{2} q,$$

ou bien

$$(-1)^{\mu} a_1 a_2 \cdots a_\lambda b_1 b_2 \cdots b_\mu \equiv 1.2.3 \cdots \frac{p-1}{2} q^{\frac{p-1}{2}}$$

ou divisant par les nombres égaux $a_1 a_2 \ldots b_\mu$ et $1.2 \ldots \frac{p-1}{2}$:

$$(-1)^\mu = q^{\frac{p-1}{2}}$$

ou, ce qui revient au même,

$$(-1)^\mu = \left(\frac{q}{p}\right). \qquad \text{c. q. f. d.}$$

14. — Généralisation d'un théorème précédent

Nous avons désigné par $\left(\frac{q}{p}\right)$, $+1$ ou -1 suivant que q est résidu ou non résidu quadrique de p.

La suite

$$\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \ldots \left(\frac{p-1}{p}\right)$$

présente $\frac{p-1}{2}$ *variations.*

En effet, considérons la congruence

$$x^2 - y^2 \equiv 1 \pmod{p} \tag{1}$$

ou

$$(x+y)(x-y) \equiv 1,$$

on la résoudra en posant

$$x - y = m,$$

m étant un des nombres $1, 2, 3 \ldots p-1$ et on en déduira

$$m(x+y) \equiv 1,$$

d'où l'on déduira $x+y$, et par suite x et y. La congruence (1) a donc $p-1$ solutions, pour que cette conclusion soit exacte il faut que si

$$m n \equiv 1$$

on ait pour m et n des nombres de même parité, or on peut toujours supposer qu'il en est ainsi puisque l'on peut ajouter à n un multiple de p.

Cela posé, les solutions de (1) peuvent se classer ainsi : 1° $y \equiv 0$, $x \equiv \pm 1$, (2 solutions) ; 2° $y^2 \equiv a$, $x^2 \equiv a+1$, alors

$\left(\frac{a}{p}\right) = 1, \left(\frac{a+1}{p}\right) = 1$, si N est le nombre des cas où a et $a+1$ sont résidus, cela fera 4 N solutions; 3° enfin on aura $x \equiv 0$, $y^2 \equiv -1$, ce qui donne deux solutions si $\left(\frac{-1}{p}\right) = 1$ ou $\left(\frac{p-1}{p}\right) = 1$ et 0 solution dans le cas contraire.

Supposons alors $\left(\frac{-1}{p}\right) = 1$, le nombre des solutions de (1) est $2 + 4N + 2 = p - 1$, $N = \frac{p-1}{4} - 1$. Or, le nombre des résidus de la suite $1, 2, \ldots p-1$ est $\frac{p-1}{2}$, $\frac{p-1}{4} - 1$ d'entre eux sont suivis de résidus, il en reste $\frac{p-1}{4}$ suivis de non-résidus, donc la suite $\left(\frac{1}{p}\right)\left(\frac{2}{p}\right)\ldots\left(\frac{p-1}{p}\right)$ présente $\frac{p-1}{4}$ variations $+-$ le premier et le dernier terme ont le signe $+$ le nombre des variations $-+$ sera donc aussi $\frac{p-1}{4}$ et le nombre total des variations est $\frac{p-1}{2}$.

Si $\left(\frac{-1}{p}\right) = -1$: on a $p - 1 = 2 + 4N$, $N = \frac{p-3}{4}$, le nombre des résidus suivis de non-résidus sera $\frac{p-1}{2} - N = \frac{p+1}{4}$, le premier terme a le signe $+$ dans la suite $\left(\frac{1}{p}\right)\ldots\left(\frac{p-1}{p}\right)$, le dernier a le signe $-$, et on trouve encore dans ce cas que le nombre des variations est $\frac{p-1}{2}$.

15. — Loi de réciprocité de Legendre

Considérons l'identité suivante où p est premier :

$$\frac{x^p - y^p}{x - y} = (x - ry)(x - r^2y)\ldots(x - r^{p-1}y),$$

r est une racine de $x^p - 1 = 0$ différente de l'unité, si l'on fait $x = y = 1$, on a

$$p = (1 - r)(1 - r^2)\ldots(1 - r^{p-1}),$$

ou encore en changeant r en r^2

$$p = (1 - r^2)(1 - r^4)\ldots(1 - r^{2\overline{p-1}}),$$

ou

$$p = r^{1+2\ldots+\overline{p-1}}(r - r^{-1})(r^2 - r^{-2})\ldots(r^{p-1} - r^{-p+1}),$$

ou enfin

$$p = (r - r^{-1})\,(r^2 - r^{-2})\ldots(r^{p-1} - r^{-p+1});$$

ou en observant que $r^{p-a} - r^{-p+a} = -(r^a - r^{-a})$:

$$p = (-1)^{\frac{p-1}{2}}(r - r^{-1})^2 \ldots (r^{\frac{p-1}{2}} - r^{-\frac{p-1}{2}})^2.$$

Élevons les deux membres à la puissance $\frac{q-1}{2}$, q désignant un nombre premier, on aura :

$$(1)\quad p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}(r - r^{-1})^{q-1}\ldots(r^{\frac{p-1}{2}} - r^{-\frac{p-1}{2}})^{q-1};$$

or, en général, si l'on pose $r^a = \rho$, on a

$$(\rho - \rho^{-1})^{q-1} = \rho^{q-1} - \frac{q-1}{1}\rho^{q-3} + \frac{q-1}{1}\cdot\frac{q-2}{2}\rho^{q-5} - \ldots$$
$$= \rho^{q-1} + \rho^{q-3}\ldots + \rho^{-q+1} + qf(\rho),$$

$f(\rho)$ désignant une fonction entière de ρ qui ne change pas quand on change ρ en $-\rho$. Donc :

$$(\rho - \rho^{-1})^{q-1} = \frac{\rho^q - \rho^{-q}}{\rho - \rho^{-1}} + qf(\rho).$$

La formule (1) s'écrit alors :

$$p^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\,\frac{r^q - r^{-q}}{r - r^{-1}}\cdot\frac{r^{2q} - r^{-2q}}{r^2 - r^{-2}}\cdots\frac{r^{\frac{p-1}{2}q} - r^{-\frac{p-1}{2}q}}{r^{\frac{p-1}{2}} - r^{-\frac{p-1}{2}}}$$
$$+ q\,\psi\left(r, r^2, \ldots r^{\frac{p-1}{2}}\right).$$

La fonction ψ est symétrique en $r, r^2 \ldots r^{\frac{p-1}{2}}$ et ne change pas quand on change r en r^{-1}, elle est donc symétrique par rapport à $r, r^2, \ldots r^{p-1}$ et s'exprime alors sous forme entière, on a donc

$$p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\,\frac{r^q - r^{-q}}{r - r^{-1}}\cdots\frac{r^{\frac{p-1}{2}q} - r^{-\frac{p-1}{2}q}}{r^{\frac{p-1}{2}} - r^{-\frac{p-1}{2}}} \pmod{q};$$

nous savons que $p^{\frac{q-1}{2}} \equiv \pm 1$; d'un autre côté, $(r - r^{-1})\ldots$

$(r^{\frac{p-1}{2}} - r^{-\frac{p-1}{2}})$, est égal à $\pm\sqrt{p}$, donc en observant que $p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right)$, on a

$$(2)\quad \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \frac{r^q - r^{-q}}{r - r^{-1}} \cdots \frac{r^{\frac{p-1}{2}q} - r^{-\frac{p-1}{2}q}}{r^{\frac{p-1}{2}} - r^{-\frac{p-1}{2}}}.$$

nous allons prouver que

$$X = \frac{r^q - r^{-q}}{r - r^{-1}} \cdots \frac{r^{\frac{p-1}{2}q} - r^{-\frac{p-1}{2}q}}{r^{\frac{p-1}{2}} - r^{-\frac{p-1}{2}}} = \left(\frac{q}{p}\right);$$

observons à cet effet que si $m \equiv n \bmod p$, $r^m = r^n$; or si l'on considère les exposants $q, 2q, \ldots \frac{p-1}{2}q$, ils seront congrus à $\frac{p-1}{2}$ nombres de la suite $\pm 1, \pm 2 \ldots \pm\frac{p-1}{2}$ différents entre eux d'ailleurs (Lemme), donc l'expression X sera égale à ± 1, on aura $X = 1$, si le nombre μ des exposants $q, 2q, \ldots \frac{p-1}{2}q$ congrus à des quantités négatives est pair, sinon on aura $X = -1$. Or, d'après le lemme, le nombre μ satisfait à la formule

$$(-1)^\mu = \left(\frac{q}{p}\right),$$

et comme $X = (-1)^\mu$, on a $X = \left(\frac{q}{p}\right)$; la formule (2) devient alors :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-2}{2}} \left(\frac{q}{p}\right)$$

c'est ce que l'on appelle la loi de réciprocité de Legendre. On peut l'écrire

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

16. — Applications du théorème de Legendre

Caractère du nombre 1. 1 est résidu quadratique de tous les nombres premiers, car ces nombres sont de la forme $2n + 1$ et l'on a $1^n \equiv 1$.

Caractère du nombre — 1. — 1 est résidu des nombres premiers $4n + 1$ et non résidu des nombres $4n - 1$. En effet

$$(-1)^{\frac{(4n+1)-1}{2}} = (-1)^{2n} = 1,$$

et

$$(-1)^{\frac{(4n-1)-1}{2}} = (-1)^{2n-1} = -1.$$

Caractère des nombres 2 *et* — 2. Partageons les nombres premiers en quatre classes : $8n \pm 1$, $8n \pm 3$.

$+ 2$ sera résidu de $8n \pm 1$ et non résidu de $8n \pm 3$.

$- 2$ sera résidu de $8n \pm 3$ et non résidu de $8n \pm 1$.

Voici la démonstration de M. Lebesgue : on a

$$2\sqrt{-1} = (1+\sqrt{-1})^2, \quad -2\sqrt{-1} = (1-\sqrt{-1})^2,$$

on en tire

$$\begin{cases} 2^{\frac{p-1}{2}} = (-\sqrt{-1})^{\frac{p-2}{2}} (1+\sqrt{-1})^{p-1}, \\ (-2)^{\frac{p-1}{2}} = (-\sqrt{-1})^{\frac{p-1}{2}} (1-\sqrt{-1})^{p-1} \end{cases}$$

en faisant dans ces formules successivement $p = 8n \pm 1$ et $8n \pm 3$, on arrive aux résultats ci-dessus énoncés, on peut les résumer dans les formules :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}\frac{p-1}{4}}, \left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{4}\frac{p-3}{4}}.$$

Caractères de 3 *et* — 3. D'après le théorème de Legendre on a :

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}} \left(\frac{p}{3}\right)$$

or $\left(\frac{p}{3}\right) \equiv p^{\frac{3-1}{2}} \equiv p$, or p est de la forme $3n \pm 1$, donc $\left(\frac{p}{3}\right) = +1$, si $p = 3n + 1$ et -1, si $p = 3n - 1$, donc :

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \text{ si } p = 3n + 1$$

$$\left(\frac{3}{p}\right) = -(-1)^{\frac{p-1}{2}} \text{ si } p = 3n - 1$$

on voit alors que si :

$p = 12n \pm 1$ 3 est résidu
$p = 12n + 1$ ou $12n - 5$... 3 est résidu.

Caractères de $+5$ *et* -5, etc. Ces caractères se trouvent comme ceux de $+3$ et -3. On est obligé de partager les nombres premiers en catégories de la forme $20n \pm 1$, $20n \pm 3$, $20n \pm 7$, $20n \pm 9$.

17. — Sommes de Gauss

On a

$$\int_{-\infty}^{\infty} \cos z^2 dz = \int_{-\infty}^{\infty} \sin z^2 dz = \sqrt{\frac{\pi}{2}},$$

et par conséquent

$$\int_{-\infty}^{\infty} \cos (z^2 + \delta)\, dz = \sqrt{\frac{\pi}{2}} (\cos \delta - \sin \delta) = \Delta,$$

et changeant z en $z\sqrt{\alpha}$

$$\int_{-\infty}^{+\infty} \cos (\alpha z^2 + \delta)\, dz = \frac{\Delta}{\sqrt{\alpha}};$$

ce que l'on peut écrire en appelant s un entier

$$\sum_{s=-\infty}^{s=+\infty} \int_{s\beta}^{(s+1)\beta} \cos (\alpha z^2 + \delta)\, dz = \frac{\Delta}{\sqrt{\alpha}},$$

β est d'ailleurs quelconque. Si l'on pose $z = \beta s + x$, on a

$$\sum \int_0^{\beta} \cos (\alpha\beta^2 s^2 + 2\alpha\beta s x + x^2\alpha + \delta)\, dx = \frac{\Delta}{\sqrt{\alpha}}.$$

Faisons $\beta = 4m\pi$, $\alpha = \frac{1}{8m\pi}$, nous aurons

$$\sum \int_0^{4m\pi} \cos \left[2m\pi + sx + \frac{x^2}{8m\pi} + \delta \right] dx = \Delta\sqrt{8m\pi},$$

ou

$$\sum \int_0^{4m\pi} \cos \left(\frac{x^2}{8m\pi} + \delta \right) \cos sx\, dx = \Delta\sqrt{8m\pi}. \tag{1}$$

Cela posé la formule de Fourier :

$$2\pi\left[\frac{1}{2}f(o)+\ldots f(2s\pi)+\ldots\frac{1}{2}f(4m\pi)\right]$$
$$=\sum\int_{o}^{4m\pi}f(x)\cos sx\,dx$$

donne en faisant $f(x)=\cos\left(\frac{x^2}{8m\pi}+\delta\right)$

$$2\pi\left[\frac{1}{2}\cos\delta\ldots\cos\left(\frac{s^2\pi}{2m}+\delta\right)\ldots+\frac{1}{2}\cos\left(2m\pi+\delta\right)\right]$$
$$=\sum\int_{o}^{4m\pi}\cos\left(\frac{x^2}{8m\pi}+\delta\right)\cos sx\,dx$$

ou en vertu de (1)

$$\cos\delta+\ldots\cos\left(\frac{s^2\pi}{2m}+\delta\right)\ldots=\Delta\sqrt{8m\pi}$$
$$=\sqrt{4\pi^2m}\,(\cos\delta-\sin\delta),$$

et comme δ est arbitraire

$$\sum_{2s=0}^{2s=2m-2}\cos\frac{s^2\pi}{2m}=\sqrt{m},$$
$$\sum\sin\frac{s^2\pi}{2m}=\sqrt{m}.$$

Si l'on fait $4m=n$ on a

$$\sum_{s=0}^{s=\frac{n-1}{2}}\cos\frac{2s^2\pi}{n}=\frac{1}{2}\sqrt{n},$$
$$\sum\sin\frac{2s^2\pi}{n}=\frac{1}{2}\sqrt{n}.$$

Ce sont les formules de Gauss ; et comme l'on a :

$$\begin{matrix}\cos\\ \sin\end{matrix}\Big)\frac{2\pi}{n}(s+n)^2=\begin{matrix}\cos\\ \sin\end{matrix}\Big)\frac{s^2 2\pi}{n}$$

on peut aussi écrire

$$\sum_{s=0}^{s=n-1} \cos\frac{2s^2\pi}{n} = \sum \sin\frac{2s^2\pi}{n} = \sqrt{n},$$

ou le radical a le signe $+$.

18. — Nouvelle démonstration de la loi de réciprocité

Posons en supposant h entier et positif,

$$\varphi(h,n) = \Sigma e^{s^2 \frac{2\pi h\sqrt{-1}}{n}}, \tag{1}$$

s prenant $n-1$ valeurs incongrues à n, alors :
1° en vertu des formules de Gauss, si n est multiple de 4

$$\varphi(1,n) = (1+\sqrt{-1})\sqrt{n}; \tag{2}$$

2° si $h \equiv h' \pmod{n}$ on a

$$\varphi(h,n) = \varphi(h',n). \tag{3}$$

3° si a est premier avec n

$$\varphi(a^2h,n) = \varphi(h,n). \tag{4}$$

4° si m et n sont premiers entre eux et positifs on a :

$$\varphi(hm,n)\,\varphi(hn,m) = \varphi(h,mn). \tag{5}$$

En effet on a

$$\varphi(hm,n)\,\varphi(hn,m) = \Sigma e^{s^2\frac{2\pi hm}{n}\sqrt{-1}}\,\Sigma e^{t^2\frac{2\pi hn}{m}\sqrt{-1}}$$
$$= \Sigma e^{\left(\frac{m}{n}s^2+\frac{n}{m}t^2\right)2\pi h\sqrt{-1}},$$

or on a

$$\left(\frac{m}{n}s^2+\frac{nt^2}{m}\right) = \frac{(ms+nt)^2}{mn} - 2st,$$

donc

$$\varphi(hm,n)\,\varphi(hn,m) = \Sigma e^{\frac{(ms+nt)^2}{mn}2\pi h\sqrt{-1}}; \tag{6}$$

mais les mh valeurs de $ms+nt$ sont incongrues mod mn.

Si l'on avait en effet

$$ms + nt = ms' + nt',$$

on aurait

$$m(s - s') + n(t - t') = 0$$
$$m(s - s') = n(t' - t).$$

Or m et n sont premiers entre eux, et pour que cette congruence ait lieu mod. mn, il faut qu'elle ait lieu mod. n ou que $m(s - s') \equiv 0$ mod. n, ce qui est absurde, $s - s'$ étant inférieur à n.

Donc dans (6) $ms + nt$ ne prenant que les valeurs incongrues à mn la formule (5) a lieu.

Dès lors il est facile de voir que

$$\varphi(1, n) = (1 + \sqrt{-1})\sqrt{n} \quad \text{si } n = 0 \pmod 4,$$
$$= (\sqrt{-1})^{\frac{(n-1)^2}{4}}\sqrt{n} \quad \text{si } n = 1 \pmod 2,$$
$$= 0 \quad \text{si } n = 2 \pmod 4.$$

La première formule résulte immédiatement des formules de Gauss ; (4) donne :

$$\varphi(2^2, n) = \varphi(1, n);$$

on a ensuite :

$$\varphi(n, 2^2) = \sum e^{\frac{\pi 2\pi\sqrt{-1}}{4}} = 1 + 1 + (\sqrt{-1})^n + (\sqrt{-1})^n = 2(1 + (\sqrt{-1})^n)$$

or d'après (5)

$$\varphi(2^n, n)\varphi(n, 2^n) = \varphi(1, 4n),$$

donc

$$\varphi(1, n).2(1 + \sqrt{-1}^n) = \varphi(1, 4n) = 2(1 + \sqrt{-1})\sqrt{n}$$
$$\varphi(1, n) = \frac{1 + \sqrt{-1}}{1 + \sqrt{-1}^n}\sqrt{n}$$

si $n \equiv 1 \pmod 4$, $\sqrt{-1}^n = \sqrt{-1}$, si $n \equiv 3 \pmod 4$, $\sqrt{-1}^n = -\sqrt{-1}$.

donc dans le premier cas

$$\varphi(1, n) = \sqrt{n} \text{ et dans le second } \varphi(1, n) = \sqrt{n}\sqrt{-1},$$

ou

$$\varphi(1,n)=(\sqrt{-1})^{\frac{(n-1)^2}{4}}\sqrt{n};$$

ce qui démontre la seconde formule. Enfin on a si $n\equiv 2$, mod. 4

$$\varphi\left(\frac{n}{2},\frac{n}{2}\right)\varphi\left(\frac{n}{2},2\right)=\varphi(1,n);$$

Or $\varphi\left(\frac{n}{2},2\right)=0$ donc $\varphi(1,n)=0$ ce qui achève la démonstration.

Si p est un nombre premier impair on a

$$\varphi(h,p)=\left(\frac{h}{p}\right)(\sqrt{-1})^{\left(\frac{p-1}{2}\right)^2}\sqrt{p},$$

En effet :

$$\varphi(h,p)=\sum e^{\alpha^2\frac{2\pi h\sqrt{-1}}{p}}$$

et en appelant α les résidus quadratiques et β les non résidus on a

$$\varphi(h,p)=1+2\sum e^{\alpha\frac{2\pi h\sqrt{-1}}{p}}$$

en observant que les résidus sont au nombre de $\frac{p-1}{2}$.

Mais quand h n'est pas divisible par p :

$$1+\sum e^{\alpha\frac{2\pi h\sqrt{-1}}{p}}+\sum e^{\beta\frac{2\pi h\sqrt{-1}}{p}}=0;$$

de sorte que, dans ce cas,

$$\varphi(h,p)=\sum e^{\alpha\frac{2\pi h\sqrt{-1}}{p}}-\sum e^{\beta\frac{2\pi h\sqrt{-1}}{p}}=\sum\left(\frac{s}{p}\right)e^{s\frac{2\pi h\sqrt{-1}}{p}}$$

ou

$$\varphi(h,p)=\left(\frac{h}{p}\right)\sum\left(\frac{hs}{p}\right)e^{s\frac{2\pi h\sqrt{-1}}{p}}$$

ou

$$\varphi(h,p)=\left(\frac{h}{p}\right)\sum\left(\frac{s}{p}\right)e^{\frac{2\pi s\sqrt{-1}}{p}};$$

pour $h = 1$

$$\varphi(1, p) = \Sigma \left(\frac{s}{p}\right) e^{2\pi \frac{s\sqrt{-1}}{p}},$$

d'où

$$\varphi(h, p) = \left(\frac{h}{p}\right) \varphi(1, p) = \left(\frac{h}{p}\right) \left(\sqrt{-1}\right)^{\left(\frac{p-1}{2}\right)^2} \sqrt{p}.$$

Voici maintenant comment en découle la loi de Legendre. h et p étant premiers, on a en outre

$$\varphi(p, h) = \left(\frac{p}{h}\right) \left(\sqrt{-1}\right)^{\left(\frac{h-1}{2}\right)^2} \sqrt{h},$$

et en multipliant membre à membre en ayant égard à (5) et à

$$\varphi(1, pq) = \left(\sqrt{-1}\right)^{\left(\frac{pq-1}{2}\right)^2} \sqrt{pq},$$

on a

$$\left(\sqrt{-1}\right)^{\left(\frac{ph-1}{2}\right)^2} \sqrt{ph} = \left(\frac{h}{p}\right) \left(\frac{p}{h}\right) \sqrt{p} \sqrt{h} \left(\sqrt{-1}\right)^{\left(\frac{p-1}{2}\right)^2 + \left(\frac{h-1}{2}\right)^2},$$

ou enfin

$$\left(\frac{h}{p}\right) \left(\frac{p}{h}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{h-1}{2}} \qquad \text{c.q.f.d.}$$

20. — Généralisation de la théorie de Legendre

Jacobi (monatsberichte *der Berliner akademie*, 1837) a généralisé le symbole $\left(\frac{q}{p}\right)$ de Legendre, en convenant que si p désignait le nombre des résidus négatifs de la suite

$$q, 2q, 3q \ldots \frac{p-1}{2} q \pmod{p}.$$

on avait

$$\left(\frac{q}{p}\right) = (-1)^{\nu}$$

mais p doit alors être impair. Il restait à étendre le symbole $\left(\frac{q}{p}\right)$ au cas où p est pair, c'est ce qu'a fait Kronecker, comme il suit (Sitzungsberichte, 1895).

Par définition, on aura si a est divisible par b,

$$\left(\frac{a}{b}\right) = 0,$$

si a et b n'ont pas de diviseur commun,

$$\left(\frac{a}{b}\right) = \left(\frac{2^q}{a}\right)\left(\frac{a}{b'}\right),$$

en supposant $b = 2^q b'$ et $b' \equiv 1 \pmod 2$.

