C. R. Acad. Sc. Paris, 1840, 1er Semestre. (T. X, No 11.)

THÉORIE DES NOMBRES.

Théorèmes divers sur les résidus et les non-résidus quadratiques

par M. Augustin Cauchy

§ Ier. *Sur les résidus inférieurs à un module donné.*

Les formules nouvelles, que nous nous proposons d'établir, se trouvant liées avec celles que M. Gauss a données, dans le Mémoire intitulé *Summatio serierum quarumdam singularium*, nous allons d'abord rappeler ces dernières en peu de mots.

On a, pour une valeur entière du nombre m, et pour une valeur quelconque de x (séance du 3 février, page 180),

$$(1-x)(1-x^3)\dots(1-x^{2m-1}) = 1 - \frac{1-x^{2m}}{1-x} + \frac{(1-x^{2m})(1-x^{2m-2})}{(1-x)(1-x^2)} - \dots + 1.$$

Si, dans cette formule, on pose $2m = n-1$, et

$$x = \rho,$$

ρ étant une racine primitive de l'équation

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

on trouvera

$$(1-\rho)(1-\rho^3)\dots(1-\rho^{n-2}) = 1 + \rho^{-1} + \rho^{-3} + \dots + \rho^{-\frac{1}{2}n(n-1)},$$

puis, en remplaçant ρ par ρ^{-2},

$$(1-\rho^{-2})(1-\rho^{-6})\dots(1-\rho^{-2(n-2)}) = 1 + \rho^2 + \rho^6 + \dots + \rho^{n(n-1)},$$

Enfin, si l'on multiplie les deux membres de la dernière équation par

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

en ayant égard aux formules

$$\left(\frac{n-1}{2}\right)^2 = 1 + 3 + 5 + \dots + (n-2),$$
$$m(m-1) + \left(\frac{n-1}{2}\right)^2 \equiv \left(\frac{2m-1 \pm n}{2}\right), \qquad (mod.\ n)$$

on trouvera définitivement

(2) $$(\rho-\rho^{-1})(\rho^3-\rho^{-3})\dots(\rho^{n-2}-\rho^{-(n-2)}) = 1 + \rho^4 + \rho^9 + \dots + \rho^{(n-1)^2}.$$

Si, pour abréger, on désigne par Δ la valeur commune des deux membres de la formule (2), on aura non-seulement

$$\Delta = (-1)^{\frac{n-1}{2}} \rho^{-\left(\frac{n-1}{2}\right)^2} (1-\rho^2)(1-\rho^4)\dots(1-\rho^{n-1}),$$

Retranscription, Denise Vella-Chemla, juin 2021 mais encore

$$\Delta = (-1)^{\frac{n-1}{2}} \rho^{-\left(\frac{n-1}{2}\right)^2} (\rho^n - \rho^2)(\rho^n - \rho^4) \dots (\rho^n - \rho^{n-1})$$
$$\rho^{\left(\frac{n-1}{2}\right)^2} (1-\rho)(1-\rho^3) \dots (1-\rho^{n-2}),$$

et par suite

(3) $$\Delta^2 = (-1)^{\frac{n-1}{2}} (1-\rho)(1-\rho^2)(1-\rho^3) \dots (1-\rho^{n-2})(1-\rho^{n-1})$$

Or de l'équation identique

$$x^n - 1 = (x-1)(x-\rho)(x-\rho^2) \dots (x-\rho^{n-1}),$$

on tirera

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

puis, en posant $x = 1$,

(4) $$n = (1-\rho)(1-\rho^2) \dots (1-\rho^{n-1}).$$

Donc la formule (3) donnera

(5) $$\Delta^2 = (-1)^{\frac{n-1}{2}} n.$$

Les diverses racines ρ de l'équation (1) peuvent être présentées sous la forme

(6) $$\rho = e^{m\omega\sqrt{-1}} = \cos m\omega + \sqrt{-1} \sin m\omega$$

la valeur de ω étant

(7) $$\omega = \frac{2\pi}{n},$$

et m désignant l'un des nombres

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

Ajoutons que la valeur de ρ, déterminée par l'équation (6), sera une racine primitive, si m est premier à n. Ainsi, par exemple, à la valeur 1 de m correspondra la racine primitive

