DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Exercices

AUTEUR : Vincent JUGÉ
STAGE : Montpellier 2013

Exercices d'arithmétique

- Énoncé des exercices -

Exercice 1 (Algorithme d'Euclide) Soit a et b deux entiers naturels, tels que $a \geqslant 1$. On définit les suites (u_n) et (v_n) telles que $u_0 = a$, $v_0 = b$ puis, si $v_k \neq 0$, $u_{k+1} = v_k$ et v_{k+1} est le reste dans la division Euclidienne de u_k par v_k. Montrer que les suites (u_n) et (v_n) sont nécessairement finies, et que $\mathrm{PGCD}(a, b)$ est égal au dernier terme u_k de la suite.

Exercice 2 Soit a, b et n trois entiers naturels, tels que $a \neq 0$. On note d le PGCD de a et b. Montrer que n divise a et b si et seulement si n divise d. En déduire, pour tout entier $c > 0$, la relation $\mathrm{PGCD}(ac, bc) = c\mathrm{PGCD}(a, b)$.

Exercice 3 Soit a un entier. Montrer que 2 divise $a^2 - a$ et que 3 divise $a^3 - a$.

Exercice 4 Soit $P(X) = aX^3 + bX^2 + cX + d$ un polynôme à coefficients entiers, et x, y deux entiers distincts. Montrer que $x - y$ divise $P(x) - P(y)$.

Exercice 5 Soit y un entier naturel non nul. Montrer que $y - 1$ divise $y^{(y^2)} - 2y^{y+1} + 1$.

Exercice 6 Trouver les entiers n tels que 5 divise $3n - 2$ et 7 divise $2n + 1$.

Exercice 7 Trouver les entiers n tels que 6 divise $n - 4$ et 10 divise $n - 8$.

Exercice 8 Trouver l'ensemble des entiers a tels que l'équation $2a^2 = 7k + 2$ admet une solution k entière.

Exercice 9 (JBMO 2013) Trouver les entiers naturels non nuls a et b tels que $\frac{a^3b-1}{a+1}$ et $\frac{b^3a+1}{b-1}$ sont entiers.

Exercice 10 Trouver l'ensemble des entiers a tels que 35 divise $a^3 - 1$.

Exercice 11 Trouver les entiers a et b tels que $3a^2 = b^2 + 1$.

Exercice 12 Trouver les entiers a, b et c tels que $a^4 + b^4 = c^4 + 3$.

Exercice 13 Montrer que l'équation $a^2 + b^2 + c^2 = 2007$ n'admet pas de solutions entières.

Exercice 14 Soit a, b et n trois entiers. Montrer que $\text{PGCD}(n^a - 1, n^b - 1) = n^{\text{PGCD}(a,b)} - 1$.

Exercice 15 (Ordre d'un élément) Soit a et n deux entiers naturels non nuls, premiers entre eux. Montrer qu'il existe un entier d tel que, pour tout entier $b \in \mathbb{N}$, n divise $a^b - 1$ si et seulement si d divise b.

Exercice 16 Soit $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des congruences modulo n représentant des entiers premiers avec n, a un élément de $(\mathbb{Z}/n\mathbb{Z})^*$. Montrer que la multiplication par a induit en fait une bijection de $\mathbb{Z}/n\mathbb{Z}$ sur lui-même, ainsi qu'une bijection de $(\mathbb{Z}/n\mathbb{Z})^*$ sur lui-même.

Exercice 17 (Petit théorème de Fermat) Soit a et n deux entiers naturels non nuls, premiers entre eux. On note $\varphi(n)$ le nombre d'entiers k tels que $0 < k < n$ et premiers avec 1. Montrer que n divise $a^{\varphi(n)} - 1$.

- Solutions des exercices -

Solution de l'exercice 1 On montre tout d'abord que les suites (u_n) et (v_n) sont finies. En effet, pour tout entier $n \geqslant 0$ tel que u_{n+1} et v_{n+1} sont définis, $0 \leqslant v_{n+1} < v_n = u_{n+1}$, car v_{n+1} et le reste d'une division par v_n. Ainsi, la suite (v_n) s'arrêtant dès qu'un de ses termes vaut 0, elle est nécessairement finie.

