POLSKA AKADEMIA NAUK, INSTYTUT MATEMATYCZNY

DISSERTATIONES MATHEMATICAE

(ROZPRAWY MATEMATYCZNE)

CCCXII

BERNADETTE DESHOMMES

Puissances binomiales dans un corps cubique

WARSZAWA 1991

Published by the Institute of Mathematics, Polish Academy of Sciences
Typeset in TEX at the Institute
Printed and bound by

drukarnia
herman & herman
02-240 Warszawa, ul. Jakobinów 23, tel: 846-79-66, tel/fax: 49-89-95

PRINTED IN POLAND

ISBN 83-85116-14-1 ISSN 0012-3862

TABLE DES MATIÈRES

1991 *Mathematics Subject Classification* : 11R16, 11B37, 11S10.

Introduction

Soit ρ un élément primitif d'un corps cubique $\mathcal{K}$ de discriminant négatif. Considérons les puissances binomiales de ρ définies par l'équation

$$\rho^n = x\rho + y\,, \tag{i}$$

où $n \in \mathbb{Z}$ et $x, y \in \mathbb{Q}$, et posons $f(X) = X^3 - SX^2 - QX - R$, où f désigne le polynôme minimal de ρ. Dans cet article nous montrons (Thm. 1), sous l'hypothèse que S ou Q est non nul, que le nombre de solutions en n de l'équation (i) est au plus égal à quatre, sauf dans trois cas où il y a cinq ou six solutions. A titre d'illustration, nous présentons dans la Table 3 une liste de seize exemples où l'équation (i) a au moins quatre solutions. Il n'est pas possible de dire si cette liste est exhaustive ou non; Cor. 6 et Cor. 7 apportent quelques précisions relatives à l'existence et à la forme des solutions non triviales.

Le Théorème 1 étend les résultats de Nagell et de Delone et Faddeev, [10, §75] sur les unités binomiales d'un ordre cubique. D'après (i), chaque couple (x, y) est solution d'une équation de Thue–Mahler de degré trois, $\mathrm{Norm}_{\mathcal{K}/\mathbb{Q}}(x\rho + y) = R^n$; en degré $r \geq 3$, voir l'article de Bombieri et Schmidt [7].

Dans Cor. 1, nous obtenons, via Déf. 1 et Rem. 1, que la zéro-multiplicité d'une suite récurrente linéaire cubique de nombres rationnels, non-dégénérée et possédant deux zéros consécutifs, est égale à quatre, avec trois exceptions. D'après Rem. 1, les résultats de ce travail s'adaptent, en se simplifiant, au cas où le polynôme f n'est pas irréductible, en supposant que f est non-dégénéré et R non nul. Les questions de multiplicité des récurrences linéaires, d'ordre $r \geq 2$, sont analysées dans le rapport de van der Poorten [31, §5], voir aussi Tijdeman [29]. Dans un article à paraître, Beukers [4] résoud une conjecture fameuse de Ward [37] et de Kubota [15, p. 99], en démontrant que la zéro-multiplicité d'une récurrence ternaire non-dégénérée de nombres rationnels est égale à six; l'historique de cette conjecture est rappelé dans [31, §5.3]. Les suites possédant quatre zéros et plus faisant figure d'exception, on peut étudier la forme et le nombre des zéros en fonction des coefficients de la récurrence ou des premiers termes de la suite.

A une translation près, la connexion est immédiate entre les solutions en

n de l'équation (i) et les zéros d'une suite récurrente linéaire qui s'annule deux fois consécutives. Pour $n \in \mathbb{N}$, les suites coordonnées de ρ^n dans la base ρ^2, ρ, 1 du corps $\mathcal{K}$ sont définies par une relation de récurrence et chaque zéro de la première coordonnée U_n est une solution de l'équation (i), la réciproque étant vraie dans les conditions de Cor. 2. Bien auparavant, Lucas [18, §173], a mis en évidence l'intérêt que présentent les fonctions récurrentes fondamentales. Les propriétés de la suite U_n sont détaillées dans Prop. 1, le terme d'indice $n+2$ est la $n$ième fonction symétrique complète des racines ρ, ρ', ρ'' du polynôme f, que Ward [35, 36] désigne sous le nom de somme des produits homogènes de poids n des racines de f; d'après Déf. 2,

$$U_{n+2} = \sum_{i+j+k=n} \rho^i \rho'^j \rho''^k \,. \tag{ii}$$

Lorsque les trois racines de f sont réelles, il est bien connu que les récurrences ternaires et, en particulier, la suite U_n, ont au plus trois zéros, voir Smiley [28], Scott [27], Ward [34], Picon [25], Beukers [4], et dans le cas où les racines de f sont des entiers rationnels, Ward [37] conjecture que l'équation diophantienne $U_{n+2} = 0$ n'a pas de solutions pour tout $n > 1$ et pour tout polynôme f. Des progrès récents sur cette question difficile sont dûs à Apostol [1] et à Turnwald [30]. Lorsque le polynôme f a des racines complexes conjugées, le terme général de la suite U_n s'exprime d'une part sous la forme d'une somme d'exponentielles, d'après (4), d'autre part sous une forme diophantienne, d'après (13),

$$U_{n+2} = \sum_{i+2j+3k=n} \frac{(i+j+k)!}{i!j!k!} S^i Q^j R^k \,; \tag{iii}$$

pour raison de congruences, nous utilisons cette dernière expression. Au vu des résultats de Lewis et Turk [17], de Beukers et Tijdeman [5] et de Beukers [4], on peut se demander si la zéro-multiplicité de la suite U_n ou d'une suite quelconque de nombres rationnels définie par la relation (2) n'est pas égale à trois, avec une liste exhaustive d'exceptions (voir Rem. 6).

Dans le paragraphe 1, après avoir énoncé le résultat principal, Thm. 1 et son corollaire, et introduit les notations et définitions utilisées dans la suite, nous démontrons Thm. 1. Dans les paragraphes suivants, nous établissons les résultats intermédiaires dans l'ordre où ils apparaissent dans la preuve de Thm. 1. Le problème ayant été réduit aux conditions de l'hypothèse 2, nous supposons que ρ est un entier primitif du corps $\mathcal{K}$ et que ρ et ρ^3/R ne sont pas des unités algébriques, ces deux cas étant traités dans [10, §75] et dans [11]. Nous discutons alors la forme et le nombre des solutions en n de l'équation (i), en fonction des diviseurs premiers de deux indices reliés à f (Déf. 5), l'indice $\mathcal{F}_2 = -(QS + R)$ pour les solutions modulo deux, et l'indice $\mathcal{F}_3 = Q^2(S^2 + Q) - RS^3$ pour les solutions modulo trois. Pour

chaque diviseur premier p de $\mathcal{F}_2$, respectivement de $\mathcal{F}_3$, qui ne divise pas R, nous étudions l'équation (i) par une méthode p-adique, d'après Mahler [21] et Robba [26]. Voir le livre de Cassels, [8, chap. 4 et 5]. Nous étendons ainsi à des unités semi-locales (Déf. 6) un procédé que Delone et Faddeev utilisent avec des unités algébriques (voir [10] et [12]). Pour les diviseurs communs de R et $\mathcal{F}_2$ ou de R et $\mathcal{F}_3$, nous étudions au moyen de congruences, via (iii), l'équation diophantienne $U_n = 0$ (Prop. 3 et Prop. 8). Les deux derniers paragraphes traitent des équations (i) possédant au moins trois solutions en n : 0, 1, 4 ou 0, 1, 3, et qui nécessitent une étude particulière mettant en œuvre les résultats des paragraphes précédents (critères $\mathcal{F}_2$ et $\mathcal{F}_3$, Cor. 3 et Cor. 5). Les remarques 1, 3 et 5 concernent le cas où f n'est pas irréductible.

D'après un argument de Ward [33], si une suite non-dégénérée de nombres rationnels, définie par la relation (2), s'annule en 0 et n alors, via (10), n vérifie l'équation

$$\rho^n = x\theta + y\,, \tag{iv}$$

où θ dépend des premiers termes de la suite. On peut étudier la forme et le nombre des solutions en n de l'équation (iv), en fonction des indices $\mathcal{F}_k$ et de l'indice de θ relatif à ρ, et en utilisant les résultats de Beukers [4].

§ 1. Résultat principal

Hypothèse 1. Soient ρ un élément primitif d'un corps cubique $\mathcal{K}$ de discriminant négatif et f le polynôme minimal de ρ. Posons $f(X) = X^3 - SX^2 - QX - R$, S ou Q étant non nul. Notations : Soit F la forme cubique binaire telle que $F(X,-1) = f(X)$. Posons $F(X,Y) = RY^3 - QY^2X + SYX^2 + X^3$ et $g(X) = R^{-1}F(-R,X)$; $\omega = R/\rho$ désigne une racine du polynôme g. Les nombres ρ et ω sont des racines, respectivement gauche et droite, de la forme F.

Théorème 1. *Sous l'hypothèse* 1, *le nombre de solutions en n de l'équation*

$$\rho^n = x\rho + y\,, \tag{1}$$

où $n \in \mathbb{Z}$ et $x, y \in \mathbb{Q}$, est au plus égal à quatre, avec trois exceptions. Il y a cinq solutions si ρ/λ, avec $\lambda \in \mathbb{Q}^*$, est une racine de $X^3 + X^2 - 1$ ou de $X^3 + 2X^2 - 4$, et six solutions dans le cas de $X^3 - 2X^2 + 4X - 4$. Voir Table 3. *La relation $n + m = 1$ donne trivialement les solutions en m de l'équation $\omega^m = x\omega + y$.*

Le paragraphe 1 s'achève par la preuve de Thm. 1. Il existe une étroite connexion entre les solutions en n de l'équation (1) et les zéros de certaines suites récurrentes, qui est à la base de ce travail (voir Ward [33]).

Définition 1. Soit u_n une suite de nombres rationnels définie par la donnée de u_0, u_1, u_2 non tous nuls, et par la relation de récurrence

$$u_{n+3} = Su_{n+2} + Qu_{n+1} + Ru_n\,, \qquad n \in \mathbb{N}\,, \tag{2}$$

où (S, Q, R) est un triplet fixé de nombres rationnels, avec R non nul. La suite u_n est une suite récurrente linéaire cubique, non triviale. Un *zéro* de la suite u_n est un indice k tel que $u_k = 0$. La *zéro-multiplicité* de la suite u_n est le nombre maximum de ses zéros. Posons $f(X) = X^3 - SX^2 - QX - R$; f est le *polynôme auxiliaire de la récurrence*. Un polynôme est *non-dégénéré* si le rapport de deux quelconques de ses racines n'est pas une racine de l'unité. La suite u_n est non-dégénérée, ainsi que la récurrence, lorsque le polynôme f est non-dégénéré; dans ce cas la suite a un nombre fini de zéros, d'après un théorème de Mahler [20, p. 48]. Les "*indices*" de la récurrence sont les nombres rationnels $\mathcal{F}_k$ dont le carré est égal au rapport des discriminants de ρ^k et de ρ pour $k \geq 1$, ρ étant une racine de f et $\mathrm{discr}(\rho) = \mathrm{discr}(f)$.

Corollaire 1. *Si une suite récurrente linéaire cubique, non triviale, de nombres rationnels, a deux zéros consécutifs : k, $k+1$, et si f, le polynôme auxiliaire de la récurrence, vérifie l'hypothèse* 1, *alors la zéro-multiplicité de la suite est égale à quatre, avec trois exceptions. Dans deux cas, la suite a cinq zéros, lorsque $k \geq 2$:*

$$k-2, k, k+1, k+5, k+14 \quad \textit{pour} \quad f(X) = X^3 + \lambda X^2 - \lambda^3\,,$$
$$k-2, k, k+1, k+6, k+22 \quad \textit{pour} \quad f(X) = X^3 + 2\lambda X^2 - 4\lambda^3\,;$$

et dans le cas de la récurrence de Berstel et Mignotte, la suite a six zéros :

$$k, k+1, k+4, k+6, k+13, k+52 \quad \textit{pour} \quad f(X) = X^3 - 2\lambda X^2 + 4\lambda^2 X - 4\lambda^3\,.$$

L'énoncé est analogue lorsque g est le polynôme auxiliaire de la récurrence.

Preuve. Soit u_n la suite récurrente. L'hypothèse $u_k = u_{k+1} = 0$ et les résultats de Prop. 1 montrent que $u_{k+m} = u_{k+2}U_m$ et $R^{m+2}u_{k-m} = u_{k+2}W'_{m+2}$, d'après (10) avec $W'_{m+2} = R^2U'_{m+1}$. Les zéros de la suite u_n de la forme $k \pm m$ correspondent aux zéros des suites U_m ou U'_{m+1}, c'est-à-dire, aux solutions en $\pm m$ de l'équation (1), d'après les formules (3) et (7). ∎

Définition 2. D'après Macdonald [19, p. 14], pour $n \geq 0$, la *n-ième fonction symétrique complète* des variables x, y, z est la somme de tous les monômes de degré total n, $\sum_{i+j+k=n} x^i y^j z^k$.

Proposition 1. *Sous l'hypothèse* 1, *soient ρ, ρ', ρ'' les racines du polynôme f.*

(i) *Le polynôme f est non-dégénéré. Pour $k \in \mathbb{N}^*$, les nombres ρ^k et ω^k, avec $\omega = R/\rho$, sont des éléments primitifs du corps $\mathcal{K}$ vérifiant l'hypothèse* 1.

(ii) *Pour $n \in \mathbb{N}$, les suites-coordonnées de ρ^n dans la base $\{\rho^2, \rho, 1\}$ du corps $\mathcal{K}$ vérifient la relation de récurrence* (2). *Posons*

$$\rho^n = U_n\rho^2 + V_n\rho + W_n\,. \tag{3}$$

Alors le terme général de la suite U_n a l'expression suivante :

$$\delta_f U_n = (\rho' - \rho'')\rho^n + (\rho'' - \rho)(\rho')^n + (\rho - \rho')(\rho'')^n\,, \tag{4}$$

où $\delta_f = -(\rho' - \rho'')(\rho'' - \rho)(\rho - \rho')$ et $\delta_f^2 = \mathrm{disc}(f) = Q^2S^2 - 18QRS + 4Q^3 - 4RS^3 - 27R^2$.

(iii) *Soit g le polynôme minimal de $\omega = R/\rho$, $g(X) = X^3 + QX^2 + RSX - R^2$. Pour $n \in \mathbb{N}$, les suites-coordonnées de ω^n dans la base $\{\omega^2, \omega, 1\}$ du corps $\mathcal{K}$ vérifient la relation de récurrence ayant g comme polynôme auxiliaire. Posons*

$$\omega^n = U'_n\omega^2 + V'_n\omega + W'_n\,. \tag{5}$$

Pour $n \in \mathbb{N}$, l'expression de ρ^n dans cette base et celle de ρ^{-n} dans la base $\{\rho^2, \rho, 1\}$ sont données par

$$\rho^n = (1/R)(U_{n+1}\omega^2 + V_{n+2}\omega + W_{n+3})\,, \tag{6}$$

$$\rho^{-n} = (1/R^n)(U'_{n+1}\rho^2 + (1/R)V'_{n+2}\rho + (1/R^2)W'_{n+3})\,. \tag{7}$$

(iv) *Soit u_n une suite de nombres rationnels vérifiant la relation* (2). *Les deux expressions suivantes sont équivalentes* :

$$u_n = u_2U_n + u_1V_n + u_0W_n\,, \tag{8}$$

$$u_n = A\rho^n + A'(\rho')^n + A''(\rho'')^n\,, \tag{9}$$

où $A = (u_0\rho^2 + (u_1 - Su_0)\rho + (u_2 - Su_1 - Qu_0))/f'(\rho)$ et A', A'' ont des expressions analogues en termes de ρ', ρ''. Plus généralement, on a pour $m \in \mathbb{N}$,

$$\begin{cases} u_{k+m} = u_{k+2}U_m + u_{k+1}V_m + u_kW_m\,, \quad k \in \mathbb{N}, \\ u_{k+2-m} = (1/R^m)(u_kR^2U'_m + u_{k+1}RV'_m + u_{k+2}W'_m)\,, \\ \qquad\qquad\qquad\qquad\qquad\qquad k+2-m \in \mathbb{N}; \end{cases} \tag{10}$$

$$u_{km+r} = u_{2k+r}\mathcal{U}_m + u_{k+r}\mathcal{V}_m + u_r\mathcal{W}_m\,, \qquad k, r \in \mathbb{N}\,, \tag{11}$$

où $\mathcal{U}_m, \mathcal{V}_m, \mathcal{W}_m$ sont les coordonnées de ρ^{km} dans la base $\{\rho^{2k}, \rho^k, 1\}$ du corps $\mathcal{K}$.

(v) *Suivant Déf.* 2, *U_{n+2} est la n-ième fonction symétrique complète des racines de f, et pour tout $\lambda \in \mathbb{Q}$,*

$$U_{n+2}(\lambda\rho) = \lambda^n U_{n+2}(\rho)\,. \tag{12}$$

La suite U_n est alors définie explicitement en fonction des coefficients S, Q, R de f, par $U_0 = U_1 = 0$ et pour $n \geq 2$,

$$U_n = \sum_{i+2j+3k=n-2} \frac{(i+j+k)!}{i!j!k!} S^iQ^jR^k\,. \tag{13}$$

P r e u v e. (i) Soit $\mathcal{N} = \mathbb{Q}(\rho, \rho', \rho'')$. $\mathcal{N}$ est une extension galoisienne sur $\mathbb{Q}$, de degré six et de groupe de Galois $\mathcal{S}_3$, qui contient trois corps cubiques distincts, l'un réel et les deux autres complexes conjugués, et une extension quadratique $\mathbb{Q}(\delta_f)$ où $\delta_f^2 = \mathrm{disc}(f)$. Supposons que le polynôme f est dégénéré (Déf. 1), et montrons que $S = Q = 0$. Soit ζ une racine de l'unité égale à l'un des rapports ρ'/ρ, ρ''/ρ ou ρ'/ρ''. ζ n'est pas égale à ± 1, les corps cubiques contenus dans $\mathcal{N}$ étant distincts. ζ est une racine primitive de l'unité, d'ordre h, $\mathbb{Q}(\zeta)$ est une extension abélienne sur $\mathbb{Q}$, contenue dans $\mathcal{N}$ et de degré $\varphi(h)$ (φ fonction d'Euler). Pour $h > 2$, $\varphi(h)$ est pair et divise 6; le groupe $\mathcal{S}_3$ n'étant pas abélien, $\mathbb{Q}(\zeta)$ ne peut être égale à $\mathcal{N}$, $\varphi(h)$ est donc égal à 2. ζ appartient à l'extension quadratique $\mathbb{Q}(\delta_f)$, invariante par le groupe $\mathcal{A}_3$ des permutations circulaires. La condition $\sigma(\zeta) = \zeta$ pour tout $\sigma \in \mathcal{A}_3$ se traduit par $\rho^3 = R$, $(\rho')^3 = R$ et $(\rho'')^3 = R$, le polynôme f est donc de la forme $X^3 - R$, et on a bien $S = Q = 0$; le corps $\mathcal{K}$ est un corps cubique pur, ainsi que chacun des corps cubiques conjugués.

Lorsque S ou Q est non nul, s'il existait $k \geq 1$ tel que ρ^k ou ω^k appartienne à $\mathbb{Q}$, avec $\omega = \rho'\rho''$, alors, $\mathbb{Q}$ étant invariant par $\mathcal{S}_3$, chacun des rapports ρ'/ρ, ρ''/ρ et ρ'/ρ'' serait une racine de l'unité d'ordre k, ce qui est impossible, le polynôme f étant non-dégénéré.

(ii) Par définition, f est le polynôme caractéristique de l'endomorphisme m_ρ de la multiplication par ρ dans le corps $\mathcal{K}$, $f(X) = \det(X 1_{\mathcal{K}} - \rho)$. Soit $\mathcal{M}$ la matrice de m_ρ dans la base $\{\rho^2, \rho, 1\}$ du corps $\mathcal{K}$. Pour $n \in \mathbb{N}$, les puissances de ρ sont définies par

$$\mathcal{M}\rho^n = \rho^{n+1} \quad \text{avec } \mathcal{M} = \begin{pmatrix} S & 1 & 0 \\ Q & 0 & 1 \\ R & 0 & 0 \end{pmatrix}.$$

Les suites-coordonnées de ρ^n, définies par la formule (3), vérifient la relation de récurrence (2). Fixons un plongement du corps $\mathcal{K}$ dans $\mathbb{C}^3$, en posant $\widehat{\rho} = (\rho, \rho', \rho'')$, et soit $\mathcal{V}$ la matrice ayant pour colonnes les vecteurs $\widehat{\rho^2}, \widehat{\rho}, \widehat{1}$. Le déterminant de cette matrice est égal à δ_f, donné dans l'énoncé; δ_f est non nul par hypothèse. Chacune des racines du polynôme f vérifie la formule (3) :

$$\widehat{\rho^n} = U_n \widehat{\rho^2} + V_n \widehat{\rho} + W_n \widehat{1}\,. \tag{14}$$

Le terme général de la suite U_n est le quotient de deux déterminants : $\delta_f U_n = \det(\widehat{\rho^n}, \widehat{\rho}, \widehat{1})$, ce qui donne la formule (4), et $\delta_f^2 = \mathrm{disc}(\rho)$, par définition du discriminant de ρ. La description des suites V_n et W_n est analogue.

(iii) Par définition, $g(X) = \det(X 1_{\mathcal{K}} - \omega)$. L'assertion se déduit de (ii)

en remplaçant ρ par ω, puis en utilisant les formules de changement de bases :

$$(15)\qquad \begin{cases} \omega = \rho^2 - S\rho - Q \text{ et } \omega^2 = -Q\rho^2 + (QS+R)\rho + (Q^2 - RS)\,, \\ \rho = (1/R)(\omega^2 + Q\omega + RS) \text{ et} \\ \rho^2 = (1/R)(S\omega^2 + (QS+R)\omega + R(S^2+Q))\,. \end{cases}$$

(iv) La série génératrice de la suite u_n est une fraction rationnelle :

$$\sum_{n\geq 0} u_n X^n = \frac{X^2(u_2 - Su_1 - Qu_0) + X(u_1 - Su_0) + u_0}{(1-X\rho)(1-X\rho')(1-X\rho'')}\,.$$

La décomposition en éléments simples de cette fraction donne l'expression classique (9) du terme général de la suite u_n, sous la forme d'une somme d'exponentielles. Les constantes complexes A, A', A'' sont déterminées par les premiers termes de la suite : $(A, A', A'')\mathcal{V} = (u_2, u_1, u_0)$, où $\mathcal{V}$ est la matrice définie ci-dessus. Le déterminant de $\mathcal{V}$ étant non nul, les expressions (8) et (9) sont équivalentes, via (14). La première formule de (10) s'obtient à partir de (3) et de (8), en utilisant la décomposition de ρ^{k+m} en $\rho^k\rho^m$,

$$\rho^{k+m} = U_m\rho^{k+2} + V_m\rho^{k+1} + W_m\rho^k \Leftrightarrow \begin{cases} U_{k+m} = U_{k+2}U_m + U_{k+1}V_m + U_kW_m\,, \\ V_{k+m} = V_{k+2}U_m + V_{k+1}V_m + V_kW_m\,, \\ W_{k+m} = W_{k+2}U_m + W_{k+1}V_m + W_kW_m\,. \end{cases}$$

Formons une combinaison linéaire de ces trois identités en multipliant la première par u_2, la seconde par u_1 et la troisième par u_0; le premier membre de cette expression est égal à u_{k+m} d'après (8), tandis que le second membre est égal à $u_{k+2}U_m + u_{k+1}V_m + u_kW_m$, en appliquant (8) trois fois. La seconde formule de (10) s'obtient de la même façon à partir de (3), (5), (8) et de la décomposition suivante :

$$R^m\rho^{k+2-m} = \rho^{k+2}\omega^m = R^2U'_m\rho^k + RV'_m\rho^{k+1} + W'_m\rho^{k+2}\,.$$

Pour établir la formule (11), considérons les coordonnées de ρ^{km} dans les deux bases de $\mathcal{K}$, $\{\rho^{2k}, \rho^k, 1\}$ et $\{\rho^2, \rho, 1\}$; d'après (3), elles sont définies par

$$(16)\qquad \begin{cases} \rho^{km} = \mathcal{U}_m\rho^{2k} + \mathcal{V}_m\rho^k + \mathcal{W}_m \\ \rho^{km} = U_{km}\rho^2 + V_{km}\rho + W_{km} \end{cases} \Leftrightarrow \begin{cases} \begin{pmatrix} U_{km} \\ V_{km} \end{pmatrix} = \begin{pmatrix} U_{2k} & U_k \\ V_{2k} & V_k \end{pmatrix} \begin{pmatrix} \mathcal{U}_m \\ \mathcal{V}_m \end{pmatrix}\,, \\ W_{km} = W_{2k}\mathcal{U}_m + W_k\mathcal{V}_m + \mathcal{W}_m\,. \end{cases}$$

D'après (10), $u_{km+r} = u_{r+2}U_{km} + u_{r+1}V_{km} + u_rW_{km}$; après substitution, via (16), $u_{km+r} = (u_{r+2}U_{2k} + u_{r+1}V_{2k} + u_rW_{2k})\mathcal{U}_m + (u_{r+2}U_k + u_{r+1}V_k + u_rW_k)\mathcal{V}_m + u_r\mathcal{W}_m$, et la formule (10) appliquée deux fois donne le résultat. Voir Bell [2].

(v) Effectuons le produit des séries géométriques figurant au second membre de la série génératrice de la suite u_n (voir (iv)). Dans le cas de la suite U_n, $U_0 = U_1 = 0$ et $U_2 = 1$, une simple vérification montre que U_{n+2} est la $n$ième fonction symétrique complète des racines de f et la formule (12) se déduit de Déf. 2. D'après Macdonald [19, p. 20] ou Lascoux [16], $U_{n+2} = \det(e_{1-i+j})_{1\le i,j\le n}$ où $e_0 = 1$, $e_1 = S$, $e_2 = -Q$, $e_3 = R$ et $e_k = 0$ autrement. La formule (13) provient du développement de ce déterminant. ∎

R e m a r q u e 1. La validité des résultats de Prop. 1 est inchangée lorsque le polynôme f n'est pas irréductible, en supposant que f est non-dégénéré et R non nul; $\widehat{\rho^n}$ étant défini par $(\rho^n, (\rho')^n, (\rho'')^n)$, les vecteurs $\widehat{\rho^2}$, $\widehat{\rho}$, $\widehat{1}$ forment une base de $\mathbb{C}^3$ et U_n, V_n, W_n sont les coordonnées de $\widehat{\rho^n}$ dans cette base, [10, §1]. L'équation (1) est remplacée par l'équation

$$\widehat{\rho^n} = x\widehat{\rho} + y\widehat{1}\,. \tag{17}$$

Posons $f(X) = (X-\rho)(X^2 - AX + B)$ et considérons la suite a_n définie par $a_0 = 1$, $a_1 = \rho$, et par la relation de récurrence binaire $a_{n+2} = Aa_{n+1} - Ba_n$. D'après (4),

$$U_n = 0 \Leftrightarrow a_n = a_1^n\,, \qquad \text{avec } a_n = \frac{(\rho')^n(a_1-\rho'') - (\rho'')^n(a_1-\rho')}{\rho'-\rho''}\,.$$

Après normalisation, en posant $b_n = a_n/a_1^n$, la zéro-multiplicité de la suite U_n est égale à la 1-multiplicité de la suite b_n telle que $b_0 = b_1 = 1$ et $b_n \in \mathbb{Q}(\rho)$. Voir Kubota [15], Beukers [3, 4], Beukers et Tijdeman [5], Lewis et Turk [17].

