
0162

ŒUVRES

COMPLÈTES

D'AUGUSTIN CAUCHY

ŒUVRES

COMPLÈTES

D'AUGUSTIN CAUCHY

PUBLIÉES SOUS LA DIRECTION SCIENTIFIQUE

DE L'ACADÉMIE DES SCIENCES

ET SOUS LES AUSPICES

DE M. LE MINISTRE DE L'INSTRUCTION PUBLIQUE.

Ire SÉRIE. — TOME III.

PARIS,
GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE
DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,
Quai des Grands-Augustins, 55.

MCMXI

PREMIÈRE SÉRIE.

MÉMOIRES, NOTES ET ARTICLES

EXTRAITS DES

RECUEILS DE L'ACADÉMIE DES SCIENCES

DE L'INSTITUT DE FRANCE.

II.

MÉMOIRES

EXTRAITS DES

MÉMOIRES DE L'ACADÉMIE DES SCIENCES

DE L'INSTITUT DE FRANCE.

MÉMOIRE

SUR

LA THÉORIE DES NOMBRES [1].

Mémoires de l'Académie des Sciences, t. XVII, p. 249; 1840.

AVERTISSEMENT DE L'AUTEUR.

Le Mémoire qu'on va lire est l'un des deux que j'ai présentés à l'Académie des Sciences le 31 mai 1830. Il renferme le développement des principes que j'avais établis dans les *Exercices de Mathématiques* et surtout dans le *Bulletin des Sciences* de M. de Férussac, pour l'année 1829 [2]. Mon absence, qui s'est prolongée pendant 8 années, ayant retardé l'impression de ce Mémoire, je le publie aujourd'hui tel que je le retrouve dans le manuscrit présenté, le 31 mai 1830, à l'Académie des Sciences, et paraphé à cette époque par le Secrétaire perpétuel M. Georges Cuvier. Toutefois, pour ne pas fatiguer l'attention du lecteur, je supprimerai une grande partie des numéros placés devant les formules et, pour éclaircir quelques passages, je joindrai au texte plusieurs notes placées, les unes au bas des pages, les autres à la suite du dernier paragraphe. Comme quelques notes de la première espèce existaient déjà dans le manuscrit, afin qu'on puisse facilement les distinguer des notes nouvelles, je marquerai celles-ci, quand elles seront placées au bas des pages, par un astérisque.

(1) Présenté à l'Académie des Sciences le 31 mai 1830.

(2) *Voir* le Tome XII de ce *Bulletin*, p. 205 et suiv. (*Œuvres de Cauchy*, S. II, T. II).

§ I.

Soient

$$p = n\varpi + 1$$

un nombre premier;
n un diviseur de $p-1$;
θ une racine primitive de

(1) $$x^p = 1;$$

τ une racine primitive de

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

t une racine primitive de

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

Alors

$$\rho = \tau^{\varpi}$$

sera une racine primitive de

(4) $$x^n = 1$$

et

$$r \equiv t^{\varpi} \pmod{p}$$

une racine primitive de

(5) $$x^n \equiv 1 \pmod{p}.$$

On aura

(6) $$\tau^{\frac{n\varpi}{2}} = -1,$$

(7) $$t^{\frac{n\varpi}{2}} \equiv -1 \pmod{p}$$

et de plus, si n est pair,

$$\rho^{\frac{n}{2}} = -1,$$

$$r^{\frac{n}{2}} \equiv -1 \pmod{p}.$$

De plus, k étant un nombre entier quelconque, nous désignerons par

$$m = \mathrm{I}(k)$$

le nombre m propre à vérifier la formule

$$k \equiv t^m \pmod{p},$$

en sorte qu'on aura

$$k^{\varpi} \equiv t^{m\varpi} \equiv r^m \equiv r^{\mathrm{I}(k)},$$

et nous poserons

$$\left(\frac{k}{p}\right) = \tau^{m\varpi} = \tau^{\varpi\,\mathrm{I}(k)} = \rho^{\mathrm{I}(k)}.$$

Par suite, comme on aura, en vertu de l'équation (7),

$$\mathrm{I}(-1) = \frac{n\varpi}{2},$$

on en conclura

$$\left(\frac{-1}{p}\right) = \rho^{\frac{n\varpi}{2}} = \tau^{\frac{\varpi}{2}\varpi} = (-1)^{\varpi}.$$

On aura d'ailleurs évidemment

$$\left(\frac{h}{p}\right)\left(\frac{k}{p}\right) = \left(\frac{hk}{p}\right), \qquad \left(\frac{k}{p}\right)^t = \left(\frac{k^t}{p}\right), \qquad \ldots$$

Soient maintenant

(8) $$\Theta_h = \theta + \rho^h \theta^t + \rho^{2h} \theta^{t^2} + \ldots + \rho^{(p-2)h} \theta^{t^{p-2}}$$

et

(9) $$\Theta_h \Theta_k = \mathrm{R}_{h,k}\, \Theta_{h+k}.$$

$\mathrm{R}_{1,m}$ sera une fonction de ρ de la forme

$$\mathrm{R}_{1,m} = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1};$$

et, si l'on pose

$$k \equiv mh \pmod{n},$$

on aura, en supposant m différent de zéro et de $\frac{n}{2}$,

$$\mathrm{R}_{h,mh} = a_0 + a_1\rho^h + a_2\rho^{2h} + \ldots + a_{n-1}\rho^{(n-1)h}$$

et

$$R_{h,k} = (-1)^{\varpi(h+k)} \sum \left(\frac{u}{p}\right)^h \left(\frac{v}{p}\right)^k, \tag{10}$$

le signe $\sum$ s'étendant à toutes les valeurs entières de u, v comprises entre les limites 1, $p-1$, et qui vérifieront l'équivalence

$$1 + u + v \equiv 0 \pmod{p}.$$

On aura d'ailleurs, en supposant h différent de zéro,

$$\Theta_h \Theta_{-h} = (-1)^{\varpi h} p, \qquad R_{h,-h} = -(-1)^{\varpi h} p, \tag{11}$$

et, en supposant h, k ainsi que $h+k$ non divisibles par n,

$$R_{h,k} R_{-h,-k} = p. \tag{12}$$

On trouvera, au contraire,

$$R_{h,0} = R_{0,h} = -1. \tag{13}$$

Enfin l'on aura

$$a_0 + a_1 + a_2 + \ldots + a_{n-1} = p - 2 \tag{14}$$

et, en supposant n pair,

$$a_0 - a_1 + a_2 - a_3 + \ldots - a_{n-1} = -(-1)^{\frac{\varpi n}{2}}. \tag{15}$$

Par suite, si l'on suppose

$$R_{h,k} = F(\rho), \tag{16}$$

on trouvera

$$F(\rho^m) = R_{mh,mk} \quad \text{et} \quad F(\rho^m) F(\rho^{-m}) = p, \tag{17}$$

si le nombre m est tel qu'aucune des équations

$$\rho^{mh} = 1, \qquad \rho^{mk} = 1, \qquad \rho^{m(h+k)} = 1 \tag{18}$$

ne soit vérifiée. On aura, au contraire,

$$F(\rho^m) = -(-1)^{\varpi mh \times \varpi mk} \tag{19}$$

si une seule des équations (18) est satisfaite, et

$$F(\rho^m) = p - 2 \tag{20}$$

si les trois équations (18) subsistent simultanément.

Soient encore h, k, l trois nombres entiers propres à vérifier la condition

$$h + k + l \equiv 0 \pmod{n}. \tag{21}$$

On aura, en supposant ces nombres tous trois différents de zéro,

$$\Theta_h \Theta_k \Theta_l = (-1)^{\varpi l} \frac{\Theta_h \Theta_k}{\Theta_{h+k}} = (-1)^{\varpi k} \frac{\Theta_h \Theta_l}{\Theta_{h+l}} = (-1)^{\varpi h} \frac{\Theta_k \Theta_l}{\Theta_{k+l}}$$

et, par conséquent,

$$(-1)^{\varpi h} R_{k,l} = (-1)^{\varpi k} R_{l,h} = (-1)^{\varpi l} R_{h,k}. \tag{22}$$

Soit maintenant s une racine primitive de

$$x^{n-1} \equiv 1 \pmod{n}, \tag{23}$$

le nombre n étant supposé premier, et faisons

$$\Theta_1 \Theta_s \Theta_{s^2} \ldots \Theta_{s^{n-2}} = \vartheta(\rho) \quad (1); \tag{24}$$

on aura

$$\Theta_s \Theta_{s^2} \Theta_{s^3} \ldots \Theta_{s^{n-1}} = \vartheta(\rho^s) \tag{25}$$

et, de plus,

$$\vartheta(\rho) = \vartheta(\rho^{s^2}) = \vartheta(\rho^{s^4}) = \ldots = \vartheta(\rho^{s^{n-3}}),$$
$$\vartheta(\rho^s) = \vartheta(\rho^{s^3}) = \vartheta(\rho^{s^5}) = \ldots = \vartheta(\rho^{s^{n-2}}).$$

Donc $\vartheta(\rho)$ sera de la forme

$$\vartheta(\rho) = c_0 + c_1(\rho + \rho^{s^2} + \rho^{s^4} + \ldots + \rho^{s^{n-3}}) + c_2(\rho^s + \rho^{s^3} + \ldots + \rho^{s^{n-2}}) \tag{26}$$

(1) Nota. — s étant une racine primitive de la formule (23), on a

$$s^{n-1} - 1 \equiv 0$$
$$\frac{s^{n-1} - 1}{s^2 - 1} = 1 + s^2 + s^4 + \ldots + s^{n-3} \equiv 0 \pmod{n},$$

et c'est ce qui permet d'établir la formule (24).

ou

$$\vartheta(\rho)=\frac{2c_0-c_1-c_2}{2}+\frac{c_1-c_2}{2}(\rho-\rho^{s}+\rho^{s^2}-\rho^{s^3}+\ldots+\rho^{s^{n-2}}-\rho^{s^{n-1}});$$

et, comme on aura

$$s^{\frac{n-1}{2}}\equiv -1 \pmod{n},$$
$$\rho+\rho^{s}+\rho^{s^2}+\ldots+\rho^{s^{n-2}}+\rho^{s^{n-1}}=-1,$$
$$(\rho-\rho^{s}+\rho^{s^2}-\rho^{s^3}+\ldots+\rho^{s^{n-2}}-\rho^{s^{n-1}})^2=(-1)^{\frac{n-1}{2}}n,$$

on trouvera

$$\vartheta(\rho)\vartheta(\rho^{s})=\left(\frac{2c_0-c_1-c_2}{2}\right)^2-(-1)^{\frac{n-1}{2}}n\left(\frac{c_1-c_2}{2}\right)^2,$$

ou, ce qui revient au même,

$$4\vartheta(\rho)\vartheta(\rho^{s})=(2c_0-c_1-c_2)^2-(-1)^{\frac{n-1}{2}}n(c_1-c_2)^2, \tag{27}$$

ou bien encore

$$\vartheta(\rho)\vartheta(\rho^{s})=(c_0-c_1)^2+(c_0-c_2)(c_1-c_2)+\frac{1-(-1)^{\frac{n-1}{2}}n}{4}(c_1-c_2)^2. \tag{28}$$

Lorsque n est de la forme $4x+3$, l'équation (27) ou (28) se réduit à

$$4\vartheta(\rho)\vartheta(\rho^{s})=(2c_0-c_1-c_2)^2+n(c_1-c_2)^2 \tag{29}$$

ou bien à

$$\vartheta(\rho)\vartheta(\rho^{s})=(c_0-c_1)^2+(c_0-c_1)(c_1-c_2)+\frac{n+1}{4}(c_1-c_2)^2. \tag{30}$$

Au contraire, lorsque n est de la forme $4x+1$, alors, $\frac{n-1}{2}$ étant pair, la formule (24) donne simplement

$$\vartheta(\rho)=p^{\frac{n-1}{4}}$$

et ρ disparaît de l'équation (26), qui se trouve réduite à la forme

$$\vartheta(\rho)=c_0.$$

Revenons au cas où n est de la forme $4x+3$. Comme on aura

$$\vartheta(\rho)\vartheta(\rho^{s})=p^{\frac{n-1}{2}},$$

l'équation (29) donnera

$$4p^{\frac{n-1}{2}}=(2c_0-c_1-c_2)^2+n(c_1-c_2)^2.$$

Donc on résoudra l'équation

$$4p^{\frac{n-1}{2}}=X^2+nY^2 \tag{31}$$

en prenant

$$X=2c_0-c_1-c_2, \qquad Y=c_1-c_2.$$

Mais ces valeurs de X et de Y seront généralement divisibles par p. Il reste à trouver la plus haute puissance de p qui les divise simultanément.

Soit υ un nombre tel qu'on ait simultanément

$$\upsilon^{\frac{n-1}{2}}\equiv 1 \quad \text{et} \quad (1+\upsilon)^{\frac{n-1}{2}}\equiv 1 \pmod{n}.$$

On trouvera

$$\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}=\Theta_{\upsilon}\Theta_{\upsilon s^2}\ldots\Theta_{\upsilon s^{n-3}}=\Theta_{1+\upsilon}\Theta_{(1+\upsilon)s^2}\ldots\Theta_{(1+\upsilon)s^{n-3}}=\vartheta(\rho)$$

et, par suite,

$$\vartheta(\rho)=\frac{\Theta_1\Theta_{\upsilon}}{\Theta_{1+\upsilon}}\frac{\Theta_{s^2}\Theta_{\upsilon s^2}}{\Theta_{(1+\upsilon)s^2}}\ldots\frac{\Theta_{s^{n-3}}\Theta_{\upsilon s^{n-3}}}{\Theta_{(1+\upsilon)s^{n-3}}}=R_{1,\upsilon}R_{s^2,\upsilon s^2}\ldots R_{s^{n-3},\upsilon s^{n-3}}, \tag{32}$$

$$\vartheta(\rho^{s})=R_{s,\upsilon s}R_{s^3,\upsilon s^3}\ldots R_{s^{n-2},\upsilon s^{n-2}}. \tag{33}$$

Si n est de la forme $8x+7$, on pourra prendre $\upsilon=1$, puisqu'on aura $2^{\frac{n-1}{2}}\equiv 1$, et les formules (32), (33) donneront

$$\begin{cases}\vartheta(\rho)=R_{1,1}R_{s^2,s^2}\ldots R_{s^{n-3},s^{n-3}},\\ \vartheta(\rho^{s})=R_{s,s}R_{s^3,s^3}\ldots R_{s^{n-2},s^{n-2}}.\end{cases} \tag{34}$$

D'autre part, comme on aura

$$\vartheta(\rho)=c_0+c_1(\rho+\rho^{s^2}+\ldots+\rho^{s^{n-3}})+c_2(\rho^{s}+\rho^{s^3}+\ldots+\rho^{s^{n-1}}),$$
$$\vartheta(\rho^{s})=c_0+c_1(\rho^{s}+\rho^{s^3}+\ldots+\rho^{s^{n-3}})+c_2(\rho+\rho^{s^2}+\ldots+\rho^{s^{n-2}}),$$

on en conclura

$$(35)\quad \begin{cases} X = 2c_0 - c_1 - c_2 = \vartheta(\rho) + \vartheta(\rho^s), \\ Y = c_1 - c_2 = \dfrac{\vartheta(\rho) - \vartheta(\rho^s)}{\rho - \rho^s + \ldots + \rho^{s^{n-3}} - \rho^{s^{n-2}}} \\ \qquad = (-1)^{\frac{n-1}{2}} n(\rho - \rho^s + \ldots - \rho^{s^{n-3}})[\vartheta(\rho) - \vartheta(\rho^s)]. \end{cases}$$

Soit maintenant

$$(36)\quad \Pi_{h,k} = \frac{1.2.3\ldots[(h+k)\varpi]}{(1.2.3\ldots h\varpi)(1.2.3\ldots k\varpi)},$$

et supposons chacun des nombres h, k renfermé entre les limites 0, n. On aura

$$(37)\quad \Pi_{h,k} \equiv 0 \pmod{p}$$

si la somme $h+k$ est renfermée entre les limites n et $2n$; et, au contraire, $\Pi_{h,k}$ ne sera point divisible par p, lorsque $h+k$ sera compris entre les limites 0, n. D'un autre côté, en supposant

$$h + k < n \quad \text{et} \quad n - h - k = l,$$

en sorte que la condition (21) soit vérifiée, on aura

$$1.2.3\ldots(n-1) \equiv [1.2.3\ldots(h+k)\varpi][(-1)(-2)\ldots(-l\varpi)]$$
$$\equiv [1.2.3\ldots(h+k)\varpi](-1)^{l\varpi}(1.2.3\ldots l\varpi) \equiv -1,$$

$$1.2.3\ldots(h+k)\varpi = (-1)^{l\varpi+1}\frac{1}{1.2.3\ldots l\varpi}$$

et, par conséquent,

$$(38)\quad \Pi_{h,k} = \frac{(-1)^{l\varpi+1}}{(1.2\ldots h\varpi)(1.2\ldots k\varpi)(1.2\ldots l\varpi)}.$$

Enfin, si l'on pose comme ci-dessus

$$R_{h,k} = F(\rho),$$

on trouvera

$$(39)\quad F(r) = -\Pi_{n-h,n-k}.$$

Cela posé, soit p^λ la plus haute puissance de p qui puisse diviser simultanément X et Y. On aura, en vertu des formules (35),

$$(40)\quad \begin{cases} \dfrac{X}{p^\lambda} = \dfrac{\vartheta(\rho)}{p^\lambda} + \dfrac{\vartheta(\rho^s)}{p^\lambda}, \\ \dfrac{Y}{p^\lambda} = (-1)^{\frac{n-1}{2}} n(\rho - \rho^s + \rho^{s^2} - \ldots + \rho^{s^{n-3}} - \rho^{s^{n-2}})\left[\dfrac{\vartheta(\rho)}{p^\lambda} - \dfrac{\vartheta(\rho^s)}{p^\lambda}\right]; \end{cases}$$

et, comme les seconds membres des formules (40) seront des fonctions symétriques de ρ, ρ^2, ..., ρ^{n-1}, ils devront rester équivalents, suivant le module p, à $\frac{X}{p^\lambda}$ et à $\frac{Y}{p^\lambda}$, quand on y remplacera ρ par r. Donc, alors, l'un et l'autre seront entiers, et l'un d'eux au moins sera non divisible par p. D'ailleurs, si, dans les seconds membres des formules (34), on remplace $R_{h,k}$ par $\frac{p}{R_{-h,-k}}$, toutes les fois que l'indice h est équivalent suivant le module n à l'un des nombres $1, 2, 3, \ldots, \frac{n-1}{2}$, on en conclura

$$(41)\quad \begin{cases} \vartheta(\rho) = p^{\nu'}\varphi(\rho), \\ \vartheta(\rho^s) = p^{\frac{n-1}{2}-\nu'}\chi(\rho) = p^{\nu''}\chi(\rho), \end{cases}$$

ν' étant le nombre de ceux des indices

$$1, \quad s^2, \quad s^4, \quad \ldots, \quad s^{n-3}$$

qui sont équivalents suivant le module n à l'un des suivants

$$(42)\quad 1, \quad 2, \quad 3, \quad \ldots, \quad \frac{n-1}{2},$$

et ν'' étant déterminé par la formule

$$\nu' + \nu'' = \frac{n-1}{2},$$

tandis que $\varphi(r)$, $\chi(r)$ ne seront équivalents ni à zéro ni à $\frac{1}{0}$ suivant le module p. Donc, si l'on prend pour λ le plus petit des nombres ν' et ν'', les seconds membres des formules (40), quand on y remplacera ρ par r, ne deviendront point équivalents à l'infini suivant le module p,

et l'un d'eux au plus sera équivalent à zéro. Donc λ sera l'exposant de la plus haute puissance de p qui divise simultanément X et Y. D'ailleurs, si l'on fait

$$X = p^\lambda x, \qquad Y = p^\lambda y,$$

la formule (31) donnera

$$4p^{\frac{n-1}{2}-2\lambda} = x^2 + ny^2, \tag{43}$$

et comme on trouvera, en posant $\lambda = \nu'$,

$$\frac{n-1}{2} - 2\lambda = \frac{n-1-4\nu'}{2}$$

et, en posant $\lambda = \frac{n-1}{2} - \nu'$,

$$\frac{n-1}{2} - 2\lambda = \frac{4\nu' - (n-1)}{2},$$

il est clair que la formule (43) pourra être réduite à

$$4p^\mu = x^2 + ny^2, \tag{44}$$

la valeur de μ étant

$$\mu = \pm\left(\frac{4\nu' - n + 1}{2}\right). \tag{45}$$

Si n était de la forme $8x+3$, on aurait

$$2^{\frac{n-1}{2}} \equiv -1 \pmod{p},$$

$$\Theta_2\Theta_{2^2}\ldots\Theta_{2^{s-1}} = \Theta_1\Theta_{3^2}\ldots\Theta_{s^{n-2}} = \vartheta(\rho^s),$$

$$R_{1,1}R_{s^2,s^2}\ldots R_{s^{n-1},s^{n-1}} = \frac{\Theta_1^2}{\Theta_2}\frac{\Theta_{3^2}^2}{\Theta_{2^2}}\cdots\frac{\Theta_{s^{n-1}}^2}{\Theta_{2^{n-1}}} = \frac{[\vartheta(\rho)]^2}{\vartheta(\rho^s)},$$

$$R_{s,s}R_{s^2,s^2}\ldots R_{s^{n-1},s^{n-1}} = \frac{[\vartheta(\rho^s)]^2}{\vartheta(\rho)}.$$

Donc alors, à la place des formules (41), on trouverait

$$\frac{[\vartheta(\rho)]^2}{\vartheta(\rho^s)} = p^{\nu'}\varphi(\rho),$$

$$\frac{[\vartheta(\rho^s)]^2}{\vartheta(\rho)} = p^{\nu'}\chi(\rho) = p^{\frac{n-1}{2}-\nu'}\chi(\rho);$$

puis on en conclurait

$$\begin{cases} [\vartheta(\rho)]^2 = p^{\frac{n-1}{2}+\nu'}[\varphi(\rho)]^2\chi(\rho), \\ [\vartheta(\rho^s)]^2 = p^{n-1-\nu'}\varphi(\rho)[\chi(\rho)]^2. \end{cases} \tag{46}$$

Donc alors on devra prendre pour λ le plus petit des deux nombres

$$\frac{1}{3}\left(\frac{n-1}{2} + \nu'\right), \quad \frac{1}{3}(n-1-\nu'),$$

en sorte qu'on aura

$$\frac{n-1}{2} - 2\lambda = \pm\frac{n-1-4\nu'}{6}.$$

Donc alors on vérifiera l'équation

$$4p^\mu = x^2 + ny^2 \tag{47}$$

en nombres entiers si l'on pose

$$\mu = \pm\frac{4\nu' - (n-1)}{6}. \tag{48}$$

Dans les formules (45) et (48), μ est toujours inférieur à $\frac{1}{2}n$, et ν' représente le nombre de ceux des indices (42) qui sont racines de l'équivalence

$$x^{\frac{n-1}{2}} \equiv 1 \pmod{n}.$$

Les autres étant nécessairement racines de l'équivalence

$$x^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

on en conclut

$$\begin{cases} 1^{\frac{n-1}{2}} + 2^{\frac{n-1}{2}} + 3^{\frac{n-1}{2}} + \ldots + \left(\frac{n-1}{2}\right)^{\frac{n-1}{2}} \\ \qquad \equiv \nu' - \left(\frac{n-1}{2} - \nu'\right) \equiv \frac{4\nu' - (n-1)}{2} \end{cases} \pmod{n}. \tag{49}$$

On a d'ailleurs

$$1 + e^{2\sqrt{-1}} + e^{4\sqrt{-1}} + \ldots + e^{\frac{n-1}{2}2\sqrt{-1}} = \frac{1 - e^{\frac{n+1}{2}2\sqrt{-1}}}{1 - e^{2\sqrt{-1}}} = \frac{e^{-\frac{1}{2}2\sqrt{-1}} - e^{\frac{n}{2}2\sqrt{-1}}}{e^{-\frac{1}{2}2\sqrt{-1}} - e^{\frac{1}{2}2\sqrt{-1}}}$$

et, par suite,

$$(50)\quad \begin{cases} 1+\cos z+\cos 2z+\ldots+\cos\dfrac{n-1}{2}z=\dfrac{1}{2}\left(1-\dfrac{\sin\dfrac{n}{2}z}{\sin\dfrac{1}{2}z}\right), \\ \sin z+\sin 2z+\ldots+\sin\dfrac{n-1}{2}z=\dfrac{1}{2}\left(\cot\dfrac{z}{2}-\dfrac{\cos\dfrac{n}{2}z}{\sin\dfrac{z}{2}}\right)=\dfrac{1}{2}\dfrac{\cos\dfrac{z}{2}-\cos\dfrac{n}{2}z}{\sin\dfrac{z}{2}}. \end{cases}$$

Si, $n-1$ étant impair, on différentie $\frac{n-1}{2}$ fois par rapport à z la première des équations (50), on en tirera

$$(-1)^{\frac{n+1}{4}}\left[\sin z+2^{\frac{n-1}{2}}\sin 2z+3^{\frac{n-1}{2}}\sin 3z+\ldots+\left(\frac{n-1}{2}\right)^{\frac{n-1}{2}}\sin\frac{n-1}{2}z\right]$$
$$=-\frac{1}{2}\frac{d^{\frac{n-1}{2}}\dfrac{\sin\frac{n}{2}z}{\sin\frac{1}{2}z}}{dz^{\frac{n-1}{2}}},$$

tandis que la seconde donnera

$$(-1)^{\frac{n-3}{4}}\left[\cos z+2^{\frac{n-1}{2}}\cos 2z+\ldots+\left(\frac{n-1}{2}\right)^{\frac{n-1}{2}}\cos\frac{n-1}{2}z\right]$$
$$=\frac{1}{2}\cdot\frac{d^{\frac{n-1}{2}}\left(\cot\frac{z}{2}-\dfrac{\cos\frac{n}{2}z}{\sin\frac{z}{2}}\right)}{dz^{\frac{n-1}{2}}}.$$

On conclura de cette dernière, en posant $z=0$, après les différentiations,

$$(51)\quad (-1)^{\frac{n-3}{4}}\left[1+2^{\frac{n-1}{2}}+\ldots+\left(\frac{n-1}{2}\right)^{\frac{n-1}{2}}\right]\equiv\frac{d^{\frac{n-1}{2}}\left(\cot\frac{z}{2}-\operatorname{cosec}\frac{z}{2}\right)}{dz^{\frac{n-1}{2}}}\pmod n.$$

D'autre part, si l'on désigne par $\mathfrak{B}_n$ le nombre de Bernoulli qui correspond à l'indice n, en sorte qu'on ait

$$\mathfrak{B}_1=\frac{1}{6},\qquad \mathfrak{B}_2=\frac{1}{30},\qquad \mathfrak{B}_3=\frac{1}{42},\qquad \ldots;$$

on trouvera

$$\operatorname{tang}\frac{z}{2}=2\left[\frac{1}{6}(2^2-1)\frac{z}{1.2}+\frac{1}{30}(2^4-1)\frac{z^3}{1.2.3.4}+\frac{1}{42}(2^6-1)\frac{z^5}{1.2.3.4.5.6}+\ldots\right]$$

et l'équation (51) pourra être réduite à

$$1+2^{\frac{n-1}{2}}+3^{\frac{n-1}{2}}+\ldots+\left(\frac{n-1}{2}\right)^{\frac{n-1}{2}}=(-1)^{\frac{n+1}{4}}\frac{1}{2}\frac{d^{\frac{n-1}{2}}\operatorname{tang}\frac{z}{4}}{dz^{\frac{n-1}{2}}}.$$

On aura donc par suite, en supposant $\frac{n-1}{2}$ impair, ou n de la forme $4x+3$,

$$(52)\quad \begin{cases} 1+2^{\frac{n-1}{2}}+3^{\frac{n-1}{2}}+\ldots+\left(\dfrac{n-1}{2}\right)^{\frac{n-1}{2}}=(-1)^{\frac{n+1}{4}}2\dfrac{2^{\frac{n+1}{2}}-1}{2^{\frac{n-1}{2}}(n+1)}\mathfrak{B}_{\frac{n+1}{4}} \\ \qquad\qquad =(-1)^{\frac{n+1}{4}}2\dfrac{\left(2^{\frac{n+1}{2}}-1\right)}{2^{\frac{n-1}{2}}}\mathfrak{B}_{\frac{n+1}{4}}. \end{cases}$$

Enfin, comme on trouvera : 1° en supposant n de la forme $8x+7$,

$$2^{\frac{n-1}{2}}\equiv 1\pmod n;$$

2° en supposant n de la forme $8x+3$,

$$2^{\frac{n-1}{2}}\equiv -1\pmod n,$$

l'équation (52) donnera, dans le premier cas,

$$1+2^{\frac{n-1}{2}}+3^{\frac{n-1}{2}}+\ldots+\left(\frac{n-1}{2}\right)^{\frac{n-1}{2}}\equiv(-1)^{\frac{n+1}{4}}2\mathfrak{B}_{\frac{n+1}{4}}$$

et, dans le second cas,

$$1+2^{\frac{n-1}{2}}+3^{\frac{n-1}{2}}+\ldots+\left(\frac{n-1}{2}\right)^{\frac{n-1}{2}}\equiv-(-1)^{\frac{n+1}{4}}6\mathfrak{B}_{\frac{n+1}{4}}.$$

On aura donc : 1° en supposant n de la forme $8x+7$,

$$\pm\mu \equiv \frac{4\nu-(n-1)}{2} \equiv (-1)^{\frac{n+1}{4}} 2\mathfrak{A}_{\frac{n+1}{4}} \pmod{n};$$

2° en supposant n de la forme $8x+3$,

$$\pm\mu = \frac{4\nu-(n-1)}{6} = -(-1)^{\frac{n+1}{4}} 2\mathfrak{A}_{\frac{n+1}{4}}.$$

Par conséquent on aura, dans tous les cas,

$$\mu = \pm 2\mathfrak{A}_{\frac{n+1}{4}}. \tag{53}$$

On pourra donc vérifier l'équation (47) en prenant pour μ le plus petit nombre entier équivalent à

$$\pm 2\mathfrak{A}_{\frac{n+1}{4}}.$$

Exemples. — Soit $n=7$. On trouvera

$$2\mathfrak{A}_{\frac{n+1}{4}} \equiv 2\mathfrak{A}_2 \equiv \frac{2}{30} \equiv \frac{1}{15} \equiv 1 \pmod{7},$$

$$\mu = 1.$$

On vérifiera donc alors en nombres entiers l'équation

$$4p = x^2 + 7y^2$$

et, par conséquent, l'équation

$$p = x^2 + 7y^2.$$

Soit encore $n=11$. On trouvera

$$2\mathfrak{A}_{\frac{n+1}{4}} \equiv 2\mathfrak{A}_3 \equiv \frac{2}{42} \equiv \frac{1}{21} \equiv -1 \pmod{11},$$

$$\mu = 1$$

et, par conséquent, on pourra vérifier en nombres entiers l'équation

$$4p^2 = x^2 + 11y^2.$$

Soit $n=163$; 2 sera une racine primitive de l'équation

$$x^{81} \equiv 1,$$

en sorte qu'on pourra supposer

$$s^2 = 2.$$

D'ailleurs, les puissances successives de 2, divisées par 163, donneront pour restes :

1,	2,	4,	8,	16,	32,	64,	−35,	−70,	23,	46,
92,	21,	42,	−79,	5,	10,	20,	40,	80,	− 3,	
− 6,	−12,	−24,	−48,	67,	−29,	−58,	−47,	−69,	25,	
50,	−63,	37,	74,	−15,	−30,	−60,	43,	86,	9,	
18,	36,	72,	−19,	−38,	−76,	11,	22,	44,	88,	
13,	26,	52,	−59,	45,	73,	−17,	−34,	−68,	−27,	
−54,	55,	−53,	57,	−49,	65,	−33,	−66,	31,	62,	
− 39,	−78,	7,	14,	28,	56,	−51,	61,	−41,	81.	

Les restes positifs et inférieurs à $\frac{163}{2} = 81,5$ étant au nombre de 48, on aura

$$\nu = 48, \qquad \frac{n-1}{2} = 81,$$

$$\mu = \pm\frac{4\nu-(n-1)}{6} = \pm\frac{1}{3}\left(2\nu - \frac{n-1}{2}\right) = \pm\frac{1}{3}(96-81) = \pm 5, \qquad \mu = 5.$$

On pourra donc satisfaire, par des valeurs entières de x, y, à l'équation

$$p^3 = x^2 + 163y^2.$$

Revenons aux formules (10) et (16) desquelles on tire

$$R_{h,k} = F(\rho) = (-1)^{\varpi(h+k)} \sum \left(\frac{u}{p}\right)^h \left(\frac{v}{p}\right)^k = (-1)^{\varpi h} \sum \left(\frac{t^m}{p}\right)^h \left(\frac{1+t^m}{p}\right)^k. \tag{54}$$

Si l'on y remplace ρ par r, on trouvera

$$\begin{cases} F(r) \equiv (-1)^{\varpi h} \sum t^{m\varpi h} (1+t^m)^{\varpi k} \\ \qquad \equiv (-1)^{\varpi h} \dfrac{1.2.3\ldots k\varpi}{[1.2.3\ldots(n-h)\varpi][1.2\ldots(h+k-n)\varpi]} n\varpi \end{cases} \pmod{p}; \tag{55}$$

et, comme on a

$$n\varpi \equiv -1, \qquad 1.2.3\ldots k\varpi \equiv \frac{(-1)^{k\varpi+1}}{1.2.3\ldots(n-k)\varpi},$$
$$\frac{1}{1.2.3\ldots(h+k-n)\varpi} \equiv (-1)^{(h+k)\varpi+1}\, 1.2.3\ldots(2n-h-k)\varpi,$$

on conclura de la formule (55)

$$(56)\quad F(r) \equiv -\frac{1.2.3\ldots(2n-h-k)\varpi}{[1.2.3\ldots(n-h)\varpi][1.2.3\ldots(n-k)\varpi]} = -\Pi_{n-h,n-k};$$

ce qui s'accorde avec la formule (39).

Si, dans l'équation (39) ou (56), on remet pour $\Pi_{n-h,n-k}$ sa valeur tirée de l'équation (38), savoir

$$\Pi_{n-h,n-k} \equiv -\frac{(-1)^{l\varpi}}{[1.2.3\ldots(n-h)\varpi][1.2.3\ldots(n-k)\varpi][1.2.3\ldots(n-l)\varpi]}$$
$$\equiv (1.2.3\ldots h\varpi)(1.2.3\ldots k\varpi)(1.2.3\ldots l\varpi)(-1)^{l\varpi+1},$$

on trouvera

$$(57)\quad \begin{cases} F(r) \equiv (-1)^{l\varpi}(1.2.3\ldots h\varpi)(1.2.3\ldots k\varpi)(1.2.3\ldots l\varpi) \\ \quad\equiv (-1)^{(h+k)\varpi}(1.2.3\ldots h\varpi)(1.2.3\ldots k\varpi)[1.2.3\ldots(n-h-k)\varpi] \end{cases} \pmod p.$$

Il est facile de trouver des nombres équivalents, suivant le module p, aux valeurs de x, y qui vérifient la formule (44) ou (47). En effet, soit toujours p^λ la plus haute puissance de p qui divise simultanément X et Y; on aura

$$(58)\quad x = \frac{X}{p^\lambda} = \frac{\vartheta(\rho)}{p^\lambda} + \frac{\vartheta(\rho^s)}{p^\lambda} \equiv \frac{\vartheta(r)}{p^\lambda} + \frac{\vartheta(r^s)}{p^\lambda} \pmod p,$$

$$(59)\quad \begin{cases} y = \dfrac{Y}{p^\lambda} = (-1)^{\frac{n-1}{2}} n(\rho - \rho^s + \ldots - \rho^{s^{n-1}})\left[\dfrac{\vartheta(\rho)}{p^\lambda} - \dfrac{\vartheta(\rho^s)}{p^\lambda}\right] \\ \quad\equiv (-1)^{\frac{n-1}{2}} n(r - r^s + \ldots - r^{s^{n-1}})\left[\dfrac{\vartheta(r)}{p^\lambda} - \dfrac{\vartheta(r^s)}{p^\lambda}\right] \end{cases} \pmod p.$$

D'ailleurs, on déduira sans peine des formules (32) et (33) les valeurs des rapports

$$\frac{\vartheta(r)}{p^\lambda}, \quad \frac{\vartheta(r^s)}{p^\lambda},$$

ou plutôt la valeur de celui qui n'est pas divisible par p. En effet, on y parviendra facilement en remplaçant chaque facteur de la forme

$$R_{h,k}$$

par $\frac{p}{R_{n-h,n-k}}$, toutes les fois que $h+k$ sera renfermé entre les limites 0, n, et remplaçant ensuite ρ par r.

§ II. — *Applications nouvelles des formules établies dans le premier paragraphe.*

Supposons maintenant que n soit un nombre composé et prenons

$$n = \omega\nu,$$

ν désignant un facteur premier de n. Soit encore

$$\omega\varpi = \psi.$$

On aura

$$p - 1 = n\varpi = \nu\psi.$$

De plus, si l'on désigne par ς une racine primitive de

$$x^\nu = 1$$

et par α une racine primitive de

$$x^{\omega} = 1,$$

on pourra prendre

$$\rho = \alpha\varsigma.$$

Cela posé, soient s une racine primitive de l'équivalence

$$x^\nu \equiv 1 \pmod p$$

et u une racine primitive de l'équivalence

$$x^{\nu-1} \equiv 1 \pmod \nu.$$

Les nombres entiers

$$1,\quad 2,\quad 3,\quad \ldots,\quad n-2,\quad n-1$$

seront équivalents, suivant le module n, aux divers termes de la suite

$$1,\quad u,\quad \ldots,\quad u^{\nu-2},\quad \nu+1,\quad \nu+u,\quad \ldots,\quad \nu+u^{\nu-2},\quad \ldots,$$
$$(\omega-1)\nu+1,\quad (\omega-1)\nu+u,\quad \ldots,\quad (\omega-1)\nu+u^{\nu-2};$$

et l'on aura

$$\Theta_h = \vartheta + \varrho^h \theta t + \varrho^{2h}\theta t^2 + \ldots + \varrho^{(p-2)h}\theta t^{p-1}$$
$$= \vartheta + \alpha^h \varsigma^h \theta t + \alpha^{2h}\varsigma^{2h}\theta t^2 + \ldots + \alpha^{(p-2)h}\varsigma^{(p-2)h}\theta t^{p-1}.$$

Supposons d'ailleurs les nombres ν, ω premiers entre eux, et faisons

$$\nu \equiv \frac{1}{\nu} \pmod{\omega};$$

on trouvera

$$\alpha^{u^m+\nu\nu(1-u^m)} = \alpha, \qquad \varsigma^{u^m+\nu\nu(1-u^m)} = \varsigma^{u^m},$$
$$\Theta_{u^m+\nu\nu(1-u^m)} = \vartheta + \alpha\varsigma^{u^m}\theta t + \alpha^2\varsigma^{2u^m}\theta t^2 + \ldots + \alpha^{p-2}\varsigma^{(p-2)u^m}\theta t^{p-1}$$

et, si l'on pose

$$(1)\qquad \Theta_1\Theta_{u^2+\nu\nu(1-u^2)}\ldots\Theta_{u^{\nu-2}+\nu\nu(1-u^{\nu-2})} = \vartheta(\alpha,\varsigma)\Theta_{\nu\nu\frac{\nu-1}{2}},$$

on aura encore

$$(2)\qquad \Theta_{u^m+\nu\nu(h-u^m)} = \Theta_{u^m+\nu\nu(h+\omega k-u^m)} = \vartheta + \alpha^h\varsigma^{u^m}\theta t + \ldots + \alpha^{(p-2)h}\varsigma^{(p-2)u^m}\theta t^{p-1},$$
$$(3)\qquad \vartheta(\alpha,\varsigma) = \vartheta(\alpha,\varsigma^{u^2}) = \vartheta(\alpha,\varsigma^{u^4}) = \ldots = \vartheta(\alpha,\varsigma^{u^{\nu-3}}),$$

et, en supposant h impair,

$$(4)\qquad \Theta_{1+\nu\nu(h-1)}\Theta_{u^2+\nu\nu(h-u^2)}\ldots\Theta_{u^{\nu-2}+\nu\nu(h-u^{\nu-2})} = \vartheta(\alpha^h,\varsigma)\Theta_{\nu\nu\frac{\nu-1}{2}h},$$

$$(5)\qquad \vartheta(\alpha^h,\varsigma) = \vartheta(\alpha^h,\varsigma^{u^2}) = \vartheta(\alpha^h,\varsigma^{u^4}) = \ldots = \vartheta(\alpha^h,\varsigma^{u^{\nu-3}}),$$

$$(6)\qquad \Theta_{-1-\nu\nu(h-1)}\Theta_{-u^2-\nu\nu(h-u^2)}\ldots\Theta_{-u^{\nu-2}-\nu\nu(h-u^{\nu-2})} = \vartheta(\alpha^{-h},\varsigma^{-1})\Theta_{-\nu\nu\frac{\nu-1}{2}h},$$

$$(7)\qquad \begin{cases} \vartheta(\alpha^{-h},\varsigma^{-1}) = \vartheta(\alpha^{-h},\varsigma^{-u^2}) \\ \qquad = \vartheta(\alpha^{-h},\varsigma^{-u^4}) = \ldots = \vartheta(\alpha^{-h},\varsigma^{-u^{\nu-3}}) = \vartheta\left(\alpha^{-h},\varsigma^{u^{\frac{\nu-1}{2}}}\right), \end{cases}$$

$$(8)\qquad \begin{cases} \vartheta(\alpha^h,\varsigma)\vartheta(\alpha^{-h},\varsigma^{-1}) \\ \quad = \dfrac{\Theta_{1+\nu\nu(h-1)}\Theta_{-1-\nu\nu(h-1)}\ldots\Theta_{u^{\nu-3}+\nu\nu(h-u^{\nu-3})}\Theta_{-u^{\nu-3}-\nu\nu(h-u^{\nu-3})}}{\Theta_{\nu\nu\frac{\nu-1}{2}h}\Theta_{-\nu\nu\frac{\nu-1}{2}h}}. \end{cases}$$

Le second membre de la formule (8) se réduit toujours, soit à

$$\pm p^{\frac{n-1}{2}},$$

soit à

$$\pm p^{\frac{n-3}{2}}.$$

Exemple. — Supposons, pour fixer les idées, $\omega = 4$. Si ν est impair et de la forme $4x+1$, on pourra prendre

$$\nu = 1.$$

Par suite, la formule (8) donnera

$$(9)\qquad \vartheta(\alpha^h,\varsigma)\vartheta(\alpha^{-h},\varsigma^{-1}) = \frac{\Theta_{1+\nu(h-1)}\Theta_{-1-\nu(h-1)}\ldots\Theta_{u^{\nu-3}+\nu(h-u^{\nu-3})}\Theta_{-u^{\nu-3}-\nu(h-u^{\nu-3})}}{\Theta_{\nu\frac{\nu-1}{2}h}\Theta_{-\nu\frac{\nu-1}{2}h}}.$$

D'ailleurs, si l'on suppose h impair, ainsi que $\frac{\nu-1}{4}$, on trouvera

$$(10)\qquad \begin{cases} \Theta_{1+\nu(h-1)}\Theta_{-1-\nu(h-1)} = (-1)^{\varpi\nu h}p = (-1)^{\varpi}p, \\ \Theta_{u^2+\nu(h-u^2)}\Theta_{-u^2-\nu(h-u^2)} = (-1)^{\varpi\nu h}p = (-1)^{\varpi}p, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \Theta_{\nu\frac{\nu-1}{2}h}\Theta_{-\nu\frac{\nu-1}{2}h} = (-1)^{\varpi\frac{\nu-1}{2}} = 1. \end{cases}$$

Donc la formule (9) donnera, pour des valeurs impaires de h,

$$(11)\qquad \vartheta(\alpha^h,\varsigma)\vartheta(\alpha^{-h},\varsigma^{-1}) = p^{\frac{\nu-3}{2}}.$$

On trouvera, en particulier,

$$(12)\qquad \vartheta(\alpha,\varsigma)\vartheta(\alpha^{-1},\varsigma^{-1}) = p^{\frac{\nu-3}{2}}.$$

D'autre part, α devant être une racine primitive de

$$x^4 = 1,$$

on pourra prendre

$$\alpha = \sqrt{-1}.$$

Ajoutons que l'on tirera de l'équation (4)

$$\vartheta(\alpha,\varsigma)=\frac{\Theta_1\,\Theta_{n^2+\nu(1-n^2)}\,\Theta_{n^4+\nu(1-n^4)}\cdots\Theta_{n^{\nu-2}+\nu(1-n^{\nu-2})}}{\Theta_{\frac{\nu(\nu-1)}{2}}}. \tag{13}$$

Supposons maintenant

$$\nu=5 \quad \text{ou} \quad n=4.5=20.$$

Les formules (12) et (13) donneront

$$\vartheta(\alpha,\varsigma)\,\vartheta(\alpha^{-1},\varsigma^{-1})=p, \tag{14}$$

$$\vartheta(\alpha,\varsigma)=\frac{\Theta_1\,\Theta_{n^2+5(1-n^2)}}{\Theta_{10}}, \tag{15}$$

u étant une racine primitive de

$$x^4\equiv 1 \pmod 5;$$

et, par conséquent [à cause de $u^2\equiv 1 \pmod 5$],

$$\vartheta(\alpha,\varsigma)=\frac{\Theta_1\,\Theta_{-11}}{\Theta_{10}}=\frac{\Theta_1\,\Theta_9}{\Theta_{10}}=R_{1,9}, \tag{16}$$

$$\vartheta(\alpha^{-1},\varsigma^{-1})=R_{-1,-9}=R_{19,11}. \tag{17}$$

Donc

$$R_{1,9}R_{19,11}=p.$$

De plus, l'équation (4) donnera

$$\vartheta(\alpha^3,\varsigma)=\vartheta(\alpha^{-1},\varsigma)=\frac{\Theta_{11}\,\Theta_{19}}{\Theta_{30}}=R_{11,19}=\vartheta(\alpha^{-1},\varsigma^{-1}). \tag{18}$$

Donc la formule (14) pourra être réduite à

$$p=\vartheta(\alpha,\varsigma)\,\vartheta(\alpha^{-1},\varsigma)=\vartheta(\sqrt{-1},\varsigma)\,\vartheta(-\sqrt{-1},\varsigma).$$

On trouvera de même, en remplaçant ς par ς^3 et α par $\alpha^3=\alpha^{-1}$,

$$p=\vartheta(\alpha,\varsigma^3)\,\vartheta(\alpha^{-1},\varsigma^3),$$

et l'on tirera des formules (16), (17), (18)

$$\vartheta(\alpha^3,\varsigma^3)=\vartheta(\alpha^{-1},\varsigma^3)=R_{3,27}=R_{3,7},$$
$$\vartheta(\alpha^{-3},\varsigma^3)=\vartheta(\alpha^{-3},\varsigma^{-3})=R_{37,33}=R_{17,13}=\vartheta(\alpha,\varsigma^3),$$

en sorte qu'on aura encore

$$R_{3,7}R_{17,13}=p.$$

On trouvera donc, en définitive,

$$p^2=R_{1,9}R_{17,13}\times R_{19,11}R_{3,7}=\vartheta(\alpha,\varsigma)\,\vartheta(\alpha,\varsigma^3)\times\vartheta(\alpha^{-1},\varsigma)\,\vartheta(\alpha^{-1},\varsigma^3);$$

et comme, en posant

$$2\vartheta(\alpha,\varsigma)=\lambda'+\mu'\sqrt{-1}+(\lambda''+\mu''\sqrt{-1})(\varsigma-\varsigma^2+\varsigma^3-\varsigma^4),$$

on en conclura

$$\begin{aligned}
2\vartheta(\alpha,\varsigma^3) &= \lambda'+\mu'\sqrt{-1}-(\lambda''+\mu''\sqrt{-1})(\varsigma-\varsigma^2-\varsigma^3+\varsigma^4),\\
2\vartheta(\alpha^{-1},\varsigma) &= \lambda'-\mu'\sqrt{-1}+(\lambda''-\mu''\sqrt{-1})(\varsigma-\varsigma^2-\varsigma^3+\varsigma^4),\\
2\vartheta(\alpha^{-1},\varsigma^3) &= \lambda'-\mu'\sqrt{-1}-(\lambda''-\mu''\sqrt{-1})(\varsigma-\varsigma^2-\varsigma^3+\varsigma^4),
\end{aligned}$$

on trouvera encore

$$\begin{aligned}
4p &= 4\vartheta(\alpha,\varsigma)\,\vartheta(\alpha^{-1},\varsigma)=4\vartheta(\alpha,\varsigma^3)\,\vartheta(\alpha^{-1},\varsigma^3)\\
&= [\lambda'+\lambda''(\varsigma-\varsigma^2-\varsigma^3+\varsigma^4)]^2+[\mu'+\mu''(\varsigma-\varsigma^2-\varsigma^3+\varsigma^4)]^2\\
&= [\lambda'-\lambda''(\varsigma-\varsigma^2-\varsigma^3+\varsigma^4)]^2+[\mu'-\mu''(\varsigma-\varsigma^2-\varsigma^3+\varsigma^4)]^2
\end{aligned}$$

et, par conséquent,

$$4p=\lambda'^2+\mu'^2+5(\lambda''^2+\mu''^2), \qquad \lambda'\lambda''=-\mu'\mu''. \tag{19}$$