En outre, soit q_n tel que $u_n = q_n v_n + v_{n+1}$. Remarquons que, si d est un diviseur de u_n et de v_n, alors d divise $u_n - q_n v_n = v_{n+1}$; si $\overline{d}$ est un diviseur de v_n et de v_{n+1}, alors $\overline{d}$ divise $q_n v_n + v_{n+1} = u_n$. Ainsi, les diviseurs communs à u_n et v_n sont ceux communs à $v_n = u_{n+1}$ et v_{n+1} : ces deux ensembles de diviseurs on le plus grand élément maximal, ce qui signifie que $\text{PGCD}(u_n, v_n) = \text{PGCD}(u_{n+1}, v_{n+1})$.

Les termes $\text{PGCD}(u_n, v_n)$ sont donc égaux deux à deux. En particulier, si u_k est le dernier terme de la suite (u_n), alors $v_k = 0$, donc $\text{PGCD}(a, b) = \text{PGCD}(u_0, v_0) = \text{PGCD}(u_k, v_k) = u_k$.

Solution de l'exercice 2 Rappelons-nous la caractérisation du PGCD en utilisant $a\mathbb{Z}$ et $b\mathbb{Z}$: si a et b sont deux entiers naturels non nuls, $\text{PGCD}(a, b)$ est l'entier $d \geqslant 1$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. En particulier, d est l'élément minimal de l'ensemble $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*$.

Maintenant, soit $d = \mathrm{PGCD}(a, b)$ et $D = \mathrm{PGCD}(ac, bc)$. Puisque $D \in (ac)\mathbb{Z}+(bc)\mathbb{Z}$, il existe des entiers u, v, U et C que $au+bv = d$ et $acu+bcv = D$. En particulier, $D = (au + bv)c$ est divisible par c, et $\frac{D}{c} = au + bv$ est un élément de $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*$. De même, $(ac)u + (bc)v = cd$ est un élément de $(ac\mathbb{Z} + bc\mathbb{Z}) \cap \mathbb{N}^*$. Par minimalité de d et de D, on en déduit que $cd \geqslant D$ et que $\frac{D}{c} \geqslant d$, c'est-à-dire que $cd = D$.

Solution de l'exercice 3 On pourrait invoquer directement le petit théorème de Fermat ci-dessous, mais on va simplement considérer les deux cas séparément :

- Si $p = 2$, alors $a^2 - a = a(a-1)$: si a est pair, alors $a(a-1)$ aussi ; si a est impair, alors $a-1$ est pair, donc $a(a-1)$ aussi.
- Si $p = 3$, alors $a^3 - a = a(a-1)(a-2) + 3(a^2 - a)$: que 3 divise a, $a-1$ ou $a-2$, il divisera toujours $a^3 - a$.

Notons que l'on aurait également pu utiliser des congruences modulo 2 ou 3.

Solution de l'exercice 4 Regardons $P(x)$ et $P(y)$ modulo $x - y$: puisque $x \equiv y$ (mod. $x - y$), alors

$$P(x) \equiv ax^3 + bx^2 + cx + d \equiv ay^3 + by^2 + cy + d \equiv P(y) \text{ (mod. } x - y).$$

Cela signifie exactement que $x - y$ divise $P(x) - P(y)$.

Solution de l'exercice 5 Plaçons nous modulo $y - 1$: $y \equiv 1$ (mod. $y - 1$), donc $y^{(y^2)} - 2y^{y+1} + 1 \equiv 1^{(y^2)} - 2 \times 1^{y+1} + 1 \equiv 1 - 2 + 1 \equiv 0$ (mod. $y - 1$).

Solution de l'exercice 6 On va utiliser le théorème Chinois. Tout d'abord, en se plaçant modulo 5, on observe que $3n - 2 \equiv 0$ (mod. 5) si et seulement si $n \equiv 4$ (mod. 5). De même, en se plaçant modulo 7, on observe que $2n + 1 \equiv 0$ (mod. 7) si et seulement si $n \equiv 3$ (mod. 7).

