DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Cours et exercices

AUTEUR : Maxime ZAVIDOVIQUE
STAGE : Montpellier 2012

Ordre modulo n

- L'indicatrice d'Euler -

Soit $n \in \mathbb{N}$, on définit $\varphi(n)$ comme étant le nombre d'entiers $k \in \mathbb{N}$ tels que $k \wedge n = 1$, $k < n$. Cette fonction s'appelle l'indicatrice d'Euler. On notera aussi $\mathcal{A}(n)$ l'ensemble des tels k.

Le nombre $\varphi(n)$ correspond aussi au nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ (on dit que u est inversible s'il existe v tel que $uv \equiv 1[n]$). En effet, si $k \wedge n = 1$ par Bezout, on trouve u et v tels que $ku + nv = 1$, donc la classe de u est inverse de la classe de k modulo n. Réciproquement, s'il existe u tel que $ku \equiv 1[n]$ alors il existe v tel que $ku + nv = 1$, et donc $k \wedge n = 1$.

Pour calculer l'indicatrice d'Euler, on commence par montrer :

l'indicatrice d'Euler est une fonction multiplicative, c'est-à-dire que si $m \wedge n = 1$ alors $\varphi(mn) = \varphi(m)\varphi(n)$.

Pour le montrer on considère la fonction :

$$\begin{aligned} \mathcal{A}(mn) &\to \mathcal{A}(m) \times \mathcal{A}(n) \\ x &\mapsto (x_1, x_2), \end{aligned}$$

où x_1 est le reste de la division euclidienne de x par m et x_2 de x par n.

Cette application est bien définie, car comme $x \wedge m = 1$, alors $x_1 \wedge m = 1$ et par définition, $x_1 < m$. De même, $x_2 \wedge n = 1$ et $x_2 < n$.

Elle est injective : en effet si x et x' ont même image (x_1, x_2), alors $x - x'$ est divisible par m et par n, donc par mn (car $m \wedge n = 1$). Donc $x = x'$ (car $|x - x'| < mn$).

Enfin, elle est surjective, en effet, si $(x_1, x_2) \in \mathcal{A}(m) \times \mathcal{A}(n)$, on applique Bezout pour obtenir $um + vn = 1$ et on a alors que $X = umx_1 + vnx_2$ vérifie

$$X \equiv x_1[m], \quad X \equiv x_2[n].$$

Enfin x, le reste de la division de X par mn appartient bien à $\mathcal{A}(mn)$ et a pour image (x_1, x_2).

Comme l'application considérée est une bijection, on a bien montré, par identification des cardinaux des ensembles, que $\varphi(mn) = \varphi(m)\varphi(n)$.

Pour calculer $\varphi(n)$ il suffit maintenant de calculer $\varphi(p^\alpha)$, pour p premier. Mais il est clair que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, les seuls nombres non premiers avec p^α étant les nombres divisibles par p.

En résumé, si

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

alors

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

On montre ensuite le <u>*théorème d'Euler*</u> : si $a \wedge n = 1$, alors

$$a^{\varphi(n)} \equiv 1[n].$$

On considère ici l'application de $\mathcal{A}(n)$ dans lui-même qui à x associe le reste de la division de ax par n. Comme a et x sont premiers avec n, ax aussi, et l'application est bien définie. Cette application est injective car si x et x' ont même image, alors n divise $a(x - x')$ et donc n divise $x - x'$ par Gauss et enfin $x = x'$. C'est donc aussi une bijection.

Notons maintenant les x_i les éléments de $\mathcal{A}_n$, on a

$$\prod_{i=1}^{\varphi(n)} x_i \equiv \prod_{i=1}^{\varphi(n)} a x_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} x_i [n].$$

On peut maintenant simplifier par le gros produit pour obtenir $a^{\varphi(n)} \equiv 1[n]$.

Exercice 1 Déterminer le nombre des dizaines de milliers de $A = 5^{5^{5^5}}$.

<u>*Solution de l'exercice 1*</u> On va déterminer le reste de la division euclidienne de A par $10000 = 2^5 \times 5^5$. On commence par diviser par 2^5. Comme $\varphi(2^5) = 16$, il suffit de déterminer le reste de la division euclidienne de $5^{5^{5^5}}$ par 16 et enfin, comme $\varphi(16) = 8$, il faut déterminer le reste de 5^{5^5} par 8. Et enfin 5^5 par 4 soit 1.

Donc on remonte $5^{5^5} \equiv 5[8]$, $5^{5^{5^5}} \equiv 5^5 \equiv 13[16]$. Et enfin, $A \equiv 5^{13} \equiv 5^5[2^5]$.

