Plaquette 3 – Nombres premiers, valuations et diviseurs

Arithmétique dans Z — Prépa MPSI / MP2I (1re année)

Corrections détaillées

Boîte à outils

Nombres premiers et valuations.

— **Critère** : si $n \geq 2$ n'a aucun diviseur premier $p \leq \sqrt{n}$, alors n est premier.

— **Décomposition** : $n = \prod_p p^{v_p(n)}$, unique. Pour $a, b \neq 0$:

$$v_p(ab) = v_p(a) + v_p(b), \qquad a \mid b \Leftrightarrow \forall p,\ v_p(a) \leq v_p(b)$$

— **PGCD, PPCM** : $v_p(a \wedge b) = \min(v_p(a), v_p(b))$, $v_p(\text{ppcm}(a,b)) = \max(v_p(a), v_p(b))$.

— **Somme** : $v_p(a+b) \geq \min(v_p(a), v_p(b))$, avec **égalité** si $v_p(a) \neq v_p(b)$.

— **Diviseurs** : si $n = \prod p_i^{\alpha_i}$, le nombre et la somme des diviseurs positifs valent

$$\tau(n) = \prod_i (\alpha_i + 1), \qquad \sigma(n) = \prod_i \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

— **Legendre** : $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$ (somme finie).

— **Coefficients binomiaux** : si p est premier et $1 \leq k \leq p-1$, alors $p \mid \binom{p}{k}$.

Correction de l'exercice 1 – Crible et test de primalité

a) Si n est composé, $n = ab$ avec $2 \leq a \leq b$. Alors $a^2 \leq ab = n$, donc $a \leq \sqrt{n}$. Un diviseur premier p de a vérifie $p \leq a \leq \sqrt{n}$ et divise n.

$$n \text{ composé} \Longrightarrow \exists p \text{ premier},\ p \mid n \text{ et } p \leq \sqrt{n}$$

b) $\sqrt{391} \approx 19{,}8$: on teste $2, 3, 5, 7, 11, 13, 17, 19$. On trouve $391 = 17 \times 23$: **composé**.

— $\sqrt{397} \approx 19{,}9$: 397 est impair, la somme des chiffres 19 n'est pas multiple de 3, il ne finit ni par 0 ni par 5 ; $397 = 7 \times 56 + 5$, $11 \times 36 + 1$, $13 \times 30 + 7$, $17 \times 23 + 6$, $19 \times 20 + 17$. Aucun diviseur : 397 est **premier**.

c) $\sqrt{50} \approx 7{,}07$: il suffit de barrer les multiples de $2, 3, 5, 7$; tout nombre restant ≤ 50 est premier d'après a).

— Liste : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$ — quinze nombres premiers.

Piège : on s'arrête à $\sqrt{n}$, pas à $\frac{n}{2}$; pour 397 cela fait 8 essais au lieu de près de 200.

Réponse. $391 = 17 \times 23$ composé ; 397 premier ; crible jusqu'à 7, quinze premiers ≤ 50.

Correction de l'exercice 2 – Nombre et somme des diviseurs

a) $360 = 2 \times 180 = 2^2 \times 90 = 2^3 \times 45 = 2^3 \times 3^2 \times 5$.

b) Si $d \mid n$, tout premier divisant d divise n, et $v_{p_i}(d) \leq v_{p_i}(n) = \alpha_i$: $d = \prod p_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$. Réciproquement un tel produit divise n. Par unicité de la décomposition, deux choix différents des β_i donnent deux diviseurs différents :

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1)$$

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).

c) En développant le produit $\prod_i (1 + p_i + \ldots + p_i^{\alpha_i})$, on obtient la somme de tous les $\prod p_i^{\beta_i}$, chacun **une seule fois** : c'est la somme des diviseurs. Chaque facteur est une somme géométrique :

$$1 + p + \ldots + p^{\alpha} = \frac{p^{\alpha+1} - 1}{p - 1}$$

d) $\tau(360) = (3+1)(2+1)(1+1) = 24$ et

$$\sigma(360) = (1+2+4+8)(1+3+9)(1+5) = 15 \times 13 \times 6 = 1170$$

Piège : τ ne dépend que des **exposants** ; $\tau(360) = \tau(2^3 \times 5^2 \times 7) = 24$ aussi, pour un nombre bien différent.