(8) $$\rho = e^{\omega\sqrt{-1}} = \cos \omega + \sqrt{-1} \sin \omega$$

En substituant cette dernière valeur de ρ dans les deux membres de l'équation (1), on trouve

(9) $$\left\{ \begin{array}{ll} \Delta & = (2\sqrt{-1})^{\frac{n-1}{2}} \sin \omega \sin 3\omega \dots \sin(n-2)\omega \\ & = 1 + \cos \omega + \cos 4\omega + \dots + \cos (n-1)^2\omega \\ & \quad + [\sin \omega + \sin 4\omega + \dots + \sin (n-1)^2\omega]\sqrt{-1}; \end{array} \right.$$

et, comme chacun des angles

$$\omega, 2\omega, \dots, \frac{n-1}{2}\omega,$$

sera compris entre les limites 0, π, il est clair que, si l'on prend

(10) $$\Omega = \sin \omega \sin 2\omega \dots \sin \left(\frac{n-1}{2}\omega\right) = \pm \sin \omega \sin 3\omega \dots \sin (n-2)\omega,$$

le produit Ω sera positif. Donc, puisqu'on tirera des formules (5), (9) et (10),

$$2^{n-1}\Omega^2 = n,$$

on aura nécessairement

(11) $$2^{\frac{n-1}{2}} \Omega = \sqrt{n};$$

et, comme on trouvera encore

$$\sin \omega \sin 2\omega \dots \sin (n-2)\omega = (-1)^{\frac{(n-1)(n-3)}{8}} \sin \omega \sin 2\omega \dots \sin \left(\frac{n-1}{2}\omega\right),$$

la formule (9) donnera

(12) $$\Delta = n^{\frac{1}{2}}(\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}.$$

En d'autres termes, on aura

(13) $$\Delta = n^{\frac{1}{2}}$$

lorsque n sera de la forme $4x+1$, et

(14) $$\Delta = n^{\frac{1}{2}}\sqrt{-1},$$

lorsque n sera de la forme $4x+3$. Ainsi, par exemple, on trouvera

pour $n=3$,

$$\begin{aligned}\rho &= \cos\frac{2\pi}{3} + \sqrt{-1}\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{3^{\frac{1}{2}}}{2}\sqrt{-1},\\ \Delta &= 1+\rho+\rho^4 = 1+2\rho = 3^{\frac{1}{2}}\sqrt{-1}\ ;\end{aligned}$$

pour $n=5$,

$$\Delta = 1+\rho+\rho^4+\rho^9+\rho^{16} = 1+2\rho+2\rho^4 = 1+4\cos\frac{2\pi}{5} = 5^{\frac{1}{2}}\ ;$$

pour $n=9=3^2$,

$$\Delta = 1+\rho+\rho^4+\ldots+\rho^{64} = 3+2(\rho+\rho^4+\rho^7) = 3+2\rho\frac{\rho^9-1}{\rho^3-1} = 3\ ;$$

pour $n=27=3^3$,

$$\begin{aligned}\Delta &= 1+\rho+\rho^4+\ldots+\rho^{26} = 3+6\rho^9+2\rho(1+\rho^3+\ldots+\rho^{24})\\ &= 3+6\rho^9+2\rho\frac{\rho^{27}-1}{\rho^3-1} = 3+6\rho^9 = 3(1+2\rho^9) = 3.3^{\frac{1}{2}}\sqrt{-1}\ ;\end{aligned}$$

pour $n=15=3.5$,

$$\begin{aligned}\Delta &= 1+\rho+\rho^4+\ldots+\rho^{14^2} = 1+4\rho+4\rho^4+2\rho^6+2\rho^9+2\rho^{10}\\ &= (1+2\rho^{10})(1+2\rho^6+2\rho^9) = (-5^{\frac{1}{2}})(-3^{\frac{1}{2}}\sqrt{-1}) = 15^{\frac{1}{2}}\sqrt{-1}\ ;\\ &\text{etc}\ldots\end{aligned}$$

Les formules (9) et (10) se rapportent au cas où la valeur de ρ est déterminée par l'équation (8). Supposons maintenant que, la valeur de ρ étant généralement déterminée par l'équation (6), on prenne encore

(15) $$\Delta = 1+\rho^4+\rho^9+\ldots+\rho^{(n-1)^2}.$$

Si m est premier à n, alors, ρ étant une racine primitive de l'équation (1), on se trouvera de nouveau conduit aux formules (4), (5), et par suite la valeur de Δ sera, au signe près, celle que détermine la formule (12).

