Plaquette 5 – Synthèse : PGCD, PPCM par décomposition et cryptographie

Nombres premiers — Terminale maths expertes

Corrections détaillées

Boîte à outils

Formules et méthodes.

— **PGCD par décomposition** : produit des facteurs premiers **communs**, chacun affecté du **plus petit** exposant.

— **PPCM par décomposition** : produit de **tous** les facteurs premiers apparaissant, chacun affecté du **plus grand** exposant.

— Conséquence : $\text{pgcd}(a\,;b)\times\text{ppcm}(a\,;b)=ab$, car pour chaque premier, $\min(\alpha\,;\beta)+\max(\alpha\,;\beta)=\alpha+\beta$.

— **Exposant d'un premier p dans $n!$** (formule de Legendre) :

$$\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\left\lfloor\frac{n}{p^3}\right\rfloor+\cdots$$

— **Somme des diviseurs** de $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$:

$$\sigma(n)=\prod_{i=1}^{k}\left(1+p_i+p_i^2+\cdots+p_i^{\alpha_i}\right)$$

Un nombre est **parfait** lorsque $\sigma(n)=2n$, c'est-à-dire qu'il est égal à la somme de ses diviseurs stricts.

— **Chiffrement RSA (version miniature)** : on choisit deux premiers p et q, on pose $n=pq$ et $\varphi=(p-1)(q-1)$. On choisit e premier avec φ, et d tel que $ed\equiv 1 \pmod{\varphi}$. On chiffre par $c\equiv m^{e} \pmod{n}$ et on déchiffre par $m\equiv c^{d} \pmod{n}$.

Correction de l'exercice 1 – PGCD et PPCM par décomposition

a) $504=8\times 63=2^3\times 3^2\times 7$.

— $1\,188=4\times 297=2^2\times 27\times 11=2^2\times 3^3\times 11$.

b) On aligne les décompositions :

Premier	2	3	7	11
Dans 504	2^3	3^2	7^1	—
Dans 1 188	2^2	3^3	—	11^1
PGCD (min)	2^2	3^2	—	—
PPCM (max)	2^3	3^3	7	11

— $\text{pgcd}(504\,;1\,188)=2^2\times 3^2=36$.

— $\text{ppcm}(504\,;1\,188)=2^3\times 3^3\times 7\times 11=8\times 27\times 77=16\,632$.

c) $\text{pgcd}\times\text{ppcm}=36\times 16\,632=598\,752$.

— $504\times 1\,188=598\,752$ ✓.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— **Pourquoi la relation est vraie** : pour chaque facteur premier, $\min(\alpha;\beta)+\max(\alpha;\beta)=\alpha+\beta$.

Réponse. a) $2^3\times3^2\times7$ et $2^2\times3^3\times11$ · b) PGCD 36, PPCM 16 632 · c) $36\times16\,632=504\times1\,188$.

Correction de l’exercice 2 – Trois nombres à la fois

On décompose les trois nombres, puis on applique la règle du minimum et du maximum, **colonne par colonne**.

— $600=2^3\times3\times5^2$; $540=2^2\times3^3\times5$; $1\,050=2\times3\times5^2\times7$.

Premier	2	3	5	7
600	3	1	2	0
540	2	3	1	0
1 050	1	1	2	1
Minimum	1	1	1	0
Maximum	3	3	2	1

— pgcd $=2\times3\times5=30$.

— ppcm $=2^3\times3^3\times5^2\times7=8\times27\times25\times7=37\,800$.

— **Vérification partielle** : $37\,800\div600=63$, $37\,800\div540=70$, $37\,800\div1\,050=36$ — trois entiers ✓.

— **Attention** : la relation pgcd × ppcm = *abc* est **fausse** pour trois nombres ; ici $30\times37\,800\neq600\times540\times1\,050$.

Réponse. PGCD = 30, PPCM = 37 800.

Correction de l’exercice 3 – Retrouver un entier

$504=2^3\times3^2\times7$ et $36=2^2\times3^2$.

— $\text{pgcd}(n;504)=36$ signifie d’abord que 36 divise n : $n=36k$.

— Ensuite, le PGCD ne doit pas être **plus grand** : n ne doit pas apporter de facteur 2 supplémentaire commun (sinon on aurait 2^3), ni de facteur 7 commun.