On peut encore remplacer ces conventions par les suivantes :

$$\sigma(x) = \frac{2}{\pi}\int_0^\infty \frac{\sin tx}{t}\,dt$$

désignera 1, 0, ou — 1 suivant que x sera positif, nul ou négatif et *par définition* on aura

$$\left(\frac{q}{p}\right) = \sigma\left[\mathcal{R}_p(q)\,\mathcal{R}_p(2q)\ldots\mathcal{R}_p\left(\frac{p-1}{2}\,q\right)\right],$$

$\mathcal{R}_p(x)$ désignant le résidu minimum de x suivant le mod. p; si alors $q \equiv q' \pmod p$, on aura

$$\left(\frac{q}{p}\right) = \left(\frac{q'}{p}\right);$$
$$\left(\frac{q}{p}\right)\left(\frac{q'}{p}\right) = \left(\frac{qq'}{p}\right),$$

car

$$\left(\frac{q}{p}\right)\left(\frac{q'}{p}\right) = \sigma\mathcal{R}(q)\ldots\mathcal{R}\left(\frac{p-1}{2}\,q\right)\sigma\mathcal{R}(q')\ldots\mathcal{R}\left(\frac{p-1}{2}\,q'\right),$$
$$\left(\frac{qq'}{p}\right) = \sigma\mathcal{R}(qq')\ldots\mathcal{R}\left(\frac{p-1}{2}\,qq'\right)$$

or

$$\mathcal{R}(iq) = iq,\ \mathcal{R}(i'q') = i'q',$$
$$\mathcal{R}(iq)\,\mathcal{R}(i'q') = ii'\,qq'.$$

mais les nombres $i,\ 2\ i \ldots \frac{p-1}{2}\,i$ sont différents (mod. p), et l'on voit que $\mathcal{R}(i\,q)\ \mathcal{R}\ (i'\,q')$ sera congru à l'un des nombres $\mathcal{R}(j\,q\,q')$ et à un seul, c'est-à-dire égal à un des nombres $\mathcal{R}(j\,q\,q')$, donc

$$\left(\frac{q}{p}\right)\left(\frac{q'}{p}\right) = \left(\frac{qq'}{p}\right).$$

On peut généraliser encore en observant que

$$\sigma \mathfrak{R}(iq) = \sigma \sin \frac{2\pi i q}{p},$$

en sorte que

$$\left(\frac{q}{p}\right) = \sigma \sin \frac{2\pi q}{p} \sin \frac{4\pi q}{p} \ldots \sin \frac{p-1}{p} \pi q,$$

et l'on peut supprimer le signe σ en écrivant

$$\left(\frac{q}{p}\right) = \frac{\sin 2\pi \frac{q}{p}}{\sin \frac{2\pi}{p}} \frac{\sin \frac{4\pi q}{p}}{\sin \frac{4\pi}{p}} \ldots \frac{\sin \frac{p-1}{p} \pi q}{\sin \frac{p-1}{p} \pi},$$

et comme le second membre se réduit à zéro pour les valeurs de q divisibles par p, on peut convenir que

$$\left(\frac{q}{p}\right) = 0$$

si q est divisible par p. On pourrait même généraliser encore et supposer que si p est pair on a

$$\left(\frac{q}{p}\right) = \frac{\sin \frac{2\pi q}{p}}{\sin \frac{2\pi}{p}} \cdot \frac{\sin \frac{4\pi 4}{p}}{\sin \frac{4\pi}{p}} \ldots \frac{\sin 2 \frac{p-2}{p} \pi q}{\sin 2 \frac{p-2}{p} \pi}.$$

Dans le cas où p et q sont des nombres impairs quelconques on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

ou, si l'on veut,

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \frac{\sin \frac{2\pi q}{p} \ldots \sin \frac{2\pi (p-1)}{2p} q}{\sin \frac{2\pi}{p} \ldots \sin \frac{2\pi (p-1)}{p}} \cdot \frac{\sin \frac{2\pi p}{q} \ldots \sin \frac{2\pi (q-1)}{2q} p}{\sin \frac{2\pi}{q} \ldots \sin \frac{2\pi (q-1)}{2q}}.$$

Pour démontrer cette proposition qui contient le théorème de Legendre, on observe que

$$(1) \qquad \left(\frac{q}{p}\right) = \tau^{a=\frac{p-1}{2}} \prod_{a=1} \mathcal{R}_p(aq);$$

Pour que $\mathcal{R}_p(aq)$ soit négatif, il faut qu'en désignant par x le quotient de aq par p à une unité près, on ait

$$px > aq, \text{ ou } px - aq > 0,$$
$$px < aq + \frac{p}{2}, \quad px - aq - \frac{p}{2} < 0,$$

c'est-à-dire

$$\left(px - aq\right)\left(px - aq - \frac{p}{2}\right) < 0.$$

Si l'on remplace dans le premier membre x par un autre entier z si $z > x$ les deux facteurs deviennent positifs, si $z < x$ ils deviennent négatifs, donc

$$\left(pz - aq\right)\left(pz - aq - \frac{p}{2}\right) > 0;$$

il en résulte que non seulement

$$\tau\,\mathcal{R}_p(aq) = \tau\,(px - aq)\left(px - aq - \frac{p}{2}\right),$$

mais encore

$$(2) \qquad \tau\,\mathcal{R}_p(aq) = \tau\,\Pi\,(pz - aq)\left(pz - aq - \frac{p}{2}\right),$$

le signe Π s'étendant à autant de facteurs que l'on voudra, pourvu que z prenne la valeur x.

or si l'on fait varier a de 1 à $\frac{p-1}{2}$, comme on a

$$px < aq + \frac{p}{2},$$
$$x < a\,\frac{q}{p} + \frac{1}{2},$$

et à fortiori

$$x < \frac{p-1}{2p}\,q + \frac{1}{2},$$

ou

$$x < \frac{q}{2} - \frac{q}{2p} + \frac{1}{2};$$

ce qui revient à dire que $x < \frac{q-1}{2}$, puisque q est impair et x entier, la formule (2) sera donc toujours vraie en faisant varier z de 1 à $\frac{q-1}{2}$, donc la formule (1) donnera

$$\left(\frac{q}{p}\right) = \sigma \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{z=1}^{z=\frac{q-1}{2}} (pz - aq) \left(pz - aq - \frac{p}{2}\right)$$
$$= \sigma \prod (pz - aq) \prod \left(pz - aq - \frac{p}{2}\right).$$

Si dans le second produit on pose

$$z = \frac{q+1}{2} - y,$$

on a

$$\left(\frac{p}{q}\right) = \sigma \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{z=1}^{z=\frac{q-1}{2}} (pz - aq) \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{y=1}^{y=\frac{q-1}{2}} \left(\frac{pq}{2} - py - aq\right);$$

ce que l'on peut écrire en changeant de notation :

$$(3) \qquad \left(\frac{p}{q}\right) = \sigma \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{z=1}^{z=\frac{p-1}{2}} (pz - aq) \left(\frac{pq}{2} - pz - aq\right).$$

d'une façon analogue, on aurait

$$\left(\frac{q}{p}\right) = \sigma \prod_{a=1}^{a=\frac{q-1}{2}} \prod_{z=1}^{z=\frac{p-1}{2}} (qz - ap) \left(\frac{pq}{2} - qz - ap\right),$$

ou par un changement de notation

$$(4) \qquad \left(\frac{q}{p}\right) = \sigma \prod_{a=1}^{a=\frac{p-1}{2}} \prod_{z=1}^{z=\frac{q-1}{2}} (aq - pz) \left(\frac{pq}{2} - qz - ap\right);$$

de (3) et (4) on tire

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \sigma \prod \left[-(aq - pz)^2\right]$$

Or dans le second membre le nombre des facteurs, tous négatifs est $\frac{p-1}{2}\frac{q-1}{2}$, donc

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Ce théorème est dû à M. Kronecker. Il constitue à notre avis la démonstration la plus belle que l'on ait donné du théorème de Legendre.

21. — Les discriminants

On sait que l'on a appelé discriminant d'une forme $ax^2 + bxy + cy^2$ la quantité $b^2 - 4ac$. Elle est congrue à b^2 (mod. 4), or tout carré est congru à 0 ou à 1 mod. 4, car s'il est pair il est divisible par 4, s'il est impair il est de la forme $(2n+1)^2 = 4n^2 + 4n + 1$, donc il est congru à 1. Par extension nous appellerons discriminant un entier congru à 0 ou à 1 (mod. 4).

Un discriminant sera fondamental s'il est de la forme :

$$p, -4p, \pm 8p,$$

p étant congru à 1 (mod. 4). Voici la raison de ces dénominations, soit

$$b^2 - 4ac = DQ^2$$

Q^2 étant le plus grand carré contenu dans $b^2 - 4ac$, si $D \equiv 1 \pmod 4$, D est encore un discriminant. Si $D \equiv 2 \pmod 4$, Q contiendra le facteur 4 que l'on adjoindra à D pour le rendre congru à 0 et lui donner la forme d'un discriminant, on procédera de même si $D \equiv 3$, il ne peut être congru à 0. Donc on aura l'une des formules

$$D = p,\ p \equiv 1 \pmod 4$$
$$D = 4p,\ p \equiv -1$$
$$D = 8p,\ p \equiv \pm 1.$$

Cela posé je dis que

$$\left(\frac{b}{a}\right) = \left(\frac{a+\lambda b}{b}\right).$$

cela est évident si b est impair d'après la définition de Jacobi.

Si $b = 2^\beta b'$, b' étant impair et si a est impair, on a

$$\left(\frac{a}{b}\right) = \left(\frac{2^\beta}{a}\right)\left(\frac{a}{b'}\right) = \left(\frac{2^\beta}{a}\right)\left(\frac{a+\lambda b'}{b'}\right) = \left(\frac{2^\beta}{a\,(a+\lambda b')}\right)\left(\frac{a+\lambda b'}{b}\right).$$

Et si β est pair

$$\left(\frac{a}{b}\right) = \left(\frac{a+\lambda b'}{b}\right).$$

Si β est impair prenons $\lambda = 8\mu$, alors

$$\left(\frac{a}{b}\right) = \left(\frac{2^\beta}{a\,(a+8\mu b')}\right)\left(\frac{a+8\mu b'}{b}\right) = \left(\frac{a+8\mu b'}{b}\right).$$

Donc si $\beta \equiv 2 \pmod 4$ et si a et b sont premiers entre eux

$$\left(\frac{a}{b}\right) = \left(\frac{a+4\lambda b}{b}\right), \lambda \gtrless 0$$

et dans tous les autres cas

$$\left(\frac{a}{b}\right) = \left(\frac{a+\lambda b}{b}\right), \lambda \lessgtr 0.$$

Théorème de Kronecker. — *Si a est un discriminant, on a*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{b+\lambda a}\right)$$

pourvu que a et $b + \lambda a$ soient positifs.

Si a et b ont un facteur commun, la formule subsiste quels que soient a, b, λ; supposons donc a et b premiers entre eux; soit $a \equiv 1 \pmod 4$, $b = 2^\beta b'$. $b' \equiv 2 \pmod 4$.

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right) = \left(\frac{b+\lambda a}{a}\right) = \left(\frac{a}{b+\lambda a}\right)$$

Si $a \equiv 0 \pmod 4$, soit $a \equiv 2^\alpha a'$, $a' \equiv 1 \pmod 2$. $\alpha \geq 2$ $b \equiv 1 \pmod 2$, on aura

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)(-1)^{\frac{a'-1}{2}\frac{b-1}{2}}$$

$$= \left(\frac{2^\alpha}{b}\right)\left(\frac{b}{a'}\right)(-1)^{\frac{a'-1}{2}\frac{b-1}{2}} = \left(\frac{2^\alpha}{b}\right)\left(\frac{b+\lambda' a'}{a'}\right)(-1)^{\frac{a'-1}{2}\frac{b-1}{2}}$$

et si $\lambda' \equiv 0 \pmod 4$

$$\left(\frac{a}{b}\right) = \left(\frac{2^\alpha}{b}\right)\left(\frac{a'}{b+\lambda' a'}\right)(-1)^{\frac{a'-1}{2}\left(\frac{b-1}{2}+\frac{\lambda' a'+b-1}{2}\right)}$$

$$= \left(\frac{2^\alpha}{b}\right)\left(\frac{a'}{b+\lambda' a}\right).$$

$$= \left(\frac{2^\alpha}{b(b+\lambda' a')}\right) = \left(\frac{2^\alpha}{b(b+\lambda' a')}\right)\left(\frac{a}{b+\lambda' a'}\right), \lambda' \equiv 0 \pmod 4$$

Si α est pair le premier facteur est égal à 1, prenant alors $\lambda' \equiv 0 \pmod{2^\alpha}$, $b + \lambda' a'$ sera > 0.

Si α est impair, il sera ≥ 3 puisque a est un discriminant, et prenant $\lambda' \equiv 0 \pmod 8$, on aura

$$b(b+\lambda' a') \equiv b^2 \equiv 1, \pmod 8$$

et le premier facteur sera encore égal à 1. En prenant $\lambda' \equiv 0 \pmod{2^\alpha}$, $b' + \lambda a'$ sera positif. Le théorème est donc démontré.

CHAPITRE IV

DÉCOMPOSITION EN CARRÉS

1. — Théorèmes préliminaires

On a les deux identités dont la première est due à Léonard de Pise et la seconde à Euler.

$$(a^2+b^2)(a'^2+b'^2)=(aa'+bb')^2+(ab'-ba')^2,$$

$$\begin{aligned}(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2)&=(aa'+bb'+cc'+dd')^2\\&+(ab'-ba'+dc'-cd')^2\\&+(ac'-ca'+bd'-db')^2\\&+(ad'-da'+cb'-bc')^2.\end{aligned}$$

La première de ces formules exprime que le module d'un produit de deux imaginaires $a+bi$ et $a-bi$ est égal au produit de leurs modules. La seconde exprime que le module du produit de deux quaternions est égal au produit de leurs modules. Elles établissent les propositions suivantes :

Le produit d'une somme de deux ou quatre carrés par une somme de deux ou quatre carrés, est aussi une somme de deux ou quatre carrés.

Théorème. — *Tout diviseur d'une somme de deux ou quatre carrés est une somme de deux ou quatre carrés.*

Supposons $a^2+b^2+c^2+d^2$ divisible par p :

$$(a-p\alpha)^2+(b-p\beta)^2+(c-p\gamma)^2+(d-p\delta)^2$$

le sera aussi, or on peut supposer $a-p\alpha$, $b-p\beta$, $c-p\gamma$, $d-p\delta$ au plus égaux à $\frac{p}{2}$ en prenant ces nombres égaux aux restes minimums de la division de a, b, c, d, par p. Donc si p divise $a^2+b^2+c^2+d^2$, il divisera une somme de 4 carrés $a'^2+b'^2+c'^2+d'^2$ dans lesquels a', b', c', d' sont moindres ou au plus égaux à $\frac{p}{2}$.

En résumé, si $\Sigma\, a^2 = p\,p'$, on aura $\Sigma\, a'^2 = p\,p''$, $a' \geq \frac{p}{2}$. De même on aura $\Sigma\, a''^2 = p''\,p'''$, $a'' \geq \frac{p''}{2}$. Or

$$\Sigma\, a'^2\, \Sigma\, a''^2 = pp''^2\, p'''$$

est un produit d'une somme de 4 carrés par une somme de 4 carrés, c'est donc une somme de 4 carrés divisible par p''', donc il existe une somme de 4 carrés divisible par pp'''. Or puisque $a' < \frac{p}{2}$, $\Sigma\, a'^2 < p$ et $p'' p$, de même $p''' < p''$, on pourra ainsi se procurer des sommes de 4 carrés produits de p par des nombres décroissants, non nuls, donc enfin p est lui-même une somme de 4 carrés.

La démonstration se fait de même pour une somme de deux carrés.

2. — Décomposition des nombres premiers

Tout nombre premier p de la forme 4n + 3 est une somme de 4 carrés.

En effet la suite

$$1, 2, 3 \ldots p - 1$$

contient un résidu α quadratique de p suivi d'un non-résidu $\alpha + 1$, car $1 \equiv (p-1)^2$ est résidu et $p - 1 \equiv -1$ ne l'est pas, car,

$$(p-1)^{\frac{p-1}{2}} = p^{\frac{p-1}{2}} \ldots + \frac{p-1}{2}\, p - 1 \equiv -1,$$

et on a vu que le caractère des non-résidus est

$$s^{\frac{p-1}{2}} \equiv -1.$$

Ainsi α est résidu. — 1 et $\alpha + 1$ étant non-résidus, leur produit $-\alpha - 1$ sera résidu, donc on peut poser

$$\alpha \equiv u^2,$$
$$-\alpha - 1 \equiv v^2,$$

et en ajoutant

$$u^2 + v^2 + 1 \equiv 0.$$

$u^2 + v^2 + 1$ est divisible par p, p divise alors une somme de

4 carrés, o, 1, u^2, v^2 il est donc bien une somme de 4 carrés.

c. q. f. d.

Un nombre p de la forme 4n + 3 premier ne peut être la somme de deux carrés.

En effet on aurait

$$u^2 + v^2 \equiv p,$$

et en posant

$$u^2 \equiv \alpha, \qquad v^2 \equiv -\alpha$$

$-1 \times \alpha$ serait résidu ce qui est absurde.

Tout nombre premier p de la forme 4n + 1 est une somme de deux carrés.

En effet — 1 est résidu cette fois et

$$u^2 + 1 \equiv 0;$$

p divisant une somme de deux carrés 1 et u^2, est une somme de deux carrés

3. — Décomposition d'un nombre quelconque

Tout nombre entier est une somme de 4 carrés. En effet ses facteurs premiers sont des sommes de 4 carrés, et en vertu de notre premier théorème, il sera lui-même une somme de 4 carrés.

En général un nombre entier donné peut être décomposé de plusieurs manières en sommes de 4 carrés.

La théorie des fonctions elliptiques conduit à l'identité remarquable

$$(1) \qquad (1 + 2q + 2q^4 + 2q^9 \ldots + 2q^{n^2} \ldots)^4 = 1 + 4q\left(\frac{q}{1-q} + \frac{2q^2}{1+q^2} + \frac{3q^3}{1-q^3} + \frac{4q^4}{1+q^4} + \ldots\right)$$

la quantité entre parenthèses peut s'écrire

$$\begin{aligned} &q + q^2 + q^3 + q^4 + \ldots \\ &+ 2(q^2 - q^4 + q^6 - q^8 + \ldots) \\ &+ 3(q^3 + q^6 + q^9 + q^{12} + \ldots) \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

elle contient q à toutes les puissances entières, le premier membre contient q avec des exposants de la forme

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

donc tout entier est la somme de 4 carrés.

La théorie des fonctions elliptiques conduit encore à un autre résultat qui mérite d'être signalé, on a en effet

$$\frac{1}{2^4}\left(2q^{\frac{1}{4}} + \ldots 2q^{\left(\frac{2n+1}{4}\right)^2}\ldots\right)^4 = \frac{q}{1-q^2} + \frac{3q^3}{1-q^6} + \frac{5q^5}{1-q^{10}}\ldots$$

et en identifiant après avoir mis le second nombre sous la forme :

$$q + q^3 + q^6 + \ldots + 3(q^3 + q^9 + \ldots) + 5(q^5 + q^{15}\ldots)$$

développement qui contient toutes les puissances impaires de q. On en conclut que :

Tout nombre impair est la somme de 4 carrés de la forme $\left(\frac{m}{2}\right)^2$, m étant un nombre impair ou :

Le quadruple d'un nombre impair est la somme de 4 carrés impairs.

Les identités qui précèdent font partie d'un groupe de formules extrêmement remarquables dues à Euler et à Jacobi, et dont la démonstration peut être rendue indépendante de la théorie des fonctions elliptiques. Mais c'est alors ôter à ces formules tout leur intérêt. Car la théorie des fonctions elliptiques fournit ces formules tout naturellement et sans que l'on ait eu besoin de les chercher.

CHAPITRE V

LES NOMBRES PREMIERS

1. — Théorème de Wilson

Nous avons déjà démontré que si p était un nombre premier on avait :

$$1.2.3...(p-1)+1 \equiv 0 \pmod{p}.$$

Nous allons démontrer de nouveau ce théorème en le complétant.

Observons d'abord que si p est premier et si $a < p$,

$$a, 2a, 3a, \ldots (p-1)a$$

divisés par p laissent des restes différents et égaux à l'ordre près à

$$1, 2, 3, \ldots p-1 ;$$

(p. 51) donc il existe un nombre b tel que

$$ab \equiv 1 \pmod{p}.$$

et il ne peut en exister qu'un seul, en effet si l'on pouvait avoir

$$ab \equiv ac,$$

on aurait $a(b-c) \equiv o$, ce qui est absurde, ni a, ni b, ni c, ni $b-c$ ne pouvant être divisibles par p.

On ne peut pas avoir en général

$$a^2 \equiv 1,$$

car on en conclurait

$$(a-1)(a+1) \equiv 0,$$

ou

$$a-1 \equiv 0, \quad a+1 \equiv 0,$$

cela peut avoir lieu si $a \equiv 1$, ou $a \equiv p - 1$, c'est-à-dire si $a = 1$ ou $a = p - 1$.

Si donc on laisse 1 et $p - 1$ de côté et si l'on associe tous les autres nombres 2, 3,... $p - 2$ deux à deux de telle sorte que

$$ab \equiv 1 ;$$

et si l'on fait le produit de ces formules, on a :

$$2.3... (p - 2) \equiv 1,$$

et si l'on multiplie par

$$1.(p - 1) \equiv -1,$$

on a le théorème de Wilson :

$$1.2.3... (p - 1) \equiv -1 \pmod{p}.$$

La démonstration suppose $p > 2$, mais on a $1 \equiv -1 \pmod{2}$.

Si p n'est pas premier, soit $p = qr$, q désignant un des diviseurs de p (supérieur à 1) ; la suite 1, 2, 3,... $(p - 1)$, contiendra les facteurs q et r, et par suite 1. 2,... $(p - 1)$ sera divisible par p. Cela peut ne pas avoir lieu, si p ne peut pas être décomposé en facteurs inégaux, p est alors le produit q^2 de deux facteurs premiers égaux à q, mais la suite 1, 2,... $p - 1$ contient alors le facteur q et si $q > 2$, le facteur $2q$ et par suite 1, 2,... $(p - 1)$ est divisible par $q^2 = p$, enfin si $q = 2$, $p = 4$ et l'on n'a pas 1. 2. 3 $\equiv 0 \pmod{4}$.

En résumé *si l'on désigne par* $\Gamma(p)$ *la fonction eulérienne de seconde espèce, et si p est premier on a :*

$$\Gamma(p) \equiv -1 \pmod{p}.$$

Si p est composé, et différent de 4

$$\Gamma(p) \equiv 0, \pmod{p} ;$$

enfin

$$\Gamma(4) \equiv 2 \pmod{4}.$$

Le théorème de Wilson exprime donc une propriété caractéristique des nombres premiers.

Corollaire 1er. — Si l'on considère le binôme $x^{\Gamma(p)} - 1$, et

si on le divise par $x^p - 1$, on trouve pour restes successifs :

$$x^{r(p)-p} - 1, \qquad x^{r(p)-2p} - 1, \qquad x^{r(p)-3p} - 1, \ldots$$

donc :

Si p est premier, $x^{r(p)} - 1$ n'est pas divisible par $x^p - 1$, et le reste est $x^{p-1} - 1$; si au contraire p est composé $x^{r(p)} - 1$ est divisible par $x^p - 1$. (On suppose $p \geq 4$).

Supposons p premier impair, on aura :

$$\begin{aligned} p - 1 &= -1, \\ p - 2 &= -2, \\ &\cdots\cdots \\ p - \frac{p-1}{2} &= -\frac{p-1}{2}. \end{aligned}$$

donc :

$$1.2.3\ldots(p-1) = \pm 1^2.2^2\ldots\left(\frac{p-1}{2}\right)^2,$$

il faudra prendre le signe + si $\frac{p-1}{2}$ est pair et — dans le cas contraire, donc comme

$$1.2\ldots(p-1) = -1,$$

on aura

$$1 = 1^2.2^2\ldots\left(\frac{p-1}{2}\right)^2 \qquad \text{si } \frac{p-1}{2} = 2k, \qquad p = 4k+1,$$

$$-1 = 1^2.2^2\ldots\left(\frac{p-1}{2}\right)^2 \qquad \text{si } \frac{p-1}{2} = 2k+1, \qquad p = 4k+3.$$

Ces résultats complètent le théorème de Wilson.

2. — Généralisation du théorème de Wilson

En général *si l'on considère une fonction symétrique f de a_1, $a_2\ldots a_{p-1}$, p désignant un nombre premier, et si l'on y fait $a_1 = 1$, $a_2 = 2, \ldots a_{p-1} = p - 1$, on obtiendra un nombre divisible par p, excepté si f est de degré $p - 1$.*

Démontrons d'abord cette proposition pour le cas où f est de la forme $a^q_1 + a^q_2 + \ldots + a^q_{p-1}$. Nous avons démontré la formule

$$\sum_1^x x^q = \frac{x(x+1)}{2!}\Delta 0^q + \frac{(x+1)x(x-1)}{3!}\Delta^2 0^q + \ldots$$

si l'on y fait $x = p - 1$, on a :

$$\sum_{1}^{p-1} x^q = \frac{p(p-1)}{2!}\Delta o^q + \frac{p(p-1)(p-2)}{3!}\Delta^2 o^q + \ldots$$

1° Supposons $q < p - 1$, le dernier terme du second membre sera

$$\frac{p(p-1)\ldots(p-q)}{1.2\ldots(q+1)}\Delta^q o^q$$

et sera divisible par p ainsi que les précédents, ce qui démontre le théorème énoncé ;

2° Si $q = p - 1$, le dernier terme est $\Delta^q o^q$, et il n'est plus possible de rien conclure ;

3° Si $q > p - 1$ le dernier terme est

$$\Delta^{p-1} o^{p-1}$$

et il est encore impossible de rien conclure. Mais si $a < p$, en vertu du théorème de Fermat

$$a^k = a^{p+k-1} \pmod{p},$$

et en sommant :

$$\sum_{1}^{p-1} a^k = \sum_{1}^{p-1} a^{p+k-1} \pmod{p};$$

or si $k < p - 1$, le premier membre est divisible par p, le second l'est aussi, donc le théorème est vrai, pour $q = 1, 2\ldots p - 1, p + 1, \ldots 2p - 2, 2p + 1, \ldots 3p - 3\ldots$

c.q.f.d.

De là il est facile de passer aux fonctions symétriques quelconques en faisant usage des formules qui lient ces fonctions aux sommes des puissances des racines. (Voyez du reste p. 53.)

3. — Autres théorèmes sur les nombres premiers

On sait qu'il existe une infinité de nombres premiers, voici une démonstration de ce fait qui jettera un peu de jour sur la nature des nombres premiers, qui est due à Euler et qui a été le point de départ de recherches importantes.

Soient $p_1 = 2$, $p_2 = 3$, p_3, p_4,... les nombres premiers successifs, on a :

$$\frac{1}{1-\frac{1}{p_1^i}}\,\frac{1}{1-\frac{1}{p_2^i}}\,\frac{1}{1-\frac{1}{p_3^i}}\ldots = \left(1+\frac{1}{p_1^i}+\frac{1}{p_1^{2i}}\ldots\right)\left(1+\frac{1}{p_2^i}+\ldots\right)$$

le second nombre développé est de la forme $\sum \frac{1}{p_1^{\alpha i}\, p_2^{\beta i}} \ldots$

or $p_1^{\alpha}\ p_2^{\beta}\ldots$ est un entier quelconque, donc

$$(1) \qquad \frac{1}{1-\frac{1}{p_1^i}}\cdot\frac{1}{1-\frac{1}{p_2^i}}\ldots = 1 + \sum \frac{1}{2^i} + \frac{1}{3^i} + \ldots \frac{1}{p^i} \ldots ;$$

si l'on suppose $i = 1$ le second membre de cette formule est divergent, le premier est donc infini, ce qui ne peut avoir lieu que si le nombre des entiers premiers est infini. Si l'on suppose $i > 1$, et si on prend les logarithmes des deux membres de (2), on a

$$\Sigma \frac{1}{p^i} + \frac{1}{2}\Sigma \frac{1}{p^{2i}} + \frac{1}{3}\Sigma \frac{1}{p^{3i}} \ldots = \sum_{2}^{\infty} \frac{1}{n^i} - \frac{1}{2}\left(\sum_{2}^{\infty} \frac{1}{n^i}\right)^2 + \ldots$$

relation remarquable entre les nombres premiers, en différenciant par rapport à i on a :

$$\Sigma \frac{1}{p^i} \log. p + \Sigma \frac{1}{p^{2i}} \log. p + \ldots = \Sigma \frac{1}{n^i} \log. n + \ldots$$

Soient $p_1 = 2, p_2, \ldots$ les nombres premiers successifs, si l'on forme le produit

$$\Pi (1 - p_i^{-s}),\ s > 1,$$

on voit qu'il sera de la forme

$$\Sigma\, \varepsilon_n\, n^{-s}$$

n désignant un entier quelconque, quand à ε_n, on voit qu'il est égal à 1, si $n = 1$, qu'il est nul si n est divisible pas un carré, enfin $\varepsilon_n = (-1)^{\nu}$ quand n est le produit de ν nombres premiers différents. On a ainsi

$$\Pi (1 - p^{-s}) = \Sigma\, \varepsilon_n\, n^{-s}$$

ou

$$\frac{1}{\Pi (1 - p^{-s})} = \frac{1}{\Sigma\, \varepsilon_n\, n^{-s}}$$

ou en vertu de la formule d'Euler :

$$\frac{1}{\Sigma \varepsilon_n n^{-s}} = \Sigma n^{-s}.$$

On peut démontrer *que* $\Sigma \varepsilon_m = 0$, *si* m *est pris successivement égal à tous les diviseurs d'un entier* k ; soient en effet d_1, d_2... d_n les diviseurs premiers de k, $\varepsilon_1 = 1$, les ε_d sont égaux à -1 et au nombre de n, les $\varepsilon_{dd'}$ sont égaux à 1 et au nombre de $\frac{n(n-1)}{1.2}$ etc., donc

$$\Sigma \varepsilon_\mu = 1 - \frac{n}{1} + \frac{n(n-1)}{1.2} - \ldots = (1-1)^n = 0.$$

c.q.f.d.

Soient $f(n)$ *et* $g(n)$ *deux fonctions de* n *et supposons que*

$$g(mn) = g(m)\, g(n), \tag{1}$$

si l'on a

$$\psi(n) = \Sigma f(d)\, g(d'), \quad (dd' = n), \tag{2}$$

on aura

$$f(n) = \Sigma \varepsilon_d\, g(d)\, \psi(d'). \tag{3}$$

En effet portant dans (3) la valeur de ψ donnée par (2) on a

$$f(n) = \Sigma \varepsilon_d\, g(d)\, g(d_1)\, f(d_2),$$
$$= \Sigma \varepsilon_d\, g(dd_1)\, f(d_2), \quad (dd_1 d_2 = n)$$

ou

$$f(n) = \Sigma f(\delta)\, g(\delta') \Sigma \varepsilon_d \quad (\delta\delta' = n),$$

ce qui se réduit à une identité, car on a

$$\Sigma \varepsilon_d = 0.$$

Excepté pour $\delta' = 1$ et $\delta = \delta'$.

