Séminaire Delange-Pisot-Poitou. Théorie des nombres

Dominique Bernardi

Résidus de puissances

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 2 (1977-1978), exp. n° 28, p. 1-12

<http://www.numdam.org/item?id=SDPP_1977-1978__19_2_A4_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 28, 12 p.

13 février 1978

RÉSIDUS DE PUISSANCES

par Dominique BERNARDI

[Université Paris-Sud, Orsay]

Introduction.

Dans ses Recherches arithmétiques, GAUSS démontre que 2 est un résidu cubique modulo un nombre premier de la forme $3n + 1$ si, et seulement si, ce nombre premier est représenté sur $\mathbb{Z}$ par la forme quadratique $X^2 + 27 Y^2$. Par la suite, de nombreux auteurs se sont penchés sur le problème de caractériser, par l'existence de solutions de certains systèmes diophantiens quadratiques, les nombres premiers p de la forme $\ell n + 1$, modulo lesquels, q est un résidu de puissance ℓ-ième, où q est un nombre entier et ℓ un nombre premier fixés. JACOBI [3] a complètement traité le cas $\ell = 3$, q premier, E. LEHMER a donné de tels critères pour $\ell = 5$, $q = 2, 3$ (cf. [4]) et LEONARD et WILLIAMS pour $\ell = 7$, $q = 2, 3, 5, 7$, et $\ell = 11$, $q = 2$ (cf. [5] et [7]). Ces résultats sont obtenus au coup par coup, et nécessitent de nombreux calculs.

Le résultat principal de ce travail est que de telles caractérisations existent toujours pour $\ell \leqslant 19$, c'est-à-dire quand l'anneau $\mathbb{Z}[\zeta_\ell]$ est principal, et q quelconque et non nécessairement premier, avec la restriction $\ell \nmid q$. On retrouve par cette méthode les résultats précédents (sauf $\ell = q = 3, 7$) et quelques autres. Toutefois les critères obtenus, s'ils permettent toujours l'établissement d'algorithmes numériques, deviennent rapidement très lourds quand ℓ ou q augmente.

Dans une première partie, on expose la méthode qui repose essentiellement sur le maniement des symboles de reste de puissance ℓ-ième et la loi générale de réciprocité relative à ces symboles. Dans la seconde, on traite explicitement les cas déjà connus relevant de cette méthode et les cas nouveaux suivants : $\ell = 3$, $q = 10$, $\ell = 5$, $q = 6$, et $\ell = 13$, $q = 2$.

1. Traitement du cas général.

(a) Notations. - Dans tout ce qui suit, ℓ est un nombre premier impair tel que le nombre de classes d'idéaux de $\mathbb{Q}(\zeta_\ell)$ soit égal à 1, c'est-à-dire $\ell = 3, 5, 7, 11, 13, 17$ ou 19 (cf. [9]). On désigne par :

$K = \mathbb{Q}(\zeta_\ell)$ le corps des racines ℓ-ièmes de l'unité,

G le groupe de Galois de l'extension $K/\mathbb{Q}$, identifié à $(\mathbb{Z}/\ell\mathbb{Z})^*$,

$A = \mathbb{Z}[\zeta_\ell]$ l'anneau des entiers de K,

$\lambda = 1 - \zeta_\ell$ un générateur de l'unique idéal premier de A divisant ℓ,

p un nombre premier congru à 1 modulo ℓ

q un nombre entier premier à p et à ℓ .

(b) L'équation $\pi\bar{\pi} = p$. - Dans K , p est décomposé en $\ell - 1$ facteurs premiers distincts conjugués deux à deux au sens de la conjugaison dans C , l'équation $(p) = \mathfrak{A}\bar{\mathfrak{A}}$, où l'inconnue $\mathfrak{A}$ est un idéal de A , a donc $2^{(\ell-1)/2}$ solutions.

PROPOSITION 1. - Si $(p) = \mathfrak{A}\bar{\mathfrak{A}}$, $\mathfrak{A}$ a un unique générateur congru à 1 modulo λ^2 vérifiant $p = \pi\bar{\pi}$.

Démonstration. - Soit $\mathfrak{p}$ un diviseur premier de p dans A , et ω un générateur de $\mathfrak{p}$. L'idéal $\mathfrak{A}$ est produit de certains conjugués de $\mathfrak{p}$, et le produit correspondant des conjugués de ω , noté $\varkappa$, est un générateur de $\mathfrak{A}$ et vérifie $\varkappa\bar{\varkappa} = N_{K/\mathbb{Q}}(\omega) = p$. En réduisant modulo λ , on trouve que $\varkappa$ est congru à ± 1 modulo λ . Les 2ℓ racines de l'unité contenues dans K parcourent les 2ℓ classes modulo λ^2 congrues à ± 1 modulo λ . En divisant $\varkappa$ par celle qui lui est congrue modulo λ^2 , on trouve un générateur π de $\mathfrak{A}$ tel que $\pi\bar{\pi} = p$, et π congru à 1 modulo λ^2 . Une autre solution s'écrirait πx , où x serait une unité de K telle que $x\bar{x} = 1$, c'est-à-dire une racine de l'unité, congrue à 1 modulo λ^2 , ce qui entraine $x = 1$.

Si maintenant H désigne l'ordre $\mathbb{Z} + \lambda^2 A$ de K , pour π tel que $\pi\bar{\pi} = p$, il est équivalent de dire que π est dans H , ou que π est congru à ± 1 modulo λ^2 . D'après ce qui précède, l'équation $\pi\bar{\pi} = p$ a exactement $2^{(\ell+1)/2}$ solutions dans H .

