BULLETIN DE LA S. M. F.

A.-E. PELLET

Sur les fonctions réduites suivant un module premier

Bulletin de la S. M. F., tome 17 (1889), p. 156-167

<http://www.numdam.org/item?id=BSMF_1889__17__156_1>

Sur les fonctions réduites suivant un module premier;
par M. A.-E. PELLET.

1. La théorie des fonctions entières, réduites suivant un module premier p, offre la plus grande analogie avec celle des équations abéliennes, et, en retour, la théorie algébrique des équations en retire le plus précieux concours au point de vue des applications.

Le théorème qui sert de base à la méthode que j'ai développée dans le *Bulletin* (t. XV, p. 66) devient ici :

$\theta(x)$ étant une fonction rationnelle à coefficients entiers, soit μ le nombre de valeurs distinctes qu'elle prend lorsqu'on remplace x successivement par les m racines d'une congruence irréductible $(\mathrm{mod}\, p)$ et de degré m; μ est un diviseur de m et ces μ valeurs sont racines d'une congruence irréductible.

Ainsi soit A une fonction rationnelle d'un nombre quelconque de racines de congruences irréductibles suivant le mod p: formons la suite

$$\mathrm{A},\quad \mathrm{A}^p,\quad \mathrm{A}^{p^2},\quad \ldots,\quad \mathrm{A}^{p^k},\quad \ldots.$$

Soit ν le nombre de valeurs distinctes comprises dans cette suite; on a $\mathrm{A}^{p^\nu} \equiv \mathrm{A}\,(\mathrm{mod}\, p)$, et ces ν valeurs sont racines d'une congruence irréductible $(\mathrm{mod}\, p)$ à coefficients entiers. En effet, quel que soit le nombre de ces congruences, leurs racines peuvent

s'exprimer en fonction entière d'une racine d'une seule congruence irréductible dont le degré est égal au plus petit multiple commun des degrés de ces diverses congruences. Posant $A \equiv f(i) \pmod p$, il vient $f(i^p) \equiv A^p$.

2. Supposons que l'on connaisse l'exposant de A, c'est-à-dire le plus petit nombre n, tel que $A^n \equiv 1 \pmod p$; on en conclura facilement le nombre ν; ν est le plus petit nombre, tel que $p^\nu - 1$ soit divisible par n. On aura des indications sur cet exposant n, lorsqu'on connaîtra une relation de la forme $A^m \equiv a \pmod p$, a étant un nombre réel ou imaginaire d'exposant connu. Remarquons d'abord qu'on peut supposer m premier avec p; car de $A^{mp} \equiv a$, on déduit $A^m \equiv a^{p^{\nu-1}}$, ν étant le degré de la fonction irréductible dont a est racine. Désignons par e l'exposant de a; de la congruence $A^m \equiv a \pmod p$, on déduit $A^{me} \equiv 1 \pmod p$. Soit g une racine primitive de la conguence

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

a et A sont des puissances de g. Posons $a \equiv g^{km}$; k est premier avec e; et $x \equiv g^{\xi m}$. La congruence $x^m \equiv a \pmod p$ deviendra

$$g^{\xi m} - g^{km} \equiv 0 \pmod p;$$

d'où

$$\xi m - km \equiv 0 \pmod{me};$$

et enfin

$$\xi \equiv k \pmod e.$$

Ainsi l'on a

$$A \equiv g^{k+\alpha e} \pmod p,$$

α étant un des nombres 0, 1, 2, 3, ... $(m-1)$.

L'exposant n auquel appartient $g^{k+\alpha e}$ est le plus petit nombre n tel que $(k+\alpha e)n$ soit divisible par me. Soit e_1 le produit des facteurs premiers de e, entrant dans m pris avec l'exposant dont ils sont affectés dans m; $\frac{m}{e_1}$ est premier avec e; k étant premier avec e l'est aussi avec $e_1 e$, et, pour que le produit $(k+\alpha e)n$ soit divisible par $e_1 e$, il faut que n le soit. En particulier, si m ne contient que des facteurs premiers divisant e, on a $e_1 = m$, $n = e_1 e$. On déduit de là ce théorème de M. Serret : Si dans une fonction $F(x)$ irréductible $(\mathrm{mod}\, p)$, de degré ν et d'exposant n, on

remplace x par x^λ, λ ne renfermant que des facteurs premiers qui entrent dans n, $F(x^\lambda)$ se décompose en facteurs irréductibles d'exposant $n\lambda$ et, par suite, d'égal degré; le degré de ces facteurs est égal à νq, q étant le plus petit nombre tel que $p^{\nu q} - 1$ soit divisible par $n\lambda$. La recherche de ce nombre q est un problème d'Arithmétique complètement résolu par M. Serret dans son *Algèbre supérieure* (t. II, chap. III).

