Énoncé n^{o} 284 (Michel Lafond, 21-Dijon)

Trouver un polynôme P(x) à coefficients entiers n'ayant aucune racine rationnelle et tel que pour tout entier n, il existe un entier m pour lequel P(m) soit divisible par n.

Solution

J'aurais dû préciser, comme l'avait fait l'auteur : « pour tout entier n non nul… ». Mille excuses.

Outre la solution de l'auteur, j'ai reçu des réponses de René Manzoni (76-Le Havre) et de Pierre Samuel (92-Bourg la Reine), et deux solutions fausses.

Les trois solutions justes sont structurées de la même manière :

- On construit un polynôme qui, pour tout nombre premier p, admette une racine modulo p.
- On prouve que, pour tout p premier et tout j entier, ce polynôme admet une racine modulo p^j.
- On prouve que, pour tout n entier non nul, il admet une racine modulo n.

Mais elles présentent des variantes qu'il convient de souligner, dans la première partie (concernant notamment les « premiers nombres premiers ») et dans la seconde.

Pour construire le polynôme, on fait appel à quelques connaissances sur les résidus quadratiques. Dire que r est résidu (quadratique) modulo p signifie que r est premier avec p et que le polynôme $x^2 - r$ s'annule dans $\mathbf{Z}/p\mathbf{Z}$. Si $p \geq 3$ est premier, $x^2 - r$ admet 0 ou 2 racines, il existe donc $\frac{p-1}{2}$ résidus modulo p ; le produit de deux résidus $r = x^2$ et $r' = x'^2$ est un résidu $rr' = (xx')^2$. Le produit d'un résidu par un non-résidu est donc un non-résidu, et le produit de deux non-résidus est un résidu.

Si l'on trouve trois entiers r_1, r_2, r_3 (non carrés parfaits) tels que pour tout nombre premier p, l'un d'entre eux soit résidu quadratique, pour tout p premier le polynôme $(x^2 - r_1)(x^2 - r_2)(x^2 - r_3)$ s'annulera modulo p bien qu'il n'ait pas de racine rationnelle. René Manzoni rappelle que si p est de la forme $4k + 1$ (resp. $8k + 3$,

$8k + 7$), -1 (resp. -2, $+2$) est résidu modulo p. Reste le nombre premier 2 : pour trouver un polynôme qui s'annule modulo tout nombre premier impair et modulo toute puissance de 2, il multiplie $(x^2 + 1)(x^2 + 2)(x^2 - 2)$ par $(x^3 + 3)$. Pierre Samuel écrit, lui, que si $p \equiv 1$ (4), -1 est un carré modulo p ; si $p \equiv 1$ (3), -3 est un carré modulo p, et si $p \equiv -1$ (12), 3 est un carré modulo p. Mais pour que le polynôme convienne également aux nombres premiers 2 et 3, il choisit en définitive : $(x^2 + 1)(x^2 + 3)(x^2 - 3)(6x^2 + x + 4)$.

L'auteur du problème résout astucieusement cette difficulté des « premiers nombres premiers » : en utilisant seulement le fait que le produit de deux non-résidus est un résidu, il constate que, si p est un nombre premier autre que 2 ou 7, soit 2 est résidu modulo p, soit -7 est résidu, soit tous deux sont non-résidus auquel cas leur produit -14 est résidu. Il construit ainsi le polynôme $(x^2 - 2)(x^2 + 7)(x^2 + 14)$ dont l'avantage est que, modulo 7, 2 est résidu ($3^2 \equiv 2 \pmod 7$), mais surtout que $x^2 + 7$ peut être divisible par n'importe quelle puissance de 2 (on a par exemple : $181^2 + 7 = 2^{15}$), ce qui n'est pas le cas de $x^2 + 1$ ni même de $x^2 + 3$. Point n'est besoin d'un facteur supplémentaire pour englober les cas $p = 2$ ou 7.