— Condition sur 2 : l’exposant de 2 dans n doit être exactement 2 (car min avec 3 doit valoir 2).

— Condition sur 7 : 7 ne doit pas diviser n.

— Donc $n=36k$ avec k **impair** et non divisible par 7.

On énumère pour $n\le200$, soit $k\le5$:

k	1	3	5
$n=36k$	36	108	180
$\text{pgcd}(n;504)$	36	36	36

— $k=2$ donnerait $n=72=2^3\times3^2$, de PGCD 72 avec 504 : rejeté.

— $k=4$ donnerait $n=144$, de PGCD 72 : rejeté également.

— **Conclusion** : $n\in\{36;108;180\}$.

Réponse. $n\in\{36;108;180\}$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s’expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Correction de l'exercice 4 – Combien de zéros à la fin ?

Un zéro final correspond à un facteur $10 = 2 \times 5$. Comme les facteurs 2 sont bien plus nombreux que les facteurs 5, **le nombre de zéros est l'exposant de** 5.

a) Formule de Legendre pour $p = 5$ et $n = 100$:

$$\left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 20 + 4 = 24$$

— $\left\lfloor \frac{100}{125} \right\rfloor = 0$: on s'arrête.
— $100\,!$ **se termine par** 24 **zéros.**
— **Pourquoi** +4 **?** Les multiples de 25 (25, 50, 75, 100) apportent chacun un **second** facteur 5, qu'il ne faut pas oublier.

b) Pour $n = 2\,026$:

— $\left\lfloor \frac{2\,026}{5} \right\rfloor = 405$; $\left\lfloor \frac{2\,026}{25} \right\rfloor = 81$; $\left\lfloor \frac{2\,026}{125} \right\rfloor = 16$; $\left\lfloor \frac{2\,026}{625} \right\rfloor = 3$; $\left\lfloor \frac{2\,026}{3\,125} \right\rfloor = 0$.
— Total : $405 + 81 + 16 + 3 = 505$ zéros.

Réponse. a) 24 zéros · b) 505 zéros.

Correction de l'exercice 5 – L'exposant d'un premier dans une factorielle

a) On applique la formule de Legendre avec $p = 3$:

$$\left\lfloor \frac{20}{3} \right\rfloor + \left\lfloor \frac{20}{9} \right\rfloor + \left\lfloor \frac{20}{27} \right\rfloor = 6 + 2 + 0 = 8$$

— **Lecture directe** : parmi $1, 2, \ldots, 20$, il y a 6 multiples de 3 ($3, 6, 9, 12, 15, 18$), dont 2 sont des multiples de 9 (9 et 18) et apportent donc un facteur 3 de plus.
— L'exposant de 3 dans $20\,!$ est 8.

b) 3^9 demanderait un exposant d'au moins 9 : ce n'est pas le cas.

— Donc $20\,!$ **n'est pas** divisible par 3^9, alors qu'il l'est par 3^8.
— **Le plus petit** n **tel que** $3^9 \mid n!$ est $n = 21$, car 21 apporte un facteur 3 supplémentaire.

Réponse. a) exposant 8 · b) non, 3^8 est la plus grande puissance qui divise $20\,!$.

Correction de l'exercice 6 – La somme des diviseurs

a) On décompose, puis on utilise la formule produit.

— $28 = 2^2 \times 7$, donc

$$\sigma(28) = (1 + 2 + 4)(1 + 7) = 7 \times 8 = 56$$

— Contrôle par la liste : $1 + 2 + 4 + 7 + 14 + 28 = 56$ ✓.
— $496 = 2^4 \times 31$, donc $\sigma(496) = (1 + 2 + 4 + 8 + 16)(1 + 31) = 31 \times 32 = 992$.

b) Dans les deux cas, $\sigma(n) = 2n$:

— $56 = 2 \times 28$ et $992 = 2 \times 496$.
— Autrement dit, chaque nombre est **égal à la somme de ses diviseurs stricts** : ce sont des **nombres parfaits**.
— Vérification avec $6 = 2 \times 3$: $\sigma(6) = (1 + 2)(1 + 3) = 12 = 2 \times 6$ ✓, et $6 = 1 + 2 + 3$.
— **Le lien avec les premiers** : $6 = 2 \times 3$, $28 = 2^2 \times 7$, $496 = 2^4 \times 31$ sont tous de la forme $2^{k-1}\left(2^k - 1\right)$ avec $2^k - 1$ premier (3, 7, 31). On ne sait toujours pas s'il existe un nombre parfait **impair**.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Réponse. a) $\sigma(28) = 56$, $\sigma(496) = 992$ · b) $\sigma(n) = 2n$: nombres parfaits.