3. Désignons par P le produit des racines de la congruence $F(x) \equiv 0 \pmod p$ et par i une de ses racines; on a

$$i^{1+p+p^2+\ldots+p^{\nu-1}} \equiv P \pmod p.$$

e étant l'exposant de P, le nombre e_1 sera tel que $\frac{p^\nu - 1}{(p-1)e_1}$ soit premier avec e, et l'exposant n de i sera un multiple de $e_1 e$, $n_1 e_1 e$, divisant $\frac{p^\nu - 1}{p-1} e$. Prenons pour λ un facteur premier de e; la fonction $F(x^\lambda)$ appartient à l'exposant $\lambda n_1 e_1 e$; on a

$$\frac{p^{\nu q} - 1}{\lambda n_1 e_1 e} = \frac{p^\nu - 1}{n_1 e_1 (p-1)} \frac{(p^{\nu q} - 1)(p-1)}{(p^\nu - 1)\lambda e}.$$

Le premier facteur du produit qui figure au second membre est un nombre entier non divisible par λ; si donc $\frac{p-1}{e}$ n'est pas divisible par λ, il faut que $\frac{p^{\nu q} - 1}{p^\nu - 1}$ le soit; ce qui exige que $q = \lambda$; donc, λ étant un facteur premier de e ne divisant pas $\frac{p-1}{2e}$, $F(x^\lambda)$ est irréductible $(\mathrm{mod}\, p)$; si λ divise $\frac{p-1}{e}$, $F(x^\lambda)$ se décompose en λ facteurs irréductibles de degré ν et d'égal exposant.

Dans le cas où λ est un nombre premier divisant $p - 1$, mais ne divisant pas e, $F(x^\lambda)$ se décompose encore en λ facteurs irréductibles de degré ν, mais l'exposant n'est pas le même pour tous les facteurs.

Exemple. — Soit $P \equiv -1 \pmod p$; e est égal à 2. Si $\frac{p-1}{2}$ est impair ou p de la forme $4m - 1$, $F(x^2)$ est irréductible; si, de plus, le degré de $F(x)$ est pair, le produit des racines de $F(x^2)$ est encore congru à -1 et $F(x^{2^\alpha})$ est irréductible, quel que soit l'entier α.

4. Comme seconde application du théorème fondamental, nous établirons le théorème suivant :

$F(x)$ étant une fonction irréductible $(\mathrm{mod}p)$, de degré ν, dans laquelle le coefficient du terme de degré $\nu - 1$ n'est pas congru à 0 $(\mathrm{mod}p)$, la fonction $F(x^p - x)$, obtenue en remplaçant x par $x^p - x$ dans la première, est irréductible.

Soit I une racine de la congruence

$$\mathrm{I}^p - \mathrm{I} \equiv i \pmod{p}, \tag{1}$$

i étant une racine de $F(x) \equiv 0$. On a

$$\mathrm{I}^{p^2} \equiv \mathrm{I} + i + i^p, \qquad \mathrm{I}^{p^3} \equiv \mathrm{I} + i + i^p + i^{p^2}, \qquad \ldots.$$

Soit $\mathrm{I}^{p^k} \equiv \mathrm{I} \pmod{p}$, on en conclut

$$i + i^p + i^{p^2} + \ldots + i^{p^{k-1}} \equiv 0 \pmod{p};$$

d'où, élevant à la puissance $p^{\text{ième}}$ et retranchant membre à membre,

$$i^{p^k} - i \equiv 0 \pmod{p},$$

ce qui exige que k soit divisible par ν. Désignons par s_1 la somme $i + i^p + i^{p^2} + \ldots + i^{p^{\nu-1}}$; on a

$$\mathrm{I}^{p^\nu} \equiv \mathrm{I} \pmod{p}$$

si $s_1 \equiv 0 \pmod{p}$, et I est alors racine d'une congruence irréductible de degré ν. Les p racines de la congruence (1) sont effectivement données par la formule