Réponse. $360 = 2^3 \times 3^2 \times 5$; $\tau(360) = 24$, $\sigma(360) = 1170$.

Correction de l'exercice 3 – PGCD, PPCM et valuations

a) d divise a et b si et seulement si $v_p(d) \leq v_p(a)$ et $v_p(d) \leq v_p(b)$ pour tout p, soit $v_p(d) \leq \min(v_p(a), v_p(b))$. Le plus grand tel d prend l'exposant maximal permis : $\prod p^{\min}$. Même raisonnement pour les multiples communs, avec le plus petit exposant permis, le max.

b) Pour deux réels, $\min(x,y) + \max(x,y) = x + y$. En valuations :

$$v_p((a \wedge b)\text{ppcm}(a,b)) = \min + \max = v_p(a) + v_p(b) = v_p(ab)$$

— Deux entiers positifs de mêmes valuations pour tout p sont égaux.

c) On prend, pour chaque premier $p \leq 10$, la **plus grande puissance** $p^k \leq 10$: $2^3 = 8$, $3^2 = 9$, 5, 7.

— $\text{ppcm}(1, \ldots, 10) = 8 \times 9 \times 5 \times 7 = 2520$.

— Jusqu'à 20 : $2^4 = 16$, $3^2 = 9$, 5, 7, 11, 13, 17, 19, soit $16 \times 9 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 = 232\,792\,560$.

Piège : le PPCM de $1, \ldots, n$ n'est **pas** $n!$; pour $n = 10$, $10! = 3\,628\,800$ est 1440 fois trop grand.

Réponse. min et max des valuations ; ppcm(1..10) = 2520 ; ppcm(1..20) = 232 792 560.

Correction de l'exercice 4 – Cigales périodiques

a) Les cigales émergent les années kc, le prédateur les années jp (en comptant à partir de la rencontre). Les années communes sont les **multiples communs** de c et p : ils se retrouvent tous les

$$\text{ppcm}(c,p) = \frac{cp}{c \wedge p} \text{ ans}$$

b) Calculs avec $c = 12$ puis $c = 13$:

— $p = 2$: $\text{ppcm}(12,2) = 12$; $\text{ppcm}(13,2) = 26$.

— $p = 3$: 12 ; 39.

— $p = 4$: 12 ; 52.

— $p = 5$: 60 ; 65.

— $p = 6$: 12 ; 78.

Avec une période 12, quatre prédateurs sur cinq sont présents à **chaque** émergence ; avec 13, chacun n'est rencontré qu'une fois tous les 26 à 78 ans.

c) $\text{ppcm}(c,p) = cp$ est maximal quand $c \wedge p = 1$. Si c est premier et $c > 6$, on a $c \wedge p = 1$ pour **tous** les $p \leq 6$: chaque prédateur n'est rencontré que tous les cp ans. Un c composé

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).

partage un facteur avec certains p (12 avec $2, 3, 4, 6$), ce qui divise la durée entre deux rencontres.

Remarque : c'est une hypothèse de biologie, pas un théorème ; l'arithmétique dit seulement qu'elle est cohérente.

Réponse. Rencontre tous les ppcm(c, p) ans : 12 ans pour $c = 12$ ($p = 2, 3, 4, 6$) contre 26 à 78 ans pour $c = 13$.

Correction de l'exercice 5 – Carrés parfaits et casiers

a) Si $n = m^2$, alors $v_p(n) = 2v_p(m)$ est pair. Réciproquement, si $v_p(n) = 2\beta_p$ pour tout p, on pose $m = \prod p^{\beta_p}$ et $m^2 = n$.

b) Avec $n = \prod p_i^{\alpha_i}$:

$$\tau(n) = \prod_i (\alpha_i + 1) \text{ impair} \Leftrightarrow \text{tous les } \alpha_i + 1 \text{ impairs} \Leftrightarrow \text{tous les } \alpha_i \text{ pairs}$$

— ce qui équivaut à « n est un carré » d'après a).

— **Seconde preuve** : $d \mapsto \frac{n}{d}$ est une involution de l'ensemble des diviseurs. Les diviseurs se groupent par paires $\left\{d, \frac{n}{d}\right\}$, sauf quand $d = \frac{n}{d}$, c'est-à-dire $d = \sqrt{n}$. Il y a donc un nombre impair de diviseurs exactement quand $\sqrt{n}$ est entier.

c) Le casier n est touché par les élèves k tels que $k \mid n$: il change $\tau(n)$ fois d'état. Il est ouvert à la fin si et seulement si $\tau(n)$ est impair, donc si n est un carré.