Ceci nous amène à la seconde partie de la démonstration. Le fait que, pour tout j, il existe un entier x tel que $x^2 + 7$ soit divisible par 2^j se démontre par récurrence sur $j \geq 3$. Si $x^2 + 7 = q\ 2^j$, soit q est pair et $x^2 + 7$ est divisible par 2^{j+1}, soit q et x sont impairs et 2^{j-2} pair, auquel cas

$$(x + 2^{j-1})^2 + 7 = (x^2 + 7) + 2^J\, x + 2^{2j-2} = (q + x + 2^{j-2})\ 2^j$$

est divisible par 2^{j+1}. Mais la récurrence ne peut commencer qu'à $j = 3$: $1^2 + 7 = 8$, alors que $x^2 + 3$ ou, *a fortiori*, $x^2 + 1$ n'est jamais divisible par 8. C'est ce qui conduit René Manzoni à introduire le facteur $x^3 + 3$: la même démonstration par récurrence prouve qu'il peut être divisible par n'importe quel 2^J, si ce n'est que pour $x^3 + 3$, la récurrence peut démarrer à $j = 1$.

Pierre Samuel énonce à ce sujet un lemme très général : si un polynôme $P(x)$ à coefficients entiers admet une racine simple a modulo p ($P'(a)$ non divisible par p), il admet, pour tout exposant j, une racine simple a_j modulo p^j ($P'(a_j)$ non divisible par p). Récurrence similaire à celle ci-dessus : pour tout polynôme P à coefficients entiers, $P(x + y) = P(x) + y\ P'(x) + y^2\ S(x,y)$ où $S(x,y)$ est un polynôme à coefficients entiers. Donc si $P(a_j) = bp^j$, $P(a_j + sp^j) \equiv (b + sP'(a_j))p^j \pmod{p^{2j}}$: $P'(a_j)$ étant inversible modulo p, il existe s tel que $b + sP'(a_j)$ soit divisible par p, donc $P(a_j + sp^j)$ par p^{j+1}. On pose alors $a_{j+1} = a_j + sp^j$, et comme $a_{j+1} \equiv a_j \pmod p$, $P'(a_{j+1}) \equiv P'(a_j) \pmod p$, donc $P'(a_{j+1})$ n'est pas divisible par p. Lorsque $p = 2$, ce lemme ne s'applique pas à $x^2 + 1$, ni même à $x^2 + 7$, qui admettent 1 pour racine double: $P'(1) \equiv 0 \pmod 2$, mais il s'applique à $x^3 + 3$. Lorsque $p = 2$ ou $p = 3$, il s'applique à $6x^2 + x + 4$. Lorsque $p \neq 2$, il s'applique à $x^2 - 2$ (resp. $x^2 + 7$, $x^2 + 14$, $x^2 + 1$, $x^2 + 2$, $x^2 + 3$, $x^2 - 3$) si 2 (resp. -7, -14, -1, -2, -3, $+3$) est résidu, ce qui achève la seconde partie des trois démonstrations ci-dessus.

La troisième partie repose sur le lemme chinois. Si $n = p_1^{j_1} p_2^{j_2} \ldots p_k^{j_k}$, alors il existe a_1, a_2, …, a_k tels que $P(a_1)$, $P(a_2)$, …, $P(a_k)$ soient divisibles respectivement

par $p_1^{j_1}$, $p_2^{j_2}$, …, $p_k^{j_k}$. Mais comme $p_1^{j_1}$, $p_2^{j_2}$, …, $p_k^{j_k}$ sont deux à deux premiers entre eux, il existe un entier m tel que $m \equiv a_1 \pmod{p_1^{j_1}}$, $m \equiv a_2 \pmod{p_2^{j_2}}$, …, $m \equiv a_k \pmod{p_k^{j_k}}$, ce qui prouve que P($m$) est divisible par $p_1^{j_1}$, $p_2^{j_2}$, …, $p_k^{j_k}$, donc par n, leur PPCM.