Définition 3. Soit (S, Q, R) un triplet d'entiers rationnels, avec R non nul. Le triplet est "*réduit*" si R est positif et si pour chaque $\lambda \in \mathbb{Z}^*$ tel que $\lambda \mid S$ et $\lambda^2 \mid Q$ on a $\lambda^3 \nmid R$.

Définition 4. Soient A et B deux entiers rationnels, "A a la *propriété* $\mathcal{P}(B)$" si tout diviseur premier de A est un diviseur de B.

Proposition 2. *Soient (S, Q, R) un triplet "réduit" vérifiant l'hypothèse* 1, *δ le pgcd de Q et de R, U_n et U'_n les suites définies dans Prop.* 1.

(i) *Il existe des entiers positifs a, b, χ tels que $\delta = a^2 b\chi$, où a et b sont premiers entre eux et sans facteurs carrés, $(\chi, S) = 1$, $ab \mid S$ et $(a, R/\delta) = 1$. Si "δ a la propriété $\mathcal{P}(S)$" alors $\chi = 1$.*

On suppose maintenant que "δ a la propriété $\mathcal{P}(S)$".

(ii) *La suite U_n n'a pas de zéros de la forme $n = 3m + 2$ à moins que $(aS, Q) = \delta$ et δ^2 divise R.*

(iii) *Si R ne divise pas Q alors, pour $n \neq 0$ et $n \neq 1$, la suite U'_n n'a pas de zéros.*

P r e u v e. (i) Le triplet étant "réduit", si p est un diviseur premier de (δ, S), avec $\delta = (Q, R)$, alors $p^3 \nmid \delta$. Posons $a = \prod p$ tels que $p^2 \parallel \delta$ et $p \mid S$, et $b = \prod p$ tels que $p \parallel \delta$ et $p \mid S$. Alors $\delta = a^2 b\chi$ et les propriétés de l'énoncé sont vérifiées.

(ii) Supposons qu'il existe un nombre premier p tel que $p|(aS, Q)$ et $p \nmid R/\delta$. Le triplet (S, Q, R) est alors de la forme $(up^{\alpha+\beta+t}, vp^{2\alpha+\beta+t}, wp^{2\alpha+\beta})$ avec $p \nmid (u, v)$ et $p \nmid w$, α et β étant des entiers tels que $\alpha + \beta = 1$ si $t = 0$ et $0 \le \alpha + \beta \le 1$ sinon. D'après la formule (13), pour $m \ge 0$

$$p^{-m(2\alpha+\beta)} U_{3m+2} = \sum_{0 \le k \le m} w^k p^{\alpha(m-k)} \Big(\sum_{i+2j=3(m-k)} \frac{(i+j+k)!}{i!j!k!} u^i v^j p^{t(i+j)+\beta(i+j+k-m)} \Big),$$

avec $i + j + k - m \ge 1$ et $i + j \ge 2$ dès que $k < m$. Nous en déduisons que $p^{-m(2\alpha+\beta)} U_{3m+2} \equiv w^m \pmod{p^{\alpha+\beta+2t}}$; comme $p \nmid w$ et $\alpha + \beta + 2t \ge 1$, alors $U_{3m+2} \ne 0$ pour $m \in \mathbb{N}$.

(iii) Soit p un diviseur premier de R/δ, lorsque $R \ne \delta$. Le triplet (S, Q, R) est de la forme $(p^e u, p^e v, p^{e+t} w)$, avec $p \nmid vw$, $t \ge 1$ entier, $e = 1$ si $p \mid \delta$ et $e = 0$ sinon. D'après la formule déduite de (13), en remplaçant le triplet (S, Q, R) par $(-Q, -RS, R^2)$, on obtient pour $n \ge 0$

$$p^{-en} U'_{n+2} = \sum_{i+2j+3k=n} \frac{(i+j+k)!}{i!j!k!} (-v)^i (-u)^j w^{j+2k} p^{tj+(2t-e)k},$$

avec $j + k \ge 1$ dès que $n - i \ge 2$, et $2t - e \ge t$. Nous en déduisons que $p^{-en} U'_{n+2} \equiv (-v)^n \pmod{p^t}$; comme $p \nmid v$ et $t \ge 1$, alors $U'_{n+2} \ne 0$ pour $n \in \mathbb{N}$. ∎

Hypothèse 2. Soient ρ un entier algébrique d'un corps cubique $\mathcal{K}$ de discriminant négatif et f le polynôme minimal de ρ, $f(X) = X^3 - SX^2 - QX - R$. On suppose que le triplet (S, Q, R) est "réduit", que R ne divise pas Q avec $R \ge 2$ et que le pgcd δ de Q et de R "a la propriété $\mathcal{P}(S)$". Notations : posons $\delta = a^2 b$ où a et b sont des entiers positifs, premiers entre eux et sans facteurs carrés; le triplet est alors de la forme $(abs, \delta q, \delta r)$ où s, q, r sont des entiers rationnels tels que $(aq, r) = 1$ et $r \ge 2$.

Corollaire 2. *Sous l'hypothèse* 2, *l'équation* (1) *est équivalente à l'équation* $U_n = 0$, *où* U_n *est la suite définie dans Prop.* 1. *Les solutions sont de la forme* $n = 3m$ *ou* $n = 3m + 1$ *et il n'existe pas de solution de la forme* $n = 3m + 2$ *à moins que* $a = 1$, $b \mid r$ *et* $(q, s) = 1$.

P r e u v e. L'équation (1) n'a pas de solutions avec n négatif, d'après (7) et Prop. 2(iii), et d'après (3), chaque solution de l'équation (1) avec $n \in \mathbb{N}$ correspond à un zéro de la suite U_n. Les conditions $(aS, Q) = \delta$ et $\delta^2 \mid R$ de

Prop. 2(ii) se traduisent, via l'hypothèse 2, par $(q,s)=1$, $ab \mid r$ et $(a,r)=1$. ∎

Lorsque ρ est un entier algébrique, nous étudions les solutions de l'équation (1) par des méthodes p-adiques classiques, en choisissant pour p certains diviseurs premiers des indices $\mathcal{F}_2$ et $\mathcal{F}_3$ (Déf. 1). Dans le cas général où ρ est un entier algébrique de degré r, Duboué [13] étudie les propriétés arithmétiques d'indices analogues.

Définition 5. Soient $\{\varphi,\rho,1\}$ et $\{\gamma,\theta,1\}$ deux bases du corps $\mathcal{K}$, $\rho = a\gamma+b\theta+c$ et $\varphi = a'\gamma+b'\theta+c'$. Le déterminant $a'b-ab'$ est "l'*indice*" de la première base (ou de ρ si $\varphi=\rho^2$) relativement à la seconde base. Lorsque ρ est un entier du corps $\mathcal{K}$ vérifiant l'hypothèse 1, pour $k\in\mathbb{N}^*$, $\mathcal{F}_k(\rho)$ ou simplement $\mathcal{F}_k$ désigne "l'*indice*" de ρ^k dans la base $\{\rho^2,\rho,1\}$. Avec les notations de Prop. 1(ii), $\mathcal{F}_k = U_{2k}V_k - U_kV_{2k}$, en particulier $\mathcal{F}_2 = -(QS+R)$ et $\mathcal{F}_3 = Q^3+Q^2S^2-RS^3$. D'après Delone et Faddeev [10, p. 102], l'entier $\mathcal{F}_k$ est alors l'*indice* de l'ordre $\mathbb{Z}[\rho^k]$ dans l'ordre $\mathbb{Z}[\rho]$, un *ordre* du corps $\mathcal{K}$ étant un $\mathbb{Z}$-module qui est un sous-anneau de $\mathcal{K}$ contenant le nombre 1.

Lemme 1. *La suite des indices $\mathcal{F}_k$ est une suite de divisibilité et pour $k\geq 1$, $\operatorname{disc}(\rho^k) = \mathcal{F}_k^2 \operatorname{disc}(\rho)$ et $\mathcal{F}_k = \operatorname{Norm}(-(\rho-S)U_k+V_k)$, où* Norm *désigne le produit pris sur les racines du polynôme f.*

Dans le cas général, voir l'article de Bézivin, Pethö et van der Poorten [6].

P r e u v e. Le polynôme f est non-dégénéré d'après Prop. 1(i), donc $\mathcal{F}_k$ est non nul pour tout $k\in\mathbb{N}^*$. D'après Duboué [13, p. 208], la suite vérifie les relations de divisibilité : $\mathcal{F}_{km}(\rho) = \mathcal{F}_k(\rho)\mathcal{F}_m(\rho^k) = \mathcal{F}_m(\rho)\mathcal{F}_k(\rho^m)$, pour $k,m\in\mathbb{N}^*$, que l'on peut déduire aussi de (16). Par définition,

$$\delta_f = \det(\widehat{\rho^2},\widehat{\rho},\widehat{1})\,, \qquad \delta_f\mathcal{F}_k = \det(\widehat{\rho^{2k}},\widehat{\rho^k},\widehat{1})\,,$$

où $\widehat{\ }$ est le plongement utilisé dans la preuve de Prop. 1; la première égalité en découle. D'après (3), l'identification de ρ^{2k} et de $(\rho^k)^2$ entraîne que

$$U_{2k} = (S^2+Q)U_k^2 + 2SU_kV_k + V_k^2 + 2U_kW_k\,,$$
$$V_{2k} = (QS+R)U_k^2 + 2QU_kV_k + 2V_kW_k\,.$$

Un calcul simple montre alors l'égalité de $U_{2k}V_k - U_kV_{2k}$ et de la norme :

$$\operatorname{Norm}(-(\rho-S)U_k+V_k) = -(QS+R)U_k^3 + (S^2-Q)U_k^2V_k + 2SU_kV_k^2 + V_k^3\,.$$ ∎

Pour résoudre l'équation $\varepsilon^n = x\theta+y$, lorsque ε est une unité algébrique d'un ordre cubique $\mathbb{Z}[\theta]$, de discriminant négatif, Delone et Faddeev [10, §75] utilisent un algorithme de montée, dont le principe est de substituer à cette équation une équation analogue

$$\varepsilon_1^{n_1} = x_1\theta_1 + y\,,$$

où $x = px_1$, avec p premier, et d'épuiser les diviseurs de x en répétant cette opération. Plus précisément, p est un diviseur premier de l'indice de l'ordre $\mathbb{Z}[\varepsilon]$ dans l'ordre $\mathbb{Z}[\theta]$, $\theta_1 = p\theta$, $\varepsilon_1 = \varepsilon^\mu$ et $n = \mu n_1$, où μ est déterminé par le "Petit Théorème" de Fermat dans le corps $\mathbb{Q}(\theta)$. Voir Nagell [24, p. 48]. Lorsque ρ n'est pas une unité algébrique, l'algorithme de montée ne s'applique à l'équation (1) que dans le cas où ρ est une *unité semi-locale* pour p.

Définition 6. Soient ζ et θ des éléments primitifs d'un corps cubique $\mathcal{K}$ avec θ entier, et h le polynôme minimal sur $\mathbb{Q}$ de ζ. Posons $h(X) = X^3 - sX^2 - qX - r$. Soit p un nombre premier fixé; $\mathbb{Z}_{(p)}$ désigne l'anneau local de $\mathbb{Z}$ en p, $\mathbb{Z}_{(p)} = \{(u/v) \in \mathbb{Q} \mid p \nmid v\}$. ζ est un *entier semi-local* du corps $\mathcal{K}$, dans le sens de Cassels [8, p. 170], si $s, q, r \in \mathbb{Z}_{(p)}$, et ζ est une *unité semi-locale* si de plus $r \notin p\mathbb{Z}_{(p)}$. Le nombre premier p est appelé un "*diviseur*" de l'unité semi-locale ζ dans l'anneau $\mathbb{Z}_{(p)}[\theta]$ si ζ a l'expression suivante :

$$\zeta = p^\alpha A\theta^2 + p^\beta B\theta + C\,,$$

où α et β sont des entiers positifs, C est une unité de $\mathbb{Z}_{(p)}$ et si A ou B est non nul alors chacun d'eux est une unité de $\mathbb{Z}_{(p)}$.

Théorème 2 [12, p. 155]. *Supposons que ζ soit une unité semi-locale du corps $\mathcal{K}$, ayant p comme "diviseur" dans l'anneau $\mathbb{Z}_{(p)}[\theta]$. Pour $n \neq 0$, l'équation*

$$\zeta^n = (p^\alpha A\theta^2 + p^\beta B\theta + C)^n = x\theta + y\,,$$

avec $n \in \mathbb{Z}$ et $x, y \in \mathbb{Q}$, n'a pas de solutions sous les conditions suivantes :

(i) *pour $p \neq 2$, si $\alpha \leq \beta$ ou si $\beta \leq \alpha < 2\beta$,*
(ii) *pour $p = 2$, si $2 \leq \alpha \leq \beta$ ou si $\beta \leq \alpha < 2\beta - 1$.*

Quand ces conditions ne sont pas satisfaites, l'équation a au plus deux solutions, sauf dans le cas spécial où $p = 3$, $\alpha \geq 2$, $\beta = 1$ et p ne divise pas la trace de θ; le nombre de solutions est alors au plus égal à trois.

Preuve du Théorème 1. Chaque solution n de l'équation (1) est un zéro d'une suite récurrente linéaire (Déf. 1), un zéro de la suite U_n si n est positif ou nul d'après (3), ou un zéro de la suite U'_{h+1} si $n = -h$ est négatif, d'après (7). Ces deux suites sont des fonctions symétriques complètes (Déf. 2 et Prop. 1(v)); chacune d'elles étant non-dégénérée d'après Prop. 1(i), leur zéro-multiplicité est finie. Pour tout $\lambda \in \mathbb{Q}^*$, les suites $U_n(\lambda\rho)$ et $U_n(\rho)$ ont les mêmes zéros d'après (12), ainsi que les suites $U'_{h+1}(\lambda\omega)$ et $U'_{h+1}(\omega)$, où $\omega = R/\rho$. Nous pouvons supposer que ρ est un entier primitif du corps $\mathcal{K}$ vérifiant l'hypothèse 1 et que le triplet (S, Q, R) est "réduit" (Déf. 3). Si k est une solution de l'équation (1) alors $1 - k$ est solution de l'équation $\omega^m = x\omega + y$. Quitte à échanger ces équations,

supposons que $k \geq 3$. Alors $U_k = 0$ et d'après (13), $S^{k-2} \equiv 0 \pmod{\delta}$, où δ est le pgcd de Q et de R. Chaque diviseur premier de δ étant un diviseur de S, d'après Déf. 4, "δ a la propriété $\mathcal{P}(S)$", ce que nous supposons.

Dans le cas où $R = 1$, ρ est une unité algébrique du corps $\mathcal{K}$. D'après un Théorème de Nagell figurant dans le livre de Delone et Faddeev [10, p. 398], l'équation (1) a deux ou trois solutions si $\mathrm{disc}(\rho) < -44$, quatre solutions si $\mathrm{disc}(\rho)$ est égal à -44 ou à -31, et cinq solutions lorsque $\mathrm{disc}(\rho) = -23$, ρ étant l'unité fondamentale de l'ordre cubique $\mathbb{Z}[\rho]$. Une démonstration p-adique du résultat de Nagell est donnée dans [12, Cor. 2]. De plus, Delone et Faddeev déterminent les unités binomiales d'un ordre cubique de discriminant négatif, en utilisant un algorithme de montée dont le principe est brièvement évoqué dans ce paragraphe. Voir [10, §75 et Table, p. 417].

Nous supposons maintenant que $R \geq 2$. Dans [11], nous traitons le cas où $\delta = R$. Le corps cubique $\mathcal{K}$ étant caractérisé par la relation $\rho^3 = R\varepsilon$ où ε est une unité algébrique, les solutions modulo trois de l'équation (1) correspondent à des unités binomiales en ρ ou en ω. Nous montrons [11, Thm. 3.4] que le nombre de solutions en n de l'équation (1) est au plus égal à quatre, sauf dans deux cas où il y a cinq ou six solutions. Ce résultat est obtenu par l'application de certains critères d'arrêt de l'algorithme de montée, établis par Delaunay [10, p. 410], et par Gordon et Mohanty [14]. Voir [11, Table, p. 42]. Nous retrouvons ainsi [11, p. 30] les six zéros de la suite de Berstel et Mignotte (voir Cerlienco, Mignotte et Piras [9, p. 99], Mignotte [22]). Dans [12], nous étendons ces critères d'arrêt à des unités semi-locales (Déf. 6) par des techniques p-adiques, pour l'essentiel : Théorème de Strassmann et séries d'interpolation de Mahler [21, pp. 122 et 224]; le résultat principal [12, Thm. 1] est rappelé dans ce paragraphe (Thm. 2). Comme application, nous étudions les solutions modulo deux de l'équation (1), c'est-à-dire, les puissances de ρ^2 binomiales en ρ ou en ω, lorsque "l'indice $\mathcal{F}_2$ n'a pas la propriété $\mathcal{P}(R)$" (Déf. 4 et Déf. 5) avec $\mathcal{F}_2 = -(QS + R)$. Cette hypothèse entraîne l'existence d'un diviseur premier de $\mathcal{F}_2$ pour lequel ρ est une unité semi-locale et nous montrons [12, Thm. 2] que le nombre de solutions en n de l'équation (1) est alors au plus égal à quatre; en particulier, lorsque $R = \delta$ avec $R \geq 2$ [12, Cor. 3], le nombre de solutions est égal à deux ou trois, sauf dans huit cas. Dans le paragraphe 2, après avoir rappelé ce résultat (Thm. 3), nous le complétons par le critère $\mathcal{F}_2$ (Thm. 4), qui donne sous les mêmes hypothèses des conditions nécessaires pour que l'équation (1) ait une ou deux solutions non triviales.

Dans la suite R et δ sont distincts. Chaque solution en n de l'équation (1) est un zéro de la suite U_n (Cor. 2). Nous supposons désormais que le triplet

(S, Q, R) vérifie l'hypothèse 2, où sont réunies les conditions précédentes. Il reste à étudier les solutions modulo deux de l'équation (1) lorsque "l'indice $\mathcal{F}_2$ a la propriété $\mathcal{P}(R)$", donc en fonction des diviseurs de $\mathcal{F}_2$ et de R. Dans Prop. 3, nous considérons le diviseur d, où d est le pgcd de S et de R/δ; pour chaque diviseur premier de d, les congruences obtenues via la formule (13) font apparaître des conditions nécessaires pour que la suite U_n ait des zéros distincts de 0 et 1. Le paragraphe 2 s'achève par une caractérisation des indices $\mathcal{F}_2$, lorsque l'équation (1) a plus de deux solutions (Cor. 3).

Nous étudions ensuite les solutions modulo trois de l'équation (1), via le système équivalent des équations (20), (22) et (23), en fonction des diviseurs premiers de l'indice $\mathcal{F}_3$, où $\mathcal{F}_3 = Q^2(S^2 + Q) - RS^3$. Dans le paragraphe 3, nous supposons que "l'indice $\mathcal{F}_3$ n'a pas la propriété $\mathcal{P}(R)$"; cette hypothèse entraîne l'existence d'un diviseur premier p de $\mathcal{F}_3$ pour lequel ρ est une unité semi-locale. Nous montrons (Thm. 5) que dans ce cas, le nombre de solutions en n de l'équation (1) est au plus égal à quatre et le critère $\mathcal{F}_3$ donne des conditions nécessaires pour que deux solutions soient congrues modulo trois. Dans la preuve de Thm. 5, nous déterminons d'abord le plus petit entier positif μ tel que p soit un "diviseur" de $\rho^{3\mu}$ relativement à ρ et à ω (Déf. 6), puis la forme des solutions en fonction de μ. Les solutions des équations (20) et (23) correspondent à des puissances de $\rho^{3\mu}$ binomiales en ρ ou en ω, tandis que les solutions de l'équation (22) sont de la forme $n = 3\mu m + 3\nu + 2$ où ν est fixé (Prop. 4). Cependant, Thm. 2 ne s'applique pas à l'équation (22); nous montrons que cette équation a au plus deux solutions (Prop. 5), par extension scalaire à $\mathbb{Q}_p$ de la première relation (10), où k et m sont remplacés par $3\nu + 2$ et $3\mu m$. Par contre, Thm. 2 s'applique à chacune des équations (20) et (23) avec $\zeta = \rho^{3\mu}$; le cas où $p = 2$ étant traité à part (Prop. 6). La compatibilité de ces trois équations est ensuite discutée. Il ressort de la discussion que l'équation (1) a deux ou trois solutions lorsque l'équation (22) n'en a aucune. Dans Prop. 2(ii) et Prop. 8(ii), nous donnons des conditions nécessaires pour que l'équation (22) ait au moins une solution. Dans le cas particulier où une première solution de cette équation est donnée, la seconde solution correspond à une puissance de $\rho^{3\mu}$ binomiale en ϕ, où ϕ s'exprime en fonction de la première solution, et Thm. 2 peut encore s'appliquer (Cor. 4).

Lorsque "l'indice $\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$", nous étudions les solutions de l'équation (1) en fonction des diviseurs premiers de $\mathcal{F}_3$ et de R. Dans le paragraphe 5, nous considérons les diviseurs premiers de $\mathcal{F}_3$ et de δ pour lesquels $\varepsilon = \rho^3/\delta$ est une unité semi-locale, l'équation (1) étant équivalente au système des deux équations (30) et (31), via Prop. 7; cette situation est l'analogue semi-local de celle de [11] où ε est une unité algébrique. Pour chaque diviseur premier de $(aS, Q)/\delta$, Thm. 2 s'applique à chacune

des équations (30) et (31), sauf dans des cas particuliers qui relèvent des Lemmes 3 et 4, via (35). Nous montrons ainsi (Thm. 6) que le nombre de solutions en n de l'équation (1) est égal à deux ou trois, lorsque $(aS, Q) \neq \delta$, et le critère $\mathcal{F}_3'$ donne des conditions nécessaires pour que deux solutions soient congrues modulo trois. On pourrait envisager de traiter le cas où $(aS, Q) = \delta$ en adaptant les résultats de [11, §4.1] et en utilisant la méthode d'extension scalaire lorsque Thm. 2 ne s'applique pas; mais nous allons procéder autrement.

Dans le paragraphe 6, nous définissons D, un diviseur de $\mathcal{F}_3$ et de R/δ, par $\delta D = (S^2 + Q, R)$. Nous établissons Prop. 8 et Cor. 5, qui sont les analogues, pour D et $\mathcal{F}_3$, de Prop. 3 et Cor. 3 pour d et $\mathcal{F}_2$. Dans le paragraphe 7 (Thm. 7), nous montrons, sous l'hypothèse que "l'indice $\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" et $(aS, Q) = \delta$, que le nombre de solutions en n de l'équation (1) est au plus égal à trois, sauf pour les triplets du type (40) ou du type (41). La preuve de Thm. 7 est élémentaire. Nous pouvons en effet supposer que chacun des indices $\mathcal{F}_2$ et $\mathcal{F}_3$ est de la forme indiquée dans Cor. 3 et Cor. 5, et que le triplet (S, Q, R) est solution du système (42), qui comporte deux équations par définition des indices. Nous discutons alors l'existence des solutions de ce système avec les résultats suivants : lorsque $QS = 0$, les triplets sont du type (41) et $n = 3$ est solution de l'équation (1); lorsque $QS < 0$ et $QS \neq -4R$, l'équation (43), déduite du système (42), est quadratique en $-Q^3$ et son discriminant est négatif, sous l'hypothèse 2, à moins que le triplet ne soit du type (40) et $n = 4$ est solution de l'équation (1); lorsque $QS > 0$ ou $QS = -4R$, il y a trois triplets solutions pour lesquels l'équation (1) a deux ou trois solutions, d'après le Lemme 6.

Dans les paragraphes 8 et 9, nous traitons les cas non résolus de Thm. 7. Si le triplet est du type (40) alors, pour $n \neq 0$, les solutions en n de l'équation (1) correspondent aux puissances de ρ^3 binomiales en ρ^3 ((48)). Les critères $\mathcal{F}_2$ et $\mathcal{F}_3$, et Cor. 3 permettent de dresser une liste de dix-huit triplets (Table 1), et pour chaque triplet l'équation (1) a trois ou quatre solutions. On vérifie (Table 2) que pour deux triplets seulement il y a quatre solutions (Thm. 8). Lorsque le triplet est du type (41), pour $n \neq 0$, les solutions en n de l'équation (1) correspondent aux puissances de ρ^2 binomiales en ρ^2, (51). D'après Thm. 9, l'équation (1) a trois ou quatre solutions en n lorsque $S = 0$, et dans deux cas au moins il y a quatre solutions. Cor. 6 et Cor. 7 donnent des conditions nécessaires à l'existence de solutions non triviales. D'après Rem. 1, les résultats précédents s'appliquent à l'équation (17), dans le cas où f n'est pas irréductible (voir Rem. 3 et Rem. 5). Un exemple relié à l'équation de Ramanujan–Nagell est traité par cette méthode. La Table 3 donne seize exemples où l'équation (1) a au moins quatre solutions.

■

§ 2. Solutions modulo deux

Nous étudions les solutions de l'équation (1) suivant leur parité, en fonction des diviseurs premiers de l'indice $\mathcal{F}_2$, lorsque ρ est un entier algébrique du corps $\mathcal{K}$. Le cas où "$\mathcal{F}_2$ n'a pas la propriété $\mathcal{P}(R)$" (Déf. 4) est traité dans [12]; nous rappelons ce résultat.