(c) Le symbole de reste de puissance ℓ-ième. - Le groupe $\{\pm 1\} \times G$ agit sur l'ensemble des solutions dans H de l'équation $\pi\bar{\pi} = p$. On notera S un système de représentants des orbites de cette action. Si σ appartient à G , on a $\sigma(q/\pm\pi)_\ell = (q/\sigma\pi)_\ell$. Si π appartient à une orbite dégénérée, c'est-à-dire dont le nombre d'éléments est strictement inférieur à $2(\ell - 1)$, il existe $\sigma \in G$, $\sigma \neq 1$, tel que $\sigma(q/\pi)_\ell = (q/\sigma\pi)_\ell = (q/\pi)_\ell$. Donc $(q/\pi)_\ell$ étant une racine ℓ-ième de l'unité est nécessairement égal à 1 .

On notera S' un système de représentants des orbites non dégénérées.

PROPOSITION 2. - Pour que q soit un résidu de puissance ℓ-ième modulo p , il faut et il suffit que, pour tout π dans S' , on ait $(q/\pi)_\ell = 1$.

Démonstration. - Si $q = x^\ell + kp$, on a $(q/\pi)_\ell = (x/\pi)_\ell^\ell = 1$.

Inversement, si, pour tout π dans S' , on a $(q/\pi)_\ell = 1$, les remarques précédentes montrent que, pour tout idéal $\mathfrak{A}$ de A tel que $\mathfrak{A}\bar{\mathfrak{A}} = (p)$, on a $(q/\mathfrak{A})_\ell = 1$. Soit $\mathfrak{A}$ un tel idéal, vérifiant $\mathfrak{p}|\mathfrak{A}$, et $\mathfrak{B} = \mathfrak{A}.\bar{\mathfrak{p}}.\mathfrak{p}^{-1}$. Alors $\mathfrak{B}$ est une autre solution et l'on a :

$$1 = \left(\frac{q}{\mathfrak{A}}\right) = \left(\frac{q}{\mathfrak{B}}\right) \Longrightarrow \left(\frac{q}{\mathfrak{p}}\right) = \left(\frac{q}{\bar{\mathfrak{p}}}\right) = \overline{\left(\frac{q}{\mathfrak{p}}\right)} \text{ , donc } \left(\frac{q}{\mathfrak{p}}\right)_\ell = 1 \text{ .}$$

Or $A/\mathfrak{p}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, donc l'égalité $(q/\mathfrak{p})_\ell = 1$ entraîne que q est une puissance ℓ-ième modulo $\mathfrak{p}$ ou encore modulo p.

PROPOSITION 3. - Si π est un élément de H tel que $\pi\bar{\pi} = p$, on a

$$\left(\frac{q}{\pi}\right)_\ell = \left(\frac{\pi}{q}\right)_\ell .$$

Démonstration. - On peut supposer π congru à 1 modulo λ^2. Comme π et q sont premiers entre eux, on a :

$$\left(\frac{q}{\pi}\right)_\ell = \left(\frac{\pi}{q}\right)_\ell \prod_v (\pi , q)_v ,$$

où v parcourt les places archimédiennes et les diviseurs de ℓ. Comme K n'a pas de plongement réel, les symboles de Hilbert relatifs aux places archimédiennes valent toujours 1. Le seul diviseur premier de ℓ est λ, et on a $q^{\ell-1}$ congru à 1 modulo ℓ, donc $q^{1-\ell}$ congru à 1 modulo $\lambda^{\ell-1}$. D'où

$$(\pi , q)_\lambda = (\pi , q^{1-\ell})_\lambda = 1 , \text{ car } \pi \in U_2 \text{ et } q^{1-\ell} \in U_{\ell-1} .$$

PROPOSITION 4. - Il existe un nombre fini de sous-groupes d'indice fini de A, notés H_i, $i \in (1 , N)$, tels que tout élément α de A premier à q appartienne à l'un des H_i, et à un seul, et tels que $(\alpha/q)_\ell$ ne dépende que de cet H_i.

Démonstration. - Le groupe $(\mathbb{Z}/q\mathbb{Z})^*$ est un sous-groupe de $(A/qA)^*$. Soit $(\alpha_i)_{i\in\{1,N\}}$ un système de représentants des classes de $(A/qA)^*$ modulo ce sous-groupe. Posons $H_i = \{x \in A ; \exists\, k \in \mathbb{Z} , x \equiv k\alpha_i \text{ modulo } q\}$. Alors H_i est un sous-groupe de A, et l'inclusion $H_i + qA \subset H_i$ montre que H_i est de rang maximal, donc d'indice fini dans A.

Si x est premier à q, l'élément x de $(A/qA)^*$ est congru à l'un des α_i, et à un seul. Donc x appartient à H_i et n'appartient pas à H_j, pour $j \neq i$. Enfin

$$\left(\frac{x}{q}\right)_\ell = \left(\frac{k}{q}\right)_\ell \left(\frac{\alpha_i}{q}\right)_\ell \quad \text{avec } k \in \mathbb{Z} \text{ et } (k , q) = 1 .$$

Si $\sigma \in G$, $\sigma \neq 1$, on a

$$\left(\frac{k}{q}\right)_\ell = \left(\frac{\sigma k}{\sigma q}\right)_\ell = \sigma\left(\frac{k}{q}\right)_\ell , \text{ donc } \left(\frac{k}{q}\right)_\ell = 1 .$$

On en déduit $(x/q)_\ell = (\alpha_i/q)_\ell$.