Correction de l'exercice 7 – Construire une clé RSA

a) $n = 5 \times 11 = 55$ et $\varphi = 4 \times 10 = 40$.

— La **clé publique** sera le couple $(n\,;e) = (55\,;3)$, la **clé privée** le nombre d.

b) $\text{pgcd}(3\,;40) = 1$: 3 est bien premier avec 40 ($40 = 3 \times 13 + 1$, et le PGCD vaut 1).

— On cherche d tel que $3d \equiv 1 \pmod{40}$.
— Identité de Bézout immédiate : $40 = 3 \times 13 + 1$, donc $1 = 40 - 3 \times 13$, c'est-à-dire $3 \times (-13) \equiv 1 \pmod{40}$.
— $-13 \equiv 27 \pmod{40}$: on prend $d = 27$.
— **Vérification** : $3 \times 27 = 81 = 40 \times 2 + 1$ ✓.
— **Conclusion** : clé publique $(55\,;3)$, clé privée $d = 27$.

Réponse. a) $n = 55$, $\varphi = 40$ · b) $d = 27$ (car $3 \times 27 = 81 \equiv 1 \pmod{40}$).

Correction de l'exercice 8 – Chiffrer et déchiffrer

a) $m^3 = 7^3 = 343$.

— $343 = 55 \times 6 + 13$, donc $c \equiv 13 \pmod{55}$.
— Le message chiffré est 13.

b) On doit calculer $13^{27} \pmod{55}$ — sans jamais écrire ce nombre, en réduisant à chaque étape.

— $13^2 = 169 = 55 \times 3 + 4$, donc $13^2 \equiv 4$.
— $13^4 \equiv 4^2 = 16$; $13^8 \equiv 16^2 = 256 = 55 \times 4 + 36 \equiv 36$; $13^{16} \equiv 36^2 = 1\,296 = 55 \times 23 + 31 \equiv 31$.
— $27 = 16 + 8 + 2 + 1$, donc

$$13^{27} \equiv 31 \times 36 \times 4 \times 13 \pmod{55}$$

— $31 \times 36 = 1\,116 = 55 \times 20 + 16 \equiv 16$; $16 \times 4 = 64 \equiv 9$; $9 \times 13 = 117 = 110 + 7 \equiv 7$.
— **On retrouve** $m = 7$ ✓ : le déchiffrement fonctionne.
— **Pourquoi ça marche** : $ed \equiv 1 \pmod{\varphi}$, et le petit théorème de Fermat appliqué à $p = 5$ et $q = 11$ montre que $m^{ed} \equiv m \pmod{55}$.

Réponse. a) $c = 13$ · b) $13^{27} \equiv 7 \pmod{55}$: on retrouve le message.

Correction de l'exercice 9 – Casser une clé trop petite

a) Toute la sécurité repose sur la **factorisation** de n.

— L'attaquant factorise $n = 55 = 5 \times 11$: c'est immédiat ici.
— Il en déduit $\varphi = (5 - 1)(11 - 1) = 40$.
— Il résout $3d \equiv 1 \pmod{40}$ par l'algorithme d'Euclide, et trouve $d = 27$.
— Il possède alors la clé privée et peut déchiffrer tous les messages.

b) Dans le RSA réel, p et q sont deux nombres premiers de plusieurs **centaines de chiffres**, et $n = pq$ en compte environ 600.

— Tester les diviseurs jusqu'à $\sqrt{n}$ demanderait de l'ordre de 10^{300} opérations : aucune machine existante ou envisageable ne peut le faire.
— **Le point clé** : multiplier deux grands nombres premiers est instantané, les retrouver à partir du produit est hors de portée. C'est cette **asymétrie** qui fait la sécurité, et c'est de l'arithmétique du chapitre.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— En revanche, on sait **fabriquer** de grands nombres premiers rapidement, grâce à des tests de primalité probabilistes fondés sur le petit théorème de Fermat.