Ouf, il vient que l'on n'est pas obligé de refaire tout le travail pour 5^5, on a immédiatement $A \equiv 5^5 = 3125[10000]$. Ainsi, le chiffre de dizaines de milliers de A est 0.

Revenons à notre couple (a, n) avec $a \wedge n = 1$. Une question pertinente maintenant est de savoir pour quels entiers $k \in \mathbb{N}$ on a $a^k \wedge 1[n]$. La solution utilise la notion d'ordre de a.

L'**ordre de** a **modulo** n est le plus petit entier k_0 tel que $a^{k_0} \wedge 1[n]$. L'ensemble des entiers k tels que $a^k \wedge 1[n]$ est exactement l'ensemble des multiples de k_0. Enfin, il vient du théorème d'Euler que $k_0 \mid \varphi(n)$.

En effet, si k vérifie $a^k \wedge 1[n]$, on effectue la division euclidienne de k par k_0 : $k = lk_0 + r$ et on trouve que

$$a^k \equiv a^{lk_0+r} \equiv a^r \equiv 1[n].$$

Ainsi, par minimalité de k_0 on doit avoir $r = 0$.

Exercice 2 Existe-t-il des entiers $n \geqslant 1$ tels que 9 divise $7^n + n^3$?

Solution de l'exercice 2 La réponse est non, voyons pourquoi. Soit n comme demandé. On a que n^3 est congru à 0, 1 ou -1 modulo 9 (c'est toujours vrai). Mais ici, n^3 ne peut pas être divisible par 9, donc on obtient que $n^6 \equiv 1[9]$. En particulier, $7^{2n} \equiv 1[n]$. Donc $2n$ est un multiple de l'ordre de 7 modulo 9. Cet ordre étant 3, n est un multiple de 3. C'est problématique vu que n^3 n'est pas divisible par 9.

- En vrac -

Exercice 3 Déterminer tous les couples d'entiers a, b tels que $a^b = b^a$.

Solution de l'exercice 3 On commence, comme d'habitude, par introduire $d = a \wedge b$ et écrire $a = da'$ et $b = db'$ où $a' \wedge b' = 1$.

On constate d'abord que $a = b$ est toujours solution.

On cherche les autres solutions. Sans perte de généralité (quitte à inverser les rôles de a et b), on va supposer que $a < b$. Ainsi, l'équation se réécrit

$$d^{b-a} a'^b = b'^a.$$

On voit tout de suite que $a' = 1$ car $a' \mid b'^a$ alors que $a' \wedge b'^a = 1$. Et donc $d = a$ et $b' \geqslant 2$:

$$d^{d(b'-1)} = b'^d.$$

On prend les racines d-ièmes :

$$d^{b'-1} = b',$$

et on a encore quelques cas à traiter. Si $d = 1$, alors $b' = 1$ ce qui n'est pas possible, on a exclu ce cas.

Si $d = 2$, on voit que pour $b' = 2$ on a une solution qui correspond à $a = 2, b = 4$. Ensuite, on montre (par récurrence ou par une étude de fonction) que pour $b' > 2$, alors $2^{b'-1} > b'$.

Enfin, si $d \geqslant 3$, la situation est encore plus dramatique et on montre que

$$d^{b'-1} \geqslant 3^{b'-1} > b'.$$

Ainsi, les seules solutions sont les couples (a, a), $(2, 4)$ et $(4, 2)$.

Exercice 4 Trouver tous les entiers a et b tels que $7^a - 3 \times 2^b = 1$.

Solution de l'exercice 4 On voit que $a = 0$ ou $b = 0$ sont impossibles. On réécrit l'équation comme suit :

$$7^a - 1 = 6 \times \sum_{i=0}^{a-1} 7^i = 6 \times 2^{b-1}.$$

Si $a = 1$, alors $b = 1$ est l'unique solution. Si $a = 2$ alors $b = 4$ est l'unique solution.

Supposons maintenant que $a > 2$ ce qui implique que $b > 4$. Comme la somme de gauche est paire, mais constituée d'éléments impairs, il doit y avoir un nombre pair de termes, a est donc pair. On regroupe termes pairs et impairs pour obtenir

$$(7 + 1) \sum_{i=0}^{a/2-1} 7^{2i} = 8 \times 2^{b-4}.$$

On simplifie, et on se rappelle que comme $b > 4$, la somme de gauche est paire mais encore constituée de termes impairs. Il y a donc un nombre pair de termes ($a/2$ est pair) et on peut recommencer la procédure :

$$(7^2 + 1) \sum_{i=0}^{a/4-1} 7^{4i} = 2^{b-4},$$

on aboutit à une contradiction car une puissance de 2 n'est pas divisible pas 50.

