ACTA ARITHMETICA
IX (1964)

Sur la réductibilité de certains trinômes

par

J. MIKUSIŃSKI et A. SCHINZEL (Warszawa)

W. Ljunggren [1] a examiné la réductibilité des trinômes $x^n \pm x^m \pm 1$. A. Schinzel [2] a étendu ses résultats aux trinômes $x^n \pm 2x^m \pm 1$ et il a énoncé la supposition suivante [3]. Si a et b sont des entiers tels que $ab \neq 0$ et $|a| - |b| \neq 0, \pm 1$, alors il n'existe qu'un nombre fini de rapports m/n pour lesquels le trinôme $x^n + ax^m + b$ est réductible. Dans ce qui suit, on démontre cette hypothèse pour le cas, où $|a|$ est un nombre premier et $|b| = 1$.

LEMME 1. *Si toutes les distances entre n ($\geqslant 3$) points sur une droite, sauf la distance entre les points extrêmes, paraissent au moins deux fois, toutes ces distances sont commensurables.*

Démonstration. Nous fixons un axe de manière que les points extrêmes aient des coordonnées rationnelles et nous considérons les points donnés comme des nombres

$$a_1 < \ldots < a_n. \tag{1}$$

Les nombres a_1 et a_n sont donc rationnels par hypothèse. Il faut démontrer que les nombres restant sont rationnels aussi.

Supposons le contraire. Alors il existe parmi (1) des nombres irrationnels $c_1, \ldots, c_r$ tels que chacun des nombres (1) est de la forme

$$k_0 + k_1 c_1 + \ldots + k_r c_r \quad (k_i - \text{nombres rationnels}) \tag{2}$$

et que les nombres $1, c_1, \ldots, c_r$ sont incommensurables, c'est-à-dire que l'égalité $k_0 + k_1 c_1 + \ldots + k_r c_r = 0$ ne subsiste que lorsque tous les coefficients $k_0, \ldots, k_r$ (rationnels) sont nuls. Alors la représentation (2) est unique pour tout nombre (1).

Soit K le plus grand des coefficients k_r qui interviennent dans les développements des nombres (1). Comme c_r est un des nombres (1), on a $K \geqslant 1$. Pareillement, soit k le plus petit des nombres k_r dans les développements des nombres (1). Comme pour a_1 on a $k_r = 0$, donc $k \leqslant 0$. Soit P le plus grand et p le plus petit des nombres (1) pour lesquels on

a $k_r = K$. Pareillement, soit B le plus grand et b le plus petit des nombres (1) pour lesquels on a $k_r = k$.

Évidemment: $b < B$ et $p < P$. Il ne peuvent donc se présenter que les trois cas suivants: 1° $p < B$ ou 2° $b < P$, ou 3° $b = B = p = P$.

Cas 1°. D'après l'hypothèse, il existe parmi (1) un couple de nombres x, y, différent du couple p, B, tel que

$$y - x = P - b. \tag{3}$$

On a donc $x < b$ ou bien $P < y$. Si $x < b$, la $r^{\text{ième}}$ coordonée k_r de x est plus grande que k. Comme la $r^{\text{ième}}$ coordonnée de y est $\leqslant K$, la $r^{\text{ième}}$ coordonnée de la différence $y - x$ est inférieure à $K - k$. Or, ceci est en contradiction avec (3), car la $r^{\text{ième}}$ coordonnée de la différence $P - b$ est égale à $K - k$. Si $P < y$, alors la $r^{\text{ième}}$ coordonnée de y est inférieure à K. Comme la $r^{\text{ième}}$ coordonnée de x est $\geqslant k$, la $r^{\text{ième}}$ coordonnée de $y - x$ est inférieure à $K - k$, ce qui contredit encore (3). Le cas 1° est donc exclus.

Cas 2°. On peut répéter un raisonnement analogue au précedent ou bien le réduire au cas 1°, en multipliant tous les nombres (1) par -1.

Il ne reste que le cas 3°. Comme les nombres b et B ont, par hypothèse, leur $r^{\text{ième}}$ coordonnée égale à k, et les nombres p et P ont leur $r^{\text{ième}}$ coordonnée égale à K, il s'ensuit que $k = K$. Or, cela est impossible, car $k \leqslant 0$ et $K \geqslant 1$. Donc le cas 3° est aussi exclus.

La contradiction obtenue prouve le lemme.

