Les problèmes de l'APMEP

Cette rubrique propose des problèmes choisis pour l'originalité de leur caractère : esthétique, subtil, ingénieux voire récréatif, dont la résolution nécessite initiatives, démarche inventive, recherche, effort intellectuel.
Elle accueille tous ceux qui aiment inventer, chercher de « beaux problèmes »… si possible trouver des solutions, et les invite à donner libre cours à leur imagination créatrice. La rubrique s'efforce de rendre compte de la pluralité des méthodes proposées par les lecteurs, des généralisations des problèmes…
Les auteurs sont priés de joindre les solutions aux propositions d'énoncés. Solutions et énoncés sont à envoyer à l'adresse suivante (réponse à des problèmes différents sur feuilles séparées S.V.P., sans oublier votre nom sur chaque feuille) :

François LO JACOMO,
42 quai de la Loire,
75019 Paris.

Solution des problèmes précédents

Énoncé n° 287 (Pierre SAMUEL, 92-Bourg la Reine)

À tout polynôme $P(w) = aw^2 + 2bw + c$ ($a, b, c \in \mathbf{Z}$, $a > 0$, $0 \leq b < a$) on associe l'équation : $x^2 - ay^2 = b^2 - ac$.

1 – Toute équation (E) : $x^2 - ay^2 = k$ ($a, k \in \mathbf{Z}$, $a > 0$) est-elle associée à des polynômes $P(w)$ et à combien (commencer par le cas où a est premier avec k) ?

2 – Quelles relations y a-t-il entre les solutions entières (x, y) de (E) et les valeurs carrées $y^2 = P(w)$ ($y, w \in Z$) des polynômes qui lui sont associés ?

3 – Y a-t-il unicité du polynôme $P(w)$ et de l'entier w (tel que $y^2 = P(w)$) fournissant une solution entière donnée (x, y) de (E) ?

Donner des exemples :

a) où k est un carré modulo a, mais où (E) n'a pas de solutions entières ;

b) où tous les polynômes auxquels (E) est associée fournissent des solutions entières de (E) ;

c) où ces solutions ne proviennent que de certains de ces polynômes.

SOLUTION

« L'idée de cet énoncé m'est venue via la remarque suivante : si le polynôme P prend une valeur $y^2 = P(w)$ qui est un carré parfait, on a

$$(aw + b)^2 - a(aw^2 + 2bw + c) = b^2 - ac,$$

d'où une solution entière $(aw + b, y)$ de $x^2 - ay^2 = b^2 - ac$ » écrit Pierre Samuel. Mais combien de solutions de l'équation de Pell-Fermat (élargie à des valeurs quelconques de a et k) trouve-t-on ainsi ?

J'ai reçu des réponses de Marie-Laure CHAILLOUT (95-Sarcelles), René MANZONI (76-Le Havre) et Pierre RENFER (67-Ostwald), outre la solution de Pierre SAMUEL.

Par définition, l'équation $x^2 - ay^2 = k$ est associée à des polynômes P(w) si et seulement si il existe b et c tels que $k = b^2 - ac$, ce qui entraîne : $b^2 \equiv k \pmod a$. Si k n'est pas un carré modulo a, l'équation n'est associée à aucun polynôme, mais dans ce cas l'équation n'admet pas de solution, car toute solution (x, y) de $x^2 - ay^2 = k$ vérifie $x^2 \equiv k \pmod a$. Si k est un carré modulo a, il existe $b \in \{0, 1, \ldots, a-1\}$ tel que $b^2 \equiv k \pmod a$, ce qui signifie qu'il existe c vérifiant $b^2 = ac + k$. Toute équation admettant des solutions est associée à un ou des polynôme P(w).

Dénombrer les polynômes P(w) associés à une équation donnée équivaut donc à dénombrer les entiers $b \in \{0, 1, \ldots, a-1\}$ tels que $b^2 \equiv k \pmod a$: désormais, a et k seront supposés fixés, k étant un carré modulo a (on supposera k non nul), et on notera $P_b(w)$ le polynôme $aw^2 + 2bw + c$, où $b^2 = ac + k$.

