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

J.-A. SERRET

Sur les fonctions entières irréductibles suivant un module premier, dans le cas où le degré est une puissance du module

Journal de mathématiques pures et appliquées 2^e série, tome 18 (1873), p. 437-451.
<http://www.numdam.org/item?id=JMPA_1873_2_18__437_0>

Sur les fonctions entières irréductibles suivant un module premier, dans le cas où le degré est une puissance du module;

PAR M. J.-A. SERRET.

---

1. Dans un précédent Article (*voir* p. 301 de ce volume), j'ai fait connaître le mode de formation des fonctions entières irréductibles suivant un module premier, et dont le degré est précisément égal au module. Je me propose d'examiner ici le cas plus général des fonctions entières irréductibles, dont le degré est égal à une puissance quelconque du module premier p.

Posons, comme dans l'article cité,

$$(1)\quad \begin{cases} X_\mu \equiv x^{p^\mu} - \dfrac{\mu}{1} x^{p^{\mu-1}} + \ldots + (-1)^k \dfrac{\mu(\mu-1)\ldots(\mu-k+1)}{1.2\ldots k} x^{p^{\mu-k}} + \ldots \\ \qquad + (-1)^{\mu-1} \dfrac{\mu}{1} x^p + (-1)^\mu x \pmod p, \end{cases}$$

formule de laquelle résulte la congruence

$$(2)\qquad X_{\mu+1} \equiv X_\mu^p - X_\mu \pmod p.$$

La formule (1) peut s'écrire *symboliquement* de la manière suivante :

$$X_\mu \equiv (\xi - 1)^\mu \pmod p,$$

en convenant que, après avoir effectué l'opération indiquée dans le second membre, on remplacera chaque puissance $\xi^{\mu-k}$ de ξ par $x^{p^{\mu-k}}$.

Alors, si l'indice μ est divisible par une puissance de p, et que l'on fasse

$$\mu = \nu p^m,$$

on aura symboliquement

$$X_{\nu p^m} \equiv (\xi - 1)^{\nu p^m} \equiv \left[(\xi - 1)^{p^m}\right]^\nu \equiv (\xi^{p^m} - 1)^\nu \pmod{p},$$

c'est-à-dire

$$(3)\quad \begin{cases} X_{\nu p^m} \equiv x^{p^\nu p^m} - \frac{\nu}{1} x^{p^{(\nu-1)p^m}} + \ldots + (-1)^k \frac{\nu(\nu-1)\ldots(\nu-k+1)}{1.2\ldots k} x^{p^{(\nu-k)p^m}} + \ldots \\ \qquad + (-1)^{\nu-1} \frac{\nu}{1} x^{p^{p^m}} + (-1)^\nu x \pmod{p}; \end{cases}$$

dans le cas de $\nu = 1$, on a

$$(4)\qquad X_{p^m} \equiv x^{p^{p^m}} - x \pmod{p}.$$

La formule (2) exprime que X_μ se change en $X_{\mu+1}$ quand on change x en $x^p - x$, c'est-à-dire en X_1; d'ailleurs la même formule se réduit, pour $\mu = 0$, à

$$X_1 = X_0^p - X_0,$$

ce qui montre qu'on doit regarder X_0 comme étant égal à x. Il résulte de là que, pour exécuter ρ fois de suite dans les formules (1) et (3) le changement de x en $x^p - x$, il suffit d'ajouter ρ unités aux indices des fonctions X qui y figurent. La formule (3) devient ainsi

$$(5)\quad \begin{cases} X_{\nu p^m + \rho} \equiv X_\rho^{p^\nu p^m} - \frac{\nu}{1} X_\rho^{p^{(\nu-1)p^m}} + \ldots + (-1)^k \frac{\nu(\nu-1)\ldots(\nu-k+1)}{1.2\ldots k} X_\rho^{p^{(\nu-k)p^m}} + \ldots \\ \qquad + (-1)^{\nu-1} \frac{\nu}{1} X_\rho^{p^{p^m}} + (-1)^\nu X_\rho \pmod{p}. \end{cases}$$

