Réponses de Maurice Bauval (Versailles), Hélène Brion (Clamart), Raymond Heitz (Lavergne), Pierre Renfer (Saint Georges d'Orques)

Ce problème m'a été inspiré par le sujet du concours général de mathématiques de 2011. Il s'agit du troisième exercice, dans lequel on regarde quelques cas particuliers. J'avais plus ou moins enterré cet énoncé, faute de trouver une réponse complète. Raymond Heitz me relance par courrier au sujet de cet énoncé. Voici donc un point sur ce problème.

On note A l'ensemble des entiers n strictement positifs pour lesquels il existe une application $f : \mathcal{U}_n \to \mathcal{U}_n$ vérifiant $f \circ f(z) = z^2$ pour tout z de $\mathcal{U}_n$. Une telle application f sera dite associée à l'entier n.

1 - Une condition nécessaire et suffisante

Les premiers résultats faciles à obtenir sont les suivants.

Théorème 1

Soit $n \in$ A et f une application associée.

1. Pour tout $z \in \mathcal{U}_n$, $f\left(z^2\right) = f(z)^2$.
2. $f(1) = 1$.
3. L'application f admet un unique point fixe, à savoir 1.

Preuve – Pour le premier point, $f\left(z^2\right) = f\left(f \circ f(z)\right) = (f \circ f)\left(f(z)\right) = \left(f(z)\right)^2$.

Pour le second point, $f(1) = f\left(1^2\right) = f(1)^2$, donc $f(1) = 1$ (car $f(1) \neq 0$).

Pour le dernier point, si $z \in \mathcal{U}_n$ est un point fixe de f, alors $f(z) = z$ donc

$$z^2 = f\left(f(z)\right) = f(z) = z,$$

donc $z = 1$.

Le résultat suivant permet de ramener l'étude aux cas des entiers n impairs.

Théorème 2

Soit $n \in$ A et f une application associée.

1. Si n est pair, $f(-1) = 1$.
2. L'entier n n'est pas divisible par 4.
3. Si n est divisible par 2, alors n est dans A si et seulement si $\dfrac{n}{2}$ est dans A.

Preuve – Si n est pair, -1 est dans $\mathcal{U}_n$ et

$$1 = f(1) = f\left((-1)^2\right) = \left(f(-1)\right)^2.$$

Donc $f(-1)$ vaut 1 ou -1 mais comme f admet un seul point fixe, $f(-1) = 1$.

Pour le second point, on suppose que 4 divise n. Le complexe i est dans $\mathcal{U}_n$. D'après le théorème 1,

$$1 = f(1) = f\left(\mathrm{i}^4\right) = f(\mathrm{i})^4,$$

donc $f(\mathrm{i})$ vaut ± 1 ou $\pm\mathrm{i}$. Mais si $f(\mathrm{i}) = \pm 1$, alors $f \circ f(\mathrm{i}) = f(\pm 1) = 1$, donc $\mathrm{i}^2 = 1$

(exclu). Et si $f(\mathrm{i}) = \pm\mathrm{i}$, alors $f(-1) = f(\mathrm{i}^2) = (f(\mathrm{i}))^2 = (\pm\mathrm{i})^2 = -1$ et l'application f aurait un second point fixe (exclu également).
Pour le dernier point, on suppose que n est pair (mais non divisible par 4). On pose $n = 2m$ avec m impair.
✧ Pour le sens indirect, si m est dans A, soit g associée. On remarque que pour $z \in \mathcal{U}_n$, un et un seul des deux complexes z ou $-z$ est dans $\mathcal{U}_m$. En effet, par imparité de m,

$$0 = 1 - z^n = 1 - z^{2m} = (1 - z^m)(1 + z^m) = (1 - z^m)(1 - (-z)^m).$$

Donc $z^m = 1$ ou $(-z)^m = 1$. Les deux ne peuvent être vrais, par imparité de m. On définit alors une application $f : \mathcal{U}_n \to \mathcal{U}_n$ ainsi : si z est dans $\mathcal{U}_n$, on pose

$$f(z) = \begin{cases} g(z) & \text{si } z \in \mathcal{U}_m \\ g(-z) & \text{si } -z \in \mathcal{U}_m \end{cases}$$

