Corrigé et barème – Divisibilité, PGCD, congruences, Bézout, Gauss et nombres premiers — niveau ★

Durée : 60 min – Calculatrice interdite – Sur 20 points · Maths expertes Terminale

Exercice 1 – Automatismes *(5 pts)*

a) $6 \times (-14) = -84 > -85$ et $6 \times (-15) = -90 \leqslant -85$. Donc $-85 = 6 \times (-15) + 5$ avec $0 \leqslant 5 < 6$: le quotient vaut -15 et le reste 5. (1 pt) (1)

b) $6 \equiv -1\ [7]$, donc $6^{41} \equiv (-1)^{41} = -1\ [7]$, car 41 est impair. Or $-1 \equiv 6\ [7]$: le reste vaut 6. (1 pt : 0,5 pour $6 \equiv -1$, 0,5 pour la conclusion) (1)

c) $546 = 2 \times 234 + 78$; $234 = 3 \times 78 + 0$. Le dernier reste non nul est 78 : $\text{pgcd}(546\,;234) = 78$. Contrôle : $546 = 78 \times 7$ et $234 = 78 \times 3$. (1 pt) (1)

d) $1\,400 = 14 \times 100 = (2 \times 7) \times (2^2 \times 5^2) = 2^3 \times 5^2 \times 7$. Nombre de diviseurs positifs : $(3+1)(2+1)(1+1) = 4 \times 3 \times 2 = 24$. (1 pt : 0,5 pour la décomposition, 0,5 pour le nombre de diviseurs) (1)

e) $17 \times 5 - 12 \times 7 = 85 - 84 = 1$, soit $17u + 12v = 1$ avec $u = 5$ et $v = -7$ entiers. D'après le théorème de Bézout, 17 et 12 sont premiers entre eux. (1 pt) (1)

Méthode — Un reste vérifie toujours $0 \leqslant r < b$: pour un dividende négatif, on descend d'un multiple du diviseur au lieu de changer les signes.

Exercice 2 – Un tableau de congruences *(4 pts)*

a) Par compatibilité des congruences avec la somme et le produit, A a le même reste modulo 3 que $r^2 + r + 1$, où r est le reste de n. Pour $r = 0$: 1 ; pour $r = 1$: $3 \equiv 0$; pour $r = 2$: $4 + 2 + 1 = 7 \equiv 1\ [3]$.

n **modulo** 3	0	1	2
A **modulo** 3	1	0	1

(1 pt) (1)

b) D'après le tableau, $A \equiv 0\ [3]$ si et seulement si $n \equiv 1\ [3]$: A est divisible par 3 exactement pour les entiers $n = 3k + 1$, $k \in \mathbb{Z}$. (1 pt) (1)

c) $A = (3k+1)^2 + (3k+1) + 1 = 9k^2 + 6k + 1 + 3k + 2 = 9k^2 + 9k + 3 = 3(3k^2 + 3k + 1)$. Or $3k^2 + 3k + 1 \equiv 1\ [3]$ n'est pas divisible par 3, donc 9 ne divise pas A. Si $n \not\equiv 1\ [3]$, 3 ne divise même pas A. Ainsi A n'est divisible par 9 pour aucun entier n. (1 pt : 0,5 pour le développement, 0,5 pour la conclusion) (1)

d) Pour $n = 4$: $A = 16 + 4 + 1 = 21 = 3 \times 7$, qui n'est pas premier. Ce contre-exemple était prévisible : $4 = 3 \times 1 + 1$, donc 3 divise A d'après b), et $A > 3$. (1 pt) (1)

Erreur fréquente — Des exemples, même nombreux, ne prouvent pas une propriété « pour tout n » ; un seul contre-exemple suffit en revanche à la réfuter.

Exercice 3 – Une équation diophantienne *(5 pts)*

a) $13 = 1\times 8 + 5$; $8 = 1\times 5 + 3$; $5 = 1\times 3 + 2$; $3 = 1\times 2 + 1$; $2 = 2\times 1 + 0$. Le dernier reste non nul vaut 1 : $\text{pgcd}(13\,;8) = 1$. (1 pt) (1)

b) On remonte l'algorithme : $1 = 3 - 2 = 3 - (5-3) = 2\times 3 - 5 = 2(8-5) - 5 = 2\times 8 - 3\times 5 = 2\times 8 - 3(13-8) = 5\times 8 - 3\times 13$. Donc $(u\,;v) = (-3\,;5)$. Vérification : $-39 + 40 = 1$. (1 pt) (1)

