DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Cours et exercices

AUTEUR : Louis NEBOUT
STAGE : Montpellier 2013

Propriétés de $\mathbb{Z}/n\mathbb{Z}$

Le but de cette séance est de vous introduire au point du vue moderne sur l'arithmétique, issu de l'algèbre. Rien de ceci n'est officiellement au programme des olympiades, pourtant une bonne connaissance de cette théorie permet de mieux comprendre ce qui se passe, et de prouver quelques résultats très puissants.

- $\mathbb{Z}/n\mathbb{Z}$ -

Soit $n \geqslant 2$ un entier naturel. Quelle est précisement la nature de la formule $a \equiv b\,[n]$? Ce n'est pas une vraie égalité : cela veut dire qu'il existe une certaine relation d'équivalence, la relation de congruence, pour laquelle a et b sont en relation. Maintenant, si $a \equiv b\,[n]$ et $c \equiv d\,[n]$, on sait bien que $a + c \equiv b + d\,[n]$, et de même avec la multiplication. Ainsi, cette relation possède en fait des propriétés tout à fait similaires à l'égalité, et on aimerait bien dire que « on peut additionner et multiplier les modulo », mais cette phrase n'a aucun sens mathématique. Pour lui donner du sens, on aimerait bien la « transformer » en une véritable égalité, en « faisant de deux entiers congrus modulo n un seul et même nombre ».

Si x est un entier, on appelle *classe d'équivalence de* x *modulo* n l'ensemble des entiers congrus à x modulo n. On note $\overline{x}$ la classe de x. Attention, si $x \equiv y \mod n$, alors $\overline{x}$ et $\overline{y}$ sont deux notations pour un seul et même objet. On obtient exactement n classes d'équivalence : $\overline{0}$, $\overline{1}$, …, $\overline{n-1}$, et on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de ces classes d'équivalence. On munit $\mathbb{Z}/n\mathbb{Z}$ de deux opérations $+$ et $\times$ en posant $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \times \overline{y} = \overline{x \times y}$. Il y a une subtilité : il faut prouver que ces opérations sont bien définies, c'est-à-dire que les résultats de ces opérations ne dépendent pas des choix des représentants x et y de $\overline{x}$ et $\overline{y}$,

par exemple pour $+$, que si $\overline{x} = \overline{x'}$ at $\overline{y} = \overline{y'}$, alors $\overline{x+y} = \overline{x'+y'}$: c'est une simple reformulation du fait que la relation de congruence est compatible avec les opérations.

La construction de $\mathbb{Z}/n\mathbb{Z}$ peut paraître conceptuellement difficile la première fois qu'on la voit, mais en fait, la manipulation de cet ensemble est très simple en pratique : écrire $\overline{x} + \overline{y} = \overline{z}$ est rigoureusement équivalent à écrire $x + y \equiv z \mod n$, par exemple. Pour passer d'une écriture à l'autre, on enlève les barres et on remplace l'égalité par une relation de congruence. Mais l'énorme avantage conceptuel de l'utilisation de $\mathbb{Z}/n\mathbb{Z}$ est, dans le cas de $\mathbb{Z}/5\mathbb{Z}$ par exemple, le fait que $\overline{2}$ et $\overline{7}$ sont *un seul et même nombre*, et non plus simplement congrus. De plus, $\mathbb{Z}/n\mathbb{Z}$ possède une certaine structure algébrique, qui nous permet de réaliser toutes nos opérations en restant à l'intérieur de $\mathbb{Z}/n\mathbb{Z}$, et donc sans avoir à repasser par les entiers.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est donc muni de deux opérations, une addition et une multiplication, toutes deux commutatives et associatives, et telles que

- La loi $+$ admet un élément neutre, $\overline{0}$, tel que pour tout $x \in \mathbb{Z}/n\mathbb{Z}$, $x+\overline{0} = x$;
- Tout élément x de $\mathbb{Z}/n\mathbb{Z}$ admet un opposé noté $-x$, tel que $x + (-x) = \overline{0}$ (celui-ci est unique).
- $\times$ est distributive sur $+$ ($(x + y) \times z = x \times z + y \times z$),
- La loi $\times$ admet un élément neutre, $\overline{1}$, tel que pour tout $x \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$, $x \times \overline{1} = x$.