Dans tous les cas, $f(z) = g(z)$ est dans $\mathcal{U}_m$, donc

$$f(f(z)) = g(g(\pm z)) = (\pm z)^2 = z^2.$$

Ainsi, l'application f est associée à n, ce qui prouve que n appartient a A.
✧ Dans le sens direct, si n est dans A et f lui est asociée, alors $f(\mathcal{U}_m) \subset \mathcal{U}_m$. En effet, les éléments de $\mathcal{U}_m$ sont les carrés de $\mathcal{U}_n$. Donc pour $z \in \mathcal{U}_m$, prenons $\omega \in \mathcal{U}_n$ tel que $z = \omega^2$. Alors $f(z) = f(\omega^2) = (f(\omega))^2$, qui est dans $\mathcal{U}_m$. On peut dès lors considérer l'application g, restriction de f à $\mathcal{U}_m$. Elle est clairement associée à m, ce qui prouve que m est dans A.

Il s'agit maintenant de savoir quels sont les entiers n impairs dans A. Les résultats suivants fournissent un algorithme pour répondre a cette question.

Théorème 3
Soit n un entier impair. L'application $z \mapsto z^2$ est une permutation de $\mathcal{U}_n$.

Preuve – Si $n = 2p + 1$, l'application $z \mapsto z^{p+1}$ est la réciproque de $z \mapsto z^2$.

Théorème 4
Soit σ une permutation d'un ensemble fini E. Il existe une permutation τ de E telle que $\sigma = \tau \circ \tau$ si et seulement dans la décomposition de σ en produit de cycles à supports disjoints, pour tout entier N pair, le nombre de cycles de longueur N est pair.

Preuve – On suppose que $\sigma = \tau \circ \tau$, et l'on regarde l'orbite d'un élément $a \in$ E sous l'action de τ : $\{a, \tau(a), \cdots, \tau^{p-1}(a)\}$ avec $\tau^p(a) = a$ et p minimal.
✧ Si p est impair ($p = 2k + 1$), l'orbite de a sous $\tau \circ \tau$ est

$$\{a, \tau^2(a), \cdots, \tau^{2k}(a), \tau^{2k+2}(a) = \tau(a), \tau^3(a), \cdots\}.$$

L'orbite de a sous $\tau \circ \tau$ possède les mêmes éléments que l'orbite de a sous τ, obtenus dans un ordre différent.

✧ En revanche, si p est pair ($p = 2k$), l'orbite de a sous $\tau \circ \tau$ est formée de a, $\tau^2(a)$, … , $\tau^{2k-2}(a)$, puis on retombe sur $\tau^{2k}(a) = a$. On obtient deux fois moins d'éléments. La deuxième partie de l'orbite donne $\tau(a)$, $\tau^3(a)$, … , $\tau^{2k-1}(a)$, puis on retombe sur $\tau^{2k+1}(a) = \tau^2(a)$.

Les orbites sous l'action de $\tau \circ \tau$ sont donc de deux types : celles de longueur impaire et celles de longueur paire mais ces dernières vont par couple de même longueur, car elles proviennent d'une orbite sous τ « coupée » en deux par $\tau \circ \tau$. D'où la condition nécessaire pour que σ s'écrive $\tau \circ \tau$: les orbites de longueurs paires doivent aller par couple.

Cette condition est suffisante : si a a des orbites de longueur paire qui vont par couple, construisons τ telle que $\tau \circ \tau = \sigma$. Partant d'un couple de deux orbites de longueur $2k$, on crée une orbite sous τ en alternant un terme d'une orbite, un de l'autre orbite. Ensuite, pour une orbite $\left\{a, \sigma(a), \sigma^2(a), \cdots, \sigma^{2k}(a)\right\}$ de longueur impaire $2k+1$, on réordonne τ de la façon suivante $\left\{a, \sigma^{k+1}(a), \sigma^2(a), \sigma^{k+2}(a), \cdots\right\}$. L'application τ ainsi construite est bijective et vérifie $\tau \circ \tau = \sigma$.