Remarque 1. - Au lieu de $\mathbb{Z}/q\mathbb{Z}$, on aurait pu utiliser n'importe quel sous-anneau C de A/qA vérifiant : $\forall\, x \in C^*$, $(x/q)_\ell = 1$.

Par exemple, si q est un nombre premier inerte, A/qA est isomorphe à $\mathbb{F}_{q^{\ell-1}}$, et on peut prendre $C = \mathbb{F}_{q^{(\ell-1)/2}}$. Cet exemple se généralise, et pour tout q, on peut prendre $C = B/qB$, où $B = \mathbb{Z}[\zeta_\ell + \zeta_\ell^{-1}]$ est l'anneau des entiers du sous-corps réel maximal de K. Ce procédé permet de réduire le nombre des H_i à considérer.

Remarque 2. - Si $\pi\bar{\pi} = p$, π appartient à l'un des H_i, et un seul, mais on

peut être sûr que le α_i correspondant vérifie $\alpha_i \bar{\alpha}_i \in \mathbb{Z}/q\mathbb{Z}$, ce qui permet aussi de réduire le nombre des H_i à considérer. Toutefois, les deux procédés de réduction ne peuvent être utilisés simultanément.

Remarque 3. - Posons, pour tout i, $L_i = H \cap H_i$, et choisissons, pour tout i, une base du groupe abélien libre L_i, $\{a_1^i, \dots, a_{\ell-1}^i\}$. Soit d'autre part $\{1, b_2, \dots, b_{(\ell-1)/2}\}$ une base de l'anneau B défini plus haut. L'équation $\pi\bar{\pi} = p$, $\pi \in L_i$, s'écrit dans ces bases comme un système de $(\ell - 1)/2$ équations diophantiennes quadratiques, i. e.

$$\Phi_i \begin{cases} p \doteq \varphi_1^i(x_1, \dots, x_{\ell-1}) \\ 0 = \varphi_2^i(x_1, \dots, x_{\ell-1}) \\ \dots \\ 0 = \varphi_{(\ell-1)/2}^i(x_1, \dots, x_{\ell-1}) \end{cases},$$

où $\pi = \sum_{k=1}^{\ell-1} x_k a_k^i$ et où les $x_1, \dots, x_{\ell-1}$ sont des variables entières, les φ_j^i des formes quadratiques à coefficients entiers.

THÉORÈME. - *Il existe un nombre fini de systèmes quadratiques Φ_i tels que q soit une puissance ℓ-ième modulo p si, et seulement si, aucun des Φ_i n'a de solution.*

Démonstration. - Considérant les ystèmes Φ_i correspondant aux H_i tels que $(\alpha_i/q)_\ell \neq 1$, on obtient l'ensemble cherché. En effet, si l'un d'eux a une solution, il existe un élément π de H tel que $(\pi/q)_\ell = (\alpha_i/q)_\ell = 1$ et $\pi\bar{\pi} = p$, et réciproquement. Or la proposition 2 établit que ceci est équivalent au fait que q n'est pas résidu de puissance ℓ-ième modulo p.

Remarque 4. - Le groupe G opère sur l'ensemble des H_i, et on peut, dans l'utilisation du théorème précédent, ne retenir qu'un représentant par orbite.

Remarque 5. - Dans les cas $\ell = 3$ (respectivement $\ell = 5$), les solutions dans H de $\pi\bar{\pi} = p$ forment une seule orbite. On peut donc renverser le théorème précédent, et, en prenant un représentant par orbite des H_i, affirmer qu'il existe une suite finie de formes (respectivement de systèmes) quadratiques Φ_i, $i \in [1, \dots, N, N+1, \dots, M]$, dont un, et un seul, représente p, les p représentés par l'un des N premiers étant ceux modulo lesquels q est un résidu cubique (respectivement de puissance cinquième).

Remarque 6. - Le théorème précédent permet effectivement de déterminer, en un nombre fini d'opérations, si q est un résidu de puissance ℓ-ième modulo p. Plus précisément on a la proposition suivante.

PROPOSITION 5. - *Si on prend pour B la base*

$$\{1, \zeta^2 + \zeta^{-2}, \zeta^3 + \zeta^{-3}, \dots, \zeta^{(\ell-1)/2} + \ell^{(1-\ell)/2}\},$$

la première forme intervenant dans chacun des systèmes Φ_i est définie positive.

Démonstration. - On peut prendre pour A la base ζ , ζ^2 , ... , $\zeta^{\ell-1}$. Alors, la matrice de la première forme a tous ses coefficients nuls excepté la diagonale formée de 1 , la sur-diagonale et la sous-diagonale formée de $-1/2$. Son mineur fondamental de rang n vaut $2^{-n}(n+1)$, donc est strictement positif. La forme sur A est définie positive ; pour tout i , sa restriction φ_1^i à L_i l'est aussi.

2. Exemples d'applications.

(a) $\ell = 3$

Dans ce cas il y a une seule orbite, et les systèmes comprennent une seule forme quadratique de deux variables. L'anneau A a pour base $\{1 , \zeta_3\}$, et le module H admet la base $\{1 , 3\zeta_3\}$, enfin pour $\pi = X + 3\zeta_3 Y$, on a $\pi\bar{\pi} = X^2 - 3XY + 9Y^2$.