THÉORÈME 3 [12, Thm. 2]. *Soit ρ un entier algébrique vérifiant l'hypothèse* 1. *S'il existe un nombre premier p tel que $p \mid \mathcal{F}_2$ et $p \nmid R$, avec $\mathcal{F}_2 = -(QS+R)$, alors le nombre de solutions en n de l'équation* (1) *est égal à deux ou trois si $p \geq 5$ ou si $p^2 \mid \mathcal{F}_2$; sinon il y a au plus quatre solutions.*

THÉORÈME 4 (CRITÈRE $\mathcal{F}_2$). *Soit p un nombre premier vérifiant les hypothèses de Thm.* 3. *Désignons par μ le plus petit entier positif tel que p soit un "diviseur" de $\rho^{2\mu}$ dans l'ordre $\mathbb{Z}[\rho]$. Suivant Déf.* 6, *posons*

$$\rho^{2\mu} = p^{\alpha} A\rho^2 + p^{\beta} B\rho + C\,.$$

Si $p \nmid \operatorname{disc}(\rho)$ alors μ est la plus petite solution de la congruence $(S^2/Q)^{\mu} \equiv 1 \pmod{p}$; sinon $\mu = p$. Les solutions de l'équation (1) *sont alors de la forme $n = 2\mu l$ ou $n = 2\mu l + 1$, avec $l \in \mathbb{Z}$. La condition $\mathcal{C}_0$ ci-dessous, respectivement la condition $\mathcal{C}_1$, est nécessaire pour que l'équation* (1) *ait deux solutions paires, respectivement deux solutions impaires (au plus trois solutions dans le cas spécial).*

<table>
<tr><th></th><th>$p = 2$</th><th>*cas spécial*
$p = 3,\ \mu = 2,\ p \,\|\, \mathcal{F}_2$</th><th>$p \geq 3$</th></tr>
<tr><td>$\mathcal{C}_0$</td><td>$\alpha \geq 2\beta - 1$</td><td>$3^2 \mid (S^2 + Q)$</td><td>$\alpha \geq 2\beta$</td></tr>
<tr><td rowspan="2">$\mathcal{C}_1$</td><td>$\beta = 1$</td><td rowspan="2">$3^2 \mid (S^3 + 2QS + R)$</td><td rowspan="2">$\alpha = \beta$ *et*
$p^{\alpha} \mid (AS + B)$</td></tr>
<tr><td>$\beta \geq 2\,,\ \alpha = \beta$ *et*
$2^{2\alpha-1} \mid (S^3 + 2QS + R)$</td></tr>
</table>

Le critère $\mathcal{F}_2$ est utilisé dans les paragraphes 7 et 8. Deux exemples extraits de [11, Table, p. 42], illustrent le cas où $p \,\|\, \mathcal{F}_2$, avec $p = 2$ ou $p = 3$ et $\mu = 2$: les solutions de l'équation (1) sont égales à 0, 1, 4, 12 pour $S = 2$, $Q = -4$, $R = 2$ et à 0, 1, 4, 9 pour $S = 3$, $Q = -9$, $R = 9$.

P r e u v e. Suivant le signe et la parité de n, l'équation (1) est équivalente à l'une des équations suivantes :

$$\rho^{\pm 2m} = x\rho + y \quad \text{ou} \quad \rho^{\pm 2m+1} = x\rho + y\,, \tag{18}$$

ce qui ressort de la formule (3) pour $U_{2m} = 0$ ou $U_{2m+1} = 0$, avec $m \in \mathbb{N}$, et de la formule (7) pour $U'_{2m+1} = 0$ ou $U'_{2m} = 0$, avec $m \in \mathbb{N}^*$. D'après (5) et (6), le système (18) est équivalent à

$$\rho^{\pm 2m} = x\rho + y \quad \text{ou} \quad \rho^{\pm 2m} = x + y\omega/R\,. \tag{19}$$

Par hypothèse, p est un nombre premier tel que $p \,|\, \mathcal{F}_2$ et $p \nmid R$. Pour $h \geq 2$, la relation $V_h = QV_{h-2} - \mathcal{F}_2 U_{h-2}$ implique $V_{2m+1} \equiv Q^m$ et $V_{2m} \equiv 0 \pmod p$. De même, pour $h \geq 1$, la relation $U_h = SU_{h-1} + V_{h-1}$ implique $U_{2m+1} \equiv SU_{2m}$ et $U_{2m} \equiv S^2 U_{2m-2} + Q^{m-1} \pmod p$; ce qui donne deux formules pour U_{2m} modulo p :

$$U_{2m} \equiv (S^{2m} - Q^m)/(S^2 - Q) \text{ si } S^2 \not\equiv Q \quad \text{et} \quad U_{2m} \equiv mQ^{m-1} \text{ si } S^2 \equiv Q\,.$$

Des congruences analogues s'obtiennent en remplaçant le triplet (S, Q, R) par $(-Q, -RS, R^2)$: $U'_{2m+1} \equiv -Q^m U_{2m}$; $U'_{2m} \equiv Q^{m-1} U_{2m}$; $V'_{2m+1} \equiv S^{2m} V_{2m+1}$ et $V'_{2m} \equiv 0 \pmod p$. La condition μ divise m, où μ est défini dans l'énoncé, est donc nécessaire pour que l'une des suites U_{2m}, U_{2m+1}, U'_{2m} ou U'_{2m+1} ait un zéro. Les coordonnées de $\rho^{2\mu}$ figurant dans (3), respectivement dans (6), vérifient alors les congruences suivantes modulo p : $U_{2\mu} \equiv V_{2\mu} \equiv 0$ et $W_{2\mu} \not\equiv 0$; $U_{2\mu+1} \equiv V_{2\mu+2} \equiv 0$ et $W_{2\mu+3} \not\equiv 0$, puisque $W_h = RU_{h-1} = V_{h+1} - QU_h$. Ainsi, p est un "diviseur" de $\rho^{2\mu}$ dans l'anneau $\mathbb{Z}[\rho]$, respectivement $\mathbb{Z}_{(p)}[\omega]$ (Déf. 6). Alors, Thm. 2 appliqué à $\zeta = \rho^{2\mu}$, avec $\theta = \rho$, puis avec $\theta = \omega$, montre que chacune des équations de (19) a au plus deux solutions (au plus trois dans le cas spécial). La compatibilité de ces équations est discutée dans la preuve de [12, Thm. 2], sur la base des relations : $U_{2\mu+1} = SU_{2\mu} + V_{2\mu}$; $V_{2\mu+2} = -\mathcal{F}_2 U_{2\mu} + QV_{2\mu}$. Les conditions $\mathcal{C}_0$ et $\mathcal{C}_1$ résultent de cette discussion. ∎

Proposition 3. *Soient (S, Q, R) un triplet vérifiant l'hypothèse 2, δ le pgcd de Q et de R, d le pgcd de S et de R/δ. Posons $\mathcal{F}_2 = \delta d \mathcal{F}''_2$ où $\mathcal{F}_2 = -(QS + R)$.*

(i) *Le triplet étant de la forme $(abs, \delta q, \delta r)$ avec $\delta = a^2 b$, alors $d = (bs, r)$. Posons $d = cd_1$ où $c = (b, r)$ et $d_1 = (s, r/c)$, puis $b = cb_1$, $s = d_1 s_1$ et $r = cd_1 r_1$; alors $R = \delta d r_1$, $\mathcal{F}''_2 = ab_1 q s_1 + r_1$ avec $(ab_1 q s_1, r_1) = 1$, et $(R, \mathcal{F}''_2) = 1$ lorsque $(d, \mathcal{F}''_2) = 1$. Si "$\mathcal{F}_2$ a la propriété $\mathcal{P}(R)$" alors "$\mathcal{F}''_2$ a la propriété $\mathcal{P}(d)$".*

(ii) *Soit U_n la suite définie dans Prop. 1. Pour $n \neq 0$, la suite U_n n'a pas de zéros pairs si $d \neq 1$ et pour $n \neq 1$, elle n'a pas de zéros impairs si $(d, \mathcal{F}''_2) \neq 1$.*

Preuve. (i) Les définitions de d, c, d_1 et l'hypothèse $(aq, r) = 1$ entraînent que $d = (abs, r) = (bs, r)$, $(b_1 s_1, r_1) = 1$, $(aq_1, r_1) = 1$ et $(b_1, cd_1) = 1$, b étant sans facteurs carrés; les expressions de R et de $\mathcal{F}''_2$ s'en déduisent ainsi que les égalités suivantes : $(R, \mathcal{F}''_2) = (\delta d, \mathcal{F}''_2) = (cd, \mathcal{F}''_2)$ avec $c \,|\, d$, en particulier, $(R, \mathcal{F}''_2) = 1$ lorsque $(d, \mathcal{F}''_2) = 1$. Si "$\mathcal{F}_2$ a la propriété $\mathcal{P}(R)$" alors chaque diviseur premier de $\mathcal{F}_2$ est un diviseur de $\delta d = (R, \mathcal{F}_2)$; comme $\mathcal{F}''_2 \,|\, \mathcal{F}_2$, chaque diviseur premier de $\mathcal{F}''_2$ est aussi un diviseur de δd, mais d'après ce qui précède, c'est un diviseur de cd, donc de d, ainsi "$\mathcal{F}''_2$ a la propriété $\mathcal{P}(d)$".

(ii) Soit p un diviseur premier de d, lorsque $d \neq 1$. Le triplet (S, Q, R) est de la forme $(up^{e+t}, vp^e, wp^{2e+t})$, avec $p \nmid v$, $p^e \parallel c$ et $p^t \parallel d_1$, $e = 0$ ou $e = 1$ et $e + t \geq 1$; $\mathcal{F}_2 = -(uv + w)p^{2e+t}$ avec $p \nmid (uv, w)$. L'expression de U_{2h+2}, respectivement celle de U_{2h+3}, est donnée par la formule combinatoire (13), pour $h \geq 1$

$$\sum_{i+2j+3k=2h \text{ (resp. } 2h+1)} \frac{(i+j+k)!}{i!j!k!} u^i v^j w^k p^{e(i+j+2k)+t(i+k)}\,.$$

Dans le cas de U_{2h+2}, les entiers non négatifs i, j, k vérifient la relation $i + 2j + 3k = 2h$. Nous montrons que $i + k \geq 2$ et $i + j + 2k \geq h + 1$ dès que $0 \leq j \leq h - 1$: la relation $i + 3k = 2(h - j)$ entraîne que $i + 3k \geq 2$ avec $i + k$ pair et non nul, l'inégalité $i + k \geq 2$ implique $i + 2k + 2h \geq 2(h + 1)$ avec $i + 2k + 2h = 2(i + j + 2k)$. Nous déduisons alors de la congruence

$$p^{-eh} U_{2h+2} \equiv v^h \pmod{p^{e+2t}}$$

que $U_{2h+2} \neq 0$ pour $h \geq 1$, avec $U_2 = 1$. Dans le cas de U_{2h+3}, on vérifie de même que $i + k \geq 3$ et $i + j + 2k \geq h + 2$ pour $0 \leq j \leq h - 2$. Nous en déduisons que

$$p^{-(eh+e+t)} U_{2h+3} \equiv (uv + h(uv + w))v^{h-1} \pmod{p^{e+2t}}\,.$$

L'hypothèse $p \,|\, \mathcal{F}_2''$ implique $p \,|\, (uv + w)$ et $p \nmid uvw$. Dans ce cas, la congruence $p^{-(eh+e+t)} U_{2h+3} \equiv uv^h \pmod{p}$ montre que $U_{2h+3} \neq 0$ pour $h \geq 1$, avec $U_3 = S$. ∎

Remarque 2. Si $U_3 = S = 0$ alors $d = r$ et $\mathcal{F}_2'' = -1$, avec $r \geq 2$. L'équation (1) a trois solutions en n : $0, 1, 3$, et toute solution supplémentaire est impaire (voir §8).

Remarque 3. Le polynôme f est irréductible lorsque $ab \neq c$, d'après le critère d'Eisenstein appliqué à f si $b \neq c$ où à g si $b = c$ [11, p. 21]. Lorsque $ab = c$, le triplet est de la forme $(cd_1 s_1, cq, cd_1 r_1)$ avec les notations de Prop. 3. Si le polynôme f a une racine dans $\mathbb{Z}$ et deux racines complexes conjuguées alors $f(X) = (X - cd_1 k)(X^2 - X cd_1(s_1 - k) + cr_1')$, en posant $r_1 = kr_1'$, où $k \in \mathbb{N}^*$ et $4r_1' > cd_1^2(s_1 - k)^2$. L'indice $\mathcal{F}_2$ est alors égal à $c^2 d_1(s_1 - k)(r_1' + cd_1^2 k s_1)$.

Corollaire 3. *Sous les hypothèses et avec les notations de Prop.* 3, *l'équation* (1) *a deux solutions en n lorsque "l'indice* $\mathcal{F}_2$ *a la propriété* $\mathcal{P}(R)$*", à moins que* $\mathcal{F}_2''$ *ne soit égal à* ± 1, *et elle possède deux ou trois solutions en n lorsque "l'indice* $\mathcal{F}_2$ *n'a pas la propriété* $\mathcal{P}(R)$*", à moins d'avoir* $\mathcal{F}_2'' = \lambda$ *avec* $\lambda \in \{\pm 2, \pm 3\}$ *et* $(\lambda, R) = 1$. *Dans ce cas le nombre de solutions est au plus égal à quatre, et s'il existe deux solutions, distinctes de* 0 *et de* 1, *alors elles ont la même parité si* $\lambda = \pm 3$ *et des parités différentes si* $\lambda = \pm 2$, *et* $d = 1$ *lorsque* $\lambda = \pm 2$.

P r e u v e. D'après Cor. 2, l'équation (1) est équivalente à l'équation $U_n = 0$. D'après Prop. 3(i), $\mathcal{F}_2 = \delta d\mathcal{F}_2''$ et la condition $(d, \mathcal{F}_2'') = 1$ est nécessaire pour que la suite U_n ait un zéro non trivial; dans ce cas $(R, \mathcal{F}_2'') = 1$, ce que nous supposons dans la suite. Lorsque "$\mathcal{F}_2$ a la propriété $\mathcal{P}(R)$" alors "$\mathcal{F}_2''$ a la propriété $\mathcal{P}(d)$", chaque diviseur premier de $\mathcal{F}_2''$ est un diviseur de $(d, \mathcal{F}_2'')$, donc $\mathcal{F}_2'' = \pm 1$. Dans le cas où "$\mathcal{F}_2$ n'a pas la propriété $\mathcal{P}(R)$", comme $(R, \mathcal{F}_2'') = 1$, chaque diviseur premier de $\mathcal{F}_2''$ vérifie les hypothèses de Thm. 3, et le résultat se déduit du critère $\mathcal{F}_2$ appliqué avec $p = 2$ ou $p = 3$ dans le cas spécial. ∎

§ 3. Solutions modulo trois : "$\mathcal{F}_3$ n'a pas la propriété $\mathcal{P}(R)$"

Sous l'hypothèse 2, chaque solution en n de l'équation (1) est un zéro de la suite U_n (Cor. 2). Suivant que n est congru à 0, 1 ou 2 modulo 3, l'équation (1) est équivalente, via (3) et (6), à l'une des équations suivantes :

$$\begin{cases} (20) \quad \rho^{3h} = V_{3h}\rho + W_{3h} \\ (21) \quad \rho^{3h+1} = V_{3h+1}\rho + W_{3h+1} \;\Leftrightarrow (23)\; \rho^{3h} = (1/R)(V_{3h+2}\omega + W_{3h+3})\,. \\ (22) \quad \rho^{3h+2} = V_{3h+2}\rho + W_{3h+2} \end{cases}$$

Théorème 5. *Soit (S, Q, R) un triplet vérifiant l'hypothèse* 2, $\mathcal{F}_3 = Q^2(S^2 + Q) - RS^3$. *Si "l'indice $\mathcal{F}_3$ n'a pas la propriété $\mathcal{P}(R)$" alors le nombre de solutions en n de l'équation* (1) *est au plus égal à quatre.*

Critère $\mathcal{F}_3$. *Supposons qu'il existe un nombre premier p tel que $p \mid \mathcal{F}_3$ et $p \nmid R$. Si $S = 0$ alors l'équation* (1) *a exactement trois solutions en n : $0, 1, 3$. Lorsque S est non nul, désignons par μ le plus petit entier positif tel que p soit un "diviseur" de $\rho^{3\mu}$ dans l'ordre $\mathbb{Z}[\rho]$; avec les conventions de Déf.* 6, *posons*

$$\rho^{3\mu} = p^{\alpha}A\rho^2 + p^{\beta}B\rho + C\,.$$

Si $p \mid QS$ alors $\mu = 1$ sauf dans le cas spécial $(*)$ (voir ci-dessous). Si $p = 3$ et $p \nmid QS$ alors $\mu = 2$ et on peut utiliser le critère $\mathcal{F}_2$. Si $p \geq 5$ et $p \nmid QS$, ν étant le plus petit entier positif et inférieur à μ tel que $U_{3\nu+2} \equiv 0 \pmod{p}$, alors μ et ν sont définis dans Prop. 4. *Posons*

$$\rho^{3\nu+2} = E\rho^2 + F\rho + G\,.$$

Les solutions modulo trois de l'équation (1) *sont alors de la forme $n = 3\mu m$, $n = 3\mu m + 1$ ou $n = 3\mu m + 3\nu + 2$. Chacune des équations* (20), (21) *et* (22) *a au plus deux solutions, deux d'entre elles ont au plus trois solutions et elles ont ensemble au plus quatre solutions. Les conditions $\mathcal{C}_0$, $\mathcal{C}_1$ et $\mathcal{C}_2^2$ ci-dessous sont nécessaires pour que respectivement chacune de ces*

équations ait deux solutions; *tandis que la condition* $\mathcal{C}_2^1$ *est nécessaire pour que l'équation* (22) *ait une solution.*

	$p \nmid QS$	$p \mid QS$ *et* $p \neq 2$	$p \mid QS$ *et* $p = 2$	
$\mathcal{C}_0$	$\alpha \geq 2\beta$		$\alpha \geq 2\beta - 1$	
$\mathcal{C}_1$	$\alpha = \beta$ *et* $p^\alpha \mid (AS + B)$	$\beta \geq 2\alpha$	$\mu = 1$	$\beta \geq 2\alpha - 1$
			$\mu = 2$	$\beta = \alpha + 1$ *et* $2^{\alpha-2} \mid (AS + B)$

(∗) *Dans le cas spécial où* $p = 2$, $\mu = 1$, $\alpha = \beta = 1$, *prendre* $\mu = 2$.

	$\alpha = \beta$		$\alpha \neq \beta$
$\mathcal{C}_2^1$	$0 \leq \lambda < \alpha$	$p^\lambda \parallel ((AS + B)F + AG)$ *et* $p^{\lambda+\alpha} \mid E$	$p^{\min(\alpha,\beta)} \mid E$
$\mathcal{C}_2^2$	$p^\alpha \mid ((AS + B)F + AG)$ *et* $p^{2\alpha} \mid E$		

P r e u v e. Pour déterminer le nombre maximum de solutions de l'équation (1), nous étudions le système équivalent formé des équations (20), (22), et (23). Supposons qu'il existe un nombre premier p tel que $p \mid \mathcal{F}_3$ et $p \nmid R$; par définition de $\mathcal{F}_3$, si $p \mid QS$ alors $p \mid Q$ et $p \mid S$. Nous distinguons deux cas suivant que p divise ou non QS.

P r e m i e r c a s : $p \mid \mathcal{F}_3$ et $p \nmid QSR$. L'indice $\mathcal{F}_3$ est impair lorsque S, Q et R sont impairs, donc $p \neq 2$. Dans le cas où $p = 3$, la congruence $Q^2(S^2 + Q) \equiv RS^3 \pmod 3$ implique $(1 + Q) \equiv RS$, $Q \equiv 1$ et $R \equiv -S \pmod 3$; donc $\mathcal{F}_2 = -(QS + R) \equiv 0 \pmod 3$. D'après le critère $\mathcal{F}_2$, l'une des conditions ($3 \parallel \mathcal{F}_2$ et $3^2 \mid (S^2 + Q)$) ou bien ($3 \parallel \mathcal{F}_2$ et $3^2 \mid (S^3 + 2QS + R)$) est nécessaire pour que l'équation (1) ait quatre solutions. Comme $S^2 + Q \equiv -1$ et $S^2 + 2Q \equiv 0 \pmod 3$, aucune de ces conditions n'est satisfaite. Nous déduisons du critère $\mathcal{F}_2$ que l'équation (1) a dans ce cas deux ou trois solutions, de la forme $n = 6m$ ou $n = 6m + 1$.

Nous supposons que $p \geq 5$. D'après Prop. 4, les solutions en h de chacune des équations (20) et (23) sont de la forme $h = \mu m$ avec $m \in \mathbb{N}$, où μ est le plus petit entier positif tel que p soit un "diviseur" de $\rho^{3\mu}$ dans les anneaux $\mathbb{Z}[\rho]$ et $\mathbb{Z}_{(p)}[\omega]$, via les formules (3) et (6). Avec les conventions de Déf. 6, posons

$$\rho^{3\mu} = p^\alpha A\rho^2 + p^\beta B\rho + C\,, \qquad \rho^{3\mu} = (1/R)(p^{\alpha_1} A_1\omega^2 + p^{\beta_1} B_1\omega + C_1)\,;$$

et les relations suivantes se déduisent de (15) :

$$p^{\alpha_1} A_1 = p^\alpha AS + p^\beta B\,, \qquad p^{\beta_1} B_1 = p^{\alpha_1} A_1 Q + p^\alpha AR\,. \tag{24}$$

D'après Thm. 2, appliqué à $\zeta = \rho^{3\mu}$ pour $p \geq 5$, avec $\theta = \rho$ puis avec $\theta = \omega$, chacune des équations (20) et (23) a au plus deux solutions. Nous montrons que ces deux équations ont ensemble deux ou trois solutions. Pour que l'équation (20) ait deux solutions il faut que $\alpha \geq 2\beta$, ce qui entraîne

d'après (24), $\alpha_1 = \beta$ et $\beta_1 = \beta$. Comme $\alpha_1 = \beta_1$, l'équation (23) a une seule solution. De même, pour que l'équation (23) ait deux solutions il faut que $\alpha_1 \geq 2\beta_1$; d'après (24) cette condition est équivalente à

$$\alpha = \beta \quad \text{et} \quad p^{\alpha} \,|\, (AS + B)\,,$$

et dans ce cas l'équation (20) a une seule solution. Dans Prop. 4 nous montrons que les solutions de l'équation (22) sont de la forme $n = 3\mu m + 3\nu + 2$ où ν est le plus petit entier positif, avec $\nu < \mu$, tel que $U_{3\nu+2} \equiv 0 \pmod{p}$. D'après Prop. 5, les conditions

$$\alpha = \beta\,, \quad p^{2\alpha} \,|\, U_{3\nu+2} \quad \text{et} \quad p^{\alpha} \,|\, ((AS + B)V_{3\nu+2} + AW_{3\nu+2})$$

sont nécessaires pour que l'équation (22) ait deux solutions et dans ce cas, chacune des équations (20) et (23) a une seule solutions d'après les résultats qui précèdent. Nous avons ainsi montré que l'équation (1) possède au plus quatre solutions lorsque $p \,|\, \mathcal{F}_3$ et $p \nmid QRS$.

S e c o n d c a s : $p \,|\, (Q, S)$ et $p \nmid R$. D'après Prop. 2(ii), la suite U_n n'a pas de zéros de la forme $n = 3h + 2$, l'équation (22) n'a donc pas de solutions. Lorsque ρ est un entier de trace nulle, montrons que l'équation (1) a exactement trois solutions en $n : 0, 1, 3$. S étant nul, les équations (20) et (23) sont de la forme suivante :

$$\rho^{3h} = (Q\rho + R)^h\,, \qquad \rho^{3h} = R^{-h}(Q\omega^2 + Q^2\omega + R^2)^h\,,$$

avec $p \,|\, Q$ et $p \nmid R$. Nous appliquons Thm. 2 à $\zeta = \rho^3$, d'une part avec $\theta = \rho$ pour $p \geq 2$, alors l'équation (20) a exactement deux solutions (pour $p = 3$, la trace de ρ est un multiple de 3), d'autre part avec $\theta = \omega$, pour $p \geq 3$ ou bien pour $p = 2$ et Q un multiple de 4, alors l'équation (23) a une seule solution. Lorsque $2 \,\|\, Q$, d'après (13), on a $U_{3h+1} \equiv hQR^{h-1} \pmod{16}$. Les solutions de l'équation (23) sont de la forme ρ^{6m} avec $m \in \mathbb{N}$ et $\rho^6 = 2Q\omega^2 + 3Q^2\omega + Q^3 + R^2$, cette équation a une seule solution, d'après Thm. 2 appliqué à $\zeta = \rho^6$ avec $\theta = \omega$, pour $p = 2$. Nous supposons que S n'est pas nul; il existe alors des entiers positifs α et β tels que $S = p^{\alpha}A$ et $Q = p^{\beta}B$ avec $p \nmid AB$, et d'après (3) et (6),

$$\rho^3 = S\rho^2 + Q\rho + R\,, \qquad \rho^3 = (1/R)(U_4\omega^2 + V_5\omega + W_6)\,.$$

Comme $U_4 = S^2 + Q$ et $V_5 = QU_4 + RS$, les relations (24) se mettent sous la forme

$$U_4 = p^{2\alpha}A^2 + p^{\beta}B = p^{\alpha_1}A_1\,, \qquad V_5 = p^{\beta+\alpha_1}BA_1 + p^{\alpha}AR = p^{\beta_1}B_1\,. \tag{25}$$

Donc, ρ^3 admet p comme "diviseur" dans $\mathbb{Z}[\rho]$ et aussi dans $\mathbb{Z}_{(p)}[\omega]$. Nous appliquons alors Thm. 2 à $\zeta = \rho^3$ avec $\theta = \rho$ puis avec $\theta = \omega$, pour $p \geq 3$ ou pour $p = 2$ lorsque 4 divise (Q, S). Remarquons que pour $p = 3$, les traces de ρ et de ω sont des multiples de 3. Pour que l'équation (20) ait deux solutions il faut que $\alpha \geq 2\beta$ pour $p \neq 2$ ou que $\alpha \geq 2\beta - 1$ pour $p = 2$;

les relations (25) impliquent dans ce cas $\alpha_1 = \beta$ et $\beta_1 \geq 2\beta$ pour $p \neq 2$, $\alpha_1 = \beta$ et $\beta_1 \geq 2\beta - 1$ pour $p = 2$. Comme $\alpha_1 < \beta_1$, avec $2 \leq \alpha_1$ pour $p = 2$, l'équation (23) a une seule solution. De même, pour que l'équation (23) ait deux solutions il faut que $\alpha_1 \geq 2\beta_1$ pour $p \neq 2$ ou que $\alpha_1 \geq 2\beta_1 - 1$ pour $p = 2$; via (25), ces conditions sont équivalentes à $\beta \geq 2\alpha$ pour $p \neq 2$ ou à $\beta \geq 2\alpha - 1$ pour $p = 2$. Comme $\alpha < \beta$, avec $2 \leq \alpha$ pour $p = 2$, l'équation (20) a une seule solution. Le cas où $p = 2$ et $2 \parallel (Q, S)$ est traité dans Prop. 6. Nous avons ainsi montré que l'équation (1) a deux ou trois solutions lorsque $p \mid (Q, S)$ et $p \nmid R$. ∎

Proposition 4. *Soient (S, Q, R) un triplet vérifiant l'hypothèse* 2, *p un nombre premier tel que $p \geq 5$, $p \mid \mathcal{F}_3$ et $p \nmid QSR$, avec $\mathcal{F}_3 = Q^2(S^2 + Q) - RS^3$, et U_n la suite définie dans Prop.* 1. *Les zéros modulo trois de la suite U_n sont alors de la forme $n = 3\mu m$, $n = 3\mu m + 1$ ou $n = 3\mu m + 3\nu + 2$, μ et ν étant des entiers positifs tels que*

(i) *si $p \nmid (QS + 3R)$ alors μ est la plus petite solution de la congruence $(1 + S^2/Q)^{3\mu} \equiv 1 \pmod p$, et ν est l'unique solution, si elle existe, de la congruence $(1 + S^2/Q)^{3\nu+2} \equiv -(2 + S^2/Q) \pmod p$, avec $1 \leq \nu \leq \mu - 1$;*

(ii) *si $p \mid (QS + 3R)$ alors $3 \mid (p - 1)$, $\mu = p$ et ν est le reste modulo p de $S^2/(3Q)$.*

Les coordonnées de $\rho^{3\mu}$ et celles de $\rho^{3\nu+2}$ dans l'ordre $\mathbb{Z}[\rho]$ vérifient alors les congruences : $U_{3\mu} \equiv V_{3\mu} \equiv 0$ et $W_{3\mu} \not\equiv 0$; $U_{3\nu+2} \equiv 0$ et $QV_{3\nu+2} \equiv SW_{3\nu+2} \not\equiv 0 \pmod p$.