$$\mathrm{I} \equiv a_0 + \frac{1}{\nu}(i^p + 2\,i^{p^2} + \ldots + (\nu - 1)\,i^{p^{\nu-1}}),$$

où a_0 est un des nombres $0, 1, 2, \ldots, p-1$, lorsque ν n'est pas divisible par p. Mais, si s_1 n'est pas congru à 0, on aura

$$\mathrm{I}^{p^\nu} \equiv \mathrm{I} + s_1, \qquad \mathrm{I}^{p^{m\nu}} \equiv \mathrm{I} + m s_1,$$

et, pour que $\mathrm{I}^{p^{m\nu}}$ soit congru à I, il faut et il suffit que m soit divisible par p. Ainsi, dans ce cas, le plus petit nombre k tel que $\mathrm{I}^{p^k} \equiv \mathrm{I} \pmod{p}$ est $p\nu$.

Il faut remarquer, pour l'application de ce théorème et de celui qui précède, que, par une transformation linéaire, on pourra presque toujours donner au produit et à la somme des racines d'une congruence une valeur assignée.

Exemple. — Si, dans $x - 1$, on change x en $x^p - x$, on obtient la fonction $x^p - x - 1$, qui est irréductible. La congruence

$$x^p + x^{p-1} - 1 \equiv 0 \pmod{p},$$

transformée de $x^p - x - 1$, en changeant x en $\frac{1}{x}$ est aussi irréductible; la somme des racines est congrue à -1; en changeant x en $x^p - x$, la nouvelle congruence sera irréductible

$$x^{p^2} - x^p + (x^p - x)^{p-1} - 1 \equiv 0 \pmod{p}.$$

Sur les périodes des racines de l'unité.

5. P étant un nombre premier, considérons la congruence

$$\frac{x^{P-1}}{x-1} \equiv 0 \pmod{p}. \tag{1}$$

Son premier membre se décompose en $\frac{P-1}{\nu}$ facteurs irréductibles de degré ν, exposant de p relativement à P, c'est-à-dire plus petit nombre, tel que $p^\nu - 1$ soit divisible par P. Désignons par G une racine primitive du nombre premier P, et par θ une racine de la congruence (1), qui peut être réelle ou imaginaire. Les racines de cette congruence seront

$$\theta, \quad \theta^G, \quad \theta^{G^2}, \quad \ldots, \quad \theta^{G^{P-2}}.$$

Soit $f(x) = 0$ l'équation aux q périodes des racines $P^{ièmes}$ de l'unité. Les racines de la congruence $f(x) \equiv 0 \pmod{p}$ sont

$$s_i \equiv \sum_{i_1=0}^{i_1=\omega-1} \theta^{G^{i+i_1 q}} \pmod{p},$$

ω désignant $\frac{P-1}{q}$ et i un des nombres $0, 1, 2, \ldots, q-1$.

Elles sont réelles si ν divise ω, et il y en a d'imaginaires si ν ne divise pas ω.

En effet, soit $p \equiv G^{\alpha+\beta q} \pmod{P}$: p^ν étant congru à $1 \pmod{P}$, $\nu(\alpha + \beta q)$ est divisible par $P - 1$; on a : $\nu\alpha = m.\omega q - \beta\nu q$; et l'on voit que α est égal à 0 si ν divise ω, différent de 0 si ν ne divise pas ω. Il vient

$$(\theta^{G^{i+i_1 q}})^p \equiv \theta^{G^{\alpha+i+(i_1+\beta)q}} \pmod{p}.$$

Si α est égal à 0, s_i^p est donc congru à s_i, qui est par suite un nombre réel; mais si α n'est pas nul, $s_i^p \equiv s_{i+\alpha} \pmod p$; si donc s_i est réel, on aura dans ce cas

$$s_i \equiv s_{i+\alpha} \equiv r_{i+2\alpha} \equiv s_{i+3\alpha} \equiv \dots \pmod p,$$

et s_i sera une racine multiple de la congruence $f(x) \equiv 0 \pmod p$, son degré de multiplicité sera un diviseur de q. D'ailleurs les q nombres s_i ne peuvent être réels, car autrement on en déduirait la décomposition de $\frac{x^p - 1}{x - 1}$ en q facteurs à coefficients entiers, et réels de degré $\frac{P-1}{q}$; ces facteurs se décomposeraient en $\frac{P-1}{q.\nu}$, facteurs d'égal degré ν; ν diviserait donc $\frac{P-1}{q} = \omega$, ce qui est contre l'hypothèse.