D'autre part, si l'on nomme s et a les racines primitives des équivalences

$$x^5\equiv 1, \qquad x^4\equiv 1 \pmod p, \tag{20}$$

on aura, pour déterminer λ, μ, λ', μ', les formules

$$\left.\begin{aligned}
&\lambda'+\mu'a+(\lambda''+\mu''a)(s-s^2-s^3+s^4)\equiv 2\vartheta(a,s) &&\equiv -2\Pi_{19,11}\equiv 0\\
&\lambda'+\mu'a-(\lambda''+\mu''a)(s-s^2-s^3+s^4)\equiv 2\vartheta(a,s^3) &&\equiv -2\Pi_{3,7}\\
&\lambda'-\mu'a+(\lambda''+\mu''a)(s-s^2-s^3+s^4)\equiv 2\vartheta(a^{-1},s) &&\equiv -2\Pi_{1,9}\\
&\lambda'-\mu'a-(\lambda''+\mu''a)(s-s^2-s^3+s^4)\equiv 2\vartheta(a^{-1},s^3) &&\equiv -2\Pi_{17,13}\equiv 0
\end{aligned}\right\} \pmod p$$

et, par suite,

$$(21)\quad \begin{cases} \lambda' + \mu' a \equiv -\Pi_{3,7}, & \lambda'' + \mu'' a = \dfrac{\Pi_{3,7}}{s - s^2 - s^3 + s^4} \\ \lambda' - \mu' a \equiv -\Pi_{1,9}, & \lambda'' - \mu'' a = \dfrac{\Pi_{1,9}}{s - s^2 - s^3 + s^4} \end{cases} \pmod{p},$$

les valeurs de $\Pi_{3,7}$, $\Pi_{1,9}$ étant

$$(22)\quad \begin{cases} \Pi_{3,7} \equiv \dfrac{10\varpi(10\varpi-1)\dots(7\varpi+1)}{1.2.3\dots 3\varpi}, \\ \Pi_{1,9} \equiv \dfrac{10\varpi(10\varpi-1)\dots(9\varpi+1)}{1.2.3\dots\varpi}. \end{cases}$$

Appliquons maintenant à un cas particulier les formules que nous venons de trouver et supposons

$$p = 41, \qquad n = \frac{p-1}{2} = 20, \qquad \nu = 5, \qquad \omega = 4, \qquad \varpi = 2.$$

On vérifiera les formules (20) en prenant

$$s = -4, \qquad a = 9,$$

et l'on trouvera

$$\Pi_{1,9} = \frac{20.19}{2} = 10.19 \equiv -5.3 \equiv -15,$$

$$\Pi_{3,7} = \frac{20.19.18.17.16.15}{1.2.3.4.5.6} \equiv 8.15.17.19 \equiv 15,$$

$$\lambda' + \mu' a \equiv -15, \qquad \lambda' - \mu' a \equiv 15, \qquad \lambda' \equiv 0, \qquad \mu' \equiv -\frac{15}{9} \equiv 12,$$

$$\frac{1}{s - s^2 - s^3 + s^4} = \frac{1}{28} \equiv -\frac{40}{28} \equiv -\frac{10}{7} \equiv 2\frac{77}{7} \equiv 22,$$

$$\lambda'' + \mu'' a \equiv 22.15 \equiv 2, \qquad \lambda'' - \mu'' a \equiv 22.15 \equiv 2,$$

$$\lambda'' = 2, \qquad \mu'' = 0.$$

Donc l'équation (19) donnera

$$4p = \mu'^2 + 5\lambda''^2$$

ou

$$p = \left(\frac{\mu'}{2}\right)^2 + 5\left(\frac{\lambda''}{2}\right)^2.$$

Effectivement

$$41 = 6^2 + 5.1^2 = 36 + 5.$$

Soit encore

$$p = 101.$$

On trouvera

$$\varpi = 5,$$

$$\Pi_{1,9} = \frac{50.49.48.47.46}{1.2.3.4.5} = 10.49.2.47.46 \equiv -18,$$

$$\Pi_{3,7} \equiv (-18)\frac{45.44.43.42.41.40.39.38.37.36}{6.7.8.9.10.11.12.13.14.15} \equiv (-18)\frac{3.37.38.41.43}{7} \equiv -18.$$

Par suite, on trouvera

$$\lambda'' = 0, \qquad \mu' = 0,$$

$$4p = \lambda'^2 + 5\mu''^2, \qquad p = \left(\frac{\lambda'}{2}\right)^2 + 5\left(\frac{\mu''}{2}\right)^2.$$

On aura d'ailleurs

$$a = 10$$

et

$$\lambda' \equiv \frac{\Pi_{1,9} + \Pi_{3,7}}{2} \equiv \Pi_{1,9} \equiv -18, \qquad \frac{\lambda'}{2} = -9.$$

Effectivement

$$101 = 81 + 5.4 = 9^2 + 5.2^2.$$

En général, lorsque, ν étant impair et de la forme $4x+1$, on suppose

$$\omega = 4,$$

on peut prendre

$$c = 1, \qquad \alpha = \sqrt{-1},$$

et l'on tire de l'équation (4) : 1° en supposant $h = 1$,

$$(23)\quad \Theta_1 \Theta_{n^2+\nu(1-n^2)} \Theta_{n^4+\nu(1-n^4)} \dots \Theta_{n^{\nu-1}+\nu(1-n^{\nu-1})} = \vartheta(\sqrt{-1}, \varsigma)\Theta_{\frac{\nu(\nu-1)}{2}};$$

2° en supposant $h = -1$,

$$(24)\quad \Theta_{1-\nu} \Theta_{n^2-\nu(1+n^2)} \Theta_{n^4-\nu(1+n^4)} \dots \Theta_{n^{\nu-1}-\nu(1+n^{\nu-1})} = \vartheta(-\sqrt{-1}, \varsigma)\Theta_{-\frac{\nu(\nu-1)}{2}}.$$

On a d'ailleurs, dans cette hypothèse,

$$(25)\quad \begin{cases} \vartheta(\sqrt{-1}, \varsigma) = \vartheta(\sqrt{-1}, \varsigma^{n^2}) \\ \qquad\qquad = \vartheta(\sqrt{-1}, \varsigma^{n^4}) = \dots = \vartheta(\sqrt{-1}, \varsigma^{n^{\nu-1}}), \\ \vartheta(-\sqrt{-1}, \varsigma) = \vartheta(-\sqrt{-1}, \varsigma^{n^2}) \\ \qquad\qquad = \vartheta(-\sqrt{-1}, \varsigma^{n^4}) = \dots = \vartheta(-\sqrt{-1}, \varsigma^{n^{\nu-1}}). \end{cases}$$

On trouvera de même

$$(26)\quad \begin{cases} \Theta_{n+\nu(1-n)}\,\Theta_{n^2+\nu(1-n^2)}\cdots\Theta_{n^{\nu-2}+\nu(1-n^{\nu-2})} = \mathfrak{F}(\sqrt{-1},\zeta^n)\,\Theta_{\frac{\nu(\nu-1)}{2}}, \\ \Theta_{n-\nu(1+n)}\,\Theta_{n^2-\nu(1+n^2)}\cdots\Theta_{n^{\nu-2}-\nu(1+n^{\nu-2})} = \mathfrak{F}(-\sqrt{-1},\zeta^n)\,\Theta_{-\frac{\nu(\nu-1)}{2}} \end{cases}$$

et

$$(27)\quad \begin{cases} \mathfrak{F}(\sqrt{-1},\zeta^n) = \mathfrak{F}(\sqrt{-1},\zeta^{n^3}) \\ \qquad\qquad = \mathfrak{F}(\sqrt{-1},\zeta^{n^5}) = \ldots = \mathfrak{F}(\sqrt{-1},\zeta^{n^{\nu-2}}), \\ \mathfrak{F}(-\sqrt{-1},\zeta^n) = \mathfrak{F}(-\sqrt{-1},\zeta^{n^3}) \\ \qquad\qquad = \mathfrak{F}(-\sqrt{-1},\zeta^{n^5}) = \ldots = \mathfrak{F}(-\sqrt{-1},\zeta^{n^{\nu-2}}). \end{cases}$$

Dans ces diverses équations, u désigne une racine primitive de l'équivalence

$$x^{\nu-1} \equiv 1 \pmod{\nu},$$

en sorte qu'on aura

$$u^{\frac{\nu-1}{2}} \equiv -1 \quad \text{ou} \quad 1 + u^{\frac{\nu-1}{2}} \equiv 0 \pmod{\nu}.$$

Cela posé, on trouvera

$$\Theta_{u^{m+\frac{\nu-1}{2}}-\nu\left(1+u^{m+\frac{\nu-1}{2}}\right)} = \Theta_{(1-\nu)u^m u^{\frac{\nu-1}{2}}-\nu} = \Theta_{-(1-\nu)u^m-\nu} = \Theta_{-u^m-\nu(1-u^m)},$$

$$\Theta_{u^m+\nu(1-u^m)}\,\Theta_{u^{m+\frac{\nu-1}{2}}-\nu\left(1+u^{m+\frac{\nu-1}{2}}\right)} = \Theta_{u^m+\nu(1-u^m)}\,\Theta_{-u^m-\nu(1-u^m)} = (-1)^{\varpi\nu^m+\varpi\nu(1-u^m)}\,p = (-1)^{\varpi\nu}p,$$

et l'on tirera : 1° des équations (23), (24),

$$(28)\quad \mathfrak{F}(\sqrt{-1},\zeta)\,\mathfrak{F}(-\sqrt{-1},\zeta) = \frac{(-1)^{\frac{\varpi\nu(\nu-1)}{2}}\,p^{\frac{\nu-1}{2}}}{\Theta_{\frac{\nu(\nu-1)}{2}}\,\Theta_{-\frac{\nu(\nu-1)}{2}}} = \frac{p^{\frac{\nu-1}{2}}}{\Theta_{\frac{\nu(\nu-1)}{2}}\,\Theta_{-\frac{\nu(\nu-1)}{2}}};$$

2° des équations (26) et (27),

$$(29)\quad \mathfrak{F}(\sqrt{-1},\zeta^n)\,\mathfrak{F}(-\sqrt{-1},\zeta^n) = \frac{p^{\frac{\nu-1}{2}}}{\Theta_{\frac{\nu(\nu-1)}{2}}\,\Theta_{-\frac{\nu(\nu-1)}{2}}}.$$

On aura donc, par suite : 1° en supposant ν de la forme $8x+5$,

$$(30)\quad \begin{cases} \mathfrak{F}(\sqrt{-1},\zeta)\,\mathfrak{F}(-\sqrt{-1},\zeta) = \dfrac{p^{\frac{\nu-1}{2}}}{p} = p^{\frac{\nu-3}{2}}, \\ \mathfrak{F}(\sqrt{-1},\zeta^n)\,\mathfrak{F}(-\sqrt{-1},\zeta^n) = p^{\frac{\nu-3}{2}}; \end{cases}$$

2° en supposant p de la forme $8x+1$ et, par conséquent,

$$\Theta_{\frac{\nu(\nu-1)}{2}} = \Theta_0 = -1,$$

$$(31)\quad \begin{cases} \mathfrak{F}(\sqrt{-1},\zeta)\,\mathfrak{F}(-\sqrt{-1},\zeta) = p^{\frac{n-1}{2}}, \\ \mathfrak{F}(\sqrt{-1},\zeta^n)\,\mathfrak{F}(-\sqrt{-1},\zeta^n) = p^{\frac{n-1}{2}}. \end{cases}$$

D'autre part, en posant $h=2$, $\omega=4$, $k=-1$ dans la formule (2), on trouvera

$$(32)\quad \begin{cases} \Theta_{1+\nu}\,\Theta_{n^2+\nu(2-n^2)}\,\Theta_{n^4+\nu(2-n^4)}\cdots\Theta_{n^{\nu-3}+\nu(2-n^{\nu-3})} = \Theta_0\,\Phi(\zeta) \\ = \Theta_{1-3\nu}\,\Theta_{n^2-\nu(2+n^2)}\,\Theta_{n^4-\nu(2+n^4)}\cdots\Theta_{n^{\nu-3}-\nu(2+n^{\nu-3})}, \end{cases}$$

$\Phi(\zeta)$ désignant une fonction de ζ et de $\sqrt{-1}$ à coefficients entiers; et, comme on aura

$$\Theta_{u^{m+\frac{\nu-1}{2}}+\nu\left(2-u^{m+\frac{\nu-1}{2}}\right)} = \Theta_{-u^m+\nu(2+u^m)},$$

on tirera de la formule (32)

$$p^{\frac{\nu-1}{4}} = \Theta_0\,\Phi(\zeta)$$

ou

$$\Phi(\zeta) = -p^{\frac{\nu-1}{4}}.$$

On trouvera de la même manière

$$\Phi(\zeta^n) = -p^{\frac{\nu-1}{4}}.$$

On aura donc

$$(33)\quad \begin{cases} \Theta_{1+\nu}\,\Theta_{n^2+\nu(2-n^2)}\,\Theta_{n^4+\nu(2-n^4)}\cdots\Theta_{n^{\nu-3}+\nu(2-n^{\nu-3})} = p^{\frac{\nu-1}{4}} \\ = \Theta_{n+\nu(2-n)}\,\Theta_{n^3+\nu(2-n^3)}\,\Theta_{n^5+\nu(2-n^5)}\cdots\Theta_{n^{\nu-2}+\nu(2-n^{\nu-2})}; \end{cases}$$

et, comme 2 sera nécessairement de l'une des formes

$$u^{2m}, \quad u^{2m+1},$$

on aura encore

$$(34)\quad \begin{cases} \Theta_2\,\Theta_{2u^2+2\nu(1-u^2)}\,\Theta_{2u^4+2\nu(1-u^4)}\cdots\Theta_{2u^{\nu-3}+2\nu(1-u^{\nu-3})} = p^{\frac{\nu-1}{4}}, \\ \Theta_{2u+2\nu(1-u)}\,\Theta_{2u^3+2\nu(1-u^3)}\,\Theta_{2u^5+2\nu(1-u^5)}\cdots\Theta_{2u^{\nu-2}+2\nu(1-u^{\nu-2})} = p^{\frac{\nu-1}{4}}. \end{cases}$$

Si maintenant on combine l'équation (23) avec la première des formules (34), puis la première des équations (26) avec la seconde des formules (34), on trouvera

$$(35)\quad [\mathfrak{F}(\sqrt{-1},\varsigma)]^2 = R_{1,1}R_{n^2+\nu(1-n^2),n^2+\nu(1-n^2)}\cdots R_{n^{\nu-1}+\nu(1-n^{\nu-2}),n^{\nu-1}+\nu(1-n^{\nu-2})}\,\frac{p^{\frac{\nu-1}{2}}}{\Theta^2_{\frac{\nu(\nu-1)}{2}}}$$

et

$$(36)\quad [\mathfrak{F}(\sqrt{-1},\varsigma^n)]^2 = R_{n+\nu(1-n),n+\nu(1-n)}\cdots R_{n^{\nu-2}+\nu(1-n^{\nu-2}),n^{\nu-2}+\nu(1-n^{\nu-2})}\,\frac{p^{\frac{\nu-1}{2}}}{\Theta^2_{\frac{\nu(\nu-1)}{2}}}.$$

On aura, au contraire,

$$(37)\quad [\mathfrak{F}(-\sqrt{-1},\varsigma)]^2 = R_{1-2\nu,1-2\nu}R_{n^2-\nu(1+n^2),n^2-\nu(1+n^2)}\cdots R_{n^{\nu-2}-\nu(1+n^{\nu-2}),n^{\nu-2}-\nu(1+n^{\nu-2})}\,\frac{p^{\frac{\nu-1}{2}}}{\Theta^2_{-\frac{\nu(\nu-1)}{2}}}$$

et

$$(38)\quad [\mathfrak{F}(-\sqrt{-1},\varsigma^n)]^2 = R_{n-\nu(1+n),n-\nu(1+n)}\cdots R_{n^{\nu-2}-\nu(1+n^{\nu-2}),n^{\nu-2}-\nu(1+n^{\nu-2})}\,\frac{p^{\frac{\nu-1}{2}}}{\Theta^2_{-\frac{\nu(\nu-1)}{2}}}.$$

D'autre part, on aura : 1° en supposant ν de la forme $8x+1$,

$$\Theta_{\frac{\nu(\nu-1)}{2}} = \Theta_{-\frac{\nu(\nu-1)}{2}} = \Theta_0 = -1$$

et, en supposant ν de la forme $8x+5$,

$$\Theta^2_{\frac{\nu(\nu-1)}{2}} = \Theta^2_{-\frac{\nu(\nu-1)}{2}} = (-1)^{\frac{\nu\nu(\nu-1)}{2}}p = p.$$

Donc les formules (35), (36), (37), (38) donneront, si ν est de la forme $8x+1$,

$$(39)\quad \begin{cases} [\mathfrak{F}(\sqrt{-1},\varsigma)]^2 = p^{\frac{\nu-1}{2}}R_{1,1}R_{n^2+\nu(1-n^2),n^2+\nu(1-n^2)}\cdots R_{n^{\nu-2}+\nu(1-n^{\nu-2}),n^{\nu-2}+\nu(1-n^{\nu-2})}, \\ [\mathfrak{F}(\sqrt{-1},\varsigma^n)]^2 = p^{\frac{\nu-1}{2}}R_{n+\nu(1-n),n+\nu(1-n)}\cdots R_{n^{\nu-2}+\nu(1-n^{\nu-2}),n^{\nu-2}+\nu(1-n^{\nu-2})}, \\ [\mathfrak{F}(-\sqrt{-1},\varsigma)]^2 = p^{\frac{\nu-1}{2}}R_{1-2\nu,1-2\nu}R_{n^2-\nu(1+n^2),n^2-\nu(1+n^2)}\cdots R_{n^{\nu-2}-\nu(1+n^{\nu-2}),n^{\nu-2}-\nu(1+n^{\nu-2})}, \\ [\mathfrak{F}(-\sqrt{-1},\varsigma^n)]^2 = p^{\frac{\nu-1}{2}}R_{n-\nu(1+n),n-\nu(1+n)}\cdots R_{n^{\nu-2}-\nu(1+n^{\nu-2}),n^{\nu-2}-\nu(1+n^{\nu-2})}. \end{cases}$$

et, si ν est de la forme $8x+5$,

$$(40)\quad \begin{cases} [\mathfrak{F}(\sqrt{-1},\varsigma)]^2 = p^{\frac{\nu-5}{2}}R_{1,1}R_{n^2+\nu(1-n^2),n^2+\nu(1-n^2)}\cdots R_{n^{\nu-2}+\nu(1-n^{\nu-2}),n^{\nu-2}+\nu(1-n^{\nu-2})}, \\ [\mathfrak{F}(\sqrt{-1},\varsigma^n)]^2 = p^{\frac{\nu-5}{2}}R_{n+\nu(1-n),n+\nu(1-n)}\cdots R_{n^{\nu-2}+\nu(1-n^{\nu-2}),n^{\nu-2}+\nu(1-n^{\nu-2})}, \\ [\mathfrak{F}(-\sqrt{-1},\varsigma)]^2 = p^{\frac{\nu-5}{2}}R_{1-2\nu,1-2\nu}R_{n^2-\nu(1+n^2),n^2-\nu(1+n^2)}\cdots R_{n^{\nu-2}-\nu(1+n^{\nu-2}),n^{\nu-2}-\nu(1+n^{\nu-2})}, \\ [\mathfrak{F}(-\sqrt{-1},\varsigma^n)]^2 = p^{\frac{\nu-5}{2}}R_{n-\nu(1+n),n-\nu(1+n)}\cdots R_{n^{\nu-2}-\nu(1+n^{\nu-2}),n^{\nu-2}-\nu(1+n^{\nu-2})}. \end{cases}$$

Observons encore qu'en vertu des formules (25) on aura

$$(41)\quad \begin{cases} \mathfrak{F}(\sqrt{-1},\varsigma) = b_0 + c_0\sqrt{-1} + (b_1+c_1\sqrt{-1})(\varsigma+\varsigma^{n^2}+\ldots+\varsigma^{n^{\nu-1}}) + (b_2+c_2\sqrt{-1})(\varsigma^n+\ldots+\varsigma^{n^{\nu-2}}) \\ \quad = \dfrac{2b_0-b_1-b_2+(2c_0-c_1-c_2)\sqrt{-1}}{2} + \dfrac{b_1-b_2+(c_1-c_2)\sqrt{-1}}{2}(\varsigma-\varsigma^n+\varsigma^{n^2}-\ldots-\varsigma^{n^{\nu-2}}) \end{cases}$$

et, par conséquent,

$$(42)\quad \begin{cases} 2\mathfrak{F}(\sqrt{-1},\varsigma) = f_0+g_0\sqrt{-1}+(f_1+g_1\sqrt{-1})(\varsigma-\varsigma^n+\varsigma^{n^2}-\ldots+\varsigma^{n^{\nu-1}}-\varsigma^{n^{\nu-2}}), \\ 2\mathfrak{F}(\sqrt{-1},\varsigma^n) = f_0+g_0\sqrt{-1}-(f_1+g_1\sqrt{-1})(\varsigma-\varsigma^n+\varsigma^{n^2}-\ldots+\varsigma^{n^{\nu-1}}-\varsigma^{n^{\nu-2}}), \\ 2\mathfrak{F}(-\sqrt{-1},\varsigma) = f_0-g_0\sqrt{-1}+(f_1-g_1\sqrt{-1})(\varsigma-\varsigma^n+\varsigma^{n^2}-\ldots+\varsigma^{n^{\nu-1}}-\varsigma^{n^{\nu-2}}), \\ 2\mathfrak{F}(-\sqrt{-1},\varsigma^n) = f_0-g_0\sqrt{-1}-(f_1-g_1\sqrt{-1})(\varsigma-\varsigma^n+\varsigma^{n^2}-\ldots+\varsigma^{n^{\nu-1}}-\varsigma^{n^{\nu-2}}), \end{cases}$$

f_0, g_0, f_1, g_1 désignant des nombres entiers. De plus, on aura

$$(43)\quad \begin{cases} \varsigma+\varsigma^n+\varsigma^{n^2}+\ldots+\varsigma^{n^{\nu-2}}+\varsigma^{n^{\nu-1}} = -1, \\ (\varsigma-\varsigma^n+\varsigma^{n^2}-\ldots+\varsigma^{n^{\nu-2}}-\varsigma^{n^{\nu-1}})^2 = (-1)^{\frac{\nu-1}{2}}\nu = \nu. \end{cases}$$

En combinant les formules (42) avec les équations (30) ou (31), on trouvera : 1° en supposant ν de la forme $8x+1$,

$$(44)\quad 4p^{\frac{\nu-1}{2}} = f_0^2+\nu f_1^2+g_0^2+\nu g_1^2, \qquad f_0f_1+g_0g_1 = 0;$$

2° en supposant ν de la forme $8x+5$,

$$(45)\quad 4p^{\frac{\nu-3}{2}} = f_0^2+\nu f_1^2+g_0^2+\nu g_1^2, \qquad f_0f_1+g_0g_1 = 0.$$

D'ailleurs on vérifie la seconde des formules (44) ou (45) en supposant

$$(46)\quad f_0 = \epsilon\delta, \qquad g_0 = \epsilon\varepsilon, \qquad f_1 = -\gamma\varepsilon, \qquad g_1 = \gamma\delta.$$

On aura donc, si ν est de la forme $8x+1$,

$$4p^{\frac{\nu-1}{2}} = (\mathcal{E}^2+\nu\gamma^2)(\delta^2+\varepsilon^2) \tag{47}$$

et, si ν est de la forme $8x+5$,

$$4p^{\frac{\nu-3}{2}} = (\mathcal{E}^2+\nu\gamma^2)(\delta^2+\varepsilon^2). \tag{48}$$

Enfin les formules (42) donneront

$$(49)\quad \begin{cases} 2\vartheta(\sqrt{-1},\varsigma) &= (\delta+\varepsilon\sqrt{-1})[\mathcal{E}+\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}],\\ 2\vartheta(\sqrt{-1},\varsigma^n) &= (\delta+\varepsilon\sqrt{-1})[\mathcal{E}-\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}],\\ 2\vartheta(-\sqrt{-1},\varsigma) &= (\delta-\varepsilon\sqrt{-1})[\mathcal{E}-\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}],\\ 2\vartheta(-\sqrt{-1},\varsigma^n) &= (\delta-\varepsilon\sqrt{-1})[\mathcal{E}+\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}]. \end{cases}$$

Il est bon de remarquer encore que, les valeurs de f_0, g_0, f_1, g_1 étant

$$f_0 = 2b_0 - b_1 - b_2, \qquad f_1 = b_1 - b_2,$$
$$g_0 = 2c_0 - c_1 - c_2, \qquad g_1 = c_1 - c_2,$$

f_1 sera toujours pair ou impair, en même temps que f_0, et g_1 pair ou impair en même temps que g_0. Cela posé, si des deux nombres $\mathcal{E}$, γ l'un était pair, l'autre impair, il faudrait, en vertu des formules (46), que δ, ε fussent tous deux pairs. On aurait donc alors, en supposant ν de la forme $8x+1$,

$$p^{\frac{\nu-1}{2}} = (\mathcal{E}^2+\nu\gamma^2)\left[\left(\frac{\delta}{2}\right)^2+\left(\frac{\varepsilon}{2}\right)^2\right] \tag{50}$$

et, en supposant ν de la forme $8x+5$,

$$p^{\frac{\nu-3}{2}} = (\mathcal{E}^2+\nu\gamma^2)\left[\left(\frac{\delta}{2}\right)^2+\left(\frac{\varepsilon}{2}\right)^2\right], \tag{51}$$

$\frac{\delta}{2}, \frac{\varepsilon}{2}$ étant deux nombres entiers, l'un pair, l'autre impair. De même, si des deux nombres δ, ε l'un était pair, l'autre impair, $\mathcal{E}$ et γ seraient nécessairement pairs, et l'on trouverait : 1° en supposant ν de la forme

$8x+1$,

$$p^{\frac{\nu-1}{2}} = \left[\left(\frac{\mathcal{E}}{2}\right)^2+\nu\left(\frac{\gamma}{2}\right)^2\right](\delta^2+\varepsilon^2); \tag{52}$$

2° en supposant ν de la forme $8x+5$,

$$p^{\frac{\nu-3}{2}} = \left[\left(\frac{\mathcal{E}}{2}\right)^2+\nu\left(\frac{\gamma}{2}\right)^2\right](\delta^2+\varepsilon^2), \tag{53}$$

$\frac{\mathcal{E}}{2}, \frac{\gamma}{2}$ étant deux nombres entiers, l'un pair, l'autre impair. D'ailleurs on ne peut supposer les nombres $\mathcal{E}$, γ, δ, ε pairs tous les quatre, puisque le second membre de la formule (47) serait alors divisible par 16, tandis que le premier est seulement divisible par 4.

Si $\mathcal{E}$, γ, δ, ε étaient supposés impairs, l'équation (47) se décomposerait en deux autres de la forme

$$2p^{\lambda'} = \mathcal{E}^2+\nu\gamma^2, \qquad 2p^{\lambda''} = \delta^2+\varepsilon^2. \tag{54}$$

Or, p étant de la forme $4x+1$ et $\mathcal{E}^2$, γ^2 de la forme $8x+1$, la première des équations (54) aurait un premier membre de la forme $8x+2$ et un second membre de la forme $8x+6$, si ν était de la forme $8x+5$, ce qui serait absurde.

Donc, lorsque ν est de la forme $8x+5$, les deux nombres $\mathcal{E}$ et γ, ou les deux nombres δ, ε, sont pairs et l'équation (47) se réduit à l'une des équations (51), (53).

Au reste, lorsque ν est de la forme $8x+5$, alors, en écrivant $2\mathcal{E}$ et 2γ au lieu de $\mathcal{E}$ et γ, ou 2δ et 2ε au lieu de δ et de ε, on réduit la formule (51) ou (53) à

$$p^{\frac{\nu-3}{2}} = (\mathcal{E}^2+\nu\gamma^2)(\delta^2+\varepsilon^2), \tag{55}$$

tandis que les formules (49) deviennent

$$(56)\quad \begin{cases} \vartheta(\sqrt{-1},\varsigma) &= (\delta+\varepsilon\sqrt{-1})[\mathcal{E}+\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}],\\ \vartheta(\sqrt{-1},\varsigma^n) &= (\delta+\varepsilon\sqrt{-1})[\mathcal{E}-\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}],\\ \vartheta(-\sqrt{-1},\varsigma) &= (\delta-\varepsilon\sqrt{-1})[\mathcal{E}-\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}],\\ \vartheta(-\sqrt{-1},\varsigma^n) &= (\delta-\varepsilon\sqrt{-1})[\mathcal{E}+\gamma(\varsigma-\varsigma^n+\ldots-\varsigma^{n\nu-1})\sqrt{-1}]. \end{cases}$$

Ajoutons que, dans ces dernières formules, on peut toujours supposer δ, ε premiers entre eux, attendu que, si δ, ε avaient pour facteur commun une certaine puissance de p, on pourrait évidemment faire passer ce facteur dans les quantités θ, γ. Cela posé, si l'on nomme a et s les racines primitives des deux équivalences

$$x^{\mu} \equiv 1 \pmod{p}, \tag{57}$$

$$x^{\nu} \equiv 1 \pmod{p} \tag{58}$$

et p^{λ} la plus haute puissance de p, qui divise à la fois θ et γ, λ devra être tel que des quatre rapports

$$\frac{\vartheta(a,s)}{p^{\lambda}}, \quad \frac{\vartheta(a,s^u)}{p^{\lambda}}, \quad \frac{\vartheta(-a,s)}{p^{\lambda}}, \quad \frac{\vartheta(-a,s^u)}{p^{\lambda}} \tag{59}$$

l'un au moins soit équivalent, suivant le module p, à un nombre fini différent de zéro, aucun d'eux n'étant équivalent à $\frac{1}{0}$. De plus, en posant

$$\mu = \frac{\nu-3}{2} - 2\lambda, \qquad \theta = p^{\lambda}x, \qquad \gamma = p^{\lambda}y, \tag{60}$$

on tirera de l'équation (55)

$$p^{\mu} = (\delta^2+\varepsilon^2)(x^2+\nu y^2). \tag{61}$$

Si μ se réduit à l'unité, alors $x^2+\nu y^2$ étant >1 (1), il faudra que l'on ait

$$\delta^2+\varepsilon^2 = 1, \qquad x^2+\nu y^2 = p^{\mu} \tag{62}$$

et, par suite,

$$\delta = 0, \quad \varepsilon = \pm 1 \quad \text{ou} \quad \delta = \pm 1, \quad \varepsilon = 0.$$

Quant à la valeur de λ, on la déduira sans peine des formules (40). Soit, en effet, ν' le nombre de ceux des indices

$$1, \quad u^2+\nu(1-u^2), \quad u^4+\nu(1-u^4), \quad \ldots, \quad u^{\nu-3}+\nu(1-u^{\nu-3}) \tag{63}$$

(1) *Voir* la Note II à la fin du Mémoire.

qui sont équivalents, suivant le module n, à l'un des suivants :

$$1, \quad 2, \quad 3, \quad \ldots, \quad \frac{n-1}{2},$$

et ν'' le nombre de ceux des indices

$$u+\nu(1-u), \quad u^3+\nu(1-u^3), \quad \ldots, \quad u^{\nu-3}+\nu(1-u^{\nu-3}) \tag{64}$$

qui remplissent la même condition,

$$\lambda - \frac{1}{2}\frac{\nu-5}{4}$$

sera évidemment le plus petit des quatre nombres

$$\frac{1}{2}\nu', \quad \frac{1}{2}\left(\frac{\nu-1}{2}-\nu'\right), \quad \frac{1}{2}\nu'', \quad \frac{1}{2}\left(\frac{\nu-1}{2}-\nu''\right). \tag{65}$$

Application. — Soit

$$\nu = 5.$$

On pourra prendre

$$u = 2, \qquad u^2 = 4, \qquad u^3 \equiv 3$$

et les formules (23), (24), (26) donneront

$$\begin{cases} \vartheta(\sqrt{-1},\varsigma) = \dfrac{\Theta_1\Theta_9}{\Theta_{10}} = R_{1,9}, & \vartheta(\sqrt{-1},\varsigma^2) = \dfrac{\Theta_{17}\Theta_{13}}{\Theta_{20}} = R_{13,17}, \\ \vartheta(-\sqrt{-1},\varsigma) = \dfrac{\Theta_{11}\Theta_{19}}{\Theta_{20}} = R_{11,19}, & \vartheta(-\sqrt{-1},\varsigma^2) = \dfrac{\Theta_7\Theta_3}{\Theta_{10}} = R_{7,3}. \end{cases} \tag{66}$$

De plus, si l'on pose

$$R_{1,9} = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{19}\rho^{19} = a_0 + a_1\varsigma\sqrt{-1} - a_2\varsigma^2 - a_3\varsigma^3\sqrt{-1} + \ldots,$$

alors, en ayant égard aux formules

$$\vartheta(\sqrt{-1},\varsigma) = \vartheta(\sqrt{-1},\varsigma^4), \qquad \vartheta(\sqrt{-1},\varsigma^2) = \vartheta(\sqrt{-1},\varsigma^2),$$
$$\vartheta(-\sqrt{-1},\varsigma) = \vartheta(-\sqrt{-1},\varsigma^4), \qquad \vartheta(-\sqrt{-1},\varsigma^2) = \vartheta(-\sqrt{-1},\varsigma^3),$$

on trouvera

$$a_2 - a_{12} = -(a_8 - a_{18}), \qquad a_4 - a_{14} = -(a_6 - a_{16}),$$
$$a_1 - a_{11} = a_9 - a_{19}, \qquad a_3 - a_{13} = a_7 - a_{17}$$

et, par suite,

$$R_{1,9} = a_0 - a_{10} - (a_2 - a_{12})(\varsigma^2 + \varsigma^3) + (a_4 - a_{14})(\varsigma + \varsigma^4) + [a_5 - a_{15} - (a_3 - a_{13})(\varsigma^2 + \varsigma^3) + (a_1 - a_{11})(\varsigma + \varsigma^4)]\sqrt{-1}.$$

On tirera d'ailleurs, de la formule (19) du paragraphe I,

$$\mathcal{F}(-1, \varsigma) = -1, \qquad \mathcal{F}(1, \varsigma) = -1, \qquad \dots$$

et, par suite,

$$\begin{aligned} &a_0 - a_5 + a_{10} - a_{15} = -1, && a_0 + a_5 + a_{10} + a_{15} = -1, \\ &a_1 - a_6 + a_{11} - a_{16} = 0, && a_1 + a_6 + a_{11} + a_{16} = 0, \\ &a_2 - a_7 + a_{12} - a_{17} = 0, && a_2 + a_7 + a_{12} + a_{17} = 0, \\ &a_3 - a_8 + a_{13} - a_{18} = 0, && a_3 + a_8 + a_{13} + a_{18} = 0, \\ &a_4 - a_9 + a_{14} - a_{19} = 0, && a_4 + a_9 + a_{14} + a_{19} = 0; \end{aligned}$$

puis on en conclura

$$a_{10} = -1 - a_0, \quad a_{11} = -a_1, \quad a_{12} = -a_2, \quad a_{13} = -a_3, \quad a_{14} = -a_4,$$
$$a_{15} = -a_5, \quad a_{16} = -a_6, \quad a_{17} = -a_7, \quad a_{18} = -a_8, \quad a_{19} = -a_9;$$
$$R_{1,9} = 1 + 2a_0 + a_2 - a_4 - (a_2 + a_4)(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4) + [2a_5 + a_3 - a_1 + (a_1 - a_3)(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)]\sqrt{-1}.$$

Enfin la formule (55) donnera

$$p = (\delta^2 + 5\gamma^2)(\delta^2 + \varepsilon^2) \tag{67}$$

et, comme $\delta^2 + 5\gamma^2$ surpassera l'unité (1), on en tirera nécessairement

$$\delta^2 + \varepsilon^2 = 1, \qquad p = \delta^2 + 5\gamma^2.$$

(1) $\delta^2 + 5\gamma^2$ pourrait se réduire à l'unité si l'on supposait

$$\delta^2 = 1, \qquad \gamma^2 = 0.$$

Mais alors la formule (67) deviendrait

$$\delta^2 + \varepsilon^2 = p$$

et l'on tirerait des équations (69)

$$4p = 4(\delta^2 + \varepsilon^2) = \Pi_{1,9}\Pi_{3,7},$$

ce qui est absurde, puisque ni $\Pi_{1,9}$ ni $\Pi_{3,7}$ ne sont divisibles par p. Donc la supposition que $\delta^2 + 5\gamma^2$ se réduit à l'unité doit être rejetée.

Donc, tout nombre premier de la forme $20x + 1$ est en même temps de la forme $\delta^2 + 5\gamma^2$, en sorte qu'on peut satisfaire, par des valeurs entières de x, y, à l'équation

$$p = x^2 + 5y^2. \tag{68}$$

Quant aux valeurs de $x = \delta$, $y = \gamma$, elles pourront être déterminées à l'aide des formules

$$\begin{aligned} R_{11,19} &= \mathcal{F}(-\sqrt{-1}, \varsigma) = (\delta - \varepsilon\sqrt{-1})[\varepsilon - \gamma(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)\sqrt{-1}], \\ R_{13,17} &= \mathcal{F}(\sqrt{-1}, \varsigma^2) = (\delta + \varepsilon\sqrt{-1})[\varepsilon - \gamma(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)\sqrt{-1}], \\ R_{1,9} &= \mathcal{F}(\sqrt{-1}, \varsigma) = (\delta + \varepsilon\sqrt{-1})[\varepsilon + \gamma(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)\sqrt{-1}], \\ R_{3,7} &= \mathcal{F}(-\sqrt{-1}, \varsigma^2) = (\delta - \varepsilon\sqrt{-1})[\varepsilon + \gamma(\varsigma - \varsigma^2 - \varsigma^3 + \varsigma^4)\sqrt{-1}], \end{aligned}$$

desquelles on tire

$$\begin{cases} R_{1,9} + R_{13,17} = 2(\delta + \varepsilon\sqrt{-1})\varepsilon, \\ R_{3,7} + R_{11,19} = 2(\delta - \varepsilon\sqrt{-1})\varepsilon \end{cases} \tag{69}$$

et, par suite,

$$(R_{1,9} + R_{13,17})(R_{3,7} + R_{11,19}) = 4(\delta^2 + \varepsilon^2)\varepsilon^2 = 4\varepsilon^2,$$

puis, en remplaçant ρ par r,

$$4\varepsilon^2 \equiv \Pi_{1,9}\Pi_{3,7} = 4x^2,$$

$$x^2 = \frac{1}{4}\Pi_{1,9}\Pi_{3,7}. \tag{70}$$

Comme on aura d'ailleurs

$$\delta = 0, \quad \varepsilon = \pm 1 \quad \text{ou} \quad \delta = \pm 1, \quad \varepsilon = 0,$$

on tirera des formules (69), en y remplaçant ρ par r,

$$\pm\Pi_{1,9} \equiv \Pi_{3,7}. \tag{71}$$

Exemples. — Si l'on prend $p = 41$, on trouvera

$$\Pi_{3,7} \equiv -\Pi_{1,9} \equiv 15 \pmod{41},$$

$$x^2 \equiv -\frac{225}{4} \equiv -\frac{20}{4} \equiv -5 \equiv 36.$$

Effectivement

$$41 = 36 + 5 = 6^2 + 5.1^2.$$

Si l'on prend $p = 101$, on aura

$$\Pi_{1,9} \equiv \Pi_{3,7} \equiv -18,$$

$$x^2 \equiv \left(\frac{18}{2}\right)^2 \equiv 9^2 \equiv 81.$$

Effectivement

$$101 = 81 + 20 = 9^2 + 5.2^2.$$

Si l'on prend $p = 61$, on aura

$$\varpi = 3,$$

$$\Pi_{1,9} = \frac{30.29.28}{1.2.3} \equiv -27 \equiv 34,$$

$$\Pi_{3,7} = (-27)\frac{27.26.25.24.23.22}{4.5.6.7.8.9} \equiv -34,$$

$$x^2 \equiv -17^2 \equiv -289 \equiv 16 \equiv -45.$$

Effectivement

$$61 = 16 + 45 = 4^2 + 5.3^2.$$

Soit encore $p = 181$. On trouvera

$$\varpi = 9,$$

$$\Pi_{1,9} = \frac{90.89.88.87.86.85.84.83.82}{1.2.3.4.5.6.7.8.9} \equiv -\frac{1}{2}\frac{1.3.5.7.9.11.13.15.17}{1.2.3.4.5.6.7.8.9} \equiv -2,$$

$$x^2 \equiv -5y^2 \equiv \pm\left(\frac{2}{2}\right)^2 \equiv \pm 1 \equiv \mp 180.$$

Effectivement

$$181 = 1 + 180 = 1^2 + 5.6^2.$$

Seconde application. — Supposons

$$\nu = 13.$$

u sera racine de

$$u^{13} \equiv 1 \pmod{13},$$

et l'on pourra prendre

$$u = 2,$$

$$u^0 \equiv 1, \quad u \equiv 2, \quad u^2 \equiv 4, \quad u^3 \equiv -5, \quad u^4 \equiv 3, \quad u^5 \equiv 6,$$
$$u^6 \equiv -1, \quad u^7 \equiv -2, \quad u^8 \equiv -4, \quad u^9 \equiv 5, \quad u^{10} \equiv -3, \quad u^{11} \equiv -6.$$

Cela posé, les termes de la série (63) seront équivalents, suivant le module $4.13 = 52$, aux quantités

$$1, \quad 4 - 39 \equiv 17, \quad 3 - 26 \equiv 29, \quad -1 + 26 \equiv 25,$$
$$-4 + 65 \equiv 9, \quad -3 + 52 \equiv 49,$$

dont quatre sont renfermées entre les limites 0 et 26, tandis que les termes de la série (64) seront équivalents, suivant le même module, aux quantités

$$2 - 13 \equiv 41, \quad -5 + 78 \equiv 21, \quad 6 - 65 \equiv 45, \quad -2 + 39 \equiv 37,$$
$$5 - 52 \equiv 5, \quad -6 + 39 \equiv 33,$$

dont deux sont renfermées entre les limites 0 et 26. On aura donc

$$\nu' = 4, \quad \nu'' = 2,$$

$$\frac{1}{2}\nu' = 2, \quad \frac{1}{2}\left(\frac{\nu - 1}{2} - \nu'\right) = 1, \quad \frac{1}{2}\nu'' = 1, \quad \frac{1}{2}\left(\frac{\nu - 1}{2} - \nu''\right) = 2$$

et, par suite,

$$\lambda - \frac{1}{2}\frac{\nu - 5}{4} = 1,$$

$$\lambda = 1 + \frac{1}{2}\frac{\nu - 5}{4} = 1 + 1 = 2, \quad \mu = \frac{\nu - 3}{2} - 2\lambda = 5 - 4 = 1.$$

Donc on pourra résoudre en nombres entiers l'équation

$$(72) \qquad p = (\delta^2 + \varepsilon^2)(x^2 + 13y^2),$$

et comme $x^2 + 13y^2$ surpassera l'unité (1), attendu qu'on ne peut supposer $\gamma = 0$, $y = 0$ (1), on aura nécessairement

$$(73) \qquad x^2 + 13y^2 = p,$$
$$\delta^2 + \varepsilon^2 = 1,$$
$$\delta = 0, \quad x = \pm 1 \quad \text{ou} \quad \delta = \pm 1, \quad \varepsilon = 0.$$

(1) Si γ s'évanouissait, les formules (56) donneraient

$$\vartheta(\sqrt{-1}, \zeta) = \vartheta(\sqrt{-1}, \zeta^{\nu})$$

On tirera d'ailleurs des formules (23) et (26)

$$(74)\qquad \begin{cases} \vartheta(\sqrt{-1},\varsigma) = \dfrac{\Theta_1\Theta_{17}\Theta_{19}\Theta_{25}\Theta_9\Theta_{33}}{\Theta_{26}} = pR_{1,25}R_{9,17}R_{29,49}, \\ \vartheta(\sqrt{-1},\varsigma^u) = \dfrac{\Theta_{41}\Theta_{21}\Theta_{15}\Theta_{27}\Theta_5\Theta_{38}}{\Theta_{26}} = pR_{37,41}R_{21,5}R_{33,45}, \end{cases}$$

et, par suite,

$$\frac{\vartheta(a,s)}{\vartheta(a,s^u)} \equiv 1 \pmod{p}\ (a),$$

ce qu'on ne saurait admettre, eu égard aux équations (74), en vertu desquelles on a

$$\frac{\vartheta(a,s)}{\vartheta(a,s^u)} \equiv 0 \pmod{p}.$$

(a) Il est bon d'observer qu'on doit entendre ici par

$$\frac{\vartheta(a,s)}{\vartheta(a,s^u)}$$

ce que devient le rapport

$$\frac{\vartheta(\sqrt{-1},\varsigma)}{\vartheta(\sqrt{-1},\varsigma^u)}$$

quand on y substitue a au lieu de $\sqrt{-1}$ et ς au lieu de s, après l'avoir transformé à l'aide de la formule (12) du paragraphe I, de manière que ces substitutions ne rendent pas le numérateur et le dénominateur simultanément divisibles par p. Sous cette condition, la remarque qu'on vient de faire est exacte et pourrait être exprimée dans les termes suivants :

L'équation

$$\vartheta(\sqrt{-1},\varsigma) = \vartheta(\sqrt{-1},\varsigma^u),$$

jointe aux formules (68), donnerait

$$R_{1,25}R_{9,17}R_{29,49} = R_{37,41}R_{21,5}R_{33,45};$$

puis, en ayant égard à la condition

$$R_{h,k} = \frac{p}{R_{-h,-k}} = \frac{p}{R_{n-h,n-k}}$$

qui subsiste quand aucun des nombres h, k, $h+k$ n'est divisible par $n = 4\nu = 4.13 = 52$, on en conclurait

$$pR_{21,17}R_{29,49} = R_{51,27}R_{13,25}R_{37,41}R_{33,45}.$$

Enfin, en remplaçant dans la dernière formule $\sqrt{-1}$ par a, ς par s, et généralement $R_{h,k}$ par $-\Pi_{n-h,n-k}$, on trouverait

$$p\Pi_{21,5}\Pi_{23,9} \equiv \Pi_{1,25}\Pi_{9,17}\Pi_{13,11}\Pi_{19,7} \pmod{p}.$$

ce qui est absurde, puisque aucun des nombres

$$\Pi_{1,25},\quad \Pi_{9,17},\quad \Pi_{13,11},\quad \Pi_{19,7}$$

ne sera divisible par p. Le rapport entre le premier et le deuxième nombre de la dernière formule est précisément ce qu'on doit entendre par l'expression $\dfrac{\vartheta(a,s)}{\vartheta(a,s^u)}$.

puis, des équations (24) et (26),

$$(75)\qquad \begin{cases} \vartheta(-\sqrt{-1},\varsigma) = pR_{51,27}R_{13,25}R_{33,9}, \\ \vartheta(-\sqrt{-1},\varsigma^u) = pR_{15,11}R_{31,17}R_{19,7}. \end{cases}$$

D'autre part, $\delta^2+\varepsilon^2$ étant réduit à l'unité, les formules (55), (56) donneront

$$p^5 = \mathfrak{E}^2 + 13\gamma^2,$$
$$4\mathfrak{E}^2 = [\vartheta(\sqrt{-1},\varsigma)+\vartheta(\sqrt{-1},\varsigma^u)][\vartheta(-\sqrt{-1},\varsigma)+\vartheta(-\sqrt{-1},\varsigma^u)],$$

ou, parce que $\mathfrak{E} = px^2$, on trouvera

$$4p^4x^2 = [\vartheta(\sqrt{-1},\varsigma)+\vartheta(\sqrt{-1},\varsigma^u)][\vartheta(-\sqrt{-1},\varsigma)+\vartheta(-\sqrt{-1},\varsigma^u)]$$
$$= p^2(R_{1,25}R_{9,17}R_{29,49}+R_{37,41}R_{21,5}R_{33,45})(R_{51,27}R_{13,25}R_{3,33}+R_{15,11}R_{31,17}R_{19,7})$$

ou, ce qui revient au même,

$$x^2 = \frac{1}{4}\left(\frac{R_{1,25}R_{9,17}}{R_{3,33}} + p\frac{R_{21,5}}{R_{11,15}R_{19,7}}\right)\left(p\frac{R_{3,33}}{R_{1,25}R_{9,17}} + \frac{R_{11,15}R_{9,17}}{R_{5,21}}\right),$$

ou bien encore

$$x^2 = \frac{1}{4}\left(p\frac{R_{29,49}}{R_{27,51}R_{33,45}} + \frac{R_{37,41}R_{33,45}}{R_{31,47}}\right)\left(\frac{R_{27,51}R_{33,45}}{R_{29,49}} + p\frac{R_{31,47}}{R_{37,41}R_{33,45}}\right).$$

Si, dans cette dernière formule, on remplace ρ par r, on tirera

$$(76)\qquad x^2 \equiv \frac{1}{4}\frac{\Pi_{11,15}\Pi_{7,19}}{\Pi_{5,21}}\frac{\Pi_{1,25}\Pi_{9,17}}{\Pi_{3,33}} \pmod{p}.$$