1° Si $q = 2$. - $A/2A \simeq F_4$. Seul 1 vérifie $(\alpha/2) = 1$, les deux autres restes non nuls forment une seule orbite sous l'action de G . On peut prendre $\alpha_1 = 1$, $\alpha_2 = \zeta_3$

$$H_1 = \{X + \zeta_3 Y ; \quad Y \equiv 0 \quad \text{modulo} \quad 2\} ,$$

$$H_2 = \{X + \zeta_3 Y ; \quad X \equiv 0 \quad \text{modulo} \quad 2\} .$$

L_1 et L_2 admettent respectivement pour base $\{1 , 6\zeta_3\}$, $\{2 , 3\zeta_3\}$ et les formes quadratiques correspondantes sont respectivement

$$X^2 - 6XY + 36Y^2 \quad \text{et} \quad 4X^2 - 6XY + 9Y^2 .$$

On obtient donc, après remplacement de ces formes par des formes équivalentes, le résultat suivant : Tout nombre premier congru à 1 modulo 3 est représenté par l'une des formes $X^2 + 27Y^2$ et $4X^2 + 2XY + 7Y^2$, et par une seulement. Ceux qui sont représentés par la première sont ceux modulo lesquels 2 est un résidu cubique.

2° Si $q = 5$. - $A/5A \simeq F_{25}$. Ce dernier a 24 éléments inversibles formant 6 classes modulo $(\mathbb{Z}/5\mathbb{Z})^*$, parmi lesquelles 2 vérifient $(\alpha/5) = 1$, et les quatre autres forment deux orbites sous l'action de G . Choisissons un représentant par orbite, soit :

$$\alpha_1 = 1 , \quad \alpha_2 = 1 + 2\zeta_3 , \quad \alpha_3 = \zeta_3 , \quad \alpha_4 = 1 - \zeta_3 .$$

Alors

$$H_1 = \{X + \zeta_3 Y ; \quad Y \equiv 0 \quad \text{modulo} \quad 5\} ,$$

$$H_2 = \{X + \zeta_3 Y ; \quad 2X - Y \equiv 0 \quad \text{modulo} \quad 5\} ,$$

$$H_3 = \{X + \zeta_3 Y ; \quad X \equiv 0 \quad \text{modulo} \quad 5\} ,$$

$$H_4 = \{X + \zeta_3 Y ; \quad X + Y \equiv 0 \quad \text{modulo} \quad 5\} ,$$

et on trouve de même quatre formes

$$\varphi_1 = X^2 + XY + 169Y^2 ,$$

$$\varphi_2 = 13\,X^2 + XY + 13\,Y^2 ,$$

$$\varphi_3 = 9\,X^2 + 3\,XY + 19\,Y^2 ,$$

$$\varphi_4 = 7\,X^2 + 5\,XY + 25\,Y^2 ,$$

Tout nombre premier congru à 1 modulo 3 est donc représenté par une, et une seule, des quatre formes précédentes. Ceux qui sont représentés par l'une des deux premières sont ceux modulo lesquels 5 est un résidu cubique.

3° Si $q = 7$. - $A/7A \simeq F_7 \times F_7$. Cet anneau a 36 éléments inversibles répartis en six classes modulo $(\mathbb{Z}/7\mathbb{Z})^*$, formant à nouveau quatre orbites, dont deux telles que $(\alpha/7) = 1$. On peut prendre $\alpha_1 = 1$, $\alpha_2 = 1 + 2\,\zeta_3$, $\alpha_3 = \zeta_3$, $\alpha_4 = 1 - 3\,\zeta_3$, d'où quatre nouvelles formes :

$$\varphi_1 = X^2 + XY + 331\,Y^2 ,$$

$$\varphi_2 = 19\,X^2 + 11\,XY + 19\,Y^2 ,$$

$$\varphi_3 = 9\,X^2 + 3\,XY + 37\,Y^2 ,$$

$$\varphi_4 = 13\,X^2 + 9\,XY + 27\,Y^2 .$$

Tout nombre premier congru à 1 modulo 3 est représenté par une et une seule des quatre formes précédentes. Ceux qui sont représentés par l'une des deux premières sont ceux modulo lesquels 7 est un résidu cubique.

De manière générale, si q est un nombre premier différent de 3 , il existe $2(q - 1)/3$ (ou $2(q + 1)/3$ selon lequel de ces deux nombres est entier) formes quadratique telles que tout nombre premier p congru à 1 modulo 3 soit représenté par exactement l'une d'entre elles, la moitié de celles-ci représentant les p modulo lesquels q est un résidu cubique.

4° Si $q = 10$. - $A/10A \simeq F_4 \times F_{25}$. Cet anneau a 72 éléments inversibles répartis en 18 classes modulo $(\mathbb{Z}/10\mathbb{Z})^*$, formant dix orbites, dont quatre vérifient $(\alpha/10) = 1$. Les formes correspondantes sont :

$$\varphi_1 = X^2 + 675\,Y^2 \qquad \varphi_2 = 25\,X^2 + 27\,Y^2$$

$$\varphi_3 = 9\,X^2 + 6\,XY + 76\,Y^2 \qquad \varphi_4 = 27\,X^2 + 18\,XY + 28\,Y^2$$

$$\varphi_5 = 13\,X^2 + 2\,XY + 52\,Y^2 \qquad \varphi_6 = 25\,X^2 + 20\,XY + 31\,Y^2$$

$$\varphi_7 = 4\,X^2 + 2\,XY + 169\,Y^2 \qquad \varphi_8 = 19\,X^2 + 6\,XY + 36\,Y^2$$

$$\varphi_9 = 28\,X^2 + 10\,XY + 35\,Y^2 \qquad \varphi_{10} = 7\,X^2 + 4\,XY + 97\,Y^2$$

Tout nombre premier congru à 1 modulo 3 est représenté par une de ces dix formes, et une seule. Ceux qui sont représentés par l'une des quatre premières formes, sont ceux, modulo lesquels, 10 est un résidu cubique. Ceux qui sont représentés par l'une des deux premières formes sont ceux, modulo lesquels, 2 et 5 sont des résidus cubiques.

