JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

E.-E. KUMMER

Sur les diviseurs de certaines formes de nombres qui résultent de la théorie de la division du cercle

Journal de mathématiques pures et appliquées 2^e série, tome 5 (1860), p. 369-386.
<http://www.numdam.org/item?id=JMPA_1860_2_5__369_0>

SUR

LES DIVISEURS DE CERTAINES FORMES DE NOMBRES

QUI

RÉSULTENT DE LA THÉORIE DE LA DIVISION DU CERCLE;

PAR M. E.-E. KUMMER.

(TRADUCTION DE M. HOÜEL.)

Si l'on partage en périodes les racines imaginaires de l'équation

$$x^p = 1,$$

p étant un nombre premier, et que l'on forme ainsi e périodes de f termes chacune, e et f étant tels qu'on ait

$$p - 1 = ef,$$

on sait que ces périodes sont les racines d'une équation algébrique du degré e, dans laquelle le coefficient du terme le plus élevé est égal à l'unité, tous les autres coefficients étant des nombres entiers. Soient x une racine imaginaire quelconque de l'équation

$$x^p = 1,$$

et g une racine primitive du nombre premier p. Ces périodes, que nous désignerons, pour abréger, par

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1},$$

auront les valeurs suivantes,

$$\begin{aligned}
\eta &= x + x^{g^e} + x^{g^{2e}} + \ldots + x^{g^{(f-1)e}},\\
\eta_1 &= x^g + x^{g^{e+1}} + x^{g^{2e+1}} + \ldots + x^{g^{(f-1)e+1}},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\eta_{e-1} &= x^{g^{e-1}} + x^{g^{2e-1}} + x^{g^{3e-1}} + \ldots + x^{g^{fe-1}}.
\end{aligned}$$

En posant maintenant

$$\varphi(y) = (y-\eta)(y-\eta_1)(y-\eta_2)\ldots(y-\eta_{e-1}),$$

on aura aussi

$$\varphi(y) = y^e + a_1 y^{e-1} + a_2 y^{e-2} + \ldots + a_{e-1} y + a_e,$$

$a_1, a_2, a_3, \ldots, a_e$ étant des nombres entiers, que l'on peut déterminer dans chaque cas particulier. Nous allons actuellement considérer cette fonction rationnelle et entière $\varphi(y)$ comme une forme sous laquelle on peut représenter certains nombres, et nous allons chercher les diviseurs que peut avoir cette forme. Pour cela, nous ferons usage de congruences où entreront non-seulement des nombres entiers réels, mais encore les périodes irrationnelles et souvent imaginaires

$$\eta, \quad \eta_1, \quad \eta_2, \ldots, \quad \eta_{e-1},$$

et, en conséquence, nous devrons commencer par fixer le sens que l'on doit attacher à de semblables congruences. Toute fonction rationnelle et entière de ces périodes, ayant pour coefficients des nombres entiers, peut se ramener, comme on sait, à la forme linéaire

$$c\eta + c_1\eta_1 + c_2\eta_2 + \ldots + c_{e-1}\eta_{e-1},$$

et cela d'une seule manière. Nous attribuerons donc, en vue de notre but actuel, à l'idée de congruence une extension telle, que deux fonctions rationnelles et entières des périodes soient dites congruentes suivant le module q (lequel doit être un nombre premier), lorsque, après avoir réduit la différence de ces fonctions à la forme

$$c\eta + c_1\eta_1 + \ldots + c_{e-1}\eta_{e-1},$$

tous les coefficients $c, c_1, c_2, \ldots, c_{e-1}$ de cette différence sont divisibles par q. D'après cette définition, on peut ici, comme dans le cas des congruences ordinaires, négliger les termes qui contiennent en facteurs le module q; on peut aussi ajouter ces nouvelles congruences entre elles, les soustraire, les multiplier, et les élever à des puissances.

