Astérisque

ANDRE SCHINZEL

Les résidus de puissances et les congruences exponentielles

Astérisque, tome 41-42 (1977), p. 103-109

<http://www.numdam.org/item?id=AST_1977__41-42__103_0>

© Société mathématique de France, 1977, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Société Mathématique de France
Astérisque 41-42 (1977) p.103-109

LES RÉSIDUS DE PUISSANCES ET LES CONGRUENCES EXPONENTIELLES

par

André SCHINZEL

Mon rapport d'aujourd'hui est la suite de ma conférence à Bordeaux en 1974 [3]. Je commence par rappeler le dernier résultat mentionné dans cette conférence sous une forme un peu simplifiée.

THÉORÈME A. Soient K un corps algébrique, $\alpha_1,\dots,\alpha_k,\beta$ des éléments de K^*. La résolubilité des congruences $x^n \equiv \alpha_i \pmod{\mathfrak{P}}$ entraîne la résolubilité de la congruence $x^n \equiv \beta \pmod{\mathfrak{P}}$ pour presque tous les idéaux premiers $\mathfrak{P}$ du corps algébrique K si et seulement si l'une au moins des quatre conditions suivantes est satisfaite : pour des éléments Γ, δ de K et des entiers l_i, q_i convenables

(i) $\beta \prod_{i=1}^{k} \alpha_i^{q_i} = \gamma^n$;

(ii) $n \not\equiv 0 \bmod 2^\tau$, $\prod_{i=1}^{k} \alpha_i^{l_i} = -\delta^2$, $\beta \prod_{i=1}^{k} \alpha_i^{q_i} = -\gamma^n$;

(iii) $n \equiv 2^\tau \bmod 2^{\tau+1}$, $\prod_{i=1}^{k} \alpha_i^{l_i} = -\delta^2$, $\beta \prod_{i=1}^{k} \alpha_i^{q_i} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n$;

(iv) $n \equiv 0 \bmod 2^{\tau+1}$, $\beta \prod_{i=1}^{k} \alpha_i^{q_i} = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n$.

Ici ζ_q est une racine primitive de l'unité de degré q et τ est le plus grand entier tel que $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$.

Une extension naturelle de ce résultat serait une condition nécessaire et suffisante pour que la résolubilité des congruences $x^n \equiv \alpha_i \bmod \mathfrak{P}$ entraîne la résolubilité d'une au moins des congruences $x^n \equiv \beta_j \bmod \mathfrak{P}$ $(1 \leqslant j \leqslant l)$ pour presque tous les idéaux premiers de K. Je ne connais pas de pareille condition et je doute que dans le cas général elle puisse être formulée algébriquement en termes du seul corps K. Cependant si $\zeta_n \in K$ alors une condition nécessaire et suffisante peut être obtenue moyennant le résultat suivant qui est conséquence simple du théorème de Tschebotareff.

THÉORÈME B. *Si* $\zeta_n, \gamma_1, \ldots, \gamma_r \in K$ *et* $\gamma_1^{x_1}\gamma_2^{x_2}\ldots\gamma_r^{x_r} = \gamma^n$, $\gamma \in K$ *entraîne* $x_1 \equiv x_2 \equiv \ldots \equiv x_r \equiv 0 \bmod n$ *alors pour tout système de nombres entiers* c_i *il existe une infinité d'idéaux premiers* $\mathfrak{P}$ *de* K *tels que*

$$\left(\frac{\gamma_i}{\mathfrak{P}}\right)_n = \zeta_n^{c_i} \qquad (1 \leqslant i \leqslant k).$$

Si nous avons maintenant les nombres $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_L$ arbitraires nous pouvons appliquer le théorème de Skolem [6] d'après lequel chaque corps algébrique possède une base multiplicative c'est-à-dire une suite d'éléments $\pi_1, \pi_2, \ldots$ telle que tout $\alpha \in K$, $\alpha \neq 0$, est représentable d'une manière unique comme

$$\zeta_q \prod_{s=1}^{r} \pi_s^{n_s}$$

où les n_s sont des entiers et ζ_q est une racine de l'unité.

Comme, par le théorème B, les valeurs de $\left(\frac{\pi_s}{\mathfrak{P}}\right)_n$ peuvent être choisies d'une façon arbitraire, la connection entre la résolubilité des congruences $x^n \equiv \alpha_i \bmod \mathfrak{P}$ et $x^n \equiv \beta_j \bmod \mathfrak{P}$ peut être exprimée en termes des exposants qui figurent dans les représentations canoniques des α_i et β_j. On voit que la chose essentielle est de généraliser le théorème B aux corps ne contenant pas ζ_n. Le cas $K = \mathbb{Q}$ a été

traité par Mills [2a]. La meilleure généralisation que j'ai trouvée est la suivante.

