Plaquette 3 – Nombres premiers, valuations et diviseurs

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

Exercices

Méthode

Tout entier $n \geq 2$ s'écrit de façon unique $n = \prod p^{v_p(n)}$: la **valuation** p**-adique** $v_p(n)$ transforme les produits en sommes, et presque tout se lit sur les exposants — divisibilité ($a \mid b \Leftrightarrow v_p(a) \leq v_p(b)$ pour tout p), PGCD (min), PPCM (max), carrés (exposants pairs), nombre de diviseurs. Pour une factorielle, la **formule de Legendre** donne $v_p(n!)$ sans rien multiplier.

Exercice 1 – Crible et test de primalité

a) Montrer que si $n \geq 2$ n'est pas premier, il admet un diviseur premier $p \leq \sqrt{n}$.

b) Les nombres 391 et 397 sont-ils premiers ? Justifier en limitant les essais.

c) Dresser la liste des nombres premiers inférieurs à 50 par le crible d'Ératosthène : jusqu'à quel nombre premier faut-il barrer les multiples ?

Exercice 2 – Nombre et somme des diviseurs

a) Décomposer 360 en facteurs premiers.

b) Montrer que les diviseurs positifs de $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ sont exactement les $\prod p_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$. En déduire $\tau(n) = \prod (\alpha_i + 1)$.

c) Montrer que la somme des diviseurs vaut $\sigma(n) = \prod_i (1 + p_i + \ldots + p_i^{\alpha_i})$.

d) Calculer $\tau(360)$ et $\sigma(360)$.

Exercice 3 – PGCD, PPCM et valuations

a) Justifier que $v_p(a \wedge b) = \min(v_p(a), v_p(b))$ et $v_p(\text{ppcm}(a,b)) = \max(v_p(a), v_p(b))$ pour $a, b \in \mathbb{N}^*$.

b) En déduire une nouvelle preuve de $\text{pgcd}(a,b) \times \text{ppcm}(a,b) = ab$.

c) Calculer $\text{ppcm}(1, 2, \ldots, 10)$, puis le plus petit entier strictement positif divisible par tous les entiers de 1 à 20.

Exercice 4 – Cigales périodiques

Certaines cigales d'Amérique du Nord n'émergent que tous les 13 ou 17 ans. Une hypothèse explique ces périodes premières par l'évitement de prédateurs eux-mêmes périodiques, de période $p \in \{2, 3, 4, 5, 6\}$ ans.

a) Des cigales de période c et un prédateur de période p émergent ensemble une année donnée. Au bout de combien d'années se retrouvent-ils ?

b) Comparer, pour chaque $p \in \{2, 3, 4, 5, 6\}$, des cigales de période 12 et de période 13.

c) Expliquer pourquoi une période **première** et assez grande minimise les rencontres.

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).

Exercice 5 – Carrés parfaits et casiers

a) Montrer que $n \in \mathbb{N}^*$ est un carré parfait si et seulement si toutes ses valuations $v_p(n)$ sont paires.

b) En déduire que $\tau(n)$ est impair si et seulement si n est un carré. Donner une seconde preuve en associant chaque diviseur d à $\frac{n}{d}$.

c) Un couloir compte 100 casiers fermés. Pour $k = 1, 2, \ldots, 100$, l'élève k change l'état (ouvert/fermé) de tous les casiers dont le numéro est multiple de k. Quels casiers sont ouverts à la fin ?

Exercice 6 – Formule de Legendre et zéros de n factorielle

Soit p premier et $n \in \mathbb{N}^*$.

a) En comptant, pour chaque $k \geq 1$, les entiers de 1 à n divisibles par p^k, établir la formule de Legendre $v_p(n!) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$.

b) Calculer $v_2(100!)$ et $v_5(100!)$.

c) Par combien de zéros se termine l'écriture décimale de 100! ? De 1000! ?

Exercice 7 – Valuations et irrationalité

a) Soit $n \in \mathbb{N}^*$ qui n'est pas un carré parfait. En raisonnant sur une valuation, montrer que $\sqrt{n}$ est irrationnel.

b) Montrer que $\sqrt[3]{2}$ est irrationnel.

c) Montrer que $\log_{10} 2 = \frac{\ln 2}{\ln 10}$ est irrationnel.

Exercice 8 – Longues suites de nombres composés

a) Soit $n \geq 1$. Montrer que les n entiers consécutifs $(n+1)! + 2$, $(n+1)! + 3$, …, $(n+1)! + (n+1)$ sont tous composés.

b) Écrire la suite obtenue pour $n = 6$ et donner un diviseur de chaque terme.

c) Trouver par un autre moyen une suite de 5 entiers consécutifs composés, tous inférieurs à 30. Que peut-on dire des écarts entre nombres premiers consécutifs ?