— Casiers ouverts : $1, 4, 9, 16, 25, 36, 49, 64, 81, 100$ — dix casiers.

Contrôle : le casier 12 est touché par $1, 2, 3, 4, 6, 12$: six fois, il finit fermé ✓.

Réponse. Carré ⇔ valuations paires ⇔ $\tau(n)$ impair ; casiers ouverts : les dix carrés $1, 4, \ldots, 100$.

Correction de l'exercice 6 – Formule de Legendre et zéros de n factorielle

a) $v_p(n!) = \sum_{m=1}^{n} v_p(m)$. On écrit $v_p(m) = \sum_{k \geq 1} 1_{p^k \mid m}$ (on compte 1 pour p, p^2, …, $p^{v_p(m)}$) et on échange les sommes :

$$v_p(n!) = \sum_{k \geq 1} \text{card}\{m \leq n,\ p^k \mid m\} = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

— car les multiples de p^k entre 1 et n sont $p^k, 2p^k, \ldots, \left\lfloor \frac{n}{p^k} \right\rfloor p^k$. La somme est finie : les termes sont nuls dès $p^k > n$.

b) $v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$ et $v_5(100!) = 20 + 4 = 24$.

c) Le nombre de zéros finaux est $v_{10}(100!) = \min(v_2, v_5)$, puisque $10 = 2 \times 5$:

— $100!$ se termine par $\min(97, 24) = 24$ zéros ;

— $1000!$: $v_5 = 200 + 40 + 8 + 1 = 249$, et v_2 est bien plus grand : 249 zéros.

Piège : compter seulement les multiples de 5 (20 pour 100!) oublie que $25, 50, 75, 100$ apportent **deux** facteurs 5.

Réponse. $v_2(100!) = 97$, $v_5(100!) = 24$; $100!$ finit par 24 zéros, $1000!$ par 249.

Correction de l'exercice 7 – Valuations et irrationalité

a) Par l'absurde, $\sqrt{n} = \frac{a}{b}$ avec $a, b \in \mathbb{N}^*$, donc $a^2 = nb^2$. On prend un premier p tel que $v_p(n)$ soit **impair** (il en existe, car n n'est pas un carré). En appliquant v_p, qui transforme

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).

les produits en sommes :

$$2v_p(a) = v_p(n) + 2v_p(b)$$

— Le membre de gauche est pair, celui de droite impair : contradiction.

b) Si $\sqrt[3]{2} = \frac{a}{b}$, alors $a^3 = 2b^3$ et $3v_2(a) = 1 + 3v_2(b)$: un multiple de 3 égal à un entier congru à 1 modulo 3, contradiction.

c) $\log_{10} 2 > 0$. Si $\log_{10} 2 = \frac{a}{b}$ avec $a, b \in \mathbb{N}^*$, alors $10^{a/b} = 2$, soit

$$10^a = 2^b, \qquad \text{donc} \qquad 2^a 5^a = 2^b$$

— Par unicité de la décomposition, v_5 donne $a = 0$: impossible puisque $a \geq 1$.

Réflexe : pour une égalité entre produits d'entiers, appliquer une valuation bien choisie ramène tout à une égalité d'entiers sur laquelle on lit une parité ou un reste.

Réponse. v_p impair donne une contradiction de parité ; $\sqrt[3]{2}$ et $\log_{10} 2$ sont irrationnels.

Correction de l'exercice 8 – Longues suites de nombres composés

a) Pour $2 \leq k \leq n+1$, k divise $(n+1)!$ (c'est l'un des facteurs), donc k divise la somme :

$$k \mid (n+1)! + k, \qquad \text{et} \qquad 2 \leq k < (n+1)! + k$$

— $(n+1)! + k$ a un diviseur strict autre que 1 : il est composé. On a bien n valeurs de k.

b) $n = 6$: $7! = 5040$, d'où $5042, 5043, 5044, 5045, 5046, 5047$, divisibles respectivement par $2, 3, 4, 5, 6, 7$. Par exemple $5047 = 7 \times 721 = 7^2 \times 103$.

c) $24 = 2^3 \times 3$, $25 = 5^2$, $26 = 2 \times 13$, $27 = 3^3$, $28 = 2^2 \times 7$: cinq composés consécutifs, entre les premiers 23 et 29.

