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

Durée : 120 min – Calculatrice interdite – Sur 20 points · Maths expertes Terminale

Exercice 1 – Automatismes *(4 pts)*

a) $2^3 = 8 \equiv -1\ [9]$, donc $2^6 \equiv 1\ [9]$. Or $100 = 6 \times 16 + 4$, donc $2^{100} = (2^6)^{16} \times 2^4 \equiv 16 \equiv 7\ [9]$. Le reste vaut 7. (1 pt) (1)

b) $7 \times 13 = 91 = 3 \times 30 + 1$: 13 est un inverse de 7 modulo 30. En multipliant les deux membres par 13 : $x \equiv 52 \equiv 22\ [30]$; réciproquement, $7 \times 22 = 154 = 5 \times 30 + 4$. Les solutions sont les entiers $22 + 30k$, $k \in \mathbb{Z}$. (1 pt : 0,5 pour l'inverse, 0,5 pour la résolution) (1)

c) Facteurs premiers communs avec le plus petit exposant : $\text{pgcd}(a\,;b) = 2^3 \times 3^2 = 72$. Les diviseurs communs sont les diviseurs du PGCD ; $72 = 2^3 \times 3^2$ en a $(3+1)(2+1) = 12$. (1 pt : 0,5 + 0,5) (1)

d) Cet entier vaut $N = 1\,000a + 100b + 10b + a$. Comme $10 \equiv -1\ [11]$, par compatibilité des congruences avec la somme, le produit et les puissances : $N \equiv a \times (-1)^3 + b \times (-1)^2 + b \times (-1) + a = -a + b - b + a = 0\ [11]$. On peut aussi factoriser : $N = 1\,001a + 110b = 11(91a + 10b)$, avec $91a + 10b$ entier. Donc 11 divise N ; par exemple $3\,773 = 11 \times 343$. (1 pt) (1)

Méthode — Pour une grande puissance, on cherche une puissance de la base congrue à 1 ou à -1, puis on divise l'exposant : on ne calcule jamais la puissance elle-même.

Exercice 2 – Qui a raison ? *(4 pts)*

a) Vraie. $12 = 2^2 \times 3$: 2 et 3 divisent $n^2 = n \times n$. Comme ils sont premiers, le lemme d'Euclide donne : 2 divise n et 3 divise n. 2 et 3 étant premiers entre eux, le corollaire du théorème de Gauss donne : 6 divise n. (1 pt : 0,5 pour le lemme d'Euclide, 0,5 pour le corollaire) (1)

b) Fausse. 4 divise $2^2 = 4$, mais 4 ne divise pas 2. Le lemme d'Euclide, utilisé en a), ne s'applique qu'à un diviseur premier : si p premier divise $b \times b$, alors p divise b. (1 pt) (1)

c) Vraie. p est impair : $p = 2k + 1$ et $p^2 - 1 = 4k(k+1)$; l'un des entiers consécutifs k et $k+1$ est pair, donc 8 divise $p^2 - 1$. De plus 3 ne divise pas p (premier différent de 3), donc $p \equiv 1$ ou $p \equiv 2 \equiv -1\ [3]$, et dans les deux cas $p^2 \equiv 1\ [3]$: 3 divise $p^2 - 1$. Comme 3 et 8 sont premiers entre eux ($3 \times 3 - 8 = 1$), le corollaire du théorème de Gauss donne : 24 divise $p^2 - 1$. (1 pt : 0,5 pour 8 et 3, 0,5 pour le corollaire) (1)

d) Fausse. $4^2 = 16 = 15 + 1$, donc $4^2 \equiv 1\ [15]$; pourtant $4 \not\equiv 1\ [15]$ et $4 \not\equiv -1 \equiv 14\ [15]$. L'affirmation serait vraie modulo un nombre premier p : p diviserait $x^2 - 1 = (x-1)(x+1)$, donc $x - 1$ ou $x + 1$ d'après le lemme d'Euclide ; mais $15 = 3 \times 5$ n'est pas premier. (1 pt) (1)

Piège — Le corollaire de Gauss exige deux diviseurs premiers entre eux : c'est parce que $\text{pgcd}(3\,;8) = 1$ qu'on passe de « 3 et 8 divisent » à « 24 divise ».