En algèbre, on appelle un tel ensemble un *anneau* (commutatif). Les anneaux sont fondamentaux, car ils apparaissent dans bien des domaines, et les mathématiciens ont donc développé une théorie générale traitant de ce type d'objets. Je n'en dirai pas plus pour l'instant.

- $\mathbb{Z}/p\mathbb{Z}$ -

On commence cette section par un rappel :

Proposition 1. On dit que $a \in \mathbb{Z}/n\mathbb{Z}$ est *inversible* s'il existe $b \in \mathbb{Z}/n\mathbb{Z}$, appelé l'*inverse* de a et noté a^{-1}, tel que $a \times b = \overline{1}$. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\overline{k}$, où k est un entier premier avec n.

Démonstration. C'est une reformulation du théorème de Bézout, en effet on a les équivalences suivantes.

Il existe $b \in \mathbb{Z}$ tel que $ab \equiv 1 \mod n$
$\Leftrightarrow$ il existe $b \in \mathbb{Z}$ et $k \in Z$ tels que $ab = kn + 1$
$\Leftrightarrow$ a est premier avec n. □

Dans toute la suite, p désignera un nombre premier. On a ainsi que tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ autres que $\overline{0}$ sont inversibles. On appelle *corps* un anneau vérifiant cette propriété. Dans un corps, on dispose donc d'une opération fondamentale qui n'existe pas dans les anneaux : la division. Ainsi, les corps sont des objets algébriques beaucoup plus riches. Par exemple, la théorie des polynômes fonctionne très bien sur les corps, et nous allons donc étudier les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Noter que de tels polynômes seraient délicats à définir sans l'introduction de $\mathbb{Z}/p\mathbb{Z}$.

Lemme 2. Soient a et b dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$, alors $a \times b$ est dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$.

Démonstration. Si on avait $a \times b = \overline{0}$, en multipliant par a^{-1} et b^{-1} on obtiendrait $\overline{1} = \overline{0}$, c'est absurde. □

Ce lemme facile nous permet de définir une notion satisfaisante de degré sur $\mathbb{Z}/p\mathbb{Z}[X]$, l'ensemble des polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. En effet, si P et Q ont pour termes dominants $a \cdot X^k$ et $b \cdot X^l$, alors $ab \cdot X^{k+l}$ sera non nul, et sera le terme dominant de $P \cdot Q$. Nous sommes maintenant en mesure de prouver :

Proposition 3. Il y a une notion de division euclidienne sur $\mathbb{Z}/p\mathbb{Z}[X]$: soient A et B dans $\mathbb{Z}/p\mathbb{Z}[X]$ avec B non nul, alors il existe un unique couple (Q, R) de polynômes de $\mathbb{Z}/p\mathbb{Z}[X]$ tels que $A = Q \cdot B + R$, avec $\deg(R) < \deg(B)$.

Démonstration. La preuve est la même que dans $\mathbb{R}[X]$. Pour l'unicité, soit (Q', R') un deuxième tel couple, alors $B \cdot (Q - Q') = R' - R$, puis $Q = Q'$ en examinant les degrés.

Pour l'existence, on vérifie que l'algorithme usuel fonctionne, car le coefficient dominant de B est inversible. Par exemple, pour diviser $A = \overline{5} \cdot X^3 + \overline{2} \cdot X^2 + \overline{5} \cdot X$ par $B = \overline{3} \cdot X^2 + \overline{6} \cdot X + \overline{2}$ dans $\mathbb{Z}/7\mathbb{Z}$, on commence par retrancher $\overline{5} \cdot \overline{3}^{-1} \cdot X \cdot B$ à A, le coefficient dominant de Q doit donc être $\overline{5} \cdot \overline{3}^{-1} \cdot X = \overline{5} \cdot \overline{5} \cdot X = \overline{4} \cdot X$. Il reste $A - \overline{4} \cdot X \cdot B = \overline{6} \cdot X^2 + \overline{4} \cdot X$. On retranche donc $\overline{6} \cdot \overline{3}^{-1} \cdot B$. Au final, on obtient $A = Q \cdot B + R$ avec $Q = \overline{4} \cdot X + \overline{2}$ et $R = \overline{6} \cdot X + \overline{3}$. □

Corollaire 4. Soit P dans $\mathbb{Z}/p\mathbb{Z}[X]$, et a une racine de P. Alors P est divisible par $(X - a)$, i.e. il existe Q dans $\mathbb{Z}/p\mathbb{Z}[X]$ tel que $P = (X - a) \cdot Q$.