2. Je désignerai généralement par V_n le produit de toutes les fonctions entières de degré p^n, irréductibles suivant le module p. D'après

la formule (4), ce produit est égal au quotient des deux fonctions X_{p^n}, $X_{p^{n-1}}$; ainsi l'on a

$$X_{p^n} \equiv X_{p^{n-1}} V_n \pmod{p}. \tag{6}$$

Ensuite la formule (2) donne

$$\left.\begin{aligned} X_{\mu+1} &\equiv X_\mu^p - X_\mu, \\ X_{\mu+2} &\equiv X_{\mu+1}^p - X_{\mu+1}, \\ &\cdots\cdots\cdots\cdots\cdots, \\ X_{\mu+\nu} &\equiv X_{\mu+\nu-1}^p - X_{\mu+\nu-1} \end{aligned}\right\} \pmod{p};$$

multipliant ces congruences entre elles et divisant la formule résultante par le produit $X_{\mu+1} X_{\mu+2} \ldots X_{\mu+\nu-1}$, il vient

$$X_{\mu+\nu} \equiv X_\mu (X_\mu^{p-1} - 1)(X_{\mu+1}^{p-1} - 1) \ldots (X_{\mu+\nu-1}^{p-1} - 1) \pmod{p}. \tag{7}$$

Faisons

$$\mu = p^{n-1}, \quad \mu + \nu = p^n,$$

il viendra, à cause de la formule (6),

$$V_n \equiv (X_{p^{n-1}}^{p-1} - 1)(X_{p^{n-1}+1}^{p-1} - 1)(X_{p^{n-1}+2}^{p-1} - 1) \ldots (X_{p^n-1}^{p-1} - 1) \pmod{p}. \tag{8}$$

Chacun des facteurs $X_{p^{n-1}+\lambda-1}^{p-1} - 1$ du second membre de la formule (8) se décompose en $p-1$ facteurs $X_{p^{n-1}+\lambda-1} - g$ où g a les valeurs $1, 2, \ldots, p-1$, et cette dernière fonction est elle-même le produit de $p^{p^{n-1}+\lambda-n-1}$ facteurs irréductibles du degré p^n.

Il y a lieu de distinguer en plusieurs genres les fonctions entières irréductibles de degré p^n, ainsi que je l'ai fait déjà dans le cas particulier de $n=1$. Je nommerai fonctions du $\lambda^{ième}$ genre celles dont $X_{p^{n-1}+\lambda-1}^{p-1} - 1$ est le produit, λ ayant les valeurs

$$1, 2, 3, \ldots, (p-1)p^{n-1},$$

et le dernier genre, celui qui répond à $\lambda = (p-1)p^{n-1}$, sera dit le *genre principal*.

Si l'on exécute le changement de x en $x^p - x$, dans le second

membre de la formule (8), chacun des $p^n - p^{n-1} - 1$ premiers facteurs entre parenthèses se changera dans le facteur suivant, d'après ce qui a été dit plus haut. Quant au dernier facteur $X_{p^{n-1}}^{p-1} - 1$, qui est le produit des fonctions irréductibles du genre principal, il se changera en $X_{p^n}^{p-1} - 1$, ce qui est le premier facteur de V_{n+1}, c'est-à-dire le produit des fonctions entières irréductibles du degré p^{n+1} et du premier genre. De cette considération résulte immédiatement le théorème suivant :

THÉORÈME. — *Soit* $F(x)$ *une fonction entière du degré* p^n, *irréductible suivant le module premier* p. *Si cette fonction appartient au* $\lambda^{ième}$ *genre supposé non principal, la fonction* $F(x^p - x)$ *ou* $F(X_1)$ *sera réductible, et elle se décomposera en* p *facteurs du degré* p^n, *irréductibles suivant le module* p *et appartenant au* $(\lambda + 1)^{ième}$ *genre. Mais, si la fonction* $F(x)$ *de degré* p^n *appartient au genre principal, la fonction* $F(x^p - x)$ *sera elle-même irréductible suivant le module* p, *et elle appartiendra au premier genre des fonctions de degré* p^{n+1}.

3. Considérons d'abord les fonctions entières irréductibles de degré p^n et du premier genre. Le produit de ces fonctions est

$$X_{p^{n-1}}^{p-1} - 1 \equiv \Pi(X_{p^{n-1}} - g) \pmod{p},$$

le signe de produit Π s'étendant aux valeurs $1, 2, \ldots, (p-1)$ de g. Le facteur $X_{p^{n-1}} - g$ est ce que devient $X_{p^{n-1}} - 1$ quand on y remplace x par $\frac{x}{g}$ et qu'on multiplie le résultat par g ; il s'ensuit que la recherche des fonctions entières irréductibles du premier genre est ramenée à la décomposition en facteurs de la seule expression

$$X_{p^{n-1}} - 1 \equiv x^{p^{p^{n-1}}} - x - 1 \pmod{p}. \tag{9}$$

Soient $F(x)$ l'un des facteurs irréductibles de la fonction (9) et i_n une racine de la congruence