Notons que 5 et 7 sont premiers entre eux : d'après le théorème de Bézout, il existe des entiers u et v tels que $5u + 7v = 1$. Par exemple, $(u, v) = (3, -1)$ convient. D'après le théorème Chinois, les entiers n tels que $n \equiv 4$ (mod. 5) et $n \equiv 3$ (mod. 7) sont donc les entiers $n \equiv 4(7v) + 3(5u) \equiv -11$ (mod. 35).

Les entiers recherchés sont donc les entiers de la forme $35k - 11$, où k est entier.

Solution de l'exercice 7 On va, une fois de plus, utiliser le théorème Chinois. Notons que $6 = 2 \times 3$ et que $10 = 2 \times 5$. Dire que $n \equiv 4$ (mod. 6) revient à dire que $n \equiv 4$ (mod. 2) et $n \equiv 1$ (mod. 3). Dire que $n \equiv 8$ (mod. 10) revient à dire que $n \equiv 8$ (mod. 2) et $n \equiv 8$ (mod. 5).

On cherche donc les entiers n tels que $n \equiv 0$ (mod. 2), $n \equiv 1$ (mod. 3) et $n \equiv 3$ (mod. 5). $n = -2$ est un tel entier. D'après le théorème Chinois, les entiers recherchés sont donc les entiers $n \equiv -2$ (mod. 30), c'est à dire les entiers de la forme $30k - 2$, où k est entier.

Solution de l'exercice 8 Le problème peut se reformuler comme suit : trouver les entiers a tels que $2a^2 \equiv 2$ (mod. 7). Une telle relation ne dépend que de la congruence de a modulo 7. On vérifie alors à la main que $2 \times 0^2 \equiv 0$ (mod. 7), $2 \times 1^2 \equiv 2 \times 6^2 \equiv 2$ (mod. 7), $2 \times 2^2 \equiv 2 \times 5^2 \equiv 1$ (mod. 7) et $2 \times 3^2 \equiv 2 \times 4^2 \equiv 4$ (mod. 7). Il s'ensuit que $\frac{2a^2-2}{7}$ est un entier si et seulement si a est de la forme $7\ell + 1$ ou $7\ell - 1$.

Solution de l'exercice 9 On veut trouver $a > 0$ et $b > 0$ entiers tels que $a^3b - 1 \equiv 0$ (mod. $a + 1$) et $b^3a + 1 \equiv 0$ (mod. $b + 1$). Or, $a \equiv -1$ (mod. $a + 1$), donc $a^3b - 1 \equiv (-1)^3b - 1 \equiv -(b + 1)$ (mod.$a + 1$). De même, $b \equiv 1$ (mod. $b - 1$), donc $b^3a + 1 \equiv 1a + 1 \equiv a + 1$ (mod.$b - 1$). En particulier, $b - 1$ divise alors $a + 1$, qui lui-même divise $b + 1$. Donc $b - 1$ divise $b + 1$ et divise même $(b + 1) - (b - 1) = 2$. Puisque $b - 1 \geqslant 0$, on en déduit que $b - 1 \in \{1, 2\}$:

1. si $b - 1 = 1$, $a + 1$ divise $b + 1 = 3$ et, puisque $a + 1 > 1$, on en déduit que $a + 1 = 3$;
2. si $b - 1 = 2$, $a + 1$ est pair et divise $b + 1 = 4$ et, puisque $a + 1 > 1$, on en déduit que $a + 1 = 2$ ou $a + 1 = 4$.

Les solutions (a, b) possibles sont donc $(2, 2)$, $(1, 3)$ et $(3, 3)$. On vérifie alors ces solutions donnent respectivement $\frac{a^3b-1}{a+1} = \frac{15}{3}, \frac{2}{2}, \frac{80}{4}$ et $\frac{b^3a+1}{b-1} = \frac{17}{1}, \frac{28}{2}, \frac{82}{2}$. Les couples recherchés sont donc bien $(2, 2)$, $(1, 3)$ et $(3, 3)$.

