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

J.-A. SERRET

Détermination des fonctions entières irréductibles, suivant un module premier, dans le cas où le degré est égal au module

Journal de mathématiques pures et appliquées 2^e série, tome 18 (1873), p. 301-304.
<http://www.numdam.org/item?id=JMPA_1873_2_18__301_0>

Détermination des fonctions entières irréductibles, suivant un module premier, dans le cas où le degré est égal au module;

PAR M. J.-A. SERRET.

1. Dans un travail qui fait partie du tome XXXV des *Mémoires de l'Académie des Sciences*, et dont la troisième édition de mon *Algèbre supérieure* reproduit les résultats, j'ai montré qu'on peut obtenir immédiatement une fonction entière du degré ν irréductible suivant le module premier p, lorsque le nombre ν ne renferme aucun facteur premier différent de ceux qui divisent $p-1$, et aussi lorsque ce degré est précisément égal au module.

Je me propose ici de revenir sur le dernier de ces deux cas, et d'exécuter la décomposition de la fonction $x^{p^p}-x$ en facteurs irréductibles suivant le module p. Posons

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

il est évident que l'on aura

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

Multiplions entre elles les $p-1$ congruences comprises dans la formule (2) quand on attribue à μ les valeurs $1, 2, 3, \ldots (p-1)$, et divisons ensuite la congruence résultante par $X_2 X_3 \ldots X_{p-1}$, il viendra

$$(3)\qquad X_p \equiv X_1 (X_1^{p-1}-1)(X_2^{p-1}-1)\ldots(X_{p-1}^{p-1}-1) \pmod{p};$$

mais la formule (1) donne

$$X_1 = x^p - x, \quad \text{et} \quad X_p \equiv x^{p^p} - x \pmod{p},$$

en sorte que le quotient V de X_p par X_1 est égal au produit de toutes les fonctions entières irréductibles de degré p; on a, par la formule (3),

$$(4)\qquad V \equiv (X_1^{p-1}-1)(X_2^{p-1}-1)\ldots(X_{p-1}^{p-1}-1) \pmod{p},$$

et l'on sait d'ailleurs que

$$(5)\qquad X_\mu^{p-1} - 1 \equiv (X_\mu - 1)(X_\mu - 2)\ldots(X_\mu - \overline{p-1}) \pmod{p}.$$

Ainsi chacun des facteurs $X_\mu^{p-1} - 1$ de V est, d'après la formule (5), le produit de $p-1$ facteurs $X_\mu - g$, où g a les valeurs $1, 2, \ldots (p-1)$, et chacun de ces facteurs $X_\mu - g$ est lui-même le produit de $p^{\mu-1}$ facteurs irréductibles du degré p. En particulier, le facteur $X_1^{p-1} - 1$ est le produit des $p-1$ polynômes irréductibles

$$x^p - x - g, \tag{6}$$

que j'ai considérés dans le Mémoire cité.

2. Les fonctions entières irréductibles du degré p peuvent être distinguées en $p-1$ genres, en comprenant dans le $\mu^{ième}$ genre toutes celles dont $X_\mu^{p-1} - 1$ est le produit. Le premier genre comprend les $p-1$ fonctions (6).

Soit i une racine de la congruence irréductible

$$i^p - i - 1 \equiv 0 \pmod{p}, \tag{7}$$

les racines de cette congruence seront

$$i, \quad i+1, \quad i+2, \ldots, \quad i+p-1,$$

et il est évident que les p racines de la congruence

$$x^p - x - g \equiv 0 \pmod{p}$$

seront

$$gi, \quad g(i+1), \quad g(i+2), \ldots, \quad g(i+p-1),$$

en sorte que les fonctions irréductibles du premier genre sont caractérisées par cette circonstance que leurs *racines* sont des fonctions linéaires de i.

Je dis que généralement *les fonctions du $\mu^{ième}$ genre ont pour racines des fonctions entières de i du degré μ.*

En effet, considérons une telle fonction, et désignons par

$$f(i) = a_0 + a_1 i + a_2 i^2 + \ldots + a_{p-1} i^{p-1} \tag{8}$$

l'une des racines de la congruence obtenue en l'égalant à zéro, suivant le module p. D'après ce qui a été dit plus haut, $f(i)$ sera racine de la congruence $X_\mu \equiv g \pmod{p}$, dans laquelle g a une valeur convenable. Exécutant la substitution et observant que $[f(i)]^{p^m} \equiv f(i^{p^m}) \equiv f(i+m) \pmod{p}$, il viendra

$$f(i+\mu) - \frac{\mu}{1} f(i+\mu-1) + \frac{\mu(\mu-1)}{1.2} f(i+\mu-2) - \ldots$$
$$+ (-1)^{\mu-1} \frac{\mu}{1} f(i+1) + (-1)^\mu f(i) \equiv g \pmod{p}.$$