D'autre part, si l désigne un nombre inférieur à $\frac{n}{2}$, on aura

$$(n-l)^2 \equiv l^2 \ (\text{mod. } n),$$

et, en conséquence, la formule (15) pourra toujours être réduite à

(16) $$\Delta = 1+2\left(\rho+\rho^4+\ldots+\rho^{\left(\frac{n-1}{2}\right)^2}\right).$$

Considérons en particulier le cas où n représente un nombre premier. Alors si, parmi les entiers positifs et inférieurs à n, on nomme

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

ceux qui, étant résidus quadratiques, vérifient la condition

$$\left(\frac{h}{n}\right) = 1, \tag{17}$$

et

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

ceux qui, étant non-résidus quadratiques, vérifient la condition

$$\left(\frac{k}{n}\right) = -1, \tag{18}$$

on verra la formule (16) se réduire à

$$\Delta = 1 + 2(\rho^h + \rho^{h'} + \rho^{h''} + \ldots) \tag{19}$$

Si d'ailleurs ρ ne se réduit pas à l'unité, on aura

$$1 + \rho + \rho^2 + \ldots + \rho^{n-1} = \frac{\rho^n - 1}{\rho - 1} = 0,$$

ou, ce qui revient au même,

$$1 + \rho^h + \rho^{h'} + \rho^{h''} + \ldots + \rho^k + \rho^{k'} + \rho^{k''} + \ldots = 0. \tag{20}$$

Donc alors la formule (19) donnera

$$\Delta = \rho^h + \rho^{h'} + \rho^{h''} + \ldots - \rho^k - \rho^{k'} - \rho^{k''} - \ldots \tag{21}$$

Donc, lorsque, n étant un nombre premier, ρ ne se réduit pas à l'unité, la valeur de Δ, fournie par l'équation (15) ou (16), est une fonction alternée des racines primitives de l'équation (1). Cette valeur sera même une somme alternée de ces racines, si ρ désigne l'une d'entre elles, et par conséquent alors on aura

$$\Delta^2 = (-1)^{\frac{n-1}{2}} n,$$

conformément à l'équation (5). Il y a plus : puisqu'en supposant la valeur de ρ donnée par l'équation (8), on a trouvé

$$\Delta = n^{\frac{n-1}{2}} (\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}.$$

on trouvera au contraire, en supposant la valeur de ρ donnée par l'équation (6),

$$\Delta = \left(\frac{m}{n}\right) n^{\frac{n-1}{2}} (\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}. \tag{22}$$

Si ρ se réduisait simplement à l'unité, la formule (15) donnerait évidemment

$$\Delta = n. \tag{23}$$

Au reste, à l'aide des formules ci-dessus établies, on calculera facilement la valeur que peut acquérir l'expression Δ, déterminée par la formule (15), non-seulement lorsque n représente un nombre premier ou une puissance d'un tel nombre, mais aussi lorsque n est le produit de certaines puissances

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

de divers nombres premiers

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

Dans ce dernier cas, on reconnaît sans peine que l'expression Δ, déterminée par la formule (15), est le produit d'expressions du même genre qui correspondent non plus à la valeur

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

mais aux valeurs

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

de l'exposant n ; puis on conclut immédiatement que la formule (22) peut être, aussi bien que la formule (12), étendue à des valeurs quelconques de n, par exemple, à la valeur

$$n = \nu^a \nu'^b \nu''^c \ldots,$$

pourvu que, m étant premier à n, on pose avec M. Jacobi

$$\left(\frac{m}{n}\right) = \left(\frac{m}{\nu}\right)^a \left(\frac{m}{\nu'}\right)^b \left(\frac{m}{\nu''}\right)^c \ldots \tag{24}$$

Lorsque les exposants

$$a, b, c, \ldots$$

se réduisent à l'unité, la formule (24) se réduit à

$$\left(\frac{m}{n}\right) = \left(\frac{m}{\nu}\right) \left(\frac{m}{\nu'}\right) \left(\frac{m}{\nu''}\right), \ldots \tag{25}$$

et la valeur de Δ peut être censée fournie par l'équation (21), pourvu que l'on nomme

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

ceux des entiers inférieurs à n, mais premiers à n, qui vérifient la condition (17) ou la condition (18).