Exercice 3 – Problème — Un chiffrement affine *(5 pts)*

a) E : $11 \times 4 + 8 = 52 = 2 \times 26 + 0$, donc $y = 0$: E est chiffrée en A. T : $11 \times 19 + 8 = 217 = 8 \times 26 + 9$, donc $y = 9$: T est chiffrée en J. (1 pt : 0,5 par lettre) (1)

b) $26 = 2 \times 11 + 4$; $11 = 2 \times 4 + 3$; $4 = 1 \times 3 + 1$. Remontée : $1 = 4 - 3 = 4 - (11 - 2 \times 4) = 3 \times 4 - 11 = 3(26 - 2 \times 11) - 11 = 3 \times 26 - 7 \times 11$. Donc $11 \times (-7) \equiv 1\ [26]$, et $-7 \equiv 19\ [26]$: l'inverse est 19. Contrôle : $11 \times 19 = 209 = 8 \times 26 + 1$. (1 pt) (1)

c) Si $y \equiv 11x + 8\ [26]$, en multipliant par 19 : $19y \equiv 209x + 152\ [26]$. Or $209 \equiv 1$ et $152 = 5 \times 26 + 22 \equiv 22\ [26]$, donc $19y \equiv x + 22$, soit $x \equiv 19y - 22 \equiv 19y + 4\ [26]$. Réciproquement, si $x \equiv 19y + 4\ [26]$, en multipliant par 11 : $11x \equiv 209y + 44 \equiv y + 18\ [26]$, donc $y \equiv 11x - 18 \equiv 11x + 8\ [26]$. (1 pt : 0,5 par implication) (1)

d) On calcule le reste de $19y + 4$ modulo 26. A ($y = 0$) : 4, soit E. U ($y = 20$) : $384 = 14 \times 26 + 20$, soit U. Z ($y = 25$) : $479 = 18 \times 26 + 11$, soit L. N ($y = 13$) : $251 = 9 \times 26 + 17$, soit R. Le mot est EULER. (1 pt) (1)

e) On cherche les rangs x tels que $11x + 8 \equiv x\ [26]$, soit $10x \equiv -8 \equiv 18\ [26]$. Il existe alors un entier k tel que $10x - 18 = 26k$; en divisant par 2 : $5x - 9 = 13k$, donc l'équation équivaut à $5x \equiv 9\ [13]$. Comme $5 \times 8 = 40 = 3 \times 13 + 1$, on multiplie par 8 : $x \equiv 72 \equiv 7\ [13]$. Entre 0 et 25 : $x = 7$ ou $x = 20$, soit H et U. Contrôle : $11 \times 7 + 8 = 85 = 3 \times 26 + 7$ et $11 \times 20 + 8 = 228 = 8 \times 26 + 20$. (1 pt : 0,5 pour la réduction modulo 13, 0,5 pour les deux lettres) (1)

Erreur fréquente — Pour déchiffrer, on ne « divise » pas par 11 : on multiplie par l'inverse de 11 modulo 26, qui n'existe que parce que $\text{pgcd}(11\,;26) = 1$.

Exercice 4 – Problème — Un robot sur une droite graduée *(3 pts)*

a) La position finale vaut $29x - 12y$ (en cm), donc $29x - 12y = 2$. Algorithme d'Euclide : $29 = 2 \times 12 + 5$; $12 = 2 \times 5 + 2$; $5 = 2 \times 2 + 1$. Remontée : $1 = 5 - 2 \times 2 = 5 - 2(12 - 2 \times 5) = 5 \times 5 - 2 \times 12 = 5(29 - 2 \times 12) - 2 \times 12 = 5 \times 29 - 12 \times 12$. En multipliant par 2 : $29 \times 10 - 12 \times 24 = 2$; le couple $(10\,;24)$ est solution. Contrôle : $290 - 288 = 2$. (1 pt : 0,5 pour l'équation et l'algorithme, 0,5 pour la solution) (1)