(b) $\ell = 5$.

Dans ce cas encore, il y a une seule orbite, mais les systèmes comprennent deux formes quadratiques de quatre variables. Prenons pour A la base normale engendrée par $\zeta = \zeta_5$, et pour B la base $\{1 , \zeta^2 + \zeta^3\}$. Posons alors $\pi = Q\zeta + R\zeta^2 + S\zeta^3 + T\zeta^4$, si π est dans H et $\pi\bar{\pi} = p$, π est congru à $\pm 1 + a\lambda^2$ modulo λ^3 . Il en est encore de même de $\bar{\pi}$, et p est congru à $1 \pm 2a\lambda^2$ modulo λ^3 . On a donc en fait a divisible par λ et π congru à ± 1 modulo λ^3 . L'équation $\pi\bar{\pi} = p$, π dans H , s'écrit donc :

$$(1) \qquad \begin{cases} p = Q^2 + R^2 + S^2 + T^2 - QR - RS - ST \\ 0 = QS + RT + TQ - QR - RS - ST \\ 0 \equiv Q + 2R - 2S - T \mod 5 \\ 0 \equiv Q - R - S + T \mod 5 \end{cases} .$$

Il est alors légitime d'introduire les nouvelles variables (cf. [2])

$$(*) \qquad \begin{cases} X = Q + R + S + T \\ 5U = Q + 2R - 2S - T \\ 5V = 2Q - R + S - 2T \\ 5W = Q - R - S + T \end{cases} ,$$

ce qui donne le système

$$(2) \qquad \begin{cases} 16\,p = X^2 + 50\,U^2 + 50\,V^2 + 125\,W^2 \\ 0 = U^2 + 4\,UV - V^2 - XW \end{cases} ,$$

et on voit facilement que le système (*) établit une bijection entre les solutions en entiers de (1) et de (2).

1° Si $q = 2$. - $A/2A \simeq F_{16}$. Le seul élément de F_{16} qui vérifie à la fois $\alpha\bar{\alpha} = \alpha^5 = 1$ et $(\alpha/2)_5 = \alpha^{(16-1)/5} = \alpha^3 = 1$ est 1 lui-même, qui est aussi le seul élément de F_{16} vérifiant $\alpha\bar{\alpha} = 1$ et $\alpha = \bar{\alpha}$. Donc si $\pi\bar{\pi} = p$, on a $(\pi/2) = 1$ si, et seulement si, π est congru à $\bar{\pi}$ modulo 2 , c'est-à-dire si $Q \equiv T$ et $R \equiv S$ modulo 2 , ou encore, dans le cas où π appartient à H , si X , U , V , W sont tous quatre divisibles par 2 . L'équation s'écrit alors

$$4\,p = X'^2 + 50\,U'^2 + 50\,V'^2 + 125\,W'^2$$
$$0 = U'^2 + 4\,U'V' - V'^2 - X'W' .$$

On peut alors remarquer (cf. [4]) que la réduction modulo 8 donne $X' \equiv W' \equiv 0$ modulo 2 et $U' \equiv V'$ modulo 2 . Posant alors $X' = 2x$, $U' = u + v$, $V' = u - v$ et $W' = 2w$, on obtient le critère cherché : 2 est un résidu de puissance cinquième modulo $p = 5n + 1$ si, et seulement si, le système

$$\begin{cases} p = x^2 + 25\,u^2 + 25\,v^2 + 125\,w^2 \\ 0 = u^2 + uv - v^2 - xw \end{cases}$$

a une solution dans $\underset{\sim}{Z}^4$.

2° Si $q = 3$. - $A/3A \simeq F_{81}$. Les 20 éléments tels que $\alpha\bar{\alpha} = \alpha^{10} = 1$ se répartissent en 5 classes modulo ceux qui appartiennent à F_9^* , et une seule de ces classes vérifie $(\alpha/3) = 1$. On en déduit que 3 est un résidu de puissance cinquième modulo p si, et seulement si, π est congru à $\bar{\pi}$ modulo 3 , c'est-à-dire $Q \equiv T$ et $R \equiv S$ modulo 3 , ou encore $U = V = 0$ modulo 3 . On a donc démontré que 3 est un résidu de puissance cinquième modulo $p = 5n + 1$ si, et seulement si, le système

$$\begin{cases} 16\,p = x^2 + 450\,u^2 + 450\,v^2 + 125\,w^2 \\ 0 = 9(u^2 + 4\,uv - v^2) - xw \end{cases}$$

a une solution dans $\underset{\sim}{Z}^4$.

3° Si $q = 6$. - $A/6A \simeq F_{16} \times F_{81}$. Parmi les 1 200 éléments inversibles de cet anneau, 100 vérifient $\alpha\bar{\alpha} \in (\underset{\sim}{Z}/6\underset{\sim}{Z})^*$. Parmi ces derniers, 4 sont dans $F_4 \times F_9 \simeq B/6B$. On a donc 25 classes intéressantes dont 5 vérifient $(\alpha/6) = 1$. Ces dernières forment deux orbites ; celle de 1 et celle de $3\zeta^2 + 2\zeta^4$. On obtient donc deux systèmes distincts. Le premier correspond à la classe de 1 , c'est-à-dire à la conjonction des deux cas précédents. Le sytème

$$\begin{cases} p = x^2 + 225\,u^2 + 225\,v^2 + 125\,w^2 \\ 0 = 9(u^2 + uv - v^2) - xw \end{cases}$$