$$F(x) \equiv 0 \pmod{p}. \tag{10}$$

La racine i_n appartiendra aussi à la congruence

$$X_{p^{n-1}} - 1 \equiv 0 \pmod{p}, \tag{11}$$

et l'on aura en conséquence

$$i_n^{p^{p^{n-1}}} - i_n \equiv 1 \pmod{p}. \tag{12}$$

En tenant compte de la formule (12), la congruence (11) peut s'écrire de la manière suivante :

$$(x - i_n)^{p^{p^{n-1}}} - (x - i_n) \equiv 0 \pmod{p},$$

et, par conséquent, les $p^{p^{n-1}}$ racines de cette congruence seront données par la formule

$$x \equiv i_n + f(i_{n-1}) \pmod{p}, \tag{13}$$

dans laquelle i_{n-1} désigne une racine d'une congruence irréductible quelconque de degré p^{n-1}, et f une fonction entière du degré $p^{n-1} - 1$, dont les coefficients peuvent avoir les valeurs 0, 1, 2, ..., $(p-1)$.

Parmi les valeurs de x comprises dans la formule (13), figurent les p^n racines de la congruence (10), et comme, d'après la théorie des congruences, l'une de ces racines est i_n^p, on aura

$$i_n^p - i_n \equiv f(i_{n-1}) \pmod{p}, \tag{14}$$

la fonction f devant être ici convenablement choisie. La formule (14) permet d'éliminer des expressions qui les contiennent les puissances de i_n au delà de la $(p-1)^{ième}$, en introduisant les diverses puissances de i_{n-1}.

De là on peut conclure que, si l'on désigne par

$$i_1, i_2, i_3, \ldots, i_n$$

des racines de congruences irréductibles suivant le module p, dont les premiers membres soient des diviseurs des fonctions respectives

$$X_1 - 1, \quad X_p - 1, \quad X_{p^2} - 1, \ldots, \quad X_{p^{n-1}} - 1,$$

on aura

$$\left\{\begin{array}{l} i_1^p - i_1 \equiv 1, \\ i_2^p - i_2 \equiv P_1, \\ i_3^p - i_3 \equiv P_2, \\ \ldots\ldots\ldots, \\ i_n^p - i_n \equiv P_{n-1} \end{array}\right\} \pmod{p}, \tag{15}$$

P_μ étant une fonction entière des racines $i_1, i_2, \ldots, i_\mu$, qui ne renferme aucune puissance de ces racines supérieure à la $(p-1)^{ième}$.

Il reste à connaître la condition que doivent remplir les fonctions P_μ pour que les valeurs de $i_1, i_2, \ldots, i_n$, définies par les formules (15), satisfassent effectivement aux congruences respectives

$$(16)\quad X_1 - 1 \equiv 0,\ X_p - 1 \equiv 0,\ X_{p_2} - 1 \equiv 0, \ldots,\ X_{p^{n-1}} - 1 \equiv 0 \pmod{p}.$$

Pour remplir cet objet, nous aurons à nous appuyer sur un lemme que nous allons d'abord établir.

4. LEMME. — *Soit*

$$f(\zeta) = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_\nu\zeta^\nu$$

une fonction entière du degré $\nu < p$, *d'une quantité* ζ *racine de la congruence*

$$\zeta^{p^{p^m}} - \zeta \equiv 1 \pmod{p},$$

et dont les coefficients a, *réels ou imaginaires, satisfont tous à la congruence*

$$a^{p^{p^m}} - a \equiv 0 \pmod{p};$$

si l'on attribue à X_ρ *la valeur* $f(\zeta)$, *on aura*

$$X_{\nu p^m + \rho} \equiv 1.2\ldots\nu.a_\nu \pmod{p}.$$

La démonstration de ce lemme se déduit très-facilement de la formule (5), qui donne l'expression de $X_{\nu p^m+\rho}$ en fonction de X_ρ. Pour élever $f(\zeta)$ à la puissance $p^{(\nu-k)p^m}$, il faut répéter $\nu - k$ fois l'opération de l'élévation à la puissance p^{p^m}; or, d'après l'énoncé du lemme, cette opération change ζ en $\zeta + 1$ et elle laisse invariables les coefficients a; donc l'hypothèse $X_\rho = f(\zeta)$ entraîne

$$X_\rho^{p^{(\nu-k)p^m}} \equiv f(\zeta + \nu - k) \pmod{p},$$

et, à cause de la formule (5),

$$X_{\nu p^m+\rho} \equiv f(\zeta+\nu) - \frac{\nu}{1} f(\zeta+\nu-1) + \frac{\nu(\nu-1)}{1.2} f(\zeta+\nu-2) + \dots + (-1)^{\nu-1} \frac{\nu}{1} f(\zeta+1) + (-1)^{\nu} f(\zeta) \pmod{p}.$$

Le second membre de cette congruence est la différence $\nu^{ième}$ de la fonction $f(\zeta)$ relative à la différence constante 1 attribuée à ζ; il a donc pour valeur

$$1.2.\dots.\nu.a_\nu,$$

ce qui démontre la proposition énoncée.