THÉORÈME 1. Soit w (respectivement w_n) le nombre des racines de l'unité de degré quelconque (respectivement de degré n) contenues dans K,

$$\sigma = (w_n, \text{p.p.c.m}_{\substack{q \mid n \\ q \text{ premier ou } q = 4}} [K(\zeta_q) : K]) .$$

Si $\gamma_1^{x_2} \gamma_2^{x_2} \cdots \gamma_r^{x_r} = \gamma^n$, $\gamma \in K$ entraîne $\sigma x_1 \equiv \ldots \equiv \sigma x \equiv 0 \bmod n$, alors pour tout système de nombres entiers c_i $(1 \leqslant i \leqslant r)$ il existe une infinité d'idéaux premiers $\mathfrak{P}$ de $K(\zeta_n)$ tels que

$$\left(\frac{\gamma_i}{\mathfrak{P}}\right)_n = \zeta_n^{\sigma c_i} \qquad (1 \leqslant i \leqslant r) .$$

De plus, si ou bien

$$\zeta_{(4,n)} \in K \quad \text{et} \quad n \equiv 0 \bmod w_n . \text{p.p.c.m}_{\substack{q \mid n \\ q \text{ premier}}} [K(\zeta_q) : K]$$

ou bien

$$\zeta_{(4,n)} \notin K \quad \text{et} \quad n \equiv 0 \bmod 2^{\tau} w_n . \text{p.p.c.m}_{\substack{q \mid n \\ q \text{ premier}}} [K(\zeta_q) : K]$$

et en outre

$$\zeta_w^{x_o} \gamma_1^{x_1} \cdots \gamma_r^{x_r} = \gamma^n \text{ entraîne } x_i \equiv 0 \bmod \frac{n}{\Gamma} \qquad (1 \leqslant i \leqslant r)$$

alors pour tout système de nombres entiers c_i $(0 \leqslant i \leqslant r)$ il existe une infinité d'idéaux premiers de $K(\zeta_n)$ tels que

$$\left(\frac{\zeta_w}{\mathfrak{P}}\right)_n = \zeta_{w_n}^{c_o} \text{ et } \left(\frac{\gamma_i}{\mathfrak{P}}\right)_n = \zeta_n^{\sigma c_i} \qquad (1 \leqslant i \leqslant r) .$$

On voit que la différence entre le cas kummérien ($\zeta_n \in K$) et le cas général est

mesurée par le paramètre σ qui ne dépasse jamais w.

Avant de présenter les conséquences du théorème 1 j'indiquerai la méthode de démonstration.

On commence par déterminer tous les binômes normaux dont le degré est une puissance d'un nombre premier. On sait déterminer d'après Darbi [1] tous les binômes normaux sur le corps rationnel. Dans le cas général j'ai réussi seulement à déterminer tous les binômes normaux de degré p^ν, p premier. Voici le résultat :

PROPOSITION 1. *Soit* p *différent de la caractéristique de* K *et* ω *le plus grand entier tel que* $\zeta_{p^L} \in K$. *Le binôme* $x^{p^\nu} - \alpha$ *est le produit des facteurs normaux sur* K *si et seulement si une des conditions suivantes est satisfaite pour un élément* γ *de* K *et un entier* λ *convenable*

(i) $\alpha^{p^{\min(\omega,\nu)}} = \gamma^{p^\nu}$;

(ii) $p = 2$, $\omega = 1$, $\nu \leqslant \tau$, $\alpha = -\gamma^2$;

(iii) $p = 2$, $\omega = 1$, $\nu = \tau+1$, $\alpha = -\gamma^2$, $\sqrt{-(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)} \in K$;

(iv) $p = 2$, $\omega = 1$, $\nu = \tau+1$, $\alpha = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^\lambda} \gamma^{2^{\lambda+1}}$; $1 \leqslant \lambda \leqslant \tau - 2$

(v) $p = 2$, $\omega = 1$, $\nu \geqslant \tau+2$, $\alpha = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\nu-2}} \gamma^{2^{\nu-1}}$.

On observe ensuite que si le binôme satisfait à une des conditions (ii) - (v) mais non à (i) alors son groupe de Galois n'est pas abélien. On tire de là :

PROPOSITION 2. *Soit* n *un entier positif non divisible par la caractéristique de* K. *Le groupe de Galois d'un binôme* $x^n - \alpha$ *sur* K *est abélien si et seulement si*

$$\alpha^{\omega_n} = \gamma^n$$

pour un élément γ *de* K *convenable.*

Ceci établi, on peut passer aux groupes des radicands. Ces groupes ont été introduits par Hasse [2] en 1950 comme les sous-groupes de K^* composés de tous les éléments de K^* représentables comme ϑ^n, $\vartheta \in K(\zeta_n)$: Hasse lui-même a déterminé ces groupes pour les entiers n égaux à une puissance d'un nombre premier. De la proposition 2 on tire :

PROPOSITION 3. Soit n un entier positif non divisible par la caractéristique de K. Si

$$\alpha = \vartheta^n , \quad \vartheta \in K(\zeta_n)$$

alors

$$\alpha^\sigma = \gamma^n , \quad \gamma \in K .$$

De plus, si n satisfait aux conditions (*), alors

$$\alpha = \gamma^{n/\sigma} , \quad \gamma \in K .$$

Le théorème 1 résulte de la proposition 3 et du théorème de Tschebotareff.

