DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Cours et exercices

AUTEUR : Louis NEBOUT
STAGE : Montpellier 2012

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

Certains théorèmes et certaines propositions de la version polycopiée de ce cours ont été présentés en tant qu'exercices en classe. Je les ai ici mis sous forme de théorèmes pour souligner leur importance, par rapport aux autres exercices.

- L'anneau $\mathbb{Z}/n\mathbb{Z}$ -

Soit $n \geqslant 2$ un entier naturel. Dans $\mathbb{Z}$, on dispose de la relation de congruence modulo n. Celle-ci est une *relation d'équivalence*, c'est-à-dire qu'elle est *réflexive* (pour tout $x \in \mathbb{Z}$, $x \equiv x \mod n$), *symétrique* (pour tous x, $y \in \mathbb{Z}$, si $x \equiv y \mod n$, alors $y \equiv x \mod n$) et *transitive* (pour tous x, y, $z \in \mathbb{Z}$, si $x \equiv y \mod n$ et $y \equiv z \mod n$, alors $x \equiv z \mod n$). De plus, elle est compatible avec les opérations $+$ et $\times$. Elle possède en fait des propriétés tout à fait similaires à l'égalité, et on aimerait bien la « transformer » en une 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, 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 est clair que ces opérations sont bien définies (c'est-à-dire, par exemple pour $+$, que si $\overline{x} = \overline{x'}$ at $\overline{y} = \overline{y'}$, alors $\overline{x+y} = \overline{x'+y'}$) : ceci découle immédiatement 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 : 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 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. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n, et on a par exemple $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\} = \{\overline{-n}, ..., \overline{-2}, \overline{-1}\}$. De plus, $\mathbb{Z}/n\mathbb{Z}$ possède une certaine structure algébrique, celle d'*anneau*, ce qui permettra par exemple d'utiliser dans certains cas de façon très puissante les polynômes.

Définition 1. Un *anneau (commutatif unitaire)* $(A, +, \times)$ est un ensemble A muni de deux lois binaires $+$ et $\times$, toutes deux commutatives ($x + y = y + x$) et associatives ($x + (y + z) = (x + y) + z$), telles que :

- $\times$ est distributive sur $+$ ($(x + y)z = xz + yz$) ;
- La loi $+$ admet un élément neutre noté 0, tel que pour tout $x \in A$, $x + 0 = x$;
- La loi $\times$ admet un élément neutre noté 1, tel que pour tout $x \in A$, $x \times 1 = x$;
- Tout élément x de A admet un opposé noté $-x$, tel que $x + (-x) = 0$ (celui-ci est unique).

Si on a de plus $\forall x, y \in A$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$, on dit alors que A est *intègre*. On dit qu'un élément x de A est inversible s'il existe x^{-1} (appelé un *inverse* de x) tel que $xx^{-1} = 1$. On note A^* l'ensemble des inversibles de A. Si x est inversible, son inverse est unique. 0 n'admet jamais d'inverse. Si $A^* = A \setminus \{0\}$, on dit que A est un *corps*. Un corps est toujours intègre.

Exemple 2. $\mathbb{Z}$ est un anneau intègre, d'inversibles 1 et -1. $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps. Si A est un anneau, alors l'ensemble des polynômes à coefficients dans A, noté $A[X]$, est un anneau. Si A est intègre, alors $A[X]$ l'est aussi. Si A est un corps, alors les inversibles de $A[X]$ sont les polynômes constants non-nuls. Et enfin, $\mathbb{Z}/n\mathbb{Z}$ est un anneau !

De nombreuses propriétés de $\mathbb{Z}$ sont communes à tous les anneaux, et encore plus le sont à tous les anneaux intègres. De nombreuses propriétés de $\mathbb{Q}$, $\mathbb{R}$ où $\mathbb{C}$ sont communes à tous les corps, d'où l'intérêt de ces notions. On n'utilise en fait pour montrer ces propriétés que le fait que l'ensemble concerné soit un anneau (éventuellement intègre), ou un corps.

Proposition 3. Les inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $\overline{a}$, où a est un entier premier avec n. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier, et dans ce cas, c'est un corps.

Démonstration. On a les équivalences suivantes :

$\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$

$\Leftrightarrow$ 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 (par Bézout).