Nous prendrons maintenant pour point de départ cette proposition

connue, que, si q est un nombre premier, les coefficients

$$b, \quad b_1, \quad b_2, \ldots, \quad b_{q-1},$$

du produit développé

$$z(z-1)(z-2)\ldots(z-q+1) = z^q - b_1 z^{q-1} + b_2 z^{q-2} - \ldots + b_{q-1} z,$$

sont tous divisibles par q, à l'exception du dernier b_{q-1}, lequel, divisé par q, donne pour reste -1. En effet, pour toute valeur de z, ce produit, résultant de la multiplication de q nombres entiers consécutifs, est divisible par q. On a par suite

$$z^q - b_1 z^{q-1} + b_2 z^{q-2} - \ldots + b_{q-1} z \equiv 0 \pmod{q},$$

et puisqu'on a, d'après le théorème de Fermat,

$$z^q \equiv z,$$

il s'ensuit que

$$-b_1 z^{q-1} + b_2 z^{q-2} - \ldots + (b_{q-1} + 1) z \equiv 0 \pmod{q}.$$

Mais cette congruence, de degré $q-1$, ne peut avoir q racines différentes. Elle doit donc être identiquement satisfaite, d'où résulte que l'on a

$$b_1 \equiv b_2 \equiv b_3 \equiv \ldots \equiv b_{q-2} \equiv b_{q-1} + 1 \pmod{q}.$$

Posons maintenant, dans l'équation précédente,

$$z = y - \eta_k,$$

et laissons de côté tous les termes divisibles par q : on obtiendra ainsi le congruence

$$(A) \left\{ \begin{array}{c} (y-\eta_k)(y-1-\eta_k)(y-2-\eta_k)\ldots(y-q+1-\eta_k) \\ \equiv (y-\eta_k)^q - (y-\eta_k) \end{array} \right\} \pmod{q}.$$

Or on sait que, dans le développement de la puissance q d'un binôme, si q est un nombre premier, tous les termes, à l'exception du premier

et du dernier, sont divisibles par q. Donc

$$(y-\eta_k)^q \equiv y^q - \eta_k^q.$$

De plus, η_k est un polynôme de f termes, et lorsqu'on élève un semblable polynôme à la puissance q, les coefficients de tous les termes sont divisibles par q, excepté ceux des termes formés des puissances $q^{tèmes}$ des f termes du polynôme. Par conséquent, on a

$$\eta_k^q \equiv x^{qg^k} + x^{qg^{e+k}} + x^{qg^{2e+k}} + \ldots + x^{qg^{(f-1)e+k}} \pmod{q},$$

et, si l'on suppose

$$q \equiv g^r \pmod{p},$$

il résulte de là, en général,

$$\eta_k^q \equiv \eta_{r+k} \pmod{q},$$

mais, dans le cas particulier où $q = p$,

$$\eta_k^p \equiv f \pmod{p}.$$

La congruence

$$(y-\eta_k)^q \equiv y^q - \eta_k^q \pmod{q}$$

se change donc généralement en

$$(y-\eta_k)^q \equiv y - \eta_{k+r} \pmod{q},$$

et, pour le cas particulier de $q = p$, elle devient

$$(y-\eta_k)^p \equiv y - f \pmod{p}.$$

En donnant successivement à k, dans cette expression, les valeurs

$$0, \quad 1, \quad 2, \ldots, \quad e-1,$$

et faisant le produit, il vient

$$[\varphi(y)]^p \equiv (y-f)^e \pmod{p},$$

d'où il résulte que $\varphi(\gamma)$ contient p en facteur pour $\gamma \equiv f$, mais ne le contient pas pour toute autre valeur de γ; en d'autres termes, la congruence

$$\varphi(\gamma) \equiv 0 \pmod{p}$$

a toujours une racine réelle, savoir

$$\gamma = f = \frac{p-1}{e}.$$

Revenons à la recherche de la valeur générale du facteur premier q pour lequel on a

$$q \equiv g^r \pmod{p}.$$

Au moyen de la congruence

$$(\gamma - \eta_k)^q \equiv \gamma - \eta_{k+r},$$

la congruence (A) se change dans la suivante,

$$(B)\left\{ \begin{array}{c} (\gamma-\eta_k)(\gamma-1-\eta_k)(\gamma-2-\eta_k)\ldots(\gamma-q+1-\eta_k) \\ \equiv \eta_k - \eta_{k+r} \end{array} \right\} \pmod{q}.$$