Lemme 2. *Soient $0 = k_0 < k_1 < \ldots < k_r$ des entiers jouissant de la propriété suivante: chacune des différences $k_j - k_i$ $(0 \leqslant i \leqslant j \leqslant r)$, sauf $k_r - k_0$, se repète au moins deux fois. On affirme que*

$$\frac{k_r}{(k_1, \ldots, k_r)} \leqslant 4^{r-1}.$$

Démonstration. Par hypothèse, pour tout couple (i, j), où $0 \leqslant i \leqslant j \leqslant r$ et $(i, j) \neq (0, r)$, il existe un couple $(g_{ij}, h_{ij}) \neq (i, j)$ tel que

$$k_j - k_i = k_{h_{ij}} - k_{g_{ij}}.$$

Considérons le système des équations linéaires homogènes

$$\begin{aligned} &x_j - x_i = x_{h_{ij}} - x_{g_{ij}} \quad (0 \leqslant i \leqslant j \leqslant r,\ (i, j) \neq (0, r)), \\ &x_0 = 0. \end{aligned} \tag{4}$$

L'une des solutions de ce système est $[k_0, k_1, \ldots, k_r]$. Soit $[a_0, a_1, \ldots, a_r]$ une solution quelconque de (4), consistant en nombres rationnels et soit ξ un nombre irrationnel. On a

$$(k_j + \xi a_j) - (k_i + \xi a_i) = (k_{h_{ij}} + \xi a_{h_{ij}}) - (k_{g_{ij}} + \xi a_{g_{ij}})$$

pour $0 \leqslant i \leqslant j \leqslant r$, $(i, j) \neq (0, r)$. Toute distance dans l'ensemble des points $k_i + \xi a_i$ $(0 \leqslant i \leqslant r)$, sauf la distance entre les points extrèmes, se repète donc au moins deux fois. D'après le lemme 1, toutes ces distances sont commensurables. Comme $k_0 + \xi a_0 = 0$, il s'ensuit que $k_i + \xi a_i = q_i(k_1 + \xi a_1)$, où les q_i $(1 \leqslant i \leqslant r)$ sont des nombres rationnels. Comme ξ est irrationnel, on obtient $k_i = q_i k_1$, $a_i = q_i a_1$ $(1 \leqslant i \leqslant r)$ d'où

$$[a_0, a_1, \ldots, a_r] = \frac{a_1}{k_1}[k_0, k_1, \ldots, k_r].$$

La solution $[a_0, a_1, \ldots, a_r]$ dépend donc linéairement de $[k_0, k_1, \ldots, k_r]$. Cela prouve que la matrice des coefficients du système (1) est d'ordre r est qu'il existe un mineur M de degré r, différent de 0. Comme $k_r \neq 0$, on peut admettre:

$$k_i = k_r \frac{A_i}{M},$$

où A_i sont des nombres entiers $(0 \leqslant i \leqslant r)$. Cela entraîne $k_r | M k_i$ pour $1 \leqslant i \leqslant r$, $k_r | M(k_1, \ldots, k_r)$ et

$$\frac{k_r}{(k_1, \ldots, k_r)} \Big| M. \tag{5}$$

De la forme du système (4) on peut conclûre que $|M| \leqslant 4^{r-1}$, ce qui achève la démonstration.

Théorème. *Soient m et n des nombres naturels et p un nombre premier tels que $m < n$ et $p > 2$. Si le trinôme $f(x) = x^n \pm p x^m \pm 1$ est réductible, on a $n/(n, m) \leqslant 4^{p^2}$. Donc, quel que soit $p > 2$, il n'existe qu'un nombre fini de rapports n/m pour lesquels le trinôme $f(x)$ est réductible.*

Démonstration. Soit $f(x) = x^n + upx^m + v$, où $|u| = |v| = 1$. Si $n = 2m$, l'inégalité est évidemment remplie. Comme les trinômes $f(x)$ et $x^n + uvpx^{n-m} + v = vx^n f(1/x)$ sont réductibles simultanément et $(n, n-m) = (n, m)$, on peut supposer sans restreindre la généralité que $2m < n$. Supposons que

$$f(x) = g(x)h(x),$$

où g et h sont des polynômes à coefficients entiers, de degrés r et s, respectivement, $r > 0$, $s > 0$, $r + s = n$. Posons

$$f_1(x) = g(x)x^s h\left(\frac{1}{x}\right) = \sum_{j=0}^{l} c_{k_j} x^{k_j},$$

où $k_0 = 0 < k_1 < \ldots < k_l = n$ et $c_{k_j} \neq 0$ $(0 \leqslant j \leqslant l)$. On a évidemment

$$f_2(x) = x^r g\left(\frac{1}{x}\right) h(x) = \sum_{j=0}^{l} c_{k_j} x^{n-k_j}.$$

et

$$\begin{aligned} f_1(x)f_2(x) &= (x^n + upx^m + v)(vx^n + upx^{n-m} + 1) \\ &= vx^{2n} + upx^{2n-m} + uvpx^{n+m} + (p^2+2)x^n + \ldots \end{aligned}$$

D'autre part

$$(6) \qquad f_1(x)f_2(x) = \left(\sum_{j=0}^{l} c_{k_j} x^{k_j}\right)\left(\sum_{j=0}^{l} c_{k_j} x^{n-k_j}\right)$$

$$= c_{k_0}c_{k_l}x^{2n} + \sum_{q=n+1}^{2n-1} x^q \sum_{n+k_j-k_i=q} c_{k_i}c_{k_j} + x^n \sum_{j=0}^{l} c_{k_j}^2 + \ldots$$