Conclusion : les écarts entre nombres premiers consécutifs **ne sont pas bornés** — d'après a), il existe des écarts au moins égaux à $n+1$ pour tout n.

Remarque : la construction de a) est très loin d'être optimale (5042 contre 24), mais elle a le mérite d'exister pour tout n.

Réponse. $k \mid (n+1)! + k$; pour $n = 6$: 5042 à 5047 ; 24 à 28 ; écarts entre premiers non bornés.

Correction de l'exercice 9 – Coefficients binomiaux et nombre premier

a) On part de la formule donnée, conséquence directe de $\binom{p}{k} = \frac{p!}{k!(p-k)!}$:

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

— p divise le membre de droite, donc $p \mid k\binom{p}{k}$.

— $1 \leq k \leq p-1$ et p premier donnent $p \wedge k = 1$; par **Gauss**, $p \mid \binom{p}{k}$.

b) Par la formule du binôme,

$$(a+b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$$

— chaque terme de la somme est multiple de p d'après a).

c) Initialisation : $0^p = 0$. **Hérédité** : par b) avec $b = 1$ puis l'hypothèse de récurrence,

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

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).

— Pour a négatif, on applique le résultat à un représentant positif de a modulo p.
— Si de plus $p \nmid a$, on simplifie par a (inversible modulo p) : $a^{p-1} \equiv 1 \pmod p$.

d) Non : $\binom{6}{2} = 15$ et $\binom{6}{3} = 20$ ne sont pas multiples de 6. L'argument de Gauss tombe, car $6 \wedge 2 \neq 1$. Contrôle pour $p = 7$: $7, 21, 35, 35, 21, 7$, tous multiples de 7 ✓.

Réponse. $p \mid \binom{p}{k}$; $(a+b)^p \equiv a^p + b^p$; $a^p \equiv a \pmod p$; faux pour 6 ($\binom{6}{2} = 15$).

Correction de l'exercice 10 – Infinité des nombres premiers de la forme 4k + 3

a) $(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1$; on conclut par récurrence sur le nombre de facteurs.

b) N est impair, donc tous ses facteurs premiers sont impairs, de la forme $4k+1$ ou $4k+3$. S'ils étaient **tous** de la forme $4k+1$, leur produit N le serait aussi d'après a) — or $N = 4k+3$. L'un d'eux au moins est de la forme $4k+3$.

c) $N = 4q_1 \cdots q_r - 1 = 4(q_1 \cdots q_r - 1) + 3$ est de la forme $4k+3$ et $N \geq 11$. D'après b), il a un diviseur premier q de la forme $4k+3$, donc $q = q_i$ pour un certain i. Alors

$$q_i \mid N \quad \text{et} \quad q_i \mid 4q_1 \cdots q_r \implies q_i \mid 4q_1 \cdots q_r - N = 1$$

— ce qui est absurde. Il y a une infinité de premiers de la forme $4k+3$.

d) $N = 4 \times 3 \times 7 - 1 = 83$, qui est premier et de la forme $4 \times 20 + 3$: c'est un premier « oublié » de la liste.

Piège : la même preuve échoue pour $4k+1$, car un produit de facteurs $4k+3$ peut être de la forme $4k+1$ ($3 \times 7 = 21$). Le résultat reste vrai, mais demande un autre argument.

Réponse. $N = 4q_1 \cdots q_r - 1$ a un facteur premier $4k+3$ hors liste ; pour $\{3, 7\}$: $N = 83$.