Démonstration. Soit $P = (X - a) \cdot Q + R$ la division euclidienne de P par $(X - a)$. Alors R est de degré inférieur strictement à 1, donc constant, et l'évaluation de l'expression précédente en a nous donne $R = \overline{0}$. □

Corollaire 5. Un polynôme de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$ a au plus n racines.

Démonstration. Soit P de degré n dans $\mathbb{Z}/p\mathbb{Z}[X]$. Supposons qu'il admette n racines $a_1, a_2, \ldots, a_n$. D'après le corollaire précédent, il existe une constante c non nulle tel que

$$P = c \cdot \Pi_{i=1}^{n}(X - a_i).$$

Soit alors a une racine de P. On a

$$\overline{0} = c \cdot \Pi_{i=1}^{n}(a - a_i),$$

et, d'après le lemme, un des $(a - a_i)$ est nul, donc a est l'un des a_i. □

Soit a dans $\mathbb{Z}/p\mathbb{Z}$, en appliquant cela au polynôme $X^k - a$, on obtient un résultat important : a a au plus k racines k-ièmes ! Voici un exemple d'application.

Proposition 6. Soit a dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$. Alors a est un carré si et seulement si

$$a^{\frac{p-1}{2}} = 1.$$

Démonstration. Tout d'abord, si a est un carré différent de $\overline{0}$, on écrit $a = x^2$, et alors $a^{(p-1)/2} = x^{p-1} = 1$ par théorème de Fermat. De plus, par ce que l'on vient de voir, il y a au plus $\frac{p-1}{2}$ solutions à l'équation $a^{(p-1)/2} = 1$. Or, il y a au moins $\frac{p-1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z} \setminus \{\overline{0}\}$! En effet, un nombre ayant au plus 2 racines carrées, il y a au moins $\frac{p-1}{2}$ carrés parmi la liste $\overline{1}^2, \overline{2}^2, \ldots, \overline{p-1}^2$. □

Ainsi, par exemple, $\overline{-1}$ est un carré modulo p si et seulement si p est congru à 1 modulo 4. Un petit lemme souvent bien pratique.

- $\mathbb{Z}/n\mathbb{Z}^*$ -

Passons à une étude plus poussée de l'opération la plus intéressante dans $\mathbb{Z}/n\mathbb{Z}$: la multiplication. Seulement, cette multiplication possède quelques propriétés pénibles, comme le fait que le produit de deux éléments non nuls puisse être nul, qui empêchent de dire grand chose d'intéressant. Ainsi, il est naturel de restreindre notre étude à l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, que l'on notera $\mathbb{Z}/n\mathbb{Z}^*$. Algébriquement, cet ensemble est muni d'une opération, la multiplication, qui possède un élément neutre $\overline{1}$, et chaque élément possède un inverse. Un tel ensemble s'appelle un groupe, une structure mathématique très importante. Un autre exemple de groupe est $\mathbb{Z}/n\mathbb{Z}$ tout entier, muni de son addition. Nous prouverons plus loin que dans certains cas ces groupes ont en fait une structure très proche.

J'insiste sur ces questions de structure, car elles sont fondamentales. Selon les ensembles ou les opérations intervenant dans un problème donné, le cadre naturel dans lequel se place le problème change. Ainsi, un problème ne faisant intervenir que des multiplications modulo n « vit » dans $\mathbb{Z}/n\mathbb{Z}^*$, et les outils que l'on peut utiliser pour aborder le problème seront ceux de la théorie des groupes, qui sont très différents de ceux de la théorie des corps par exemple.

Commençons par un rappel : la forme générale du petit théorème de Fermat.

Théorème 7. Soit a dans $\mathbb{Z}/n\mathbb{Z}^*$. Alors $a^{\varphi} = 1$. (On rappelle que φ désigne l'indicatrice d'Euler, et que $\varphi(n)$ est le nombre d'entiers inférieurs à n et premiers avec n, qui est aussi le cardinal de $\mathbb{Z}/n\mathbb{Z}^*$, d'après notre reformulation du théorème de Bézout).