Comme le produit $1.2.3\dots(p-1)$ est congru à -1, suivant le module p, on déduit de ce qui précède le corollaire suivant, relatif au cas de $\nu = p-1$.

COROLLAIRE. — *Si l'on attribue à* X_ρ *une valeur représentée par une fonction entière* $f(\zeta)$ *du degré* $p-1$, *d'une racine* ζ *de la congruence* $\zeta^{p^{p^m}} - \zeta \equiv 1 \pmod{p}$, *dont les coefficients a satisfassent à la congruence* $a^{p^{p^m}} - a \equiv 0 \pmod{p}$, *la fonction* $X_{p^{m+1}-p^m+\rho}$ *prendra une valeur congrue au coefficient changé de signe de la puissance* ζ^{p-1} *dans* $f(\zeta)$.

5. Revenons maintenant aux formules (15). Supposons les fonctions

$$P_1, P_2, \dots, P_{n-2},$$

telles que $i_1, i_2, \dots, i_{n-1}$ soient respectivement racines des $n-1$ premières congruences (16), et cherchons dans quel cas la valeur de i_n, définie par la dernière des formules (15), est racine de la dernière des congruences (16). Il est évident que cela revient à chercher dans quel cas la congruence

$$X_1 \equiv P_{n-1} \pmod{p}$$

entraîne

$$X_{p^{n-1}} \equiv 1 \pmod{p}.$$

Désignons par $P^{(1)}_{n-1}$ le coefficient de i_{n-1}^{p-1} dans P_{n-1}, par $P^{(2)}_{n-1}$ le coefficient de i_{n-2}^{p-1} dans $P^{(1)}_{n-1}$, par $P^{(3)}_{n-1}$ le coefficient de i_{n-3}^{p-1} dans $P^{(2)}_{n-1}$, et ainsi de suite; le coefficient $P^{(n-1)}_{n-1}$ de i_1 dans $P^{(n-2)}_{n-1}$ sera un nombre entier.

Cela posé, le corollaire du lemme du n° 4 est applicable successivement dans les $n-1$ hypothèses suivantes :

$$\begin{array}{llll}
m = n-2, & \rho = 1, & \zeta = i_{n-1}, & f(\zeta) = +P_{n-1}, \\
m = n-3, & \rho = p^{n-1} - p^{n-2} + 1, & \zeta = i_{n-2}, & f(\zeta) = -P^{(1)}_{n-1}, \\
m = n-4, & \rho = p^{n-1} - p^{n-3} + 1, & \zeta = i_{n-3}, & f(\zeta) = +P^{(2)}_{n-1}, \\
m = n-5, & \rho = p^{n-1} - p^{n-4} + 1, & \zeta = i_{n-4}, & f(\zeta) = -P^{(3)}_{n-1}, \\
\dots\dots\dots, & \dots\dots\dots\dots\dots, & \dots\dots\dots, & \dots\dots\dots\dots\dots, \\
m = 0, & \rho = p^{n-1} - p + 1, & \zeta = i_1, & f(\zeta) = (-1)^{n-2} P^{(n-2)}_{n-1}.
\end{array}$$

Effectivement les conditions de ce corollaire, savoir :

$$\zeta^{p^{p^m}} - \zeta \equiv 1, \quad a^{p^{p^m}} - a \equiv 0 \pmod{p},$$

sont remplies dans chacune de nos $n-1$ hypothèses; donc la congruence

$$X_1 \equiv P_{n-1} \pmod{p}$$

entraînera successivement les suivantes :

$$\left.\begin{array}{ll}
X_{p^{n-1}-p^{n-2}+1} & \equiv -P^{(1)}_{n-1}, \\
X_{p^{n-1}-p^{n-3}+1} & \equiv +P^{(2)}_{n-1}, \\
X_{p^{n-1}-p^{n-4}+1} & \equiv -P^{(3)}_{n-1}, \\
\dots\dots\dots\dots\dots, & \\
X_{p^{n-1}-p+1} & \equiv (-1)^{n-2} P^{(n-2)}_{n-1}, \\
X_{p^{n-1}} & \equiv (-1)^{n-1} P^{(n-1)}_{n-1}
\end{array}\right\} \pmod{p},$$