4. — Autres théorèmes sur les nombres premiers

Soit $f(x)$ *un polynôme à coefficients entiers*

$$f(x) = a_0 + a_1 x + a_2 x_2 \ldots$$

Les nombres $f(0)$, $f(1)$, $f(2)$... *ne peuvent pas être tous premiers.*

En effet en appelant p un nombre premier égal à $f(x_0)$ on aura

$$f(x_0 + py) = f(x_0), \text{ (mod. } p),$$

donc

$$f(x_0 + py) = 0$$

et $f(x_0 + py)$ n'est pas premier.

Pour qu'un nombre impair p soit premier, il faut et il suffit qu'il soit et d'une seule manière la différence de deux carrés.

En effet si l'on pose :

$$p = x^2 - y^2,$$

on aura

$$p = (x + y)(x - y);$$

comme p est premier, il faut que

$$x - y = 1, \quad x + y = p,$$

et

$$p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2.$$

Pour reconnaître si p est premier, on formera toutes les sommes $p + 1^2$, $p + 2^2$, aucune de ces sommes ne devra être un carré excepté, $p + \left(\frac{p-1}{2}\right)^2$.

On peut toujours trouver n nombres consécutifs qui ne soient pas premiers.

En effet soit $m = 1.2 \ldots (n+1)$ ou même soit m un multiple de 2, 3... $(n+1)$ les nombres

$$m + 2, m + 3, \ldots m + n + 1$$

ne sauraient être premiers, car ils sont divisibles, le premier par 2, le suivant par 3, le suivant par 4...

Tous les nombres premiers sont des nombres représentés par les formes suivantes, qui malheureusement en représentent beaucoup d'autres :

$$2n \pm 1, \text{ et } 2 ; x^2 + x + 17 ; 2x^2 + 29 ;$$
$$6n \pm 1, \text{ et } 2, 3 ; (1)\ x^2 + x + 41.$$

---

(1) M. Hermite a remarqué que

$$e^{\pi\sqrt{43}}, \qquad e^{\pi\sqrt{67}}, \qquad e^{\pi\sqrt{163}}$$

étaient extrêmement peu différents de nombres entiers, il y aurait

5. — Une application du théorème de Wilson

Le reste de la division de $x^m - 1$ par $x^n - 1$, en supposant $n < m$ est $x^k - 1$, k désignant le reste de la division de m pas n, donc en observant que $\Gamma(n)$ est divisible par n, si n est composé $\leqq 4$, et que le reste de la division est $n - 1$ si n est premier, on en conclura que le reste de la division de $x^{\Gamma(n)} - 1$ par $x^n - 1$ est 0 ou $x^{n-1} - 1$ suivant que n est composé ou premier. Donc si n est premier

$$x^{\Gamma(n)} - 1 = Q(x^n - 1) + x^{n-1} - 1,$$

ou

$$x^{\Gamma(n)} = Q(x^n - 1) + x^{n-1},$$

et même Q désignant un polynôme entier

$$\left(\frac{x}{n}\right)^{\Gamma(n)} = Q\left[\left(\frac{x}{n}\right)^n - 1\right] + \left(\frac{x}{n}\right)^{n-1};$$

en divisant par $\left(\frac{x}{n}\right)^n - 1$ et en observant que Q est un polynôme entier

$$\mathcal{E}\frac{\left(\frac{x}{n}\right)^{\Gamma(n)}}{\left(\frac{x}{n}\right)^n - 1} = \mathcal{E}\frac{\left(\frac{x}{n}\right)^{n-1}}{\left(\frac{n}{x}\right)^n - 1} = n,$$

et plus généralement

$$\mathcal{E}\frac{\left(\frac{x}{n}\right)^{\Gamma(n)}}{\left(\frac{x}{n}\right)^n - 1}\frac{1}{n^i} = \frac{1}{n^i - 1}$$

Si n est composé, le second membre de cette formule doit être remplacé par zéro.

Examinons le cas de $n = 4$, $\Gamma(4) = 6$, on a :

$$x^6 - 1 = (x^3 - 1)x^2 + x^2 - 1,$$
$$x^6 = (x^3 - 1)x^2 + x^2,$$
$$\frac{x^6}{x^3 - 1} = x^2 + \frac{x^2}{x^3 - 1}.$$

---

peut-être lieu de se demander si p désignant un nombre premier, $e^{\pi f(p)}$ ne serait pas un entier en choisissant convenablement la fonction $f(p)$.

Le résidu de $\frac{x^n}{x^4-1}$ est nul, ainsi le nombre 4 ne fait pas exception à la règle.

Posons alors

$$\psi_1(x) = 1 + \frac{\left(\frac{x}{2}\right)^{\Gamma(2)}}{\left(\frac{x}{2}\right)^2 - 1}\frac{1}{2^1} + \ldots \frac{\left(\frac{x}{n}\right)^{\Gamma(n)}}{\left(\frac{x}{n}\right)^n - 1}\frac{1}{n^1} + \ldots$$

la série $\psi_1(x)$ sera convergente quel que soit x, excepté pour les valeurs de x rendant quelque terme infini. Et l'on a

$$\mathcal{E}\,\psi^1(x) = \Sigma\,\frac{1}{p^1-1}$$

p désignant un nombre premier.

Considérons alors la fonction

$$\theta(x) = \left(1 - \frac{x^2}{p_1^2}\right)\left(1 - \frac{x^2}{p_2^2}\right)\left(1 - \frac{x^2}{p_3^2}\right)\ldots,$$

où $p_1 = 2$, $p_2 = 3$, $p_3 = 5\ldots$ désignent les nombres premiers successifs, on aura :

$$\frac{\theta'(x)}{\theta(x)} = \sum\left(\frac{1}{x+p} + \frac{1}{x-p}\right),$$

c'est-à-dire

$$\frac{\theta'(x)}{\theta(x)} = -2\left[x\,\Sigma\,\frac{1}{p^2} + x^3\,\Sigma\,\frac{1}{p^4} + \ldots\right],$$

ou

$$\frac{\theta'(x)}{\theta(x)} = -2x\left[\mathcal{E}\,\psi_2(x) + x^2\,\mathcal{E}\,\psi_3(x) + \ldots\right];$$

ce qui donne en remplaçant les ψ par leurs valeurs

$$-\frac{\theta'(x)}{\theta(x)} = 2x\left[\mathcal{E}\sum\frac{\left(\frac{x}{n}\right)^{\Gamma(n)}}{\left(\frac{x}{n}\right)^n - 1}\frac{1}{n^2} + \mathcal{E}\sum\frac{\left(\frac{x}{n}\right)^{\Gamma(n)}}{\left(\frac{x}{n}\right)^n - 1}\frac{x^2}{n^3} + \ldots\right],$$

ou enfin

$$\frac{\theta'(x)}{\theta(x)} = 2\mathcal{E}\sum \frac{\left(\frac{x}{n}\right)^{\Gamma(n)}}{\left(\frac{x}{n}\right)^{n}-1}\,\frac{x}{n}\,\frac{1}{x^2-n^2}$$

Si alors on pose

$$f(x) = \mathcal{E}\sum \frac{\left(\frac{x}{n}\right)^{\Gamma(n)}}{\left(\frac{x}{n}\right)^{n}-1}\,\frac{2x}{x^2-n^2}\,\frac{1}{x},$$

on voit que

$$\frac{\theta'(x)}{\theta(x)} = f(x), \qquad \theta(x) = e^{\int f(x)\,dx},$$

et l'on a ainsi une fonction $\theta(x)$ qui s'annule pour toutes les valeurs de x qui sont des entiers positifs ou négatifs premiers, et qui ne s'annule pour aucune autre valeur de x.

6. — Théorème de Polignac

Soit $\Pi(n) = 1.2.3\ldots n$ *et* $P(n)$ *le produit des nombres premiers inférieurs à* $n+1$, *on aura :*

$$\Pi(n) = P(n) \times P\left(\frac{n}{2}\right) \times P\left(\frac{n}{3}\right)\ldots$$
$$\times P\left(\sqrt{n}\right) \times P\left(\sqrt{\frac{n}{2}}\right) \times P\left(\sqrt{\frac{n}{3}}\right)\ldots$$
$$\times P\left(\sqrt[3]{n}\right) \times P\left(\sqrt[3]{\frac{n}{2}}\right) \times P\left(\sqrt[3]{\frac{n}{3}}\right)\ldots$$
$$\times \ldots\ldots\ldots\ldots\ldots\ldots$$

En effet soit θ un nombre premier, cherchons combien de fois il entre en facteur dans $\Pi(n)$, soit :

$$\theta^i \leq n < \theta^{i+1}.$$

Les facteurs de 1, 2,... n, multiples de θ, sont :

$$\theta,\ 2\theta,\ 3\theta,\ldots\ E\left(\frac{n}{\theta}\right)\theta;$$

θ entre donc au moins $E\left(\frac{n}{\theta}\right)$ fois comme facteur dans $\Pi(n)$;

mais ce n'est pas tout, car parmi ces facteurs, multiples de 0, il y en a qui contiennent plusieurs fois 0, il y entrera encore autant de fois que dans le produit

$$1.2.3...\mathrm{E}\left(\frac{n}{0}\right),$$

c'est-à-dire au moins $\mathrm{E}\left(\frac{n}{0^2}\right)$ fois, et ainsi de suite ; il y entre donc en tout

$$\mathrm{E}\left(\frac{n}{0}\right)+\mathrm{E}\left(\frac{n}{0^2}\right)+\mathrm{E}\left(\frac{n}{0^3}\right)\ldots\text{fois.}$$

Si 0 entre en facteur dans $\mathrm{P}\left(\sqrt[k]{\frac{n}{\mathrm{N}}}\right)$, ce produit ne le renferme qu'une fois, mais s'il le renferme

$$\mathrm{P}\left(\sqrt[k]{n}\right),\ \mathrm{P}\left(\sqrt[k]{\frac{n}{2}}\right)\ldots\ \mathrm{P}\left(\sqrt[k]{\frac{n}{\mathrm{N}-1}}\right)$$

le renfermeront aussi une fois en sorte que

$$\mathrm{P}\left(\sqrt[k]{n}\right)\times\mathrm{P}\left(\sqrt[k]{\frac{n}{2}}\right)\times\mathrm{P}\left(\sqrt[k]{\frac{n}{3}}\right)\ldots$$

renfermera le facteur 0 autant de fois qu'il y a d'unités dans le nombre N défini par la relation

$$\sqrt[k]{\frac{n}{n+1}}<0\leq\sqrt[k]{\frac{n}{\mathrm{N}}}$$

ou

$$\frac{n}{\mathrm{N}+1}<0^k<\frac{n}{\mathrm{N}},$$

ou

$$\mathrm{N}+1>\frac{n}{0^k}>\mathrm{N},$$

donc

$$\mathrm{N}=\mathrm{E}\left(\frac{n}{0^k}\right).$$

e second membre de (1) contient donc 0

$$\mathrm{E}\left(\frac{0}{n}\right)+\mathrm{E}\left(\frac{n}{0^2}\right)+\mathrm{E}\left(\frac{n}{0^3}\right)\ldots\text{ fois}$$

comme le premier, la formule (1) est donc démontrée.

7. — Théorème de Tchebychef

Si l'on a

$$F(x) = \sum_{n=1}^{n=\infty} \sum_{\alpha=1}^{\alpha=\infty} f(n x^{\alpha}),$$

on aura

$$\log 2\, f(2) + \log 3\, f(3) \ldots + \log n\, f(n) + \ldots$$
$$= \log 2\, F(2) + \log 3\, F(3) + \log 5\, F(5) \ldots + \log p\, F(p) \ldots$$

p désignant un nombre premier.

Si en effet dans la série

$$(1) \qquad \log 2\, f(2) + \log 3\, f(3) \ldots + \log n\, f(n) \ldots,$$

on met le terme général sous la forme

$$\log (p^{\alpha} N)\, f(p^{\alpha} N), \quad (n = p^{\alpha} N),$$

p désignant un facteur premier qui n'entre plus dans N, cette série devient

$$\log 2\, f(2) + \ldots + (\alpha \log p + \log N)\, f(p^{\alpha} N) + \ldots;$$

le coefficient de $\log p$ est

$$f(pN) + 2 f(p^2 N) \ldots + \alpha f(p^{\alpha} N) \ldots$$

ou

$$\begin{aligned} f(pN) + f(p^2 N) \ldots + f(p^{\alpha} N) \ldots \\ + f(p^2 N) \ldots + f(p^{\alpha} N) \ldots \\ + \ldots\ldots\ldots \\ + f(p^{\alpha} N), \end{aligned}$$

ou encore

$$\begin{aligned} f(pN) + f(pN.p) + f(pN.p^{\alpha-1}) + \ldots \\ + f(p^2 N) + f(p^2 N.p^{\alpha-2}) + \ldots \\ \ldots\ldots\ldots\ldots \\ + f(p^{\alpha} N) + \ldots; \end{aligned}$$

or N, pN, p^2N... est la suite des nombres naturels, quand N prend toutes les valeurs possibles, donc (1) peut s'écrire :

$$\Sigma \log p \sum_{\alpha=1}^{\alpha=\infty} \sum_{k=1}^{k=\infty} f(p^{\alpha} n) = \Sigma \log p\, F(p).$$

c.q f.d.

Pour $f(x) = 1$ quand $x \leq n$ et $f(x) = 0$ pour $x > n$, on a le théorème de Polignac.

8. — Sur le nombre des entiers premiers compris entre des limites données

On a vu que $\Gamma(x) + 1$ est divisible par x quand x est premier, si au contraire x est composé $\Gamma(x)$ est divisible par x, le nombre 4 fait exception à cette règle.

Si donc on considère la fonction

$$\sin 2\pi \frac{\Gamma(x)}{x},$$

si x est premier, elle se réduira à $-\sin \frac{2\pi}{x}$; et si x est composé elle se réduira à 0, donc

$$\frac{\sin \frac{2\pi \Gamma(x)}{x}}{\sin \frac{2\pi}{x}}$$

se réduit à -1 ou à 0, suivant que x est premier ou composé, donc

$$S = -\sum_{x=a}^{x=b} \frac{\sin 2\pi \frac{\Gamma(x)}{x}}{\sin \frac{2\pi}{x}}$$

si $a > 4$ donnera la totalité des nombres premiers compris entre a et b ; on peut aussi écrire :

$$S = -2\pi\sqrt{-1}\, \mathcal{E} \frac{\sin 2\pi \frac{\Gamma(z)}{z}}{\sin \frac{2\pi}{z}} \frac{e^{2\pi z\sqrt{-1}}}{e^{2\pi z\sqrt{-1}} - 1}$$

et l'on peut supprimer sans inconvénient le facteur $e^{2\pi z\sqrt{-1}}$ au numérateur sous le signe $\mathcal{E}$.

La totalité des nombres premiers contenus dans la progression arithmétique

$$a, \quad a+r, \quad a+2r \ldots \quad a+kr$$

s'obtiendra en observant que ces nombres sont racines de

$$e^{\frac{2\pi\sqrt{-1}}{r}z} - e^{\frac{2\pi\sqrt{-1}}{r}a} = 0$$

en sorte que le nombre en question sera

$$-\mathcal{E}\frac{\sin 2\pi\frac{\Gamma(z)}{z}}{\sin\frac{2\pi}{z}}\cdot\frac{2\pi\sqrt{-1}}{r}\cdot\frac{e^{2\pi\sqrt{-1}\frac{z}{r}}}{e^{2\pi\sqrt{-1}\frac{z}{r}} - e^{2\pi\sqrt{-1}\frac{a}{r}}}$$

Le signe $\mathcal{E}$ s'étendant à toutes les valeurs $z = a, a + r \ldots, a + kr$ de z, parmi lesquelles ne doit pas figurer le nombre 1.

Le jeune Dérichlet a prouvé que toute progression arithmétique dont la raison et le premier terme sont premiers entre eux, renferme une infinité de nombres premiers, une traduction de son mémoire par Terquem, a paru dans le T. IV du *Journal de Liouville* (1re série). Malheureusement cette démonstration est très longue et ne saurait trouver place ici. Peut être les considérations qui précèdent permettront-elles d'en trouver une plus simple.

9. — Autre solution

Considérons le produit

$$\left.\begin{array}{l}(1-x)(1-x^2)\ldots(1-x^{n-1})\\(1-x^2)(1-x^4)\ldots(1-x^{2n-2})\\\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\(1-x^{n-1})(1-x^{2n-2})\ldots(1-x^{(n-1)(n-1)})\end{array}\right\} = F_n(x)$$

si n est premier, toutes les racines $\alpha, \alpha^2, \alpha^{n-1}$ différentes de 1 de $x^n - 1 = 0$ sont primitives, toutes les lignes qui forment le produit $F_n(n)$ sont égales entre elles pour $x = \alpha, \alpha^2, \ldots \alpha^{n-1}$, en sorte que

$$\begin{aligned}F_n(x) &= [(1-x)(1-x^2)\ldots(1-x^{n-1})]^{n-1}\\&= [(z-\alpha)(z-\alpha^2)\ldots(z-\alpha^{n-1})]^{n-1} \text{ pour } z = 1\\&= \left(\frac{z^n-1}{z-1}\right)^{n-1} \text{ pour } z = 1\\&= n^{n-1}.\end{aligned}$$

si n est composé, l'une des lignes du produit F_n est nulle pour $x = \alpha$, α étant une racine de $x^n - 1 = 0$, et

$$F_n(\alpha) = 0$$

donc $F_n(\alpha)$ *est égal à* n^{n-1} *ou à zéro, suivant que n est premier ou composé,* α *désignant une racine quelconque de*

$$\frac{x^n - 1}{x - 1} = 0.$$

Si n est composé $F(x)$ est divisible par $\frac{x^n - 1}{x - 1}$; si n est premier, on a en appelant Q un polynôme entier :

$$\frac{F_n(x)}{x^n - 1} = Q(x) + \sum \frac{F_n(\alpha)}{x - \alpha} \cdot \frac{\alpha}{n},$$

ou

$$\frac{F_n(x)}{x^n - 1} = Q(x) + \sum \frac{n^{n-2}}{x - \alpha} \alpha ;$$

mais

$$\frac{1}{x^n - 1} = \frac{1}{x - 1} \cdot \frac{1}{n} + \sum \frac{\alpha}{x - \alpha} \frac{1}{n} ;$$

donc

$$\frac{F_n(x)}{x^n - 1} = Q(x) + n^{n-2} \left[\frac{n}{x^n - 1} - \frac{1}{x - 1} \right],$$

et

$$F_n(x) = Q(x)(x^n - 1) + n^{n-1} - n^{n-2} \frac{x^n - 1}{x - 1} ;$$

cette équation est de la forme

$$F_n(x) = Q'(x) \frac{x^n - 1}{x - 1} + n^{n-1},$$

Q' étant un polynôme entier. Donc :

Le reste de la division de $F_n(x)$ *par* $\frac{x^n - 1}{x - 1}$ *est* 0 *ou* n^{n-1} *suivant que n est un nombre composé ou premier.*

Le résidu de $\frac{F_n(z)}{z^n - 1}$ sera $\Sigma \frac{F_n(\alpha)}{n z^{n-1}}$ ou $\frac{1}{n} \Sigma F_n(\alpha) \alpha$ et comme $F_n(\alpha) = n^{n-1}$ et $\Sigma \alpha = -1$ (Si n est premier)

$$\mathcal{E} \frac{F_n(z)}{z^n - 1} = -n^{n-2},$$

et

$$\mathcal{E}\,\frac{F_n(z)}{1-z^n} = n^{n-2},$$

par suite

$$\mathcal{E}\,\frac{F_n\left(\frac{z}{n}\right)}{n^n - z^n} = \frac{1}{n}$$

Si n est composé $F_n(z)$ est divisible par $z^n - 1$ et le résidu est nul, de sorte que

$$(1) \qquad \mathcal{E}\,\frac{n\,F_n\left(\frac{z}{n}\right)}{n^n - z^n} = \begin{cases} 1 \text{ si } n \text{ est premier,} \\ 0 \text{ si } n \text{ est composé.} \end{cases}$$

et

$$\sum_{n=a}^{n=b} \mathcal{E}\,\frac{n\,F_n\left(\frac{z}{n}\right)}{n^n - z^n}$$

donnera le nombre des entiers premiers compris entre a et b inclusivement.

La série

$$\sum \frac{n\,F_n\left(\frac{z}{n}\right)}{n^n - z^n}$$

est manifestement convergente pour toutes les valeurs de z qui ne sont pas entières.

La formule (1) montre en outre que

$$\mathcal{E}\,\frac{1}{n^{i+1}}\,\frac{F_n\left(\frac{z}{n}\right)}{n^n - z^n} \begin{cases} \frac{1}{n^i} \text{ si } n \text{ est premier,} \\ 0 \text{ si } n \text{ est composé,} \end{cases}$$

et en général

$$\mathcal{E}\,\frac{n}{n^2 - x^2}\,\frac{F_n\left(\frac{z}{n}\right)}{n^n - z^n}$$

sera égal à $\frac{1}{n^2 - x^2}$, si n est premier et à zéro dans le cas

contraire ; on a donc en appelant p un nombre premier

$$\sum \mathcal{E} \frac{2nx}{n^2 - x^2} \frac{F_n\left(\frac{z}{n}\right)}{n^n - z^n} = \sum \frac{2x}{p^2 - x^2}.$$

Nous avons un nouveau moyen pour former la fonction θ dont toutes les racines sont les nombres premiers positifs ou négatifs, car la fonction précédente est $\frac{\theta'(x)}{\theta(x)}$ au signe près.

Cette formule a sur celle que nous avons trouvée plus haut l'avantage de ne pas contenir dans son expression la transcendante Γ.

10. — Nouvelle solution

La série double

$$(1) \qquad \begin{array}{l} \frac{1}{1-x^2} + \frac{1}{2^2-x^2} + \frac{1}{3^2-x^2} + \cdots \\ \frac{1}{2^2-x^2} + \frac{1}{4^2-x^2} + \frac{1}{6^2-x^2} + \cdots \\ \frac{1}{3^2-x^2} + \frac{1}{6^2-x^2} + \frac{1}{9^2-x^2} + \cdots \\ \cdots\cdots\cdots\cdots\cdots \end{array}$$

est convergente, car son terme général est $\frac{1}{m^2 n^2 - x^2}$, et l'intégrale double :

$$\int_a^\infty \int_a^\infty \frac{dm\,dn}{m^2 n^2 - x^2}, \quad (a > x)$$

est finie. Otons la première ligne et la première colonne, nous aurons encore une série convergente dont la valeur $\varphi(x)$ est une fonction admettant pour infinis tous les nombres composés positifs ou négatifs et seulement ces nombres. Ces infinis sont d'ailleurs simples. Il en résulte, d'après un théorème connu de Cauchy, que la totalité des nombres composés compris entre a et b sera donnée par la formule :

$$\frac{1}{\pi} \int_a^b \frac{\varphi'(x)\,dx}{1 + \varphi^2(x)}$$

à la quantité $\frac{1}{\pi}$ (arctg $\varphi(b)$ — arctg $\varphi(a)$ près.

Donc à cette quantité près la totalité des nombres premiers compris entre a et b sera

$$b - a - \frac{1}{\pi} \int_a^b \frac{\varphi'(x)\,dx}{1 + \varphi^2(x)}.$$

Quant à la fonction $\varphi(x)$ on l'obtient comme il suit : La fonction représentée par la formule (1) est :

$$\left[\frac{1}{2x}\left(\pi \operatorname{cotg} \pi x - \frac{1}{x}\right) + \frac{2}{2x}\left(\pi \operatorname{cotg} \frac{\pi x}{2} - \frac{2}{x}\right) + \dots \right]$$

donc :

$$\varphi(x) = -\sum_2^\infty \frac{n\pi}{2x}\left[\operatorname{cotg}\frac{\pi x}{n} - \frac{n}{x}\right] + \frac{\pi}{2x}\operatorname{cotg}\pi x - \frac{1}{2x^2} + \frac{1}{1-x^2}$$

11. — Recherches de Tchebychef

Désignons par $\varphi(x)$ la totalité des nombres premiers inférieurs à x, alors $\varphi(x+1) - \varphi(x)$ ou $\Delta\varphi(x)$ représentera 1 ou zéro suivant que x sera premier ou ne le sera pas.

Considérons les expressions :

$$(1) \quad \begin{cases} \sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}\log\rho - \sum' \log\left(1 - \frac{1}{\mu^{1+\rho}}\right) \\ \sum' \log\left(1 - \frac{1}{\mu^{1+\rho}}\right) + \sum' \frac{1}{\mu^{1+\rho}}, \end{cases}$$

dans lesquelles Σ' est une somme relative aux nombres premiers, en sorte que par exemple :

$$\sum' \frac{1}{\mu^3} = \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{5^3} + \frac{1}{7^3} \dots ;$$

d'ailleurs nous supposerons que les sommes Σ sont prises de 2 à ∞ en sorte que, par exemple

$$\sum \frac{1}{m^3} = \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \dots$$

Chacune des expressions (1) *tend vers une limite finie quand* ρ *tend vers* 0, *ainsi que ses dérivées relatives à* ρ.

Occupons-nous de la première, on a

$$\int_0^\infty e^{-mx} x^\rho dx = \frac{\Gamma(\rho+1)}{m^{\rho+1}},$$

et par conséquent

$$\int_0^\infty \frac{e^{-x}}{e^x-1} x^\rho dx = \Gamma(\rho+1) \sum \frac{1}{m^{\rho+1}}.$$

or, on a aussi

$$\int_0^\infty e^{-x} x^{\rho-1} dx = \frac{1}{\rho} \Gamma(\rho+1);$$

d'où l'on conclut par soustraction

$$\int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) x^\rho dx = \Gamma(\rho+1) \left[\sum \frac{1}{m^{\rho+1}} - \frac{1}{\rho}\right],$$

et par conséquent, pour la première de nos expressions, la formule

$$\sum \frac{1}{m^{\rho+1}} - \frac{1}{\rho} = \frac{1}{\Gamma(\rho+1)} \int_0^\infty \left(\frac{1}{e^x-1} - \frac{1}{x}\right) x^\rho dx.$$

Cette formule est remarquable en elle-même et elle met en évidence le fait que nous avons énoncé.

Considérons maintenant la seconde expression ; on sait que (voir p. 95 formule d'Euler)

$$\left[\left(1-\frac{1}{2^{\rho+1}}\right)\left(1-\frac{1}{3^{\rho+1}}\right)\left(1-\frac{1}{5^{\rho+1}}\right)\cdots\right]^{-1} = 1 + \frac{1}{2^{\rho+1}} + \frac{1}{3^{\rho+1}} + \cdots$$

en prenant les logarithmes, on a

$$\sum{}' - \log\left(1-\frac{1}{\mu^{\rho+1}}\right) = \log\left(1+\sum \frac{1}{m^{\rho+1}}\right),$$

et en ajoutant $\log \rho$.

$$\log\rho - \sum{}' \log\left(1-\frac{1}{\mu^{\rho+1}}\right) = \log\left(1+\sum \frac{1}{m^{\rho+1}}\right)\rho$$
$$= \log\left[1+\rho+\rho\left(\sum \frac{1}{m^{\rho+1}} - \frac{1}{\rho}\right)\right].$$

Le premier membre est l'expression que nous voulons considérer, le dernier montre que cette expression est finie pour $\rho = 0$, ainsi que ses dérivées; car nous venons de prouver que cette propriété appartient à l'expression $\sum \frac{1}{m\rho + 1} - \frac{1}{\rho}$.

