DOMAINE : Arithmétique
NIVEAU : Intermédiaire
CONTENU : Exercices

AUTEUR : François LO JACOMO
STAGE : Montpellier 2013

# Exercices d'arithmétique

**- Exercices -**

**Exercice 1**

Trouver tous les entiers congrus simultanément à 1 modulo 2, à 2 modulo 3, à 3 modulo 5 et à 4 modulo 7.

**Exercice 2**

Montrer que pour tout entier $n \geqslant 1$, dans toute suite arithmétique de raison $r$ (ensemble des $a_k = a + kr$ pour $k \in \mathbb{N}$, $a$ étant un entier donné quelconque) on peut trouver $n$ termes consécutifs $a_{K+1}, ...a_{K+n}$ tous composés (c'est-à-dire non premiers).

**Exercice 3**

On considère une suite $(p_n)$ de nombres premiers définie par $p_0, p_1$ et pour tout $n \geqslant 1$, $p_{n+1}$ est le plus grand facteur premier de $p_{n-1} + p_n + 100$. Montrer que cette suite est bornée (c'est-à-dire qu'il existe $P$ tel que pour tout $n$, $p_n \leqslant P$).

**Exercice 4**

Montrer que pour tout $n \geqslant 2$, on peut trouver un ensemble $A = \{a_1, a_2, \cdots a_n\}$ de $n$ entiers distincts tous $\geqslant 2$ tel que pour tout entier $k$ tel que $1 \leqslant k \leqslant n$ le produit des $n-1$ entiers de $A$ autres que $a_k$ soit congru à 1 ou $-1$ modulo $a_k$.

**Exercice 5**

Soit $p$ un nombre premier. A quelle condition existe-t-il un entier $k$ tel que $k^2 \equiv -1 \pmod{p}$ ?

**Exercice 6**

Trouver tous les triplets d'entiers $(x, y, z)$ tels que $x^2 + y^2 + z^2 - 2xyz = 0$.

**Exercice 7**

Soient $a$ et $b$ des entiers naturels non nuls et premiers entre eux, tels que $a \geqslant 2$. Montrer que si $a^m + b^m$ divise $a^n + b^n$, alors $m$ divise $n$.

**Exercice 8**

Montrer qu'il n'existe aucun entier $n > 1$ tel que $n$ divise $2^n - 1$.

**Exercice 9**

Trouver tous les couples d'entiers positifs $(x, y)$ tels que : $7^x - 3 \cdot 2^y = 1$.

**- Solutions -**

*Solution de l'exercice 1*

C'est une mise en pratique immédiate du théorème chinois : $2, 3, 5, 7$ étant deux à deux premiers entre eux, puisqu'ils sont premiers, n'importe quel système d'équations : $x \equiv a \pmod 2, x \equiv b \pmod 3, x \equiv c \pmod 5, x \equiv d \pmod 7$ admet une infinité de solutions, de la forme : $x \equiv N \pmod{2\times3\times5\times7}$. On commence par résoudre les deux premières équations : $x \equiv 1 \pmod 2$ entraine $x \equiv 1, 3$ ou $5 \pmod{2 \times 3}$ et comme 2 et 3 sont premiers entre eux, $1, 3, 5$ prend toutes les valeurs possibles modulo 3, donc une fois la valeur voulue 2 : $x \equiv 1 \pmod 2$ et $x \equiv 2 \pmod 3$ entraine $x \equiv 5 \pmod 6$ donc $x \equiv 5, 11, 17, 23$ ou $29 \pmod{6 \times 5}$. Parmi ces cinq valeurs, une et une seule, 23, est congrue à 3 modulo 5. Donc $x \equiv 23, 53, 83, 113, 143, 173, 203 \pmod{30 \times 7}$). Une et une seule de ces sept valeurs est congrue à 4 modulo 7, en l'occurrence 53, donc la solution du problème est : $x \equiv 53 \pmod{210}$.

*Solution de l'exercice 2*

C'est une conséquence du théorème chinois. Pour prouver que des nombres sont non premiers, il suffit de leur trouver des diviseurs. Par exemple, $n$ nombres premiers distincts, donc premiers entre eux deux à deux, $p_1, p_2, \cdots p_n$. On cherchera donc $x$ tel que $x + r$ divisible par $p_1$, $x + 2r$ divisible par $p_2$, $\cdots x + nr$ divisible par $p_n$, ce qui peut s'écrire : $x \equiv -r \pmod{p_1}, x \equiv -2r \pmod{p_2}, \cdots x \equiv -nr \pmod{p_n}$. Le théorème chinois affirme qu'il existe une infinité de tels $x$, qui peuvent s'écrire : $x \equiv R \pmod{p_1 p_2 \cdots p_n}$. Mais encore faut-il que ce $x$ soit dans la suite arithmétique donnée, donc que $x = a + kr$, ou encore $x \equiv a \pmod r$. Si l'on a choisi nos $p_i$ tous premiers avec $r$, nous avons une nouvelle application du théorème chinois, qui fournit une infinité de tels $x$ sous la forme : $x \equiv Q \pmod{r \times p_1 p_2 \cdots p_n}$. Et il reste une dernière chose à vérifier : que $x + r$ n'est pas égal à $p_1$ ni $x + 2r$ à $p_2$ ni $x + nr$ à $p_n$. Il suffit pour cela que $x$ soit plus grand que tous les $p_i$, par exemple qu'il soit plus grand que leur produit : parmi les $x \equiv Q \pmod{rp_1 \cdots p_n}$, si $Q > 0$, tous