Il faut distinguer ici deux cas: le premier, lorsque r est divisible par e; le second, lorsqu'il ne l'est pas. Si r est divisible par e, alors $\eta_k = \eta_{k+r}$, et par suite

$$(\gamma-\eta_k)(\gamma-1-\eta_k)(\gamma-2-\eta_k)\ldots(\gamma-q+1-\eta_k) \equiv 0 \pmod{q}.$$

En prenant successivement

$$k = 0, 1, 2, \ldots, e-1,$$

et faisant le produit de toutes ces congruences, il vient

$$\varphi(\gamma)\varphi(\gamma-1)\varphi(\gamma-2)\ldots\varphi(\gamma-q+1) \equiv 0 \pmod{q^e}.$$

Il faut donc que e de ces facteurs soient divisibles par q, ou bien que quelques-uns d'entre eux contiennent plusieurs fois ce facteur q,

toutes les fois que l'on a

$$q \equiv g^r \pmod{p},$$

et que r est divisible par e, c'est-à-dire toutes les fois que q est un résidu de puissance $e^{ième}$ pour le nombre premier. De là on déduit le théorème suivant :

Tout nombre premier qui est un résidu de puissance $e^{ième}$ de p, est un diviseur de la forme $\varphi(\gamma)$; ou, en d'autres termes, la congruence

$$\varphi(\gamma) \equiv 0 \pmod{q},$$

lorsque q est un nombre premier et en même temps un résidu de puissance $e^{ième}$ de p, a toujours e racines réelles, dont plusieurs peuvent devenir égales entre elles dans des cas particuliers.

Le cas particulier où les périodes sont composées chacune d'un seul terme, et où elles sont, par conséquent, égales aux racines imaginaires elles-mêmes de l'équation

$$x^p = 1,$$

donne ce résultat connu, que la congruence

$$x^{p-1} + x^{p-2} + x^{p-3} + \ldots + x + 1 \equiv 0 \pmod{q}$$

à toujours $p - 1$ racines réelles, lorsque le nombre premier q est un résidu de puissance $(p-1)^{ième}$ de p, c'est-à-dire lorsque

$$q = 2mp + 1.$$

Après avoir fait voir que tous les nombres premiers, qui sont des résidus de puissance $e^{ième}$ de p, sont des diviseurs de la forme $\varphi(\gamma)$, il reste en second lieu à examiner si cette forme a encore, ou non, d'autres diviseurs que ceux que nous venons de citer et le diviseur p. Soit donc encore

$$q \equiv g^r \pmod{p},$$

mais supposons r non divisible par e. Dans ce cas, si l'on remplace successivement, dans la congruence (B), k par

$$0, \quad 1, \quad 2, \ldots, \quad e - 1,$$

et que l'on fasse le produit des résultats, il vient

$$\varphi(\gamma)\,\varphi(\gamma-1)\,\varphi(\gamma-2)\ldots\varphi(\gamma-q+1)\equiv \mathrm{P} \pmod{q},$$

en posant

$$\mathrm{P}=(\eta-\eta_r)(\eta_1-\eta_{r+1})(\eta_2-\eta_{r+2})\ldots(\eta_{e-1}-\eta_{r+e-1}).$$

P, étant une fonction symétrique de toutes les périodes, sera un nombre entier. Pour des valeurs déterminées de p et de e, lors même qu'on donne à r toutes les valeurs possibles, ce nombre P ne pourra contenir qu'un nombre fini, déterminé et relativement très-petit de facteurs premiers différents; et comme $\varphi(\gamma)$ ne peut contenir d'autres facteurs premiers différents que ceux qui entrent dans P, il s'ensuit que c'est seulement dans des cas exceptionnels que $\varphi(\gamma)$ pourra contenir un nombre toujours limité de ces facteurs qui ne sont pas des résidus de puissance $e^{ième}$ de p. Pour examiner de plus près dans quels cas ces facteurs premiers exceptionnels peuvent se rencontrer dans P et par suite dans $\varphi(\gamma)$, nous emploierons la congruence

$$(\eta_k-\eta_{r+k})^q\equiv\eta_{k+r}-\eta_{k+2r} \pmod{q},$$

que l'on peut vérifier en jetant un simple coup d'œil sur les principes établis précédemment. En élevant les deux membres de cette congruence plusieurs fois de suite à la puissance q, on obtient la congruence plus générale

$$(\mathrm{C}) \qquad (\eta_k-\eta_{r+k})^{q^h}\equiv\eta_{hr+k}-\eta_{(h+1)r+k} \pmod{q}.$$

