DOMAINE : Arithmétique
NIVEAU : Avancé
CONTENU : Cours et exercices

AUTEUR : Igor KORTCHEMSKI
STAGE : Grésillon 2011

Ordre modulo n, LTE

Nous rappelons ici quelques éléments vus dans le cours d'arithmétique avancé. On suppose connus les résultats classiques d'arithmétique (congruences, inversibilité modulo n, petit théorème de Fermat, fonction ϕ d'Euler ; pour ces notions voir le cours d'arithmétique sur le site d'Animath). Les solutions aux exercices se trouvent à la fin du cours.

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

Le théorème suivant nous permettra de définir la notion d'ordre.

Théorème 1. Soient a, n des entiers naturels. Les propositions suivantes sont équivalentes :

1. a et n sont premiers entre eux.
2. Il existe un entier k tel que :

$$a^k \equiv 1 \quad \text{modulo } n.$$

Démonstration. Prouvons d'abord le sens direct. D'après le théorème relatif à la fonction ϕ d'Euler, il suffit de prendre $k = \phi(n)$.

Donnons une autre preuve plus simple qui n'utilise pas ce théorème. Comme l'ensemble des résidus modulo n est fini, il existe deux entiers distincts $r < s$ tels que :

$$a^s \equiv a^r \quad \text{modulo } n.$$

Alors n divise $a^r(a^{s-r} - 1)$, donc aussi $a^{s-r} - 1$ car a et n sont premiers entre eux. Il suffit donc de prendre $k = r - s$.

Pour le sens réciproque, raisonnons par l'absurde en supposant que $d = \text{pgcd}(a, n) > 1$. Par hypothèse, il existe un entier r tel que $a^k + rn = 1$. Cela implique que d divise 1, ce qui est contradictoire. □

Définition 2. Soient a, n des entiers naturels premiers entre eux. On appelle *ordre de* a *modulo* n le plus petit entier non nul noté $\omega_n(a)$, vérifiant :

$$a^{\omega_n(a)} \equiv 1 \quad \text{modulo } n.$$

Lorsqu'il n'y a pas d'ambiguité possible, on notera $\omega(a)$ à la place de $\omega_n(a)$. D'après le théorème 1, cette définition a bien un sens. Le théorème suivant illustre un des intérêts de cette définition.

Théorème 3. Soient a, n des entiers naturels premiers entre eux et k un entier vérifiant :

$$a^k \equiv 1 \quad \text{modulo } n.$$

Alors $\omega(a)$ divise k.

Démonstration. Par l'absurde, supposons que $\omega(a)$ ne divise pas k. Soit $\omega(a) = qk + r$ la division euclidiennt de $\omega(a)$ par k, avec $0 < r < k - 1$. Alors :

$$\begin{aligned} 1 &\equiv a^{\omega(a)} \quad \text{modulo } n \\ &\equiv (a^k)^q a^r \quad \text{modulo } n \\ &\equiv a^r \quad \text{modulo } n. \end{aligned}$$

Ceci contredit le caractère minimal de $\omega(a)$ et permet de conclure. □

Corollaire 4. Soient a, n des entiers naturels premiers entre eux. Alors l'ordre de a divise $\phi(n)$. En particulier, lorsque $n = p$ et premier, l'ordre de a divise $p - 1$.

Démonstration. Ceci provient du théorème précédent et du fait que $a^{\phi(n)} \equiv 1 \quad \text{modulo } n.$ □

Ce corollaire est en particulier utile lorsqu'on veut cherche l'ordre d'un entier modulo n à la main : il suffit de test les diviseurs de $\phi(n)$.

Remarque 5. Attention ; il faut bien garder de croire que si p et premier et $0 < a \leqslant p - 1$, alors l'ordre de a est $p - 1$. Comme nous venons de le voir, s'il est vrai que l'ordre de a divise $p - 1$, il n'y a pas en général égalité : il suffit par exemple de prendre $p = 7$ et $a = 2$ pour s'en convaincre. Cependant, le théorème suivant donne un résultat allant en ce sens.

