BULLETIN DE LA S. M. F.

PELLET

Sur les résidus cubiques et biquadratiques suivant un module premier

Bulletin de la S. M. F., tome 10 (1882), p. 157-162

<http://www.numdam.org/item?id=BSMF_1882__10__157_1>

Sur les résidus cubiques et biquadratiques, suivant un module premier; par M. A.-E. PELLET.

(Séance du 16 juin 1882.)

1. Soient 0 une racine de l'équation $\frac{x^p-1}{x-1}=0$, p étant un nombre premier, g une racine primitive de p, et e un diviseur de $p-1$; nous poserons

$$\frac{p-1}{e}=\omega.$$

$0^{g^{i+je}}$ ne prend que ω valeurs différentes lorsque, i étant constant, on fait varier j. Soit

$$s_i=\sum_{j=0}^{j=\omega-1}0^{g^{i+je}};$$

s_i admet e valeurs distinctes, qu'on obtiendra en donnant à i les valeurs 0, 1, 2, ..., $e-1$; ces e valeurs de s_i se transforment l'une dans l'autre, lorsqu'on remplace θ par une autre racine, θ^{g^k}, de $\frac{x^p-1}{x-1}=0$. Ces quantités s_i sont dites les périodes des racines d'ordre p de l'unité correspondant au diviseur e de $p-1$. Depuis Gauss, on connaît l'équation aux périodes pour e égal à l'un des trois nombres 2, 3, 4.

I. L'équation à deux périodes est

$$s^2+s+\frac{1-p}{4}=0 \quad \text{ou} \quad s^2+s+\frac{1+p}{4}=0,$$

suivant que $p-1$ est divisible ou non par 4.

II. L'équation à trois périodes est

$$\omega^3-3p\omega-p\mathrm{L}=0,$$

ω représentant $3s+1$, et L un nombre entier déterminé par l'équation $4p=\mathrm{L}^2+27\mathrm{M}^2$, avec la condition $\mathrm{L}\equiv 1 \pmod 3$.

III. L'équation à quatre périodes affecte deux formes différentes suivant que $p-1$ est ou n'est pas divisible par 8. Désignons dans l'un et l'autre cas par y une racine de l'équation

$$y^2+y+\frac{1-p}{4}=0,$$

et par a un nombre entier déterminé par l'équation

$$p=a^2+b^2,$$

avec la condition $a\equiv -1 \pmod 4$.

L'équation à quatre périodes est

$$s^2-ys-\frac{p-1+(a+1)(2+4y)}{16}=0,$$

si $p-1$ est divisible par 8;

$$s^2-ys+\frac{3p+1-(a+1)(2+4y)}{16}=0,$$

si $p-1$ n'est pas divisible par 8.

2. La fonction $\frac{x^p - 1}{x - 1}$ se décompose suivant le module premier q en $\frac{p-1}{\nu}$ facteurs irréductibles de degré ν, ν étant l'exposant auquel appartient q relativement au module p, c'est-à-dire le plus petit nombre tel que $q^\nu \equiv 1 \pmod{p}$ (SERRET, *Algèbre supérieure*, t. II). Le premier membre de l'équation aux e périodes des racines d'ordre p de l'unité se décompose en facteurs du premier degré, suivant le module premier q, si e divise $\frac{p-1}{\nu}$; dans le cas ou e ne divise pas $\frac{p-1}{\nu}$, le premier membre de l'équation aux e périodes admet des facteurs irréductibles de degré supérieur à 1.

Comme on connaît l'équation aux périodes pour e égal à 2, 3 ou 4, ce théorème permet souvent de voir si $\frac{p-1}{\nu}$ est divisible par l'un de ces trois nombres, c'est-à-dire si q est résidu quadratique, cubique et biquadratique suivant le module premier p.

D'ailleurs si $p - 1$ n'est pas divisible par 3, tout nombre q est résidu cubique mod. p; et si $p - 1$ n'est pas divisible par 4, tout nombre q résidu quadratique mod. p est aussi résidu biquadratique.

Ainsi, d'après I du n° 1, le nombre premier q est ou n'est pas résidu quadratique mod. p, suivant que la fonction

$$s^2 + s + \frac{1 - (-1)^{\frac{p-1}{2}} p}{4}$$

est ou n'est pas réductible suivant le mod. q; ou, si q est différent de 2, suivant que $(-1)^{\frac{p-1}{2}} p$ est ou n'est pas résidu quadratique suivant le mod. q. Ainsi les deux congruences

$$q^{\frac{p-1}{2}} \pm 1 \equiv 0 \pmod{p} \quad \text{et} \quad (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}} \pm 1 \equiv 0 \pmod{q}$$

ont lieu en même temps, en faisant correspondre les signes supérieurs entre eux, et de même pour les inférieurs. Ce qui se traduit dans le système de notation de Legendre par

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

et démontre le célèbre théorème auquel ce géomètre a attaché son nom. Cette démonstration a été donnée la première fois par M. Mathieu, dans le *Journal de Mathématiques pures et appliquées* (année 1867).