Démonstration. L'idée est d'utiliser le fait que la multiplication par a est une bijection. Appelons $x_1, x_2, \ldots, x_{\phi(n)}$ les éléments de $\mathbb{Z}/n\mathbb{Z}^*$. On a que

$$\{x_1, x_2, \ldots, x_{\phi(n)}\} = \{ax_1, ax_2, \ldots, ax_{\phi(n)}\},$$

et on obtient donc le résultat en comparant le produit de tous les éléments de nos deux ensembles, puis en simplifiant par le produit de x_i. □

Proposition 8. Soit x dans $\mathbb{Z}/n\mathbb{Z}^*$. La suite $(x^k)_{k\in\mathbb{Z}}$ est périodique. Appelons $\omega(x)$ sa période. Alors $x^l = 1 \Leftrightarrow \omega(x)|l$.

Démonstration. La seule chose à prouver est la périodicité. Or la suite $(x^k)_{k\in\mathbb{N}}$ prend ses valeurs dans un ensemble fini, il existe donc par principe des tiroirs $p < q$ tels que $x^p = x^q$, et alors $x^{p-q} = 1$, et la suite est $p - q$ périodique. □

Attention, dans cette preuve $p - q$ n'est pas nécessairement l'ordre de x. Calculer l'ordre d'un élément x n'est pas un problème facile : en général, il n'y a pas de méthode plus beaucoup plus intelligente que le calcul des puissances de x. Introduire cet ordre peut pourtant s'avérer très fructueux. Il y a un cas particulièrement agréable : si on dispose d'une relation de type $x^l = 1$: on saura alors que l'ordre divise à la fois l et $\phi(n)$, ce qui peut permettre de le déterminer.

- $\mathbb{Z}/p\mathbb{Z}^*$ -

Étudier les ordres est plus agréable dans $\mathbb{Z}/p\mathbb{Z}^*$, grâce aux bonnes propriétes des polynômes de la forme $X^k - 1$ montrées dans ma deuxième partie.

Définition 9. Un *générateur* de $\mathbb{Z}/n\mathbb{Z}^*$ est un élément x de $\mathbb{Z}/n\mathbb{Z}^*$ tel que la suite des puissances de x recouvre tout $\mathbb{Z}/n\mathbb{Z}^*$.

Théorème 10. Pour tout p premier, $\mathbb{Z}/p\mathbb{Z}$ possède un générateur.

Pour prouver ce théorème, il faut trouver un moyen de construire des éléments d'ordre donnés. Je commence par un lemme allant dans ce sens. il est vrai de manière générale sur $\mathbb{Z}/n\mathbb{Z}^*$, je l'énonce donc dans ce cadre.

Lemme 11. Soient a et b dans $\mathbb{Z}/n\mathbb{Z}^*$ tels que $\omega(a) \wedge \omega(b) = 1$. Alors $\omega(ab) = \omega(a)\omega(b)$.

Démonstration. Tout d'abord, $(ab)^{\omega(a)\omega(b)} = 1$, donc $\omega(ab)|\omega(a)\omega(b)$. Pour terminer, il suffit de prouver que si k est tel que $(ab)^k = 1$, alors k est multiple de $\omega(a)$ et de $\omega(b)$. Or, si $(ab)^k = 1$, en élevant à la puissance $\omega(a)$ on trouve que $b^{k\omega(a)} = 1$, donc que $\omega(b)$ divise $k\omega(a)$, donc $\omega(b)$ divise k par lemme de Gauss. □

Lemme 12. Posons $m := \mathrm{PPCM}((\omega(x))_{x\in\mathbb{Z}/n\mathbb{Z}^*})$. Alors il existe dans $\mathbb{Z}/n\mathbb{Z}^*$ un élément d'ordre m.