Exercice 1 Existe-t-il des entiers $n \geqslant 1$ tels que 9 divise $7^n + n^3$?

Exercice 2

(i) Trouver tous les entiers $n \geqslant 1$ tels que n divise $2^n - 1$.

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

Exercice 3 Trouver tous les entiers $m, n \geqslant 1$ tels que mn divise $3^m + 1$ et mn divise $3^n + 1$.

Finissons par quelques résultats algébriques concernant l'ordre. Pour des entiers a, n on note $a \wedge n$ le PGCD de a et de n.

Proposition 6. Soient a, b, n des entiers avec $a \wedge n = 1$ et $b \wedge n = 1$. Supposons que $\omega(a) \wedge \omega(b) = 1$. Alors $\omega(ab) = \omega(a)\omega(b)$.

Démonstration. Il est clair que $(ab)^{\omega(a)\omega(b)} = 1$. On en déduit que $\omega(ab)$ divise $\omega(a)\omega(b)$.

Soit maintenant $k \geqslant 1$ tel que $(ab)^k = 1$ et montrons que $k \geqslant \omega(a)\omega(b)$. En élevant à la puissance $\omega(a)$, il vient $b^{k\omega(a)} = 1$. On en tire que $\omega(b)$ divise $k\omega(a)$, et d'après l'hypothèse cela implique que $\omega(b)$ divise k. On montre de même que $\omega(a)$ divise k. D'après l'hypothèse, on en déduit encore que $\omega(a)\omega(b)$ divise k, d'où le résultat. □

Si a et n sont premiers entre eux, nous conseillons au lecteur d'essayer de déterminer l'ordre de a^k modulo n en fonction de l'ordre de a modulo n.

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

Nous venons de voir que le fait que a^k soit congru à 1 modulo n donnait une relation de divisibilité entre k et l'ordre de a modulo n. Nous allons maintenant voir que des informations similaires peuvent être déduites d'une relation de type $a^k \equiv b^k \bmod n$. À cet effet, rappelons le résultat suivant :

Théorème 7. Si $a \wedge n = 1$, il existe un entier b tel que $ab \equiv 1 \bmod n$. Cet entier est appelé inverse de b modulo n et sera noté b^{-1} ou $1/b$.

Démonstration. Donnons deux preuves de ce résultats.

Première démonstration : il suffit de prendre $n = a^{\omega_n(a)-1}$.

Seconde démonstration : d'après le théorème de Bézout, il existe des entiers b, d tels que $ab+nd = 1$. En réduisant modulo n, on obtient $ab \equiv 1 \bmod n$. □

Exercice 4 Soient p, q deux nombres premiers tels que q divise $3^p - 2^p$. Montrer que p divise $q - 1$.

Exercice 5 Trouver les $a, n \geqslant 1$ tels que $((a+1)^n - a^n)/n$ est un entier.

Exercice 6 Soient $a, b > 1$ impairs tels que $a + b = 2^\alpha$ avec $\alpha \geqslant 1$. Montrer qu'il n'y a pas d'entiers $k > 1$ tels que k^2 divise $a^k + b^k$.

- Racines primitives -

Considérons deux entiers a et n premiers entre eux. Nous avons vu $\omega_n(a)$, l'ordre de a modulo n, divise $\phi(n)$. Il est donc naturel de se demander s'il existe des entiers a tels que $\omega_n(a) = \phi(n)$.

Définition 8. Soient a, n deux entiers premiers entre eux. On dit que a est une racine primitive modulo n si $\omega_a(n) = \phi(n)$.

Si a est racine primitive modulo n, on voit que les restes modulo n des entiers de l'ensemble $\{1, a, a^2, \ldots, a^{\phi(n)-1}\}$ sont tous distincts.

Remarquons tout de suite qu'il n'existe pas forcément de racines primitives : il est facile de voir qu'il n'y a pas de racine primitive modulo 6. À titre culturel, mentionnons le résultat suivant :

Théorème 9. Il existe une racine primitive modulo n si, et seulement si, $n = 2, 4, p^k$ ou $2p^k$ avec p un nombre premier impair et $k \geqslant 1$.