Réponse. a) factoriser 55, calculer $\varphi = 40$, résoudre $3d \equiv 1 \pmod{40}$ · b) factoriser un n de 600 chiffres est hors de portée.

Correction de l'exercice 10 – Un produit imposé

On pose $a = 6a'$ et $b = 6b'$ avec $\text{pgcd}(a' ; b') = 1$.

— $ab = 36\,a'b' = 2\,520$, donc $a'b' = 70$.

— $70 = 2 \times 5 \times 7$: on cherche les couples de produit 70, premiers entre eux, avec $a' \leq b'$.

$(a' ; b')$	pgcd	$(a ; b)$	$\text{pgcd}(a ; b)$
$(1 ; 70)$	1 ✓	$(6 ; 420)$	6 ✓
$(2 ; 35)$	1 ✓	$(12 ; 210)$	6 ✓
$(5 ; 14)$	1 ✓	$(30 ; 84)$	6 ✓
$(7 ; 10)$	1 ✓	$(42 ; 60)$	6 ✓

— Comme $70 = 2 \times 5 \times 7$ n'a que des facteurs premiers simples, **toutes** ses décompositions en deux facteurs sont formées de nombres premiers entre eux.

— **Vérification** sur $(30 ; 84)$: $30 \times 84 = 2\,520$ ✓ et $\text{pgcd}(30 ; 84) = 6$ ✓.

Réponse. $(6 ; 420)$, $(12 ; 210)$, $(30 ; 84)$ et $(42 ; 60)$.

Correction de l'exercice 11 – Une fraction et ses facteurs

a) $2\,520 = 2^3 \times 3^2 \times 5 \times 7$ et $1\,188 = 2^2 \times 3^3 \times 11$.

— Facteurs communs, plus petit exposant : $2^2 \times 3^2 = 36$ — c'est le PGCD.

— On simplifie :

$$\frac{2\,520}{1\,188} = \frac{2\,520 \div 36}{1\,188 \div 36} = \frac{70}{33}$$

— Contrôle : $70 = 2 \times 5 \times 7$ et $33 = 3 \times 11$ n'ont aucun facteur commun ✓, la fraction est irréductible.

b) $2\,520 = 2^3 \times 3^2 \times 5 \times 7$: pour que le quotient soit **impair**, il faut retirer **tous** les facteurs 2.

— Le plus petit k qui les retire est $k = 2^3 = 8$.

— $\dfrac{2\,520}{8} = 315 = 3^2 \times 5 \times 7$, qui est bien impair ✓.

— **Conclusion** : $k = 8$. Tout k plus petit laisserait au moins un facteur 2… sauf s'il ne divise pas 2 520, auquel cas le quotient ne serait pas entier.

Réponse. a) $\dfrac{70}{33}$ · b) $k = 8$ (quotient 315).

Correction de l'exercice 12 – Des cartes à distribuer

a) La taille d'un paquet doit diviser $504 = 2^3 \times 3^2 \times 7$.

— On construit les diviseurs en combinant les exposants :
$1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 18, 21, 24, 28, 36, 42, 56, 63, 72, 84, 126, 168, 252, 504$.

— On retient ceux compris entre 20 et 80 : 21, 24, 28, 36, 42, 56, 63, 72.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Paquet	21	24	28	36	42	56	63	72
Nombre de paquets	24	21	18	14	12	9	8	7

— **Huit** tailles conviennent.

b) $504 = 2^3 \times 3^2 \times 7^1$ a $(3+1)(2+1)(1+1) = 24$ diviseurs.

— La liste écrite plus haut en compte bien 24 ✓ — c'est un bon moyen de vérifier qu'on n'en a oublié aucun.

Réponse. a) 21, 24, 28, 36, 42, 56, 63, 72 · b) 24 diviseurs.

Correction de l'exercice 13 – Deux roues et un PPCM

a) L'instant cherché est un multiple commun des deux périodes : c'est le **PPCM**.

— $540 = 2^2 \times 3^3 \times 5$ et $600 = 2^3 \times 3 \times 5^2$.

— PPCM (maximum de chaque exposant) : $2^3 \times 3^3 \times 5^2 = 8 \times 27 \times 25 = 5\,400$ minutes.