Si l'on substitue dans la formule (22) la valeur de Δ, tirée des équations (16) et (6), on trouvera

$$\left\{\begin{aligned} &\frac{1}{2} + \cos m\omega + \cos 4m\omega + \ldots + \cos \left(\frac{n-1}{2}\right)^2 m\omega \\ &\quad + \left(\frac{1}{2} + \sin m\omega + \sin 4m\omega + \ldots + \sin \left(\frac{n-1}{2}\right)^2 m\omega\right) \sqrt{-1} \\ &\quad = \frac{1}{2} \left(\frac{m}{n}\right) n^{\frac{1}{2}} (\sqrt{-1})^{\left(\frac{n-1}{2}\right)^2}. \end{aligned}\right. \tag{26}$$

On aura donc par suite, si n est de la forme $4x+1$,

$$\frac{1}{2} + \cos m\omega + \cos 4m\omega + \ldots + \cos \left(\frac{n-1}{2}\right)^2 m\omega = \frac{1}{2} \left(\frac{m}{n}\right) \sqrt{n}, \tag{27}$$

et, si n est de la forme $4x+3$,

$$\sin m\omega + \sin 4m\omega + \ldots + \sin \left(\frac{n-1}{2}\right)^2 m\omega = \frac{1}{2} \left(\frac{m}{n}\right) \sqrt{n}. \tag{28}$$

Pareillement, on tirera des formules (6), (16) et (21), lorsque n sera de la forme $4x+1$,

$$S \cos mh\omega - S \cos mk\omega = \left(\frac{m}{n}\right) \sqrt{n}, \tag{29}$$

et lorsque n sera de la forme $4x+3$,

$$S \sin mh\omega - S \sin mk\omega = \left(\frac{m}{n}\right) \sqrt{n}, \tag{30}$$

le signe S indiquant une somme de termes semblables entre eux, et relatifs aux diverses valeurs de h ou de k, qui vérifient la condition (17) ou (18). Si l'on suppose en particulier $m = 1$, on aura simplement, lorsque n sera de la forme $4x+1$,

$$S \cos h\omega - S \cos k\omega = \sqrt{n}, \tag{31}$$

et lorsque n sera de la forme $4x+3$,

$$S \sin h\omega - S \sin k\omega = \sqrt{n}. \tag{32}$$

§. II. *Sur les résidus et les non-résidus quadratiques inférieurs à la moitié d'un module donné.*

Parmi les entiers inférieurs à un nombre impair n, mais premiers à n, considérons en particulier ceux qui ne surpassent pas la moitié de ce même nombre, et soit l un de ces entiers.

On aura généralement

$$\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}},\qquad \left(\frac{n-l}{n}\right)=(-1)^{\frac{n-1}{2}}\left(\frac{l}{n}\right),\tag{1}$$

puis on en conclura, si n est de la forme $4x+1$,

$$\left(\frac{n-l}{n}\right)=\left(\frac{l}{n}\right)\tag{2}$$

et, si n est de la forme $4x+3$,

$$\left(\frac{n-l}{n}\right)=-\left(\frac{l}{n}\right)\tag{3}$$

Cela posé, parmi les entiers inférieurs à $\frac{n}{2}$ mais premiers à n, nommons h un quelconque de ceux qui vérifient la condition

$$\left(\frac{h}{n}\right)=1\tag{4}$$

et k l'un quelconque de ceux qui vérifient la condition

$$\left(\frac{k}{n}\right)=-1\tag{5}$$

Les entiers inférieurs à n, mais premiers à n, seront entre les limites 0, $\frac{n}{2}$ de l'une des formes

$$h,\qquad k,$$

et entre les limites $\frac{n}{2}, n$, de l'une des formes,

$$n-h,\qquad n-k.$$

De plus on aura, si n est de la forme $4x+1$,

$$\left(\frac{h}{n}\right)=1,\qquad \left(\frac{n-h}{n}\right)=1,\qquad \left(\frac{k}{n}\right)=-1,\qquad \left(\frac{n-k}{n}\right)=-1;\tag{6}$$

et, si n est de la forme $4x+3$,

$$\left(\frac{h}{n}\right)=1,\qquad \left(\frac{n-k}{n}\right)=1,\qquad \left(\frac{k}{n}\right)=-1,\qquad \left(\frac{n-h}{n}\right)=-1;\tag{7}$$