Si n est premier, les éléments non-nuls de $\mathbb{Z}/n\mathbb{Z}$ étant $\overline{1}$, $\overline{2}$, ..., $\overline{n-1}$, il sont tous inversibles. Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps. Il ne reste plus qu'à montrer que si n est composé, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre ; mais si n est composé, on écrit $n = ab$ avec $1 \leqslant a, b \leqslant n$, et on a alors $\overline{a}$, $\overline{b} \neq 0$ et $\overline{a}\overline{b} = \overline{n} = 0$.

□

- Ordre multiplicatif -

Soit $n \geqslant 2$. L'ensemble $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{x} \mid 1 \leqslant x \leqslant n-1, \text{PGCD}(x, n) = 1\}$ est stable par produit, par passage à l'inverse, et contient $\overline{1}$ (on dit que c'est un *groupe*). Cet ensemble est de cardinal $\phi(n)$, et par le théorème d'Euler, pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $x^{\phi(n)} = \overline{1}$.

Définition 4. Soit $x \in \mathbb{Z}$. L'*ordre* de $\overline{x}$ dans $(\mathbb{Z}/n\mathbb{Z})^*$ (ou encore l'ordre de x modulo n) est le plus petit entier $\omega \geqslant 1$ tel que $\overline{x}^\omega = \overline{1}$ (ou encore $x^\omega \equiv 1 \mod n$). On le note $\omega_n(x)$ ou simplement $\omega(x)$ lorsqu'il n'y a pas d'ambiguité.

Le théorème d'Euler montre que l'ordre est bien défini. On remarquera qu'alors, $\overline{x}^{\omega-1}$ est l'inverse de $\overline{x}$. En particulier, si $\overline{x}$ n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$, il n'existe aucun entier $\omega \geqslant 1$ tel que $\overline{x}^\omega = \overline{1}$.

Exercice 1

Sans le théorème d'Euler, montrer que l'ordre est bien défini.

L'intérêt de l'ordre est la proposition suivante :

Proposition 5. Soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$, et $n \in \mathbb{Z}$. Alors $x^n = \overline{1}$ si et seulement si $\omega(x)$ divise n.

Démonstration. Si $\omega(x) \mid n$, on pose $n = k\omega(x)$ et on a $x^n = (x^{\omega(x)})^k = \overline{1}^k = \overline{1}$. Réciproquement, si $x^n = \overline{1}$, alors on écrit $n = q\omega(x) + r$ avec $0 \leqslant r < \omega(x)$ et on a $x^r = x^r(x^{\omega(x)})^q = x^n = 1$. On ne peut pas avoir $1 \leqslant r < \omega(x)$, sinon ceci contredirait la minimalité de $\omega(x)$. Donc $r = 0$ et $\omega(x) \mid n$.

□

On en déduit, en particulier, que pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^*$, $\omega(x) \mid \phi(n)$ (et donc $\omega(x) \mid n-1$ si n est permier). Ceci est particulièrement pratique lorsque $\phi(n)$ a une forme particulière. Par exemple, si p est un nombre premier et $n \geqslant 1$, alors $\phi(p^n) = p^n(p-1)$. Pour $p = 2$ par exemple, $\phi(2^n) = 2^{n-1}$, et donc tout les éléments de $(\mathbb{Z}/2^n\mathbb{Z})^*$ ont pour ordre une puissance de 2.

Exercice 2

Soit n un entier naturel. Montrer que les diviseurs premiers du $n^{\text{ième}}$ nombre de Fermat $2^{2^n} + 1$ sont tous de la forme $k \cdot 2^{n+1} + 1$.

Exercice 3

Déterminer tous les entiers $n \geqslant 1$ tels que n divise $2^n - 1$.

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

Sauf mention contraire, dans toute la suite, p désignera un nombre premier, et on travaillera dans le corps $\mathbb{Z}/p\mathbb{Z}$.