L'auteur proposait même un exemple numérique pour $n = 1998 = 2 \times 3^3 \times 37$ (le problème était posé en 1999, mais 1999 était un nombre premier !), avec $P(x) = (x^2 - 2)(x^2 + 7)(x^2 + 14)$.

- Modulo 2, $-7 \equiv 1$ est résidu (en fait, P(x) est pair pour tout x).
- Modulo 3, $-14 \equiv 1$ est résidu : $1^2 + 14$ étant divisible par 3, l'un des trois nombres $1^2 + 14$, $4^2 + 14$, $7^2 + 14$ (à savoir $7^2 + 14$) est divisible par 3^2, et l'un des trois nombres $7^2 + 14$, $16^2 + 14$, $25^2 + 14$ (en l'occurrence $16^2 + 14$) est divisible par 3^3.
- Modulo 37, c'est -7 qui est résidu: $17^2 \equiv -7 \pmod{37}$,

Il suffit donc que : $m \equiv 1 \pmod 2$, $m \equiv 16 \pmod{27}$ et $m \equiv 17 \pmod{37}$, soit : $m = 2u + 1 \equiv 16 \pmod{27}$, donc : $u = 27v - 6$, et $m = 54v - 11 \equiv 17 \pmod{37}$, $27v \equiv 14$, $9v \equiv 17$ et $v \equiv 6 \pmod{37}$, donc $v = 37w + 6$ et $m = 1\,998w + 313$. Effectivement P(313) est divisible par 1998. Comme 2003 est lui aussi premier, je me suis intéressé à $n = 2\,002 = 2 \times 7 \times 11 \times 13$: m doit être congru à $\pm 5 \pmod{13}$, $\pm 2 \pmod{11}$, ± 3 ou $0 \pmod 7$, ± 1 ou $0 \pmod 2$, vu le rôle particulier que jouent 2 et 7 dans le polynôme P : $n \equiv 31 \pmod{1\,001}$ convient, mais $n \equiv 112 \pmod{1\,001}$ convient tout autant.

Si l'on remplace la condition « polynôme sans racine rationnelle » par « polynôme sans racine entière », René Manzoni signale l'énoncé 6/249 de Sierpinski, *250 problèmes de théorie élémentaire des nombres*, qui prouve (à l'aide du lemme chinois ci-dessus) que « la congruence $6x^2 + 5x + 1 \equiv 0$ [m] admet des solutions $x \in \mathbf{Z}$ quel que soit m ($m \in \mathbf{N}$) bien que l'équation $6x^2 + 5x + 1 = 0$ n'admette pas de solution $x \in \mathbf{Z}$ ». Avec la condition « polynôme sans racine rationnelle », l'auteur du présent énoncé a trouvé un polynôme solution de degré 6. On peut prouver que, sous cette condition, il n'existe pas de solution du second degré. En effet, considérons un trinôme du second degré $ax^2 + bx + c$. Soit son discriminant $b^2 - 4ac$ est un carré parfait d^2, et le trinôme admet deux racines rationnelles. Soit $b^2 - 4ac = -d^2 < 0$, et un nombre premier $p \equiv 3 \pmod 4$ ne divisant pas d ne peut pas diviser $(2ax + b)^2 + d^2 = 4a(ax^2 + bx + c)$. Soit dans la décomposition en facteurs de $b^2 - 4ac$, l'un au moins des facteurs premiers p admet un exposant impair j : en ce cas, $ax^2 + bx + c$ ne peut pas être divisible par p^{j+1}, sinon $4a(ax^2 + bx + c) + (b^2 - 4ac) = (2ax + b)^2$ serait divisible par p^j et pas par p^{j+1}, ce qui est absurde vu que j est impair.

Maintenant, existe-t-il des polynômes solutions de degré 3, 4 ou 5 ? Avis aux amateurs…