Démonstration. Décomposons m en facteurs premiers : $m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Soit x_i un élément dont l'ordre est un multiple de $p_i^{\alpha_i}$: $\omega(x_i) = k_i p_i^{\alpha_i}$ (un tel x_i existe par définition du PPCM). Posons $y_i := x_i^{k_i}$. On vérifie que y_i est d'ordre $p_i^{\alpha_i}$ et, en utilisant de façon répétée notre lemme précedent, le produit des y_i est d'ordre m. □

Démonstration. Il est temps de finir la preuve du théorème annoncé. Appliquons donc les lemmes à $\mathbb{Z}/p\mathbb{Z}^*$. Soit donc x un élément d'ordre m. On sait que $p-1$ est multiple de tous les ordres des éléments de $\mathbb{Z}/p\mathbb{Z}^*$, il est donc multiple de leur PPCM : m, et donc $m \leqslant p-1$. Or, on sait que le polynôme $X^m - 1$ a au plus m racines, et que les $p-1$ éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont racines de ce polynôme (car m est multiple de tous les ordres), donc on a $p-1 \leqslant m$, puis $p-1 = m$, et notre élément d'ordre m est notre générateur recherché. □

Que veut dire ce théorème ? Choisissons x un générateur. Alors

$$\mathbb{Z}/p\mathbb{Z}^* = \{1, x, x^2, \dots, x^{p-2}\}.$$

La multiplication de telles puissances de x est très facile : il suffit d'ajouter les exposants modulo $p-1$. En fait, ce choix de x permet même d'identifier $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$ avec $(\mathbb{Z}/p\mathbb{Z}^*, x)$, via la fonction $k \mapsto x^k$. Ainsi, la structure

multiplicative du groupe $(\mathbb{Z}/p\mathbb{Z}^*, \times)$ n'est pas plus compliquée que la structure additive du groupe $(\mathbb{Z}/(p-1)\mathbb{Z}, +)$. Attention, tout n'est pas si rose, car trouver un générateur x n'est pas facile. Toutefois, l'introduction d'un générateur peut faire des miracles dans un problème plutôt théorique. Mentionnons, enfin, qu'il existe des résultats plus généraux, plus difficiles, explicitant pour tout n la structure de $\mathbb{Z}/n\mathbb{Z}^*$. En particulier, on a :

Théorème 13. Le groupe $\mathbb{Z}/n\mathbb{Z}^*$ possède un générateur si et seulement si n vaut 2, 4, p^k ou $2p^k$, où p est un nombre premier plus grand que 3.

- Quelques exercices -

Exercice 1 Trouver tous les entiers $n \geqslant 1$ impairs tels que n divise $3^n + 1$.

Exercice 2 Soit p un nombre premier. Trouver tous les entiers k tels que p divise $1^k + 2^k + \ldots + (p-1)^k$.

Exercice 3 Soit p un nombre premier impair. Prouver que si q est un diviseur premier de $x^{p-1} + x^{p-2} + \cdots + 1$ alors $p = q$ ou p divise $q - 1$.

Exercice 4 Combien y-a-t'il d'élements d'ordre k dans $\mathbb{Z}/p\mathbb{Z}^*$?

Exercice 5 Trouver tous les p, q premiers tels que pq divise $2^p + 2^q$.

- Solutions des exercices -

Solution de l'exercice 1 Soit $n > 1$ tel que n divise $3^n + 1$. Une autre façon de le dire est que $3^n \equiv -1\,[n]$, on est donc face à un problème purement multiplicatif. On aimerait bien utiliser le théorème de Fermat, mais il est difficile à exploiter car on contrôle mal $\varphi(n)$. Soit donc p un facteur premier de n, qui est impair. On a $3^{2n} \equiv 1\,[p]$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1\,[p]$. Ainsi ω divise $p-1$. On en déduit que ω divise $\mathrm{PGCD}(2n, p-1)$. Si on impose de plus que p soit le plus petit facteur premier de n, alors nécessairement $\omega = 1$ ou 2 (car un facteur premier de $p-1$ ne peut pas diviser n par minimalité). Dans le premier cas de figure, $3 \equiv 1\,[p]$ et donc $p = 2$, ce qui est exclu. Dans le deuxième cas, $3^2 \equiv 1\,[p]$ et donc p divise 8, ce qui est exclu également. On en déduit que $n = 1$.

Solution de l'exercice 2 La somme des puissances k-ièmes va être difficile à manipuler telle quelle. L'idée est d'introduire un générateur x de $\mathbb{Z}/p\mathbb{Z}^*$. En effet,

$$1^k + 2^k + \ldots + (p-1)^k \equiv 1 + x^k + x^{2k} \ldots + x^{(p-2)k}\,[p]\,.$$

On reconnaît la somme des termes d'une suite géométrique. Ainsi, si $(p-1)|k$, chaque terme de la somme vaut 1, et la somme vaut $p-1$ qui est non nul. Sinon, x^k est différent de 1, x^k-1 est inversible, et la somme vaut $\frac{x^{(p-1)k}-1}{x^k-1}$, qui est nul par théorème de Fermat.