Si A est un anneau intègre, de nombreux résultats vrais dans $\mathbb{Z}[X]$ le restent dans $A[X]$. En particulier, on a l'existence d'une division euclidienne par les polynômes unitaires, si $r \in A$ est racine de $P \in A[X]$, alors $P(X)$ est divisible par $X - r$, et un polynôme de degré n possède au plus n racines, comptées avec multiplicités. En conséquence, si un polynôme P est de degré n, a pour coefficient dominant λ, a pour racines r_1, ..., r_k avec pour multiplicités respectives α_1, ..., α_k telles que $\alpha_1 + ... + \alpha_k = n$, alors $P(X) = \lambda(X - r_1)^{\alpha_1}...(X - r_k)^{\alpha_k}$. Si, de plus, A est un corps, alors on dispose d'une division euclidienne par n'importe quel polynôme non-nul, et dans $A[X]$ on a un PGCD, un PPCM, des théorèmes de Bézout et de Gauss, et existence et unicité de la décomposition en produit d'irréductibles. En particulier, toutes ces propriétés sont vraies dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Exercice 4

Résoudre dans $\mathbb{Z}/12\mathbb{Z}$ l'équation $x^2 + \overline{3}x + \overline{2} = 0$.

Exercice 5

Soit $p \geqslant 2$ un entier naturel. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \mod p$.

(Théorème de Wilson)

Exercice 6

Soit $p \geqslant 5$ un nombre premier. Soient $a,\ b \in \mathbb{Z}$ tels que $1+\frac{1}{2}+...+\frac{1}{p-1} = \frac{a}{b}$. Montrer que $p^2 \mid a$.

- Résidus quadratiques -

Définition 6. Soit $x \in \mathbb{Z}$. On dit que x est un résidu quadratique modulo p (ou encore que $\overline{x}$ est un résidu quadratique dans $\mathbb{Z}/p\mathbb{Z}$) si x n'est pas divisible par p et si $\overline{x}$ est le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$.

On note $\left(\frac{x}{p}\right) = 1$ si x est un résidu quadratique modulo p, $\left(\frac{x}{p}\right) = 0$ si $p \mid x$ et $\left(\frac{x}{p}\right) = -1$ sinon. Le symbole $\left(\frac{x}{p}\right)$ s'appelle le symbole de Legendre.

Théorème 7 (Critère d'Euler)**.** Soit p un nombre premier impair, et $x \in (\mathbb{Z}/p\mathbb{Z})^*$. Alors x est un résidu quadratique si et seulement si $x^{\frac{p-1}{2}} = \overline{1}$. Sinon, on a $x^{\frac{p-1}{2}} = -\overline{1}$.

Démonstration. Commençons par dénombrer les résidus quadratiques de $(\mathbb{Z}/p\mathbb{Z})^*$. Soit x un résidu quadratique, disons que $x = y^2$ avec $y \in (\mathbb{Z}/p\mathbb{Z})^*$. On a alors aussi $x = (-y)^2$, or $y \neq -y$ puisque p est impair, donc x est le carré d'au moins deux éléments de $(\mathbb{Z}/p\mathbb{Z})^*$. En fait, c'est le carré d'exactement deux éléments, car le polynôme $X^2 - x$ est de degré 2, donc admet au plus deux racines dans $\mathbb{Z}/p\mathbb{Z}$. Puisque $(\mathbb{Z}/p\mathbb{Z})^*$ possède $p-1$ éléments, et puisque chaque résidu quadratique est le carré d'exactement deux de ces éléments, on en déduit qu'il y a exactement $\frac{p-1}{2}$ résidus quadratiques.

Tous ces résidus quadratiques vérifient $x^{\frac{p-1}{2}} = \overline{1}$, puisqu'en les écrivant $x = y^2$, on obtient $x^{\frac{p-1}{2}} = y^{p-1} = \overline{1}$, par petit Fermat. Il s'agit de montrer que c'est les seuls. Mais le polynôme $X^{\frac{p-1}{2}} - \overline{1}$ a au plus $\frac{p-1}{2}$ racines dans $\mathbb{Z}/p\mathbb{Z}$,

et tous les résidus quadratiques, qui sont au nombre de $\frac{p-1}{2}$, en sont racines. Donc ce sont les seules, ce qui conclut la première affirmation du théorème.

Pour démontrer la seconde partie, il suffit de montrer que la fonction $f(x) = x^{\frac{p-1}{2}}$ ne prend que les valeurs $\overline{1}$ et $-\overline{1}$ lorsque x parcourt $(\mathbb{Z}/p\mathbb{Z})^*$. Mais $f(x)^2 = x^{p-1} = \overline{1}$, donc les valeurs prises par f sur $(\mathbb{Z}/p\mathbb{Z})^*$ sont des racines carrées de 1 : ce sont donc $\overline{1}$ et $-\overline{1}$.

