En d'autres termes, on aura généralement

$$\left[\frac{abc\ldots}{p}\right]=\left[\frac{a}{p}\right]\left[\frac{b}{p}\right]\left[\frac{c}{p}\right]\ldots.$$

On trouvera de même

$$\left[\frac{a^n}{p}\right]=\left[\frac{a}{p}\right]^n.$$

On peut voir, dans le *Bulletin de M. de Férussac* déjà cité, comment les mêmes principes peuvent être appliqués à la théorie des résidus cubiques, biquadratiques, etc.

NOTE V.

DÉTERMINATION DES FONCTIONS $R_{h,k}$, ... ET DES COEFFICIENTS QU'ELLES RENFERMENT.

Si, en désignant par p un nombre premier impair, par θ, τ des racines primitives des équations

$$x^p=1, \qquad x^{p-1}=1,$$

par t une racine primitive de l'équivalence

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

enfin par h, k des quantités entières, on pose

$$\Theta_h=\theta+\tau^h\theta^t+\tau^{2h}\theta^{t^2}+\ldots+\tau^{(p-2)h}\theta^{t^{p-2}}, \tag{1}$$

il est clair que la condition

$$k\equiv h \pmod{p-1}$$

entraînera les formules

$$\tau^k=\tau^h, \qquad \Theta_k=\Theta_h,$$

en vertu desquelles on pourra toujours, si l'on veut, réduire l'exposant h d'une puissance entière soit positive, soit négative de τ, ou l'indice h d'une expression de la forme Θ_h, à l'un des nombres

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2.$$

D'ailleurs, ainsi qu'on l'a prouvé, on trouvera : 1° en supposant h divisible par $p-1$,

$$\Theta_h=\Theta_0=-1; \tag{2}$$

2° en supposant h non divisible par $p-1$,

$$\Theta_h\Theta_{-h}=(-1)^h p. \tag{3}$$

Donc, si l'on pose généralement

$$\Theta_h\Theta_k=R_{h,k}\Theta_{h+k}$$

ou, ce qui revient au même,

$$R_{h,k}=\frac{\Theta_h\Theta_k}{\Theta_{h+k}}, \tag{4}$$

on aura : 1° en supposant h ou k divisible par $p-1$,

$$R_{h,k}=-1; \tag{5}$$

2° en supposant h non divisible par $p-1$,

$$R_{h,-h}=-(-1)^h p; \tag{6}$$

et, comme on trouvera encore

$$R_{h,k}R_{-h,-k}=\frac{\Theta_h\Theta_k}{\Theta_{h+k}}\frac{\Theta_{-h}\Theta_{-k}}{\Theta_{-h-k}},$$

on en conclura, eu égard à la formule (3) et en supposant h, k, ainsi que $h+k$, non divisibles par $p-1$,

$$R_{h,k}R_{-h,-k}=p. \tag{7}$$

Ajoutons que, si $h+k$ n'est pas divisible par $p-1$, on aura [*voir* la

formule (3) de la page 88]

$$R_{h,k} = S(\tau^{ih+jk}), \tag{8}$$

le signe S s'étendant à toutes les valeurs de i comprises dans la suite

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

et les valeurs correspondantes de i, j étant choisies de manière à vérifier la condition

$$ij + 1 \equiv 0 \pmod{p}. \tag{9}$$

Concevons maintenant que, dans le second membre de la formule (8), on réduise l'exposant de chaque puissance de τ à l'un des nombres

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2.$$

Ce second membre deviendra une fonction entière de τ du degré $p-2$ et l'on aura identiquement

$$S(\tau^{ih+jk}) = a_0 + a_1\tau + a_2\tau^2 + \ldots + a_{p-2}\tau^{p-2}, \tag{10}$$

a_0, a_1, a_2, ..., a_{p-2} désignant des nombres entiers dont plusieurs pourront s'évanouir et dont la somme, égale au nombre des valeurs de i, vérifiera la formule

$$a_0 + a_1 + a_2 + \ldots + a_{p-2} = p - 2. \tag{11}$$

Cela posé, l'équation (10) donnera

$$R_{h,k} = a_0 + a_1\tau + a_2\tau^2 + \ldots + a_{p-2}\tau^{p-2}. \tag{12}$$

D'ailleurs si, dans l'équation (10), on remplace τ par τ^m, on trouvera

$$S(\tau^{imh+jmk}) = a_0 + a_1\tau^m + a_2\tau^{2m} + \ldots + a_{p-2}\tau^{(p-2)m}. \tag{13}$$

Donc, si le produit

$$m(h+k) = mh + mk$$

n'est pas divisible par $p-1$, l'équation (12) entraînera la suivante :

$$R_{mh,mk} = a_0 + a_1\tau^m + a_2\tau^{2m} + \ldots + a_{p-2}\tau^{(p-2)m}. \tag{14}$$

Si $p-1$ divisait le produit

$$m(h+k),$$

alors on trouverait : 1° en supposant mh, mk non divisibles par $p-1$,

$$S(\tau^{imh+jmk}) = -1, \tag{15}$$

par conséquent

$$a_0 + a_1\tau^m + a_2\tau^{2m} + \ldots + a_{p-2}\tau^{(p-2)m} = -1; \tag{16}$$

2° en supposant mh et mk séparément divisibles par $p-1$,

$$S(\tau^{imh+jmk}) = p - 2, \tag{17}$$

par conséquent

$$a_0 + a_1\tau^m + a_2\tau^{2m} + \ldots + a_{p-2}\tau^{(p-2)m} = p - 2. \tag{18}$$

Il est bon d'observer que, dans le premier membre de l'équation (18), les seules puissances de τ, qui se trouveront multipliées par des coefficients positifs et distincts de zéro, seront les puissances qui offriront des exposants divisibles par $p-1$ ou, ce qui revient au même, celles qui se réduiront à l'unité. Donc le premier membre de la formule (18) se réduira identiquement au premier membre de la formule (11).

Un moyen fort simple d'obtenir, pour des valeurs données de t, h et k, les coefficients

$$a_0, \quad a_1, \quad a_2, \quad \ldots, \quad a_{p-2}$$

est de résoudre l'équation (9) par rapport à j et d'en tirer, pour chaque valeur de i, la valeur correspondante de j. Concevons, par exemple, qu'on prenne $p = 5$. Alors τ sera une racine primitive

$$\sqrt{-1} \quad \text{ou} \quad -\sqrt{-1}$$

de l'équation

$$x^4 = 1,$$

tandis que t désignera une racine primitive de l'équivalence

$$x^4 \equiv 1 \pmod{5}.$$

On pourra donc prendre

$$t = 2$$

et en effet, aux valeurs

$$0, \quad 1, \quad 2, \quad 3$$

de l'exposant i correspondront des valeurs essentiellement distinctes et non équivalentes

$$1, \quad 2, \quad 4, \quad 8 \equiv 3 \pmod 5$$

de la puissance 2^i. D'ailleurs, si l'on attribue successivement à i les valeurs

$$1, \quad 2, \quad 3,$$

les valeurs correspondantes de

$$1 - 2^i \equiv 2^j \pmod 4$$

seront

$$1 - 2 \equiv 4, \quad 1 - 4 \equiv 2, \quad 1 - 8 \equiv 1 - 3 \equiv 3 \pmod 5$$

et, par suite, on trouvera, pour valeurs correspondantes de j,

$$2, \quad 1, \quad 3.$$

Cela posé, on aura

$$S(\tau^{lh+jk}) = \tau^{h+2k} + \tau^{3h+h} + \tau^{3(h+k)}$$

et de cette dernière formule, jointe aux équations (8) et (10), on tirera :

Pour $h = 1$, $k = 1$, $h + k = 2$,

$$R_{1,1} = 2\tau^3 + \tau^6 = \tau^5 + 2\tau^3, \quad a_0 = 0, \quad a_1 = 0, \quad a_2 = 1, \quad a_3 = 2;$$

Pour $h = 1$, $k = 2$, $h + k = 3$,

$$R_{1,2} = \tau^5 + \tau^3 + \tau^9 = 1 + 2\tau, \quad a_0 = 1, \quad a_1 = 2, \quad a_2 = 0, \quad a_3 = 0;$$

Pour $h = 3$, $k = 3$, $h + k = 6 \equiv 2 \pmod 4$,

$$R_{3,3} = 2\tau^9 + \tau^{18} = \tau^3 + 2\tau, \quad a_0 = 0, \quad a_1 = 2, \quad a_2 = 1, \quad a_3 = 0, \quad \ldots$$

$\ldots\ldots$

Il serait facile d'exprimer les valeurs des constantes positives

$$a_0, \quad a_1, \quad a_2, \quad \ldots, \quad a_{p-2},$$

comprises dans les formules (10) et (13), en fonction des sommes de la forme

$$S(\tau^{lh+jk}) \quad \text{ou} \quad S(\tau^{lmh+jmk}).$$

En effet, si, dans la formule (13), on prend successivement pour m chacun des termes de la suite

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2,$$

on en tirera

$$(19) \quad \begin{cases} a_0 + a_1 + a_2 + \ldots + a_{p-2} = p - 2, \\ a_0 + a_1\tau + a_2\tau^2 + \ldots + a_{p-2}\tau^{p-2} = S(\tau^{lh+jk}), \\ a_0 + a_1\tau^2 + a_2\tau^4 + \ldots + a_{p-2}\tau^{2(p-2)} = S(\tau^{2(lh+jk)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_0 + a_1\tau^{p-2} + a_2\tau^{2(p-2)} + \ldots + a_{p-2}\tau^{(p-2)^2} = S(\tau^{(p-2)(lh+jk)}). \end{cases}$$

Or, comme, en désignant par h une quantité entière positive ou négative, on aura généralement, si h est non divisible par $p - 1$,

$$(20) \qquad 1 + \tau^h + \tau^{2h} + \ldots + \tau^{(p-2)h} = 0$$

et, si h est divisible par $p - 1$,

$$(21) \qquad 1 + \tau^h + \tau^{2h} + \ldots + \tau^{(p-2)h} = p - 1,$$

on conclura des formules (19), respectivement multipliées par les facteurs

$$1, \quad \tau^{-m}, \quad \tau^{-2m}, \quad \ldots, \quad \tau^{-(p-2)m},$$

puis combinées entre elles par voie d'addition,

$$(22) \quad \begin{cases} (p-1)a_m = p - 2 + \tau^{-m} S(\tau^{lh+jk}) \\ \qquad + \tau^{-2m} S(\tau^{2(lh+jk)}) + \ldots + \tau^{-(p-2)m} S(\tau^{(p-2)(lh+jk)}) \end{cases}$$

ou, ce qui revient au même,

$$(23) \quad \begin{cases} (p-2)a_m = p - 2 + \tau^{(p-2)m} S(\tau^{lh+jk}) \\ \qquad + \tau^{(p-3)m} S(\tau^{2(lh+jk)}) + \ldots + \tau^{m} S(\tau^{(p-2)(lh+jk)}). \end{cases}$$

Ce n'est pas tout. Si, en attribuant à i et j deux valeurs correspon-

dantes, propres à vérifier la formule (9), on a

$$ih + jk \equiv l \pmod{p-1},$$

l désignant l'un des nombres

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2$$

on en conclura, non seulement

$$\tau^{ih+jk} = \tau^{l},$$

mais aussi

$$t^{ih+jk} = t^{l} \pmod{p}.$$

Donc la formule (10) entraînera la suivante :

$$(24) \qquad S(t^{ih+jk}) \equiv a_0 + a_1 t + a_2 t^2 + \ldots + a_{p-2} t^{p-2} \pmod{p}$$

et la formule (13) donnera pareillement

$$(25) \qquad S(t^{imh+jmk}) \equiv a_0 + a_1 t^m + a_2 t^{2m} + \ldots + a_{p-2} t^{(p-2)m} \pmod{p}.$$

Si, dans cette dernière, on prend successivement pour m chacun des termes de la suite,

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2,$$

on en tirera

$$(26) \quad \begin{cases} a_0 + a_1 + a_2 + \ldots + a_{p-2} \equiv p-2 \\ a_0 + a_1 t + a_2 t^2 + \ldots + a_{p-2} t^{p-2} \equiv S(t^{ih+jk}) \\ a_0 + a_1 t^2 + a_2 t^4 + \ldots + a_{p-2} t^{2(p-2)} \equiv S(t^{2(ih+jk)}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_0 + a_1 t^{p-2} + a_2 t^{2(p-2)} + \ldots + a_{p-2} t^{(p-2)^2} \equiv S(t^{(p-2)(ih+jk)}) \end{cases} \pmod{p}.$$

Or, comme, en désignant par h une quantité entière positive ou négative, on aura généralement, si h est non divisible par $p-1$,

$$(27) \qquad 1 + t^h + t^{2h} + \ldots + t^{(p-2)h} \equiv 0 \pmod{p}$$

et, si h est divisible par $p-1$,

$$(28) \qquad 1 + t^h + t^{2h} + \ldots + t^{(p-2)h} \equiv p-1 \pmod{p},$$

on conclura des formules (26), respectivement multipliées par les facteurs

$$1, \quad t^{-m}, \quad t^{-2m}, \quad \ldots, \quad t^{-(p-2)m},$$

puis combinées entre elles par voie d'addition,

$$(29) \quad \begin{cases} (p-1)a_m \equiv p-2 + t^{-m} S(t^{ih+jk}) + t^{-2m} S(t^{2(ih+jk)}) + \ldots \\ \qquad\qquad + t^{-(p-2)m} S(t^{(p-2)(ih+jk)}) \end{cases} \pmod{p}$$

ou, ce qui revient au même,

$$(30) \quad \begin{cases} a_m \equiv 2 - t^{(p-2)m} S(t^{ih+jk}) - t^{(p-2)m} S(t^{2(ih+jk)}) - \ldots \\ \qquad - t^{m} S(t^{(p-2)(ih+jk)}) \end{cases} \pmod{p}.$$

La quantité positive a_m devant être, en vertu de la formule (11), inférieure à $p-2$ pourra être aisément déterminée à l'aide de la formule (30), si l'on parvient à trouver des quantités équivalentes, suivant le module p, à des sommes de la forme

$$S(t^{ih+jk}) \quad \text{ou} \quad S(t^{imh+jmk}).$$

Or concevons que, dans la somme

$$S(t^{ih+jk}),$$

h et k se réduisent, comme on peut toujours le supposer, à deux termes de la suite

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2.$$

Alors, si l'on a

$$(31) \qquad h + k = 0,$$

ce qui suppose $h = 0$, $k = 0$, on trouvera évidemment

$$(32) \qquad S(\tau^{ih+jk}) = p-2,$$

par conséquent,

$$(33) \qquad S(t^{ih+jk}) \equiv -2 \pmod{p}$$

et, si l'on suppose

$$(34) \qquad h + k = p-1,$$

on trouvera

$$S(\tau^{ih+jk}) = S(\tau^{(j-l)k}) = \tau + \tau^2 + \ldots + \tau^{p-2}$$

ou, ce qui revient au même,

$$S(\tau^{ih+jk}) = -1, \tag{35}$$

par conséquent,

$$S(t^{ih+jk}) \equiv S(t^{(j-l)k}) \equiv t + t^2 + \ldots + t^{p-2} \pmod{p}$$

ou, ce qui revient au même,

$$S(t^{ih+jk}) \equiv -1 \pmod{p}. \tag{36}$$

Si $h + k$ est renfermé entre les limites 0, $p-1$, en sorte qu'on ait

$$p - 1 > h + k > 0, \tag{37}$$

on trouvera, en vertu de la formule (9),

$$S(t^{ih+jk}) = S[t^{ih}(1-t^i)^k] \pmod{p} \tag{38}$$

et puisque, pour $i = 0$, on aura

$$1 - t^i = 0,$$

il est clair que, dans le second membre de la formule (38), on pourra étendre la sommation, indiquée par le signe S, ou comme dans le premier membre, aux seules valeurs de i comprises dans la suite

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

ou bien encore à toutes les valeurs de i comprises dans la suite

$$0, \quad 1, \quad 2, \quad 3, \quad \ldots, \quad p-2.$$

D'ailleurs, dans cette dernière hypothèse, on aura, en vertu des formules (27) et (37),

$$S(t^{ih}) = 0, \quad S(t^{i(h+1)}) = 0, \quad \ldots, \quad S(t^{i(h+k)}) \equiv 0 \pmod{p};$$

et, par suite, après le développement de

$$(1-t^i)^k$$

suivant les puissances ascendantes de t^i, le second membre de la formule (38) se composera d'une suite de termes dont chacun sera équivalent à zéro suivant le module p. Donc la condition (37) entrainera l'équivalence

$$S(t^{ih+jk}) \equiv 0 \pmod{p}. \tag{39}$$

Supposons enfin

$$h + k > p - 1. \tag{40}$$

Alors, $h + k$ étant renfermé entre les limites $p-1$, $2(p-1)$, si l'on pose

$$\mathrm{h} = (p-1) - h, \qquad \mathrm{k} = (p-1) - k, \tag{41}$$

la somme

$$\mathrm{h} + \mathrm{k} = 2(p-1) - (h+k)$$

sera renfermée entre les limites 0, $p-1$, de manière à vérifier la condition

$$p - 1 > \mathrm{h} + \mathrm{k} > 0. \tag{42}$$

Alors aussi on aura

$$S(t^{ih+jk}) \equiv S(t^{-ih-jk}) \pmod{p};$$

puis, en posant

$$j - i \equiv \iota, \pmod{p} \tag{43}$$

ou, ce qui revient au même,

$$j \equiv i + \iota,$$

on trouvera

$$S(t^{ih+jk}) \equiv S(t^{-ik}t^{-i(h+k)}) \pmod{p}.$$

D'ailleurs, comme, en vertu de l'équivalence (43), la formule (9) se réduit à

$$t^{-i} \equiv 1 + t^{\iota} \pmod{p} \tag{44}$$

on trouvera encore

$$S(\iota^{ih+jk}) \equiv S[\iota^{-ik}(1+\iota^i)^{h+k}] \pmod{p}. \tag{45}$$

Dans le second membre de la formule (45), la sommation indiquée par le signe S doit s'étendre aux diverses valeurs de ι^i qui permettent de vérifier la condition (44), par conséquent aux diverses valeurs de i comprises dans la suite

$$0,\ 1,\ 2,\ 3,\ \ldots\ p-2,$$

mais distinctes de la valeur

$$i = \frac{p-1}{2},$$

pour laquelle il ne serait plus possible de vérifier la condition (44), réduite à la forme inadmissible

$$\iota^{-i} \equiv 0,$$

et comme, pour $i = \frac{p-1}{2}$, on aura $\iota^i \equiv -1$, par conséquent

$$1+\iota^i \equiv 0 \pmod{p},$$

il en résulte que, dans le second membre de la formule (45), la sommation indiquée par le signe S pourra être étendue sans inconvénient à toutes les valeurs

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2$$

de l'exposant i. Or, dans cette dernière hypothèse, en développant

$$(1+\iota^i)^{h+k}$$

suivant les puissances ascendantes de ι^i, puis ayant égard aux formules (27), (28) et (42), on tirera de l'équation (45)

$$S(\iota^{ih+jk}) \equiv (p-1)\frac{1.2.3.\ldots.(h+k)}{(1.2.\ldots.h)(1.2.\ldots.k)} \pmod{p}$$

ou, ce qui revient au même,

$$S(\iota^{ih+jk}) \equiv -\Pi_{h,k} \pmod{p}, \tag{46}$$

la valeur de $\Pi_{h,k}$ étant

$$\Pi_{h,k} \equiv \frac{1.2.3.\ldots.(h+k)}{(1.2.\ldots.h)(1.2.\ldots.k)}. \tag{47}$$

Il est bon d'observer que la formule (46), dans laquelle h,k et h,k sont liés entre eux par les équations (41), s'étend au cas même où la somme

$$h+k$$

redeviendrait inférieure à $p-1$ et se trouverait comprise entre les limites

$$0,\ p-1.$$

Alors, en effet, comme on aurait

$$h+k > p-1 \tag{48}$$

et, par suite,

$$1.2.3.\ldots.(h+k) \equiv 0 \pmod{p},$$

l'équivalence (47) donnerait évidemment

$$\Pi_{h,k} \equiv 0 \tag{49}$$

et, en conséquence, la formule (46) se trouverait réduite à la formule (39).

Observons encore que de la formule (46), jointe aux équations (41), on tire immédiatement

$$S(\iota^{ih+jk}) \equiv -\Pi_{p-1-h,p-1-k} \pmod{p}. \tag{50}$$

Dans les formules qui précèdent, chacune des lettres h, k représente l'un des nombres

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2$$

et, par suite, chacune des lettres h, k représente l'un des nombre

$$1,\ 2,\ 3,\ 4,\ \ldots,\ p-1.$$

Pour rendre les notations facilement applicables au cas où

$$h,\ k,\ h,\ k$$

représenteraient des quantités entières quelconques, soit positives, soit négatives, nous désignerons généralement par

$$\Pi_{h,k}$$

ce que devient le rapport

$$\frac{1.2.3.\ldots.(h+k)}{(1.2.\ldots.h)(1.2.\ldots.k)}$$

quand on y remplace les quantités entières

$$h \quad \text{et} \quad k$$

par les deux termes qui, dans la suite

$$1,\ 2,\ 3,\ 4,\ \ldots,\ p-1,$$

sont équivalentes à ces quantités, suivant le module $p-1$. Cela posé, la formule (50), étendue à des valeurs entières quelconques de h et de k, donnera généralement, si $h+k$ n'est pas divisible par $p-1$,

$$\mathbf{S}(t^{ih+jk}) \equiv -\Pi_{-h,-k} \pmod{p}. \tag{51}$$

Ajoutons que, si $h+k$ devient divisible par $p-1$, la formule (51) devra être remplacée, ou par la formule (33), ou par la formule (36); savoir : par la formule (33) lorsque $p-1$ divisera séparément h et k et par la formule (36) dans le cas contraire.

Concevons maintenant que, dans les formules (33), (36) et (51), on remplace

$$h \text{ par } mh \quad \text{et} \quad k \text{ par } mk,$$

m étant un terme de la suite

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2.$$

Alors on trouvera : 1° en supposant mh et mk séparément divisibles par $p-1$,

$$\mathbf{S}(t^{m(ih+jk)}) \equiv -2 \pmod{p} \tag{52}$$

2° en supposant que $p-1$ divise la somme

$$m(h+k) = mh + mk$$

sans diviser ses deux parties mh, mk,

$$\mathbf{S}(t^{m(ih+jk)}) \equiv -1 \pmod{p}; \tag{53}$$

3° en supposant le produit $m(h+k)$ non divisible par $p-1$,

$$\mathbf{S}(t^{m(ih+jk)}) \equiv -\Pi_{-mh,-mk} \pmod{p}. \tag{54}$$

En vertu de ces dernières équivalences, la formule (30) donnera

$$\begin{cases} a_m \equiv 2 + \Pi_{-h,-k}\, t^{(p-2)m} \\ \qquad + \Pi_{-2h,-2k}\, t^{(p-3)m} + \ldots + \Pi_{-(p-2)h,-(p-2)k}\, t^{m} \end{cases} \pmod{p} \tag{55}$$

ou, ce qui revient au même,

$$a_m \equiv 2 + \Pi_{h,k}\, t^m + \Pi_{2h,2k}\, t^{3m} + \ldots + \Pi_{(p-3)h,(p-3)k}\, t^{(p-2)m} \pmod{p}, \tag{56}$$

pourvu que, t désignant l'un quelconque des nombres entiers

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

on ait soin de remplacer généralement le coefficient t^{im}, savoir

$$\Pi_{ih,ik} :$$

1° par l'unité, quand $p-1$ divisera la somme des produits ih, ik sans diviser chacun d'eux ; 2° par le nombre 2 quand $p-1$ divisera séparément chacun de ces produits.

Lorsque, à l'aide de la formule (56), on aura calculé les valeurs de

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_{p-2},$$

correspondant à une valeur donnée de t et à des valeurs de h, k pour lesquelles la somme $h+k$ n'est pas divisible par $p-1$, alors, pour obtenir la valeur de

$$R_{h,k},$$

il suffira de recourir à l'équation (12).

Pour montrer une application de la formule (56), considérons en particulier le cas où l'on aurait

$$p = 5.$$

Alors, si l'on suppose, comme on peut le faire, $t = 2$, la formule (56)

donnera

$$a_m \equiv 2 + \Pi_{h,k} 2^m + \Pi_{2h,2k} 2^{2m} + \Pi_{3h,3k} 2^{3m} \pmod 5.$$

Si d'ailleurs on prend

$$h = 1, \qquad k = 1,$$

on trouvera

$$a_m \equiv 2 + \Pi_{1,1} 2^m + \Pi_{2,2} 2^{2m} + \Pi_{3,3} 2^{3m} \pmod 5$$

ou plutôt

$$a_m \equiv 2 + \Pi_{1,1} 2^m + 2^{2m} + \Pi_{3,3} 2^{3m} \pmod 5$$

en remplaçant, comme on doit le faire,

$$\Pi_{2,2}$$

par l'unité, attendu que $p - 1 = 4$ divise la somme

$$2 + 2$$

des indices placés ici au bas de la lettre Π sans diviser séparément chacun d'eux. Comme on aura d'ailleurs, en vertu de la formule (47),

$$\Pi_{1,1} = \frac{1.2}{1.1} = 2$$

et, en vertu de la formule (49),

$$\Pi_{3,3} = 0,$$

on trouvera définitivement, dans l'hypothèse admise,

$$a_m \equiv 2 + 2^{m+1} + 2^{2m} \pmod 5,$$

ou, ce qui revient au même,

$$a_m \equiv 2 + (-1)^m + 2^{m+1} \pmod 5,$$

puis on conclura : 1° pour des valeurs paires de m,

$$a_m \equiv -2 + 2^{m+1};$$

2° pour des valeurs impaires de m,

$$a_m \equiv 1 + 2^{m+1}$$

et, par suite,

$$a_0 \equiv 0, \quad a_1 \equiv 5 \equiv 0, \quad a_2 \equiv 6 \equiv 1, \quad a_3 \equiv 17 \equiv 2 \pmod 5.$$

Donc, puisque chacun des coefficients

$$a_0, \quad a_1, \quad a_2, \quad a_3$$

doit être nul ou positif et ne peut surpasser $p - 2 = 3$, on aura nécessairement

$$a_0 = 0, \quad a_1 = 0, \quad a_2 = 1, \quad a_3 = 2.$$

Cela posé, la formule (12) donnera

$$R_{1,1} = r^3 + 2r^3.$$

On se trouve donc ainsi ramené à l'une des formules que nous avions déduites directement de la formule (8).

On pourrait remarquer que l'unité, par laquelle nous avons remplacé le coefficient

$$\Pi_{2,2} = \frac{1.2.3.4}{(1.2)(1.2)} = 6,$$

est équivalente à ce coefficient suivant le module 5. Mais on se tromperait si l'on supposait que, dans le cas où $p - 1$ divise $h + k$ sans diviser h et k, on a toujours

$$\Pi_{h,k} \equiv 1 \pmod p.$$

Effectivement, en prenant comme ci-dessus $p = 5$, on trouvera

$$\Pi_{1,3} = \frac{1.2.3.4}{1.(1.2.3)} = 4 \equiv -1 \pmod 5.$$

En général, si $p - 1$ divise $h + k$ sans diviser h et k, alors h et k, étant réduits chacun à l'un des nombres

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

fourniront une somme précisément égale à $p - 1$, en sorte qu'on aura

$$h + k = p - 1 \equiv -1 \pmod p,$$
$$k \equiv -h - 1 \pmod p,$$

et, par suite,

$$(k+1)(k+2)\ldots(k+h) \equiv (-1)^h 1.2.3.\ldots.h.$$

Or, on tire de cette dernière formule

$$(-1)^h \equiv \frac{(k+1)(k+2)\ldots(k+h)}{1.2\ldots.h} = \frac{1.2.3\ldots.(k+h)}{(1.2\ldots.h)(1.2\ldots.k)},$$

par conséquent

$$\Pi_{h,k} \equiv (-1)^h \pmod{p}; \tag{57}$$

et il résulte évidemment de l'équivalence (57) que, dans la formule (56), on peut laisser à t^{tm}, pour coefficient, l'expression

$$\Pi_{th,tk},$$

lors même que $p-1$ divise la somme $th+tk$, sans diviser th et tk, pourvu que th et tk offrent des valeurs paires.

Une conséquence importante à laquelle on se trouve immédiatement conduit par la seule inspection des formules (8) et (51), c'est que, dans le cas où la somme $h+k$ n'est pas divisible par $p-1$, l'expression

$$\Pi_{-h,-k}$$

équivaut, au signe près, à ce que devient la fonction entière de τ représentée par

$$R_{h,k},$$

quand on y remplace une racine primitive τ de l'équation

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

par une racine primitive t de l'équivalence

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

Cette dernière racine t doit d'ailleurs coïncider avec celle que renferme la formule (9).

Lorsqu'on veut appliquer à des cas particuliers les formules ci-dessus établies, toute la difficulté se réduit à trouver, pour des valeurs de h et de k positives, mais inférieures au module p, des quantités équivalentes aux expressions de la forme

$$\Pi_{h,k} = \frac{1.2.3\ldots.(h+k)}{(1.2\ldots.h)(1.2\ldots.k)},$$

c'est-à-dire aux coefficients numériques que renferme le développement de la puissance

$$(1+t)^{h+k}$$

du binome $1+t$. Le calcul direct de ces coefficients devient assez pénible lorsque le nombre t acquiert une valeur considérable. Mais alors même des quantités équivalentes à ces coefficients, suivant le module p, peuvent être assez facilement obtenues par l'une des méthodes que nous allons indiquer.

D'abord, si, en désignant par t une racine primitive de l'équivalence

$$t^{p-1} \equiv 1 \pmod{p},$$

on nomme *indices* des nombres entiers

$$1,\ 2,\ 3,\ 4,\ \ldots$$

les diverses valeurs de l'exposant i, pour lesquelles la puissance t^i deviendra successivement équivalente à ces nombres entiers suivant le module p, il est clair, d'une part, que deux nombres seront équivalents, suivant le module p, quand leurs indices seront, ou égaux, ou équivalents suivant le module $p-1$, d'autre part que l'indice d'un produit sera équivalent à la somme des indices de ses facteurs et l'indice d'un rapport à la différence des indices de ses deux termes. Cela posé, si, en se bornant à considérer des nombres entiers et des indices plus petits que la limite p, on construit deux Tables qui offrent le nombre correspondant à chaque indice et l'indice correspondant à chaque nombre, l'addition successive des indices placés à la suite les uns des autres dans la seconde Table fournira les indices des produits

$$1.2,\ 1.2.3,\ 1.2.3.4,\ \ldots$$

et dès lors il deviendra facile de calculer l'indice du rapport

$$\Pi_{h,k} = \frac{1.2.3\ldots.(h+k)}{(1.2\ldots.h)(1.2\ldots.k)},$$

par conséquent une quantité qui soit équivalente à ce rapport suivant

le module p. M. Jacobi ayant effectivement construit les Tables dont nous venons de parler pour toute valeur de p inférieure à 1000, il en résulte que, pour une semblable valeur, on obtiendra sans peine un nombre équivalent à $\Pi_{h,k}$ suivant le module p.

Il est bon d'observer qu'au lieu de réduire chaque indice à l'un des nombres

$$0,\ 1,\ 2,\ 3,\ \ldots,\ p-2,$$

on pourrait le réduire à l'une des quantités

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

Supposons, pour fixer les idées,

$$p=17.$$

Alors en prenant, comme on peut le faire, $t=10$, on reconnaîtra qu'aux nombres

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

correspondent les indices

$$0,\ 10,\ 11,\ 4,\ 7,\ 5,\ 9,\ 14,\ 6,\ 1,\ 13,\ 15,\ 12,\ 3,\ 2,\ 8$$

ou

$$0,\ -6,\ -5,\ 4,\ 7,\ 5,\ -7,\ -2,\ 6,\ 1,\ -3,\ -1,\ -4,\ 3,\ 2,\ 8.$$

Or les sommes formées par l'addition successive de ces indices seront équivalentes, suivant le module 16, aux quantités

$$0,\ -6,\ 5,\ -7,\ 0,\ 5,\ -2,\ -4,\ 2,\ 3,\ 0,\ -1,\ -5,\ -2,\ 0,\ 8.$$

Donc ces dernières quantités représenteront les indices des produits de la forme

$$1.2.3.4.\ldots.h,$$

pour les valeurs de h représentées par les nombres

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

Ainsi, en particulier, quatre de ces produits correspondront à l'indice 0 et seront, en conséquence, équivalents à l'unité suivant le module 17; tandis qu'un seul produit, ayant 8 pour indice, sera équivalent à 16 ou à -1, suivant ce même module. Les quatre produits équivalents à $+1$ seront ceux qu'on obtiendra en prenant pour h un des nombres

$$1,\ 5,\ 11,\ 15$$

et se réduiront à

$$1,\quad 1.2.3.4.5,$$

$$1.2.3.4.5.6.7.8.9.10.11,\quad 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15,$$

tandis que le seul produit, équivalent à -1, sera, conformément à un théorème connu, le produit de tous les nombres entiers positifs inférieurs au module 17, savoir:

$$1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16.$$

Il sera maintenant facile de calculer les valeurs de

$$\Pi_{h,k}$$

correspondant à la valeur 17 du module p et à des valeurs données de h, k. Ainsi, par exemple, en posant

$$h=4,\qquad k=4,\qquad h+k=8,$$

on trouvera pour indice des produits

$$1.2.3.4,\quad 1.2.3.4.5.6.7.8$$

les quantités

$$-7,\quad -4.$$

Donc l'indice du rapport

$$\Pi_{h,k}=\frac{1.2.3.4.5.6.7.8}{(1.2.3.4)(1.2.3.4)}$$

sera

$$-4+7+7=10\equiv -6\pmod{16},$$

et, en conséquence, ce rapport sera équivalent, suivant le module 17, au nombre 2. Pareillement, si l'on prend

$$h=2,\qquad k=6,\qquad h+k=8,$$

on trouvera pour indices des produits

$$1.2, \quad 1.2.3.4.5.6, \quad 1.2.3.4.5.6.7.8$$

les quantités

$$-6, \quad 5, \quad -4.$$

Donc l'indice du rapport

$$\Pi_{2,6} = \frac{1.2.3.4.5.6.7.8}{(1.2)(1.2.3.4.5.6)}$$

sera

$$-4+6-5=-3,$$

et, en conséquence, ce rapport sera équivalent, suivant le module 17, au nombre 11 ou, ce qui revient au même, à la quantité négative -6.