Solution de l'exercice 3 Un tel diviseur q divise $x^p-1=(x-1)\left(x^{p-1}+x^{p-2}+...+1\right)$ donc l'ordre de x modulo q divise p premier. Si cet ordre est p, comme d'après le théorème de Fermat il divise également $q-1$, p divise $q-1$. Si l'ordre est 1, pour tout k, $x^k \equiv 1\,[q]$ donc la somme des p termes : $x^{p-1}+x^{p-2}+...+1 \equiv p\,[q]$ est divisible par q si et seulement si q divise p, soit $q=p$.

Solution de l'exercice 4 Soit x un générateur de $\mathbb{Z}/p\mathbb{Z}^*$ (le résultat de l'exercice implique l'existence d'un générateur, donc, à moins de vouloir tout reprouver, il faudra de toute façon utiliser ce résultat). Les éléments de $\mathbb{Z}/p\mathbb{Z}^*$ sont donc les x^k avec k entre 0 et $p-2$. Quel est l'ordre d'un tel x^k ? C'est le plus petit a tel que ak soit multiple de $p-1$, c'est donc $\frac{\mathrm{PPCM}(p-1,k)}{k}$, autrement dit $\frac{p-1}{\mathrm{PGCD}(p-1,k)}$. Soit donc d un diviseur de $p-1$. L'élément x^k est d'ordre $\frac{p-1}{d}$ si et seulement si $\mathrm{PGCD}(p-1,k)=d$, donc si k est de la forme αd avec α premier avec $\frac{p-1}{d}$. Il y a $\phi(\frac{p-1}{d})$ tels k.

Deux remarques : la notion d'ordre fonctionne aussi dans $(\mathbb{Z}/n\mathbb{Z},+)$, l'ordre de x étant le plus petit entier n tel que nx soit nul (où nx est défini comme valant $x+x+\ldots+x$ n fois). Un raisonnement identique montre alors que, pour d divisant n, il y a $\phi(d)$ éléments d'ordre d (moralement, notre preuve consistait à, via le choix d'un générateur, se placer dans $(\mathbb{Z}/(p-1)\mathbb{Z},+)$. On en déduit en comptant selon leur ordre les éléments de $\mathbb{Z}/n\mathbb{Z}$, la très jolie, et importante, identité combinatoire suivante :

$$\phi(n)=\Sigma_{d|n}\phi(d).$$

Solution de l'exercice 5 Remarquons tout d'abord que si $p=2$, $2q$ divise $4+2^q$ si et seulement si soit $q=2$, soit $2q$ divise 6, puisque, pour tout q impair, q divise $2^{q-1}-1$, donc $2q$ divise 2^q-2. D'où les solutions : $(p,q)=(2,2),(2,3)$ ou $(3,2)$. On supposera désormais p et q impairs. Appelons ω_p et ω_q les ordres de 2 modulo p et q respectivement. Supposons que p divise 2^p+2^q, donc $2^{p-1}+2^{q-1}$ (car 2 est inversible modulo p, on peut donc diviser par 2), comme p divise $2^{p-1}-1$, p divise $2^{q-1}+1$, donc p divise $2^{2(q-1)}-1$. Dès lors, ω_p divise $p-1$ et $2(q-1)$ mais ne divise pas $q-1$. Appelons v_2 la valuation 2-adique. Le fait

que ω_p divise $p-1$ implique que $v_2(\omega_p) \leqslant v_2(p-1)$, et le fait que ω_p divise $q-1$ mais pas $2(q-1)$ implique que $v_2(\omega_p) = 1+v_2(q-1)$ (pour vous en convaincre, regardez les décompositions en facteurs premiers). Or, symétriquement, on a $v_2(\omega_q) \leqslant v_2(q-1)$, et donc $v_2(\omega_p) = 1+v_2(q-1) > v_2(\omega_q)$. Symétriquement, $v_2(\omega_q) > v_2(\omega_p)$, c'est absurde.