P r e u v e. Le polynôme minimal et le discriminant de ρ sont donnés par

$$\begin{cases} \operatorname{disc}(\rho) = 4\mathcal{F}_3 - 3(QS + 3R)^2\,, \\ f(X) = (X - (S^2 + Q)/S)(X^2 + X(Q/S) + (Q/S)^2) + \mathcal{F}_3/S^3\,. \end{cases}$$

Rappelons que, suivant la décomposition de f modulo p, le polynôme f a trois racines distinctes ρ_1, ρ_2, ρ_3 dans $\mathbb{Q}_p$ ou dans une extension quadratique de $\mathbb{Q}_p$. D'après la formule (4), U_n a l'expression suivante :

$$\delta_f U_n = (\rho_2 - \rho_3)\rho_1^n + (\rho_3 - \rho_1)\rho_2^n + (\rho_1 - \rho_2)\rho_3^n\,,$$

avec $\delta_f = -(\rho_2 - \rho_3)(\rho_3 - \rho_1)(\rho_1 - \rho_2)$ et $\delta_f^2 = \operatorname{disc}(\rho)$. Si f a une seule racine modulo p alors $p + 1$ est un multiple de 3. D'après le Lemme de Hensel (voir le livre de Cassels [8, p. 49]), l'une des racines de f est dans $\mathbb{Z}_p$, l'anneau des entiers p-adiques, les deux autres racines appartiennent à $\mathbb{Z}_p[j] = \mathbb{Z}_p + j\mathbb{Z}_p$, où j est une racine cubique de l'unité, distincte de 1. Nous avons dans ce cas les congruences

$$\begin{cases} \rho_1 \equiv (S^2 + Q)/S \pmod{p\mathbb{Z}_p}\,, \\ \rho_2 \equiv jQ/S\,,\ \rho_3 \equiv j^2Q/S \pmod{p\mathbb{Z}_p[j]}\,. \end{cases} \tag{26}$$

Lorsque $p-1$ est un multiple de 3, $j \in \mathbb{Z}_p$ et la formule

$$f(X) = (X-(S^2+Q)/S)^2(X+(S^2+2Q)/S) \\ +(X-(S^2+Q)/S)(3\mathcal{F}_3+S^3(QS+3R))/(QS^2)+\mathcal{F}_3/S^3$$

montre que f a deux racines modulo p, lorsque p divise $\mathrm{disc}(\rho)$, et dans ce cas $j \equiv (S^2+Q)/Q \pmod p$. Le polynôme f a une racine dans $\mathbb{Z}_p$, les deux autres racines appartiennent soit à $\mathbb{Z}_p$, soit à une extension quadratique de $\mathbb{Q}_p$, qui est ramifiée lorsque p divise le discriminant du corps $\mathcal{K}$. Lorsque p ne divise pas $\mathrm{disc}(\rho)$, $p-1$ étant un multiple de 3, le polynôme f a trois racines dans $\mathbb{Z}_p$ et les formules (26) sont vérifiées avec $j \in \mathbb{Z}_p$.

(i) Si $p \nmid (QS+3R)$ alors $p \nmid \mathrm{disc}(\rho)$. L'expression de $\delta_f U_n$ et les formules (26) entraînent les congruences suivantes modulo p :

$$\begin{cases} U_{3h} \equiv S(Q/S)^{3h-3}(y^{3h}-1)/(y^3-1)\,, \\ U_{3h+1} \equiv Q(Q/S)^{3h-3}y(y^{3h}-1)/(y^3-1)\,, \\ U_{3h+2} \equiv Q(Q/S)^{3h-2}(y^{3h+2}+y+1)/(y^3-1)\,, \end{cases}$$

où $y \equiv (S^2+Q)/Q$ et $y^2+y+1 \not\equiv 0 \pmod p$. Soit μ l'ordre de y^3 dans le groupe à $p-1$ éléments $(\mathbb{Z}/p\mathbb{Z})^*$. Si $n=3h$ ou $n=3h+1$ est un zéro de la suite U_n alors $y^{3h} \equiv 1 \pmod p$ et h est un multiple de μ. Si $n=3h+2$ est un zéro de la suite U_n et si $h \equiv \nu \pmod \mu$, alors la congruence $y^{3\nu+2}+y+1 \equiv 0 \pmod p$ a au plus une solution avec $1 \le \nu \le \mu-1$.

(ii) Si $p \mid (QS+3R)$ alors $p \mid \mathrm{disc}(\rho)$. Comme $p \nmid R$, la récurrence modulo p est d'ordre trois. D'après Ward [32], l'expression de U_n modulo p est donnée par

$$U_n \equiv (x_2^n - x_1^n - n(x_2-x_1)x_1^{n-1})/(x_2-x_1)^2\,,$$

où $x_1 \equiv (S^2+Q)/S$ et $x_2 \equiv -(S^2+2Q)/S \pmod p$. Nous avons dans ce cas les congruences suivantes modulo p :

$$U_{3h} \equiv hS(Q/S)^{3h-3}\,, \quad U_{3h+1} \equiv hyQ(Q/S)^{3h-3}\,, \\ U_{3h+2} \equiv -(3h+1-y)S^{-1}(Q/S)^{3h+1}\,;$$

où $y \equiv (S^2+Q)/Q$ et $y^2+y+1 \equiv 0 \pmod p$. Si $n=3h$ ou $n=3h+1$ est un zéro de la suite U_n alors h est un multiple de p, et on pose $\mu = p$. Si $n=3h+2$ est un zéro de la suite U_n alors $3h \equiv S^2/Q \pmod p$ et 3ν est le reste modulo p de S^2/Q.

Les coordonnées de $\rho^{3\mu}$ et celles de $\rho^{3\nu+2}$ dans l'ordre $\mathbb{Z}[\rho]$ sont données par la formule (3). D'après ce qui précède, $U_{3\mu} \equiv 0$, $V_{3\mu} = U_{3\mu+1} - SU_{3\mu} \equiv 0$ et $W_{3\mu} = RU_{3\mu-1} \not\equiv 0 \pmod p$. Comme $U_{3\nu+2} \equiv 0 \pmod p$, un calcul simple montre que $V_{3\nu+2} \equiv U_{3\nu+3} \equiv -(Q/S)^{3\nu+1}$, $W_{3\nu+2} \equiv U_{3\nu+4} - SU_{3\nu+3} \equiv -(Q/S)^{3\nu+2} \pmod p$. ∎

PROPOSITION 5. *Sous les hypothèses de Prop.* 4, *l'équation* (22) *a au plus deux solutions.*

P r e u v e. Nous traitons par une méthode p-adique l'équation $U_{3h+2} = 0$, qui est équivalente à l'équation (22). Soit μ l'entier positif défini dans Prop. 4. D'après (24), $\rho^{3\mu} = p^\alpha A\rho^2 + p^\beta B\rho + C$; posons $t = \min(\alpha, \beta)$, $\rho^{3\mu} = c(p^t\gamma + 1)$ et pour $k \in \mathbb{N}$, $\gamma^k = u_k\rho^2 + v_k\rho + w_k$. Il est utile pour la suite de calculer les coordonnées de γ^k pour $k \in \{0, 1, 2\}$; elles sont données par

$$(27)\qquad \begin{cases} u_0 = v_0 = 0\,;\ w_0 = 1\,;\ cu_1 = p^{\alpha-t}A\,;\ cv_1 = p^{\beta-t}B\,;\ w_1 = 0\,;\\ u_2 = (Su_1 + v_1)^2 + Qu_1^2\,;\ v_2 = Qu_1(Su_1 + 2v_1) + Ru_1^2\,;\\ w_2 = Ru_1(Su_1 + 2v_1)\,. \end{cases}$$

Nous déduisons de [12, Lemme 1], le résultat suivant. La série d'interpolation $\mathcal{U}(m)$ de la suite $c^{-m}U_{3\mu m}$ représente une fonction analytique sur $\mathbb{Z}_p$; elle est donnée par

$$\begin{cases} \mathcal{U}(m) = c^{-m}U_{3\mu m} & \text{pour } m \in \mathbb{N},\\ \mathcal{U}(m) = \sum_{1\le j} m^j\mathcal{U}_j & \text{pour } m \in \mathbb{Z}_p, \text{ avec } \mathcal{U}_j = \sum_{j\le k}(1/k!)s(k,j)p^{tk}u_k, \end{cases}$$

où $s(k, j)$ est le coefficient de x^j dans $x(x-1)\dots(x-k+1)$. Les résultats sont analogues pour les séries d'interpolation $\mathcal{V}(m)$ et $\mathcal{W}(m)$ des suites $c^{-m}V_{3\mu m}$ et $c^{-m}W_{3\mu m}$. D'après Prop. 4, les zéros de la suite U_{3h+2} sont de la forme $3\mu m + 3\nu + 2$ et d'après (10), nous avons la relation suivante :

$$U_{3\mu m+3\nu+2} = U_{3\nu+4}U_{3\mu m} + U_{3\nu+3}V_{3\mu m} + U_{3\nu+2}W_{3\mu m}\,.$$

Pour $m \in \mathbb{Z}_p$, considérons la série d'interpolation $\mathcal{T}(m)$ de la suite $c^{-m}U_{3\mu m+3\nu+2}$; elle est définie par

$$\begin{cases} \mathcal{T}(m) = U_{3\nu+4}\mathcal{U}(m) + U_{3\nu+3}\mathcal{V}(m) + U_{3\nu+2}\mathcal{W}(m)\,,\\ \mathcal{T}(m) = \mathcal{T}_0 + \sum_{1\le j} m^j\mathcal{T}_j\,,\\ \mathcal{T}_j = U_{3\nu+4}\mathcal{U}_j + U_{3\nu+3}\mathcal{V}_j + U_{3\nu+2}\mathcal{W}_j\,, \quad \mathcal{T}_0 = U_{3\nu+2}\,. \end{cases}$$

Posons $E = U_{3\nu+2}$, $F = V_{3\nu+2}$, $G = W_{3\nu+2}$. Alors, par définition, $U_{3\nu+4} = E(S^2 + Q) + FS + G$, $U_{3\nu+3} = ES + F$, et il résulte de Prop. 4 que $p \,|\, E$, $p \nmid FG$ et $QF \equiv SG \pmod p$. Les hypothèses $p \,|\, \mathcal{F}_3$ et $p \nmid QSR$ entraînent les congruences modulo p

$$FS + G \equiv F(S^2 + Q)/S\,, \qquad Q^2(S^2 + Q) \equiv RS^3\,, \qquad QSR \not\equiv 0\,.$$

Nous obtenons $|U_{3\nu+2}| < 1$, $|U_{3\nu+4}| = |U_{3\nu+3}| = 1$, en prenant les valeurs absolues p-adiques. $|\mathcal{T}_0| = |E|$ et pour $j \ge 1$, appliquons l'inégalité ultramétrique à $\mathcal{T}_j$:

$$|\mathcal{T}_j| \le \max(|\mathcal{U}_j|, |\mathcal{V}_j|, |E\mathcal{W}_j|)\,.$$

Nous déduisons alors d'un résultat de Mahler [21, p. 224] que la série $\mathcal{T}(m)$ est une fonction analytique sur $\mathbb{Z}_p$. D'après le Théorème de Strassmann, tel

qu'il est énoncé dans le livre de Cassels [8, p. 62], l'équation $\mathcal{T}(m) = 0$ a au plus N solutions dans $\mathbb{Z}_p$, N étant défini par

$$|\mathcal{T}_N| = \max_j |\mathcal{T}_j|\,, \qquad |\mathcal{T}_N| > |\mathcal{T}_j| \quad \text{pour tout } j > N\,.$$

A fortiori, l'équation (22) a au plus N solutions dans $\mathbb{N}$. Pour déterminer N utilisons les congruences suivantes qui proviennent de [12, Lemme 2] pour $p \geq 5$:

$$\begin{cases} \mathcal{T}_1 \equiv p^t T_1 - (1/2)p^{2t} T_2 & (\mathrm{mod}\ p^{3t}), \\ \mathcal{T}_2 \equiv (1/2)p^{2t} T_2 & (\mathrm{mod}\ p^{3t}), \\ \mathcal{T}_j \equiv 0 \quad (j \geq 3) & (\mathrm{mod}\ p^{3t}), \end{cases}$$

avec $T_1 = (E(S^2+Q)+FS+G)u_1 + (ES+F)v_1$ et $T_2 = (E(S^2+Q)+FS+G)u_2 + (ES+F)v_2 + Ew_2$. Après réduction modulo p nous obtenons

$$T_1 \equiv (FS+G)u_1 + Fv_1 \quad \text{et} \quad T_2 \equiv (FS+G)u_2 + Fv_2\,.$$

Montrons maintenant que si $p \,|\, T_1$ alors $p \nmid T_2$. Remarquons que $p \,|\, T_1$ implique $\alpha = \beta = t$ et les congruences $F(AS+B) \equiv -AG \pmod p$, par définition de u_1 et de v_1, formules (27), puis compte-tenu de $QF \equiv SG$, $S(AS+B) \equiv -AQ$. Remplaçons $AS+B$ par $-AQ/S$ dans les expressions de u_2 et de v_2, formules (27), et $FS+G$ par $F(S^2+Q)/S$ dans l'expression de T_2, ce qui donne les congruences modulo p

$$c^2 T_2 \equiv FA^2(Q(S^2+Q)^2 + RS^3 - QS^2(S^2+2Q))/S^3 \equiv FA^2Q^2(S^2+2Q)/S^3\,.$$

Via l'hypothèse $p \,|\, \mathcal{F}_3$, et d'après Prop. 4, $p \nmid T_2$.

L'application répétée du Théorème de Strassmann permet de conclure. En effet, dans le cas où $p \nmid T_1$ nous obtenons que $|\mathcal{T}_1| = |p^t|$, avec $|\mathcal{T}_1| > |\mathcal{T}_j|$ pour tout $j \geq 2$, ainsi $N = 1$ si $|\mathcal{T}_0| \leq |\mathcal{T}_1|$ auquel cas $p^t \,|\, E$, et $N = 0$ sinon. Lorsque $p^\lambda \,\|\, T_1$ avec $\lambda \geq 1$, alors $\alpha = \beta = t$, nous obtenons que $|\mathcal{T}_2| = |p^{2\alpha}|$, avec $|\mathcal{T}_2| > |\mathcal{T}_j|$ pour tout $j \geq 3$. Si $\lambda < \alpha$ alors $|\mathcal{T}_1| = |p^{\lambda+\alpha}|$ et $|\mathcal{T}_1| > |\mathcal{T}_2|$, dans ce cas $N = 1$ si $|\mathcal{T}_0| \leq |\mathcal{T}_1|$, donc si $p^{\lambda+\alpha} \,|\, E$, et $N = 0$ sinon. Enfin, si $\lambda \geq \alpha$ alors $|\mathcal{T}_1| \leq |\mathcal{T}_2|$, $N = 2$ si $|\mathcal{T}_0| \leq |\mathcal{T}_2|$, c'est-à-dire, pour $p^{2\alpha} \,|\, E$, et $N = 0$ sinon. L'équation (22) a donc au plus deux solutions. Les conditions $\alpha = \beta$, $p^{2\alpha} \,|\, E$ et $p^\alpha \,|\, ((AS+B)F + AG)$ sont nécessaires pour qu'il y ait deux solutions. ∎

Remarque 4. Beukers [4, Lemme 7] utilise, dans des conditions non banales, la série d'interpolation d'une suite récurrente linéaire sans faire appel au Théorème de Strassmann.

Proposition 6. *Soit (S, Q, R) un triplet vérifiant l'hypothèse 2 et les conditions suivantes : Q et S sont pairs, R est impair, Q ou S n'est pas un multiple de 4. Les équations (20) et (23) ont alors deux ou trois solutions.*

Preuve. Posons $S = 2^\sigma s$ pour $S \neq 0$, $Q = 2^\tau q$ avec q et s impairs,

$\sigma = 1$ ou $\tau = 1$. D'après (3) et (6), les formules

$$\rho^3 = S\rho^2 + Q\rho + R\,,$$
$$\rho^3 = (1/R)((S^2+Q)\omega^2 + (Q(S^2+Q)+RS)\omega + R(S^3+2QS+R))$$

montrent que 2 est un "diviseur" de ρ^3 dans $\mathbb{Z}[\rho]$ et aussi dans $\mathbb{Z}_{(2)}[\omega]$. D'après Thm. 2 appliqué à $\zeta = \rho^3$, pour $p = 2$, avec $\theta = \rho$ puis $\theta = \omega$, chacune des équations (20) et (23) a au plus deux solutions, et pour $S = 0$, l'équation (20) a exactement deux solutions. Nous allons montrer que ces deux équations ont au plus trois solutions. Trois cas sont à considérer :

$$\text{cas 1 : } \sigma \geq 2 \text{ et } \tau = 1\,, \quad \text{cas 2 : } \sigma = 1 \text{ et } \tau \geq 2\,, \quad \text{cas 3 : } \sigma = \tau = 1\,.$$

D'après ce qui précède, l'équation (20) dans le cas 1 et l'équation (23) dans le cas 2 ont chacune au plus deux solutions. Remarquons que $\rho^3 \notin \mathbb{Z}[2\rho]$ dans les cas 2 et 3, et que $\rho^3 \notin \mathbb{Z}_{(2)}[2\omega]$ dans les cas 1 et 3. Il résulte de la formule (13) que dans les cas 2 et 3, $U_{3h} \equiv 2hsR^{h-1} \pmod 4$ et que dans les cas 1 et 3 $U_{3h+1} \equiv 2hqR^{h-1} \pmod 4$. Nous déduisons de ces congruences que les solutions de l'équation (20) dans les cas 2 et 3, et celles de l'équation (23) dans les cas 1 et 3, sont de la forme $6m$ avec $m \in \mathbb{N}$ et 2 est un "diviseur" de ρ^6. D'après (3) et (6), nous avons en effet

$$\rho^6 = U_6\rho^2 + V_6\rho + W_6\,, \quad \rho^6 = (1/R)(U_7\omega^2 + V_8\omega + W_9)\,;$$

ainsi que les relations suivantes correspondant à (24) pour $\mu = 2$:

$$(28) \qquad \begin{cases} U_6 = S^4 + 3QS^2 + Q^2 + 2RS = 2^\alpha A\,, \\ V_6 = (QS+R)(S^2+2Q) = 2^\beta B\,, \\ U_7 = SU_6 + V_6 = 2^{\alpha_1}A_1\,, \quad V_8 = QU_7 + RU_6 = 2^{\beta_1}B_1\,. \end{cases}$$

Dans les cas 1 et 2 nous obtenons $\alpha = \beta = \alpha_1 = \beta_1 = 2$. D'après Thm. 2 appliqué à $\zeta = \rho^6$, pour $p = 2$, avec $\theta = \rho$ respectivement $\theta = \omega$, l'équation (20) dans le cas 2, respectivement l'équation (23) dans le cas 1, a une seule solution. Dans le cas 3, nous obtenons $\alpha \geq 3$ et $\beta \geq 3$, ainsi que $\alpha_1 \geq 3$ et $\beta_1 \geq 3$; nous appliquons encore Thm. 2. La condition $\alpha \geq 2\beta - 1$ est nécessaire pour que l'équation (20) ait deux solutions; cette condition implique, via (28), $\alpha_1 = \beta$ et $\beta_1 = \beta + 1$. Comme $3 \leq \alpha_1 < \beta_1$, l'équation (23) a une seule solution. La condition $\alpha_1 \geq 2\beta_1 - 1$ est nécessaire pour que l'équation (23) ait deux solutions. Cette condition est équivalente, d'après (28), à

$$\beta = \alpha + 1 \quad \text{et} \quad 2^{\alpha-2} \mid (As + B)\,.$$

Comme $3 \leq \alpha \leq \beta$, l'équation (20) a une seule solution. Les équations (20) et (23) ont donc deux ou trois solutions. ∎

Corollaire 4. *Sous les hypothèses de Thm.* 5, *si l'équation* (22) *n'a pas de solutions alors l'équation* (1) *a deux ou trois solutions. Supposons qu'il existe* k *tel que* $\rho^{3k+2} = V_{3k+2}\rho + W_{3k+2}$ *et soit* p *un nombre premier*

vérifiant les hypothèses du critère $\mathcal{F}_3$. Alors pour $m \geq k$ l'équation (22) *est équivalente à*

$$\rho^{3(m-k)} = x\phi + y \tag{29}$$

où $\phi = -V_{3k+2}\rho^2 + (SV_{3k+2} + W_{3k+2})\rho$. Cette équation a au plus deux solutions de la forme $m-k = \mu l$ et les conditions $\alpha = \beta$ et $p^\alpha \mid ((AS+B)V_{3k+2} + AW_{3k+2})$ sont nécessaires pour qu'il y ait deux solutions.

P r e u v e. Posons $V = V_{3k+2}$, $W = W_{3k+2}$ et $\phi = -V\rho^2 + (SV+W)\rho$; alors $\phi^2 = (QV^2+W^2)\rho^2 + ((R-QS)V^2 - 2QVW)\rho - VR(SV+2W)$. Soit $\mathcal{G}$ l'indice de ϕ dans $\mathbb{Q}(\rho)$; d'après Déf. 5 et Lemme 1, $\mathcal{G} = \mathrm{Norm}(V\rho + W) = R^{3k+2}$. Pour $h \in \mathbb{N}$, définissons les coordonnées de ρ^{3h} dans $\mathbb{Q}(\phi)$ par $\rho^{3h} = (\mathcal{A}_h\phi^2 + \mathcal{B}_h\phi + \mathcal{C}_h)/\mathcal{G}$; elles vérifient les relations

$$\begin{pmatrix} \mathcal{A}_h \\ \mathcal{B}_h \end{pmatrix} = \begin{pmatrix} SV+W & V \\ (QS-R)V^2 + 2QVW & QV^2+W^2 \end{pmatrix} \begin{pmatrix} U_{3h} \\ V_{3h} \end{pmatrix}$$

et $\mathcal{C}_h = RV(SV+2W)\mathcal{A}_h + \mathcal{G}W_{3h}$. D'après la formule (11), $\mathcal{G}\mathcal{A}_h = U_{3h+3k+2}$ et pour $m \geq k$ les zéros de la suite $\mathcal{A}_{m-k}$ correspondent aux solutions de l'équation (22). L'indice de ρ^3 dans $\mathbb{Q}(\phi)$ est égal à $\mathcal{F}_3/\mathcal{G}$, p étant un diviseur premier de $\mathcal{F}_3$ tel que $p \nmid QSR$, alors $p \nmid \mathcal{G}$. Nous déduisons de Prop. 4 et des formules ci-dessus où $QV \equiv SW \pmod p$ et $p \nmid VW$, que les solutions de l'équation (29) sont de la forme $h = \mu l$ et que p est un "diviseur" de $\rho^{3\mu}$ dans l'anneau $\mathbb{Z}_{(p)}[\phi]$. Les relations

$$\mathcal{A}_\mu = p^\alpha A(SV+W) + p^\beta BV\,, \qquad \mathcal{B}_\mu = QV\mathcal{A}_\mu + p^\alpha AV(QW-RV) + p^\beta BW^2$$

et Thm. 2 appliqué à $\zeta = \rho^{3\mu}$ avec $\theta = \phi$ montrent que les conditions de l'énoncé sont nécessaires pour que l'équation (29) ait deux solutions. ∎

§ 4. Solutions modulo trois : "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" et $(aS, Q) \neq \delta$

Théorème 6. *Soient (S, Q, R) un triplet vérifiant l'hypothèse* 2, *$\delta = (Q, R)$ avec $\delta = a^2b$ et $\mathcal{F}_3 = Q^2(S^2+Q) - RS^3$. Si "l'indice $\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" et si $(aS, Q) \neq \delta$ alors l'équation* (1) *a deux ou trois solutions en n.*

Critère $\mathcal{F}_3'$. *Le triplet étant donné par $(abs, \delta q, \delta r)$, supposons qu'il existe un nombre premier p et des entiers positifs α et β tels que $p^\alpha \parallel s$, $p^\beta \parallel q$ et $p \mid ab$, posons $\alpha = +\infty$ si $s = 0$. Alors, l'équation* (1) *n'a pas de solutions de la forme $n = 3m+2$ et chacune des conditions $\mathcal{C}_0$ et $\mathcal{C}_1$ ci-dessous est nécessaire pour qu'elle possède deux solutions, soit de la forme*

$n = 3m$, soit de la forme $n = 3m + 1$.

	$2 \mid a$	$2 \mid b$	$p \mid a$	$p \mid b$
$\mathcal{C}_0$	$\alpha \geq 2\beta$	$\alpha \geq 2\beta - 1$	$\alpha \geq 2\beta + 1$	$\alpha \geq 2\beta$
$\mathcal{C}_1$	$\beta \geq 2\alpha - 1$	$\beta \geq 2\alpha$	$\beta \geq 2\alpha$	$\beta \geq 2\alpha + 1$

P r e u v e. Supposons que "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" et que $(aS, Q) \neq \delta$ où $\delta = a^2 b$. Alors, d'après Prop. 7(v), $(q, s) \neq 1$ et chaque diviseur premier p de (q, s) est un diviseur de ab avec $p \nmid r$. Il existe donc des entiers positifs α et β tels que $p^\alpha \parallel s$, $p^\beta \parallel q$, $p \mid ab$ et on pose $\alpha = +\infty$ lorsque $s = 0$. D'après Prop. 7(ii), (v), chaque solution de l'équation (1) correspond à un zéro de l'une des suites X_m ou Y_m. Suivant que $n = 3m$ ou $n = 3m + 1$, l'équation (1) est donc équivalente, via (36) et (37), à l'une des équations

$$\varepsilon^m = Y_m \rho + Z_m - abs Y_m \,, \tag{30}$$

$$\varepsilon^m = X_m \overline{\omega} + Z_m \,, \tag{31}$$

où $\overline{\omega} = \omega / a$ et $\varepsilon = \rho^3 / \delta$ est une unité semi-locale pour p. Nous considérons deux cas suivant que p divise a ou que p divise b.