Au reste, sans recourir aux Tables qui fournissent, pour chaque module, l'indice correspondant à un nombre ou le nombre correspondant à un indice donné, on pourrait, à l'aide de simples additions et soustractions, obtenir facilement des quantités équivalentes aux diverses valeurs de $\Pi_{h,k}$, c'est-à-dire aux nombres figurés des divers ordres. En effet, d'après les propriétés bien connues de ces nombres, on peut les déduire par addition les uns des autres en formant ce qu'on appelle le *triangle arithmétique* de Pascal. Il suffira donc, pour arriver au but qu'on se propose, de calculer quelques-uns des termes que doit renfermer le triangle arithmétique en réduisant chacun d'eux à un nombre inférieur au module donné ou à une quantité dont la valeur numérique ne surpasse pas la moitié de ce module. Entrons à ce sujet dans quelques détails.

Supposons les deux nombres h, k inférieurs au module p ou même à $p-1$. Il suit évidemment de la formule (47) que les valeurs de

$$\Pi_{h,k}, \quad \Pi_{h-1,k}, \quad \Pi_{h,k-1}$$

seront respectivement égales aux produits du rapport

$$\frac{1.2.3.\ldots.(h+k-1)}{[(1.2.\ldots.(h-1)][(1.2.\ldots.(k-1)]}$$

par les trois nombres

$$\frac{h+k}{hk}, \quad \frac{1}{k}, \quad \frac{1}{h}.$$

Or, comme le premier de ces trois nombres est précisément la somme des deux autres, nous devons en conclure qu'on aura

$$\Pi_{h,k} = \Pi_{h-1,k} + \Pi_{h,k-1}. \tag{58}$$

De plus, il est clair qu'on aura, en vertu de la formule (47), non seulement

$$\Pi_{h,k} = \Pi_{k,h}, \tag{59}$$

mais encore

$$\Pi_{h,1} = h+1, \qquad \Pi_{1,k} = k+1. \tag{60}$$

Cela posé, imaginons une Table, analogue à la Table de Pythagore, dans laquelle la première ligne verticale et la première ligne horizontale renferment les valeurs de h, k positives et inférieures à p ou même à $p-1$, c'est-à-dire les nombres

$$1, \quad 2, \quad 3, \quad 4, \quad \ldots, \quad p-2,$$

et concevons que, dans la case correspondant à des valeurs données de h, k, on place une quantité, non seulement équivalente à $\Pi_{h,k}$, suivant le module p, mais, de plus, renfermée entre les limites $-\frac{p}{2}, +\frac{p}{2}$.

Il résulte des formules (60) que, dans la Table dont il s'agit, chaque terme de la seconde ligne horizontale ou verticale sera équivalent au terme correspondant de la première ligne augmenté de l'unité, et de la formule (58) que, dans chacune des autres lignes horizontales et verticales, un terme quelconque sera équivalent à la somme des deux termes antérieur et supérieur, c'est-à-dire des deux termes qui le précèdent immédiatement, l'un dans la même ligne horizontale, l'autre dans la même ligne verticale. Or, ces remarques fournissent un moyen très simple de construire la Table que nous venons d'imaginer et qui, dans le cas où l'on suppose $p=17$, se réduit à la suivante :

Quantités équivalentes aux nombres figurés suivant le module $p = 17$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8	−8	−7	−6	−5	−4	−3	−2	−1	0
2	3	6	−7	−2	4	−6	2	−6	4	−2	−7	6	3	1	0	
3	4	−7	3	1	5	−1	1	−5	−1	−3	7	−4	−1	0		
4	5	−2	1	2	7	6	7	2	1	−2	5	1	0			
5	6	4	5	7	−3	3	−7	−5	−4	−6	−1	0				
6	7	−6	−1	6	3	6	−1	−6	7	1	0					
7	8	2	1	7	−7	−1	−2	−8	−1	0						
8	−8	−6	−5	2	−5	−6	−8	1	0							
9	−7	4	−1	1	−4	7	−1	0								
10	−6	−2	−3	−2	−6	1	0									
11	−5	−7	7	5	−1	0										
12	−4	6	−4	1	0											
13	−3	3	−1	0												
14	−2	1	0													
15	−1	0														
16	0															

Dans la Table précédente, on s'est dispensé d'écrire les quantités auxquelles $\Pi_{h,k}$ devient équivalent, lorsque la somme $h + k$ est renfermée entre les limites p, $2(p-1)$; attendu que ces quantités, en vertu de la formule (49), se réduisent toutes à zéro, comme celles qui correspondent au cas où l'on a

$$h + k = p.$$

Quant à celles qui répondent au cas où l'on a

$$h + k = p - 1,$$

elles se réduisent alternativement, en vertu de la formule (57), à $+1$ ou à -1, selon que h est pair ou impair, et occupent les cases situées sur l'une des diagonales de la Table. Les cases situées sur l'autre diagonale renferment les quantités

$$2,\ 6,\ 3,\ 2,\ -3,\ 6,\ -2,\ 1$$

qui représentent les valeurs de

$$\Pi_{h,h}$$

correspondant aux valeurs

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8$$

du nombre h; et, dans les cases symétriquement placées à l'égard de cette autre diagonale, on trouve des quantités deux à deux égales entre elles, conformément à l'équation (59). Ajoutons que les quantités écrites dans la partie du Tableau comprise entre la première ligne horizontale, la première ligne verticale et la première diagonale, sont encore, dans chaque ligne horizontale ou verticale, égales deux à deux, au signe près, à distances égales des extrémités de chaque ligne. Or, c'est ce qu'il était facile de prévoir. Car si l'on nomme

$$h,\ k,\ l$$

trois quantités entières, non divisibles par $p-1$ et choisies de manière à vérifier la formule

$$h + k + l = p - 1 \tag{61}$$

ou même, plus généralement, de manière à vérifier l'équivalence

$$h + k + l \equiv 0 \pmod{p-1}, \tag{62}$$

on aura, en vertu de l'équation (3),

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

et, par suite,

$$R_{h,k} = \frac{\Theta_h \Theta_k}{\Theta_{h+k}} = (-1)^l \frac{\Theta_h \Theta_k \Theta_l}{p}.$$

Or, cette dernière équation devant subsister, ainsi que la for-

mule (61) ou (62), lorsqu'on échange entre eux les nombres

$$h, \quad k, \quad l,$$

on en conclura

$$\frac{\Theta_h \Theta_k \Theta_l}{p} = (-1)^k R_{k,l} = (-1)^k R_{l,h} = (-1)^l R_{h,k}. \tag{63}$$

On aura donc, dans l'hypothèse admise,

$$(-1)^h R_{k,l} = (-1)^k R_{l,h} = (-1)^l R_{h,k}; \tag{64}$$

et, en remplaçant τ par t, on trouvera

$$(-1)^h \Pi_{k,l} \equiv (-1)^k \Pi_{l,h} \equiv (-1)^l \Pi_{h,k} \pmod{p}. \tag{65}$$

On tirera d'ailleurs de la formule (65)

$$\Pi_{h,l} \equiv (-1)^{l-k} \Pi_{h,k} \equiv (-1)^h \Pi_{h,k} \pmod{p}$$

ou, ce qui revient au même,

$$\Pi_{h,p-1-h-k} \equiv (-1)^h \Pi_{h,k} \pmod{p}. \tag{66}$$

Il serait au reste facile de déduire directement la formule (66) de l'équation (47), par un calcul semblable à celui qui nous a conduits à la formule (57).

Les formules (49), (57), (58), (59), (60), (66) offrent le moyen de simplifier la recherche des quantités équivalentes à $\Pi_{h,k}$, et la construction de la Table qui les renferme; et d'abord il résulte des formules (49), (57) qu'on pourra se borner à calculer, dans cette Table, les termes correspondant à des valeurs de h, k, pour lesquelles on aura

$$h + k < p - 1. \tag{67}$$

De plus, eu égard à la formule (59), on pourra supposer que h est le plus petit des deux nombres h, k, lorsque ces deux nombres deviennent inégaux; et, en admettant cette supposition, on tirera de la formule (67)

$$h < \frac{p-1}{2}. \tag{68}$$

Ce n'est pas tout : en vertu de la formule (66), on pourra se borner à calculer celles des quantités équivalentes à $\Pi_{h,k}$ pour lesquelles on a

$$k \leq p - 1 - h - k,$$

par conséquent,

$$k \leq \frac{p-1-h}{2}; \tag{69}$$

et, de la condition

$$h \leq k,$$

combinée avec la formule (69), on tirera

$$h \leq \frac{p-1}{3}. \tag{70}$$

On pourra donc, dans la Table ci-dessus mentionnée, conserver seulement la première ligne horizontale et la première ligne verticale, avec les cases correspondant aux valeurs de h, comprises entre les limites

$$h = 1, \quad h = \frac{p-1}{3} \quad \text{ou} \quad \frac{p-2}{3},$$

et aux valeurs de k, renfermées entre les limites

$$k = h, \quad k = \frac{p-1-h}{2} \quad \text{ou} \quad \frac{p-2-k}{2}.$$

Ainsi, en particulier, si l'on suppose $p = 17$, la Table dont il s'agit pourra être réduite à la suivante :

Quantités équivalentes aux nombres figurés suivant le module 17.

	1	2	3	4	5	6	7
1	2	3	4	5	6	7	8
2		6	−7	−2	4	−6	2
3			3	1	5	−1	
4				2	7	6	
5					−3		

Pour construire cette dernière Table, il suffit de placer dans la première ligne verticale les valeurs de h inférieures à

$$\frac{p-1}{3} = 5 + \frac{1}{3},$$

savoir

$$1,\ 2,\ 3,\ 4,\ 5,$$

et dans la première ligne horizontale, les valeurs de k inférieures à

$$\frac{p-1}{2} = 8,$$

savoir

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7;$$

puis de remplir, pour chaque valeur de h, les cases correspondant aux valeurs de k comprises entre les limites

$$h,\quad \frac{p-1-h}{2},$$

en opérant comme il suit :

Pour obtenir les termes

$$2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8$$

qui devront composer la deuxième ligne horizontale, on ajoutera l'unité aux termes correspondants de la première ligne. De plus, comme des formules (58) et (59) on tire

$$\Pi_{h,h} = 2\,\Pi_{h-1,h}, \tag{71}$$

il est clair que, dans chacune des lignes horizontales qui suivront la deuxième, le premier terme conservé devra être équivalent, suivant le module 17, au double du terme immédiatement supérieur, et chacun des autres termes conservés à la somme faite des deux termes placés en avant et au-dessus de celui que l'on considère.

En opérant de cette manière, on trouvera pour termes de la troisième ligne horizontale, les quantités

$$6 = 2.3,\quad -7 \equiv 6+4,\quad -2 = -7+5,\quad 4 = -2+6,$$
$$-6 \equiv 4+7,\quad 2 \equiv -6+8;$$

pour termes de la quatrième ligne, les quantités

$$3 \equiv 2(-7),\quad 1 = 3-2,\quad 5 = 1+4,\quad -1 = 5-6;$$

pour termes de la cinquième ligne, les quantités

$$2 = 2.1,\quad 7 = 2+5,\quad 6 = 7-1;$$

enfin, pour terme unique de la sixième ligne horizontale, la quantité

$$-3 \equiv 2.7 \pmod{17}.$$

A la seule inspection de la Table construite comme on vient de le dire, on obtiendra immédiatement les quantités équivalentes à $\Pi_{h,k}$, pour des valeurs de h et de k non situées hors des limites

$$h = 1,\quad h = \frac{p-1}{3};\quad k = h,\quad k = \frac{p-1-h}{2}; \tag{72}$$

et l'on trouvera, par exemple, en supposant toujours $p = 17$,

$$\Pi_{4,4} \equiv 2,\quad \Pi_{2,6} \equiv -6 \pmod{17}.$$

Si les valeurs de h, k, n'étant plus situées entre les limites (72), étaient néanmoins des valeurs positives propres à vérifier encore la condition (67), on devrait joindre à la Table construite les formules (59) et (66). On trouverait ainsi, par exemple,

$$\begin{aligned} &\Pi_{8,8} = \Pi_{6,2} = \Pi_{2,6} = 6 \\ &\Pi_{7,7} = -\Pi_{7,2} = -\Pi_{2,7} = -2 \end{aligned} \pmod{17}.$$

Enfin, si les quantités h, k acquéraient des valeurs quelconques positives ou négatives, mais non divisibles par $p-1$, on devrait d'abord les réduire, par l'addition ou la soustraction de $p-1$ ou de ses multiples, à des quantités positives, mais inférieures à $p-1$, puis, après cette réduction, on aurait recours soit à la formule (49), soit à la formule (57), soit à la Table construite et aux formules (59), (66),

suivant que la somme h + k serait supérieure, égale ou inférieure au nombre $p - 1$.

Il est inutile de s'occuper du cas où l'une des quantités h, k et, par suite, l'une des quantités h, k deviendrait divisible par p, attendu que, dans cette hypothèse, on n'a plus besoin de recourir à la formule (56) pour déterminer la valeur de $R_{h,k}$ qui, en vertu de l'équation (5), se réduit à -1.

Un moyen fort simple de prévenir et de reconnaître les erreurs qui pourraient se glisser dans la construction de la Table ci-dessus mentionnée, consiste à introduire dans chaque ligne horizontale un terme de plus. Effectivement, en vertu de la formule (66), si l'on fait entrer un nouveau terme dans une ligne horizontale correspondant à une valeur donnée de h, ce nouveau terme devra être égal au terme précédent, pris en signe contraire, ou à l'avant-dernier terme de la même ligne, suivant que la valeur de h sera un nombre impair ou un nombre pair. Donc si, au moment où l'on parvient à l'extrémité d'une ligne horizontale, il arrivait que la condition dont nous venons de parler ne fût pas remplie, on devrait recommencer le calcul des termes compris dans cette ligne. En opérant comme on vient de le dire, et supposant par exemple $n = 17$, on obtiendra, au lieu de la Table trouvée plus haut, celle que nous allons transcrire :

Quantités équivalentes aux nombres figurés suivant le module 17.

	1	2	3	4	5	6	7	8
1	2	3	4	5	6	7	8	−8
2		6	−7	−2	4	−6	2	−6
3			3	1	5	−1	1	
4				2	7	6	7	
5					−3	3		

Si l'on supposait au contraire $p = 19$ ou $p = 29$, on obtiendrait les Tableaux suivants :

Quantités équivalentes aux nombres figurés suivant le module 19.

	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	−9
2		6	−9	−4	2	9	−2	7	−2
3			1	−3	−1	8	6	−6	
4				−6	−7	1	7	1	
5					5	6	−6		
6						−7			

Quantités équivalentes aux nombres figurés suivant le module 29

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

Lorsque, dans la formule (56), on substitue les quantités équivalentes à

$$\Pi_{h,k},\quad \Pi_{2h,2k},\quad \ldots,\quad \Pi_{(p-2)h,(p-2)k},$$

déterminées par l'une des méthodes que nous venons d'exposer, on obtient une valeur de a_m qui dépend évidemment de la valeur attribuée

à t. Or, t désignant une des racines primitives de l'équation

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

si l'on pose

$$t^{\iota} = t',$$

ι étant un nombre premier à $p-1$, t' sera une autre racine primitive de la même équivalence; et comme, dans Θ_h, le coefficient de

$$\theta^{t^{\iota m}} = \theta^{t^{\iota m}}$$

sera

$$\tau^{m\iota h},$$

il est clair que, remplacer dans Θ_h, t par t', revient à y remplacer τ^h par $\tau^{\iota h}$. Donc, substituer à la racine primitive t la racine primitive $t' \equiv t^{\iota}$, c'est, en d'autres termes, transformer Θ_h en $\Theta_{\iota h}$, par conséquent Θ_h en $\Theta_{\iota h}$, et

$$R_{h,k} = \frac{\Theta_h \Theta_k}{\Theta_{h+k}}$$

en

$$R_{\iota h,\iota k} = \frac{\Theta_{\iota h}\Theta_{\iota k}}{\Theta_{\iota(h+k)}}.$$

Ainsi, par exemple, comme, en prenant $p = 5$ et

$$t = 2,$$

on trouve

$$R_{1,1} = \tau^2 + 2\tau^3, \qquad R_{3,3} = \tau^6 + 2\tau,$$

si l'on prend, au contraire,

$$t = 3 \equiv 2^3 \pmod{5},$$

on trouvera

$$R_{1,1} = \tau^6 + 2\tau^9 = \tau^2 + 2\tau^3, \qquad R_{3,3} = \tau^{18} + 2\tau^{27} = \tau^2 + 2\tau^3.$$

Donc, substituer à la racine primitive 2 la racine primitive

$$3 \equiv 2^3 \pmod{5},$$

ce sera transformer

$$R_{1,1} \quad \text{en} \quad R_{3,3}$$

et réciproquement

$$R_{3,3} \quad \text{en} \quad R_{9,9} = R_{1,1}.$$

Les diverses formules obtenues dans cette Note se rapportent au cas où la valeur de Θ_h est donnée par l'équation (1). Si, en désignant par n un diviseur de $p-1$, et posant

$$p - 1 = n\varpi, \tag{73}$$

on nommait

$$\rho, \quad r$$

des racines primitives des formules

$$x^n \equiv 1 \quad \text{et} \quad x^{\varpi} \equiv 1 \pmod{p},$$

on pourrait prendre

$$\rho = \tau^{\varpi}, \qquad r \equiv t^{\varpi} \pmod{p}.$$

Alors, en remplaçant

$$h \text{ par } \varpi h, \qquad k \text{ par } \varpi k,$$

puis écrivant, pour abréger,

$$\begin{aligned} \Theta_h &\quad \text{au lieu de} \quad \Theta_{\varpi h}, \\ R_{h,k} &\quad \text{»} \quad R_{\varpi h,\varpi k}, \\ \Pi_{h,k} &\quad \text{»} \quad \Pi_{\varpi h,\varpi k}, \end{aligned}$$

on obtiendrait, à la place des formules trouvées dans cette Note, des formules analogues obtenues dans le Mémoire. Ainsi, en particulier, la valeur de Θ_h serait généralement fournie, non plus par l'équation (1), mais par la suivante

$$\Theta_h = \theta + \rho^h \theta^r + \rho^{rh}\theta^{r^2} + \ldots + \rho^{(p-2)h}\theta^{r^{p-2}}, \tag{74}$$

et l'on aurait : 1° en supposant h divisible par n,

$$\Theta_h = \Theta_0 = -1; \tag{75}$$

2° en supposant h non divisible par n,

$$\Theta_h \Theta_{-h} = (-1)^{\varpi h} p. \tag{76}$$

De plus, en posant toujours

$$\Theta_h\Theta_k = R_{h,k}\Theta_{h+k},$$

ou, ce qui revient au même,

$$R_{h,k} = \frac{\Theta_h\Theta_k}{\Theta_{h+k}}, \tag{77}$$

on trouverait : 1° pour des valeurs de h ou de k divisibles par n,

$$R_{h,k} = -1; \tag{78}$$

2° pour des valeurs de h non divisibles par n,

$$R_{h,-h} = -(-1)^{\varpi h} p; \tag{79}$$

3° pour des valeurs de h, de k et de $h+k$, non divisibles par n,

$$R_{h,k}R_{-h,-k} = p. \tag{80}$$

Ajoutons que, si $h+k$ n'est pas divisible par n, l'on aura

$$R_{h,k} = S(\rho^{ih+jk}), \tag{81}$$

le signe S s'étendant à toutes les valeurs de i comprises dans la suite

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

et les valeurs correspondantes de i, j étant choisies de manière à vérifier la condition (9), c'est-à-dire la formule

$$i^j + i^j \equiv 1 \pmod{p}.$$

Concevons maintenant que, dans le second membre de la formule (81), on réduise l'exposant de chaque puissance de ρ à l'un des nombres

$$0,\ 1,\ 2,\ 3,\ \ldots,\ n-1.$$

Ce second membre deviendra une fonction entière de ρ, du degré $n-1$; et l'on aura identiquement

$$S(\rho^{ih+jk}) = a_0 + a_1\rho + a_2\rho^2 + \ldots + a^{n-1}\rho^{n-1}, \tag{82}$$

$a_0, a_1, a_2, \ldots, a_{n-1}$ désignant des nombres entiers, dont plusieurs pourront s'évanouir, et dont la somme, égale au nombre des valeurs de i, vérifiera la formule

$$a_0 + a_1 + a_2 + \ldots + a_{n-1} = p - 2. \tag{83}$$

Cela posé, l'équation (81) donnera

$$R_{h,k} = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1}. \tag{84}$$

Concevons d'ailleurs que, pour se conformer aux conventions ci-dessus adoptées, l'on remplace

$$h \text{ par } \varpi h \quad \text{et} \quad k \text{ par } \varpi k,$$

dans le second membre de la formule (47). Cette formule, réduite à

$$\Pi_{h,k} = \frac{1.2.3\ldots[\varpi(h+k)]}{(1.2\ldots\varpi h)(1.2\ldots\varpi k)}, \tag{85}$$

fournira la valeur de $\Pi_{h,k}$, dans le cas où les quantités h, k se réduiront à deux termes de la suite

$$1,\ 2,\ 3,\ \ldots,\ n;$$

et, dans le cas contraire, $\Pi_{h,k}$ représentera ce que devient le rapport

$$\frac{1.2.3\ldots[\varpi(h+k)]}{(1.2.3\ldots\varpi h)(1.2.3\ldots\varpi k)}$$

quand on y remplace les quantités entières h, k par les deux termes de la suite

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

qui sont équivalents à ces mêmes quantités, suivant le module n. D'autre part, à l'aide de raisonnements semblables à ceux par lesquels nous avons établi les formules (19) et (26), on prouvera que les valeurs de

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},$$

renfermées dans les équations (82) et (84), vérifient non seulement

les formules

$$(86)\quad \begin{cases} a_0 + a_1 + a_2 + \ldots + a_{n-1} = p-2, \\ a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1} = S(\rho^{ih+jk}), \\ a_0 + a_1\rho^2 + a_2\rho^4 + \ldots + a_{n-1}\rho^{2(n-1)} = S(\rho^{2(ih+jk)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_0 + a_1\rho^{n-1} + a_2\rho^{2(n-1)} + \ldots + a_{n-1}\rho^{(n-1)^2} = S(\rho^{(n-1)(ih+jk)}), \end{cases}$$

mais encore les suivantes :

$$(87)\quad \begin{cases} a_0 + a_1 + a_2 + \ldots + a_{n-1} \equiv p-2 \pmod p, \\ a_0 + a_1 r + a_2 r^2 + \ldots + a_{n-1} r^{n-1} \equiv S(r^{ih+jk}), \\ a_0 + a_1 r^2 + a_2 r^4 + \ldots + a_{n-1} r^{2(n-1)} \equiv S(r^{2(ih+jk)}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_0 + a_1 r^{n-1} + a_2 r^{2(n-1)} + \ldots + a_{n-1} r^{(n-1)^2} \equiv S(r^{(n-1)(ih+jk)}), \end{cases}$$

et de ces dernières, respectivement multipliées par les facteurs

$$1,\quad r^{-m},\quad r^{-2m},\quad \ldots,\quad r^{-(n-1)m},$$

puis, combinées entre elles par voie d'addition, l'on conclura

$$(88)\quad \begin{cases} n a_m \equiv p-2 + r^{-m}S(r^{ih+jk}) + r^{-2m}S(r^{2(ih+jk)}) + \ldots \\ \qquad + r^{-(n-1)m}S(r^{(n-1)(ih+jk)}) \end{cases} \pmod p.$$

De plus, si l'on remplace h par ϖh et k par ϖk dans les premiers membres des formules (52), (53), (54), on tirera de ces formules : 1° en supposant mh et nk séparément divisibles par n,

$$(89)\qquad S(r^{m(ih+jk)}) \equiv -2 \pmod p;$$

2° en supposant que n divise la somme

$$m(h+k) = mh + mk,$$

sans diviser ses deux parties mh, mk,

$$(90)\qquad S(r^{m(ih+jk)}) \equiv -1 \pmod p;$$

3° en supposant le produit $m(h+k)$ non divisible par n

$$(91)\qquad S(r^{m(ih+jk)}) \equiv -\Pi_{-mh,-mk} \pmod p,$$

attendu que l'on devra, en vertu des conditions admises, écrire simplement $\Pi_{mh,mk}$ au lieu de $\Pi_{m\varpi h,m\varpi k}$. Donc la formule (88) donnera

$$(92)\quad \begin{cases} -n a_m \equiv 2 + \Pi_{-h,-k} r^{-m} + \Pi_{-2h,-2k} r^{-2m} + \ldots \\ \qquad + \Pi_{-(n-1)h,-(n-1)k} r^{-(n-1)m} \end{cases} \pmod p,$$

ou, ce qui revient au même,

$$(93)\qquad -n a_m \equiv 2 + \Pi_{h,k} r^m + \Pi_{2h,2k} r^{2m} + \ldots + \Pi_{(n-1)h,(n-1)k} r^{(n-1)m} \pmod p,$$

pourvu que, t désignant l'un quelconque des nombres entiers,

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

l'on ait soin de remplacer généralement le coefficient de r^{tm}, savoir :

$$\Pi_{th,tk},$$

1° par l'unité, quand n divisera la somme des produits th, tk sans diviser chacun d'eux ; 2° par le nombre 2 quand n divisera séparément chacun de ces produits. Enfin, comme on tire de l'équation (73)

$$n\varpi \equiv -1 \pmod p,$$

il est clair qu'en multipliant par ϖ les deux membres de la formule (93), on la réduira immédiatement à celle-ci

$$(94)\qquad a_m \equiv (2 + \Pi_{h,k} r^m + \Pi_{2h,2k} r^{2m} + \ldots + \Pi_{(n-1)h,(n-1)k} r^{(n-1)m})\varpi \pmod p.$$

Pour appliquer à des cas particuliers la formule (94), on devra d'abord rechercher des quantités équivalentes, suivant le module p, aux nombres figurés qui représenteront les diverses valeurs de $\Pi_{h,k}$. On y parviendra sans peine à l'aide des méthodes précédemment exposées, en commençant par réduire chacune des quantités h, k à un terme de la suite

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

Après cette réduction, si l'on a

$$h + k > n,$$

ou

$$h + k = n,$$

on en conclura, dans le premier cas,

$$\Pi_{h,k} \equiv 0 \pmod{p}, \tag{95}$$

et, dans le second cas,

$$\Pi_{h,k} \equiv (-1)^{\varpi h} \pmod{p}. \tag{96}$$

Si l'on a, au contraire,

$$h + k < n,$$

on pourra, eu égard aux deux formules

$$\Pi_{k,h} = \Pi_{h,k} \tag{97}$$

et

$$\Pi_{h,n-k-h} \equiv (-1)^{\varpi h} \Pi_{h,k} \pmod{p}, \tag{98}$$

ramener la recherche d'une quantité qui soit équivalente à $\Pi_{h,k}$ suivant le module p, au cas particulier dans lequel h, k représenteraient deux nombres non situés hors des limites

$$h = 1, \quad h = \frac{n}{3}; \quad k = h, \quad k = \frac{n-h}{2}. \tag{99}$$

D'ailleurs, h, k étant deux nombres de cette espèce, le terme équivalent à $\Pi_{h,k}$, dans la Table que nous avons appris à construire, sera celui que renfermeront la ligne horizontale, dont le premier terme est ϖh, et la ligne verticale, dont le premier terme est ϖk.