Enfin la troisième expression

$$\sum' \log\left(1 - \frac{1}{\mu^2 + 1}\right) + \sum' \frac{1}{\mu^2 + 1}$$

est égale à

$$-\frac{1}{2}\sum' \frac{1}{\mu^{2\rho} + 2} - \frac{1}{3}\sum' \frac{1}{\mu^{3\rho} + 3} - \dots;$$

et sous cette forme, on voit qu'elle est finie pour $\rho = 0$, ainsi que ses dérivées.

La somme

$$(1) \qquad \sum_{x=2}^{x=\infty} \left[\Delta\varphi(x) - \frac{1}{\log x}\right] \frac{\log^n x}{x^{1+\rho}}$$

tend vers une limite finie pour $\rho = 0$.

En effet, cette somme peut s'écrire :

$$\sum' \frac{\log^n \mu}{\mu^{1+\rho}} - \sum \frac{\log^{n-1} m}{m^{1+\rho}},$$

elle est égale au signe près à

$$\frac{d^{n-1}}{d\rho^{n-1}}\left(\sum \frac{1}{m^{1+\rho}} - \frac{1}{\rho}\right) + \frac{d^n}{d\rho^n}\left[\log\rho - \sum' \log\left(1 - \frac{1}{\mu^{1+\rho}}\right)\right]$$
$$- \frac{d^n}{d\rho^n}\left[\sum' \log\left(1 - \frac{1}{\mu^{1+\rho}}\right) + \sum' \frac{1}{\mu^{1+\rho}}\right].$$

Expression composée de sommes d'expressions que nous avons reconnu finies pour $\rho = 0$.

La somme

$$A = \sum_{x=2}^{x=\infty} \left[\Delta\varphi(x) - \int_x^{x+1} \frac{dx}{\log x}\right] \frac{\log^n x}{x^{1+\rho}}$$

tend vers une limite finie quand ρ *tend vers* 0.

En effet, considérons la différence

$$\frac{1}{\log x} - \int_x^{x+1} \frac{dx}{\log x} = \frac{1}{\log x} - \frac{1}{\log z},$$

z désignant une quantité comprise entre x et $x + 1$, elle peut s'écrire en posant $z = x + h$:

$$\frac{1}{\log x} - \frac{1}{\log (x+h)} = \frac{-h}{\log^2 (x+\theta h)} \frac{1}{(x+\theta h)},$$

elle est donc infiniment petite par rapport à $\frac{1}{x}$, et :

$$\left(\frac{1}{\log x} - \int_x^{x+1} \frac{dx}{\log x}\right) \frac{\log^n x}{x^{1+\rho}},$$

pour de grandes valeurs de x, sera d'ordre supérieur à $2 + \rho$ par rapport à $\frac{1}{x}$, et la somme

$$\sum_{x=x}^{x=\infty} \left[\frac{1}{\log x} - \int_x^{x+1} \frac{dx}{\log x}\right] \frac{\log^n x}{x^{1+\rho}}$$

sera finie pour des valeurs de ρ positives ou nulles reste fini pour $\rho = 0$.

Ajoutant cette expression avec (1) on voit que :

$$A = \sum_{x=2}^{x=\infty} \left(\Delta \varphi - \int_x^{x+1} \frac{dx}{\log x}\right) \frac{\log^n x}{x^{1+\rho}}$$

Reste fini pour $\rho = 0$.

12. — Valeur asymptotique de $\varphi(x)$

Mettons maintenant la valeur de A du § précédent qui pour $\rho = 0$ reste finie, sous la forme :

$$A_s = C + \sum_{a+1}^{s} \left[\Delta \varphi(x) - \int_x^{x+1} \frac{dx}{\log x}\right] \frac{\log^n x}{x^{1+\rho}},$$

en nous réservant de faire $s = \infty$, et en appelant C la somme des $a - 1$ premiers termes de A.

On a l'identité

$$\sum_{a+1}^{x} u_x (v_{n+1} - v_x) = u_x v_{x+1} - u_{a+1} v_a - \sum_{a+1}^{x} v_x (u_x - u_{x-1});$$

si l'on y fait

$$v_x = \varphi(x) - \int_2^x \frac{dx}{\log x}, \quad u_x = \frac{\log^n x}{x^{1+\varepsilon}},$$

on a

$$\begin{aligned} A_x = C &- \left[\varphi(a+1) - \int_2^{a+1} \frac{dx}{\log x}\right] \frac{\log^n a}{a^{1+\varepsilon}} \\ &+ \left[\varphi(s+1) - \int_2^{s+1} \frac{dx}{\log x}\right] \frac{\log^n s}{s^{1+\varepsilon}} \\ &- \sum_{a+1}^{x} \left[\varphi(x) - \int_2^x \frac{dx}{\log x}\right] \left[\frac{\log^n x}{x^{1+\varepsilon}} - \frac{\log^n (x-1)}{(x-1)^{1+\varepsilon}}\right] \end{aligned}$$

ou en supposant $1 > \theta > 0$

$$\begin{aligned} (1) \quad A_x = C &- \left[\varphi(a+1) - \int_2^{a+1} \frac{dx}{\log x}\right] \frac{\log^n a}{a^{1+\varepsilon}} + \left[\varphi(s+1) - \int_2^{s+1} \frac{dx}{\log x}\right] \frac{\log^n s}{s^{1+\varepsilon}} \\ &+ \sum_{a+1}^{x} \left[\varphi(x) - \int_2^x \frac{dx}{\log x}\right] \left[1 + \varepsilon - \frac{x}{\log(x-\theta)}\right] \frac{\log^n (x-\theta)}{(x-\theta)^{1+\varepsilon}}. \end{aligned}$$

Cela posé, je dis que :

$$(2) \qquad \varphi(x) < \int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x},$$

quels que soient α et n, pour une infinité de valeurs de x. Soit a un entier supérieur à e^n et au plus grand nombre qui satisfait à l'inégalité précédente, alors pour $x > a$, on aura si cette hypothèse (2) n'a pas lieu

$$\varphi(x) \geq \int_2^x \frac{dx}{\log x} + \frac{dx}{\log^n x}, \quad \log x < n,$$

et par suite

$$\varphi(x) - \int_2^x \frac{dx}{\log x} \geq \frac{dx}{\log^n x}, \quad \frac{n}{\log x} < 1. \tag{3}$$

Si nous nous reportons à la formule (1) et si nous désignons pour abréger par F l'expression qui précède le signe Σ, nous aurons

$$A_x = F + \sum_{a+1}^{x} \left[\varphi(x) - \int_2^x \frac{dx}{\log x} \right] \left[1 + \rho - \frac{n}{\log(x+\theta)} \right] \frac{\log^n(x-\theta)}{(x-\theta)^{x+\rho}},$$

en tenant compte de (3), en observant que

$$1 + \rho - \frac{n}{\log(x-\theta)} > 1 - \frac{n}{\log a},$$

$$\varphi(x) - \int_2^x \frac{dx}{\log x} > \frac{\alpha(x-\theta)}{\log^n(x-\theta)},$$

nous aurons

$$A_x > F + \sum_{a+1}^{x} \frac{\alpha(x-\theta)}{\log^n(x-\theta)} \left(1 - \frac{n}{\log a} \right) \frac{\log^n(x-\theta)}{(x-\theta)^{1+\rho}},$$

ou

$$A_x > F + \alpha \left(1 - \frac{n}{\log a} \right) \sum_{a+1}^{x} \frac{1}{(x-\theta)^{1+\rho}},$$

ou

$$A_x > F + \alpha \left(1 - \frac{n}{\log x} \right) \sum_{a+1}^{x} \frac{1}{x^{1+\rho}},$$

ou

$$(A_x)_{x=\infty} > F + \alpha \left(1 - \frac{x}{\log a} \right) \sum_{a+1}^{\infty} \frac{1}{x^{1+\rho}},$$

ou enfin

$$(A_x)_{x=\infty} > F + \alpha \left(1 - \frac{x}{\log a} \right) \cdot \frac{\int_0^\infty \frac{e^{-\rho x}}{e^x - 1} x^\rho dx}{\int_0^\infty e^{-x} x^\rho dx}.$$

Si l'on fait $\rho = 0$, cette quantité converge vers $+\infty$;

ainsi A_s croît indéfiniment pour $\rho = 0$, ce qui est en contradiction avec les conclusions du § précédent, donc : l'inégalité

$$\varphi(x) < \int_2^x \frac{dx}{\log x} + \frac{\alpha x}{\log^n x}$$

est satisfaite pour une infinité de valeurs de x; on verrait de même que, pour une infinité de valeurs de x, on a aussi

$$\varphi(x) > \int_2^x \frac{dx}{\log x} - \frac{\alpha x}{\log^n x}.$$

Théorème. — *On a*

$$\operatorname{Lim} \frac{x}{\varphi(x)} - \log x = -1, \text{ pour } x = \infty.$$

En effet, en vertu des inégalités que nous venons de démontrer, on a une infinité de fois

$$\varphi(x) = \int_2^x \frac{dx}{\log x} + \theta \frac{\alpha x}{\log^n x},$$

θ étant compris entre -1 et $+1$, donc

$$\frac{x}{\varphi(x)} = \frac{x}{\int_2^x \frac{dx}{\log x} + \theta \frac{\alpha x}{\log^n x}}$$

$$= \frac{x}{\frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{dx}{\log^2 x} + \theta \frac{\alpha x}{\log^n x}}$$

$$= \frac{\log x}{1 - \frac{2\log x}{x} + \frac{\log x}{x} \int_2^x \frac{dx}{\log^2 x} + \theta \frac{\alpha}{\log^{n-1} x}};$$

pour $x = \infty$ on a :

$$\frac{x}{\varphi(x)} - \log x + 1 = 0,$$

d'où l'on conclut pour de très grandes valeurs de x

$$\varphi(x) = \frac{x}{\log x - 1}.$$

Legendre avait trouvé d'une façon empirique en interpolant les tables de nombres premiers à sa disposition

$$\varphi(x) = \frac{x}{\log x - 1{,}08366}.$$

On voit aussi que pour de grandes valeurs de x

$$\varphi(x) = \int_2^x \frac{dx}{\log x}.$$

13. — Nombres premiers complexes

Si a et b sont entiers, on regarde encore $a + bi$ ou $a + b\sqrt{-1}$ comme un entier. $a^2 + b^2$ est la norme de $a + bi$.

Soient $A + Bi$ et $a + bi$ deux entiers on a

$$\frac{A + Bi}{a + bi} = \frac{Aa - Bb}{a^2 + b^2} + \frac{Ba + Ab}{a^2 + b^2} i.$$

soit x le quotient de $\frac{Aa - Bb}{a^2 + b^2}$ pris de telle sorte qu'il soit approché à une demi-unité près, etc. Alors

$$\frac{Aa - Bb}{a^2 + b^2} - x \leq \frac{1}{2},$$
$$\frac{Ba + Ab}{a^2 + b^2} - y \leq \frac{1}{2},$$

et en appelant $a^2 + b^2$ la norme de $a + bi$

$$\text{Norme}\left[\frac{Aa + Bb}{a^2 + b^2} + \frac{Ba + Ab}{a^2 + b^2} i - x - yi\right] \leq \frac{1}{2},$$

ou

$$\text{Norme}\left[\frac{A + Bi}{a + bi} - x - yi\right] \leq \frac{1}{2};$$

si donc on pose

$$\frac{A + Bi}{a + bi} - (x + yi) = \frac{p + qi}{a + bi},$$

on aura

$$A + Bi = (x + yi)(a + bi) + p + qi,$$

et

$$\text{Norme}\,\frac{p+qi}{a+bi} < \frac{1}{2},$$

$$\text{Norme}\,(p+qi) < \frac{1}{2}\,\text{norme}\,(a+bi)$$

dans ces conditions $x+yi$ est le quotient et $p+qi$ le reste de la division de $A+Bi$ par $a+bi$.

La division n'est possible que d'une seule manière, car si l'on avait à la fois

$$A+Bi=(a+bi)(x+yi)+p+qi,$$
$$A+Bi=(a+bi)(x'+y'i)+p'+q'i,$$

on en conclurait

$$(1)\quad (a+bi)[(x-x')+(y-y')i]+p-p'+(q-q')i=0,$$

ou

$$(a^2+b^2)[(x-x')^2+(y-y')^2]=(p-p')^2+(q-q')^2.$$

Si l'on n'a pas $x=x'$, $y=y'$ le premier membre est au moins égal à a^2+b^2.

Or le module de $p+qi=(p'+q'i$, est moindre que la somme des modules $\sqrt{p^2+q^2}+\sqrt{p'^2+q'^2}$ ou que :

$$\frac{2}{\sqrt{2}}\sqrt{a^2+b^2}.$$

Le second membre est donc inférieur à $2(a^2+b^2)$, c'est-à-dire égal à a^2+b^2. Dans ce cas $x-x'$ et $y-y'$ sont l'un nul, l'autre égal à ± 1.

Ce cas peut se présenter. Supposons

$$A+Bi=(a+bi)\,x+\frac{a+bi}{2},$$

la norme de $\frac{a+bi}{2}$ est encore $\frac{a^2+b^2}{4}<\frac{a^2+b^2}{2}$, et l'on a :

$$A+Bi=(a+bi)(x+1)-\frac{a+bi}{2},$$

et la norme de $-\frac{a+bi}{2}$ est encore $\frac{a^2+b^2}{4}<\frac{a^2+b^2}{2}$; mais

alors le quotient est purement réel ou purement imaginaire.

Considérons alors $+1$, -1, $+i$, $-i$ comme des unités et soient a et b deux nombres complexes, divisons a par b, soit r le reste,

$$\text{norme } r \leq \frac{1}{2} \text{ norme } b,$$

divisons b par r, soit r' le reste

$$\text{norme } r' \leq \frac{1}{2} \text{ norme } r,$$

et ainsi de suite, on finira par tomber sur un reste de norme nulle ou de norme unité, c'est-à-dire $+1$, -1, $\sqrt{-1}$ ou $-\sqrt{-1}$. Dans le premier cas le dernier reste sera *le plus grand commun diviseur* de a et b, dans le cas contraire a et b seront *premiers entre eux*.

Un nombre sera *premier* quand il n'aura d'autres diviseurs que ± 1 ou $\pm i$, ou lui-même ou ses produits par des unités ; on voit comme dans la théorie des nombres réels, qu'un nombre n'est décomposable que d'une manière, en facteurs premiers.

Pour qu'un nombre soit premier, il suffit et il faut que sa norme soit un nombre premier réel.

En effet si $a + bi$ est composé, on a :

$$a + bi = (x + yi)(p + qi),$$
$$a^2 + b^2 = (x^2 + y^2)(p^2 + q^2),$$

donc sa norme est composée. Si $a + bi$ est premier $a - bi$ l'est aussi, car si l'on avait

$$a - bi = (x + yi)(p + qi),$$

on aurait

$$a + bi = (x - yi)(p - qi).$$

Je dis que $a^2 + b^2$ est un nombre premier, en effet si l'on avait

$$a^2 + b^2 = pq,$$

on aurait

$$(a + bi)(a - bi) = pq ;$$

or p et q sont des sommes de deux carrés, car ils divisent une somme de deux carrés donc

$$(a+bi)(a-bi)=(u^2+v^2)(u'^2+v'^2)$$
$$=(u+v\sqrt{-1})(u-v\sqrt{-1})(u'+v'\sqrt{-1})(u'-v'\sqrt{-1}),$$

donc $a+bi$ pourrait être décomposé soit en deux, soit en un plus grand nombre de facteurs premiers, ce qui est absurde.

Il résulte de là que les seuls nombres premiers complexes sont ceux dont les normes sont premières.

Ce raisonnement suppose a et b différents de zéro : il reste donc à examiner si un nombre premier réel peut être premier dans le domaine des nombres imaginaires.

Si un nombre premier p est de la forme $4n+1$, ou 2, il est la somme de deux carrés $a^2+b^2=(a+b\sqrt{-1})(a-b\sqrt{-1})$ et il n'est pas premier par rapport aux nombres imaginaires. S'il est de la forme de $4n-1$, il est encore premier par rapport aux imaginaires, en effet s'il était décomposable, on aurait par exemple :

$$p=(a+b\sqrt{-1})(c+d\sqrt{-1})$$

il serait divisible par $a-bi$ et $c-di$ et par suite par a^2+b^2 et c^2+d^2.

Nous ne pousserons pas plus loin l'étude des entiers imaginaires, laissant au lecteur le soin de généraliser les notions acquises sur les nombres réels.

Nous allons dans le chapitre suivant présenter la notion du nombre premier sous la forme la plus générale.

CHAPITRE VI

FONCTIONS IRRÉDUCTIBLES

1. — Préliminaires

Dans ce qui va suivre nous généraliserons la notion de congruence ; ainsi nous dirons souvent que deux fonctions de x, $F(x)$ et $f(x)$ sont congrues suivant le module p et la fonction modulaire $\varphi(x)$, quand on aura :

$$F(x) - f(x) = \text{multiple de } p + \text{multiple de } \varphi(x)$$

et les notations :

$$A = B \pmod{p},\ A = B \pmod{\varphi(x)}$$
$$A = B \bmod. (p, \varphi(x))$$

seront respectivement équivalentes à :

$$A - B = \text{multiple de } p,\ A - B = \text{multiple de } \varphi(x)$$
$$A - B = \text{multiple de } p + \text{multiple de } \varphi(x).$$

une fonction $f(x)$ sera dite *réduite* suivant le module p et la fonction modulaire $f(x)$, si la plus haute puissance de x dans $F(x)$ est moindre que le degré de $f(x)$ et si ses coefficients sont entiers et inférieurs à p.

Une fonction entière $F(x)$ sera *irréductible* suivant le module p : 1° Si le coefficient de la plus haute puissance de x dans cette fonction est un ; 2° si elle n'admet pas de diviseur suivant le module p.; 3° si ses coefficients sont entiers.

Théorème 1er. — *Si les fonctions de x, φ et ψ n'ont pas de diviseur commun (mod. p), il existera des fonctions de x, u et v telles que* :

$$u\varphi - v\psi = 1 \pmod{p}$$

Soient a et b les coefficients des plus hautes puissances de x dans φ et ψ, soient α et β des entiers tels que :

$$\alpha a \equiv 1,\ \beta b \equiv 1,\ (\text{mod. } p)$$

divisons $\alpha\varphi,\ \alpha x\varphi \ldots \alpha x^{n-1}\varphi$, par $\beta\psi$, en supposant n égal au degré de ψ, soit Δ le déterminant des coefficients des restes, on a :

$$\alpha U\varphi - \beta V\psi = \Delta,\ \Delta \gtrless 0$$

U et V désignant des polynomes entiers à coefficients entiers.

Soit :

$$\partial\Delta \equiv 1 \text{ mod. } p$$

on aura

$$\alpha\partial U\varphi - \beta\partial V\psi \equiv 1 \text{ mod. } p.$$

c. q. f. d.

Théorème 2. — *Si la fonction $f(x)$ est irréductible mod. p, et si elle divise $\varphi(x)\ \psi(x)$, elle divisera φ ou ψ.*

En effet soient u et v des polynômes tels que

$$uf - v\varphi = 1,$$

ces polynômes existeront si f est irréductible, car φ et f n'auront pas de facteur commun, à moins que f ne divise φ, mais alors ce serait admettre le théorème *à priori*, mais f divisant $\varphi\psi$, on a :

$$\varphi\psi - fQ \equiv 0 \text{ (mod. } p)$$

Q désignant un polynôme entier. Eliminant φ, on a :

$$u\psi f - vfQ = \psi,$$

donc f divise ψ s'il ne divise pas φ. c. q. f. d.

Corollaire 1er. — Si l'on a :

$$\varphi\psi \equiv 0, (\text{mod. } p, f),$$

on a ou :

$$\varphi \equiv 0, \text{ ou } \psi \equiv 0 \text{ (mod. } p, f)$$

Corollaire 2e. — Si f est irréductible et si elle divise le

produit $\varphi \varkappa \psi \ldots$ mod. p, elle divise l'un des facteurs $\varphi, \varkappa, \psi \ldots$
ou si l'on veut la congruence

$$\varphi\chi\psi\ldots \equiv 0, (\text{mod. } p, f)$$

entraîne l'une des congruences

$$\varphi \equiv 0, \chi \equiv 0, \psi \equiv 0, \ldots$$

Mais seulement une seule d'entre elles aura lieu nécessairement. Ce qui n'empêchera pas les autres d'avoir lieu en totalité ou en partie.

Théorème 3. — *Si une fonction f n'est pas irréductible mod. p, elle est décomposable en facteurs irréductibles.*

En effet multiplions la par $\varkappa$ et désignons par a le coefficient de la plus haute puissance de x, si l'on pose :

$$a\varkappa \equiv 1, \text{ mod. } p,$$

$\varkappa f(x)$ aura pour premier coefficient l'unité. Si $\varkappa f(x)$ est irréductible, on considère $f(x)$ comme décomposé, sinon $\varkappa f(x)$ aura un diviseur $f_1(x)$ et on aura :

$$\varkappa f(x) = \varphi(x) f_1(x).$$

on peut supposer le premier coefficient de f_1 égal à un, et si $f_1(x)$ n'est pas irréductible, il aura un diviseur $f_2(x)$ qui pourra être irréductible; sinon on continuera, jusqu'à ce que l'on tombe sur une fonction $f_i(x)$ qui sera irréductible, après un nombre fini d'opérations ; car $f_i(x)$ finira par être du premier degré, s'il n'y a pas de polynôme irréductible f_j de degré supérieur.

Soit alors f_1 un diviseur irréductible de f on aura :

$$\varkappa f = f_1 \varphi ;$$

soit f_2 un diviseur irréductible de φ on aura :

$$\varkappa f = f_1 f_2 \psi ;$$

et ainsi de suite.

Théorème 4. — *La décomposition de $f(x)$ en facteurs irréductibles mod. p, ne peut se faire que d'une seule manière.*

En effet si l'on avait suivant le module p.

$$f(x) = P^{\alpha}Q^{\beta}R^{\gamma}\dots$$
$$f(x) = G^{a}H^{b}K^{c}\dots$$

P, Q, ... étant irréductibles, on aurait

$$P^{\alpha}Q^{\beta}\dots = G^{a}H^{b}\dots$$

et en raisonnant comme en arithmétique élémentaire dans une circonstance analogue, en s'aidant de théorème 2e on démontre la proposition énoncée.

Théorème 5. — *Soit* F (x) *une fonction réduite suivant le module p et la fonction modulaire* $f(x)$ *de degré n, si les fonctions* $f_1(x)$, $f_2(x)$ ... $f_m(x)$ *satisfont aux relations*

$$F(f_1) = 0, \dots F(f_m) = 0 \ (\text{mod. } p, f(x))$$

si enfin F *est de degré m (nécessairement inférieur à n) on aura :*

$$F(X) = a_0 (X - f_1)(X - f_2)\dots (X - f_m), \ (\text{mod. } p, f)$$

a_0 *désignant le coefficient de* X^m *dans* F (X).

En effet la division algébrique donne :

$$(1) \quad \begin{cases} F(X) = (X - f_1) F_1(X) + R_1 ; \\ \dots\dots\dots\dots\dots\dots \\ F_{m-1}(X) = (X - f_m) a_0 + R_m, \end{cases}$$

R_1, R_2 ... désignant les quantités $F(f_1)$, $F_1(f_2)$ ...
on en conclut :

$$F(X) = F(f_1) + (X - f_1) F_1(f_2)\dots (X - f_1)\dots + (X - f_{m-1}) F_{m-1}(f_m) + a_0 (X - f_1)\dots (X - f_m).$$

donc faisant successivement $X = f_1, f_2 \dots$

$$F(f_1) = F(f_1),$$
$$F(f_2) = F(f_1) + (f_2 - f_1) F_1(f_2),$$
$$\dots\dots\dots\dots\dots\dots$$
$$F(f_m) = F(f_1) + (f_m - f_1) F_1(f_2) + \dots (f_m - f_1)\dots (f_m - f_{m-1}) F_{m-1}(f_m).$$

En négligeant alors les multiples de $f(x)$ et de p, les premiers membres sont nuls, et

$$F(f_1) = 0, F_1(f_2) = 0 \dots F_{m-1}(f_m) = 0.$$

R_1, R_2, sont congrus à zéro, les formules (1) deviennent alors

$$F(X) = (X - f_1)\, F_1(X),$$

. . . . . .

$$F_{m-1}(X) = (X - f_m)\, a_0,$$

ou :

$$F(X) = a_0(X - f_1) \ldots (X - f_m)$$

Nous allons donner à ces théorèmes une autre forme.

2. — Imaginaires de Galois

Si l'on considère la congruence :

$$F(x) \equiv 0 \pmod{p} \tag{1}$$

elle ne peut avoir pour racines que $0, 1, \ldots p - 1$, mais si $F(x)$ est irréductible elle n'a pas de racines, en effet si elle avait pour racine a, $F(x)$ serait divisible pour $x - a$ mod. p.

Mais si nous désignons par i une indéterminée et si nous remplaçons (1) par :

$$F(x) \equiv 0 \pmod{p, \chi(x)},$$

en remplaçant x par $f(i)$, il peut arriver que l'on ait

$$F(f(i)) \equiv 0 \pmod{p, \chi(i)},$$

$f(i)$ sera alors une racine de $F(x) \equiv 0$ mod p, *par définition*.

En vertu du théorème (4) du paragraphe précédent, si (1) a pour racines $f_1(i)$, $f_2(i) \ldots f_m(i)$, on aura :

$$F(X) \equiv a_0(x - f_1)\,(x - f_2) \ldots (x - f_i) \pmod{p, \chi(i)}.$$

Théorème. — *Si l'on a*

$$F(\alpha) \equiv 0 \pmod{p, \chi(i)},$$

on aura

$$F(x) \equiv (x - \alpha)\, Q, \pmod{p, \chi(i)}.$$

En effet on a identiquement :

$$F(x) = a_0(x - \alpha)\,(x - \alpha_1) \ldots$$

Jusqu'à présent rien ne prouve l'existence des fonctions irréductibles de degré supérieur à 1, mais nous pouvons énoncer les faits suivants.

Une congruence

$$F(x) \equiv 0 \pmod{p, \chi(x)}$$

quand p est premier et $\chi(x)$ irréductible, ne peut avoir plus de racines qu'il n'y a d'unités dans son degré.

En effet on a :

$$F(x) \equiv a_0 (x - f_1) \dots (x - f_n)$$

en supposant $f_1, \dots f_n$ racines de $F(x) \equiv 0$ et en désignant par n le degré de $F(x)$; mais si l'on pouvait avoir $F(f_{n+1}) \equiv 0$, on aurait :

$$a_0 (f_{n+1} - f_1) \dots (f_{n+1} - f_n) \equiv 0,$$

et par suite $a_0 \equiv 0$, $F(x)$ serait quel que soit x divisible par p et $\chi(x)$.