□

Cette preuve, ou du moins le premier paragraphe, est à connaître, car elle donne des informations sur la répartition des résidus quadratiques : leur nombre, et le fait que chacun soit le carré d'exactement deux éléments *opposés*. On peut en déduire, par exemple, que 1^2, 2^2, ..., $\left(\frac{p-1}{2}\right)^2$ forme un système complet de représentants des résidus quadratiques de $\mathbb{Z}/p\mathbb{Z}$, car ils sont au nombre de $\frac{p-1}{2}$ et sont deux-à-deux non-opposés.

Une autre remarque importante est que le critère d'Euler peut se reformuler de la façon suivante à l'aide du symbole de Legendre : pour tout nombre premier impair p et pour tout $x \in \mathbb{Z}$, on a $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \mod p$ (on remarquera que ceci marche *même* si $p \mid x$). On en déduit immédiatement que le symbole de Legendre est *complètement multiplicatif* par rapport à son argument supérieur, autrement dit, pour tous $x, y \in \mathbb{Z}$, on a $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$. En particulier, le produit de deux résidus quadratiques est un résidu quadratique, et l'inverse d'un résidu quadratique est un résidu quadratique (on dit que l'ensemble des résidus quadratiques est un *sous-groupe* de $(\mathbb{Z}/p\mathbb{Z})^*$), mais aussi, le produit de deux non-résidus quadratiques est un résidu quadratique, et le produit d'un résidu quadratique et d'un non-résidu quadratique n'est pas un résidu quadratique.

Exercice 7

(1) Trouver tous les nombres premiers p vérifiant la propriété suivante : pour tous entiers $a, b \in \mathbb{Z}$, si $p \mid (a^2 + b^2)$ alors $p \mid a$ et $p \mid b$.

(2) Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

Voici un célèbre résultat dû à Gauss, que j'énoncerai sans preuve :

Théorème 8 (Loi de réciprocité quadratique)**.** Soient p et q deux nombres premiers impairs.

- Si au moins un des deux nombres p et q est congru à 1 modulo 4, alors q est un résidu quadratique modulo p si et seulement si p est un résidu quadratique modulo q ;
- Si les deux nombres p et q sont congrus à 3 modulo 4, alors q est un résidu quadratique modulo p si et seulement si p n'est pas un résidu quadratique modulo q.

À l'aide du symbole de Legendre, on peut reformuler ce résultat de la manière suivante : pour tous nombre premiers impairs p et q, on a $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$.

Ce théorème ne dit rien du cas où $p = 2$. Pour cela, on a la proposition suivante :

Proposition 9. Soit p un nombre premier impair. Alors 2 est un résidu quadratique modulo p si et seulement si p est congru à 1 où à -1 modulo 8. Autrement dit, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Avec la loi de réciprocité quadratique ainsi que la proposition précédente, on peut déterminer très rapidement si un entier est où non un résidu quadratique modulo un nombre premier p. On peut aussi, pour simplifier les calculs (même si ce n'est en réalité pas nécessaire), utiliser le fait que -1 est un résidu quadratique modulo p si et seulement si p est congru à 1 où 2 modulo 4, autrement dit $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Exercice 8

219 est-il un résidu quadratique modulo 383 ?

- Solution des exercices -

Solution de l'exercice 1

Soit $x \in (\mathbb{Z}/n\mathbb{Z})^*$; on cherche $\omega \geqslant 1$ tel que $x^\omega = \overline{1}$. Considérons la suite x, x^2, x^3, ... Elle possède une infinité de termes et prend ses valeurs dans l'ensemble fini $\mathbb{Z}/n\mathbb{Z}$, donc par le principe des tiroirs, il existe des entiers s et t tels que $1 \leqslant s < t$ et $x^s = x^t$. En simplifiant par x^s, on obtient $x^{t-s} = \overline{1}$, donc $\omega = t - s$ convient.