Correction de l'exercice 11 – Polynômes à valeurs premières

a) $P(0) = 41$, $P(1) = 43$, $P(2) = 47$: premiers. Pour $n = 40$:

$$P(40) = 40^2 + 40 + 41 = 40 \times 41 + 41 = 41^2 = 1681$$

— composé. De même $P(41) = 41^2 + 41 + 41 = 41 \times 43$: composé. (Euler a remarqué que $P(n)$ est premier pour $n = 0, \ldots, 39$.)

b) Écrivons $Q = \sum_j c_j X^j$. Pour chaque j, $a - b \mid a^j - b^j$; avec $a = n_0 + km$ et $b = n_0$, on obtient $m \mid (n_0 + km)^j - n_0^j$. En sommant avec les coefficients c_j :

$$Q(n_0 + km) - Q(n_0) = \sum_j c_j \Big((n_0 + km)^j - n_0^j \Big) \equiv 0 \pmod m$$

— donc $Q(n_0 + km) \equiv Q(n_0) = m \equiv 0 \pmod m$.

c) Supposons $Q(n)$ premier pour tout $n \in \mathbb{N}$; soit $m = Q(0)$, premier donc ≥ 2. D'après b), $m \mid Q(km)$ pour tout $k \in \mathbb{N}$, et $Q(km)$ est premier : $Q(km) = m$. Le polynôme $Q - m$ a alors une infinité de racines $0, m, 2m, \ldots$: il est nul, et Q est constant. Contradiction.

Réponse. $P(40) = 41^2$, $P(41) = 41 \times 43$; $m \mid Q(n_0 + km)$; aucun polynôme non constant n'est « générateur de premiers ».

Correction de l'exercice 12 – Nombres parfaits pairs

a) 6 : $1 + 2 + 3 = 6$. 28 : $1 + 2 + 4 + 7 + 14 = 28$.

b) Si $a \wedge b = 1$, les décompositions de a et b n'ont aucun premier commun ; la formule du

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).

cours se scinde :

$$\sigma(ab) = \prod_{p \mid ab} \frac{p^{v_p(ab)+1}-1}{p-1} = \prod_{p \mid a} \frac{p^{v_p(a)+1}-1}{p-1} \times \prod_{p \mid b} \frac{p^{v_p(b)+1}-1}{p-1}$$

— soit $\sigma(ab) = \sigma(a)\sigma(b)$. Contrôle : $\sigma(4)\sigma(9) = 7 \times 13 = 91 = \sigma(36)$ ✓.

c) 2^{p-1} et $q = 2^p - 1$ sont premiers entre eux (q est impair). Par b) :

— $\sigma(2^{p-1}) = 1 + 2 + \ldots + 2^{p-1} = 2^p - 1$;
— $\sigma(q) = 1 + q = 2^p$, car q est premier.

Donc $\sigma(n) = (2^p - 1) \times 2^p = 2 \times 2^{p-1}(2^p - 1) = 2n$.

d) $2^p - 1$ est premier pour $p = 2, 3, 5, 7$ (3, 7, 31, 127), mais pas pour $p = 4$ (15) ni $p = 6$ (63) : $n = 6$, 28, 496, 8128.

Remarque : Euler a montré que **tous** les parfaits pairs sont de cette forme ; on ne sait pas s'il existe un parfait impair.

Réponse. σ est multiplicative ; $\sigma\left(2^{p-1}(2^p-1)\right) = 2^p(2^p-1)$; 6, 28, 496, 8128.

Correction de l'exercice 13 – La série harmonique ne donne jamais d'entier

a) Si $v_2(k) \geq m$ et $k \leq n < 2^{m+1}$, alors $k = 2^m \times j$ avec j impair et $j < 2$: $j = 1$. Donc $k = 2^m$ est l'unique entier de valuation m, et aucun n'a de valuation $> m$. La valuation d'un PPCM est le maximum :

$$v_2(L) = \max_{1 \leq k \leq n} v_2(k) = m$$

b) Chaque $\frac{L}{k}$ est entier puisque $k \mid L$. Par additivité des valuations :

$$v_2\left(\frac{L}{k}\right) = m - v_2(k)$$

— nul pour $k = 2^m$ (terme **impair**), strictement positif pour les autres (termes **pairs**).
— La somme d'un impair et de pairs est **impaire** : LH_n est un entier impair.

c) Si H_n était entier, LH_n serait pair, car $v_2(L) = m \geq 1$ pour $n \geq 2$. Contradiction : $H_n \notin \mathbb{N}$.

— $H_4 = \frac{25}{12}$: $L = 12$, $LH_4 = 25$ impair ✓. $H_6 = \frac{49}{20}$: $L = 60$, $LH_6 = 147$ impair ✓.

Réponse. LH_n est impair et L est pair : H_n n'est jamais entier pour $n \geq 2$ ($H_4 = \frac{25}{12}$, $H_6 = \frac{49}{20}$).