— $5\,400$ minutes = 90 heures = 3 jours et 18 heures.

— **Conclusion** : ils seront de nouveau alignés trois jours et dix-huit heures plus tard, soit à 6 h du matin le quatrième jour.

b) On divise le PPCM par chaque période :

— Premier satellite : $5\,400 \div 540 = 10$ révolutions.

— Second satellite : $5\,400 \div 600 = 9$ révolutions.

— **Cohérence** : le satellite le plus rapide (période la plus courte) a bien fait un tour de plus ✓.

— Contrôle par le PGCD : $\text{pgcd}(540\,;600) = 2^2 \times 3 \times 5 = 60$, et $\dfrac{540 \times 600}{60} = 5\,400$ ✓.

Réponse. a) 5 400 min, soit 3 jours et 18 h · b) 10 et 9 révolutions.

Correction de l'exercice 14 – Un code de vérification

a) On calcule $4^5 \pmod{23}$ en réduisant au fur et à mesure.

— $4^2 = 16$; $4^4 \equiv 16^2 = 256 = 23 \times 11 + 3 \equiv 3$.

— $4^5 \equiv 3 \times 4 = 12 \pmod{23}$.

— L'identifiant codé est 12.

b) 23 est premier, donc le petit théorème de Fermat donne $a^{22} \equiv 1$ pour $23 \nmid a$.

— On cherche d tel que $\left(a^5\right)^d = a^{5d} \equiv a$, c'est-à-dire $5d \equiv 1 \pmod{22}$.

— $\text{pgcd}(5\,;22) = 1$, donc d existe : $5 \times 9 = 45 = 44 + 1 \equiv 1 \pmod{22}$, donc $d = 9$.

— **Vérification du mécanisme** : $a^{45} = \left(a^{22}\right)^2 \times a \equiv a \pmod{23}$ ✓.

— Contrôle sur l'exemple : $12^9 \pmod{23}$ doit redonner 4. En effet $12^2 = 144 \equiv 6$; $12^4 \equiv 36 \equiv 13$; $12^8 \equiv 169 \equiv 8$; $12^9 \equiv 8 \times 12 = 96 = 92 + 4 \equiv 4$ ✓.

Réponse. a) $c = 12$ · b) $d = 9$, car $5 \times 9 \equiv 1 \pmod{22}$.

Correction de l'exercice 15 – Bilan : tout le chapitre

a) $1\,050 = 2 \times 3 \times 5^2 \times 7$ et $2\,520 = 2^3 \times 3^2 \times 5 \times 7$.

— PGCD (minimums) : $2 \times 3 \times 5 \times 7 = 210$.

— PPCM (maximums) : $2^3 \times 3^2 \times 5^2 \times 7 = 12\,600$.

— Contrôle : $210 \times 12\,600 = 2\,646\,000 = 1\,050 \times 2\,520$ ✓.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— Nombre de diviseurs de $2\,520$: $(3+1)(2+1)(1+1)(1+1) = 48$.

b) 17 est premier et ne divise pas 6 : $6^{16} \equiv 1 \pmod{17}$.

— $2\,026 = 16 \times 126 + 10$ (car $16 \times 126 = 2\,016$), donc $6^{2026} \equiv 6^{10} \pmod{17}$.

— $6^2 = 36 \equiv 2$; donc $6^{10} = \left(6^2\right)^5 \equiv 2^5 = 32 \equiv 15 \pmod{17}$.

— **Le reste est** 15**.**

c) $35 = 5 \times 7$, donc $\varphi = 4 \times 6 = 24$.

— On cherche d tel que $5d \equiv 1 \pmod{24}$: $5 \times 5 = 25 \equiv 1$, donc $d = 5$.

— Déchiffrement : $m \equiv 3^5 = 243 \pmod{35}$, et $243 = 35 \times 6 + 33$, donc $m = 33$.

— **Vérification** : on rechiffre $33^5 \pmod{35}$. $33 \equiv -2$, donc $33^5 \equiv (-2)^5 = -32 \equiv 3 \pmod{35}$ ✓.

Réponse. a) PGCD 210, PPCM 12 600, 48 diviseurs · b) reste 15 · c) $d = 5$ et $m = 33$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).