Solution de l'exercice 10 On pourrait procéder comme ci-dessus, regardant une par une les 35 classes de congruences modulo 35. Cela dit, il y a plus rapide, en utilisant le théorème Chinois.

En effet, puisque $35 = 5 \times 7$, $a^3 \equiv 1$ (mod. 35) si et seulement si $a^3 \equiv 1$ (mod. 5) et $a^3 \equiv 1$ (mod. 73). On vérifie alors à la main que $0^3 \equiv 0$ (mod. 7), que $1^3 \equiv 2^3 \equiv 4^3 \equiv 1$ (mod. 7) et que $3^3 \equiv 5^3 \equiv 6^3 \equiv 6$ (mod. 7) ; on vérifie également $0^3 \equiv 0$ (mod. 53), que $1^3 \equiv 1$ (mod. 5), que $2^3 \equiv 3$ (mod. 5), que $3^3 \equiv 2$ (mod. 5) et que $4^3 \equiv 4$ (mod. 5).

Ainsi, a est solution du problème si et seulement si $a \equiv 1, 2$ ou 4 (mod. 7), et $a \equiv 1$ (mod.5). D'après le théorème Chinois, ces conditions reviennent à dire que $a \equiv 1, 11$ ou 16 (mod. 35) Cela signifie que 35 divise $a^3 - 1$ si et seulement si a est de la forme $35\ell + 1$, $35\ell + 11$ ou $35\ell + 16$.

Solution de l'exercice 11 Dans ce genre d'exercices, où l'on doit manipuler un grand nombre tel que 2007, il est important de rechercher des simplifications du problème, par exemple en regardant ce qui se passe modulo de petits entiers.

C'est ainsi que l'on en vient tout naturellement, après quelques essais éventuellement infructueux, à considérer l'équation dans $\mathbb{Z}/8\mathbb{Z}$, où elle devient : $a^2+b^2+c^2 \equiv 7 \pmod 8$. Or, les carrés modulo 8 sont 0, 1 et 4.

Pour que l'équation soit vérifiée, il faut donc avoir au moins 2 carrés égaux à 4 modulo 8 (ce sans quoi leur somme vaudra ente 0 et 3 modulo 8), et alors cette somme sera égale au dernier carré, donc différente de 7 (modulo 8). Ainsi, l'équation $a^2 + b^2 + c^2 \equiv 7 \pmod 8$ n'admet aucune solution. *A fortiori*, l'équation $a^2 + b^2 + c^2 = 2007$ n'admet aucune solution en nombres entiers.

Solution de l'exercice 12 Tout d'abord, on note $d = \text{PGCD}(a, b)$ et $D = \text{PGCD}(n^a - 1, n^b - 1)$: on commence par montrer que $n^d - 1$ divise D. En effet, soit a' et b' deux entiers tels que $a = da'$ et $b = bd'$. Il s'ensuit que $n^a - 1 \equiv (n^d)^{a'} - 1 \equiv 1^{a'} - 1 \equiv 0 \pmod d$ et que $n^b - 1 \equiv (n^d)^{b'} - 1 \equiv 1^{b'} - 1 \equiv 0 \pmod d$. En particulier, cela signifie que d divise $n^a - 1$ et $n^b - 1$, donc divise D.

Réciproquement, montrons que D divise $n^d - 1$. Pour ce faire, on va montrer un autre résultat : si $x \geqslant y > 0$, alors $\text{PGCD}(n^x - 1, n^y - 1)$ divise $\text{PGCD}(n^y - 1, n^{x-y} - 1)$. Notons qu'on peut se douter qu'un tel résultat sera vrai, puisque $\text{PGCD}(x, y) = \text{PGCD}(y, x - y)$. Il nous suffit alors de montrer que $\text{PGCD}(n^x - 1, n^y - 1)$ divise $n^{x-y} - 1$, ce qui découle du fait que $n^x - 1 = n^{x-y}(n^y - 1) + (n^{x-y} - 1)$.