6. L'équation aux deux périodes des racines P$^{\text{ièmes}}$ de l'unité est

$$x^2 + x + \frac{1 - (-1)^{\frac{P-1}{2}} P}{4} = 0.$$

Elle est irréductible (mod 2) si le produit de ses racines est un nombre impair, et elle a deux racines réelles (mod 2) si ce produit est un nombre pair. Ainsi 2 est résidu quadratique pour les nombres premiers de la forme $8k \pm 1$, non-résidu quadratique pour les nombres premiers de la forme $8k \pm 3$.

Pour tout nombre premier p différent de 2, nous pouvons mettre le premier membre de l'équation aux deux périodes sous la forme

$$(2x+1)^2 - (-1)^{\frac{P-1}{2}} P = 0.$$

Elle a deux racines réelles (mod p) ou est irréductible (mod p), suivant que $\left[(-1)^{\frac{P-1}{2}} P\right]^{\frac{p-1}{2}}$ est congru à 1 ou $-1 \pmod p$; d'où, en employant le symbole $\left(\frac{P}{p}\right)$ pour désigner ± 1 suivant que P est résidu quadratique ou non suivant le module p,

$$(-1)^{\frac{P-1}{2}\cdot\frac{p-1}{2}} \left(\frac{P}{p}\right)\left(\frac{p}{P}\right) = 1,$$

qui exprime un théorème célèbre de Legendre.

7. Si P — 1 est divisible par 8, on a, pour l'équation aux quatre périodes,

$$y^2 - xy - (b^2 + m^2 + mx) = 0,$$

b et m étant définis par l'équation

$$16b^2 + (4m - 1)^2 = P,$$

et x étant une des racines de l'équation

$$x^2 + x + \frac{1 - P}{4} = 0.$$

(*Voir* mon Mémoire *Sur la théorie des équations algébriques, Bulletin de la Société*, année 1887.)

Pour le nombre premier 2, les racines de la congruence aux deux périodes sont 0 et 1; les quatre périodes sont données par les congruences

$$y^2 - (b^2 + m^2) \equiv 0, \qquad y^2 + y - b^2 \equiv 0 \pmod 2,$$

en remarquant que $m^2 + m$ est toujours divisible par 2. Les quatre périodes sont réelles si b est pair; il y en a deux d'imaginaires si b est impair; dans le premier cas, 2 est résidu biquadratique (mod P); dans le second cas, il est non-résidu biquadratique (mod P).

Pour tout nombre premier p différent de 2, nous pouvons mettre le premier membre de la congruence aux quatre périodes sous la forme

$$\left(z^2 - \frac{P}{16}\right)^2 - \frac{P}{4}\left(z + \frac{a}{4}\right)^2 \equiv 0 \pmod p, \tag{1}$$

en posant

$$y + \tfrac{1}{4} = z, \qquad a = 4m - 1.$$

Cherchons dans quel cas p est résidu biquadratique (mod P). Il faut d'abord qu'il soit résidu quadratique et alors P, d'après le théorème de Legendre, est aussi résidu quadratique (mod p); soit $P \equiv \alpha^2 \pmod p$. La congruence (1) se décompose dans les deux suivantes :

$$z^2 - \frac{\alpha}{2}z - \frac{\alpha^2 + 2a\alpha}{16} \equiv 0, \qquad z^2 + \frac{\alpha}{2}z - \frac{\alpha^2 - 2a\alpha}{16} \equiv 0 \pmod p.$$

Pour que les quatre périodes soient réelles, il faut et il suffit

que les deux nombres

$$(n) \qquad 2\alpha(\alpha+a), \qquad 2\alpha(\alpha-a)$$

soient résidus quadratiques (mod p). Leur produit, étant congru à $4\alpha^2(\alpha^2-a^2)\equiv\frac{\alpha^2b^2}{4}$, est résidu quadratique (mod p) si p ne divise pas b.