P r e m i e r c a s : p divise q, s et a. Posons $s = p^\alpha s'$, $q = p^\beta q'$ et $a = pa'$, avec $p \nmid a'q'$ et $p \nmid s'$ lorsque $s \neq 0$. D'après (36) pour $m = 1$, $\varepsilon \in \mathbb{Z}_{(p)}[\rho]$ et nous avons

$$\varepsilon = p^{\alpha - 1}(s'/a')\rho^2 + p^\beta q' \rho + r \,;$$

$\varepsilon \in \mathbb{Z}_{(p)}[\overline{\omega}]$ d'après (37) pour $m = 1$, et nous posons

$$\varepsilon = p^{\alpha_1} A_1 \overline{\omega}^2 / (br) + p^{\beta_1} B_1 \overline{\omega} / r + C_1 \,.$$

Ces deux expressions vérifient les relations suivantes :

$$\begin{cases} p^{\alpha_1} A_1 = p^\beta q' + p^{2\alpha} b s'^2 \,, \\ p^{\beta_1} B_1 = p^{\alpha_1 + \beta + 1} a' q' A_1 + p^\alpha s' r \,. \end{cases} \tag{32}$$

Ainsi, p est un "diviseur" de ε dans $\mathbb{Z}_{(p)}[\overline{\omega}]$ et aussi dans $\mathbb{Z}_{(p)}[\rho]$ pour $\alpha \geq 2$.

Supposons que $\alpha \geq 2$ pour $p \neq 2$ et que $\min(\alpha - 1, \beta) \geq 2$ pour $p = 2$. Appliquons Thm. 2 à $\zeta = \varepsilon$ avec $\theta = \rho$, puis avec $\theta = \overline{\omega}$, en remarquant que pour $p = 3$, les traces de ρ et de $\overline{\omega}$ sont des multiples de 3. Pour que l'équation (30) ait deux solutions il faut que $\alpha \geq 2\beta + 1$ pour $p \neq 2$ et $\alpha \geq 2\beta$ pour $p = 2$. D'après (32), $\alpha_1 = \beta$ et $\beta_1 \geq 2\beta + 1$ pour $p \neq 2$, $\alpha_1 = \beta$ et $\beta_1 \geq 2\beta$ pour $p = 2$. L'équation (31) a alors une seule solution du fait que $\alpha_1 < \beta_1$, avec $2 \leq \alpha_1$ pour $p = 2$. De même, pour que l'équation (31) ait deux solutions il faut que $\alpha_1 \geq 2\beta_1$ pour $p \neq 2$ et $\alpha_1 \geq 2\beta_1 - 1$ pour $p = 2$. Ces conditions sont équivalentes, via (32), à $\beta \geq 2\alpha$ pour $p \neq 2$ et à $\beta \geq 2\alpha - 1$ pour $p = 2$. L'équation (30) a alors une seule solution car $\alpha < \beta$, avec $2 \leq \alpha$ pour $p = 2$.

Supposons maintenant que $p = 2$ et $\min(\alpha - 1, \beta) = 1$. Si $\alpha - 1 \geq \beta$ alors l'équation (30) a une ou deux solutions d'après Thm. 2 et l'équation (31) a une seule solution d'après le Lemme 2(ii), Y_m étant non nul pour m positif. Si $\beta > \alpha - 1$ alors, d'après le Lemme 2(i), X_m est non nul pour m positif, et l'équation (30) a une seule solution. Les relations (32) impliquent $\beta_1 = 2$ et pour $\beta \geq 3$, $\alpha_1 \geq 2\beta_1 - 1$. D'après Thm. 2, l'équation (31) a une ou deux solutions.

Supposons enfin que $\alpha = 1$. D'après le Lemme 2(i), X_m est non nul pour m positif, et l'équation (30) a une seule solution. D'après (32), nous avons $\beta_1 = 1$ et pour $p \neq 2$, $\alpha_1 \geq 2\beta_1$ lorsque $\beta \geq 2$. Thm. 2 appliqué à ε pour $p = 2$ ou pour $p \neq 2$ avec $\beta \geq 2$ montre que l'équation (31) a une ou deux solutions. Dans tous les cas envisagés, les équations (30) ou (31) ont deux ou trois solutions et il en est de même pour l'équation (1).

S e c o n d c a s : p divise q, s et b. La démarche est la même que dans le premier cas, en remplaçant le Lemme 2 par le Lemme 3. ∎

Proposition 7. *Sous l'hypothèse* 2, *le triplet* (S, Q, R) *étant de la forme* $(abs, \delta q, \delta r)$ *avec* $\delta = a^2 b$, *soient* $\overline{\omega}$ *et* ε *les deux entiers du corps* $\mathcal{K}$ *définis par* $\overline{\omega} = \omega/a$ *où* $\omega = R/\rho$ *et* $\varepsilon = \rho^3/\delta$.

(i) *Le triplet* $(\mathcal{S}_3, \mathcal{Q}_3, \mathcal{R}_3)$ *représentant le polynôme minimal* h_3 *de* ε *est égal à* $(ab^2s^3+3(abqs+r), a^2bq^3-3r(abqs+r), r^3)$ *et il vérifie l'hypothèse* 2. *Pour* $m \in \mathbb{N}$, *les suites-coordonnées de* ε^m *dans l'ordre* $\mathbb{Z}[\varepsilon]$ *vérifient la relation de récurrence ayant* h_3 *comme polynôme auxiliaire*; *elles sont définies par*

$$\varepsilon^m = \mathcal{U}_m \varepsilon^2 + \mathcal{V}_m \varepsilon + \mathcal{W}_m \,. \tag{33}$$

(ii) *Pour* $m \in \mathbb{N}$, *posons* $aU_{3m} = \delta^m X_m$, $U_{3m+1} = \delta^m Y_m$ *et* $U_{3m+2} = \delta^m Z_m$. *Les suites* X_m, Y_m, Z_m *s'expriment en termes de la suite* $\mathcal{U}_m$:

$$\begin{cases} \begin{pmatrix} X_m \\ Y_m \end{pmatrix} = \begin{pmatrix} aq^2 - rs & s \\ -qr & q + bs^2 \end{pmatrix} \begin{pmatrix} \mathcal{U}_m \\ \mathcal{U}_{m+1} \end{pmatrix}, \\ Z_m = r^2 \mathcal{U}_m - (2r + abqs)\mathcal{U}_{m+1} + \mathcal{U}_{m+2}\,; \end{cases} \tag{34}$$

chacune d'entre elles est donnée explicitement par la formule suivante :

$$\sum_{i+2j+3k=3m+\lambda-2} \frac{(i+j+k)!}{i!j!k!} s^i q^j r^k b^{i+j+k-m} a^{m-1-k+[\lambda/2]} \tag{35}$$

respectivement pour $\lambda = 0$, $\lambda = 1$, $\lambda = 2$, *et* $[\lambda/2]$ *désigne la partie entière de* $\lambda/2$. *Chaque solution de l'équation* (1) *correspond alors à un zéro de l'une des suites* X_m, Y_m *ou* Z_m; *la suite* Z_m *n'a pas de zéros lorsque* $\delta \nmid r$.

(iii) *Pour* $m \in \mathbb{N}$, *les coordonnées de* ε^m *dans la base* $\{\rho^2, \rho, 1\}$ *du corps*

$\mathcal{K}$ ainsi que dans la base $\{\overline{\omega}^2,\overline{\omega},1\}$ sont données par les formules suivantes :

$$\text{(36)}\qquad \begin{cases}\varepsilon^m = X_m(\rho^2/a)+(Y_m-bsX_m)\rho+(Z_m-absY_m-abqX_m)\,,\\ \text{(37)}\qquad \varepsilon^m = Y_m(\overline{\omega}^2/br)+(rX_m+aqY_m)(\overline{\omega}/r)+Z_m\,;\end{cases}$$

en particulier pour $m=1$: $\varepsilon=(bs^2+q)(\overline{\omega}^2/br)+(rs+aq(bs^2+q))(\overline{\omega}/r)+(ab^2s^3+2abqs+r)$; $\varepsilon=(s/a)\rho^2+q\rho+r$.

(iv) *Soit $\mathcal{F}_3'$ l'indice de ε dans l'ordre $\mathbb{Z}[\overline{\omega},\rho,1]$. Alors*

$$\mathcal{F}_3=a^5b^3\mathcal{F}_3' \quad et \quad \mathcal{F}_3'=aq^3+abq^2s^2-brs^3\,.$$

(v) *Si $(aS,Q)\neq\delta$ alors $(q,s)\neq 1$, la suite Z_m n'a pas de zéros et ε est une unité semi-locale pour chaque diviseur premier de (q,s). Si "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" alors "(q,s) a la propriété $\mathcal{P}(ab/c)$" où $c=(b,r)$.*

P r e u v e. (i) Soit f_3 le polynôme minimal de ρ^3 et h_3 celui de ε. Par définition, $f_3(X)=\det(X1_{\mathcal{K}}-\rho^3)$ et $\delta^3h_3(X/\delta)=f_3(X)$. Un calcul simple montre que le triplet représentant f_3 est $(S^3+3(QS+R),Q^3-3R(QS+R),R^3)$, le triplet "réduit" $(\mathcal{S}_3,\mathcal{Q}_3,\mathcal{R}_3)$ s'en déduit. Il vérifie l'hypothèse 1 d'après Prop. 1(i); on obtient que $(\mathcal{Q}_3,\mathcal{R}_3)=c$ où $c=(b,r)$, $c\,|\,\mathcal{S}_3$ et $c\neq\mathcal{R}_3$ (Prop. 3(i)), le triplet vérifie donc l'hypothèse 2. La formule (33) résulte de Prop. 1(ii).

(ii) D'après (11), pour $m\in\mathbb{N}$ et $\lambda\in\{0,1,2\}$, $U_{3m+\lambda}=U_{6+\lambda}\mathbb{U}_m+U_{3+\lambda}\mathbb{V}_m+U_\lambda\mathbb{W}_m$ où $\mathbb{U}_m$, $\mathbb{V}_m$, $\mathbb{W}_m$ sont les coordonnées de ρ^{3m} dans l'ordre $\mathbb{Z}[\rho^3]$. D'après (12), $\mathbb{U}_m=\delta^{m-2}\mathcal{U}_m$, $\mathbb{V}_m=\delta^{m-1}\mathcal{V}_m$ et $\mathbb{W}_m=\delta^m\mathcal{W}_m$ où $\mathcal{U}_m$, $\mathcal{V}_m$ et $\mathcal{W}_m$ sont les suites définies par (33), avec $\mathcal{V}_m=\mathcal{U}_{m+1}-\mathcal{S}_3\mathcal{U}_m$, $\mathcal{W}_m=\mathcal{U}_{m+2}-\mathcal{S}_3\mathcal{U}_{m+1}-\mathcal{Q}_3\mathcal{U}_m$. Après division par δ^m ou par δ^m/a lorsque $\lambda=0$, on obtient les formules (34). La formule (35) provient de (13) après simplification. D'après Cor. 2, chaque solution de l'équation (1) est un zéro de la suite U_n, qui correspond à un zéro de l'une des suites X_m, Y_m ou Z_m suivant que $n=3m$, $n=3m+1$ ou $n=3m+2$, et $Z_m\neq 0$ si $\delta\nmid r$ d'après Prop. 2(ii).

(iii) La formule (36) se déduit de la formule (3) pour $n=3m$ après division par δ^m compte-tenu de $V_{3m}=U_{3m+1}-SU_{3m}$ et de $W_{3m}=U_{3m+2}-SU_{3m+1}-QU_{3m}$; la formule (37) s'obtient de la même façon à partir de (6) pour $n=3m$ avec $\omega=a\overline{\omega}$.

(iv) Dans la formule (36), remplaçons ρ^2 par l'expression $a(\overline{\omega}+bs\rho+abq)$ déduite de (15), ce qui donne $\varepsilon^m=X_m\overline{\omega}+Y_m\rho+Z_m-absY_m$, et d'après (33), $\varepsilon^m=\mathcal{U}_m\varepsilon^2+\mathcal{V}_m\varepsilon+\mathcal{W}_m$. Nous déduisons de (34) les formules de changement de coordonnées entre ces deux bases de $\mathcal{K}$:

$$\begin{pmatrix}X_m\\Y_m\end{pmatrix}=\begin{pmatrix}aq^2-rs+s\mathcal{S} & s\\ -qr+(bs^2+q)\mathcal{S} & bs^2+q\end{pmatrix}\begin{pmatrix}\mathcal{U}_m\\\mathcal{V}_m\end{pmatrix}.$$

L'indice de l'ordre $\mathbb{Z}[\varepsilon]$ dans l'ordre $\mathbb{Z}[\overline{\omega},\rho,1]$ est alors égal au déterminant de cette matrice, c'est-à-dire à $\mathcal{F}_3'$, et par définition de $\mathcal{F}_3$, $\mathcal{F}_3=a^5b^3\mathcal{F}_3'$.

(v) Si $(aS,Q)\neq\delta$ alors $(q,s)\neq 1$ du fait que $(aS,Q)=\delta(q,s)$. D'après Prop. 2(ii), la suite U_{3m+2} n'a pas de zéros, ainsi que la suite Z_m d'après (ii). Suivant Déf. 6, ε est une unité semi-locale pour chaque nombre premier qui ne divise pas $\mathcal{R}_3=r^3$, ce qui est le cas de chacun des diviseurs premiers de (q,s), par l'hypothèse $(q,r)=1$; de plus, chacun d'entre eux est un diviseur de $\mathcal{F}_3$, d'après (iv). Si "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" alors chaque diviseur premier de $\mathcal{F}_3$ est un diviseur de $R=a^2br$, et il en est de même pour chaque diviseur premier p de (q,s); mais d'après ce qui précède, $p\,|\,ab$ et $p\nmid r$, donc "(q,s) a la propriété $\mathcal{P}(ab/c)$" où $c=(b,r)$. ∎

p étant un nombre premier fixé, X un entier rationnel non nul et ν un entier positif ou nul tel que $p^\nu\,\|\,X$ alors $|X|=p^{-\nu}$ et $\nu=v_p(X)$; pour $X=0$, $|0|=0$ et par convention, $v_p(0)=+\infty$. [ ] désignant la partie entière, rappelons que la définition $v_p(X!)=[X/p]+[X/p^2]+[X/p^3]+\dots$ implique $v_p(X!)<X/(p-1)$. La valuation v_p vérifie l'inégalité ultramétrique : $v_p(X+Y)\geq\min(v_p(X),v_p(Y))$ et il y a égalité lorsque $v_p(X)\neq v_p(Y)$.

Lemme 2. *Soient p un diviseur premier de a vérifiant les hypothèses du critère $\mathcal{F}_3'$, X_m et Y_m les suites définies par* (35).

(i) *Si $\alpha=1$ ou si $p=2$, $\alpha=2$ et $\beta\geq 2$ alors $X_m\neq 0$ pour m positif.*
(ii) *Pour $p=2$, si $\alpha\geq 2$ et $\beta=1$ alors $Y_m\neq 0$ pour m positif.*

P r e u v e. Pour m positif, nous déduisons de la formule (35) les expressions respectives de $Y_m-r^{m-1}(\binom{m+1}{2}bs^2+mq)$ pour $\lambda=1$ ou de X_m-msr^{m-1} pour $\lambda=0$,

$$\sum_{\substack{0\leq k\leq m-2\\ i+2j=3(m-1-k)+1+\lambda}}\frac{(i+j+k)!}{i!j!k!}s^iq^jb^{i+j+k-m}r^ka^{m-1-k}\,.$$

(i) Supposons qu'il existe un entier m positif tel que $X_m=0$. L'inégalité ultramétrique appliquée à $v_p(msr^{m-1})=v_p(X_m-msr^{m-1})$ implique

$$\alpha+v_p(m)\geq\min v_p(E)\,, \tag{38}$$

où $v_p(msr^{m-1})=\alpha+v_p(m)$ et $E=p^{\alpha i+\beta j+l}\binom{i+j+m-1-l}{i+j}\binom{i+j}{j}$, le minimum étant pris sur tous les entiers non négatifs i,j,l tels que $i+2j=3l+1$ et $1\leq l\leq m-1$, en remplaçant k par $m-1-l$. Par une minoration convenable de $v_p(E)$ nous allons montrer que l'inégalité (38) est en contradiction avec les hypothèses, $\alpha=1$ ou lorsque $p=2$, $\alpha=2$ et $\beta\geq 2$. Commençons par vérifier que p divise m. Nous avons $v_p(E)\geq\alpha i+\beta j+l\geq\alpha(i+j)+l$, car $\beta\geq\alpha$. Il est utile pour la suite de calculer le minimum de $i+j$ lorsque $i+2j=3l+1$ avec $l\geq 1$: $\min(i+j)=(3l+2)/2$ pour $j=3l/2$ lorsque $2\,|\,l$, $\min(i+j)=(3l+1)/2$ pour $j=(3l+1)/2$ lorsque $2\nmid l$. Nous en déduisons que $v_p(E)\geq 2\alpha+1$ et d'après (38), $v_p(m)\geq\alpha+1$. La décomposition des

coefficients binomiaux figurant dans E sous la forme

$$m\binom{m+2l-j}{m}\binom{m-1}{l}(l!(2l-j)!)/(j!(3l+1-2j)!)$$

et $v_p(X!) < X/(p-1)$ impliquent que $v_p(E) > (\alpha i + \beta j + l + v_p(m)) - (3l+1-j)/(p-1)$. Pour $p \neq 2$ et $\alpha = 1$, nous obtenons que $v_p(E) - v_p(m)$ est supérieur à $(7l+4)/2$ si l est pair, à $(7l+1)/2$ sinon, ainsi $v_p(E) > 2 + v_p(m)$ en contradiction avec (38) pour $\alpha = 1$. Pour $p = 2$, $\beta \geq \alpha$ avec $\alpha = 2$ ou $\alpha = 1$, nous obtenons que $v_2(E) - v_2(m)$ est supérieur à $l(3\alpha-1)/2 + (\alpha-1)/2$ si l est impair, à $l(3\alpha-1)/2 + (\alpha-1)$ sinon, ainsi $v_2(E) > (2\alpha-1) + v_2(m)$, ce qui contredit (38) pour $\alpha = 1$ ou $\alpha = 2$.

(ii) Supposons que $Y_m = 0$ pour un certain entier m positif. Appliquons l'inégalité ultramétrique au second membre de l'égalité

$$v_2\left(\left(mq + \binom{m+1}{2}bs^2\right)r^{m-1}\right) = v_2\left(Y_m - \left(mq + \binom{m+1}{2}bs^2\right)r^{m-1}\right),$$

ce qui donne la condition

$$1 + v_2(m) \geq \min v_2(E)\,, \tag{39}$$

pour E défini ci-dessus, en prenant le minimum sur tous les entiers non négatifs i, j, l tels que $i + 2j = 3l + 2$ avec $1 \leq l \leq m-1$. Comme dans le cas (i), nous montrons que l'inégalité (39) n'est pas vérifiée lorsque $\alpha \geq 2$ et $\beta = 1$. Sous ces hypothèses, $v_2(E) \geq \alpha i + \beta j + l \geq 2i + j + l$. Calculons le minimum de $2i+j$ lorsque $i+2j = 3l+2$ avec $l \geq 1$, $\min(2i+j) = (3l+2)/2$ pour $j = (3l+2)/2$ si $2 \,|\, l$, $\min(2i+j) = (3l+5)/2$ pour $j = (3l+1)/2$ si $2 \nmid l$. Ainsi $v_2(E) \geq 5$ et d'après (39), $v_2(m) \geq 4$. La décomposition des coefficients binomiaux figurant dans E sous la forme

$$m\binom{m+2l+1-j}{m}\binom{m-1}{l}(l!(2l+1-j)!)/(j!(3l+2-2j)!)$$

et $v_2(X!) < X$ impliquent $v_2(E) > (\alpha i + \beta j + l + v_2(m)) - (3l+2-j)$. Nous en déduisons que $v_2(E) > 2 + v_2(m)$, en contradiction avec (39). ∎

Lemme 3. *Soient p un diviseur premier de b vérifiant les hypothèses du critère $\mathcal{F}_3'$, X_m et Y_m les suites définies par* (35).

(i) *Pour $p = 2$, si $\alpha = 1$ et $\beta \geq 2$ alors $X_m \neq 0$ pour m positif.*

(ii) *Si $\beta = 1$ ou si $p = 2$, $\beta = 2$ et $\alpha \geq 2$ alors $Y_m \neq 0$ pour m positif.*

Le Lemme 3 se démontre de la même façon que le Lemme 2.

§ 5. Diviseurs de $\mathcal{F}_3$ et de R/δ

Lorsque "$\mathcal{F}_2$ a la propriété $\mathcal{P}(R)$", le critère $\mathcal{F}_2$ ne s'applique pas, et nous avons montré que la condition $\mathcal{F}_2'' = \pm 1$ est nécessaire pour que l'équation (1) ait une solution non triviale (Cor. 3). Nous mettons en évidence une condition analogue lorsque "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" (Cor. 5).

Lemme 4. *Pour $n \geq 1$, soient A_n et B_n les deux suites définies par*

$$A_n = \sum_{i+2j=n} \binom{i+j}{j} (-1)^j\,, \qquad B_n = \sum_{i+2j=n} j\binom{i+j}{j} (-1)^{j-1}\,.$$

Si n prend les valeurs $3m-2$, $3m-1$ ou $3m$ alors $(-1)^m A_n$ est égal respectivement à -1, 0 ou 1 et $(-1)^{m+1} B_n$ est égal respectivement à $1-m$, m ou $2m$.

P r e u v e. Nous utilisons la relation de récurrence définissant les coefficients binomiaux pour décomposer A_{n+2} sous la forme

$$A_{n+2} = \sum_{i+2j=n+2} \left(\binom{i-1+j}{j} (-1)^j - \binom{i+j-1}{j-1} (-1)^{j-1} \right)\,.$$

La suite A_n vérifie la relation de récurrence $A_{n+2} = A_{n+1} - A_n$ avec $A_1 = 1$ et $A_2 = 0$. La série génératrice de cette suite est une fraction rationnelle

$$\mathcal{A}(z) = \sum_{n\geq 1} A_n z^n = (z - z^2)/(1 - z + z^2)\,.$$

Nous en déduisons l'expression $A_n = (-j)^n (j^{n+1} - 1)/(j-1)$ pour $n \geq 1$, où j désigne une racine de l'équation $1 + z + z^2 = 0$. Nous décomposons de même B_{n+2} :

$$\begin{aligned} B_{n+2} = \sum_{i+2j=n+2} \Bigg(& j\binom{i-1+j}{j} (-1)^{j-1} \\ & -(j-1)\binom{i+j-1}{j-1} (-1)^{j-2} + \binom{i+j-1}{j-1} (-1)^{j-1} \Bigg)\,. \end{aligned}$$

La suite B_n vérifie la relation de récurrence $B_{n+2} = B_{n+1} - B_n + A_n$ avec $B_1 = 0$ et $B_2 = 1$. La série génératrice de cette suite est une fraction rationnelle

$$\mathcal{B}(z) = \sum_{n\geq 2} B_n z^n = z^2/(1 - z + z^2)^2\,,$$

et nous obtenons l'expression suivante de B_n, pour $n \geq 1$:

$$B_n = (1/3)(-j)^n (2(j^{n+1} - 1)/(j-1) - (n+1)(j^n + 1))\,.$$

Les valeurs de A_n et de B_n figurant dans l'énoncé se déduisent de leurs expressions respectives. ∎

PROPOSITION 8. *Soient (S,Q,R) un triplet vérifiant l'hypothèse* 2, $\delta = (Q,R)$ *avec* $\delta = a^2b$ *et* $\delta D = (S^2+Q,R)$. *Posons* $\mathcal{F}_3 = a^5b^3D\mathcal{F}_3''$ *où* $\mathcal{F}_3 = Q^2(S^2+Q) - RS^3$.

(i) *Le triplet étant de la forme $(abs, \delta q, \delta r)$ avec $(aq,r)=1$ et $r \geq 2$, $d=(bs,r)$ et $c=(b,r)$ dans les notations de Prop.* 3, *alors $D=(q+bs^2,r)$, $(D,abqsd)=1$ et on pose $r=Ddr'$. Soient $\sigma=(s,a)$ et $\tau=(q,b)$, on pose $a=\sigma a'$, $s=\sigma s'$, $b=\tau b'$, $q=\tau q'$ où $(a',\sigma s')=(b',\tau q')=1$; alors $(ab,\mathcal{F}_3'')=\sigma\tau$ lorsque $(q,s)=1$. Si "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" alors "$\mathcal{F}_3''$ a la propriété $\mathcal{P}(Dab/c)$" et si, de plus, $(D,\mathcal{F}_3'')=1$ et $(aS,Q)=\delta$ alors $\mathcal{F}_3'' = \pm\sigma\tau$.*

(ii) *Soit U_n la suite définie dans Prop.* 1. *Pour $n \neq 0$, la suite U_n n'a pas de zéros de la forme $n=3m$ ou $n=3m+2$ si $D \neq 1$, et pour $n \neq 1$, elle n'a pas de zéros de la forme $n=3m+1$ si $(D,\mathcal{F}_3'') \neq 1$.*

P r e u v e. (i) Par définition de D, $\delta D = (S^2+Q,R)$ avec $S^2+Q = \delta(bs^2+q)$ et $R=\delta r$, donc $D=(q+bs^2,r)$. Nous montrons que $(D,abqsd)=1$: $(aq,r)=1$ et $D \mid r$ impliquent $(aq,D)=1$, et d'autre part, $(D,d) = (q+bs^2,bs,r) = (D,bs)$ et $(q,r)=1$ impliquent $(dbs,D)=1$. D'après Prop. 7(iv), $\mathcal{F}_3 = a^5b^3\mathcal{F}_3'$ où $\mathcal{F}_3' = aq^2(q+bs^2) - brs^3$; après avoir posé $q+bs^2 = DY$ et $r=Ddr'$, nous obtenons que $\mathcal{F}_3' = D\mathcal{F}_3''$ et $\mathcal{F}_3'' = aq^2Y - bs^3dr'$ avec $(aq^2Y,dr')=1$, donc $(\mathcal{F}_3'',dr')=1$. Comme $(ab,D)=1$ alors $(ab,\mathcal{F}_3'') = (ab,\mathcal{F}_3')$; vu la forme de $\mathcal{F}_3'$ et compte-tenu des hypothèses, chaque diviseur premier de $(ab,\mathcal{F}_3')$ est un diviseur de $(s,a)=\sigma$ ou de $(q,b)=\tau$. Si $(q,s)=1$ alors $(\tau q',\sigma s')=1$, et $\mathcal{F}_3'$ a l'expression suivante : $\mathcal{F}_3' = D\mathcal{F}_3'' = \sigma\tau(a'\tau^2q'^3 + a'b'(\sigma\tau q's')^2 - b'\sigma^2s'^3r)$, avec $(D,\sigma\tau) = (D,ab)=1$ et $(\tau,r)=(q,r)=1$. Nous déduisons alors de $(\tau a'q',\sigma)=1$ que $\sigma \parallel \mathcal{F}_3''$ et de $(\sigma b's'r,\tau)=1$ que $\tau \parallel \mathcal{F}_3''$. Si "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" alors chaque diviseur premier de $\mathcal{F}_3$ est un diviseur de R; d'après ce qui précède, $(R,\mathcal{F}_3) = a^2bD(a^3b^2\mathcal{F}_3'',dr') = a^2bD(c^2,dr')$, donc chaque diviseur premier de $\mathcal{F}_3$ est un diviseur de Dab, "$\mathcal{F}_3$ a la propriété $\mathcal{P}(Dab)$", et il en est de même pour $\mathcal{F}_3''$ qui est un diviseur de $\mathcal{F}_3$, avec $(Dab,\mathcal{F}_3'') = (Dab/c,\mathcal{F}_3'')$. Si, de plus, $(D,\mathcal{F}_3'')=1$ alors chaque diviseur premier de $\mathcal{F}_3''$ est un diviseur de ab/c, "$\mathcal{F}_3''$ a la propriété $\mathcal{P}(ab/c)$", et sous l'hypothèse $(aS,Q)=\delta$, qui s'écrit simplement $(q,s)=1$, $(ab,\mathcal{F}_3'')=\sigma\tau$, dans ce cas $\mathcal{F}_3'' = \pm\sigma\tau$.