Il reste à savoir si une congruence peut avoir effectivement dans tous les cas, autant de racines qu'il y a d'unités dans son degré.

C'est ce qui résultera des théories qui vont suivre.

3. — Théorème fondamental

Théorème. — *Soit $f(x)$ une fonction entière quelconque de x, m un entier quelconque, p un module premier, on a*

$$f(x, p^m) \equiv f(x^{p^m}) \pmod{p}.$$

En effet soit $f(x) = \Sigma a_\mu x^\mu$, on aura par la formule du binôme

$$f(x)^{p^m} = \sum a_\mu^{p^m} x^{\mu p^m} + \sum \frac{p^m !}{\alpha ! \beta ! \dots} C ;$$

et p étant premier, le second terme du second membre est divisible par p, donc

$$f(x)^{p^m} \equiv \sum a_\mu^{p^m} x^{\mu p^m}, \pmod{p}. \tag{1}$$

or, d'après le théorème de Fermat :

$$a_\mu^p = a_\mu,$$

et en élevant à la puissance p :

$$a_\mu^{p^2} = a_\mu^p = a_\mu \dots a_\mu^{p^m} = a_\mu.$$

(1) devient alors :

$$f(x)^{p^m} = \sum a_\mu (x^{p^m})^\mu = f(x^{p^m}) \qquad \text{c. q. f. d.}$$

Corollaire. — *Si la fonction $f(x)$ s'annule pour $x \equiv a$, la congruence $f(x) \equiv 0$ (mod. p) admettra non seulement pour racine a, mais encore a^p, a^{p^2}..., a^{p^m}... (p est premier).*

En effet, on a $f(a)^{p^m} \equiv f(a^{p^m})$, si donc $f(a) \equiv 0$ on en conclut $f(a^{p^m}) \equiv 0$, ce qui démontre le théorème énoncé.

4. — Sur la congruence $x^{p^\nu - 1} - 1 \equiv 0$, mod. $(p, \chi(i))$.

Soit ν le degré de la fonction modulaire $\chi(i)$, le nombre des fonctions réduites suivant ce module est le nombre de valeurs de

$$a_0 + a_1 i + \dots + a_{\nu-1} i^{\nu-1},$$

réduite suivant le module p, ou p^ν; faisons abstraction de la valeur nulle et nous en aurons $p^\nu - 1$ autres :

$$I_1, I_2, \dots, I_{p^\nu - 1}.$$

Soit $f(i)$ une fonction qui ne soit pas divisible par $\chi(i)$, et formons le produit des quantités

$$I_1 f(i), I_2 f(i), \dots, I_{p^\nu - 1} f(i),$$

nous obtiendrons, en observant que ces quantités divisées par $\chi(i)$ laissent des restes différents, c'est-à-dire égaux à l'ordre pris à $I_1, I_2, \dots$

$$I_1 I_2 \dots I_{p^\nu - 1} [f(i)]^{p^\nu - 1} = I_1 I_2 \dots I_{p^\nu - 1},$$

ou bien

$$[f(i)]^{p^\nu - 1} = 1,$$

ou enfin

$$[f(i)]^{p^\nu} - f(i) = 0 ;$$

la congruence

$$x^{p^\nu} - x = 0$$

a donc outre la solution 0, les $p^\nu - 1$ autres valeurs dont est susceptible la fonction réduite $f(i)$, elle a donc p^ν racines qui sont tous les entiers réels et imaginaires. $x^{p^\nu - 1} - 1 = 0$ admet tous les entiers sauf zéro.

Corollaire. — *En vertu de la formule :*

$$f(x)^{p^\nu} = f(x^{p^\nu}),$$

on voit que x^{p^ν} étant congru à x, on a aussi

$$f(x)^{p^\nu} = f(x).$$

5. — Résolution de la congruence $\chi(x) \equiv 0$.

La congruence $\chi(x) \equiv 0$ admet la racine i, puisque $\chi(i) = 0$ donc elle admet les racines

$$i,\ i^p,\ i^{p^2},\ \ldots,\ i^{p^\nu - 1}.$$

1° Ces racines au nombre de ν sont distinctes, en effet si l'on avait

$$i^{p^\alpha} = i^{p^\beta}, \qquad (1)$$

en appelant $f(i)$ un nombre complexe quelconque, on aurait

$$f(i)^{p^\alpha} = f(i^{p^\alpha}) = f(i^{p^\beta}) = f(i)^{p^\beta},$$

la congruence

$$x^{p^\alpha} = x^{p^\beta}$$

admettrait donc pour racines les p^ν entiers complexes, or, elle est de degré inférieur à p^ν donc la formule (1) ne saurait avoir lieu :

2° Les racines $i,\ i^p, \ldots i^{p^\nu - 1}$ étant au nombre de ν sont les seules racines de $\chi(x) \equiv 0$:
on appelle *expressions conjuguées* des expressions de la forme $\varphi(i)$, $\varphi(i^p)$, $\varphi(i^{p^2})$... $\varphi(i^{p^\nu - 1})$, leur somme, leur produit

sont réels, car ce sont des fonctions symétriques des racines de $\chi(x) \equiv 0$.

Si l'entier complexe $\varphi(i)$ *satisfait à une congruence à coefficients réels* $F(x) \equiv 0$ *mod p, ses conjuguées y satisfont aussi.* En effet si l'on a :

$$F(\varphi, (i)) = 0,$$

$F(\varphi(x))$ est divisible par la fonction modulaire $\chi(x)$, il admet donc toutes les racines, donc $F[\varphi(i^{p^h})] \equiv 0$. c. q. f. d.

Soient $x_0, x_1, \ldots, x_\mu$ *les racines de la congruence*

$$F(x, i) = 0,$$

les racines de

$$F(x, i^{p^q}) = 0,$$

seront $x_0^{p^q}, x_1^{p^q}, \ldots$

En effet si l'on fait $F(x, i) = \Sigma a_{mn} x^m i^n$, on a :

$$F(x, i)^{p^q} = \sum a_{mn}^{p^q} x^{mp^q} i^{np^q} + \sum \frac{p^q!}{k!\,k!} C,$$

ou

$$F(x, i)^{p^q} = \sum a_{mn}^{p^q} x^{mp^q} i^{np^q} \pmod p;$$

mais par le théorème de Fermat, $a_{mn}^p = a_{mn}$ et $a_{mn}^{p^s} = a_{mn}^p = a_{mn}^m$, etc., donc :

$$F(x, i)^{p^q} = \sum a_{mn} (x^m i^n)^{p^q} = F(x^{p^q}, i^{p^q});$$

si donc $F(x, i) = 0$ on aura $F(x^{p^q}, i^{p^q}) = 0$. c. q. f. d.

6. — On prouve qu'il existe une fonction irréductible d'ordre ν.

Lemme. — *Soit* $\varkappa(x) \equiv 0$ *(mod p) une congruence irréductible et appelons i,* $i^p, \ldots$ *ses racines, la suite*

$$i, i^p, \ldots i^{p^{\nu-1}}, i^{p^\nu}, \ldots$$

sera circulaire

en effet on a $i^{p^\nu} \equiv i$, $i^{p^{\nu+1}} \equiv i^p$....., et comme i, i^p..., sont différents on ne pourra avoir $i^{p^m} \equiv i$, que si m est un multiple de ν. On peut énoncer ce lemme ainsi :

$x^{p^m} - x$ ne peut être divisible par le facteur irréductible $\varphi(x)$ de degré ν que si m est multiple de ν, et il l'est toujours dans ce cas suivant le module p bien entendu.

Ceci posé considérons la congruence

$$X \equiv x^{p^r} - x \equiv 0 \pmod{p},$$

et supposons son premier membre décomposé en facteurs irréductibles, $\varphi_1(x)$, $\varphi_2(x)$..., comme la congruence en question n'a pas de racines égales, les facteurs φ_1, φ_2..., sont distincts.

D'après le lemme, toute fonction irréductible de degré ν divise X, donc elle fait partie de la suite $\varphi_1(x)$, $\varphi_2(x)$... Si l'on appelle μ_1, μ_2..., les degrés de φ_1, φ_2..., ces fonctions ne pourront diviser X, d'après le lemme, que si μ_1, μ_2..., divisent ν; d'ailleurs φ_1 divise $x^{p^{\mu_1}} - x$..., suivant le module p. Soit alors Z le produit des fonctions φ_α pour lesquelles $\mu_\alpha < \nu$, le quotient $H \equiv \frac{X}{Z} \pmod{p}$ ne contiendra plus que les facteurs φ dont le degré est ν :

1° Supposons ν premier, les diviseurs φ de $x^{p^\nu} - x$ qui sont de degré inférieur à ν sont du premier degré, ils sont relatifs aux racines réelles de la congruence $x^{p^\nu} - x \equiv 0 \pmod{p}$ ou

$$x(x-1)(x-2)\ldots(x-p+1) \equiv x^p - x,$$

on a donc

$$H \equiv \frac{x^{p^\nu} - x}{x^p - x};$$

le degré de H est $p^\nu - p$, et par suite *le nombre des facteurs irréductibles de degré ν quand ν est premier est* :

$$\frac{p^\nu - p}{\nu};$$

2° Supposons $\nu = a^\alpha b^\beta c^\gamma \ldots$, a, b, c étant premiers posons :

$$V_0 = x^{p^\nu} - x,$$

$$V_1 = (x^{p^{\frac{\nu}{a}}} - x)(x^{p^{\frac{\nu}{b}}} - x)(x^{p^{\frac{\nu}{c}}} - x)\ldots,$$

$$V_2 = (x^{p^{\frac{\nu}{ab}}} - x)\ (x^{p^{\frac{\nu}{ac}}} - x)\dots\ (x^{p^{\frac{\nu}{bc}}} - x)\dots,$$

$$V_3 = (x^{p^{\frac{\nu}{abc}}} - x)\ (\dots\dots),$$

Je dis que l'on a :

$$H = \frac{V_0\, V_2\, V_4 \dots}{V_1\, V_3\, V_5 \dots}.$$

En effet soit $F(x)$ un facteur irréductible de degré ν de $x^{p^\nu} - x$, il entre une fois dans V_0; mais il n'entre ni dans V_1, ni dans V_2... Considérons maintenant un facteur irréductible φ de degré μ, μ devant diviser ν sera, par exemple, un diviseur de $\frac{\nu}{abc\dots k}$, sans être diviseur de $\frac{\nu}{abc\dots lk}$. Soit S le nombre des facteurs $a, b, c \dots k$; φ entre 1 fois dans V_0, S fois dans V_1, $\frac{S(S-1)}{2}$ fois dans V_2, etc..., donc dans H ce facteur entre :

$$1 - S + \frac{S(S-1)}{1.2} - \dots = (1-1)^S \text{ fois}$$

ainsi H est bien le produit des facteurs irréductibles de $x^{p^\nu} - x$ de degré ν, évaluons le degré δ de H; il est égal à

$$\delta = p^\nu - \sum p^{\frac{\nu}{a}} + \sum p^{\frac{\nu}{ab}} - \sum p^{\frac{\nu}{abc}} \dots$$

ou en appelant n le nombre des facteurs $a, b \dots$

$$\delta = 1 + \frac{\nu}{1}\log p + \frac{\nu^2}{1.2}\log^2 p + \frac{\nu^3}{1.2.3.}\log^3 p \dots$$
$$- \left[n + \sum \frac{\nu}{a}\log p + \sum \frac{\nu^2}{1.2.a^2}\log^2 p + \dots \right]$$
$$+ \left[\frac{n(n-1)}{1.2} + \sum \frac{\nu}{ab}\log p + \dots \right]$$

on déduit de là

$$\delta = \nu \log p \left[1 - \sum \frac{1}{a} + \sum \frac{1}{ab} - \dots \right]$$
$$+ \frac{\nu^2}{1.2}\log^2 p \left[1 - \sum \frac{1}{a^2} + \sum \frac{1}{a^2 b^2} - \dots \right]$$

ou

$$(a)\quad \delta = \nu\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots\log p + \frac{\nu^2}{1.2}\left(1-\frac{1}{a^2}\right)\left(1-\frac{1}{b^2}\right)\ldots\log^2 p + \ldots$$

ce nombre δ est plus grand que zéro, *il y a donc des fonctions irréductibles de degré* ν. On a évidemment

$$\delta > \varphi(\nu)\log p + \frac{1}{1.2}\varphi^2(\nu)\log^2 x + \ldots$$

$\varphi(\nu)$ désignant le nombre des entiers inférieurs et premiers avec ν; donc

$$\delta + 1 > \log p^{\varphi(\nu)}, \qquad \delta > \log p^{\varphi(\nu)} - 1,$$

on peut trouver des limites plus utiles. On a

$$\nu\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\ldots < \nu\left(1-\frac{1}{\nu}\right) \text{ et égal } \varphi(\nu)$$

$$\nu^2\left(1-\frac{1}{a^2}\right)\left(1-\frac{1}{b^2}\right)\ldots < \nu\left(1-\frac{1}{\nu^2}\right) \text{ et} > \nu\varphi(\nu)\left(1+\frac{1}{\nu}\right)$$

donc

$$\delta < \nu\left[\left(1-\frac{1}{\nu}\right)\log p + \frac{\nu}{1.2}\left(1-\frac{1}{\nu^2}\right)\log^2 p + \ldots\right],$$

c'est-à-dire

$$\frac{\delta}{\nu} > \frac{p^\nu - p}{\nu},$$

de même

$$\frac{\delta}{\nu} > \frac{\varphi(\nu)}{\nu}\left[\nu\log p + \frac{\nu^2}{1.2}\left(1+\frac{1}{\nu}\right)\log^2 p + \frac{\nu^3}{1.2.3.}\left(1+\frac{1}{\nu}+\frac{1}{\nu^2}\right)\log^3.\right]$$

ou

$$\frac{\delta}{\nu} > \frac{\varphi(\nu)}{\nu}\left[\nu\log p + \frac{\nu^2}{1.2}\frac{1-\frac{1}{\nu^2}}{1-\frac{1}{\nu}}\log^2 p + \ldots\right],$$

ou

$$\frac{\delta}{\nu} > \frac{\varphi(\nu)}{\nu-1}\cdot\frac{p^\nu - p}{\nu},$$

Ainsi en appelant N le nombre des congruences irréductibles selon le module premier p et de degré ν, on a

$$\frac{p^\nu - p}{\nu} > N > \frac{\varphi(\nu)}{\nu - 1} \frac{p^\nu - p}{\nu} ;$$

quand ν est premier les deux limites sont égales à $\frac{p^\nu - p}{\nu}$.

7. — Nombre des racines d'une congruence quelconque

Soit $F(x) \equiv 0 \bmod p$, une congruence quelconque, si elle n'est pas irréductible, soient $\varphi_1(x)$, $\varphi_2(x)$... Les facteurs irréductibles de son premier membre, m_1, m_2,..., leurs degrés soit ν le plus petit multiple de m_1, m_2,..., φ_1, φ_2,..., diviseront respectivement suivant le module p les fonctions

$$x^{p^{m_1}} - x, x^{p^{m_2}} - x, \ldots$$

et toutes diviseront $x^{p^\nu} - x$. Considérons alors une congruence irréductible de degré ν, à savoir $\varkappa(x) \equiv 0$, et prenons $\varkappa$ pour fonction modulaire. Si $\varphi_1 \equiv 0$, $\varphi_2 \equiv 0$,..., ont respectivement m_1, m_2,..., racines, $F(x) \equiv 0 \bmod. (p, \varkappa(i)$, aura m_1, m_2..., racines, c'est-à-dire autant qu'il y a d'unités dans son degré.

Il reste à prouver que $\varphi_1 \equiv 0$, par exemple, a m_1 racines, c'est ce qui est évident si l'on observe que

$$x^{p^\nu} - x$$

est divisible par $\varphi_1(x)$; soit donc :

$$x^{p^\nu} - x = \varphi_1(x)\,\psi(x) \pmod{p, \varkappa(i)},$$

l'équation $x^{p^\nu} - x \equiv 0$, a comme l'on sait p^ν racines, donc si $\varphi_1 \equiv 0$ n'avait pas m_1 racines, $\psi(x) \equiv 0$ en aurait plus de $p^\nu - m_1$, ce qui est absurde, puisque $p^\nu - m_1$ est son degré, donc, etc... c. q. f. d.

8. — Recherche des fonctions irréductibles de degré ν

Ces fonctions sont les facteurs irréductibles de $x^{p^\nu} - x$ de degré ν. Voyons donc comment on décomposera $F(x)$ en facteurs irréductibles.

1° Si $F(x)$ a des facteurs égaux, on découvrira, comme dans l'algèbre ordinaire, par la méthode des racines égales, le produit des facteurs simples, doubles...

2° Si $F(x)$ n'a pas de facteurs égaux on cherchera le plus grand commun diviseur de $F(x)$ et de $x^{p^\alpha} - x$, on aura ainsi le produit des facteurs irréductibles du degré α;

3° Enfin quand on aura le produit des facteurs de degré α que j'appellerai $\theta(x)$ on divisera $\theta(x)$ par le polynôme indéterminé :

$$a_0 + a_1 x \ldots + x^\nu,$$

et l'on exprimera que le reste est nul, on aura alors ν congruences du premier degré pour calculer $a_0, a_1, \ldots, a_{\nu-1}$.

CHAPITRE VII

LES ENTIERS ALGÉBRIQUES

1. — Définitions

Nous rappelons qu'une équation irréductible de degré n est une équation dans laquelle : 1° bien entendu les coefficients sont des nombres entiers ; 2° dans laquelle le coefficient de la plus haute puissance de l'inconnue est l'unité ; 3° dont le premier membre n'a pas de diviseurs à coefficients entiers.

Un *nombre algébrique* est un nombre qui satisfait à une équation à coefficients entiers.

Un nombre *entier* algébrique est un nombre qui satisfait à une équation irréductible (définie comme on vient de le faire).

Les nombres entiers $0, \pm 1, \pm 2, \pm 3\ldots$ ordinaires rentrent évidemment dans la définition que nous venons de donner, quand il y aura lieu de les distinguer des autres entiers, on leur donnera le nom d'entiers *rationnels*.

Théorème fondamental. — *Si* $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ *sont des entiers algébriques, et si* $p_1, p_2 \ldots, p_n$ *sont fonctions entières de* $\alpha_1 \ldots \alpha_\lambda$, *les racines de*

$$x^m + p_1 x^{m-1} + p_2 x^{m-2} \ldots + p_m = 0 \tag{1}$$

seront des entiers algébriques.

Pour le démontrer, il suffit de faire voir qu'en éliminant les α entre les équations

$$f_1(\alpha_1) = 0, f_2(\alpha_2) = 0 \ldots f_\lambda(\alpha_\lambda) = 0 \tag{2}$$

qui servent à les définir et (1) on obtient une équation irréductible en x.

Appelons F le premier membre de (1), soient $\omega_1, \ldots \omega_\mu$ les μ arguments de la forme

$$\alpha_1^a \alpha_2^b \ldots \alpha_\lambda^l$$

où $a < k_1$ degré de f_1, $b < k_2$ degré de f_2... et où $\mu = k_1 k_2 \ldots k_n$. Divisons $\omega_h F$ par f_1 (x) soit Q_1^h le quotient et r_1 le reste; divisons r_1 par f_2 (x_2) soit Q_2^h le quotient r_2 le reste, etc., soit R_h le dernier reste on aura

$$\omega_h F = Q_1^h f_1 + \ldots Q_n^h f_n + R_h ;$$

en supposant $h = 1, 2, \ldots \mu$ on aura ainsi μ équations, dans lesquelles les R_h ne renfermeront les x que sous la forme linéaire d'arguments tels que ω_1, $\omega_2 \ldots \omega_\mu$, faisons dans ces équations successivement x_1, $x_2 \ldots$ égaux à toutes les racines des équations (2) on aura μ^2 équations de la forme

$$\omega_h^{(i)} F^{(i)} = R_h^{(i)}, \tag{3}$$

l'indice (i) indiquant que les x ont reçu des valeurs particulières. Soit alors

$$\Omega = \Sigma \pm \omega_1^{(1)} \omega_2^{(2)} \ldots \omega_\mu^{(\mu)},$$

et C le déterminant des coefficients des R_h, les formules (3) montrent que

$$\Omega \Pi F(x, x_1, \ldots x_n) = \Omega C,$$

et par suite $C = 0$ est la résultante cherchée pour avoir le coefficient de la plus haute puissance de x dans C, il suffit d'observer que ce coefficient est indépendant de p_1, $p_2 \ldots$ p_m et que si l'on suppose $p_1 = p_2, = 0$ le coefficient de x^{n^m} dans C se réduit à l'unité.

Alors *a fortiori* une fonction entière et à coefficients entiers, d'un ou de plusieurs entiers algébriques, sera un entier algébrique.

Une fois pour toutes, dans ce qui va suivre nous considérerons *toujours* la même équation $\varphi(x) = 0$ où

$$\varphi(x) = x^n + p_1 x^{n-1} + \ldots + p_n$$

comme définissant des nombres algébriques entiers qui seront : 1° ses racines désignées, *une fois pour toutes* par θ, θ', θ''... ; 2° les fonctions entières de θ ou de θ', ou de θ''... — Par entiers du domaine $\varphi(\theta)$ il faudra entendre des fonctions entières à coefficients entiers de θ.

Toutes les fois que nous parlerons dans la suite d'entiers

algébriques sans spécifier davantage, il sera sous-entendu qu'il s'agit d'entiers du domaine $\varphi(\theta)$.

Les racines θ', θ''... de $\varphi(x) = 0$ donnent lieu à des domaines $\varphi(\theta')$, $\varphi(\theta'')$... qui sont dits conjugués de $\varphi(\theta)$; les entiers $\psi(\theta)$, $\psi(\theta')$... sont dits conjugués [ψ désignant un polynôme entier].

Tout nombre entier du domaine $\varphi(\theta)$, peut se ramener à la forme

$$a_{n-1}\theta^{n-1} + a_{n-2}\theta^{n-2} + \dots a_0, \tag{1}$$

les a désignant des entiers rationnels. En effet si $\psi(\theta)$ désigne un entier, divisons $\psi(x)$ par $\varphi(x)$, soit Q, le quotient R (x) le reste, on aura

$$\psi(x) = Q(x)\,\varphi(x) + R(x)$$

et pour $x = \theta$

$$\psi(\theta) = R(\theta) ;$$

or $R(\theta)$ est de la forme (1) donc, etc.

Un nombre *fractionnaire* est un nombre de la forme $\frac{\psi(\theta)}{\varpi(\theta)}$, ψ et ϖ désignant des entiers ; quand par hasard $\frac{\psi(\theta)}{\varpi(\theta)}$ est entier, on dit que ψ est *divisible* par ϖ.

Etant donné un nombre $\psi(\theta)$ entier, il existe un autre entier $\psi_1(\theta)$ tel que $\psi(\theta)\,\psi_1(\theta)$ est rationnel.

En effet, le résultant de $\psi(x) = 0$ et $\varphi(x) = 0$ est

$$\psi(\theta)\,\psi(\theta')\,\psi(\theta'')\dots = R.$$

R est rationnel, quand à $\psi(\theta')\,\psi(\theta'')$...., c'est une fonction symétrique des racines de $\frac{\varpi(x)}{\theta - x}$, c'est-à-dire une fonction entière de x, dont le coefficient de x^{n-1} est 1, quand on y suppose $x = \theta$ elle se réduit à un entier algébrique $\psi_1(\theta)$ du domaine $\varphi(\theta)$.

2. — Discriminants et normes

Soient $\xi_1, \xi_2, \dots \xi_n$ des entiers du domaine $\varphi(\theta)$, supposons-les *linéairement distincts*, c'est-à-dire tels que si

$$\xi_i = \alpha_{0i} + \alpha_{1i}\theta + \dots \alpha_{n-1\,i}\theta^{n-1} \tag{1}$$

on n'ait pas

$$\begin{vmatrix} \alpha_{01} & \alpha_{11} \dots & \alpha_{n-1,1} \\ \dots & \dots & \dots \\ \alpha_{0n} & \alpha_{1n} \dots & \alpha_{n-1,n} \end{vmatrix} = 0.$$

Tout entier du domaine $\varphi(\theta)$ pourra se mettre sous la forme

$$c_1 \xi_1 + c_2 \xi_2 \dots + c_n \xi_n,$$

c_1, c_2... désignant des nombres rationnels, car les équations (1) permettent de calculer θ, $\theta^2 \dots \theta^{n-1}$, et par suite tout entier algébrique en fonction des ξ.

ξ_1, $\xi_2 \dots \xi_n$ constituent alors une base du domaine $\varphi(\theta)$. Soit $f(\theta)$ un entier ou un nombre fractionnaire, si θ', $\theta'' \dots$ sont les autres racines de $\varphi = 0$. $f(\theta)$, $f(\theta')$, $f(\theta'') \dots$ sont des nombres *conjugués*. Le produit

$$f(\theta) f(\theta') f(\theta'') \dots$$

résultant de f et de φ est la *norme* de $f(\theta)$ ou de $f(\theta') \dots$ on le désigne par $N(f)$. *On a évidemment*

$$N(abc \dots) = N(a) N(b) N(c) \dots$$

si $f(\theta)$ est entier $N f(\theta)$ est évidemment entier et rationnel.

Soient p_{11}, $p_{12} \dots p_{1n}$ des nombres linéairement indépendants, et

$$\begin{aligned} &p_{21}, p_{22} \dots p_{2n}; \\ &p_{31}, p_{32} \dots p_{3n}; \\ &\dots \dots \dots \end{aligned}$$

leurs conjugués, on pourra poser en appelant a_{ij} des nombres rationnels

$$p_{1i} = a_{1i} \xi_1 + \dots a_{ni} \xi_n,$$

et en appelant

$$\begin{aligned} &\xi'_1, \xi'_2 \dots, \\ &\xi''_1, \xi''_2 \dots, \end{aligned}$$

les conjugués de ξ_1, $\xi_2 \dots$

$$p_{2i} = a_{1i} \xi'_1 + a_{2i} \xi'_2 \dots a_{ni} \xi'_n,$$

$$\dots \dots \dots \dots \dots \dots \dots$$

on en conclut

$$\Sigma \pm p_{11} p_{22} \dots = \Sigma \pm a_{11} a_{22} \dots \Sigma \pm \xi_1 \xi'_2 \dots,$$

$(\Sigma \pm p_{11}, p_{22}\ldots)^2$ est ce qu'on appelle le *discriminant* de p_{11}, $p_{12}\ldots p_{1n}$. Ce discriminant ne peut être nul, car $\Sigma \pm a_{11}, a_{12}\ldots$ n'est pas nul, puisque les p sont linéairement distincts, et $\Sigma \pm \xi' \xi'_2\ldots$ n'est pas nul. En effet

$$\xi_i = x_{i0} + x_{i0}\,\theta + \ldots,$$
$$\xi'_i = x_{i0} + x_{i1}\,\theta' + \ldots,$$
$$\ldots\ldots\ldots\ldots,$$

donc

$$\Sigma \pm x_{10}\, x_{21}\ldots \Delta = \Sigma \pm \xi_1\, \xi'_2\ldots,$$

Δ est le produit des différences des racines de $\varphi(\theta) = 0$, qui étant irréductible, n'a pas de racines égales, Δ est donc différent de zéro et $\Sigma \pm \xi_1\, \xi'_2\ldots$ ne saurait être nul.