Comme on aura, d'ailleurs,

$$\vartheta(\sqrt{-1},\varsigma) = \pm\vartheta(-\sqrt{-1},\varsigma^u), \qquad \vartheta(-\sqrt{-1},\varsigma) = \pm\vartheta(\sqrt{-1},\varsigma^u),$$

on en conclura

$$\frac{\Pi_{11,15}\Pi_{7,19}}{\Pi_{5,21}} = \pm\frac{\Pi_{1,25}\Pi_{9,17}}{\Pi_{3,33}}$$

et, par suite,

$$(77)\qquad x^2 = \pm\left(\frac{1}{2}\frac{\Pi_{1,25}\Pi_{9,17}}{\Pi_{3,33}}\right)^2.$$

On aura de plus

$$(78)\qquad \begin{cases} \Pi_{1,25}=\dfrac{26\varpi(26\varpi-1)\dots(25\varpi+1)}{1.2.3\dots\varpi}, \\ \Pi_{3,23}=\dfrac{26\varpi(26\varpi-1)\dots(23\varpi+1)}{1.2.3\dots3\varpi}, \\ \Pi_{9,17}=\dfrac{26\varpi(26\varpi-1)\dots(17\varpi+1)}{1.2.3\dots9\varpi}. \end{cases}$$

Exemples. — Supposons

$$p=53.$$

On aura

$$\varpi=1,$$

$$\Pi_{1,25}=26\equiv-\frac{1}{2},$$

$$\Pi_{3,23}=\frac{26.25.24}{1.2.3}\equiv-\frac{1}{8}\frac{1.3.5}{1.2.3}\equiv3,$$

$$\Pi_{9,17}=\frac{26.25.24.23.22.21.20.19.18}{1.2.3.4.5.6.7.8.9}\equiv\frac{3}{14}\frac{7.9.11.13.15.17}{4.5.6.7.8.9}\equiv\frac{5}{4}\equiv-12,$$

$$\frac{1}{2}\frac{\Pi_{1,25}\Pi_{9,17}}{\Pi_{3,23}}\equiv\frac{3}{3}\equiv1,$$

$$x^3\equiv1.$$

Effectivement

$$53=1+52=1+13.2^2.$$

Supposons encore

$$p=157.$$

On trouvera

$$\varpi=3,$$

$$\Pi_{1,22}=\frac{78.77.76}{1.2.3}\equiv-\frac{1}{8}\frac{1.3.5}{1.2.3}\equiv-\frac{5}{16},$$

$$\frac{\Pi_{9,17}}{\Pi_{3,23}}=\frac{1}{2^{18}}\frac{19.21.23.25.27.29.31.33.35.37.39.41.43.45.47.49.51.53}{10.11.12.13.14.15.16.17.18.19.20.21.22.23.24.25.26.27}$$

$$=\frac{1}{2^{18}}\frac{29.31.33.35.37.39.41.43.45.47.49.51.53}{10.11.12.13.14.15.16.17.18.20.22.24.26}\equiv-\frac{1}{2},$$

$$\frac{1}{2}\frac{\Pi_{1,25}\Pi_{9,17}}{\Pi_{3,23}}\equiv\frac{5}{64}\equiv-22,$$

$$x^3\equiv\pm(22)^2\equiv\pm13\equiv\mp144.$$

Effectivement

$$157=144+13=12^2+13.1^2.$$

§ III. — *Suite du même sujet.*

Reprenons les formules (4) et (5) du paragraphe II. On en tire

$$(1)\qquad \begin{cases} \vartheta(\alpha^h,\varsigma)=\vartheta(\alpha^h,\varsigma^{n^1})=\vartheta(\alpha^h,\varsigma^{n^2})=\dots=\vartheta(\alpha^h,\varsigma^{n^{\nu-1}}) \\ \qquad=\dfrac{\Theta_{1+\nu\nu(h-1)}\Theta_{n^1+\nu\nu(h-n^1)}\Theta_{n^2+\nu\nu(h-n^2)}\dots\Theta_{n^{\nu-1}+\nu\nu(h-n^{\nu-1})}}{\Theta_{\nu^{\frac{\nu(\nu-1)}{2}}h}}; \end{cases}$$

et l'on trouve de la même manière

$$(2)\qquad \begin{cases} \vartheta(\alpha^h,\varsigma)=\vartheta(\alpha^h,\varsigma^{n^1})=\vartheta(\alpha^h,\varsigma^{n^2})=\dots=\vartheta(\alpha^h,\varsigma^{n^{\nu-1}}) \\ \qquad=\dfrac{\Theta_{n+\nu\nu(h-n^1)}\Theta_{n^1+\nu\nu(h-n^2)}\Theta_{n^2+\nu\nu(h-n^3)}\dots\Theta_{n^{\nu-2}+\nu\nu(h-n^{\nu-1})}}{\Theta_{\nu^{\frac{\nu(\nu-1)}{2}}h}}. \end{cases}$$

On aura d'ailleurs, en vertu de la formule (2) du paragraphe II,

$$\Theta_{n^m+\nu\nu(h-n^m)}=\Theta_{n^m+\nu\nu(h+k\omega-n^m)}.$$

Enfin, comme, en supposant ν premier, on aura

$$u^{\frac{\nu-1}{2}}\equiv-1 \pmod{\nu},$$

on trouvera, si ν est de la forme $4x+1$,

$$(3)\qquad \vartheta(\alpha^h,\varsigma^{-1})=\vartheta\left(\alpha^h,\varsigma^{u^{\frac{\nu-1}{2}}}\right)=\vartheta(\alpha^h,\varsigma)$$

et, si ν est de la forme $4x+3$,

$$(4)\qquad \vartheta(\alpha^h,\varsigma^{-1})=\vartheta\left(\alpha^h,\varsigma^{u^{\frac{\nu-1}{2}}}\right)=\vartheta(\alpha^h,\varsigma^u).$$

Supposons maintenant que ω soit un nombre premier et nommons a une racine primitive de

$$(5)\qquad x^{\omega-1}\equiv0 \pmod{\omega}.$$

Si l'on prend

$$(6)\qquad \vartheta(\alpha,\varsigma)\vartheta(\alpha^a,\varsigma)\dots\vartheta(\alpha^{a^{\omega-2}},\varsigma)=\varphi(\alpha,\varsigma),$$

on aura

$$\varphi(\alpha,\zeta)=\varphi(\alpha^{a},\zeta)=\ldots=\varphi(\alpha^{a^{\nu-1}},\zeta), \tag{7}$$

$$\vartheta(\alpha^{a},\zeta)\vartheta(\alpha^{a^{2}},\zeta)\ldots\vartheta(\alpha^{a^{\omega-1}},\zeta)=\varphi(\alpha^{a},\zeta), \tag{8}$$

$$\varphi(\alpha^{a},\zeta)=\varphi(\alpha^{a^{2}},\zeta)=\ldots=\varphi(\alpha^{a^{\omega-1}},\zeta). \tag{9}$$

On trouvera de plus

$$a^{\frac{\omega-1}{2}}\equiv -1 \pmod{\omega}.$$

Cela posé, si ω et ν ne sont pas tous deux de la forme $4x+1$, on aura

$$\begin{aligned}\varphi(\alpha,\zeta)=\;& a+b\,(\alpha+\alpha^{a^{2}}+\ldots+\alpha^{a^{\nu-1}})+c\,(\alpha^{a}+\alpha^{a^{3}}+\ldots+\alpha^{a^{\nu-2}})\\&+[a'+b'(\alpha+\alpha^{a^{2}}+\ldots+\alpha^{a^{\nu-1}})+c'(\alpha^{a}+\alpha^{a^{3}}+\ldots+\alpha^{a^{\nu-2}})](\zeta+\zeta^{a^{2}}+\ldots+\zeta^{a^{\nu-1}})\\&+[a''+b''(\alpha+\alpha^{a^{2}}+\ldots+\alpha^{a^{\nu-1}})+c''(\alpha^{a}+\alpha^{a^{3}}+\ldots+\alpha^{a^{\nu-2}})](\zeta^{a}+\zeta^{a^{2}}+\ldots+\zeta^{a^{\nu-1}}),\end{aligned}$$

ou, ce qui revient au même,

$$\begin{aligned}2\varphi(\alpha,\zeta)=\;& 2a-b-c+(b-c)(\alpha-\alpha^{a}+\alpha^{a^{2}}-\ldots+\alpha^{a^{\nu-1}}-\alpha^{a^{\nu-2}})\\&+[2a'-b'-c'+(b'-c')(\alpha-\alpha^{a}+\alpha^{a^{2}}-\ldots+\alpha^{a^{\nu-1}}-\alpha^{a^{\nu-2}})](\zeta+\zeta^{a}+\ldots+\zeta^{a^{\nu-1}})\\&+[2a''-b''-c''+(b''-c'')(\alpha-\alpha^{a}+\alpha^{a^{2}}-\ldots+\alpha^{a^{\nu-1}}-\alpha^{a^{\nu-2}})](\zeta^{a}+\zeta^{a^{2}}+\ldots+\zeta^{a^{\nu-1}}),\end{aligned}$$

ou enfin

$$\begin{aligned}4\varphi(\alpha,\zeta)=\;& 2(2a-b-c)-(2a'-b'-c')-(2a''-b''-c'')\\&+[(2a'-b'-c')-(2a''-b''-c'')](\zeta-\zeta^{a}+\zeta^{a^{2}}-\ldots+\zeta^{a^{\nu-2}}-\zeta^{a^{\nu-1}})\\&+[2(b-c)-(b'-c')-(b''-c'')](\alpha-\alpha^{a}+\alpha^{a^{2}}-\ldots+\alpha^{a^{\omega-2}}-\alpha^{a^{\omega-1}})\\&+[(b'-c')-(b''-c'')](\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}})(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}}).\end{aligned}$$

Si l'on fait, pour abréger,

$$\begin{aligned}A&=2(2a-b-c)-(2a'-b'-c')-(2a''-b''-c''),\\B&=2(b-c)-(b'-c')-(b''-c''),\\C&=2a'-b'-c'-(2a''-b''-c''),\\D&=(b'-c')-(b''-c''),\end{aligned}$$

les quatre nombres A, B, C, D seront tous pairs, ou tous impairs, et l'on aura

$$\left\{\begin{aligned}4\varphi(\alpha,\zeta)=\;&A+B(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})+C(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}})\\&+D(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}}).\end{aligned}\right. \tag{10}$$

Si ν et ω étaient tous deux de la forme $4x+1$, alors l'expression

$$\varphi(\alpha,\zeta)=\varphi(\alpha^{-1},\zeta^{-1})$$

se réduirait à une puissance entière de p, et l'équation (10) prendrait la forme

$$4\varphi(\alpha,\zeta)=A, \tag{11}$$

en sorte qu'on aurait

$$B=0,\qquad C=0,\qquad D=0.$$

Lorsque ω et ν ne sont pas tous deux de la forme $4x+1$, le produit

$$\varphi(\alpha,\zeta)\varphi(\alpha^{-1},\zeta^{-1})$$

se réduit à une puissance entière de p. On a d'ailleurs généralement

$$\left\{\begin{aligned}(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})^{2}&=(-1)^{\frac{\omega-1}{2}}\omega,\\(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}})^{2}&=(-1)^{\frac{\nu-1}{2}}\nu.\end{aligned}\right. \tag{12}$$

De plus, on tirera de l'équation (10), en y remplaçant successivement α par α^{a} et ζ par ζ^{a},

$$\left\{\begin{aligned}4\varphi(\alpha,\zeta^{a})=\;&A+B(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})-C(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}})\\&-D(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}}),\\4\varphi(\alpha^{a},\zeta)=\;&A-B(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})+C(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}})\\&-D(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}}),\\4\varphi(\alpha^{a},\zeta^{a})=\;&A-B(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})-C(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}})\\&+D(\alpha-\alpha^{a}+\ldots-\alpha^{a^{\omega-2}})(\zeta-\zeta^{a}+\ldots-\zeta^{a^{\nu-2}});\end{aligned}\right. \tag{13}$$

et l'on trouvera : 1° en supposant ω et ν de la forme $4x+1$,

$$\varphi(\alpha,\zeta)=\varphi(\alpha^{-1},\zeta)=\varphi(\alpha,\zeta^{-1})=\varphi(\alpha^{-1},\zeta^{-1});$$

2° en supposant ν de la forme $4x+1$ et ω de la forme $4x+3$,

$$\varphi(\alpha,\zeta)=\varphi(\alpha,\zeta^{-1}),\qquad \varphi(\alpha^{a},\zeta)=\varphi(\alpha^{-1},\zeta^{-1});$$

3° en supposant ν de la forme $4x+3$ et ω de la forme $4x+1$,

$$\varphi(\alpha,\zeta)=\varphi(\alpha^{-1},\zeta),\qquad \varphi(\alpha,\zeta^{a})=\varphi(\alpha^{-1},\zeta^{-1});$$

4° en supposant ν et ω de la forme $4x+3$,

$$\varphi(\alpha^a, \zeta^u) = \varphi(\alpha^{-1}, \zeta^{-1}).$$

Donc, si l'on fait généralement

$$\varphi(\alpha, \zeta)\,\varphi(\alpha^{-1}, \zeta^{-1}) = p^k, \tag{14}$$

on aura : 1° en supposant ν de la forme $4x+1$ et ω de la forme $4x+3$,

$$p^k = \varphi(\alpha, \zeta)\,\varphi(\alpha^a, \zeta) = \varphi(\alpha, \zeta^u)\,\varphi(\alpha^a, \zeta^u); \tag{15}$$

2° en supposant ν de la forme $4x+3$ et ω de la forme $4x+1$,

$$p^k = \varphi(\alpha, \zeta)\,\varphi(\alpha, \zeta^u) = \varphi(\alpha^a, \zeta)\,\varphi(\alpha^a, \zeta^u); \tag{16}$$

3° en supposant ν et ω de la forme $4x+3$,

$$p^k = \varphi(\alpha, \zeta)\,\varphi(\alpha^a, \zeta^u) = \varphi(\alpha, \zeta^u)\,\varphi(\alpha^a, \zeta). \tag{17}$$

Si maintenant on substitue dans les formules (15), (16), (17) les valeurs de

$$Q(\alpha, \zeta), \quad Q(\alpha^a, \zeta), \quad Q(\alpha, \zeta^u), \quad Q(\alpha^a, \zeta^u)$$

tirées des équations (10), (13), on trouvera, en ayant égard aux formules (12) : 1° en supposant ν de la forme $4x+1$ et ω de la forme $4x+3$,

$$16p^k = A^2 + \omega B^2 + \nu C^2 + \omega\nu D^2, \qquad AC + \omega BD = 0; \tag{18}$$

2° en supposant ν de la forme $4x+3$ et ω de la forme $4x+1$,

$$16p^k = A^2 + \omega B^2 + \nu C^2 + \omega\nu D^2, \qquad AB + \nu CD = 0; \tag{19}$$

3° en supposant ω et ν de la forme $4x+3$,

$$16p^k = A^2 + \omega B^2 + \nu C^2 + \omega\nu D^2, \qquad AD - BC = 0. \tag{20}$$

On vérifie les équations (18) en prenant

$$A = \varepsilon\delta, \qquad B = \varepsilon\varepsilon, \qquad C = -\omega\gamma\varepsilon, \qquad D = \gamma\delta$$

et, par suite,

$$16p^k = (\delta^2 + \omega\varepsilon^2)(\varepsilon^2 + \nu\omega\gamma^2), \tag{21}$$

ou bien

$$A = \omega\varepsilon\delta, \qquad B = \varepsilon\varepsilon, \qquad C = -\gamma\varepsilon, \qquad D = \gamma\delta$$

et, par suite,

$$16p^k = (\omega\delta^2 + \varepsilon^2)(\omega\varepsilon^2 + \nu\gamma^2). \tag{22}$$

On vérifie les équations (19) en prenant

$$A = \varepsilon\delta, \qquad B = \nu\gamma\varepsilon, \qquad C = -\varepsilon\varepsilon, \qquad D = \gamma\delta$$

et, par suite,

$$16p^k = (\delta^2 + \nu\varepsilon^2)(\varepsilon^2 + \omega\nu\gamma^2), \tag{23}$$

ou bien

$$A = \nu\varepsilon\delta, \qquad B = \gamma\varepsilon, \qquad C = -\varepsilon\varepsilon, \qquad D = \gamma\delta$$

et, par suite,

$$16p^k = (\nu\delta^2 + \varepsilon^2)(\nu\varepsilon^2 + \omega\gamma^2). \tag{24}$$

Enfin, on vérifie les équations (20) en prenant

$$A = \varepsilon\delta, \qquad B = \varepsilon\varepsilon, \qquad C = \gamma\delta, \qquad D = \gamma\varepsilon$$

et, par suite,

$$16p^k = (\delta^2 + \omega\varepsilon^2)(\varepsilon^2 + \nu\gamma^2). \tag{25}$$

Applications. — Supposons, pour fixer les idées,

$$\nu = 5, \qquad \omega = 3, \qquad \omega\nu = 15;$$

on aura

$$v \equiv \frac{1}{\nu} \equiv \frac{1}{5} \equiv -1 \pmod 3;$$

$$u = 2, \quad a = 2; \quad u^5 = 1, \quad u = 2, \quad u^3 \equiv 4, \quad u^3 \equiv 3 \pmod 5;$$

$$u^m + v\nu(h - u^m) = u^m - 5(h - u^m) = 6u^m - 5h,$$

$$\vartheta(\alpha^h, \zeta) = \vartheta(\alpha^h, \zeta^h) = \frac{\Theta_{6-5h}\Theta_{24-5h}}{\Theta_{30-10h}} = \frac{\Theta_{6-5h}\Theta_{9-5h}}{\Theta_{-10h}},$$

$$\vartheta(\alpha^h, \zeta^2) = \vartheta(\alpha^h, \zeta^3) = \frac{\Theta_{12-5h}\Theta_{18-5h}}{\Theta_{30-10h}} = \frac{\Theta_{12-5h}\Theta_{3-5h}}{\Theta_{-10h}};$$

on trouvera par suite

$$(26)\qquad \begin{cases} \varphi(\alpha,\varsigma) = \vartheta(\alpha,\varsigma) = \dfrac{\Theta_1\Theta_5}{\Theta_{-10}} = \dfrac{\Theta_1\Theta_5}{\Theta_5} = R_{1,5}, \\ \varphi(\alpha^3,\varsigma) = \vartheta(\alpha^3,\varsigma) = \dfrac{\Theta_{-3}\Theta_{-1}}{\Theta_{-5}} = R_{-1,-3} = R_{14,11}, \\ \varphi(\alpha,\varsigma^2) = \vartheta(\alpha,\varsigma^2) = \dfrac{\Theta_7\Theta_{-7}}{\Theta_5} = R_{7,-2} = R_{7,13}, \\ \varphi(\alpha^3,\varsigma^2) = \vartheta(\alpha^3,\varsigma^2) = \dfrac{\Theta_2\Theta_{-7}}{\Theta_{-5}} = R_{2,-7} = R_{2,8}. \end{cases}$$

Cela posé, on aura

$$p^k = \varphi(\alpha,\varsigma)\varphi(\alpha^3,\varsigma) = \varphi(\alpha,\varsigma^3)\varphi(\alpha^3,\varsigma^2) = R_{1,5}R_{14,11} = R_{7,13}R_{2,8} = p,$$
$$k = 1$$

et la formule (21) ou (22) donnera

$$(27)\qquad 16p = (\delta^2 + 3\varepsilon^2)(\mathfrak{E}^2 + 15\gamma^2)$$

ou

$$(28)\qquad 16p = (\varepsilon^2 + 3\delta^2)(3\mathfrak{E}^2 + 5\gamma^2).$$

Revenons aux formules (10) et (13) et supposons ν de la forme $4x+1$ et ω de la forme $4x+3$. On trouvera : 1° en prenant

$$A = \mathfrak{E}\delta, \qquad B = \mathfrak{E}\varepsilon, \qquad C = -\omega\gamma\varepsilon, \qquad D = \gamma\delta,$$

$$(29)\quad \begin{cases} 4\varphi(\alpha,\varsigma) = [\delta + \varepsilon(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][\mathfrak{E} + \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})], \\ 4\varphi(\alpha,\varsigma^\alpha) = [\delta + \varepsilon(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][\mathfrak{E} - \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})], \\ 4\varphi(\alpha^\alpha,\varsigma) = [\delta - \varepsilon(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][\mathfrak{E} - \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})], \\ 4\varphi(\alpha^\alpha,\varsigma^\alpha) = [\delta - \varepsilon(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][\mathfrak{E} + \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})]. \end{cases}$$

Si l'on prend, au contraire,

$$A = \omega\mathfrak{E}\delta, \qquad B = \mathfrak{E}\varepsilon, \qquad C = -\gamma\varepsilon, \qquad D = \gamma\delta,$$

on aura

$$(30)\quad \begin{cases} 4\varphi(\alpha,\varsigma) = [\varepsilon - \delta(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][\ \mathfrak{E}(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}}) - \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})], \\ 4\varphi(\alpha,\varsigma^\alpha) = [\varepsilon - \delta(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][\ \mathfrak{E}(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}}) + \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})], \\ 4\varphi(\alpha^\alpha,\varsigma) = [\varepsilon + \delta(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][-\mathfrak{E}(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}}) - \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})], \\ 4\varphi(\alpha^\alpha,\varsigma^\alpha) = [\varepsilon + \delta(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})][-\mathfrak{E}(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}}) + \gamma(\varsigma-\varsigma^\alpha+\ldots-\varsigma^{\alpha^{\nu-2}})]. \end{cases}$$

Dans les équations (29), (30) on peut toujours supposer ε, δ premiers entre eux et faire passer les facteurs communs qu'ils pourraient avoir dans $\mathfrak{E}$ et γ. De plus, si les quatre nombres A, B, C, D sont impairs, $\mathfrak{E}$, γ, δ, ε devront l'être aussi, et l'équation (21) se partagera en deux autres de la forme

$$(31)\qquad 4p^{k'} = \delta^2 + \omega\varepsilon^2, \qquad 4p^{k''} = \mathfrak{E}^2 + \nu\omega\gamma^2,$$

ou l'équation (22) en deux autres de la forme

$$(32)\qquad 4p^{k'} = \varepsilon^2 + \omega\delta^2, \qquad 4p^{k''} = \omega\mathfrak{E}^2 + \nu\gamma^2.$$

Si, au contraire, A, B, C, D sont pairs, $\mathfrak{E}$, γ seront impairs et les équations (21), (22) se partageront, ou comme on vient de le dire lorsque δ, ε seront impairs, ou dans le cas contraire, ainsi qu'il suit :

$$(33)\qquad p^{k'} = \delta^2 + \omega\varepsilon^2, \qquad 4p^{k''} = \left(\frac{\mathfrak{E}}{2}\right)^2 + \nu\omega\left(\frac{\gamma}{2}\right)^2,$$

$$(34)\qquad p^{k'} = \varepsilon^2 + \omega\delta^2, \qquad 4p^{k''} = \omega\left(\frac{\mathfrak{E}}{2}\right)^2 + \nu\left(\frac{\gamma}{2}\right)^2.$$

Ajoutons que l'on déterminera facilement $p^{k''}$ en cherchant la plus haute puissance de p qui divise simultanément les deux produits

$$\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^\alpha), \quad \varphi(\alpha^\alpha,\varsigma)\varphi(\alpha^\alpha,\varsigma^\alpha),$$

qui se réduiront, si l'on admet les formules (29), à

$$\frac{1}{16}[\delta + \varepsilon(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})]\ (\mathfrak{E}^2 + \nu\omega\gamma^2),$$
$$\frac{1}{16}[\delta - \varepsilon(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})]^2(\mathfrak{E}^2 + \nu\omega\gamma^2),$$

et, dans le cas contraire, à

$$-\frac{1}{16}[\varepsilon - \delta(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})]\ (\omega\mathfrak{E}^2 + \nu\gamma^2),$$
$$-\frac{1}{16}[\varepsilon - \delta(\alpha-\alpha^\alpha+\ldots-\alpha^{\alpha^{\omega-2}})]^2(\omega\mathfrak{E}^2 + \nu\gamma^2).$$

Supposons, comme ci-dessus,

$$\omega = 3, \qquad \nu = 5, \qquad \omega\nu = 15;$$

on aura

$$\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^{\alpha}) = R_{1,4}\ R_{7,13} = p\frac{R_{7,13}}{R_{14,11}},$$

$$\varphi(\alpha^{\alpha},\varsigma)\varphi(\alpha^{\alpha},\varsigma^{\alpha}) = R_{14,11}R_{2,8} = p\frac{R_{14,11}}{R_{13,7}}.$$

Donc alors $k^{\prime}=1$, et comme on a trouvé $k=1$, on aura nécessairement $k'=0$. Par suite, la somme

$$\delta^2+\omega\varepsilon^2 \qquad \text{ou} \qquad \varepsilon^2+\omega\delta^2$$

se réduira nécessairement ou à l'unité, ou à

$$4=1+\omega=1+3$$

et les nombres 6, γ vérifieront l'une des formules

$$4p=6^2+15\gamma^2, \qquad 4p=3\,6^2+5\gamma^2,$$

$$4p=\left(\frac{6}{2}\right)^2+15\left(\frac{\gamma}{2}\right)^2, \qquad 4p=3\left(\frac{6}{2}\right)^2+5\left(\frac{\gamma}{2}\right)^2.$$

D'ailleurs, les seconds membres de ces dernières formules seraient divisibles par 8 si 6 et γ ou $\frac{6}{2}$ et $\frac{\gamma}{2}$ étaient impairs, tandis que les premiers membres sont divisibles seulement par 4. Donc 6 et γ ou $\frac{6}{2}$ et $\frac{\gamma}{2}$ doivent être pairs et l'on peut résoudre en nombres entiers l'une des équations

$$p=x^2+15y^2, \qquad p=3x^2+5y^2.$$

Or, comme on a généralement

$$x^2\equiv\pm 1 \pmod 5,$$

on en conclut

$$3x^2+5y^2\equiv\pm 2 \pmod 5.$$

Donc p étant de la forme $15x+1$ ne pourra être en même temps de la forme $3x^2+5y^2$, et tout nombre premier de la forme $15x+1$ vérifiera la formule

(35) $$p=x^2+15y^2.$$

Il reste à trouver la valeur de x.

Or, d'après ce qui vient d'être dit, on aura : 1° si l'on suppose $\delta^2+\omega\varepsilon^2=1$,

$$16p=6^2+15\gamma^2=16(x^2+15y^2),$$

$$x^2=\frac{6^2}{16}=\frac{6^2}{16}(\delta^2+\omega\varepsilon^2), \qquad y^2=\frac{\gamma^2}{16}(\delta^2+\omega\varepsilon^2);$$

2° si l'on suppose $\delta^2+\omega\varepsilon^2=4$,

$$4p=6^2+15\gamma^2=4(x^2+15y^2),$$

$$x^2=\frac{6^2}{16}=\frac{6^2}{16}(\delta^2+\omega\varepsilon^2), \qquad y^2=\frac{\gamma^2}{16}(\delta^2+\omega\varepsilon^2).$$

On aura donc, dans tous les cas,

$$x^2=\frac{6^2}{16}(\delta^2+\omega\varepsilon^2), \qquad y^2=\frac{\gamma^2}{16}(\delta^2+\omega\varepsilon^2).$$

D'ailleurs, on tire des formules (29) et (26)

$$\varphi(\alpha,\varsigma)\varphi(\alpha^{\alpha},\varsigma^{\alpha})=\frac{1}{16}(\delta^2+\omega\varepsilon^2)[6+\gamma(\varsigma-\varsigma^{\alpha}+\ldots-\varsigma^{\alpha^{\nu-2}})(\alpha-\alpha^{\alpha}+\ldots-\alpha^{\alpha^{\omega-2}})]^2=R_{1,4}R_{2,8},$$

$$\varphi(\alpha^{\alpha},\varsigma)\varphi(\alpha,\varsigma^{\alpha})=\frac{1}{16}(\delta^2+\omega\varepsilon^2)[6-\gamma(\varsigma-\varsigma^{\alpha}+\ldots-\varsigma^{\alpha^{\nu-2}})(\alpha-\alpha^{\alpha}+\ldots-\alpha^{\alpha^{\omega-2}})]^2=R_{14,11}R_{7,13}.$$

On aura donc, par suite,

$$\frac{1}{2}(R_{14,11}R_{7,13}+R_{1,4}R_{2,8})=x^2-\omega\gamma y^2=x^2-15y^2,$$

puis on conclura, en remplaçant ρ par r,

$$x^2-15y^2\equiv\frac{1}{2}\Pi_{1,4}\Pi_{2,8} \pmod p$$

et, comme on aura de plus

$$x^2+15y^2\equiv 0 \pmod p,$$

on trouvera définitivement

$$x^2\equiv-15y^2\equiv\frac{1}{4}\Pi_{1,4}\Pi_{2,8}.$$

Exemples. — Supposons $p = 31$. On aura

$$\varpi = 2,$$

$$\Pi_{1,4} = \frac{5\varpi(5\varpi-1)\dots(4\varpi+1)}{1.2.3\dots\varpi} = \frac{10.9}{1.2} = 45 \equiv 14,$$

$$\Pi_{2,8} = \frac{10\varpi(10\varpi-1)\dots(8\varpi+1)}{1.2.3\dots 2\varpi} = \frac{20.19.18.17}{1.2.3.4} = 5.19.3.17 \equiv 9,$$

$$x^2 \equiv \frac{1}{4}9.14 \equiv \frac{1}{2}9.7 \equiv \frac{1}{2} \equiv 16 \equiv -15 \equiv -15y^2.$$

Donc

$$p = x^2 + 15y^2 = 16 + 15 = 4^2 + 15.1^2.$$

Supposons encore $p = 61$. On trouvera

$$\varpi = 4,$$

$$\Pi_{1,4} = \frac{20.19.18.17}{1.2.3.4} = 5.19.3.17 \equiv -5.7 \equiv -35 \equiv -\frac{9}{2},$$

$$\Pi_{2,8} = \frac{40.39.38.37.36.35.34.33}{1.2.3.4.5.6.7.8} = 5.17.19.33.37.39 = \frac{5}{2},$$

$$x^2 \equiv \frac{1}{4}\Pi_{1,4}\Pi_{2,8} \equiv -\frac{5}{2}\frac{1}{4}\frac{9}{2} \equiv -\frac{45}{16} \equiv 1 \equiv -60.$$

Effectivement

$$61 = p = 1 + 60 = 1^2 + 15.2^2.$$

En général, ν étant de la forme $4x+1$, ω de la forme $4x+3$, et δ, ε étant supposés premiers entre eux, on conclura des formules (31), (32) ou (33), (34) qu'on peut satisfaire en nombres entiers à l'une des deux équations

$$4p^{k''} = X^2 + \nu\omega Y^2, \qquad 4p^{k''} = \nu X^2 + \omega Y^2, \tag{36}$$

et comme les seconds membres de ces dernières seraient divisibles par 8, si

$$\nu + \omega \qquad \text{ou} \qquad 1 + \nu\omega$$

étant eux-mêmes divisibles par 8, les deux quantités X, Y étaient impaires, tandis que les premiers membres sont seulement divisibles par 4; on aura nécessairement, dans cette hypothèse,

$$X = 2X', \qquad Y = 2Y',$$

$$p^{k''} = X'^2 + \nu\omega Y'^2 \qquad \text{ou} \qquad p^{k''} = \nu X'^2 + \omega Y'^2. \tag{37}$$

Dans ces diverses formules $p^{k''}$ est la plus haute puissance de p qui divise simultanément les deux produits

$$\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^n), \quad \varphi(\alpha^\alpha,\varsigma)\varphi(\alpha^\alpha,\varsigma^n). \tag{38}$$

Soit d'ailleurs p^λ la plus haute puissance de p qui divise simultanément les quatre expressions

$$\varphi(\alpha,\varsigma), \quad \varphi(\alpha,\varsigma^n), \quad \varphi(\alpha^\alpha,\varsigma), \quad \varphi(\alpha^\alpha,\varsigma^n). \tag{39}$$

X, Y seront divisibles par p^λ; et, en posant

$$X = p^\lambda x, \qquad Y = p^\lambda y,$$
$$\mu = k'' - 2\lambda,$$

on tirera des formules (36)

$$4p^\mu = x^2 + \nu\omega y^2 \qquad \text{ou} \qquad 4p^\mu = \nu x^2 + \omega y^2. \tag{40}$$

D'ailleurs, p étant de la forme $\nu\omega x + 1$, la seconde des équations (40) ne pourra être vérifiée qu'autant que l'on aura

$$\nu x^2 \equiv 4 \pmod{\omega},$$
$$\omega y^2 \equiv 4 \pmod{\nu}$$

et, par suite,

$$\nu^{\frac{\omega-1}{2}} \equiv 1 \pmod{\omega},$$
$$\omega^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$$

ou, ce qui revient au même,

$$\left[\frac{\nu}{\omega}\right] = \left[\frac{\omega}{\nu}\right] = 1.$$

Donc, si l'on a

$$\left[\frac{\nu}{\omega}\right] = \left[\frac{\omega}{\nu}\right] = -1, \tag{41}$$

on ne pourra satisfaire à la seconde des formules (40) et l'on aura nécessairement

$$4p^\mu = x^2 + \nu\omega y^2. \tag{42}$$

Application. — Soit $\omega = 3$. Alors, si ν est de la forme $12x+5$, on

aura

$$\left[\frac{\nu}{3}\right]=\left[\frac{5}{3}\right]=-1$$

et, par conséquent, on pourra vérifier, en nombres entiers, l'équation (42). Mais, si ν est de la forme $12x+1$, on aura

$$\left[\frac{\nu}{3}\right]=\left[\frac{1}{3}\right]=1$$

et l'on pourra seulement assurer que l'une des équations (40) est résoluble en nombres entiers.

Exemple. — Soient

$$\omega=3, \qquad \nu=17, \qquad \omega\nu=51.$$

On trouvera

$$u=3, \qquad \alpha=2,$$

$$u^0=1, \quad u=3, \quad u^2\equiv-8, \quad u^3\equiv-7, \quad u^4\equiv-4, \quad u^5\equiv5, \quad u^6\equiv-2 \quad u^7\equiv-6,$$
$$u^8\equiv-1, \quad u^9\equiv-3, \quad u^{10}\equiv8, \quad u^{11}\equiv7, \quad u^{12}\equiv4, \quad u^{13}\equiv-5, \quad u^{14}\equiv2, \quad u^{15}\equiv6,$$

$$v\equiv\frac{1}{\nu}\equiv\frac{1}{17}\equiv-1 \pmod 3,$$

$$u^m+\nu\nu(h-u^m)\equiv u^m-17(h-u^m)\equiv 18u^m-17h;$$

$$\mathfrak{F}(\alpha^h,\zeta)=\frac{\Theta_{18-17h}\Theta_{9-17h}\Theta_{30-17h}\Theta_{15-17h}\Theta_{33-17h}\Theta_{42-17h}\Theta_{21-17h}\Theta_{36-17h}}{\Theta_{17h}},$$

$$\mathfrak{F}(\alpha^h,\zeta^u)=\frac{\Theta_{3-17h}\Theta_{27-17h}\Theta_{39-17h}\Theta_{45-17h}\Theta_{48-17h}\Theta_{24-17h}\Theta_{12-17h}\Theta_{6-17h}}{\Theta_{17h}},$$

puis on en conclura

$$\varphi(\alpha,\zeta)=\frac{\Theta_1\Theta_{13}\Theta_{13}\Theta_{47}\Theta_{16}\Theta_{25}\Theta_1\Theta_{19}}{\Theta_{17}}=R_{1,16}\,R_{43,25}R_{13,4}\,R_{49,19}\frac{\Theta_{17}^2\,\Theta_{68}^2}{\Theta_{17}}$$
$$=R_{1,16}R_{49,25}R_{13,4}R_{49,19}\Theta_{17}^3 \qquad =R_{1,16}\,R_{13,25}R_{13,4}\,R_{49,19}\rho R_{17,17},$$

$$\varphi(\alpha,\zeta^u)=\frac{\Theta_{37}\Theta_{10}\Theta_{22}\Theta_{28}\Theta_{31}\Theta_7\Theta_{16}\Theta_{40}}{\Theta_{17}}=R_{37,31}R_{10,7}\,R_{22,16}R_{28,40}\Theta_{17}^3$$
$$=R_{37,31}R_{10,7}\,R_{22,46}R_{28,40}\rho R_{17,17},$$

$$\varphi(\alpha^2,\zeta)\;=R_{50,35}R_{8,26}\,R_{38,17}R_{2,32}\,\rho R_{34,34},$$
$$\varphi(\alpha^2,\zeta^u)=R_{11,35}R_{11,11}R_{29,5}\,R_{23,11}\rho R_{34,34}.$$

En d'autres termes, on aura

$$(43)\qquad\begin{cases}\varphi(\alpha,\zeta) &=\rho^3\dfrac{R_{13,25}R_{49,19}}{R_{50,35}R_{38,17}R_{34,34}},\\ \varphi(\alpha,\zeta^u) &=\rho^3\dfrac{R_{37,31}R_{25,11}R_{28,40}}{R_{11,11}R_{34,34}},\\ \varphi(\alpha^2,\zeta) &=\rho^3\dfrac{R_{50,35}R_{38,17}R_{34,34}}{R_{13,25}R_{49,19}},\\ \varphi(\alpha^2,\zeta^u)&=\rho^3\dfrac{R_{11,11}R_{34,34}}{R_{37,31}R_{25,46}R_{28,40}}.\end{cases}$$

Or, la plus haute puissance de p, qui divise simultanément les expressions (43), sera p^3. On aura donc

$$\lambda=3.$$

De plus, les produits

$$\varphi(\alpha,\zeta)\varphi(\alpha,\zeta^u), \quad \varphi(\alpha^2,\zeta)\varphi(\alpha^2,\zeta^u)$$

seront l'un et l'autre divisibles par p^7. On aura donc

$$k''=7,$$
$$\mu=k''-2\lambda=7-6=1$$

et l'on pourra résoudre en nombres entiers l'équation

$$(44)\qquad 4p=x^2+51y^2.$$

On trouvera d'ailleurs, en raisonnant comme plus haut,

$$\frac{1}{4}(x^2-51y^2)\equiv\frac{1}{2}\frac{\Pi_{15,20}\Pi_{29,5}\Pi_{23,11}}{\Pi_{40,7}\Pi_{17,17}}\frac{\Pi_{1,16}\Pi_{13,4}\Pi_{17,17}}{\Pi_{8,26}\Pi_{2,32}}$$
$$\equiv\frac{1}{2}\frac{\Pi_{15,20}\Pi_{29,5}\Pi_{23,11}\Pi_{1,16}\Pi_{13,4}}{\Pi_{10,7}\Pi_{8,26}\Pi_{2,32}}$$

et, par suite,

$$(45)\qquad x^2\equiv-51y^2\equiv\frac{\Pi_{1,16}\Pi_{4,13}\Pi_{5,29}\Pi_{11,23}\Pi_{14,20}}{\Pi_{2,32}\Pi_{7,11}\Pi_{8,26}}.$$

En général, lorsque ω est de la forme $4x+3$ et ν de la forme $4x+1$, on peut décomposer l'équation (21) en deux autres de la

forme

$$4p^{k'} = \delta^2 + \omega\varepsilon^2, \qquad 4p^{k'} = \hat{\varepsilon}^2 + \nu\omega\gamma^2, \tag{46}$$

ou l'équation (22) en deux autres de la forme

$$4p^{k'} = \omega\delta^2 + \varepsilon^2, \qquad 4p^{k'} = \omega\hat{\varepsilon}^2 + \nu\gamma^2. \tag{47}$$

Car, chacun des binomes

$$\delta^2 + \omega\varepsilon^2, \quad \omega\delta^2 + \varepsilon^2, \quad \hat{\varepsilon}^2 + \nu\omega\gamma^2, \quad \omega\hat{\varepsilon}^2 + \nu\gamma^2$$

sera nécessairement impair ou divisible par 4 et, si l'un d'eux était impair, les deux termes de l'autre binome dans la formule (21) ou (22) seraient pairs et divisibles par le facteur 4, qu'on pourrait évidemment faire passer dans le binome impair. Ajoutons que l'on pourra toujours supposer $\hat{\varepsilon}$ et ε premiers entre eux ou n'ayant d'autre commun diviseur que le nombre 2.

Cela posé, soit toujours p^λ la plus haute puissance de p qui divise simultanément les expressions (39). $p^{k''}$ sera la plus haute puissance de p qui divise simultanément les produits (38). On aura d'ailleurs

$$k' = k - k'',$$

et l'on pourra résoudre l'équation

$$4p^{k'-2\lambda} = x^2 + \nu\omega y^2, \tag{48}$$

ou

$$4p^{k'-2\lambda} = \omega x^2 + \nu y^2. \tag{49}$$

De plus, on tirera des équations (29)

$$\begin{aligned} 16[\varphi(\alpha,\varsigma)\varphi(\alpha^n,\varsigma^n) + \varphi(\alpha,\varsigma^n)\varphi(\alpha^n,\varsigma)] &= 2(\delta^2 + \omega\varepsilon^2)(\hat{\varepsilon}^2 - \omega\nu\gamma^2) \\ &= 8p^{k'+2\lambda}(x^2 - \omega\nu y^2), \\ 16[\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^n) + \varphi(\alpha^n,\varsigma)\varphi(\alpha^n,\varsigma^n)] &= 2(\delta^2 - \omega\varepsilon^2)(\hat{\varepsilon}^2 + \omega\nu\gamma^2) \\ &= 8p^{k''}(\delta^2 - \omega\varepsilon^2); \end{aligned}$$

ou, ce qui revient au même,

$$\begin{cases} x^2 - \nu\omega y^2 = 2\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha^n,\varsigma^n) + \varphi(\alpha,\varsigma^n)\varphi(\alpha^n,\varsigma)}{p^{k'+2\lambda}}, \\ \delta^2 - \omega\varepsilon^2 = 2\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^n) + \varphi(\alpha^n,\varsigma)\varphi(\alpha^n,\varsigma^n)}{p^{k''}}. \end{cases} \tag{50}$$

En opérant de la même manière, on tirera des formules (30)

$$\begin{cases} \omega x^2 - \nu y^2 = 2\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha^n,\varsigma^n) + \varphi(\alpha,\varsigma^n)\varphi(\alpha^n,\varsigma)}{p^{k'+2\lambda}}, \\ \varepsilon^2 - \omega\delta^2 = 2\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^n) + \varphi(\alpha^n,\varsigma)\varphi(\alpha^n,\varsigma^n)}{p^{k''}}. \end{cases} \tag{51}$$

Si, dans les équations (50), (51), on remplace ρ par r, on déduira facilement des formules ainsi obtenues et des équations (46), (47), (48), (49) les valeurs de x, y, δ, ε.

Exemple. — Soient toujours

$$\omega = 3, \qquad \nu = 5.$$

On aura

$$\begin{aligned} &\varphi(\alpha,\varsigma) = R_{1,4}, \quad \varphi(\alpha^n,\varsigma) = R_{14,11}, \quad \varphi(\alpha,\varsigma^n) = R_{7,13}, \quad \varphi(\alpha^n,\varsigma^n) = R_{2,8}, \\ &k = 1, \quad k' = 0, \quad k'' = 1, \quad \lambda = 0, \end{aligned}$$

et les formules (50) donneront

$$\begin{cases} x^2 - 15y^2 = 2(R_{1,4}R_{2,8} + R_{7,13}R_{14,11}), \\ \delta^2 - 3\varepsilon^2 = 2\dfrac{R_{1,4}R_{7,13} + R_{2,8}R_{14,11}}{p}. \end{cases} \tag{52}$$

De plus, les formules (46) et (48) donneront

$$\delta^2 + 3\varepsilon^2 = 4, \qquad x^2 + 15y^2 = 4p. \tag{53}$$

Enfin, on aura

$$R_{1,4}R_{14,11} = p, \qquad R_{2,8}R_{13,7} = p,$$

et, par suite, les formules (52) se réduiront à

$$x^2-15y^2=2\left(R_{7,13}R_{14,11}+\frac{p^2}{R_{7,13}R_{14,11}}\right),$$
$$\delta^2-3\varepsilon^2=2\left(\frac{R_{7,13}}{R_{14,11}}+\frac{R_{14,11}}{R_{7,13}}\right).$$

Si, dans ces dernières, on remplace ρ par r, on trouvera

$$(54)\qquad \begin{cases} x^2-15y^2\equiv 2\Pi_{1,4}\Pi_{2,8} \\ \delta^2-3\varepsilon^2=2\left(\dfrac{\Pi_{1,4}}{\Pi_{2,8}}+\dfrac{\Pi_{2,8}}{\Pi_{1,4}}\right) \end{cases} \pmod p;$$

puis, en combinant les formules (54) avec les suivantes,

$$\delta^2+3\varepsilon^2=4, \qquad x^2+15y^2\equiv 0 \pmod p,$$

on trouvera

$$x^2\equiv -15y^2\equiv \Pi_{1,4}\Pi_{2,8} \pmod p.$$

Ajoutons que la première des équations (53) entraine l'une des suppositions

$$\delta^2=4, \qquad \varepsilon^2=0,$$
$$\delta^2=1, \qquad \varepsilon^2=1,$$

en vertu desquelles

$$\delta^2-3\varepsilon^2$$

se réduit à 4 ou à -2. Donc

$$(55)\qquad \frac{\Pi_{1,4}}{\Pi_{2,8}}+\frac{\Pi_{2,8}}{\Pi_{1,4}}\equiv 2 \text{ ou } -1 \pmod p.$$

Quant aux valeurs de x, y, elles doivent être paires pour que la seconde des équations (53) puisse être vérifiée.