Concevons, pour fixer les idées, que l'on prenne

$$p = 17, \quad n = 4.$$

On aura

$$\varpi = \frac{p-1}{n} = \frac{16}{4} = 4,$$

et par suite le terme équivalent à $\Pi_{1,1}$, dans la Table de la page 208, sera celui que renferment les lignes horizontale et verticale, dont les

premiers termes se réduisent au nombre $\varpi = 4$. On aura donc

$$\Pi_{1,1} \equiv 2 \pmod{17}.$$

Si, en supposant toujours $p = 17$, on prenait

$$n = 8,$$

on trouverait

$$\varpi = \frac{16}{8} = 2;$$

et, par suite, le terme équivalent à $\Pi_{1,3}$ dans la Table dont il s'agit, serait celui que renferment les lignes horizontale et verticale dont les premiers termes se réduisent aux nombres

$$\varpi = 2, \quad 3\varpi = 6.$$

On aurait donc alors

$$\Pi_{1,3} \equiv -6 \pmod{17}.$$

Soit encore

$$p = 29, \quad n = 7.$$

On trouvera

$$\varpi = \frac{28}{7} = 4;$$

et le second Tableau de la page 209, joint à la formule (98), donnera

$$\Pi_{1,1} \equiv 12, \quad \Pi_{2,2} \equiv -6, \quad \Pi_{3,3} \equiv \Pi_{1,3} \equiv -7 \pmod{29}.$$

On aura d'ailleurs

$$\Pi_{4,4} \equiv 0, \quad \Pi_{5,5} \equiv 0, \quad \Pi_{6,6} \equiv 0.$$

Enfin, si, en nommant ρ une racine primitive de l'équation

$$x^7 = 1,$$

l'on pose

$$R_{1,1} = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + a_4\rho^4 + a_5\rho^5 + a_6\rho^6,$$

la formule (94), jointe à celles que nous venons d'obtenir, donnera

$$a_m \equiv 4(2 + 12r^m - 6r^{2m} - 7r^{3m}) \pmod{p},$$

r étant une racine primitive de l'équivalence

$$x^7 \equiv 1 \pmod{29}.$$

D'autre part,

$$t = 10$$

étant une racine primitive de l'équivalence

$$x^{28} \equiv 1 \pmod{29},$$

on pourra prendre

$$r = t^{\varpi} = t^{4} \equiv -5 \pmod{29},$$

ce qui réduira la valeur trouvée de a_m à

$$a_m \equiv 4[2 + 12(-5)^m - 6.5^{2m} - 7(-5)^{3m}] \pmod{p}.$$

Si, dans cette dernière formule, on attribue successivement à m les valeurs

$$0, \quad 1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6,$$

on trouvera

$$a_0 \equiv a_4 \equiv a_5 \equiv 4, \qquad a_1 \equiv 0, \qquad a_2 \equiv a_3 \equiv 6, \qquad a_6 \equiv 3 \pmod{29};$$

et, par suite, puisque chacun des coefficients

$$a_0, \quad a_1, \quad a_2, \quad a_3, \quad a_4, \quad a_5, \quad a_6$$

doit être nul ou positif, mais inférieur au module 29, on aura

$$a_0 = a_4 = a_5 = 4, \qquad a_1 = 0, \qquad a_2 = a_3 = 6, \qquad a_6 = 3$$
$$R_{1,1} = 3\rho^6 + 4(1 + \rho^4 + \rho^5) + 6(\rho^2 + \rho^3).$$

Si maintenant on substitue à ρ l'une des puissances

$$\rho^2, \quad \rho^3, \quad \rho^4, \quad \rho^5, \quad \rho^6,$$

on trouvera immédiatement

$$R_{2,2} = 3\rho^5 + 4(1 + \rho + \rho^3) + 6(\rho^4 + \rho^6),$$
$$R_{3,3} = 3\rho^4 + 4(1 + \rho^5 + \rho) + 6(\rho^6 + \rho^2),$$
$$R_{4,4} = 3\rho^2 + 4(1 + \rho^2 + \rho^6) + 6(\rho + \rho^5),$$
$$R_{5,5} = 3\rho^3 + 4(1 + \rho^6 + \rho^4) + 6(\rho^2 + \rho),$$
$$R_{6,6} = 3\rho + 4(1 + \rho^3 + \rho^2) + 6(\rho^5 + \rho^4).$$

Si, en prenant toujours

$$p = 29, \qquad n = 7,$$

on supposait

$$R_{1,2} = a_0 + a_1\rho + a_2\rho^2 + a_3\rho^3 + a_4\rho^4 + a_5\rho^5 + a_6\rho^6,$$

alors de la formule (94), combinée avec les suivantes :

$$\Pi_{1,2} = 2, \qquad \Pi_{2,4} = \Pi_{2,1} = 2, \qquad \Pi_{4,8} = \Pi_{4,1} = \Pi_{2,1} = 2,$$
$$\Pi_{3,6} = 0, \qquad \Pi_{5,10} = \Pi_{5,3} = 0, \qquad \Pi_{6,12} = \Pi_{6,5} = 0,$$

on tirerait

$$a_m \equiv 8(1 + r^m + r^{2m} + r^{4m}) \pmod{29},$$
$$a_0 \equiv 8.4 \equiv 32 \equiv 3 \pmod{29}$$
$$a_0 = 3;$$

puis, en prenant $r = -5$, on trouverait

$$a_1 = a_2 = a_4 = 6, \qquad a_3 = a_5 = a_6 = 2,$$

et l'on aurait par suite

$$R_{1,2} = 3 + 6(\rho + \rho^2 + \rho^4) + 2(\rho^3 + \rho^5 + \rho^6).$$

Comme on aura d'ailleurs

$$\rho + \rho^2 + \rho^3 + \rho^4 + \rho^5 + \rho^6 = -1,$$

si l'on pose, pour abréger,

$$\rho + \rho^2 + \rho^4 - \rho^3 - \rho^5 - \rho^6 = \Delta,$$

on trouvera encore

$$\rho + \rho^4 + \rho^5 = -\frac{1 - \Delta}{2}, \qquad \rho^3 + \rho^2 + \rho^6 = -\frac{1 + \Delta}{2},$$

et par suite la valeur de $R_{1,2}$ deviendra

$$R_{1,2} = -1 + 2\Delta.$$

En remplaçant successivement dans cette dernière formule ρ par chacune des puissances

$$\rho^2, \quad \rho^3, \quad \rho^4, \quad \rho^5, \quad \rho^6,$$

on en tirera

$$R_{1,2}=R_{2,4}=R_{4,8}=-1+2\Delta, \qquad R_{3,6}=R_{5,10}=R_{6,12}=-1-2\Delta,$$

ou, ce qui revient au même,

$$R_{1,2}=R_{2,4}=R_{4,1}=-1+2\Delta, \qquad R_{3,6}=R_{5,3}=R_{6,5}=-1-2\Delta.$$

Nous remarquerons, en terminant cette Note, que, dans le cas où l'on suppose la valeur de Θ_h déterminée, non par l'équation (1), mais par l'équation (74), la formule (63) doit être, eu égard aux notations adoptées dans la seconde hypothèse, remplacée par cette autre formule

$$\frac{\Theta_h\Theta_k\Theta_l}{p}=(-1)^{\varpi h}R_{k,l}=(-1)^{\varpi k}R_{l,h}=(-1)^{\varpi l}R_{h,k},$$

qui, pour des valeurs paires du nombre ϖ, se réduit simplement à

$$\frac{\Theta_h\Theta_k\Theta_l}{p}=R_{k,l}=R_{l,h}=R_{h,k}.$$

On doit d'ailleurs, dans ces deux dernières formules, prendre pour

$$h, \quad k, \quad l$$

trois quantités entières, non divisibles par n, et choisies de manière à vérifier non plus la condition (62), mais la suivante :

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

Si, pour fixer les idées, on suppose $n=7$, on pourra prendre

$$h=1, \quad k=2, \quad l=4,$$

ou bien

$$h=3, \quad k=5, \quad l=6,$$

attendu qu'on aura, dans le premier cas

$$h+k+l=7,$$

et dans le second

$$h+k+l=14=2.7.$$

D'ailleurs, le nombre $n=7$ étant impair, le nombre

$$\varpi=\frac{p-1}{n}=\frac{p-1}{7}$$

devra être pair ainsi que $p-1$. Donc, en supposant $n=7$, on trouvera

$$\frac{\Theta_1\Theta_2\Theta_4}{p}=R_{1,2}=R_{2,4}=R_{4,1}, \qquad \frac{\Theta_3\Theta_5\Theta_6}{p}=R_{3,6}=R_{5,3}=R_{6,5};$$

ce qui s'accorde avec les formules déjà obtenues. Comme on aura d'ailleurs, dans la même supposition, non seulement

$$R_{1,1}=\frac{\Theta_1^2}{\Theta_2}, \qquad R_{2,2}=\frac{\Theta_2^2}{\Theta_4},$$

mais encore

$$R_{4,4}=\frac{\Theta_4^2}{\Theta_8}=\frac{\Theta_4^2}{\Theta_1},$$

on en conclura

$$R_{1,1}R_{2,2}R_{4,4}=\Theta_1\Theta_2\Theta_4=pR_{1,2}.$$

Or, il sera facile de vérifier cette dernière formule, en prenant $p=29$. Alors, en effet, en vertu de la formule

$$\rho+\rho^2+\rho^3+\rho^4+\rho^5+\rho^6=-1,$$

on pourra réduire les valeurs précédemment calculées de $R_{1,1}$, $R_{2,2}$, $R_{4,4}$ à celles qui suivent

$$R_{1,1}=2(\rho^2+\rho^3)-(\rho^6+4\rho), \qquad R_{2,2}=2(\rho^4+\rho^6)-(\rho^5+4\rho^2),$$
$$R_{4,4}=2(\rho+\rho^5)-(\rho^3+4\rho^4);$$

et l'on aura par suite

$$R_{1,1}R_2R_{4,4}=-25+62(\rho+\rho^2+\rho^4)-54(\rho^3+\rho^5+\rho^6)=-29+58\Delta=29R_{1,2}.$$

NOTE VI.

SUR LA SOMME DES RACINES PRIMITIVES D'UNE ÉQUATION BINOME, ET SUR LES FONCTIONS SYMÉTRIQUES DE CES RACINES.

m et n désignant deux quantités entières, et ω leur plus grand commun diviseur numérique, on peut toujours, comme l'on sait, trouver deux autres quantités entières u, v, propres à vérifier la formule

$$mu - nv = \omega.$$

Donc toute racine commune des deux équations binomes

$$x^m = 1, \qquad x^n = 1,$$

et par conséquent des suivantes .

$$x^{mu} = 1, \qquad x^{nv} = 1,$$

vérifiera encore l'équation binome

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

puisqu'en supposant

$$mu - nv = \omega,$$

on en conclura

$$\frac{x^{mu}}{x^{nv}} = x^{mu-nv} = x^{\omega}.$$

Si d'ailleurs, n étant positif, on a pris pour x une racine primitive de l'équation

$$x^n = 1,$$

ou, en d'autres termes, si x^n est la plus petite puissance positive de x qui se réduise à l'unité, ω ne pourra différer de n; et par conséquent m sera divisible par n, en sorte qu'on aura

$$m \equiv 0 \pmod{n}.$$

Cela posé, n étant un nombre entier quelconque, nommons ρ une

racine primitive de l'équation binome

$$x^n = 1, \tag{1}$$

et

$$h, \quad k, \quad l, \quad \ldots$$

les entiers inférieurs à n, mais premiers à n. D'après ce qu'on vient de dire, ρ ne pourra représenter une valeur de x, propre à vérifier une équation de la forme

$$x^{mh} = 1,$$

que dans le cas où mh, et par conséquent m, sera divisible par n. Or, la plus petite valeur positive de m qui remplisse cette condition est $m = n$. Donc

$$\rho^{nh}$$

sera la plus petite puissance de ρ^h qui se réduise à l'unité. Donc

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots$$

seront autant de racines primitives de l'équation (1). Ces racines seront d'ailleurs distinctes les unes des autres. Car si l'on avait

$$\rho^h = \rho^k,$$

on en conclurait

$$\rho^{k-h} = 1, \qquad \text{et} \qquad k - h \equiv 0 \pmod{n},$$

ou, ce qui revient au même,

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

et par conséquent

$$k = h,$$

h, k devant être tous deux positifs et inférieurs à n. Ajoutons que les seules racines primitives de l'équation (1) seront les puissances entières de ρ, dont les exposants, premiers à n, pourront être réduits, par l'addition ou la soustraction de n ou d'un multiple de n, à l'un des nombres

$$h, \quad k, \quad l, \quad \ldots.$$

En effet, si m représente, au signe près, un entier qui ne soit pas premier à n, alors, ω étant le plus commun diviseur de m et de n, le produit

$$\frac{mn}{\omega}$$

sera le plus petit multiple de m, qui devienne divisible par n; et, par suite,

$$\rho^{\frac{mn}{\omega}}$$

sera la plus petite puissance positive de ρ^m qui se réduise à l'unité.

Donc, alors ρ^m représentera une racine primitive, non plus de l'équation (1), mais de la suivante :

$$x^{\frac{n}{\omega}} = 1. \tag{2}$$

Si m devient premier à n, on pourra en dire autant des produits

$$mh, \quad mk, \quad ml, \quad \ldots.$$

Donc alors

$$\rho^{mh}, \quad \rho^{mk}, \quad \rho^{ml}, \quad \ldots$$

seront encore des racines primitives de l'équation (1). D'ailleurs ces racines seront encore distinctes les unes des autres. Car on ne pourrait supposer

$$\rho^{mh} = \rho^{mk},$$

sans en conclure

$$\rho^{m(k-h)} = 1, \qquad m(k-h) \equiv 0 \pmod{n},$$

par conséquent

$$k - h \equiv 0, \qquad k \equiv h \pmod{n}$$

et

$$k = h,$$

h et k devant être tous deux inférieurs à n. Donc, si m devient premier à n, les diverses racines primitives de l'équation (1) pourront être représentées, soit par les termes de la suite

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots,$$

soit par les termes de la suite

$$\rho^{mh}, \quad \rho^{mk}, \quad \rho^{ml}, \quad \ldots,$$

qui coïncideront avec les termes de la première, rangés dans un ordre différent.

Si, au contraire, m et n n'étant pas premiers entre eux, ω désigne leur plus grand commun diviseur, alors ceux des termes de la suite

$$\rho^{mh}, \quad \rho^{mk}, \quad \rho^{ml}, \quad \ldots,$$

qui resteront distincts les uns des autres, représenteront les diverses racines primitives de l'équation (2).

Supposons à présent que le nombre n soit décomposé en deux facteurs

$$\varphi, \quad \chi,$$

premiers entre eux, et nommons

$$\xi, \quad \eta$$

des racines primitives des deux équations

$$x^{\varphi} = 1, \tag{3}$$

$$x^{\chi} = 1. \tag{4}$$

Les puissances

$$\xi^m, \quad \eta^m,$$

et, par suite, leur produit

$$\xi^m \eta^m = (\xi\eta)^m,$$

se réduiront évidemment à l'unité, si m est divisible simultanément par φ et par χ, ou, ce qui revient au même, par le produit

$$\varphi\chi = n.$$

Donc on vérifiera l'équation (1) en posant

$$x = \xi\eta.$$

Il y a plus : si m est choisi de manière à vérifier la condition

$$(\xi\eta)^m = 1,$$

on en conclura

$$(\xi\eta)^{m\varphi} = 1, \qquad \eta^{m\varphi} = 1,$$

par conséquent

$$m\varphi \equiv 0 \pmod{\chi}, \qquad m \equiv 0 \pmod{\chi},$$

et

$$(\xi\eta)^{m\chi} = 1, \qquad \xi^{m\chi} = 1,$$

par conséquent

$$m\chi \equiv 0 \pmod{\varphi}, \qquad m \equiv 0 \pmod{\varphi}.$$

Donc, pour que la puissance m^e du produit $\xi\eta$ se réduise à l'unité, il sera nécessaire que m soit divisible à la fois par χ et par φ, ou, en d'autres termes, que m soit un multiple de n; et, comme $m = n$ sera la plus petite valeur positive de m pour laquelle cette condition soit remplie, nous devons conclure que le produit $\xi\eta$ de deux racines primitives, propres à vérifier les équations (3) et (4), sera une racine primitive de l'équation (1).

Enfin, chaque racine primitive ρ de l'équation (1) ne pourra être formée que d'une seule manière par la multiplication de deux racines primitives propres à vérifier les équations (3) et (4). En effet, concevons que

$$\xi_i, \quad \eta_i$$

désignent encore deux racines primitives de ces équations. Si l'on a

$$\xi\eta = \xi_i\eta_i,$$

on en conclura

$$(\xi\eta)^\varphi = (\xi_i\eta_i)^\varphi, \qquad \eta^\varphi = \eta_i^\varphi,$$

par conséquent

$$\left(\frac{\eta_i}{\eta}\right)^\varphi = 1;$$

et, comme on aura d'autre part

$$\eta^\chi = \eta_i^\chi = 1,$$

par conséquent

$$\left(\frac{\eta_i}{\eta}\right)^\chi = 1,$$

il est clair que le rapport $\frac{\eta_i}{\eta}$ devra être une racine commune des équations (2) et (3). Or, φ, χ étant par hypothèse premiers entre eux, leur plus grand commun diviseur ω sera l'unité. Donc la racine commune dont il s'agit sera la racine unique de l'équation

$$x = 1,$$

et l'on aura

$$\frac{\eta_i}{\eta} = 1, \qquad \eta_i = \eta.$$

On trouvera de même $\xi_i = \xi$. Donc les produits

$$\xi\eta, \quad \xi_i\eta_i$$

ne pourront être égaux entre eux que dans le cas où l'on aura

$$\xi_i = \xi, \qquad \eta_i = \eta.$$

En conséquence, on peut énoncer la proposition suivante.

THÉORÈME I. — *Si le nombre entier n est le produit de deux facteurs φ, χ premiers entre eux, on obtiendra les diverses racines primitives de l'équation*

$$x^n = 1,$$

et on les obtiendra chacune d'une seule manière, en multipliant successivement les diverses racines primitives de l'équation

$$x^\varphi = 1$$

par chacune des racines primitives de l'équation

$$x^\chi = 1.$$

Le théorème que nous venons d'énoncer entraîne évidemment ceux qui suivent.

THÉORÈME II. — *Le nombre entier n étant le produit de deux facteurs φ, χ, premiers entre eux, désignons par*

$$\rho, \quad \rho_1, \quad \rho_2, \quad \dots$$

les diverses racines primitives de l'équation

$$x^n = 1;$$

puis nommons

$$\xi,\ \xi_1,\ \xi_2,\ \ldots \quad \text{et} \quad \eta,\ \eta_1,\ \eta_2,\ \ldots\ ,$$

les diverses racines primitives des équations

$$x^\varphi = 1 \quad \text{et} \quad x^\chi = 1;$$

on aura

$$(5) \qquad (\rho + \rho_1 + \rho_2 + \ldots) = (\xi + \xi_1 + \xi_2 + \ldots)(\eta + \eta_1 + \eta_2 + \ldots).$$

THÉORÈME III. — *Le nombre entier n étant le produit de deux facteurs* φ, χ *premiers entre eux, si l'on désigne par*

$$\mathrm{N},\ \Phi,\ \mathrm{X}$$

le nombre des racines primitives successivement calculé par chacune des trois équations

$$x^n = 1, \qquad x^\varphi = 1, \qquad x^\chi = 1,$$

on aura

$$(6) \qquad \mathrm{N} = \Phi \mathrm{X}.$$

Comme ces trois théorèmes sont évidemment applicables non seulement au nombre n, mais encore aux nombres φ, χ, facteurs de n, ou même aux facteurs de φ, lorsqu'il en existe, etc., et ainsi de suite, il est clair qu'on pourra énoncer encore les théorèmes suivants :

THÉORÈME IV. — *Si le nombre entier n est le produit de plusieurs facteurs*

$$\varphi,\ \chi,\ \psi,\ \ldots$$

premiers entre eux, on obtiendra les diverses racines primitives de l'équation

$$(1) \qquad x^n = 1,$$

et on les obtiendra chacune d'une seule manière, en cherchant d'abord

les diverses racines primitives des équations auxiliaires

$$(7) \qquad x^\varphi = 1, \qquad x^\chi = 1, \qquad x^\psi = 1, \qquad \ldots,$$

et formant tous les produits, qui ont chacun pour facteurs : 1° l'une des racines primitives de l'équation $x^\varphi = 1$; *2° l'une des racines primitives de l'équation* $x^\chi = 1$; *3° l'une des racines primitives de l'équation* $x^\psi = 1$, *etc.*

THÉORÈME V. — *Le nombre entier n étant le produit de plusieurs facteurs*

$$\varphi,\ \chi,\ \psi,\ \ldots$$

premiers entre eux, désignons par

$$\rho,\ \rho_1,\ \rho_2,\ \ldots$$

les diverses racines primitives de l'équation binome

$$x^n = 1,$$

et soient respectivement

$$\xi,\ \xi_1,\ \xi_2,\ \ldots;\quad \eta,\ \eta_1,\ \eta_2,\ \ldots;\quad \zeta,\ \zeta_1,\ \zeta_2,\ \ldots$$

les diverses racines primitives des équations binomes

$$x^\varphi = 1, \qquad x^\chi = 1, \qquad x^\psi = 1, \qquad \ldots,$$

la somme des racines primitives de la première équation sera le produit des sommes séparément formées avec les racines primitives de chacune des autres; en sorte qu'on aura

$$(8) \qquad \rho + \rho_1 + \rho_2 + \ldots = (\xi + \xi_1 + \xi_2 + \ldots)(\eta + \eta_1 + \eta_2 + \ldots)(\zeta + \zeta_1 + \zeta_2 + \ldots)\ldots,$$

et, par suite, si l'on nomme s *la somme des racines primitives de l'équation* (1), *l'on aura*

$$(9) \qquad s = (\xi + \xi_1 + \xi_2 + \ldots)(\eta + \eta_1 + \eta_2 + \ldots)(\zeta + \zeta_1 + \zeta_2 + \ldots)\ldots.$$

THÉORÈME VI. — *Le nombre entier n étant le produit de plusieurs facteurs*

$$\varphi,\ \chi,\ \psi,\ \ldots$$

premiers entre eux, désignons par

$$\mathrm{N},\quad \Phi,\quad \mathrm{X},\quad \Psi,\quad \ldots$$

le nombre des racines primitives successivement calculé pour chacune des équations

$$x^n=1,\qquad x^\varphi=1,\qquad x^\chi=1,\qquad x^\psi=1\qquad \ldots,$$

on aura

$$\mathrm{N}=\Phi\mathrm{X}\Psi\ldots. \tag{10}$$

Soient maintenant

$$\nu,\quad \nu',\quad \nu'',\quad \ldots$$

les facteurs premiers de n, dont l'un pourra se réduire à 2. Le nombre n sera de la forme

$$n=\nu^a\nu'^b\nu''^c\ldots, \tag{11}$$

a, b, c, ... désignant des exposants entiers, et, si l'on veut décomposer n en facteurs premiers entre eux, on pourra prendre pour ces facteurs les quantités

$$\nu^a,\quad \nu'^b,\quad \nu''^c,\quad \ldots,$$

dont chacune est une puissance entière d'un nombre premier.

Cela posé, les théorèmes que nous venons d'établir fourniront le moyen d'obtenir facilement, dans tous les cas, la somme

$$s$$

des racines primitives de l'équation (1) et le nombre

$$\mathrm{N}$$

de ces racines primitives. C'est ce que nous allons faire voir.

Si d'abord on suppose le nombre n égal à 2, l'équation (1), réduite à la forme

$$x^2=1,$$

offrira une seule racine primitive

$$\rho=-1;$$

et par suite on aura

$$s=-1,\qquad \mathrm{N}=1.$$

Si n est un nombre premier impair, les racines primitives de l'équation

$$x^n=1$$

seront les puissances entières de ρ correspondant à des exposants positifs, mais inférieurs à n, savoir

$$\rho,\quad \rho^2,\quad \rho^3,\quad \ldots,\quad \rho^{n-1}.$$

On aura donc

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

ou, ce qui revient au même,

$$s=-1,$$

et de plus

$$\mathrm{N}=n-1.$$

Si n est une puissance de 2, les racines primitives de l'équation

$$x^n=1$$

seront les puissances entières de ρ correspondant à des exposants impairs et inférieurs à n, savoir

$$\rho,\quad \rho^3,\quad \rho^5,\quad \ldots,\quad \rho^{n-1}.$$

On aura donc

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

ou, ce qui revient au même,

$$s=0,$$

et de plus

$$\mathrm{N}=\frac{n}{2}.$$

On peut encore observer que dans ce cas on a

$$\rho^{\frac{n}{2}}=-1,\qquad \rho^{\frac{n}{2}+k}=-\rho^k;$$

d'où il résulte que les diverses racines primitives seront, deux à deux, égales au signe près, mais affectées de signes contraires. Leur somme sera donc nulle, comme on l'a trouvé.

Supposons à présent que n soit une puissance d'un nombre premier impair ν; en sorte qu'on ait

$$n = \nu^a.$$

Alors, pour obtenir les racines primitives de l'équation

$$x^n = 1,$$

il faudra, entre toutes les racines représentées par les termes de la suite

$$1, \quad \rho, \quad \rho^2, \quad \ldots, \quad \rho^{n-1},$$

choisir celles dans lesquelles l'exposant de ρ est premier à n, et non divisible par ν, en laissant de côté celles où l'exposant est multiple de ν, savoir

$$\rho^0, \quad \rho^\nu, \quad \rho^{2\nu}, \quad \ldots, \quad \rho^{n-\nu},$$

ou, ce qui revient au même, en laissant de côté les racines non primitives

$$1, \quad \rho^\nu, \quad \rho^{2\nu}, \quad \ldots, \quad \rho^{\left(\frac{n}{\nu}-1\right)\nu}.$$

Or, ces dernières, dont le nombre est $\frac{n}{\nu}$, n'étant autre chose que les diverses racines de l'équation

$$x^{\frac{n}{\nu}} = 1,$$

leur somme totale sera nulle, aussi bien que la somme des racines de l'équation (1). Donc la différence de ces deux sommes, ou la somme s des racines primitives, s'évanouira elle-même; et l'on aura d'une part

$$s = 0,$$

d'autre part

$$N = n - \frac{n}{\nu},$$

ou, ce qui revient au même,

$$N = n\left(1 - \frac{1}{\nu}\right) = \nu^{a-1}\left(1 - \frac{1}{\nu}\right).$$

En résumé, si n est, ou un nombre premier ν, pair ou impair, ou une puissance ν^a d'un tel nombre, on trouvera toujours

$$N = n\left(1 - \frac{1}{\nu}\right), \tag{12}$$

et l'on aura de plus

$$s = -1, \tag{13}$$

ou

$$s = 0, \tag{14}$$

suivant qu'il s'agira de la première puissance ou d'une puissance supérieure à la première; ce que l'on pourra démontrer dans tous les cas à l'aide des raisonnements dont nous avons fait usage, lorsque n était une puissance d'un nombre premier impair.

Passons maintenant au cas où, n étant un nombre quelconque, sa valeur est donnée par la formule (11). Alors le nombre N des racines primitives de l'équation (1) et la somme s de ces racines se déduiront immédiatement des formules (10) et (12), ou des formules (9), (13) et (14). En effet, pour décomposer n, dans ce cas, en facteurs

$$\varphi, \quad \chi, \quad \psi, \quad \ldots$$

premiers entre eux, il suffira de prendre

$$\varphi = \nu^a, \qquad \chi = \nu'^b, \qquad \psi = \nu''^c, \qquad \ldots.$$

Cela posé, on aura, dans la formule (10),

$$\Phi = \nu^a\left(1 - \frac{1}{\nu}\right), \qquad X = \nu'^b\left(1 - \frac{1}{\nu'}\right), \qquad \Psi = \nu''^c\left(1 - \frac{1}{\nu''}\right), \qquad \ldots$$

et par suite cette formule donnera

$$(15)\qquad \begin{cases} N = \nu^a \nu'^b \nu''^c \ldots \left(1-\frac{1}{\nu}\right)\left(1-\frac{1}{\nu'}\right)\left(1-\frac{1}{\nu''}\right)\cdots \\ \quad = \nu^{a-1}\nu'^{b-1}\nu''^{c-1}\ldots(\nu-1)(\nu'-1)(\nu''-1)\ldots, \end{cases}$$

ou, ce qui revient au même,

$$(16)\qquad N = n\left(1-\frac{1}{\nu}\right)\left(1-\frac{1}{\nu'}\right)\left(1-\frac{1}{\nu''}\right)\cdots.$$

De plus, en vertu de la formule (9), la valeur de s, correspondant à l'équation (1), sera le produit des valeurs de s, correspondant aux équations

$$x^{\nu^a} = 1, \quad x^{\nu'^b} = 1, \quad x^{\nu''^c} = 1, \quad \ldots,$$

et dont chacune se réduira simplement à -1 ou à 0, suivant que le nombre a ou b ou c, ... sera égal ou supérieur à l'unité. Par suite, si n est un nombre composé, pair ou impair, qui renferme deux ou plusieurs facteurs égaux entre eux, on aura toujours

$$(17)\qquad s = 0.$$

Mais, si n est un nombre premier, ou un nombre composé dont les facteurs premiers ν, ν', ν'', ... soient inégaux, en sorte qu'on ait

$$(18)\qquad n = \nu\nu'\nu''\ldots,$$

alors on trouvera

$$(19)\qquad s = \pm 1,$$

savoir

$$(20)\qquad s = -1,$$

quand les facteurs premiers ν, ν', ν'', ... seront en nombre impair, et

$$(21)\qquad s = 1,$$

quand ces facteurs premiers seront en nombre pair.

Ainsi, en particulier, la somme des racines primitives sera -1

pour chacune des équations

$$x^3 = 1, \quad x^5 = 1, \quad x^7 = 1, \quad x^{11} = 1, \quad x^{13} = 1, \quad \ldots,$$

zéro pour chacune des équations

$$x^2 = 1, \quad x^4 = 1, \quad x^8 = 1, \quad x^{12} = 1, \quad x^{14} = 1, \quad x^{16} = 1, \quad \ldots,$$

et $+1$ pour chacune des équations

$$x^6 = 1, \quad x^{10} = 1, \quad x^{14} = 1, \quad x^{18} = 1, \quad x^{21} = 1, \quad x^{22} = 1, \quad \ldots.$$

Soit maintenant

$$f(\rho)$$

une fonction entière d'une racine primitive ρ de l'équation (1). On pourra toujours, dans cette fonction, réduire l'exposant de chaque puissance de ρ, à un nombre entier plus petit que n, et poser en conséquence

$$(22)\qquad f(\rho) = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1},$$

a_0, a_1, a_2, ..., a_{n-1} désignant des coefficients indépendants de ρ. Supposons d'ailleurs que, dans la fonction $f(\rho)$, les différents termes se transforment les uns dans les autres, quand on y remplace la racine primitive ρ par une autre racine primitive ρ^m. Alors $f(\rho)$ sera ce qu'on peut nommer une *fonction symétrique* des racines primitives de l'équation (1), ou, ce qui revient au même, une fonction symétrique des puissances

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots,$$

$h, k, l, \ldots$ étant les entiers inférieurs à n et premiers à n. Or, en écrivant successivement à la place de ρ chacune des racines primitives

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots,$$

on reconnaîtra que, dans $f(\rho)$, ceux des termes de chacune des suites

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots,$$
$$\rho^{2h}, \quad \rho^{2k}, \quad \rho^{2l}, \quad \ldots,$$
$$\rho^{3h}, \quad \rho^{3k}, \quad \rho^{3l}, \quad \ldots$$

qui sont distincts les uns des autres, doivent avoir les mêmes coefficients. Mais ces mêmes termes se réduisent toujours, ou aux diverses racines primitives de l'équation (1), ou du moins aux diverses racines primitives d'une équation de la forme

$$x^{\omega}=1, \tag{23}$$

ω étant un diviseur du nombre n, qui peut devenir égal à ce même nombre. Par conséquent, *dans une fonction symétrique des racines primitives de l'équation* (1), *les racines primitives de l'équation* (28) *devront toujours offrir les mêmes coefficients;* et une telle fonction se réduira toujours à une fonction linéaire des diverses valeurs que peut acquérir la somme des racines primitives de l'équation (23), quand on prend successivement pour ω chacun des diviseurs du nombre n, y compris ce nombre lui-même. Si, par exemple, n est un nombre premier, alors, les entiers

$$h,\ k,\ l,\ \ldots,$$

inférieurs à n, et premiers à n, se réduisant aux divers termes de la progression arithmétique

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

et les racines primitives

$$\rho^h,\ \rho^k,\ \rho^l,\ \ldots$$

de l'équation (1) aux divers termes de la progression géométrique

$$\rho,\ \rho^2,\ \rho^3,\ \ldots,\ \rho^{n-1},$$

on aura

$$a_1=a_2=\ldots=a_{n-1}$$

et

$$f(\rho)=a_0+a_1(\rho+\rho^2+\ldots+\rho^{n-1}). \tag{24}$$

Donc alors *une fonction symétrique des racines primitives de l'équation* (1) *sera en même temps une fonction linéaire de la somme de ces racines.*

Comme nous l'avons déjà remarqué, si l'on désigne par ρ une racine primitive de l'équation (1), et par

$$h,\ k,\ l,\ \ldots$$

les entiers inférieurs à n, mais premiers à n, les diverses racines primitives de la même équation pourront être représentées, non seulement par les termes de la suite

$$\rho^h,\ \rho^k,\ \rho^l,\ \ldots,$$

mais encore par les termes de la suite

$$\rho^{mh},\ \rho^{mk},\ \rho^{ml},\ \ldots,$$

pourvu que m soit lui-même premier à n. Il est essentiel d'observer que, pour passer de la première suite à la seconde, il suffit de multiplier par m les divers exposants

$$h,\ k,\ l,\ \ldots,$$

qui se transforment alors en ceux-ci

$$mh,\ mk,\ ml,\ \ldots.$$

Si l'on multiplie de nouveau ces derniers par m, une ou plusieurs fois, on obtiendra encore d'autres suites qui seront propres elles-mêmes à représenter les diverses racines primitives, savoir :

$$\begin{array}{llll} \rho^{m^2h}, & \rho^{m^2k}, & \rho^{m^2l}, & \ldots, \\ \rho^{m^3h}, & \rho^{m^3k}, & \rho^{m^3l}, & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots \end{array}$$

Concevons, maintenant, qu'avec les termes correspondants, par exemple, avec les premiers termes de ces différentes suites on forme une suite nouvelle

$$\rho^h,\ \rho^{mh},\ \rho^{m^2h},\ \rho^{m^3h},\ \ldots.$$

Cette nouvelle suite, dans laquelle les exposants de ρ forment une

progression géométrique

$$h, \quad mh, \quad m^2h, \quad m^3h, \quad \ldots,$$

offrira autant de racines primitives distinctes qu'il y aura d'unités dans l'exposant ι de la plus petite puissance de m propre à vérifier l'équivalence

$$m^\iota \equiv 1 \pmod{n}. \tag{25}$$

En effet, la valeur de ι étant choisie comme on vient de le dire, et la progression géométrique étant réduite aux seuls termes

$$h, \quad mh, \quad m^2h, \quad \ldots, \quad m^{\iota-1}h,$$

la différence entre deux termes de cette progression ne sera jamais divisible par n; et, en conséquence, les deux puissances de ρ, qui auront ces deux termes pour exposants, ne seront jamais égales entre elles. Donc, alors les divers termes de la suite

$$\rho^h, \quad \rho^{mh}, \quad \rho^{m^2h}, \quad \ldots, \quad \rho^{m^{\iota-1}h} \tag{26}$$

seront tous distincts les uns des autres.

Si n est un nombre premier impair ν, ou une puissance d'un tel nombre, tous les entiers premiers à n vérifieront l'équivalence

$$x^N = 1, \tag{27}$$

la valeur de N étant donnée par la formule (12), ou

$$N = n\left(1 - \frac{1}{\nu}\right).$$

Alors, si l'on prend pour m une racine primitive s de la formule (27), on trouvera

$$\iota = N,$$

et la suite (26) deviendra

$$\rho^h, \quad \rho^{sh}, \quad \rho^{s^2h}, \quad \rho^{s^{N-1}h}. \tag{28}$$

Cette suite se réduira même à

$$\rho, \quad \rho^s, \quad \rho^{s^2}, \quad \ldots, \quad \rho^{s^{N-1}}, \tag{29}$$

si l'on pose, comme on peut le faire, $h = 1$. D'ailleurs, N étant précisément le nombre des entiers

$$h, \quad k, \quad l, \quad \ldots,$$

inférieurs à n et premiers à n, il en résulte que chacune des suites (28), (29) comprendra toutes les racines primitives de l'équation (1).

Si n se réduit à un nombre premier, alors, la valeur de N étant

$$N = n - 1,$$

les suites (28), (29) deviendront

$$\rho^h, \quad \rho^{sh}, \quad \rho^{s^2h}, \quad \ldots, \quad \rho^{s^{n-2}h}, \tag{30}$$

$$\rho, \quad \rho^s, \quad \rho^{s^2}, \quad \ldots, \quad \rho^{s^{n-2}}, \tag{31}$$

et ces deux suites, dans lesquelles les exposants de ρ croissent en progression géométrique, offriront chacune, à l'ordre près, les mêmes termes que la suite

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

dans laquelle les exposants de ρ croissent en progression arithmétique.

NOTE VII.

SUR LES SOMMES ALTERNÉES DES RACINES PRIMITIVES DES ÉQUATIONS BINOMES, ET SUR LES FONCTIONS ALTERNÉES DE CES RACINES.