Si p divise b, l'un des nombres (n) est congru à 0 (mod p), l'autre à $4\alpha^2$(mod p); p est donc résidu biquadratique (mod P). Si p divise a, les deux nombres n se réduisent à $2\alpha^2$ (mod p); ils sont résidus quadratiques (mod p), et, par suite, p résidu biquadratique (mod P) si p est de la forme $8k\pm1$.

p ne divisant ni b ni a, posons $a\equiv r\alpha$ (mod p). Pour que les nombres (n) soient résidus quadratiques (mod p), il faut qu'on ait à la fois

$$r^{p-1}-1\equiv 0, \qquad (1+r)^{\frac{p-1}{2}}\equiv(1-r)^{\frac{p-1}{2}}\equiv 2^{\frac{p-1}{2}} \pmod p.$$

Ces congruences sont incompatibles pour p égal à 3, 5, 7, et, par conséquent, ces nombres ne peuvent être résidus biquadratiques (mod P) que s'ils divisent b ou a.

8. Si P — 1 est divisible par 4, mais non par 8, 2 n'est pas résidu biquadratique (mod P); en désignant par $z-\frac{1}{4}$ une des quatre périodes des racines P$^{\text{ièmes}}$ de l'unité, on a l'équation

$$\left(z^2+\frac{3P}{4}\right)^2-\frac{P}{4}\left(z+\frac{a}{4}\right)^2=0,$$

a étant déterminé par les deux conditions

$$4b^2+a^2=P, \qquad a\equiv -1 \pmod 4.$$

Supposant p résidu quadratique (mod P), nous pourrons poser $P\equiv\alpha^2$ (mod p), α étant réel, comme plus haut. La congruence

$$\left(z^2+\frac{3\alpha^2}{16}\right)^2-\frac{\alpha^2}{4}\left(z+\frac{a}{4}\right)^2\equiv 0 \pmod p$$

se décompose dans les deux suivantes :

$$z^2-\frac{\alpha}{2}z+\frac{3\alpha^2-2a\alpha}{16}\equiv 0, \qquad z^2+\frac{\alpha}{2}z+\frac{3\alpha^2+2a\alpha}{16}\equiv 0 \pmod p.$$

Pour que leurs racines soient réelles, il faut et il suffit que les

deux nombres

$$(n') \qquad -2\alpha(\alpha-a), \qquad -2\alpha(\alpha+a)$$

soient résidus quadratiques (mod p). C'est donc la condition nécessaire et suffisante pour que p soit résidu biquadratique (mod P).

Si p divise b, l'un des nombres (n') est congru à 0 (mod p), l'autre à $-4\alpha^2$; p sera donc résidu biquadratique (mod P) s'il est de la forme $4m+1$, non-résidu biquadratique s'il est de la forme $4m-1$. Si p divise a, les nombres (n') sont congrus à $-2\alpha^2$; p sera donc résidu biquadratique (mod P) s'il est de l'une des deux formes $8k+1$ ou $8k+3$, non-résidu biquadratique s'il est de l'une des formes $8k+5$, $8k+7$.

p ne divisant ni a ni b, posons $a \equiv r\alpha \pmod p$. Pour que les nombres (n') soient résidus biquadratiques (mod p), il faut qu'on ait à la fois

$$r^{p-1}-1 \equiv 0, \qquad (1+r)^{\frac{p-1}{2}} \equiv (1-r)^{\frac{p-1}{2}} \equiv (-2)^{\frac{p-1}{2}} \pmod p.$$

Ces congruences sont incompatibles si p est égal à 3 ou à 5; toujours satisfaites si $p=7$.

9. L'équation aux trois périodes des racines P$^{\text{ièmes}}$ de l'unité est

$$x^3+x^2-\omega x-\frac{P(n_0+1)-\omega^2}{3}=0,$$

ω désignant le rapport $\frac{P-1}{3}$ et n_0 étant déterminé par l'équation

$$27N^2+(9n_0-3\omega+7)^2=4P.$$

Posons $n_0=-1+\omega^2+3m$; l'équation aux trois périodes devient

$$x^3+x^2-\omega x-\omega^3-3m\omega-m=0,$$

et la relation précédente montre que l'on a

$$N^2-m+\omega^2(\omega-1)\equiv 0 \pmod 3.$$

Faisant dans la congruence

$$x^3+x^2-\omega x-\omega^3-m\equiv 0 \pmod 3,$$

ou

$$x^3+x^2-\omega x-N^2+\omega^3+\omega^2\equiv 0 \pmod 3,$$

les trois hypothèses ω congru à 0, 1 ou 2 (mod 3), on voit que,

pour qu'elle ait ses trois racines réelles, il faut et il suffit dans chaque cas que N soit divisible par 3. La condition nécessaire et suffisante pour que 3 soit résidu cubique (mod P) est donc que $4P = 27.9.N_1^2 + L^2$.