et, par conséquent, pour avoir $X_{p^{n-1}} \equiv 1 \pmod{p}$, il faut et il suffit que

$$P^{(n-1)}_{n-1} \equiv (-1)^{n-1} \pmod{p},$$

c'est-à-dire que P_{n-1} contienne le terme $i_1^{p-1} i_2^{p-1} \dots i_{n-1}^{p-1}$ avec le coefficient $(-1)^{n-1}$.

De là nous pouvons tirer la conclusion suivante :

Pour que les quantités $i_1, i_2, \ldots, i_n$, *définies par les formules* (15), *soient respectivement racines des congruences* (16), *il faut et il suffit que chaque fonction* P_μ *contienne le terme* $i_1^{p-1} i_2^{p-1} \ldots i_\mu^{p-1}$ *avec le coefficient* $(-1)^\mu$.

6. Il est facile maintenant d'établir une règle générale pour former les fonctions entières irréductibles du degré p^n et du premier genre.

La congruence irréductible de laquelle i_n dépend résulte de l'élimination de $i_1, i_2, \ldots, i_{n-1}$ entre les congruences (15). Cette quantité i_n étant l'une quelconque des racines de la congruence (11), si l'on désigne par g un entier quelconque, le produit gi_n représentera une racine d'une congruence irréductible quelconque du degré p^n et du premier genre. Faisant donc $gi_n = x$, la dernière des congruences (15) deviendra

$$X_1 \equiv P_{n-1} \pmod{p}, \tag{17}$$

P_{n-1} désignant ici une fonction entière de $i_1, i_2, \ldots, i_{n-1}$, du degré $p-1$ par rapport à chacune de ces quantités, et dans laquelle le coefficient de $i_1^{p-1} i_2^{p-1} \ldots i_{n-1}^{p-1}$ est un entier quelconque autre que zéro.

D'un autre côté, on peut remplacer les racines $i_1, i_2, \ldots, i_{n-1}$, qu'il faut éliminer de la formule (17), par $\frac{i_1}{g_1}, \frac{i_2}{g_2}, \ldots, \frac{i_{n-1}}{g_{n-1}}$, $g_1, g_2, \ldots, g_{n-1}$ étant des nombres entiers, et il est évident que cela revient à substituer aux $n-1$ premières congruences (15) les suivantes :

$$\left.\begin{array}{l} i_1^p - i_1 \equiv P_0, \\ i_2^p - i_2 \equiv P_1, \\ \ldots\ldots\ldots\ldots, \\ i_{n-1}^p - i_{n-1} \equiv P_{n-2} \end{array}\right\} \pmod{p}, \tag{18}$$

où P_0 est un entier autre que zéro, et où P_μ n'est assujetti, généralement, qu'à la seule condition de renfermer le terme $i_1^{p-1} i_2^{p-1} \ldots i_\mu^{p-1}$ avec un coefficient différent de zéro.

Si l'on représente par

$$F_n(X_1) \equiv 0 \pmod{p}$$

le résultat de l'élimination de $i_1, i_2, \ldots, i_{n-1}$ entre les congruences (17) et (18), $F_n(X_1)$ ou $F_n(x^p - x)$ sera l'expression générale des fonctions entières, irréductibles, suivant le module p, du degré p^n et du premier genre.

On peut, sans diminuer la généralité du résultat, attribuer telles valeurs que l'on voudra aux coefficients des congruences (18), en excluant toutefois la valeur zéro pour le coefficient de $i_1^{p-1} i_2^{p-1} \ldots i_\mu^{p-1}$ dans P_μ. Effectivement, d'après l'analyse du n° 3, $i_1, i_2, \ldots, i_{n-1}$ ne sont que des auxiliaires assujetties à la seule condition d'être des racines de congruences irréductibles du premier genre et des degrés $p, p^2, \ldots, p^{n-1}$ respectivement; il n'y a donc pas dans $F_n(X_1)$ d'autres arbitraires que les coefficients de P_{n-1}.