Solution de l'exercice 2

Soit p un diviseur premier de $2^{2^n} + 1$. Alors $2^{2^n} \equiv -1 \mod p$ et $2^{2^{n+1}} \equiv 1 \mod p$, donc l'ordre de 2 modulo p divise 2^{n+1} mais pas 2^n, donc c'est 2^{n+1}. Il s'ensuit que $2^{n+1} \mid (p-1)$, ce qui est le résultat voulu.

Solution de l'exercice 3

$n = 1$ convient, et on va montrer que c'est la seule solution. Soit $n \geqslant 2$, supposons que $n \mid 2^n - 1$. Déjà, il est clair que n est impair, puisque $2^n - 1$ l'est. Notons alors p le plus petit diviseur premier de n, et posons $n = kp$. On a $p \mid (2^n - 1)$ et par le petit théorème de Fermat, $2^n = (2^k)^p \equiv 2^k \mod p$, donc $2^k \equiv 1 \mod p$. Donc $\omega_p(2) \mid k$ et $\omega_p(2) \mid (p-1)$. De cette dernière relation de divisibilité, on tire que tous les diviseurs premiers de $\omega_p(2)$ sont strictement inférieurs á p. Or, $\omega_p(2) > 1$ puisque $p \geqslant 3$, et comme $\omega_p(2) \mid k$, on en déduit que k possède un diviseur premier strictement inférieur à p, donc n aussi. Ceci contredit la minimalité de k.

Solution de l'exercice 4

En factorisant, on obtient $(x + \overline{1})(x + \overline{2}) = 0$. Mais attention, on ne peut pas en déduire que $x = -\overline{1}$ ou $x = -\overline{2}$, car l'anneau $\mathbb{Z}/12\mathbb{Z}$ n'est pas intègre ! Dans un tel anneau, un polynôme de degré 2 peut avoir bien plus de deux racines. Il faut éviter d'essayer d'utiliser des résultats classiques sur les polynômes dans un anneau non intègre, car en général, très peu sont vrais. Ici, le seul moyen de résoudre l'équation est de tester tous les cas possibles, et de cette façon on obtient que l'ensemble des solutions est $\{\overline{2}, -\overline{5}, -\overline{2}, -\overline{1}\}$.

Solution de l'exercice 5

Si p est composé, on choisit $a \in [\![1, p-1]\!]$ divisant p. p et $(p-1)!$ ont alors a pour facteur commun, donc ne sont pas premiers entre eux. p n'est donc pas premier, sinon il diviserait $(p-1)!$ donc aussi un entier inférieur à $p-1$.

Réciproquement, supposons p premier. Il existe alors deux méthodes pour obtenir la congruence demandée.

Première méthode. On va partitionner $(\mathbb{Z}/p\mathbb{Z})^*$ en paires d'éléments deux à deux inverses. Pour cela, il faut connaître les $x \in (\mathbb{Z}/p\mathbb{Z})^*$ qui sont leur propre inverse ; ceux-là sont racines du polynôme $X^2 - \overline{1}$, de degré 2, donc il y en a au plus deux : ce sont donc $\overline{1}$ et $-\overline{1} = \overline{p-1}$. On regroupe les autres par paires d'inverses $\{x_i, x_i^{-1}\}$, de sorte que $\{\overline{1}\}$, $\{\overline{p-1}\}$ et les $\{x_i, x_i^{-1}\}$ forment une partition de $(\mathbb{Z}/p\mathbb{Z})^*$.

En réorganisant l'ordre des facteurs du produit, on a alors

$$\overline{(p-1)!} = \overline{1} \cdot \overline{p-1} \cdot (x_1 x_1^{-1}) \cdot \ldots \cdot (x_r x_r^{-1}) = \overline{p-1} = -\overline{1}.$$

Seconde méthode. Pour $p = 2$, le résultat est vrai. Supposons maintenant que $p \geqslant 3$. Considérons le polynôme $P(X) = X^{p-1} - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$. Il est unitaire et de degré $p-1$, et par le petit théorème de Fermat, tous les $p-1$ éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ en sont racines. Par la remarque précédant l'exercice, on en déduit que $P(X) = (X-\overline{1})(X-\overline{2})\ldots(X-\overline{p-1})$. Le polynôme P étant de degré pair, son coefficient constant est produit de ses racines, autrement dit $\overline{(p-1)!} = -\overline{1}$.