Cela posé, si, dans les formules (31), (32) du § I$^{\text{er}}$, on étend le signe S aux seules valeurs de h ou de k qui ne surpassent pas $\frac{n}{2}$, on verra évidemment ces formules se réduire aux suivantes,

$$S\ \cos h\omega - S\ \cos k\omega = \frac{1}{2}\sqrt{n},\qquad \text{pour } n\equiv 1 \text{ (mod. 4)},\tag{8}$$

$$S\ \sin h\omega - S\ \sin k\omega = \frac{1}{2}\sqrt{n},\qquad \text{pour } n\equiv 3 \text{ (mod. 4)}\tag{9}$$

la valeur de ω étant toujours

$$\omega=\frac{\pi}{2n}.\tag{10}$$

Alors aussi, m étant premier à n, on aura, en vertu des formules (29), (30) du § I$^{\text{er}}$,

$$S\cos mh\omega - S\cos mk\omega = \frac{1}{2}\left(\frac{m}{n}\right)\sqrt{n},\qquad \text{pour } n\equiv 1 \text{ (mod. 4)}\tag{11}$$

$$S\sin mh\omega - S\sin mk\omega = \frac{1}{2}\left(\frac{m}{n}\right)\sqrt{n},\qquad \text{pour } n\equiv 3 \text{ (mod. 4)}\tag{12}$$

Observons maintenant que, n étant impair, ou premier à 2, les entiers inférieurs à n, mais premiers à n, pourront être représentés indifféremment ou par les divers termes de l'une des formes

$$h,\qquad k,\qquad n-h,\qquad n-k,$$

ou par les nombres qu'on obtiendrait en doublant ces termes et divisant les résultats par n. D'ailleurs ces derniers nombres seront de l'une des formes

$$2h, \qquad 2k, \qquad n-2h, \qquad n-2k.$$

Enfin l'on trouvera généralement

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}, \tag{13}$$

c'est-à-dire que $\left(\frac{2}{n}\right)$ se réduira simplement à $+1$, si n est de l'une des formes $8x+1, 8x+7$, et à -1, si n est de l'une des formes $8x+3, 8x+5$; et l'on aura par suite, eu égard aux formules (6), (7):

1° si n est de la forme $8x+1$,

$$\left(\frac{2h}{n}\right) = 1, \qquad \left(\frac{n-2h}{n}\right) = 1, \qquad \left(\frac{2k}{n}\right) = -1, \qquad \left(\frac{n-2k}{n}\right) = -1\ ; \tag{14}$$

2° si n est de la forme $8x+5$,

$$\left(\frac{2k}{n}\right) = 1, \qquad \left(\frac{n-2k}{n}\right) = 1, \qquad \left(\frac{2h}{n}\right) = -1, \qquad \left(\frac{n-2h}{n}\right) = -1\ ; \tag{15}$$

3° si n est de la forme $8x+3$,

$$\left(\frac{2k}{n}\right) = 1, \qquad \left(\frac{n-2h}{n}\right) = 1, \qquad \left(\frac{2h}{n}\right) = -1, \qquad \left(\frac{n-2k}{n}\right) = -1\ ; \tag{16}$$

4° si n est de la forme $8x+7$,

$$\left(\frac{2h}{n}\right) = 1, \qquad \left(\frac{n-2k}{n}\right) = 1, \qquad \left(\frac{2k}{n}\right) = -1, \qquad \left(\frac{n-2h}{n}\right) = -1\ ; \tag{17}$$

Cela posé, il est clair que, si l'on suppose le module n de la forme $8x+1$, les mêmes nombres inférieurs à n, et premiers à n pourront être représentés, à l'ordre près, soit par les termes de la forme

$$h, \qquad n-h,$$

soit par les termes de la forme

$$2h, \qquad n-2h.$$

Donc, en étendant le signe S à toutes les valeurs de h, on aura, dans cette hypothèse,

$$S(h) + S(n-h) \ = \ S(2h) + S(n-2h),$$

et même plus généralement

$$Sf(h) + Sf(n-h) \ = \ Sf(2h) + Sf(n-2h),$$

$f(x)$ désignant une fonction quelconque de x. On trouvera, par exemple, en prenant pour m un nombre entier

$$Sh^m + S(n-h)^m \ = \ S(2h)^m + S(n-2h)^m.$$

Par des raisonnements semblables, on tirera des formules (14), (15), (16), (17), comparées aux formules (6) et (7):