les $krp_1 \cdots p_n + Q$ pour $k \geqslant 1$ sont largement assez grands pour que le risque soit exclu.

*Solution de l'exercice 3*

L'idée est de prouver que ces nombres premiers ne croissent que de manière limitée, et qu'à un moment ils se trouveront face à une succession de nombres non premiers qu'ils ne parviendront pas à franchir.

Tout d'abord, ce n'est pas $p_n$ qui croît de manière limitée, mais $b_n = max(p_n, p_{n-1})$. Par ailleurs, soit l'un des deux nombres premiers $p_n$ ou $p_{n-1}$ est égal à 2, auquel cas $p_{n+1}$ est le plus grand facteur premier de $b_n + 2 + 100$, soit les deux nombres premiers $p_n$ et $p_{n+1}$ sont tous deux impairs, auquel cas $p_{n-1}+p_n+100$ est pair et distinct de 2, son plus grand facteur premier est au plus la moitié : $\frac{p_{n-1}+p_n+100}{2} \leqslant b_n + 50$ car par hypothèse $p_n$ et $p_{n-1}$ sont tous deux inférieurs ou égaux à $b_n$. Dans tous les cas, $b_{n+1} \leqslant b_n + 102$.

Or il n'est pas difficile de trouver une plage de 102 nombres consécutifs tous composés : par exemple, $103! + 2$ est divisible par 2, $103! + 3$ est divisible par 3, $\cdots 103! + 103$ est divisible par 103. Mais encore faut-il initialiser la récurrence : rien ne prouve que $b_1 \leqslant 103! + 1$.

On peut néanmoins affirmer qu'il existe un $k$ tel que $b_1 \leqslant k \cdot 103! + 1$. Et l'hypothèse de récurrence que nous utiliserons est que pour tout $n$, $b_n \leqslant k \cdot 103! + 1$. C'est manifestement vrai pour $n = 1$ (initialisation), et si c'est vrai pour $n$ donné, la relation ci-dessus entraîne que $b_{n+1} \leqslant b_n + 102 \leqslant k \cdot 103! + 103$. Or $b_{n+1}$ est par définition un nombre premier, et aucun des nombres $k \cdot 103! + 2$, $k \cdot 103! + 3, \cdots k \cdot 103! + 103$ n'est premier, donc nécessairement $b_{n+1} \leqslant k \cdot 103! + 1$, ce qui achève la démonstration.

*Solution de l'exercice 4*

Démontrons-le par récurrence : pour $n = 2$ (initialisation), l'ensemble $A_2 = \{2, 3\}$ convient, puisque $2 \equiv -1 \pmod 3$ et $3 \equiv 1 \pmod 2$. Supposons donc qu'un tel ensemble existe avec $n$ éléments, $A_n = \{a_1, a_2 \cdots a_n\}$ et construisons l'ensemble $A_{n+1}$ en ajoutant un $(n+1)-$ième élément $a_{n+1}$ à $A_n$. Pour que la condition de l'énoncé soit remplie, $a_{n+1}$ doit être congru à 1 ou $-1$ modulo $a_1 a_2 \cdots a_n$, on choisira donc : soit $a_{n+1} = (a_1 a_2 \cdots a_n) + 1$ soit $a_{n+1} = (a_1 a_2 \cdots a_n) - 1$. Ces deux valeurs conviennent toutes les deux, car si l'on considère un élément $a_k$ pour $1 \leqslant k \leqslant n$, par hypothèse de récurrence le produit des $(n-1)$ éléments de $A_n$ autres que $a_k$ est congru à 1 ou $-1$ modulo $a_k$, et $a_{n+1}$ est lui aussi congru à 1 ou $-1$ modulo $a_k$, donc le produit des $n$ éléments de $A_{n+1}$ autres que $a_k$ est bien congru à 1 ou $-1$ modulo $a_k$.