Solution de l'exercice 6

L'égalité de l'énoncé se réécrit $(p-1)! \cdot a = bc_1$, où $c_1 = 2 \cdot 3 \cdot \ldots \cdot \ldots \cdot (p-1) + 1 \cdot 3 \cdot \ldots \cdot (p-1) + \ldots + 1 \cdot 2 \cdot \ldots \cdot (p-2)$ est le coefficient du terme en X du polynôme $P(X) = (X-1)\ldots(X-(p-1))$. Pour résoudre le problème, il suffit de montrer que $p^2 \mid c_1$, car alors comme p^2 est premier avec $(p-1)!$, on en déduit par Gauss que $p^2 \mid a$.

Si on tente d'appliquer directement une méthode simillaire à la seconde méthode du problème précédent, on obtiendra, en réduisant P modulo p que $c_1 \equiv 0 \mod p$, ce qui n'est pas suffisant pour résoudre le problème. On va en fait utiliser une autre méthode : si on note $P(X) = \sum_{k=0}^{p-1} c_k X^k$, en évaluant P en p, on obtient $(p-1)! = \sum_{k=0}^{p-1} c_k p^k$, en remarquant que $c_0 = (p-1)!$ et simplifiant par p, on obtient $\sum_{k=1}^{p-1} c_k p^{k-1} = 0$. En réduisant modulo p^2, on obtient $c_2 p + c_1 \equiv 0 \mod p^2$. Il suffit donc de montrer que c_2 est divisible par p, mais ceci est clair en réduisant P modulo p.

Solution de l'exercice 7

(1) Il est clair que cette propriété n'est pas vérifiée par 2, en prenant par exemple $a = b = 1$. Soit maintenant p un nombre premier impair. On a $(-1)^{\frac{p-1}{2}} = 1$ si $p \equiv 1 \mod 4$ et -1 si $p \equiv 3 \mod 4$, donc par le critère d'Euler, -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1 \mod 4$. Ceci montre immédiatement qu'aucun nombre premier congru à 1 modulo 4 ne vérifie la propriété demandée, car un tel nombre premier divise un entier de la forme $n^2 + 1$ (prendre pour n un représentant de la classe dont le carré vaut $-\overline{1}$).

Montrons maintenant que tout nombre premier congru à 3 modulo 4 vérifie la propriété demandée. Supposons qu'il existe a, $b \in \mathbb{Z}$, avec a non divisible par p, tel que $p \mid (a^2 + b^2)$. Il est alors clair que p ne divise pas b non plus, donc $\overline{a}$ et $\overline{b}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$. On a alors $\overline{a}^2 = -\overline{b}^2$, donc $(\overline{a}\overline{b}^{-1})^2 = -\overline{1}$, ce qui contredit le fait que -1 ne soit pas un résidu quadratique modulo p.

(2) Supposons que l'ensemble des nombres premiers congrus à 1 modulo 4 soit fini et notons-le $\{p_1, ..., p_n\}$. Posons alors $N = (2p_1...p_n)^2+1$. Il est clair que ni 2 ni aucun des p_i ne divise N, donc tous ses diviseurs premiers sont congrus à 3 modulo 4. Soit p un des diviseurs premiers de N ; comme p divise $(2p_1...p_n)^2+1^2$, alors par la question précédente il divise 1, absurde.

Solution de l'exercice 8

Par multiplicativité du symbole de Legendre, on a $\left(\frac{219}{384}\right) = \left(\frac{3}{383}\right)\left(\frac{7}{383}\right)$. Par deux applications de la loi de réciprocité quadratique, on en déduit que $\left(\frac{219}{383}\right) = -\left(\frac{383}{3}\right)\left(\frac{383}{73}\right)$. Puis en réduisant modulo 3 et 73 respectivement, $\left(\frac{219}{383}\right) = -\left(\frac{-1}{3}\right)\left(\frac{18}{73}\right) = \left(\frac{18}{73}\right)$. Une nouvelle fois par multiplicativité, on a $\left(\frac{219}{383}\right) = \left(\frac{2}{73}\right)\left(\frac{3}{73}\right)^2 = \left(\frac{2}{73}\right)$, puis par la proposition 9, on finit par en déduire que $\left(\frac{2}{73}\right) = 1$, donc que 219 est un résidu quadratique modulo 383.