a une solution dans $\underset{\sim}{Z}^4$ si, et seulement si, 2 et 3 sont des résidus de puissance cinquième modulo p . Le deuxième cas s'écrit $(3\zeta^2 + 2\zeta^4)^{-1}\pi \equiv (3\zeta^2 + 2\zeta^4)^{-1}\bar{\pi}$ modulo 6 , soit $S \equiv 3Q$ et $2R \equiv 2Q + 3T$ modulo 6 . Le module L des quadruplets d'entiers vérifiant ces congruences ainsi que

$$Q + 2\,R - 2\,S - T \equiv Q - R - S - T \equiv 0 \quad \text{modulo } 5$$

est donné par :

$$\begin{bmatrix} Q \\ R \\ S \\ T \end{bmatrix} = \begin{bmatrix} -2 & 1 & 3 & 4 \\ -1 & 1 & 3 & 1 \\ -2 & 1 & 3 & 3 \\ 0 & 1 & -2 & 0 \end{bmatrix} \begin{bmatrix} 15\,X \\ 6\,Y \\ Z \\ 2\,T \end{bmatrix}$$

et on obtient le système

$$\begin{cases} p = 1\,125\,X^2 + 36\,Y^2 + 19\,Z^2 + 76\,T^2 - 180\,XY \\ \qquad\qquad - 240\,XZ - 570\,XT + 6\,YZ + 48\,YT + 54\,ZT \\ 0 = 3\,Z^2 - 4\,T^2 - 18\,XY - 24\,XZ + 18\,XT + 6\,YZ + 4\,ZT \end{cases}$$

qui a une solution dans $\underset{\sim}{Z}^4$ si, et seulement si, 6 est un résidu de puissance cinquième modulo p , sans que 2 , ou 3 , le soit. Par exemple, pour $p = 31$, la

solution de (1) est par exemple $6, 3, 0, 2$, et $1, 1, 2, 3$ est une solution du système précédent. Modulo 31, on a $(-5)^5 \equiv 6$, tandis que $2^{(31-1)/5} \equiv 64 \equiv 2 \not\equiv 1$.

(c) $\ell = 7$.

Dans ce cas, il y a une orbite non dégénérée (à 12 éléments) et une dégénérée à 4 éléments. Prenons pour A la base normale engendrée par $\zeta = \zeta_7$, et pour B la base $\{1, \zeta + \zeta^6, \zeta^2 + \zeta^5\}$, et posons $\pi = \sum_1^6 c_i \zeta^i$. Si $\pi\bar{\pi} = p$ et $\pi \in H$, les nombres $\sum_1^6 ic_i$, $\sum_1^6 i^2 c_i$, et $\sum_1^6 i^4 c_i$ sont divisibles par 7. On pose alors (cf. [2] et [6])

$$a_1 = c_1 c_4 + c_2 c_5 + c_3 c_6 + c_5 c_1 + c_6 c_2$$
$$a_2 = c_1 c_2 + c_2 c_3 + c_3 c_4 + c_4 c_5 + c_5 c_6$$
$$a_3 = c_1 c_3 + c_2 c_4 + c_3 c_5 + c_4 c_6 + c_6 c_1$$
$$x_1 = c_1 + c_2 + c_3 + c_4 + c_5 + c_6$$
$$x_2 = c_1 - c_6$$
$$x_3 = c_2 - c_5$$
$$x_4 = c_3 - c_4$$
$$7\,x_5 = c_1 + c_2 - 2c_3 - 2c_4 + c_5 + c_6$$
$$7\,x_6 = c_1 - c_2 - c_5 + c_6 .$$

L'équation $\pi\bar{\pi} = p$ s'écrit, pour π dans H,

$$(3)\quad \begin{cases} p = c_1^2 + c_2^2 + c_3^2 + c_4^2 + c_5^2 + c_6^2 - a_1 \\ 0 = a_2 - a_1 \\ 0 = a_3 - a_1 \\ 0 \equiv c_1 + 2c_2 + 3c_3 - 3c_4 - 2c_5 - c_6 \ \text{modulo } 7 \\ 0 \equiv c_1 - 3c_2 + 2c_3 + 2c_4 - 3c_5 + c_6 \ \text{modulo } 7 \\ 0 \equiv c_1 + 2c_2 - 3c_3 - 3c_4 + 2c_5 + c_6 \ \text{modulo } 7 \end{cases}$$

ou encore

$$(4)\quad \begin{cases} 72\,p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_3^2) \\ 0 = 12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 - 56x_1x_6 + 24x_2x_3 - 24x_2x_4 \\ \qquad + 48x_3x_4 + 98x_5x_6 \\ 0 = 12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 - 28x_1x_5 - 28x_1x_6 + 48x_2x_3 \\ \qquad + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 \end{cases}$$

et la correspondance ci-dessus induit encore une bijection entre les solutions en entiers de (3) et de (4). Les auteurs de [6] montrent que l'orbite dégénérée est donnée par les solutions "triviales"

$$(x_1 , x_2 , x_3 , x_4 , x_5 , x_6) = \pm(6t , \pm 2u , \pm 2u , \mp 2u , 0 , 0) ,$$

où $p = t^2 + 7u^2$. L'orbite non dégénérée est obtenue à partir d'un de ses éléments par l'action du groupe $\{\pm 1\} \times G$, soit :

$$(y_1 , y_2 , y_3 , y_4 , y_5 , y_6) = (x_1 , x_2 , x_3 , x_4 , x_5 , x_6) \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1/2 & -1/2 \\ 0 & 0 & 0 & 0 & -3/2 & -1/2 \end{bmatrix}^k$$

où $k = 1 , 2 , 3 , 4 , 5 , 6$. Nous exprimerons les critères obtenus sous forme de congruences portant sur une solution non triviale représentée par la suite des x_i correspondants. On pourrait, conformément au théorème général, construire des systèmes quadratiques mais les résultats seraient beaucoup plus encombrants.

