Corrigé et barème – Arithmétique — congruences et applications

Congruences modulo n, critères de divisibilité et arithmétique modulaire (programme de Maths expertes Terminale)

Durée : 120 min – Calculatrice interdite – Sur 20 points · Maths expertes (option Tle) Terminale

Exercice 1 – Restes et critères de divisibilité *(4 pts)*

a) Somme des chiffres : $3+4+2+8=17\equiv 8\ [9]$ (car $17=9+8$). Reste : **8** (vérification : $9\times 380=3\,420$). (1)

b) Somme alternée à partir des unités : $8-2+4-3=7$. Reste : **7** (vérification : $11\times 311=3\,421$). (1)

c) $99=9\times 11$; or 3 428 n'est pas divisible par 9 (reste 8), donc il ne l'est pas non plus par 99. (1)

d) $3\,428^2\equiv 8^2=64\ [9]$ et $64=7\times 9+1$: le reste est **1**. (1)

Erreur fréquente — La somme alternée du critère par 11 se calcule en partant du chiffre des unités, affecté du signe $+$.

Exercice 2 – Grandes puissances et divisibilité *(4 pts)*

a) $2^3=8\equiv 1\ [7]$ et $45=3\times 15$, donc $2^{45}=(2^3)^{15}\equiv 1\ [7]$. Reste : **1**. (1)

b) 7 étant premier et ne divisant pas 3, $3^6\equiv 1\ [7]$; $45=6\times 7+3$ donc $3^{45}\equiv 3^3=27\equiv 6\ [7]$. Reste : **6**. (1)

c) Par compatibilité avec l'addition, $2^{45}+3^{45}\equiv 1+6=7\equiv 0\ [7]$: le nombre est divisible par 7. (1)

d) Non : 2^{45} est pair et 3^{45} est impair, donc leur somme est impaire et n'est pas divisible par 2. Comme $14=2\times 7$, **le nombre n'est pas divisible par 14** bien qu'il le soit par 7. (1)

Le point clé — Un nombre divisible par 7 ne l'est par 14 que s'il est aussi pair : on vérifie chaque facteur premier du module séparément.

Exercice 3 – Équations de congruence *(4 pts)*

a) $\text{pgcd}(5,9)=1$ et $5\times 2=10\equiv 1\ [9]$: l'inverse de 5 est 2, donc $x\equiv 2\times 4=8\ [9]$. Solutions : $x=8+9k$**,** $k\in\mathbb{Z}$ (vérification : $5\times 8=40=4\times 9+4$). (1)

b) $\text{pgcd}(10,14)=2$ divise 4 : on simplifie en $5x\equiv 2\ [7]$. Comme $5\times 3=15\equiv 1\ [7]$, $x\equiv 3\times 2=6\ [7]$. Solutions : $x\equiv 6\ [\mathbf{14}]$ **ou** $x\equiv 13\ [\mathbf{14}]$. (1)

c) $\text{pgcd}(6,9)=3$; s'il existait x et k tels que $6x-9k=4$, alors 3 diviserait 4, ce qui est faux. **Pas de solution.** (1)

d) $4n+1\equiv 0\ [13]$ équivaut à $4n\equiv 12\ [13]$; or $4\times 10=40\equiv 1\ [13]$, donc $n\equiv 10\times 12=120\equiv 3\ [13]$. Solutions : $n=3+13k$**,** $k\in\mathbb{Z}$. (1)

Attention — La réponse d'une équation de congruence est une réunion de classes : on l'écrit toujours sous la forme $x\equiv c\ [\text{n}]$.

Exercice 4 – Petit théorème de Fermat *(4 pts)*

a) Si p est un nombre premier et si p ne divise pas l'entier a, alors $a^{p-1} \equiv 1$ [p]. Sans l'hypothèse sur a, on dispose de la forme générale $a^p \equiv a$ [p]. (1)

b) 19 est premier et ne divise pas 4, donc $4^{18} \equiv 1$ [19] ; $2\,022 = 18 \times 112 + 6$, donc $4^{2022} \equiv 4^6$. Or $4^3 = 64 \equiv 7$ [19], donc $4^6 \equiv 7^2 = 49 \equiv 11$ [19]. Reste : **11**. (1)

c) 5 est premier et ne divise pas n, donc $n^4 \equiv 1$ [5]. En élevant au carré : $n^8 = (n^4)^2 \equiv 1^2 = 1$ [5]. (1)

d) $2^4 = 16 \equiv 1$ [15], donc $2^{14} = (2^4)^3 \times 2^2 \equiv 4$ [15] : le reste est **4**. Si 15 était premier, comme il ne divise pas 2, on aurait $2^{14} \equiv 1$ [15] : contradiction. Donc **15 n'est pas premier**. (1)

À retenir — Le théorème de Fermat ne prouve jamais qu'un nombre est premier ; sa contraposée prouve en revanche qu'il ne l'est pas.

Exercice 5 – Application : chiffrement affine *(4 pts)*

a) T a pour rang 19 : $5 \times 19 + 8 = 103 = 3 \times 26 + 25$, donc $y = 25$: **T est codée Z**. (1)

b) $26 = 2 \times 13$ et 5 n'est divisible ni par 2 ni par 13, donc $\text{pgcd}(5, 26) = 1$. De plus $5 \times 21 = 105 = 4 \times 26 + 1$, donc l'inverse de 5 modulo 26 est **21**. (1)

c) De $y \equiv 5x + 8$ on tire $y - 8 \equiv 5x$, puis en multipliant par 21 : $21(y - 8) \equiv 105x \equiv x$ [26]. Or $21 \times (-8) = -168$ et $-168 + 182 = 14$ avec $182 = 7 \times 26$, donc $x \equiv 21y + 14$ [26]. (1)

d) I a pour rang 8 : $21 \times 8 + 14 = 182 = 7 \times 26$, donc $x \equiv 0$ [26] : **la lettre déchiffrée est A** (on vérifie que A donne bien $5 \times 0 + 8 = 8$, soit I). (1)

Astuce — Un codage affine n'est déchiffrable que si le coefficient multiplicateur est premier avec 26.