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 *(3 pts)*

a) $2\,026 = 7 \times 289 + 3$, donc $2\,026^{2\,026} \equiv 3^{2\,026}\ [7]$. 7 est premier et ne divise pas 3 : $3^6 \equiv 1\ [7]$ (petit théorème de Fermat). Or $2\,026 = 6 \times 337 + 4$, donc $3^{2\,026} \equiv 3^4 = 81 = 11 \times 7 + 4\ [7]$. Le reste vaut 4. (1 pt) (1)

b) $12^{10} = (2^2 \times 3)^{10} = 2^{20} \times 3^{10}$: il a $(20+1)(10+1) = 231$ diviseurs positifs, de la forme $2^{\alpha} \times 3^{\beta}$ avec $0 \leqslant \alpha \leqslant 20$ et $0 \leqslant \beta \leqslant 10$. Un tel diviseur est un carré si et seulement si α et β sont pairs : 11 choix pour α $(0, 2, \dots, 20)$ et 6 pour β $(0, 2, \dots, 10)$, soit 66 carrés. (1 pt : 0,5 + 0,5) (1)

c) $65 = 2 \times 26 + 13$ et $26 = 2 \times 13$: $\operatorname{pgcd}(26\,;65) = 13$, qui divise 39. $26x - 39 = 65k$ équivaut, en divisant par 13, à $2x - 3 = 5k$: l'équation équivaut à $2x \equiv 3\ [5]$. Comme $2 \times 3 = 6 \equiv 1\ [5]$, on multiplie par 3 : $x \equiv 9 \equiv 4\ [5]$. Les solutions sont les entiers $4 + 5k$, $k \in \mathbb{Z}$ (treize classes modulo 65). Contrôle : $26 \times 4 = 104 = 65 + 39$. (1 pt) (1)

Méthode — Avant d'appliquer le petit théorème de Fermat, on réduit la base modulo p ; l'exposant, lui, se réduit modulo $p - 1$.

Exercice 2 – Démontrer *(4 pts)*

a) Comme $\operatorname{pgcd}(a\,;b) = 1$, le théorème de Bézout donne des entiers u et v tels que $au + bv = 1$. En multipliant par c : $acu + bcv = c$. Or a divise acu, et a divise bc donc bcv : a divise la somme c. (1 pt) (1)

b) Soit $d \geqslant 1$ un diviseur commun. Il divise la combinaison $(n+1)! + 1 - (n+1)(n! + 1) = (n+1)! + 1 - (n+1)! - (n+1) = -n$, donc d divise n. Or n divise $n! = 1 \times 2 \times \cdots \times n$, donc d divise $n!$; divisant aussi $n! + 1$, il divise la différence 1. Ainsi $d = 1$: les deux entiers sont premiers entre eux. (1 pt : 0,5 pour la combinaison, 0,5 pour la conclusion) (1)

c) Pour $1 \leqslant k \leqslant p - 1$, p ne divise pas k ; comme p est premier, le petit théorème de Fermat donne $k^{p-1} \equiv 1\ [p]$. En ajoutant ces $p - 1$ congruences : la somme est congrue à $p - 1 \equiv -1\ [p]$. (1 pt) (1)

d) $(n^2+2)^2 - 4n^2 = n^4 + 4n^2 + 4 - 4n^2 = n^4 + 4$, donc $n^4 + 4 = (n^2 + 2 - 2n)(n^2 + 2 + 2n) = (n^2 - 2n + 2)(n^2 + 2n + 2)$. Pour $n \geqslant 2$: $n^2 - 2n + 2 = (n-1)^2 + 1 \geqslant 2$, et $n^2 + 2n + 2 > n^2 - 2n + 2 \geqslant 2$. Ainsi $n^4 + 4$ est le produit de deux entiers supérieurs ou égaux à 2 : il admet un diviseur strictement compris entre 1 et lui-même, il n'est pas premier. Exemple : $3^4 + 4 = 85 = 5 \times 17$. Pour $n = 1$, en revanche, $1^4 + 4 = 5$ est premier. (1 pt : 0,5 pour la factorisation, 0,5 pour les deux facteurs supérieurs ou égaux à 2) (1)

Erreur fréquente — Le théorème de Gauss et le petit théorème de Fermat ont une hypothèse (premiers entre eux ; p premier ne divisant pas l'entier) : on l'écrit et on la justifie avant de conclure, sinon la preuve ne vaut rien.