1° Si $q = 2$. - $A/2A \simeq F_8 \times F_8$. Parmi les 49 éléments inversibles, 7 vérifient $\alpha\bar{\alpha} = 1$, et parmi ceux-ci seul 1 vérifie $(\alpha/2)_7 = 1$. C'est aussi le seul élément tel que $\alpha\bar{\alpha} = 1$ et $\alpha = \bar{\alpha}$. On a donc $(\pi/2)_7 = 1$ si, et seulement si, $\pi \equiv \bar{\pi}$ modulo 2 , c'est-à-dire si, et seulement si, $c_1 \equiv c_6$, $c_2 \equiv c_5$, $c_3 \equiv c_4$ modulo 2 , ou encore 2 est un résidu de puissance septième modulo $p = 7n + 1$ si, et seulement si, on a $x_2 \equiv x_3 \equiv x_4 \equiv 0$ modulo 2 , où $(x_1,x_2,x_3,x_4,x_5,x_6)$ est une solution "non triviale" de (4).

2° Si $q = 3$. - $A/3A \simeq F_{729}$. Les 56 éléments non nuls qui vérifient $\alpha\bar{\alpha} = \pm 1$ se répartissent en sept classes modulo F_9^* , seule la classe principale vérifiant $(\alpha/3)_7 = 1$. L'image de π est dans F_9^* si, et seulement si, $c_1 \equiv c_2 \equiv c_4$, $c_3 \equiv c_5 \equiv c_6$ modulo 3 , ou encore $x_1 \equiv x_5 \equiv x_6 \equiv 0$, $x_2 \equiv x_3 \equiv -x_4$ modulo 3 , ce qui représente une condition nécéssaire et suffisante portant sur une solution non triviale de (4) pour que 3 soit un résidu de puissance septième modulo $p = 7n + 1$.

3° Si $q = 5$. - $A/5A \simeq F_{15625}$. Les 504 éléments vérifient $\alpha\bar{\alpha} \in F_5^*$ se répartissent en 21 classes modulo F_{25}^* , dont trois vérifient $(\alpha/5)_7 = 1$, c'est-à-dire les classes de 1 , de η et de $\bar{\eta}$, où η est une racine primitive neuvième de l'unité dans F_{15625} . Posons $M = \{\alpha \in F_{15625} ; \alpha + \alpha^{25} + \alpha^{625} = 0\}$, alors $M = \eta F_{25} + \bar{\eta} F_{25}$. De plus, si $\alpha = x\eta + y\bar{\eta}$, et $\alpha\bar{\alpha} \in F_5^*$, on a $x^2+y^2+(\eta+\bar{\eta})xy \in F_5^*$, donc x ou y est nul et α est dans l'une des classes ηF_{25}^* ou $\bar{\eta} F_{25}^*$. En résumé, si $\alpha\bar{\alpha} \in F_5^*$, on a $(\alpha/5)_7 = 1$ si, et seulement si, $\alpha \in F_{25}$ ou bien $\alpha \in M$. On en déduit que $(\pi/5)_7 = 1$ si, et seulement si, on a $c_1 \equiv c_2 \equiv c_4$, $c_3 \equiv c_5 \equiv c_6$ modulo 5 ou bien $c_1 + c_2 + c_4 \equiv c_3 + c_5 + c_6 \equiv 0$ modulo 5 , ou encore 5 est un résidu de puissance septième modulo $p = 7n + 1$ si, et seulement si, une solution non triviale quelconque de (4) vérifie l'une des conditions suivantes :

$$x_5 \equiv x_6 \equiv 0 \quad \text{et} \quad x_2 \equiv x_3 \equiv -x_4 ,$$

ou bien

$$x_1 \equiv 0 \quad \text{et} \quad x_2 + x_3 - x_4 \equiv 0 \ ,$$

toutes les congruences étant prises modulo 5 .

(d) $\ell = 11$.

Posons $\pi = \sum_{k=1}^{10} c_k \zeta^k$ et $c_{11} = 0$, $c_{k+11} = c_k$. Si $a_j = \sum_{k=1}^{10} c_k c_{k+j}$, $j \in \{1 , 2 , 3 , 4\}$, le système $\pi\bar{\pi} = p$, π dans H , s'écrit :

$$\begin{cases} p = \sum_{k=1}^{10} c_k^2 - a_1 \\ a_1 = a_2 = a_3 = a_4 \\ \sum_{k=1}^{10} kc_k \equiv \sum_{k=1}^{10} k^2 c_k \equiv \sum_{k=1}^{10} k^4 c_k \equiv 0 \quad \text{modulo} \quad 11 \end{cases}$$

les deux dernières congruences étant "en prime", car ce sont des conséquences des équations et de $\sum_{k=1}^{10} kc_k \equiv 0$ modulo 11 . Ce système a donc 64 solutions, dont quatre "triviales" $(u , v , u , u , u , v , v , v , u , v)$, où (u , v) est une des quatres solutions de $p = 3u^2 + 3v^2 - 5uv$. Les 60 autres sont engendrées à partir de trois d'entre elles, notées $(c_k^i)_{k \in (1,10)}$, $i \in \{1 , 2 , 3\}$, par l'opération de $\{\pm 1\} \times G$.