En remplaçant l'expression $\text{PGCD}(n^x - 1, n^y - 1)$ par $\text{PGCD}(n^{\min\{x,y\}} - 1, n^{|x-y|} - 1)$, les exposants que l'on obtient sont en fait des termes que l'on trouvera dans l'algorithme d'Euclide (sauf que, quand on a une division Euclidienne $a = bq + r$, on considère tous les couples $(b, r + kq)$ au lieu de passer directement de (a, b) à (b, r)). Ce faisant, on montre bien que $\text{PGCD}(n^a - 1, n^b - 1)$ divise $\text{PGCD}(n^d - 1, n^0 - 1) = n^d - 1$, ce qui conclut l'exercice.

Solution de l'exercice 13 Tout d'abord, en appliquant le principe des tiroirs, il existe deux entiers naturels $u < v$ tels que $a^u \equiv a^v \pmod n$. Cela veut dire que n divise $a^v - a^u = a^u(a^{v-u} - 1)$. Or, n est premier avec a, donc avec a^u : par théorème de Gauss, n divise $a^{v-u} - 1$, et il existe donc un plus petit entier $d > 0$ tel que $a^d \equiv 1 \pmod n$.

On note alors que, pour tout entier naturel k, $a^{dk} \equiv (a^d)^k \equiv 1^k \equiv 1 \pmod n$:

si b est un multiple de d, alors n divise $a^b - 1$. Réciproquement, si b n'est pas multiple de d, effectuons la division Euclidienne de b par d : $b = ud + v$, avec $0 < v < d$. Alors $a^b \equiv (a^d)^u a^v \equiv 1^u a^v \equiv a^v \not\equiv 1 \pmod{n}$, par définition de d. Cela montre bien que, si n divise $a^b - 1$, alors d divise b.

Solution de l'exercice 14 Tout d'abord, on note que $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^*$ sont deux ensembles finis. Il nous suffit donc de montrer que la multiplication par a induit une injection de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même, et envoie bien $(\mathbb{Z}/n\mathbb{Z})^*$ sur lui-même.

La première partie se montre comme suit : si $ab \equiv ac \pmod{n}$, alors n divise $a(b-c)$. Puisque n est premier avec a, le théorème de Gauss indique que n divise $b - c$, c'est-à-dire que $b \equiv c \pmod{n}$.

Quant à la deuxième partie, elle découle du fait que, si b est premier avec n, alors ab est premier avec n également : en effet, d'après le théorème de Gauss, ab n'admettra aucun facteur premier p commun avec n, puisqu'un tel p devrait diviser soit n et a, doit n et b.

Solution de l'exercice 15 On utilise ici le fait que la multiplication par a induit une bijection de $(\mathbb{Z}/n\mathbb{Z})^*$ sur lui-même. En effet, $\varphi(n)$ se trouve être exactement le cardinal de l'ensemble $(\mathbb{Z}/n\mathbb{Z})^*$. Notons f cette bijection.

L'idée est alors d'utiliser la bijection pour écrire une égalité de la forme $xa^{\varphi(n)} \equiv x \pmod{n}$, où x est premier avec n : il en résultera bien que $a^{\varphi(n)} \equiv 1 \pmod{n}$. En pratique, on procède en multipliant tous les éléments de $(\mathbb{Z}/n\mathbb{Z})^*$, qui sont en quantité $\varphi(n)$. D'un côté, ce produit est égal à $\prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} u$. De l'autre, en remarquant que $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ est une bijection, ce produit est aussi égal (modulo n) à

$$\prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} f(u) \equiv \prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} au \equiv a^{\varphi(n)} \left(\prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} u \right) \pmod{n}.$$

En posant $x = \prod_{u \in (\mathbb{Z}/n\mathbb{Z})^*} u$, on a donc la relation $xa^{\varphi(n)} \equiv x \pmod{n}$. Or, x est un produit d'éléments premiers avec n, donc x est premier avec n également. Il s'ensuit donc bien que $a^{\varphi(n)} \equiv 1 \pmod{n}$.