Passons maintenant aux applications de notre théorème aux congruences exponentielles. J'entends par congruence exponentielle une congruence de la forme

$$\sum_{h=1}^{g} A_h \prod_{j=L}^{k} \alpha_{hj}^{x_j} \equiv 0 \bmod \mathfrak{m}$$

où A_h et α_{hj} sont des éléments d'un corps K et $\mathfrak{m}$ un idéal de K. La conjecture fondamentale formulée par Skolem [5] en 1937 dit qu'un système de congruences exponentielles résolubles pour tous les modules $\mathfrak{m}$, traité comme un système d'équations, est résoluble en entiers. Skolem lui-même a esquissé la démonstration de sa conjecture pour les systèmes dont toutes les congruences ne contiennent que deux termes. Le théorème 1 entraîne le théorème suivant :

THÉORÈME 2. Si le système de congruences

$$\prod_{h=1}^{g_i} \left(\prod_{j=1}^{k} \alpha_{hij}^{x_j} - \beta_{Li} \right) \equiv 0 \bmod \mathfrak{m} \qquad (1 \leqslant i \leqslant l)$$

est résoluble pour tous les modules $\mathfrak{m}$, alors le système correspondant d'équations est résoluble en entiers.

On sait que pour les congruences algébriques il suffit de considérer seulement les modules qui sont des puissances de nombres premiers. Pour les congruences exponentielles la situation est différente. Par exemple la congruence

$$(2^x+1)(4^x-2) \equiv 0 \bmod m$$

est résoluble pour tous $m = p^n$, où $p > 2$ mais non pour $m = 91$.

Pour les modules premiers j'ai le résultat suivant :

THÉORÈME 3. Soit f un polynôme à coefficients de K, de degré d et $\alpha_1,\ldots,\alpha_k$ des éléments de K. Si la congruence

$$f(\alpha_1^{x_1}\ldots\alpha_k^{x_k}) \equiv 0 \bmod \mathfrak{P}$$

est résoluble pour presque tous les idéaux premiers de K, alors l'équation

$$f(\alpha_1^{x_1}\ldots\alpha_k^{x_k}) = 0$$

est résoluble en nombres rationnels dont le plus petit dénominateur commun ne dépasse pas $\max(1,d-1)$.

L'exemple donné plus haut montre que l'estimation pour le dénominateur est exacte. Je mentionne encore deux corollaires dont le premier est immédiat.

COROLLAIRE 1. Si la congruence $\alpha_1^{x_1}\ldots\alpha_k^{\Gamma_k} \equiv \beta \bmod \mathfrak{P}$ est résoluble pour presque tous les idéaux premiers $\mathfrak{P}$ de K alors l'équation correspondante est résoluble en entiers.

COROLLAIRE 2. Soit $\{u_n\}$ la suite de Fibonacci. Si la congruence $u_n \equiv c \bmod p$ est résoluble pour presque tous les nombres premiers p, alors $c = u_m$ pour un m entier.

Les démonstrations de tous les résultats cités paraîtront dans mon travail [4] aux Acta Arithmetica vol. 32. La démonstration du théorème A a déjà paru dans [3a].

-:-:-:-

BIBLIOGRAPHIE

[1] G. DARBI.- Sulla reducibilita delle equazioni algebriche. Annali Mat. Pura Appl. (4) 4 (1925), pp. 185-208.

[2] H. HASSE.- Zum Existensatz von Grunwald in der Klassenkörpertheorie. J. Reine Angew. Math. 188 (1950), pp. 40-64.

[2a] W.H. MILLS.- Characters with preassigned values. Canad. J. Math. 15 (1963), 169-171.

[3] A. SCHINZEL.- Les extensions pures et les résidus des puissances. Astérisque 24-25 (1975), pp. 69-74.

[3a] A. SCHINZEL.- On power residues and exponential congruences. Acta Arith. 27 (1975), pp. 397-420.

[4] A. SCHINZEL.- Abelian binomials, power residus and exponential congruences. Acta Arith. 32 (à paraître).

[5] Th. SKOLEM.- Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen. Vid. Akad. Avh. Oslo I (1937), nr 12.

[6] Th. SKOLEM.- On the existence of a multiplicative basis for an arbitrary algebraic field. Norske Vid. Selsk. Forh. (Trondheim), 20 (1957), nr 2.

André Schinzel
Institut Math. Académie Polonaise
des Sciences
B.P. 137, 00-950 WARSZAWA (Pologne)