Pour tout nombre premier p autre que 3, nous poserons $3x + 1 = y$, et l'équation aux trois périodes devient

$$y^3 - 3Py - PL = 0,$$

L étant déterminé par les deux conditions

$$4P = L^2 + 27N^2, \qquad L \equiv 1 \pmod 3.$$

p sera résidu cubique (mod P) si la congruence

$$y^3 - 3Py - PL \equiv 0 \pmod p$$

a ses trois racines réelles. Si p divise N, cette congruence devient

$$y^3 - \frac{3L^2}{4}y - \frac{L^3}{4} \equiv 0 \pmod p;$$

elle admet la racine simple L et la racine double $-\frac{L}{2}$. Si p divise L, elle devient

$$y^3 - \frac{9^2N^2}{4}y \equiv 0 \pmod p;$$

elle a encore ses trois racines réelles. Ainsi, tout nombre divisant N ou L est résidu cubique (mod P).

Pour que le nombre premier p, ne divisant ni L ni N, soit résidu cubique mod P, il faut et il suffit que la congruence

$$y^3 - 3Py - PL \equiv 0 \pmod p$$

ait trois racines distinctes et différentes de 0. Il en sera de même de la congruence

$$z^3 - \frac{3P}{\alpha^2}z - \frac{PL}{\alpha^3} \equiv 0 \pmod p,$$

transformée de la précédente en posant $y \equiv \alpha z$, et l'on peut choisir α de manière que $\frac{3P}{\alpha^2}$ soit congru à 1 si 3P est résidu quadratique (mod p), à un nombre non-résidu quadratique assigné si 3P est non-résidu quadratique, à 2 par exemple, pour p égal à 5, 11, 13, à 3 si $p = 7$. On voit alors, par un calcul assez court, qu'une telle congruence est impossible pour p égal à 2, 5, 7; ces nom-

bres premiers ne peuvent donc être résidus cubiques (mod P) que s'ils divisent L ou N. Pour p égal à 11, les valeurs (mod 11) de $x^3 - x$ et $x^3 - 2x$ sont respectivement

$x^3 - x$..... 0, −5, 2, 5, −1, 0, 5, −2, −5, +1
$x^3 - 2x$..... −1, 4, −1, 1, 5, 1, −4, 1, −1, 6

pour les valeurs 1, 2, 3, 4, 5, −1, −2, −3, −4, −5 de x.

Les seules congruences satisfaisant aux conditions requises sont donc

$$x^3 - 2x \pm 1 \equiv 0 \pmod{11}.$$

Si donc 11 est résidu cubique (mod P), on doit avoir

$$\frac{3P}{\alpha^2} \equiv 2, \qquad \frac{PL}{\alpha^3} \equiv \pm 1 \pmod{11};$$

d'où, par l'élimination de α,

$$L^2 \equiv 2P \pmod{11}.$$

Cette condition nécessaire est aussi suffisante.

Pour P égal à 13, les valeurs (mod 13) de $x^3 - x$ et de $x^3 - 2x$ sont

$x^3 - x$..... 0, 6, −2, −5, 3, 2, 0, −6, 2, 5, −3, −2,
$x^3 - 2x$..... −1, 4, −5, 4, −2, −4, 1, −4, 5, −4, 2, 4

pour les valeurs 1, 2, 3, 4, 5, 6, −1, −2, −3, −4, −5, −6 de x.

Les seules congruences satisfaisant aux conditions requises sont donc

$$x^3 - 2x \pm 4 \equiv 0 \pmod{13}.$$

Pour que 13 soit résidu (mod P), il faut et il suffit que l'on ait

$$3P \equiv 2\alpha^2, \qquad PL \equiv \pm L\alpha^3 \pmod{13},$$

α étant un nombre réel; d'où, par l'élimination de α,

$$L^2 \equiv 2P \pmod{13}.$$

Ainsi, lorsque l'un des nombres 11 ou 13 ne divise ni L ni N, pour qu'il soit résidu cubique (mod P), il faut et il suffit que l'on ait

$$L^2 \equiv 2, N^2 \equiv 2P \pmod{11 \text{ ou } 13}.$$

Cette condition implique que P soit non-résidu quadratique (mod 11 ou 13).