*Solution de l'exercice 5*

Trouver une condition nécessaire et suffisante exige des outils mathématiques que vous n'avez pas, mais vous pouvez au moins trouver une condition nécessaire. Si $k^2 \equiv -1 \pmod{p}$, $k^4 \equiv 1 \pmod{p}$, donc l'ordre de $k$ - plus petit exposant $n$ tel que $k^n \equiv 1 \pmod{p}$ - divise 4. Si $-1 \neq 1 \pmod{p}$, donc si $p \neq 2$ (pour $p = 2$, la condition est vérifiée), cet ordre n'est pas 2 car $k^2 \equiv -1 \pmod{p}$, ce n'est a fortiori pas 1 car si $k \equiv 1 \pmod{p}$, on aurait $k^2 \equiv 1 \pmod{p}$, donc c'est nécessairement 4. Or tout autre $n$ tel que $k^n \equiv 1 \pmod{p}$ est divisible par l'ordre 4 de $k$ - sinon, on aurait $n = 4k + r$ avec $0 \leqslant r < 4$ et $k^r \equiv 1 \pmod{p}$ ce qui contredirait la minimalité -. Par ailleurs, d'après le théorème de Fermat, comme $k$ n'est pas divisible par $p$ (sinon on aurait $k^2 \equiv 0 \pmod{p}$ -, $k^{p-1} \equiv 1 \pmod{p}$, ce qui entraîne que $p-1$ est divisible par 4. Une condition nécessaire est donc que $p = 2$ ou $p \equiv 1 \pmod{4}$.

Donnons un aperçu de la preuve que cette condition est suffisante. On travaille dans l'ensemble des classes de congruence modulo $p$ : $a$ et $b$ sont dans la même classe si $a \equiv b \pmod{p}$. Cet ensemble de classes, $\mathbb{Z}/p\mathbb{Z}$, est muni d'une addition et d'une multiplication, car si $a \equiv b \pmod{p}$ et $a' \equiv b' \pmod{p}$, $a + a' \equiv b + b' \pmod{p}$ et $aa' \equiv bb' \pmod{p}$. Les éléments $k$ et $-k$ ont même carré : les "carrés parfaits" (on les appelle : résidus quadratiques) de $\mathbb{Z}/p\mathbb{Z}$ sont donc 0 et au plus la moitié des $p-1$ autres éléments. En réalité, c'est exactement la moitié des $p-1$ autres éléments, et un entier donné, par exemple $-1$, a "une chance sur deux" d'être résidu quadratique (pour environ la moitié des nombres premiers, $-1$ est résidu quadratique). Car - et c'est là qu'il conviendrait d'approfondir - l'équation $x^2 = a$ ne peut pas avoir plus de deux racines distinctes, et plus généralement un polynôme de degré $d$ ne peut pas avoir plus de $d$ racines distinctes, tout comme dans l'ensemble des réels par exemple. Or dans $\mathbb{Z}/p\mathbb{Z}$, l'équation : $x^{p-1} = 1$ a $p-1$ racines distinctes : tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$. Si $p$ est impair, et $x$ non nul, $x^{\frac{p-1}{2}}$ a pour carré 1, il est donc égal soit à 1 soit à $-1$. Si $x$ est résidu quadratique, il existe $y$ tel que $y^2 = x$, donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$ : tous les résidus quadratiques sont racines de $x^{\frac{p-1}{2}} = 1$. Mais comme il existe $\frac{p-1}{2}$ résidus quadratiques, et que cette équation de degré $\frac{p-1}{2}$ ne peut pas avoir plus de $\frac{p-1}{2}$ racines, toutes ses racines sont résidus quadratiques. Dès lors, si $(-1)^{\frac{p-1}{2}} = 1$, $-1$ est résidu quadratique. Or si $p \equiv 1 \pmod{4}$, $(-1)^{\frac{p-1}{2}} = 1$, d'où le résultat.

*Solution de l'exercice 6*

Tout d'abord, puisque $x^2 + y^2 + z^2$ est pair, $x, y, z$ ne peuvent pas être tous

trois impairs : l'un au moins est pair, ce qui entraîne que $2xyz = x^2 + y^2 + z^2$ est divisible par 4. Mais modulo 4, un carré ne peut être congru qu'à 0 ou 1. Donc pour que $x^2+y^2+z^2 \equiv 0 \pmod 4$, il est nécessaire que $x^2$, $y^2$ et $z^2$ soient tous trois $\equiv 0 \pmod 4$, donc $x, y, z$ tous trois pairs.