1° si n est de la forme $8x+1$,

$$\left\{ \begin{aligned} Sh^m + S(n-h)^m &= S(2h)^m + S(n-2h)^m\ , \\ Sk^m + S(n-k)^m &= S(2k)^m + S(n-2k)^m\ ; \end{aligned} \right. \tag{18}$$

2° si n est de la forme $8x+5$,

$$\left\{ \begin{aligned} Sh^m + S(n-h)^m &= S(2k)^m + S(n-2k)^m\ , \\ Sk^m + S(n-k)^m &= S(2h)^m + S(n-2h)^m\ ; \end{aligned} \right. \tag{19}$$

3° si n est de la forme $8x+3$,

$$(20)\qquad \begin{cases} Sh^m + S(n-k)^m &= S(2k)^m + S(n-2h)^m , \\ Sk^m + S(n-h)^m &= S(2h)^m + S(n-2k)^m ; \end{cases}$$

4° si n est de la forme $8x+7$,

$$(21)\qquad \begin{cases} Sh^m + S(n-k)^m &= S(2h)^m + S(n-2k)^m , \\ Sk^m + S(n-h)^m &= S(2k)^m + S(n-2h)^m ; \end{cases}$$

Posons maintenant

$$(22)\qquad S.h^m = s_m, \quad Sk^m = t_m ,$$

$$(23)\qquad i = s_0, \quad j = t_0.$$

i sera le nombre des valeurs de h, et j le nombre des valeurs de k inférieures à $\frac{n}{2}$ tandis que

$$s_1 \quad \text{ou} \quad t_1$$

représentera la somme de ces valeurs de h ou de k,

$$s_2 \quad \text{ou} \quad t_2$$

la somme de leurs carrés,

$$s_3 \quad \text{ou} \quad t_3$$

la somme de leurs cubes, etc...; et, si dans les formules (18), (19), (20), (21), on pose successivement

$$m=0, \quad m=1, \quad m=2, \quad m=3, ...$$

on obtiendra des relations diverses entre les quantités

$$i,\ s_1,\ s_2,\ s_3, \ldots, j,\ t_1,\ t_2,\ t_3, \ldots$$

Si l'on combine, par voie d'addition, les deux formules (18), ou (19), ou (20), ou (21), on obtiendra seulement des relations entre les sommes

$$i+j, s_1+t_1, s_2+t_2, s_3+t_3, \ldots$$

dont la valeur est connue, puisque le système entier des nombres des deux formes h et k, ne diffère pas du système des entiers inférieurs à $\frac{1}{2}n$, et premiers à n. Mais, si la combinaison a lieu par voie de soustraction, on obtiendra des relations entre les différences

$$i-j, s_1-t_1, s_2-t_2, s_3-t_3, \ldots$$

Alors, en posant

$$(24)\qquad \left[2^m - \left(\frac{2}{n}\right)\right] \frac{s_m - t_m}{n^m} = v_m,$$

en sorte qu'on ait

$$(25)\qquad \frac{2^m-1}{n^m}(s_m - t_m) = v_m, \qquad \text{pour} \quad n \equiv 1 \text{ ou } 7 \text{ (mod. 8)},$$

et

$$(26)\qquad \frac{2^m+1}{n^m}(s_m - t_m) = v_m, \qquad \text{pour} \quad n \equiv 3 \text{ ou } 5 \text{ (mod. 8)},$$

on trouvera:

1° si n est de la forme $4x+1$,

$$(27)\qquad v_m + v_0 - mv_1 + \frac{m(m-1)}{1.2}v_2 - \ldots \pm v_m = 0 ;$$

2° si n est de la forme $4x+3$,

$$-v_m+v_0-mv_1+\frac{m(m-1)}{1.2}v_2-\ldots\pm v_m=0\,. \tag{28}$$

On aura donc, si n est de la forme $4x+1$,

$$\left\{\begin{array}{rcl} v_0 &=& 0,\\ v_0-2v_1+2v_2 &=& 0\\ v_0-3v_1+3v_2 &=& 0,\\ v_0-4v_1+6v_2-4v_3+2v_4 &=& 0,\\ \text{etc.},\ldots \end{array}\right. \tag{29}$$

par conséquent

$$v_0 \;=\; 0, \qquad v_2-v_1 \;=\; 0, \qquad v_4-2v_3+v_2 \;=\; 0, \qquad \text{etc.}\ldots\;; \tag{30}$$

et, si n est de la forme $4x+3$,

$$\left\{\begin{array}{rcl} v_0-2v_1 &=& 0\\ v_0-3v_1+3v_2-2v_3 &=& 0,\\ v_0-4v_1+6v_2-4v_3 &=& 0,\\ \text{etc.},\ldots \end{array}\right. \tag{31}$$

par conséquent

$$v_0-2v_1 \;=\; 0, \qquad v_1-3v_2+2v_3 \;=\; 0, \qquad \text{etc.}\ldots\;; \tag{32}$$

On aura d'ailleurs, en vertu des formules (23), (25) et (26),

$$v_0=0, \qquad \text{si} \quad n\equiv 1 \;\text{ ou }\; 7, \;\; (\text{mod. } 8), \tag{33}$$

$$v_0=2(i-j), \qquad \text{si} \quad n\equiv 3 \;\text{ ou }\; 5, \;\; (\text{mod. } 8), \tag{34}$$

Cela posé, les formules (30) et (32) donneront :

1° si n est de la forme $8x+1$,

$$3(s_2-t_2)=n(s_1-t_1), 15(s_4-t_4)=n[14(s_3-t_3)-3n(s_2-t_2)], \text{etc.}\ldots\;; \tag{35}$$

2° si n est de la forme $8x+5$,

$$i=j, 5(s_2-t_2)=3n(s_1-t_1), 17(s_4-t_4)=n[18(s_3-t_3)-5n(s_2-t_2)], \text{etc.}\ldots\;; \tag{36}$$

3° si n est de la forme $8x+3$,

$$3(s_1-t_1)=n(i-j), 6(s_3-t_3)=n[5(s_2-t_2)-n(s_1-t_1)], \text{etc.}\ldots\;; \tag{37}$$

4° si n est de la forme $8x+7$,

$$s_1=t_1, 14(s_3-t_3)=9n(s_2-t_2), \text{etc.}\ldots. \tag{38}$$

Ajoutons que, si l'on désigne par

$$S_m \qquad \text{ou} \qquad T_m$$

la somme des $m^{\text{ièmes}}$ puissances des entiers inférieurs non plus à $\frac{n}{2}$, mais à n et qui, étant premiers à n, vérifient la condition (4) ou (5), les valeurs de S_m, T_m, pourront être représentées par les premiers membres des formules (18) et (19), ou (20) et (21); et que l'on aura en conséquence,

1° si n est de la forme $4x+1$,

$$S_m-T_m=s_m-t_m+n^m(i-j)-mn^{nm-1}(s_1-t_1)+\frac{m(m-1)}{2}n^{m-2}(s_2-t_2)-\text{etc.}\;; \tag{39}$$

2° si n est de la forme $4x+3$,

$$S_m-T_m=s_m-t_m-n^m(i-j)+mn^{nm-1}(s_1-t_1)-\frac{m(m-1)}{2}n^{m-2}(s_2-t_2)+\text{etc.}\;; \tag{40}$$

D'autre part les sommes

$$S_0 + T_0, \quad S_1 + T_1, \quad S_2 + T_2, \ldots$$

seront des quantités connues ; et, en nommant N le nombre des entiers inférieurs à n mais premiers à n, on trouvera, si n n'est pas un carré,

$$S_0 = T_0 = \frac{1}{2}N, \qquad S_0 + T_0 = N. \tag{41}$$

Cela posé, si dans les formules (39), (40), on attribue simultanément à m les valeurs 0, 1, 2, 3,..., on tirera de ces formules :

1° en supposant que n soit un nombre, non carré, de la forme $4x + 1$,

$$i = j, \quad S_1 = T_1, \quad S_2 - T_2 = 2[s_2 - t_2 - n(s_1 - t_1)], \quad \text{etc.} \ldots \tag{42}$$