Soient toujours ρ une racine primitive de l'équation binome

$$x^n = 1, \tag{1}$$

et

$$h, \quad k, \quad l, \quad \ldots$$

les entiers inférieurs à n mais premiers à n, dont l'un se réduira sim-

plement à l'unité. Les diverses racines primitives de l'équation (1) pourront être représentées, soit par les termes de la suite

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots,$$

soit par les termes de la suite

$$\rho^{mh}, \quad \rho^{mk}, \quad \rho^{ml}, \quad \ldots,$$

m étant un nombre quelconque premier à n. Or, on pourra généralement, comme on le verra ci-après, partager les entiers

$$h, \quad k, \quad l, \quad \ldots$$

en deux groupes

$$h, \quad h', \quad h'', \quad \ldots \quad \text{et} \quad k, \quad k', \quad k'', \quad \ldots,$$

et par suite les racines primitives

$$\rho^h, \quad \rho^k, \quad \rho^l, \quad \ldots$$

en deux groupes correspondants

$$\rho^h, \quad \rho^{h'}, \quad \rho^{h''}, \quad \ldots \quad \text{et} \quad \rho^k, \quad \rho^{k'}, \quad \rho^{k''}, \quad \ldots,$$

de telle sorte qu'après la substitution de ρ^m à ρ, les deux derniers groupes se trouvent encore composés chacun des mêmes racines, ou transformés l'un dans l'autre. Ainsi, par exemple, si l'on suppose $n = 5$, les quatre racines primitives de l'équation (1), ou

$$x^5 = 1,$$

formeront les deux groupes

$$\rho, \quad \rho^4 \quad \text{et} \quad \rho^2, \quad \rho^3,$$

qui deviendront respectivement, après la substitution de ρ^2 à ρ,

$$\rho^2, \quad \rho^3 \quad \text{et} \quad \rho^4, \quad \rho$$

après la substitution de ρ^3 à ρ,

$$\rho^3, \quad \rho^2 \quad \text{et} \quad \rho, \quad \rho^4,$$

enfin, après la substitution de ρ^4 à ρ,

$$\rho^4, \quad \rho \quad \text{et} \quad \rho^2, \quad \rho^3.$$

Or, il est clair que, dans le premier et dans le dernier cas, les deux groupes resteront composés chacun des mêmes racines, tandis que dans les deux cas précédents les racines du premier groupe se transformeront en celles qui composaient le second, et réciproquement.

Les racines primitives de l'équation (1) étant partagées en deux groupes, comme on vient de le dire, de telle sorte, qu'après la substitution de ρ^m à ρ, les deux groupes restent, pour certaines valeurs de m, composés chacun des mêmes racines, et se trouvent, pour d'autres valeurs de m, échangés entre eux; il est clair que le nombre des racines

$$\rho^h, \quad \rho^{h'}, \quad \rho^{h''}, \quad \ldots$$

du premier groupe devra être égal au nombre des racines

$$\rho^k, \quad \rho^{k'}, \quad \rho^{k''}, \quad \ldots$$

du second groupe. Donc, si l'on représente par N, comme nous l'avons fait dans la note précédente, le nombre total des racines primitives ou des entiers

$$h, \quad k, \quad l, \quad \ldots$$

inférieurs à n, mais premiers à n, on verra le nombre des entiers

$$h, \quad h', \quad h'', \quad \ldots,$$

ou de racines comprises dans le premier groupe, et le nombre des entiers

$$k, \quad k', \quad k'', \quad \ldots,$$

ou des racines comprises dans le second groupe, se réduire séparément à $\frac{N}{2}$; ce qui suppose N pair.

Cela posé, concevons que l'on ajoute les unes aux autres les diverses racines primitives de l'équation (1), prises avec le signe + ou avec le signe −, suivant qu'elles font partie de l'un ou de l'autre groupe. On

obtiendra ainsi une somme algébrique dans laquelle on pourra faire succéder à chaque terme précédé du signe + un terme correspondant précédé du signe —. Cette somme algébrique pouvant être considérée en conséquence comme composée de termes alternativement positifs et négatifs, nous la désignerons sous le nom de *somme alternée*. Donc, si l'on pose

$$(2) \qquad \mathfrak{D} = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots,$$

$\mathfrak{D}$ sera une somme alternée des racines primitives de l'équation (1). Lorsque, dans une semblable somme, on remplacera la racine primitive ρ par une autre racine primitive ρ^m, les différents termes se transformeront, au signe près, les uns dans les autres, et deux termes, qui se déduiront ainsi l'un de l'autre, se trouveront toujours affectés du même signe pour certaines valeurs de m, mais affectés de signes contraires pour d'autres valeurs de m; par conséquent, la substitution de ρ^m à ρ laissera invariable la valeur de la somme, ou la fera seulement changer de signe. Supposons, pour fixer les idées, que des deux groupes

$$h, \quad h', \quad h'', \quad \ldots \qquad \text{et} \qquad k, \quad k', \quad k'', \quad \ldots,$$

le premier renferme l'exposant 1. Alors la substitution de ρ^m à ρ n'altèrera point la valeur de la somme alternée $\mathfrak{D}$, si l'on a pris pour m un des nombres

$$h, \quad h', \quad h'', \quad \ldots,$$

et la fera seulement changer de signe, si l'on a pris pour m un des nombres

$$k, \quad k', \quad k'', \quad \ldots.$$

Si, par exemple, on suppose $n = 5$, la somme alternée

$$\mathfrak{D} = \rho + \rho^2 - \rho^3 - \rho^4$$

changera de signe, quand on y remplacera ρ par ρ^2 ou par ρ^3, mais elle ne sera nullement altérée quand on y remplacera ρ par ρ^4.

Il est important d'observer que, dans le cas où la substitution de ρ^m

à ρ laisse invariable la somme alternée $\mathfrak{D}$, les termes

$$\rho^l \qquad \text{et} \qquad \rho^{ml},$$

par conséquent les termes

$$\rho^{ml} \qquad \text{et} \qquad \rho^{m^2 l}, \quad \ldots,$$

doivent se trouver affectés du même signe dans cette somme, l pouvant désigner ici l'un quelconque des nombres

$$h, \quad h', \quad h'', \quad \ldots, \quad k, \quad k', \quad k'', \quad \ldots,$$

c'est-à-dire l'un quelconque des nombres premiers à n. Donc, dans le cas dont il s'agit, le même signe doit affecter tous les termes de la suite

$$(3) \qquad \rho^l, \quad \rho^{ml}, \quad \rho^{m^2 l}, \quad \ldots, \quad \rho^{m^{\iota-1} l},$$

ι étant l'exposant de la plus petite puissance de m propre à vérifier l'équivalence

$$(4) \qquad m^\iota \equiv 1 \pmod{n}.$$

Mais, si la substitution de ρ^m à ρ fait varier le signe de la somme alternée $\mathfrak{D}$, alors les termes

$$\rho^l \quad \text{et} \quad \rho^{ml}$$

devront y être affectés de signes contraires, et l'on pourra en dire autant des termes

$$\rho^{ml} \qquad \text{et} \qquad \rho^{m^2 l},$$

ou

$$\rho^{m^2 l} \qquad \text{et} \qquad \rho^{m^3 l}, \quad \ldots.$$

Donc alors chacun des termes de la suite (3) sera, dans la somme alternée $\mathfrak{D}$, précédé du même signe que ρ^l ou d'un signe contraire, suivant que l'exposant de ρ contiendra comme facteur une puissance paire ou une puissance impaire de m. Dans tous les cas,

$$l \quad \text{et} \quad m$$

étant deux nombres premiers à n,

$$\rho^{m's'}$$

sera précédé du même signe que $\rho^{s'}$. Donc, si l'on a pris l'unité pour l'un des nombres

$$h,\quad h',\quad h'',\quad \ldots,$$

$\rho^{m's}$ sera précédé du signe $+$, ainsi que ρ; et, par conséquent, le groupe

$$h,\quad h',\quad h'',\quad \ldots$$

renfermera tous ceux des nombres

$$h,\quad k,\quad l,\quad \ldots$$

qui sont équivalents à des carrés

$$m^2,\quad m'^2,\quad \ldots,$$

suivant le module n, c'est-à-dire tous les résidus quadratiques relatifs à ce module.

Supposons maintenant que n soit un nombre premier impair, ou une puissance d'un tel nombre. Alors les entiers

$$h,\quad k,\quad l,\quad \ldots,$$

inférieurs à n et premiers à n, vérifieront l'équivalence

$$x^N \equiv 1 \pmod{n}, \tag{5}$$

les uns, dont le nombre sera $\frac{N}{2}$, étant résidus quadratiques suivant le module n, et racines de l'équivalence

$$x^{\frac{N}{2}} \equiv 1 \pmod{n}, \tag{6}$$

les autres, dont le nombre sera encore $\frac{N}{2}$, étant non-résidus quadratiques, et racines de l'équivalence

$$x^{\frac{N}{2}} \equiv -1 \pmod{n}. \tag{7}$$

D'ailleurs, si, dans la somme alternée ω, le terme ρ est précédé du signe $+$, on pourra en dire autant de toutes les puissances de ρ, qui offriront pour exposants des résidus quadratiques; et, comme le nombre de ces puissances sera précisément $\frac{N}{2}$, les autres puissances, qui auront pour exposants des non-résidus quadratiques, devront toutes être affectées du signe $-$. Donc alors

$$h,\quad h',\quad h'',\quad \ldots$$

devra représenter la suite des résidus quadratiques, et

$$k,\quad k',\quad k'',\quad \ldots,$$

la suite des non-résidus. D'ailleurs, si l'on prend pour m une racine primitive s de l'équivalence (5), les diverses racines primitives de l'équation (1) pourront être représentées par les divers termes de la suite

$$\rho,\quad \rho^s,\quad \rho^{s^2},\quad \rho^{s^{N-1}},$$

et, parmi les exposants de ρ dans cette suite, ceux qui représenteront des résidus quadratiques, relatifs au module n, seront les exposants carrés

$$1,\quad s^2,\quad s^4,\quad \ldots,\quad s^{N-2}.$$

Donc, si le terme ρ se trouve précédé du signe $+$ dans la somme alternée ω, la valeur de cette somme, dans l'hypothèse admise, ne pourra être que la suivante :

$$\omega = \rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{N-1}}. \tag{8}$$

Il est au reste facile de s'assurer que, dans le cas où n se réduit à un nombre premier impair ou à une puissance d'un tel nombre, le second membre de la formule (8) représente effectivement une somme alternée des racines primitives

$$\rho,\quad \rho^s,\quad \rho^{s^2},\quad \ldots,\quad \rho^{s^{N-1}}$$

de l'équation (1). Car, si, dans ce second membre, on remplace ρ

par ρ^s, chaque terme se trouvera remplacé par le suivant, pris en signe contraire, le dernier terme étant remplacé par $-\rho$. Or, de cette seule observation, il résulte que le second membre de l'équation (8) restera composé des mêmes termes, tous ces termes étant pris avec des signes contraires à ceux dont ils étaient d'abord affectés, ou tous étant pris avec ces mêmes signes, si l'on y remplace la racine primitive ρ par l'une des racines primitives

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

ce qui revient à remplacer une ou plusieurs fois de suite ρ par ρ^s.

Dans le cas particulier où n se réduit à un nombre premier, on a

$$N = n - 1,$$

et la formule (8) donne simplement

$$(9) \qquad \mathfrak{D} = \rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}},$$

s étant une racine primitive de l'équivalence

$$(10) \qquad x^{n-1} \equiv 1 \pmod{n}.$$

Alors, aussi, en vertu de la formule (14) de la Note I, on aura

$$(11) \qquad (\rho - \rho^s + \rho^{s^2} - \rho^{s^3} + \ldots - \rho^{s^{n-2}})^2 = (-1)^{\frac{n-1}{2}} n,$$

par conséquent

$$(12) \qquad \mathfrak{D}^2 = (-1)^{\frac{n-1}{2}} n.$$

Donc, n étant un nombre premier impair, on aura

$$(13) \qquad \mathfrak{D}^2 = n, \qquad \mathfrak{D} = \pm\sqrt{n},$$

si ce nombre premier n est de la forme $4x+1$, et l'on trouvera, au contraire,

$$(14) \qquad \mathfrak{D}^2 = -n, \qquad \mathfrak{D} = \pm n^{\frac{1}{2}}\sqrt{-1},$$

si n est de la forme $4x+3$.

Si l'on suppose, par exemple, $n = 3$, on trouvera

$$\mathfrak{D} = \rho - \rho^2,$$

ρ, ρ^2 représentant les deux racines primitives de l'équation

$$x^3 - 1 = 0,$$

ou, ce qui revient au même, les deux racines de l'équation

$$x^2 + x + 1 = 0.$$

Or, ces deux racines étant

$$-\frac{1}{2} + \frac{1}{2}3^{\frac{1}{2}}\sqrt{-1}, \quad -\frac{1}{2} - \frac{1}{2}3^{\frac{1}{2}}\sqrt{-1},$$

il est clair qu'en supposant $n = 3$, on trouvera

$$\mathfrak{D} = 3^{\frac{1}{2}}\sqrt{-1} \quad \text{ou} \quad \mathfrak{D} = -3^{\frac{1}{2}}\sqrt{-1},$$

suivant que l'on prendra pour ρ la première ou la seconde racine.

Lorsque, n étant une puissance entière d'un nombre premier impair ν, on aura

$$n = \nu^a,$$

et $a > 1$, alors, d'après ce qui a été dit ci-dessus, deux monomes de la forme

$$\rho^l, \quad \rho^{l'}$$

seront, dans la somme alternée $\mathfrak{D}$, affectés du même signe, si les nombres l, l', premiers à n, vérifient la condition

$$l' \equiv m^2 l \pmod{n},$$

m^2 étant un carré premier à n, ou, ce qui revient au même, si le rapport

$$\frac{l'}{l},$$

étant équivalent suivant le module n à un carré, vérifie par suite la

formule

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

Or, c'est évidemment ce qui arrivera, si l'on a

$$l' \equiv l \pmod \nu. \tag{15}$$

Car, en élevant plusieurs fois de suite à la puissance ν les deux membres de la formule (15), on en tirera successivement

$$\begin{aligned} l'^{\nu} &\equiv l^{\nu} \pmod{\nu^2},\\ l'^{\nu^2} &\equiv l^{\nu^2} \pmod{\nu^3},\\ &\dots\dots\dots\dots\dots,\\ l'^{\nu^{\alpha-1}} &\equiv l^{\nu^{\alpha-1}} \pmod{\nu^{\alpha}}, \end{aligned}$$

par conséquent,

$$\left(\frac{l'}{l}\right)^{\nu^{\alpha-1}} \equiv 1 \pmod \nu;$$

puis, en élevant les deux membres de cette dernière formule à la puissance entière $\frac{\nu-1}{2}$, et ayant égard aux équations

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

on trouvera définitivement

$$\left(\frac{l'}{l}\right)^{\frac{N}{2}} \equiv 1 \pmod n.$$

Donc, lorsque n représente le carré, le cube, ou une puissance plus élevée d'un nombre premier impair ν, le même signe doit affecter, dans la somme alternée $\mathfrak{D}$, toutes les puissances de ρ dont les exposants sont équivalents, suivant le module ν, à un même nombre l; par conséquent, le même signe doit affecter, dans la somme alternée $\mathfrak{D}$, tous les termes de la suite

$$\rho^{l}, \quad \rho^{l+\nu}, \quad \rho^{l+2\nu}, \quad \dots, \quad \rho^{l+n-\nu}.$$

Or, la somme de ces derniers termes, savoir,

$$\rho^{l} + \rho^{l+\nu} + \rho^{l+2\nu} + \dots + \rho^{l+n-\nu} = \rho^{l}\frac{1-\rho^{n}}{1-\rho^{\nu}},$$

étant nulle avec la différence $1-\rho^{n}$, il est clair que, dans le cas dont il s'agit, la somme alternée $\mathfrak{D}$ se composera de diverses parties séparément égales à zéro. Donc, la somme $\mathfrak{D}$ s'évanouira elle-même; et, lorsque n sera le carré, le cube ou une puissance plus élevée d'un nombre premier impair, on aura toujours

$$\mathfrak{D} = 0. \tag{16}$$

Si n se réduisait au nombre 2, l'équation binome

$$x^2 = 1$$

n'offrirait qu'une seule racine primitive

$$\rho = -1,$$

avec laquelle on ne pourrait composer une somme alternée. C'est au reste le seul cas où la formation d'une somme alternée des racines primitives devienne impossible, et où le nombre N cesse d'être pair, en se réduisant à l'unité.

Il n'en sera plus de même si l'on prend pour n une puissance de 2. Concevons qu'alors on réduise toujours l'un des nombres

$$h, \quad h', \quad h'', \quad \dots$$

à l'unité. Si, pour fixer les idées, on suppose $n = 4$, on trouvera

$$h = 1, \qquad k = 3,$$

et

$$\mathfrak{D} = \rho - \rho^{3} \tag{17}$$

sera une somme alternée des racines primitives de l'équation

$$x = 1.$$

Cette même somme, égale à

$$2\rho = \pm 2\sqrt{-1},$$

vérifiera d'ailleurs la formule

$$\mathfrak{D}^2 = -4. \tag{18}$$

Si l'on suppose $n = 8$, on pourra prendre

$$h = 1, \quad h' = 3, \quad k = 5, \quad k' = 7,$$

ou bien

$$h = 1, \quad h' = 5, \quad k = 3, \quad k' = 7,$$

ou bien

$$h = 1, \quad h' = 7, \quad k = 3, \quad k' = 5,$$

et obtenir ainsi trois sommes alternées des racines primitives de l'équation

$$x^8 = 1.$$

De ces trois sommes la première, savoir

$$(19) \qquad \mathfrak{S} = \rho + \rho^3 - \rho^5 - \rho^7$$

vérifiera la formule

$$(20) \qquad \mathfrak{S}^2 = -8;$$

la seconde, savoir

$$(21) \qquad \mathfrak{S} = \rho + \rho^5 - \rho^3 - \rho^7,$$

se réduira simplement à

$$(22) \qquad \mathfrak{S} = 0;$$

et la troisième, savoir

$$(23) \qquad \mathfrak{S} = \rho + \rho^7 - \rho^3 - \rho^5$$

vérifiera la formule

$$(24) \qquad \mathfrak{S}^2 = 8.$$

Enfin, si n est une puissance de 2, supérieure à la troisième, alors en posant

$$(25) \qquad l' = l + \frac{n}{2},$$

et choisissant le nombre entier d de manière à vérifier la formule

$$ld \equiv 1 \quad \text{ou} \quad \frac{1}{l} \equiv d \pmod{n},$$

on trouvera

$$\frac{l'}{l} = 1 + \frac{n}{2l} \equiv 1 + \frac{n}{2} d \pmod{n},$$

ou, ce qui revient au même,

$$\frac{l'}{l} \equiv \left(1 + \frac{n}{4} d\right)^2 \pmod{n},$$

attendu que, n étant divisible par 16,

$$\left(\frac{n}{4} d\right)^2 = \frac{n}{16} n d^2$$

sera divisible par n. Donc alors la valeur de l', déterminée par l'équation (25), sera équivalente, suivant le module n, à un produit de la forme

$$\left(1 + \frac{n}{4} d\right)^2 l \quad \text{ou} \quad m^2 l,$$

m étant premier à n, c'est-à-dire, impair; et les termes

$$\rho, \quad \rho^{l'} = \rho^{l + \frac{n}{2}}$$

seront généralement affectés de signes contraires dans une somme alternée $\mathfrak{S}$ des racines primitives de l'équation (1). D'autre part, puisque, pour des valeurs paires de n, l'équation (1) se décompose en deux autres, savoir

$$(26) \qquad x^{\frac{n}{2}} = 1,$$

$$(27) \qquad x^{\frac{n}{2}} = -1,$$

et qu'une racine primitive ρ de l'équation (1) ne peut vérifier l'équation (26), on aura nécessairement

$$\rho^{\frac{n}{2}} = -1 \quad \text{et} \quad \rho^{l'} = -\rho^l,$$

ou, ce qui revient au même,

$$\rho^l + \rho^{l'} = 0.$$

Donc, si n est une puissance de 2 supérieure à la troisième, une

somme alternée $\mathfrak{D}$ des racines primitives de l'équation (1) sera composée de telle manière, que les termes affectés du même signe se détruiront deux à deux, en fournissant des sommes partielles égales à zéro. Donc alors, la somme $\mathfrak{D}$ sera nulle elle-même, et l'on aura

$$\mathfrak{D} = 0.$$

En résumé, si n est un nombre premier ou une puissance d'un tel nombre, la somme alternée $\mathfrak{D}$ sera nulle, à moins que n ne se réduise à 4 ou à 8, ou à un nombre premier impair.

D'ailleurs, lorsque $\mathfrak{D}$ ne sera pas nul, on aura toujours

$$\mathfrak{D}^2 = \pm n,$$

savoir

$$\mathfrak{D}^2 = n, \tag{28}$$

si n est de la forme $4x+1$;

$$\mathfrak{D}^2 = -n, \tag{29}$$

si n est égal à 4, ou de la forme $4x+3$; enfin, si n est égal à 8,

$$\mathfrak{D}^2 = n \quad \text{ou} \quad \mathfrak{D}^2 = -n, \tag{30}$$

suivant qu'on placera dans le même groupe les deux nombres 1 et 3, ou 1 et 7.

Concevons maintenant que, n étant un nombre entier quelconque, on pose

$$n = \nu^{\alpha}\nu'^{\beta}\nu''^{\gamma}\ldots, \tag{31}$$

ν, ν', ν'', ... étant les facteurs premiers de n, dont l'un pourra se réduire à 2. Alors, comme on l'a vu dans la Note précédente, une racine primitive

$$\rho$$

de l'équation (1) sera le produit de racines primitives

$$\xi, \quad \eta, \quad \zeta, \quad \ldots,$$

propres à vérifier respectivement les diverses équations

$$x^{\nu^{\alpha}} = 1, \quad x^{\nu'^{\beta}} = 1, \quad x^{\nu''^{\gamma}} = 1, \quad \ldots. \tag{32}$$

Alors aussi on obtiendra les diverses valeurs de ρ et on les obtiendra chacune d'une seule manière, si dans le second membre de la formule

$$\rho = \xi\eta\zeta\ldots \tag{33}$$

on substitue successivement les divers systèmes de valeurs de

$$\xi, \quad \eta, \quad \zeta, \quad \ldots$$

combinées entre elles de toutes les manières possibles. D'ailleurs, ξ étant une des racines primitives de l'équation

$$x^{\nu^{\alpha}} = 1,$$

chacune des autres racines primitives de la même équation sera de la forme

$$\xi^{l},$$

l étant un nombre entier premier à ν. Pareillement, η étant une racine primitive de l'équation

$$x^{\nu'^{\beta}} = 1,$$

chacune des autres racines primitives de la même équation sera de la forme

$$\eta^{l'},$$

l' étant un nombre entier, premier à ν', etc. Donc, si l'on désigne, comme ci-dessus, par

$$\xi, \quad \eta, \quad \zeta, \quad \ldots$$

certaines racines primitives, propres à vérifier respectivement les équations

$$x^{\nu^{\alpha}} = 1, \quad x^{\nu'^{\beta}} = 1, \quad x^{\nu''^{\gamma}} = 1, \quad \ldots,$$

les diverses racines primitives de l'équation (1) se trouveront représentées par des produits de la forme

$$\xi^{l}\eta^{l'}\zeta^{l''}\ldots,$$

l étant premier à ν, l' à ν', l'' à ν'', ... Cela posé, considérons une somme alternée $\mathfrak{D}$ des racines primitives de l'équation (1). Comme les différents termes de la somme $\mathfrak{D}$ se réduiront à de semblables produits,

pris, les uns avec le signe +, les autres avec le signe —, cette somme sera évidemment une fonction entière de chacune des racines primitives

$$\xi,\ \eta,\ \zeta,\ \ldots.$$

On arriverait, au reste, à la même conclusion, en partant de la formule (33). En effet, la valeur de ρ, que détermine cette formule, étant une racine primitive de l'équation (1), la somme alternée $\mathfrak{S}$ sera nécessairement une fonction entière de ρ, et par suite une fonction entière de ξ, de η, de ζ, ... Or, concevons que, dans cette fonction, on écrive à la place de ξ, une autre racine primitive de la première des équations (32). La somme alternée $\mathfrak{S}$ devra rester composée des mêmes termes, tous étant pris avec les signes qui les affectaient d'abord, ou tous étant pris avec des signes contraires. Donc, chaque somme partielle de termes qui ne différeront les uns des autres que par la valeur de ξ, et par suite la somme $\mathfrak{S}$ elle-même, seront proportionnelles à la somme de toutes les valeurs de ξ, ou à une somme alternée de ces valeurs. On prouvera pareillement que $\mathfrak{S}$ est proportionnel à la somme des valeurs de η, ou à une somme alternée de ces valeurs, à la somme des valeurs de ξ, ou à une somme alternée de ces valeurs, etc. Donc la somme alternée $\mathfrak{S}$ renfermera, comme facteur, ou la somme ou une somme alternée des racines primitives de chacune des équations (32); et sera proportionnelle au produit de divers facteurs de cette nature, correspondant à ces diverses équations. D'ailleurs, si l'on développe le produit dont il est ici question, le développement offrira, au signe près, chacun des termes que renferme la somme alternée $\mathfrak{S}$, et deux termes devront encore être affectés du même signe ou de signes contraires dans le produit, suivant qu'ils seront affectés du même signe ou de signes contraires dans la somme $\mathfrak{S}$. Donc la somme alternée $\mathfrak{S}$ sera égale au produit obtenu, comme on vient de le dire, ou à ce produit pris en signe contraire.

Réciproquement, si l'on forme un produit dont les divers facteurs, correspondant aux diverses équations (32), représentent chacun la somme des racines primitives de l'une de ces équations, ou une somme

alternée de ces racines, il est clair que ce produit développé sera composé de termes égaux, au signe près, aux diverses racines primitives de l'équation (1), et pourra être considéré comme une fonction entière, non seulement d'une racine primitive ρ de l'équation (1), mais encore de certaines racines primitives

$$\xi,\ \eta,\ \zeta,\ \ldots,$$

propres à vérifier respectivement les équations (32). D'ailleurs, dans ce produit, on verra évidemment reparaître les mêmes termes, tous pris avec des signes contraires à ceux dont ils étaient d'abord affectés, ou tous pris avec les mêmes signes, quand on y remplacera la racine ξ par une autre racine primitive de l'équation

$$x^{\nu^\alpha} = 1,$$

ou la racine primitive η par une autre racine primitive de l'équation

$$x^{\nu^\beta} = 1, \quad \ldots,$$

par conséquent aussi quand on effectuera simultanément plusieurs remplacements de ce genre, ce qui revient à remplacer la racine primitive

$$\rho = \xi\eta\zeta\ldots$$

de l'équation (1) par une autre racine primitive de la même équation. Donc le produit, formé comme nous l'avons dit, ne pourra être qu'une fonction alternée des racines primitives de l'équation (1), dans le cas où il ne se réduirait pas à une fonction symétrique de ces racines.

Il est bon d'observer que la somme des racines primitives de l'équation

$$x^{\nu^\alpha} = 1,$$

étant égale à -1, a pour carré l'unité, et que la somme alternée de ces racines primitives, quand elle ne s'évanouit pas, offre pour carré $\pm\nu^\alpha$. Une pareille observation pouvant être appliquée à chacune des équations (32), le produit de plusieurs facteurs, dont chacun sera, ou la somme, ou une somme alternée des racines primitives de l'une de ces

équations, devra toujours, quand il ne s'évanouira pas, offrir un carré qui soit égal, abstraction faite du signe, au produit des nombres

$$\nu^a,\quad \nu^b,\quad \nu^c,\quad \ldots,$$

ou de plusieurs d'entre eux, par conséquent à n, ou à un diviseur de n. D'ailleurs, comme nous l'avons prouvé, le premier de ces deux produits peut représenter une somme alternée quelconque $\mathfrak{S}$ des racines primitives de l'équation (1). Donc, si une semblable somme ne s'évanouit pas, elle offrira pour carré $\pm n$, ou un diviseur de $\pm n$.

Observons encore qu'on aura toujours, ou

$$\mathfrak{S} = 0, \tag{34}$$

ou

$$\mathfrak{S}^2 = \pm n, \tag{35}$$

si chacun des facteurs du produit qui représente $\mathfrak{S}$ est une somme alternée. Au contraire, si l'un de ces facteurs est la somme des racines primitives de l'une des équations (32), $\mathfrak{S}^2$, en cessant d'être nul, sera généralement de la forme

$$\mathfrak{S}^2 = \pm\omega, \tag{36}$$

ω étant un diviseur de n. Alors aussi, $\mathfrak{S}$, considéré comme fonction des racines primitives des équations (32), sera, pour une ou pour plusieurs des équations dont il s'agit, fonction symétrique de ces racines.

Pour qu'on trouve en particulier

$$\mathfrak{S}^2 = \pm n,$$

il sera nécessaire que, dans le produit propre à représenter $\mathfrak{S}$, chaque facteur se réduise à une somme alternée différente de zéro. C'est ce qui arrivera lorsque, dans le nombre composé n, les facteurs premiers impairs seront inégaux, le facteur pair, s'il existe, étant précisément 4 ou 8.

Soit maintenant

$$f(\rho)$$

une fonction entière de la racine primitive ρ de l'équation (1). On pourra, dans cette fonction, réduire l'exposant de chaque puissance de ρ à un nombre entier plus petit que n, et poser en conséquence

$$f(\rho) = a_0 + a_1\rho + a_2\rho^2 + \ldots + a_{n-1}\rho^{n-1}, \tag{37}$$

$a_0, a_1, a_2, \ldots, a_{n-1}$ désignant des coefficients indépendants de ρ. Supposons d'ailleurs que, dans le cas où l'on remplace la racine primitive ρ de l'équation (1) par une autre racine primitive ρ^m de la même équation, les différents termes contenus dans $f(\rho)$ se transforment, au signe près, les uns dans les autres, et que deux termes, qui se déduisent ainsi l'un de l'autre, se trouvent toujours affectés du même signe pour certaines valeurs

$$h,\quad h',\quad h'',\quad \ldots$$

du nombre m, mais affectés de signes contraires pour d'autres valeurs

$$k,\quad k',\quad k'',\quad \ldots$$

du même nombre; en sorte que, sous ce point de vue, les entiers

$$h,\quad k,\quad l,\quad \ldots,$$

inférieurs à n et premiers à n, se partagent en deux groupes

$$h,\quad h',\quad h'',\quad \ldots \qquad \text{et} \qquad k,\quad k',\quad k'',\quad \ldots.$$

Alors, dans $f(\rho)$, les coefficients a_0 s'évanouiront nécessairement, et $f(\rho)$ sera une fonction linéaire de chacune des sommes algébriques

$$\begin{cases} \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots, \\ \rho^{2h} + \rho^{2h'} + \rho^{2h''} + \ldots - \rho^{2k} - \rho^{2k'} - \rho^{2k''} - \ldots, \\ \rho^{3h} + \rho^{3h'} + \rho^{3h''} + \ldots - \rho^{3k} - \rho^{3k'} - \rho^{3k''} - \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{cases} \tag{38}$$

chacune d'elles étant censée ne renfermer que des termes distincts les uns des autres. Sous cette condition, les sommes algébriques dont il s'agit se réduiront toujours, ou, comme la première, à une somme alternée des racines primitives de l'équation (1), ou du moins à des

sommes alternées des racines primitives d'équations de la forme

$$x^{\omega} = 1, \tag{39}$$

les exposants ou les valeurs de ω étant des diviseurs de n. Cela posé, dans la fonction $f(\rho)$, aussi bien que dans chaque somme alternée, les termes précédés du signe $+$ seront évidemment en même nombre que les termes précédés du signe $-$; et, si à un terme que précède le signe $+$ on fait succéder un terme correspondant que précède le signe $-$, on pourra obtenir, pour représenter la fonction, une suite de termes alternativement positifs et négatifs. Pour cette raison, nous désignerons sous le nom de *fonction alternée* la fonction $f(\rho)$, formée comme il a été dit ci-dessus. Il est clair qu'une semblable fonction pourra seulement acquérir deux formes distinctes, et deux valeurs égales au signe près, mais affectées de signes contraires, si l'on y remplace une racine primitive ρ de l'équation (1) par une autre racine primitive ρ^m de la même équation. Ajoutons qu'en vertu des relations établies par la formule (33) entre les racines primitives de l'équation (1) et celles des équations (32), toute fonction alternée des racines primitives de l'équation (1) sera en même temps, ou une fonction alternée, ou une fonction symétrique des racines primitives de chacune des équations (32). Il sera maintenant facile de trouver la forme la plus simple à laquelle se réduise, pour une valeur donnée de n, une fonction alternée $f(\rho)$ des racines primitives de l'équation (1); surtout lorsque n représentera un nombre premier ou une puissance d'un tel nombre. Entrons à ce sujet dans quelques détails.

Supposons d'abord que le nombre n se réduise à un nombre premier impair ν, ou à une puissance de ce nombre premier, en sorte qu'on ait

$$n = \nu^{a},$$

l'exposant a pouvant se réduire à l'unité. Les divers diviseurs du nombre n, y compris ce nombre lui-même, ou les diverses valeurs que pourra prendre l'exposant ω dans la formule (39), seront respectivement

$$\nu,\ \nu^2,\ \nu^3,\ \ldots,\ \nu^{a-1},\ \nu^{a};$$

et les sommes alternées des racines primitives de l'équation (38), qui correspondront à ces diverses valeurs de ω, seront toutes nulles, à l'exception d'une seule, que nous désignerons par Δ, et à laquelle la fonction $f(\rho)$ deviendra proportionnelle; en sorte qu'on aura

$$f(\rho) = a\Delta, \tag{40}$$

a étant indépendant de ρ. La somme Δ dont il s'agit sera d'ailleurs la somme alternée des racines primitives de l'équation

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

qu'on obtient en posant, dans l'équation (39), $\omega = \nu$.