Si l'on y fait successivement

$$h=0,\ 1,\ 2,\ \ldots,\ e-1,$$

et que l'on forme le produit, il vient

$$\left.\begin{aligned}&(\eta_k-\eta_{r+k})^{1+q+q^2+\ldots+q^{e-1}}\\ \equiv\ &(\eta_k-\eta_{r+k})(\eta_{r+k}-\eta_{2r+k})\ldots(\eta_{(e-1)r}-\eta_{(e-1)r+k})\end{aligned}\right\}\pmod{q}.$$

Si maintenant r n'a aucun facteur commun avec e, les indices des périodes

$$k,\quad r+k,\quad 2r+k,\ \ldots,\quad (e-1)r+k,$$

pris dans un autre ordre, seront congrus aux indices

$$0, \quad 1, \quad 2, \ldots, \quad e-1,$$

suivant le module e. Le produit qui compose le second membre n'est donc autre chose que le produit P, et comme, par hypothèse, P doit être divisible par q, on a donc

$$(\eta_k - \eta_{k+k})^{1+q+q^2+\ldots+q^{e-1}} \equiv 0 \pmod{q}.$$

En élevant maintenant à la puissance $q-1$, on a

$$(\eta_k - \eta_{r+k})^{q^e-1} \equiv 0 \pmod{q},$$

puis, en multipliant par $\eta_k - \eta_{k+r}$,

$$(\eta_k - \eta_{r+k})^{q^e} \equiv 0 \pmod{q},$$

d'où résulterait, en vertu de la congruence (C),

$$\eta_k - \eta_{r+k} \equiv 0 \pmod{q},$$

ce qui est impossible. Le produit P n'a donc point de facteur premier q tel, que l'on ait

$$q \equiv g^r \pmod{p},$$

r n'ayant aucun facteur commun avec e. Donc, dans le cas où e est un nombre premier, on a le théorème suivant :

La forme $\varphi(y)$, lorsque son degré e est un nombre premier, n'a, outre le diviseur p, que des diviseurs résidus de puissance e par rapport à p.

Mais dans le cas où le degré de la forme $\varphi(y)$ n'est pas un nombre premier, le résultat trouvé peut s'énoncer comme il suit :

La forme $\varphi(y)$ n'a en général, outre le diviseur p, pour diviseurs que des nombres premiers, résidus de puissance e par rapport à p; mais elle peut, en outre, avoir encore un nombre fini et déterminé d'autres diviseurs, lesquels doivent être, par rapport à p, des résidus

de quelqu'une des puissances α, β, γ,..., *en désignant par* α, β, γ,..., *les diviseurs e autres que l'unité.*

On peut indiquer d'une manière encore plus précise les conditions pour que $\varphi(\gamma)$ contienne des diviseurs spéciaux, qui ne soient pas résidus de puissance $e^{ième}$. Soit, en effet, α le plus grand diviseur commun de r et de e, et

$$r = r'\alpha, \quad e = e'\alpha;$$

dans la congruence (C) faisons successivement

$$h = 0, 1, 2, \ldots, e' - 1,$$

et multiplions entre elles les congruences ainsi obtenues; il viendra

$$(\eta_k - \eta_{r+k})^{1+q+q^2+\ldots+q^{e'-1}} \equiv (\eta_k - \eta_{r+k})(\eta_{r+k} - \eta_{2r+k})\ldots(\eta_{(e'-1)r+k} - \eta_{e,r+k}).$$