2° en supposant n de la forme $4x + 3$,

$$S_1 - T_1 = 2(s_1 - t_1) - n(i - j), \quad S_2 - T_2 = 2n(s_1 - t_1) - n^2(i - j), \quad \text{etc.} \ldots \tag{43}$$

et par conséquent

$$T_2 - S_2 = n(T_1 - S_1) \tag{44}$$

On trouvera en effet, pour $n = 3$,

$$T_1 - S_1 = 2 - 1 = 1, \qquad T_2 - S_2 = 4 - 1 = 3.1 \;;$$

pour $n = 7$,

$$T_1 - S_1 = 3 + 5 + 6 - 1 - 2 - 4 = 7, \qquad T_2 - S_2 = 49 = 7.7 \;;$$

pour $n = 11$,

$$T_1 - S_1 = 2 + 6 + 7 + 8 + 10 - 1 - 3 - 4 - 5 - 9 = 11, T_2 - S_2 = 121 = 11.11 \;;$$

pour $n = 15$,

$$T_1 - S_1 = 7 + 11 + 13 + 14 - 1 - 2 - 4 - 8 = 30, T_2 - S_2 = 450 = 15.30 \;; \text{etc.}$$

En combinant les formules (42), (43), (44), avec les formules (35), (36), (37), (38), on en conclura:

1° si n est de la forme $8x + 1$, sans être un carré,

$$i = j, \quad S_1 = T_1, \quad S_2 = T_2 = 4(t_2 - s_2), \quad \text{etc.} \ldots \;; \tag{45}$$

2° si n est de la forme $8x + 5$,

$$i = j, \quad S_1 = T_1, \quad 3(S_2 = T_2) = 4(t_2 - s_2), \quad \text{etc.} \ldots \;; \tag{46}$$

3° si n est de la forme $8x + 3$,

$$T_1 - S_1 = n\frac{i - j}{3}, \quad T_2 - S_2 = n^2\frac{i - j}{3}, \quad \text{tec.} \ldots \;; \tag{47}$$

4° si n est de la forme $8x + 7$,

$$T_1 - S_1 = n(i - j), \quad T_2 - S_2 = n^2\frac{i - j}{2}, \quad \text{tec.} \ldots \;; \tag{48}$$

Si n était un carré impair, alors, la condition (4) se trouvant vérifiée pour tout nombre premier à n, t_m et T_m s'évanouiraient généralement, et l'on tirerait des formules (35), (39), jointes à la seconde des formules (41),

$$3s_2 = ns_1, \quad 15s_4 = n(14s_3 - ns_2), \quad \text{etc.} \ldots \tag{49}$$

$$S_0 = 2i = N, \quad S_1 = ni, \quad S_2 = n^2 i - 4s_2, \quad \text{etc.} \ldots . \tag{50}$$

Dans le cas particulier où n se réduit à un nombre premier impair, les entiers ci-dessus désignés par h ou k ne sont autres que les résidus ou les non-résidus quadratiques inférieurs à $\frac{n}{2}$. Donc alors i ou j représente le nombre de ces résidus, ou le nombre de ces non-résidus, et s_m ou t_m la somme de leurs puissances du degré m. Cette même somme devient S_m ou T_m, lorsqu'on y admet tous les résidus ou non-résidus inférieurs à m.

Parmi les formules qui précédent, celles qui renferment seulement les trois différences

$$i - j, \qquad s_1 - t_1, \qquad S_1 - T_1,$$

étaient déjà connues, au moins pour le cas où n se réduit à un nombre premier. Ainsi, en particulier, on connaissait les deux premières des formules (42) ; et M. Liouville m'a dit être parvenu à démontrer directement la première des équations (37) ou (38), ainsi que la première des équations (47) ou (48). J'ajouterai que la première des équations (47), et la première des équations (48), résultaient déjà de la comparaison de formules données par M. Dirichlet.

Dans un autre article, je montrerai comment des formules précédentes, combinées avec les équations connues, qui fournissent les développements de $\sin \omega s$ ou de $\cos \omega s$ en séries ordonnées suivant les sinus ou cosinus des multiples de ω, on peut déduire le signe de la différence $i - j$, quand n est de la forme $4x + 3$, et des limites entre lesquelles cette différence se trouve comprise. J'examinerai aussi quelles sont les formules qui doivent remplacer les précédentes, lorsque la lettre n représente, non plus un nombre impair, mais un nombre pair.