Congruences

Rappelons qu'un entier λ est divisible par un autre μ quand $\frac{\lambda}{\mu}$ est entier.

Deux entiers p, q du domaine φ, sont congrus suivant le module μ, si leur différence est divisible par μ; on exprime cette circonstance au moyen de la formule

$$p \equiv q \pmod{\mu}.$$

les nombres congrus entre eux (mod. μ) sont censés former une même *classe* (mod. μ).

Le nombre des classes suivant le module μ, est égal à la norme de μ.

En effet formons les produits μ, $\mu\theta$, $\mu\theta^2\ldots$ $\mu\theta^{n-1}$ et soit, en général

$$(1) \qquad \mu\theta^i = c_{i0} + c_{i1}\,\theta\ldots + c_{i\,n-1}\,\theta_{n-1},$$

le déterminant $\Sigma \pm c_{00}\, c_{11}\ldots$ sera le résultant de $\varphi(x)$ et $\mu(x)$, comme l'on sait, il ne peut être nul, puisque $\varphi(x) = 0$ étant irréductible, ne saurait avoir de racine commune avec $\mu = 0$ qui est de degré moindre. Des équations (1) on pourra donc éliminer une, deux... $n-1$ des quantités $\theta, \theta^2, \theta^3\ldots \theta^{n-1}$,

de sorte qu'il y aura des multiples $\mu_1, \mu_2, \ldots \mu_n$ de μ qui seront de la forme

$$(2)\quad \begin{cases} \mu_1 = a_{11}, \\ \mu_2 = a_{21} + a_{22}\theta, \\ \cdots\cdots\cdots \\ \mu_n = a_{n1} + a_{n2}\theta \ldots + a_{nn}\theta^{n-1}, \end{cases}$$

on pourra toujours supposer, dans ces formules, que les a_{ii} y ont leur plus petite valeur positive, on pourra en outre supposer que dans le tableau des coefficients

$$\begin{array}{l} a_{11} \\ a_{21}\ a_{22} \\ a_{31}\ a_{32}\ a_{33} \\ \ldots\ldots \end{array}$$

chaque coefficient est positif ou nul et respectivement moindre que celui qui est placé le premier dans sa colonne. si a_{21} n'était pas compris entre o et a_{11} on remplacerait la seconde formule (2) par une autre obtenue en ajoutant ou en retranchant la première un nombre de fois convenable, et ainsi de suite.

Maintenant considérons les quantités z définies par les équations

$$\begin{cases} z_1 = b_{11}, \\ z_2 = b_{21} + b_{22}\theta, \\ \cdots\cdots\cdots \\ z_n = b_{n1} + b_{n2}\theta \ldots + b_{nn}\theta^{n-1}. \end{cases}$$

Supposons en général $b_{ij} \leq a_{ij}$, le nombre des quantités z sera $a_{11}\, a_{22}\, a_{33} \ldots a_{nn}$.

1° Les entiers z_i sont incongrus (mod. μ), car si l'on avait

$$b_{i1} + b_{i2}\theta \ldots \equiv b'_{i1} + b'_{i2}\theta \ldots,$$

on en conclurait :

$$b_{i1} - b'_{i1} + \ldots + (b_{ii} - b'_{ii})\theta^{i-1} \equiv 0,$$

et en y ajoutant un certain nombre de fois

$$a_{i-1.1} + a_{i-1.2}\theta + \ldots \equiv 0, \ldots a_{11} \equiv 0;$$

on finirait par trouver une formule

$$B_1 + B_2\,\theta \ldots + (b_{ii} - b'_{ii})\,\theta^{i-1} = 0$$

dans laquelle tous les B et $b_{ii} - b'_{ii}$ seraient positifs et où le coefficient de θ^{i-1} serait inférieur à a_{ii}, ce qui est contraire à nos hypothèses.

2° On ne peut pas avoir $z_i \equiv z_j$ ou

$$b_{i1} - b_{j1} + \theta\,(b_{i2} - b_{j2}) \ldots + b_{ii}\,\theta^{i-1} = 0\,;$$

(en supposant $i > j$) car ici encore en combinant cette formule avec des formules (2), on rendrait tous les coefficients positifs, et on aurait un résultat absurde, car $b_{ii} < a_{ii}$.

3° Tout entier c non multiple de μ est congru à l'un des nombres z, en effet si

$$c = A_0 + A_1\,\theta + \ldots A_{n-1}\,\theta^{n-1},$$

en combinant cette formule avec (2) on aura :

$$c = \alpha_0 + \alpha_1\,\theta \ldots + \alpha_{n-1}\,\theta^{n-1},$$

et on pourra supposer tous les α positifs et le nombre c rentrera dans la catégorie des nombres z, si l'on veut.

En résumé le nombre des classes, par rapport au module μ, sera égal au nombre des quantités z, qui sont représentants de ces classes, c'est-à-dire égal à

$$a_{11}\,a_{22} \ldots a_{nn}.$$

Si l'on remplace successivemeut θ par θ', θ''... dans les formules (2), μ_1, μ_2... deviendront successivement μ'_1, μ'_2... puis μ''_1, μ''_2... et en posant

$$\Delta = \begin{vmatrix} 1, & 1, & 1 \ldots \\ \theta, & \theta', & \theta'' \ldots \\ \theta^2, & \theta'^2 & \theta''^2 \ldots \\ \cdot & \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \\ \end{vmatrix},$$

$$M = \begin{vmatrix} \mu_1, & \mu_2, \ldots \\ \mu'_1, & \mu'_2, \ldots \\ \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \\ \mu_1^{n-1}, & \ldots \end{vmatrix},$$

on aura

$$M = a_{11}\,a_{22} \ldots a_{nn}\,\Delta\,;$$

mais on aura aussi

$$M = \mu(\theta)\ \mu(\theta')\ \mu(\theta'')\ldots\ \Delta$$
$$= N(\mu)\ \Delta,$$

donc

$$N(\mu) = a_{11}\, a_{22}\, \ldots\, a_{nn}.$$

Le nombre des classes est donc limité et égal à la norme de μ.

On peut remarquer que quand les a_{ii} sont égaux à l'unité on a $N(\mu) = 1$.

3. — Les unités

Il y a des nombres, par exemple $-1 + 1$ qui divisent tous les entiers du domaine $\varphi(\theta)$, on dit que ce sont des *unités*, leurs normes devant diviser tous les entiers rationnels sont égales à 1 ou à -1; si $\psi(\theta)$ est une unité, $\psi(\theta')$, $\psi(\theta'')$,... $\psi(\theta)$ seront des unités *conjuguées*.

Nous allons démontrer que si $n > 2$ il y a d'autres unités que -1 et $+1$.

Soient ψ, ψ', ψ''... des entiers conjugués du domaine $\varphi(\theta)$ et soit :

$$\psi = h_0 + h_0\theta + \ldots + h_{n-1}\theta^{n-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\psi^{n-1} = h_0 + h_1\theta^{n-1} \ldots + h_{n-1}(\theta^{n-1})^{n-1},$$

considérons les sommes

$$1 + \text{mod. } \theta + \text{mod. } \theta^2 \ldots + \text{mod. } \theta^{n-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$1 + \text{mod. } \theta^{n-1} + \ldots + \text{mod. } (\theta^{n-1})^{n-1},$$

et soit c la plus grande d'entre elles. Si k est un nombre positif suffisamment grand on aura

$$\text{mod. } \psi^{(i)} \leqslant ck.$$

k sera, si l'on veut, le plus grand des entiers h pris en valeur absolue. Si l'on se donne le nombre k, cette inégalité ne pourra avoir lieu que pour un nombre fini de valeurs des h car mod. ψ croît avec mod. θ, au delà de toute limite.

Maintenant répartissons les quantités ψ, ψ'... en deux classes, de telle sorte que dans une classe il y ait au moins une de ces quantités, et que deux quantités ψ, ψ', ψ''... imaginaires conjuguées soient placées dans une même classe.

Je dis que l'on peut choisir ψ de telle sorte que a et b étant des nombres positifs donnés, α, β désignant des valeurs des ψ appartenant à des classes différentes, on ait à la fois.

$$\text{mod. } \alpha < a, \text{ mod. } \beta > b, N(\psi) < (3c)^n.$$

Nous dirons que α appartient à la *première* classe et β à la seconde; soit r la totalité des nombres ψ de première classe et $n - r$ la totalité des nombres ψ de seconde classe. Soit w_1, w_2... w_r les parties réelles des nombres de la première classe.

Donnons à h_0, h_1... toutes les valeurs 0, 1, 2... k, on obtiendra $(k+1)^n$ nombres ψ dans le domaine $\varphi(0)$, pour lesquels on aura :

$$\text{mod. } \alpha \leq ck,$$

les valeurs de w_1, w_2... seront comprises entre $-ck$ et $+ck$ et il est facile de voir que l'on aura :

$$(1) \qquad (k+1)^{\frac{n}{r}} - k^{\frac{n}{r}} > 1.$$

En effet la fonction $(k+1)^{\frac{n}{r}} - k^{\frac{n}{r}} - 1$ a pour dérivée relative à k,

$$\frac{n}{r}\left[(k+1)^{\frac{n}{r}-1} - k^{\frac{n}{r}-1}\right]$$

qui est positive pour $k > 0$, elle se réduit à 0 pour $k = 0$, donc elle est croissante, et l'on a bien la formule (1). Or entre $(k+1)^{\frac{n}{r}}$ et $k^{\frac{n}{r}}$ dont la différence est supérieure à 1, il y a au moins un entier m, donc il y a au moins un entier m, tel que

$$(k+1)^n > m^r > k^n.$$

Posons

$$(2) \qquad d = \frac{2ck}{m} < \frac{2c}{k^{\frac{n}{r}-1}},$$

et considérons les nombres en progression arithmétique

$$(3) \qquad -ck+d, -ck+2d\ldots, -ck+(m-1)\,d,$$

qui déterminent $m-1$ intervalles entre lesquels sont compris les nombres compris entre $-ck$ et $+ck$.

Supposons que pour un nombre ψ, les $w_1, \ldots w_r$ soient compris entre les intervalles des nombres (3), de rangs $s_1\, s_2 \ldots s_r$.

Les rangs simultanés posibles s_1, $s_2\ldots$ quand on fait varier les h sont $m_r < (k+1)^n$, il doit exister deux nombres ψ que nous appellerons λ et μ donnant lieu à des mêmes rangs s_1, $s_2\ldots s_r$ pour les w, soient p_1, $p_2\ldots p_r$ lesvaleurs des w correspondant à λ et $q_1, q_2\ldots q_r$ les valeurs des w correspondant à μ, alors les différences

$$p_1-q_1,\ p_2-q_2-\ldots p_r-q_r$$

seront inférieures à d. Considérons alors l'entier

$$\psi = \lambda - \mu,$$

auquel correspondent les valeurs

$$w_1 = p_1-q_1,\ w_2 = p_2-q_2\ldots w_r = p_r-q_r,$$

et dont les coefficients h sont toujours inférieurs à k ou aux plus égaux à ce nombre, on a toujours

$$\text{mod. } \psi \leq ck,$$

et $w_1 = p_1 - q_1\ldots$ sont toujours inférieurs à d. Les nombres α que nous avons rangés dans la première classe et qui sont de la forme w ou $w + \mathrm{W}\sqrt{-1}$ satisfont à la relation

$$\text{mod. } \alpha \leq d\sqrt{2},$$

ou en vertu de (2)

$$(4) \qquad \text{mod. } \alpha < \frac{3c}{k\,\frac{n}{r}-1}.$$

Soit A le produit des r nombres d, B le produit des $n-r$ nombres β, on aura

$$\mathrm{N}(\psi) = \mathrm{AB} = \pm \text{ mod. A mod. B.}$$

or (4) donne

$$\text{mod. } A < (3c)^r k^{r-n},$$

et comme mod. $\psi \leq ck$, on a

$$\text{mod. } B \leq c^{n-r} k^{n-r},$$

et, par suite,

$$N(\psi) < (3c)^n. \tag{5}$$

Mais $N(\psi)$ est un entier rationnel, donc :

$$\text{mod. } A \text{ mod. } B \geq 1,$$
$$\text{mod. } B > (3c)^{-r} k^{n-r}.$$

Soit β un nombre de seconde classe, posons

$$B = \beta B',$$

on aura

$$\text{mod. } B' \leq (ck)^{n-r-1},$$
$$\text{mod. } B = \text{mod. } \beta \text{ mod. } B',$$
$$\text{mod. } \beta > (3c)^{1-n} k. \tag{6}$$

Donc on peut, en vertu de (5) et (6) choisir k assez grand pour que, quels que soient a et b, on ait

$$\text{mod. } \alpha < a, \text{ mod. } \beta > b, \ N(\psi) < (3c)^n.$$

c. q. f. d.

Tel est le théorème qui va maintenant nous permettre de mettre en évidence l'existence des unités.

Considérons une suite de nombres entiers

$$\psi_1, \psi_2 \ldots \psi_s, \psi_{s+1}, \ldots \tag{S}$$

de normes inférieures à $(3c)^n$ en valeur absolue. Soit a_s le plus petit des modules

$$\text{mod. } (\psi_s), \text{ mod. } (\psi'_s) \ldots \text{ mod. } (\psi_s^{n-1}),$$

b_s le plus grand, supposons que

$$\text{mod. } (\psi_{s+1}), \text{ mod. } (\psi'_{s+1}) \ldots \text{ mod. } (\psi_{s+1}^{n-1})$$

soient plus petits que a_s ou plus grands que b_s suivant qu'ils

appartiennent à la première ou à la seconde classe, on aura

$$a_{i+1} < a_i, \quad b_{i+1} > b_i.$$

Les nombres $\psi_1, \psi_2 \ldots$ de la suite (S) ont des normes inférieures à $(3c)^n$, il doit donc y en avoir parmi eux une infinité qui ont la même norme m, et comme le nombre des entiers incongrus (mod. m) est fini et égal à $(\pm m)^n$, il doit y avoir parmi les nombres de norme m, une infinité congrus entre eux (mod m), soit donc

$$\lambda \equiv \mu \pmod{m},$$

et supposons que λ précède μ dans la suite (S); comme $m = N(\mu)$ est divisible par μ, λ est aussi divisible par μ, posons alors

$$\lambda = \mu\varepsilon,$$

comme $N(\lambda) = N(\mu)$, il faut que $N(\varepsilon) = 1$, et ε est une unité.

L'existence des unités est ainsi mise en évidence pour tous les cas ou $n > 2$. Nous verrons que le cas où $n = 2$ fait exception à la règle.

La démonstration précédente a été donnée par M. Dedekind (Zahlen théorie de Dirichlet). Elle est peu naturelle et l'auteur, vraisemblablement, nous a caché la voie qui l'a conduit au résultat.

Il est évident que si u, v, w,... sont des unités les puissances positives et négatives de u, v, w..., leurs produits seront encore des unités, il y a donc, en général, une infinité d'unités.

Si l'on considère une unité $u = \psi(\eta)$, elle satisfera à une équation de degré n au plus

$$u^n + q_1 u^{n-1} + \ldots + q_n = 0,$$

et q_n sera la norme de u, il sera donc égal à l'unité.

On peut toujours supposer que l'équation précédente est irréductible, car si elle ne l'était pas, son premier membre admettrait un diviseur de la forme

$$u^h + r_1 u^{h-1} + \ldots + 1,$$

qui égalé à zéro définirait une unité.

On voit qu'il existe des domaines dans lesquels l'existence des unités est évidente, par exemple ceux $\varphi(0)$ où le terme constant dans $\varphi(x)$ est égal à ± 1.

Les théories qui suivent ont pu être édifiées sans qu'il ait été nécessaire de s'assurer de l'existence des unités irrationnelles.

4. — Quelques lemmes

Si le nombre premier rationnel p divise le nombre algébrique $\psi(0)$, les coefficients de

$$\psi(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots$$

sont divisibles par p.

En effet soit un entier $\chi(0)$ tel que :

$$\psi(0) = p\chi(0),$$

cela veut dire que

$$\psi(x) = p\chi(x) + \varphi(x)\varpi(x),$$

$\varpi(x)$ désignant un polynôme entier. Et alors $\psi(x) - p\chi(x)$ s'annule avec $\varphi(x)$, ce qui ne peut avoir lieu, que si $\psi(x) - p\chi(x)$ est identiquement nul ; puisque $\varphi(x)$ est irréductible et que $\psi(x)$ et $\chi(x)$ sont de degrés inférieurs à $\varphi(x)$, si l'on pose alors :

$$\chi(x) = \beta_0 + \beta_1 x + \beta_2 x^2 \ldots,$$

les coefficients de $\psi(x) - p\chi(x)$ seront nuls et on aura

$$\alpha_0 - p\beta_0 = 0, \quad \alpha_1 - p\beta_1 = 0 ;$$

donc α_0, $\alpha_1 \ldots$ seront divisible par p.

Si la fonction $\varphi(x)$ est irréductible suivant le module p, le nombre p sera indécomposable (p est supposé premier).

En effet on ne saurait avoir

$$\varphi(x) = PQ + R(x)p,$$

P, Q, R désignant des polynômes entiers, donc on ne saurait avoir

$$P(0)Q(0) + R(0)p = 0,$$

ni *a fortiori* :

$$p = \mathrm{P}(0)\,\mathrm{Q}(0).$$

Dans la suite V, V_1, V_2... seront les facteurs irréductibles de $\varphi(x)$ mod p et l'on aura :

$$\varphi(x) = V^{\alpha} V_1^{\alpha_1} \ldots + p\varpi(x).$$

$\varpi(x)$ désignant un polynôme entier. On pourra toujours supposer que $\varpi(x)$ ne contient pas V^{α} en facteur, car les facteurs irréductibles de $\varphi(x)$ ne sont déterminés qu'à des multiples de p près, si alors on remplace V par $W + p f(x)$, on aura :

$$\varphi(x) = W^{\alpha} V_1^{\alpha_1} \ldots + p\left[\varpi(x) + W^{\alpha-1} p \frac{\alpha}{1} f + W^{\alpha-2} p^2 f^2 \frac{\alpha(\alpha+1)}{1.2} + \ldots\right]$$

et le coefficient de p ne contient plus W à la puissance α en facteur, si l'on choisit convenablement la fonction f.

D'ailleurs f peut être choisi d'une infinité de manières différentes.

Il est à peine nécessaire de faire observer que si la fonction φ n'est pas irréductible (mod. p) le nombre premier p ne sera pas en général indécomposable.

5. — Propriétés des facteurs irréductibles de φ

Soient V, V_1, V_2 ... les facteurs irréductibles de φ suivant le module p, en sorte que

$$\varphi(x) = V^{\alpha} V_1^{\alpha_1} \ldots + p\varpi(x) \pmod{p},$$

p désignant un nombre rationnel premier.

Théorème 1er. — *Si $\psi(0)$ est un entier divisible par p, $\psi(x)$ sera divisible par $\varphi(x)$ (mod. p) et réciproquement si $\psi(x)$ est divisible par $\varphi(x)$ (mod. p), $\psi(0)$ sera divisible par p.*

(Nous supposons que $\psi(x)$ est de degré supérieur à φ et n'a pas été réduit, ce sera si l'on veut le produit de deux polynômes.)

On a vu que si $\psi(0)$ était divisible par p (au paragraphe précédent), tous les coefficients de $\psi(x)$ étaient divisibles par p ; donc en divisant $\psi(x)$ par $\varphi(x)$, le reste aura ses coefficients divisibles par p, et l'on aura

$$\psi(x) - \varpi(x)\,\varphi(x) = 0, \text{ mod. } p,$$

et $\psi(x)$ sera divisible par $\varphi(x)$ mod. p, réciproquement si $\psi(x)$ est divisible par $\varphi(x)$ mod. p, la formule précédente aura lieu et les coefficients de $\psi(x)$ seront divisibles par p, et $\psi(0)$ le sera.

Théorème 2e. — *Les normes de* V, V_1, V_2 ... *sont divisibles par* p^α, p^{α_1}..., μ, μ_1, ... *désignant les degrés de* V, V_1, ...

En effet soient ν_1, ν_2 ... ν_μ les racines de $V = 0$ la norme de $V(0)$ sera :

$$(-1)^{\alpha\mu}\varphi(\nu_1)\varphi(\nu_2)\ldots\varphi(\nu_\mu) = V(0)V(0')\ldots;$$

or, en divisant $\varphi(x)$ par $V^\alpha V_1^{\alpha_1} V_2^{\alpha_2}$ ... on a

$$\varphi(x) = V^\alpha V_1^{\alpha_1}\ldots + p f(x),$$

$f(x)$ étant un polynôme à coefficients entiers; donc en faisant $x = \nu, \nu_1, \nu_2$ ... et en multipliant les formules ainsi obtenues

$$\varphi(\nu_1)\varphi(\nu_2)\ldots = p^\alpha f(\nu_1) f(\nu_2)\ldots$$

or $f(\nu_1) f(\nu_2)$ ... est le résultant de V et de f, c'est un entier; donc, comme le premier membre est au signe près la norme de V, on voit que cette norme est divisible par p^α. c. q. f. d.

Théorème 3e. — *Pour que la norme de* $\psi(0)$ *soit divisible par* p, *il faut que* $\psi(x)$ *soit divisible par un des facteurs irréductibles de* φ *mod.* p *et réciproquement si* $\psi(x)$ *est divisible par un des facteurs irréductibles de* φ *mod.* p, $N[\psi(0)]$ *sera divisible par* p.

En effet si φ et ψ n'ont pas de facteur commun (mod. p) il existera des polynômes entiers λ, μ tels que

$$\lambda(x)\psi(x) - \mu(x)\varphi(x) = 1 \pmod{p},$$

et en faisant $x = 0, 0'$ ... et en multipliant

$$N(\psi(0))\,N(\lambda(0)) = 1.$$

$N[\psi(0)]$ n'est donc pas divisible par p. Si au contraire ψ admet le facteur V (mod. p), on aura :

$$\psi(x) = V(x)Q(x) + p f(x),$$

f et Q désignant des polynômes entiers, faisant $x = 0, 0' \ldots$ et multipliant on a

$$N(\psi(0)) = N(V(0))\, N(Q(0)) + \text{mult. } p;$$

or N [V(0)] est divisible par p^{μ} donc N [ψ(0)] est divisible par p.

Théorème 4e. — *L'exposant de la plus haute puissance de p qui divise* N(V) *est multiple de* μ.

En effet on a vu théorème 2 que

$$N(V(0)) = \pm p^{\mu} f(\nu_1) f(\nu_2) \ldots$$

Pour que N [V (0)] contienne le facteur p à une puissance supérieure à μ, il faut que $f(\nu_1)\, f(\nu_2) \ldots$ soit divisible par p, or c'est la norme de $f(x)$ par rapport au domaine V, elle ne peut être divisible par p que si f est divisible par V (mod. p), soit donc

$$f(x) = f_1(x)\, V + p\, \varpi(x);$$

faisons $x = \nu_1, \nu_2 \ldots$ et multiplions, nous aurons

$$f(\nu_1) f(\nu_2) \ldots = p^{\mu}\, \varpi(\nu_1)\, \varpi(\nu_2) \ldots$$

donc N [V(0)] contient le facteur $p^{2\mu}$ et ainsi de suite.

Théorème 5e. — *Les modules suivant lesquels* $\varphi(x)$ *a des facteurs multiples sont les facteurs premiers de son discriminant.*

En effet soit Δ le discriminant de φ, qui n'est pas nul puisque φ est irréductible ; on a :

$$\varphi(x) = V^{\alpha} f(x) + p\, \varpi(x)$$

donc

$$\varphi'(x) = \alpha V^{\alpha - 1} V' f(x) + V^{\alpha} f'(x) + p\, \varpi'(x)$$

et $\varphi'(x)$ est divisible par V mod. p donc N [φ'(0)] ou Δ est divisible par p ; donc les facteurs de Δ sont les seuls suivant lesquels φ est décomposable.

Réciproquement soit p un facteur premier de Δ, si l'on avait

$$\varphi(x) = V V_1 V_2 \ldots + \varpi p,$$

on aurait

$$\varphi'(x) = V' V_1 \ldots + V V'_1 \ldots + \varpi p ;$$

et φ' ne serait divisible par aucun facteur V s'il était simple.

Théorème. — *La condition nécessaire et suffisante pour que* $\lambda(0)$ *soit divisible par* p *est que* $\lambda(x)$ *soit divisible par* $V^{\alpha} V_1^{\alpha_1} \ldots$ (*mod.* p).

En effet divisons $\lambda(x)$ par $\varphi(x)$, nous aurons :

$$\lambda(x) = \mu(x)\varphi(x), \text{ (mod. } p),$$

si $\lambda(0)$ est divisible par p, et comme

$$\varphi(x) = V^{\alpha} V_1^{\alpha_1} \ldots,$$

on aura

$$\lambda(x) = V^{\alpha} V_1^{\alpha_1} \ldots \mu(x) \text{ (mod. } p).$$

Réciproquement si $\lambda(x)$ est divisible par $V^{\alpha} V_1^{\alpha_1} \ldots$ cette dernière formule aura lieu et par suite

$$\lambda(x) = \varphi(x)\, \mu(x) \text{ (mod. } p),$$

et

$$\lambda(0) = 0 \text{ (mod. } p).$$

Il en résulte que pour voir si un produit $\lambda(0)\ \mu(0) \ldots$ est divisible par p, on peut décomposer $\lambda(x)\ \mu(x) \ldots$ en facteurs irréductibles suivant le module p.

6. — Les nombres adjoints

Supposons $\varphi(x)$ réductible (mod. p) et, comme plus haut,

$$\varphi(x) = V^{\alpha}(x)\ V_1^{\alpha_1} \ldots + p\, \varpi(x)$$

si l'on y fait $x = 0$, on a une relation que l'on peut écrire en changeant de notation (en changeant ϖ en $-\varpi$)

$$V^{\alpha} V_1^{\alpha_1} \ldots = p\, \varpi ; \tag{1}$$

on satisfait à cette équation en posant :

$$V = \varpi^{\frac{1}{s}} u,\ V_1 = \varpi^{\frac{1}{s}} u_1, \ldots$$
$$s = \alpha + \alpha_1 + \alpha_2 \ldots,$$
$$p = u^{\alpha} u_1^{\alpha_1} \ldots$$

Les u ne sont pas des entiers du domaine $\varphi(0)$, ce sont des nombres d'un autre domaine, nous les *adjoindrons* au domaine $\varphi(0)$, et nous dirons que ce sont des entiers *adjoints*.

Les u sont les facteurs adjoints de p. Si $\varphi(x)$ est irréductible (mod. p), p n'a plus de facteurs *adjoints*[1].

Si le nombre entier $f(0)$ est divisible par un facteur V irréductible de $\varphi(x)$ (mod. p), il a des facteurs adjoints. Voici maintenant une remarque importante au sujet du degré de multiplicité des facteurs adjoints.