(ii) Soit p un diviseur premier de D, lorsque $D \neq 1$. D'après (i), le triplet (S,Q,R) est de la forme $(S,-S^2+p^tV,p^tW)$ où $p^t \parallel D$ avec $t \geq 1$ entier, $p \nmid S$ et $p \nmid (V,W)$. D'après la formule (13), U_n a l'expression suivante :

$$U_n = \sum_{k=0}^{[n/3]} (p^tW)^k \Bigg(\sum_{i+2j=n-3k-2} \frac{(i+j+k)!}{i!j!k!} S^i(-S^2+p^tV)^j \Bigg),$$

où $[n/2]$ est la partie entière de $n/2$. Par réduction modulo p^t nous obtenons

$$U_n \equiv \sum_{i+2j=n-2} \binom{i+j}{j} (-1)^j S^{i+2j} \equiv A_{n-2} S^{n-2}\,,$$

où A_n est la suite définie dans le Lemme 4. Nous déduisons des valeurs de A_n figurant dans ce lemme que $U_n \not\equiv 0 \pmod{p^t}$ et donc $U_n \neq 0$ lorsque $n = 3m$ ou $n = 3m+2$ avec $n \neq 0$, tandis que $U_n \equiv 0 \pmod{p^t}$ pour $n = 3m+1$, A_{3m+1} étant nul. Réduisons alors U_{3m+1} modulo p^{t+1} :

$$\begin{aligned} U_{3m+1} \equiv A_{3m-1} S^{3m-1} + V p^t S^{3m-3} &\sum_{i+2j=3m-1} j \binom{i+j}{j} (-1)^{j-1} \\ &+ W p^t S^{3m-4} \sum_{i+2j=3m-4} (j+1) \binom{i+j+1}{j+1} (-1)^j\,, \end{aligned}$$

où $A_{3m-1} = 0$, et utilisons la suite B_n définie dans le Lemme 4, ce qui donne

$$U_{3m+1} \equiv p^t (VSB_{3m-1} + WB_{3m-2}) S^{3m-4} \pmod{p^{t+1}}\,.$$

Par définition de $\mathcal{F}_3$, $\mathcal{F}_3 = p^t((VS - W)S^3 + p^t(2S^2 - p^t V)V^2)$, avec $\mathcal{F}_3 = a^5 b^3 D \mathcal{F}_3''$ et $(ab, D) = 1$ d'après (i). Supposons que $p \,|\, (D, \mathcal{F}_3'')$; alors $p^{t+1} \,|\, \mathcal{F}_3$ et $SV \equiv W \pmod{p}$. Nous déduisons alors des congruences ci-dessus et du Lemme 4 que

$$p^{-t} U_{3m+1} \equiv W S^{3m-4} (-1)^{m-1} \not\equiv 0 \pmod{p}\,;$$

par conséquent, la suite U_{3m+1} ne s'annule pas pour $m \geq 1$. ∎

Corollaire 5. *Sous les hypothèses et avec les notations de Prop.* 8, *l'équation* (1) *a deux solutions en n si "l'indice* $\mathcal{F}_3$ *a la propriété* $\mathcal{P}(R)$*" et si* $(aS, Q) = \delta$, *à moins que* $\mathcal{F}_3''$ *ne soit égal à* $\pm\sigma\tau$, *où* $\sigma = (s, a)$ *et* $\tau = (q, b)$, *et lorsque "l'indice* $\mathcal{F}_3$ *n'a pas la propriété* $\mathcal{P}(R)$*", elle possède deux ou trois solutions si* $D \neq 1$ *et deux solutions si* $(D, \mathcal{F}_3'') \neq 1$.

P r e u v e. D'après Cor. 2, l'équation (1) est équivalente à l'équation $U_n = 0$. D'après Prop. 8(ii), la condition $(D, \mathcal{F}_3'') = 1$ est nécessaire pour que la suite U_n ait un zéro non trivial, l'assertion résulte alors de Prop. 8(i) et de Thm. 5. ∎

§ 6. Solutions modulo trois : "$\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$" et $(aS, Q) = \delta$

Théorème 7. *Soient* (S, Q, R) *un triplet vérifiant l'hypothèse* 2, $\delta = (Q, R)$ *avec* $\delta = a^2 b$, $\mathcal{F}_2 = -(QS + R)$ *et* $\mathcal{F}_3 = Q^2(S^2 + Q) - RS^3$. *Si "l'indice* $\mathcal{F}_3$ *a la propriété* $\mathcal{P}(R)$*" et si* $(aS, Q) = \delta$ *alors le nombre de*

solutions en n de l'équation (1) *est égal à deux lorsque "l'indice $\mathcal{F}_2$ a la propriété $\mathcal{P}(R)$", et il est au plus égal à trois dans le cas contraire, à moins que le triplet ne soit de l'un des deux types suivants* :

$$(ab, -(ab)^2, (ab)^3 - \lambda a^2 b)\,, \tag{40}$$

où $\lambda \in \{\pm 1, \pm 2, \pm 3\}$, $(D, \lambda) = 1$ et $D \geq 2$, en posant $D = ab^2 - \lambda$, alors l'équation (1) *a au moins trois solutions en n : $0, 1, 4$ et au plus quatre solutions si $\lambda \neq \pm 1$;*

$$(0, -\delta, \delta d)\,, \tag{41}$$

où $d \geq 2$, dans ce cas, l'équation (1) *a au moins trois solutions en n : $0, 1, 3$.*

P r e u v e. Supposons que "l'indice $\mathcal{F}_3$ a la propriété $\mathcal{P}(R)$". Pour que l'équation (1) ait quatre solutions lorsque "$\mathcal{F}_2$ n'a pas la propriété $\mathcal{P}(R)$" et au moins trois solutions lorsque "$\mathcal{F}_2$ a la propriété $\mathcal{P}(R)$", il faut que le triplet (S, Q, R) vérifie le système suivant :

$$\begin{cases} QS + R = -\mathcal{F}_2\,, \\ Q^2(S^2 + Q) - RS^3 = \mathcal{F}_3\,, \end{cases} \tag{42}$$

où chacun des indices $\mathcal{F}_2$ et $\mathcal{F}_3$ est de la forme indiquée dans Cor. 3 et Cor. 5. Nous pouvons donc supposer, d'après Cor. 3 et avec les notations de Prop. 3, que $\mathcal{F}_2 = \delta d \lambda$ avec $\lambda \in \{\pm 1, \pm 2, \pm 3\}$, $(\lambda, R) = 1$ et $d = (S, R/\delta)$, et d'après Cor. 5, les notations étant celles de Prop. 8, que $\mathcal{F}_3 = \delta^2 D a b \sigma \tau f$ avec $f = \pm 1$ et $\delta D = (S^2 + Q, R)$.

Soit (S, Q, R) un triplet solution de (42). Si QS est nul alors S est nul, $Q = \pm\delta$ et d'après (13), Q est négatif. Le triplet est de la forme (41), avec $U_3 = S = 0$, donc $n = 3$ est solution de l'équation (1). Lorsque QS est non nul, multiplions $\mathcal{F}_3$ par Q^3, remplaçons $-QS$ par $\mathcal{F}_2 + R$ et posons $X = -Q^3$; nous obtenons ainsi une équation quadratique en X

$$X^2 - X((\mathcal{F}_2 + R)^2 - \mathcal{F}_3) + R(\mathcal{F}_2 + R)^3 = 0\,. \tag{43}$$

Cette équation a des solutions réelles uniquement si son discriminant est positif ou nul, ce qui donne la condition

$$((\mathcal{F}_2 + R)^2 - \mathcal{F}_3)^2 \geq 4R(\mathcal{F}_2 + R)^3\,, \tag{44}$$

que l'on peut écrire sous une forme équivalente

$$(\mathcal{F}_2 + R)(\mathcal{F}_2 - 3R) \geq \mathcal{F}_3(2(\mathcal{F}_2 + R)^2 - \mathcal{F}_3)\,. \tag{45}$$

La condition (44) est trivialement vérifiée lorsque $\mathcal{F}_2 + R$ est négatif. Dans le cas où $\mathcal{F}_2 + R$ est positif, si $(\mathcal{F}_2 + R)^2 \geq \mathcal{F}_3$ et $\mathcal{F}_3$ positif alors d'après (45), $\mathcal{F}_2 \geq 3R$, ce qui s'écrit après simplification et avec les notations de Prop. 8, $\lambda \geq 3Dr'$. Les hypothèses $\lambda \leq 3$ et $Dr' \geq 1$ impliquent $\lambda = 3$ et $Dr' = 1$, donc $\mathcal{F}_2 = 3R$ et $0 < \mathcal{F}_3 < 16R^2$, mais alors le discriminant de (43) est négatif puisqu'il est égal à $\mathcal{F}_3(\mathcal{F}_3 - 32R^2)$, et aucun triplet n'est

solution de (42). Nous avons donc $(\mathcal{F}_2+R)^2<\mathcal{F}_3$ ou $\mathcal{F}_3<0$, $\mathcal{F}_3$ étant non nul, et dans le cas spécial où $\mathcal{F}_2=3R$ et $\mathcal{F}_3<0$, la condition (44) est vérifiée. Par conséquent, nous étudions trois cas.

P r e m i e r c a s : $\mathcal{F}_2+R>0$ et $\mathcal{F}_2\neq 3R$. La condition (44) prend la forme

$$f\mathcal{F}_3\geq(\mathcal{F}_2+R)(f(\mathcal{F}_2+R)+2\sqrt{R(\mathcal{F}_2+R)})\,.$$

Avec les notations de Prop. 8, nous avons d'une part $\mathcal{F}_2+R=\delta d(Dr'+\lambda)$ et d'autre part $\mathcal{F}_2+R=-QS=\delta ab\sigma\tau(-q's')$. Après avoir divisé par $f\mathcal{F}_3$ et simplifié, nous obtenons

$$1\geq(-q's'r'd)(f(1+\lambda/Dr')+2\sqrt{1+\lambda/Dr'})$$

lorsque $Dr'+\lambda\geq 1$. Avec les notations du Lemme 5, la condition (44) implique

$$1\geq(-q's'r'd)M_\lambda^f(Dr') \tag{46}$$

lorsque $Dr'\geq\max(1,1-\lambda)$, avec $-q's'r'd\geq 1$, $f=\pm1$, $\lambda\in\{\pm1,\pm2,\pm3\}$ et $(\lambda,Ddr')=1$. Nous allons montrer que la condition (46) implique $f=-1$ et $-q's'r'd=1$.

Si $f=1$ alors, d'après le Lemme 5(i), $M_\lambda^1(Dr')>1$, en contradiction avec (46), donc $f=-1$. Posons M_λ pour M_λ^f lorsque $f=-1$. Dans le cas spécial où $\lambda=3$ et $Dr'=1$ remarquons que $M_3(1)=0$. Si $\lambda\in\{1,2\}$ et $Dr'=1$ alors $d\geq\lambda+1$, car $(\lambda,d)=1$ et $Ddr'\geq 2$ par hypothèse, (46) implique $1\geq(\lambda+1)M_\lambda(1)$, ce qui est impossible d'après le Lemme 5(iii), donc $Dr'>1$. Pour $\lambda\in\{1,3\}$ et $Dr'\geq 2$, d'après le Lemme 5(iv), $M_\lambda(Dr')\geq M_\lambda(2)$ avec $2M_\lambda(2)>1$; alors (46) implique $1\geq(-q's'r'd)M_\lambda(2)$ et on doit avoir $-q's'r'd=1$. Le résultat est identique dans le cas où $\lambda=2$, comme $2\nmid Dr'$, $dr'\geq 3$, $M_2(Dr')\geq M_2(3)$ avec $2M_2(3)>1$, et $1\geq(-q's'r'd)M_2(3)$ d'après (46), donc $-q's'r'd=1$. Lorsque $\lambda<0$, $Dr'\geq 1-\lambda$ et d'après le Lemme 5(v), $M_\lambda(Dr')>M_\lambda(1-\lambda)$ et $2M_\lambda(1-\lambda)>1$, (46) implique $1\geq(-q's'r'd)M_\lambda(1-\lambda)$, ce qui est impossible à moins que $-q's'r'd=1$.

Les conditions $f=-1$ et $-q's'r'd=1$ se traduisant par $(\mathcal{F}_2+R)=\delta(D+\lambda)$, $\mathcal{F}_3=-\delta D^2(D+\lambda)$ avec $D+\lambda=ab\sigma\tau$, le triplet (S,Q,R) est de la forme $(\pm ab\sigma,\mp\delta\tau,\delta D)$ où $\delta=a^2b$ et $D>1$. L'équation (43) s'écrit

$$X^2-X\delta^2(D+\lambda)(2D+\lambda)+\delta^4D(D+\lambda)^3=0\,,$$

elle possède deux solutions positives : $\delta^2D(D+\lambda)$ et $\delta^2(D+\lambda)^2$. X étant égal à $-Q^3$, Q est négatif et S positif. La première solution ne convient pas : en effet, pour $Q=-\delta\tau$ et $D+\lambda=ab\sigma\tau$, $-Q^3=\delta^2D(D+\lambda)$ est équivalent à $a\tau^2=\sigma D$ avec $(a\tau^2,\sigma D)=\sigma$ et $D>1$. La seconde solution $-Q^3=\delta^2(D+\lambda)^2$, via $D+\lambda=ab\sigma\tau$, donne après simplification $\tau=b\sigma^2$, $\sigma=1$, $\tau=b$ puis $s=1$ et $q=-b$. Les triplets (S,Q,R) solutions de (42)

sont bien du type (40); comme $U_4 = S^2 + Q = 0$, alors $n = 4$ est solution de l'équation (1).

Deuxième cas : $\mathcal{F}_2 = 3R$. Le système (42) est de la forme

$$\begin{cases} QS = -4R\,, \\ Q(S^2 + 2Q)^2 = 4\mathcal{F}_3\,. \end{cases}$$

Nous avons vu plus haut que $\mathcal{F}_3 < 0$, donc $Q < 0$ et $S > 0$. Les notations étant celles de Prop. 3 et de Prop. 8, posons $t = cd_1^2$ où $d = cd_1$. On obtient après simplification

$$\begin{cases} (-aq)(b_1 s_1) = 4\,, \\ (-aq)(b_1 s_1^2 t + 2q)^2 = 4\sigma\tau\,, \end{cases}$$

et par hypothèse $t \geq 2$ et $3 \nmid t$; rappelons que $\sigma = (s, a) = (s_1, a)$ et $\tau = (q, b) = (q, b_1)$. On distingue trois cas suivant que $-aq$ est égal à 1, 2 ou 4. Il n'y a pas de solutions en t avec $t \geq 2$ et $3 \nmid t$ dans le premier cas : $-aq = 1$ implique $\sigma\tau = 1$, $b_1 s_1 = 4$ et $2ts_1 = 1 \pm 1$, d'où $t = 0$ ou $t = 1$. Il en est de même dans le second cas : $-aq = 2$ implique $b_1 s_1 = 2$ et $2(ts_1 + q)^2 = \sigma\tau$, donc $\sigma\tau = 2$ et $-qs_1 \neq 1$, ce qui donne $t = 3$ ou $t = 1$ pour $s_1 = 1$ et $q = -2$, ainsi que $t = 1$ ou $t = 0$ pour $s_1 = 2$ et $q = -1$. Dans le troisième cas : $-aq = 4$ implique $b_1 s_1 = 1$, $\sigma\tau = 1$ et $t = -2q \pm 1$, on trouve d'une part $t = 5$ ou $t = 3$ pour $a = 2$ et $q = -2$, donc $c = d = 5$; et d'autre part $t = 7$ ou $t = 9$ pour $a = 1$ et $q = -4$, donc $c = d = 7$. Nous obtenons ainsi deux triplets solutions de (42), $(10, -4 \cdot 10, 10^2)$ et $(7, -4 \cdot 7, 7^2)$, pour lesquels l'équation (1) a respectivement deux et trois solutions d'après le Lemme 6.

Troisième cas : $\mathcal{F}_2 + R < 0$. Comme $QS \neq 0$ et $\mathcal{F}_2 + R = -QS$ alors $Q < 0$ et $S < 0$, d'après (13). La condition $-(\mathcal{F}_2 + R) \geq 1$ entraîne, après simplification, que $1 \leq Dr' \leq -1 - \lambda$; nous en déduisons que $Dr' = 1$ pour $\lambda \in \{-2, -3\}$ et $Dr' = 2$ pour $\lambda = -3$.

Dans le cas où $Dr' = 1$, alors $R = \delta d$ avec $d \geq 2$ et $\mathcal{F}_2 = \lambda R$ avec $(d, \lambda) = 1$; le système (42) est de la forme

$$\begin{cases} QS = -(\lambda + 1)R\,, \\ Q(2S^2 + (\lambda + 1)Q)^2 = (\lambda + 1)((\lambda - 3)Q^3 + 4\mathcal{F}_3)\,. \end{cases}$$

Avec les notations de Prop. 3 et de Prop. 8, en posant $t = cd_1^2$ où $d = cd_1$, après simplification on obtient

$$\begin{cases} (-aq)(-b_1 s_1) = -(\lambda + 1)\,, \\ (-aq)(2b_1 s_1^2 t + (\lambda + 1)q)^2 = -(\lambda + 1)((\lambda - 3)aq^3 + 4\sigma\tau f)\,, \end{cases}$$

où $t \geq 2$ et $(\lambda, t) = 1$ par hypothèse. Pour $\lambda = -2$, d'après la première équation $-aq = -b_1 s_1 = \sigma\tau = 1$ et d'après la seconde, $(2t + 1)^2 = 4(1 \pm 1)$, ce qui est impossible pour $t \geq 2$. Pour $\lambda = -3$, on distingue deux cas suivant que $-aq$ est égal à 2 ou 1. Il n'y a pas de solutions en t avec $t \geq 2$ dans le

premier cas : $-aq = 2$ implique $-b_1 s_1 = \sigma\tau = 1$ et $(t-q)^2 = 3q^2 + f$, ce qui donne $(t+2)^2 = 12 \pm 1$ pour $q = -2$ et $a = 1$, $t = 1$ ou $t = -3$ pour $q = -1$ et $a = 2$. Il en est de même dans le second cas : $-aq = 1$ implique $-b_1 s_1 = 2$, $\sigma\tau = 1$ et $(2ts_1 - 1)^2 = 3 \pm 2$, d'où $t = 0$ ou $t = -1$.

Enfin, dans le cas où $\lambda = -3$ et $Dr' = 2$, $\mathcal{F}_2 = -3\delta d$ et $R = 2\delta d$, le système (42) est

$$\begin{cases} 2QS = R\,, \\ Q(2S^2 + Q)(S^2 + Q) = -\mathcal{F}_3\,, \end{cases}$$

et après simplification, comme précédemment, on obtient

$$\begin{cases} (-aq)(-b_1 s_1) = 1\,, \\ (-aq)(2b_1 s_1^2 t + q)(b_1^2 s_1 t - q) = D\sigma\tau f\,, \end{cases}$$

en posant $t = cd_1^2$ pour $d = cd_1$, avec $t \geq 1$ et $6 \nmid t$ par hypothèse. On déduit de ce système que $-aq = -b_1 s_1 = \sigma\tau = 1$ et que t est donné par $(2t-1)(t+1) = \pm D$, avec $D = 1$ ou $D = 2$; $t = 1$ est la seule solution qui convienne. Nous obtenons dans ce cas un seul triplet solution de (42), $(-1, -1, 2)$, pour lequel l'équation (1) a deux solutions, d'après le Lemme 6.

∎

Lemme 5. *Pour $\lambda \in \{\pm 1, \pm 2, \pm 3\}$, $f = \pm 1$ et $x \geq \max(1, 1-\lambda)$, soit M_λ^f la fonction définie par $M_\lambda^f(x) = f(1+\lambda/x) + 2\sqrt{1+\lambda/x}$. M_λ désigne simplement M_λ^f lorsque $f = -1$.*

(i) *La fonction M_λ^1 est minorée par 1 au sens strict.*

(ii) *La fonction M_λ est croissante et majorée strictement par 1.*

(iii) *Pour $\lambda \in \{1, 2\}$, si $x \geq 1$ alors $M_\lambda(x) \geq M_\lambda(1)$ et $(\lambda+1)M_\lambda(1) > 1$. $M_3(1) = 0$ pour $\lambda = 3$.*

(iv) *Pour $\lambda \in \{1, 3\}$, si $x \geq 2$ alors $M_\lambda(x) \geq M_\lambda(2)$ et $2M_\lambda(2) > 1$; pour $\lambda = 2$, si $x \geq 3$ alors $M_2(x) \geq M_2(3)$ et $2M_2(3) > 1$.*

(v) *Pour $\lambda < 0$, si $x \geq 1-\lambda$ alors $M_\lambda(x) \geq M_\lambda(1-\lambda)$ et $2M_\lambda(1-\lambda) > 1$.*

Preuve. Soit $(M_\lambda^f)'(x) = (-\lambda/x^2)(f + 1/\sqrt{1+\lambda/x})$, la dérivée en x de la fonction M_λ^f; elle est positive lorsque $f = 1$ et $\lambda < 0$ ou lorsque $f = -1$.

(i) Il est clair que pour $\lambda > 0$ et $x \geq 1$, $M_\lambda^1(x) > 3$. Pour $\lambda < 0$ et $x \geq 1 - \lambda$, $M_\lambda^1(x) \geq M_\lambda^1(1-\lambda)$ avec $M_\lambda^1(1-\lambda) = (1 + 2\sqrt{1-\lambda})/(1-\lambda)$. Cette expression prend les valeurs respectives $(1+2\sqrt{2})/2$, $(1+2\sqrt{3})/3$, $5/4$ pour $\lambda \in \{-1, -2, -3\}$, donc $M_\lambda^1(1-\lambda) > 1$.

(ii) La fonction M_λ a pour limite 1 quand x croît indéfiniment.

(iii) La fonction M_λ est croissante. Une simple vérification montre que $M_3(1) = 0$ et que chacune des quantités suivantes est supérieure à 1 : $2M_1(1) = 4(\sqrt{2} - 1)$, $3M_2(1) = 3\sqrt{3}(2 - \sqrt{3})$, $2M_1(2) = 2\sqrt{6} - 3$, $2M_3(2) = 2\sqrt{10} - 5$ et $2M_2(3) = 2\sqrt{5/3}(2 - \sqrt{5/3})$.

(iv) Si $x \geq 1-\lambda > 1$ alors $M_\lambda(x) \geq M_\lambda(1-\lambda)$ et $2M_\lambda(1-\lambda) = 2(-1+2\sqrt{1-\lambda})/(1-\lambda)$. Cette expression prend les valeurs respectives $-1+2\sqrt{2}$, $2(-1+2\sqrt{3})/3$, $3/2$ lorsque $\lambda \in \{-1,-2,-3\}$, donc $M_\lambda(1-\lambda) > 1$. ∎

LEMME 6. *Pour n distinct de 0 et de 1, l'équation (1) n'a pas de solutions dans le cas du triplet $(10, -4\cdot 10, 10^2)$, et elle possède une solution non triviale dans les deux cas suivants : $n = 5$ pour le triplet $(7, -4\cdot 7, 7^2)$; $n = 4$ pour le triplet $(-1,-1,2)$.*

P r e u v e. On constate que chacun des trois triplets (S, Q, R) du lemme vérifie l'hypothèse 2. L'indice $\mathcal{F}_2$ du triplet $(10, -4\cdot 10, 10^2)$ est égal à $3\cdot 10^2$. Appliquons le critère $\mathcal{F}_2$ à $\rho^{2\mu} = 20(3\rho^2 - 15\rho + 50)$, pour $p = 3$ et $\mu = 2$, dans le cas spécial. Du fait que $U_4 = S^2 + Q = 60$ et $U_5 = S^3 + 2QS + R = 300$, aucune des deux conditions $\mathcal{C}_0$ et $\mathcal{C}_1$ n'est vérifiée et l'équation (1) a deux solutions en n, 0 et 1.

L'indice $\mathcal{F}_2$ du triplet $(7, -4\cdot 7, 7^2)$ est égal à $3\cdot 7^2$. Le critère $\mathcal{F}_2$ appliqué à $\rho^{2\mu} = 7(3\rho^2 - 21\rho + 49)$, pour $p = 3$ et $\mu = 2$ (cas spécial), montre que pour $n \neq 0$, l'équation (1) a deux ou trois solutions de la forme $n = 4m+1$, U_5 étant nul. D'après (11), pour $m \in \mathbb{N}$ et $U_5 = 0$, $U_{4m+1} = U_9\mathbb{U}_m + U_5\mathbb{V}_m = U_9\mathbb{U}_m$, où $\mathbb{U}_m$ est la fonction symétrique complète de ρ^4, ρ'^4, ρ''^4 (Prop. 1(v)). Le triplet représentant le polynôme minimal de ρ^2 est donné par $(S^2+2Q, 2RS-Q^2, R^2)$; après réduction, on obtient pour $\rho^2/7$ le triplet $(-1,-2,7)$ et pour $\rho^4/7^2$ le triplet $(-3,-18,7^2)$. Posons $\varphi = \rho^4/7^2$; d'après Prop. 1(i), φ vérifie l'hypothèse 1, ainsi que l'hypothèse 2. D'après (12), $\mathbb{U}_m = 7^{2(m-2)}\mathcal{U}_m$ où $\mathcal{U}_m$ est la fonction symétrique complète de φ, φ', φ''. Les zéros de la suite U_{4m+1} correspondent aux zéros de la suite $\mathcal{U}_m$ où m vérifie l'équation $\varphi^m = x\varphi + y$. L'indice $\mathcal{F}_2(\varphi)$ étant égal à -103, on montre que cette équation a deux solutions en m, 0 et 1, en appliquant le critère $\mathcal{F}_2$ à $\varphi^{2\mu}$ pour $p = 103$, avec $\mu = 102$ et $\varphi^{2\mu} \equiv 67\cdot 103\varphi^2 + 32\cdot 103\varphi + 99\cdot 103 + 1 \pmod{103^2}$; les conditions $\mathcal{C}_0$ et $\mathcal{C}_1$ ne sont pas vérifiées. L'équation (1) a trois solutions en n : 0, 1, 5.