En donnant ensuite à k les valeurs

$$0, \quad 1, \quad 2, \ldots, \quad \alpha - 1,$$

et faisant la multiplication, le produit dans le second membre devient égal à P, comme on peut s'en convaincre immédiatement, en remarquant que les nombres de la forme $hr + k$, pour

$$h = 0, 1, 2, \ldots, e' - 1, \quad k = 0, 1, 2, \ldots, \alpha - 1,$$
$$r = r'\alpha, \qquad\qquad e = e'\alpha,$$

donnent, relativement au module e, tous les restes

$$0, \quad 1, \quad 2, \ldots, \quad e - 1.$$

On a donc, P devant être divisible par q,

$$[(\eta - \eta_r)(\eta_1 - \eta_{r+1})\ldots(\eta_{\alpha-1} - \eta_{\alpha+r-1})]^{1+q+q^2+\ldots+q^{e'-1}} \equiv 0 \pmod{q}$$

En élevant encore à la puissance $q - 1$, et multipliant par

$$(\eta - \eta_r)(\eta_1 - \eta_{r+1})\ldots(\eta_{\alpha-1} - \eta_{\alpha+r-1}),$$

il vient

$$[(\eta - \eta_r)(\eta_1 - \eta_{r+1})\dots(\eta_{\alpha-1} - \eta_{\alpha+r-1})]^{q^e} \equiv 0 \pmod{q},$$

relation qui, en vertu de la congruence (C), peut se mettre sous la forme plus simple

$$(\eta - \eta_r)(\eta_1 - \eta_{r+1})\dots(\eta_{\alpha-1} - \eta_{\alpha+r-1}) \equiv 0 \pmod{q}.$$

Il faut donc déjà que le produit des α premiers facteurs du produit P contienne le facteur q, pour que P ou $\varphi(y)$ puissent le contenir. Cette condition restrictive pourrait faire soupçonner que ces facteurs exceptionnels, qui ne sont pas résidus de puissance e, pourraient bien ne pas exister non plus dans le cas où e est un nombre composé. Mais on peut s'assurer, sur un exemple simple, qu'il n'en est pas ainsi, et qu'il existe réellement de tels facteurs. Prenons

$$p = 109, \quad e = 6.$$

On a, par les méthodes connues,

$$\varphi(y) = y^6 + y^5 - 45y^4 - 10y^3 + 135y^2 + 9y - 27,$$

d'où il est facile de tirer, pour

$$y = 0, 1, 2, 3, 4, 5,$$

les valeurs suivantes de $\varphi(y)$,

$$\varphi(0) = -3^3, \qquad \varphi(1) = 2^6, \qquad \varphi(2) = -173,$$
$$\varphi(3) = -2^6.3^3, \quad \varphi(4) = -4871, \quad \varphi(5) = -2^6.113.$$

Les diviseurs 2 et 3, qui se rencontrent dans ces valeurs, ne sont pas des résidus de puissance 6e de 109; ce sont donc des diviseurs tels que ceux que nous avons signalés. 2 est un résidu cubique, et 3 un résidu quadratique de 109, ce qui est parfaitement d'accord avec le théorème précédent. D'ailleurs, dans le cas actuel, 2 et 3 sont les seuls facteurs premiers de $\varphi(y)$ qui ne soient pas résidus de puissance 6e.

Nous allons considérer encore deux cas particuliers importants, pour lesquels nous ferons voir qu'il ne peut jamais exister de facteurs qui ne soient pas résidus de puissance $e^{ième}$ par rapport à p: ces cas sont celui où la période n'a qu'un terme, et celui où elle en a deux. Si l'on a

$$e = p - 1 \quad \text{et} \quad f = 1,$$

alors

$$\eta = x, \quad \eta_1 = x^g, \quad \eta_2 = x^{g^2}, \ldots;$$

par conséquent,

$$\mathrm{P} = (x - x^g)(x^g - x^{g^2}) \ldots (x^{g^{p-2}} - x^{g^{p-1}})$$

et, en détachant du premier facteur x, du second x^g, du troisième $x^{g^2}, \ldots$, il vient