b) Si $(x\,;y)$ est solution, en soustrayant $29 \times 10 - 12 \times 24 = 2$: $29(x - 10) = 12(y - 24)$. Donc 12 divise $29(x - 10)$; comme $\text{pgcd}(12\,;29) = 1$ (dernier reste non nul de l'algorithme de a), le théorème de Gauss donne : 12 divise $x - 10$, soit $x = 10 + 12k$, $k \in \mathbb{Z}$. En reportant, $29 \times 12k = 12(y - 24)$, d'où $y = 24 + 29k$. Réciproquement, $29(10 + 12k) - 12(24 + 29k) = 290 - 288 = 2$. Les solutions sont les couples $(10 + 12k\,;24 + 29k)$, $k \in \mathbb{Z}$. (1 pt : 0,5 pour Gauss, 0,5 pour la réciproque et l'ensemble des solutions) (1)

c) Les nombres de pas sont des entiers naturels : $10 + 12k \geqslant 0$ et $24 + 29k \geqslant 0$ imposent $k \geqslant 0$ ($k = -1$ donne $x = -2$). Le nombre total de pas vaut $x + y = 34 + 41k$. Pour 75 pas : $41k = 41$, donc $k = 1$, soit 22 pas en avant et 53 en arrière ; contrôle : $29 \times 22 - 12 \times 53 = 638 - 636 = 2$. Pour 100 pas : $41k = 66$, impossible car 41 ne divise pas 66. Le robot peut s'arrêter au point 2 après 75 pas, mais pas après 100. (1 pt : 0,5 par cas) (1)

Méthode — Les contraintes de l'énoncé (entiers naturels, nombre total de pas imposé) deviennent des conditions sur le paramètre k de la solution générale : on résout d'abord dans $\mathbb{Z}^2$, on trie ensuite.

Exercice 5 – Problème — Les nombres $2^n - 1$ *(4 pts)*

a) $2 \equiv -1\ [3]$, donc $2^n \equiv (-1)^n\ [3]$. Si n est pair, $2^n \equiv 1$ et $M_n \equiv 0\ [3]$; si n est impair, $2^n \equiv -1$ et $M_n \equiv -2 \equiv 1\ [3]$. Donc 3 divise M_n si et seulement si n est pair. (1 pt) (1)

b) $2^1 = 2$, $2^2 = 4$, $2^3 = 8 \equiv 1\ [7]$: le cycle a pour longueur 3. Si $n = 3q + r$ avec $r \in \{0\,;1\,;2\}$, $2^n = (2^3)^q \times 2^r \equiv 2^r\ [7]$, qui vaut 1, 2 ou 4. Donc $M_n \equiv 0\ [7]$ si et seulement si $r = 0$: 7 divise M_n exactement quand n est un multiple de 3. (1 pt) (1)

c) $2^r \equiv 1\ [M_r]$, donc $2^n = (2^r)^s \equiv 1^s = 1\ [M_r]$: M_r divise M_n. De plus $2 \leqslant r < n$ donne $3 \leqslant M_r < M_n$: si n n'est pas premier, M_n a un diviseur strictement compris entre 1 et lui-même, il n'est pas premier. Par contraposée, si M_n est premier, n est premier. (1 pt : 0,5 pour la divisibilité, 0,5 pour la contraposée) (1)

d) $2^5 = 32 \equiv 9\ [23]$, donc $2^{10} \equiv 81 = 3 \times 23 + 12 \equiv 12$ et $2^{11} \equiv 24 \equiv 1\ [23]$. Ainsi 23 divise M_{11}, et $M_{11} \neq 23$ (car $2^{11} > 24$) : M_{11} n'est pas premier alors que 11 l'est. La réciproque est fausse ($M_{11} = 2\,047 = 23 \times 89$). (1 pt : 0,5 pour la congruence, 0,5 pour la conclusion) (1)

Astuce — De $2^r \equiv 1\ [2^r - 1]$, on tire $2^{rs} \equiv 1$: une congruence modulo une expression fournit un diviseur sans aucune division à poser.

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).