Dans le cas du triplet $(-1,-1,2)$, on a : $\mathcal{F}_3 = -3$, $\delta D = (S^2+Q, R) = 2$ et $\delta = (Q, R) = 1$. D'après Thm. 3, l'équation (1) a trois ou quatre solutions en n, U_4 étant nul, et d'après Prop. 8, pour $n \neq 0$, les solutions sont de la forme $n = 3m+1$. D'après (11), pour $m \in \mathbb{N}$ et $U_4 = 0$, $U_{3m+1} = U_7\mathcal{U}_m + U_4\mathcal{V}_m = U_7\mathcal{U}_m$, où $\mathcal{U}_m$ est la fonction symétrique complète de ρ^3, ρ'^3, ρ''^3. Le polynôme minimal de ρ^3 est représenté par le triplet $(\mathcal{S}_3, \mathcal{Q}_3, \mathcal{R}_3) = (8, -19, 8)$; d'après Prop. 7(i) pour $\varepsilon = \rho^3$ lorsque $\delta = 1$, ce triplet vérifie l'hypothèse 2 et $\delta_\varepsilon = (\mathcal{Q}_3, \mathcal{R}_3) = 1$. Comme $\mathcal{F}_2(\varepsilon) = -16\cdot 9$ et $d_\varepsilon = (\mathcal{S}_3, \mathcal{R}_3) = 8$, d'après Prop. 3, pour m distinct de 0 et 1, la suite $\mathcal{U}_m$ n'a pas de zéros. L'équation (1) a dans ce cas trois solutions en n : 0, 1, 4. ∎

§ 7. Cas particulier : $U_4 = 0$

THÉORÈME 8. *Soit* (S, Q, R) *un triplet vérifiant l'hypothèse* 2. *Supposons que* $U_4 = S^2 + Q = 0$. *Alors, l'équation* (1) *a exactement trois solutions en* n : 0, 1, 4, *sauf dans deux cas où il y a une solution supplémentaire* :

$$\begin{cases} n = 10 \text{ pour le triplet } (3, -9, 18)\,, \\ n = 16 \text{ pour le triplet } (5, -25, 50)\,. \end{cases}$$

P r e u v e. D'après Prop. 9, via le Lemme 7, le nombre de solutions en n de l'équation (1) est égal à trois, sauf pour un nombre fini de triplets (S, Q, R) du type (40). Pour $n \neq 0$, les solutions étant de la forme $n = 3m + 1$ où m vérifie l'équation (48), elles correspondent aux puissances ε^m binomiales en ε, où ε est défini dans Prop. 7(i), et il y a un nombre fini de triplets $(\mathcal{S}_3, \mathcal{Q}_3, \mathcal{R}_3)$ représentant le polynôme minimal de ε. Dans Prop. 10, le nombre de ces triplets est réduit à dix-huit (voir Table 1) par l'application du critère $\mathcal{F}_2$ à ε^4 ou du critère $\mathcal{F}_3$ à ε^3 pour $p = 3$; pour chacun de ces triplets, le nombre de solutions en m de l'équation (48) est au plus égal à trois et il existe trois solutions dans les deux cas suivants :

$$\begin{cases} \text{cas } 7 : & \varepsilon^3 = -3\varepsilon + 8, \\ \text{cas } 18 : & \varepsilon^5 = -95\varepsilon + 72. \end{cases}$$

Il reste à montrer que l'équation (48) a seulement deux solutions dans les autres cas. Soit p un diviseur premier de $\mathcal{F}_2(\varepsilon) = -(\mathcal{Q}_3\mathcal{S}_3 + \mathcal{R}_3)$. Si $p \,|\, \mathcal{R}_3$ alors $p \,|\, d_\varepsilon$ où $d_\varepsilon = (\mathcal{S}_3, \mathcal{R}_3)$; d'après Prop. 3(ii), pour m distinct de 0 et 1, l'équation (48) n'a pas de solutions dans le cas 3 où $d_\varepsilon = 8$ et $\mathcal{F}_2(\varepsilon) = -8 \cdot 16$, et il peut exister des solutions impaires dans les cas 1, 6, 8, 16 où $d_\varepsilon \neq 1$. Le cas 3 étant réglé, dans les quinze cas restants, nous choisissons p tel que $p \geq 5$ et $p \nmid \mathcal{R}_3$, puis nous appliquons le critère $\mathcal{F}_2$ à $\varepsilon^{2\mu}$ (voir Table 2), où μ est le plus petit entier positif tel que $\varepsilon^{2\mu} \equiv pA\varepsilon^2 + pB\varepsilon + C \pmod{p^2}$, avec $p \nmid AC$ et $p \nmid B$ (sauf dans les cas 2 et 15 où $p \,|\, B$); il est clair que la condition $\mathcal{C}_0$ n'est pas vérifiée, et du fait que $\mathcal{S}_3 A + B \not\equiv 0 \pmod{p}$, la condition $\mathcal{C}_1$ n'est pas non plus vérifiée. L'équation (48) a donc deux solutions en h et l'équation (1) trois solutions en n, dans tous les cas de la Table 2. ∎

La Table 1 donne la liste des dix-huit triplets $(\mathcal{S}_3, \mathcal{Q}_3, \mathcal{R}_3)$ définis en fonction de a et de λ (Prop. 10) et pour chaque triplet, $-\mathcal{F}_2(\varepsilon) = \mathcal{Q}_3\mathcal{S}_3 + \mathcal{R}_3$ et $d_\varepsilon = (\mathcal{S}_3, \mathcal{R}_3)$.

La Table 2 donne, dans chaque cas, un diviseur premier p de $\mathcal{F}_2(\varepsilon)$ tel que $p \geq 5$ et $p \nmid \mathcal{R}_3$, un élément primitif e de $(\mathbb{Z}/p\mathbb{Z})^*$, le plus petit entier positif μ tel que $(\mathcal{S}_3^2/\mathcal{Q}_3)^\mu \equiv 1 \pmod{p}$ (sauf dans les cas 2 et 15 où $\mu = p$), et les coordonnées $\mathcal{U}_{2\mu}$, $\mathcal{V}_{2\mu}$, $\mathcal{W}_{2\mu}$ de $\varepsilon^{2\mu}$ dans l'ordre $\mathbb{Z}[\varepsilon]$, après réduction modulo p^2.

Table 1

cas	λ	a	$a-\lambda$	$\mathcal{S}_3$	$-\mathcal{Q}_3$	$\mathcal{R}_3$	$-\mathcal{F}_2(\varepsilon)$	d_ε
1	-1	1	2	4	7	8	4·5	4
2		2	3	5	13	27	2·19	1
3		5	6	8	43	216	8·16	8
4		6	7	9	57	343	10·17	1
5		10	11	13	133	1331	2·199	1
6		15	16	18	273	4096	2·409	2
7	1	3	2	0	3	8	-8	8
8		5	4	2	13	64	-2·19	2
9		10	9	7	73	729	-2·109	1
10		30	29	27	813	24389	-2·23·53	1
11	-2	1	3	7	19	27	2·53	1
12		3	5	9	39	125	2·113	1
13		5	7	11	67	343	2·197	1
14	2	5	3	-1	7	27	-2·17	1
15		15	13	9	147	2197	-2·19·23	1
16	-3	1	4	10	37	64	2·9·17	2
17		10	13	19	217	2197	2·9·107	1
18	3	5	2	-4	7	8	-4·9	4

Table 2

cas	p	e	μ	$\mathcal{U}_{2\mu}$	$\mathcal{V}_{2\mu}$	$\mathcal{W}_{2\mu}$
1	5	2	4	5·3	5·4	5·2 + 1
2	19	2	19	19·1	0	19·6 + 6
4	5	2	4	5·2	5·3	5·4 + 4
5	199	3	33	199·101	199·144	199·185 + 106
6	409	21	68	409·222	409·381	409·194 + 53
8	19	2	3	19·15	19·13	19·10 +7
9	109	6	18	109·48	109·79	109·91 + 63
10	23	5	22	23·2	23·4	23·1 + 1
11	53	2	52	53·27	53·16	53·51 + 1
12	113	3	112	113·104	113·89	113·75 + 1
13	197	2	196	197·13	197·164	197·91 + 1
14	17	3	16	17·10	17·3	17·2 + 1
15	19	2	19	19·1	0	19·17 + 5
16	17	3	16	17·7	17·6	17·11 + 1
17	107	2	106	107·48	107·30	107·98 + 1

LEMME 7. *Soient* (S, Q, R) *un triplet du type* (40), Y_m *la suite définie dans Prop.* 7(ii) *et* p *un diviseur premier de* ab. *Si* p *divise* a *avec* $p \geq 7$ *ou si* p *divise* b *avec* $p \geq 5$ *alors, pour* $m \geq 2$, *la suite* Y_m *n'a pas de zéros.*

P r e u v e. Dans la formule (35) pour $\lambda = 1$, posons $s = 1$, $q = b$ et $r = D$; A_{3m-1} étant nul d'après le Lemme 4, nous obtenons

$$Y_m = bD \sum_{l=0}^{m-2} (ab^2)^l D^{m-2-l} \Bigg(\sum_{i+2j=3l+2} \frac{(i+j+k)!}{i!j!k!} (-1)^j \Bigg),$$

ainsi que la congruence $Y_m/(bD) \equiv \binom{m}{2} D^{m-2} \pmod{ab^2}$. Nous en déduisons que, pour p impair, p divise $m(m-1)$, via l'hypothèse $(ab, D) = 1$. Supposons que Y_m s'annule pour un certain m, avec $m \geq 2$; alors

$$v_p\left(\binom{m}{2}\right) = v_p\left(\frac{Y_m}{bD} - \binom{m}{2} D^{m-2}\right).$$

Appliquons l'inégalité ultramétrique au second membre de cette égalité :

$$v_p\left(\binom{m}{2}\right) \geq \min v_p(E) \tag{47}$$

en posant

$$E = (ab^2)^l \binom{i+j+m-1-l}{i+j} \binom{i+j}{j},$$

et le minimum est pris sur tous les entiers non négatifs i, j, l tels que $i + 2j = 3l + 2$ et $1 \leq l \leq m-2$. Suivant que p divise m ou bien $m-1$, décomposons les combinaisons figurant dans E

$$m \binom{m+2l+1-j}{m} \binom{m-1}{l} \frac{l!(2l+1-j)!}{(3l+2-2j)!j!},$$

$$(m-1) \binom{m+2l+1-j}{m-1} \binom{m-2}{l-1} \frac{(l-1)!(2l+2-j)!}{(3l+2-2j)!j!}.$$

Nous déduisons de ces expressions et de la relation $v_p(X!) < X/(p-1)$ que la valuation de E vérifie la relation suivante, pour p impair et pour $l \geq 1$:

$$v_p(E) > v_p\left(\binom{m}{2}\right) + l v_p(ab^2) - \frac{3l+2}{p-1}.$$

La différence $v_p(E) - v_p(\binom{m}{2})$ est alors minorée par $3/4$ si p divise b avec $p \geq 5$, ou par $1/6$ si p divise a avec $p \geq 7$, ce qui contredit (47). ∎

Proposition 9. *Sous les hypothèses de Thm.* 8, *le nombre de solutions en n de l'équation* (1) *est égal à trois, à moins que le triplet (S, Q, R) ne soit du type* (40), *avec $a \in \{1, 2, 3, 5, 6, 10, 15, 30\}$ et $b \in \{1, 2, 3, 6\}$. Dans ce cas, pour $n \neq 0$, les solutions sont de la forme $n = 3m + 1$ et m vérifie l'équation*

$$\varepsilon^m = x\varepsilon + y \tag{48}$$

où $\varepsilon = \rho^3/(a^2 b)$. Le triplet $(\mathcal{S}_3, \mathcal{Q}_3, \mathcal{R}_3)$ représentant le polynôme minimal de ε vérifie l'hypothèse 2 *et il est défini par $(D - 2\lambda, -(D^2 - \lambda D + \lambda^2), D^3)$*

où $D = ab^2 - \lambda$ *et* $\delta_\varepsilon = (\mathcal{Q}_3, \mathcal{R}_3) = 1$. *L'équation* (48) *n'a pas de solutions avec* m *négatif.*

P r e u v e. Soit (S, Q, R) un triplet vérifiant l'hypothèse 2, avec $\delta = (Q, R) = a^2 b$. L'hypothèse $U_4 = S^2 + Q = 0$ entraîne que $\mathcal{F}_3 = -RS^3$ et $(aS, Q) = aS$. L'équation (1) a exactement trois solutions lorsque $aS \neq \pm\delta$, d'après Thm. 5 et Thm. 6, et d'après Thm. 7, elle possède au moins trois solutions lorsque $aS = \pm\delta$, à condition que le triplet soit du type (40), $(ab, -\delta b, \delta D)$ où $D = ab^2 - \lambda$, ce que nous supposons dans la suite. Chaque solution en n de l'équation (1) est un zéro de la suite U_n (Cor. 2). Comme $D \geq 2$, pour $n \neq 0$, les zéros de la suite U_n sont de la forme $n = 3m + 1$ (Prop. 8(ii)). Chaque zéro de la suite U_{3m+1} correspond à un zéro de la suite Y_m (Prop. 7(ii)) et pour $m \geq 2$, la suite Y_m n'a pas de zéros, à moins que a et b ne vérifient les conditions de l'énoncé (Lemme 7). D'après (34), $Y_m = -bD\mathcal{U}_m$ et d'après (33), chaque zéro de la suite $\mathcal{U}_m$ est une solution de l'équation (48). Il résulte de Prop. 7(i) que le triplet $(\mathcal{S}_3, \mathcal{Q}_3, \mathcal{R}_3)$ représentant le polynôme minimal de ε vérifie l'hypothèse 2 et qu'il est de la forme indiquée lorsque (S, Q, R) est du type (40), $\delta_\varepsilon = (\mathcal{Q}_3, \mathcal{R}_3) = 1$ du fait que $(ab, \lambda) = 1$. L'équation (48) est alors équivalente à l'équation $\mathcal{U}_m = 0$ (Cor. 2). ∎

Proposition 10. *Pour que l'équation* (48) *ait une solution non triviale en* m, *il faut que le triplet* $(\mathcal{S}_3, \mathcal{Q}_3, \mathcal{R}_3)$, *défini dans Prop.* 9, *soit de la forme*

$$(a - 3\lambda, -(a^2 - 3a\lambda + 3\lambda^2), (a - \lambda)^3)\,,$$

où $a \in \{1, 2, 3, 5, 6, 10, 15, 30\}$, $\lambda \in \{\pm 1, \pm 2, \pm 3\}$, $(a, \lambda) = 1$ *et* $a \geq \lambda + 2$. *Il faut de plus que* $3^2 \,|\, (a - 3\lambda)$ *si* $3 \,|\, a$ *et que* $3^2 \,|\, (a\lambda - 15)$ *si* $\lambda = \pm 3$. *La liste des dix-huit triplets vérifiant ces conditions est donnée dans la Table* 1. *Pour chacun d'entre eux, l'équation* (48) *a deux ou trois solutions, et dans deux cas il existe une solution distincte de* 0 *et de* 1 : $m = 3$ *dans le cas* 7, $m = 5$ *dans le cas* 18.

P r e u v e. Pour $m = 3$ et $m = 4$, les coordonnées $\mathcal{U}_n$, $\mathcal{V}_n$, $\mathcal{W}_n$ de ε^n dans l'ordre $\mathbb{Z}[\varepsilon]$ sont données par les formules suivantes où $\mathcal{S}$, $\mathcal{Q}$, $\mathcal{R}$ désignent simplement $\mathcal{S}_3$, $\mathcal{Q}_3$, $\mathcal{R}_3$:

$$\begin{cases} \mathcal{U}_3 = \mathcal{S} = ab^2 - 3\lambda\,, \\ \mathcal{V}_3 = \mathcal{Q} = -(a^2b^4 - 3\lambda ab^2 + 3\lambda^2)\,, \\ \mathcal{W}_3 = \mathcal{R} = (ab^2 - \lambda)^3\,; \end{cases} \tag{49}$$

$$\begin{cases} \mathcal{U}_4 = \mathcal{S}^2 + \mathcal{Q} = -3\lambda(ab^2 - 2\lambda)\,, \\ \mathcal{V}_4 = \mathcal{Q}\mathcal{S} + \mathcal{R} = \lambda(3a^2b^4 - 9\lambda ab^2 + 8\lambda^2)\,, \\ \mathcal{W}_4 = \mathcal{R}\mathcal{S} = (ab^2 - 3\lambda)(ab^2 - \lambda)^3\,. \end{cases} \tag{50}$$

Remarquons que $-\mathcal{V}_3 = ab^2\mathcal{U}_3 + 3\lambda^2$ et rappelons que $\mathcal{F}_2(\varepsilon) = -\mathcal{V}_4$. D'après

Prop. 9, $b \in \{1,2,3,6\}$; nous montrons d'abord que l'équation (48) a deux solutions lorsque $b \neq 1$. Si $3 \,|\, b$ alors $3 \nmid a\lambda$, $3 \,\|\, \mathcal{U}_3$, $3 \,\|\, \mathcal{V}_3$ et $3 \nmid \mathcal{W}_3$, via (49). Le critère $\mathcal{F}_3$ appliqué à ε^3, pour $p = 3$ et $\alpha = \beta = 1$, montre que l'équation (48) a deux solutions. Si maintenant $2 \,|\, b$ alors $2 \nmid a\lambda$, $2 \,\|\, \mathcal{U}_4$, $4 \,\|\, \mathcal{V}_4$ et $2 \nmid \mathcal{W}_4$, via (50). L'équation (48) a encore deux solutions, d'après le critère $\mathcal{F}_2$ appliqué à ε^4 pour $p = 2$, $\alpha = 1$ et $\beta = 2$. Nous pouvons supposer que $b = 1$, le triplet $(\mathcal{S}, \mathcal{Q}, \mathcal{R})$ est bien de la forme indiquée. Nous étudions ensuite le cas où $3 \,|\, a\lambda$.

Si $3 \,|\, a$ alors $a \in \{3, 6, 15, 30\}$ et $\lambda \in \{\pm 1, \pm 2\}$, ainsi $3 \,|\, \mathcal{U}_3$, $3 \,\|\, \mathcal{V}_3$ et $3 \nmid \mathcal{W}_3$, via (49). D'après le critère $\mathcal{F}_3$ appliqué à ε^3 pour $p = 3$, $\alpha \geq 1$ et $\beta = 1$, la condition $3^2 \,|\, \mathcal{U}_3$, où $\mathcal{U}_3 = a - 3\lambda$, est nécessaire pour que l'équation (48) ait trois solutions. Comme $(a, \lambda) = 1$ et $a \geq \lambda + 2$, nous obtenons ainsi les cas 4, 6, 7, 10, 12, 15 de la Table 1; remarquons que $\mathcal{U}_3 = 0$ dans le cas 7, $m = 3$ est solution de l'équation (48).

Lorsque $\lambda = \pm 3$, alors $a \in \{1, 2, 5, 10\}$; on vérifie que $3^2 \,\|\, \mathcal{U}_4$, $3^2 \,\|\, \mathcal{V}_4$ et $3 \nmid \mathcal{W}_4$, via (50). D'après le critère $\mathcal{F}_2$ appliqué à ε^4 pour $p = 2$ et $\alpha = \beta = 2$, la condition $3^4 \,|\, \mathcal{U}_5$, où $\mathcal{U}_5 = \mathcal{S}^3 + 2\mathcal{Q}\mathcal{S} + \mathcal{R}$, est nécessaire pour que l'équation (48) ait trois solutions. Comme $\mathcal{U}_5 = 6\lambda(a\lambda - 15)$, la condition s'écrit $3^2 \,|\, (a\lambda - 15)$ et nous obtenons les cas 16, 17, 18 de la Table 1, en tenant compte de $a \geq \lambda + 2$. Remarquons que $\mathcal{U}_5 = 0$ dans le cas 18, $m = 5$ est solution de l'équation (48).

La Table 1 est alors complétée par les neufs cas où $3 \nmid a\lambda$. Nous constatons que pour chaque triplet, il existe un nombre premier p tel que $p \geq 5$, $p \,|\, \mathcal{F}_2(\varepsilon)$ et $p \nmid \mathcal{R}$, l'équation (48) a donc deux ou trois solutions, d'après Thm. 3. ∎

§ 8. Cas particulier : $U_3 = 0$

Théorème 9. *Soit (S, Q, R) un triplet vérifiant l'hypothèse* 2. *Supposons que $U_3 = S = 0$. Alors l'équation* (1) *a trois ou quatre solutions en n. Dans les deux cas suivants, il existe une solution distincte de* 0, 1, 3 :

$$\begin{cases} n = 13 \text{ pour le triplet } (0, -20, 100)\,, \\ n = 15 \text{ pour le triplet } (0, -15, 45)\,. \end{cases}$$

Preuve. L'hypothèse $U_3 = S = 0$ entraîne que $\mathcal{F}_2 = -R$, $\mathcal{F}_3 = Q^3$ et $(aS, Q) = Q$. Soit $\delta = (Q, R)$. L'équation (1) a trois solutions en n : 0, 1, 3 lorsque $Q \neq \pm\delta$, d'après Thm. 5 et Thm. 6, et d'après Thm. 7, elle possède au moins trois solutions lorsque $Q = \pm\delta$, à condition que le triplet soit du type (41), $(0, -\delta, \delta d)$ avec $\delta = a^2 b$ et $d \geq 2$, ce que nous supposons dans la suite. L'équation (1) est équivalente à l'équation $U_n = 0$ (Cor. 2). Comme $d \geq 2$, pour $n \neq 0$ les zéros de la suite U_n sont de la forme $n = 2h + 1$

(Prop. 3(ii)). D'après (11) et Déf. 2, pour $h \in \mathbb{N}$, $U_{2h+1} = U_5\mathbb{U}_h + U_3\mathbb{V}_h = U_5\mathbb{U}_h$ où $\mathbb{U}_h$ est la fonction symétrique complète de ρ^2, ρ'^2, ρ''^2 et d'après (12), $\mathbb{U}_h(\rho^2) = (ac)^{h-2}\mathbb{U}_h(\rho^2/(ac))$ où $c = (\delta, d)$. Posons $\gamma = \rho^2/(ac)$ et $\mathcal{U}_h = \mathbb{U}_h(\gamma)$; d'après Prop. 11, l'équation (51), $\gamma^h = x\gamma + y$, a deux ou trois solutions en h et chaque solution est un zéro de la suite $\mathcal{U}_h$. Dans les deux cas particuliers du Lemme 8, on trouve une solution distincte de 0 et 1 : $h = 6$ pour $\delta = 20$ et $d = 5$, $h = 7$ pour $\delta = 15$ et $d = 3$. L'équation (1) a donc trois ou quatre solutions en n et dans les deux cas précédents, elle possède quatre solutions : 0, 1, 3, 13 et 0, 1, 3, 15. ∎

Proposition 11. *Soit* $(0, -\delta, \delta d)$ *un triplet vérifiant l'hypothèse* 2, *avec* $\delta = a^2 b$ *et* $d \geq 2$. *Posons* $b = cb_1$, $d = cd_1$, $t = cd_1^2$ *où* $c = (b, d)$ *et* $1 = (a, d)$. *Désignons par* γ *l'entier* $\rho^2/(ac)$ *et par* $\mathcal{U}_h$ *la fonction symétrique complète de* γ, γ', γ'' (*Déf.* 2). *Le triplet* $(\mathcal{S}_2, \mathcal{Q}_2, \mathcal{R}_2)$ *représentant le polynôme minimal de* γ *est défini par*

$$(-2b_1 a, -(b_1 a)^2, b_1^2 at)\,;$$

ce triplet vérifie l'hypothèse 2. *Chaque solution en* h *de l'équation*

$$\gamma^h = x\gamma + y \tag{51}$$

est un zéro de la suite $\mathcal{U}_h$. *L'équation* (51) *a deux ou trois solutions en* h, *et seulement deux solutions lorsque* $4 \mid (t + 2a^2 b_1)$.

P r e u v e. Un calcul simple montre que le triplet $(-2\delta, -\delta^2, \delta^2 d^2)$ représente le polynôme minimal de ρ^2; ce triplet vérifie l'hypothèse 1 (Prop. 1(i)). Avec les notations de l'énoncé, $\delta = a^2 b_1 c$ et $d = cd_1$; après réduction par ac on obtient le triplet $(\mathcal{S}_2, \mathcal{Q}_2, \mathcal{R}_2)$ représentant le polynôme minimal h_2 de $\gamma = \rho^2/(ac)$. Les hypothèses $(t, ab_1) = 1$ et $t \geq 2$ entraînent que $\delta_\gamma = (\mathcal{Q}_2, \mathcal{R}_2) = b_1^2 a$ et $\mathcal{R}_2 \nmid \mathcal{Q}_2$. Le triplet $(\mathcal{S}_2, \mathcal{Q}_2, \mathcal{R}_2)$ vérifie bien l'hypothèse 2. D'après Prop. 1(ii) où ρ est remplacé par γ, pour $h \in \mathbb{N}$, les suites-coordonnées de γ^h dans l'ordre $\mathbb{Z}[\gamma]$ vérifient la relation de récurrence ayant h_2 comme polynôme auxiliaire, et elles sont définies par $\gamma^h = \mathcal{U}_h\gamma^2 + \mathcal{V}_h\gamma + \mathcal{W}_h$. Chaque solution en h de l'équation (51) est un zéro de la suite $\mathcal{U}_h$ (Cor. 2).

Nous étudions les solutions modulo deux de cette équation en fonction de l'indice $\mathcal{F}_2(\gamma) = -(\mathcal{Q}_2\mathcal{S}_2 + \mathcal{R}_2)$. Posons $\mathcal{F}_2(\gamma) = \delta_\gamma d_\gamma \mathcal{F}_2''(\gamma)$; alors $d_\gamma \mathcal{F}_2''(\gamma) = -(t + 2a^2 b_1)$ où $d_\gamma = (\mathcal{S}_2, \mathcal{R}_2/\delta_\gamma) = (2, t)$. Dans le cas où t est pair, d'après Prop. 3(ii), pour h distinct de 0 et 1, l'équation (51) n'a pas de solutions en h si $2 \parallel t$ et il peut exister des solutions impaires si $4 \mid t$, $\mathcal{F}_2''(\gamma)$ étant impair. Si $2 \nmid t$ ou si $4 \mid t$ alors il existe un diviseur premier p impair de $\mathcal{F}_2''(\gamma)$ tel que $p \nmid ab_1 t$, "$\mathcal{F}_2(\gamma)$ n'a pas la propriété $\mathcal{P}(\mathcal{R}_2)$". D'après Cor. 3, les conditions $t + 2a^2 b_1 = 6$ si $4 \mid t$ et $t + 2a^2 b_1 = 3$ si $2 \nmid t$ sont nécessaires pour que l'équation (51) ait quatre solutions. La première condition implique $ab_1 = 1$ et $t = 4$, donc $\delta = 1$, $d = 2$ et le polynôme

minimal de ρ n'est pas irréductible, ce qui contredit l'hypothèse 1. Le cas du triplet $(0,-1,2)$ est traité en exemple. La seconde condition implique $ab_1 = t = 1$, en contradiction avec $t \geq 2$. D'après Thm. 3, l'équation (51) a deux ou trois solutions. ∎

LEMME 8. *Sous les hypothèses et avec les notations de Prop.* 11 :

(i) *Pour* $h \neq 0$, *la suite* $\mathcal{U}_h$ *n'a pas de zéros de la forme* $h = 3m$ *ou* $h = 3m+2$ *si* $3 \,|\, t$ *et pour* $h \neq 1$, *elle n'a pas de zéros de la forme* $h = 3m+1$ *si* $9 \,|\, (8t + 3a^2b_1)$.