$$\mathrm{P} = (1 - x^{g-1})(1 - x^{g(g-1)}) \ldots (1 - x^{g^{p-2}(g-1)}).$$

Puisque l'on a maintenant

$$(z - x^m)(z - x^{mg}) \ldots (z - x^{m \cdot g^{p-2}}) = z^{p-1} + z^{p-2} + \ldots + z + 1,$$

il viendra, en faisant $z = 1$, $m = g - 1$,

$$\mathrm{P} = p.$$

P ne contenant pas d'autre facteur que p, il en résulte la proposition connue que $y^{p-1} + y^{p-2} + \ldots + y + 1$ ne peut contenir, outre le diviseur p, que des facteurs résidus de puissance $(p-1)^{ième}$ par rapport à p, et représentés par conséquent par la forme linéaire

$$q = 2mp + 1.$$

Si maintenant les périodes sont à deux termes, c'est-à-dire si l'on a

$$e = \tfrac{1}{2}(p - 1), \quad f = 2,$$

alors

$$\eta = x + x^{-1}, \quad \eta_1 = x^g + x^{-g}, \quad \eta_2 = x^{g^2} + x^{-g^2}, \ldots,$$

et l'on sait que, dans ce cas,

$$\varphi(y) = y^e + y^{e-1} - \frac{e-1}{1} y^{e-2} - \frac{e-2}{1} y^{e-3} + \frac{(e-2)(e-3)}{1 \cdot 2} y^{e-4} + \frac{(e-3)(e-4)}{1 \cdot 2} y^{e-5} - \ldots.$$

De plus, on a

$$\eta_k - \eta_{r+k} = x^{g^k} + x^{-g^k} - x^{g^{r+k}} - x^{-g^{r+k}},$$

expression qui se décompose en facteurs de la manière suivante,

$$\eta_r - \eta_{r+k} = x^{g^k}\left(1 - x^{(g^r-1)g^k}\right)\left(1 - x^{-(g^r+1)g^k}\right).$$

En donnant maintenant à k les valeurs

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

et faisant le produit, on trouve facilement

$$P^2 = p^2,$$

d'où

$$P = \pm p.$$

Donc, dans ce cas encore, P n'a pas d'autre diviseur que p; d'où il résulte que la forme

$$\varphi(y) = y^e + y^{e-1} - \frac{e-1}{1} y^{e-2} - \frac{e-2}{1} y^{e-3} + \ldots$$

n'a, outre le diviseur p, que des diviseurs résidus de puissance $\left(\frac{p-1}{2}\right)^{ième}$ par rapport à p, lesquels sont par suite de la forme

$$2mp \pm 1,$$

La méthode que nous avons appliquée, dans ce qui précède, à la forme $\varphi(y)$, donne presque de la même manière les facteurs premiers d'une forme, beaucoup plus générale et très-remarquable, du degré e avec e indéterminées. En effet, si l'on multiplie entre elles les fonctions linéaires suivantes des périodes,

$$\begin{aligned}
F(\eta) &= z\eta + z_1\eta_1 + z_2\eta_2 + \ldots + z_{e-1}\eta_{e-1},\\
F(\eta_1) &= z\eta_1 + z_1\eta_2 + z_2\eta_3 + \ldots + z_{e-1}\eta,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
F(\eta_{e-1}) &= z\eta_{e-1} + z_1\eta + z_2\eta_1 + \ldots + z_{e-1}\eta_{e-2},
\end{aligned}$$

leur produit

$$\Psi = F(\eta)F(\eta_1)F(\eta_2)\ldots F(\eta_{e-1})$$

sera une fonction homogène, de degré e et à coefficients entiers, des e indéterminées

$$z,\quad z_1,\quad z_2,\ldots,\quad z_{e-1}.$$

Cette forme, comme nous allons le faire voir, présente, relativement à ses diviseurs, une analogie complète avec la forme moins générale $\varphi(y)$ que nous venons d'étudier. Nous démontrerons d'abord le théorème suivant :

Tout nombre premier q, résidu de puissance $e^{ième}$ de p, est, ainsi que p lui-même, un diviseur de la forme Ψ.