En comparant les coefficients de x^{2n} et x^n dans (5) et (6), on trouve $c_{k_0}c_{k_l} = v$ et $\sum_{j=0}^{l} c_{k_j}^2 = p^2+2$. D'où

$$(7) \qquad c_{k_0} = vw, \quad c_{k_l} = w, \quad \text{où} \quad w = \pm 1, \quad \text{et} \quad \sum_{j=1}^{l-1} c_{k_j}^2 = p^2.$$

Si $l = 2$, on peut supposer, pour les raisons de symmétrie de $f_1x)$ (et $f_2(x)$, que $2k_1 \leqslant n$. En comparant les coefficients dans (5) et (6), on trouve que $k_1 = m$ et

$$c_{k_2}c_{k_1} = up, \qquad c_{k_1}c_{k_2} = uvp,$$

donc, en vertu de (7): $c_{k_1} = wup$. Finalement, on a $f_1(x) = wf(x)$, c'est-à-dire $g(x)x^s h(1/x) = wg(x)h(x)$. Cela entraîne

$$(8) \qquad x^s h(1/x) = wh(x).$$

Comme $s > 0$, l'équation $h(x)$ a une racine b. En vertu de (8) on a $h(1/b)=0$, ce qui entraîne $f(b) = 0$ et $b^n f(1/b) = 0$. Les égalités

$$b^n + upb^m + v = 0, \qquad vb^n + upb^{n-m} + 1 = 0$$

entraînent $upb^m = uvpb^{n-m}$, d'où $|b|^{n-2m} = 1$. Comme $n-2m \neq 0$, on obtient $|b| = 1$. Or, ceci est impossible, car on aurait alors $p = |upb^m| = |-b^n - v| \leqslant 2$, par contre à la supposition.

On a donc $l > 2$. Cela étant, on tire de (7)

$$|c_{k_j}| < p \qquad (0 \leqslant j \leqslant l).$$

Comme p est un nombre premier, la dernière inégalité entraîne $|c_{k_i}c_{k_j}| \neq p$ $(0 \leqslant i \leqslant j \leqslant l)$ et l'on voit, en comparant les coefficients dans (5) et (6), que toute somme non vide $\sum_{n+k_j-k_i=q} c_{k_i}c_{k_j}$ $(n < q < 2n)$ contient au moins deux termes. Cela veut dire que chacune des différences $k_j - k_i$ $(0 \leqslant i \leqslant j \leqslant l)$, exceptée $k_l - k_0$, apparaît au moins deux fois. Donc, en vertu du lemme 2, on a

$$(9) \qquad \frac{k_l}{(k_1, \ldots, k_l)} \leqslant 4^{l-1}.$$

Mais $n = k_l$ et, en comparant les formules (5) et (6), on trouve que $m = k_j - k_i$ pour certains i et j. Par conséquent,

$$(10) \qquad (n, m) = (k_l, k_j - k_i) \geqslant (k_1, \ldots, k_l).$$

Les inégalités (9) et (10) entraînent la conclusion du théorème, car $l \leqslant p^2+1$, en vertu de (7).

Remarques ajoutées pendant la correction des epreuves:

1. La démonstration du lemme 1 donne, en réalité, une proposition plus forte suivante:

Si toutes les distances entre n $(\geqslant 3)$ points sur une droite ou bien paraissent au moins deux fois ou bien sont commensurables avec la distance entre les points extrêmes, toutes ces distances sont commensurables.

2. La suite

$$k_i = \frac{\varrho}{2}\left(\sqrt{3}^{r-\varrho} + \operatorname{sgn}(2i-r)\sqrt{3}^{|2i-r|-\varrho}\right) \qquad (i = 0, 1, \ldots, r),$$

où $\varrho = 1$ ou 2 pour r impair ou pair, respectivement, satisfait aux conditions du lemme 2 et vérifie l'égalité $k_2/(k_1, \ldots, k_r) = \varrho\sqrt{3}^{r-\varrho}$.

3. Un example non-trivial de trinôme réductible de la forme $x^n \pm px^m \pm 1$ (p premier > 2), trouvé M. Z. Łutczyk, est le suivant:

$$x^8 + 3x^3 - 1 = (x^3 + x - 1)(x^5 - x^3 + x^2 + x + 1).$$

Travaux cités

[1] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. 8 (1960), pp. 65-70.

[2] A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels*, Colloq. Math. 9 (1962), pp. 291-296.

[3] — *Nouveau Livre Ecossais*, Probl. 579, cf. aussi: *Some unsolved problems on polynomials*, Matematička Biblioteka 25 (1963), pp. 63-70.

Reçu par la Rédaction le 11. 7. 1963