Sachant qu'il existe au moins un entier $b \in \{0, 1, \ldots, a-1\}$ tel que $b^2 \equiv k \pmod a$, pour qu'il en existe un autre, b', il faut et il suffit que $b^2 - b'^2$ soit divisible par a. Or $b^2 - b'^2 = (b - b')(b + b')$: si b' est distinct de b, $b - b'$ ne peut pas être divisible par a car b et b' appartiennent tous deux, par hypothèse, à $\{0, \ldots, a-1\}$. Par contre, si $b \neq 0$, $b + b'$ peut être égal à a, donc divisible par a : si $b^2 = ac + k$, $(a - b)^2 = a(a - 2b + c) + k$, donc $P_{a-b}(w) = aw^2 + 2(a - b)w + (a - 2b + c)$ est associé à la même équation (E) que $P_b(w)$. Remarquons que ce polynôme prend les mêmes valeurs que $P_b(w) = aw^2 + 2bw + c$: pour tout w, $P_{a-b}(w) = P_b(-1 - w)$.

Mais pour que a divise $(b - b')(b + b')$, il n'est pas nécessaire que a soit égal à $(b - b')$ ou à $(b + b')$: il faut et il suffit que, si l'on décompose en facteurs premiers $a = p_1^{n_1} p_2^{n_2} \ldots p_j^{n_j}$, chaque p^n divise $(b - b')(b + b')$.

Pierre Samuel commence par le cas où a est premier avec k. Si p est un facteur premier impair de a, d'exposant n, p ne peut pas diviser simultanément $(b - b')$ et $(b + b')$, sinon il diviserait leur somme $2b$, donc b, donc $k = b^2 - ac$. Dès lors, p^n divise soit $(b - b')$, soit $(b + b')$, ce qui signifie que b' est congru soit à b soit à $-b$ modulo p^n. Si $p = 2$, b et b' sont tous deux impairs car $k = b^2 - ac = b'^2 - ac'$ est premier avec a, donc impair. L'un des facteurs $(b - b')$ ou $(b + b')$ est non multiple de 4, vu que leur somme $2b$ est non multiple de 4 : l'autre doit être multiple de 2^{n-1} pour que $(b - b')(b + b')$ soit multiple de 2^n. Donc b' doit être congru soit à b soit à $-b$ modulo 2^{n-1} : si $n = 1$, b' doit être congru à 1 modulo 2, si $n = 2$, b' congru à 1 ou -1 modulo 4 et si $n \geq 3$, b' congru à b, $-b$, $b + 2^{n-1}$ ou $-b + 2^{n-1}$ modulo 2^n. Comme, d'après le lemme chinois, chaque famille de congruences : $b' \equiv b'_1 \pmod{p_1^{n_1}}$, $b' \equiv b'_2 \pmod{p_2^{n_2}}$, …, $b' \equiv b'_j \pmod{p_j^{n_j}}$ a une et une seule solution modulo $a = p_1^{n_1} p_2^{n_2} \ldots p_j^{n_j}$, le nombre de solutions de $b'^2 \equiv b^2 \pmod a$ vaut : $2^{j+j'}$, j étant le nombre de facteurs premiers de a et $j' = -1$ si a est multiple de 2 et non de 4, $j' = +1$ si a est multiple de 8, $j' = 0$ sinon.

Si maintenant a et k ne sont pas premiers entre eux, appelons d leur PGCD. Dans le cas où d n'est divisible par aucun carré parfait, pour chaque b tel que $b^2 \equiv k \pmod a$, d divise $b^2 = ac + k$, donc d divise b puisqu'il est sans facteur carré. En posant $b = db_1$, $a = da_1$ et $k = dk_1$, on a : $db_1^2 = a_1c + k_1 \equiv k_1 \pmod{a_1}$. Comme k_1 est premier avec a_1, d doit l'être également : il existe d_1 tel que $dd_1 \equiv 1 \pmod{a_1}$. D'où $b_1^2 \equiv d_1k_1 \pmod{a_1}$, avec d_1k_1 et a_1 premiers entre eux, ce qui nous ramène au cas précédent : le nombre de solutions de $b_1^2 \equiv d_1k_1 \pmod{a_1}$, vaut : $2^{j+j'}$, j étant le nombre de facteurs premiers de $a_1 = \dfrac{a}{d}$ et $j' = -1$ si a_1 multiple de 2 et non de 4, $+1$ si a_1 multiple de 8, 0 sinon. Et à chacune de ces solution b_1 (vérifiant $0 \leq b_1 < a_1$) correspond une et une seule solution b de l'équation initiale : $b^2 \equiv k \pmod a$ telle que $0 \leq b = db_1 < a = da_1$.

