

---

## Arithmétique modulaire

---

### Solutions

**Exercice 1** – La comète  $A$  est visible l'année  $n$  si et seulement si on a la congruence  $n \equiv 2014 \pmod{5}$ . De même, l'année de passage de la comète  $B$  vérifie la congruence  $n \equiv 2013 \pmod{8}$ . On est donc ramené à résoudre le système

$$\begin{cases} n \equiv 4 \pmod{5}, \\ n \equiv 5 \pmod{8}. \end{cases}$$

En considérant l'identité de Bézout  $2 \cdot 8 - 3 \cdot 5 = 1$ , on obtient la solution particulière  $n_0 = 4 \cdot 2 \cdot 8 - 5 \cdot 4 \cdot 5 = -11$  et le théorème des restes chinois affirme que la solution générale est donnée par l'expression  $n = 40m - 11$ , avec  $m$  entier. La plus petite valeur de  $n$  supérieure ou égale à 2015 est alors  $n = 2029 = 40 \cdot 51 - 11$ .

**Exercice 2** – Un entier  $n$  est congru à 1 modulo 2, 3, 4, 5 et 6 si et seulement si  $n - 1$  est divisible par 3, 4 et 5. Ces derniers entiers étant premiers entre eux deux à deux, le lemme de Gauss affirme que  $n - 1$  est divisible par leur produit  $3 \cdot 4 \cdot 5 = 60$ , ce qui amène à l'identité  $n = 60m + 1$ , avec  $m$  entier.

On cherche  $n$  multiple de 7 :  $\exists k \in \mathbb{Z}$  t.q.  $60m + 1 = 7k \Leftrightarrow 4m + 1 = 7(k - 8m)$ . Cela nous donne  $4m \equiv 6 \pmod{7}$ , donc  $m \equiv 6 \times 2 \equiv 5 \pmod{7}$ . On en déduit que la plus petite valeur positive de  $n$  qui satisfait est  $n = 301 = 60 \cdot 5 + 1$ . Cependant, le plus petit  $n$  en valeur absolue est  $n = -119 = 60 \cdot (-2) + 1$ .

**Exercice 3** – La congruence  $9 \equiv -4 \pmod{13}$  amène aux relations

$$2^{70} + 3^{70} \equiv 4^{35} + 9^{35} \equiv 4^{35} + (-4)^{35} \equiv 4^{35} + (-1)^{35} 4^{35} \equiv 4^{35} - 4^{35} \equiv 0 \pmod{13}.$$

**Exercice 4** – D'après le petit théorème de Fermat, pour tout entier  $a$  premier avec 13, on a la congruence  $a^{12} \equiv 1 \pmod{13}$ . En effectuant deux divisions euclidiennes, on obtient les identités  $100 = 7 \cdot 13 + 9$  et  $1000 = 83 \cdot 12 + 4$ , ce qui amène aux congruences

$$100^{1000} \equiv 9^4 \equiv (-4)^4 \equiv 16^2 \equiv 3^2 \equiv 9 \pmod{13}$$

et le reste de la division euclidienne de  $100^{1000}$  par 13 est donc 9.

**Exercice 5** – Posons  $N = a^n - 1$ . La congruence  $a^n \equiv 1 \pmod{N}$  implique que  $a$  est premier avec  $N$  et que son ordre  $d$  (en tant qu'élément de  $(\mathbb{Z}/N\mathbb{Z})^\times$ ) divise  $n$ . De plus, pour tout entier  $m$  vérifiant  $0 < m < n$ , on a l'inégalité  $0 < a^m - 1 < a^n - 1$  et, en particulier, l'entier  $a^m$  n'est pas congru à 1 modulo  $N$ . On en déduit l'identité  $d = n$  et le théorème de Lagrange affirme alors que  $n$  divise l'ordre de  $(\mathbb{Z}/N\mathbb{Z})^\times$ , qui est égal à  $\varphi(N)$ .

**Exercice 6 –**

1. L'entier  $N$  étant un multiple commun à  $n$  et  $m$ , pour tout élément  $x = (a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ , on a les identités

$$Nx = N(a, b) = (Na, Nb) = (0, 0) = 0.$$

2. Si  $\text{pgcd}(n, m) > 1$ , on a l'inégalité stricte  $N < nm$ . D'après le point précédent, tout élément de  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$  est d'ordre divisant  $N$ . Le groupe  $\mathbb{Z}/nm\mathbb{Z}$  étant cyclique, il possède un élément d'ordre  $nm$  et ne peut donc pas être isomorphe à  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ .

**Exercice 7 –** D'après le petit théorème de Fermat, pour tout entier  $a$  premier avec 19, on a la relation  $2^{18} \equiv 1 \pmod{19}$ . Pour tout entier naturel  $n$ , on a les congruences

$$2^{6n+2} \equiv 0 \equiv 4 \pmod{2} \text{ et}$$

$$2^{6n+2} \equiv 4 \cdot (2^6)^n \equiv 4 \cdot 64^n \equiv 4 \pmod{9}.$$

Le théorème des restes chinois affirme alors que  $2^{6n+2}$  est congru à 4 modulo 18, ce qui amène aux relations

$$2^{2^{6n+2}} + 3 \equiv 2^4 + 3 \equiv 16 + 3 \equiv 0 \pmod{19}.$$

**Exercice 8 –**

1. Notons  $\bar{a}$  la classe de  $a \in \mathbb{Z}$  dans  $\mathbb{Z}/n\mathbb{Z}$ . De manière générale, l'élément  $\bar{a}$  est nilpotent si et seulement si tout diviseur premier  $p$  de  $n$  divise  $a$ . En effet la condition  $\bar{a}^m = 0$  implique que  $p$  divise  $a^m$  et donc que  $p$  divise  $a$  (car  $p$  est premier). Réciproquement, si tout diviseur premier  $p$  de  $n$  divise  $a$ , en posant  $m = \max_{p|n} \{v_p(n)\}$ , on en déduit que  $n$  divise  $a^m$  et donc que  $\bar{a}$  est nilpotent. Supposons maintenant  $n$  sans facteur carré et posons  $n = p_1 \cdots p_r$  avec  $p_1 < \cdots < p_r$  premiers. D'après ce qui précède, l'élément  $\bar{a}$  est nilpotent si et seulement si, pour tout  $i \in \{1, \dots, r\}$ , le nombre premier  $p_i$  divise  $a$  et le lemme de Gauss affirme alors que  $a$  est un multiple de  $n$ , ou encore que  $\bar{a} = 0$ . L'anneau  $\mathbb{Z}/n\mathbb{Z}$  est donc réduit. Réciproquement, si  $n$  est divisible par un carré, soit  $n = u^2v$ , avec  $u > 0$ , en considérant l'entier  $a = uv$ , on a les relations  $\bar{a} \neq 0$  et

$$a^2 \equiv u^2v^2 \equiv vn \equiv 0 \pmod{n}.$$

L'élément  $\bar{a}$  est alors un élément nilpotent non nul et l'anneau  $\mathbb{Z}/n\mathbb{Z}$  n'est pas réduit.

2. On a la factorisation  $40 = 2^3 \cdot 5$ . Les éléments nilpotents de  $\mathbb{Z}/40\mathbb{Z}$  sont les classes  $\bar{a}$ , où  $a$  est un entier naturel inférieur ou égal à 40 et divisible par 10. On obtient donc  $a \in \{0, 10, 20, 30\}$ .

### Exercice 9 –

1. La factorisation  $65 = 5 \cdot 13$  amène à l'identité  $\varphi(65) = 4 \cdot 12 = 48$ . En appliquant l'algorithme d'Euclide, on montre que 13 est l'inverse de 37 modulo 48 et la clé privée d'Alice est donc le couple  $(13, 48)$ .
2. Le message initial  $m$  est égal au reste de la division Euclidienne de  $3^{13}$  par 65. On remarquera que le petit théorème de Fermat affirme que  $3^{12}$  est congru à 1 modulo 5 et 12. En appliquant le théorème des restes chinois, on obtient alors la congruence  $3^{12} \equiv 1 \pmod{65}$ , ce qui donne  $3^{13} \equiv 3 \pmod{65}$ , d'où l'identité  $m = 3$ .

### Exercice 10 –

1. Afin de déterminer  $M$ , il suffit de connaître l'entier  $M^3$  (il existe en effet des algorithmes rapides d'extraction de racine cubique d'un entier). On a les congruences

$$\begin{cases} M^3 \equiv A \pmod{a}, \\ M^3 \equiv B \pmod{b}, \\ M^3 \equiv C \pmod{c}, \end{cases}$$

et, les entiers  $a, b$  et  $c$  étant premiers entre eux deux à deux, le théorème des restes chinois affirme que l'entier  $M^3$  est univoquement déterminé modulo  $abc$  et fournit une méthode explicite pour le déterminer. Finalement, l'inégalité  $M < \min\{a, b, c\}$  amène à la relation  $M^3 < abc$  et l'entier  $M^3$  est donc l'unique solution du système ci-dessus vérifiant la condition  $0 < M^3 < abc$ .

2. Nous allons illustrer la méthode présentée dans le point précédent par un exemple explicite, en posant  $(a, b, c) = (35, 38, 39)$  et  $(A, B, C) = (1, 1, 5)$  : on a le système de congruences

$$\begin{cases} M^3 \equiv 1 \pmod{35}, \\ M^3 \equiv 1 \pmod{38}, \\ M^3 \equiv 5 \pmod{39}. \end{cases}$$

On en déduit tout d'abord que l'entier  $M^3$  est congru à 1 modulo  $1330 = 35 \cdot 38$ . L'algorithme d'Euclide amène à l'identité de Bézout  $10 \cdot 1330 - 341 \cdot 39 = 1$ , ce qui donne la solution particulière  $53201 = 5 \cdot 10 \cdot 1330 - 1 \cdot 341 \cdot 39$ . La solution générale est donc donnée par l'expression  $53201 + 51870m$ , avec  $m$  entier, ce qui donne  $M^3 = 1331 = 11^3$  (en posant  $m = -1$ ), d'où  $M = 11$ .