Supposons en second lieu que le nombre n se réduise à une puissance

$$2^{a}$$

du nombre 2. Alors, pour qu'on puisse former avec les racines de l'équation (1) une fonction alternée, il sera nécessaire que cette équation offre plus d'une racine primitive et qu'on ait en conséquence

$$a > 1.$$

Cela posé, n pourra être l'un quelconque des termes de la progression géométrique

$$4,\ 8,\ 16,\ \ldots;$$

et, les valeurs de ω, dans l'équation (39), devant aussi se réduire à des termes de cette progression, la somme des racines primitives de l'équation (39) ne pourra cesser de s'évanouir que lorsqu'on prendra

$$\omega = 4 \quad \text{ou} \quad \omega = 8.$$

Donc alors une fonction alternée $f(\rho)$ des racines primitives de l'équation (1) renfermera tout au plus deux termes qui ne s'évanouiront pas, ces deux termes étant proportionnels, le premier à une fonction alternée des racines primitives de l'équation

$$x^4 = 1, \tag{41}$$

le second à une fonction alternée des racines primitives de l'équation

$$x^8 = 1. \tag{42}$$

Or, évidemment de ces deux termes le premier subsistera seul, si l'on a $n = 4$, et alors la fonction alternée $f(\rho)$ sera encore de la forme indiquée par l'équation (40), la valeur de Δ étant

$$\Delta = \rho - \rho^3 = \pm 2\sqrt{-1}.$$

Si n devient égal à 8, on aura trois cas à considérer, suivant que le second terme deviendra proportionnel à l'une ou à l'autre des trois sommes alternées

$$(43) \qquad 4\rho + \rho^3 - \rho^5 - \rho^7, \qquad \rho + \rho^3 - \rho^5 - \rho^7 = 0, \qquad \rho + \rho^7 - \rho^3 - \rho^5.$$

Or, quand on fait successivement coïncider avec chacune de ces trois sommes la première des expressions (38), savoir

$$\rho^h + \rho^{h'} + \ldots - \rho^k - \rho^{k'} - \ldots,$$

on trouve que les valeurs correspondantes de la seconde expression

$$\rho^{2h} + \ldots - \rho^{2k} - \ldots,$$

réduite à ne contenir que des puissances de ρ non équivalentes entre elles, deviennent respectivement

$$(44) \qquad 0, \qquad \rho^2 - \rho^6 = \pm 2\sqrt{-1}, \qquad 0.$$

Donc, n étant égal à 8, le second des termes dont nous avons parlé disparaît lorsque le premier subsiste, et réciproquement; en sorte que, dans ce cas encore, la fonction $f(\rho)$ est de la forme indiquée par l'équation (40), Δ désignant une somme alternée des racines primitives ou de l'équation (41) ou de l'équation (42).

Au reste, ces conclusions doivent être étendues au cas même où n, étant une puissance de 2, deviendrait supérieur à 8, puisqu'alors la fonction $f(\rho)$, dans laquelle tous les termes disparaîtraient, à l'exception des deux termes ci-dessus mentionnés, pourrait encore être considérée comme une fonction alternée des racines primitives de l'équation (42).

Revenons à des valeurs quelconques de n, et posons de nouveau

$$n = \nu^a \nu'^b \nu''^c \ldots,$$

$\nu, \nu', \nu'', \ldots$ désignant les facteurs premiers de n, dont l'un pourra se réduire à 2. Comme nous l'avons déjà dit, une fonction alternée $f(\rho)$ des racines primitives de l'équation (1) sera en même temps ou une fonction symétrique, ou une fonction alternée des racines primitives de chacune des équations (32). Occupons-nous d'ailleurs spécialement du cas où $f(\rho)$, considéré comme fonction des racines primitives de l'une quelconque des équations (32), est toujours une fonction alternée, jamais une fonction symétrique de ces racines; ce qui suppose n impair ou divisible plusieurs fois par le facteur 2. Dans ce cas spécial, d'après ce qu'on a vu tout à l'heure, ou la fonction $f(\rho)$ s'évanouira, ou elle deviendra simultanément proportionnelle à divers facteurs

$$\Delta, \quad \Delta', \quad \Delta'', \quad \ldots,$$

qui représenteront des sommes alternées, respectivement formées avec les racines primitives des équations

$$(45) \qquad x^\nu = 1, \qquad x^{\nu'} = 1, \qquad x^{\nu''} = 1, \qquad \ldots$$

si les facteurs premiers

$$\nu, \quad \nu', \quad \nu'', \quad \ldots$$

sont tous des nombres impairs. Donc alors $f(\rho)$ sera proportionnel au produit

$$\Delta \; \Delta' \; \Delta'' \; \ldots,$$

qui représentera une somme alternée des racines primitives de l'équation

$$(46) \qquad x^{\nu\nu'\nu''\ldots} = 1$$

ou

$$(47) \qquad x^\omega = 1,$$

la valeur de ω étant

$$(48) \qquad \omega = \nu\nu'\nu''\ldots,$$

et l'on aura en conséquence

$$(49) \qquad f(\rho) = a\Delta\Delta'\Delta''\ldots,$$

a désignant dans $f(\rho)$ le coefficient d'une racine primitive de l'équation (46). Si, parmi les facteurs

$$\nu,\quad \nu',\quad \nu'',\quad \ldots,$$

le premier ν se réduisait à 2, on devrait remplacer la première des équations (45) par l'équation (41) ou (42); et par suite on devrait, dans la formule (49), prendre pour Δ une somme alternée des racines primitives de l'une des équations

(50) $$x^4=1,\qquad x^8=1.$$

Alors le produit

$$\Delta\Delta'\Delta''\ldots$$

serait une somme alternée des racines primitives de l'équation (47), la valeur de ω étant donnée non plus par la formule (48), mais par l'une des deux suivantes :

(51) $$\omega=4\nu'\nu''\ldots,\qquad \omega=8\nu'\nu''\ldots.$$

D'ailleurs, en supposant n impair avec chacun des facteurs

$$\nu,\quad \nu',\quad \nu'',\quad \ldots,$$

on trouvera

(52) $$\Delta^2=(-1)^{\frac{\nu-1}{2}}\nu,\qquad \Delta'^2=(-1)^{\frac{\nu'-1}{2}}\nu',\qquad \Delta''^2=(-1)^{\frac{\nu''-1}{1}}\nu'',\qquad \ldots$$

et, par suite,

(53) $$\Delta^2\Delta'^2\Delta''^2\ldots=(-1)^{\frac{\nu-1}{2}+\frac{\nu'-1}{2}+\frac{\nu''-1}{2}+\ldots}\nu\nu'\nu''\ldots,$$

ou, ce qui revient au même,

(54) $$\Delta^2\Delta'^2\Delta''^2\ldots=(-1)^{\frac{\omega-1}{2}}\omega=\pm\omega,$$

la valeur de ω étant donnée par la formule (48). Si au contraire on suppose $\nu=2$, n étant divisible par 4 ou par 8, la première des formules (52) se trouvera remplacée par l'une des équations

(55) $$\Delta^2=-4,\qquad \Delta^2=\pm 8,$$

et la formule (53) par l'une des équations

(56) $$\Delta^2\Delta'^2\Delta''^2\ldots=\pm 4\nu'\nu''\ldots,\qquad \Delta^2\Delta'^2\Delta''^2\ldots=\pm 8\nu'\nu''\ldots;$$

par conséquent on aura encore

(57) $$\Delta^2\Delta'^2\Delta''^2\ldots=\pm\omega,$$

la valeur de ω étant donnée, non plus par la formule (48), mais par l'une des formules (51). Dans l'une et l'autre hypothèses, on tirera de la formule (49)

(58) $$[f(\rho)]^2=\pm\omega a^2.$$

L'équation (58) se réduira simplement à

(59) $$[f(\rho)]^2=\pm n a^2,$$

si l'on a

(60) $$\omega=n.$$

Or, pour que le nombre ω, déterminé par la formule (48), ou par l'une des formules (51), devienne précisément égal à n, il est nécessaire que les facteurs premiers et impairs de n soient inégaux, le facteur pair, s'il existe, étant 4 ou 8.

L'équation (59) se réduira en particulier à

(61) $$[f(\rho)]^2=n a^2,$$

si, les facteurs premiers et impairs du nombre n étant inégaux, ce nombre est de l'une des formes

$$4x+1,\quad 4(4x+3),$$

ou bien encore de l'une des formes

$$8(4x+1),\quad 8(4x+3),$$

pourvu toutefois que, dans ce dernier cas, on place dans le même groupe ceux des entiers

$$h,\quad k,\quad l,\quad \ldots$$

inférieurs à n, mais premiers à n, qui, divisés par 8, donnent pour restes 1 et 7, quand $\frac{n}{8}$ est de la forme $4x+1$, et ceux qui, divisés par 8, donnent pour restes 1 et 3, quand $\frac{n}{8}$ est de la forme $4x+3$.

Enfin l'équation (59) se trouvera réduite à

$$[f(\rho)]^2 = -na^2, \tag{62}$$

si, les facteurs premiers et impairs du nombre n étant inégaux, ce nombre est de l'une des formes

$$4x+3, \quad 4(4x+1),$$

ou bien encore de l'une des formes

$$8(4x+1), \quad 8(4x+3),$$

pourvu toutefois que, dans ce dernier cas, on place dans le même groupe ceux des entiers

$$h, \quad k, \quad l, \quad \ldots$$

inférieurs à n, mais premiers à n, qui, divisés par 8, donnent pour restes 1 et 3, quand $\frac{n}{8}$ est de la forme $4x+1$, et ceux qui donnent pour restes 1 et 7, quand $\frac{n}{8}$ est de la forme $4x+3$.

Nous observerons en finissant que, dans le cas où l'on a $n = \omega$, et où la formule (58) se réduit à la formule (59), le produit

$$\Delta\Delta'\Delta'' \ldots,$$

renfermé dans le second membre de la formule (49), se réduit à une somme alternée $\mathfrak{D}$ des racines primitives de l'équation (1). Donc alors la formule (49) pourra s'écrire comme il suit :

$$f(\rho) = a\mathfrak{D}. \tag{63}$$

Or, en élevant au carré chaque membre de cette dernière formule, et ayant égard à l'équation (35), on retrouvera, comme on devait s'y attendre, l'équation (59).

NOTE VIII.

PROPRIÉTÉS DES NOMBRES QUI, DANS UNE SOMME ALTERNÉE DES RACINES PRIMITIVES D'UNE ÉQUATION BINOME, SERVENT D'EXPOSANTS AUX DIVERSES PUISSANCES DE L'UNE DE CES RACINES.

Soient, comme dans la Note précédente :

n un nombre entier quelconque;
$h, k, l, \ldots$ les entiers inférieurs à n, et premiers à n;
N le nombre des entiers $h, k, l, \ldots$;
ρ une racine primitive de l'équation

$$x^n = 1, \tag{1}$$

et

$$\mathfrak{D} = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots \tag{2}$$

une somme alternée des racines primitives de cette équation, les entiers

$$h, \quad k, \quad l, \quad \ldots$$

étant partagés en deux groupes

$$h, \quad h', \quad h'', \quad \ldots \qquad \text{et} \qquad k, \quad k', \quad k'', \quad \ldots,$$

de telle manière qu'un changement opéré dans la valeur de la racine primitive ρ puisse produire un changement de signe dans la somme $\mathfrak{D}$, sans avoir jamais d'autre effet sur cette même somme. Enfin, supposons, pour plus de commodité, que le nombre 1 fasse partie du groupe

$$h, \quad h', \quad h'', \quad \ldots.$$

Si le nombre n est premier, il sera en même temps impair, et l'on aura

$$N = n - 1.$$

Alors aussi, d'après ce qui a été dit dans la Note précédente, les nombres

$$h, \quad h', \quad h'', \quad \ldots$$

seront résidus quadratiques suivant le module n, et racines de l'équation

$$x^{\frac{n-1}{2}} \equiv 1 \pmod{n}, \tag{3}$$

en sorte que chacun d'eux vérifiera la condition

$$\left[\frac{h}{n}\right] = 1. \tag{4}$$

Au contraire les nombres

$$k,\ k',\ k'',\ \ldots$$

seront non-résidus quadratiques suivant le module n, et racines de l'équivalence

$$x^{\frac{n-1}{2}} \equiv -1 \pmod{n}, \tag{5}$$

en sorte que chacun d'eux vérifiera la condition

$$\left[\frac{k}{n}\right] = -1. \tag{6}$$

D'ailleurs, pour chacune des équations

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

la somme des racines se réduira toujours à zéro, lorsque $\frac{n-1}{2}$ sera un nombre entier supérieur à l'unité; et, par conséquent, pour chacune des formules (3), (5), la somme des racines sera équivalente à zéro, suivant le module n, lorsqu'on aura

$$\frac{n-1}{2} > 1, \qquad n > 3.$$

Donc, n étant un nombre premier supérieur à 3, on aura toujours

$$h + h' + h'' + \ldots \equiv k + k' + k'' + \ldots \equiv 0. \tag{7}$$

La formule (7) comprend évidemment un théorème qu'on peut énoncer comme il suit :

THÉORÈME I. — *n étant un nombre premier supérieur à 3, si, parmi les*

entiers inférieurs à n, mais premiers à n, on distingue les résidus quadratiques

$$h,\ h',\ h'',\ \ldots$$

et les non-résidus quadratiques

$$k,\ k',\ k'',\ \ldots,$$

la somme $h + h' + h'' + \ldots$ des résidus et la somme $k + k' + k'' + \ldots$ des non-résidus seront l'une et l'autre divisibles par n.

Ainsi, en particulier, on trouvera, pour $n = 5$,

$$\begin{aligned} &h = 1, \quad h' = 4, \quad h + h' = 5 \equiv 0 \pmod{5}. \\ &k = 2, \quad k' = 3, \quad k + k' = 5 \equiv 0 \pmod{5}, \end{aligned}$$

pour $n = 7$,

$$\begin{aligned} &h = 3, \quad h' = 2, \quad h'' = 4, \quad h + h + h'' = 7 \equiv 0 \pmod{7}, \\ &k = 1, \quad k' = 5, \quad k'' = 6, \quad k + k + k'' = 14 \equiv 0 \pmod{7}, \end{aligned}$$

etc. Mais, si l'on prend

$$n = 3,$$

on aura

$$h = 1, \qquad k = 2,$$

et la condition (7), qui cessera d'être vérifiée, se trouvera remplacée par la suivante :

$$h \equiv -k \equiv 1 \pmod{3}.$$

On pourrait démontrer encore le premier théorème comme il suit.

n étant un nombre premier impair, nommons s une racine primitive de l'équivalence

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

Les entiers inférieurs à n, mais premiers à n, seront équivalents aux diverses puissances de s d'un degré plus petit que $n - 1$, savoir, les résidus quadratiques aux puissances paires

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

et les non-résidus aux puissances impaires

$$s,\ s^3,\ s^5,\ \ldots,\ s^{n-2}.$$

On trouvera, par suite,

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

$$k + k' + k'' + \ldots \equiv s + s^3 + s^5 + \ldots + s^{n-2} \equiv \frac{s^{n-1} - 1}{s^2 - 1} \equiv 0 \pmod{n},$$

excepté dans le cas où, n étant égal à 3, on aurait non seulement

$$s^{n-1} \equiv 1 \pmod{n},$$

mais encore $n - 1 = 2$, et par conséquent

$$s^2 \equiv 1 \pmod{n}.$$

Supposons maintenant que n devienne une puissance d'un nombre premier impair ν, en sorte qu'on ait

$$n = \nu^a.$$

Alors on trouvera

$$N = \nu^{a-1}(\nu - 1) = n\left(1 - \frac{1}{\nu}\right).$$

Alors aussi

$$h, \quad h', \quad h'', \quad \ldots$$

seront résidus quadratiques suivant le module n, et racines de l'équivalence

$$x^{\frac{N}{2}} \equiv 1 \pmod{n}, \tag{8}$$

tandis que

$$k, \quad k', \quad k'', \quad \ldots$$

seront non-résidus suivant le module n, et racines de l'équivalence

$$x^{\frac{N}{2}} \equiv -1 \pmod{n}. \tag{9}$$

Donc, si, en nommant l un nombre entier premier à n, on désigne par

$$\left[\frac{l}{n}\right]$$

le reste $+1$ ou -1, qu'on obtient en divisant par n la puissance

$$l^{\frac{N}{2}},$$

chacun des nombres $h, h', h'', \ldots$ vérifiera encore la condition (4), et chacun des nombres $k, k', k'', \ldots$ la condition (6). D'autre part, chacun des groupes

$$h, \quad h', \quad h'', \quad \ldots,$$
$$k, \quad k', \quad k'', \quad \ldots$$

pouvant être décomposé (p. 248-249) en plusieurs suites de termes de la forme

$$l, \quad l + \nu, \quad l + 2\nu, \quad \ldots, \quad l + n - \nu,$$

et la somme de ces derniers termes étant égale à

$$\frac{n}{\nu}\left(l + \frac{n - \nu}{2}\right),$$

par conséquent divisible par $\nu^{a-1} = \frac{n}{\nu}$, il est clair que, dans l'hypothèse admise, la formule (7) pourra être remplacée par la suivante :

$$h + h' + h'' + \ldots \equiv k + k' + k'' + \ldots \equiv 0 \quad \left(\text{mod. } \nu^{a-1} = \frac{n}{\nu}\right). \tag{10}$$

Ainsi, en particulier, on trouvera pour $n = 9 = 3^2$,

$$h = 1, \quad h' = 4, \quad h'' = 7, \quad h + h' + h'' = 12 \equiv 0 \pmod{3},$$
$$h = 2, \quad k' = 5, \quad k'' = 8, \quad k + k' + k'' = 15 \equiv 0 \pmod{3}.$$

La formule (11) renferme un théorème qu'on peut énoncer comme il suit :

THÉORÈME II. — *ν étant un nombre premier impair, et $n = \nu^a$ une puissance de ν dont le degré surpasse l'unité, si parmi les entiers inférieurs à n, mais premiers à n, on distingue les résidus quadratiques*

$$h, \quad h', \quad h'', \quad \ldots$$

et les non-résidus

$$k, \quad k', \quad k'', \quad \ldots,$$

la somme $h + h' + h'' + \ldots$ des résidus et la somme $k + k' + k'' + \ldots$ des non-résidus seront, l'une et l'autre, divisibles par ν^{a-1} ou, ce qui revient au même, par $\frac{n}{\nu}$.

Au reste, on pourrait encore établir le théorème II de la manière suivante :

Si, en supposant

$$n = \nu^a \qquad \text{et} \qquad N = \nu^{a-1}(\nu - 1),$$

on nomme s une racine primitive de l'équivalence

$$x^N \equiv 1 \pmod{n},$$

on trouvera, par des raisonnements semblables à ceux dont nous avons précédemment fait usage,

$$h + h' + h'' + \ldots \equiv 1 + s^2 + s^4 + \ldots + s^{N-2} \equiv \frac{s^N - 1}{s^2 - 1} \pmod{n},$$

$$k + k' + k'' + \ldots \equiv s + s^3 + s^5 + \ldots + s^{N-2} \equiv s\frac{s^N - 1}{s^2 - 1} \pmod{n},$$

et, par suite,

$$(s^2 - 1)(h + h' + h'' + \ldots) \equiv s^N - 1 \equiv 0 \pmod{n},$$
$$(s^2 - 1)(k + k' + k'' + \ldots) \equiv s(s^N - 1) \equiv 0 \pmod{n}.$$

Donc chacun des produits

$$(s^2 - 1)(h + h' + h'' + \ldots), \qquad (s^2 - 1)(k + k' + k'' + \ldots)$$

sera divisible par $n = \nu^a$; et, dans chacun d'eux, le second facteur

$$h + h' + h'' + \ldots \qquad \text{ou} \qquad k + k' + k'' + \ldots$$

sera nécessairement divisible par ν^{a-1}, si le premier facteur

$$s^2 - 1$$

ne peut être qu'une seule fois divisible par ν. Or, c'est précisément ce qui arrivera. Car, si le facteur $s^2 - 1$ était seulement divisible par ν^2, on en conclurait

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

et, par suite (*voir* la note placée au bas de la page 81),

$$\begin{aligned} s^{\nu(\nu-1)} &\equiv 1 \pmod{\nu^3}, \\ s^{\nu^2(\nu-1)} &\equiv 1 \pmod{\nu^4}, \\ \ldots\ldots\ldots\ldots &\quad \ldots\ldots\ldots, \\ s^{\nu^{a-1}(\nu-1)} &\equiv 1 \pmod{\nu^a}. \end{aligned}$$

Donc s vérifierait la formule

$$s^{\nu^{a-1}(\nu-1)} \equiv 1 \pmod{\nu^a},$$

ou, ce qui revient au même, la formule

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

et ne pourrait représenter, comme nous le supposons, une racine primitive de l'équivalence

$$x^N \equiv 1 \pmod{n}.$$

Lorsque ν est de la forme $4x + 1$, et n de la forme ν^a, l'exposant a étant supérieur à l'unité, alors

$$\frac{N}{2} = \nu^{a-1}\frac{\nu - 1}{2}$$

est, ainsi que $\frac{\nu - 1}{2}$, un nombre pair; donc, par suite, la quantité -1 vérifie l'équation

$$x^{\frac{N}{2}} = 1$$

et représente un résidu quadratique suivant le module n. D'ailleurs, l et m étant premiers à n, les deux nombres

$$l, \quad ml$$

sont toujours en même temps ou résidus ou non-résidus. Donc, dans le cas que nous considérons ici,

$$l \quad \text{et} \quad -l \quad \text{ou} \quad n - l$$

seront en même temps résidus ou non-résidus, et la somme des résidus

$$h, \quad h', \quad h'', \quad \ldots$$

se composera, ainsi que la somme des non-résidus, de termes qui, ajoutés deux à deux, donneront des sommes partielles égales à n. En conséquence, on peut énoncer la proposition suivante :

THÉORÈME III. — *ν étant un nombre premier de la forme* $4x+1$, *et*

$$n=\nu^{\alpha}$$

une puissance de ν, dont le degré α surpasse l'unité, si, parmi les entiers inférieurs à n, mais premiers à n, on distingue les résidus quadratiques

$$h,\quad h',\quad h'',\quad \ldots$$

et les non-résidus

$$k,\quad k',\quad k'',\quad \ldots,$$

la somme $h+h'+h''+\ldots$ *des résidus et la somme* $k+k'+k''+\ldots$ *des non-résidus seront, l'une et l'autre, divisibles par n.*

Ainsi, en particulier, on trouvera, pour $n=25=5^2$,

$$\begin{aligned} h+h'+h''+\ldots &= 1+4+6+9+11+14+16+19+21+24 \\ &= 1+4+6+9+11-11-9-6-4-1=0 \end{aligned} \pmod{25},$$

$$\begin{aligned} k+k'+k''+\ldots &= 2+3+7+8+12+13+17+18+22+23 \\ &= 2+3+7+8+12-12-8-7-3-2=0 \end{aligned} \pmod{25}.$$

Aux théorèmes I, II, III on peut évidemment joindre le suivant :

THÉORÈME IV. — *n représentant un nombre entier supérieur à 2, la somme des entiers inférieurs à n, mais premiers à n, sera divisible par n, de sorte qu'en désignant ces entiers par*

$$h,\quad k,\quad l,\quad \ldots$$

on aura

$$h+k+l+\ldots\equiv 0 \pmod{n}. \tag{11}$$

Effectivement, les entiers inférieurs à n et premiers à n, étant deux à deux de la forme

$$l,\quad n-l,$$

fourniront des sommes partielles toutes égales à n. On doit seulement excepter le cas où les nombres

$$l,\quad n-l$$

pourraient devenir égaux, en restant premiers à n. Or, l'équation

$$l=n-l$$

donne

$$l=\frac{1}{2}n,$$

et pour que $\frac{1}{2}n$ soit entier, mais premier à n, il faut qu'on ait $n=2$.

Avant d'aller plus loin, nous présenterons une observation importante. La somme alternée $\mathfrak{S}$ étant déterminée par la formule (2), et le groupe des exposants

$$h,\quad h',\quad h'',\quad \ldots$$

étant supposé, dans cette somme, renfermer l'exposant 1, enfin, le nombre l étant inférieur, ou même supérieur à n, mais premier à n; si, dans la somme alternée $\mathfrak{S}$, on remplace ρ par ρ^l, alors, suivant que l sera équivalent à l'un des nombres

$$h,\quad h',\quad h'',\quad \ldots$$

ou à l'un des nombres

$$k,\quad k',\quad k'',\quad \ldots$$

cette même somme se trouvera multipliée par $+1$ ou par -1, c'est-à-dire que les termes précédés du signe $+$ s'y trouveront échangés ou non contre les termes précédés du signe $-$, cette espèce de multiplication ou d'échange ayant lieu dans le cas même où n renfermerait des facteurs égaux, et où, par suite, en vertu des propriétés de la racine ρ, la somme alternée $\mathfrak{S}$ s'évanouirait. D'ailleurs, si n est un nombre premier ou une puissance d'un tel nombre, on aura, dans le premier cas,

$$\left[\frac{l}{n}\right]=1,$$

dans le second cas

$$\left[\frac{l}{n}\right]=-1.$$

Donc, alors, changer, dans la somme alternée $\mathfrak{S}$, ρ en ρ^l revient à multiplier cette somme, ou plutôt ses divers termes, par $\left[\frac{l}{n}\right]$.

Concevons à présent que n représente un nombre impair quelconque. Il sera le produit de facteurs premiers impairs

$$\nu, \quad \nu', \quad \nu'', \quad \ldots$$

élevés à diverses puissances; et, si l'on désigne les exposants de ces puissances par

$$a, \quad b, \quad c, \quad \ldots,$$

on aura

$$n = \nu^a \nu'^b \nu''^c \ldots, \tag{12}$$

$$\begin{aligned} N &= \nu^{a-1}\nu'^{b-1}\nu''^{c-1}\ldots(\nu-1)(\nu'-1)(\nu''-1)\ldots \\ &= n\left(1-\frac{1}{\nu}\right)\left(1-\frac{1}{\nu'}\right)\left(1-\frac{1}{\nu''}\right)\cdots \end{aligned} \tag{13}$$

Soient d'ailleurs

$$\xi, \quad \eta, \quad \zeta, \quad \ldots$$

des racines primitives qui appartiennent respectivement aux diverses équations

$$x^{\nu^a} = 1, \qquad x^{\nu'^b} = 1, \qquad x^{\nu''^c} = 1, \qquad \ldots. \tag{14}$$

On pourra prendre

$$\rho = \xi\eta\zeta\ldots. \tag{15}$$

Soient, de plus,

$$\Delta, \quad \Delta', \quad \Delta'', \quad \ldots$$

des sommes alternées, respectivement formées avec les racines primitives de la première, ou de la seconde, ou de la troisième, etc. des équations (14), et de manière que la racine

$$\xi \quad \text{ou} \quad \eta \quad \text{ou} \quad \zeta, \quad \ldots$$

représente l'un des termes affectés du signe +. D'après ce qui a été dit dans la Note précédente, si la somme alternée $\mathfrak{S}$ est en même temps une fonction alternée des racines primitives de chacune des équations (14), non seulement cette somme $\mathfrak{S}$ vérifiera l'une des conditions

$$\mathfrak{S} = 0, \tag{16}$$

$$\mathfrak{S}^2 = \pm n, \tag{17}$$

mais en outre le produit

$$\Delta\Delta'\Delta''\ldots$$

sera égal, au signe près, à la somme $\mathfrak{S}$; et comme, dans ce produit, aussi bien que dans la somme $\mathfrak{S}$, le terme

$$\xi\eta\zeta\ldots$$

sera évidemment affecté du signe +, on aura nécessairement

$$\mathfrak{S} = \Delta\Delta'\Delta''\ldots. \tag{18}$$

Il y a plus : les divers termes compris dans la somme $\mathfrak{S}$ seront les produits partiels qu'on peut former en multipliant les divers termes de la somme Δ par les divers termes de la somme Δ', puis par les divers termes de la somme Δ'', et ainsi de suite. Cela posé, on pourra facilement décider si un entier l, inférieur à n et premier à n, fait partie du groupe

$$h, \quad h', \quad h'', \quad \ldots$$

ou du groupe

$$k, \quad k', \quad k'', \quad \ldots.$$

En effet, pour y parvenir, il suffira de savoir si, dans la somme $\mathfrak{S}$, les termes précédés du signe + se trouvent échangés ou non contre les termes précédés du signe −, quand on remplace

$$\rho = \xi\eta\zeta\ldots \quad \text{par} \quad \rho^l = \xi^l\eta^l\zeta^l\ldots,$$

ou, ce qui revient au même, quand on substitue simultanément

$$\xi^l \text{ à } \xi, \qquad \eta^l \text{ à } \eta, \qquad \zeta^l \text{ à } \zeta, \qquad \ldots.$$

Or, de ces diverses substitutions, la première équivaut à la multiplication des divers termes de la somme Δ par

$$\left[\frac{l}{\nu^a}\right],$$

la seconde à la multiplication des divers termes de Δ' par

$$\left[\frac{l}{\nu'^b}\right],$$

la troisième à la multiplication des divers termes de $\Delta^{\prime\prime}$ par

$$\left[\frac{l}{\nu^{\prime\prime c}}\right],$$

etc. Donc, en vertu de ces substitutions réunies, les divers termes du produit $\Delta\Delta'\Delta''\ldots$ ou de la somme $\mathfrak{S}$ pourront être censés multipliés par

$$\left[\frac{l}{\nu^{a}}\right]\left[\frac{l}{\nu'^{b}}\right]\left[\frac{l}{\nu^{\prime\prime c}}\right]\cdots.$$

Donc, en définitive, l fera partie du groupe

$$h,\quad h',\quad h'',\quad \ldots$$

ou du groupe

$$k,\quad k',\quad k'',\quad \ldots,$$

suivant que le produit

$$\left[\frac{l}{\nu^{a}}\right]\left[\frac{l}{\nu'^{b}}\right]\left[\frac{l}{\nu^{\prime\prime c}}\right]\cdots$$

sera égal à $+1$ ou à -1.

Si, en supposant toujours

$$n=\nu^{a}\nu'^{b}\nu^{\prime\prime c},\quad \ldots,$$

on se sert de la notation

$$\left[\frac{l}{n}\right]$$

pour représenter le produit

$$\left[\frac{l}{\nu^{a}}\right]\left[\frac{l}{\nu'^{b}}\right]\left[\frac{l}{\nu^{\prime\prime c}}\right]\cdots,$$

on déduira immédiatement des principes que nous venons d'établir la proposition suivante :

THÉORÈME V. — *Soient n un nombre impair; ν, ν', ν'', ... ses facteurs premiers; a, b, c, ... les exposants de ces facteurs dans le nombre n; l un des entiers inférieurs à n mais premiers à n; et ρ une des racines primitives de l'équation* (1). *Si une somme alternée $\mathfrak{S}$ de ces racines est en même temps une fonction alternée des racines primitives de chacune*

des équations (14), *les deux termes*

$$\rho,\quad \rho^{l}$$

seront, dans la somme alternée $\mathfrak{S}$, affectés du même signe ou de signes contraires suivant qu'on aura

$$\left[\frac{l}{n}\right]=1 \quad \text{ou} \quad \left[\frac{l}{n}\right]=-1. \tag{19}$$

Il en résulte encore que, dans le cas où, comme nous l'avons supposé, le groupe des nombres

$$h,\quad h',\quad h'',\quad \ldots$$

renferme l'unité, l fait partie ou non de ce même groupe suivant que la première ou la seconde des formules (19) *se vérifie.*

Supposons maintenant que, n étant déterminé par la formule (12), et l désignant l'un des nombres entiers inférieurs à n, on nomme

$$\lambda,\quad \lambda',\quad \lambda'',\quad \ldots$$

les restes positifs qu'on obtient quand on divise successivement l par chacun des nombres

$$\nu^{a},\quad \nu'^{b},\quad \nu^{\prime\prime c},\quad \ldots.$$

L'équation

$$\rho=\xi^{\lambda}\eta^{\lambda'}\zeta^{\lambda''}\ldots$$

donnera non seulement

$$\rho^{l}=\xi^{l}\eta^{l'}\zeta^{l''}\ldots,$$

mais aussi

$$\rho^{l}=\xi^{\lambda}\eta^{\lambda'}\zeta^{\lambda''}\ldots; \tag{20}$$

et pareillement la formule

$$\left[\frac{l}{n}\right]=\left[\frac{l}{\nu^{a}}\right]\left[\frac{l}{\nu'^{b}}\right]\left[\frac{l}{\nu^{\prime\prime c}}\right]\cdots$$

entrainera la suivante :

$$\left[\frac{l}{n}\right]=\left[\frac{\lambda}{\nu^{a}}\right]\left[\frac{\lambda}{\nu'^{b}}\right]\left[\frac{\lambda}{\nu^{\prime\prime c}}\right]\cdots. \tag{21}$$

D'ailleurs les diverses racines primitives de l'équation

$$x^{\nu^a} = 1$$

seront les diverses valeurs qu'on obtient pour

$$\xi^{\lambda},$$

en prenant successivement pour λ tous les entiers inférieurs à ν^a et premiers à ν^a. De même les diverses racines primitives de l'équation

$$x^{\nu'^b} = 1$$

seront les diverses valeurs qu'on obtient pour

$$\eta^{\lambda'},$$

en prenant successivement pour λ' tous les entiers inférieurs à ν'^b et premiers à ν'^b; etc. Donc, en vertu du théorème IV de la Note VI, les diverses racines primitives de l'équation (1) seront représentées par les diverses valeurs du produit

$$\xi^{\lambda}\eta^{\lambda'}\zeta^{\lambda''},$$

correspondant aux divers systèmes de valeurs que peuvent acquérir les exposants

$$\lambda, \quad \lambda', \quad \lambda'', \quad \ldots,$$

quand on prend pour λ un entier inférieur à ν^a, mais premier à ν^a, pour λ' un entier inférieur à ν'^b, mais premier à ν'^b, pour λ'' un entier inférieur à ν''^c, mais premier à ν''^c, etc. Donc, puisque les diverses racines primitives de l'équation (1) peuvent encore être représentées par les diverses valeurs qu'on obtient pour

$$\rho^{l},$$

en prenant successivement pour l tous les entiers inférieurs à n, mais premiers à n, on peut affirmer non seulement qu'à chaque valeur de l correspondra, comme il était facile de le prévoir, un seul système des valeurs de

$$\lambda, \quad \lambda', \quad \lambda'', \quad \ldots,$$

mais, réciproquement, qu'à chaque système de valeurs de $\lambda, \lambda', \lambda'', \ldots$ correspondra une valeur de l.