Voici un exemple avec E = [1, 16] et σ donnée par

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\sigma(n)$	2	4	5	8	9	10	11	13	15	12	14	16	1	7	3	6

Dans σ, il y a deux orbites de longueur impaire : O(1) = {1, 2, 4, 8, 13} et O(7) = {7, 11, 14}. Et il y deux orbites de longeur 4, que l'on va regrouper :
O(3) = {3, 5, 9, 15}, O(6) = {6, 10, 12, 16}.
Avec l'orbite de 1, on fabrique le cycle (1, 8, 2, 13, 4), avec l'orbite de 7, le cycle (7, 14, 11). Avec les orbites de 3 et 6, on fabrique le cycle (3, 6, 5, 10, 9, 12, 15, 16).
On peut donc prendre pour τ l'application suivante :

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\sigma(n)$	8	13	6	1	10	5	14	2	12	9	7	15	4	11	16	3

On vérifie sans problème que $\tau \circ \tau = \sigma$.

Afin de rendre automatisable le théorème précédent, il est préférable de travailler avec $\mathbb{Z}/n\mathbb{Z}$ plutôt que $\mathcal{U}_n$. Pour alléger la rédaction, on note k un élément de $\mathbb{Z}/n\mathbb{Z}$ au lieu de k mod n. Parfois, k sera aussi un des représentants dans $\mathbb{Z}$ de la classe k mod n, l'abus de notation ne prêtant pas à confusion.

Théorème 5

L'entier n est dans A si et seulement si il existe $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ telle que $f\left(f\left(k\right)\right) = 2k$ pour tout $k \in \mathbb{Z}/n\mathbb{Z}$.

Preuve – On utilise la bijection $k \in \mathbb{Z}/n\mathbb{Z} \mapsto \exp(2ik/n) \in \mathcal{U}_n$.

Par la suite, l'application f désignera l'application sur $\mathbb{Z}/n\mathbb{Z}$ plutôt que sur $\mathcal{U}_n$. Pour savoir si n est dans A, il faut (et il suffit de) vérifier si $\sigma : k \in \mathbb{Z}/n\mathbb{Z} \mapsto 2k$ donne des orbites de longueurs paires allant par couples.

Prenons $n = 7$. Les orbites de $\sigma : k \in \mathbb{Z}/n\mathbb{Z} \mapsto 2k$ sont O(0) = {0}, O(1) = {1, 2, 4}

et O(3) = {3, 6, 5}. Il n'y a pas d'orbite de longeur paire donc σ s'écrit $f \circ f$ et 7 appartient à A.
Prenons $n = 13$. Les orbites sont {0} et O(1) = {1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7}. Il y a une seule orbite de longeur 12. Donc 13 n'appartient pas à A.

2 - Une condition suffisante

On trouve facilement une infinité d'éléments de A. Des tests informatiques semblent indiquer que « la plupart » des éléments de A sont obtenus ainsi.

Théorème 6

Soit $n \in \mathbb{N}^*$. Si l'équation $\alpha^2 = 2$ admet une solution dans $\mathbb{Z}/n\mathbb{Z}$, alors n appartient à A.

Preuve – On applique le théorème 5 avec $f : k \in \mathbb{Z}/n\mathbb{Z} \mapsto \alpha k$.

On retrouve ainsi que 7 est dans A puisque $3^2 \equiv 2 \bmod 7$.

Ce théorème précédent ne caractérise pas les éléments de A. En effet, 2 n'est pas un carré modulo $n = 37 \times 109 = 4033$, pourtant n est dans A. De même pour $n = 1093^2 = 1194649$. Cette question a donné lieu a une jolie séance d'informatique il y a deux ans avec mes étudiants. Il fallait trouver des entiers n appartenant à A mais tels que 2 ne soit pas un carré modulo n. **Jean Bruant** et **Raphaël Berthon** ont obtenu de grandes valeurs de n.

Dans la lignée de ce théorème, on peut prolonger l'étude arithmétique. Par exemple, on sait décrire les entiers n tels que 2 soit un carré modulo n.