Considérons d'abord le diviseur p. On a, d'après les principes dont on a fait précédemment usage,

$$F(\eta_k)^p \equiv (z + z_1 + z_2 + \ldots + z_{e-1})f \pmod{p};$$

si donc on choisit les indéterminées $z, z_1, z_2,\ldots, z_{e-1}$ de telle sorte que leur somme soit divisible par p, on aura alors

$$F(\eta_k)^p \equiv 0 \pmod{p};$$

et en faisant successivement

$$k = 0,\ 1,\ 2,\ldots,\ e-1,$$

et multipliant entre elles les congruences résultantes, il vient

$$\Psi^p \equiv o \pmod{p},$$

et par suite aussi

$$\Psi \equiv o \pmod{p};$$

p est donc un diviseur de la forme Ψ.

Pour démontrer ensuite que tout nombre premier q, résidu de puissance $e^{ième}$ par rapport à p, est toujours aussi un diviseur de Ψ, je suppose la seconde période η_1 mise sous la forme d'une fonction rationnelle et entière de la première période η, ce qui, comme on sait, est toujours possible. Soit donc

$$\eta_1 = \Theta(\eta);$$

alors on aura

$$\eta_2 = \Theta\Theta(\eta), \qquad \eta_3 = \Theta\Theta\Theta(\eta), \ldots$$

Prenons, au lieu de η, une quantité indéterminée y, et formons l'expression

$$F(y).F(\Theta y).F(\Theta\Theta y)\ldots F[\Theta^{(e-i)}y] - \Psi,$$

laquelle sera une fonction rationnelle et entière de y. Cette expression s'annule évidemment si l'on y fait $y = \eta$, ou $y = \eta_1$, ou $y = \eta_2, \ldots$; elle doit donc contenir le facteur

$$(y-\eta)(y-\eta_1)(y-\eta_2)\ldots(y-\eta_{e-1}),$$

que nous avons désigné ci-dessus par $\varphi(y)$. On a, par conséquent,

$$F(y).F(\Theta y).F(\Theta\Theta y)\ldots F[\Theta^{(e-1)}y] - \Psi = \varphi(y).\Phi,$$

Φ désignant encore une fonction rationnelle et entière de y. Si l'on prend maintenant pour y une racine quelconque de la congruence

$$\varphi(y) \equiv o \pmod{q}$$

(laquelle a toujours e racines réelles, comme nous l'avons prouvé lors-

que q est un résidu de puissance $e^{ième}$ par rapport à p), on aura

$$F(\gamma).F(\Theta\gamma).F(\Theta\Theta\gamma)\ldots F[\Theta^{(e-1)}\gamma]\equiv\Psi \pmod{q}.$$

Si donc un facteur quelconque de ce produit devient divisible par q, Ψ deviendra également divisible par q. On peut donc toujours choisir les indéterminées

$$z,\quad z_1,\quad z_2,\ldots,\quad z_{e-1}$$

de telle manière que la forme Ψ admette le diviseur q, et la condition qui nous sert à fixer ces valeurs est simplement que, si dans l'expression

$$F(\eta)=z\eta+z_1\eta_1+z_2\eta_2+\ldots+z_{e-1}\eta_{e-1},$$

on remplace η, η_1, $\eta_2,\ldots,\eta_{e-1}$, non plus par les racines de l'équation

$$\varphi(\gamma)=0,$$

mais par les racines de la congruence

$$\varphi(\gamma)\equiv 0 \pmod{q},$$

prises dans un ordre convenable, on doit avoir

$$F(\eta)\equiv 0 \pmod{q}.$$

Les facteurs premiers, résidus de puissance $e^{ième}$ par rapport à p, forment encore ici les diviseurs les plus importants de la forme Ψ, et ce n'est qu'exceptionnellement qu'il peut, outre ceux-là, en exister certains autres, dont nous allons étudier de plus près les conditions d'existence. Soit q un nombre premier tel que l'on ait

$$q\equiv g^r \pmod{p},$$

r n'étant pas divisible par e. On a alors

$$F(\eta)^q\equiv F(\eta_r) \pmod{q}.$$

Élevons cette congruence plusieurs fois de suite à la puissance q, ce

qui donne

$$F(\eta)^{q^h} \equiv F(\eta_{hr}) \pmod{q}.$$

Faisant successivement

$$h = 0,\ 1,\ 2,\ 3, \ldots,\ e-1,$$

et multipliant entre elles les congruences ainsi obtenues, il vient

$$F(\eta)^{1+q+q^2+\ldots+q^{e-1}} \equiv F(\eta)\,(\eta_r)\,F(\eta_{2r}) \ldots F(\eta_{(e-1)r}) \pmod{q}.$$