Reste le cas où $d = \text{PGCD}(a, k)$ est divisible par un carré parfait. Soit q^2 le plus grand carré divisant d. Pour chaque b tel que $b^2 \equiv k \pmod a$, q^2 divise $b^2 = ac + k$, donc q divise b. On pose, cette fois-ci, $b = qb_2$, mais $a = q^2a_2$ et $k = q^2k_2$, ce qui donne : $b_2^2 \equiv k_2 \pmod{a_1}$. Le PGCD de a_2 et k_2 n'étant divisible par aucun carré parfait, nous sommes ramenés au cas précédent, si ce n'est qu'à chaque solution b_2 vérifiant $0 \leq b_2 < a_2$ correspondent q solutions distinctes de l'équation initiale : $b^2 \equiv k \pmod a$, telles que $0 \leq b \equiv qb_2 \pmod{qa_2} < a = q^2a_2$. Pierre Samuel prend pour exemple $a = 75$, $k = 1\,150$: $q = 5$, $a_2 = 3$ et $k_2 = 46$. Il existe deux solutions de $b_2^2 \equiv 46 \pmod 3$ vérifiant $0 \leq b_2 < 3 = a_2$, à savoir 1 et 2, mais il existe 10 solutions correspondantes $b \equiv 5$ ou $10 \pmod{15}$ vérifiant : $0 \leq b < 75$, et chacune d'elles vérifie $b^2 \equiv k \pmod a$.

La solution de Pierre Renfer est voisine de celle de Pierre Samuel, mais rédigée en des termes plus savants. Il commence par : a nombre primaire (puissance d'un nombre premier), et s'intéresse au passage à : $k = 0$, qui n'était pas exclu par l'énoncé. Marie-Laure Chaillout a exploré une autre piste : si a et k sont premiers entre eux et a impair, le fait que $b^2 \equiv b'^2 \equiv k \pmod a$, donc $(b - b')(b + b') = am$, permet de trouver d_1 et d_2 premiers entre eux, m_1 et m_2, tels que : $a = d_1d_2$, $m = m_1m_2$, $b - b' = d_1m_1$, $b + b' = d_2m_2$. Si un autre b'' vérifiant $b^2 \equiv b''^2$ est associé au même couple (d_1, d_2), donc si $b - b'' = d_1m_1'$, $b + b'' = d_2m_2'$, on a : $b' - b'' = d_1(m_1' - m_1) = d_2(m_2 - m_2')$. Comme d_2 est premier avec d_1, d_2 divise $(m_1' - m_1)$, donc $d_1d_2 = a$ divise $b' - b''$, ce qui entraîne $b' = b''$ puisque tous deux appartiennent à $\{0, \ldots, a - 1\}$. Le nombre de solutions distinctes de $b'^2 \equiv b^2 \pmod a$ est donc au plus égal au nombre de décompositions : $a = d_1d_2$ avec d_1 et d_2 premiers entre eux. Et il est au moins égal à ce même nombre, car quels que soient d_1 et d_2 premiers entre eux, d'après Bézout, il existe un et un seul couple (m_1, m_2) tel que $2b = d_1m_1 + d_2m_2$, avec $b - a < d_1m_1 \leq b$. Mais généraliser cette méthode au cas général exige des précautions : d'une part, notamment lorsque a est multiple de 8 et k impair, les d_1 et d_2 déterminés par $b - b' = d_1m_1$, $b + b' = d_2m_2$ ne sont pas

nécessairement premiers entre eux. D'autre part, lorsque a et k admettent un PGCD d, les solutions b de $b^2 \equiv k \pmod a$ ne sont pas nécessairement divisibles par d.

Les questions suivantes sont plus immédiates. Comme

$$(aw + b)^2 - a(aw^2 + 2bw + c) = b^2 - ac,$$

si $k = b^2 - ac$, toute valeur carrée $y^2 = \mathrm{P}_b(w)$ fournit une solution (x, y) de (E) : $x^2 - ay^2 = k$, en posant $x = aw + b$. Réciproquement, pour toute solution (x, y) de (E), il existe un et un seul b tel que $0 \leq b < a$ et $x \equiv b \pmod a$. Si l'on pose $x = aw + b$, on a : $y^2 = \mathrm{P}_b(w)$, donc à toute solution de (E) on peut faire correspondre une valeur carrée d'un polynôme associé.