Prenons, pour fixer les idées, $p=31$. On aura

$$\Pi_{1,4}=14, \qquad \Pi_{2,8}=9 \pmod{31},$$
$$\frac{\Pi_{1,4}}{\Pi_{2,8}}+\frac{\Pi_{2,8}}{\Pi_{1,4}}\equiv 5+\frac{1}{5}\equiv 5-6\equiv -1 \pmod{31},$$
$$\delta^2=1, \qquad \varepsilon^2=1,$$
$$\frac{x^2}{4}\equiv -15\frac{y^2}{4}\equiv 16\equiv -15 \pmod{31},$$
$$31=16+15=4^2+15.1^2.$$

Prenons encore $p=61$. On trouvera

$$\Pi_{1,4}\equiv -\frac{9}{2}, \qquad \Pi_{2,8}\equiv\frac{5}{2} \pmod{61},$$
$$\frac{\Pi_{1,4}}{\Pi_{2,8}}+\frac{\Pi_{2,8}}{\Pi_{1,4}}\equiv -\frac{9}{5}-\frac{5}{9}\equiv -1,$$
$$\frac{x^2}{4}\equiv -15\frac{y^2}{4}\equiv 1\equiv -60,$$
$$61=1+60=1^2+15.2^2.$$

Supposons maintenant que ω soit de la forme $4x+1$ et ν de la forme $4x+3$. L'équation (23) sera divisible en deux autres de la forme

$$(56)\qquad 4p^{k'}=\delta^2+\nu\varepsilon^2, \qquad 4p^{k''}=\mathcal{E}^2+\omega\gamma^2,$$

ou l'équation (24) en deux autres de la forme

$$(57)\qquad 4p^{k'}=\nu\delta^2+\varepsilon^2, \qquad 4p^{k''}=\nu\mathcal{E}^2+\omega\gamma^2,$$

δ, ε étant des nombres non divisibles par p. Si d'ailleurs p^λ désigne la plus haute puissance de p qui divise simultanément $\mathcal{E}$ et γ, alors, en posant

$$\mathcal{E}=p^\lambda x, \qquad \gamma=p^\lambda y,$$

on réduira la seconde des équations (56) ou (57) à

$$(58)\qquad 4p^{k''-2\lambda}=x^2+\nu\omega y^2$$

ou bien à

$$(59)\qquad 4p^{k''-2\lambda}=\nu x^2+\omega y^2.$$

Enfin, au lieu des formules (29) ou (30), on trouvera

$$(60)\qquad \begin{cases} 4\varphi(\alpha,\varsigma) &= [\delta-\varepsilon(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})][\mathcal{E}+\gamma(\alpha-\alpha^n+\ldots-\alpha^{n^{\nu-2}})(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})], \\ 4\varphi(\alpha,\varsigma^n) &= [\delta+\varepsilon(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})][\mathcal{E}-\gamma(\alpha-\alpha^n+\ldots-\alpha^{n^{\nu-2}})(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})], \\ 4\varphi(\alpha^n,\varsigma) &= [\delta-\varepsilon(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})][\mathcal{E}-\gamma(\alpha-\alpha^n+\ldots-\alpha^{n^{\nu-2}})(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})], \\ 4\varphi(\alpha^n,\varsigma^n) &= [\delta+\varepsilon(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})][\mathcal{E}+\gamma(\alpha-\alpha^n+\ldots-\alpha^{n^{\nu-2}})(\varsigma-\varsigma^n+\ldots-\varsigma^{n^{\nu-2}})] \end{cases}$$

ou bien

$$(61)\quad \begin{cases} 4\varphi(\alpha,\zeta) &= [\varepsilon+\delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})][-\delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})+\gamma(\alpha-\alpha^a+\ldots-\alpha^{a^{\mu-1}})],\\ 4\varphi(\alpha,\zeta^n) &= [\varepsilon-\delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})][\ \delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})+\gamma(\alpha-\alpha^a+\ldots-\alpha^{a^{\mu-1}})],\\ 4\varphi(\alpha^a,\zeta) &= [\varepsilon+\delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})][-\delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})-\gamma(\alpha-\alpha^a+\ldots-\alpha^{a^{\mu-1}})],\\ 4\varphi(\alpha^a,\zeta^n) &= [\varepsilon-\delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})][\ \delta(\zeta-\zeta^n+\ldots-\zeta^{n^{\nu-1}})-\gamma(\alpha-\alpha^a+\ldots-\alpha^{a^{\mu-1}})]; \end{cases}$$

puis on en conclura, dans le premier cas,

$$(62)\quad \begin{cases} x^2-\omega\nu y^2 = 2\dfrac{\varphi(\alpha,\zeta)\varphi(\alpha^a,\zeta^n)+\varphi(\alpha^a,\zeta)\varphi(\alpha,\zeta^n)}{p^{k'+2\lambda}},\\ \delta^2-\nu\varepsilon^2 \;\; = 2\dfrac{\varphi(\alpha,\zeta)\varphi(\alpha^a,\zeta)+\varphi(\alpha,\zeta^n)\varphi(\alpha^a,\zeta^n)}{p^{k'}}, \end{cases}$$

et, dans le second cas,

$$(63)\quad \begin{cases} \omega y^2-\nu x^2 = 2\dfrac{\varphi(\alpha,\zeta)\varphi(\alpha^a,\zeta^n)+\varphi(\alpha^a,\zeta)\varphi(\alpha,\zeta^n)}{p^{k'+2\lambda}},\\ \varepsilon^2 \;\; -\nu\delta^2 = 2\dfrac{\varphi(\alpha,\zeta)\varphi(\alpha^a,\zeta)+\varphi(\alpha,\zeta^n)\varphi(\alpha^a,\zeta^n)}{p^{k'}}. \end{cases}$$

Exemple. — Supposons

$$\omega=5,\qquad \nu=7.$$

On trouvera

$$u=3,\qquad a=2,$$

$$v=\frac{1}{7}\equiv -2 \pmod 5,$$

$$u^m+v\nu(h-u^m)=u^m-14(h-u^m)=15u^m-14h,$$

$$\vartheta(\alpha^h,\zeta) = \frac{\Theta_{15-14h}\Theta_{3-14h}\Theta_{10-14h}}{\Theta_{-42h}},$$

$$\vartheta(\alpha^h,\zeta^n) = \frac{\Theta_{-15-14h}\Theta_{3-14h}\Theta_{10-14h}}{\Theta_{-42h}},$$

$$\varphi(\alpha,\zeta) = R_{1,16}\,R_{11,17}R_{4,9}\,R_{13,29}=p^3\frac{R_{13,29}}{R_{34,19}R_{24,18}R_{31,26}},$$

$$\varphi(\alpha,\zeta^n) = R_{34,19}R_{24,18}R_{26,31}R_{22,6}=p\,\frac{R_{34,19}R_{24,18}R_{31,26}}{R_{13,29}},$$

$$\varphi(\alpha^a,\zeta) = R_{2,22}\,R_{24,32}R_{8,18}\,R_{26,23}=p^2\frac{R_{24,32}R_{26,23}}{R_{33,13}R_{27,17}},$$

$$\varphi(\alpha^a,\zeta^n) = R_{33,3}\,R_{1,13}\,R_{27,17}R_{9,12}=p^2\frac{R_{33,3}R_{27,17}}{R_{34,22}R_{26,23}}$$

et

$$k=4,\qquad k'=3,\qquad k''=1,\qquad \lambda=1.$$

On aura, par suite,

$$x^2-\omega\nu y^2 \quad\text{ou}\quad \omega y^2-\nu x^2=2\left(\frac{R_{34,19}R_{24,18}R_{31,26}R_{24,32}R_{26,23}}{R_{13,29}R_{33,13}R_{27,17}}+p^2\times\ldots\right),$$

$$\delta^2-\nu\varepsilon^2 \quad\text{ou}\quad \varepsilon^2-\nu\delta^2=2\left(\frac{R_{34,19}R_{24,18}R_{31,26}R_{33,3}R_{27,17}}{R_{13,29}R_{34,22}R_{26,23}}+p^2\times\ldots\right);$$

puis on en conclura

$$x^2-35y^2 \quad\text{ou}\quad 5y^2-7x^2\equiv 2\frac{\Pi_{1,16}\Pi_{11,17}\Pi_{4,9}}{\Pi_{22,6}}\frac{\Pi_{11,3}\Pi_{9,12}}{\Pi_{2,22}\Pi_{8,18}} \pmod p.$$

$$\delta^2-7\varepsilon^2 \quad\text{ou}\quad \varepsilon^2-7\delta^2\equiv 2\frac{\Pi_{1,16}\Pi_{11,17}\Pi_{4,9}}{\Pi_{22,6}}\frac{\Pi_{2,22}\Pi_{8,18}}{\Pi_{1,13}\Pi_{9,12}} \pmod p.$$

On aura d'ailleurs, en vertu des formules (56),

$$\delta^2+7\varepsilon^2 \quad\text{ou}\quad \varepsilon^2+7\delta^2=4p,$$

$$x^2+35y^2 \quad\text{ou}\quad 5y^2+7x^2=4p.$$

D'autre part, p étant de la forme $15x+1$, on ne peut supposer

$$5y^2+7x^2=4p,$$

puisqu'on en tirerait

$$7x^2\doteq 4,\qquad 7\equiv\left(\frac{2}{x}\right)^2,\qquad 7^2\equiv 1 \pmod 5,$$

tandis que

$$7^2=49\equiv -1 \pmod 5.$$

Donc, on aura simplement

$$(64)\qquad \delta^2+7\varepsilon^2=4p,\qquad x^2+35y^2=4p,$$

les valeurs de

$$x^2,\quad y^2,\quad \delta^2,\quad \varepsilon^2$$

pouvant être déterminées par les formules

$$(65)\quad \begin{cases} x^2=35y^2=\dfrac{\Pi_{1,16}\Pi_{11,17}\Pi_{4,9}}{\Pi_{22,6}}\dfrac{\Pi_{11,3}\Pi_{9,12}}{\Pi_{2,22}\Pi_{8,18}},\\ \delta^2=\;7\varepsilon^2\equiv\dfrac{\Pi_{1,16}\Pi_{11,17}\Pi_{4,9}}{\Pi_{22,6}}\dfrac{\Pi_{2,22}\Pi_{8,18}}{\Pi_{1,13}\Pi_{9,12}}. \end{cases}$$

Si l'on eût pris, au contraire,

$$\omega = 7, \qquad \nu = 5,$$

on aurait trouvé

$$u = 2, \qquad a = 3,$$

$$v = \frac{1}{5} = 3 \pmod 7,$$

$$u^m + v\nu(h - u^m) = 15h - 14u^m,$$

$$\vartheta'(\alpha^h, \varsigma) = \frac{\Theta_{15h-14}\Theta_{15h+14}}{\Theta_{30h}},$$

$$\vartheta'(\alpha^h, \varsigma^u) = \frac{\Theta_{15h+7}\Theta_{15h-7}}{\Theta_{30h}},$$

$$\varphi(\alpha, \varsigma) = \frac{\Theta_7\Theta_{-6}\Theta_{14}\Theta_8\Theta_{11}\Theta_4}{\Theta_{30}\Theta_{25}\Theta_{15}} = R_{1,29}R_{16,9}R_{11,4} = p^3\frac{1}{R_{31,6}R_{19,26}R_{24,31}},$$

$$\varphi(\alpha, \varsigma^u) = \frac{\Theta_{22}\Theta_8\Theta_2\Theta_{23}\Theta_{32}\Theta_{18}}{\Theta_{30}\Theta_{25}\Theta_{15}} = R_{22,8}R_{2,23}R_{32,18} = p^3\frac{R_{32,18}}{R_{13,27}R_{33,12}},$$

$$\varphi(\alpha^a, \varsigma) = R_{31,6}R_{19,26}R_{24,31},$$

$$\varphi(\alpha^a, \varsigma^u) = p\frac{R_{13,27}R_{33,12}}{R_{32,18}},$$

$$k = 3, \qquad k' = 1, \qquad k' = 2, \qquad \lambda = 0,$$

(66) $$4p = x^2 + 35y^2, \qquad 4p = \delta^2 + 7\varepsilon^2,$$

(67)
$$\begin{cases} x^2 \equiv 35y^2 \equiv \dfrac{\Pi_{2,17}}{\Pi_{22,8}\Pi_{2,23}}\Pi_{1,29}\Pi_{16,9}\Pi_{11,4}, \\ \delta^2 \equiv 7\varepsilon^2 \equiv \dfrac{\Pi_{27,8}\Pi_{2,23}}{\Pi_{2,17}}\Pi_{1,29}\Pi_{16,9}\Pi_{11,4}. \end{cases}$$

Il est important d'observer que les équations (65) peuvent être présentées sous les formes

(68)
$$\begin{cases} x^2 \equiv 35y^2 \equiv \dfrac{1}{p^3}[\varphi(\alpha, \varsigma^u)\varphi(\alpha^a, \varsigma) + \varphi(\alpha, \varsigma)\varphi(\alpha^a, \varsigma^u)] \\ \qquad \equiv \dfrac{1}{p^3}\left(\dfrac{\Theta_6\Theta_{26}\Theta_{21}\Theta_{14}\Theta_{19}\Theta_{24}}{\Theta_{28}\Theta_7}\,\dfrac{\Theta_{22}\Theta_3\Theta_{32}\Theta_6\Theta_{18}\Theta_{23}}{\Theta_{21}\Theta_{14}} + \dots\right), \\ \delta^2 \equiv 7\varepsilon^2 \equiv \dfrac{1}{p^3}\left(\dfrac{\Theta_6\Theta_{26}\Theta_{21}\Theta_{14}\Theta_{19}\Theta_{24}}{\Theta_{28}\Theta_7}\,\dfrac{\Theta_{27}\Theta_{11}\Theta_{12}\Theta_{12}\Theta_{23}\Theta_3}{\Theta_{21}\Theta_{14}} + \dots\right). \end{cases}$$

On tirera, au contraire, des formules (67)

(69)
$$\begin{cases} x^2 \equiv 35y^2 \equiv \dfrac{1}{p^3}[\varphi(\alpha, \varsigma^u)\varphi(\alpha^a, \varsigma) + \varphi(\alpha, \varsigma)\varphi(\alpha^a, \varsigma^u)] \\ \qquad \equiv \dfrac{1}{p^3}\left(\dfrac{\Theta_{34}\Theta_{19}\Theta_{24}\Theta_6\Theta_{26}\Theta_{31}}{\Theta_5\Theta_{10}\Theta_{20}}\,\dfrac{\Theta_{22}\Theta_5\Theta_{32}\Theta_5\Theta_{18}\Theta_{23}}{\Theta_{30}\Theta_{25}\Theta_{15}} + \dots\right), \\ \delta^2 \equiv 7\varepsilon^2 \equiv \dfrac{1}{p}[\varphi(\alpha^a, \varsigma)\varphi(\alpha^a, \varsigma^u) + \varphi(\alpha, \varsigma)\varphi(\alpha, \varsigma^u)] \\ \qquad \equiv \dfrac{1}{p}\left(\dfrac{\Theta_{34}\Theta_{19}\Theta_{24}\Theta_6\Theta_{26}\Theta_{31}}{\Theta_5\Theta_{10}\Theta_{20}}\,\dfrac{\Theta_{12}\Theta_{23}\Theta_5\Theta_{27}\Theta_{17}\Theta_{12}}{\Theta_5\Theta_{10}\Theta_{20}} + \dots\right). \end{cases}$$

Or, la première des formules (68) coïncide évidemment avec la première des formules (69), attendu qu'on a

$$p^3\Theta_{28}\Theta_7\Theta_{21}\Theta_{14} = p^3 = p^2\Theta_5\Theta_{10}\Theta_{20}\Theta_{25}\Theta_{15}.$$

Quant à la seconde des formules (68), elle fournit des valeurs de $\hat{\sigma}$, ε distinctes de celles que fournit la seconde des équations (69), et si, pour plus de commodité, on désigne ces dernières par

$$\delta', \quad \varepsilon',$$

on aura

$$\frac{\delta'^2}{\delta^2} = \frac{\varepsilon'^2}{\varepsilon^2} \equiv p^2\frac{\Theta_{28}\Theta_7\Theta_{14}\Theta_{21}}{(\Theta_5\Theta_{10}\Theta_{20})^5} \equiv \frac{p^4}{(\Theta_5\Theta_{10}\Theta_{20})^2} \equiv \frac{p^4}{p^2R_{5,10}^2} \equiv R_{20,20}^2 \equiv \Pi_{5,10}^2.$$

Ainsi les équations

(70) $$\delta^2 + 7\varepsilon^2 = 4p, \qquad \delta'^2 + 7\varepsilon'^2 = 4p^2$$

seront vérifiées simultanément de manière qu'on ait

(71) $$\frac{\delta'^2}{\delta^2} \equiv \frac{\varepsilon'^2}{\varepsilon^2} \equiv \Pi_{5,10}^2 \pmod p.$$

Exemple. — Supposons $p = 71$. On aura

$$71 = 64 + 7 = 8^2 + 7.1^2 = (8 + 7^{\frac{1}{2}}\sqrt{-1})(8 - 7^{\frac{1}{2}}\sqrt{-1}),$$

$$71^2 = (8 + 7^{\frac{1}{2}}\sqrt{-1})^2(8 - 7^{\frac{1}{2}}\sqrt{-1})^2$$

$$= (57 + 16.7^{\frac{1}{2}}\sqrt{-1})(57 - 16.7^{\frac{1}{2}}\sqrt{-1}) = 57^2 + 7.16^2,$$

$$\frac{\delta}{2} = 8, \qquad \frac{\varepsilon}{2} = 1, \qquad \frac{\delta'}{2} = 57, \qquad \frac{\varepsilon'}{2} = 16$$

et l'équation (71) donnera

$$\left(\frac{57}{8}\right)^2 \equiv 16^2 \equiv \Pi_{5,10}^2 \pmod{71}.$$

Effectivement

$$57 \equiv 8.16 \pmod{71}$$

et, de plus,

$$\Pi_{5,10} \equiv \frac{15\varpi(15\varpi-1)\dots(10\varpi+1)}{1.2\dots5\varpi} \equiv \frac{30.29.28.27.26.25.24.23.22.21}{1.2.3.4.5.6.7.8.9.10} \equiv 16.$$

Supposons enfin que ω et ν soient tous deux de la forme $4x+3$. Alors, en posant

$$A = \delta\delta, \quad B = \delta\varepsilon, \quad C = \gamma\delta, \quad D = \gamma\varepsilon,$$

on tirera des formules (10), (13)

$$(72)\quad \begin{cases} 4\varphi(\alpha,\varsigma) &= [\delta+\varepsilon(\alpha-\alpha^a+\dots-\alpha^{a^{u-2}})][\delta+\gamma(\varsigma-\varsigma^a+\dots-\varsigma^{a^{v-2}})], \\ 4\varphi(\alpha,\varsigma^a) &= [\delta+\varepsilon(\alpha-\alpha^a+\dots-\alpha^{a^{u-1}})][\delta-\gamma(\varsigma-\varsigma^a+\dots-\varsigma^{a^{v-2}})], \\ 4\varphi(\alpha^a,\varsigma) &= [\delta-\varepsilon(\alpha-\alpha^a+\dots-\alpha^{a^{u-1}})][\delta+\gamma(\varsigma-\varsigma^a+\dots-\varsigma^{a^{v-2}})], \\ 4\varphi(\alpha^a,\varsigma^a) &= [\delta-\varepsilon(\alpha-\alpha^a+\dots-\alpha^{a^{u-1}})][\delta-\gamma(\varsigma-\varsigma^a+\dots-\varsigma^{a^{v-2}})]. \end{cases}$$

De plus, comme, dans la formule (25), $\delta^2+\omega\varepsilon^2$ ne peut être impair sans que δ, γ deviennent pairs l'un et l'autre, et qu'alors on peut faire passer dans δ^2 et ε^2 le facteur 4 commun à δ^2 et γ^2, on pourra toujours partager la formule (25) en deux autres de la forme

$$(73)\qquad 4p^{k'} = \delta^2+\omega\varepsilon^2, \qquad 4p^{k'} = \varepsilon^2+\nu\gamma^2.$$

On pourra d'ailleurs supposer δ, ε non divisibles par p; et, si l'on nomme p^λ la plus haute puissance de p qui divise δ et γ, alors, en faisant

$$\delta = p^\lambda x, \qquad \gamma = p^\lambda y,$$

on trouvera

$$(74)\qquad 4p^{k'-2\lambda} = x^2+\nu y^2.$$

D'autre part, il est clair que $p^{k''}$ sera la plus haute puissance de p qui divise les deux produits

$$\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^a), \quad \varphi(\alpha^a,\varsigma)\varphi(\alpha^a,\varsigma^a),$$

et p^λ la plus haute puissance de μ, qui divise simultanément les expressions

$$\varphi(\alpha,\varsigma), \quad \varphi(\alpha,\varsigma^a), \quad \varphi(\alpha^a,\varsigma), \quad \varphi(\alpha^a,\varsigma^a),$$

et l'on tirera des équations (72)

$$(75)\quad \begin{cases} x^2-\nu y^2 = 2\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha^a,\varsigma)+\varphi(\alpha,\varsigma^a)\varphi(\alpha^a,\varsigma^a)}{p^{k'+2\lambda}}, \\ \delta^2-\omega\varepsilon^2 = 2\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha,\varsigma^a)+\varphi(\alpha^a,\varsigma)\varphi(\alpha^a,\varsigma^a)}{p^{k'}}. \end{cases}$$

Exemple. — Prenons

$$\omega = 3, \qquad \nu = 7.$$

On trouvera

$$a = 2, \qquad u = 3,$$

$$v \equiv \frac{1}{\nu} \equiv 1 \pmod{\omega},$$

$$u^m+\nu v(h-u^m) = u^m+7(h-u^m) = 7h-6u^m,$$

$$\vartheta^2(\alpha^h,\varsigma) = \frac{\Theta_{7h-6}\Theta_{7h-12}\Theta_{7h+18}}{\Theta_{21h}},$$

$$\vartheta^2(\alpha^h,\varsigma^a) = \frac{\Theta_{7h+6}\Theta_{7h+12}\Theta_{7h-18}}{\Theta_{21h}},$$

$$\varphi(\alpha,\varsigma) = \frac{\Theta_1\Theta_{16}\Theta_4}{\Theta_{21}} = pR_{1,4} = pR_{4,16} = pR_{1,16},$$

$$\varphi(\alpha,\varsigma^a) = \frac{\Theta_{13}\Theta_{19}\Theta_{10}}{\Theta_{21}} = pR_{10,13} = pR_{13,19} = pR_{10,19},$$

$$\varphi(\alpha^2,\varsigma) = \frac{\Theta_8\Theta_2\Theta_{11}}{\Theta_{22}} = pR_{2,8} = pR_{8,11} = pR_{2,11},$$

$$\varphi(\alpha^2,\varsigma^a) = \frac{\Theta_{20}\Theta_5\Theta_{17}}{\Theta_{22}} = pR_{20,5} = pR_{5,17} = pR_{20,17}.$$

Ainsi l'on aura

$$\varphi(\alpha,\varsigma) = \frac{p^2}{R_{20,17}}, \qquad \varphi(\alpha,\varsigma^a) = pR_{13,19},$$

$$\varphi(\alpha^2,\varsigma) = \frac{p^2}{R_{13,19}}, \qquad \varphi(\alpha^2,\varsigma^a) = pR_{20,17};$$

$$k=3, \qquad k'=3, \qquad k''=0, \qquad \lambda=1$$

et, par suite,

$$4 = \delta^2 + 3\varepsilon^2, \qquad 4p = x^2 + 7y^2, \tag{76}$$

$$\begin{cases} x^2 \equiv -7y^2 \equiv \mathrm{R}_{13,19}\mathrm{R}_{20,17} \equiv \Pi_{2,8}\Pi_{1,4}, \\ \dfrac{1}{2}(\delta^2 - 3\varepsilon^2) \equiv \dfrac{\mathrm{R}_{13,19}}{\mathrm{R}_{20,17}} + \dfrac{\mathrm{R}_{20,17}}{\mathrm{R}_{13,19}} \equiv \dfrac{\Pi_{2,8}}{\Pi_{1,4}} + \dfrac{\Pi_{1,4}}{\Pi_{2,8}}. \end{cases} \tag{77}$$

Supposons, pour fixer les idées, $p = 43$. On aura

$$\varpi = 2,$$

$$\Pi_{1,4} = \frac{5\varpi \ldots (4\varpi + 1)}{1.2 \ldots \varpi} = \frac{10.9}{1.2} = 45 \equiv 2,$$

$$\Pi_{2,8} = \frac{10\varpi \ldots (8\varpi + 1)}{1.2 \ldots 2\varpi} = \frac{20.19.18.17}{1.2.3.4} = 3.17.19.5 \equiv -14,$$

$$\frac{x^2}{4} \equiv -7\frac{y^2}{4} \equiv -\frac{28}{4} \equiv -7 \equiv 36,$$

$$\frac{1}{2}(\delta^2 - 3\varepsilon^2) \equiv -7 - \frac{1}{7} \equiv -1,$$

$$\delta^2 - 3\varepsilon^2 \equiv -2, \qquad \delta^2 + 3\varepsilon^2 = 4$$

et, par suite,

$$\delta^2 = 1, \qquad \varepsilon^2 = 1, \qquad \frac{1}{4}x^2 = 36, \qquad \frac{1}{2}y^2 = 1.$$

Effectivement

$$43 = 36 + 7 = 6^2 + 7.1^2.$$

Il est bon d'observer qu'on aura encore, en vertu des principes établis dans le paragraphe I,

$$x^2 \equiv \Pi_{3,6}^2. \tag{78}$$

Donc

$$\Pi_{3,6}^2 \equiv \Pi_{1,4}\Pi_{2,8}. \tag{79}$$

Effectivement, si l'on prend $p = 43$, on trouvera

$$\Pi_{3,6} = \frac{18.17.16.15.14.13}{1.2.3.4\ 5.6} = 6.13.14.17 \equiv -12,$$

$$\Pi_{3,6}^2 \equiv 144 \equiv 15 \equiv -28 \equiv \Pi_{1,4}\Pi_{2,8}.$$

On aura d'ailleurs, en vertu de la première des formules (75),

$$x^2 - 7y^2 = \frac{p^2}{2}\left(\frac{\Theta_1\Theta_2\Theta_{16}}{\Theta_{21}}\frac{\Theta_2\Theta_8\Theta_{11}}{\Theta_{21}} + \frac{\Theta_2\Theta_{20}\Theta_{17}}{\Theta_{21}}\frac{\Theta_{16}\Theta_{19}\Theta_{13}}{\Theta_{21}}\right),$$

$$x^2 - 7y^2 = \frac{p^2}{2}\left(\Theta_1\Theta_2\Theta_{16} \times \Theta_2\Theta_8\Theta_{11} + \frac{p^2}{\Theta_1\Theta_2\Theta_{16} \times \Theta_2\Theta_8\Theta_{11}}\right),$$

tandis que les principes ci-dessus rappelés donneront

$$x^2 - 7y^2 = \frac{2}{p^2}\left(\Theta_1^2\Theta_2^2\Theta_4^2 + \frac{p^2}{\Theta_1^2\Theta_2^2\Theta_4^2}\right).$$

En général, on vérifie l'équivalence

$$v \equiv \frac{1}{\nu} \pmod{\omega},$$

lorsque ω est premier, en prenant

$$\nu = \nu^{\omega-2}.$$

Donc la formule (1) peut être réduite à

$$\mathfrak{F}(\alpha^h, \varsigma) = \frac{\Theta_{1+\nu^{\omega-1}(h-1)}\Theta_{n^2+\nu^{\omega-1}(h-n^2)} \ldots \Theta_{n^{\omega-2}+\nu^{\omega-1}(h-n^{\omega-1})}}{\Theta_{\nu^{\omega-1}\frac{\nu-1}{2}h}}, \tag{80}$$

et la formule (2) à

$$\mathfrak{F}(\alpha^h, \varsigma^n) = \frac{\Theta_{n+\nu^{\omega-1}(h-n)}\Theta_{n^2+\nu^{\omega-1}(h-n^2)} \ldots \Theta_{n^{\omega-2}+\nu^{\omega-1}(h-n^{\omega-2})}}{\Theta_{\nu^{\omega-1}\frac{\nu-1}{2}h}}. \tag{81}$$

Par suite, les divers facteurs que renfermera le numérateur de la fraction équivalente à $\varphi(\alpha, \varsigma)$ seront de la forme

$$\Theta_{n^{\lambda m}+\nu^{\omega-1}(\alpha^{\lambda m'}-n^{\lambda m})}.$$

De même, les numérateurs des fractions équivalentes à $\varphi(\alpha, \varsigma^n)$, $\varphi(\alpha^a, \varsigma)$, $\varphi(\alpha^a, \varsigma^n)$ auront pour facteurs des expressions de la forme

$$\Theta_{n^{\lambda m+1}+\nu^{\omega-1}(\alpha^{\lambda m'}-n^{\lambda m+1})},$$

$$\Theta_{n^{\lambda m}+\nu^{\omega-1}(\alpha^{\lambda m'+1}-n^{\lambda m})},$$

$$\Theta_{n^{\lambda m+1}+\nu^{\omega-1}(\alpha^{\lambda m'+1}-n^{\lambda m'+1})}.$$

Cela posé, il sera facile de déterminer les nombres ci-dessus désignés par

$$k, \quad k', \quad k'', \quad \lambda$$

si l'on parvient à trouver combien il y a de nombres entiers de chacune des formes

$$u^{2m} + \nu^{\omega-1}(a^{2m'} - u^{2m}), \quad u^{2m+1} + \nu^{\omega-1}(a^{2m'} - u^{2m+1}),$$
$$u^{2m} + \nu^{\omega-1}(a^{2m'+1} - u^{2m}), \quad u^{2m+1} + \nu^{\omega-1}(a^{2m'+1} - u^{2m+1})$$

entre les limites o, $\frac{n}{2}$.

§ IV. — *Suite du même sujet.*

Supposons, comme dans le paragraphe II,

$$n = \omega\nu \qquad (\nu \text{ étant un nombre premier}),$$
$$p - 1 = n\varpi = \nu\psi, \qquad \psi = \omega\varpi,$$

et soient

$$\varphi, \quad \alpha, \quad \varsigma$$

des racines primitives des équations

$$x^n = 1, \qquad x^{\omega} = 1, \qquad x^{\nu} = 1.$$

Soient encore θ, τ des racines primitives de

$$x^p = 1, \qquad x^{p-1} = 1$$

et t, s, u des racines primitives des équivalences

$$x^{p-1} \equiv 1 \pmod{p}, \qquad x^{\nu} \equiv 1 \pmod{p}, \qquad x^{\nu-1} \equiv 1 \pmod{\nu}.$$

Soit enfin

$$\nu \equiv \frac{1}{\nu} \pmod{\omega}.$$

On aura

$$\vartheta(\alpha^h, \varsigma) = \vartheta(\alpha^h, \varsigma^{u^1}) = \vartheta(\alpha^h, \varsigma^{u^2}) = \ldots = \vartheta(\alpha^h, \varsigma^{u^{\nu-1}})$$
$$= \frac{\Theta_{1+\nu\psi(h-1)}\,\Theta_{u^1+\nu\psi(h-u^1)}\,\Theta_{u^2+\nu\psi(h-u^2)}\ldots\Theta_{u^{\nu-1}+\nu\psi(h-u^{\nu-1})}}{\Theta_{\nu\frac{\psi(\nu-1)}{2}h}},$$

$$\vartheta(\alpha^h, \varsigma^u) = \vartheta(\alpha^h, \varsigma^{u^1}) = \vartheta(\alpha^h, \varsigma^{u^2}) = \ldots = \vartheta(\alpha^h, \varsigma^{u^{\nu-1}})$$
$$= \frac{\Theta_{u+\nu\psi(h-u)}\,\Theta_{u^1+\nu\psi(h-u^1)}\,\Theta_{u^2+\nu\psi(h-u^2)}\ldots\Theta_{u^{\nu-1}+\nu\psi(h-u^{\nu-1})}}{\Theta_{\nu\frac{\psi(\nu-1)}{2}h}}.$$

Si ω est un nombre premier, on pourra prendre

$$\varphi = \nu^{\omega-2}.$$

Soit d'ailleurs a une racine de l'équivalence

$$x^{\omega-1} \equiv 1 \pmod{\omega}$$

et faisons

$$\varphi(\alpha, \varsigma) = \vartheta(\alpha; \varsigma)\,\vartheta(\alpha^a, \varsigma)\,\vartheta(\alpha^{a^2}, \varsigma)\ldots\vartheta(\alpha^{a^{\omega-2}}, \varsigma),$$
$$\chi(\alpha, \varsigma) = \varphi(\alpha, \varsigma)\,\varphi(\alpha^a, \varsigma^a).$$

On aura

$$\chi(\alpha, \varsigma) = \varphi(\alpha, \varsigma)\ \varphi(\alpha^a, \varsigma^a) = \chi(\alpha^a, \varsigma^a),$$
$$\chi(\alpha^a, \varsigma) = \varphi(\alpha^a, \varsigma)\,\varphi(\alpha, \varsigma^a) = \chi(\alpha, \varsigma^a).$$

Observons maintenant : 1° que a et u vérifient les formules

$$a^{\frac{\omega-1}{2}} \equiv -1 \pmod{\omega}, \qquad u^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}$$

et que $\frac{\omega-1}{2}$, $\frac{\nu-1}{2}$ seront pairs ou impairs, suivant que ω, ν seront de la forme $4x+1$ ou $4x+3$; 2° que, dans une expression de la forme

$$\Theta_{u^m+\nu^{\omega-1}(a^{m'}-u^m)} = \Theta_{(1-\nu^{\omega-1})u^m+\nu^{\omega-1}a^{m'}},$$

on peut remplacer u^m par un nombre équivalent à u^m, suivant le module ν, et $a^{m'}$ par un nombre équivalent à $a^{m'}$ suivant le module ω. On en conclura sans peine : 1° que chacune des expressions

$$\vartheta(\alpha, \varsigma), \quad \vartheta(\alpha^a, \varsigma), \quad \ldots, \quad \vartheta(\alpha, \varsigma^u), \quad \ldots,$$
$$\varphi(\alpha, \varsigma), \quad \varphi(\alpha^a, \varsigma), \quad \varphi(\alpha, \varsigma^u), \quad \varphi(\alpha^a, \varsigma^u)$$

se réduit à une puissance de p lorsque ν et ω sont tous deux de la forme $4x+1$; 2° que les expressions

$$\varphi(\alpha,\zeta)\ \varphi(\alpha^a,\zeta^u)=\chi(\alpha,\zeta)\ =\chi(\alpha^a,\zeta^u),$$
$$\varphi(\alpha^a,\zeta)\,\varphi(\alpha,\zeta^u)\ =\chi(\alpha^a,\zeta)=\chi(\alpha,\zeta^u)$$

se réduisent à des puissances de p lorsque ν et ω sont tous deux de la forme $4x+3$. Mais si des deux nombres ω, ν l'un est de la forme $4x+3$, l'autre de la forme $4x+1$, le produit

$$\chi(\alpha,\zeta)\,\chi(\alpha^a,\zeta)$$

qui se réduira à une puissance entière de p. Alors, si l'on fait, pour abréger,

$$\zeta-\zeta^u+\zeta^{u^2}-\ldots+\zeta^{u^{\omega-1}}-\zeta^{u^{\omega-1}}=\Delta,$$
$$\alpha-\alpha^a+\alpha^{a^2}-\ldots+\alpha^{a^{\omega-1}}-\alpha^{a^{\omega-1}}=\Delta',$$

on aura

$$\zeta+\zeta^{u^2}+\ldots+\zeta^{u^{\omega-1}}=\frac{\Delta-1}{2},\qquad \zeta^u+\zeta^{u^3}+\ldots+\zeta^{u^{\omega-2}}=-\frac{\Delta+1}{2},$$
$$\alpha+\alpha^{a^2}+\ldots+\alpha^{a^{\omega-1}}=\frac{\Delta'-1}{2},\qquad \alpha^a+\alpha^{a^3}+\ldots+\alpha^{a^{\omega-2}}=-\frac{\Delta'+1}{2},$$

et $\chi(\alpha,\zeta)$ sera une fonction entière et linéaire des polynomes

$$\zeta+\zeta^{u^2}+\ldots+\zeta^{u^{\omega-1}},\quad \zeta^u+\zeta^{u^3}+\ldots+\zeta^{u^{\omega-2}},$$
$$\alpha+\alpha^{a^2}+\ldots+\alpha^{a^{\omega-1}},\quad \alpha^a+\alpha^{a^3}+\ldots+\alpha^{a^{\omega-2}}$$

qui restera invariable, tandis que l'on remplacera simultanément ζ par ζ^u et α par α^a (¹). Donc $2\chi(\alpha,\zeta)$ sera une fonction entière et

(¹) Il faudra que l'on ait

$$\begin{aligned}\chi(\alpha,\zeta)=f+g[&(\alpha+\alpha^{a^2}+\ldots+\alpha^{a^{\omega-1}})(\zeta+\zeta^{u^2}+\ldots+\zeta^{u^{\omega-1}})\\&+(\alpha^a+\alpha^{a^3}+\ldots+\alpha^{a^{\omega-2}})(\zeta^u+\zeta^{u^3}+\ldots+\zeta^{u^{\omega-2}})]\\+h[&(\alpha+\alpha^{a^2}+\ldots+\alpha^{a^{\omega-1}})(\zeta^u+\zeta^{u^3}+\ldots+\zeta^{u^{\omega-2}})\\&+(\alpha^a+\alpha^{a^3}+\ldots+\alpha^{a^{\omega-2}})(\zeta+\zeta^{u^2}+\ldots+\zeta^{u^{\omega-1}})]\\=f+\frac{g}{2}(\Delta\Delta'+1)+&\frac{h}{2}(1-\Delta\Delta'),\end{aligned}$$

f, g, h étant entiers.

$$2\chi(\alpha,\zeta)=2f+g+h+(g-h)\Delta\Delta'$$

ou

$$(\alpha,\zeta)=A+B\Delta\Delta',$$

A, B étant de même espèce.

linéaire de Δ et Δ', qui ne changera pas quand on remplacera simultanément Δ par $-\Delta$, Δ' par $-\Delta'$. On aura donc

$$2\chi(\alpha,\zeta)=A+B\Delta\Delta'; \tag{1}$$

A, B désignent deux quantités entières. On trouvera, au contraire,

$$2\chi(\alpha^a,\zeta)=A-B\Delta\Delta' \tag{2}$$

et, par suite,

$$4\chi(\alpha,\zeta)\chi(\alpha^a,\zeta)=A^2-B^2\Delta^2\Delta'^2=A^2+\nu\omega B^2$$

ou, ce qui revient au même,

$$4p^{2k}=A^2+\nu\omega B^2\ (^1), \tag{3}$$

A, B étant deux nombres de même espèce, c'est-à-dire tous deux pairs ou tous deux impairs.

Exemple. — Soient

$$\omega=3,\qquad \nu=5.$$

On trouvera

$$k=2,$$
$$4p^2=A^2+15B^2.$$

Cette dernière équation ne peut subsister, quand A et B sont impairs, puisque alors A^2+15B^2 est divisible par 8. Donc

$$A=2X,\qquad B=2Y,$$
$$p^2=X^2+15Y^2. \tag{4}$$

D'ailleurs p^2, divisé par 8, donne 1 pour reste. Donc X doit être impair et y impair. Donc

$$Y^2=4x^2y^2,$$
$$p^2-X^2=60x^2y^2. \tag{5}$$

Enfin $p-X$, $p+X$ devant être pairs et $\frac{p-X}{2}$, $\frac{p+X}{2}$ devant être

(¹) $\chi(\alpha,\zeta)$ et $\chi(\alpha^a,\zeta)$ sont des produits de plusieurs facteurs de la forme $R_{h,k'}$ dont le nombre est nécessairement pair ou de la forme $2k$.

premiers entre eux, puisque leur somme p est un nombre premier, l'équation (5) ou

$$\frac{p-X}{2}\,\frac{p+X}{2}=15x^2y^2$$

se décomposera en deux autres de la forme

$$\frac{p+X}{2}=x^2,\qquad \frac{p-X}{2}=15y^2$$

ou

$$\frac{p+X}{2}=3x^2,\qquad \frac{p-X}{2}=5y^2.$$

Mais, dans le dernier cas, on trouverait

$$p=3x^2+5y^2,\qquad 3x^2\equiv 1 \pmod 5,$$

$$x^2\equiv\frac{1}{3}\equiv 2 \pmod 5,$$

ce qui est impossible. Donc, le premier cas est seul admissible et l'on aura

$$p=x^2+15y^2,\qquad X=x^2-15y^2. \tag{6}$$

En général, l'équation (3) peut s'écrire comme il suit :

$$(2p^k-A)(2p^k+A)=\nu\omega B^2. \tag{7}$$

Soit p^λ la plus haute puissance de p qui divise simultanément A et B; on pourra faire

$$A=p^\lambda X,\qquad B=p^\lambda Y,\qquad 2k-2\lambda=2\mu \tag{8}$$

et l'équation (7) deviendra

$$4p^{2k-2\lambda}=4p^{2\mu}=X^2+\nu\omega Y^2$$

ou

$$(2p^\mu+X)(2p^\mu-X)=\omega\nu Y^2. \tag{9}$$

Alors X et Y seront premiers à p et, comme tout diviseur commun des facteurs

$$2p^\mu+X,\qquad 2p^\mu-X \tag{10}$$

divisera nécessairement leur somme $4p^\mu$, ces facteurs ne pourront avoir d'autre commun diviseur que 2 ou 4. Cela posé, si les facteurs (10) sont premiers entre eux, on vérifiera la formule (9) en prenant

$$2p^\mu+X=\nu x^2,\qquad 2p^\mu-X=\omega y^2 \tag{11}$$

et, par suite,

$$4p^\mu=\nu x^2+\omega y^2, \tag{12}$$

ou bien en prenant

$$2p^\mu+X=x^2,\qquad 2p^\mu-X=\nu\omega y^2 \tag{13}$$

et, par suite,

$$4p^\mu=x^2+\nu\omega y^2. \tag{14}$$

Si les facteurs (10) sont pairs l'un et l'autre, X sera pair ainsi que Y et, en posant

$$X=2X',\qquad Y=2Y',$$

on tirera de la formule (9)

$$(p^\mu+X')(p^\mu-X')=\omega\nu Y'^2 \tag{15}$$

ou

$$p^{2\mu}=X'^2+\nu\omega Y'^2.$$

Dans cette dernière formule, le premier membre, divisé par 4, donne 1 pour reste. Il doit en être de même du second membre, ce qui exige que X′ soit impair et Y′ pair, puisque $\nu\omega$, divisé par 4, donne 3 pour reste. Donc, on ne peut vérifier l'équation (15) qu'en supposant

$$p^\mu+X'=\nu x^2,\qquad p^\mu-X'=\omega y^2$$

et, par suite,

$$2p^\mu=\nu x^2+\omega y^2,$$

ce qui est inadmissible, puisque $2p^\mu$, divisé par 4, donne 2 pour reste, tandis que $\nu x^2+\omega y^2$ ne peut être pair sans être divisible par 4; ou

bien en supposant

$$p^{\mu}+X'=x^2, \qquad p^{\mu}-X'=\omega\nu y^2,$$
$$2p^{\mu}=x^2+\omega\nu y^2,$$

ce qui est encore inadmissible pour la même raison, attendu que $x^2+\omega\nu y^2$, en devenant pair, sera toujours divisible par 4; ou en adoptant l'une des hypothèses suivantes :

$$p^{\mu}+X'=2\nu x^2, \qquad p^{\mu}-X'=2\omega y^2,$$
$$p^{\mu}=\nu x^2+\omega y^2; \tag{16}$$

$$p^{\mu}+X'=2x^2, \qquad p^{\mu}-X'=2\omega\nu y^2,$$
$$p^{\mu}=x^2+\omega\nu y^2. \tag{17}$$

Donc, en définitive, on pourra toujours satisfaire par des valeurs entières de x, y à l'une des équations (12), (14), (16), (17).

Comme p est de la forme $\nu\omega x+1$, les équations (12), (16) ne peuvent subsister qu'autant que l'on a

$$\nu x^2\equiv 1 \text{ ou } 4 \pmod{\omega},$$
$$\omega x^2\equiv 1 \text{ ou } 4 \pmod{\nu}$$

et, par suite,

$$\nu^{\frac{\omega-1}{2}}\equiv 1 \pmod{\omega} \qquad \omega^{\frac{\nu-1}{2}}\equiv 1 \pmod{\nu}$$

ou, ce qui revient au même,

$$\left[\frac{\nu}{\omega}\right]=1, \qquad \left[\frac{\omega}{\nu}\right]=1.$$

On a d'ailleurs, dans tous les cas,

$$\left[\frac{\nu}{\omega}\right]=\left[\frac{\omega}{\nu}\right].$$

Si

$$\left[\frac{\nu}{\omega}\right]=\left[\frac{\omega}{\nu}\right]=-1,$$

on ne peut admettre que la formule (14) ou (17). Si, de plus, $1+\nu\omega$ est divisible par 8, on ne peut admettre que la formule (17).

Observons encore que l'on tire des équations (1), (2) et (8)

$$A=p^{\lambda}X=\chi(\alpha,\varsigma)+\chi(\alpha^{\alpha},\varsigma).$$

Donc

$$X=\frac{\chi(\alpha,\varsigma)+\chi(\alpha^{\alpha},\varsigma)}{p^{\lambda}}=\frac{\varphi(\alpha,\varsigma)\varphi(\alpha^{\alpha},\varsigma)+\varphi(\alpha,\varsigma^{\alpha})\varphi(\alpha^{\alpha},\varsigma^{\alpha})}{p^{\lambda}}.$$

D'ailleurs, on tire des formules (11)

$$2X=\nu x^2-\omega y^2$$

et des formules (13)

$$2X=x^2-\nu\omega y^2.$$

Donc

$$\nu x^2-\omega y^2 \quad \text{ou} \quad x^2-\nu\omega y^2=2\frac{\varphi(\alpha,\varsigma)\varphi(\alpha^{\alpha},\varsigma)+\varphi(\alpha,\varsigma^{\alpha})\varphi(\alpha^{\alpha},\varsigma^{\alpha})}{p^{\lambda}}.$$

A l'aide de cette dernière équation et de la formule

$$4p^{\mu}=\nu x^2+\omega y^2 \quad \text{ou} \quad x^2+\nu\omega y^2,$$

on pourra déterminer x et y. On aura, en effet,

$$\begin{cases} \nu x^2\equiv -\ \omega y^2=\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha^{\alpha},\varsigma)+\varphi(\alpha,\varsigma^{\alpha})\varphi(\alpha^{\alpha},\varsigma^{\alpha})}{p^{\lambda}} \\ \text{ou} \\ x^2\equiv -\nu\omega y^2=\dfrac{\varphi(\alpha,\varsigma)\varphi(\alpha^{\alpha},\varsigma)+\varphi(\alpha,\varsigma^{\alpha})\varphi(\alpha^{\alpha},\varsigma^{\alpha})}{p^{\lambda}} \end{cases} \pmod{p^{\mu}}. \tag{18}$$

Ces dernières formules offriront le moyen de déterminer x et y lorsqu'on aura $\mu=1$. Alors, en effet, il suffira de remplacer dans ces formules α et ς par les racines primitives des équivalences

$$x^{\omega}\equiv 1 \pmod{p}, \qquad x^{\nu}\equiv 1 \pmod{p}.$$

En vertu de cette substitution, l'expression

$$R_{h,k}=\frac{\Theta_h\Theta_k}{\Theta_{h+k}}=\left[\frac{1+1}{p}\right]^{-h-k}+\rho^h\left[\frac{1+t}{p}\right]^{-h-k}+\ldots+\rho^{(p-2)h}\left[\frac{1+t^{p-2}}{p}\right]^{-h-k}$$
$$=\left[\frac{1+1}{p}\right]^{t}+\rho^h\left[\frac{1+t}{p}\right]^{t}+\ldots+\rho^{(p-2)h}\left[\frac{1+t^{p-2}}{p}\right]^{t},$$

dans laquelle on suppose

$$k+h+l\equiv 0 \pmod{n},$$

deviendra

$$\begin{aligned}&(1+1)^{l\varpi}+r^{h}(1+t)^{l\varpi}+\ldots+r^{(p-2)h}(1+t^{p-2})^{l\varpi}\\&=(1+1)^{l\varpi}+t^{h\varpi}(1+t)^{l\varpi}+\ldots+t^{(p-2)h\varpi}(1+t^{p-2})^{l\varpi}\\&\equiv(p-1)\Pi_{n-h,n-k} \pmod{p},\end{aligned}$$

la valeur de $\Pi_{h,k}$ étant

$$\Pi_{h,k}=\frac{1.2.3.\ldots.(h+k)\varpi}{(1.2.\ldots.h\varpi)(1.2.\ldots.k\varpi)}.$$

Soit maintenant

$$R_{h,k}=a_0+a_1\rho+a_2\rho^2+\ldots+a_{n-1}\rho^{n-1}. \tag{19}$$

On aura identiquement

$$\begin{aligned}&a_0+a_1\rho+a_2\rho^2+\ldots+a_{n-1}\rho^{n-1}\\&=\left[\frac{1+1}{p}\right]^{l}+\rho^{h}\left[\frac{1+t}{p}\right]^{l}+\ldots+\rho^{(p-2)h}\left[\frac{1+t^{p-2}}{p}\right]^{l}\end{aligned}$$

ou

$$\begin{aligned}&a_0+a_1\tau^{\varpi}+a_2\tau^{2\varpi}+\ldots+a_{n-1}\tau^{(n-1)\varpi}\\&=\tau^{l\varpi(2)}+\tau^{h\varpi}\tau^{l\varpi(1+t)}+\ldots+t^{(p-2)h\varpi}\tau^{l\varpi(1+t^{p-2})}.\end{aligned}$$

Si, dans cette dernière formule, on remplace τ par t, on aura

$$\begin{cases}a_0+a_1t^{\varpi}+a_2t^{2\varpi}+\ldots+a_{n-1}\tau^{(n-1)\varpi}\\\quad\equiv(1+1)^{l\varpi}+t^{h\varpi}(1+t)^{l\varpi}+\ldots+t^{(p-2)h\varpi}(1+t^{p-2})^{l\varpi}\end{cases} \pmod{p}. \tag{20}$$

Soit maintenant T une racine primitive de l'équivalence

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

Je dis qu'on aura

$$\begin{cases}a_0+a_1T^{\varpi p^{\mu-1}}+a_2T^{2\varpi p^{\mu-1}}+\ldots+a_{n-1}t^{(n-1)\varpi p^{\mu-1}}\\\quad\equiv(1+1)^{l\varpi p^{\mu-1}}+T^{h\varpi p^{\mu-1}}(1+T)^{l\varpi p^{\mu-1}}+\ldots+T^{(p-2)h\varpi p^{\mu-1}}(1+T^{p-2})^{l\varpi p^{\mu-1}}\end{cases} \pmod{p^{\mu}}. \tag{21}$$

En effet, t étant une racine primitive de l'équivalence

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

on pourra supposer

$$T\equiv t \pmod{p}$$

ou

$$T=t+py,$$

et l'on en conclura

$$T^{p^{\mu-1}}=(t+py)^{p^{\mu-1}}=t^{p^{\mu-1}}+p^{\mu}Y$$

ou

$$T^{p^{\mu-1}}\equiv t^{p^{\mu-1}} \pmod{p^{\mu}}\ (^1).$$

De même, si l'on a

$$(1+t^{l})^{l}\equiv t^{l} \pmod{p}$$

on en conclura

$$(1+T^{l})^{l}\equiv(1+t^{l})^{l}\equiv t^{l}=T^{l} \pmod{p}$$

ou

$$(1+T^{l})^{l}=T^{l}+pz,$$

et, par suite,

$$(1+T^{l})^{lp^{\mu-1}}=(T^{l}+pz)^{p^{\mu-1}}=T^{lp^{\mu-1}}+p^{\mu}Z$$

ou

$$(1+T^{l})^{lp^{\mu-1}}=T^{lp^{\mu-1}} \pmod{p^{\mu}}\ (^2).$$

(1) En effet, une équivalence de la forme

$$x\equiv y \pmod{p^{l}},$$

pouvant s'écrire comme il suit,

$$x\equiv y+p^{l}z,$$

entraîne la formule

$$x^{p}=y^{p}+p^{l+1}z+\ldots$$

ou

$$x^{p}\equiv y^{p} \pmod{p^{l+1}}.$$

Donc l'équivalence

$$T\equiv t \pmod{p}$$

entraînera les suivantes :

$$T^{p}\equiv t^{p} \pmod{p^{2}},\quad T^{p^{2}}\equiv t^{p^{2}} \pmod{p^{3}},\quad \ldots \text{ et } T^{p^{\mu-1}}\equiv t^{p^{\mu-1}} \pmod{p^{\mu}}.$$

(2) De ce que l'équivalence

$$(1+t^{l})^{l}\equiv t^{l} \pmod{p}$$

entraîne les suivantes,

$$(1+t^{l})^{lp^{\mu-1}}\equiv t^{lp^{\mu-1}} \pmod{p^{\mu}} \text{ et } (1+T^{l})^{lp^{\mu-1}}\equiv T^{lp^{\mu-1}} \pmod{p^{\mu}},$$

résulte immédiatement que l'équivalence

$$t^{lh\varpi}(1+t^{l})^{l\varpi}=t^{k\varpi} \pmod{p}$$

Au reste, l'équation (20) entraîne encore la suivante :

$$(22)\quad \begin{cases} a_0 + a_1 t^{\varpi p^{k-1}} + \ldots + a_{n-1} t^{(n-1)\varpi p^{k-1}} \\ \equiv (1+1)^{l\varpi p^{k-1}} + t^{h\varpi p^{k-1}}(1+t)^{l\varpi p^{k-1}} + \ldots + t^{(p-2)h\varpi p^{k-1}}(1+t^{p-2})^{l\varpi p^{k-1}} \end{cases} \pmod{p^k}.$$

Il est bon d'observer que, pour obtenir le premier membre de la formule (21), il suffit de remplacer, dans $R_{h,k}$,

$$\rho \quad \text{par} \quad T^{\varpi p^{k-1}},$$

qui est, ainsi que T^{ϖ}, une racine primitive de l'équivalence

$$x^n \equiv 1 \pmod{p^k}.$$

D'autre part, comme on aura

$$T^{p-1} \equiv 1 \pmod{p^k}$$

et, par suite,

$$T^{p^k} \equiv T^{p^{k-1}} \equiv \ldots \equiv T^p \equiv T \pmod{p^k},$$

la formule (21) pourra être réduite à

$$(23)\quad \begin{cases} a_0 + a_1 T^{\varpi p^{k-1}} + \ldots + a_{n-1} T^{(n-1)\varpi p^{k-1}} \\ \equiv (1+1)^{l\varpi p^{k-1}} + T^{h\varpi}(1+T)^{l\varpi p^{k-1}} + \ldots + T^{(p-2)h\varpi}(1+T^{p-2})^{l\varpi p^{k-1}} \end{cases} \pmod{p^k}.$$

Il est facile de trouver un nombre équivalent suivant le module p^k au second membre de la formule (23). En effet, on a

$$(1+T^i)^{l\varpi p^{k-1}} = 1 + \frac{l\varpi p^{k-1}}{1} T^i + \frac{l\varpi p^{k-1}(l\varpi p^{k-1}-1)}{1.2} T^{2i} + \ldots$$

et, par suite,

$$\Sigma(1+T^i)^{l\varpi p^{k-1}} = p - 1 + \frac{l\varpi p^{k-1}}{1} \Sigma T^i + \frac{l\varpi p^{k-1}(l\varpi p^{k-1}-1)}{1.2} \Sigma T^{2i} + \ldots,$$

$$\Sigma T^{ih\varpi}(1+T^i)^{l\varpi p^{k-1}} = \Sigma T^{ih\varpi} + \frac{l\varpi p^{k-1}}{1} \Sigma T^{i(h\varpi+1)} + \ldots,$$

entraîne les suivantes :

$$t^{ih\varpi p^{k-1}}(1+t^i)^{l\varpi p^{k-1}} \equiv t^{k\varpi p^{k-1}} \pmod{p^k},$$

$$T^{ih\varpi p^{k-1}}(1+T^i)^{l\varpi p^{k-1}} \equiv T^{k\varpi p^{k-1}} \pmod{p^k}.$$

Or, en vertu de ces dernières formules, l'équivalence (20) entraîne à son tour les équivalences (22) et (21).

le signe Σ s'étendant à toutes les valeurs de i, renfermées entre les limites 0, $p-2$. D'ailleurs, on aura

$$\Sigma T^{ik} \equiv 0 \pmod{p^k}$$

lorsque k ne sera pas divisible par $p-1 = n\varpi$, et

$$\Sigma T^{ik} = p - 1 \equiv n\varpi \pmod{p^k}$$

dans le cas contraire. Donc

$$(24)\quad \Sigma T^{ih\varpi}(1+T^i)^{l\varpi p^{k-1}} \equiv (p-1)(\Pi_{n-h,lp^{k-1}+h-n} + \Pi_{2n-h,lp^{k-1}+h-2n} + \ldots),$$

la valeur de $\Pi_{h,k}$ étant

$$(25)\quad \Pi_{h,k} = \frac{1.2.3.\ldots.(h+k)\varpi}{(1.2.\ldots.h\varpi)(1.2.\ldots.k\varpi)}.$$

Cela posé, on aura

$$\Pi_{n-h,lp^{k-1}+h-n} \equiv \frac{1.2.3.\ldots.(lp^{k-1}\varpi)}{[1.2.\ldots.(n-h)\varpi][1.2.\ldots.(lp^{k-1}+h-n)\varpi]}$$

$$\equiv \frac{(lp^{k-1}\varpi)(lp^{k-1}\varpi-1)\ldots[(lp^{k-1}+h-n)\varpi+1]}{1.2.3.\ldots.(n-h)\varpi} \pmod{p^k},$$

$$\equiv -\frac{lp^{k-1}}{n-h}$$

$$\Pi_{2n-h,lp^{k-1}+h-2n} \equiv \frac{(lp^{k-1}\varpi)(lp^{k-1}\varpi-1)\ldots[(lp^{k-1}+h-2n)\varpi+1]}{1.2.3.\ldots.(2n-h)\varpi}$$

$$\equiv \frac{(lp^{k-1}\varpi)(lp^{k-1}\varpi-p)}{(2n-h)\varpi p} \pmod{p^k},$$

$$\equiv \frac{(lp^{k-2}\varpi)(lp^{k-2}\varpi-1)}{1.(2n-h)\varpi} p$$

$$\Pi_{3n-h,lp^{k-1}+h-3n} \equiv \frac{(lp^{k-1}\varpi)(lp^{k-1}\varpi-1)\ldots[(lp^{k-1}+h-3n)\varpi+1]}{1.2.3.\ldots.(3n-h)\varpi}$$

$$\equiv -\frac{(lp^{k-1}\varpi)(lp^{k-1}\varpi-p)(lp^{k-1}\varpi-2p)}{p.2p.(3n-h)\varpi} \pmod{p^k},$$

$$\equiv -\frac{(lp^{k-2}\varpi)(lp^{k-2}\varpi-1)(lp^{k-2}\varpi-2)}{1.2.(3n-h)\varpi} p$$

. . . . . .