(ii) *La suite* $\mathcal{U}_h$ *n'a pas de zéros de la forme* $h = 3m+2$ *lorsque* $ab_1 \neq 1$. *Soit* p *un diviseur premier de* ab_1. *Pour* $h \neq 0$, *la suite* $\mathcal{U}_h$ *n'a pas de zéros de la forme* $h = 3m$ *si* $p \,|\, a$ *avec* $p \geq 3$ *ou si* $p \,|\, b_1$ *avec* $p \geq 5$, *et pour* $h \neq 1$, *elle n'a pas de zéros de la forme* $h = 3m+1$ *si* $a \neq 1$ *ou si* $p \,|\, b_1$ *avec* $p \geq 7$. *Cas particuliers* : $\mathcal{U}_6 = 0$ *pour* $a^2b_1 = 4$ *et* $t = 5$; $\mathcal{U}_7 = 0$ *pour* $a^2b_1 = 5$ *et* $t = 3$.

P r e u v e. La partie (i) du lemme résulte de Prop. 8(ii) appliquée au triplet $(\mathcal{S}_2, \mathcal{Q}_2, \mathcal{R}_2)$ avec $D_\gamma = (3,t)$ et $D_\gamma \mathcal{F}_3''(\gamma) = a(8t + 3a^2b_1)$.

(ii) Soient $\mathcal{X}_m$, $\mathcal{Y}_m$, $\mathcal{Z}_m$ les suites définies par $b_1\mathcal{U}_{3m} = \delta_\gamma^m \mathcal{X}_m$, $\mathcal{U}_{3m+1} = \delta_\gamma^m \mathcal{Y}_m$ et $\mathcal{U}_{3m+2} = \delta_\gamma^m \mathcal{Z}_m$ où $\delta_\gamma = b_1^2 a$. Par hypothèse $(t, ab_1) = 1$ et $t \geq 2$; d'après Prop. 7(ii) où ρ est remplacé par γ, la suite $\mathcal{Z}_m$ ne s'annule pas lorsque $ab_1 \neq 1$, et nous déduisons de (35) les expressions respectives de $\mathcal{X}_m$ et $(1/a)\mathcal{Y}_m$, pour $\lambda = 0$ et $\lambda = 1$:

$$\sum_{k=0}^{m-1} (t)^k (a^2b_1)^{m-1-k} \Bigg(\sum_{i+2j=3m-2+\lambda-3k} \frac{(i+j+k)!}{i!j!k!} (-1)^{i+j} 2^i \Bigg),$$

$$(-1)^{m-2+\lambda-k} \binom{3m-1+\lambda-k}{2k+1} = \sum_{i+2j+3k=3m-2+\lambda} \frac{(i+j+k)!}{i!j!k!} (-1)^{i+j} 2^i,$$

ce qui s'écrit plus simplement, en posant $l = m-1-k$,

$$\text{(52)} \qquad \begin{cases} \mathcal{X}_m = - \displaystyle\sum_{0 \leq l \leq m-1} (-a^2b_1)^l t^{m-1-l} \binom{2m+l}{3l+1}, \\ \mathcal{Y}_m = a \displaystyle\sum_{0 \leq l \leq m-1} (-a^2b_1)^l t^{m-1-l} \binom{2m+l+1}{3l+2}. \end{cases}$$

Supposons que $ab_1 \neq 1$; nous obtenons alors les congruences modulo a^2b_1 : $\mathcal{X}_m \equiv -2mt^{m-1}$, $(1/a)\mathcal{Y}_m \equiv m(2m+1)t^{m-1}$; p désigne dans la suite un diviseur de ab_1.

Si la suite $\mathcal{X}_m$ s'annule pour $m \geq 1$ alors l'inégalité ultramétrique appliquée au second membre de $v_p(2m) = v_p(\mathcal{X}_m + 2mt^{m-1})$, via (52), entraîne

que

$$v_p(2m) \geq \min_{1\leq l} v_p\left((a^2b_1)^l \binom{2m+l}{3l+1}\right) . \tag{53}$$

Ecrivons $\binom{2m+l}{3l+1}$ sous la forme

$$2m\binom{2m+l}{2m}\binom{2m-1}{2l}\frac{l!(2l)!}{(3l+1)!} ;$$

alors, par définition de $v_p(X!)$, la condition (53) implique

$$0 > lv_p(a^2b_1) - (3l+1)/(p-1) .$$

Cette condition n'est pas vérifiée lorsque p divise a avec $p \geq 3$ ou lorsque p divise b_1 avec $p \geq 5$. Dans le cas où $a = 2$, chaque zéro de la suite $\mathcal{X}_m$ est de la forme $m = 2l$ où m vérifie l'équation $\varepsilon^m = x\gamma + y$, en posant $\varepsilon = \gamma^3/(b_1^2 a)$ dans (36). Les expressions de ε et de ε^2 pour $a = 2$ sont données par $\varepsilon = -2\gamma^2/b_1 - 2\gamma + t$, $\varepsilon^2 = 4(5b_1 - t)\gamma^2/b_1 + 4(t + 8b_1)\gamma + t(t - 16b_1)$. On vérifie que $\mathcal{U}_6 = 0$ lorsque $t = 5$ et $a^2b_1 = 4$, via $\varepsilon^2 = 52\gamma - 55$.

Remarquons que la suite $\mathcal{Y}_m$ ne s'annule pas pour $m \geq 1$, lorsque a est pair, d'après Thm. 6 où ρ est remplacé par γ. Supposons maintenant que $\mathcal{Y}_m$ s'annule avec $m \geq 1$; alors $v_p(m(2m+1)) = v_p((1/a)\mathcal{Y}_m - m(2m+1)t^{m-1})$ et d'après l'inégalité ultramétrique, via (52), nous obtenons

$$v_p(m(2m+1)) \geq \min_{1\leq l} v_p\left((a^2b_1)^l \binom{2m+l+1}{3l+2}\right) , \tag{54}$$

a étant impair. Nous distinguons deux cas suivant que p divise m ou bien $2m+1$. Si p divise m alors, $\binom{2m+l+1}{3l+2}$ étant écrit sous la forme

$$2m\binom{2m+l+1}{2m}\binom{2m-1}{2l}\frac{(l+1)!(2l)!}{(3l+2)!} ,$$

par définition de $v_p(X!)$, la condition (54) implique

$$0 > lv_p(a^2b_1) - (3l+2)/(p-1) .$$

Cette condition n'est pas vérifiée lorsque p divise a avec $p \geq 5$ ou lorsque p divise b_1 avec $p \geq 7$. De même, si p divise $2m+1$ alors $\binom{2m+l+1}{3l+2}$ est de la forme

$$(2m+1)\binom{2m+l+1}{2m+1}\binom{2m}{2l+1}\frac{l!(2l+1)!}{(3l+2)!} ,$$

et la condition (54) implique

$$0 > lv_p(a^2b_1) - (3l+2)/(p-1) + v_p((2l+1)!) .$$

Cette condition n'est pas vérifiée lorsque p divise a avec $p \geq 3$ ou lorsque p divise b_1 avec $p \geq 7$. Dans le cas où $a = 3$, chaque zéro de la suite $\mathcal{Y}_m$ est de la forme $m = 9l$ où m vérifie l'équation $\varepsilon^m = x\eta + y$, en posant $\varepsilon = \gamma^3/(b_1^2 a)$ et $\gamma\eta = ab_1 t$ dans (37). Les expressions de ε et de ε^3, pour $a = 3$, sont

données par $\varepsilon = 3\eta^2/t-(2t+27b_1)\eta/t+(t-36b_1)$, $\varepsilon^3 = 3A\eta^2/t-3B\eta/t+C$, avec $A \equiv 7t^2$, $B \equiv 2t^3$, $C \equiv t^3 \pmod 3$. Alors Thm. 2 appliqué à $\zeta = \varepsilon^3$ avec $p = 3$ et $\theta = \eta$, montre que ε^{3l} n'est pas binomial en η pour $l \geq 1$, donc $a \neq 3$. On vérifie que $\mathcal{U}_7 = 0$ lorsque $t = 3$ et $a^2b_1 = 5$, via $\varepsilon^2 = 13\eta - 116$. ∎

Conclusion

Nous avons rassemblé dans deux corollaires des conditions nécessaires pour que l'équation (1) ait quatre solutions en n. Nous appliquons ensuite ces conditions dans le cas où f n'est pas irréductible (Rem. 5). Nous traitons en exemple le cas du triplet $(0,-1,2)$ mis en évidence dans la preuve de Prop. 11. Rem. 6 concerne les fonctions récurrentes fondamentales.

Corollaire 6. *Sous les hypothèses de Thm.* 9, *si l'équation* (1) *a une solution* n *distincte de* 0, 1, 3 *alors* n *est un entier positif impair, le triplet est de la forme* $(0,-\delta,\delta d)$, *avec* $4c \nmid (2\delta + d^2)$ *où* $\delta = a^2b$ *et* $c = (b,d)$, *et* δ *et* d *vérifient les conditions suivantes* :

(i) *pour* $n = 6m+1$: $a \in \{1,2\}$, $b/c \in \{1,2,3,6\}$ *et* $3 \nmid d$;
(ii) *pour* $n = 6m+3$: $a = 1$, $b/c \in \{1,2,3,5,6,10,15,30\}$, $9c \nmid (3\delta+8d^2)$;
(iii) *pour* $n = 6m+5$: $a = 1$, $b = c$ *et* $3 \nmid d$.

Corollaire 7. *Soit* (S,Q,R) *un triplet vérifiant l'hypothèse* 2 *et ne figurant pas dans la Table* 3, *avec* S *non nul. Si l'équation* (1) *a quatre solutions en* n : 0, 1, h, k, *alors* h *et* k *sont positifs et distincts de* 4, h *ou* k *est congru à* 2 *modulo* 3. *La forme du triplet et certaines conditions sur* h *et* k *se déduisent des Corollaires* 2, 3, 4 *et* 5.

Remarque 5. Regardons les conséquences immédiates de ces corollaires, lorsque le polynôme f a une racine dans $\mathbb{Z}$, $\rho = K$, et deux racines complexes conjuguées (voir Rem. 1). Une vérification élémentaire des conditions de Cor. 7, pour f donné dans Rem. 3, montre que l'équation (17) a deux ou trois solutions en n si S est non nul. D'après Cor. 6, si S est nul alors l'équation (17) a trois ou quatre solutions en n pour $K \neq 1$ et trois solutions pour $K = 1$, sauf dans le cas du triplet $(0,-1,2)$, où il y a quatre solutions en n : 0, 1, 3, 11. Voir exemple.

Exemple. Déterminons les solutions de l'équation (17), $\widehat{\rho^n} = x\widehat{\rho} + y\widehat{1}$, dans le cas du triplet $(0,-1,2)$. D'après Rem. 1 et Cor. 2, chaque solution en n de l'équation (17) est un zéro de la suite U_n. Le polynôme $f(X) = X^3 + X - 2$ a trois racines $1, -\theta, -\bar{\theta}$ où $\theta = (1+i\sqrt{7})/2$. D'après (4), pour $n \in \mathbb{N}$,

$$\theta^{n+2} - \bar{\theta}^{n+2} = (-1)^n(\theta - \bar{\theta}) \Leftrightarrow U_n = 0\,, \tag{55}$$

et $n+2 \in \{1,2,3,5,13\}$, d'après Kubota [15, p. 24] ou d'après Beukers [3, p. 266]; mais $n \in \mathbb{N}$, la suite U_n a donc quatre zéros : 0, 1, 3, 11, qui sont les seules solutions en n de l'équation (17). Il est bien connu que l'équation (55) est équivalente à l'équation de Ramanujan–Nagell, $x^2+7=2^{n+4}$, où $n \in \mathbb{N}$ et $x \in \mathbb{Z}$ (voir le livre de Cassels [8, p. 70 et note, p. 73], Mignotte [23], ainsi que leurs références). A titre d'illustration, retrouvons les solutions de l'équation (17) par des congruences modulo 2 et 31. Pour simplifier les notations, $\widehat{\ }$ est supprimé, ρ^n désigne le vecteur $(1,(-\theta)^n,(-\bar{\theta})^n)$, le vecteur $(1,1,1)$ est omis.

La suite U_n est définie par $U_0=U_1=0$, $U_2=1$ et par la relation de récurrence $U_{n+3}=SU_{n+2}+QU_{n+1}+RU_n$ où $(S,Q,R)=(0,-1,2)$ est le triplet définissant ρ. Comme $U_3=S=0$, nous supposons qu'il existe $n>3$ tel que $U_n=0$. D'après (13), $U_{2l+2} \equiv (-1)^l \pmod 4$, $(1/2)U_{2l+1} \equiv (-1)^l(l-1) \pmod 4$. La suite U_n s'annule pour $n=8m+3$ avec $m \geq 1$, après vérification $U_{11}=0$. Nous avons obtenu les quatre zéros de la suite U_n : 0, 1, 3, 11. Supposons alors qu'il existe $m>1$ tel que $U_{8m+3}=0$. D'après (11), $U_{8m+3}=U_{19}\mathcal{U}_m+U_{11}\mathcal{V}_m+U_3\mathcal{W}_m=U_{19}\mathcal{U}_m$, $U_{19}=72$, donc $\mathcal{U}_m=0$ où $\mathcal{U}_m$ est la fonction symétrique complète de $\varphi=\rho^8$ et φ est défini par le triplet $(\mathcal{S},\mathcal{Q},\mathcal{R})=(-30,-225,256)$. Les zéros de la suite $\mathcal{U}_m$ correspondent aux puissances φ^m binomiales en φ, via (3), $\varphi^m=\mathcal{U}_m\varphi^2+\mathcal{V}_m\varphi+\mathcal{W}_m$. L'indice $\mathcal{F}_2(\varphi)$, défini par $-(\mathcal{QS}+\mathcal{R})$, est égal à $-2\cdot 31\cdot 113$, et pour $p=31$, on vérifie que $\mu=10$ est le plus petit exposant de φ^2 tel que 31 divise les deux premières coordonnées de $\varphi^{2\mu}$ dans la base $\{\varphi^2,\varphi,1\}$ de $\mathbb{C}^3$. Le critère $\mathcal{F}_2$ appliqué à $\varphi^{2\mu}$, pour $p=31$ et $\mu=10$, avec $\varphi^{2\mu} \equiv 31(11\varphi^2+9\varphi+11)+1 \pmod{31^2}$, montre que l'équation $\varphi^m=x\varphi+y$ n'a pas de solutions pour m distinct de 0 et 1. Pour $m>1$, $U_{8m+3}=72\mathcal{U}_m$ ne s'annule pas.

Explicitons le critère $\mathcal{F}_2$ sur cet exemple. Par réduction modulo 31 de la récurrence, $\mathcal{U}_{2l+1} \equiv \mathcal{SU}_{2l}$ et $\mathcal{U}_{2l} \equiv (\mathcal{S}^{2l}-\mathcal{Q}^l)/(\mathcal{S}^2-\mathcal{Q})$, chacune des congruences $\mathcal{U}_{2l} \equiv 0$ et $\mathcal{U}_{2l+1} \equiv 0 \pmod{31}$ implique $l \equiv 0 \pmod{10}$ et par réduction modulo 4, via (13), $\mathcal{U}_{2l+2} \equiv (-1)^l$. Les solutions de $\mathcal{U}_m=0$ sont donc de la forme $m=20h+1$. D'après (6),

$$2^8\varphi^{20h}=\mathcal{U}_{20h+1}\psi^2+\mathcal{V}_{20h+2}\psi+\mathcal{W}_{20h+3} \tag{56}$$

où $\psi=2^8/\varphi$. L'expression de $\varphi^{2\mu}$ ci-dessus, et les formules de changement de bases (15), donnent $\varphi^{20} \equiv 31(18\psi^2+22\psi+5)+1 \pmod{31^2}$, la congruence est prise dans $\mathbb{Z}_{(31)}=\{(u/v)\in\mathbb{Q} \mid 31\nmid v\}$. Posons $\varphi^{20}=31\gamma+1$; par la formule du binôme,

$$\varphi^{20h}=1+\sum_{1\leq j\leq h} 31^j\binom{h}{j}\gamma^j\,, \tag{57}$$

avec $\gamma^j=x_j\psi^2+y_j\psi+z_j$ et $x_j,\ y_j,\ z_j \in \mathbb{Z}_{(31)}$. On identifie les coor-

données de φ^{20h} dans la base $\{\psi^2, \psi, 1\}$ de $\mathbb{C}^3$, via (56) et (57). L'équation $\mathcal{U}_{20h+1} = 0$, après division par 31, est équivalente à

$$-hx_1 = \sum_{2\le j\le h} 31^{j-1}\binom{h}{j}x_j\,, \tag{58}$$

avec $x_1 \equiv 18 \pmod{31}$, donc $h \equiv 0 \pmod{31}$. Si $h \ge 1$ alors $\nu = v_{31}(h)$ avec $\nu \ge 1$ entier, où v_{31} est la valuation 31-adique dans $\mathbb{Q}$. D'après l'inégalité ultramétrique appliquée à (58), $\nu \ge \min_{j\ge 2}(j - 1 + v_{31}(\binom{h}{j}))$; comme $v_{31}(\binom{h}{j}) > \nu - j/30$ pour $j \ge 2$, on en déduit que $\nu > \nu + 14/15$, ce qui est impossible. Donc $h = 0$. L'équation $\varphi^{20h} = x\psi + y$ n'a pas de solutions pour $h \ge 1$.

R e m a r q u e 6. D'après Beukers [4], la zéro-multiplicité d'une récurrence ternaire non-dégénérée de nombres rationnels est égale à six (voir Déf. 1). Il n'est pas évident de trouver des suites ayant au moins quatre zéros, en dehors des fonctions récurrentes fondamentales U_n, V_n, W_n. Les suites V_n et W_n, définies par (3), ont chacune au moins deux zéros, elles s'expriment en termes de la suite U_n, via les relations : $V_n = U_{n+1} - SU_n = QU_{n-1} + RU_{n-2}$ avec $V_1 = 1$ et $V_0 = V_2 = 0$; $W_n = RU_{n-1}$ avec $W_0 = 1$ et $W_1 = W_2 = 0$. Les zéros de la suite W_n se déduisent trivialement des zéros de la suite U_n et, lorsque $QS = 0$, il en est de même pour la suite V_n. Dans le cas où QS est non nul, on peut discuter le nombre des zéros impairs de la suite V_n en fonction du nombre de ses zéros pairs, qui sont déterminés par l'équation $V_{2m} = -\mathcal{F}_2\mathcal{U}_m = 0$ où $\mathcal{U}_m$ est la fonction symétrique complète de ρ^2, ρ'^2, ρ''^2 et $\mathcal{F}_2$ est l'indice de ρ^2 relatif à ρ (Déf. 5). Cette étude n'est pas immédiate.

La Table 3 donne les solutions en n de l'équation $\rho^n = x\rho + y$, où ρ est l'une quelconque des racines du polynôme $f(X) = X^3 - SX^2 - QX - R$, non-dégénéré et à coefficients dans $\mathbb{Z}$, avec $R \ne 0$, lorsque le nombre de solutions est au moins égal à quatre. Les solutions en m de l'équation $\omega^m = x\omega + y$ où $\omega = R/\rho$ se déduisent trivialement par la relation $n + m = 1$. La liste des triplets (S, Q, R) est exhaustive dans le cas où $R \mid Q$ (voir [12, p. 164]), dans le cas où $Q = -S^2$ (voir Thm. 8), et dans le cas où $f(K)$=0, avec $K \in \mathbb{Z}^*$, pour $K = 1$ ou bien pour $K \ne 1$ et $S \ne 0$ (voir Rem. 5). Les trois premiers triplets sont extraits de [10, p. 417]. Le triplet $(*)$ est relié à l'équation de Ramanujan–Nagell (voir l'exemple ci-dessus). Dans le cas du triplet $(2, -4, 4)$, les six solutions sont les zéros de la suite de Berstel et Mignotte, définie par $U_{n+3} = 2U_{n+2} - 4U_{n+1} + 4U_n$ avec $U_0 = U_1 = 0$, $U_2 = 1$ (voir [9, p. 99] et [11, pp. 30 et 42].

Table 3

S	Q	R	$n : \rho^n = x\rho + y$				
-1	0	1	-2	0	1	5	14
0	-1	1	0	1	3	8	
-1	-1	1	0	1	4	17	
^{*0}	-1	2	0	1	3	11	
-2	0	2	-2	0	1	24	
-2	0	4	-2	0	1	6	22
-3	0	9	-2	0	1	7	
0	-3	3	0	1	3	10	

S	Q	R	$n : \rho^n = x\rho + y$					
0	-6	6	0	1	3	12		
0	-15	45	0	1	3	15		
0	-20	100	0	1	3	13		
2	-4	4	0	1	4	6	13	52
2	-4	2	0	1	4	12		
3	-9	9	0	1	4	9		
3	-9	18	0	1	4	10		
5	-25	50	0	1	4	16		

Bibliographie

[1] T. M. Apostol, *On the nonvanishing of homogeneous product sums*, J. Number Theory 24 (1986), 95–106.

[2] E. Bell, *Notes on recurring series of the third order*, Tôhoku Math. J. 24 (1924), 168–184.

[3] F. Beukers, *The multiplicity of binary recurrences*, Compositio Math. 40 (1980), 251–267.

[4] —, *The zero-multiplicity of ternary recurrences*, Compositio Math. 77 (1991), 165–177.

[5] F. Beukers and R. Tijdeman, *On the multiplicities of binary complex recurrences*, Compositio Math. 51 (1984), 193–213.

[6] J. P. Bézivin, A. Pethö and A. J. van der Poorten, *A full characterisation of divisibility sequences*, Amer. J. Math. 112 (6) (1990), 985–1001.

[7] E. Bombieri and W. M. Schmidt, *On Thue's equation*, Invent. Math. 88 (1) (1987), 69–82.

[8] J. W. S. Cassels, *Local Fields*, London Math. Soc. Stud. Texts 3, Cambridge 1986.

[9] L. Cerlienco, M. Mignotte et F. Piras, *Suites récurrentes linéaires. Propriétés algébriques et arithmétiques*, Enseign. Math. 33 (1987), 67–108.

[10] B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs 10, A.M.S., 1964.

[11] B. Deshommes, *Sur les zéros des fonctions symétriques complètes des corps cubiques*, Pacific J. Math. 139 (1) (1989), 17–44.

[12] —, *On semi-local binomial units in cubic number fields*, J. Reine Angew. Math. 402 (1989), 153–165.

[13] M. Duboué, *Une suite récurrente remarquable*, Europ. J. Combin. 4 (3) (1983), 205–214.

[14] B. Gordon and S. P. Mohanty, *On a theorem of Delaunay and some related results*, Pacific J. Math. 68 (2) (1977), 399–409.

[15] K. K. Kubota, *On a conjecture of Morgan Ward*, *I*, *II*, *III*, Acta Arith. 33 (1977), 11–28, 29–48, 99–109.

[16] A. Lascoux, *Suites récurrentes linéaires*, Adv. in Appl. Math. 7 (2) (1986), 228–235.

[17] D. J. Lewis and J. Turk, *Repetitiveness in binary recurrences*, J. Reine Angew. Math. 356 (1985), 19–48.

[18] E. Lucas, *Théorie des Nombres*, Gauthier-Villars, Paris 1891.

[19] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Oxford Math. Monographs, 1979.

[20] K. Mahler, *On the Taylor coefficients of rational functions*, Proc. Cambridge Philos. Soc. 52 (1956), 39–48.

[21] —, *p-Adic Numbers and Their Functions*, 2nd ed., Cambridge Tracts in Math. 76, Cambridge 1981.

[22] M. Mignotte, *Détermination des répétitions d'une certaine suite récurrente linéaire*, Publ. Math. Debrecen 33 (1986), 297–306.

[23] —, *Une nouvelle résolution de l'équation* $x^2 + 7 = 2^n$, Rend. Sem. Fac. Sci. Univ. Cagliari 54 (2) (1984), 41–43.

[24] T. Nagell, *L'analyse indéterminée de degré supérieur*, Mémorial Sci. Math. 39, Gauthier-Villars, Paris 1929.
[25] P. A. Picon, *Sur certaines suites récurrentes cubiques ayant deux ou trois termes nuls*, Discrete Math. 21 (1978), 285–296.
[26] P. Robba, *Zéros des suites récurrentes linéaires*, Groupe d'étude d'Analyse ultramétrique, 5e année, 1977/78, Paris, Exp. 13, 5 pp.
[27] S. J. Scott, *On the number of zeros of a cubic recurrence*, Amer. Math. Monthly 67 (1960), 169–170.
[28] M. F. Smiley, *On the zeros of a cubic recurrence*, ibid. 63 (1956), 171–172.
[29] R. Tijdeman, *Multiplicities of binary recurrences*, Sémin. Théorie de Nombres, Univ. Bordeaux I, 1980/1981, Exp. 29, 11 pp.
[30] G. Turnwald, *On the nonvanishing of homogeneous product sums*, J. Number Theory 32 (1989), 257–262.
[31] A. J. van der Poorten, *Some facts that should be better known, especially about rational functions*, in: Number Theory and Application (NATO-ASI, Banff 1988), R. A. Mollin (ed.), Kluwer Academic Publishers, Dordrecht 1989, 497–528.
[32] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. 33 (1931), 153–165.
[33] —, *Notes on an arithmetical property of recurring series*, Math. Z. 39 (1934), 211–214.
[34] —, *On the number of vanishing terms in an integral cubic recurrence*, Amer. Math. Monthly 62 (1955), 155–160.
[35] —, *The vanishing of the homogeneous product sum of the roots of a cubic*, Duke Math. J. 26 (1959), 553–562.
[36] —, *The vanishing of the homogeneous product sum on three letters*, ibid. 27 (1960), 619–624.
[37] —, *Some Diophantine problems connected with linear recurrences*, Report Institute Th. Numbers, Univ. Colorado, Boulder 1959, 250–257.

UNIVERSITÉ DE POITIERS
MATHÉMATIQUES
40, AVENUE DU RECTEUR PINEAU
F-86022 POITIERS CEDEX, FRANCE

*Received January 25, 1991**

* The paper was originally submitted for publication in Acta Arithmetica (received by the editors of Acta Arith. July 25, 1989 and in revised form August 21, 1990).