La seule fonction irréductible (mod. 2) du second degré est $x^2 + x + 1$; on en déduit facilement que 2 est résidu quadratique pour tous les nombres premiers de la forme $8k \pm 1$, et n'est pas résidu quadratique pour les nombres premiers de la forme $8k \pm 3$.

Si $p \equiv 1$ (mod. 3), pour que le nombre premier q soit résidu cubique suivant le module p, il faut et il suffit que la fonction $x^3 - 3px - pL$ se réduise suivant le module premier q, supposé différent de 3. Pour $q = 2$, on voit qu'il faut et suffit que L soit pair. L'entier L est déterminé par l'équation $L^2 + 27M^2 = 4p$, avec la condition $L \equiv 1$ (mod. 3). Si L est pair, M l'est aussi et p est de la forme $l^2 + 27m^2$; donc la condition nécessaire et suffisante pour que 2 soit résidu cubique de p est

$$p = l^2 + 27m^2;$$

lorsque $p - 1$ est divisible par 3.

2 n'est pas résidu quadratique pour les nombres premiers de la forme $4k + 1$, k étant impair; donc 2 ne peut être résidu biquadratique que pour les nombres premiers de la forme $8k + 1$, k pouvant être quelconque. Soient donc $p = 8k + 1$, a le nombre entier déterminé par l'équation $p = a^2 + b^2$, avec la condition $a \equiv -1$ (mod. 4); en se reportant au n° III du paragraphe précédent, on voit que la condition nécessaire et suffisante pour que 2 soit résidu biquadratique (mod. p) est que le nombre

$$\frac{4k - a - 1}{8},$$

qui est toujours entier, soit pair.

3. Pour qu'un nombre de la forme $a^n - 1$ soit premier, il est nécessaire que a soit égal à 2, et n premier. De ce qui précède on déduit facilement les propositions suivantes.

Si $n = 4q - 1$ est un nombre premier en même temps que $2n + 1$, le nombre $N = 2^n - 1$ est divisible par $2n + 1$.

Si $n = 4q + 1$ est un nombre premier en même temps que $6n + 1$, le nombre $N = 2^n - 1$ est divisible par $6n + 1$, pourvu qu'on puisse satisfaire à l'équation

$$6n + 1 = 4l^2 + 27m^2.$$

Un nombre de la forme $a^b + 1$ ne peut être premier que si b est égal à une puissance de 2. Les nombres premiers diviseurs de $2^{2^n} + 1$ sont de la forme $2^{n+1}m + 1 = p$; et il faut que 2 soit résidu d'une puissance $m^{\text{ième}}$ suivant ce module p. Ainsi 2 n'est pas résidu cubique suivant les deux nombres premiers

$$2^{12}.3 + 1 = 12289, \quad 2^{18}.3 + 1 = 786433,$$

car aucun d'eux n'est de la forme $l^2 + 27m^2$; ces nombres ne divisent par conséquent aucun nombre de la forme $2^{2^n} + 1$.

Caractère biquadratique de 2.

4. Soit un nombre premier impair $p = 2^{3+\alpha}m + 1$, m n'étant pas divisible par 2. Nous avons vu que, a étant déterminé par l'équation $p = a^2 + b^2$ avec la condition $a \equiv -1 \pmod 4$, 2 est résidu biquadratique ou non suivant que

$$\frac{2^{\alpha+2}m - a - 1}{8}$$

est un nombre pair ou impair. Si 2 est résidu biquadratique (mod. p), on a donc

$$a \equiv 2^{\alpha+2}m - 1 \pmod{16},$$

d'où

$$b^2 = p - a^2 \equiv -2^{2\alpha+4}m^2 + 2^{\alpha+4}m \pmod{32};$$

$2^{\alpha+4}m - 2^{2\alpha+4}m^2$ est divisible par 32, pour $\alpha = 0$ comme pour les valeurs de α supérieures à 0; donc b^2 est divisible par 64.

Si 2 n'est pas résidu biquadratique (mod. p), on a

$$a \equiv 2^{\alpha+2}m - 1 + 8 \equiv 2^{\alpha+2}m + 7 \pmod{16},$$

d'où

$$b^2 = p - a^2 \equiv -2^{2\alpha+4}m^2 - 3.2^{\alpha+4}m - 16 \pmod{32};$$

on en déduit $b^2 \equiv +16 \pmod{32}$. Donc, dans ce cas, b^2 n'est

pas divisible par une puissance de 2 supérieure à 16. Ainsi 2 *est résidu biquadratique pour les nombres premiers de la forme* $a^2 + 64b^2$; 2 *n'est pas résidu biquadratique pour les nombres premiers de la forme* $a^2 + 16b^2$, b *étant impair dans la dernière formule.* Ce caractère a déjà été donné par Lejeune-Dirichlet (*Journal de Liouville,* 1859); comme on voit, il découle facilement de la méthode précédente.