Il est bon d'observer encore que, le nombre n étant impair, la somme alternée $\mathfrak{D}$, déterminée par l'équation (2), ne pourra, en vertu des principes établis dans la Note précédente, vérifier la formule (17), ou

$$\mathfrak{D}^2 = \pm n,$$

que dans deux cas particuliers, savoir : 1° lorsque n sera un nombre premier; 2° lorsque, n étant le produit de facteurs premiers inégaux

$$\nu, \quad \nu', \quad \nu'', \quad \ldots,$$

$\mathfrak{D}$ sera une fonction alternée des racines primitives de chacune des équations

$$(22) \qquad x^{\nu} = 1, \qquad x^{\nu'} = 1, \qquad x^{\nu''} = 1, \qquad \ldots.$$

Ajoutons que, dans l'un et l'autre cas, on aura

$$\mathfrak{D}^2 = n,$$

si n est de la forme $4x + 1$, et

$$\mathfrak{D}^2 = -n,$$

si n est de la forme $4x + 3$.

Jusqu'à présent nous avons supposé que dans l'équation (1) l'exposant n était un nombre impair. Concevons maintenant qu'il devienne un nombre pair, et supposons d'abord qu'il se réduise à une puissance de 2.

Pour qu'on puisse former avec les racines primitives de l'équation (1) une somme alternée

$$\mathfrak{D} = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots,$$

il sera nécessaire que la puissance de 2, représentée par n, soit une puissance supérieure à la première, par conséquent un terme de la progression géométrique

$$4, \quad 8, \quad 16, \quad \ldots.$$

Alors, on pourra supposer, si n est égal à 4,

$$\mathfrak{D} = \rho - \rho^3;$$

et si n est égal à 8,

$$\mathfrak{D} = \rho + \rho^3 - \rho^5 - \rho^7,$$

ou bien

$$\mathfrak{D} = \rho + \rho^5 - \rho^3 - \rho^7,$$

ou bien encore

$$\mathfrak{D} = \rho + \rho^7 - \rho^3 - \rho^5,$$

etc. Alors aussi la formule (17) ne pourra être vérifiée que dans trois cas spéciaux, savoir : 1° lorsque, n étant égal à 4, on aura

$$\mathfrak{D} = \rho - \rho^3, \qquad \mathfrak{D}^2 = -4;$$

2° lorsque, n étant égal à 8, on aura

$$\mathfrak{D} = \rho + \rho^3 - \rho^5 - \rho^7, \qquad \mathfrak{D}^2 = -8;$$

3° lorsque, n étant égal à 8, on aura

$$\mathfrak{D} = \rho + \rho^7 - \rho^3 - \rho^5, \qquad \mathfrak{D}^2 = 8.$$

Or, de ces trois cas le dernier est le seul dans lequel les sommes

$$h + h' + \ldots, \qquad k + k' + \ldots$$

deviennent divisibles par n. En effet, on aura dans le premier cas

$$h = 1, \qquad k = 3,$$

par conséquent

$$h \equiv -k \equiv 1 \pmod{n};$$

dans le second cas

$$h + h' = 1 + 3 = 4, \qquad k + k' = 5 + 7 = 12,$$

par conséquent

$$h + h' \equiv k + k' \equiv \frac{1}{2} n \pmod{n};$$

et dans le troisième cas

$$h + h' = 1 + 7 = 8, \qquad k + k' = 3 + 5 = 8,$$

par conséquent

$$h + h' = k + k' = n.$$

Concevons maintenant que n, étant un nombre pair, ne se réduise plus à une puissance de 2. Si l'on nomme ν, ν', ν'', ... les facteurs premiers de n, dont l'un, ν par exemple, se réduira simplement au nombre 2, on pourra supposer encore la valeur de n déterminée par l'équation (12), et la valeur de ρ par l'équation (15),

$$\xi, \quad \eta, \quad \zeta, \quad \ldots$$

diésgnant des racines primitives qui appartiennent respectivement à la première, à la seconde, à la troisième, etc. des formules (14). Il y a plus : si l'on nomme

$$\Delta, \quad \Delta', \quad \Delta'', \quad \ldots$$

des sommes alternées respectivement formées avec les racines primitives de la première, de la seconde, de la troisième, etc. des équations (14), et de manière que la racine

$$\xi \text{ ou } \eta \text{ ou } \zeta \ldots$$

représente l'un des termes affectés du signe +; si d'autre part on nomme

$$\lambda, \quad \lambda', \quad \lambda'', \quad \ldots$$

les restes qu'on obtient quand on divise successivement par chacun des facteurs

$$\nu^a, \quad \nu'^{b'}, \quad \nu''^{c''}, \quad \ldots$$

un entier l inférieur à n, mais premier à n, on se trouvera de nouveau conduit aux formules (18) et (20) : et l'on conclura toujours de la formule (20) qu'à chaque système de valeurs de

$$\lambda, \quad \lambda', \quad \lambda'', \quad \ldots$$

correspond une seule valeur de l. D'ailleurs la formule (18) fournira encore le moyen de décider si un entier l, inférieur à n, mais premier à n, fait partie du groupe

$$h, \quad h', \quad h'', \quad \ldots$$

qui par hypothèse renferme l'unité, ou du groupe

$$k, \quad k', \quad k'', \quad \ldots.$$

En effet, pour y parvenir, il suffira de savoir si, dans la somme $\mathfrak{S}$, les termes du signe $+$ se trouvent échangés ou non contre les termes précédés du signe $-$, quand on remplace

$$\rho = \xi\eta\zeta\ldots \quad \text{par} \quad \rho' = \xi^l\eta'^l\zeta'^l\ldots,$$

ou, ce qui revient au même, quand on substitue simultanément

$$\xi^l \text{ à } \xi, \quad \eta^l \text{ à } \eta, \quad \zeta^l \text{ à } \zeta, \quad \ldots.$$

Or, de ces diverses substitutions, la seconde, la troisième, ..., simultanément effectuées, changeront ou ne changeront pas les termes précédés d'un signe en ceux que précède le signe contraire, par exemple, les termes affectés du signe $+$ en ceux qu'affecte le signe $-$, suivant que l'expression

$$\left[\frac{l}{\gamma^b}\right]\left[\frac{l}{\gamma'^c}\right]\ldots = \left[\frac{l}{\gamma^b\gamma'^c\ldots}\right]$$

sera égale à $+1$ ou à -1. Cela posé, en passant du cas où la lettre n désigne un nombre impair au cas où cette lettre représente un nombre pair, on obtiendra, au lieu du théorème V, la proposition suivante :

THÉORÈME VI. — *Soient n un nombre pair,*

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

ses facteurs premiers,

$$a, \quad b, \quad c, \quad \ldots$$

les exposants de ces facteurs dans le nombre n, l un des entiers inférieurs à n et premiers à n, et ρ une des racines primitives de l'équation (1). *Si une somme alternée* $\mathfrak{S}$ *de ces racines est en même temps une fonction alternée des racines primitives de chacune des équations* (14), *et a, en conséquence, pour facteur une somme alternée* Δ *des racines primitives* $\xi, \xi', \ldots$ *de l'équation*

$$x^{2^a} = 1, \tag{23}$$

les deux termes

$$\rho, \quad \rho'$$

seront, dans la somme alternée $\mathfrak{S}$, *affectés du même signe : 1° lorsque les termes*

$$\xi, \quad \xi'$$

étant affectés du même signe dans la somme alternée Δ, *on aura*

$$\left[\frac{l}{\gamma^b\gamma'^c\ldots}\right] = 1,$$

ou, ce qui revient au même,

$$\left[\frac{l}{\frac{1}{2^a}n}\right] = 1; \tag{24}$$

2° lorsque les termes

$$\xi, \quad \xi'$$

étant affectés de signes contraires dans la somme alternée Δ, *on aura*

$$\left[\frac{l}{\gamma^b\gamma'^c\ldots}\right] = -1,$$

ou, ce qui revient au même,

$$\left[\frac{l}{\frac{1}{2^a}n}\right] = -1. \tag{25}$$

Considérons en particulier le cas où, n étant pair, la somme $\mathfrak{S}$ vérifie la condition (17), savoir :

$$\mathfrak{S}^2 = \pm n.$$

Dans ce cas, en vertu des principes établis dans la Note précédente, $\mathfrak{S}$ sera nécessairement une fonction alternée des racines primitives de chacune des équations (14), et, de plus, on aura, d'une part,

$$a = 2, \quad 2^a = 4,$$

ou

$$a = 3, \quad 2^a = 8;$$

d'autre part,

$$b = 1, \quad c = 1, \quad \ldots, \quad n = 2^a\nu'^\nu\ldots.$$

Or, supposons d'abord

$$2^a = 4.$$

Alors on trouvera

$$n = 4\nu\nu'\nu'' \ldots, \qquad \Delta = \rho - \rho^3 = \rho^1 - \rho^{-1},$$

et le théorème VI entraînera le suivant :

THÉORÈME VII. — *Soient n un nombre pair divisible par* 4,

$$\nu', \quad \nu'', \quad \ldots$$

les facteurs premiers $\frac{n}{4}$, *supposés impairs et inégaux, l un des entiers inférieurs à n, mais premiers à n, et* ρ *l'une des racines primitives de l'équation*

$$x^n = 1.$$

Si une somme alternée $\mathfrak{S}$ *de ces racines vérifie la condition*

$$\mathfrak{S}^2 = \pm n,$$

non seulement $\mathfrak{S}$ *sera une fonction alternée des racines primitives de chacune des équations*

$$x^3 = 1, \qquad x^{\nu} = 1, \qquad x^{\nu'} = 1, \qquad \ldots, \tag{26}$$

mais de plus les deux termes

$$\rho, \quad \rho^l$$

seront, dans la somme alternée $\mathfrak{S}$, *affectés du même signe quand on aura simultanément*

$$\begin{cases} l \equiv 1 \pmod 4, & \left[\dfrac{l}{\frac{1}{4}n}\right] = 1, \\ \text{ou bien} \\ l \equiv -1 \pmod 4, & \left[\dfrac{l}{\frac{1}{4}n}\right] = -1, \end{cases} \tag{27}$$

et affectés de signes contraires, quand on aura

$$\begin{cases} l \equiv 1 \pmod 4, & \left[\dfrac{l}{\frac{1}{4}n}\right] = -1, \\ \text{ou bien} \\ l \equiv -1 \pmod 4, & \left[\dfrac{l}{\frac{1}{4}n}\right] = 1. \end{cases} \tag{28}$$

Supposons, en second lieu,

$$2^a = 8.$$

Alors on aura

$$n = 8\nu'\nu'' \ldots;$$

et, si l'on veut que la fonction alternée $\mathfrak{S}$ vérifie la condition

$$\mathfrak{S}^2 = n,$$

on devra supposer

$\Delta = \rho + \rho^7 - \rho^3 - \rho^5$, lorsque n sera de la forme $4x+1$,

et

$\Delta = \rho + \rho^3 - \rho^5 - \rho^7$, lorsque n sera de la forme $4x+3$.

Au contraire, si l'on veut que la somme alternée $\mathfrak{S}$ vérifie la condition

$$\mathfrak{S}^2 = -n,$$

on devra supposer

$\Delta = \rho + \rho^3 - \rho^5 - \rho^7$, lorsque n sera de la forme $4x+1$,

et

$\Delta = \rho + \rho^7 - \rho^3 - \rho^5$, lorsque n sera de la forme $4x+1$.

Cela posé, le théorème VI entraînera évidemment les propositions suivantes :

THÉORÈME VIII. — *Soient n un nombre pair divisible par* 8;

$$\nu', \quad \nu'', \quad \ldots$$

les facteurs premiers de $\frac{n}{8}$ *supposés impairs et inégaux; l un des entiers inférieurs à n, mais premiers à n; et* ρ *une racine primitive de l'équation*

$$x^n = 1.$$

Enfin, supposons qu'une somme alternée $\mathfrak{D}$ *de ces racines vérifie la condition*

$$\mathfrak{D}^2 = n.$$

Non seulement cette somme sera une fonction alternée des racines primitives de chacune des équations

$$x^8 = 1, \quad x^{\nu'} = 1, \quad x^{\nu''} = 1, \quad \ldots, \tag{29}$$

mais de plus les termes

$$\rho, \quad \rho^l$$

seront, dans la somme $\mathfrak{D}$, *affectés du même signe : 1° si,* $\frac{n}{8}$ *étant de la forme* $4x+1$, *on a*

$$\begin{cases} l \equiv 1 \quad ou \quad 7, & \left[\frac{l}{\frac{1}{8}n}\right] = 1, \\ ou\ bien \\ l \equiv 3 \quad ou \quad 5, & \left[\frac{l}{\frac{1}{8}n}\right] = -1; \end{cases} \tag{30}$$

2° si, $\frac{n}{8}$ *étant de la forme* $4x+3$, *on a*

$$\begin{cases} l \equiv 1 \quad ou \quad 3, & \left[\frac{l}{\frac{1}{8}n}\right] = 1, \\ ou\ bien \\ l \equiv 3 \quad ou \quad 7, & \left[\frac{l}{\frac{1}{8}n}\right] = -1. \end{cases} \tag{31}$$

THÉORÈME IX. — *Soient n un nombre pair divisible par* 8,

$$\nu', \quad \nu'', \quad \ldots$$

les facteurs premiers de $\frac{n}{8}$, *supposés impairs et inégaux, l un des entiers inférieurs n, mais premiers à n, et* ρ *une racine primitive de l'équation*

$$x^n = 1.$$

Enfin, supposons qu'une somme alternée $\mathfrak{D}$ *de ces racines vérifie la condition*

$$\mathfrak{D}^2 = -n.$$

Non seulement cette somme sera une fonction alternée des racines primitives de chacune des équations

$$x^8 = 1, \quad x^{\nu'} = 1, \quad x^{\nu''} = 1, \quad \ldots; \tag{32}$$

mais de plus les termes

$$\rho, \quad \rho^l$$

seront, dans la somme alternée $\mathfrak{D}$, *affectés du même signe : 1° si,* $\frac{n}{8}$ *étant de la forme* $4x+1$, *on a*

$$\begin{cases} l \equiv 1 \quad ou \quad 3, & \left[\frac{l}{\frac{1}{8}n}\right] = 1, \\ ou\ bien \\ l \equiv 5 \quad ou \quad 7, & \left[\frac{l}{\frac{1}{8}n}\right] = -1; \end{cases} \tag{33}$$

2° si, $\frac{n}{8}$ *étant de la forme* $4x+3$, *on a*

$$\begin{cases} l \equiv 1 \quad ou \quad 7, & \left[\frac{l}{\frac{1}{8}n}\right] = 1, \\ ou\ bien \\ l \equiv 3 \quad ou \quad 5, & \left[\frac{l}{\frac{1}{8}n}\right] = -1. \end{cases} \tag{34}$$

Revenons maintenant à la formule (7), où les nombres

$$h, \quad h', \quad h'', \quad \ldots \quad \text{ou} \quad k, \quad k', \quad k'', \quad \ldots$$

représentent les exposants des termes affectés du signe + ou du signe − dans la somme alternée $\mathfrak{D}$. Il suit des théorèmes I et III que cette formule se vérifie : 1° quand n est un nombre premier impair, supérieur à 3; 2° quand n est une puissance quelconque d'un nombre premier de la forme $4x+1$. J'ajoute qu'elle se vérifiera encore, si n est un nombre composé qui renferme plusieurs facteurs premiers, l'un de

ces facteurs pouvant être le nombre 2 élevé à une puissance dont le degré surpasse l'unité, et si, d'ailleurs, la valeur de n étant donnée par la formule (12), la somme alternée $\mathfrak{D}$ est une fonction alternée des racines primitives de chacune des équations (14). En effet, supposons d'abord n impair. Alors, en vertu du cinquième théorème joint à la formule (21), les valeurs de l qui appartiendront au groupe

$$h,\quad h',\quad h'',\quad \ldots$$

seront celles qui vérifieront la condition

$$\left[\frac{l}{n}\right]=1 \tag{35}$$

ou

$$\left[\frac{\lambda}{\nu^a}\right]\left[\frac{\lambda'}{\nu'^b}\right]\left[\frac{\lambda''}{\nu''^c}\right]\cdots=1; \tag{36}$$

par conséquent, celles qui vérifieront ou les conditions

$$\left[\frac{\lambda}{\nu^a}\right]=1,\qquad \left[\frac{\lambda'}{\nu'^b}\right]\left[\frac{\lambda''}{\nu''^c}\right]\cdots=1 \tag{37}$$

ou les conditions

$$\left[\frac{\lambda}{\nu^a}\right]=-1,\qquad \left[\frac{\lambda'}{\nu'^b}\right]\left[\frac{\lambda''}{\nu''^c}\right]\cdots=-1. \tag{38}$$

Or, le nombre des valeurs de l qui vérifieront la condition (35), ou, ce qui revient au même, le nombre des systèmes de valeurs de λ, λ', λ'', ... qui vérifieront la condition (36), sera

$$\frac{1}{2}N=\frac{1}{2}\nu^{a-1}\nu'^{b-1}\nu''^{c-1}\ldots(\nu-1)(\nu'-1)(\nu''-1)\ldots,$$

aussi bien que le nombre des valeurs de l qui vérifieront la condition

$$\left[\frac{l}{n}\right]=-1$$

ou

$$\left[\frac{\lambda}{\nu^a}\right]\left[\frac{\lambda'}{\nu'^b}\right]\left[\frac{\lambda''}{\nu''^c}\right]\cdots=-1.$$

Pareillement, on reconnaîtra que le produit

$$\frac{1}{2}\nu'^{b-1}\nu''^{c-1}\ldots(\nu'-1)(\nu''-1)\ldots$$

exprime le nombre des systèmes de valeurs de

$$\lambda',\quad \lambda'',\quad \ldots,$$

qui sont propres à vérifier, soit la seconde des formules (37), soit la seconde des formules (38). Donc ce dernier produit, que nous représentons par $\frac{1}{2}\mathfrak{N}$, en posant, pour abréger,

$$\mathfrak{N}=\nu'^{b-1}\nu''^{c-1}\ldots(\nu'-1)(\nu''-1)\ldots, \tag{39}$$

exprimera le nombre des valeurs de l, qui, étant comprises dans le groupe

$$h,\quad h',\quad h'',\quad \ldots,$$

seront équivalentes, suivant le module ν^a, à une même valeur de λ, par laquelle la première des formules (37) ou (38) se trouve vérifiée. Donc la somme des valeurs de l, comprises dans le groupe

$$h,\quad h',\quad h'',\quad \ldots,$$

c'est-à-dire, en d'autres termes, la somme

$$h+h'+h''+\ldots$$

sera équivalente, suivant le module ν^a, au produit du nombre

$$\frac{1}{2}\mathfrak{N}$$

par la somme des valeurs de λ, qui vérifieront l'une des formules

$$\left[\frac{\lambda}{\nu^a}\right]=1,\qquad \left[\frac{\lambda}{\nu^a}\right]=-1. \tag{40}$$

Or, comme chaque valeur de λ satisfera nécessairement à l'une des équations (40), il est clair que la dernière somme comprendra toutes les valeurs de λ, et sera, par suite, en vertu du théorème IV,

divisible par ν^a. Donc aussi la première somme

$$h + h' + h'' + \dots$$

sera divisible par ν^a; et, comme elle devra être, pour les mêmes raisons, divisible par ν'^b, par ν''^c, ..., il est clair que, dans l'hypothèse admise, elle sera divisible par le produit

$$n = \nu^a \nu'^b \nu''^c \dots.$$

On pourra encore en dire autant de la somme

$$k + k' + k'' + \dots,$$

puisque, en vertu du théorème IV, la somme totale

$$h + h' + h'' + \dots + k + k' + k'' + \dots$$

devra encore être divisible par n. Donc si, n étant impair, la somme alternée $\mathfrak{D}$ est en même temps une fonction alternée des racines primitives de chacune des équations (14), les deux sommes

$$h + h' + h'' + \dots, \quad k + k' + k'' + \dots$$

vérifieront la formule (7).

Supposons maintenant que, dans l'équation (12), l'un des facteurs

$$\nu, \quad \nu', \quad \nu'', \quad \dots$$

se réduise au nombre 2, mais se trouve élevé à une puissance dont le degré surpasse l'unité. On prouvera encore, non plus à l'aide d'une seule formule (21), mais à l'aide des formules (18) et (28), que la moitié du produit $\mathfrak{H}$, déterminé par l'équation (38), exprime le nombre des valeurs de l qui, étant comprises dans le groupe

$$h, \quad h', \quad h'', \quad \dots,$$

sont équivalentes, suivant le module ν^a, à une même valeur de λ. D'ailleurs, parmi les termes affectés du signe + dans la somme $\mathfrak{D}$ que détermine la formule (18), on en trouvera qui auront pour facteur un terme donné quelconque, affecté du signe + ou du signe − dans la somme Δ. Donc la somme

$$h + h' + h'' + \dots,$$

sera encore, dans l'hypothèse admise, équivalente, suivant le module ν^a, au produit de $\frac{1}{2}\mathfrak{H}$, par la somme totale des valeurs de λ. Donc, cette dernière somme devant être, en vertu du théorème IV, divisible par ν^a, on pourra en dire autant de la première, qui devra être divisible par chacun des nombres

$$\nu^a, \quad \nu'^b, \quad \nu''^c, \quad \dots,$$

et se réduire, en conséquence, à un multiple de n. La somme totale

$$h + h' + h'' + \dots + k + k' + k'' + \dots$$

devant être elle-même, en vertu du théorème IV, un multiple de n, il suit de ce qu'on vient de dire que les deux sommes

$$h + h' + h'' + \dots, \qquad k + k' + k'' + \dots$$

devront encore vérifier la formule (7).

En résumé, on pourra énoncer la proposition suivante :

THÉORÈME X. — *n étant un nombre composé qui renferme divers facteurs premiers ν, ν', ν'', ... et ne puisse devenir pair, sans être divisible par 4, si l'on suppose que, la valeur de n étant fournie par l'équation (12), la somme alternée $\mathfrak{D}$, déterminée par la formule (2), soit en même temps une fonction alternée des racines primitives de chacune des équations (4), on aura*

$$h + h' + h'' + \dots \equiv k + k' + k'' + \dots \equiv 0 \pmod{n}.$$

Il est bon d'observer que, dans le théorème précédent, les exposants de tous les facteurs impairs pourraient se réduire à l'unité.

En vertu des principes établis dans la Note précédente, pour que la somme alternée $\mathfrak{D}$ vérifie la condition

$$\mathfrak{D}^2 = \pm n,$$

n étant un nombre premier ou composé, pair ou impair, déterminé par la formule (12), il est nécessaire que les facteurs premiers impairs de n soient inégaux, le facteur pair, s'il existe, étant 4 ou 8, et qu'en outre $\mathfrak{D}$ soit une fonction alternée des racines primitives de chacune des équations (14). Cela posé, les théorèmes I et II entraînent évidemment la proposition suivante :

THÉORÈME XI. — *Lorsque la somme alternée* $\mathfrak{D}$, *déterminée par la formule* (2), *vérifie l'équation* (17), *savoir*

$$\mathfrak{D}^2 = \pm n,$$

les deux groupes d'exposants

$$h,\ h',\ h'',\ \ldots,$$
$$k,\ k',\ k'',\ \ldots$$

vérifient la condition (7), *savoir*

$$h + h' + h'' + \ldots \equiv k + k' + k'' + \ldots \equiv 0 \pmod{n},$$

à moins toutefois que le module n ne se réduise à l'un des trois nombres

$$3,\ 4,\ 8.$$

On peut d'ailleurs observer que la condition dont il s'agit est vérifiée, pour le cas même où l'on suppose $n = 8$, lorsque $\mathfrak{D}$, étant réduit à la somme alternée

$$\rho + \rho^7 - \rho^3 - \rho^5,$$

vérifie l'équation

$$\mathfrak{D}^2 = 8 = n,$$

mais cesse de l'être lorsque $\mathfrak{D}$, étant réduit à

$$\rho + \rho^3 - \rho^5 - \rho^7,$$

vérifie l'équation

$$\mathfrak{D}^2 = -8 = -n.$$

NOTE IX.

THÉORÈMES DIVERS RELATIFS AUX SOMMES ALTERNÉES DES RACINES PRIMITIVES DES ÉQUATIONS BINOMES.

Soient :

n un nombre entier supérieur à 2 ;
$h, k, l, \ldots$ les entiers inférieurs à n, mais premiers à n ;
N le nombre des entiers $h, k, l, \ldots$;
ρ une racine primitive de l'équation

$$x^n = 1; \tag{1}$$

enfin, supposons les entiers

$$h,\ k,\ l,\ \ldots$$

partagés en deux groupes

$$h,\ h',\ h'',\ \ldots \quad \text{et} \quad k,\ k',\ k'',\ \ldots,$$

de telle manière que l'expression

$$\mathfrak{D} = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots \tag{2}$$

représente une somme alternée des racines primitives de l'équation (1), et que l'unité fasse partie du premier groupe

$$h,\ h',\ h'',\ \ldots.$$

Alors, la quantité m étant équivalente, suivant le module n, à l'un des entiers

$$h,\ k,\ l,\ \ldots,$$

les produits

$$mh,\ mh',\ mh'',\ \ldots$$

seront équivalents, à l'ordre près, soit aux termes du premier groupe

$$k,\ k',\ k'',\ \ldots,$$

soit aux termes du second groupe

$$h,\ h',\ h'',\ \ldots,$$

selon que m fera partie du premier ou du second groupe; et, au contraire, les produits

$$mk, \quad mk', \quad mk'', \quad \dots$$

seront équivalents, dans le premier cas, aux nombres

$$k, \quad k', \quad k'', \quad \dots,$$

dans le second cas, aux nombres

$$h, \quad h', \quad h'', \quad \dots.$$

Donc, l étant l'un quelconque des entiers inférieurs à n, mais premiers à n, le nombre l et le produit ml, ou plutôt le reste de la division de ml par n, appartiendront ou non au même groupe, selon que la quantité m deviendra équivalente à un terme du premier ou du second groupe. Ainsi, par exemple,

$$l \text{ et } -l, \qquad \text{ou plutôt} \qquad n-l,$$

appartiendront ou non au même groupe, suivant que la quantité

$$-1, \qquad \text{ou plutôt} \qquad n-1,$$

fera partie du premier ou du second groupe. Pareillement, si le nombre n est impair,

$$l \text{ et } \iota l$$

appartiendront ou non au même groupe, et par suite les produits

$$\iota h, \quad \iota h', \quad \iota h'', \quad \dots$$

seront équivalents, à l'ordre près, aux nombres

$$h, \quad h', \quad h'', \quad \dots$$

ou aux nombres

$$k, \quad k', \quad k'', \quad \dots,$$

suivant que le nombre ι fera partie du premier groupe ou du second.

Des principes que nous venons de rappeler il résulte encore que, si l'on remplace

$$\rho \qquad \text{par} \qquad \rho^m,$$

les deux groupes des racines primitives

$$\rho^h, \quad \rho^{h'}, \quad \rho^{h''}, \quad \dots \qquad \text{et} \qquad \rho^k, \quad \rho^{k'}, \quad \rho^{k''}, \quad \dots$$

resteront composés chacun des mêmes racines, où se transformeront l'un dans l'autre, suivant que m sera équivalent, suivant le module n, à l'un des nombres

$$h, \quad h', \quad h'', \quad \dots$$

ou à l'un des nombres

$$k, \quad k', \quad k'', \quad \dots.$$

Donc, si l'on nomme

$$\mathrm{I} = \mathrm{f}(\rho^h, \rho^{h'}, \rho^{h''}, \dots)$$

une fonction symétrique des racines

$$\rho^h, \quad \rho^{h'}, \quad \rho^{h''}, \quad \dots,$$

et

$$\mathrm{J} = \mathrm{f}(\rho^k, \rho^{k'}, \rho^{k''}, \dots)$$

ce que devient la fonction I, quand on y remplace

$$\rho^h, \quad \rho^{h'}, \quad \rho^{h''}, \quad \dots$$

par

$$\rho^k, \quad \rho^{k'}, \quad \rho^{k''}, \quad \dots,$$

la somme

$$\mathrm{I} + \mathrm{J}$$

ne changera jamais ni de valeur ni de signe, et la différence

$$\mathrm{I} - \mathrm{J}$$

pourra seulement changer de signe, en conservant toujours, au signe près, la même valeur, lorsqu'on remplacera la racine primitive ρ par une autre racine primitive ρ^m. Donc alors la somme $\mathrm{I} + \mathrm{J}$ sera une fonction symétrique, et la différence $\mathrm{I} - \mathrm{J}$ une fonction alternée des racines primitives de l'équation (1).

Si le nombre n est tel que l'on ait

$$\mathfrak{G}^2 = \pm n, \tag{3}$$

alors, en vertu des principes établis dans la Note précédente, ce

nombre sera de l'une des formes

$$\nu\nu'\nu'', \quad \ldots, \quad 4\nu'\nu'', \quad \ldots, \quad 8\nu'\nu'', \quad \ldots,$$

$\nu, \nu', \nu'', \ldots$ désignant des facteurs impairs et premiers, inégaux entre eux; et, si d'ailleurs n ne se réduit pas à l'un des trois nombres

$$3, \quad 4, \quad 8,$$

on aura

$$h + h' + h'' + \ldots \equiv k + k' + k'' + \ldots \equiv 0 \pmod{n}. \tag{4}$$

Ajoutons que l'équation (3) pourra se réduire à

$$\omega^2 = n, \tag{5}$$

dans le cas seulement où, les facteurs impairs de n étant inégaux, n sera de l'une des formes

$$4x+1, \quad 4(4x+3), \quad 8(2x+1),$$

et qu'alors chacun des nombres

$$h, \quad h', \quad h'', \quad \ldots$$

vérifiera : 1° si n est de la forme $4x+1$, la condition

$$\left[\frac{h}{n}\right] = 1; \tag{6}$$

2° si $\frac{n}{4}$ est entier et de la forme $4x+8$, les conditions

$$\left[\frac{h}{\frac{1}{4}n}\right] = 1, \qquad h \equiv 1 \pmod{4}, \tag{7}$$

ou

$$\left[\frac{h}{\frac{1}{4}n}\right] = -1, \qquad h \equiv -1 \pmod{4}; \tag{8}$$

3° si $\frac{n}{8}$ est entier et de la forme $4x+3$, les conditions

$$\left[\frac{h}{\frac{1}{8}n}\right] = 1, \qquad h \equiv 1 \text{ ou } 7 \pmod{8}, \tag{9}$$

ou

$$\left[\frac{h}{\frac{1}{8}n}\right] = -1, \qquad h \equiv 3 \text{ ou } 5 \pmod{7}; \tag{10}$$

4° si $\frac{n}{8}$ est entier et de la forme $4x+3$, les conditions

$$\left[\frac{h}{\frac{1}{8}n}\right] = 1, \qquad h \equiv 1 \text{ ou } 3 \pmod{8}, \tag{11}$$

ou

$$\left[\frac{h}{\frac{1}{8}n}\right] = -1, \qquad h \equiv 5 \text{ ou } 7 \pmod{8}. \tag{12}$$

Au contraire, l'équation (3) pourra se réduire à

$$\omega^2 = -n, \tag{13}$$

dans le cas seulement où, les facteurs impairs de n étant inégaux, n sera de l'une des formes

$$4x+3, \quad 4(4x+1), \quad 8(2x+1);$$

et alors chacun des nombres

$$h, \quad h', \quad h'', \quad \ldots$$

vérifiera : 1° si n est de la forme $4x+3$, la condition (6); 2° si $\frac{n}{4}$ est entier et de la forme $4x+1$, les conditions (7) ou (8); 3° si $\frac{n}{8}$ est entier et de la forme $4x+3$, les conditions (9) ou (10); 4° si $\frac{n}{8}$ est entier et de la forme $4x+1$, les conditions (11) ou (12).