Généralement, on aura

$$(26)\quad \begin{cases} \Pi_{in-h,lp^{\mu-1}+h-in} \equiv (-1)^i \dfrac{(lp^{\mu-2}\varpi)(lp^{\mu-2}\varpi-1)\dots(lp^{\mu-2}\varpi-i+1)}{1.2.3.\dots.(i-1)(in-h)\varpi}\, p \\ \qquad\qquad \equiv (-1)^i p^{\mu-1}\dfrac{l}{in-h}\dfrac{(lp^{\mu-2}\varpi-1)\dots(lp^{\mu-2}\varpi-i+1)}{1.2.3.\dots.(i-1)} \end{cases} \pmod{p^\mu}.$$

Lorsque μ surpasse 2, la formule (26) donne

$$\Pi_{in-h,lp^{\mu-1}+h-in} \equiv -p^{\mu-1}\frac{l}{in-h}.$$

Lorsque $\mu = 2$, elle donne

$$\Pi_{in-h,lp+h-in} \equiv (-1)^i p \frac{l}{in-h}\frac{(l\varpi-1)(l\varpi-2)\dots(l\varpi-i+1)}{1.2.3.\dots.(i-1)}.$$

Pour montrer une application des formules qui précèdent, supposons $n=3$. On trouvera, en prenant $h=1$, $k=1$, $l=1$,

$$\mathrm{R}_{1,1} = a_0 + a_1\rho + a_2\rho^2 = \left[\frac{1+1}{p}\right] + \rho\left[\frac{1+t}{p}\right] + \rho^2\left[\frac{1+t^2}{p}\right] + \dots,$$

$$\mathrm{R}_{2,2} = a_0 + a_1\rho^2 + a_2\rho^4 = \left[\frac{1+1}{p}\right]^2 + \rho^2\left[\frac{1+t}{p}\right]^2 + \rho^4\left[\frac{1+t^2}{p}\right]^2 + \dots,$$

$$(27)\qquad 4p = (2a_0 - a_1 - a_2)^2 + 3(a_1 - a_2)^2 = x^2 + 3y^2,$$

$$(28)\quad \begin{cases} x = \mathrm{R}_{1,1} + \mathrm{R}_{2,2} \equiv (1+1)^\varpi + t^\varpi(1+t)^\varpi + t^{2\varpi}(1+t^2)^\varpi + \dots \\ \qquad + (1+1)^{2\varpi} + t^{2\varpi}(1+t)^{2\varpi} + t^{4\varpi}(1+t^2)^{2\varpi} + \dots \\ \qquad \equiv (p-1)\Pi_{1,1}. \end{cases}$$

D'autre part, en ayant égard aux formules (21), (24), et prenant $\mu = 2$, on trouvera encore

$$(29)\quad \begin{cases} x \equiv \Sigma T^{i\varpi p}(1+T^i)^{\varpi p} + \Sigma T^{2i\varpi p}(1+T^i)^{2\varpi p} \\ \qquad \equiv (p-1)(\Pi_{2,p-2} + \Pi_{3,p-3} + \Pi_{5,p-5} + \dots + \Pi_{1,2p-1} + \Pi_{1,2p-4} + \dots). \end{cases}$$

Enfin, la formule (26) donnera

$$\Pi_{3i-1,p+1-3i} \equiv (-1)^i \frac{p}{3i-1}\frac{(\varpi-1)(\varpi-2)\dots(\varpi-i+1)}{1.2.3\dots(i-1)}$$

$$\Pi_{3i-2,2p+2-3i} \equiv (-1)^i \frac{2p}{3i-2}\frac{(2\varpi-1)(2\varpi-2)\dots(2\varpi-i+1)}{1.2.3\dots(i-1)} \pmod{p^2}.$$

Donc, on tirera de la formule (29)

$$(30)\quad \begin{cases} x \equiv (p-1)\left[-\dfrac{p}{2} + \dfrac{p}{5}\dfrac{\varpi-1}{1} - \dfrac{p}{8}\dfrac{(\varpi-1)(\varpi-2)}{1.2} + \dots\right] \\ \quad + (p-1)\left[-\dfrac{2p}{1} + \dfrac{2p}{4}\dfrac{2\varpi-1}{1} - \dfrac{2p}{7}\dfrac{(2\varpi-1)(2\varpi-2)}{1.2} + \dots\right]. \end{cases}$$

Il est important d'observer qu'en prenant

$$h = n-1 \quad \text{et} \quad i = \frac{p+n-1}{n} = \varpi + 1,$$

on obtiendra une valeur de

$$\Pi_{in-h,lp^{\mu-1}+h-in} = \Pi_{p,lp^{\mu-1}-p}$$

déterminée, non plus par la formule (26), mais par la suivante :

$$\Pi_{p,(lp^{\mu-2}-1)p} \equiv \frac{(lp^{\mu-1}\varpi)(lp^{\mu-1}\varpi-1)\dots(lp^{\mu-1}\varpi-p\varpi+1)}{1.2.3.\dots.p\varpi},$$

de laquelle on tirera, en supposant $n=3$, $\mu=2$, $l=2$,

$$(31)\qquad \Pi_{p,p} = \frac{2p\varpi(2p\varpi-1)\dots(p\varpi+1)}{1.2.3.\dots.p\varpi} \pmod{p^2}.$$

Comme on a d'ailleurs

$$\begin{aligned} &(1+px)(2+px)\dots(p-1+px) \\ &\equiv 1.2.3.\dots.(p-1)(1+px)\left(1+\frac{px}{2}\right)\left(1+\frac{px}{3}\right)\dots\left(1+\frac{px}{p-1}\right) \pmod{p^2}\ (1), \\ &\equiv 1.2.3.\dots.(p-1)\left[1+px\left(1+\frac{1}{2}+\frac{1}{3}+\dots+\frac{1}{p-1}\right)\right] \\ &\equiv 1.2.3.\dots.(p-1) \end{aligned}$$

(1) En effet, les divers termes de la progression arithmétique

$$1,\ 2,\ 3,\ \dots,\ p-1$$

seront équivalents, suivant le module p, si l'on fait abstraction de l'ordre dans lequel on les range, aux divers termes de la progression géométrique

$$1,\ t,\ t^2,\ \dots,\ t^{p-2};$$

d'où il résulte que les divers termes de la suite

$$1,\ \frac{1}{2},\ \frac{1}{3},\ \dots,\ \frac{1}{p-1}$$

on en conclut

$$\frac{(1+px)(2+px)\dots(p-1+px)}{1.2.3.\dots.(p-1)} \equiv 1 \pmod{p^2},$$

et la formule (31) peut être réduite à

$$(32)\qquad \begin{cases} \Pi_{p,p} \equiv \dfrac{2p\varpi(2p\varpi-p)\dots(p\varpi+p)}{p.2p\dots p\varpi} \\ \qquad \equiv \dfrac{2\varpi(2\varpi-1)\dots(\varpi+1)}{1.2.3.\dots.\varpi} \equiv \Pi_{1,1} \end{cases} \pmod{p^2}.$$

D'ailleurs, dans la formule (29), les quantités désignées à l'aide de la lettre Π étant égales deux à deux, à l'exception de

$$\Pi_{p,p} \equiv \Pi_{1,1} \pmod{p^2},$$

on trouvera

$$x \equiv (p-1)\Big[\Pi_{p,p} + 2\Big(\Pi_{2,p-2} + \Pi_{3,p-3} + \dots + \Pi_{\frac{p-3}{2},\frac{p+3}{2}}\Big) + 2(\Pi_{1,2p-1} + \Pi_{2,2p-2} + \dots + \Pi_{p-2,p+2})\Big],$$

seront équivalents, abstraction faite de l'ordre suivant lequel ils sont rangés, aux divers termes de la progression géométrique

$$1,\ \frac{1}{t},\ \frac{1}{t^2},\ \dots,\ \frac{1}{t^{p-2}},$$

ou, ce qui revient au même, aux divers termes de la suivante :

$$t^{p-1},\ t^{p-2},\ t^{p-3},\ \dots,\ t.$$

D'ailleurs, la somme de ces derniers termes, savoir

$$t + t^2 + t^3 + \dots + t^{p-1} = \frac{t^p - t}{t-1}$$

sera, ainsi que la différence $t^p - t$, équivalente à zéro, suivant le module p. On aura donc aussi

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p};$$

puis on en conclura

$$p\Big(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}\Big) \equiv 0 \pmod{p^2}$$

et

$$1.2.3.\dots.(p-1)\Big[1 + px\Big(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}\Big)\Big] \equiv 1.2.3.\dots.(p-1) \pmod{p^2}.$$

ou, ce qui revient au même,

$$(33)\qquad x \equiv (p-1)\frac{2\varpi(2\varpi+1)\dots(\varpi+1)}{1.2.3.\dots.\varpi} \pmod{p^2},$$

$$-2p(p-1)\left[\frac{1}{2} - \frac{1}{5}\frac{\varpi-1}{1} + \frac{1}{8}\frac{(\varpi-1)(\varpi-2)}{1.2} - \dots \pm \frac{1}{\frac{1}{2}(p-3)}\frac{(\varpi-1)\dots\left(\frac{\varpi+2}{2}\right)}{1.2.\dots.\left(\frac{\varpi-2}{2}\right)}\right]$$

$$-2p(p-1)\left[2 - \frac{2}{4}\frac{2\varpi-1}{1} + \frac{2}{7}\frac{(2\varpi-1)(2\varpi-2)}{1.2} - \dots \mp \frac{2}{p-3}\frac{(2\varpi-1)\dots(\varpi+1)}{1.2.3.\dots.(\varpi-1)}\right].$$

Ainsi, par exemple, on trouvera, en prenant $p = 7$, $\varpi = 2$,

$$x \equiv 6[\Pi_{7,7} + 2(\Pi_{2,5} + \Pi_{1,13} + \Pi_{4,10})] \equiv 6.6 + 14\left(\frac{1}{2} + 2 - \frac{3}{2}\right) \equiv 36 + 14 \equiv 1 \pmod{49};$$

en prenant $p = 13$, $\varpi = 4$,

$$x \equiv 12[\Pi_{13,13} + 2(\Pi_{2,11} + \Pi_{5,8} + \Pi_{1,25} + \Pi_{4,22} + \Pi_{7,19} + \Pi_{10,16})]$$
$$\equiv 12\left[70 - 26\left(\frac{1}{2} - \frac{3}{5} + 2 - \frac{7}{2} + 6 - 7\right)\right] \pmod{13^2},$$
$$\equiv 12\left[70 + 26\left(2 + \frac{3}{5}\right)\right] \equiv 12.70 \equiv (13-1)(13+1)5 \equiv -5$$

NOTE I.

PROPRIÉTÉS FONDAMENTALES DES FONCTIONS Θ_h, Θ_k, ...

n étant un nombre entier quelconque et u, v deux quantités entières positives ou négatives, nous disons que u est *équivalent* à v, suivant le *module* n, lorsque la différence $u - v$ ou $v - u$ est divisible par n, et nous indiquons cette *équivalence*, nommée *congruence* par M. Gauss, à l'aide de la notation

$$u \equiv v \pmod{n}$$

employée par ce géomètre. De plus, p étant un nombre premier, nous disons, avec Euler d'une part et de l'autre avec M. Poinsot, que r est *racine primitive* de l'équivalence

$$x^n \equiv 1 \pmod{p}$$

et ρ *racine primitive* de l'équation

$$x^n = 1$$

lorsque r^n est la plus petite puissance de r qui soit équivalente à l'unité suivant le module p, et ρ^n la plus petite puissance de ρ qui se réduise à l'unité. Dans cette hypothèse, les diverses racines de l'équation

$$x^n = 1$$

sont les diverses puissances de ρ, et comme deux puissances, dont les exposants restent équivalents suivant le module n, sont égales entre elles, il est clair que ces diverses racines peuvent être réduites à

$$1, \quad \rho, \quad \rho^2, \quad \ldots, \quad \rho^{n-1}.$$

De plus, m étant une quantité entière, on peut affirmer que la somme

$$1 + \rho^m + \rho^{2m} + \ldots + \rho^{(n-1)m} = \frac{\rho^{nm} - 1}{\rho^m - 1}$$

se réduira au nombre n ou à zéro, suivant que m sera divisible ou non divisible par n. Enfin, si n est un nombre pair, on aura

$$\rho^{\frac{n}{2}} = -1.$$

Pareillement, si l'équivalence

$$x^n \equiv 1 \pmod{p}$$

offre n racines distinctes, ce qui arrivera si n est diviseur de $p - 1$, ces diverses racines seront les diverses puissances de r, et comme deux puissances, dont les exposants seraient équivalents entre eux suivant le module n, resteraient équivalentes entre elles suivant le module p, il est clair que ces diverses racines pourront être réduites à

$$1, \quad r, \quad r^2, \quad \ldots, \quad r^{n-2}.$$

De plus, m étant une quantité entière, on peut affirmer que la somme

$$1 + r^m + r^{2m} + \ldots + r^{(n-1)m} = \frac{r^{nm} - 1}{r^m - 1}$$

sera équivalente, suivant le module p, au nombre n ou à zéro, selon que m sera divisible ou non divisible par n. Enfin, si n est un nombre pair, on aura

$$r^{\frac{n}{2}} \equiv -1 \pmod{p}.$$

Ces principes étant admis, les propositions rappelées dans les premières pages de ce Mémoire et relatives aux propriétés fondamentales des fonctions

$$\Theta_h, \quad \Theta_k, \quad \ldots$$

pourront être facilement établies de la manière suivante.

Nommons :

p un nombre premier impair;
θ une racine primitive de l'équation

$$x^p = 1;$$

τ une racine primitive de l'équation

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

et t une racine primitive de l'équivalence

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

Comme les diverses racines de cette équivalence peuvent être représentées par les divers termes de la progression arithmétique

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

ou, si l'on ne tient pas compte de l'ordre dans lequel elles sont rangées, par les divers termes de la progression géométrique

$$1,\ t,\ t^2,\ \ldots,\ t^{p-2},$$

l'équation

$$1+\theta+\theta^2+\ldots+\theta^{p-1}=0$$

pourra s'écrire comme il suit :

$$1+\theta^t+\theta^{t^2}+\ldots+\theta^{t^{p-2}}=0. \tag{1}$$

On aura, d'autre part,

$$\tau^{\frac{p-1}{2}}=-1$$

et

$$1+\tau^m+\tau^{2m}+\ldots+\tau^{(p-2)m}=p-1$$

ou bien

$$1+\tau^m+\tau^{2m}+\ldots+\tau^{(p-2)m}=0,$$

suivant que m sera divisible ou non divisible par $p-1$. Soient d'ailleurs h, k des quantités entières et posons

$$\Theta_h=\theta+\tau^h\theta^t+\tau^{2h}\theta^{t^2}+\ldots+\tau^{(p-2)h}\theta^{t^{p-2}};$$

il est clair que Θ_h, Θ_k seront égaux lorsque h et k seront équivalents entre eux suivant le module $p-1$. De plus, l'équation (1) pourra être présentée sous la forme

$$\Theta_0=-1.$$

Enfin l'on aura évidemment, quels que soient h et k,

$$\Theta_h\Theta_k=S(\tau^{t^{(h+jk}}\theta^{t^{i+t^j}}), \tag{2}$$

le signe S s'étendant à toutes les valeurs de i et de j comprises dans la suite

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2.$$

Les valeurs de i et de j qui, dans l'équation (2), rendront, sous le signe S, l'exposant 0 équivalent à zéro, suivant le module p, sont celles qui vérifieront la formule

$$t^i+t^j\equiv 0 \pmod{p},$$

de laquelle on tire

$$t^{j-i}\equiv -1\equiv t^{\pm\frac{p-1}{2}} \pmod{p}$$

et, par suite,

$$j-i=\pm\frac{p-1}{2}$$

ou, ce qui revient au même,

$$j=i\pm\frac{p-1}{2};$$

le signe supérieur ou inférieur devant être adopté, suivant que i est inférieur ou supérieur à $\frac{p-1}{2}$. Donc, dans l'équation (2), l'exposant de θ, sous le signe S, deviendra équivalent à zéro, suivant le module p, pour $p-1$ systèmes de valeurs correspondantes de i et de j, la valeur de i pouvant être un quelconque des termes de la suite

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2;$$

et, dans la somme que représente le second membre de l'équation (2), la partie correspondante à ces valeurs de i et de j sera

$$S(\tau^{t^{(h+jk}})=S\left(\tau^{t^{(h+ik}}\tau^{\pm\frac{p-1}{2}t^k}\right)$$

ou, ce qui revient au même,

$$(-1)^k S(\tau^{t^{(h+ik}})=(-1)^k(1+\tau^{t^h+k}+\tau^{2(t^h+k)}+\ldots+\tau^{(p-2)(t^h+k)}).$$

Donc, en vertu de ce qui a été dit plus haut, cette partie se réduira simplement à

$$(-1)^k(p-1) = (-1)^h(p-1)$$

ou bien à zéro, suivant que $h+k$ sera divisible ou non divisible par $p-1$.

Considérons à présent les systèmes de valeurs de i et de j qui, dans l'équation (2), rendent, sous le signe S, l'exposant de 0 équivalent à l'unité suivant le module p. Ces systèmes seront ceux pour lesquels l'équivalence

$$i^i + i^j \equiv 1 \pmod{p}$$

se trouvera vérifiée. Or, cette équivalence, présentée sous la forme

$$i^j \equiv 1 - i^i,$$

fournira une seule valeur de j, comprise dans la suite

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2,$$

pour toute valeur de i qui, étant comprise dans la même suite, ne rendra pas nulle la différence

$$1 - i^i,$$

et, comme la seule valeur $i = 0$ fera évanouir cette différence, il en résulte que l'équivalence dont il s'agit se vérifiera pour $p-2$ systèmes de valeurs correspondantes de i et de j, chacune des valeurs de j étant un terme de la suite

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

Cela posé, concevons d'abord que la somme $h+k$ ne soit pas divisible par $p-1$ et désignons alors par $R_{h,k}$ la somme des termes qui, dans le second membre de l'équation (2), seront proportionnels à la première puissance de 0. La valeur de $R_{h,k}$, qui sera déterminée par la formule

$$R_{h,k} = S(\tau^{ih+jk}), \tag{3}$$

jointe à la condition

$$i^i + i^j \equiv 1 \pmod{p}, \tag{4}$$

se composera seulement de $p-2$ termes de la forme

$$\tau^{ih+jk},$$

et, comme chacun de ces termes sera nécessairement égal à l'un des termes de la progression géométrique

$$1,\ \tau,\ \tau^2,\ \ldots,\ \tau^{p-2},$$

il est clair qu'on aura

$$R_{h,k} = a_0 + a_1\tau + a_2\tau^2 + \ldots + a_{p-2}\tau^{p-2}, \tag{5}$$

$a_0, a_1, \ldots, a_{p-2}$ désignant des nombres entiers dont plusieurs pourront s'évanouir et dont la somme vérifiera la condition

$$a_0 + a_1 + a_2 + \ldots + a_{p-2} = p-2. \tag{6}$$

Soit maintenant m l'un quelconque des nombres entiers compris dans la suite

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

La somme des termes proportionnels à

$$\vartheta^m,$$

dans le second membre de la formule (2), sera évidemment

$$\vartheta^m S(\tau^{ih+jk}),$$

pourvu que l'on étende le signe S à toutes les valeurs de i et de j qui, n'étant pas situées hors des limites 0, $p-2$, vérifient l'équivalence

$$i^i + i^j \equiv i^m \pmod{p}.$$

Or, cette équivalence pouvant être présentée sous la forme

$$i^{i-m} + i^{j-m} \equiv 1 \pmod{p},$$

si l'on étend le signe S à toutes les valeurs de $i-m$ et de $j-m$ qui

la vérifient, on trouvera, en faisant usage de la notation ci-dessus adoptée,

$$R_{h,k} = S(\tau^{(i-m)h+(j-m)k})$$

ou, ce qui revient au même,

$$R_{h,k} = \tau^{-m(h+k)} S(\tau^{ih+jk}),$$

et, par suite,

$$S(\tau^{ih+jk}) = R_{h,k}\tau^{m(h+k)}.$$

Donc, dans le second membre de l'équation (2), la somme des termes proportionnels à

$$\theta t^m$$

sera généralement

$$R_{h,k}\tau^{m(h+k)}\theta t^m.$$

Donc, la somme des termes qui renfermeront des puissances positives de 0 sera

$$R_{h,k} S(\tau^{m(h+k)}\theta t^m),$$

le signe S s'étendant à toutes les valeurs de m non situées hors des limites 0, $p-2$. D'ailleurs, on aura évidemment, sous cette condition,

$$\Theta_h = S(\tau^{mh}\theta t^m)$$

et, par suite,

$$\Theta_{h+k} = S(\tau^{m(h+k)}\theta t^m).$$

Ainsi, dans l'hypothèse admise, c'est-à-dire lorsque $h+k$ n'est pas divisible par $p-1$, la somme des termes qui, dans le second membre de l'équation (2), renferment des puissances positives de 0 se réduit simplement à

$$R_{h,k}\Theta_{h+k},$$

et comme alors, d'après ce qui a été dit ci-dessus, la somme des autres termes se réduit à zéro, il en résulte qu'on a

$$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k}, \tag{7}$$

la valeur de $R_{h,k}$ étant déterminée par la formule (3) jointe à la formule (4), ou, ce qui revient au même

$$\Theta_h\Theta_k = \Theta_{h+k} S(\tau^{ih+jk}), \tag{8}$$

pourvu que l'on étende le signe S à toutes les valeurs de i et de j qui, étant comprises dans la suite

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2,$$

vérifient la condition (4).

Passons au cas où la somme $h+k$ est divisible par $p-1$. Alors, d'après ce qui a été dit ci-dessus, on devra remplacer l'équation (8) par la suivante :

$$\Theta_h\Theta_k = \Theta_{h+k} S(\tau^{ih+jk}) + (-1)^h(p-1),$$

que l'on pourra réduire à

$$\Theta_h\Theta_{-h} = -S(\tau^{(i-j)h}) + (-1)^h(p-1),$$

attendu que l'équivalence

$$h+k \equiv 0 \quad \text{ou} \quad k \equiv -h \pmod{p-1}$$

entrainera les formules

$$\tau^k = \tau^{-h}, \qquad \Theta_k = \Theta_{-h}, \qquad \Theta_{h+k} = \Theta_0 = -1.$$

Donc, si l'on suppose la formule (7) étendue au cas où la somme $h+k$ est divisible par $p-1$, c'est-à-dire si, en choisissant $R_{h,k}$ de manière à vérifier dans tous les cas cette formule, on pose

$$\Theta_h\Theta_{-h} = R_{h,-h}\Theta_0, \tag{9}$$

on aura

$$R_{h,-h} = S(\tau^{(i-j)h}) - (-1)^h(p-1).$$

Dans le second membre de cette dernière formule, le signe S doit toujours être étendu aux valeurs de i et de j qui, étant comprises dans la suite

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2$$

vérifient la condition (4) ou, ce qui revient au même, à toutes les valeurs de $i-j$ qui, étant comprises dans la même suite, vérifient la formule

$$t^{i-j} \equiv t^{-j} - 1 \pmod{p-1}$$

et, par conséquent, à toutes les valeurs de $i-j$ distinctes de la valeur

$$\frac{p-1}{2}$$

qui donnerait

$$t^{i-j} \equiv -1 \pmod{p-1}.$$

Or, comme en admettant cette dernière valeur de $i-j$ on aurait généralement

$$S(\tau^{(i-j)h}) = 0,$$

on trouvera au contraire, en l'excluant,

$$S(\tau^{(i-j)h}) = -\tau^{\frac{p-1}{2}h} = -(-1)^h,$$

et, par suite, la valeur trouvée de $R_{h,-h}$ deviendra

$$R_{h,-h} = -(-1)^h p, \tag{10}$$

pourvu que h ne soit pas divisible par $p-1$. Alors aussi l'équation (9) donnera

$$\Theta_h \Theta_{-h} = (-1)^h p. \tag{11}$$

Si h devenait lui-même divisible par $p-1$, il serait pair et, comme on aurait

$$(-1)^h \equiv 1, \qquad \tau^h \equiv 1,$$

la valeur trouvée de $R_{h,-h}$ se réduirait à

$$p - 2 - (p-1) = -1.$$

Au reste, on peut conclure immédiatement de la formule (7) : 1° que la valeur de $R_{h,k}$ ne varie pas lorsqu'on fait croître ou décroître h ou k d'un multiple de $p-1$; 2° que $R_{h,k}$ se réduit à -1 dès que l'une des

quantités h, k est divisible par $p-1$. Ainsi, par exemple, si l'on suppose k divisible par $p-1$, l'on aura

$$\Theta_k = \Theta_0 = -1$$

et, par suite, la formule (7) donnera

$$R_{h,0} = R_{0,h} = -1. \tag{12}$$

Si, dans la formule (7), on change les signes de h et de k, l'on trouvera

$$\Theta_{-h}\Theta_{-k} = R_{-h,-k}\Theta_{-h,-k},$$

puis, de cette équation combinée par voie de multiplication avec la formule (7), on tirera, en ayant égard à la formule (11),

$$R_{h,k}R_{-h,-k} = p. \tag{13}$$

L'équation (13) suppose évidemment h, k et $h+k$ non divisibles par $p-1$.

Les équations (7), (10), (11), (12), (13) coïncident avec les formules (9), (11), (13) et (12) du paragraphe I de ce Mémoire lorsque le diviseur de $p-1$, représenté dans ce paragraphe par la lettre ϖ, se réduit à l'unité. Dans le cas contraire, pour passer des unes aux autres, il suffira de remplacer

$$h \text{ par } \varpi h, \qquad k \text{ par } \varpi k,$$

puis d'écrire, pour abréger,

$$\Theta_h \text{ au lieu de } \Theta_{\varpi h} \quad \text{et} \quad R_{h,k} \text{ au lieu de } R_{\varpi h,\varpi k}.$$

Lorsque dans la formule (11) on pose

$$h = \frac{p-1}{2},$$

elle fournit un théorème, très remarquable, de M. Gauss et se réduit à

$$\Theta^2_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} p \tag{14}$$

ou, ce qui revient au même, à

$$(14) \qquad (\theta - \theta^{t} + \theta^{t^2} - \theta^{t^3} + \ldots + \theta^{t^{p-2}} - \theta^{t^{p-1}})^2 = (-1)^{\frac{p-1}{2}} p.$$

Cette dernière équation coïncide avec diverses formules du Mémoire, par exemple avec les formules (12) du paragraphe III.

NOTE II.

SUR DIVERSES FORMULES OBTENUES DANS LE DEUXIÈME PARAGRAPHE.

Il est facile de s'assurer que la formule (61) du paragraphe II entraîne les formules (62), non seulement, comme nous l'avons avancé, dans le cas particulier où μ se réduit à l'unité, mais généralement et quelle que soit la valeur de μ. C'est ce que nous allons démontrer.

Lorsque ν sera de la forme $4x+1$, les termes des suites (63), (64) étant eux-mêmes de cette forme, puisqu'on a généralement

$$u^m + \nu(1-u^m) = 1 + (\nu-1)(1-u^m) \qquad \text{et} \qquad \nu - 1 \equiv 0 \pmod 4,$$

seront équivalents, suivant le module $n = 4\nu$, à certains termes de la suite

$$1, \quad 5, \quad 9, \quad \ldots, \quad 4\nu-11, \quad 4\nu-7, \quad 4\nu-3.$$

D'ailleurs celle-ci renfermera : 1° un terme égal à ν; 2° $\nu - 1$ termes premiers, non seulement à ν, mais encore à

$$n = 4\nu,$$

et qui, étant en même nombre que les termes des deux suites (63), (64), devront être équivalents, les uns aux termes de la suite (63), les autres aux termes de la suite (64). Parmi ces $\nu - 1$ termes, ceux

qui se réduiront à l'un des suivants :

$$1, \quad 2, \quad 3, \quad \ldots, \quad \frac{n}{2} = 2\nu,$$

étant précisément

$$1, \quad 5, \quad 9, \quad \ldots, \quad 2\nu-9, \quad 2\nu-5, \quad 2\nu-1,$$

seront en nombre égal à

$$\frac{\nu-1}{2};$$

les uns, dont le nombre sera ν', étant équivalents à certains termes de la suite (63) et les autres, dont le nombre sera ν'', étant équivalents à certains termes de la suite (64). On aura, en conséquence,

$$\nu' + \nu'' = \frac{\nu-1}{2}.$$

Observons maintenant qu'en vertu des formules

$$u^{\frac{\nu-1}{2}} + 1 \equiv 0 \pmod \nu, \qquad \nu - 1 \equiv 0 \pmod 4,$$

on trouvera, quel que soit le nombre entier m,

$$[u^m + \nu(1-u^m)] + \left[u^{m+\frac{\nu-1}{2}} + \nu\left(1-u^{m+\frac{\nu-1}{2}}\right)\right] \equiv 2\nu \pmod{n = 4\nu}.$$

Donc, chacune des suites (63), (64) se composera de termes qui, pris deux à deux, pourront être représentés par des nombres de la forme

$$h, \quad 2\nu - h,$$

auxquels ils seront équivalents, suivant le module $n = 4\nu$. D'ailleurs, si l'indice h se trouve compris dans la suite

$$1, \quad 5, \quad 9, \quad \ldots, \quad 2\nu-9, \quad 2\nu-5, \quad 2\nu-1,$$

on pourra en dire autant de l'indice $2\nu - h$ qui sera distinct de h si h diffère de ν. Donc, chacun des nombres désignés par ν', ν'' sera pair et

$$\frac{1}{2}\nu', \quad \frac{1}{2}\nu''$$

seront entiers. Enfin, comme on aura

$$\frac{\nu'+\nu''}{2}=\frac{\nu-1}{4},$$

on peut affirmer que, si ν est non seulement de la forme $4x+1$, mais aussi de la forme $8x+5$, les deux entiers

$$\frac{1}{2}\nu', \quad \frac{1}{2}\nu''$$

seront l'un pair, l'autre impair. Donc alors, la différence

$$\frac{1}{2}\nu'-\frac{1}{2}\nu''$$

sera impaire elle-même et ne pourra se réduire à zéro.

A l'aide des observations qui précèdent, on peut ramener à une forme très simple les valeurs de

$$\mathfrak{F}(\sqrt{-1},\varsigma), \quad \mathfrak{F}(\sqrt{-1},\varsigma^u)$$

fournies par les équations (23), (26); et d'abord, puisque les différents termes de chacune des séries (63), (64), pris deux à deux, peuvent être censés de la forme

$$h, \quad 2\nu-h,$$

les équations (23), (26), combinées avec la formule

$$\Theta_h\Theta_{2\nu-h}=R_{h,2\nu-h}\Theta_{2\nu},$$

donneront

$$\mathfrak{F}(\sqrt{-1},\varsigma)=R_{1,2\nu-1}R_{\nu-(\nu-1)u^2,\nu+(\nu-1)u^2}\dots R_{\nu-(\nu-1)u^{\frac{\nu-5}{2}},\nu+(\nu-1)u^{\frac{\nu-5}{2}}}\frac{\Theta_{2\nu}^{\frac{\nu-1}{4}}}{\Theta_{\frac{\nu(\nu-1)}{2}}},$$

$$\mathfrak{F}(\sqrt{-1},\varsigma^u)=R_{\nu-(\nu-1)u,\nu+(\nu-1)u}\dots R_{\nu-(\nu-1)u^{\frac{\nu-5}{2}},\nu+(\nu-1)u^{\frac{\nu-5}{2}}}\frac{\Theta_{2\nu}^{\frac{\nu-1}{4}}}{\Theta_{\frac{\nu(\nu-1)}{2}}}.$$

Si d'ailleurs ν est de la forme $8x+5$, alors $\frac{\nu-5}{4}$ sera un nombre pair

et l'on aura, non seulement

$$\Theta_{2\nu}=\Theta_{-2\nu}, \qquad \Theta_{2\nu}\Theta_{-2\nu}=\Theta_{2\nu}^2=(-1)^{2\nu\square}p=p,$$

mais encore

$$\Theta_{\frac{\nu(\nu-1)}{2}}=\Theta_{2\nu}, \qquad \frac{\Theta_{2\nu}^{\frac{\nu-1}{4}}}{\Theta_{\frac{\nu(\nu-1)}{2}}}=\Theta_{2\nu}^{\frac{\nu-5}{4}}=p^{\frac{\nu-5}{8}},$$

ce qui réduira les formules précédentes à

$$\mathfrak{F}(\sqrt{-1},\varsigma)=p^{\frac{\nu-5}{8}}R_{1,2\nu-1}R_{\nu-(\nu-1)u^2,\nu+(\nu-1)u^2}\dots R_{\nu-(\nu-1)u^{\frac{\nu-5}{2}},\nu+(\nu-1)u^{\frac{\nu-5}{2}}},$$

$$\mathfrak{F}(\sqrt{-1},\varsigma^u)=p^{\frac{\nu-5}{8}}R_{\nu-(\nu-1)u,\nu+(\nu-1)u}\dots R_{\nu-(\nu-1)u^{\frac{\nu-5}{2}},\nu+(\nu-1)u^{\frac{\nu-5}{2}}}.$$

Ces dernières équations et les équations analogues, qui fourniraient les valeurs de

$$\mathfrak{F}(-\sqrt{-1},\varsigma), \quad \mathfrak{F}(-\sqrt{-1},\varsigma^u),$$

coïncident, comme on devait s'y attendre, avec les formules (66) lorsqu'on prend $\nu=5$ et avec les formules (74), (75) lorsqu'on prend $\nu=13$.

Si ν était de la forme $8x+1$, alors, $\frac{\nu-1}{4}$ étant un nombre pair, on aurait

$$\Theta_{\frac{\nu(\nu-1)}{2}}=\Theta_{4\nu}=\Theta_0=-1, \qquad \Theta_{2\nu}^{\frac{\nu-1}{4}}=p^{\frac{\nu-1}{8}},$$

ce qui réduirait les formules précédemment obtenues à

$$\mathfrak{F}(\sqrt{-1},\varsigma)=-p^{\frac{\nu-1}{8}}R_{1,2\nu-1}R_{\nu-(\nu-1)u^2,\nu+(\nu-1)u^2}\dots R_{\nu-(\nu-1)u^{\frac{\nu-3}{2}},\nu+(\nu-1)u^{\frac{\nu-3}{2}}},$$

$$\mathfrak{F}(\sqrt{-1},\varsigma^u)=-p^{\frac{\nu-1}{8}}R_{\nu-(\nu-1)u,\nu+(\nu-1)u}\dots R_{\nu-(\nu-1)u^{\frac{\nu-3}{2}},\nu+(\nu-1)u^{\frac{\nu-3}{2}}}.$$

Dans tous les cas, en divisant la valeur de $\mathfrak{F}(\sqrt{-1},\varsigma)$ par celle de $\mathfrak{F}(\sqrt{-1},\varsigma^u)$, on trouvera

$$\frac{\mathfrak{F}(\sqrt{-1},\varsigma)}{\mathfrak{F}(\sqrt{-1},\varsigma^u)}=\frac{R_{1,2\nu-1}R_{\nu-(\nu-1)u^2,\nu+(\nu-1)u^2}\dots R_{\nu-(\nu-1)u^{\frac{\nu-3}{2}},\nu+(\nu-1)u^{\frac{\nu-3}{2}}}}{R_{\nu-(\nu-1)u,\nu+(\nu-1)u}\dots R_{\nu-(\nu-1)u^{\frac{\nu-3}{2}},\nu+(\nu-1)u^{\frac{\nu-3}{2}}}}.$$

Si, dans cette dernière formule, on remplace

$$R_{h,k} \quad \text{par} \quad \frac{p}{R_{n-h,n-k}},$$

toutes les fois que h et k sont équivalents, suivant le module $n = 4\nu$, à des nombres compris entre les limites

$$0, \quad 2\nu,$$

on en tirera

$$\frac{\mathcal{F}(\sqrt{-1}, \varsigma)}{\mathcal{F}(\sqrt{-1}, \varsigma^n)} = \frac{p^{\frac{\nu}{2}} f(\rho)}{p^{\frac{\nu'}{2}} \mathrm{f}(\rho)},$$

$f(\rho)$ et $\mathrm{f}(\rho)$ désignant des produits de la forme

$$R_{h,2\nu-h} R_{k,2\nu-k} \ldots$$

composés de facteurs

$$R_{h,2\nu-h}, \quad R_{k,2\nu-k}, \quad \ldots$$

dont aucun ne deviendra divisible par p lorsqu'on y substituera r à ρ; puis, en ayant égard aux formules (49) ou (56) et représentant par $\frac{x}{y}$ la valeur du rapport $\frac{\mathcal{E}}{\gamma}$ réduit à sa plus simple expression, l'on trouvera successivement

$$\frac{\mathcal{E} + \gamma(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}}{\mathcal{E} - \gamma(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}} = \frac{p^{\frac{\nu}{2}} f(\rho)}{p^{\frac{\nu'}{2}} \mathrm{f}(\rho)}$$

et

$$\frac{x + y(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}}{x - y(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}} = \frac{p^{\frac{\nu}{2}} f(\rho)}{p^{\frac{\nu'}{2}} \mathrm{f}(\rho)}.$$

On aura d'ailleurs, en vertu de la seconde des formules (43),

$$[x + y(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}][x - y(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}] = x^2 + \nu y^2$$

et, par suite, on trouvera encore

$$[x + y(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}]^2 \mathrm{f}(\rho) = p^{\frac{\nu'-\nu}{2}}(x^2 + \nu y^2) f(\rho),$$

$$[x - y(\varsigma - \varsigma^n + \ldots - \varsigma^{n^{\nu-1}})\sqrt{-1}]^2 f(\rho) = p^{\frac{\nu'-\nu}{2}}(x^2 + \nu y^2) \mathrm{f}(\rho).$$

Si, dans ces dernières équations, on remplace ρ par r, on devra y remplacer en même temps ς par s, $\sqrt{-1}$ par a et le signe $=$ par $\equiv$, le module étant le nombre p. On trouvera ainsi

$$\begin{aligned} &[x + (s - s^n + \ldots - s^{n^{\nu-1}})ay]^2 \mathrm{f}(r) \equiv p^{\frac{\nu'-\nu}{2}}(x^2 + \nu y^2) f(r) \\ &[x - (s - s^n + \ldots - s^{n^{\nu-1}})ay]^2 f(r) \equiv p^{\frac{\nu'-\nu}{2}}(x^2 + \nu y^2) \mathrm{f}(r) \end{aligned} \pmod{p}.$$

Observons à présent que x et y, n'ayant pas de facteurs communs, ne peuvent être simultanément divisibles par p. Par suite, on pourra en dire autant des expressions

$$x + (s - s^n + \ldots - s^{n^{\nu-1}})ay, \quad x - (s - s^n + \ldots - s^{n^{\nu-1}})ay,$$

qui ne peuvent devenir simultanément divisibles par p qu'avec leur somme

$$2x$$

et leur différence

$$2(s - s^n + \ldots - s^{n^{\nu-1}})ay,$$

par conséquent avec x et y, attendu que les quantités

$$s - s^n + \ldots - s^{n^{\nu-1}} \quad \text{et} \quad a$$

sont racines des équivalences

$$x^2 \equiv \nu \pmod{p}, \qquad x^4 \equiv 1 \pmod{p}.$$

Cela posé, comme $\mathrm{f}(r)$ et $f(r)$ ne seront pas non plus divisibles par p, il est clair que, des deux produits

$$[x + (s - s^n + \ldots - s^{n^{\nu-1}})ay]^2 \mathrm{f}(r), \quad [x - (s - s^n + \ldots - s^{n^{\nu-1}})ay]^2 f(r),$$

l'un au moins sera équivalent, suivant le module p, à un terme de la suite

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

Donc, en vertu des formules obtenues, on pourra en dire autant de l'un des produits

$$p^{\frac{\nu'-\nu}{2}}(x^2 + \nu y^2), \quad p^{\frac{\nu'-\nu}{2}}(x^2 + \nu y^2).$$

D'ailleurs le binome

$$x^2+\nu y^2,$$

étant diviseur de

$$\xi^2+\nu\eta^2,$$

devra, en vertu de la formule (47) ou (48), diviser l'un des produits

$$4p^{\frac{\nu-1}{2}},\quad 4p^{\frac{\nu-3}{2}},$$

et par conséquent il sera, ou de la forme

$$p^{\mu}$$

si l'un des deux nombres x, y est pair, l'autre impair, ou de la forme

$$2p^{\mu}$$

si x, y sont tous deux impairs, attendu qu'alors $x^2+\nu y^2$, divisé par 4, donnera 2 pour reste et ne pourra devenir égal à $4p^{\mu}$. Or, comme les produits

$$p^{\frac{\nu'-\nu''}{2}}(x^2+\nu y^2),\quad p^{\frac{\nu''-\nu'}{2}}(x^2+\nu y^2)$$

se réduiront, dans le premier cas, à

$$p^{\mu+\frac{\nu'-\nu''}{2}},\quad p^{\mu+\frac{\nu''-\nu'}{2}},$$

et, dans le second cas, à

$$2p^{\mu+\frac{\nu'-\nu''}{2}},\quad 2p^{\mu+\frac{\nu''-\nu'}{2}},$$

il est clair que l'un des exposants

$$\mu+\frac{\nu'-\nu''}{2},\quad \mu+\frac{\nu''-\nu'}{2}$$

devra être égal à zéro. Par conséquent, *si, en prenant pour μ la valeur numérique de la différence $\frac{\nu'}{2}-\frac{\nu''}{2}$, on pose*

$$\mu=\pm\frac{\nu'-\nu''}{2},$$

on pourra satisfaire, par des nombres x, y entiers et premiers entre eux, à l'une des formules

$$p^{\mu}=x^2+\nu y^2,$$
$$2p^{\mu}=x^2+\nu y^2,$$

savoir, à la première, par deux nombres entiers, l'un pair, l'autre impair, ou à la seconde par deux nombres entiers impairs. Mais la seconde formule ne peut subsister lorsque ν est de la forme $8x+5$, puisque alors, pour des valeurs impaires de x, y, $x^2+\nu y^2$ est de la forme $8x+6$, tandis que

$$2p^{\mu}=2(4\nu\varpi+1)^{\mu}$$

est de la forme $8x+2$. Donc, *si ν est de la forme $8x+5$, des nombres x, y, entiers et premiers entre eux, vérifieront la formule*

$$p^{\mu}=x^2+\nu y^2,$$

pourvu que l'on y suppose μ égal à la valeur numérique de la différence $\frac{1}{2}\nu'-\frac{1}{2}\nu''$, par conséquent

$$\mu=\pm\frac{\nu'-\nu''}{2}.$$

D'ailleurs, la valeur précédente de μ est précisément celle que fournit la première des équations (60). En effet, les expressions (65) se réduisant, en vertu de la formule

$$\nu'+\nu''=\frac{\nu-1}{2},$$

aux deux suivantes,

$$\frac{1}{2}\nu',\quad \frac{1}{2}\nu'',$$

si l'on égale l'une ou l'autre à la différence $\lambda-\frac{1}{2}\frac{\nu-5}{4}$, on aura

$$2\lambda-\frac{\nu-5}{4}=\nu'\quad\text{ou}\quad\nu''$$

et la première des formules (60) donnera

$$\mu=\frac{\nu-3}{2}-2\lambda=\frac{\nu-1}{4}+\left(\frac{\nu-5}{4}-2\lambda\right)=\frac{\nu'+\nu''}{2}+\left(\frac{\nu-5}{4}-2\lambda\right)=\pm\frac{\nu'-\nu''}{2}.$$

