PREMIÈRE SÉRIE.

MÉMOIRES, NOTES ET ARTICLES

EXTRAITS DES

RECUEILS DE L'ACADÉMIE DES SCIENCES

DE L'INSTITUT DE FRANCE.

II.

MÉMOIRES

EXTRAITS DES

MÉMOIRES DE L'ACADÉMIE DES SCIENCES

DE L'INSTITUT DE FRANCE.

MÉMOIRE

SUR

LA THÉORIE DES NOMBRES [1].

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

AVERTISSEMENT DE L'AUTEUR.

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

(1) Présenté à l'Académie des Sciences le 31 mai 1830.
(2) *Voir* le Tome XII de ce *Bulletin*, p. 205 et suiv. (*OEuvres de Cauchy*, S. II, T. II).

§ I.

Soient

$$p = n\varpi + 1$$

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

$$x^p = 1; \tag{1}$$

τ une racine primitive de

$$x^{p-1} = 1; \tag{2}$$

t une racine primitive de

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

Alors

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

sera une racine primitive de

$$x^n = 1 \tag{4}$$

et

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

une racine primitive de

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

On aura

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

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

et de plus, si n est pair,

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

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

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

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

le nombre m propre à vérifier la formule

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

en sorte qu'on aura

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

et nous poserons

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

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

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

on en conclura

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

On aura d'ailleurs évidemment

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

Soient maintenant

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

et

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

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

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

et, si l'on pose

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

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

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

et

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

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

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

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

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

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

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

On trouvera, au contraire,

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

Enfin l'on aura

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

et, en supposant n pair,

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

Par suite, si l'on suppose

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

on trouvera

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

si le nombre m est tel qu'aucune des équations

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

ne soit vérifiée. On aura, au contraire,

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

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

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

si les trois équations (18) subsistent simultanément.

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

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

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

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

et, par conséquent,

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

Soit maintenant s une racine primitive de

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

le nombre n étant supposé premier, et faisons

$$\Theta_1 \Theta_{s^2} \Theta_{s^4} \ldots \Theta_{s^{n-3}} = \mathfrak{F}(\rho) \quad (1); \tag{24}$$

on aura

$$\Theta_s \Theta_{s^3} \Theta_{s^5} \ldots \Theta_{s^{n-2}} = \mathfrak{F}(\rho^s) \tag{25}$$

et, de plus,

$$\begin{aligned} \mathfrak{F}(\rho) &= \mathfrak{F}(\rho^{s^2}) = \mathfrak{F}(\rho^{s^4}) = \ldots = \mathfrak{F}(\rho^{s^{n-3}}), \\ \mathfrak{F}(\rho^s) &= \mathfrak{F}(\rho^{s^3}) = \mathfrak{F}(\rho^{s^5}) = \ldots = \mathfrak{F}(\rho^{s^{n-2}}). \end{aligned}$$

Donc $\mathfrak{F}(\rho)$ sera de la forme

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

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

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

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

ou

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

et, comme on aura

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

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

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

on trouvera

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

ou, ce qui revient au même,

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

ou bien encore

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

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

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

ou bien à

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

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

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

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

$$\mathfrak{F}(\rho) = c_0.$$

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

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

l'équation (29) donnera

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

Donc on résoudra l'équation

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

en prenant

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

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

Soit υ un nombre tel qu'on ait simultanément

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

On trouvera

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

et, par suite,

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

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

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

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

D'autre part, comme on aura

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

on en conclura

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

Soit maintenant

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

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

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

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

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

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

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

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

et, par conséquent,

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

Enfin, si l'on pose comme ci-dessus

$$\mathrm{R}_{h,k} = \mathrm{F}(\rho),$$

on trouvera

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

Cela posé, soit p^λ la plus haute puissance de p qui puisse diviser simul-