Si maintenant r et e n'ont aucun facteur commun, les indices

$$0,\quad r,\quad 2r,\quad 3r, \ldots,\quad (e-1)r$$

seront congrus suivant le module e avec les indices

$$0,\quad 1,\quad 2, \ldots,\quad e-1,$$

pris dans un autre ordre; donc le produit du second membre est égal à Ψ. Or Ψ devant admettre le diviseur q, il s'ensuit que l'on doit avoir

$$F(\eta)^{1+q+q^2+\ldots+q^{e-1}} \equiv 0 \pmod{q},$$

d'où résulte, comme précédemment,

$$F(\eta) \equiv 0 \pmod{q}.$$

Mais, pour que $F(\eta)$ soit divisible par q, il faut que chacun des coefficients des périodes, et par suite que les indéterminées

$$z,\quad z_1,\quad z_2, \ldots,\quad z_{e-1}$$

soient toutes divisibles par q. De là nous concluons le théorème suivant :

S'il n'existe pas de facteurs communs à toutes les indéterminées de la forme Ψ, cette forme n'admettra pour facteurs premiers, outre le diviseur p, que des résidus de puissance e par rapport à p; en d'autres termes, si e contient les diviseurs $\alpha, \beta, \gamma, \ldots$, différents de l'unité, la

forme pourra aussi contenir des facteurs premiers, résidus de puissance α, *ou* β, *ou* $\gamma, \ldots$ *par rapport à* p.

On en déduit encore, comme corollaire, que *s'il n'existe pas de facteur commun à toutes les indéterminées de la forme* Ψ, *et que le degré* e *de cette forme soit un nombre premier, alors cette forme n'admettra, outre le diviseur* p, *que des diviseurs résidus de puissance* e *par rapport à* p.

Si e n'est pas un nombre premier et que α soit un diviseur de e, soit

$$q \equiv g^r \pmod{p},$$

et α le plus grand diviseur commun de r et de e, de sorte que l'on ait

$$r = r'\alpha, \quad e = e'\alpha.$$

En vertu de la congruence

$$F(\eta_k)^{q^h} \equiv F(\eta_{rh+k}) \pmod{q},$$

où l'on fera successivement

$$h = 0, 1, 2, \ldots, e' - 1,$$

et où l'on donnera ensuite à k les valeurs

$$0, \quad 1, \quad 2, \ldots, \quad \alpha - 1,$$

il viendra, dans ce cas,

$$[F(\eta)\,F(\eta_1)\,F(\eta_2)\ldots F(\eta_{\alpha-1})]^{1+q+q^2+\ldots+q^{e'-1}} \equiv \Psi \pmod{q};$$

car le produit des seconds membres est évidemment égal à Ψ, puisque, pour les valeurs en question de h et de k, l'expression $hr + k$ devient congrue suivant le module e à tous les nombres

$$0, \quad 1, \quad 2, \ldots, \quad e - 1.$$

Si Ψ doit admettre maintenant pour facteur q, il s'ensuivra que l'on

devra avoir

$$[F(\eta)F(\eta_1)\dots F(\eta_{\alpha-1})]^{1+q+q^2+\dots+q^{e'-1}} \equiv 0 \pmod{q},$$

d'où l'on conclut aisément qu'il faudra aussi que l'on ait

$$F(\eta)F(\eta_1)F(\eta_2)\dots F(\eta_{\alpha-1}) \equiv 0 \pmod{q}.$$

Donc, pour que Ψ admette un facteur premier q qui ne soit pas résidu de puissance e, mais seulement résidu de puissance α par rapport à p, α étant un diviseur de e, il faudra toujours que ce facteur q divise le produit des α premiers facteurs de Ψ.