Supposons que $f(0)$ admette λ fois le facteur adjoint u, posons

$$\lambda = \varkappa q + r,$$

q désignant le quotient et r le reste de la division de λ par $\varkappa$, l'équation (1) donnera

$$V^{q\varkappa+\varkappa} V_1^{q\varkappa_1+\varkappa_1}\ldots = \varpi^{q+1} p^{q+1},$$

ou

$$\varpi^{\frac{\lambda-r+\varkappa}{\varkappa}} u^{\lambda-r+\varkappa} V_1^{q\varkappa_1+\varkappa_1}\ldots = \varpi^{q+1} p^{q+1}$$

ou encore

$$u^{\lambda-r+\varkappa} V_1^{q\varkappa_1+\varkappa_1}\ldots = \varpi^{q+1-\frac{\lambda-r+\varkappa}{\varkappa}} p^{q+1}.$$

Si alors $f(0)$ admet λ fois le facteur u, on aura

$$f(0) = u^\lambda \Pi,$$

et alors en appelant G un nombre algébrique entier, on aura

$$f(0) V^{\varkappa-r} V_1^{q\varkappa_1+\varkappa_1}\ldots = G p^{q+1};$$

et il est clair que si $f(0)$ ne contient pas u, $\lambda+1$ fois ; on n'aura pas

$$f(0) V^{2\varkappa-r} V_1^{q\varkappa_1+2\varkappa_1}\ldots = G p^{q+2},$$

puisque l'on devrait avoir

$$f(0) V^{2\varkappa-r-1} V^{q\varkappa_1+2\varkappa_1}\ldots = G p^{q+2},$$

---

[1] Le nombre p sans facteurs adjoints, sera censé premier dans le domaine $\varphi(0)$ et traité comme un facteur adjoint.

ainsi qu'il est facile de voir, en recommençant les calculs précédents, mais en élevant les deux membres de (1) à la puissance $q+2$.

7. — Théorèmes sur les nombres adjoints

1° *Si le nombre $f(0)$ contient le facteur adjoint u^λ, et si $f_1(0)$ n'est pas divisible par u, le produit $f(0)\,f_1(0)$ sera divisible par u^λ.*

En effet on a :

$$f(0)\,V^{\alpha-r}V_1^{\alpha_1+\alpha_1}\ldots = Gp^{q+1}, \tag{2}$$

et on n'a pas [1]

$$G = VQ + \mu p,$$

Q et μ désignant des entiers, sans quoi on aurait :

$$f(0)\,V^{\alpha-r}V_1^{\alpha_1+\alpha_1}\ldots = VQp^{q+1} + \mu p^{q+2},$$

et en multipliant par $V^\alpha V_1^{\alpha_1}\ldots$

$$f(0)\,V^{2\alpha-r}V_1^{\alpha_1+\alpha_1}\ldots = V^{\alpha+1}V_1^{\alpha_1}\ldots Qp^{q+1} + \mu V^\alpha\ldots p^{q+2},$$

et le premier membre serait divisible par p^{q+2}, comme le second ; $f(0)$ admettrait le facteur $u^{\lambda+1}$. En multipliant (2) par $f_1(0)$ on a :

$$f(0)\,f_1(0)\,V^{\alpha-r}V_1^{\alpha_1+\alpha_1}\ldots = f_1(0)\,Gp^{q+1},$$

$f(0)\,f_1(0)$ contient donc le facteur u^λ, il ne contient pas le facteur $u^{\lambda+1}$, car en multipliant par $V^{\alpha-1}V_1^{\alpha_1}\ldots$ on a :

$$f(0)\,f_1(0)\,V^{2\alpha-r-1}V_1^{\alpha_1+\alpha_1}\ldots = f_1(0)\,V^{\alpha-1}V_1^{\alpha_1}Gp^{q+1},$$

et comme G n'est pas de la forme $VQ+\mu p$ le second membre ne contient pas le facteur p^{q+2}.

2° *Si $f(0)$ contient le facteur u^λ et $f_1(0)$ le facteur $u^{\lambda'}$, le produit $f(0)\,f_1(0)$ contiendra le facteur $u^{\lambda+\lambda'}$.*

Posant comme plus haut

$$\lambda = q\alpha + r,$$
$$\lambda' = q'\alpha + r';$$

---

[1] G n'est pas divisible par V (mod. p).

on a, par hypothèse,

$$f(0)\,V^{\alpha-r}V_1^{q\alpha_1+\alpha_1}\ldots = Gp^{q+1},$$
$$f_1(0)\,V^{\alpha-r'}V_1^{q'\alpha_1+\alpha_1}\ldots = G_1p^{q'+1},$$

G et G_1 n'étant pas divisibles par V (mod. p). En multipliant membre à membre, on a :

$$(A)\qquad f(0)\,f_1(0)\,V^{2\alpha-r-r'}\ldots = GG_1\,p^{q+q'+2}.$$

Si $r+r'<\alpha$, en ayant égard à

$$V^{\alpha}V_1^{\alpha_1}\ldots = \varpi p,$$

on a

$$f(0)\,f_1(0)\,V^{\alpha-r-r'}\ldots\,\varpi = GG_1\,p^{q+q'+1};$$

et $f(0)f_1(0)$ contient le facteur $u^{\lambda+\lambda'}$ et ne contient pas le facteur $u^{\lambda+\lambda'+1}$, puisque ϖ n'est pas divisible par V.

Si $r+r'>\alpha$, comme il est moindre que 2α, on posera $r+r'=\alpha+\beta$, la formule (A) deviendra

$$f(0)\,f_1(0)\,V^{\alpha-\beta}\ldots = GG_1\,p^{q+q'+2};$$

$f(0)\,f_1(0)$ contiendra alors u à la puissance

$$(q+q'+1)\alpha+\beta = \lambda+\lambda'.$$

3° *Si le nombre entier $f(0)$ contient le facteur $u^{\lambda\alpha}$, le facteur $u_1^{\lambda\alpha_1}$ ...* Il est divisible par p^{λ}.

En effet on a, puisque $f(0)$ contient le facteur $u^{\lambda\alpha}$

$$f(0)\,V^{\alpha}\,V_1^{\lambda+1}\ldots = p^{\lambda+1}G;$$

or on a

$$V^{\alpha}V^{\alpha_1}\ldots = p\varpi,$$

donc

$$f(0)\,\varpi\,V_1^{\lambda-\alpha_1+1}\ldots = p^{\lambda}G_1.$$

De même

$$f(0)\,\varpi\,V^{\lambda-\alpha+1}\ldots = p^{\lambda}G,$$

. . . . . .

G_1 désignant un entier ... donc

$$f(0)\,\varpi[V_1^{\lambda-\alpha_1+1}\ldots + V^{\lambda-\alpha+1}\ldots + \ldots]$$

est divisible par p^{ν} et le multiplicateur de $f(\theta)$ dans cette expression, n'est divisible, ni par V, ni par V_1 ... (mod. p) donc $f(\theta)$ doit être divisible par p, posant

$$f(\theta) = pf_1(\theta).$$

On prouvera de même que $f_1(\theta)$ est divisible par p et $f(\theta)$ par p^2 ... et ainsi de suite.

4° *Si le nombre entier $f(\theta)$ contient le facteur u^{λ}, $u_1^{\lambda'}$, ... sa norme sera divisible par $p^{\Sigma\lambda\nu}$, ν_i désignant le degré de V_i.*

En effet le nombre

$$f(\theta)\, V^{\alpha k-\lambda} V_1^{\alpha_1 k-\lambda_1} \ldots = C,$$

k étant tel que $\alpha k > \lambda$, $\alpha_1 k > \lambda_1$, ... contient en facteur u^{λ}, $u_1^{\lambda_1}$, ...

il est donc de la forme $p^{\lambda} F(\theta)$, $F(\theta)$ n'étant divisible par aucun des nombres V, V_1 ... (mod. p). La norme du nombre C sera :

$$N(f)\, N(V)^{\alpha k-\lambda} N(V_1)^{\alpha_1 k-\lambda_1} \ldots = p^{\lambda n} N(F),$$

ou en observant que N(V) est divisible par p^{ν}

$$N(f)\, p^{\Sigma\alpha k-\Sigma\lambda\nu} \ldots = p^{\lambda n} N(F) ;$$

or $\Sigma\alpha\nu = n$ donc

$$N(f) = \ldots = p^{\Sigma\lambda\nu} N(F),$$

et N F contient donc le facteur $p^{\Sigma\lambda\nu}$. c. q. f. d.

5° *Le nombre $f(\theta)$ contient les facteurs adjoints, diviseurs des nombres premiers qui divisent sa norme seulement.*

Car quand il contient un facteur adjoint diviseur de p, la norme est divisible par p.

Si l'on met de côté les nombres premiers rationnels suivant lesquels $\varphi(x)$ est irréductible, le nombre total des nombres adjoints est limité.

6° *Un entier algébrique du domaine $\varphi(\theta)$ est décomposable en facteurs adjoints.*

En effet soit $f(\theta)$ un entier algébrique, il en existe un autre $f_1(\theta)$ tel que

$$f(\theta)\, f_1(\theta) = N(f) ;$$

or le nombre $N(f)$ est décomposable en facteurs adjoints, si

$f(0)$ n'avait pas de facteur adjoint, tous ceux de $N(f)$ appartiendraient à f_1 ce qui est absurde, donc $f(0)$ est divisible par un facteur adjoint, le quotient par ce facteur aussi, etc. ; parmi les facteurs de décomposition pourront d'ailleurs figurer des unités.

7° *Pour qu'un nombre* $\varkappa(0)$ *en divise un autre* $\psi(0)$ *il faut et il suffit que* $\varkappa(0)$ *ne contienne que des facteurs adjoints de* $\psi(0)$, *à une puissance égale ou inférieure.*

Il est évident que si

$$\psi(0) = \varkappa(0)\,\varpi(0),$$

$\psi(0)$ contient les facteurs adjoints de $\varkappa(0)$; démontrons la réciproque, et supposons que $\psi(0)$ contienne les facteurs adjoints de $\varkappa(0)$, on aura :

$$\frac{\psi(0)}{\varkappa(0)} = \frac{\psi(0)\,\varkappa_1(0)}{N(\varkappa)},$$

$\varkappa_1$ étant le nombre qui, multiplié par $\varkappa$, donne $N(\varkappa)$. Or tout facteur de $N(\varkappa)$ entre dans $\psi(0)$ et $\varkappa_1(0)$ avec un exposant plus élevé (Th. 4) donc $\frac{\psi(0)}{\varkappa(0)}$ est entier. c. q. f. d.

8° *Un nombre entier n'est décomposable que d'une seule manière en facteurs adjoints.*

En effet soit $f(0)$ un nombre entier, u, u_1, u_2 ... et v, v_1, v_2 ... des facteurs adjoints, si l'on avait

$$f(0) = v^{\beta} v_1^{\beta_1} \ldots = u^{\alpha} u_1^{\alpha_1} \ldots$$

on en conclurait que

$$\frac{v^{\beta} v_1^{\beta_1} \ldots}{u^{\alpha} u_1^{\alpha_1} \ldots} \text{ et } \frac{u^{\alpha} u_1^{\alpha_1} \ldots}{v^{\beta} v_1^{\beta_1} \ldots}$$

sont des unités donc les facteurs u^{α}, $u_1^{\alpha_1}$ ... entrent dans v^{β}, $v_1^{\beta_1}$ ... et les facteurs de $v^{\beta} v_1^{\beta_1}$ ... entrent dans $u^{\alpha} u_1^{\alpha_1}$ ... et $f(0)$ ne peut se décomposer de deux manières différentes.

9° *Si le produit de plusieurs facteurs adjoints est un nombre du domaine* $\varphi(0)$, *ce sera un nombre entier.*

En effet soient $\psi(0)$ et $\varkappa(0)$ deux entiers, a, b, c ... a', des nombres adjoints

$$\psi(0) = abc\ldots,\ \varkappa(0) = a'b'c' \ldots,$$

si l'on avait

$$a''b''c''\ldots = \frac{\psi(\theta)}{\varkappa(\theta)} = \frac{abc\ldots}{a'b'c'\ldots},$$

on en déduirait

$$a''b''c''\ldots a'b'c'\ldots = abc\ldots ;$$

or la décomposition d'un entier ne pouvant avoir lieu que d'une manière, les facteurs a, b, c ... entrent dans le premier membre, on peut les supposer différents de a', b', c' ... il resterait en les supprimant

$$a'b'c'f'\ldots = 1,$$

ce qui est absurde, l'unité ne pouvant avoir de facteurs adjoints.

10° *Si* u, u_1 ... v, v_1, ... *sont des facteurs adjoints et si l'on a*

$$u\,u_1\,u_2\ldots = v\,v_1\,v_2\ldots$$

les u *et les* v *sont égaux deux à deux.*

Il existera des facteurs adjoints w, w_1 ... tels que u, u_1, u_2 ... w, w_1 w_2, ... soit un entier $f(\theta)$, et alors on aura :

$$f(\theta) = u\,u_1\,u_2\ldots ww_1\ldots = vv_1\ldots ww_1\ldots$$

or $f(\theta)$ ne pouvant se décomposer que d'une seule manière, il faut que les u soient deux à deux égaux aux v.

Ce sont les facteurs adjoints, dont Kummer et M. Zolotaref ont fait usage, sous le nom de nombres *idéaux*, sans oser en affirmer l'existence, très réelle comme nous l'avons vu.

Il est clair que les nombres adjoints qui jouent dans la théorie précédente le rôle de nombres premiers peuvent être choisis de plusieurs manières, mais peu importe.

CHAPITRE VIII

LES IDÉAUX

1. — Définitions

Un *idéal* du domaine $\varphi(\theta)$ est un ensemble de nombres algébriques entiers de ce domaine, tels que α, β, γ... étant des nombres de cet ensemble, toute fonction linéaire à coefficients entiers algébriques de α, β, γ... fait également partie de l'ensemble.

Soit A un idéal, ξ, l'un de ses nombres, l'expression $a_1 \xi_1$ fera, quel que soit l'entier a_1 partie de l'idéal A ; soit ξ_2 un nombre non compris dans la formule $a_1 \xi_1$, s'il en existe, et faisant partie de A l'expression $a_1 \xi_1 + a_2 \xi_2$, dans laquelle a_2 est un entier arbitraire, fournira encore des nombres de l'idéal, si tous les nombres de l'idéal ne sont pas fournis par l'expression précédente, en appelant ξ_3 un entier non compris dans la formule $a_1 \xi_1 + a_2 \xi_2$, mais faisant partie de l'idéal A ; l'expression $a_1 \xi_1 + a_2 \xi_2 + a_3 \xi_3$ représentera encore des nombres de l'idéal ; on peut continuer ainsi, jusqu'à ce que l'on trouve une formule

$$a_1 \xi_1 + a_2 \xi_2 \ldots + a_p \xi_p$$

qui fournisse tous les nombres de l'idéal. ξ_1, ξ_2... ξ_p ce qui constitue ce qu'on appelle la *trame de l'idéal*.

L'idéal de trame ξ_1, ξ_2... ξ_p se désigne souvent ainsi

$$(\xi_1 \xi_2 \ldots \xi_p).$$

Lorsque la trame d'un idéal se compose d'un seul nombre ξ, on dit que l'idéal est un idéal *principal*.

L'ensemble de tous les nombres entiers du domaine $\varphi(\theta)$ est évidemment un *idéal*, on dit que c'est l'idéal *général*.

Tout idéal contient un entier rationnel, car soit ξ_1, ξ_2... sa

trame, il existe un entier a_1, tel que $a_1 \xi_1$ est un entier rationnel, mais si cet entier est 1, l'idéal est évidemment l'idéal général, il en est de même de tout idéal qui contiendrait une unité, même si cette unité était irrationnelle.

Un idéal qui contient deux entiers rationnels, premiers entre eux, est l'idéal général ; car soient p et q ces entiers, $\alpha p + \beta q$, α et β étant entiers, fera partie de l'idéal ; or α et β peuvent être choisis de telle sorte que $\alpha p + \beta q = 1$, donc l'idéal considéré contient une unité et est l'idéal général.

Si $\xi_1, \xi_2 \ldots \xi_n$ sont linéairement indépendants, ils constitueront une trame de l'idéal général.

Le nombre des termes de la trame d'un idéal est nécessairement fini, on peut en effet constituer la trame comme il suit ; ayant choisi le premier terme ξ_1, arbitrairement, appelons ξ_2, $\xi_3 \ldots$ des représentants des diverses classes relativement au module ξ_1 ; si ξ_2 est contenu dans l'idéal on pourra prendre pour second terme de la trame ξ_2, l'idéal contiendra alors tous les multiples de ξ_1 et de ξ_2 et par suite tous les nombres que représentent ξ_1 et ξ_2, car :

1° Il contiendra tous les nombres que représente ξ_1 et qui sont multiples de ξ_1.

2° Il contiendra les nombres $\xi_2 - \xi'_2$, ξ'_2 étant un nombre représenté par ξ_2, car ces nombres sont de la forme $a_1 \xi_2$, contenant ξ_2 et la différence $\xi'_2 - \xi_2$ il contiendra ξ'_2,

Si ξ_3 est contenu dans l'idéal on pourra prendre ξ_3 pour troisième terme de la trame et ainsi de suite. Donc la trame contiendra au plus $N(\xi_1)$ termes, et si elle contient $\xi_1, \xi_2 \ldots \xi_{N(\xi_1)}$ ce sera l'idéal général.

On dit en général en arithmétique que le nombre p divise q, quand q se trouve parmi les nombres $\pm p$, $\pm 2p$, $\pm 3p, \ldots$ il sera alors naturel de dire qu'un idéal divise un nombre quand ce nombre fera partie de l'idéal. Alors en généralisant on est conduit à dire qu'un idéal A est *divisible* par un autre B, quand les nombres de A font partie des nombres de B.

On appelle plus grand commun diviseur de deux idéaux de trames $\xi_1 \ldots \xi_p$ et $\eta_1 \ldots \eta_q$, l'idéal qui a pour trame

$$\xi_1, \xi_2 \ldots \xi_p, \eta_1 \ldots \eta_q.$$

---

[1] Car il existe un polynôme $\psi(x)$ tel que $\psi(x)\,\xi(x) + \lambda(x)\,\varphi(x) =$ un entier.

Le plus petit *multiple* de deux idéaux, sera l'idéal contenu à la fois dans ces deux idéaux.

Un idéal quelconque

$$a_1\xi_1 + a_2\xi_2 \ldots + a_p\xi_p$$

est donc le plus grand commun diviseur de p idéaux principaux (ξ_1), $(\xi_2)\ldots$

On voit que l'idéal général divise tous les autres idéaux et tous les nombres du domaine $\varphi(\theta)$, c'est en quelques sorte l'idéal unité.

On appelle *produit* de deux idéaux de trames $\xi_1, \ldots \xi_p$ et $\eta_1, \eta_2 \ldots \eta_q$ l'idéal dont la trame se compose des nombres $\xi_i\eta_j$.

Le produit de plusieurs idéaux est donc par définition indépendant de l'ordre des facteurs.

2. — Divisibilité. Normes

Deux nombres λ et μ sont *congrus* par rapport à un idéal, quand leur différence est contenue dans cet idéal ou est divisible par cet idéal. On exprime que λ et μ sont congrus par rapport à l'idéal A en écrivant :

$$\lambda \equiv \mu, \text{ (mod. A)},$$

ou

$$\lambda - \mu \equiv 0, \text{ (mod. A)}.$$

Les nombres du domaine $\varphi(\theta)$ peuvent être rangés en classes, une même classe contenant des nombres congrus (mod. A), et deux nombres de classes différentes n'étant jamais congrus.

Le nombre des classes est la norme de A, on la désigne par le symbole N(A). Des nombres pris au hasard (mais fixés une fois pour toutes) dans chaque classe sont ce qu'on appelle des représentants de ces classes.

Au lieu de considérer tous les entiers du domaine $\varphi(\theta)$, ou de l'idéal général, on peut considérer les nombres d'un idéal B et partager ces nombres en classes, deux nombres d'une même classe étant congrus (mod. A) et deux nombres de classes différentes étant incongrus. Le nombre des classes, ou des représentants de B dans l'idéal A sera représenté par $N_B(A)$.

Le nombre des classes relatives à l'idéal principal (μ) est évidemment $N(\mu)$, il est fini. Je dis que *la norme d'un idéal quelconque est finie.*

En effet considérons un idéal quelconque A, soit ξ_1 un des nombres de cet idéal, et soient $\xi_1, \xi_2 \ldots \xi_\nu$ les ν représentants des nombres entiers relativement au module ξ_1 en sorte que $\nu = N(\xi_1)$. L'idéal A contient ξ_1 par hypothèse et ses multiples, ξ_1 sera un élément de sa trame, il pourra contenir $\xi_2, \ldots \xi_\mu$ et leurs multiples et par suite $\xi_1, \ldots \xi_\mu$ feront partie de sa trame ; si $\mu = \nu$, A contient tous les nombres, c'est l'idéal général de norme 1. Supposons donc $\mu < \nu$, $\xi_{\mu+1}, \ldots \xi_\nu$ n'étant pas contenus dans A.

Deux nombres de la classe de $\xi_{\mu+i}$ sont congrus, mod. ξ_1, leur différence appartient à A, ils sont congrus (mod. A). Deux nombres appartenant respectivement aux classes de $\xi_{\mu+i}$, $\xi_{\mu+j}$ sont incongrus (mod. ξ_1), mais ils peuvent être congrus (mod. A). Il résulte de là que le nombre des classes relatives au module A ou que N(A) est moindre que ν, donc :

La norme d'un idéal est un nombre fini moindre ou au plus égal à la norme d'un quelconque des éléments de sa trame.

Or les éléments de la trame, ou au moins l'un d'eux est un nombre arbitraire de l'idéal, donc : *La norme d'un idéal est plus petite ou au plus égale à la norme de celui de ses nombres qui a la norme la plus petite.*

Si l'idéal B *contient* A *ou divise* A, *on aura* :

$$N(B) < N(A);$$

En effet soient $\xi_1, \xi_2 \ldots \xi_\nu$ les représentants de tous les nombres suivant le module A, les nombres de la classe de ξ_1, faisant partie, si l'on veut, de A et par suite de B. Les nombres de la classe ξ_i $(i > 1)$ ont des différences contenues dans A et par suite dans B, deux nombres des classes ξ_i et ξ_j peuvent avoir leur différence contenue dans B, mais non dans A, donc le nombre des classes relativement à B est supérieur ou au plus égal au nombre des classes relatives à A, on a donc :

$$N(B) \leq N(A);$$

j'ajoute que le signe $=$ doit être rejeté, car la trame de B

contient plus de nombres que la trame de A et qu'un des nombres ξ_1... devra faire partie de B. c. q. f. d.

Il est bon d'observer que tout idéal A *contient sa norme ou divise sa norme.*

En effet si α_1, α_2... α_ν sont les représentants des entiers (mod. A), $\alpha_1 + 1$,... $\alpha_\nu + 1$ seront encore des représentants des entiers (mod. A), car si

$$\alpha_i \equiv \alpha_j \text{ mod. A}$$
$$\alpha_i + 1 \equiv \alpha_j + 1,$$

et si l'on n'a pas

$$\alpha_i \equiv \alpha_j,$$

on n'aura pas non plus

$$\alpha_i + 1 \equiv \alpha_j + 1;$$

si alors β_1, β_2... β_ν sont dans un autre ordre les nombres α_1, α_2... α_ν on aura :

$$\alpha_1 \equiv \beta_1 + 1, \alpha_2 \equiv \beta_2 + 1 \ldots \alpha_\nu \equiv \beta_\nu + 1;$$

en ajoutant et en observant que $\Sigma\alpha \equiv \Sigma\beta$, on a

$$0 \equiv \nu,$$

ou

$$0 \equiv N(A),$$

ce qui exprime que N(A) se trouve parmi les nombres de l'idéal A. c. q. f. d.

3. — Norme d'un produit

La norme d'un produit d'idéaux est le produit des normes des facteurs.

Ce théorème paraît difficile à établir directement, et nous serons obligés de démontrer quelques lemmes.

1° *Si l'idéal* C *divise* B *et si* B *divise* A, *on aura :*

$$N_C(A) \equiv N_C(B)\, N_B(A).$$

En effet soient en général α, α'... les nombres de A, β, β'.., ceux de B, γ, γ'... ceux de C. Les nombres $\beta + \gamma$ appartiennent à C, supposons que β_1, β_2... soient les représentants de B par

rapport au module A et que γ_1, γ_2... soient les représentants de C par rapport au module B, les $\gamma + \beta_j$ feront toujours partie de C.

On n'aura pas

$$\gamma_i + \beta_j = \gamma_k + \beta_l \text{ (mod. A)},$$

car on aurait *a fortiori*

$$\gamma_i + \beta_j = \gamma_k + \beta_l \text{ (mod. B)};$$

et comme $\beta_i \equiv \beta_j$ (mod. B), on aurait $\gamma_i \equiv \gamma_k$ ce qui exigerait que $\gamma_i \equiv \gamma_k$ et par suite $\beta_j \equiv \beta_l$ (mod. A) ou $\beta_j = \beta_l$.

Tout nombre γ de C est congru suivant le module A à un nombre $\beta_i + \gamma_j$, en effet les nombres β sont des nombres γ, donc on peut poser $\beta_i \equiv \gamma - \gamma_j$ et

$$\gamma = \beta_i + \gamma_j$$

De même, on peut poser

$$\beta_i = \alpha_k + \beta_l,$$

d'où

$$\gamma = \alpha_k + \beta_l + \gamma_j = \beta_l + \gamma_k \text{ (mod. A)}.$$

Ainsi, en résumé si β_1, β_2... sont les représentants de B (mod. A) et γ_1, γ_2... ceux de C (mod. B), les $\gamma_i + \beta_j$ sont incongrus (mod. A), mais sont congrus à des nombres de C (mod. A), ce sont des représentants de C (mod. A), leur nombre est $N_C(B)\, N_B(A)$, donc

$$N_C(A) = N_C(B)\, N_B(A). \tag{I}$$

2° *Soient deux idéaux* A, B, *on aura*

$$N_B(AB) = N(A).$$

En effet soient a_1, a_2, a_3... des nombres de A, b_1, b_2, b_3... des nombres de B, u_1, u_2... des représentants des entiers (mod. A). Les entiers du domaine $\varphi(0)$ seront de l'une des formes :

$$u_1 + a_1,\ u_2 + a_2,\ u_3 + a_3 \ldots$$

par suite, les multiples des nombres de A et de B seront de la forme :

$$b_1 u_1,\ b_2 u_2,\ b_3 u_3 \ldots$$

à des multiples de $a_i b_j$ près. Ces nombres sont incongrus suivant le module AB, car si l'on avait :

$$b_i u_j \equiv b_k u_l \pmod{AB},$$

en observant que

$$b_i u_l \equiv b_k u_l \pmod{AB},$$

car

$$(b_i - b_k)\, u_l \equiv 0,$$

on aurait

$$b_i (u_j - u_l) \equiv 0 \pmod{AB}.$$

Or $u_j - u_l$ n'est pas un nombre de A. Mais les nombres $b_1 u_1$, $b_2 u_2$... sont en nombre égal à N(A). On a donc

$$N_B(AB) = N(A), \qquad (2)$$
$$N_A(AB) = N(B).$$

3° Le théorème énoncé se déduit de là, en effet si dans (1) on suppose que C est l'idéal général, et que A y soit remplacé par AB, on aura

$$N(AB) = N(B)\, N_B(AB),$$

ou, en vertu de (2),

$$N(AB) = N(A)\, N(B).$$

4. — Théorèmes fondamentaux

Considérons un idéal $A = (\xi_1, \xi_2 .., \xi_n)$, soit F le produit des facteurs adjoints communs à $\xi_1, \xi_2 \ldots \xi_n$ en sorte que

$$\xi_1 = FG_1, \quad \xi_2 = FG_2 \ldots \xi_n = FG_n.$$

D'après la définition des nombres adjoints, il existera un entier rationnel s, assez grand pour que F^s soit un nombre entier algébrique du domaine $\varphi(0)$; alors G_1^s, G_2^s... seront des entiers de ce domaine, A^s aura pour trame $\xi_1^s\ \xi_2^s \ldots$ et des nombres de la forme $\xi_1^\alpha\ \xi_2^\beta \ldots \xi_n^\lambda$, $\alpha + \beta \ldots + \lambda$ étant égal à s.
Or :

$$\xi_1^\alpha \xi_2^\beta \ldots = F^s G_1^\alpha G_2^\beta \ldots,$$

et tous les éléments de la trame de A^s contiendront F^s en facteur, quant aux facteurs $G_1^{\alpha} G_2^{\beta}\ldots$ qui multiplient F^s, ils n'auront pas de facteur adjoint commun ; soient, pour abréger,

$$F^s g_1, F^s g_2 \ldots F^s g_\omega,$$

les éléments de la trame de A^s, g_1, g_2.... n'ont pas de diviseur adjoint commun. Or si l'on désigne par ε le plus grand commun diviseur de $N(g_1)$, $N(g_2)\ldots$, il existera des entiers rationnels α_1, $\alpha_2\ldots$ α_ω tels que

$$\alpha_1 N(g_1) + \ldots, \alpha_\omega N(g_\omega) = \varepsilon ;$$

mais il existe des entiers g' tels que $N(g_i) = g_i g_i'$; donc en posant $\alpha_i g_i = \beta_i$, on aura

$$\beta_1 g_1 + \beta_2 g_2 \ldots + \beta_\omega g_\omega = \varepsilon,$$

β_1, $\beta_2\ldots$ désignant des entiers.