Les seules solutions sont donc $(1,1)$ et $(2,4)$.

Exercice 5 (OIM 99-4) Déterminer les couples d'entiers strictement positifs (n,p) tels que

– p est un nombre premier,
– $n \leqslant 2p$,
– $(p-1)^n + 1$ est divisible par n^{p-1}.

Solution de l'exercice 5 On trouve d'abord des solutions évidentes : $(1,p)$ est toujours solution.

Si $p = 2$, et $n > 1$ alors seul $n = 2$ fonctionne et $(2,2)$ est solution.

On suppose désormais que $p \geqslant 3$. Ainsi, n est nécessairement impair. Comme il est toujours plus simple de travailler avec des nombres premiers, soit q premier tel que $q \mid n$. Alors, les hypothèses impliquent $(p-1)^n \equiv -1[q]$, et plus généralement, $(p-1)^{an} \equiv (-1)^a[q]$. Fermat nous apprend aussi que $(p-1)^{b(q-1)} \equiv 1[q]$ car $p-1$ n'est pas divisible par q. On résume :

$$(p-1)^{an+b(q-1)} \equiv (-1)^a[q].$$

On se demande maintenant pour quelles valeurs de a et b on peut obtenir quelquechose d'intéressant, et on pense à Bezout. Mais il faut pour l'utiliser que $q-1 \wedge n = 1$. Pour ce faire, on suppose que q est le plus petit diviseur premier de n (qui est impair) et on prend a et b donnés par Bezout, de sorte que $an + b(q-1) = 1$. On voit immédiatement que a doit être impair, et donc

$$p - 1 \equiv -1[q]$$

soit $q \mid p$! Comme $n < 2p$ on a même que $n = p$, par minimalité de q.

On est prêt du but. En développant

$$(p-1)^p + 1 = \sum_{i=1}^{p} (-1)^{p-k} p^k \binom{p}{k} = p^2 + A,$$

on observe que A est divisible par p^3, donc $(p-1)^p + 1$ n'est pas divisible par p^3. Ainsi, on obtient que $p \leqslant 3$, soit $p = 3$ et $(3,3)$ est bien une solution du problème, la dernière.

Exercice 6 (OIM 2002-4) Soit n un entier strictement plus grand que 1. On note $d_1, d_2, \cdots, d_k$ les diviseurs positifs de n avec

$$1 = d_1 < d_2 < \cdots < d_k = n.$$

On pose $D = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$.

Montrer que $D < n^2$.

Trouver les n tels que D est un diviseur de n^2.

Solution de l'exercice 6 Il est clair que pour tout m, $d_{k-m} \leqslant n/(m+1)$. Ainsi, il vient que

$$\begin{aligned} D &\leqslant n^2\Big(\frac{1}{1\times 2} + \frac{1}{2\times 3} + \cdots + \frac{1}{(k-1)\times k}\Big) \\ &= n^2\Big(\frac{1}{1} - \frac{1}{\times 2} + \frac{1}{\times 2} - \frac{1}{\times 3} + \cdots + \frac{1}{k-1} - \frac{1}{k}\Big) \\ &= n^2\Big(1 - \frac{1}{k}\Big) < n^2. \end{aligned}$$

Pour la seconde partie de la question, on commence par remarquer que si n est premier, alors $D = d_1d_2 = n \mid n^2$.

Si n est composé, soit $p = d_2$ les plus petit diviseur premier de n. Alors

$$n^2 > D > d_{k-1}d_k = n \times \frac{n}{p} = \frac{n^2}{p}.$$

Mais c'est alors impossible que $D \mid n^2$ car n^2/p est le plus grand diviseur strict de n^2.

Exercice 7 Soit A la somme des chiffres de 2012^{2012}. On pose B la somme des chiffres de A, et C la somme des chiffres de B. Déterminer C.

Solution de l'exercice 7 On commence par majorer brutalement C. Comme $2012^{2012} \leqslant 10000^{2012}$, il possède moins de $4 \times 2012 + 1 < 10000$ chiffres, donc $A < 9 \times 10000 = 90000$. De même, $B < 9 \times 5 = 45$ et finalement $C \leqslant 13$.

Maintenant on regarde modulo 9 car on sait que l'opération de prendre la somme des chiffres laisse invariant cette congruence. Ainsi

$$2012^{2012} \equiv 5^{2012} \equiv 5^2 \equiv 7[9].$$

Ainsi, $C = 7$.