Exercice 9 – Coefficients binomiaux et nombre premier

Soit p un nombre premier.

a) Montrer que p divise $\binom{p}{k}$ pour $1 \leq k \leq p-1$ (on pourra partir de $k\binom{p}{k} = p\binom{p-1}{k-1}$).

b) En déduire que $(a+b)^p \equiv a^p + b^p \pmod{p}$ pour tous $a, b \in \mathbb{Z}$.

c) En déduire par récurrence sur $a \in \mathbb{N}$ que $a^p \equiv a \pmod{p}$ (petit théorème de Fermat).

d) Le résultat de a) reste-t-il vrai pour $p = 6$?

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).

Exercice 10 – Infinité des nombres premiers de la forme 4k + 3

a) Montrer qu'un produit d'entiers tous de la forme $4k+1$ est encore de cette forme.

b) Montrer que tout entier $N \geq 2$ de la forme $4k+3$ admet un diviseur premier de la forme $4k+3$.

c) On suppose qu'il n'existe qu'un nombre fini de premiers de la forme $4k+3$, notés $q_1, \ldots, q_r$. En considérant $N = 4q_1 \cdots q_r - 1$, aboutir à une contradiction.

d) Calculer N si la liste était $\{3, 7\}$ et le décomposer.

Exercice 11 – Polynômes à valeurs premières

a) Vérifier que $P(n) = n^2 + n + 41$ est premier pour $n = 0, 1, 2$, puis montrer sans calculatrice que $P(40)$ ne l'est pas. Et $P(41)$?

b) Soit $Q \in \mathbb{Z}[X]$ non constant et $n_0 \in \mathbb{N}$ tel que $m = Q(n_0) \geq 2$. Montrer que m divise $Q(n_0 + km)$ pour tout $k \in \mathbb{Z}$.

c) En déduire qu'aucun polynôme non constant à coefficients entiers ne prend que des valeurs premières sur $\mathbb{N}$.

Exercice 12 – Nombres parfaits pairs

Un entier $n \geq 2$ est **parfait** si $\sigma(n) = 2n$ (la somme de ses diviseurs stricts vaut n).

a) Vérifier que 6 et 28 sont parfaits.

b) Montrer que $\sigma(ab) = \sigma(a)\sigma(b)$ si $a \wedge b = 1$.

c) Soit p tel que $2^p - 1$ soit premier. Montrer que $n = 2^{p-1}(2^p - 1)$ est parfait.

d) Donner les quatre plus petits nombres parfaits obtenus ainsi.

Exercice 13 – La série harmonique ne donne jamais d'entier

Pour $n \geq 2$, on pose $H_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n}$. On note m l'entier tel que $2^m \leq n < 2^{m+1}$, et $L = \text{ppcm}(1, \ldots, n)$.

a) Montrer que 2^m est le seul entier $k \in \{1, \ldots, n\}$ tel que $v_2(k) = m$, et que $v_2(L) = m$.

b) Montrer que $LH_n = \sum_{k=1}^{n} \frac{L}{k}$ est une somme d'entiers dont un seul est impair.

c) En déduire que H_n n'est jamais un entier. Vérifier sur H_4 et H_6.

Exercice 14 – Facteurs premiers du coefficient binomial central

Soit $n \geq 1$ et p premier.

a) Montrer que pour tout réel x, $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\}$.

b) À l'aide de la formule de Legendre, montrer que $v_p\left(\binom{2n}{n}\right) \leq \max\{k,\ p^k \leq 2n\}$, et en déduire que $p^{v_p\left(\binom{2n}{n}\right)} \leq 2n$.

c) Montrer que tout premier p tel que $n < p \leq 2n$ divise $\binom{2n}{n}$ exactement une fois.

d) Décomposer $\binom{20}{10} = 184\,756$ et vérifier b) et c).

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).

Exercice 15 – Synthèse : entiers ayant un nombre de diviseurs imposé

a) Quelles sont les formes possibles de la décomposition d'un entier n tel que $\tau(n) = 10$? En déduire le plus petit tel n.

b) Même question pour $\tau(n) = 12$.

c) Montrer que $\tau(n) = 2$ si et seulement si n est premier, et décrire les n tels que $\tau(n) = 3$.

d) Montrer que $\tau(n) \leq 2\sqrt{n}$ pour tout $n \geq 1$.

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).