Si l'on désigne par

$$\nu, \quad \nu', \quad \nu'', \quad \ldots$$

les facteurs premiers de n, et par

$$a, \quad b, \quad c, \quad \ldots$$

les exposants des puissances auxquelles ces mêmes facteurs sont élevés, l'équation

$$n = \nu^a \nu'^b \nu''^c, \quad \ldots \tag{14}$$

entrainera généralement la suivante :

$$(15) \qquad N = \nu^{\alpha-1}\nu'^{\beta-1}\nu''^{\gamma-1} - (\nu-1)(\nu'-1)(\nu''-1)\ldots.$$

Si l'on suppose en particulier n impair, et composé de facteurs impairs inégaux

$$\nu, \quad \nu', \quad \nu'', \quad \ldots,$$

alors l'équation

$$(16) \qquad n = \nu'\nu\nu''\ldots$$

entrainera les suivantes :

$$(17) \qquad N = (\nu-1)(\nu'-1)(\nu''-1)\ldots,$$

$$(18) \qquad \left[\frac{-1}{n}\right] = \left[\frac{-1}{\nu}\right]\left[\frac{-1}{\nu'}\right]\left[\frac{-1}{\nu''}\right]\ldots,$$

$$(19) \qquad \left[\frac{2}{n}\right] = \left[\frac{2}{\nu}\right]\left[\frac{2}{\nu'}\right]\left[\frac{2}{\nu''}\right]\ldots.$$

D'ailleurs, ν étant un nombre premier impair, l'expression

$$\left[\frac{-1}{\nu}\right] = (-1)^{\frac{\nu-1}{2}}$$

se réduira simplement à $+1$ ou à -1, suivant que ν sera de la forme $4x+1$ ou $4x-1$. Donc, en vertu de la formule (18), l'expression

$$\left[\frac{-1}{n}\right]$$

sera égale à $+1$ ou à -1, suivant que les facteurs premiers de n, de la forme $4x-1$, seront en nombre pair ou en nombre impair; et, comme le nombre n sera, dans le premier cas, de la forme $4x+1$, dans le second cas, de la forme $4x-1$, il est clair que l'équation (18) pourra être réduite à

$$(20) \qquad \left[\frac{-1}{n}\right] = (-1)^{\frac{n-1}{2}}.$$

De plus, ν étant un nombre premier impair, l'expression

$$\left[\frac{2}{\nu}\right] = (-1)^{\frac{\nu^2-1}{8}}$$

se réduira simplement à $+1$ ou à -1, suivant que ν^2 sera de la forme $16x+1$ ou $16x+9$. Donc, en vertu de la formule (19), l'expression

$$\left[\frac{2}{n}\right]$$

sera égale à $+1$ ou à -1, suivant que, parmi les carrés

$$\nu^2, \quad \nu'^2, \quad \nu''^2, \quad \ldots,$$

ceux qui se présenteront sous la forme

$$16x+9$$

seront en nombre pair ou en nombre impair. D'ailleurs, le produit de deux facteurs de la forme $16x+9$ étant lui-même de la forme $16x+1$, il est clair que le carré

$$n^2 = \nu^2\nu'^2\nu''^2\ldots$$

sera dans le premier cas de la forme $16x+1$, dans le second cas de la forme $16x+9$. Donc, par suite n sera, dans le premier cas, de la forme $8x\pm1$, ou, ce qui revient au même, de l'une des formes

$$8x+1 \qquad \text{ou} \qquad 8x+7;$$

dans le second cas, de la forme $8x\pm3$, ou, ce qui revient au même, de l'une des formes

$$8x+3 \qquad \text{ou} \qquad 8x+5;$$

et l'équation (19) pourra être réduite à

$$(21) \qquad \left[\frac{2}{n}\right] = (-1)^{\frac{n^2-1}{8}}.$$

Supposons maintenant que, les facteurs impairs de n étant inégaux et représentés par

$$\nu'\nu'', \quad \ldots,$$

n renferme, en outre, un facteur pair représenté par 4 ou par 8; alors, eu égard à la formule (20), il est clair que l'équation

$$(22) \qquad n = 4\nu'\nu''\ldots$$

entrainera la suivante :

$$\left[\frac{-1}{\frac{1}{4}n}\right] = (-1)^{\frac{n-1}{2}}, \tag{23}$$

ou que l'équation

$$n = 8\sqrt{\sqrt{\ldots}} \tag{24}$$

entrainera la suivante :

$$\left[\frac{-1}{\frac{1}{8}n}\right] = (-1)^{\frac{n-1}{8}}. \tag{25}$$

Des formules (20), (23), (25) jointes aux conditions (6), (7), (8), (9), (10), (11), (12), on déduit immédiatement les propositions que nous allons énoncer.

THÉORÈME I. — *Soit* ρ *l'une des racines primitives de l'équation* (1), *et supposons les exposants des puissances diverses de* ρ *partagés en deux groupes*

$$h,\ h',\ h'',\ \ldots,\qquad k,\ k',\ k'',\ \ldots,$$

chaque exposant étant censé appartenir au premier ou au second groupe, suivant que la puissance correspondante se trouve affectée du signe + *ou du signe* — *dans une somme alternée* $\mathfrak{S}$ *de ces racines primitives. Les deux exposants*

$$1 \text{ et } -1 \quad \text{ou} \quad n-1$$

appartiendront au même groupe, si la somme $\mathfrak{S}$ *vérifie la condition*

$$\mathfrak{S}^2 = n,$$

et à des groupes différents, si la somme $\mathfrak{S}$ *vérifie la condition*

$$\mathfrak{S}^2 = -n.$$

Par suite, l étant premier à n, les exposants

$$l \text{ et } -l \quad \text{ou} \quad n-l$$

appartiendront au même groupe, si l'on a $\mathfrak{S} = n$, ce qui suppose que

n soit de l'une des formes

$$4x+1,\quad 4(4x+3),\quad 8(2x+1),$$

et à des groupes différents, si l'on a $\mathfrak{S}^2 = -n$, ce qui suppose que n soit de l'une des formes

$$4x+3,\quad 4(4x+1),\quad 8(2x+1).$$

On peut aussi, de l'équation (21), jointe à ce qui a été dit plus haut, déduire le théorème dont voici l'énoncé :

THÉORÈME II. — *Le nombre* n *étant impair, soit* ρ *l'une des racines primitives de l'équation* (1), *et supposons les exposants des puissances diverses de* ρ *partagés en deux groupes, chaque exposant étant censé appartenir au premier ou au second groupe, suivant que la puissance correspondante se trouve affectée du signe* + *ou du signe* — *dans une somme alternée* $\mathfrak{S}$ *de ces racines, qui offre pour carré* $\pm n$. *Les deux exposants*

$$1 \text{ et } 2$$

ou plus généralement

$$l \text{ et } 2l$$

appartiendront au même groupe, ou à des groupes différents, suivant que le module n *sera de l'une des formes*

$$8x+1,\quad 8x+7$$

ou de l'une des formes

$$8x+3,\quad 8x+5.$$

Le deuxième théorème entraine immédiatement la proposition suivante :

THÉORÈME III. — n *étant un nombre impair, et* ρ *une des racines primitives de l'équation* (1), *soient*

$$h,\ h',\ h'',\ \ldots \quad \text{et} \quad k,\ k',\ k'',\ \ldots$$

les deux groupes d'exposants de ρ *dans une somme alternée* $\mathfrak{S}$ *de ces racines, qui offre pour carré* $\pm n$. *Si* n *est de la forme*

$$8x+1 \quad \text{ou} \quad 8x+7,$$

le groupe des exposants

$$h,\quad h',\quad h'',\quad \ldots$$

pourra être remplacé, dans la somme alternée $\mathfrak{S}$, *par le groupe des exposants*

$$2h,\quad 2h',\quad 2h'',\quad \ldots,$$

qui seront, à l'ordre près, équivalents aux premiers suivant le module n, et le groupe des exposants

$$k,\quad k',\quad k'',\quad \ldots$$

par le groupe des exposants

$$2k,\quad 2k',\quad 2k'',\quad \ldots.$$

Si, au contraire, n est de l'une des formes

$$8x+3,\quad 8x+5,$$

le groupe des exposants

$$h,\quad h',\quad h'',\quad \ldots$$

pourra être remplacé par le groupe des exposants

$$2k,\quad 2k',\quad 2k'',\quad \ldots,$$

et le groupe des exposants

$$k,\quad k',\quad k'',\quad \ldots$$

par le groupe des exposants

$$2h,\quad 2h',\quad 2h'',\quad \ldots.$$

Supposons maintenant que, l'équation

$$\mathfrak{S}^2=\pm n$$

étant vérifiée, n représente, non plus un nombre impair, mais un nombre pair. Alors n sera de l'une des formes

$$4\nu'\nu''\ldots,\quad 8\nu'\nu''\ldots,$$

ν', ν'', ... étant des facteurs impairs inégaux. Or, si l'on suppose

d'abord

$$n=4\nu'\nu''\ldots,$$

un nombre l inférieur à n, mais premier à n, fera partie du premier groupe

$$h,\quad h',\quad h'',\quad \ldots,$$

si ce nombre l, pris pour h, vérifie les conditions (7) ou (8), et n'en fera pas partie dans le cas contraire. Par suite, deux nombres impairs

$$l,\quad l',$$

inférieurs à n, mais premiers à n, appartiendront l'un au premier groupe, l'autre au second groupe, si ces nombres vérifient la condition

$$\left[\frac{l'}{\frac{1}{4}n}\right]=\left[\frac{l}{\frac{1}{4}n}\right],\tag{26}$$

sans vérifier la suivante :

$$l'\equiv l \pmod 4;$$

en sorte que l'on ait, non pas

$$l'-l\equiv 0 \pmod 4,$$

mais, au contraire,

$$l'-l\equiv 2 \pmod 4.\tag{27}$$

Or, les conditions (26), (27) seront évidemment vérifiées si, l étant inférieur à $\frac{n}{2}$, on pose

$$l'=l+\frac{n}{2},\tag{28}$$

puisque alors on aura

$$l'-l=\frac{n}{2}=2\nu'\nu''\ldots\equiv 2 \pmod 4.$$

Supposons maintenant

$$n=8\nu'\nu''\ldots,$$

ν', ν'', ... étant toujours des facteurs impairs inégaux, et la valeur de

Θ^2 étant $\pm n$. En vertu des conditions (9) ou (10), (11) ou (12), deux nombres impairs

$$l, \quad l'$$

inférieurs à n, mais premiers à n, appartiendront nécessairement, l'un au premier groupe, l'autre au second groupe, si ces nombres vérifient les deux conditions

$$\left[\frac{l'}{\frac{1}{8}n}\right] = \left[\frac{l}{\frac{1}{8}n}\right], \tag{29}$$

$$l' - l \equiv 4 \pmod 8. \tag{30}$$

Or, c'est précisément ce qui arrivera, si, l étant inférieur à $\frac{n}{2}$, on suppose la valeur de l' déterminée par l'équation (28), puisque alors on aura

$$l' - l - \frac{n}{2} = 4\nu'\nu'' \ldots \equiv 4 \pmod 8.$$

Observons maintenant que la formule (28) entraîne immédiatement la suivante :

$$2l' \equiv 2l \pmod n. \tag{31}$$

Donc, lorsque, n étant pair, le carré de Θ sera $\pm n$, on pourra, aux termes du premier groupe

$$h, \quad h', \quad h'', \quad \ldots,$$

faire correspondre les termes du second groupe

$$k, \quad k', \quad k'', \quad \ldots,$$

de manière que l'on ait, par exemple,

$$2h \equiv 2k, \quad 2h' \equiv 2k', \quad 2h'' \equiv 2k'', \quad \ldots \pmod n.$$

En conséquence, on peut énoncer la proposition suivante :

THÉORÈME IV. — *n étant un nombre pair, et ρ une des racines primitives de l'équation* (1), *soient*

$$h, \quad h', \quad h'', \quad \ldots \quad \text{et} \quad k, \quad k', \quad k'', \quad \ldots$$

les deux groupes d'exposants de ρ, dans une somme alternée Θ de ces racines, qui offrent pour carré $\pm n$. Les nombres

$$2h, \quad 2h', \quad 2h'', \quad \ldots$$

seront équivalents, à l'ordre près, suivant le module n, aux nombres

$$2k, \quad 2k', \quad 2k'', \quad \ldots.$$

Le nombre total des entiers

$$h, \quad k, \quad l, \quad \ldots$$

inférieurs à n, mais premiers à n, étant représenté par N, et la somme alternée Θ renfermant toujours autant de termes positifs que de termes négatifs, il est clair que dans chacun des groupes

$$h, \quad h', \quad h'', \quad \ldots \quad \text{et} \quad k, \quad k', \quad k'', \quad \ldots$$

le nombre des termes doit être égal à $\frac{N}{2}$. Cela posé, l'unité étant censée faire partie du premier groupe

$$h, \quad h', \quad h'', \quad \ldots,$$

nommons i le nombre des termes qui, dans ce groupe, sont inférieurs à $\frac{n}{2}$, et j le nombre de ceux qui surpassent $\frac{n}{2}$. On aura

$$i + j = \frac{N}{2}. \tag{32}$$

D'autre part, l étant un entier inférieur à $\frac{n}{2}$, mais premier à l,

$$n - l$$

sera un autre entier supérieur à $\frac{n}{2}$, mais inférieur à n, et premier à n. Donc, les entiers inférieurs à n, mais premiers à n, se correspondront deux à deux, au-dessus et au-dessous de $\frac{n}{2}$, le nombre des uns et des autres étant encore $\frac{N}{2}$. Donc, ceux qui feront partie du second groupe seront, au-dessous de $\frac{n}{2}$, en nombre égal à

$$\frac{N}{2} - i = j,$$

et au-dessus de $\frac{n}{2}$, en nombre égal à

$$\frac{N}{2} - j = i.$$

Il y a plus : deux termes correspondants, c'est-à-dire de la forme

$$t, \quad n - t,$$

seront, en vertu du théorème I, deux termes qui feront partie d'un même groupe, si la somme alternée $\mathfrak{D}$ vérifie la condition

$$\mathfrak{D}^2 = n.$$

Donc, alors, à l'équation (32) on pourra joindre celle-ci

$$i = j, \tag{33}$$

et l'on aura, par suite,

$$i = j = \frac{N}{4}. \tag{34}$$

On peut donc énoncer la proposition suivante :

THÉORÈME V. — *Le nombre n étant tel que la somme alternée $\mathfrak{D}$, déterminée par l'équation* (2), *vérifie la condition*

$$\mathfrak{D}^2 = n,$$

chacun des groupes d'exposants

$$k, \quad k', \quad k'', \quad \ldots \qquad \text{et} \qquad k, \quad k', \quad k'', \quad \ldots$$

offrira autant de termes inférieurs à $\frac{n}{2}$ que de termes supérieurs à $\frac{n}{2}$, le nombre des termes de chaque groupe, inférieurs à $\frac{1}{2}$, étant $\frac{N}{4}$.

En terminant cette Note, nous joindrons ici quelques observations qui ne sont pas sans intérêt.

Si, dans le cas où n représente une puissance d'un nombre premier impair, et l un entier premier à n, on désigne par

$$\left[\frac{l}{n}\right],$$

comme nous l'avons fait dans la Note précédente, le reste $+1$ ou -1, qu'on obtient en divisant par n le nombre entier

$$l^{\frac{N}{2}},$$

alors on devra, dans les formules (20) et (21), supposer, ainsi que nous l'avons admis, le nombre n non seulement impair, mais composé de facteurs inégaux. Car, si l'on supposait, par exemple,

$$n = 9 = 3^2,$$

on trouverait

$$N = 2.3, \qquad \frac{N}{2} = 3,$$

et les expressions

$$\left[\frac{-1}{n}\right] = (-1)^3 = -1, \qquad \left[\frac{2}{n}\right] \equiv 2^3 \equiv -1 \pmod 9$$

cesseraient d'être égales aux quantités

$$(-1)^{\frac{n-1}{2}} = (-1)^4 = 1, \qquad (-1)^{\frac{n^2-1}{8}} = (-1)^{10} = 1.$$

Toutefois les formules (20), (21) continueraient d'être vérifiées, si, dans le cas où n représente une puissance ν^a d'un nombre ν premier et impair, on désignait, avec M. Jacobi, par la notation

$$\left[\frac{l}{n}\right],$$

non plus le reste $+1$ ou -1, qu'on obtient en divisant par n le nombre

$$l^{\frac{N}{2}},$$

mais l'expression

$$\left[\frac{l}{\nu}\right]^a.$$

Alors aussi l'on pourrait étendre à des nombres impairs quelconques la loi de réciprocité qui existe entre deux nombres premiers impairs; en sorte qu'on aurait généralement, pour des valeurs impaires des

nombres entiers m et n,

$$\left[\frac{m}{n}\right] = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left[\frac{n}{m}\right]. \tag{35}$$

NOTE X.

SUR LES FONCTIONS RÉCIPROQUES ET SUR LES MOYENS QU'ELLES FOURNISSENT D'ÉVALUER LES SOMMES ALTERNÉES DES RACINES PRIMITIVES D'UNE ÉQUATION BINOME.

$f(x)$ étant une fonction donnée de la variable x, on a généralement, pour une valeur de x, renfermée entre les limites x_0, X (*voir* le IX^e Cahier du *Journal de l'École Polytechnique*, et le Tome II des *Exercices de Mathématiques*, p. 118),

$$f(x) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{x_0}^{X} e^{r(x-u)\sqrt{-1}} f(u)\,du\,dr,$$

ou, ce qui revient au même,

$$f(x) = \frac{1}{\pi}\int_{0}^{\infty}\int_{x_0}^{X} \cos r(x-u)\, f(u)\,du\,dr; \tag{1}$$

et pour une valeur de x, située hors des limites x_0, X,

$$0 = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{x_0}^{X} e^{r(x-u)\sqrt{-1}} f(u)\,du\,dr,$$

ou, ce qui revient au même,

$$0 = \frac{1}{\pi}\int_{0}^{\infty}\int_{x_0}^{X} \cos r(x-u)\, f(u)\,du\,dr. \tag{2}$$

Ainsi, en particulier, si l'on suppose

$$x_0 = 0, \qquad X = \infty,$$

la formule (1) donnera, pour des valeurs positives de x,

$$f(x) = \frac{1}{\pi}\int_{0}^{\infty}\int_{0}^{\infty} \cos r(x-u)\, f(u)\,du\,dr; \tag{3}$$

mais on conclura de la formule (2), en y remplaçant x par $-x$,

$$0 = \frac{1}{\pi}\int_{0}^{\infty}\int_{0}^{\infty} \cos r(x-u)\, f(u)\,du\,dr. \tag{4}$$

Comme on aura, d'ailleurs,

$$\cos r(x+u) = \cos rx\cos ru - \sin rx\sin ru,$$
$$\cos r(x-u) = \cos rx\cos ru + \sin rx\sin ru,$$

on tirera des équations (3) et (4)

$$f(x) = \frac{2}{\pi}\int_{0}^{\infty}\int_{0}^{\infty} \cos rx\cos ru\, f(u)\,du\,dr, \tag{5}$$

$$f(x) = \frac{2}{\pi}\int_{0}^{\infty}\int_{0}^{\infty} \sin rx\sin ru\, f(u)\,du\,dr. \tag{6}$$

De ces dernières formules, données pour la première fois par M. Fourier, il résulte que, si l'on suppose

$$\varphi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_{0}^{\infty} \cos rx\, f(r)\,dr, \tag{7}$$

on aura réciproquement

$$f(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_{0}^{\infty} \cos rx\,\varphi(r)\,dr, \tag{8}$$

et que, si l'on suppose

$$\psi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_{0}^{\infty} \sin rx\, f(x)\,dr, \tag{9}$$

on aura réciproquement

$$f(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_{0}^{\infty} \sin rx\,\psi(r)\,dr. \tag{10}$$

On voit donc ici se manifester une loi de réciprocité : 1°. entre les fonctions f et φ; 2°. entre les fonctions f et ψ, de telle sorte, que chacune des équations (7), (9) subsiste, pour des valeurs positives

de x, quand on échange entre elles les fonctions f et φ, ou f et ψ. C'est pour cette raison que, dans le *Bulletin de la Société philomatique* d'août 1817, j'ai désigné les fonctions

$$f(x), \quad \varphi(x)$$

sous le nom de *fonctions réciproques de première espèce*, et les fonctions

$$f(x), \quad \psi(x)$$

sous le nom de *fonctions réciproques de seconde espèce*. Ces deux espèces de fonctions peuvent être, ainsi que les formules citées de M. Fourier, employées avec avantage dans la solution d'un grand nombre de problèmes, et jouissent de propriétés importantes, dont je rappellerai quelques-unes en peu de mots.

D'abord, puisqu'on a généralement, pour des valeurs positives de ω,

$$\int_0^\infty e^{-\omega r}\cos rx\,dr = \frac{\omega}{\omega^2+x^2}, \qquad \int_0^\infty e^{-\omega r}\sin rx\,dr = \frac{x}{\omega^2+x^2},$$

il en résulte que la fonction

$$f(x) = e^{-\omega x}$$

a pour réciproque de première espèce

$$\varphi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \frac{\omega}{\omega^2+x^2},$$

et pour réciproque de seconde espèce

$$\psi(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \frac{x}{\omega^2+x^2}.$$

On a donc, par suite,

$$(11) \qquad \int_0^\infty \frac{\omega}{\omega^2+r^2}\cos rx\,dr = \frac{\pi}{2}e^{-\omega}, \qquad \int_0^\infty \frac{r}{\omega^2+r^2}\sin rx\,dr = \frac{\pi}{2}e^{-\omega}.$$

On se trouve ainsi ramené à deux formules données par M. Laplace.

Lorsque, dans la dernière de ces formules, on pose $\omega = 0$, on retrouve la formule connue

$$(12) \qquad \int_0^\infty \frac{\sin rx}{r}\,dr = \frac{\pi}{2},$$

qui subsiste seulement pour des valeurs positives de la variable x.

Il résulte encore de la formule connue

$$(13) \qquad \int_0^\infty e^{-\frac{r^2}{2}}\cos rx\,dr = \frac{\pi}{2}e^{-\frac{x^2}{2}},$$

que la fonction

$$e^{-\frac{x^2}{2}}$$

se confond avec sa réciproque de première espèce.

Soient maintenant z une variable, dont le module reste inférieur à l'unité, et a une quantité positive. Si la série

$$f(0), \quad z\,f(a), \quad z^2 f(2a), \quad \ldots$$

est convergente, on tirera des formules (8) et (10)

$$(14) \quad f(0) + z\,f(a) + z^2 f(2a) + \ldots = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_0^\infty \frac{1 - z\cos ar}{1 - 2z\cos ar + z^2}\varphi(r)\,dr$$

et

$$(15) \qquad z\,f(a) + z^2 f(2a) + \ldots = \left(\frac{2}{\pi}\right)^{\frac{1}{2}} \int_0^\infty \frac{z\sin ar}{1 - 2z\cos ar + z^2}\psi(r)\,dr.$$

Si, d'ailleurs, on fait converger z vers la limite 1, le rapport

$$\frac{1 - z\cos ar}{1 - 2z\cos ar + z^2}$$

s'approchera indéfiniment de la limite $\frac{1}{2}$, à moins que l'on attribue à r des valeurs peu différentes de celles qui vérifient l'équation

$$\cos ar = 1.$$

Or, les racines positives de cette équation seront de la forme

$$r = nb,$$

n étant un nombre entier, et b une constante positive liée à la constante a par la formule

$$ab = 2\pi. \tag{16}$$

Cela posé, on reconnaîtra sans peine [*voir* le 2ᵉ Volume des *Exercices de Mathématiques*, p. 148 et suivantes (¹)] que, si ε s'approche indéfiniment de la limite 1, l'intégrale renfermée dans le second membre de la formule (14) aura pour limite, non pas l'expression

$$\int_0^\infty \frac{1}{2}\varphi(r)\,dr = \frac{1}{2}\left(\frac{\pi}{2}\right)^{\frac{1}{2}} f(0),$$

comme on pourrait le croire au premier abord, mais cette expression augmentée de certaines intégrales singulières dont la somme sera

$$\frac{\pi}{a}\left[\frac{1}{2}\varphi(0) + \varphi(b) + \varphi(2b) + \dots\right].$$

En conséquence, on trouvera

$$\frac{1}{2}f(0) + f(a) + f(2a) + \dots = \left(\frac{2\pi}{a}\right)^{\frac{1}{2}}\left[\frac{1}{2}\varphi(0) + \varphi(b) + \varphi(2b) + \dots\right], \tag{17}$$

ou, ce qui revient au même,

$$a^{\frac{1}{2}}\left[\frac{1}{2}f(0) + f(a) + f(2a) + \dots\right] = b^{\frac{1}{2}}\left[\frac{1}{2}\varphi(0) + \varphi(b) + \varphi(2b) + \dots\right]. \tag{18}$$

Ainsi, lorsque la série

$$f(0),\quad f(a),\quad f(2a),\quad \dots$$

est convergente, l'équation (18) subsiste entre les fonctions réciproques de première espèce désignées par les lettres f et φ, pourvu que les nombres a, b vérifient la condition (16).

Il importe d'observer que la série

$$\varphi(0),\quad \varphi(b),\quad \varphi(2b),\quad \dots$$

peut quelquefois se réduire à un nombre fini de termes, et qu'alors

(¹) *OEuvres de Cauchy*, S. II, t. VI.

l'équation (17) fournit immédiatement la somme de la série

$$f(0),\quad f(a),\quad f(2a),\quad \dots$$

C'est ce que nous allons montrer par un exemple.

Comme on a généralement

$$\sin\omega r\cos rx = \frac{\sin r(\omega + x) + \sin r(\omega - x)}{2},$$

on en conclura, eu égard à la formule (12),

$$\int_0^\infty \frac{\sin\omega r}{r}\cos rx\,dr = \frac{\pi}{2} \tag{19}$$

ou

$$\int_0^\infty \frac{\sin\omega r}{r}\cos rx\,dr = 0, \tag{20}$$

suivant que x sera inférieur ou supérieur à ω. Donc, si l'on pose

$$f(x) = \frac{\sin\omega x}{x},$$

on aura

$$\varphi(x) = \left(\frac{\pi}{2}\right)^{\frac{1}{2}} \quad \text{ou} \quad \varphi(x) = 0,$$

suivant que la valeur de x sera inférieure ou supérieure à la constante positive ω; et alors, pour réduire l'équation (17) à la formule

$$\frac{1}{2}f(0) + f(a) + f(2a) + \dots = \left(\frac{\pi}{2}\right)^{\frac{1}{2}}\frac{\varphi(0)}{a},$$

par conséquent à la formule

$$\frac{1}{2}a\omega + \sin a\omega + \frac{\sin 2a\omega}{2} + \frac{\sin 3a\omega}{3} + \dots = \frac{\pi}{2}, \tag{21}$$

il suffira de choisir la constante a, de manière à vérifier la condition

$$\omega < b$$

ou

$$a\omega < 2\pi.$$

La formule (21) était déjà connue. Lorsqu'on y pose $a = 1$, elle donne,

pour des valeurs de ω, renfermées entre les limites $0, 2\pi$,

$$\frac{1}{2}\omega + \sin\omega + \frac{\sin 2\omega}{2} + \frac{\sin 3\omega}{3} + \ldots = \frac{\pi}{2}. \tag{22}$$

Si, dans la formule (18), on pose

$$f(x) = e^{-\frac{x^2}{2}},$$

elle donnera

$$a^{\frac{1}{2}}\left(\frac{1}{2} + e^{-\frac{a^2}{2}} + e^{-4\frac{a^2}{2}} + \ldots\right) = b^{\frac{1}{2}}\left(\frac{1}{2} + e^{-\frac{b^2}{2}} + e^{-4\frac{b^2}{2}} + \ldots\right), \tag{23}$$

les nombres a, b étant toujours assujettis à la condition

$$ab = 2\pi.$$

Si, dans l'équation (23), on remplace a^2 par $2a^2$, et b^2 par $2b^2$, on en conclura

$$a^{\frac{1}{2}}\left(\frac{1}{2} + e^{-a^2} + e^{-4a^2} + e^{-9a^2} + \ldots\right) = b^{\frac{1}{2}}\left(\frac{1}{2} + e^{-b^2} + e^{-4b^2} + e^{-9b^2} + \ldots\right), \tag{24}$$

les nombres a, b étant maintenant assujettis à vérifier la condition

$$ab = \pi. \tag{25}$$

J'ai signalé les formules (18) et (24), avec la méthode par laquelle je viens de les reproduire, dans le *Bulletin de la Société philomatique* de 1817 (1), et j'ai développé cette méthode dans les leçons données la même année au Collège de France. La relation établie par la formule (24) entre les termes des deux séries

$$1,\quad e^{-a^2},\quad e^{-4a^2},\quad e^{-9a^2},\quad \ldots, \tag{26}$$

$$1,\quad e^{-b^2},\quad e^{-4b^2},\quad e^{-9b^2},\quad \ldots \tag{27}$$

parut digne d'attention à l'auteur de la *Mécanique céleste*, qui me dit l'avoir vérifiée dans le cas où l'un des nombres a, b devient très petit. Effectivement la formule (24), que l'on peut écrire comme il suit,

$$a\left(\frac{1}{2} + e^{-a^2} + e^{-4a^2} + \ldots\right) = \pi^{\frac{1}{2}}\left(\frac{1}{2} + e^{-\frac{\pi^2}{a^2}} + e^{-4\frac{\pi^2}{a^2}} + \ldots\right), \tag{28}$$

(1) *Œuvres de Cauchy*, S. II, t. II.

donnera sensiblement, si a se réduit à un très petit nombre α,

$$\alpha\left(\frac{1}{2} + e^{-\alpha^2} + e^{-4\alpha^2} + \ldots\right) = \frac{1}{2}\pi^{\frac{1}{2}};$$

et, pour vérifier cette dernière équation, il suffit d'observer que, d'après la définition des intégrales définies, le produit

$$\alpha(1 + e^{-\alpha^2} + e^{-4\alpha^2} + \ldots)$$

a pour limite

$$\int_0^\infty e^{-x^2}\,dx = \frac{1}{2}\pi^{\frac{1}{2}}. \tag{29}$$

La formule (18), avec la démonstration que nous en avons donnée, peut être étendue, ainsi que la formule (24), à des valeurs imaginaires de a, renfermées entre certaines limites. Ainsi, en particulier, la formule (24) continue de subsister, comme l'a dit M. Poisson, quand on y remplace a^2 par $a^2\sqrt{-1}$. Elle subsiste même généralement, quand on prend pour a^2 une expression imaginaire, pourvu que les parties réelles de a et de b soient nulles ou positives; et l'on peut retrouver aussi une autre formule, déduite par M. Poisson de l'équation (18), dans un Mémoire sur le calcul numérique des intégrales définies. J'ajouterai que, pour arriver au cas où la partie réelle de a s'évanouit, il convient d'examiner d'abord celui où la même partie réelle est infiniment petite, mais positive; et qu'en opérant de cette manière, on peut, de la formule (24), déduire la somme de certaines puissances d'une racine de l'équation binome

$$x^n = 1, \tag{30}$$

n étant un nombre entier quelconque; savoir : la somme des puissances qui ont pour exposants les carrés des nombres entiers inférieurs à n. C'est ce que nous allons expliquer plus en détail.