Montrons par récurrence que pour tout $n$, $x, y, z$ doivent être tous trois multiples de $2^n$. C'est vrai, nous venons de le voir, pour $n = 1$ : la récurrence est initialisée. Supposons-le vrai pour $n \geqslant 1$, et posons $x = 2^n x_n, y = 2^n y_n$ et $z = 2^n z_n$. L'équation s'écrit : $2^{2n}(x_n^2 + y_n^2 + z_n^2) = 2^{3n+1} x_n y_n z_n$, ou encore $x_n^2+y_n^2+z_n^2 = 2^{n+1} x_n y_n z_n$. Comme $n \geqslant 1$, $x_n^2+y_n^2+z_n^2$ est divisible par 4, donc d'après le raisonnement ci-dessus, $x_n, y_n$ et $z_n$ sont tous les trois pairs, ce qui signifie que $x, y, z$ sont tous trois divisibles par $2^{n+1}$.

Or un entier non nul ne peut pas être divisible par toutes les puissances de 2. Si $k$ est l'exposant de 2 dans la décomposition en facteurs premiers de $x$, pour $n > k$, $x$ n'est pas divisible par $2^n$. La récurrence ci-dessus implique donc que $x, y$ et $z$ sont nécessairement tous trois nuls. La seule solution de l'équation est $(0, 0, 0)$.

*Solution de l'exercice 7*

Ecrivons la division euclidienne de $n$ par $m$ : $n = mq + r$ avec $0 \leqslant r < m$. Si $q$ est impair, $a^m + b^m$ divise $a^{qm} + b^{qm}$, donc on utilisera la relation : $a^n + b^n = a^r(a^{qm} + b^{qm}) - b^{qm}(a^r - b^r)$ pour en déduire que $a^m + b^m$ doit diviser $a^r - b^r$, ce qui n'est possible que si $r = 0$ car $|a^r - b^r| < a^m + b^m$. Si $q$ est pair, $a^m + b^m$ divise $a^{2m} - b^{2m}$, donc également $a^{qm} - b^{qm}$, et on utilisera la relation : $a^n + b^n = a^r(a^{qm} - b^{qm}) + b^{qm}(a^r + b^r)$ pour en déduire que $a^m + b^m$ doit diviser $a^r + b^r$, ce qui n'est jamais possible car $0 < a^r + b^r < a^m + b^m$. Donc $a^m + b^m$ ne peut diviser $a^n + b^n$ que si $q$ est impair et $r = 0$, c'est-à-dire si $n$ est multiple impair de $m$.

*Solution de l'exercice 8*

Soit $p$ le plus petit facteur premier de $n$, et $k$ l'ordre de 2 par rapport à $p$, c'est-à-dire le plus petit exposant non nul tel que $2^k \equiv 1 \pmod p$. D'après le théorème de Fermat, $k \leqslant p - 1 < n$, et l'on a par ailleurs $k \geqslant 2$ car 2 n'est pas congru à 1 modulo $p$. Or par hypothèse, $2^n \equiv 1 \pmod p$, ce qui entraîne : $k$ divise $n$. $k$ est donc un facteur de $n$ strictement plus petit que $p$, ce qui contredit le fait que $p$ est le plus petit facteur premier de $n$. On en conclut (raisonnement par l'absurde) qu'il n'existe aucun $n > 1$ qui divise $2^n - 1$.

*Solution de l'exercice 9*

Il s'agit d'une équation diophantienne, c'est-à-dire d'une équation à ré-

soudre en nombres entiers. Certaines de ces équations diophantiennes sont parmi les problèmes les plus difficiles des mathématiques.

Ecrivons l'équation : $7^x - 1 = 3 \cdot 2^y$. On ne peut pas avoir $x = 0$ car le membre de droite ne peut pas être nul. Or pour $x \geqslant 1$, le membre de gauche est divisible par $7 - 1 = 6$. Plus précisément, après simplification par $7 - 1$, on trouve : $7^{x-1} + 7^{x-2} + \cdots + 7 + 1 = 2^{y-1}$. On voit là une première solution évidente : $x = 1, y = 1$. Pour $x > 1$, le membre de gauche contient $x$ termes tous impairs, et le membre de droite est une puissance de 2 autre que 1. Donc $x$ doit être pair, pour que la somme de gauche soit paire. On peut donc grouper les termes deux par deux et factoriser $(7 + 1)$ à gauche : $(7 + 1)(7^{x-2} + 7^{x-4} + \cdots + 49 + 1 = 8 \cdot 2^{y-4}$. D'où une deuxième solution évidente : $x = 2, y = 4$. Pour $x > 2$, après simplification par 8, le membre de gauche contient une somme de $\frac{x}{2}$ termes, tous impairs, distincte de 1 et égale à une puissance de 2, donc paire, ce qui entraîne que $\frac{x}{2}$ doit être pair, et on peut factoriser à gauche $7^2 + 1 = 50$ : $(7^2 + 1)(7^{x-4} + 7^{x-8} + \cdots + 1 = 2^{y-4}$. Mais 50 ne peut pas diviser une puissance de 2, donc il n'existe pas de racine pour $x > 2$. Les seuls couples solution sont donc : $(1, 1)$ et $(2, 4)$.