c) En multipliant $13\times(-3) + 8\times 5 = 1$ par 5 : $13\times(-15) + 8\times 25 = 5$. Le couple $(-15\,;25)$ est solution ; contrôle : $-195 + 200 = 5$. (1 pt) (1)

d) Si $(x\,;y)$ est solution, en soustrayant $13\times(-15) + 8\times 25 = 5$: $13(x+15) = 8(25-y)$. Donc 8 divise $13(x+15)$; comme $\text{pgcd}(8\,;13) = 1$, le théorème de Gauss donne : 8 divise $x+15$, soit $x = -15 + 8k$, $k\in\mathbb{Z}$. En reportant, $13\times 8k = 8(25-y)$, d'où $y = 25 - 13k$. Réciproquement, $13(-15+8k) + 8(25-13k) = -195 + 200 = 5$. Les solutions sont les couples $(-15+8k\,;25-13k)$, $k\in\mathbb{Z}$. (1 pt : 0,5 pour Gauss, 0,5 pour la réciproque et l'ensemble des solutions) (1)

e) $13x \equiv 5\ [8]$ équivaut à l'existence d'un entier y tel que $13x - 5 = -8y$, c'est-à-dire $13x + 8y = 5$. D'après d), $x = -15 + 8k$: les solutions sont les entiers $x \equiv -15 \equiv 1\ [8]$. Contrôle : $13\times 1 = 13 = 8 + 5$. (1 pt) (1)

Astuce — Une équation $ax + by = c$ se lit aussi comme une congruence : modulo b, elle devient $ax \equiv c\ [b]$. Ses solutions en x sont donc exactement une classe modulo b quand a et b sont premiers entre eux.

Exercice 4 – Premiers, puissances et fractions *(6 pts)*

a) $15^2 = 225 \leqslant 227 < 256 = 16^2$: il suffit de tester les nombres premiers p tels que $p^2 \leqslant 227$, soit 2, 3, 5, 7, 11 et 13. 227 est impair ; $2+2+7 = 11$ n'est pas un multiple de 3 ; il ne se termine ni par 0 ni par 5 ; $7\times 32 = 224$ (reste 3), $11\times 20 = 220$ (reste 7), $13\times 17 = 221$ (reste 6). Aucun ne divise 227 : il est premier. (1,5 pt : 0,5 pour la borne, 1 pour les divisions) (1,5)

b) 11 est premier et ne divise pas 3 : d'après le petit théorème de Fermat, $3^{10} \equiv 1\ [11]$. Or $503 = 10\times 50 + 3$, donc $3^{503} = (3^{10})^{50}\times 3^3 \equiv 1\times 27\ [11]$, et $27 = 2\times 11 + 5$. Le reste vaut 5. (1,5 pt : 0,5 pour Fermat avec ses hypothèses, 0,5 pour la division de l'exposant, 0,5 pour le reste) (1,5)

c) $1\,260 = 2^2\times 315 = 2^2\times 3^2\times 35 = 2^2\times 3^2\times 5\times 7$; $1\,188 = 2^2\times 297 = 2^2\times 3^3\times 11$. On garde les facteurs premiers communs avec le plus petit exposant : $\text{pgcd}(1\,260\,;1\,188) = 2^2\times 3^2 = 36$. (1,5 pt : 1 pour les décompositions, 0,5 pour le PGCD) (1,5)

d) $1\,188 = 36\times 33$ et $1\,260 = 36\times 35$, donc $\dfrac{1\,188}{1\,260} = \dfrac{33}{35}$. Comme on a divisé par le PGCD, 33 et 35 sont premiers entre eux ; on le voit aussi sur $33 = 3\times 11$ et $35 = 5\times 7$, sans facteur premier commun. (1,5 pt) (1,5)

Piège — Pour tester si n est premier, on s'arrête aux nombres premiers p tels que $p^2 \leqslant n$: s'arrêter avant laisse passer des entiers composés, aller au-delà est inutile.

Ce document est la propriété intellectuelle de Ben, professeur particulier (benprofparticulier.fr), protégée par le Code de la propriété intellectuelle (art. L. 111-1 et L. 122-4). Il est mis à disposition pour un usage personnel de révision. Toute reproduction, diffusion, mise en ligne ou revente, totale ou partielle, sans autorisation écrite est interdite et constitue une contrefaçon (art. L. 335-2).