Théorème 7

1. Soit m et n deux entiers premiers entre eux, impairs. Alors 2 est un carré modulo mn si et seulement si 2 est un carré modulo m et modulo n.
2. Soit p un nombre premier impair et $\alpha \in \mathbb{N}^*$. Alors 2 est un carré modulo p si et seulement si c'est un carre modulo p^α.

Preuve – Le premier point résulte du théorème des restes chinois. Le second se montre par récurrence sur α.

Théorème 8

Soit un entier n impair. Alors 2 est un carré modulo n si et seulement si les facteurs premiers de n sont congrus à ±1 modulo 8.

3 - Propriétés arithmétiques des éléments de A

Voici pour finir quelques propriétés arithmétiques.

Théorème 9

Si $n_1, n_2 \in$ A sont premiers entre eux, alors $n_1 n_2$ reste dans A.

Preuve – On suppose n_1 et n_2 dans A. Il existe donc deux applications $f_i : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ telles que $f_i \circ f_i(x_i) = 2x_i$.

On pose

$$g : (x_1, x_2) \in \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \to (f_1(x_1), f_2(x_2)) \in \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

Soit l'isomorphisme d'anneaux

$$h : \mathbb{Z}/n_1n_2\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

On définit

$$f = h^{-1} \circ g \circ h : \mathbb{Z}/n_1n_2\mathbb{Z} \to \mathbb{Z}/n_1n_2\mathbb{Z}.$$

Soit $x \in \mathbb{Z}/n_1n_2\mathbb{Z}$. On vérifie que $f \circ f(x) = 2x$. En posant $h(x) = (x_1, x_2)$,

$$f \circ f(x) = h^{-1} \circ g^2(h(x)) = h^{-1} \circ g^2(x_1, x_2) = h^{-1}(f_1^2(x_1), f_2^2(x_2)).$$

Mais par définition de f_1 et f_2, puis en utilisant le morphisme d'anneaux h^{-1},

$$f \circ f(x) = h^{-1}(2x_1, 2x_2) = 2h^{-1}(x_1, x_2) = 2x.$$

La réciproque est fausse : voir dans les exemples le cas où $n_1 = 37$ et $n_2 = 109$

Hélène Brion pousse un peu plus loin l'étude. Pour $n \in \mathbb{N}^*$, on note $\omega_n(2)$ l'ordre de 2 dans $\mathbb{Z}/n\mathbb{Z}$. On montre alors le résultat suivant :

1. Si n est un nombre premier impair, l'ensemble $\mathbb{Z}/n\mathbb{Z} - \{0\}$ se partitionne sous l'action de l'application $\sigma : k \mapsto 2k$ en $\dfrac{n-1}{\omega_n(2)}$ orbites, toutes de cardinal $\omega_n(2)$. Ainsi,

(a) $\dfrac{n-1}{\omega_n(2)}$ est impair, comme $\omega_n(2)$ est pair, une application f telle que $f \circ f = \sigma$ ne peut exister. Donc n n'appartient pas à A.

(b) si $\dfrac{n-1}{\omega_n(2)}$ est pair, alors n appartient a A.

2. Si n est la puissance k-ième d'un nombre premier impair p, l'ensemble $\mathbb{Z}/n\mathbb{Z} - \{0\}$ se partitionne sous l'action de l'application : $\sigma : k \mapsto 2k$ en $\dfrac{p-1}{\omega_n(2)}$ orbites de longueur $\omega_n(2) \times p$, $\dfrac{p-1}{\omega_n(2)}$ orbites de longueur $\omega_n(2) \times p^2$, … , $\dfrac{p-1}{\omega_n(2)}$ orbites de longueur $\omega_n(2) \times p^{k-1}$. Ainsi, n appartient à A si et seulement si $\dfrac{p-1}{\omega_n(2)}$ est pair.

Hélène Brion creuse encore un peu l'étude des orbites et conclut en donnant des exemples. Par exemple, pour $n = 49 = 7^2$, c'est-à-dire pour $p = 7$ et $k = 2$, on trouve que $\omega_7(2) = 3$, donc $\dfrac{p-1}{\omega_n(2)} = \dfrac{6}{3} = 2$, qui est pair. Donc 49 est dans A.

Pour d'autres compléments, la RMS a également publié un texte autour de ce problème dans son numéro 125.1.