Pour établir les propositions ci-dessus énoncées, nous avons eu recours à la formule qui fournit la valeur du rapport des expressions imaginaires

$$\mathfrak{F}(\sqrt{-1},\varsigma),\quad \mathfrak{F}(\sqrt{-1},\varsigma^u)$$

et nous avons transformé la fraction qui représente cette valeur, de manière à mettre en évidence tous les facteurs égaux à p, soit dans le numérateur, soit dans le dénominateur. On pourrait faire subir une semblable transformation aux valeurs mêmes des deux expressions imaginaires

$$\mathfrak{F}(\sqrt{-1},\varsigma),\quad \mathfrak{F}(\sqrt{-1},\varsigma^u)$$

ou bien encore les deux suivantes :

$$\mathfrak{F}(-\sqrt{-1},\varsigma),\quad \mathfrak{F}(-\sqrt{-1},\varsigma^u).$$

Concevons en particulier que, dans les valeurs précédemment trouvées de $\mathfrak{F}(\sqrt{-1},\varsigma)$ et de $\mathfrak{F}(\sqrt{-1},\varsigma^u)$, l'on remplace

$$R_{h,k}\quad \text{par}\quad \frac{p}{R_{n-h,n-k}},$$

toutes les fois que h et k sont équivalents, suivant le module $n=4\nu$, à des nombres compris entre les limites

$$0,\quad 2\nu.$$

On trouvera, si ν est de la forme $8x+5$,

$$\mathfrak{F}(\sqrt{-1},\varsigma)=p^{\frac{\nu-5}{8}+\frac{\nu'}{2}}\varphi(\rho),\qquad \mathfrak{F}(\sqrt{-1},\varsigma^u)=p^{\frac{\nu-5}{8}+\frac{\nu'}{2}}\chi(\rho),$$

en désignant par

$$\varphi(\rho),\quad \chi(\rho)$$

deux fractions qui auront pour numérateurs et pour dénominateurs des produits de la forme

$$R_{h,n-h}R_{k,n-k}\ldots,$$

composés de facteurs dont aucun ne deviendra divisible par p lorsqu'on

substituera r à ρ; puis, en ayant égard aux équations (30) du paragraphe II et à la formule

$$\frac{\nu-3}{2}=\frac{\nu-5}{4}+\frac{\nu-1}{4}=\frac{\nu-5}{4}+\frac{\nu'+\nu''}{2},$$

on trouvera encore

$$\mathfrak{F}(-\sqrt{-1},\varsigma)=p^{\frac{\nu-5}{8}+\frac{\nu''}{2}}\frac{1}{\varphi(\rho)},\qquad \mathfrak{F}(-\sqrt{-1},\varsigma^u)=p^{\frac{\nu-5}{8}+\frac{\nu'}{2}}\frac{1}{\chi(\rho)}.$$

Si ν, au lieu d'être de la forme $8x+5$, était de la forme $8x+1$, les valeurs de

$$\mathfrak{F}(\sqrt{-1},\varsigma),\quad \mathfrak{F}(\sqrt{-1},\varsigma^u),\quad \mathfrak{F}(-\sqrt{-1},\varsigma),\quad \mathfrak{F}(-\sqrt{-1},\varsigma^u)$$

seraient semblables à celles que nous venons de trouver, à cela près que, dans les exposants de p, la première partie

$$\frac{\nu-5}{8}$$

se trouverait remplacée par

$$\frac{\nu-1}{8}.$$

Dans l'un et l'autre cas, on aura

$$\frac{\mathfrak{F}(\sqrt{-1},\varsigma)}{p^{\frac{\nu'}{2}}\varphi(\rho)}=\frac{\mathfrak{F}(\sqrt{-1},\varsigma^u)}{p^{\frac{\nu'}{2}}\chi(\rho)}=\frac{\mathfrak{F}(-\sqrt{-1},\varsigma)}{p^{\frac{\nu'}{2}}\frac{1}{\varphi(\rho)}}=\frac{\mathfrak{F}(-\sqrt{-1},\varsigma^u)}{p^{\frac{\nu'}{2}}\frac{1}{\chi(\rho)}};$$

puis on tirera de cette dernière formule, combinée avec les équations (49),

$$\frac{\delta+\varepsilon\sqrt{-1}}{\delta-\varepsilon\sqrt{-1}}=\frac{\mathfrak{F}(\sqrt{-1},\varsigma)}{\mathfrak{F}(-\sqrt{-1},\varsigma^u)}=\frac{\mathfrak{F}(\sqrt{-1},\varsigma^u)}{\mathfrak{F}(-\sqrt{-1},\varsigma)}=\varphi(\rho)\chi(\rho)$$

et, par suite,

$$(\delta+\varepsilon\sqrt{-1})^2=(\delta^2+\varepsilon^2)\varphi(\rho)\chi(\rho),$$
$$(\delta-\varepsilon\sqrt{-1})^2=(\delta^2+\varepsilon^2)\frac{1}{\varphi(\rho)\chi(\rho)}.$$

Si, dans ces dernières formules, on remplace ρ par r, on devra rem-

placer en même temps $\sqrt{-1}$ par a et le signe $=$ par le signe $\equiv$, le module étant le nombre p. On trouvera ainsi

$$\begin{aligned}(\delta+\varepsilon a)^2&\equiv(\delta^2+\varepsilon^2)\varphi(r)\chi(r)\\(\delta-\varepsilon a)^2&\equiv(\delta^2+\varepsilon^2)\frac{1}{\varphi(r)\chi(r)}\end{aligned}\pmod p.$$

Donc, puisque $\varphi(r)$, $\chi(r)$ ne sont équivalents ni à zéro ni à $\frac{1}{0}$, suivant le module p, la somme

$$\delta^2+\varepsilon^2$$

ne pourra devenir divisible par p qu'avec les deux binomes

$$\delta+\varepsilon a,\quad \delta-\varepsilon a,$$

par conséquent, avec les deux nombres

$$\delta,\quad \varepsilon.$$

D'ailleurs, il est permis de supposer que les nombres δ, ε sont premiers entre eux, attendu qu'on n'altère pas les équations (49) en transportant dans $\mathfrak{E}$ et dans γ les facteurs qui seraient communs à δ et à ε. Donc, cette hypothèse étant admise, $\delta^2+\varepsilon^2$ sera premier à p; et, si l'on nomme comme ci-dessus $\frac{x}{y}$ la forme la plus simple de la fraction $\frac{\varepsilon}{\gamma}$, l'équation (47) ou (48) entraînera, ou les deux suivantes :

$$\delta^2+\varepsilon^2=1,\qquad x^2+\nu y^2=p^\mu$$

si des nombres x, y l'un est pair et l'autre impair, ou les deux suivantes :

$$\delta^2+\varepsilon^2=2,\qquad x+\nu y^2=2p^\mu$$

si les nombres x, y sont tous deux impairs. Dans le premier cas, on aura

$$\delta=\pm1,\qquad \varepsilon=0$$

ou

$$\delta=0,\qquad \varepsilon=\pm1,$$

par conséquent

$$(\delta\pm\varepsilon a)^2\equiv\pm1\qquad(\mathrm{mod}.p)$$

et

$$\begin{aligned}\varphi(r)\chi(r)&\equiv\pm1\\[\varphi(r)\chi(r)]^2&\equiv1\end{aligned}\pmod p.$$

Dans le second cas, qui ne se présente jamais lorsque ν est de la forme $8x+5$, on aurait

$$\delta=\pm1,\qquad \varepsilon=\pm i,$$

par conséquent

$$(\delta\pm\varepsilon a)^2\equiv\pm2a\qquad(\mathrm{mod}.p)$$

et

$$\begin{aligned}\varphi(r)\chi(r)&\equiv\pm a\\[\varphi(r)\chi(r)]^2&\equiv-1\end{aligned}\pmod p.$$

Pour déduire de ce qui a été dit plus haut la valeur du produit

$$\varphi(r)\chi(r),$$

il suffirait d'observer que les deux expressions

$$p^{\frac{\nu'}{2}}\varphi(\rho),\quad p^{\frac{\nu'}{2}}\chi(\rho)$$

renferment tous les facteurs de la forme

$$R_{h,2\nu-h}=R_{h,a+2\nu-h}=R_{h,6\nu-h},$$

h désignant un nombre distinct de ν et compris parmi les termes de la suite

$$1,\ 5,\ 9,\ \ldots,\ 4\nu-11,\ 4\nu-7,\ 4\nu-3.$$

Comme d'ailleurs, pour mettre en évidence les facteurs égaux à p, il suffit de remplacer

$$R_{h,2\nu-h}\quad\text{par}\quad\frac{p}{R_{a-h,a-2\nu+h}}=\frac{p}{R_{4\nu-h,2\nu+h}},$$

lorsque h est renfermé entre les limites 0, 2ν, on trouvera

$$\varphi(\rho)\chi(\rho)=\frac{R_{2\nu+3,4\nu-2}R_{2\nu+7,4\nu-7}\cdots R_{3\nu-2,3\nu+2}}{R_{2\nu+1,4\nu-1}R_{2\nu+5,4\nu-5}\cdots R_{3\nu-4,3\nu+4}}.$$

Il y a plus : comme on aura généralement, ainsi qu'il est facile de le

prouver,

$$R_{h,2\nu-k}^2 = R_{h,h} R_{2\nu-h,2\nu-k},$$

on trouvera encore

$$[\varphi(\rho)\chi(\rho)]^2 = \frac{R_{2\nu+3,2\nu+3} R_{2\nu+7,2\nu+7} \dots R_{3\nu-3,3\nu-3}}{R_{2\nu+1,2\nu+1} R_{2\nu+5,2\nu+5} \dots R_{3\nu-1,3\nu-1}}.$$

Si maintenant on remplace ρ par r et le signe $=$ par le signe $\equiv$, on devra remplacer généralement

$$R_{h,k}$$

par

$$-\Pi_{n-h,n-k}$$

et l'on aura, par suite,

$$\varphi(r)\chi(r) \equiv \frac{\Pi_{3,2\nu-3}\Pi_{7,2\nu-7}\dots\Pi_{\nu-2,\nu+2}}{\Pi_{1,2\nu-1}\Pi_{5,2\nu-5}\dots\Pi_{\nu-4,\nu+4}} \pmod{p}.$$

$$[\varphi(r)\chi(r)]^2 \equiv \frac{\Pi_{3,3}\Pi_{7,7}\dots\Pi_{\nu-2,\nu-2}\Pi_{\nu+2,\nu+2}\dots\Pi_{2\nu-3,2\nu-3}}{\Pi_{1,1}\Pi_{5,5}\dots\Pi_{\nu-4,\nu-4}\Pi_{\nu+4,\nu+4}\dots\Pi_{2\nu-1,2\nu-1}}$$

En joignant cette dernière formule à celles que nous avons précédemment obtenues, on arrivera immédiatement aux conclusions renfermées dans le théorème suivant :

THÉORÈME. — *ν et p étant deux nombres premiers, l'un de la forme $4x+1$ et l'autre de la forme $4\nu x+1$, supposons que la suite des nombres*

$$1,\ 5,\ 9,\ \dots,\ 2\nu-9,\ 2\nu-5,\ 2\nu-1$$

offre ν' racines de l'équivalence

$$x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$$

et ν'' racines de l'équivalence

$$x^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu},$$

on aura

$$\nu' + \nu'' = \frac{\nu-1}{2};$$

et, si l'on nomme

$$\mu$$

la valeur numérique de

$$\frac{\nu'-\nu''}{2},$$

on pourra satisfaire, par des nombres x, y entiers et premiers entre eux, à l'équation

$$x^2 + \nu y^2 = p^{2\mu},$$

non seulement lorsque ν sera de la forme $8x+5$, mais aussi lorsque, ν étant de la forme $8x+1$, le rapport

$$\frac{\Pi_{1,2\nu-1}\Pi_{3,2\nu-5}\dots\Pi_{\nu-4,\nu+4}}{\Pi_{3,2\nu-3}\Pi_{7,2\nu-7}\dots\Pi_{\nu-2,\nu+2}}$$

sera une des racines de l'équivalence

$$x^2 \equiv 1 \pmod{p}.$$

Si le même rapport cessait d'être équivalent, suivant le module p, à $+1$ ou à -1, il suit de ce qu'on a dit qu'il deviendrait racine de l'équivalence

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

et alors on pourrait satisfaire, par des nombres x, y entiers et premiers entre eux, à l'équation

$$x^2 + \nu y^2 = 2p^{2\mu}.$$

Au reste, nous n'avons pas encore trouvé d'exemple dans lequel le rapport dont il s'agit ne fût équivalent, suivant le module p, à ± 1; et, si l'on démontrait qu'il en est toujours ainsi, on en conclurait immédiatement qu'on peut satisfaire, par des nombres x, y entiers et premiers entre eux, à l'équation

$$x^2 + \nu y^2 = p^{2\mu},$$

non seulement lorsque ν est de la forme $8x+5$, mais encore lorsque ν est de la forme $8x+1$.

Il nous reste à montrer comment on peut déterminer directement la valeur du nombre

$$\mu = \pm\frac{\nu'-\nu''}{2}.$$

Parmi les termes de la suite

$$1,\ 5,\ 9,\ \dots,\ 2\nu-9,\ 2\nu-5,\ 2\nu-1,$$

plusieurs, en nombre égal à ν', vérifient l'équivalence

$$x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu};$$

d'autres, en nombre égal à ν'', vérifient l'équivalence

$$x^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu},$$

et un seul, savoir le terme ν, satisfait à la condition

$$x^{\frac{\nu-1}{2}} \equiv 0 \pmod{\nu}.$$

Cela posé, il est clair qu'on aura non seulement

$$\nu' + \nu'' = \frac{\nu-1}{2},$$

mais encore

$$\nu' - \nu'' \equiv 1^{\frac{\nu-1}{2}} + 5^{\frac{\nu-1}{2}} + 9^{\frac{\nu-1}{2}} + \ldots + (2\nu-9)^{\frac{\nu-1}{2}} + (2\nu-5)^{\frac{\nu-1}{2}} + (2\nu-1)^{\frac{\nu-1}{2}} \pmod{\nu};$$

par conséquent

$$\nu' - \nu'' \equiv \frac{d^{\frac{\nu-1}{2}}}{dz^{\frac{\nu-1}{2}}}(e^z + e^{3z} + e^{9z} + \ldots + e^{(2\nu-9)z} + e^{(2\nu-5)z} + e^{(2\nu-1)z}) \pmod{\nu},$$

pourvu que l'on suppose $z = 0$ après les différentiations effectuées. On aura d'ailleurs

$$e^z + e^{3z} + e^{9z} + \ldots + e^{(2\nu-1)z} = \frac{e^{(2\nu+3)z} - e^z}{e^{4z} - 1} = (e^{2\nu z} - 1)\frac{e^z}{e^{2z} - e^{-2z}} + \frac{1}{e^z + e^{-z}},$$

et comme le facteur

$$e^{2\nu z} - 1,$$

ainsi que ses dérivées relatives à z, devient, pour une valeur nulle de z, équivalent à zéro suivant le module ν, on trouvera, en définitive,

$$\nu' - \nu'' \equiv \frac{d^{\frac{\nu-1}{2}}}{dz^{\frac{\nu-1}{2}}}\left(\frac{1}{e^z + e^{-z}}\right) \pmod{\nu};$$

par conséquent

$$\nu' - \nu'' \equiv \frac{1}{2}\frac{d^{\frac{\nu-1}{2}}}{dz^{\frac{\nu-1}{2}}}\left(1 + \frac{z^2}{1.2} + \frac{z^4}{1.2.3.4} + \ldots\right)^{-1} \pmod{\nu}$$

et

$$\mu \equiv \pm\frac{1}{4}\frac{d^{\frac{\nu-1}{2}}}{dz^{\frac{\nu-1}{2}}}\left(1 + \frac{z^2}{1.2} + \frac{z^4}{1.2.3.4} + \ldots\right)^{-1} \pmod{\nu},$$

z devant être réduit à zéro après les différentiations; puis on en conclura

$$\mu = \pm\frac{1.2.3.\ldots.\frac{\nu-1}{2}}{4} S\left[(-1)^{f+g+h+\ldots}\frac{1.2.3.\ldots.(f+g+\ldots)}{(1.2.\ldots.f)(1.2.\ldots.g)\ldots}\left(\frac{1}{1.2}\right)^f\left(\frac{1}{1.2.3.4}\right)^g\ldots\right] \pmod{\nu},$$

le signe S devant s'étendre à toutes les valeurs entières, nulles ou positives, de f, g, ... qui vérifient la formule

$$f + 2g + 3h + \ldots = \frac{\nu-1}{4},$$

et chacun des produits $1.2.\ldots.f$, $1.2.\ldots.g$, ... devant être remplacé par l'unité lorsque le dernier facteur f, ou g, ... se réduit à zéro. La valeur de l'exposant μ se trouvera ainsi complètement déterminée, puisque d'ailleurs cet exposant doit être positif et inférieur à

$$\frac{\nu' + \nu''}{2} = \frac{\nu-1}{4}.$$

Si l'on prend successivement pour ν les différents termes de la suite

$$5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ \ldots,$$

on trouvera successivement, pour $\nu = 5$,

$$\mu \equiv \mp\frac{1.2}{4}\frac{1}{2} \equiv \mp\frac{1}{4} \equiv \pm 1, \qquad \mu = 1;$$

pour $\nu = 13$,

$$\mu \equiv \mp\frac{1.2.3.4.5.6}{4}\left(\frac{1}{2^3} - \frac{1}{1.2.3.4} + \frac{1}{1.2.3.4.5.6}\right) \equiv \pm 1, \qquad \mu = 1;$$

pour $\nu = 17$,

$$\mu = 2, \quad \ldots$$

NOTE III.

SUR LA MULTIPLICATION DES FONCTIONS Θ_h, Θ_k, ...

Les principales formules auxquelles nous sommes parvenus dans le précédent Mémoire y sont déduites de la considération des produits de la forme

$$\Theta_h \Theta_k \Theta_l \ldots.$$

Lorsque, p étant un nombre premier impair, on désigne par

$$\vartheta, \quad \tau$$

des racines primitives des équations

$$x^p = 1, \qquad x^{p-1} = 1$$

et par t une racine primitive de l'équivalence

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

alors la valeur de Θ_h, déterminée par la formule

$$\Theta_h = \vartheta + \tau^h \vartheta t + \tau^{2h} \vartheta t^2 + \ldots + \tau^{(p-2)h} \vartheta t^{p-2},$$

ne varie pas quand on fait croître ou diminuer h d'un multiple de $p-1$; et l'on a : 1° en supposant h divisible par $p-1$,

$$\Theta_h = \Theta_0 = -1;$$

2° en supposant h non divisible par $p-1$,

$$\Theta_h \Theta_{-h} = (-1)^h p.$$

Si, au contraire, en nommant h un diviseur de $p-1$, on pose

$$\varpi = \frac{p-1}{n}, \qquad \rho = \tau^{\varpi}$$

et, de plus,

$$\Theta_h = \vartheta + \rho^h \vartheta t + \rho^{2h} \vartheta t^2 + \ldots + \rho^{(p-2)h} \vartheta t^{p-2}, \tag{1}$$

alors Θ_h sera une fonction des racines primitives

$$\vartheta, \quad \rho$$

des deux équations

$$x^p = 1, \qquad x^n = 1,$$

qui ne variera pas quand on fera croître ou diminuer h d'un multiple de n; et l'on aura : 1° en supposant h divisible par n,

$$\Theta_h = \Theta_0 = -1; \tag{2}$$

2° en supposant h non divisible par n,

$$\Theta_h \Theta_{-h} = (-1)^{\varpi h} p = \Theta_h \Theta_{n-h}. \tag{3}$$

Ajoutons qu'en vertu des principes établis dans la première Note, si l'on multiplie Θ_h par Θ_k, on trouvera

$$\Theta_h \Theta_k = R_{h,k} \Theta_{h+k}, \tag{4}$$

$R_{h,k}$ désignant une fonction qui ne renfermera plus ϑ, mais seulement la racine primitive $\rho = \tau^{\varpi}$ et ses puissances entières. On aura d'ailleurs, lorsque $h + k$ ne sera pas divisible par n,

$$R_{h,k} = S(\rho^{ih+jk}), \tag{5}$$

le signe S s'étendant à toutes les valeurs de i et de j qui, étant comprises dans la suite

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2,$$

vérifient la formule

$$t^i + t^j \equiv 1 \pmod{p}. \tag{6}$$

Soient maintenant

$$h, \quad k, \quad l, \quad \ldots$$

des nombres entiers divers. On trouvera successivement

$$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k},$$
$$\Theta_h\Theta_k\Theta_l = R_{h,k}\Theta_{h+k}\Theta_l = R_{h,k}R_{h+k,l}\Theta_{h+k+l}, \quad \ldots.$$

Donc, si l'on pose généralement

$$\Theta_h\Theta_k\Theta_l\ldots = R_{h,k,l,\ldots}\Theta_{h+k+l+\ldots}, \tag{7}$$

$R_{h,k,l,\ldots}$ sera encore une fonction de ρ déterminée par une équation de la forme

$$R_{h,k,l,\ldots} = R_{h,k}R_{h+k,l}, \quad \ldots.$$

Il est bon d'observer que, si

$$h + k + l + \ldots$$

n'est pas divisible par n, on aura

$$R_{h,k,l,\ldots} = S(\rho^{ih+i'k+i''l+\ldots}), \tag{8}$$

le signe S s'étendant à toutes les valeurs de i, i', i'', ... qui, étant comprises dans la suite

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2,$$

vérifient la condition

$$i + i' + i'' + \ldots \equiv 1 \pmod{p}. \tag{9}$$

Ajoutons qu'en vertu de la formule (7), l'expression

$$R_{h,k,l,\ldots} = \frac{\Theta_h\Theta_k\Theta_l\ldots}{\Theta_{h+k+l+\ldots}}$$

sera, comme le produit

$$\Theta_h\Theta_k\Theta_l\ldots$$

et comme l'expression

$$\Theta_{h+k+l+\ldots} = \theta + \rho^h\rho^k\rho^l\ldots\theta^t + \rho^{2h}\rho^{2k}\rho^{2l}\ldots\theta^{t^2} + \ldots + \rho^{(p-2)h}\rho^{(p-2)k}\rho^{(p-2)l}\ldots\theta^{t^{p-2}},$$

une fonction entière et symétrique de

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots,$$

par conséquent une fonction linéaire des sommes

$$\begin{aligned}
&\rho^h + \rho^k + \rho^l + \ldots,\\
&\rho^{2h} + \rho^{2k} + \rho^{2l} + \ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\rho^{(n-1)h} + \rho^{(n-1)k} + \rho^{(n-1)l} + \ldots,
\end{aligned}$$

dans lesquelles les coefficients seront des nombres entiers.

Les équations (2), (3) et (7) entraînent les diverses formules que nous avons données dans le Mémoire, et particulièrement celles qui changent le quadruple d'un nombre premier p, ou d'une puissance entière de p, et quelquefois ce nombre lui-même en expressions de la forme

$$x^2 + ny^2,$$

n étant un diviseur de $p-1$.

D'abord, si l'on suppose $n = 2$, et par suite $\varpi = \frac{p-1}{2}$, la racine primitive ρ de l'équivalence

$$x^2 \equiv 1$$

sera simplement

$$\rho = -1,$$

et, en posant $h = 1$, on tirera de la formule (3)

$$\Theta_1^2 = (-1)^{\frac{p-1}{2}}p$$

ou, ce qui revient au même,

$$(\theta - \theta^t + \theta^{t^2} - \ldots - \theta^{t^{p-2}})^2 = (-1)^{\frac{p-1}{2}}p. \tag{10}$$

On se trouvera ainsi ramené à la formule (14) de la première Note.

Concevons maintenant que n soit un nombre premier impair. Alors les diverses racines primitives de l'équation

$$x^n = 1 \tag{11}$$

seront

$$\rho, \quad \rho^2, \quad \rho^3, \quad \ldots, \quad \rho^{n-3}, \quad \rho^{n-2}, \quad \rho^{n-1};$$

et si l'on prend successivement pour h les divers exposants de ρ dans

ces racines primitives, c'est-à-dire les divers termes de la progression arithmétique

$$1,\ 2,\ 3,\ \ldots,\ n-3,\ n-2,\ n-1,$$

on obtiendra pour valeurs correspondantes de Θ_h les expressions

$$\Theta_1,\ \Theta_2,\ \Theta_3,\ \ldots,\ \Theta_{n-3},\ \Theta_{n-2},\ \Theta_{n-1},$$

lesquelles, eu égard à l'équation (3), vérifieront la formule

$$\Theta_1\Theta_{n-1}=\Theta_2\Theta_{n-2}=\ldots=\Theta_{\frac{n-1}{2}}\Theta_{\frac{n+1}{2}}=p,$$

par conséquent la suivante :

$$p^{\frac{n-1}{2}}=\Theta_1\Theta_2\Theta_3\ldots\Theta_{n-3}\Theta_{n-2}\Theta_{n-1}. \tag{12}$$

D'ailleurs, les divers termes de la progression arithmétique

$$1,\ 2,\ 3,\ \ldots,\ n-3,\ n-2,\ n-1$$

peuvent être censés représenter les diverses racines de l'équivalence

$$x^{n-1}\equiv 1 \pmod{n}. \tag{13}$$

Il y a plus : si l'on nomme s une racine primitive de cette équivalence, les termes dont il s'agit, abstraction faite de l'ordre dans lequel ils sont rangés, seront équivalents, suivant le module n, aux divers termes de la progression géométrique

$$1,\ s,\ s^2,\ \ldots,\ s^{n-2},$$

et, par suite, la formule (12) donnera

$$p^{\frac{n-1}{2}}=\Theta_1\Theta_s\Theta_{s^2}\ldots\Theta_{s^{n-3}}\Theta_{s^{n-2}}. \tag{14}$$

Observons à présent que l'équivalence (13) se décompose en deux autres dont la première,

$$x^{\frac{n-1}{2}}\equiv 1 \pmod{n},$$

a pour racines les puissances paires de s, savoir

$$1,\ s^2,\ s^4,\ \ldots,\ s^{n-3},$$

tandis que la seconde,

$$x^{\frac{n-1}{2}}\equiv -1 \pmod{n},$$

a pour racines les puissances impaires de s. Donc le produit qui constitue le second membre de l'équation (14) peut être décomposé en deux autres produits de la forme

$$\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}=R_{1,s^2,s^4,\ldots,s^{n-3}}\Theta_{1+s^2+s^4+\ldots+s^{n-3}},$$
$$\Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}}=R_{s,s^3,s^5,\ldots,s^{n-3}}\Theta_{s+s^3+s^5+\ldots+s^{n-2}};$$

et comme on aura

$$1+s^2+s^4+\ldots+s^{n-3}=\frac{s^{n-1}-1}{s^2-1}\equiv 0 \pmod{n},$$
$$s+s^3+s^5+\ldots+s^{n-2}=s\frac{s^{n-1}-1}{s^2-1}\equiv 0 \pmod{n},$$

par conséquent

$$\Theta_{1+s^2+s^4+\ldots+s^{n-3}}=\Theta_0=-1,$$
$$\Theta_{s+s^3+s^5+\ldots+s^{n-2}}=\Theta_0=-1,$$

il est clair que les deux produits

$$\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}},\quad \Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}},$$

se réduiront, le premier, avec $R_{1,s^2,s^4,\ldots,s^{n-3}}$, à une fonction entière et symétrique de

$$\rho,\ \rho^{s^2},\ \rho^{s^4},\ \ldots,\ \rho^{s^{n-3}},$$

le second, avec $R_{s,s^3,s^5,\ldots,s^{n-3}}$, à une fonction semblable de

$$\rho^s,\ \rho^{s^3},\ \rho^{s^5},\ \ldots,\ \rho^{s^{n-2}},$$

les coefficients étant des nombres entiers. D'ailleurs, une fonction entière et symétrique de

$$\rho,\ \rho^{s^2},\ \rho^{s^4},\ \ldots,\ \rho^{s^{n-3}}$$

sera simplement une fonction linéaire des sommes de la forme

$$\rho^m+\rho^{ms^2}+\rho^{ms^4}+\ldots+\rho^{ms^{n-3}},$$

m désignant un entier inférieur à n; et une semblable somme se réduit toujours à

$$\rho+\rho^{s^2}+\rho^{s^4}+\ldots+\rho^{s^{n-3}}$$

ou bien à

$$\rho^{s}+\rho^{s^3}+\rho^{s^5}+\ldots+\rho^{s^{n-2}},$$

selon que m est équivalent, suivant le module n, à une puissance paire ou à une puissance impaire de s. On aura donc, en désignant par c_0, c_1, c_2 des quantités entières,

$$\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}=c_0+c_1(\rho+\rho^{s^2}+\ldots+\rho^{s^{n-3}})+c_2(\rho^s+\rho^{s^3}+\ldots+\rho^{s^{n-2}}),$$

puis on en conclura, en remplaçant ρ par ρ^s,

$$\Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}}=c_0+c_1(\rho^s+\rho^{s^3}+\ldots+\rho^{s^{n-2}})+c_2(\rho+\rho^{s^2}+\ldots+\rho^{s^{n-3}}).$$

D'autre part, les expressions

$$1,\quad \rho,\quad \rho^s,\quad \ldots,\quad \rho^{s^{n-2}},$$

qui coïncident, à l'ordre près, avec les suivantes :

$$1,\quad \rho,\quad \rho^2,\quad \ldots,\quad \rho^{n-1},$$

représentent les diverses racines de l'équation

$$x^n=1$$

et offrent une somme nulle; en sorte qu'on a

$$\rho+\rho^s+\rho^{s^2}+\ldots+\rho^{s^{n-2}}=-1.$$

Ce n'est pas tout; si l'on pose

$$\rho-\rho^s+\rho^{s^2}-\ldots-\rho^{s^{n-2}}=\Delta,$$

on tirera de l'équation (10), en y remplaçant p par n, θ par ρ et t par s,

$$\Delta^2=(-1)^{\frac{n-1}{2}}n. \tag{15}$$

Cela posé, on trouvera

$$\rho+\rho^{s^2}+\ldots+\rho^{s^{n-3}}=-\frac{1-\Delta}{2},$$

$$\rho^s+\rho^{s^3}+\ldots+\rho^{s^{n-2}}=-\frac{1+\Delta}{2}$$

et, par suite,

$$\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}=\frac{1}{2}(A+B\Delta),$$

$$\Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}}=\frac{1}{2}(A-B\Delta),$$

ou, ce qui revient au même,

$$\begin{cases}2\Theta_1\Theta_{s^2}\Theta_{s^4}\ldots\Theta_{s^{n-3}}=A+B\Delta,\\ 2\Theta_s\Theta_{s^3}\Theta_{s^5}\ldots\Theta_{s^{n-2}}=A-B\Delta,\end{cases} \tag{16}$$

les valeurs de A, B étant

$$A=2c_0-c_1-c_2,\qquad B=c_1-c_2; \tag{17}$$

puis on tirera des équations (16), combinées avec les formules (14) et (15),

$$4p^{\frac{n-1}{2}}=A^2-B^2\Delta^2$$

ou, ce qui revient au même,

$$4p^{\frac{n-1}{2}}=A^2-(-1)^{\frac{n-1}{2}}nB^2, \tag{18}$$

les valeurs numériques de A, B étant deux entiers qui, en vertu des formules (17), seront de même espèce, c'est-à-dire tous deux pairs ou tous deux impairs.

Observons encore qu'en vertu de la formule

$$s^{\frac{n-1}{2}}\equiv -1 \pmod{n},$$

l'équation

$$\Theta_h\Theta_{-h}=p$$

pourra s'écrire comme il suit :

$$\Theta_{s^m}\Theta_{s^{m\pm\frac{n-1}{2}}}=p \pmod{n}. \tag{19}$$

D'ailleurs, si l'exposant m est un terme de la suite

$$0,\ 1,\ 2,\ 3,\ \ldots,\ n-2,$$

pour que l'exposant $m \pm \frac{n-1}{2}$ soit lui-même un terme de cette suite, il suffira de réduire le double signe $\pm$ au signe $+$ ou au signe $-$, selon que m sera inférieur ou supérieur à $\frac{n-1}{2}$. Enfin, dans la formule (19), les exposants

$$m,\quad m \pm \frac{n-1}{2}$$

seront évidemment de même espèce, c'est-à-dire tous deux pairs ou tous deux impairs si n est de la forme $4x+1$; tandis qu'ils seront d'espèces différentes si n est de la forme $4x+3$. Donc, si n est de la forme $4x+1$, chacune des expressions

$$\Theta_1\Theta_{g^2}\Theta_{g^4}\ldots\Theta_{g^{n-3}},\quad \Theta_g\Theta_{g^3}\Theta_{g^5}\ldots\Theta_{g^{n-2}}$$

se composera de facteurs qui, multipliés deux à deux l'un par l'autre, fourniront des produits égaux à p. Donc alors, les formules (16) devront se réduire à

$$\Theta_1\Theta_{g^2}\Theta_{g^4}\ldots\Theta_{g^{n-3}} = p^{\frac{n-1}{4}},$$

$$\Theta_g\Theta_{g^3}\Theta_{g^5}\ldots\Theta_{g^{n-2}} = p^{\frac{n-1}{4}}$$

et l'on aura, en conséquence,

$$A = 2p^{\frac{n-1}{4}},\qquad B = 0.$$

Si, au contraire, n est de la forme $4x+3$, alors $\frac{n-1}{2}$ étant pair, l'équation (18) donnera

$$4p^{\frac{n-1}{2}} = A^2 + nB^2 \tag{20}$$

et si, en nommant p^λ la plus haute puissance de p qui divise simultanément A et B, on pose

$$A = p^\lambda x,\qquad B = p^\lambda y,$$

$$\mu = \frac{n-1}{2} - 2\lambda,$$

on verra la formule (20) se réduire à

$$4p^\mu = x^2 + ny^2. \tag{21}$$

Si, pour abréger, on désignait par la notation

$$[1]$$

le produit

$$\Theta_1\Theta_{g^2}\Theta_{g^4}\ldots\Theta_{g^{n-3}}$$

composé des facteurs de la forme Θ_h qui correspondent aux valeurs de h propres à vérifier la formule

$$x^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

et par la notation

$$[-1]$$

le produit

$$\Theta_g\Theta_{g^3}\Theta_{g^5}\ldots\Theta_{g^{n-2}}$$

composé des facteurs de la forme Θ_h qui correspondent aux valeurs de h propres à vérifier la formule

$$x^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

les équations (14), (16) se présenteraient sous les formes

$$p^{\frac{n-1}{2}} = [1][-1],$$

$$2[1] = A + B\Delta,\qquad 2[-1] = A - B\Delta$$

et les deux dernières se réduiraient, lorsque n serait de la forme $4x+1$, aux deux équations

$$[1] = p^{\frac{n-1}{4}},\qquad [-1] = p^{\frac{n-1}{4}}.$$

Concevons maintenant que n soit un nombre composé, en sorte qu'on ait

$$n = \nu\omega$$

et supposons d'abord les facteurs

$$\nu, \quad \omega$$

premiers entre eux. L'un d'eux, ν par exemple, sera nécessairement impair. Si d'ailleurs on nomme ς une racine primitive de l'équation

$$x^p = 1$$

et α une racine primitive de l'équation

$$x^{\omega} = 1,$$

on pourra prendre

$$\rho = \varsigma\alpha;$$

puis, en supposant qu'un nombre entier donné h soit équivalent à i suivant le module ν, et j suivant le module ω, on trouvera

$$\rho^h = \varsigma^i \alpha^j.$$

Par suite, l'équation (1) donnera

$$\Theta_h = 0 + \varsigma^i \alpha^j 0^t + \varsigma^{2i} \alpha^{2j} 0^t + \ldots + \varsigma^{(p-2)i} \alpha^{(p-2)j} 0^{p-1}. \tag{22}$$

Pour abréger, nous désignerons par

$$\Theta_{i,j}$$

la valeur de Θ_h que fournit l'équation (22). Cela posé, on reconnaîtra sans peine : 1° que la valeur de l'expression

$$\Theta_{i,j},$$

complètement déterminée pour chaque système de valeurs de i et de j, ne varie pas quand on fait croître i d'un multiple de ν ou j d'un multiple de ω; 2° que l'équation

$$\Theta_h = \Theta_{i,j}$$

entraîne la suivante :

$$\Theta_{-h} = \Theta_{-i,-j};$$

3° que les nombres h et i seront de même espèce, c'est-à-dire tous deux pairs ou tous deux impairs si

$$\varpi = \frac{p-1}{\nu\omega}$$

est un nombre impair, puisque, ν étant impair et $p-1$ pair, ϖ ne pourra devenir impair que pour des valeurs paires de ω. De plus, on tirera des formules (2) et (3) : 1° en supposant à la fois i divisible par ν et j par ω,

$$\Theta_{i,j} = \Theta_{0,0} = -1; \tag{23}$$

2° dans la supposition contraire,

$$\Theta_{i,j}\,\Theta_{-i,-j} = (-1)^{\varpi j} p = \Theta_{i,j}\,\Theta_{\nu-i,\omega-j}. \tag{24}$$

Si ω est impair ainsi que ν, alors ϖ étant nécessairement pair, la formule (24) donnera simplement

$$\Theta_{i,j}\,\Theta_{-i,-j} = p. \tag{25}$$

Pour montrer une application de ces nouvelles formules, considérons d'abord le cas où

$$\omega \quad \text{et} \quad \nu$$

seraient deux nombres premiers impairs. Soient, dans ce cas, u une racine primitive de l'équivalence

$$x^{\nu-1} \equiv 1 \pmod{\nu} \tag{26}$$

et a une racine primitive de l'équivalence

$$x^{\omega-1} \equiv 1 \pmod{\omega}. \tag{27}$$

Les diverses racines de l'équivalence (26), en nombre égal à $\nu - 1$, pourront être représentées indifféremment, soit par les divers termes

de la progression arithmétique

$$1,\ 2,\ 3,\ \ldots,\ \nu-2,\ \nu-1,$$

soit par les divers termes de la progression géométrique

$$1,\ u,\ u^2,\ \ldots,\ u^{\nu-3},\ u^{\nu-2},$$

et pareillement les diverses racines de l'équivalence (17), en nombre égal à $\omega-1$, pourront être représentées indifféremment, soit par les divers termes de la progression arithmétique

$$1,\ 2,\ 3,\ \ldots,\ \omega-2,\ \omega-1,$$

soit par les divers termes de la progression géométrique

$$1,\ a,\ a^2,\ \ldots,\ a^{\omega-3},\ a^{\omega-2}.$$

Or, parmi les valeurs de

$$\Theta_h=\Theta_{i,j}$$

que fournira l'équation (22), celles qu'on obtiendra, en supposant h premier à n, ne différeront pas de celles qu'on peut obtenir en prenant pour i une racine quelconque de la formule (26) et pour j une racine quelconque de la formule (27). Donc elles coïncideront avec l'une quelconque de celles que présente le Tableau suivant :

$$(28)\qquad \left\{\begin{array}{llllll} \Theta_{1,1}, & \Theta_{u,1}, & \Theta_{u^2,1}, & \ldots, & \Theta_{u^{\nu-2},1}, \\ \Theta_{1,a}, & \Theta_{u,a}, & \Theta_{u^2,a}, & \ldots, & \Theta_{u^{\nu-2},a}, \\ \Theta_{1,a^2}, & \Theta_{u,a^2}, & \Theta_{u^2,a^2}, & \ldots, & \Theta_{u^{\nu-2},a^2}, \\ \ldots\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots\ldots\ldots, \\ \Theta_{1,a^{\omega-2}}, & \Theta_{u,a^{\omega-2}}, & \Theta_{u^2,a^{\omega-2}}, & \ldots, & \Theta_{u^{\nu-2},a^{\omega-2}}, \end{array}\right.$$

et leur nombre N, déterminé par la formule

$$N=(\nu-1)(\omega-1),$$

ne sera autre chose que le nombre des termes de la suite

$$1,\ 2,\ 3,\ \ldots,\ n-1$$

inférieurs à

$$n=\omega\nu,$$

mais premiers à n. D'ailleurs, l'équation (7), combinée avec la formule

$$\Theta_{h+k+l+\ldots}=-1$$

et réduite ainsi à la forme

$$\Theta_h\Theta_k\Theta_l\ldots=-R_{h,k,l,\ldots},$$

fournira pour valeur du produit

$$\Theta_h\Theta_k\Theta_l\ldots$$

une fonction entière et symétrique de

$$\rho^h,\ \rho^k,\ \rho^l,\ \ldots,$$

par conséquent une fonction entière et symétrique, non seulement de

$$\varsigma^h,\ \varsigma^k,\ \varsigma^l,\ \ldots,$$

mais encore de

$$\alpha^h,\ \alpha^k,\ \alpha^l,\ \ldots$$

si la somme

$$h+k+l+\ldots$$

est divisible par

$$n=\omega\nu,$$

c'est-à-dire, en d'autres termes, si cette somme est divisible à la fois par ν et par ω. Or cette condition sera évidemment remplie si l'on fait coïncider

$$\Theta_h,\ \Theta_k,\ \Theta_l,\ \ldots$$

avec celles des expressions de la forme

$$\Theta_{i,j}$$

qui, dans le Tableau (28), offrent pour premier indice une puissance paire de u et pour second indice une puissance paire de a, puisqu'alors la somme

$$h+k+l+\ldots$$

sera équivalente, suivant le module ν, au produit

$$\frac{\omega-1}{2}(1+u^2+\ldots+u^{\nu-2})=\frac{\omega-1}{2}\,\frac{u^{\nu-1}-1}{u^2-1}\equiv 0$$

et, suivant le module ω, au produit

$$\frac{\nu-1}{2}(1+\alpha^2+\ldots+\alpha^{\omega-2})=\frac{\nu-1}{2}\,\frac{\alpha^{\omega-1}-1}{\alpha^2-1}\equiv 0.$$

D'autre part, en supposant

$$\Theta_h=\Theta_{i,j}$$

et, par conséquent,

$$i\equiv h \pmod{\nu}, \qquad j\equiv h \pmod{\omega},$$

on en conclura

$$\varsigma^h=\varsigma^i, \qquad \alpha^h=\alpha^j.$$

Donc, en vertu des remarques précédentes, le produit

$$(\Theta_{1,1}\Theta_{u^2,1}\ldots\Theta_{u^{\nu-1},1})(\Theta_{1,\alpha^2}\Theta_{u^2,\alpha^2}\ldots\Theta_{u^{\nu-1},\alpha^2})\ldots(\Theta_{1,\alpha^{\omega-1}}\Theta_{u^2,\alpha^{\omega-1}}\ldots\Theta_{u^{\nu-1},\alpha^{\omega-1}})$$

sera en même temps fonction symétrique de

$$\varsigma,\ \varsigma^{u^2},\ \varsigma^{u^4},\ \ldots,\ \varsigma^{u^{\nu-1}}$$

et de

$$\alpha,\ \alpha^{\alpha^2},\ \alpha^{\alpha^4},\ \ldots,\ \alpha^{\alpha^{\omega-1}}.$$

Concevons maintenant que, pour abréger, on désigne par la notation

$$[1,1]$$

le produit dont nous venons de parler, c'est-à-dire, en d'autres termes, le produit des valeurs de Θ_h, correspondant aux valeurs de h, qui, étant premières à n, vérifient les deux équivalences

$$(29)\qquad x^{\frac{\nu-1}{2}}\equiv 1 \pmod{\nu}, \qquad x^{\frac{\omega-1}{2}}\equiv 1 \pmod{\omega}.$$

Désignons de même par

$$[1,-1]$$

le produit des valeurs de Θ_h, correspondant aux valeurs de h, qui

vérifient les deux équivalences

$$(30)\qquad x^{\frac{\nu-1}{2}}\equiv 1 \pmod{\nu}, \qquad x^{\frac{\omega-1}{2}}\equiv -1 \pmod{\omega};$$

par

$$[-1,1]$$

le produit des valeurs de Θ_h, correspondant aux valeurs de h, qui vérifient les deux équivalences

$$(31)\qquad x^{\frac{\nu-1}{2}}\equiv -1 \pmod{\nu}, \qquad x^{\frac{\omega-1}{2}}\equiv 1 \pmod{\omega};$$

enfin par

$$[-1,-1]$$

le produit des valeurs de Θ_h, correspondant aux valeurs de h, qui vérifient les équivalences

$$(32)\qquad x^{\frac{\nu-1}{2}}\equiv -1 \pmod{\nu}, \qquad x^{\frac{\omega-1}{2}}\equiv -1 \pmod{\omega};$$

on aura

$$(33)\quad [1,1] = (\Theta_{1,1}\Theta_{u^2,1}\ldots\Theta_{u^{\nu-2},1})(\Theta_{1,\alpha^2}\Theta_{u^2,\alpha^2}\ldots\Theta_{u^{\nu-2},\alpha^2})\ldots(\Theta_{1,\alpha^{\omega-2}}\Theta_{u^2,\alpha^{\omega-2}}\ldots\Theta_{u^{\nu-2},\alpha^{\omega-2}}),$$

$$(34)\quad [1,-1] = (\Theta_{1,\alpha}\Theta_{u^2,\alpha}\ldots\Theta_{u^{\nu-2},\alpha})(\Theta_{1,\alpha^3}\Theta_{u^2,\alpha^3}\ldots\Theta_{u^{\nu-2},\alpha^3})\ldots(\Theta_{1,\alpha^{\omega-1}}\Theta_{u^2,\alpha^{\omega-1}}\ldots\Theta_{u^{\nu-2},\alpha^{\omega-1}}),$$

$$(35)\quad [-1,1] = (\Theta_{u,1}\Theta_{u^3,1}\ldots\Theta_{u^{\nu-1},1})(\Theta_{u,\alpha^2}\Theta_{u^3,\alpha^2}\ldots\Theta_{u^{\nu-1},\alpha^2})\ldots(\Theta_{u,\alpha^{\omega-2}}\Theta_{u^3,\alpha^{\omega-2}}\ldots\Theta_{u^{\nu-1},\alpha^{\omega-2}}),$$

$$(36)\quad [-1,-1] = (\Theta_{u,\alpha}\Theta_{u^3,\alpha}\ldots\Theta_{u^{\nu-1},\alpha})(\Theta_{u,\alpha^3}\Theta_{u^3,\alpha^3}\ldots\Theta_{u^{\nu-1},\alpha^3})\ldots(\Theta_{u,\alpha^{\omega-1}}\Theta_{u^3,\alpha^{\omega-1}}\ldots\Theta_{u^{\nu-1},\alpha^{\omega-1}}),$$

et, d'après ce qu'on a dit ci-dessus, le produit

$$[1,1]$$

sera une fonction symétrique, non seulement de

$$\varsigma,\ \varsigma^{u^2},\ \varsigma^{u^4},\ \ldots,\ \varsigma^{u^{\nu-1}},$$

mais encore de

$$\alpha,\ \alpha^{\alpha^2},\ \alpha^{\alpha^4},\ \ldots,\ \alpha^{\alpha^{\omega-1}}.$$

Pareillement, on reconnaîtra que le produit

$$[1,-1]$$

est fonction symétrique, non seulement de

$$\varsigma,\ \varsigma^{u^2},\ \varsigma^{u^4},\ \ldots,\ \varsigma^{u^{\nu-3}},$$

mais encore de

$$\alpha^a,\ \alpha^{a^3},\ \alpha^{a^5},\ \alpha^{a^{\nu-2}};$$

que le produit

$$[-1, 1]$$

est fonction symétrique, non seulement de

$$\varsigma^u,\ \varsigma^{u^3},\ \varsigma^{u^5},\ \ldots,\ \varsigma^{u^{\nu-2}},$$

mais encore de

$$\alpha,\ \alpha^{a^2},\ \alpha^{a^4},\ \ldots,\ \alpha^{a^{\nu-1}};$$

enfin que le produit

$$[-1, -1]$$

est fonction symétrique, non seulement de

$$\varsigma^u,\ \varsigma^{u^3},\ \ldots,\ \varsigma^{u^{\nu-2}},$$

mais encore de

$$\alpha^a,\ \alpha^{a^3},\ \ldots,\ \alpha^{a^{\omega-2}}.$$

D'autre part, comme on aura

$$u^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}, \qquad \alpha^{\frac{\omega-1}{2}} \equiv -1 \pmod{\omega},$$

l'équation (25) pourra s'écrire comme il suit :

$$\Theta_{u^m, \alpha^{m'}} \Theta_{u^{m+\frac{\nu-1}{2}}, \alpha^{m'+\frac{\omega-1}{2}}} = p, \tag{37}$$

et il est clair que, dans cette équation, les exposants

$$m, \quad m \pm \frac{\nu-1}{2}$$

seront de même espèce, c'est-à-dire tous deux pairs ou tous deux impairs, si ν est de la forme $4x+1$, mais d'espèces différentes si ν est de la forme $4x+3$. Pareillement, les exposants

$$m', \quad m' \pm \frac{\omega-1}{2}$$

seront de même espèce si ω est de la forme $4x+1$ et d'espèces différentes si ω est de la forme $4x+3$. Cela posé, si les nombres

$$\nu, \quad \omega$$

sont tous deux de la forme $4x+1$, chacun des produits

$$[1, 1], \quad [1, -1], \quad [-1, 1], \quad [-1, -1],$$

composé de facteurs de la forme $\Theta_{i,j}$, en nombre égal à $\frac{N}{4}$, se réduira évidemment, en vertu de l'équation (37), à

$$p^{\frac{N}{8}}.$$

On aura donc alors les formules

$$[1, 1] = p^{\frac{N}{8}}, \qquad [1, -1] = p^{\frac{N}{8}}, \qquad [-1, 1] = p^{\frac{N}{8}}, \qquad [-1, -1] = p^{\frac{N}{8}}$$

qui entraîneront l'équation

$$p^{\frac{N}{2}} = [1, 1][1, -1][-1, 1][-1, -1], \tag{38}$$

analogue à la formule (14).