Nommons ρ une racine primitive de l'équation (30). On pourra supposer

$$\rho = e^{\omega\sqrt{-1}}, \tag{31}$$

la valeur de ω étant

$$\omega = \frac{2\pi}{n}, \tag{32}$$

et alors les diverses racines de l'équation (30) pourront être représentées par celles des puissances de ρ, qui offriront des valeurs distinctes; par exemple, par les termes de la progression géométrique

$$1 = \rho^0,\ \rho^1,\ \rho^2,\ \rho^3,\ \ldots,\ \rho^{n-1}. \tag{33}$$

Si, dans cette même progression, l'on remplace les exposants

$$0,\ 1,\ 2,\ 3,\ \ldots,\ n-1$$

par leurs carrés

$$0,\ 1,\ 4,\ 9,\ \ldots\ (n-1)^2,$$

on obtiendra une nouvelle suite ; savoir :

$$1,\ \rho,\ \rho^4,\ \rho^9,\ \ldots,\ \rho^{(n-1)^2}, \tag{34}$$

et, si l'on nomme Ω la somme des termes de cette nouvelle suite, on aura

$$\Omega = 1 + \rho + \rho^4 + \rho^9 + \ldots + \rho^{(n-1)^2}, \tag{35}$$

ou, ce qui revient au même,

$$\Omega = 1 + e^{\omega\sqrt{-1}} + e^{4\omega\sqrt{-1}} + \ldots + e^{(n-1)^2\omega\sqrt{-1}}. \tag{36}$$

Cela posé, Ω sera évidemment ce que devient la somme des n premiers termes de la série (26), quand on y remplace α^2 par $-\omega\sqrt{-1}$, c'est-à-dire, lorsqu'on prend

$$\alpha^2 = -\frac{2\pi}{n}\sqrt{-1}. \tag{37}$$

Or, dans ce cas, la formule (25), ou

$$\alpha^2 b^2 = \pi^2,$$

donnera

$$b^2 = \frac{n\pi}{2}\sqrt{-1}; \tag{38}$$

et, en adoptant cette valeur de b^2, on verra les termes distincts de la série (27) se réduire aux deux premiers, c'est-à-dire, aux deux termes du binome

$$1 + e^{-b^2} = 1 + e^{-\frac{n\pi}{2}\sqrt{-1}}.$$

On doit donc s'attendre à voir l'équation (24) fournir une relation entre la somme représentée par Ω et le binome dont il s'agit. Or, effectivement, pour obtenir cette relation, il suffira de supposer, dans l'équation (24),

$$a^2 = \alpha^2 - \frac{2\pi}{n}\sqrt{-1} = \alpha^2 - \omega\sqrt{-1}, \tag{39}$$

α^2 désignant un nombre infiniment petit. Dans cette supposition, a^2 différant très peu de $-\frac{2\pi}{n}\sqrt{-1}$, b^2 devra très peu différer de $\frac{n\pi}{2}\sqrt{-1}$. Donc, si l'on pose

$$b^2 = 6^2 + \frac{n\pi}{2}\sqrt{-1}, \tag{40}$$

6^2 s'évanouira en même temps que α^2 ; et, comme la condition (25) donnera

$$\alpha^2 6^2 + \left(\frac{n}{2}\alpha^2 - \frac{2}{n}6^2\right)\pi\sqrt{-1} = 0,$$

ou, ce qui revient au même,

$$\frac{4\,6^2}{n^2\alpha^2} = \left(1 + \frac{n}{2\pi}\alpha^2\sqrt{-1}\right)^{-1},$$

on en conclura sensiblement

$$\frac{4\,6^2}{n^2\alpha^2} = 1, \qquad \frac{2\,6}{n\alpha} = 1. \tag{41}$$

Concevons maintenant que l'on multiplie par $n\alpha$ et par $2\,6$ les sommes des séries (26) et (27), en ayant égard aux formules (39), (40), et

supposant $\alpha, \mathcal{E}$ infiniment petits. Comme chacun des produits

$$n\alpha\left(\frac{1}{2}+e^{-n^2\alpha^2}+e^{-4n^2\alpha^2}+\ldots\right),$$
$$n\alpha\left[e^{-\alpha^2}+e^{-(n+1)^2\alpha^2}+\ldots\right],$$
$$n\alpha\left[e^{-(n-1)^2\alpha^2}+e^{-(2n-1)^2\alpha^2}+\ldots\right],$$
$$2\mathcal{E}\left(\frac{1}{2}+e^{-4\beta^2}+e^{-16\beta^2}+\ldots\right),$$
$$2\mathcal{E}\left[e^{-\beta^2}+e^{-9\beta^2}+\ldots\right]$$

se réduira sensiblement à l'intégrale définie

$$\int_0^\infty e^{-x^2}dx=\frac{1}{2}\pi^{\frac{1}{2}},$$

on trouvera, sans erreur sensible, non seulement

$$n\alpha\left(\frac{1}{2}+e^{-n^2}+e^{-4n^2}+\ldots\right)=\frac{1}{2}\pi^{\frac{1}{2}}\left(1+e^{n\alpha\sqrt{-1}}+\ldots+e^{(n-1)^2\alpha\sqrt{-1}}\right),$$

ou, ce qui revient au même,

$$n\alpha\left(\frac{1}{2}+e^{-n^2}+e^{-4n^2}+\ldots\right)=\frac{1}{2}\pi^{\frac{1}{2}}\Omega,$$

mais encore

$$2\mathcal{E}\left(\frac{1}{2}+e^{-b^2}+e^{-4b^2}+\ldots\right)=\frac{1}{2}\pi^{\frac{1}{2}}\left(1+e^{-\frac{n\pi}{2}\sqrt{-1}}\right),$$

puis, on conclura, eu égard à la seconde des formules (41),

$$\frac{\frac{1}{2}+e^{-a^2}+e^{-4a^2}+e^{-9a^2}+\ldots}{\frac{1}{2}+e^{-b^2}+e^{-4b^2}+e^{-9b^2}+\ldots}=\frac{\Omega}{1+e^{-\frac{n\pi}{2}\sqrt{-1}}}. \tag{42}$$

D'ailleurs, en vertu de la formule (24) ou (28), le premier membre de l'équation (42) sera équivalent au rapport

$$\frac{\pi^{\frac{1}{2}}}{a}.$$

Donc, en supposant que les valeurs de a^2, b^2 déterminées par les formules (37), (38), c'est-à-dire, en faisant évanouir α et $\mathcal{E}$, dans les

formules (39), (40), on trouvera

$$\frac{\Omega}{1+e^{-\frac{n\pi}{2}\sqrt{-1}}}=\frac{\pi^{\frac{1}{2}}}{a},$$

ou, ce qui revient au même,

$$\Omega=\frac{\pi^{\frac{1}{2}}}{a}\left(1+e^{-\frac{n\pi}{2}\sqrt{-1}}\right). \tag{43}$$

Mais alors de l'équation (37) présentée sous la forme

$$a^2=\frac{2\pi}{n}e^{-\frac{\pi}{2}\sqrt{-1}},$$

on tirera (voir l'*Analyse algébrique*, Chap. VII et IX) (1)

$$a=\left(\frac{2\pi}{n}\right)^{\frac{1}{2}}e^{-\frac{\pi}{4}\sqrt{-1}},\qquad \frac{\pi^{\frac{1}{2}}}{a}=\left(\frac{n}{2}\right)^{\frac{1}{2}}e^{\frac{\pi}{4}\sqrt{-1}}=\frac{n^{\frac{1}{2}}}{2}\left(1+\sqrt{-1}\right).$$

Donc la formule (43) donnera

$$\Omega=\frac{n^{\frac{1}{2}}}{2}\left(1+\sqrt{-1}\right)\left(1+e^{-\frac{n\pi}{2}\sqrt{-1}}\right). \tag{44}$$

En conséquence, l'on aura : 1° si n est de la forme $4x$,

$$\Omega=n^{\frac{1}{2}}\left(1+\sqrt{-1}\right); \tag{45}$$

2° si n est de la forme $4x+1$,

$$\Omega=n^{\frac{1}{2}}; \tag{46}$$

3° si n est de la forme $4x+2$,

$$\Omega=0; \tag{47}$$

4° si n est de la forme $4x+3$,

$$\Omega=n^{\frac{1}{2}}\sqrt{-1}. \tag{48}$$

Ainsi les formules (44), (45), (46), (47), (48) que M. Gauss a établies dans l'un de ses plus beaux Mémoires, et dont M. Dirichlet a

(1) *Œuvres de Cauchy*, S. II, t. III.

donné une démonstration nouvelle en 1835, se trouvent comprises, comme cas particuliers, dans l'équation (24) de laquelle on déduit immédiatement la formule (44), en attribuant à l'exposant $-a^2$ une valeur infiniment rapprochée de la valeur imaginaire $\frac{2\pi}{n}\sqrt{-1}$, ou, ce qui revient au même, en réduisant l'exponentielle e^{-a^2} à une racine primitive ρ de l'équation (30).

Il est important d'observer que, dans les équations précédentes, la valeur de Ω, déterminée par la formule (35), peut encore s'écrire comme il suit

$$\Omega = 1 + 2\left(\rho^1 + \rho^4 + \rho^9 + \ldots + \rho^{\left(\frac{n-1}{2}\right)^2}\right), \tag{49}$$

puisque, l étant un entier quelconque inférieur à $\frac{1}{2}n$, on aura généralement

$$(n-l)^2 \equiv l^2 \pmod{n}.$$

Nous avons supposé, dans ce qui précède, la valeur de ρ déterminée par la formule (31). Pour savoir ce qui arriverait dans la supposition contraire, il convient d'examiner d'abord séparément le cas où n est un nombre premier impair. Dans ce cas, si l'on nomme

$$h,\ h',\ h'',\ \ldots$$

les résidus, et

$$k,\ k',\ k'',\ \ldots,$$

les non-résidus, inférieurs à n, les termes de la série

$$\rho^h,\ \rho^{h'},\ \rho^{h''},\ \ldots$$

se confondront, à l'ordre près, avec les termes de la série

$$\rho,\ \rho^4,\ \rho^9,\ \ldots,\ \rho^{\left(\frac{n-1}{2}\right)^2};$$

et, par suite, on aura non seulement

$$1 + \rho^h + \rho^{h'} + \rho^{h''} + \ldots + \rho^k + \rho^{k'} + \rho^{k''} + \ldots = 1 + \rho + \rho^2 + \ldots + \rho^{n-1} = 0,$$

ou, ce qui revient au même,

$$1 + \rho^h + \rho^{h'} + \rho^{h''} + \ldots = -\rho^k - \rho^{k'} - \rho^{k''} - \ldots,$$

mais encore

$$\rho + \rho^4 + \ldots + \rho^{\left(\frac{n-1}{2}\right)^2} = \rho^h + \rho^{h'} + \rho^{h''} + \ldots.$$

Cela posé, la valeur de Ω, donnée par la formule (49), deviendra

$$\Omega = 1 + 2(\rho^h + \rho^{h'} + \rho^{h''} + \ldots), \tag{50}$$

ou même

$$\Omega = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots. \tag{51}$$

D'ailleurs, le second membre de la formule (51) est une fonction alternée des racines primitives de l'équation (30), et si, dans cette fonction, l'on remplace ρ par ρ^m, m étant premier à n, elle changera ou ne changera pas de signe, en conservant, au signe près, la même valeur, suivant que m sera ou ne sera pas résidu quadratique (p. 232). Donc, si n est un nombre premier impair, la valeur de Ω déterminée par la formule (35) ou (49) ne sera autre chose qu'une fonction alternée des racines primitives de l'équation (30); et la substitution de ρ^m à ρ, dans cette fonction, n'aura d'autre effet que de faire varier la valeur de Ω dans le rapport de 1 à $\left[\frac{m}{n}\right]$. Donc, puisqu'en supposant

$$\rho = e^{\omega\sqrt{-1}},$$

on a, en vertu de la formule (46) ou (48),

$$\Omega = n^{\frac{1}{2}}(\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}, \tag{52}$$

si l'on suppose au contraire

$$\rho = e^{m\omega\sqrt{-1}}, \tag{53}$$

m étant premier à n, on trouvera

$$\Omega = \left[\frac{m}{n}\right] n^{\frac{1}{2}}(\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}. \tag{54}$$

Si m cessait d'être premier à n, c'est-à-dire, s'il était divisible par n, alors la formule (35) donnerait immédiatement

$$\Omega = n. \tag{55}$$

Supposons maintenant que n soit le carré d'un nombre premier ν, en sorte qu'on ait

$$n = \nu^2;$$

alors ces deux entiers

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

qui seront divisibles par ν, et dont le nombre sera ν, offriront des carrés divisibles par ν^2 ou n. Donc, dans le second membre de la formule (35), ν puissances de ρ, qui offriront ces carrés pour exposants, se réduiront chacune à l'unité. Si d'ailleurs on continue de nommer

$$h, \quad h', \quad h'', \quad \ldots$$

les résidus quadratiques inférieurs à n, on obtiendra, au lieu de la formule (30), la suivante :

$$\Omega = \nu + 2(\rho^h + \rho^{h'} + \rho^{h''} + \ldots). \tag{56}$$

Enfin, si ρ désigne une racine primitive de l'équation (30), et si, parmi les résidus quadratiques

$$h, \quad h', \quad h'', \quad \ldots,$$

relatifs au module

$$n = \nu^2,$$

on considère ceux qui sont équivalents à un même nombre, représentant un résidu quadratique relatif au module ν, ces résidus correspondront à des puissances de ρ, dont la somme sera nulle (p. 248-249). Il y a plus, pour que cette somme s'évanouisse, il ne sera pas nécessaire que ρ désigne une racine primitive de l'équation (30), mais seulement une racine distincte de l'unité. Donc par suite si, n étant le carré d'un nombre premier impair ν, ρ diffère de l'unité, la somme totale des diverses puissances de ρ, qui offriront pour exposants les divers résidus quadratiques, s'évanouira, en sorte que l'on aura

$$\rho^h + \rho^{h'} + \rho^{h''} + \ldots = 0,$$

et l'équation (56) donnera simplement

$$\Omega = \nu. \tag{57}$$

Si ρ se réduisait à l'unité, la même équation donnerait

$$\Omega = n,$$

et l'on se retrouverait ainsi ramené à l'équation (55). Au reste il est facile de reconnaître que l'équation (57) se trouve elle-même comprise, comme cas particulier, dans la formule (54), lorsqu'on attribue généralement à la notation $\left[\frac{m}{n}\right]$ le sens que lui donne M. Jacobi, et que l'on pose en conséquence

$$\left[\frac{m}{\nu^2}\right] = \left[\frac{m}{\nu}\right]^2 = 1.$$

Supposons enfin que n soit une puissance entière d'un nombre premier et impair ν, en sorte qu'on ait

$$n = \nu^a.$$

Alors, par des raisonnements semblables à ceux qui précèdent, l'on prouvera encore que l'équation (54) subsiste, pour des valeurs de m premières à n, pourvu que l'on pose généralement avec M. Jacobi

$$\left[\frac{m}{\nu^a}\right] = \left[\frac{m}{\nu}\right]^a.$$

Effectivement, m étant premier à n, posons

$$\rho^{\nu^{a-1}} = \varsigma.$$

ς sera une racine primitive de l'équation

$$x^\nu = 1;$$

et l'on reconnaîtra sans peine : 1° que, dans le développement de Ω, la somme des puissances de ρ dont l'exposant est divisible par une puissance de ν d'un degré inférieur à $a-1$ s'évanouit ; 2° que la somme des autres termes se réduit, pour des valeurs paires de a, au nombre

$$\frac{a}{\nu^2} = n^{\frac{1}{2}},$$

et pour des valeurs impaires de a, au produit

$$\nu^{\frac{a-1}{2}}(1 + \varsigma^1 + \varsigma^4 + \ldots + \varsigma^{(\nu-1)^2}).$$

Or, comme on aura pour $\rho = e^{\omega\sqrt{-1}}$

$$\varsigma = e^{\frac{2\pi}{\nu}\sqrt{-1}},$$

et pour $\rho = e^{m\omega\sqrt{-1}}$

$$\varsigma = e^{\frac{2m\pi}{\nu}\sqrt{-1}},$$

il en résulte que la somme

$$1 + \varsigma + \varsigma^2 + \ldots + \varsigma^{(\nu-1)^2}$$

se réduira pour

$$\rho = e^{\omega\sqrt{-1}} \quad \text{à} \quad \nu^{\frac{1}{2}}(\sqrt{-1})^{\left(\frac{\nu-1}{2}\right)^2},$$

et pour

$$\rho = e^{m\omega\sqrt{-1}} \quad \text{à} \quad \left[\frac{m}{\nu}\right]\nu^{\frac{1}{2}}(\sqrt{-1})^{\left(\frac{\nu-1}{2}\right)^2}.$$

Donc, par suite, pour des valeurs impaires de a, le produit

$$\nu^{\frac{a-1}{2}}(1 + \varsigma^2 + \varsigma^4 + \ldots + \varsigma^{(\nu-1)^2})$$

se réduira, tant que m et n seront premiers entre eux, à l'expression

$$\left(\frac{m}{\nu}\right)\nu^{\frac{a}{2}}(\sqrt{-1})^{\left(\frac{\nu-1}{2}\right)^2},$$

qui ne différera pas de la suivante,

$$\left(\frac{m}{n}\right)n^{\frac{1}{2}}(\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2},$$

en sorte que la formule (54) se trouvera encore vérifiée. Par des raisonnements semblables, on déterminera généralement la valeur que prend Ω, lorsque, la valeur de n étant

$$n = \nu^a,$$

m cesse d'être premier à n ; et l'on reconnaîtra que, dans ce cas, Ω est le produit d'une certaine puissance de ν par la valeur de Ω qu'on aurait obtenue, si l'on eût substitué au module n le dénominateur de la fraction $\frac{m}{n}$ réduite à sa plus simple expression. Si l'on supposait $m = \nu^a$,

on trouverait

$$\rho = 1,$$

et la valeur de Ω serait précisément celle que fournit l'équation (55).

Il est facile de vérifier sur des exemples particuliers les principes généraux que nous venons d'établir. Ainsi l'on trouvera, pour $n = 3$,

$$\Omega = 1 + \rho + \rho^4 = 1 + 2\rho.$$

Donc alors, en supposant

$$\rho = e^{\omega\sqrt{-1}}, \qquad \omega = \frac{2\pi}{3},$$

ou, ce qui revient au même,

$$\rho = \cos\frac{2\pi}{3} + \sqrt{-1}\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{3^{\frac{1}{2}}}{2}\sqrt{-1},$$

on aura

$$\Omega = 3^{\frac{1}{2}}\sqrt{-1},$$

tandis qu'en posant successivement

$$\rho = e^{2\omega\sqrt{-1}} = -\frac{1}{2} - \frac{3^{\frac{1}{2}}}{2}\sqrt{-1}$$

et

$$\rho = 1,$$

on trouvera, dans le premier cas,

$$\Omega = -3^{\frac{1}{2}}\sqrt{-1} = \left[\frac{2}{3}\right]3^{\frac{1}{2}}\sqrt{-1},$$

et dans le second cas

$$\Omega = 3.$$

On trouvera de même, pour $n = 5$,

$$\Omega = 1 + \rho + \rho^4 + \rho^9 + \rho^{16} = 1 + 2\rho + 2\rho^4.$$

Donc alors, en supposant

$$\rho = e^{\frac{2\pi}{5}\sqrt{-1}} = \cos\frac{2\pi}{5} + \sqrt{-1}\sin\frac{2\pi}{5},$$

on aura

$$\Omega = 1 + 4\cos\frac{2\pi}{5} = 5^{\frac{1}{2}},$$

tandis qu'en posant successivement

$$\rho = e^{2\omega\sqrt{-1}}, \quad \rho = e^{3\omega\sqrt{-1}}, \quad \rho = e^{4\omega\sqrt{-1}}, \quad \rho = 1,$$

on trouvera, dans le premier et le second cas,

$$\rho = 1 + 4\cos\frac{4\pi}{5} = 1 + 4\cos\frac{6\pi}{5} = -5^{\frac{1}{2}},$$

ou, ce qui revient au même,

$$\rho = \left[\frac{2}{5}\right] 5^{\frac{1}{2}} = \left[\frac{3}{5}\right] 5^{\frac{1}{2}};$$

dans le troisième cas,

$$\rho = 1 + 4\cos\frac{8\pi}{5} = 1 + 4\cos\frac{2\pi}{5} = 5^{\frac{1}{2}},$$

ou, ce qui revient au même,

$$\rho = \left[\frac{4}{5}\right] 5^{\frac{1}{2}};$$

et dans le dernier cas,

$$\rho = 5.$$

De même on trouvera, pour $x = 9 = 3^2$,

$$\Omega = 1 + \rho + \rho^2 + \rho^3 + \ldots + \rho^{26} = 3 + 2(\rho + \rho^2 + \rho^7) = 3 + 2\rho\frac{\rho^9 - 1}{\rho^3 - 1} = 3;$$

et, par suite,

$$\Omega = 3 = 9^{\frac{1}{2}},$$

à moins que ρ ne se réduise à l'unité, et la valeur de Ω à celle que donne la formule

$$\Omega = 9.$$

Si au contraire l'on prend $x = 27 = 3^3$, on trouvera

$$\Omega = 1 + \rho + \rho^2 + \ldots + \rho^{26} = 3 + 6\rho^3 + 2\rho(1 + \rho^3 + \ldots + \rho^{24});$$

et, par suite, en supposant

$$\rho = e^{\omega\sqrt{-1}} = e^{\frac{2\pi}{27}\sqrt{-1}},$$

on aura

$$\Omega = 3(1 + 2\rho^3),$$

ou, ce qui revient au même,

$$\Omega = 3\left(1 + 2e^{\frac{2\pi}{3}\sqrt{-1}}\right) = 3.3^{\frac{1}{2}}\sqrt{-1} = 27^{\frac{1}{2}}\sqrt{-1},$$

tandis que, si l'on pose

$$\rho = e^{m\omega\sqrt{-1}},$$

m étant premier à 3, l'on trouvera

$$\Omega = 3^{\frac{1}{2}}\left(1 + 2\cos\frac{2m\pi}{3}\sqrt{-1}\right) = \left[\frac{m}{3}\right] 27^{\frac{1}{2}}\sqrt{-1},$$

ou, ce qui revient au même,

$$\Omega = \left[\frac{m}{27}\right] 27^{\frac{1}{2}}\sqrt{-1}.$$

Si m cessait d'être premier à 27, alors on trouverait : 1° en supposant m divisible une seule fois par 3,

$$\Omega = 3 + 6\rho^{27} = 9;$$

2° en supposant m divisible par $3^2 = 9$,

$$\Omega = 3 + 6 + 2.9 = 27.$$

Passons maintenant au cas où le module se réduit à 2 ou à une puissance de 2.

Lorsqu'on a précisément $n = 2$, l'équation

$$x^2 = 1$$

offre pour racines

$$-1, \quad +1;$$

et par suite la valeur de

$$\Omega = 1 + \rho$$

se réduit à zéro ou à 2, suivant que l'on prend pour ρ la racine positive ou la racine négative. Dans le premier cas, on retrouve la formule (55).

Lorsqu'on suppose $x = 2^2 = 4$, l'équation

$$x^4 = 1,$$

a, pour racines primitives,

$$\rho = e^{\omega\sqrt{-1}} = e^{\frac{\pi}{2}\sqrt{-1}} = \sqrt{-1}$$

et

$$\rho = e^{3\omega\sqrt{-1}} = e^{\frac{3\pi}{2}\sqrt{-1}} = -\sqrt{-1}.$$

Alors les valeurs de Ω que fournit l'équation

$$\Omega = 1 + \rho + \rho^4 + \rho^9 = 2(1+\rho),$$

quand on y pose successivement

$$\rho = \sqrt{-1}, \qquad \rho = -\sqrt{-1},$$

sont

$$\Omega = 2(1+\sqrt{-1}),$$
$$\Omega = 2(1-\sqrt{-1}).$$

La première de ces valeurs est, comme on devait s'y attendre, celle que fournirait l'équation (45). Si l'on prenait pour ρ, non plus une racine primitive de l'équation

$$x^4 = 1,$$

mais l'une des deux autres racines -1, 1, la formule

$$\Omega = 2(1+\rho)$$

donnerait, pour $\rho = -1$,

$$\Omega = 0$$

et, pour $\rho = 1$,

$$\Omega = 2.2 = 4.$$

Lorsqu'on suppose $n = 2^3 = 8$, l'équation

$$x^8 = 1$$

a pour racines primitives les expressions imaginaires

$$e^{\omega\sqrt{-1}}, \quad e^{3\omega\sqrt{-1}}, \quad e^{5\omega\sqrt{-1}}, \quad e^{7\omega\sqrt{-1}},$$

l'arc ω étant $\frac{2\pi}{8} = \frac{\pi}{4}$, ou, ce qui revient au même, les expressions imaginaires

$$\frac{1+\sqrt{-1}}{\sqrt{2}}, \quad \frac{-1+\sqrt{-1}}{\sqrt{2}}, \quad \frac{-1-\sqrt{-1}}{\sqrt{2}}, \quad \frac{+1-\sqrt{-1}}{\sqrt{2}};$$

et, si l'on prend alors pour ρ l'une de ces expressions, la valeur de Ω, généralement déterminée par la formule

$$\Omega = 1 + \rho + \rho^4 + \rho^9 + \rho^{16} + \rho^{25} + \rho^{36} + \rho^{49} = 2(1 + 2\rho + \rho^4),$$

se réduira simplement à

$$4\rho = 8^{\frac{1}{2}}(\pm 1 \mp \sqrt{-1}).$$

Lorsque, dans ce dernier produit, on réduit chaque double signe au signe $+$, on retrouve, comme on devait s'y attendre, la valeur de Ω fournie par l'équation (45). Si l'on prenait pour ρ une racine non primitive de l'équation

$$x^8 = 1,$$

c'est-à-dire l'une des racines

$$\sqrt{-1}, \quad -\sqrt{-1}, \quad -1, \quad 1,$$

qui vérifient l'équation de degré moindre

$$x^4 = 1,$$

la valeur de Ω, réduite à

$$4(1+\rho),$$

serait évidemment double de celle qu'on aurait trouvée en supposant, non plus $n = 8$, mais $n = 4$.

On obtiendrait avec la même facilité les valeurs de Ω correspondant à $n = 2^4 = 16$, à $n = 2^5 = 32$, etc.

Concevons maintenant que n, cessant de représenter un nombre premier ou une puissance d'un tel nombre, désigne le produit de plusieurs facteurs premiers

$$\nu, \quad \nu', \quad \nu'', \quad \ldots$$

élevés à des puissances entières, dont les degrés soient respective-

ment

$$a,\quad b,\quad c,\quad \ldots,$$

en sorte que l'on ait

$$n = \nu^a \nu'^b \nu''^c \ldots. \tag{58}$$

Alors, en vertu du théorème IV de la Note VI, si l'on représente par ρ une racine primitive de l'équation (1), ρ sera de la forme

$$\rho = \xi\eta\zeta\ldots, \tag{59}$$

chacun des facteurs $\xi, \eta, \zeta, \ldots$ désignant une racine primitive de la première, ou de la seconde, ou de la troisième, etc. des équations

$$x^{\nu^a} = 1, \quad x^{\nu'^b} = 1, \quad x^{\nu''^c} = 1, \quad \ldots, \tag{60}$$

et les n racines de l'équation (1) seront les n valeurs qu'on obtient pour ρ', en prenant successivement pour l tous les entiers

$$0,\ 1,\ 2,\ 3,\ \ldots,\ n-1$$

inférieurs à n. Soient d'ailleurs

$$\lambda,\quad \lambda',\quad \lambda'',\quad \ldots$$

les restes qu'on obtient en divisant successivement l'exposant l par les divers facteurs

$$\nu^a,\quad \nu'^b,\quad \nu''^c,\quad \ldots$$

de l'exposant n. Comme les valeurs de λ seront en nombre égal à ν^a, les valeurs de λ' en nombre égal à ν'^b, les valeurs de λ'' en nombre égal à $\nu''^c, \ldots$, les systèmes de valeurs de $\lambda, \lambda', \lambda'', \ldots$ seront en nombre égal au produit

$$\nu^a \nu'^b \nu''^c \ldots = n,$$

c'est-à-dire, en même nombre que les valeurs de l. Donc à chaque valeur de l correspondra un seul système de valeurs de $\lambda, \lambda', \lambda'', \ldots$, et réciproquement. Ce n'est pas tout. Comme les formules

$$l \equiv \lambda \pmod{\nu^a}, \qquad l \equiv \lambda' \pmod{\nu'^b}, \qquad l \equiv \lambda'' \pmod{\nu''^c}, \qquad \ldots$$

entraîneront évidemment les suivantes,

$$l^t \equiv \lambda^t \pmod{\nu^a}, \qquad l^t \equiv \lambda'^t \pmod{\nu'^b}, \qquad l^t \equiv \lambda''^t \pmod{\nu''^c}, \qquad \ldots,$$

quel que soit l'entier désigné par t, on peut affirmer que l'équation (59) entraînera non seulement la formule

$$\rho^t = \xi^\lambda \eta^{\lambda'} \zeta^{\lambda''} \ldots, \tag{61}$$

mais encore la suivante,

$$\rho^{t'} = \xi^{\lambda'} \eta^{\lambda''} \zeta^{\lambda'''} \ldots. \tag{62}$$

Donc, en posant, pour abréger,

$$\nu^a = \varphi, \quad \nu'^b = \chi, \quad \nu''^c = \psi, \quad \ldots,$$

on aura non seulement

$$\left\{\begin{array}{l} 1 + \rho + \rho^2 + \rho^3 + \ldots + \rho^{n-1} \\ \quad = (1 + \xi + \xi^2 + \xi^3 + \ldots + \xi^{\varphi-1})(1 + \eta + \eta^2 + \eta^3 + \ldots + \eta^{\chi-1})\ldots, \end{array}\right. \tag{63}$$

mais encore

$$\left\{\begin{array}{rl} & 1 + \rho + \rho^{2^t} + \rho^{3^t} + \ldots + \rho^{(n-1)^t} \\ = & (1 + \xi + \xi^{2^t} + \xi^{3^t} + \ldots + \xi^{(\varphi-1)^t}) \\ & \times (1 + \eta + \eta^{2^t} + \eta^{3^t} + \ldots + \eta^{(\chi-1)^t}) \ldots. \end{array}\right. \tag{64}$$

Ainsi, en particulier, en prenant $t = 2$, on trouvera

$$\left\{\begin{array}{rl} & 1 + \rho + \rho^4 + \rho^9 + \ldots + \rho^{(n-1)^2} \\ = & (1 + \xi + \xi^4 + \xi^9 + \ldots + \xi^{(\varphi-1)^2}) \\ & \times (1 + \eta + \eta^4 + \eta^9 + \ldots + \eta^{(\chi-1)^2}) \ldots. \end{array}\right. \tag{65}$$

De cette dernière formule, que M. Gauss a établie comme nous venons de le faire, il résulte évidemment qu'une valeur de Ω, correspondant à une valeur donnée du degré n de l'équation (30), est le produit de divers facteurs dont chacun représente une valeur de Ω correspondant, non plus au degré donné n et à l'équation (30), mais à l'un des degrés $\nu^a, \nu'^b, \nu''^c, \ldots$ et à l'une des équations (60). Donc, puisque nous avons appris à trouver la valeur de Ω correspondant au cas où n

est une puissance d'un nombre premier, la formule (65) offrira le moyen d'obtenir la valeur de Ω dans tous les cas possibles.

Considérons en particulier le cas où n est un nombre impair composé de facteurs impairs inégaux

$$\nu,\quad \nu',\quad \nu'',\quad \ldots,$$

en sorte qu'on ait simplement

$$\nu\nu'\nu''\ldots = n.$$

Alors les équations (60) deviendront

$$x^{\nu}=1,\qquad x^{\nu'}=1,\qquad x^{\nu''}=1,\qquad \ldots; \tag{66}$$

par conséquent, la formule (65) sera réduite à

$$\left.\begin{aligned} &1+\rho+\rho^{4}+\rho^{9}+\ldots+\rho^{(n-1)^2}\\ =\;&(1+\xi+\xi^{4}+\xi^{9}+\ldots+\xi^{(\nu-1)^2})\\ &\times(1+\eta+\eta^{4}+\eta^{9}+\ldots+\eta^{(\nu'-1)^2})\ldots, \end{aligned}\right\} \tag{67}$$

et l'on conclura de cette formule que la valeur de Ω, correspondant à l'équation (30), est le produit de facteurs dont chacun représente une valeur de Ω correspondant à l'une des équations (66). D'ailleurs, d'après ce qui a été dit plus haut, le premier, le second, le troisième, etc. de ces facteurs représenteront des sommes alternées des racines primitives de la première, de la seconde, de la troisième, etc. des équations (66). Donc, le produit de ces mêmes facteurs, ou la valeur de Ω correspondant à l'équation (30), représentera une somme alternée des racines primitives de cette équation : et, en raisonnant comme à la page 276, on reconnaitra facilement que la formule (52) entraine encore, dans le cas dont il s'agit, la formule (54).

Pour montrer une application de la formule (67), supposons en particulier

$$n=15=3.5.$$

Alors on trouvera

$$\begin{aligned}\Omega&=1+\rho+\rho^{4}+\rho^{9}+\ldots+\rho^{14^2}\\ &=1+4\rho+4\rho^{4}+2\rho^{6}+2\rho^{9}+2\rho^{10}=(1+2\rho^{10})(1+2\rho^{6}+2\rho^{9});\end{aligned}$$

et, par suite, si l'on pose

$$\xi=\rho^{10},\qquad \eta=\rho^{6},$$

on aura

$$\Omega=(1+2\xi)(1+2\eta+2\eta^{4}),$$

ou, ce qui revient au même,

$$\Omega=(1+\xi+\xi^{4})(1+\eta+\eta^{4}+\eta^{9}+\eta^{16}),$$

attendu que, ρ étant racine de l'équation

$$x^{15}=1,$$

$\xi=\rho^{10}$ sera racine de l'équation

$$x^{3}=1,$$

et $\eta=\rho^{6}$ racine de l'équation

$$x^{5}=1.$$

Si, pour fixer les idées, on suppose

$$\rho=e^{\frac{2\pi}{15}\sqrt{-1}}=\cos\frac{2\pi}{15}+\sqrt{-1}\,\sin\frac{2\pi}{15},$$

on trouvera

$$\xi=e^{\frac{4\pi}{3}\sqrt{-1}},\qquad \eta=e^{\frac{4\pi}{5}\sqrt{-1}},$$

$$1+2\xi=-3^{\frac{1}{2}}\sqrt{-1},\qquad 1+2\eta+2\eta^{4}=-5^{\frac{1}{2}},$$

et par suite on aura, conformément à l'équation (52),

$$\Omega=\left(-3^{\frac{1}{2}}\sqrt{-1}\right)\left(-5^{\frac{1}{2}}\right)=15^{\frac{1}{2}}\sqrt{-1}.$$