Nous verrons en TD que si n est divisible par au moins deux nombres premiers impairs distincts, alors il n'existe pas de racine primitive modulo n. Nous allons maintenant démontrer un cas particulier du théorème précédent. Sa démonstration peut être sautée en première lecture, mais le résultat est à retenir.

Proposition 10. Si p est premier, il existe une racine primitive modulo p.

Démonstration. Montrons d'abord que si q est un nombre premier tel que q^α divise $p - 1$ avec $\alpha \geqslant 1$, alors il existe un élément d'ordre q^α modulo p. À cet effet, pour $x = 1, \ldots, p - 1$ on introduit :

$$y_x = x^{\frac{p-1}{q^\alpha}}.$$

En particulier, d'après le petit théorème de Fermat, $y_x^{q^\alpha} \equiv 1 \bmod p$. On en déduit que l'ordre de y_x modulo p divise q^α. Écrivons donc :

$$\omega_p(y_x) = q^{n_x}.$$

Notons ensuite $n_{max} = \max\{n_x;\ x = 1, \ldots, p - 1\}$. Il suffit de montrer que $n_{max} = \alpha$ (ceci impliquera qu'il existe un élément d'ordre q^α modulo p). Pour cela, on introduit le polynôme :

$$P(X) = X^{\frac{p-1}{q^\alpha} q^{n_{max}}} - 1$$

et remarque que pour $x = 0, 1, \ldots, p-1$:

$$P(x) = y_x^{q^{n_{max}}} \equiv 1 \bmod p$$

car $\omega_p(y_x)$ divise $q^{n_{max}}$.

Il en découle que le polynôme $P(X)$ a $p-1$ racines distinctes dans $\mathbb{Z}/p\mathbb{Z}$, qui est un corps (si vous ne savez pas ce que c'est qu'un corps, vous pouvez sauter cet argument). On en déduit que le degré de P vaut au moins $p-1$, de sorte que $n_{max} \geqslant \alpha$. Comme il est clair que $n_{max} \leqslant \alpha$, on en déduit que $n_{max} = \alpha$.

Revenons maintenant à la preuve du théorème. Soit $p-1 = q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ la décomposition en facteurs premiers de $p-1$. D'après ce qui précède, pour $1 \leqslant i \leqslant k$ il existe un élément x_i d'ordre $q_i^{\alpha_k}$. En utilisant la proposition 6, il vient :

$$\omega(x_1 x_2 \cdots x_k) = \omega(x_1)\omega(x_2)\cdots\omega(x_k) = q_1^{\alpha_1} \cdots q_k^{\alpha_k} = p-1.$$

L'élément $x_1 x_2 \cdots x_k$ est donc d'ordre exactement $p-1$. □

Remarquons que la preuve précédente ne s'applique pas au cas général $\mathbb{Z}/n\mathbb{Z}$, car ce dernier anneau n'est un corps que pour n premier.

Remarque 11. La preuve précédente montre que si p est premier et que si d divise $p-1$, alors il existe un élément d'ordre d. Il est possible de montrer qu'il y a alors exactement $\phi(d)$ éléments d'ordre d.

Exercice 7 Trouver tous les entiers n tels que 19 divise $2^{3n+4} + 3^{2n+1}$.

Exercice 8 Soient a, b, n des nombres entiers strictement positifs avec $a > b$. Montrer que n divise $\phi(a^n - b^n)$.

- LTE : Lifting The Exponent -

Nous concluons ce cours par un théorème extrêmement utile en arithmétique. Pour un entier n et un nombre premier p, on note $v_p(n)$ l'exposant de la plus grande puissance de p divisant n.

Théorème 12. Soit p un nombre premier **impair**. Soient a, b des nombres entiers (non nécessairement positifs) et un entier $n \geqslant 1$. On suppose que p divise $a-b$ mais que p ne divise ni a ni b. Alors :

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$

Ce théorème doit être connu. Nous renvoyons au texte suivant :
http ://www.artofproblemsolving.com/Resources/Papers/LTE.pdf
pour une preuve, des extensions au cas $p = 2$ et de nombreux exemples d'application. Nous ne pouvons qu'encourager fortement le lecteur à lire attentivement ce dernier texte.