La forme la plus générale que l'on puisse supposer à P_{n-1} est la suivante :

$$(19)\quad \left\{\begin{array}{l} P_{n-1} = g\,(a_0 + a_1 i_1 + a_2 i_1^2 + \ldots + a_{p-2} i_1^{p-2} + i_1^{p-1}) \\ \qquad \times (a_0^{(1)} + a_1^{(1)} i_2 + a_2^{(1)} i_2^2 + \ldots + a_{p-2}^{(1)} i_2^{p-2} + i_2^{p-1}) \\ \qquad \times (a_0^{(2)} + a_1^{(2)} i_3 + a_2^{(2)} i_3^2 + \ldots + a_{p-2}^{(2)} i_3^{p-2} + i_3^{p-1}) \\ \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad \times (a_0^{(n-2)} + a_1^{(n-2)} i_{n-1} + a_2^{(n-2)} i_{n-2}^2 + \ldots + a_{p-2}^{(n-2)} i_{n-1}^{p-2} + i_{n-1}^{p-1}), \end{array}\right.$$

$g, a_0, a_1, \ldots, a_{p-2}$ étant des entiers arbitraires, et $a_0^{(\mu)}, a_1^{(\mu)}, \ldots, a_{p-2}^{(\mu)}$ des fonctions entières de $i_1, i_2, \ldots, i_\mu$ du degré $p-1$, au plus, par rapport à chacune de ces quantités. Il y a donc dans P_{n-1} un nombre de coefficients arbitraires égal à p^{n-1}; mais il est facile de voir que ce nombre doit être diminué, pour notre objet, de $n-1$ unités. En effet les congruences (18) ne changent pas quand on y remplace

$$i_1, \quad i_2, \quad i_3, \ldots, \quad i_{n-1}$$

respectivement par

$$i_1 + h_1, \quad i_2 + h_2 + Q_1, \quad i_3 + h_3 + Q_2, \ldots, \quad i_{n-1} + h_{n-1} + Q_{n-2},$$

$h_1, h_2, \ldots, h_{n-1}$ étant des entiers arbitraires et $Q_1, Q_2, \ldots, Q_{n-2}$ des fonctions convenablement choisies, de même nature que $P_1, P_2, \ldots, P_{n-2}$. Si l'on désigne par P'_μ ce que devient P_μ par le changement dont

il s'agit, la fonction Q_μ sera déterminée par la congruence

$$Q_\mu^p - Q_\mu \equiv P'_\mu - P_\mu \pmod{p},$$

dont le second membre ne renferme pas le terme $i_1^{p-1} i_2^{p-1} \dots i_\mu^{p-1}$; il s'ensuit, d'après l'analyse du n° 5, que Q_μ sera exprimable en fonction des seules quantités $i_1, i_2, \dots, i_\mu$.

Il est donc permis d'exécuter le même changement dans le second membre P_{n-1} de la congruence (17); la forme (19) de P_{n-1} sera conservée, mais on pourra disposer des indéterminées $h_1, h_2, \dots, h_{n-1}$ pour faire disparaître $n-1$ termes, par exemple, les parties constantes des coefficients de $i_1^{p-2}, i_2^{p-2}, \dots, i_{n-1}^{p-2}$ dans les divers facteurs entre parenthèses de la formule (19); ainsi donc il est permis de supposer que a_{p-2} est nul et que les coefficients $a_{p-2}^{(\mu)}$ n'ont pas de terme constant. Alors notre expression de P_{n-1} ne renferme plus que $p^{n-1} - n + 1$ coefficients; chacun de ceux-ci peut avoir les valeurs $0, 1, 2, \dots, (p-1)$, à l'exception du coefficient g, qui ne prend que les valeurs $1, 2, \dots, (p-1)$. Il s'ensuit que le nombre des fonctions $F_n(X_1)$ est $(p-1)p^{p^{n-1}-n}$, ce qui s'accorde avec ce qu'on a vu plus haut.

Je dois rappeler ici que, dans mon premier Article, j'ai donné l'expression des fonctions irréductibles de degré p. En changeant x en $x^p - x$ dans les fonctions du genre principal, on obtiendra immédiatement, par le théorème du n° 2, les fonctions entières irréductibles du degré p^2 et du premier genre.

7. Si l'on veut se borner à la recherche d'une seule fonction entière irréductible du degré p^n, le plus simple sera, en général, de réduire P_{n-1} au seul terme qui doit y figurer nécessairement, ou à ce terme augmenté d'une constante. Ainsi l'on prendra, pour la congruence (17),

$$X_1 \equiv \pm i_1^{p-1} i_2^{p-1} \dots i_{n-1}^{p-1} - g \pmod{p},$$

g étant une constante quelconque.