Pour $q = 2$, $A/2A$ est isomorphe à F_{1024} . Les 33 éléments qui vérifient $\alpha\bar{\alpha} = 1$ se répartissent en 11 classes modulo F_4^* . Seule la classe de 1 vérifie $(\alpha/2)_{11} = 1$, donc 2 est un résidu de puissance onzième modulo $p = 11m + 1$ si, et seulement si, pour $i \in \{1 , 2 , 3\}$, on a :

$$\begin{matrix} c_1^i \equiv c_4^i \equiv c_5^i \equiv c_9^i \equiv c_3^i \\ c_2^i \equiv c_8^i \equiv c_{10}^i \equiv c_7^i \equiv c_6^i \end{matrix} \quad \text{modulo} \quad 2 \ .$$

Dans les notations de [9], cela revient à dire que, pour $i \in \{1 , 2 , 3\}$, on a:

$$\begin{matrix} x_1^i \equiv x_6^i \equiv x_7^i \equiv x_8^i \equiv x_9^i \equiv x_{10}^i \\ x_2^i \equiv x_3^i \equiv x_4^i \equiv x_5^i \equiv 0 \end{matrix} \quad \text{modulo} \quad 2 \ ,$$

certaines de ces conditions étant superfétatoires. Cette dernière caractérisation n'est pas plus difficile à mettre en oeuvre que celle de [6].

(e) $\ell = 13$.

Posons encore $\pi = \sum_{k=1}^{12} c_k^k$ et $c_{13} = 0$, $c_{k+13} = c_k$. Si $a_j = \sum_{k=1}^{12} c_k c_{k+j}$, $j \in \{1 , 2 , 3 , 4 , 5\}$, le système $\pi\bar{\pi} = p$, π dans H , s'écrit :

$$\begin{cases} p = \sum_{k=1}^{12} c_k^2 - a_1 \\ a_1 = a_2 = a_3 = a_4 = a_5 \\ \sum_{k=1}^{12} kc_k \equiv \sum_{k=1}^{12} k^2 c_k \equiv \sum_{k=1}^{12} k^4 c_k \equiv 0 \quad \text{modulo} \quad 13 \end{cases}$$

avec la même remarque. Ce système a donc 128 solutions, dont huit "triviales" $(a , b , a , c , b , b , d , d , a , c , d , c)$ où (a , b , c , d) est une des huit solutions de

$$\begin{cases} p = 3a^2 + 2b^2 + 3c^2 + 2d^2 - 2ab - 2ac - 2cd - bd - ad - bc \\ 0 = a^2 - b^2 + c^2 - d^2 - ab - ac - cd + bd + ad + bc \end{cases}.$$

Les 120 autres sont engendrées à partir de cinq d'entre elles, notées $(c_k^i)_{k\in(1,12)}$, $i \in \{1 , 2 , 3 , 4 , 5\}$, par l'opération de $\{\pm 1\} \times G$.

Pour $q = 2$, $A/2A$ est isomorphe à F_{4096} . Parmi les 65 éléments tels que $\alpha\bar{\alpha} = 1$, cinq vérifient $(\alpha/2)_{13} = 1$, et ce sont les éléments de F_{16} tels que $\alpha\bar{\alpha} = 1$. Donc 2 est un résidu de puissance treizième modulo $p = 13n + 1$ si, et seulement si, pour $i \in \{1 , 2 , 3 , 4 , 5\}$, on a :

$$\begin{matrix} c_1^i \equiv c_3^i \equiv c_9^i \\ c_2^i \equiv c_6^i \equiv c_5^i \\ c_4^i \equiv c_{12}^i \equiv c_{10}^i \\ c_8^i \equiv c_{11}^i \equiv c_7^i \end{matrix} \quad \text{modulo } 2 .$$

BIBLIOGRAPHIE

[1] DICKSON (L. E.). - Cyclotomy, higher congruences and Waring's problem, I and II, Amer. J. Math., t. 57, 1935, p. 391-424 and p. 463-474.

[2] DICKSON (L. E.). - Cyclotomy and trinomial congruences, Trans. Amer. math. Soc., t. 37, 1935, p. 363-380.

[3] JACOBI (J. G. D.). - De residuis cubicis commentatio numerosa, J. für die reine und angew. Math., t. 2, 1827, p. 66-69.

[4] LEHMER (E.). - The quintic character of 2 and 3 , Duke math. J., t. 18, 1951, p. 11-18.

[5] LEONARD (P. A.) and WILLIAMS (K. S.). - The septic character of 2 , 3 , 5 an and 7 , Pacific J. Math., t. 52, 1974, p. 143-147.

[6] LEONARD (P. A.) and WILLIAMS (K. S.). - A diophantine system of Dickson, Atti Accad. naz. Lincei, Rend., t. 56, 1974, p. 145-150.

[7] LEONARD (P. A.), MORTIMER (B. C.) and WILLIAMS (K. S.). - The elenventh power character of 2 , J. für die reine und angew. Math., t. 286-287, 1976, p. 213-222.

[8] LEONARD (P. A.) and WILLIAMS (K. S.). - The cyclotomic numbers of order eleven, Acta Arithm., Warszawa, t. 26, 1975, p. 365-383.

[9] MASLEY (J. M.) and MONTGOMERY (H. L.). - Cyclotomic fields with unique factorization, J. für die reine und angew. Math., t. 286-287, 1976, p. 248-256.

[10] WILLIAMS (K. S.). - A quadratic partition of primes $= 1 \pmod 7$, Math. of Comput., t. 28, 1974, p. 1 133-1 136.

(Texte reçu le 15 juin 1978)

Dominique BERNARDI
14 bis rue Pierre Nicole
75005 PARIS