Exercice 9 Soient a, n deux entiers strictement positifs et p un nombre premier impair tel que $a^p \equiv 1 \bmod p^n$. Montrer que $a \equiv 1 \bmod p^{n-1}$.

Exercice 10 Soit k un entier strictement positif. Trouver tous les entiers strictement positifs n tels que 3^k divise $2^n - 1$.

- Solutions des exercices du cours -

Solution de l'exercice 1 Soit $n \geqslant 1$ tel que 9 divise $7^n + n^3$. Comme un cube est congru à $0, -1$ ou 1 modulo 9, on en déduit que $n^6 \equiv 1 \bmod 9$ et donc que $7^{2n} \equiv 1 \bmod 9$. Or l'ordre de 7 modulo 9 est 3. On en déduit que 3 divise $2n$. Ainsi 3 divise n. Il faudrait donc que 3 divise 7^n, ce qui est absurde. Il n'y a donc pas de tels entiers.

Solution de l'exercice 2

(i) Soit $n > 1$ tel que n divise $2^n - 1$. Il est clair que n est impair. Soit p le plus petit facteur premier de n, qui est donc impair. Alors $2^n \equiv 1 \bmod p$. Soit ω l'ordre de 2 modulo p. Alors ω divise n. D'autre part, d'après le petit théorème de Fermat, $2^{p-1} \equiv 1 \bmod p$. Ainsi ω divise $p - 1$. D'après la condition sur p, on a nécessairement $\omega = 1$. Alors $2 \equiv 1 \bmod p$, ce qui est absurde. On a donc forcément $n = 1$.

(ii) Soit $n > 1$ tel que n divise $3^n + 1$. Soit p le plus petit facteur premier de n, qui est donc impair, qui vérifie donc $p > 3$. Alors $3^{2n} \equiv 1 \bmod p$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \bmod p$. Ainsi ω divise $p - 1$. On en déduit que ω divise $\text{pgcd}(2n, p - 1)$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas de figure, $3 \equiv 1 \bmod p$ et donc $p = 2$, ce qui est exclu. Dans le deuxième cas, $3^2 \equiv 1 \bmod p$ et donc p divise 8, ce qui est exclu également. On en déduit que $n = 1$.

Solution de l'exercice 3 On suppose $m, n \geqslant 2$. Soit p le plus petit diviseur de n. Alors $3^{2n} \equiv 1 \bmod p$. Soit ω l'ordre de 3 modulo p. Alors ω divise $2n$. D'autre part, d'après le petit théorème de Fermat, $3^{p-1} \equiv 1 \bmod p$. Ainsi ω divise $p-1$.

On en déduit que ω divise $\text{pgcd}(p-1, 2n)$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas de figure, Dans le premier cas de figure, $3 \equiv 1 \bmod p$ et donc $p = 2$. Dans le deuxième cas, $3^2 \equiv 1 \bmod p$ et donc $p = 2$. On en déduit que n est pair. On montre de même que m est pair. Alors 4 divise $3^{mn} + 1$, ce qui n'est pas possible car mn est pair.

Il reste à examiner le cas où m ou n vaut 1 et il vient que les solutions sont $(1,1)$, $(1,2)$ et $(2,1)$.

Solution de l'exercice 4 Il est clair que $q \geqslant 5$. Notons ω l'ordre 3/2 modulo q (rappelons que $1/2$ désigne l'inverse de 2 modulo q). Alors ω divise p, donc $\omega = 1$ ou p. Le premier cas n'étant pas possible, on a donc $\omega = p$. Or d'après le petit théorème de Fermat, $(3/2)^{q-1} \equiv 1 \bmod q$. On en tire que ω divise $q-1$, d'où le résultat.