Considérons, par exemple, le cas de $n = 2$. On posera

$$i_1^p - i_1 \equiv 1, \quad X_1 \equiv i_1^{p-1} - 1 \equiv \frac{1}{i_1} \pmod{p};$$

remplaçant donc i_1 par $\frac{1}{X_1}$ dans la première congruence, il vient

$$X_1^p + X_1^{p-1} - 1 \equiv 0 \pmod{p}.$$

Ainsi $X_1^p + X_1^{p-1} - 1$, c'est-à-dire $(x^p - x)^p + (x^p - x)^{p-1} - 1$, est une fonction irréductible du degré p^2 et du premier genre.

Considérons encore le cas de $n = 3$. Nous poserons

$$i_1^p - i_1 \equiv 1, \quad i_2^p - i_2 \equiv i_1^{p-1} - 1 \equiv \frac{1}{i_1}, \quad X_1 \equiv i_1^{p-1} i_2^{p-1} - 1 \pmod{p},$$

et nous ferons en outre

$$i_1 i_2 = \frac{1}{z},$$

d'où

$$z^{p-1} \equiv \frac{1}{X_1 + 1} \pmod{p}.$$

On tire de ces formules

$$\frac{\frac{1}{z^p}}{i_1^p} \equiv \frac{\frac{1}{z} + 1}{i_1} \equiv \frac{\frac{1}{z^p} - \frac{1}{z} - 1}{1} \pmod{p},$$

d'où

$$i_1 \equiv \frac{1 + z}{X_1 - z}, \quad i_1^p \equiv \frac{X_1 + 1}{X_1 - z} \pmod{p},$$

et l'élimination de i_1 donne

$$\frac{X_1(X_1 + 1)(X_1^p + X_1^{p-1} - 1) - X_1 z + z^2}{z(X_1 - z)} \equiv 0 \pmod{p},$$

ou, en désignant par z_1, z_2 les valeurs de z qui annulent le numérateur,

$$\frac{(z_1 - z)(z_2 - z)}{z(X_1 - z)} \equiv 0 \pmod{p}.$$

Multiplions entre elles la précédente congruence et celles qu'on déduit de celle-ci par le changement de z en $2z$, $3z$, ..., $(p-1)z$; remplaçons ensuite z^{p-1} par $\frac{1}{X_1 + 1}$; il viendra

$$\frac{(X_1 + 1)^2 (z_1 z_2)^{p-1} - (X_1 + 1)(z_1^{p-1} + z_2^{p-1} - X_1^{p-1})}{X_1^p + X_1^{p-1} - 1} - 1 \equiv 0 \pmod{p}.$$

Faisons, pour abréger l'écriture,

$$P = X_1(X_1+1)(X_1^p + X_1^{p-1} - 1),$$

$$Q = X_1^{p-3} + \frac{4}{2}X_1^{p-5}P + \ldots + \frac{(\mu+2)(\mu+3)\ldots 2\mu}{2.3.\ldots\mu}X_1^{p-2\mu-1}P^{\mu-1} + \ldots + \frac{\left(\frac{p-1}{2}+2\right)\ldots(p-1)}{2.3\ldots\frac{p-1}{2}}P^{\frac{p-3}{2}},$$

on aura

$$z_1 z_2 \equiv P, \quad z_1^{p-1} + z_2^{p-1} \equiv X_1^{p-1} + PQ \pmod{p},$$

et notre congruence deviendra

$$(X_1+1)^3 X_1 P^{p-2} - (X_1+1)^2 X_1 Q - 1 \equiv 0 \pmod{p}.$$

Le premier membre de cette congruence est une fonction entière irréductible du degré p^3 et du premier genre.

8. Les formules (15) du n° **3** peuvent être regardées comme définissant un premier groupe de fonctions entières irréductibles du premier genre et des degrés respectifs $p, p^2, \ldots, p^n$. Nous allons montrer, en terminant cet Article, de quelle manière les fonctions irréductibles du degré p^n des divers genres se rattachent à ce groupe fondamental.

Revenons donc à la formule (8) et considérons l'un quelconque des facteurs de son second membre. Posons

$$Z_\mu \equiv X_\mu^{p-1} - 1 \pmod{p}; \tag{20}$$

l'indice μ a l'une quelconque des valeurs

$$p^{n-1}, \quad p^{n-1}+1, \quad p^{n-1}+2, \ldots, \quad p^n - 1;$$

nous le supposerons mis sous la forme

$$\mu = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots + \alpha_{n-1} p^{n-1},$$

$\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ étant des entiers positifs ou nuls et inférieurs à p.