Si les nombres ν, ω sont tous deux de la forme $4x+3$, alors on tirera des formules (33) et (36) ou (34) et (35), jointes à la formule (37),

$$[1, 1][-1, -1] = p^{\frac{N}{4}}, \qquad [1, -1][-1, 1] = p^{\frac{N}{4}}, \tag{39}$$

et l'on déduira encore de ces dernières l'équation (38).

Enfin, si des nombres ν, ω, un seul, ν par exemple, est de la forme $4x+1$, l'autre, ω, étant de la forme $4x+3$, alors on tirera des formules (33) et (34) ou (35) et (36), jointes à la formule (37),

$$[1, 1][1, -1] = p^{\frac{N}{4}}, \qquad [-1, 1][-1, -1] = p^{\frac{N}{4}}, \tag{40}$$

et l'on déduira encore de ces dernières l'équation (38).

L'équation (38), analogue à (14), conduit aussi à des conclusions

du même genre lorsque les nombres

$$\nu, \quad \omega$$

ne sont pas tous deux de la forme $4x+1$; et d'abord, supposons qu'ils soient tous deux de la forme $4x+3$. Alors, dans le second membre de l'équation (38), le produit

$$[1, 1][1, -1]$$

représentera une fonction symétrique, non seulement de

$$\varsigma, \quad \varsigma^{n^2}, \quad \ldots, \quad \varsigma^{n^{\nu-1}},$$

mais encore de

$$\alpha, \quad \alpha^n, \quad \alpha^{n^2}, \quad \ldots, \quad \alpha^{n^{\omega-1}}, \quad \alpha^{n^{\omega-1}};$$

par conséquent, une fonction linéaire, non seulement des sommes

$$\varsigma+\varsigma^{n^2}+\ldots+\varsigma^{n^{\nu-1}}, \quad \varsigma^n+\varsigma^{n^3}+\ldots+\varsigma^{n^{\nu-2}},$$

mais encore de la somme

$$\alpha+\alpha^n+\alpha^{n^2}+\alpha^{n^3}+\ldots+\alpha^{n^{\omega-1}}+\alpha^{n^{\omega-2}}.$$

Or, comme cette dernière somme, qui comprend toutes les racines de l'équation

$$x^{\omega}=1,$$

à l'exception de la racine 1, se réduira simplement à -1, il est clair qu'en supposant ν et ω tous deux de la forme $4x+3$ et désignant par c_0, c_1, c_2 des quantités entières, on trouvera

$$[1, 1][1, -1]=c_0+c_1(\varsigma+\varsigma^{n^2}+\ldots+\varsigma^{n^{\nu-1}})+c_2(\varsigma^n+\varsigma^{n^3}+\ldots+\varsigma^{n^{\nu-2}}),$$

puis, en remplaçant ς par ς^n,

$$[-1, 1][-1, -1]=c_0+c_1(\varsigma^n+\varsigma^{n^3}+\ldots+\varsigma^{n^{\nu-2}})+c_2(\varsigma+\varsigma^{n^2}+\ldots+\varsigma^{n^{\nu-1}}).$$

On pourra d'ailleurs présenter les deux équations qui précèdent sous une forme analogue à celle des équations (16) et alors, en les multipliant l'une par l'autre, on obtiendra, au lieu de la formule (20), la

suivante :

$$4p^{\frac{N}{2}}=A^2+\nu B^2, \tag{41}$$

les valeurs entières de A, B étant toujours déterminées par les formules (17). Enfin si, en nommant p^λ la plus haute puissance de p qui divise simultanément A et B, on pose

$$A=p^\lambda x, \qquad B=p^\lambda y,$$
$$\mu=\frac{N}{2}-2\lambda,$$

on verra la formule (41) se réduire à

$$4p^\mu=x^2+\nu y^2. \tag{42}$$

On pourrait encore, dans l'hypothèse admise, c'est-à-dire lorsque ν, ω sont tous deux de la forme $4x+3$, décomposer le second membre de la formule (38) en deux facteurs égaux, non plus aux deux produits

$$[1, 1][1, -1], \quad [-1, 1][-1, -1],$$

mais aux deux produits

$$[1, 1][-1, 1], \quad [1, -1][-1, -1],$$

et alors on se trouverait conduit, non plus à la formule (42), mais à une équation de la forme

$$4p^\mu=x^2+\omega y^2. \tag{43}$$

Considérons maintenant le cas où ν serait de la forme $4x+1$, ω étant de la forme $4x+3$. Alors la formule (41) se trouverait remplacée par les formules (40), en sorte qu'on aurait simplement

$$A=2p^{\frac{N}{2}}, \qquad B=0;$$

et, en conséquence, la formule (42) cesserait de fournir la transformation d'une puissance entière de p, multipliée par 4, en un binome

de la forme

$$x^2 + \nu y^2.$$

Mais la formule (43) continuerait de subsister et l'on pourrait au reste déduire une nouvelle formule de la décomposition du second membre de l'équation (38) en deux facteurs de la forme

$$[1, 1][-1, -1], \quad [1, -1][-1, 1].$$

Alors, en effet, le produit

$$[1, 1][-1, -1]$$

serait une fonction entière et symétrique, non seulement de

$$\varsigma, \quad \varsigma^{a^2}, \quad \ldots, \quad \varsigma^{a^{\nu-2}}$$

et de

$$\varsigma^a, \quad \varsigma^{a^3}, \quad \ldots, \quad \varsigma^{a^{\nu-2}},$$

mais encore de

$$\alpha, \quad \alpha^{a^2}, \quad \ldots, \quad \alpha^{a^{\nu-2}}$$

et de

$$\alpha^a, \quad \alpha^{a^3}, \quad \ldots, \quad \alpha^{a^{\nu-2}},$$

qui ne serait point altérée quand on y remplacerait simultanément

$$\varsigma \text{ par } \varsigma^a, \qquad \alpha \text{ par } \alpha^a,$$

les coefficients numériques des différents termes étant d'ailleurs des nombres entiers. Par suite, le produit

$$[1, 1][-1, -1]$$

se réduirait à une fonction linéaire, non seulement des sommes

$$(\varsigma + \varsigma^{a^2} + \ldots + \varsigma^{a^{\nu-2}}) + (\varsigma^a + \varsigma^{a^3} + \ldots + \varsigma^{a^{\nu-2}}),$$
$$(\alpha + \alpha^{a^2} + \ldots + \alpha^{a^{\nu-2}}) + (\alpha^a + \alpha^{a^3} + \ldots + \alpha^{a^{\nu-2}}),$$

mais encore des sommes

$$(\alpha + \alpha^{a^2} + \ldots + \alpha^{a^{\nu-2}})(\varsigma + \varsigma^{a^2} + \ldots + \varsigma^{a^{\nu-2}})$$
$$+ (\alpha^a + \alpha^{a^3} + \ldots + \alpha^{a^{\nu-2}})(\varsigma^a + \varsigma^{a^3} + \ldots + \varsigma^{a^{\nu-2}}),$$
$$(\alpha^a + \alpha^{a^3} + \ldots + \alpha^{a^{\nu-2}})(\varsigma + \varsigma^{a^2} + \ldots + \varsigma^{a^{\nu-2}})$$
$$+ (\alpha + \alpha^{a^2} + \ldots + \alpha^{a^{\nu-2}})(\varsigma^a + \varsigma^{a^3} + \ldots + \varsigma^{a^{\nu-2}}).$$

Or, des quatre sommes qui précèdent, les deux premières se réduiront à -1, puisqu'on aura généralement

$$\varsigma + \varsigma^a + \varsigma^{a^2} + \ldots + \varsigma^{a^{\nu-2}} + \varsigma^{a^{\nu-1}} = -1,$$
$$\alpha + \alpha^a + \alpha^{a^2} + \ldots + \alpha^{a^{\nu-2}} + \alpha^{a^{\nu-1}} = -1,$$

et, quant aux deux dernières, comme, en posant pour abréger

$$\varsigma - \varsigma^a + \varsigma^{a^2} - \ldots + \varsigma^{a^{\nu-2}} - \varsigma^{a^{\nu-1}} = \Delta,$$
$$\alpha - \alpha^a + \alpha^{a^2} - \ldots + \alpha^{a^{\nu-2}} - \alpha^{a^{\nu-1}} = \Delta',$$

on trouve

$$\varsigma + \varsigma^{a^2} + \ldots + \varsigma^{a^{\nu-2}} = -\frac{1-\Delta}{2}, \qquad \varsigma^a + \varsigma^{a^3} + \ldots + \varsigma^{a^{\nu-1}} = -\frac{1+\Delta}{2},$$
$$\alpha + \alpha^{a^2} + \ldots + \alpha^{a^{\nu-2}} = -\frac{1-\Delta'}{2}, \qquad \alpha^a + \alpha^{a^3} + \ldots + \alpha^{a^{\nu-1}} = -\frac{1+\Delta'}{2},$$

elles pourront être représentées par les expressions

$$\frac{1-\Delta'}{2}\frac{1+\Delta}{2} + \frac{1+\Delta'}{2}\frac{1-\Delta}{2} = \frac{1+\Delta\Delta'}{2},$$
$$\frac{1-\Delta'}{2}\frac{1-\Delta}{2} + \frac{1+\Delta'}{2}\frac{1+\Delta}{2} = \frac{1-\Delta\Delta'}{2}.$$

Donc, dans l'hypothèse admise, le produit

$$[1, 1][-1, -1]$$

se réduira simplement à une fonction entière et linéaire des rapports

$$\frac{1+\Delta\Delta'}{2}, \qquad \frac{1-\Delta\Delta'}{2},$$

les coefficients étant des nombres entiers; en sorte qu'on aura

$$[1, 1][-1, -1] = c_0 + c_1\frac{1+\Delta\Delta'}{2} + c_2\frac{1-\Delta\Delta'}{2},$$

c_0, c_1, c_2 désignant des quantités entières. Si l'on pose maintenant

$$A = 2c_0 + c_1 + c_2, \qquad B = c_1 - c_2,$$

la formule précédente donnera

$$2[1, 1][-1, -1] = A + B\Delta\Delta', \tag{44}$$

les valeurs numériques de A, B étant deux entiers de même espèce, c'est-à-dire tous deux pairs ou tous deux impairs. D'autre part, si, dans la formule (44), on remplace ς par ς^{α}, sans remplacer en même temps α par α^{α}, alors, au lieu de cette formule, on obtiendra la suivante :

$$2[1, -1][-1, 1] = A - B\Delta\Delta', \tag{45}$$

puis on tirera des formules (44), (45), combinées avec l'équation (38),

$$4p^{\frac{N}{2}} = A^2 - B^2\Delta^2\Delta'^2. \tag{46}$$

De plus on aura, en vertu de l'équation (10),

$$(\varsigma - \varsigma^{\alpha} + \varsigma^{\alpha^2} - \ldots + \varsigma^{\alpha^{\nu-2}} - \varsigma^{\alpha^{\nu-1}})^2 = (-1)^{\frac{\nu-1}{2}}\nu,$$

$$(\alpha - \alpha^{\alpha} + \alpha^{\alpha^2} - \ldots + \alpha^{\alpha^{\omega-2}} - \alpha^{\alpha^{\omega-1}})^2 = (-1)^{\frac{\omega-1}{2}}\omega$$

ou, ce qui revient au même,

$$\Delta^2 = (-1)^{\frac{\nu-1}{2}}\nu, \qquad \Delta'^2 = (-1)^{\frac{\omega-1}{2}}\omega.$$

Donc, lorsque ν sera, comme on le suppose, de la forme $4x+1$, ω étant de la forme $4x+3$, on trouvera

$$\Delta^2 = \nu, \qquad \Delta'^2 = -\omega$$

et la formule (46) donnera

$$4p^{\frac{N}{2}} = A^2 + \nu\omega B^2. \tag{47}$$

Enfin, si l'on nomme p^{λ} la plus haute puissance de p qui divise simultanément A et B, alors, en posant

$$A = p^{\lambda}x, \qquad B = p^{\lambda}y,$$

$$\mu = \frac{N}{2} - 2\lambda,$$

on verra la formule (47) se réduire à

$$4p^{\mu} = x^2 + \nu\omega y^2 \tag{48}$$

ou, ce qui revient au même, à l'équation

$$4p^{\mu} = x^2 + ny^2, \tag{49}$$

la valeur de n étant

$$n = \nu\omega.$$

Il est bon d'observer que, le nombre ν étant supposé de la forme $4x+1$ et le nombre ω de la forme $4x+3$, le nombre n sera de la forme $4x+3$, dans l'équation (49) aussi bien que dans l'équation (21). On peut ajouter que n, étant le produit de deux facteurs premiers impairs, ν, ω, ne pourra être de la forme $4x+3$ que dans le cas où un seul des facteurs sera de cette forme. Effectivement, si ν et ω étaient tous deux de la forme $4x+3$ ou tous deux de la forme $4x+1$, leur produit

$$n = \nu\omega$$

serait évidemment de la forme $4x+1$.

Les diverses formules qui précèdent s'accordent avec celles que nous avons établies dans le premier et les deux derniers paragraphes du Mémoire. Elles peuvent d'ailleurs être facilement étendues au cas où n serait le produit de plusieurs nombres premiers impairs

$$\nu, \quad \nu', \quad \nu'', \quad \ldots$$

Ainsi, en particulier, supposons

$$n = \nu\nu'\nu'',$$

ν, ν', ν'' désignant trois nombres premiers impairs, et représentons par

$$[1, 1, 1]$$

le produit des diverses valeurs de Θ_h correspondant aux valeurs de h

qui, étant premières à n, vérifient les équivalences

$$(50)\quad x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}, \quad x^{\frac{\nu'-1}{2}} \equiv 1 \pmod{\nu'}, \quad x^{\frac{\nu''-1}{2}} \equiv 1 \pmod{\nu''}.$$

Soit encore

$$[-1, -1, -1]$$

le produit des diverses valeurs de Θ_h correspondant aux valeurs de h qui, étant premières à n, vérifient les équivalences

$$(51)\quad x^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}, \quad x^{\frac{\nu'-1}{2}} \equiv -1 \pmod{\nu'}, \quad x^{\frac{\nu''-1}{2}} \equiv -1 \pmod{\nu''},$$

et concevons que l'on emploie, dans un sens analogue, chacune des huit expressions comprises dans la formule

$$[\pm 1, \pm 1, \pm 1],$$

de sorte qu'à un changement de signe opéré dans le dernier membre de la première, ou de la seconde, ou de la troisième des formules (50), doive toujours correspondre un changement du signe qui affecte la première, la seconde ou la troisième unité dans la notation

$$[1, 1, 1].$$

Soient d'ailleurs respectivement

$$u, \quad u', \quad u''$$

des racines primitives des trois équivalences

$$x^{\nu-1} \equiv 1 \pmod{\nu}, \quad x^{\nu'-1} \equiv 1 \pmod{\nu'}, \quad x^{\nu''-1} \equiv 1 \pmod{\nu''}$$

et

$$\varsigma, \quad \varsigma', \quad \varsigma''$$

des racines primitives des trois équations

$$x^{\nu} = 1, \quad x^{\nu'} = 1, \quad x^{\nu''} = 1.$$

Enfin posons

$$(52)\quad \varsigma - \varsigma^{n} + \varsigma^{n^2} - \ldots + \varsigma^{n^{\nu-2}} - \varsigma^{n^{\nu-1}} = \Delta$$

et nommons Δ', Δ'' ce que devient Δ quand on remplace ν par ν' ou ν''. Chacune des huit expressions

$$(53)\quad \begin{cases} [1, 1, 1], & [1, -1, -1], & [-1, 1, -1], & [-1, -1, 1], \\ [-1, -1, -1], & [-1, 1, 1], & [1, -1, 1], & [1, 1, -1] \end{cases}$$

sera une fonction entière et symétrique, non seulement de

$$\varsigma, \quad \varsigma^{n^2}, \quad \ldots, \quad \varsigma^{n^{\nu-2}}$$

ou de

$$\varsigma^{n}, \quad \varsigma^{n^3}, \quad \ldots, \quad \varsigma^{n^{\nu-1}},$$

mais encore de

$$\varsigma', \quad \varsigma'^{n^2}, \quad \ldots, \quad \varsigma'^{n^{\nu-2}}$$

ou de

$$\varsigma'^{n}, \quad \varsigma'^{n^3}, \quad \ldots, \quad \varsigma'^{n^{\nu-1}}$$

et aussi de

$$\varsigma'', \quad \varsigma''^{n^2}, \quad \ldots, \quad \varsigma''^{n^{\nu''-2}}$$

ou de

$$\varsigma''^{n}, \quad \varsigma''^{n^3}, \quad \ldots, \quad \varsigma''^{n^{\nu''-1}},$$

les coefficients numériques étant des nombres entiers. Par suite, on pourra en dire autant des produits qu'on obtient en multipliant l'une par l'autre deux ou plusieurs des expressions (53), et chacun de ces produits, ainsi que chacune de ces expressions, sera non seulement une fonction linéaire des deux sommes

$$\varsigma + \varsigma^{n^2} + \ldots + \varsigma^{n^{\nu-2}} = -\frac{1-\Delta}{2}, \qquad \varsigma^{n} + \varsigma^{n^3} + \ldots + \varsigma^{n^{\nu-1}} = -\frac{1+\Delta}{2},$$

par conséquent des deux rapports

$$\frac{1-\Delta}{2}, \quad \frac{1+\Delta}{2},$$

mais encore une fonction linéaire des deux rapports

$$\frac{1-\Delta'}{2}, \quad \frac{1+\Delta'}{2}$$

et aussi une fonction linéaire des deux rapports

$$\frac{1-\Delta''}{2}, \quad \frac{1+\Delta''}{2}.$$

Donc chacune des expressions (53), ou chacun de leurs produits, multiplié par $2^3 = 8$, deviendra non seulement une fonction linéaire de

$$1 - \Delta, \quad 1 + \Delta,$$

par conséquent de Δ, mais encore une fonction linéaire de

$$1 - \Delta', \quad 1 + \Delta',$$

par conséquent de Δ', et aussi une fonction linéaire de

$$1 - \Delta'', \quad 1 + \Delta'',$$

par conséquent de Δ'', de manière à offrir généralement huit termes dont l'un sera constant, les sept autres termes étant respectivement proportionnels à

$$\Delta, \quad \Delta', \quad \Delta'', \quad \Delta\Delta', \quad \Delta\Delta'', \quad \Delta'\Delta'', \quad \Delta\Delta'\Delta''$$

et les coefficients numériques étant toujours des nombres entiers. Ajoutons que de la première des expressions (53) on peut déduire successivement les sept autres en y remplaçant séparément ou simultanément

$$\Delta \text{ par } -\Delta, \quad \Delta' \text{ par } -\Delta', \quad \Delta'' \text{ par } -\Delta'',$$

c'est-à-dire en changeant le signe de Δ, ou de Δ', ou de Δ'', au moment où, dans la notation

$$[1, 1, 1],$$

on change le signe qui affecte la première, la deuxième ou la troisième unité. Cela posé, si l'on considère en particulier les deux produits

$$(54) \quad \begin{cases} [1,1,1][1,-1,-1][-1,1,-1][-1,-1,1], \\ [-1,-1,-1][-1,1,1][1,-1,1][1,1,-1], \end{cases}$$

il est clair que chacun d'eux restera invariable, tandis que, des trois différences représentées par

$$\Delta, \quad \Delta', \quad \Delta'',$$

deux seulement changeront de signe et que, pour déduire le second produit du premier, il suffira de changer à la fois le signe de Δ, celui de Δ' et celui de Δ''. Il suit de cette remarque, et de ce qui a été dit plus haut, que les produits (54), multipliés par le nombre $2^3 = 8$, ne devront renfermer aucun terme proportionnel à une seule des différences

$$\Delta, \quad \Delta', \quad \Delta''$$

ou à l'un des produits partiels

$$\Delta\Delta', \quad \Delta\Delta'', \quad \Delta'\Delta''$$

et devront se réduire à deux binomes de la forme

$$a + b\Delta\Delta'\Delta'',$$
$$a - b\Delta\Delta'\Delta'',$$

a, b désignant deux quantités entières. On aura donc

$$(55) \quad \begin{cases} 8[1,1,1][1,-1,-1][-1,1,-1][-1,-1,1] = a + b\Delta\Delta'\Delta'', \\ 8[-1,-1,-1][-1,1,1][1,-1,1][1,1,-1] = a - b\Delta\Delta'\Delta''. \end{cases}$$

D'autre part, chacun des produits (54), pouvant être considéré comme une fonction entière des rapports

$$\frac{1-\Delta}{2}, \quad \frac{1+\Delta}{2}, \quad \frac{1-\Delta'}{2}, \quad \frac{1+\Delta'}{2}, \quad \frac{1-\Delta''}{2}, \quad \frac{1+\Delta''}{2},$$

dans laquelle les coefficients numériques sont entiers, se réduira, au signe près, à un nombre entier si l'on y remplace chacune des différences

$$\Delta, \quad \Delta', \quad \Delta''$$

par un nombre impair; par exemple, par l'unité. Donc un tel remplacement doit rendre le premier membre et, par suite, le second membre de chacune des équations (55), divisible par 8. Donc les deux binomes

$$a + b, \quad a - b$$

seront divisibles par 8; d'où il suit que leur demi-somme a et leur

demi-différence b seront divisibles par 4 ou de la forme

$$a = 4\mathrm{A}, \qquad b = 4\mathrm{B},$$

A, B étant des quantités entières. Donc les formules (55) donneront

$$(56)\quad \begin{cases} 2[1,1,1][1,-1,-1][-1,1,-1][-1,-1,1] = \mathrm{A} + \mathrm{B}\Delta\Delta'\Delta'', \\ 2[-1,-1,1][-1,1,1][1,-1,1][1,1,-1] \quad = \mathrm{A} - \mathrm{B}\Delta\Delta'\Delta'', \end{cases}$$

les valeurs numériques de A, B étant des nombres entiers.

Observons à présent que -1 sera une racine de l'équivalence

$$(57)\qquad x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}$$

si, ν étant de la forme $4x+1$, le rapport $\frac{\nu-1}{2}$ est un nombre pair et sera, au contraire, une racine de l'équivalence

$$(58)\qquad x^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}$$

si, ν étant de la forme $4x+3$, le rapport $\frac{\nu-1}{2}$ est un nombre impair. Donc, par suite, des deux quantités

$$h, \quad -h,$$

l'une sera racine de l'équivalence (57) et l'autre racine de l'équivalence (58) si ν est de la forme $4x+1$; mais toutes deux seront racines d'une seule de ces équivalences si ν est de la forme $4x+3$. Pareillement, les deux quantités $+h$, $-h$ seront racines, l'une de l'équivalence

$$(59)\qquad x^{\frac{\nu'-1}{2}} \equiv 1 \pmod{\nu'},$$

l'autre de l'équivalence

$$(60)\qquad x^{\frac{\nu'-1}{2}} \equiv -1 \pmod{\nu'}$$

si ν' est de la forme $4x+1$; et toutes deux, au contraire, seront racines

d'une seule de ces équivalences si ν est de la forme $4x+3$. Enfin, les deux quantités $+h$, $-h$ seront racines, l'une de l'équivalence

$$(61)\qquad x^{\frac{\nu''-1}{2}} \equiv 1 \pmod{\nu''},$$

l'autre de l'équivalence

$$(62)\qquad x^{\frac{\nu''-1}{2}} \equiv 1 \pmod{\nu''}$$

si ν'' est de la forme $4x+1$; et toutes deux, au contraire, seront racines d'une seule de ces équivalences si ν'' est de la forme $4x+3$. Cela posé, il est clair que les deux monômes

$$\Theta_h, \quad \Theta_{-h}$$

appartiendront, comme facteurs, à une seule des expressions (53) si les nombres

$$\nu, \quad \nu', \quad \nu''$$

sont tous trois de la forme $4x+1$; et, comme le nombre des facteurs compris dans chacune de ces expressions est égal au huitième du produit

$$\mathrm{N} = (\nu-1)(\nu'-1)(\nu''-1),$$

qui représente le nombre des termes premiers à $n = \nu\nu'\nu''$ dans la suite

$$1, \quad 2, \quad 3, \quad \ldots, \quad n-1,$$

on aura évidemment, dans le cas dont il s'agit, eu égard à la formule (3),

$$(63)\quad \begin{cases} [1,1,1] \quad = p^{\frac{\mathrm{N}}{16}}, & [1,-1,-1] = p^{\frac{\mathrm{N}}{16}}, & [-1,1,-1] = p^{\frac{\mathrm{N}}{16}}, & [-1,-1,1] = p^{\frac{\mathrm{N}}{16}}, \\ [-1,-1,-1] = p^{\frac{\mathrm{N}}{16}}, & [-1,1,1] \quad = p^{\frac{\mathrm{N}}{16}}, & [1,-1,1] \quad = p^{\frac{\mathrm{N}}{16}}, & [1,1,-1] \quad = p^{\frac{\mathrm{N}}{16}}. \end{cases}$$

Si des nombres

$$\nu, \quad \nu', \quad \nu''$$

deux seulement, par exemple ν, ν', sont de la forme $4x+1$, le troisième, ν'', étant de la forme $4x+3$, alors les monômes

$$\Theta_h, \quad \Theta_{-h}$$

appartiendront comme facteurs, non plus à une seule, mais à deux des expressions (53) qui ne diffèrent entre elles que par le signe de la troisième unité, et l'on trouvera, par suite,

$$(64)\quad \begin{cases} [1,1,1][1,1,-1] = p^{\frac{N}{8}}, & [-1,-1,-1][-1,-1,1] = p^{\frac{N}{8}}, \\ [1,-1,1][1,-1,-1] = p^{\frac{N}{8}}, & [-1,1,1][1,-1,1] = p^{\frac{N}{8}}. \end{cases}$$

Pareillement, si des nombres

$$\nu,\quad \nu',\quad \nu''$$

un seul, ν par exemple, est de la forme $4x+1$, les deux autres, ν', ν'', étant de la forme $4x+3$, les monômes

$$\Theta_{\Lambda},\quad \Theta_{-\Lambda}$$

appartiendront, comme facteurs, à deux des expressions (53) qui ne différeront entre elles que par les signes de la deuxième et de la troisième unité. On aura donc, par suite,

$$(65)\quad \begin{cases} [1,1,1][1,-1,-1] = p^{\frac{N}{8}}, & [-1,1,-1][-1,-1,1] = p^{\frac{N}{8}}, \\ [1,-1,1][1,1,-1] = p^{\frac{N}{8}}, & [-1,1,1][-1,-1,-1] = p^{\frac{N}{8}}. \end{cases}$$

Enfin, si les trois nombres

$$\nu,\quad \nu',\quad \nu''$$

sont tous trois de la forme $4x+3$, les monômes

$$\Theta_{\Lambda},\quad \Theta_{-\Lambda}$$

appartiendront, comme facteurs, à deux des expressions (53) qui différeront entre elles par les signes des trois unités, et l'on aura, par suite,

$$(66)\quad \begin{cases} [1,1,1][-1,-1,-1] = p^{\frac{N}{8}}, & [1,-1,-1][-1,1,1] = p^{\frac{N}{8}}, \\ [-1,1,-1][1,-1,1] = p^{\frac{N}{8}}, & [-1,-1,1][1,1,-1] = p^{\frac{N}{8}}. \end{cases}$$

Il est d'ailleurs évident que, dans tous les cas, les formules (63), ou (64), ou (65), ou (66), entraînent la suivante :

$$(67)\quad p^{\frac{N}{2}} = [1,1,1][1,-1,-1][-1,1,-1][-1,-1,1][-1,-1,-1][-1,1,1][1,-1,1][1,1,-1].$$

Comme, dans le premier et le troisième cas, on tire des formules (63) ou (64)

$$(68)\quad \begin{cases} [1,1,1][1,-1,-1][-1,1,-1][-1,-1,1] = p^{\frac{N}{4}}, \\ [-1,-1,-1][-1,1,1][1,-1,1][1,1,-1] = p^{\frac{N}{4}}, \end{cases}$$

il est clair qu'alors on doit avoir, dans les formules (56),

$$A = 2p^{\frac{N}{4}},\qquad B = 0.$$

Au contraire, dans le deuxième et le quatrième cas, on tire de l'équation (67), jointe aux formules (56),

$$(69)\qquad 4p^{\frac{N}{2}} = A^2 - B^2\Delta^2\Delta'^2\Delta''^2.$$

On trouve d'ailleurs, dans le deuxième cas,

$$\Delta^2 = \nu,\qquad \Delta'^2 = \nu',\qquad \Delta''^2 = -\nu'',$$

et, dans le quatrième,

$$\Delta^2 = -\nu,\qquad \Delta'^2 = -\nu',\qquad \Delta''^2 = -\nu''.$$

On aura donc, dans l'un et l'autre cas,

$$\Delta^2\Delta'^2\Delta''^2 = -\nu\nu'\nu'' = -n;$$

et, en conséquence, la formule (69) donnera

$$(70)\qquad 4p^{\frac{N}{2}} = A^2 + nB^2.$$

D'ailleurs, parmi les trois facteurs premiers de n, ceux qui sont de la forme $4x+3$ seront en nombre impair dans le deuxième et le qua-

trième cas, et en nombre pair dans le premier et le troisième cas. Donc le deuxième et le quatrième cas, auxquels se rapporte l'équation (70), seront précisément ceux où le nombre n est de la forme $4x+3$.

Au reste, des raisonnements, semblables à ceux qui précèdent, s'appliqueraient aux cas où le nombre entier n serait le produit de quatre, cinq, ... facteurs premiers impairs

$$\nu,\ \nu',\ \nu'',\ \nu''',\ \ldots;$$

et alors, en désignant par N le nombre des termes premiers à n qui seront compris dans la suite

$$1,\ 2,\ 3,\ \ldots,\ n-1,$$

c'est-à-dire en posant

$$N=(\nu-1)(\nu'-1)(\nu''-1)(\nu'''-1)\ldots,$$

on se trouvera de nouveau conduit à la formule (70), A, B étant deux quantités entières dont la seconde sera nulle, si n est de la forme $4x+1$, mais cessera de s'évanouir, si n est de la forme $4x+3$.

Si maintenant on désigne par p^λ la plus haute puissance de p qui divise simultanément A et B, alors, en posant

$$A=p^\lambda x,\qquad B=p^\lambda y,$$
$$\mu=\frac{N}{2}-2\lambda,$$

on tirera de la formule (70)

$$4p^\mu=x^2+ny^2. \tag{71}$$

Dans ce qui précède, nous avons supposé le nombre n composé de facteurs premiers impairs. Supposons maintenant le nombre n pair et composé de facteurs dont l'un soit 2 ou une puissance de 2, les autres étant des facteurs premiers impairs. Si l'on suppose d'abord ceux-ci réduits à un seul facteur premier ν, n sera de l'une des formes

$$2\nu,\ 4\nu,\ 8\nu,\ \ldots.$$

Or, en supposant n divisible une seule fois par 2 ou de la forme 2, on retrouvera des formules analogues à celles qu'on obtient quand on pose simplement $n=\nu$. Mais, si l'on suppose

$$n=4\nu,$$

ν étant un nombre premier impair, on obtiendra des résultats dignes de remarque. Soient, dans cette hypothèse,

$$\alpha,\ \varsigma,\ \rho$$

des racines primitives des trois équations

$$x^4=1,\qquad x^\nu=1,\qquad x^n=1;$$

on pourra prendre

$$\rho=\alpha\varsigma.$$

Si d'ailleurs l'indice h de Θ_h est équivalent à i, suivant le module ν, et à j suivant le module 4, on aura

$$\rho^h=\alpha^j\varsigma^i,$$

ce qui suffira pour réduire l'équation (1) à l'équation (22); et, si l'on désigne par

$$\Theta_{i,j}$$

la valeur générale de Θ_h que fournit l'équation (22), les valeurs particulières de Θ_h, qui correspondront à des valeurs de h premières à n, seront celles que présente le Tableau suivant :

$$\left\{\begin{array}{llll}\Theta_{1,1}, & \Theta_{u,1}, & \Theta_{u^2,1}, & \ldots,\ \Theta_{u^{\nu-2},1},\\ \Theta_{1,3}, & \Theta_{u,3}, & \Theta_{u^2,3}, & \ldots,\ \Theta_{u^{\nu-2},3},\end{array}\right. \tag{72}$$

u étant une racine primitive de l'équivalence

$$x^{\nu-1}\equiv 1 \pmod{\nu}.$$

Concevons maintenant que, dans la formule (7), on fasse coïncider

$$\Theta_h,\ \Theta_k,\ \Theta_l,\ \ldots$$

avec celles des expressions de la forme $\Theta_{i,j}$ qui, dans le Tableau (72), offrent pour premier indice une puissance paire de u et, pour second indice, l'unité. Il est clair qu'alors la somme

$$h + k + l + \dots$$

sera équivalente, suivant le module 4, à

$$\frac{\nu - 1}{2},$$

et, suivant le module ν, au produit

$$1 + u^2 + \dots + u^{\nu-3} = \frac{u^{\nu-1} - 1}{u^2 - 1} \equiv 0.$$

Donc, cette somme sera divisible par

$$n = 4\nu,$$

ou seulement par

$$\frac{1}{2} n = 2\nu,$$

ou enfin par

$$\frac{1}{4} n = \nu,$$

suivant que $\nu - 1$ sera divisible par 8 ou par 4, ou seulement par 2, c'est-à-dire suivant que ν sera de la forme

$$8x + 1, \quad \text{ou} \quad 8x + 5, \quad \text{ou} \quad 4x + 3.$$

On aura donc, dans le premier cas,

$$\begin{aligned} \Theta_{h+k+l+\dots} &= \Theta_0 = -1, \\ \Theta_h \Theta_k \Theta_l \dots &= -R_{h,k,l,\dots}, \end{aligned} \tag{73}$$

dans le deuxième cas,

$$\begin{aligned} \Theta_{h+k+l+\dots} &= \Theta_{\frac{1}{2}n} = \Theta_{2\nu}, \\ \Theta_h \Theta_k \Theta_l \dots &= R_{h,k,l,\dots} \Theta_{2\nu} \end{aligned} \tag{74}$$

et, dans le troisième cas,

$$\begin{aligned} \Theta_{h+k+l+\dots} &= \Theta_{\frac{1}{4}n} = \Theta_\nu, \\ \Theta_h \Theta_k \Theta_l \dots &= R_{h,k,l,\dots} \Theta_\nu, \end{aligned} \tag{75}$$

pourvu que

$$\Theta_h, \quad \Theta_k, \quad \Theta_l, \quad \dots$$

remplissent les conditions ci-dessus énoncées, c'est-à-dire, en d'autres termes, pourvu qu'on fasse coïncider les indices

$$h, \quad k, \quad l, \quad \dots$$

avec ceux qui vérifient simultanément les deux équivalences

$$x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}, \qquad x \equiv 1 \pmod{4}. \tag{76}$$

On prouvera d'ailleurs facilement : 1° que, si n est de la forme $8x + 1$ ou $8x + 5$, l'équation (73) ou (74) s'étendra au cas même où l'on ferait coïncider les indices

$$h, \quad k, \quad l, \quad \dots$$

avec ceux qui vérifient simultanément les deux équivalences

$$x^{\frac{\nu-1}{2}} \equiv 1 \pmod{\nu}, \qquad x \equiv 3 \equiv -1 \pmod{4}, \tag{77}$$

ou les deux équivalences

$$x^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}, \qquad x \equiv 1 \pmod{4}, \tag{78}$$

ou bien encore les deux équivalences

$$x^{\frac{\nu-1}{2}} \equiv -1 \pmod{\nu}, \qquad x \equiv -1 \pmod{4}; \tag{79}$$

2° que si ν est de la forme $4x + 3$, l'équation (75) s'étendra au cas même où l'on ferait coïncider les indices

$$h, \quad k, \quad l, \quad \dots$$

avec ceux qui vérifient simultanément les équivalences (76) ou (78), mais devra être remplacée par l'équation suivante :

$$\Theta_h \Theta_k \Theta_l \dots = R_{h,k,l,\dots} \Theta_{-\nu}, \tag{80}$$

si l'on fait coïncider les indices

$$h,\quad k,\quad l,\quad \ldots$$

avec ceux qui vérifient les équations (77) ou (79). Donc, si l'on désigne respectivement par les quatre notations

$$[1,1],\quad [1,-1],\quad [-1,1],\quad [-1,-1]$$

les quatre produits formés par la multiplication des valeurs de

$$\Theta_h,\quad \Theta_k,\quad \Theta_l,\quad \ldots$$

correspondantes aux valeurs de

$$h,\quad k,\quad l,\quad \ldots$$

qui vérifient les formules

$$(76),\quad \text{ou}\quad (77),\quad \text{ou}\quad (78),\quad \text{ou}\quad (79),$$

on pourra, dans l'équation (73), lorsque ν sera de la forme $8x+1$, et dans l'équation (74), lorsque ν sera de la forme $8x+5$, remplacer successivement le produit

$$\Theta_h\Theta_k\Theta_l\ldots$$

par chacune des quatre expressions

$$(81)\qquad \begin{cases} [1,1] &= \Theta_{1,1}\,\Theta_{n^2,1}\,\Theta_{n^4,1}\ldots\Theta_{n^{\nu-1},1},\\ [1,-1] &= \Theta_{1,3}\,\Theta_{n^2,3}\,\Theta_{n^4,3}\ldots\Theta_{n^{\nu-1},3},\\ [-1,1] &= \Theta_{n,1}\,\Theta_{n^3,1}\,\Theta_{n^5,1}\ldots\Theta_{n^{\nu-1},1},\\ [-1,-1] &= \Theta_{n,3}\,\Theta_{n^3,3}\,\Theta_{n^5,3}\ldots\Theta_{n^{\nu-1},3}. \end{cases}$$

Mais, lorsque ν sera de la forme $4x+3$, alors on pourra remplacer le produit

$$\Theta_h\Theta_k\Theta_l\ldots,$$

dans l'équation (75), par chacune des expressions

$$[1,1],\quad [1,-1]$$

ou, dans l'équation (80), par chacune des expressions

$$[1,-1],\quad [-1,-1].$$

Observons à présent que -1 sera une des racines de l'équivalence (57), si ν est de la forme $4x+1$, et de l'équivalence (58), si ν est de la forme $4x+3$. Donc, par suite, les deux quantités

$$h,\quad -h$$

satisferont, l'une aux formules (76), l'autre aux formules (77), ou l'une aux formules (78), l'autre aux formules (79), si ν est de la forme $4x+1$; et, au contraire, ces deux quantités satisferont, l'une aux formules (76), l'autre aux formules (79), ou l'une aux formules (77) et l'autre aux formules (78), si ν est de la forme $4x+3$. Donc, en vertu de la formule (3), on aura : 1° si ν est de la forme $8x+1$ ou $8x+5$,

$$(82)\qquad [1,1][1,-1]=p^{\frac{\nu-1}{2}},\qquad [-1,1][-1,-1]=p^{\frac{\nu-1}{2}};$$

2° si ν est de la forme $4x+3$,

$$(83)\qquad [1,1][-1,-1]=p^{\frac{\nu-1}{2}},\qquad [1,-1][-1,1]=p^{\frac{\nu-1}{2}}.$$

Dans l'un et l'autre cas, les formules (82) ou (83) donneront

$$(84)\qquad p^{\nu-1}=[1,1][1,-1][-1,1][-1,-1].$$

D'ailleurs, comme, dans chacune des formules (73), (74), (75), (80), l'expression

$$R_{h,k,l,\ldots}$$

représentera une fonction entière et symétrique de

$$\rho^h,\quad \rho^k,\quad \rho^l,\quad \ldots,$$

par conséquent une fonction entière et symétrique, non seulement de

$$\varsigma^h,\quad \varsigma^k,\quad \varsigma^l,\quad \ldots,$$

mais encore de

$$\alpha^h,\quad \alpha^k,\quad \alpha^l,\quad \ldots,$$

les coefficients numériques étant des nombres entiers, il est clair

que, si ν est de la forme $8x+1$, le produit

$$[1,1][1,-1]$$

sera, en vertu de la formule (73), une fonction entière et symétrique, non seulement de

$$\varsigma,\quad \varsigma^{\alpha^2},\quad \ldots,\quad \varsigma^{\alpha^{\nu-3}},$$

mais encore de

$$\alpha,\quad \alpha^2,$$

par conséquent une fonction linéaire, non seulement des deux sommes

$$\varsigma+\varsigma^{\alpha^2}+\ldots+\varsigma^{\alpha^{\nu-3}},\quad \varsigma^{\alpha}+\varsigma^{\alpha^3}+\ldots+\varsigma^{\alpha^{\nu-2}},$$

mais encore de la somme

$$\alpha+\alpha^2.$$

Or, cette dernière somme étant nulle, en vertu de l'équation

$$\alpha^2=-1,$$

à laquelle doit satisfaire la racine primitive $\alpha=\sqrt{-1}$ ou $\alpha=-\sqrt{-1}$ de l'équation

$$x^4=1,$$

il en résulte qu'en supposant ν de la forme $8x+1$, on aura

$$[1,1][1,-1]=c_0+c_1(\varsigma+\varsigma^{\alpha^2}+\ldots+\varsigma^{\alpha^{\nu-1}})+c_2(\varsigma^{\alpha}+\varsigma^{\alpha^3}+\ldots+\varsigma^{\alpha^{\nu-2}}),$$

c_0, c_1, c_2 désignant des quantités entières. Si, dans l'équation précédente, on remplace ς par ς^{α}, on trouvera

$$[-1,1][-1,-1]=c_0+c_1(\varsigma^{\alpha}+\varsigma^{\alpha^3}+\ldots+\varsigma^{\alpha^{\nu-2}})+c_2(\varsigma+\varsigma^{\alpha^2}+\ldots+\varsigma^{\alpha^{\nu-1}});$$

puis en posant, pour abréger,

$$\varsigma-\varsigma^{\alpha}+\varsigma^{\alpha^2}-\ldots+\varsigma^{\alpha^{\nu-2}}-\varsigma^{\alpha^{\nu-1}}=\Delta,$$
$$A=2c_0-c_1-c_2,\qquad B=c_1-c_2,$$

on réduira les deux équations que nous venons d'obtenir à la forme

$$(85)\qquad \begin{cases} 2[1,1][1,-1] &= A+B\Delta,\\ 2[-1,1][-1,-1] &= A-B\Delta. \end{cases}$$

Si le nombre ν était de la forme $8x+5$, alors on devrait à l'équation (73) substituer l'équation (74) et, par suite, en ayant égard à la formule

$$\Theta_{2\nu}^2=\Theta_{2\nu}\Theta_{-2\nu}=p,$$

on obtiendrait, au lieu des équations (85), les deux suivantes :

$$(86)\qquad \begin{cases} 2[1,1][1,-1] &= (A+B\Delta)p,\\ 2[-1,1][-1,-1] &= (A-B\Delta)p. \end{cases}$$

Enfin, si ν était de la forme $4x+3$, on devrait à l'équation (73) substituer l'équation (75) ou (80) et, par suite, en ayant égard à la formule

$$\Theta_{\nu}\Theta_{-\nu}=-p,$$

on se trouverait de nouveau conduit à deux équations de la même forme que les équations (86). Observons d'ailleurs que les équations (86) peuvent être censées comprises elles-mêmes dans les formules (85), desquelles on les déduit en remplaçant les deux quantités entières A, B par deux autres quantités entières pA, pB.

Les résultats que fournissent les équations (82), (84), (85), (86) sont analogues à ceux que nous avons obtenus en prenant $n=\nu$; et d'abord, si ν est de la forme $8x+1$, on tirera des formules (82) et (85)

$$A=2p^{\frac{\nu-1}{2}},\qquad B=0.$$

Si, au contraire, ν est de la forme $8x+5$, on tirera des formules (82) et (86)

$$A=2p^{\frac{\nu-3}{2}},\qquad B=0.$$

Enfin, si ν est de la forme $4x+3$, alors des formules (84) et (86), jointes à l'équation

$$\Delta^2=-\nu,$$

on tirera

$$(87)\qquad 4p^{\nu-2}=A^2+\nu B^2;$$

puis, en nommant p^{λ} la plus haute puissance de p, qui divise simul-

tanément A, B, et posant

$$A = p^{\lambda} x, \qquad B = p^{\lambda} y,$$
$$\mu = \nu - 3 - 2\lambda,$$

on trouvera

$$4p^{\mu} = x^2 + \nu y^2. \tag{88}$$

Considérons maintenant les deux produits

$$[1, 1][-1, -1], \quad [1, -1][-1, 1],$$

que l'on déduit l'un de l'autre, en remplaçant ς par ς^{α}, ou α par $\alpha^3 = \alpha^{-1}$. Chacun de ces produits sera une fonction entière de α et, de plus, une fonction entière et symétrique, non seulement de

$$\varsigma, \quad \varsigma^{n^2}, \quad \ldots, \quad \varsigma^{n^{\nu-1}},$$

mais encore de

$$\varsigma^{n}, \quad \varsigma^{n^3}, \quad \ldots, \quad \varsigma^{n^{\nu-2}},$$

les coefficients étant des nombres entiers. Comme d'ailleurs chacun de ces produits ne sera point altéré, lorsqu'on y remplacera simultanément

$$\varsigma \text{ par } \varsigma^{n} \quad \text{et} \quad \alpha \text{ par } \alpha^3,$$

il devra se réduire, non seulement à une fonction linéaire de

$$\alpha, \quad \alpha^3$$

et, en même temps, à une fonction linéaire des deux sommes

$$\varsigma + \varsigma^{n^2} + \ldots + \varsigma^{n^{\nu-2}}, \quad \varsigma^{n} + \varsigma^{n^3} + \ldots + \varsigma^{n^{\nu-1}},$$

mais encore, évidemment, à une fonction linéaire des sommes

$$\alpha\,(\varsigma + \varsigma^{n^2} + \ldots + \varsigma^{n^{\nu-2}}) + \alpha^3(\varsigma^{n} + \varsigma^{n^3} + \ldots + \varsigma^{n^{\nu-1}}),$$
$$\alpha^3(\varsigma + \varsigma^{n^2} + \ldots + \varsigma^{n^{\nu-2}}) + \alpha\,(\varsigma^{n} + \varsigma^{n^3} + \ldots + \varsigma^{n^{\nu-1}}).$$

Or, en vertu de la formule

$$\alpha^2 = -1,$$

on a

$$\alpha^3 = -\alpha,$$

et, par suite, chacune des deux dernières sommes se réduit, au signe près, à

$$\alpha(\varsigma - \varsigma^{n} + \varsigma^{n^2} - \ldots + \varsigma^{n^{\nu-2}} - \varsigma^{n^{\nu-1}}) = \alpha\Delta.$$

Donc les deux produits

$$[1, 1][-1, -1], \quad [1, -1][-1, 1]$$

se réduiront à deux fonctions linéaires du monôme

$$\alpha\Delta$$

qu'on déduira l'une de l'autre, en remplaçant α par $\alpha^3 = -\alpha$ ou, ce qui revient au même, en remplaçant

$$\alpha\Delta \quad \text{par} \quad -\alpha\Delta.$$

D'ailleurs, chacun de ces produits aura pour facteur

$$\Theta_{1\nu}^2 = p$$

si ν est de la forme $8x + 1$, et

$$\Theta_{\nu}\Theta_{-\nu} = -p$$

si ν est de la forme $4x + 3$. On aura donc généralement

$$\begin{cases} [1, 1][-1, -1] = A + B\alpha\Delta, \\ [1, -1][-1, 1] = A - B\alpha\Delta, \end{cases} \tag{89}$$

A, B désignant deux quantités entières qui seront divisibles par p si ν est de l'une des formes $8x + 5$, $4x + 3$. Ces principes étant admis, si l'on suppose ν de l'une des formes

$$8x + 1, \quad 8x + 5,$$

alors des équations (84), (89), jointes aux deux formules

$$\alpha^2 = -1, \qquad \Delta^2 = \nu,$$

on tirera

$$p^{\nu-1} = A^2 + \nu B^2. \tag{90}$$

Si, au contraire, ν est de la forme $4x + 3$, on tirera des équations (83)

et (89)

$$A = p^{\frac{\nu-1}{2}}, \qquad B = 0.$$

L'équation (90), dans laquelle A, B sont divisibles par p, lorsque ν est de la forme $8x+5$, mérite d'être remarquée. Si l'on désigne par p^λ la plus haute puissance de p qui, dans cette équation, divise simultanément A et B, alors, en posant

$$A = p^\lambda x, \qquad B = p^\lambda y,$$
$$\mu = \nu - 1 - 2\lambda,$$

on trouvera

$$p^\mu = x^2 + \nu y^2. \tag{91}$$

Il est bon d'observer que, dans le cas où l'on suppose

$$n = 4\nu,$$

le nombre N des termes premiers à n et compris dans la suite

$$1, \quad 2, \quad 3, \quad \ldots, \quad n-1$$

est précisément

$$2(\nu - 1).$$

Donc, alors, l'exposant de p se réduit à $\frac{N}{2}$ dans les formules (84) et (90), aussi bien que dans les formules (38) et (47), (67) et (70).