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

a) $40 = 13 \times 3 + 1$, donc $3 \times (-13) + 40 \times 1 = 1$: d'après le théorème de Bézout, $\text{pgcd}(3\,;40) = 1$, et $3 \times (-13) \equiv 1\ [40]$. Comme $-13 \equiv 27\ [40]$, $d = 27$. Contrôle : $3 \times 27 = 81 = 2 \times 40 + 1$. (1 pt) (1)

b) Si 5 divise m, les deux membres sont congrus à 0. Sinon, 5 étant premier, le petit théorème de Fermat donne $m^4 \equiv 1\ [5]$; comme $81 = 4 \times 20 + 1$, $m^{81} = (m^4)^{20} \times m \equiv m\ [5]$. (1 pt : 0,5 par cas) (1)

c) Si 11 divise m, c'est clair. Sinon $m^{10} \equiv 1\ [11]$ (Fermat, 11 premier) et $81 = 10 \times 8 + 1$, donc $m^{81} \equiv m\ [11]$. Ainsi 5 et 11 divisent $m^{81} - m$; ce sont deux nombres premiers distincts, donc premiers entre eux, et le corollaire du théorème de Gauss donne : 55 divise $m^{81} - m$. (1 pt : 0,5 pour le cas modulo 11, 0,5 pour le recollement) (1)

d) $m^3 \equiv 13\ [55]$; en élevant à la puissance 27 : $m^{81} \equiv 13^{27}\ [55]$. D'après c), $m^{81} \equiv m\ [55]$, donc $m \equiv 13^{27}\ [55]$. Comme $0 \leqslant m \leqslant 54$, m est le reste de 13^{27} modulo 55 : le message est unique. (1 pt) (1)

e) Modulo 5 : $13 \equiv 3$, $3^4 \equiv 1$ et $27 = 4 \times 6 + 3$, donc $13^{27} \equiv 3^3 = 27 \equiv 2\ [5]$. Modulo 11 : $13 \equiv 2$, $2^{10} \equiv 1$ et $27 = 10 \times 2 + 7$, donc $13^{27} \equiv 2^7 = 128 = 11 \times 11 + 7 \equiv 7\ [11]$. On cherche m entre 0 et 54 avec $m \equiv 7\ [11]$, parmi 7, 18, 29, 40, 51 : seul 7 vérifie $m \equiv 2\ [5]$. Donc $m = 7$. Vérification : $7^3 = 343 = 6 \times 55 + 13$. (1 pt : 0,5 pour les deux restes, 0,5 pour m) (1)

Astuce — Pour un module pq produit de deux nombres premiers distincts, on travaille séparément modulo p et modulo q (Fermat), puis le corollaire de Gauss recolle les deux congruences modulo pq.

Exercice 4 – Problème — Deux lignes de bus *(4 pts)*

a) Le bus A passe aux instants $t = 12 + 35x$ et le bus B aux instants $t = 5 + 24y$, avec x et y entiers naturels (nombre d'intervalles écoulés depuis le premier passage). Ils passent ensemble si et seulement si un même t s'écrit des deux façons : $12 + 35x = 5 + 24y$, c'est-à-dire $24y - 35x = 7$. (1 pt) (1)

b) $35 = 1 \times 24 + 11$; $24 = 2 \times 11 + 2$; $11 = 5 \times 2 + 1$. Remontée : $1 = 11 - 5 \times 2 = 11 - 5(24 - 2 \times 11) = 11 \times 11 - 5 \times 24 = 11(35 - 24) - 5 \times 24 = 11 \times 35 - 16 \times 24$. Donc $24 \times (-16) - 35 \times (-11) = 1$, puis, en multipliant par 7 : $24 \times (-112) - 35 \times (-77) = 7$. Si $(x\,;y)$ est solution, $24(y + 112) = 35(x + 77)$; 35 divise $24(y + 112)$ et $\text{pgcd}(35\,;24) = 1$, donc par Gauss $y = -112 + 35k$, puis $x = -77 + 24k$, $k \in \mathbb{Z}$. Réciproquement, $24(-112 + 35k) - 35(-77 + 24k) = -2\,688 + 2\,695 = 7$. (1 pt : 0,5 pour la solution particulière, 0,5 pour Gauss et la réciproque) (1)