Exercice 8 (OIM 1990-4) Déterminer les entiers $n \in \mathbb{N}$ tels que $n^2 \mid 2^n + 1$.

Solution de l'exercice 8 Les solutions évidentes sont 1 et 3. Supposons dorénavant que $n > 1$. Au hasard, considérons p le plus petit entier qui divise n. Il est clair que n doit être impair, et donc que p aussi. L'hypothèse implique que $2^n \equiv -1[p]$ et donc que $2^{2n} \equiv 1[p]$. Ainsi, l'ordre de 2 modulo p divise $2n$.

Mais il divise également $p-1$ (petit théorème de Fermat) et par définition de p, $p-1 \wedge n = 1$. Ainsi on obtient que cet ordre vaut 1 ou 2. Dans le premier cas, on trouve $2 \equiv 1[p]$ ce qui est impossible, la seconde possibilité, implique que $p = 3$. On écrit donc $n = 3^l \times k$ et on va déterminer les valeurs possibles de l. Pour cela, on factorise

$$2^{3^l k} + 1 = (2^{3^{l-1}k} + 1)(2^{2\times 3^{l-1}k} - 2^{3^{l-1}k} + 1).$$

On voit que cette formule (en particulier le terme de gauche) ce prête particulièrement bien à une récurrence. On évalue le terme de droite modulo 9. 2 est d'ordre 6 modulo 9 et ses premières puissances sont $2, 4, -1, -2, -4, 1$. En se rappelant que k est impair, on obtient immédiatement que

$$2^{2\times 3^{l-1}k} - 2^{3^{l-1}k} + 1 \equiv 3[9].$$

Enfin, 2^k+1 est aussi divisible par 3, mais pas par 9, du fait que k est pair, mais pas divisible par 3. En conclusion, la valuation de 3 dans $2^{3^l k}+1$ est exactement $l+1$. Mais par hypothèse, $3^{2l} \mid 2^n + 1$, ainsi, la seule possibilité est que $l = 1$.

Maintenant qu'on a réglé son compte à 3, on passe au diviseur premier suivant. On suppose $k \geqslant 2$, sinon on a la solutions $n = 3$. Soit encore p le plus petit diviseur de k. Ainsi, $p \geqslant 5$, et on recommence comme tout à l'heure. De $2^{6k} \equiv 1[p]$ on déduit que l'ordre de 2 modulo p divise $6l$ mais aussi $p-1$ et donc par définition de p, il doit diviser 6. Il vaut dont 1, 2, 3, ou 6. Et on a que 2, 4, 8 ou 64 est congru à 1 modulo p. De tous ces cas, comme p n'est ni 2 ni 3, la seule possibilité est $p = 7$. Mais 7 ne divise jamais $2^n + 1$, en effet les puissances successives de 2 modulo 7 sont $2, 4, 1$. Il n'y a donc pas d'autre solution.

Exercice 9 Soient $a > b$ deux entiers premiers entre eux. Montrer que pour tout m, n entiers,

$$(a^m - b^m) \wedge (a^n - b^n) = a^{m\wedge n} - b^{m\wedge n}.$$

Solution de l'exercice 9 On pose $D = (a^m - b^m) \wedge (a^n - b^n)$ et $d = a \wedge b$. Posons $n = mq + r$ la division euclidienne de n par m. Essayons d'effectuer celle de $a^n - b^n$ par $a^m - b^m$:

$$a^n - b^n = a^{mq+r} - b^{mq+r} = a^r(a^{mq} - b^{mq}) + b^{mq}(a^r - b^r).$$

Or $a^{mq} - b^{mq} = (a^m - b^m)(a^{(q-1)m} + a^{(q-2)m}b^m + \cdots + a^m b^{(q-2)m} + b^{(q-1)m})$.

On n'a pas forcément la division euclidienne cherchée, mais on apprend tout de même que, comme $b^{mq} \wedge (a^m - b^m) = 1$ par le lemme de Gauss que $D \mid a^r - b^r$.

Ainsi, si $r_1, r_2, \ldots, d$ est la suite des restes dans l'algorithme d'Euclide, on obtient par récurrence immédiate que $D \mid a^d - b^d$.

Montrons maintenant que $a^d - b^d \mid D$ c'est-à-dire que c'est un diviseur commune à $a^m - b^m$ et $a^n - b^n$. Soit l tel que $n = ld$, alors on a vu comment $a^{ld} - b^{ld}$ est divisible par $a^d - b^d$. De même $a^m - b^m$ est divisible par $a^d - b^d$ donc $D = a^d - b^d$.