L'unicité du polynôme $\mathrm{P}(w)$ doit se comprendre ainsi : (x, y) étant une solution de (E) : $x^2 - ay^2 = k$, existe-t-il un seul polynôme P_b et un seul entier w tels que $y^2 = \mathrm{P}_b(w)$? À cette question, la réponse est clairement non, puisqu'on a vu au début que $\mathrm{P}_b(w) = \mathrm{P}_{a-b}(-1 - w)$. Mais par le procédé ci-dessus, $y^2 = \mathrm{P}_{a-b}(-1 - w)$ est associé à la solution $(-x, y)$, que l'on pourrait considérer distincte de (x, y). Quoi qu'il en soit, il n'en existe pas d'autre : si $\mathrm{P}_b(w) = \mathrm{P}_{b'}(w')$,

$$(aw + b)^2 = a\mathrm{P}_b(w) + k = = a\mathrm{P}_{b'}(w') + k = (aw' + b')^2,$$

ce qui entraîne soit $aw + b = aw' + b'$, donc $b - b' = a(w' - w) = 0$, soit $aw + b = -(aw' + b')$, donc $b + b' = -a(w + w') = a$ (ou 0 si $b = b' = 0$).

Quant aux exemples, chacun fournit les siens. Comme exemple où k est un carré modulo a, mais où (E) n'a pas de solution entière, Pierre Renfer propose : $x^2 - 2y^2 = 3$. 3 est un carré modulo 2, l'équation est bien associée à un polynôme : $\mathrm{P}_1(w) = 2w^2 + 2w - 1$, mais elle n'a pas de solution : x^2 et y^2 étant toujours congrus à 0 ou 1 modulo 3, pour que $x^2 - 2y^2$ soit divisible par 3 il faut que x^2 et y^2 soient tous deux divisibles par 3, donc par 9, auquel cas $x^2 - 2y^2$ est divisible par 9. Donc $2w^2 + 2w - 1$ ne prend pas de valeurs carrées : d'ailleurs il est congru soit à 2 modulo 3, soit à 3 modulo 36. Sur le même modèle (modulo 7), Pierre Samuel propose : $x^2 - 13y^2 = 14$. Marie-Laure Chaillout choisit : $x^2 - 3y^2 = 7$ (modulo 4, $x^2 - 3y^2 \equiv 0$, 1 ou 2) et René Manzoni : $x^2 - 3y^2 = 39$ (x serait divisible par 3 et $y^2 \equiv 2$ modulo 3).

Comme exemples où tous les polynômes auxquels (E) est associée fournissent des solutions entières de (E), Pierre Renfer et René Manzoni proposent : $x^2 - 3y^2 = 1$, dont les solutions, classiquement, sont les $(\pm x_n, \pm y_n)$ avec $x_n + y_n\sqrt{3} = \left(2 + \sqrt{3}\right)^n$. L'équation est associée à : $\mathrm{P}_1(w) = 3w^2 + 2w$ et $\mathrm{P}_2(w) = 3w^2 + 4w + 1$. Si n est pair, $x_n \equiv 1 \pmod 3$ donc la solution est fournie par $\mathrm{P}_1(w)$; n est impair, $x_n \equiv 2 \pmod 3$ et la solution est fournie par $\mathrm{P}_2(w)$. Sous réserve que P_1 et P_2 prennent les mêmes valeurs… Marie-Laure Chaillout et René Manzoni proposent : $x^2 - 15y^2 = 34$, associée à quatre polynômes, et qui admet pour solutions, entre autres, (7, 1) associée à $\mathrm{P}_7(w) = 15w^2 + 14w + 1$ et $\mathrm{P}_8(w) = 15w^2 + 16w + 2$: $1 = \mathrm{P}_7(0) = \mathrm{P}_8(-1)$, ainsi que (13, 3) associée à $\mathrm{P}_{13}(w) = 15w^2 + 26w + 9$ et $\mathrm{P}_2(w) = 15w^2 + 4w - 2$: $9 = \mathrm{P}_{13}(0) = \mathrm{P}_2(-1)$. Enfin, Pierre Samuel choisit $x^2 - 105y^2 = 184$, associée à huit polynômes, dont les quatre solutions (17, 1), (53, 5), (73, 7) et (277, 27) correspondent respectivement à $\mathrm{P}_{17}(0) = \mathrm{P}_{88}(-1)$, $\mathrm{P}_{53}(0) = \mathrm{P}_{52}(-1)$, $\mathrm{P}_{73}(0) = \mathrm{P}_{32}(-1)$ et $\mathrm{P}_{67}(2) = \mathrm{P}_{38}(-3)$.