Solution de l'exercice 5 Supposons que $n > 2$. Soit p le plus petit facteur premier de n. Alors p divise $(a+1)^n - a^n$. En d'autres termes, $((a+1)/a)^n \equiv 1 \bmod p$. Soit ω l'ordre de $(a+1)/a$ modulo p. Alors ω divise n. D'autre part, d'après le petit théorème de Fermat, $((a+1)/a)^{p-1} \equiv 1 \bmod p$ de sorte que ω divise $p-1$. D'après la condition sur p, nécessairement $\omega = 1$. Ceci implique $a + 1 \equiv a \bmod p$, ce qui est absurde.

Les solutions sont donc $n = 1$ et a quelconque.

Solution de l'exercice 6 Raisonnons par l'absurde et considérons un entier $k > 1$ tel que k^2 divise $a^k + b^k$. En raisonnant modulo 4 on voit que k est impair. Comme $a + b$ est une puissance de 2, il en découle que a et b sont premiers entre eux. Soit p le plus petit facteur premier de k qui est donc différent de 2 et ne divise ni a, ni b.

Soit ω l'ordre de a/b modulo p. Comme dans les exercices précédents, on voit que ω divise $2k$ ainsi que $p-1$. D'après la condition sur p, on a nécessairement $\omega = 1$ ou 2. Dans le premier cas de figure, $a \equiv b \bmod p$ et donc $2a^k \equiv 0 \bmod p$, ce qui est absurde. Dans le deuxième cas de figure, $a^2 \equiv b^2 \bmod p$. Ainsi p divise $(a-b)(a+b)$. On a vu que $a \equiv b \bmod p$ n'était pas possible. Mais comme $a + b = 2^\alpha$, on ne peut pas non plus avoir $a + b \equiv 0 \bmod p$ car p est impair. Ceci conclut la solution.

Solution de l'exercice 7 Les conditions de l'énoncé impliquent que $9^n \equiv 8^n \bmod 19$. Mais l'inverse de 8 modulo 19 est 12. On en déduit que $13^n \equiv 108^n \equiv (9 \times 8)^n \equiv 1 \bmod 19$. Or 13 est racine primitive modulo 19. Les entiers recherchés sont donc l'ensemble des multiples de 18.

Solution de l'exercice 8 Traitons d'abord le cas où a et b sont premiers entre eux.

Alors a et b sont premiers avec $a^n - b^n$ et il est clair que l'ordre de a/b modulo $a^n - b^n$ est n. On en déduit que n divise $\phi(a^n - b^n)$.

Si $d > 1$ est le PGCD de a et de b, notons $u = a/d$ et $v = b/d$ de sorte que u et v sont premiers entre eux. D'après ce qui précède, n divise $\phi(u^n - v^n)$. En utilisant la formule exprimant $\phi(n)$ en fonction des facteurs premiers de n, on voit que $\phi(u^n - v^n)$ divise $\phi(d^n(u^n - v^n)) = \phi(a^n - b^n)$, ce qui conclut.

Solution de l'exercice 9 Il est clair que a et p sont premiers entre eux. D'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \bmod p$. Comme $a^p \equiv 1 \bmod p$, on en déduit que $a \equiv 1 \bmod p$. On peut donc utiliser LTE et on obtient :

$$v_p(a-1) + 1 = v_p(a-1) + v_p(p) = v_p(a^p - 1).$$

Par hypothèse, le dernier terme est supérieur ou égal à n. Il en découle que $v_p(a-1) \geqslant n-1$, ce qu'il fallait démontrer.

Solution de l'exercice 10 Soit k tel que 3^k divise $2^n - 1$. En raisonnant modulo 3, on voit que n est pair. Écrivons donc $n = 2m$ avec $m > 0$. Alors 3^k divise $4^n - 1$. Comme 3 divise $4 - 1$, on peut appliquer LTE :

$$v_3(4-1) + v_3(n) = v_3(4^n - 1) \geqslant k.$$

On en déduit que $v_3(n) \geqslant k-1$. Ainsi $2 \times 3^{k-1}$ divise n.

Réciproquement, le même raisonnement nous donne que 3^k divise $2^n - 1$ si $2 \times 3^{k-1}$ divise n.