c) $x \geqslant 0$ impose $24k \geqslant 77$, soit $k \geqslant 4$; $y \geqslant 0$ impose $35k \geqslant 112$, soit $k \geqslant 4$. Pour $k = 4$: $x = 19$, $y = 28$ et $t = 12 + 35 \times 19 = 677 = 5 + 24 \times 28$. Or 677 min = 11 h 17 min : premier passage commun à 18 h 17. Plus généralement $t = 12 + 35(-77 + 24k) = 840k - 2\,683$: deux rencontres sont séparées de 840 min, soit 14 h. La suivante tomberait à $t = 1\,517$, au-delà de $t = 960$ (23 h) : une seule rencontre par jour. (1 pt : 0,5 pour 18 h 17, 0,5 pour l'unicité) (1)

d) Ils passeraient ensemble s'il existait des entiers x et z tels que $12 + 35x = 3 + 21z$, soit $21z - 35x = 9$. Or 7 divise 21 et 35, donc $21z - 35x$; il diviserait 9, ce qui est faux. Les bus A et C ne se croisent jamais à cet arrêt. (1 pt) (1)

Piège — Le pas des solutions de $24y - 35x = 7$ est 35 pour y et 24 pour x ; en temps, deux rencontres sont donc séparées de $35 \times 24 = 840$ minutes, et non de 35 ou de 24 minutes.

Exercice 5 – Pour aller plus loin *(4 pts)*

a) $x^2 - y^2 = (x-y)(x+y) = 2\,025$. Comme $x + y \geqslant 0$ et que le produit est strictement positif, $x + y > 0$, puis $x - y > 0$. Ce sont donc deux diviseurs positifs de $2\,025$ de produit $2\,025$, et $x - y \leqslant x + y$ car $y \geqslant 0$. (1 pt) (1)

b) $2\,025 = 81 \times 25 = 3^4 \times 5^2$. On pose $\delta = x - y$ et $D = x + y$, avec $\delta D = 2\,025$ et $\delta \leqslant D$, donc $\delta \leqslant 45$: $\delta \in \{1\,;3\,;5\,;9\,;15\,;25\,;27\,;45\}$. Les deux sont impairs, donc $x = \dfrac{\delta + D}{2}$ et $y = \dfrac{D - \delta}{2}$ sont entiers ; réciproquement, chaque couple vérifie $(x-y)(x+y) = \delta D = 2\,025$. Solutions : $(1\,013\,;1\,012)$, $(339\,;336)$, $(205\,;200)$, $(117\,;108)$, $(75\,;60)$, $(53\,;28)$, $(51\,;24)$ et $(45\,;0)$. (1 pt : 0,5 pour la décomposition et les diviseurs, 0,5 pour les couples) (1)

c) Un carré est congru à 0 ou 1 modulo 4 ($0^2 = 0$, $1^2 = 1$, $2^2 = 4 \equiv 0$, $3^2 = 9 \equiv 1$). Donc $x^2 - y^2$ est congru à 0, 1 ou $-1 \equiv 3$ modulo 4, jamais à 2. Or $2\,026 = 4 \times 506 + 2 \equiv 2\ [4]$: pas de solution. (1 pt) (1)

d) Si $N = x^2 - y^2$, c) montre que $N \not\equiv 2\ [4]$. Réciproquement, si N est impair, $N = 2k + 1 = (k+1)^2 - k^2$; si $N \equiv 0\ [4]$, $N = 4k = (k+1)^2 - (k-1)^2$, car $(k+1)^2 - (k-1)^2 = 4k$. Ces deux cas couvrent tous les $N \not\equiv 2\ [4]$. (1 pt : 0,5 par sens) (1)

Astuce — Une factorisation $(x-y)(x+y) = N$ ramène l'équation à la liste des diviseurs de N, et les carrés modulo 4 (seulement 0 et 1) suffisent à exclure les entiers congrus à 2 modulo 4.

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).