Cette congruence est nécessairement identique, car son premier membre est un polynôme en i de degré inférieur à p; d'ailleurs ce premier membre est la différence $\mu^{ième}$ de $f(i)$ relative à la différence constante 1 attribuée à i; donc, puisqu'il se réduit à la constante g différente de zéro, le degré de $f(i)$ est précisément égal à μ; on a, en conséquence,

$$a_\mu = \frac{g}{1.2\ldots\mu} \quad \text{et} \quad a_{\mu+1} = a_{\mu+2} = \ldots = a_{p-1} = 0.$$

3. Il est aisé d'obtenir les fonctions irréductibles des différents genres. Supposons que les p coefficients $a_0, a_1, \ldots, a_{p-1}$ de la formule (8) restent indéterminés, en exclnant le cas où $f(i)$ se réduirait à la constante a_0, et considérons la congruence

$$i^\lambda [f(i) - x] \equiv 0 \pmod{p}, \tag{9}$$

dans laquelle λ prendra les p valeurs $0, 1, 2, \ldots, p-1$. Si l'on rabaisse au-dessous de p les exposants de i, en faisant usage de la congruence (7), la formule (9) donnera p congruences, dont les premiers membres seront des fonctions homogènes et linéaires des puissances $i^0, i^1, i^2, \ldots, i^{p-1}$. En égalant à zéro, suivant le module p, le déterminant $F(x)$ formé avec les coefficients de ces puissances de i, on obtiendra la congruence irréductible dont les racines sont

$$f(i), \quad f(i+1), \ldots, \quad f(i+p-1); \tag{10}$$

$F(x)$ sera donc une fonction entière irréductible du degré p.

Si l'on fait, pour abréger l'écriture,

$$a_k + a_{k-1} = a'_k,$$

et qu'on regarde a_p comme équivalant à a_0, en sorte que a'_0 représente $a_0 + a_{p-1}$, on trouve immédiatement

$$F(x) = -\begin{vmatrix} a_0 - x, & a_1, & a_2, \ldots, & a_{p-3}, & a_{p-2}, & a_{p-1}, \\ a_{p-1}, & a'_0 - x, & a_1, \ldots, & a_{p-4}, & a_{p-3}, & a_{p-2}, \\ a_{p-2}, & a'_{p-1}, & a'_0 - x, \ldots, & a_{p-5}, & a_{p-4}, & a_{p-3}, \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots, \\ a_3, & a'_4, & a'_5, \ldots, & a'_0 - x, & a_1, & a_2, \\ a_2, & a'_3, & a'_4, \ldots, & a'_{p-1}, & a'_0 - x, & a_1, \\ a_1, & a'_2, & a'_3, \ldots, & a'_{p-2}, & a'_{p-1}, & a'_0 - x. \end{vmatrix} \tag{11}$$

Telle est l'expression générale des fonctions irréductibles du degré p suivant le module p.

Si l'on veut avoir les fonctions du $\mu^{ième}$ genre, on fera

$$a_{\mu+1} = 0, \quad a_{\mu+2} = 0, \quad \ldots, \quad a_{p-1} = 0, \tag{12}$$

et l'on peut supposer aussi

$$a_{\mu-1} = 0. \tag{13}$$

En effet, la congruence $F(x) \equiv 0 \pmod{p}$ est celle dont dépendent les racines (10); or, parmi ces expressions (10), il y en a une, $f(i+\lambda)$, dans laquelle le coefficient de $i^{\mu-1}$ est congru à zéro, et rien n'empêche de substituer dans notre analyse $f(i+\lambda)$ à $f(i)$.

Ayant donc égard aux équations (12) et (13), si l'on attribue aux coefficients $a_0, a_1, \ldots, a_{\mu-2}$ les valeurs $0, 1, 2, \ldots, p-1$ et à a_μ les mêmes valeurs, zéro excepté, la formule (11) fera connaître les $(p-1)p^{\mu-1}$ fonctions irréductibles du $\mu^{ième}$ genre.

Si on fait l'application au cas de $\mu = 1$ et à celui de $\mu = 2$, on trouvera :

1° Pour $\mu = 1$, $F(x) = x^p - x - a_1$;

2° Pour $\mu = 2$, $F(x) = (x-a_0)\left[(x-a_0)^{\frac{p-1}{2}} - a_2^{\frac{p-1}{2}}\right]^2 - a_2$.

4. Parmi les fonctions du $(p-1)^{ième}$ genre, il faut remarquer celles qui répondent au cas où les coefficients de la formule (8) sont nuls, à l'exception de a_0 et a_{p-1}; ces fonctions ont pour expression

$$F(x) = (x-a'_0)^p + a_{p-1}[(x-a'_0)^{p-1} - 1],$$

et elles ont cette propriété que les racines de la congruence $F(x) \equiv 0 \pmod{p}$ sont des fonctions rationnelles et linéaires de l'une d'entre elles. Effectivement, la congruence dont il s'agit peut, si l'on y introduit la racine a'_0, se mettre sous la forme

$$x^p \equiv \frac{(a_{p-1}+a'_0)x - a'^2_0}{x + (a_{p-1} - a'_0)} \pmod{p},$$

et l'on sait d'ailleurs que ses racines peuvent être représentées par $x, x^p, x^{p^2}, \ldots, x^{p^{p-1}}$.