Détaillons davantage l'autre exemple de Pierre Samuel $x^2 - 160y^2 = 9$. $160 = 2^5 \cdot 5$, et $b = 3$ est une racine évidente de $b^2 \equiv 9$ (mod. 160). Les autres racines sont donc congrues à ±3 (mod 5), ±3 ou ±19 (mod 32), ce qui donne : 3, 13, 67, 77, 83, 93, 147 et 157. Les solutions (3, 0) et (13, 1) de (E) sont associées à $P_3(0) = P_{157}(-1)$ et $P_{13}(0) = P_{147}(-1)$. Le polynôme $P_{67}(w) = 160w^2 + 134w + 28$, lui, prend pour valeur carrée $P_{67}(-2) = 20^2$, ce qui conduit à la solution (277, 20) de l'équation diophantienne (E). Or $277 + 20\sqrt{160}$ est divisible par $13 - \sqrt{160}$:

$$\frac{277 + 20\sqrt{160}}{13 - \sqrt{160}} = \frac{\left(277 + 20\sqrt{160}\right)\left(13 + \sqrt{160}\right)}{9} = 721 + 57\sqrt{160},$$

ce qui fournit une unité de l'anneau $\mathbf{Z}\left(\sqrt{160}\right)$ (en fait, $721 + 57\sqrt{160} = \left(3 + \sqrt{10}\right)^4$, $3 + \sqrt{10}$ étant une unité du corps quadratique $\mathbf{Q}\left(\sqrt{160}\right) = \mathbf{Q}\left(\sqrt{10}\right)$, mais pas de l'anneau $\mathbf{Z}\left(\sqrt{160}\right)$, qui n'est pas « intégralement clos »). En multipliant $13 - \sqrt{160}$ par $\left(721 + 57\sqrt{160}\right)^n$, on obtient $x_n + y_n\sqrt{160}$ où (x_n, y_n) est une solution de : $x^2 - 160y^2 = 9$, associée à P_{13} (et P_{147}) pour n pair, à P_{67} (et P_{93}) pour n impair. De même, en multipliant 3 par $\left(721 + 57\sqrt{160}\right)^n$, on obtient $x'_n + y'_n\sqrt{160}$, (x'_n, y'_n) parcourant une autre famille de solutions associées à P_3 (et P_{157}) pour n pair, P_{77} (et P_{83}) pour n impair. On trouve ainsi, notamment, la solution (2 163, 171). Tous les polynômes auxquels (E) est associée nous ont fourni des solutions entières de (E).

Quant au dernier cas, Pierre Renfer propose $x^2 - 4y^2 = 16$, associée à deux polynômes : $P_0(w) = 4w^2 - 4$ et $P_2(w) = 4w^2 - 4w - 3$, mais qui possède pour seules solutions (4, 0) et (–4, 0), associées toutes deux à P_0 et non à P_2 qui ne prend que des valeurs impaires. De même, Marie-Laure Chaillout utilise $x^2 - 4y^2 = 28$: $P_0(2) = 3^2$, d'où les solutions (±8, ±3), mais $P_2(w) = 4w^2 + 4w - 6 \equiv 2$ (mod 4) n'est jamais un carré. L'exemple : $x^2 - 9y^2 = 45$, de René Manzoni, se traite de la même manière, mais René Manzoni cite un autre exemple : $x^2 - 12y^2 = 88$ qui, à la différence des précédents, admet une infinité de solutions (par exemple : (10, 1)), toutes associées à $P_2(w) = 12w^2 + 4w - 7$ et $P_{10}(w) = 12w^2 + 20w + 1$. Aucune solution n'est associée à $P_4(w) = 12w^2 + 8w - 6$ ou $P_8(w) = 12w^2 + 16w - 2$, qui, congrus à 2 modulo 4, ne prennent aucune valeur carrée.