Correction de l'exercice 14 – Facteurs premiers du coefficient binomial central

a) On écrit $x = \lfloor x \rfloor + t$ avec $t \in [0, 1[$. Alors $\lfloor 2x \rfloor = 2\lfloor x \rfloor + \lfloor 2t \rfloor$ et $\lfloor 2t \rfloor \in \{0, 1\}$.

b) $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$, donc par la formule de Legendre

$$v_p\binom{2n}{n} = \sum_{k \geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor \right)$$

— Chaque terme vaut 0 ou 1 d'après a), et il est nul dès que $p^k > 2n$ (les deux parties entières sont nulles).
— La somme compte donc au plus les k tels que $p^k \leq 2n$, soit $v_p\binom{2n}{n} \leq K$ avec $p^K \leq 2n$, d'où $p^{v_p} \leq p^K \leq 2n$.

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).

c) Si $n < p \leq 2n$: pour $k = 1$, $\left\lfloor \frac{2n}{p} \right\rfloor = 1$ (car $p \leq 2n < 2p$) et $\left\lfloor \frac{n}{p} \right\rfloor = 0$, terme 1 ; pour $k \geq 2$, $p^2 > 2n$ dès que $n \geq 2$, termes nuls. Donc $v_p = 1$ (et pour $n = 1$, $\binom{2}{1} = 2$ ✓).

d) $184\,756 = 2^2 \times 11 \times 13 \times 17 \times 19$.

— Les premiers de $]10, 20]$ — $11, 13, 17, 19$ — apparaissent chacun une fois ✓.

— $v_2 = (10 - 10) + (5 - 4) + (2 - 2) + (1 - 0) = 2$ et $2^2 = 4 \leq 20$ ✓ ; $v_3 = v_5 = v_7 = 0$.

Intérêt : ces majorations sont le point de départ de la preuve du **postulat de Bertrand** (il y a toujours un premier entre n et $2n$).

Réponse. $v_p\binom{2n}{n} \leq \log_p(2n)$; premiers de $]n, 2n]$ avec exposant 1 ; $\binom{20}{10} = 2^2 \times 11 \times 13 \times 17 \times 19$.

Correction de l’exercice 15 – Synthèse : entiers ayant un nombre de diviseurs imposé

a) $\tau(n) = \prod(\alpha_i + 1) = 10$: on écrit 10 comme produit de facteurs ≥ 2, soit 10 ou 5×2. Donc

$$n = p^9 \qquad \text{ou} \qquad n = p^4 q \quad (p \neq q)$$

— Minimum dans chaque cas : $2^9 = 512$ et $2^4 \times 3 = 48$ (on met le plus grand exposant sur le plus petit premier). Le plus petit est 48 : diviseurs $1, 2, 3, 4, 6, 8, 12, 16, 24, 48$ ✓.

b) $12 = 12 = 6 \times 2 = 4 \times 3 = 3 \times 2 \times 2$: p^{11}, $p^5 q$, $p^3 q^2$, $p^2 qr$. Minima : 2048, 96, 72, $2^2 \times 3 \times 5 = 60$. Le plus petit est 60.

c) $\tau(n) = 2$: les seuls diviseurs sont 1 et $n \neq 1$ — c’est la définition d’un premier. $\tau(n) = 3$: 3 est premier, donc $n = p^2$ avec p premier $(4, 9, 25, \ldots)$.

d) On associe à chaque diviseur d le diviseur $\frac{n}{d}$: l’un des deux est $\leq \sqrt{n}$. Tout diviseur s’obtient donc à partir d’un diviseur $\leq \sqrt{n}$ (lui-même ou son associé) :

$$\tau(n) \leq 2\,\mathrm{card}\{d \mid n,\ d \leq \sqrt{n}\} \leq 2\sqrt{n}$$

— Contrôle : $\tau(60) = 12 \leq 2\sqrt{60} \approx 15{,}5$ ✓ ; $\tau(48) = 10 \leq 13{,}9$ ✓.

Réponse. $\tau(n) = 10$: plus petit $48 = 2^4 \times 3$; $\tau(n) = 12$: 60 ; $\tau(n) = 2 \Leftrightarrow n$ premier, $\tau(n) = 3 \Leftrightarrow n = p^2$; $\tau(n) \leq 2\sqrt{n}$.

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).