Dans le cas particulier où, ν se réduisant à l'unité, on a simplement

$$n = 4,$$

on a aussi

$$\rho = \alpha,$$

α désignant toujours une racine primitive $\sqrt{-1}$ ou $-\sqrt{-1}$ de l'équation

$$x^4 = 1.$$

Alors on tire de l'équation (3)

$$\Theta_2^2 = p, \qquad \Theta_1\Theta_3 = (-1)^{\frac{p-1}{4}} p,$$

et de l'équation (4)

$$\Theta_1^2 = R_{1,1}\Theta_2, \qquad \Theta_3^2 = R_{3,3}\Theta_2,$$

puis de ces dernières combinées avec les deux précédentes

$$p = R_{1,1}R_{3,3}. \tag{92}$$

Dans cette même hypothèse, $R_{1,1}$, se réduisant à une fonction entière de α, sera de la forme

$$R_{1,1} = A + B\alpha,$$

A, B étant des quantités entières, et l'on aura encore

$$R_{3,3} = A + B\alpha^3$$

ou, puisque $\alpha^2 = -1$,

$$R_{3,3} = A - B\alpha.$$

Par suite, la formule (92) donnera

$$p = (A + B\alpha)(A - B\alpha) = A^2 - B\alpha^2$$

ou, ce qui revient au même,

$$p = A^2 + B^2. \tag{93}$$

Donc, alors, la multiplication de Θ_1^2 par Θ_3^2, ou plutôt de $R_{1,1}$ par $R_{3,3}$, fournira la décomposition du nombre p en deux carrés, c'est-à-dire, en d'autres termes, la résolution de l'équation indéterminée

$$p = x^2 + y^2, \tag{94}$$

dans laquelle p désigne un nombre premier de la forme $4x+1$.

Si, au lieu de supposer $n = 4\nu$, on supposait

$$n = 4\nu\nu' \ldots,$$

$\nu, \nu', \ldots$ étant des nombres premiers impairs, on se trouverait conduit, en raisonnant toujours de la même manière, à une formule analogue à l'équation (90). Supposons, pour fixer les idées, que, le nombre des facteurs premiers impairs étant réduit à 2, l'on ait

$$n = 4\nu\nu'.$$

Alors, en nommant toujours N le nombre des termes qui, dans la suite

$$1, \quad 2, \quad 3, \quad \ldots, \quad n-1,$$

sont premiers à $n = 4\nu\nu'$, on trouvera

$$N = 2(\nu - 1)(\nu' - 1).$$

Cela posé, en étendant l'usage des notations (53) au cas où, dans le produit

$$n = \nu\nu'\nu'',$$

on remplace le facteur impair ν'' par le facteur 4, par conséquent, au cas où l'on remplace les équivalences

$$x^{\frac{\nu''-1}{2}} \equiv 1 \pmod{\nu''}, \qquad x^{\frac{\nu''-1}{2}} \equiv -1 \pmod{\nu''}$$

par les équivalences

$$x \equiv 1 \pmod 4, \qquad x \equiv -1 \pmod 4$$

et les sommes

$$\zeta^{\rho} + \zeta^{\rho\alpha^2} + \ldots + \zeta^{\rho\alpha^{\nu''-3}} = -\frac{1-\Delta''}{2}, \qquad \zeta^{\rho\alpha} + \zeta^{\rho\alpha^3} + \ldots + \zeta^{\rho\alpha^{\nu''-2}} = -\frac{1+\Delta''}{2}$$

par

$$\alpha \quad \text{et} \quad \alpha^3 = -\alpha,$$

on obtiendra, pour représenter les produits (54), non plus des fonctions linéaires de

$$\frac{1-\Delta''}{2}, \quad \frac{1+\Delta''}{2},$$

mais des fonctions linéaires de

$$\alpha, \quad -\alpha,$$

lesquelles, d'ailleurs, ne cesseront pas d'être en même temps fonctions linéaires de

$$\frac{1-\Delta}{2}, \quad \frac{1+\Delta}{2}$$

et fonctions linéaires de

$$\frac{1-\Delta'}{2}, \quad \frac{1+\Delta'}{2}.$$

Donc, alors, au lieu des équations (55), on en obtiendra d'autres de la

forme

$$(95)\quad \begin{cases} 4[1,1,1][1,-1,-1][-1,1,-1][-1,-1,1] = a + b\alpha\Delta\Delta', \\ 4[-1,-1,-1][-1,1,1][1,-1,1][1,1,-1] = a - b\alpha\Delta\Delta', \end{cases}$$

a, b désignant des quantités entières qui, comme les produits (54), seront divisibles par p^2, c'est-à-dire par le carré de

$$\Theta^2_{\frac{1}{2}n} \quad \text{ou de} \quad \Theta_{\frac{1}{4}n}\Theta_{-\frac{1}{4}n},$$

si le nombre

$$\frac{N}{8} = \frac{\nu-1}{2}\frac{\nu'-1}{2}$$

n'est pas divisible par 4. Comme, d'ailleurs, dans chacune des équations (95), le premier membre, ou le quadruple de l'un des produits (54), devra se réduire au quadruple d'un nombre entier, si l'on remplace Δ, Δ' par des nombres impairs tels que l'unité et α par un nombre pair ou par un nombre impair, par exemple par 0 ou par 1, il est clair que

$$a \quad \text{et} \quad a + b$$

devront être des multiples de 4. Donc a, b seront divisibles par 4 ou de la forme

$$a = 4A, \qquad b = 4B$$

et les formules (95) donneront

$$(96)\quad \begin{cases} [1,1,1][1,-1,-1][-1,1,-1][-1,-1,1] = A + B\alpha\Delta\Delta', \\ [-1,-1,-1][-1,1,1][1,-1,-1][1,1,-1] = A - B\alpha\Delta\Delta', \end{cases}$$

les valeurs numériques de A, B étant des nombres entiers qui seront certainement divisibles par p^2 si le nombre

$$\frac{N}{8} = \frac{\nu-1}{2}\frac{\nu'-1}{2}$$

n'est pas divisible par 4. D'autre part, on reconnaîtra sans peine que les formules (64) sont applicables au cas où, dans le produit

$$n = 4\nu\nu',$$

les facteurs impairs ν, ν' sont tous deux de la forme $4x+1$; les formules (65), au cas où un seul de ces facteurs impairs, ν par exemple, est de la forme $4x+1$; enfin les formules (66), au cas où les facteurs ν, ν' sont de la forme $4x+3$. Dans les trois cas, les formules (64), (65) ou (66) entraineront la formule (67) et, dans le second cas en particulier, les formules (65) ou (68), jointes aux équations (96), donneront

$$A = p^{\frac{N}{2}}, \qquad B = 0.$$

Mais, dans le premier et le troisième cas, on tirera de l'équation (67), jointe aux formules (96),

$$p^{\frac{N}{2}} = A^2 - B^2\alpha^2\Delta^2\Delta'^2 = A^2 + B^2\Delta^2\Delta'^2; \tag{97}$$

et, comme on aura, dans le premier cas,

$$\Delta^2 = \nu, \qquad \Delta'^2 = \nu',$$

dans le troisième cas,

$$\Delta^2 = -\nu, \qquad \Delta'^2 = -\nu',$$

il en résulte que, dans le premier et le troisième cas, on trouvera

$$\Delta^2\Delta'^2 = \nu\nu',$$

par conséquent

$$p^{\frac{N}{2}} = A^2 + \nu\nu' B^2. \tag{98}$$

On peut remarquer, d'ailleurs, que les deux cas dont il s'agit sont précisément ceux où le produit

$$\nu\nu' = \frac{n}{4}$$

est de la forme $4x+1$. Ajoutons que les quantités entières A, B seront divisibles par p^2, si les deux nombres ν, ν' sont de la forme $4x+3$.

Généralement, si n est de la forme

$$n = 4\nu\nu'\nu'' \ldots,$$

ν, ν', ν'', ... désignant des facteurs premiers impairs, alors, en nommant toujours N le nombre des termes premiers à n et compris dans la suite

$$1, \quad 2, \quad 3, \quad \ldots, \quad n-1,$$

c'est-à-dire en posant

$$N = 2(\nu-1)(\nu'-1)(\nu''-1)\ldots,$$

on trouvera

$$p^{\frac{N}{2}} = A^2 + \nu\nu'\nu'' \ldots B^2,$$

ou, ce qui revient au même,

$$p^{\frac{N}{2}} = A^2 + \frac{n}{4}B^2, \tag{99}$$

A, B désignant des quantités entières, dont la seconde sera nulle lorsque le produit

$$\nu\nu'\nu'' \ldots = \frac{n}{4}$$

sera de la forme $4x+3$ et cessera de s'évanouir lorsque le même produit sera de la forme $4x+1$. Ajoutons que les quantités A, B seront divisibles par la puissance de p, dont le degré est le nombre des facteurs impairs

$$\nu, \quad \nu', \quad \nu'', \quad \ldots$$

si le produit

$$\frac{\nu-1}{2}\,\frac{\nu'-1}{2}\,\frac{\nu''-1}{2}\ldots$$

n'est pas divisible par 4.

Si maintenant on désigne par p^λ la plus haute puissance de p qui divise simultanément A et B, alors, en posant

$$A = p^\lambda x, \qquad B = p^\lambda y,$$

$$\mu = \frac{N}{2} - 2\lambda,$$

on tirera de la formule (99)

$$p^\mu = x^2 + \frac{n}{4}y^2. \tag{100}$$

Supposons encore $n = 8$. Alors, si l'on nomme α une racine primi-

tive de l'équation

$$x^8 = 1,$$

les quatre racines primitives de cette même équation seront

$$\alpha, \quad \alpha^3, \quad \alpha^5, \quad \alpha^7$$

et l'on aura

$$\alpha^4 = -1.$$

Alors aussi la formule (3) donnera

$$\Theta_1^2 = p, \qquad \Theta_1\Theta_7 = \Theta_3\Theta_5 = (-1)^{\frac{p-1}{8}} p,$$

et l'on tirera de la formule (4)

$$\Theta_1\Theta_3 = R_{1,3}\Theta_4, \qquad \Theta_5\Theta_7 = R_{5,7}\Theta_4,$$

puis, de ces dernières équations combinées avec les deux précédentes,

(101) $$p = R_{1,3}R_{5,7}.$$

D'ailleurs

$$R_{1,3}$$

sera une fonction entière et symétrique de

$$\alpha, \quad \alpha^3,$$

par conséquent, une fonction linéaire des sommes de la forme

$$\alpha^m + \alpha^{3m},$$

le coefficient numérique de chaque somme étant un nombre entier; et, d'autre part, la somme

$$\alpha^m + \alpha^{3m}$$

se réduit, pour $m = 1$ ou 3, à

$$\alpha + \alpha^3 = \alpha^3 + \alpha^9,$$

pour $m = 2$ ou 6, à

$$\alpha^2 + \alpha^6 = \alpha^6 + \alpha^{18} = 0,$$

pour $m = 4$, à

$$\alpha^4 + \alpha^{12} = -2,$$

enfin, pour $m = 5$ ou 7, à

$$\alpha^5 + \alpha^{15} = \alpha^7 + \alpha^{21} = \alpha^5 + \alpha^7 = -(\alpha + \alpha^3).$$

Donc $R_{1,3}$ se réduira simplement à une fonction linéaire de la somme

$$\alpha + \alpha^3;$$

et, comme on déduira $R_{5,7}$ de $R_{1,3}$ en remplaçant

$$\alpha \quad \text{et} \quad \alpha^3$$

par

$$\alpha^3 = -\alpha \quad \text{et} \quad \alpha^7 = -\alpha^3,$$

on aura nécessairement

(102) $$\begin{cases} R_{1,3} = A + B(\alpha + \alpha^3), \\ R_{5,7} = A - B(\alpha + \alpha^3), \end{cases}$$

A, B désignant des quantités entières.

Si maintenant on combine les formules (101) avec les équations (102), on en conclura

$$p = A^2 - B^2(\alpha + \alpha^3)^2,$$

et, comme on aura

$$(\alpha + \alpha^3)^2 = \alpha^2 + \alpha^6 + 2\alpha^4 = 2\alpha^4 = -2,$$

on trouvera définitivement

(103) $$p = A^2 + 2B^2.$$

Donc, p étant un nombre premier de la forme $8x + 1$, on pourra toujours satisfaire, par des valeurs entières de x, y, à l'équation indéterminée

(104) $$p = x^2 + 2y^2.$$

On pourrait encore facilement étendre les principes que nous venons d'exposer au cas où le nombre n serait de la forme

$$n = 8\nu$$

ou même de la forme

$$n = 8\nu\nu'\nu'' \dots,$$

ν, ν', ν'', ... étant des facteurs premiers impairs. Alors les résultats seraient analogues à ceux que nous avons obtenus en supposant

$$n = 4\nu\nu'\nu'' \dots.$$

Seulement, en passant d'une hypothèse à l'autre, il faudrait substituer aux racines primitives

$$\alpha \quad \text{et} \quad \alpha^3 = -\alpha$$

de l'équation

$$x^4 = 1$$

les sommes

$$\alpha + \alpha^3 \quad \text{et} \quad \alpha^5 + \alpha^7 = -(\alpha + \alpha^3)$$

ou

$$\alpha + \alpha^7 \quad \text{et} \quad \alpha^3 + \alpha^5 = -(\alpha + \alpha^7),$$

formées par l'addition de deux des racines primitives

$$\alpha, \quad \alpha^3, \quad \alpha^5, \quad \alpha^7$$

de l'équation

$$x^8 = 1.$$

Cela posé, en nommant N le nombre de ceux des termes de la suite

$$1, \quad 2, \quad 3, \quad \dots, \quad n-1$$

qui sont premiers à

$$n = 8\nu\nu'\nu'' \dots,$$

c'est-à-dire en posant

$$N = 4(\nu - 1)(\nu' - 1)(\nu'' - 1) \dots,$$

et désignant par A, B deux quantités entières, on trouverait : 1° dans le cas où le quotient

$$\frac{n}{8} = \nu\nu'\nu'' \dots$$

serait de la forme $4x + 1$,

$$p^{\frac{N}{2}} = A^2 - B^2(\alpha + \alpha^3)^2 \quad \Delta'^2\Delta''^2 \dots;$$

2° dans le cas où le même quotient serait de la forme $4x + 3$,

$$p^{\frac{N}{2}} = A^2 - B^2(\alpha + \alpha^7)^2\Delta^2\Delta'^2\Delta''^2 \dots,$$

les valeurs de Δ^2, Δ'^2, Δ''^2, ... étant dans l'un et l'autre cas

$$\Delta^2 = (-1)^{\frac{\nu-1}{1}}\nu, \qquad \Delta'^2 = (-1)^{\frac{\nu'-1}{1}}\nu', \qquad \Delta''^2 = (-1)^{\frac{\nu''-1}{2}}\nu'', \qquad \dots;$$

et, comme on aurait évidemment dans le premier cas

$$(\alpha + \alpha^3)^2 = \alpha^2 + \alpha^6 - 2 = -2,$$

$$\frac{\nu-1}{2} + \frac{\nu'-1}{2} + \frac{\nu''-1}{2} + \dots \equiv 0 \pmod 2,$$

$$\Delta^2\Delta'^2\Delta''^2 \dots = \nu\nu'\nu'' \dots,$$

puis, dans le second cas,

$$(\alpha + \alpha^7)^2 = \alpha^2 + \alpha^6 + 2 = 2,$$

$$\frac{\nu-1}{2} + \frac{\nu'-1}{2} + \frac{\nu''-1}{2} + \dots \equiv 1 \pmod 2,$$

$$\Delta^2\Delta'^2\Delta''^2 \dots = -1\,\nu\nu'\nu'' \dots,$$

il est clair que, dans l'une et l'autre hypothèse, on se trouvera conduit à la formule

$$p^{\frac{N}{2}} = A^2 + 2\nu\nu'\nu'' \dots B^2,$$

qu'on peut encore écrire comme il suit :

$$p^{\frac{N}{2}} = A^2 + 2\left(\frac{n}{8}\right)B^2. \tag{105}$$

Ajoutons que, dans le premier cas, les quantités A, B seront divisibles par la puissance de p qui a pour degré le nombre des facteurs impairs

$$\nu, \quad \nu', \quad \nu'', \quad \dots$$

si tous ces facteurs sont de la forme $4x + 3$, attendu qu'alors le produit

$$(1 + 3)\frac{\nu-1}{2}\frac{\nu'-1}{2}\frac{\nu''-1}{2} \dots$$

sera divisible, non par 8, mais seulement par 4, et qu'on aura d'ailleurs

$$\Theta_{\frac{1}{2}\nu\nu'\nu''}^2 = \Theta_{\frac{1}{2}n}^2 = p.$$

Dans tous les cas, si l'on désigne par p^λ la plus haute puissance de p, qui divise simultanément A et B, alors, en posant

$$A = p^\lambda x, \qquad B = p^\lambda y,$$
$$\mu = \frac{N}{2} - 2\lambda,$$

on tirera de la formule (105)

$$p^\mu = x^2 + 2\left(\frac{n}{8}\right)y^2. \tag{106}$$

Nous remarquerons en finissant que, si le nombre premier p, étant de la forme $4x+3$, se réduit précisément au nombre 3, les formules (16) deviendront inexactes. Mais alors, pour retrouver l'équation (20), il suffira d'observer qu'on tire de la formule (3)

$$\Theta_1 \Theta_2 = p,$$

et de la formule (4)

$$\Theta_1^2 = R_{1,1}\Theta_2, \qquad \Theta_2^2 = R_{2,2}\Theta_1,$$

puis de ces dernières, combinées avec la précédente,

$$p = R_{1,1}R_{2,2}. \tag{107}$$

Dans cette même hypothèse, si, en nommant ρ une des deux racines primitives de l'équation

$$x^3 = 1,$$

l'on pose

$$\rho - \rho^2 = \Delta,$$

on aura, non seulement

$$\Delta^2 = -3, \tag{108}$$

mais encore, eu égard à la formule $\rho + \rho^2 = -1$,

$$\rho = -\frac{1-\Delta}{2}, \qquad \rho^2 = -\frac{1+\Delta}{2}.$$

Comme on aura, d'autre part,

$$R_{1,1} = c_0 + c_1\rho + c_2\rho^2, \qquad R_{2,2} = c_0 + c_1\rho^2 + c_2\rho,$$

c_0, c_1 désignant des quantités entières, on en conclura

$$2R_{1,1} = A + B\Delta, \qquad 2R_{2,2} = A - B\Delta, \tag{109}$$

les valeurs de A, B étant

$$A = 2c_0 - c_1 - c_2, \qquad B = c_1 - c_2,$$

puis on conclura des formules (107) et (109)

$$4p = A^2 - B^2\Delta^2,$$

ou, ce qui revient au même, eu égard à la formule (108),

$$4p = A^2 + 3B^2. \tag{110}$$

L'équation (110) est évidemment de la forme de celle qu'on obtiendrait en posant $n = 3$ dans la formule (20).

NOTE IV.

SUR LES RÉSIDUS QUADRATIQUES.

p étant un nombre entier quelconque, on a, comme on sait,

$$(1)\quad (x+y+z+\ldots)^p = S\frac{1.2.3.\ldots.p}{(1.2.\ldots.f)(1.2.\ldots.g)(1.2.\ldots.h)\ldots}x^f y^g z^h \ldots,$$

le signe S s'étendant à toutes les valeurs entières, nulles ou positives, de

$$f, \quad g, \quad h, \quad \ldots$$

qui vérifient la condition

$$f + g + h + \ldots = p.$$

Si p est un nombre premier, le coefficient numérique

$$\frac{1.2.3.\ldots.p}{(1.2.\ldots.f)(1.2.\ldots.g)(1.2.\ldots.h)\ldots}$$

se réduira toujours évidemment à un multiple de p, à moins que l'on ne suppose un seul des exposants f, g, h, ... égal à p, tous les autres étant nuls. Donc alors la formule (1) donnera

$$(2) \qquad (x+y+z+\ldots)^p = x^p + y^p + z^p + \ldots + p\mathrm{P},$$

P désignant une fonction entière de x, y, z, ... dans laquelle les coefficients numériques seront des nombres entiers. Donc, si l'on attribue à x, y, z, ... des valeurs entières, on aura

$$(3) \qquad (x+y+z+\ldots)^p \equiv x^p + y^p + z^p + \ldots \pmod{p}.$$

Si maintenant on pose

$$x = y = z = \ldots = 1,$$

alors, en nommant k le nombre des quantités x, y, z, ..., on verra la formule (3) se réduire à

$$(4) \qquad k^p \equiv k \pmod{p}.$$

L'équivalence (4) comprend le théorème énoncé par Fermat et suivant lequel la différence

$$x^p - x$$

est, pour des valeurs entières de x, toujours divisible par p, lorsque p est un nombre premier. Comme d'autre part l'équivalence

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

ou

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

entraine la suivante

$$(5) \qquad x^{p-1} - 1 \equiv 0 \pmod{p}$$

lorsque x n'est pas divisible par p, il en résulte que tout nombre premier à p est racine de l'équivalence (5), qu'on peut encore écrire

comme il suit :

$$(6) \qquad x^{p-1} \equiv 1 \pmod{p}.$$

Si d'ailleurs on nomme t une racine primitive de l'équivalence (6), les diverses racines de cette équivalence pourront être représentées également, ou par les divers termes de la progression arithmétique

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

ou par les divers termes de la progression géométrique

$$1, \quad t, \quad t^2, \quad \ldots, \quad t^{p-2};$$

et, par suite, tout nombre entier, premier à p, sera équivalent, suivant le module p, à une puissance entière de t. Ajoutons qu'en vertu de la formule

$$t^{p-1} \equiv 1 \pmod{p}$$

on aura généralement

$$t^h \equiv t^k$$

si l'on suppose

$$h \equiv k \pmod{p-1}.$$

Donc une racine

$$t^h$$

de l'équivalence (6) ne devra point être censée altérée lorsqu'on y fera croître ou diminuer l'exposant h d'un multiple de $p-1$. Enfin, comme, en supposant p impair, on aura

$$x^{p-1} - 1 = \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right),$$

l'équivalence (5) ou (6) se décomposera, dans cette hypothèse, en deux autres dont la première

$$x^{\frac{p-1}{2}} - 1 \equiv 0$$

ou

$$(7) \qquad x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

aura évidemment pour racines les puissances paires de t, savoir

$$1, \quad t^2, \quad t^4, \quad \ldots, \quad t^{p-3},$$

tandis que la seconde

$$x^{\frac{p-1}{2}} - 1 \equiv 0$$

ou

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p} \tag{8}$$

aura nécessairement pour racines les puissances impaires de t, savoir

$$t,\ t^3,\ t^5,\ \ldots,\ t^{p-2}.$$

Ainsi, parmi les termes de la progression arithmétique

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

représentant les restes ou résidus qui peuvent provenir de la division d'un entier par p, les uns, en nombre égal à $\frac{p-1}{2}$, seront équivalents, suivant le module p, à des puissances paires de t, par conséquent à des carrés parfaits. Ces termes, dont chacun est le reste ou résidu de la division d'un carré par p, se nomment, pour cette raison, *résidus quadratiques*, aussi bien que les nombres équivalents aux mêmes termes suivant le module p; et comme, dans le cas où l'on prend p pour module, tout nombre premier à p équivaut à une puissance entière de t, le carré d'un tel nombre équivaudra nécessairement à une puissance paire de t, c'est-à-dire à une racine de la formule (7); d'où il résulte que tout résidu quadratique, différent de zéro, sera une semblable racine. Donc, les racines de l'équivalence (8) qui sont distinctes des racines de l'équivalence (7), mais, comme elles, en nombre égal à $\frac{p-1}{2}$, ne pourront être des résidus quadratiques suivant le module p. C'est ce que l'on exprime en disant que chacune des racines de l'équivalence (8) est *non-résidu* quadratique suivant le même module.

Pour abréger, nous désignerons, avec M. Legendre, par la notation

$$\left[\frac{k}{p}\right]$$

le reste de la division de $k^{\frac{p-1}{2}}$ par le nombre premier p. Cela posé, on aura généralement

$$\left[\frac{k}{p}\right] = 0,$$

si k est divisible par p, et, dans le cas contraire,

$$\left[\frac{k}{p}\right] = 1 \quad \text{ou} \quad \left[\frac{k}{p}\right] = -1$$

suivant que k sera *résidu* ou *non-résidu quadratique*. Comme d'ailleurs t, étant une racine primitive de l'équation (6), ne pourra vérifier la formule (7), on aura nécessairement

$$t^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \tag{9}$$

et comme $t^{\frac{p-1}{2}}$ sera évidemment une puissance paire ou impaire de t, suivant que p sera de la forme $4x+1$ ou $4x+3$, on peut affirmer que -1 sera résidu quadratique dans le premier cas et non-résidu quadratique dans le second. Enfin, comme, d'après ce qui a été dit plus haut, la progression arithmétique

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

renferme autant de résidus que de non-résidus, on aura nécessairement

$$\left[\frac{1}{p}\right] + \left[\frac{2}{p}\right] + \left[\frac{3}{p}\right] + \ldots + \left[\frac{p-1}{p}\right] = 0. \tag{10}$$

Généralement, si, une suite de nombres entiers

$$a,\ b,\ c,\ \ldots,\ l$$

étant composée de n termes différents premiers à p, on suppose que, dans cette suite, les résidus quadratiques sont en nombre égal à n' et les non-résidus en nombre égal à n'', on aura, non seulement

$$n' + n'' = n, \tag{11}$$

mais encore

$$(12)\qquad n' - n'' = \left[\frac{a}{p}\right] + \left[\frac{b}{p}\right] + \left[\frac{c}{p}\right] + \ldots + \left[\frac{l}{p}\right]$$

et, par conséquent,

$$(13)\qquad n' - n'' \equiv a^{\frac{p-1}{2}} + b^{\frac{p-1}{2}} + c^{\frac{p-1}{2}} + \ldots + l^{\frac{p-1}{2}} \pmod{p}.$$

On peut d'ailleurs écrire l'équivalence (13) comme il suit :

$$(14)\qquad n' - n'' \equiv \frac{d^{\frac{p-1}{2}}(e^{az} + e^{bz} + e^{cz} + \ldots + e^{lz})}{dz^{\frac{p-1}{2}}} \pmod{p},$$

la variable z devant être réduite à zéro après les différentiations effectuées.

La formule (14) offre un moyen facile de déterminer la différence $n' - n''$, et par suite, eu égard à la formule (11), chacun des nombres n', n'' lorsque, le nombre n étant inférieur à p, la suite

$$a,\quad b,\quad c,\quad \ldots,\quad l$$

se réduit à une progression arithmétique

$$h,\quad h+k,\quad h+2k,\quad \ldots,\quad h+(n-1)k.$$

Alors, en effet, la somme

$$e^{az} + e^{bz} + e^{cz} + \ldots + e^{lz}$$

devient

$$e^{hz}(1 + e^{kz} + e^{2kz} + \ldots + e^{(n-1)kz}) = e^{hz}\frac{e^{nkz} - 1}{e^{kz} - 1},$$

et, par suite, la formule (14) se réduit à

$$(15)\qquad n' - n'' = \frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left[e^{hz}\frac{e^{nkz} - 1}{e^{kz} - 1}\right].$$

Concevons, pour fixer les idées, qu'on demande le nombre n' des résidus quadratiques et le nombre n'' des non-résidus inférieurs à $\frac{p}{2}$,

c'est-à-dire compris dans la progression arithmétique

$$1,\quad 2,\quad 3,\quad \ldots,\quad \frac{p-1}{2}.$$

Alors on aura

$$n = \frac{p-1}{2},\qquad h = 1,\qquad k = 1$$

et, par suite,

$$(16)\qquad n' - n'' = \frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{p+1}{2}z} - e^{z}}{e^{z} - 1}\right).$$

D'autre part, la différence entre le rapport

$$\frac{e^{\frac{p+1}{2}z} - e^{z}}{e^{z} - 1}$$

et celui dans lequel il se transforme, quand on y remplace p par zéro, est

$$(17)\qquad \frac{e^{\frac{p+1}{2}z} - e^{z}}{e^{z} - 1} - \frac{e^{\frac{1}{2}z} - e^{z}}{e^{z} - 1} = \frac{e^{\frac{p+1}{2}z} - e^{\frac{1}{2}z}}{e^{z} - 1}.$$

Elle est donc égale au produit

$$\left(e^{\frac{p+1}{2}z} - e^{\frac{1}{2}z}\right)(e^{z} - 1)^{-1}$$

et sa dérivée de l'ordre $\frac{p-1}{2}$, relative à z, se composera d'une suite de termes dont chacun sera proportionnel au facteur

$$e^{\frac{p+1}{2}z} - e^{\frac{1}{2}z}$$

ou à l'une des dérivées de ce facteur. Or, comme ces dérivées s'évanouissent avec le facteur lui-même quand on y remplace z et p par zéro, comme d'ailleurs on trouvera

$$\frac{e^{\frac{1}{2}z} - e^{z}}{e^{z} - 1} = -\frac{e^{\frac{1}{2}z}}{1 + e^{\frac{1}{2}z}} = -\frac{1}{2}\left(1 + \frac{e^{\frac{1}{4}z} - e^{-\frac{1}{4}z}}{e^{\frac{1}{4}z} + e^{-\frac{1}{4}z}}\right),$$

il suit de la formule (17) qu'on aura, pour une valeur nulle de z,

$$\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{p+1}{2}z}-e^{z}}{e^{z}-1}-\frac{e^{\frac{1}{2}z}-e^{z}}{e^{z}-1}\right)\equiv 0 \pmod{p},$$

par conséquent

$$\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{p+1}{2}z}-e^{z}}{e^{z}-1}\right)=\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{1}{2}z}-e^{z}}{e^{z}-1}\right)=-\frac{1}{2}\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{1}{2}z}-e^{-\frac{1}{2}z}}{e^{\frac{1}{2}z}+e^{-\frac{1}{2}z}}\right) \pmod{p}.$$

Donc la formule (16) donnera, dans l'hypothèse admise,

$$(18)\qquad n'-n''\equiv-\frac{1}{2}\frac{d^{\frac{p-1}{2}}}{dz^{\frac{p-1}{2}}}\left(\frac{e^{\frac{1}{2}z}-e^{-\frac{1}{2}z}}{e^{\frac{1}{2}z}+e^{-\frac{1}{2}z}}\right) \pmod{p}.$$

Enfin, z devant être réduit à zéro après les différentiations, on pourra, sans inconvénient, remplacer z par $z\sqrt{-1}$ dans la formule (18), qui se trouvera ainsi réduite à

$$(19)\qquad n'-n''\equiv(-1)^{\frac{p-1}{4}}\frac{1}{2}\frac{d^{\frac{p-1}{2}}\operatorname{tang}\frac{z}{4}}{dz^{\frac{p-1}{2}}} \pmod{p}.$$

Ajoutons qu'en vertu de formules connues, la valeur de $\operatorname{tang}\frac{z}{4}$ sera généralement fournie par l'équation

$$(20)\qquad \begin{cases}\operatorname{tang}\frac{z}{4}=2\left(\frac{1}{6}\frac{2^2-1}{2}\frac{z}{1.2}+\frac{1}{30}\frac{2^4-1}{2^3}\frac{z^3}{1.2.3.4}\right.\\ \qquad\qquad\left.+\frac{1}{42}\frac{2^6-1}{2^5}\frac{z^5}{1.2.3.4.5.6}+\cdots\right),\end{cases}$$

dans laquelle les coefficients numériques

$$\frac{1}{6},\ \frac{1}{30},\ \frac{1}{42},\ \cdots,$$

que nous désignerons généralement par

$$\mathfrak{B}_1,\ \mathfrak{B}_2,\ \mathfrak{B}_3,\ \cdots,$$

sont ce qu'on appelle les *nombres de Bernoulli*.

Pour appliquer la formule (19), il convient de distinguer deux cas suivant que $\frac{p-1}{2}$ est pair ou impair, c'est-à-dire, en d'autres termes, suivant que p est de la forme $4x+1$ ou $4x+3$. Dans le premier cas on a, pour une valeur nulle de z,

$$\frac{d^{\frac{p-1}{2}}\operatorname{tang}\frac{z}{4}}{dz^{\frac{p-1}{2}}}=0,$$

et, par suite, la formule (19) étant réduite à

$$n'-n''\equiv 0 \pmod{p},$$

on tire de cette formule, jointe à l'équation

$$n'+n''=n=\frac{p-1}{2},$$

$$n'\equiv n''\equiv\frac{p-1}{4} \pmod{p},$$

par conséquent,

$$(21)\qquad n'=n''=\frac{p-1}{4}.$$

Au contraire, lorsque $\frac{p-1}{2}$ est impair et p de la forme $4x+3$, alors, en ayant égard à l'équivalence

$$2^{p-1}\equiv 1 \pmod{p},$$

on tire de la formule (20), pour une valeur nulle de z,

$$\frac{d^{\frac{p-1}{2}}\operatorname{tang}\frac{z}{4}}{dz^{\frac{p-1}{2}}}=4\frac{2^{\frac{p+1}{2}}-1}{2^{\frac{p-1}{2}}}\frac{1}{p+1}\mathfrak{B}_{\frac{p+1}{4}}\equiv 4\left(2-2^{\frac{p-1}{2}}\right)\mathfrak{B}_{\frac{p+1}{4}} \pmod{p},$$

et, par suite, la formule (19) donne

$$(22)\qquad n'-n''\equiv(-1)^{\frac{p+1}{4}}2\left(2-2^{\frac{p-1}{2}}\right)\mathfrak{B}_{\frac{p+1}{4}} \pmod{p}.$$

D'ailleurs, lorsque p est de la forme $4x+3$, il est nécessairement de

l'une des formes $8x+3$, $8x+7$ et, comme on le verra tout à l'heure, on a : 1° en supposant p de la forme $8x+3$,

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p};$$

2° en supposant p de la forme $8x+7$,

$$2^{\frac{p-1}{2}} \equiv 1.$$

Donc, la formule (22) donnera, lorsque p sera de la forme $8x+3$,

$$(23) \qquad n' - n'' \equiv -6\mathfrak{A}_{\frac{p+1}{4}}, \qquad \frac{n'-n''}{2} \equiv -3\mathfrak{A}_{\frac{p+1}{4}},$$

et, lorsque p sera de la forme $8x+7$,

$$(24) \qquad n' - n'' \equiv 2\mathfrak{A}_{\frac{p+1}{4}}, \qquad \frac{n'-n''}{2} \equiv \mathfrak{A}_{\frac{p+1}{4}}.$$

Ainsi, lorsque p est premier et de la forme $4x+3$, la demi-différence entre le nombre des résidus et le nombre des non-résidus inférieurs à $\frac{1}{2}p$ est équivalente, suivant le module p, à un nombre de Bernoulli ou au triple de ce nombre pris en signe contraire. Cette proposition remarquable a été, pour la première fois, énoncée et démontrée, en 1830, dans le précédent Mémoire dont un extrait a été publié dans le *Bulletin de M. de Férussac* sous la date de mars 1831.

En joignant aux équivalences (23) ou (24) la formule (11), ou

$$n' + n'' = \frac{p-1}{2},$$

on en tire : 1° lorsque p est de la forme $8x+3$,

$$(25) \qquad n' \equiv \frac{p-1}{4} - 3\mathfrak{A}_{\frac{p+1}{4}}, \qquad n'' \equiv \frac{p-1}{4} + 3\mathfrak{A}_{\frac{p+1}{4}} \pmod{p};$$

2° lorsque p est de la forme $8x+7$,

$$(26) \qquad n' \equiv \frac{p-1}{4} + \mathfrak{A}_{\frac{p+1}{4}}, \qquad n'' \equiv \frac{p-1}{4} - \mathfrak{A}_{\frac{p+1}{4}} \pmod{p}.$$

Au reste, les formules (11) et (15) fourniraient, avec la même facilité, le nombre des résidus et le nombre des non-résidus quadratiques compris dans une progression arithmétique dont les termes seraient positifs et inférieurs à

$$\frac{p}{3}, \quad \text{ou à} \quad \frac{p}{4}, \quad \text{ou à} \quad \frac{p}{5}, \quad \ldots$$

Concevons maintenant que, p étant un nombre premier impair, on demande la valeur de

$$\left[\frac{2}{p}\right]$$

ou, ce qui revient au même, le reste de la division de 2^{p-1} par p. Pour y parvenir, il suffira, comme on sait, d'élever à la puissance du degré p l'un quelconque des facteurs imaginaires dans lesquels peut se décomposer le nombre 2. Or on a évidemment

$$2 = (1+\sqrt{-1})(1-\sqrt{-1})$$

ou, ce qui revient au même,

$$2 = (1+\alpha)(1-\alpha),$$

α désignant une des deux racines primitives $\sqrt{-1}$, $-\sqrt{-1}$ de l'équation

$$x^4 = 1.$$

D'ailleurs, on tirera de la formule (2)

$$(27) \qquad (1+\alpha)^p = 1 + \alpha^p + p\mathrm{P},$$

P désignant une fonction entière de α dans laquelle les coefficients numériques seront des nombres entiers, et comme on aura, d'autre part,

$$\alpha^2 = -1, \qquad (1+\alpha)^2 = 2\alpha,$$

par conséquent,

$$(1+\alpha)^{p-1} = 2^{\frac{p-1}{2}}\alpha^{\frac{p-1}{2}}$$

et

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

la formule (27) donnera

$$2^{\frac{p-1}{2}}\alpha^{\frac{p-1}{2}}(1+\alpha)=1+\alpha^p+p\mathrm{P}$$

ou, ce qui revient au même,

$$2^{\frac{p-1}{2}}=\frac{1+\alpha^p}{\alpha^{\frac{p-1}{2}}(1+\alpha)}+p\frac{\mathrm{P}}{\alpha^{\frac{p-1}{2}}(1+\alpha)}. \tag{28}$$

Enfin, comme on aura : 1° en supposant p de la forme $4x+1$,

$$1+\alpha^p=1+\alpha,$$
$$\frac{1}{\alpha^{\frac{p-1}{2}}}=\alpha^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{4}}=(-1)^{\frac{p+1}{2}\frac{p-1}{4}};$$

2° en supposant p de la forme $4x+3$,

$$1+\alpha=\alpha(1+\alpha^3)=\alpha(1+\alpha^p),$$
$$\frac{1}{\alpha^{\frac{p+1}{2}}}=\alpha^{\frac{p+1}{2}}=(-1)^{\frac{p+1}{4}}=(-1)^{\frac{p-1}{2}\frac{p+1}{4}};$$

on en conclura, dans tous les cas,

$$\frac{1+\alpha^p}{\alpha^{\frac{p-1}{2}}(1+\alpha)}=(-1)^{\frac{(p-1)(p+1)}{8}},$$

ce qui permettra de réduire l'équation (28) à la suivante :

$$2^{\frac{p-1}{2}}=(-1)^{\frac{1}{2}\frac{p-1}{2}\frac{p+1}{2}}\left(1+p\frac{\mathrm{P}}{1+\alpha^p}\right). \tag{29}$$

En vertu de cette dernière équation, le produit

$$p\frac{\mathrm{P}}{1+\alpha^p}=p\frac{\mathrm{P}(1-\alpha^p)}{2}$$

sera égal, au signe près, à l'un des nombres entiers

$$2^{\frac{p-1}{2}}-1,\quad 2^{\frac{p-1}{2}}+1;$$

et comme l'expression

$$\mathrm{P}(1-\alpha^p)$$

sera nécessairement une fonction entière de α dans laquelle les coefficients seront entiers, cette expression, en devenant indépendante de α ne pourra se réduire qu'à une quantité entière. Donc le produit

$$p\,\mathrm{P}(1-\alpha^p)$$

et sa moitié

$$p\frac{\mathrm{P}(1-\alpha^p)}{2}$$

seront deux multiples du nombre premier p, et la formule (29) donnera

$$2^{\frac{p-1}{2}}\equiv(-1)^{\frac{1}{2}\frac{p-1}{2}\frac{p+1}{2}}\pmod{p} \tag{30}$$

ou, ce qui revient au même,

$$\left[\frac{2}{p}\right]=(-1)^{\frac{1}{2}\frac{p-1}{2}\frac{p+1}{2}}. \tag{31}$$

On tirera, en particulier, de la formule (31) : 1° en supposant p de la forme $8x\pm1$, c'est-à-dire de l'une des formes $8x+1$, $8x+7$,

$$\left[\frac{2}{p}\right]=(-1)^0=1;$$

2° en supposant p de la forme $8x\pm3$, c'est-à-dire de l'une des formes $8x+3$, $8x+5$,

$$\left[\frac{2}{p}\right]=(-1)^1=-1.$$

Ainsi le nombre 2 sera résidu quadratique pour les modules premiers de la forme $8x+1$, $8x+7$ et non-résidu pour les modules de la forme $8x+3$, $8x+5$.

Observons encore qu'on tirera de la formule (31) : 1° en supposant p de la forme $4x+1$,

$$\left[\frac{2}{p}\right]=(-1)^{\frac{p-1}{4}};$$

2° en supposant p de la forme $4x+3$,

$$\left[\frac{2}{p}\right]=(-1)^{\frac{p+1}{4}}.$$

Ces deux dernières formules sont précisément celles que, dans les deux cas dont il s'agit, on déduirait immédiatement de la formule (28). Il résulte de la seconde que, le nombre premier p étant de la forme $4x+3$, $2^{\frac{p-1}{2}}$ sera équivalent, suivant le module p, à $+1$ si ce module est, en outre, de la forme $8x+7$ et à -1 si le même module est de la forme $8x+3$.

Comme la démonstration de la formule (30) ou (31) repose entièrement sur le développement de la puissance p du binome

$$1+\alpha,$$

α étant une racine de l'équation $x^2=-1$, on arriverait encore à la même formule en développant immédiatement, à l'aide du théorème de Newton, l'expression

$$(1+\sqrt{-1})^p \quad \text{ou} \quad (1-\sqrt{-1})^p$$

et ayant égard à la formule

$$(1+\sqrt{-1})^2=2\sqrt{-1} \qquad \text{ou} \qquad (1-\sqrt{-1})^2=-2\sqrt{-1}.$$

Effectivement, on trouverait alors : 1° en supposant p de la forme $4x+1$,

$$(32)\qquad 2^{\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}\left[1+p-\frac{p(p-1)}{1.2}-\frac{p(p-1)(p-2)}{1.2.3}+\ldots\pm\frac{p(p-1)\ldots\left(\frac{p+1}{2}\right)}{1.2.3.\ldots\left(\frac{p-1}{2}\right)}\right];$$

2° en supposant p de la forme $4x+3$,

$$(33)\qquad 2^{\frac{p-1}{2}}=(-1)^{\frac{p+1}{2}}\left[1-p-\frac{p(p-1)}{2}+\frac{p(p-1)(p-2)}{1.2.3}+\ldots\pm\frac{p(p-1)\ldots\left(\frac{p+1}{2}\right)}{1.2.3.\ldots\left(\frac{p-1}{2}\right)}\right].$$

Ainsi, en particulier, en prenant

$$p=3, \qquad p=5, \qquad p=7, \qquad p=11, \qquad \ldots,$$

on trouvera successivement

$$\begin{aligned}
2&=-(1-3),\\
2^2&=-(1+5-10),\\
2^3&=1-7-21+35,\\
2^5&=-(1-11-55+165+330-462),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Une méthode semblable à celle que nous venons de rappeler et par laquelle on obtient la valeur de

$$\left[\frac{2}{p}\right]$$

peut servir à trouver généralement la relation qui existe entre les deux expressions

$$\left[\frac{q}{p}\right] \quad \text{et} \quad \left[\frac{p}{q}\right]$$

ou, ce qui revient au même, entre les restes de la division de 2^{q-1} par p et de 2^{p-1} par q, p et q désignant deux nombres premiers impairs. Effectivement, pour obtenir une transformation de l'expression

$$\left[\frac{q}{p}\right]=p^{q-1},$$

il suffit d'élever à la puissance p l'une des racines carrées imaginaires de $\pm p$. Or, d'après ce qui a été dit dans la Note I, si l'on désigne par θ une racine primitive de l'équation

$$(34)\qquad x^p=1,$$

alors, en posant

$$(35)\qquad \theta-\theta^4+\theta^{11}-\ldots+\theta^{p^2-3}-\theta^{p^2-1}=\Delta,$$

on aura

$$(36)\qquad \Delta^2=(-1)^{\frac{p-1}{2}}p.$$

D'autre part, q étant un nombre premier impair, il résulte de la formule (2) que l'équation (35) entraînera la suivante :

$$\Delta^q = \theta^q - \theta^{qt} + \theta^{qt^2} - \ldots + \theta^{qt^{p-3}} - \theta^{qt^{p-2}} + q\,\mathrm{Q}, \tag{37}$$

$q\mathrm{Q}$ étant une fonction entière de θ dans laquelle les coefficients numériques seront non seulement des entiers, mais encore des multiples de q ; et comme, t étant une racine primitive de l'équation (6), on aura évidemment

$$\theta^q - \theta^{qt} + \theta^{qt^2} - \ldots + \theta^{qt^{p-3}} - \theta^{qt^{p-2}} = \pm(\theta - \theta^t + \theta^{t^2} - \ldots + \theta^{t^{p-3}} - \theta^{t^{p-2}}) = \pm\Delta,$$

le double signe devant être réduit au signe + ou au signe − selon que le nombre q sera équivalent, suivant le module p, à une puissance paire ou impaire de t, c'est-à-dire suivant que l'on aura

$$\left[\frac{q}{p}\right] = 1 \qquad \text{ou} \qquad \left[\frac{q}{p}\right] = -1,$$

il est clair que l'équation (37) pourra être réduite à

$$\Delta^q = \left[\frac{q}{p}\right]\Delta + q\,\mathrm{Q}. \tag{38}$$

Enfin, comme

$$\Delta^q = (\theta - \theta^t + \theta^{t^2} - \ldots + \theta^{t^{p-3}} - \theta^{t^{p-2}})^q$$

sera évidemment une fonction entière et symétrique, non seulement de

$$\theta,\ \theta^{t^2},\ \theta^{t^4},\ \ldots,\ \theta^{t^{p-3}},$$

mais encore de

$$\theta^t,\ \theta^{t^3},\ \theta^{t^5},\ \ldots,\ \theta^{t^{p-2}},$$

par conséquent une fonction entière et linéaire des deux sommes

$$\theta + \theta^{t^2} + \theta^{t^4} + \ldots + \theta^{t^{p-3}},$$
$$\theta^t + \theta^{t^3} + \theta^{t^5} + \ldots + \theta^{t^{p-2}}$$

et même une fonction qui changera de signe lorsqu'on remplacera θ par θ', par conséquent lorsqu'on remplacera la première somme par la seconde, on peut affirmer que Δ^q sera proportionnel à la différence de

ces deux sommes, c'est-à-dire à Δ, le coefficient numérique de Δ étant un nombre entier. Donc, puisque, dans le second membre de l'équation (38), le premier terme se réduit à $\pm\Delta$, le second terme

$$q\,\mathrm{Q}$$

sera encore proportionnel à Δ, le coefficient numérique de Δ étant un nombre entier multiple de q. Cela posé, l'équation (38), divisée par Δ, donnera

$$\Delta^{q-1} = \left[\frac{q}{p}\right] \pmod{q}. \tag{39}$$

De cette dernière équation, combinée avec la formule (36), on tire

$$\left[\frac{q}{p}\right] \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \pmod{q},$$

par conséquent

$$\left[\frac{q}{p}\right] = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left[\frac{p}{q}\right]. \tag{40}$$

Telle est la loi de réciprocité qu'a trouvée M. Legendre et qui sert de base à la théorie des résidus quadratiques. La démonstration (1) que je viens d'en donner, et que j'avais déjà exposée dans le *Bulletin de M. de Férussac* de septembre 1829, est plus rigoureuse que celle qu'avait obtenue M. Legendre et plus courte que celles auxquelles M. Gauss était d'abord parvenu.

Si le nombre k est le produit de plusieurs facteurs a, b, c, ..., l'équation

$$k = abc\ldots$$

entraînera évidemment la suivante :

$$\left[\frac{k}{p}\right] = \left[\frac{a}{p}\right]\left[\frac{b}{p}\right]\left[\frac{c}{p}\right]\ldots$$

(1) Dans la troisième édition de la *Théorie des nombres*, qui a paru en 1830, M. Legendre présente cette démonstration comme étant la plus simple de toutes et l'attribue à M. Jacobi, sans indiquer aucun Ouvrage où ce géomètre l'ait publiée, et dont la date soit antérieure au mois de septembre 1829.