Les exemples de Pierre Samuel sont : $x^2 - 105y^2 = 109$ et $x^2 - 120y^2 = 241$. Dans le premier de ces exemples, b peut prendre 8 valeurs : 2, 23, 37, 47 et leurs symétriques par rapport à $\frac{a}{2}$. Les solutions (23, 2) et (103, 10) donnent les restes 23 et 2. La multiplication par l'unité $41 + 4\sqrt{105}$ échange les restes 23 et 2, car $41 \times 2 \equiv -23$ (mod 105). Dès lors, les solutions (x_n, y_n) telles que

$$x_n + y_n\sqrt{105} = \left(\pm 23 \pm 2\sqrt{105}\right)\left(41 + 4\sqrt{105}\right)^n$$

ou telles que

$$x_n + y_n\sqrt{105} = \left(\pm 103 \pm 10\sqrt{105}\right)\left(41 + 4\sqrt{105}\right)^n$$

sont toutes associées à $b = 23$ ou 2 (ou leurs symétriques). Y a-t-il des solutions associées à $b = 37$ ou 47 ? Non, car la multiplication par l'unité $41 + 4\sqrt{105}$ échange aussi les restes 37 et 47. S'il existait une solution (x, y) associée à 37 ou 47, toutes les solutions (x_n, y_n) telles que $x_n + y_n\sqrt{105} = \left(x + y\sqrt{105}\right)\left(41 + 4\sqrt{105}\right)^n$, pour $n \in \mathbf{Z}$, seraient elles aussi associées à 37 ou 47, et parmi elles il y en aurait une vérifiant $0 \leq y < 42$. En effet, à partir d'une solution (x, y), avec x et y positifs, la multiplication : $\left(x + y\sqrt{105}\right)\left(41 - 4\sqrt{105}\right) = (41x - 420y) + (41y - 4x)\sqrt{105}$ nous fournit une solution plus petite : $x' = 41x - 420y > 0$, $y' = 41y - 4x > 0$ si $41x > 420y$ et $41y > 4x$. La première relation est toujours vérifiée puisque $x > y\sqrt{105}$; la seconde l'est si : $(41y)^2 = y^2 + 16(105y^2) = y^2 + 16(x^2 - 109) > (4x)^2$, donc si $y^2 > 16 \times 109$. Comme l'équation (E) n'admet pas d'autre solution que (23, 2) et (103, 10) pour $0 \leq y < 42$, elle n'admet pas de solution associée à 37 ou 47 (ou leurs symétriques), et les polynômes correspondants ne prennent pas de valeur carrée.

De même pour l'autre exemple : $x^2 - 120y^2 = 241$. Les solutions (19, 1) et (89, 8) sont associées aux restes 19, 31 et leurs symétriques, mais les autres restes : 1, 11, 29, 41, 49, 59 et symétriques ne sont associés à aucune solution. À l'aide de l'unité $11 + \sqrt{120}$, on voit que toute solution (x, y) avec $x > 0$, $y \geq 16$ se déduit d'une solution plus petite ; or il n'y a pas d'autre solution pour $0 \leq y < 16$.

On trouve ainsi des polynômes qui ne prennent aucune valeur carrée. Mais cette méthode fournit également des polynômes qui prennent une infinité de valeurs carrées, dans la mesure où, lorsque a n'est pas un carré, l'équation de Pell-Fermat admet généralement une infinité de solutions. Marie-Laure Chaillout cite l'équation : $x^2 - 5y^2 = 4$ dont les polynômes associés, $P_2(w) = 5w^2 + 4w$ et $P_3(w) = 5w^2 + 6w + 1$, prennent nécessairement une infinité de valeurs carrées, tout comme l'équation $x^2 - 5y^2 = -4$, associée à $P_1(w) = 5w^2 + 2w + 1$ et $P_4(w) = 5w^2 + 8w + 4$. D'ailleurs, si F_n désigne le n-ième terme de la suite de Fibonacci ($F_0 = 0$, $F_1 = 1$) : pour $w = (-1)^n F_n^2$,

$$P_2(w) = P_3(-1 - w) = F_{2n}^2,$$

et pour $w = (-1)^n F_n F_{n+1}$,

$$P_1(w) = P_4(-1 - w) = F_{2n+1}^2.$$