Or le nombre g_i contient les facteurs adjoints qui divisent sa norme, et seulement ceux-là ; il résulte de là que les normes de g_1, $g_2\ldots$ n'ont pas de diviseur commun et $\varepsilon = 1$. Il existe donc des nombres β tels que

$$\beta_1 g_1 + \beta_2 g_2 \ldots + \beta_\omega g_\omega = 1.$$

En résumé tous les éléments de A^s contiennent en facteur le nombre entier F^s, et l'idéal A^s contient le nombre F^s, c'est un idéal principal. Donc :

Théorème 1er. — *Étant donné un idéal A, il existe un exposant s, tel que A^s est un idéal principal.*

Et par suite :

Théorème 2e. — *Étant donné un idéal A, il existe toujours un idéal B ($= A^{s-1}$), tel que AB soit un idéal principal.*

Nous déduirons encore de là un autre théorème important :

Si l'idéal A est divisible par l'idéal B, il existera un idéal C tel que :

$$A = BC.$$

En effet soit B' l'idéal qui, multiplié par B, donne l'idéal principal BB', et A' l'idéal qui, multiplié par A, donne l'idéal principal AA'. Or A est divisible par B, il est contenu dans B,

donc AA′ est contenu dans BB′ ou est divisible par BB′ ; mais dire que AB′ est contenu dans BB′, c'est dire *à fortiori* qu'il est contenu dans l'ensemble de tous les multiples des nombres de B ou parmi les multiples d'un certain nombre b trame de l'idéal principal BB′, la trame de AB′ est donc de la forme $(\xi_1 b, \xi_2 b, ..)$ et l'on peut, poser

$$AB' = C\,(b),$$

C désignant l'idéal $(\xi_1, \xi_2 ...)$ et en multipliant par B en observant que $BB' = (b)$

$$A\,(b) = BC\,(b),$$

d'où l'on conclut

$$A = BC.$$

En effet, en général si $PQ = PQ'$, en multipliant par P′ tel que PP′ soit l'idéal principal (p)
on a

$$(p)\,Q = (p)\,Q',$$

et si

$$Q = (\eta_1, \eta_2 ...),\ Q' = (\xi_1, \xi_2 ...),$$

on a

$$(p\eta_1, p\eta_2 ...) = (p\xi_1, p\xi_2 ...),$$

c'est-à-dire

$$(\eta_1 ...) = (\xi_1 ...),$$

ou $Q = Q'$.

Ainsi se trouve justifiée, une fois de plus, la locution *A est divisible par B quand A est contenu dans B.*

5. — Idéaux premiers

Un idéal est *premier* quand il n'admet pas de diviseurs autres que lui-même ou l'idéal général.

Deux ou plusieurs idéaux sont *premiers entre eux* quand leur seul diviseur commun est l'idéal général.

Nous avons vu : 1° que la norme d'un idéal était moindre que la norme d'un quelconque des éléments de sa trame, c'est-à-dire en définitive moindre que la norme d'un quelconque des nombres qu'il contient ; 2° que si un idéal A en divise un autre B, la norme de B est supérieure à celle de A.

Il résulte immédiatement de là, *qu'il existe des idéaux premiers*. En effet soit A un idéal, s'il n'est pas premier, il admet un diviseur de norme moindre A', si A' n'est pas premier, il admet un diviseur de norme encore moindre A'', et ainsi de suite; or on finira ainsi par tomber sur un diviseur premier ou de norme 1, qui sera l'idéal général, et alors le diviseur précédent sera premier.

De là résulte enfin la possibilité de décomposer un idéal A en facteurs premiers idéaux.

Tout idéal qui en divise deux autres, divise leur plus grand commun diviseur.

Car si A contient $(\xi_1 \dots \xi_\mu)$ et $(\eta_1, \eta_2 \dots \eta_\nu)$ ou les divise, il contiendra leur plus grand commun diviseur qui est par définition

$$(\xi_1 \dots \xi_\mu, \eta_1 \dots \eta_\nu).$$

Si les idéaux A, B ont pour plus grand commun diviseur D; MA et MB auront pour plus grand commun diviseur MD.

En effet si

$$A = (\xi_1, \xi_2 \dots), \quad B = (\eta_1, \eta_2 \dots),$$
$$M = (m_1, m_2 \dots),$$

on a

$$D = (\xi_1, \xi_2 \dots \eta_1, \eta_2 \dots),$$
$$MA = (\dots m_i \xi_j \dots), \quad MB = (\dots m_i \eta_j \dots)$$

et le plus grand commun diviseur de MA et MB est

$$(\dots m_i \xi_j \dots m_k \eta_l \dots) = MD.$$

Si l'idéal P est premier avec A et s'il divise AB, il divisera B.

En effet le plus grand commun diviseur, le seul diviseur de P et de A est l'idéal général. Le plus grand commun diviseur de PB et AB sera donc B; or P divisant PB et AB, doit diviser B. c. q. f. d.

De là résulte, comme dans la théorie des entiers rationnels, qu'*un idéal ne peut être décomposé que d'une seule manière en idéaux premiers*, et une foule d'autres théorèmes analogues que nous nous dispensons d'énoncer.

Si un idéal est premier, le plus petit nombre rationnel qu'il contient est premier.

Car s'il était composé et égal à ab, ab serait divisible (contenu dans) par l'idéal ; (ab) serait divisible par l'idéal, a ou b le serait, et ab ne serait pas le plus petit nombre de l'idéal :

Soit I un idéal premier, s'il contient le nombre premier p, il divisera l'idéal (p), sa norme sera un diviseur de p^n.

Si la fonction $\varphi(x)$ est irréductible (mod. p), l'idéal (p) sera premier.

En effet, le nombre p sera indécomposable, car si l'on avait

$$p = \psi(\theta)\,\varkappa(\theta)$$

$\varkappa$ et ψ désignant des entiers, p diviserait $\psi(\theta)$; on pourrait poser

$$\psi(\theta) = p\psi_1(\theta),$$

on aurait :

$$\psi_1(\theta)\,\varkappa(\theta) = 1,$$

et $\varkappa(\theta)$ serait une unité. Dans ce cas la norme de l'idéal est p^n.

Considérons un idéal premier P, il contient un nombre premier p, une de ses puissances P^h est un idéal principal, qui, lui aussi, doit contenir le nombre p^h ; si ξ est sa trame, on aura $p^h = \xi\eta$, η désignant un nombre de cet idéal principal, or on a

$$\mathrm{P}^h = (\xi),$$

donc

$$\mathrm{P}^h(\eta) = (p^h).$$

Donc tout idéal premier qui contient le nombre p divise l'idéal de trame p^h, h désignant un certain exposant, et comme $(p)^h = (p^h)$, tout idéal contenant un nombre premier p divise l'idéal principal (p).

Si $\varphi(x)$ n'est pas irréductible (mod. p), en appelant V, V_1... ses facteurs irréductibles, on aura

$$\varphi(x) = \mathrm{V}^{\alpha}\,\mathrm{V}_1^{\alpha_1}\ldots + \varpi(x)\,p,$$

et si $\varpi(x)$ n'est divisible par aucun des polynômes V, V_1,... (mod. p) ; $\mathrm{V}(\theta)$, $\mathrm{V}_1(\theta)$... seront des nombres algébriques indécomposables en facteurs. Les idéaux $[\mathrm{V}(\theta)]$, $[\mathrm{V}_1(\theta)]$... seront des idéaux dont les facteurs premiers diviseront l'idéal (p).

Considérons l'idéal A composé de tous les multiples du

facteur adjoint u, il contient le nombre premier p, car on a

$$p = u^{\varepsilon} u_1^{\varepsilon_1} \dots$$

u, $u_1 \dots$ désignent les nombres adjoints définis par les formules

$$V = u\varpi^{\frac{1}{\varepsilon}}, \quad V_1 = u_1 \varpi^{\frac{1}{\varepsilon_1}} \dots,$$

l'idéal A contenant le nombre premier p, est un idéal premier ; en effet, supposons que A^r soit un idéal principal, cet idéal principal sera (p^r) de norme p^r, la norme de A sera donc p et il ne pourra être divisible par aucun autre idéal.

Nous avons donc à notre disposition un moyen de nous procurer des idéaux premiers, et il n'y en a évidemment pas d'autres ; car l'idéal formé des multiples du produit de plusieurs facteurs adjoints est le produit des idéaux premiers relatifs à chaque facteur.

Il n'y a qu'un nombre fini d'idéaux de norme donnée.

Car un idéal A de norme ν contient ou divise ν et par suite l'idéal (ν), donc

$$(\nu) = AQ,$$

Q désignant un idéal, or (ν) n'a qu'un nombre limité de diviseurs ; donc il n'y a qu'un nombre limité d'idéaux de norme ν.

Il n'y a qu'un nombre limité d'entiers de norme donnée ν, *dans le domaine* $\varphi(\theta)$.

En effet à chaque idéal principal (ξ) de norme $N(\xi)$, correspond un nombre ξ, à des facteurs unités près ; donc il n'existe qu'un nombre limité d'entiers de norme ν, à des facteurs unités près.

Il résulte de là que si l'on pouvait établir qu'il existe une infinité d'idéaux de norme donnée, on prouverait du coup qu'il existe des unités. Au moins dans le domaine pour lequel l'existence d'une infinité d'idéaux de norme donné serait établie.

6. — Sur les classes d'idéaux

Deux idéaux A et B qui multipliés par un même idéal M fournissent des idéaux principaux, sont considérés comme appartenant à une même *classe*.

Si l'on a deux nombres μ et ν tels que

$$\mu A = \nu B,$$

les idéaux A et B seront équivalents : en effet si D A est un idéal principal, on a

$$\mu DA = \nu DB,$$

et νDB est un idéal principal.

Tous les idéaux principaux appartiennent à une même classe, que l'on appelle *classe principale*.

Soient A et B deux classes, a et b des idéaux de ces classes, les produits ab appartiendront à une même classe que l'on appelle AB.

En effet supposons que P et Q désignent des idéaux principaux, il existera des idéaux U et V tels que

$$aU = P,\ bV = Q;$$

donc

$$ab.\ UV = PQ,$$

ce qui démontre notre théorème.

Le symbole A^m se comprend de lui-même, c'est le produit de m facteurs A, alors $A^1 = A$, et A^0 désignera la classe principale et on posera $A^0 = 1$.

Pour définir le symbole $A^{-m} = (A^{-1})^m$, on remarquera qu'il existe une classe P telle que

$$PA = 1,$$

car tous les nombres de A peuvent être transformés en idéal principal, en les multipliant par un même idéal p, tous les idéaux de la classe P de p jouiront de la même propriété. Si Q désignant une autre classe, on pouvait avoir

$$QA = 1,$$

on aurait

$$Q.\ 1 = Q$$

et

$$QPA = Q,$$
$$PQA = Q,$$
$$P = Q.$$

On pourra donc définir A^{-1}, par la formule

$$AA^{-1} = 1.$$

Il résulte de là que si

$$AB = AC,$$

on aura $B = C$.

Car

$$AA^{-1}B = AA^{-1}C,$$
$$B = C.$$

Le nombre des classes d'idéaux est limité.

Considérons en effet un nombre algébrique

$$a_0 + a_1\theta + \dots a_{n-1}\theta^{n-1},$$

et soit a le plus grand des entiers rationnels a_0, a_1... pris en valeur absolue. Ce nombre aura un module inférieur à

$$a \bmod. \frac{\theta^n - 1}{\theta - 1},$$

et sa norme sera plus petite que

$$a^n \bmod. \frac{\theta^n - 1}{\theta - 1} \cdot \frac{\theta'^n - 1}{\theta' - 1} \dots \text{ ou } a^n k.$$

ainsi en appelant a le plus grand coefficient d'un nombre algébrique ω pris en valeur absolue

$$N(\omega) < a^n k,$$

k désignant un nombre constant pour tout le domaine $\varphi(\theta)$.

Cela posé, *je dis que dans la classe M il existe un idéal m, dont la norme ne surpasse pas k.*

En effet soit μ un idéal de la classe M^{-1}, et choisissons un nombre rationnel a, tel que

$$a^n < N(\mu) < (a+1)^n.$$

(a désignant toujours le plus grand des nombres a_0, a_1... pris en valeur absolue), ces entiers

$$(1) \qquad a_0 + a_1\theta \dots + a_{n-1}\theta^{n-1}$$

sont au nombre de $(a+1)^n > N(\mu)$; il y en aura au moins

deux congrus (mod. μ), leur différence δ, qui est aussi un de ces nombres, sera contenue dans μ, et par suite divisible par μ. L'idéal d de trame δ sera divisible par μ; donc si $d = \mu\nu$,

$$N(d) = N(\mu)\,N(\nu).$$

or la norme δ de d, faisant partie des nombres (1), est inférieure à $a^n k$, donc

$$N(\mu)\,N(\nu) < a^n k\,;$$

mais $N(\nu) < a^n$, donc

$$N(\nu) < k.$$

Dans chaque classe il y a donc un idéal de norme inférieure à un nombre fixe, qui dépend seulement de la nature du domaine étudié ; or le nombre des idéaux de norme donné est limité, donc le nombre des classes est lui-même limité.

Puisque le nombre des classes est limité, soit A une classe, les puissances A^0, A, A^2... A ... seront en nombre limité, il existera un exposant h tel que

$$A^h = A \text{ et même } A^{h-1} = 1.$$

d'où ce théorème capital : *si l'on considère les puissances successives d'un idéal, on finira par trouver parmi elles un idéal principal.*

Soit alors ξ, un idéal principal, il existera ou il n'existera pas d'idéal A tel que

$$A^h = \xi.$$

si A existe, on pourra le représenter par le symbole $\sqrt[h]{\xi}$.

7. — Considérations générales

La théorie des nombres algébriques, généralisation des nombres complexes de Gauss a été inaugurée par Kummer qui a étudié d'abord les domaines de la forme $\frac{\theta^n - 1}{\theta - 1}$, et a découvert les nombres idéaux ou adjoints, qui, pour lui, n'avaient pas d'existence réelle. Dedekind est parvenu à donner une théorie plus satisfaisante et à créer la théorie des idéaux; mais l'exposé qu'il a fait de sa doctrine, principalement dans l'édition qu'il a donnée de la théorie des nombres

de Dirichelet, est extrêmement pénible à lire, à cause de la forme synthétique qu'il a adoptée, pour masquer la voie qui l'a conduit aux résultats qu'il a fait connaître. Aussi faut-il être reconnaissant à M. Zolotaref qui a contribué à jeter quelque lumière sur ces questions, en exposant la théorie des nombres algébriques par une méthode analytique, et facile à suivre (*Journal de math. pures et appliquées*, t. VI, 3e série). La lecture du travail de ce savant nous a servi de guide dans ce qui précède, bien que pour lui, comme pour Kummer, les nombres adjoints n'aient pas d'existence réelle.

8. — Étude de la fonction $\frac{x^n-1}{x-1}$

Considérons l'expression $x^n - 1$, si p désigne un nombre premier et si

$$n = p^\mu \nu$$

on aura

$$x^n - 1 \equiv (x^\nu - 1)^{p^\mu}, (\text{mod. } p),$$

on a vu en effet qu'en général

$$f(x)^{p^\mu} \equiv f(x^{p^\mu}), \text{ mod. } p.$$

Les facteurs irréductibles de $x^n - 1$ dépendront donc de ceux de $x^\nu - 1$, où ν n'est pas divisible par p.

Théorème 1er. — *Tout diviseur de* $\frac{x^n-1}{x-1}$ et de $\frac{x^m-1}{x-1}$ (mod. p) *divise* $\frac{x^\delta-1}{x-1}$, δ *étant le plus grand commun diviseur de* m *et* n.

En effet il existe des entiers a, b tels que

$$an - bm = \delta,$$

or tout diviseur de $\frac{x^n-1}{x-1}$ et de $\frac{x^m-1}{x-1}$ mod. p divisera aussi

$$\frac{x^{an}-1}{x-1} \text{ et } \frac{x^{bm}-1}{x-1}$$

et leur différence

$$\frac{x^{an}-x^{bm}}{x-1} = \frac{x^\delta-1}{x-1}x^{bm},$$

et par suite $\frac{x^\delta-1}{x-1}$. c.q.f.d.

Théorème 2e. — *Si n est premier et si p appartient à l'exposant λ mod. n :*

$$\frac{x^n - 1}{x - 1}$$

sera le produit de $\frac{n-1}{\lambda}$ *fonction irréductible du degré* λ *suivant le module p.*

Supposons $\frac{x^n - 1}{x - 1}$ divisible par une fonction irréductible du degré ν (mod. p) cette fonction divisera :

$$x^{p^\nu} - x = x\,(x^{p^\nu - 1} - 1)$$

comme on l'a vu plus haut ; alors $p^\nu - 1$ est divisible par n donc

$$p^\nu \equiv 1 \pmod{n};$$

or p appartient à l'exposant λ donc :

$$p^\lambda \equiv 1$$

et ν est divisible par λ.

La fonction $\frac{x^n - 1}{x - 1}$ divise $x^{p^\lambda} - x$, ou $(x^{p^\lambda - 1} - 1)$, si une fonction de degré λh, en supposant $\lambda > 1$ divisait $x^n - 1$ (mod. p), elle diviserait $x^{p^h} - x$, or $h < \nu$, cela est donc impossible, notre théorème est donc démontré.

Théorème 3. — $1, x, x^2, \ldots$ *sont tous incongrus* mod. $\frac{x^n - 1}{x - 1}$ si μ et ν sont inférieurs à n, $x^\mu - x^\nu$ ne peut être divisible par $x^n - 1$, ensuite si l'on pose pour abréger

$$\frac{x^n - 1}{x - 1} = f(x)$$

et si l'on fait

$$\mu = an + \alpha,\ \nu = bn + \beta,$$

en supposant α et β inférieurs à n, on aura :

$$x^\mu - x^\nu = x^{an+\alpha} - x^{bn+\beta},$$

si $b = 0$:

$$x^{\mu} - x^{\nu} = x^{\beta}(x^{m\alpha + \alpha - \beta} - 1)$$

si l'on prend $\alpha = \beta$, $x^{\mu} - x^{\nu}$ sera divisible par $x^{n} - 1$ et par suite par $f(x)$; donc :

Théorème 4e. — *Les termes de la suite* $1, x, x^2, \ldots$ *renfermant des termes incongrus mod.* f, *puis* $n - 1$ *termes congrus à ceux-ci et ainsi de suite.*

9. Les périodes de Kummer

Soit g une racine primitive du nombre n, les fonctions

$$x^{g}, x^{g^2}, \ldots x^{g^{n-1}}$$

sont congrues à l'ordre près à

$$1, x, \ldots x^{n-1}$$

suivant le module $f(x)$ et si l'on pose

$$n - 1 = \alpha\beta$$

on pourra former β quantités,

$$\xi_0 = x + x^{g^{\alpha}} + x^{g^{2\alpha}} \ldots + x^{g^{(\beta-1)\alpha}}$$

. . . . . .

$$\xi_{\beta-1} = x^{g^{\alpha-1}} + x^{g^{2\alpha-1}} + \ldots x^{g^{\alpha\beta-1}}$$

. . . . . .

Ce sont les *périodes de Kummer*, ces périodes se déduisent les unes des autres en changeant x en x^g.

Il est facile de voir que

$$\xi_{p\alpha+\lambda} = \xi^{\lambda}, \ (\text{mod. } f(x))$$

ce qui justifie le nom de périodes.

10. — Théorème de Kummer

Supposons n premier on aura

$$\frac{x^n - 1}{x - 1} = (x - 0)\ldots(x - 0^{n-1})$$

et pour $x = 1$

$$n = (1 - 0) \dots (1 - 0^{n-1}),$$

$0, 0^2, \dots 0^{n-1}$ sont des unités,

$$(1 + 0)(1 + 0 + 0^2) \dots (1 + 0 \dots + 0^{n-2})$$

valeur de $\frac{x^2-1}{x-1} \cdot \frac{x^3-1}{x-1} \dots$ pour $x = 1$ a pour norme 1, c'est aussi une unité.

Théorème de Kummer. — Nous avons vu que si n était premier et que si p appartenait à l'exposant h mod. p, $\frac{x^n-1}{x-1}$ était le produit de $\frac{n-1}{h}$ fonctions irréductibles. Il résulte de là qu'il existe pour chaque valeur de h, des nombres adjoints et par suite des idéaux premiers que l'on peut former. Tel est le résultat capital de l'analyse de Kummer.

11. — Les nombres du second degré

Si l'on considère l'équation irréductible

$$x^2 + 2px + q = 0, \tag{1}$$

et si l'on pose

$$D = p^2 - q,$$

les entiers du domaine $0^2 + 2p0 + q$ seront de la forme

$$a + b\sqrt{D},$$

a et b désignant deux entiers rationnels, ici les domaines conjugués sont confondus.

Pour que $a + b\sqrt{D}$ soit une unité, il faut et il suffit que

$$(a + b\sqrt{D})(a - b\sqrt{D}) = \pm 1,$$

ou que

$$a^2 - b^2(p^2 - q) = \pm 1.$$

Supposons $p^2 - q > 0$ et D réel, les nombres a et 1 qui

fournissent l'unité $a + b\sqrt{D}$ sont racines de l'équation indéterminée

$$a^2 - b^2 D = 1,$$

on lui donne le nom d'équation de Pell. Elle a évidemment des solutions. En effet si l'on forme les nombres $2^2 - 1$, $3^2 - 1$, ... $a^2 - 1$, ... ils sont divisibles respectivement par $2 - 1 = 1$, $3 - 1 = 2$ ... $a - 1$ ... c'est-à-dire par tous les nombres, il y en aura une infinité qui seront divisibles par b, il en résulte pour l'équation $x^2 + 2px + q = 0$ une infinité d'unités si $p^2 - q > 0$, et l'on arriverait aux mêmes conclusions pour l'équation $x^2 + px + q = 0$ si $4p^2 - q > 0$.

Mais il n'en est plus de même lorsque $D = p^2 - q$ est négatif, l'équation de Pell est remplacée par

$$a^2 + b^2 D = 1$$

qui n'a de solution que si $b = 0$ et $a = \pm 1$, à moins que $D = 1$, auquel cas on a encore la solution $a = 0$, $b = \pm 1$ (nombres complexes de Gauss).

Ce cas singulier était à signaler, il a d'ailleurs été exclu de la démonstration que nous avons donnée de l'existence des unités.

Appliquons les théories précédentes au domaine $0^2 + 1$ qui définit les nombres imaginaires ordinaires $a + b\sqrt{-1}$, décomposons $x^2 + 1$ en facteurs irréductibles suivant le module premier p et posons

$$(1) \qquad x^2 + 1 = (x + a)(x + a') \pmod{p}.$$

ou, en identifiant,

$$a + a' = 0,$$
$$aa' = 1.$$

On tire de là $a^2 \equiv -1$. Donc si $x^2 + 1$ n'est pas irréductible mod. p, c'est-à-dire si p n'est pas premier dans le domaine $0^2 + 1$, -1 sera résidu quadratique de p qui sera alors de la forme $4n + 1$. Les nombres premiers de la forme $4n - 1$ sont donc seuls premiers dans le domaine $0^2 + 1$.

Si un nombre $a + b\sqrt{-1}$ est donné, pour le décomposer en facteurs adjoints, il faudra prendre un de ses diviseurs

à norme première. Soit donc $a + b\sqrt{-1}$ un nombre de norme première $a^2 + b^2$. Les diviseurs adjoints de $a + b\sqrt{-1}$ seront ceux du nombre premier $a^2 + b^2$; et l'on voit que l'on peut satisfaire à la relation

$$(\theta + a)(\theta + a') + (m\theta + n)(a^2 + b^2) = 0$$

en prenant $a^2 + b^2 = (a + b\theta)(a - b\theta)$ en sorte que les facteurs adjoints dans ce cas exceptionnel, pourront faire partie effective du domaine.

TABLE DES MATIÈRES

CHAPITRE IV. — DÉCOMPOSITION EN CARRÉS

CHAPITRE V. — LES NOMBRES PREMIERS

CHAPITRE VI. — FONCTIONS IRRÉDUCTIBLES

CHAPITRE VII. — LES ENTIERS ALGÉBRIQUES

CHAPITRE VIII. — LES IDÉAUX

ÉVREUX, IMPRIMERIE DE CHARLES HÉRISSEY

ERRATA

Au lieu de :	*Lisez :*
Page 2, ligne 8 : $\overline{14}$, $\overline{13}$, $\overline{12}$, $\overline{11}$,	$1\bar{4}$, $1\bar{3}$, $1\bar{2}$, $1\bar{1}$.
— 20, — 19 : si $f(n) =$ quand	si $f(n) = 1$ quand.
— 40, — 6 : $\frac{a+b'}{b+b'}$,	$\frac{a+a'}{b+b'}$.
— 49, — 20 : si x ne divise pas p	si p ne divise pas x
— 99, — 15 : $\mathcal{E}\frac{\left(\frac{x}{n}\right)^{n-1}}{\left(\frac{n}{x}\right)^{n}-1}$,	$\mathcal{E}\frac{\left(\frac{x}{n}\right)^{n-1}}{\left(\frac{x}{n}\right)^{n}-1}$.
— 131, — 16 : $\log^3$,	$\log^3 p$.