Désignons par ξ_0 un entier arbitraire, et faisons généralement

$$(21)\quad \xi_{k+1} \equiv a_0^{(k)} + a_1^{(k)} i_{k+1} + a_2^{(k)} i_{k+1}^2 + \ldots + a_{\alpha_k - 1}^{(k)} i_{k+1}^{\alpha_k - 1} + i_{k+1}^{\alpha_k} \pmod{p},$$

a_0^k, a_1^k, ... étant des fonctions entières de $i_1, i_2, \ldots, i_k$ qui se réduisent à des entiers dans le cas de $k = 0$; la quantité ξ_{k+1} se réduira elle-même à l'unité dans le cas de $\alpha_k = 0$. Quant aux racines $i_1, i_2, \ldots, i_n$, elles sont, je le répète, définies par les formules (15).

Cela posé, je dis que les $(p-1)p^\mu$ racines de la congruence

$$(22)\qquad Z_\mu \equiv 0 \pmod{p}$$

sont données par la formule

$$(23)\qquad x \equiv \xi_0 \xi_1 \xi_2 \ldots \xi_n \pmod{p},$$

dont le second membre est effectivement susceptible de $(p-1)p^\mu$ valeurs différentes. Deux de ces valeurs de x sont nécessairement distinctes, car leur différence est une fonction de degré inférieur à p par rapport aux quantités i qui y figurent, et notamment par rapport à celle i_m de ces quantités qui a le plus grand indice. Si donc la différence dont nous parlons était congrue à zéro, i_m serait racine d'une congruence de degré inférieur à p^m, ce qui n'a pas lieu.

D'après cela, il nous suffit de prouver que la valeur (23) de x satisfait à la congruence (22), et nous y parvenons sans difficulté au moyen du lemme du n° 4.

Faisons, pour abréger,

$$\mu_k = \alpha_0 + \alpha_1 p + \ldots + \alpha_k p^k$$

et

$$A_k = 1.2\ldots\alpha_{n-1} \times 1.2\ldots\alpha_{n-2} \times \ldots \times 1.2\ldots\alpha_k;$$

si l'on applique le lemme du n° 4 dans les n hypothèses suivantes :

$m = n-1$,	$\nu = \alpha_{n-1}$,	$\rho = 0$,	$\zeta = i_n$.	$f(\zeta) = \xi_0 \xi_1 \ldots \xi_{n-1} \xi_n$,
$m = n-2$,	$\nu = \alpha_{n-2}$,	$\rho = \mu - \mu_{n-2}$,	$\zeta = i_{n-1}$,	$f(\zeta) = A_{n-1} \xi_0 \xi_1 \ldots \xi_{n-1}$,
$m = n-3$.	$\nu = \alpha_{n-3}$,	$\rho = \mu - \mu_{n-3}$,	$\zeta = i_{n-2}$,	$f(\zeta) = A_{n-2} \xi_0 \xi_1 \ldots \xi_{n-2}$,
.....	.....	.....	.....	.....
$m = 0$,	$\nu = \alpha_0$,	$\rho = \mu - \mu_0$,	$\zeta = i_1$,	$f(\zeta) = A_1 \xi_0 \xi_1$,

on reconnaîtra que la formule (23) entraîne successivement les suivantes :

$$\left.\begin{aligned}
&X_{\mu-\mu_{n-2}} \equiv A_{n-1}\,\xi_0\,\xi_1 \dots \xi_{n-1},\\
&X_{\mu-\mu_{n-3}} \equiv A_{n-2}\,\xi_0\,\xi_1 \dots \xi_{n-2},\\
&\dots\dots\dots\dots\dots\dots\dots\dots,\\
&X_{\mu-\mu_0} \equiv A_1\,\xi_0\,\xi_1,\\
&X_{\mu} \equiv A_0\,\xi_0
\end{aligned}\right\} \pmod{p},$$

et, puisque X_μ se réduit ainsi à une constante, il est évident que la congruence (22) est satisfaite.

La formule (23) définit, avec les formules (15), les congruences irréductibles des divers genres de degré p^n. Celles-ci s'obtiennent effectivement en éliminant $i_1, i_2, \dots, i_n$ de la formule (23). Par les motifs indiqués au n° 6, on peut, en vue de cette élimination, supposer nulle la partie constante du coefficient de l'avant-dernier terme des fonctions ξ.

FIN DU TOME DIX-HUITIÈME (2^e SÉRIE)

PARIS. — IMPRIMERIE DE GAUTHIER-VILLARS, SUCCESSEUR DE MALLET-BACHELIER,
Quai des Augustins, 55.