Terminale Maths expertes

Les nombres premiers

Fiche d'exercices

Dans toute la fiche, la lettre n désigne un entier naturel et la lettre p un nombre premier, sauf mention contraire. Les exercices sont rangés par difficulté croissante ; la série D rassemble cinq problèmes tirés de situations concrètes.

Série A ⋆ Automatismes

Exercice 1 : premier ou pas ? ⋆

Les entiers suivants sont-ils premiers ? Justifier en précisant jusqu'à quel nombre premier on teste les divisions.

a. 97 **b.** 111 **c.** 221 **d.** 289 **e.** 331 **f.** 1 001

Exercice 2 : décompositions ⋆

Décomposer en produit de facteurs premiers :

a. 504 **b.** 1 960 **c.** 3 600 **d.** 10 395

Exercice 3 : compter les diviseurs ⋆

a. Déterminer le nombre de diviseurs positifs de chacun des entiers : 180, 96, 1 024 et 6 125.

b. Écrire la liste de tous les diviseurs positifs de 96, en s'aidant d'un tableau.

Exercice 4 : PGCD et PPCM ⋆

À l'aide des décompositions en facteurs premiers, déterminer le PGCD et le PPCM des couples suivants, puis vérifier la relation $\text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) = ab$.

a. $a = 84$ et $b = 120$; **b.** $a = 1\,386$ et $b = 1\,960$.

Exercice 5 : petit théorème de Fermat ⋆

a. Montrer, sans calculatrice, que 17 divise $3^{16} - 1$.

b. Déterminer le reste de la division euclidienne de 2^{60} par 7.

c. Déterminer le reste de la division euclidienne de $5^{2\,026}$ par 11.

Série B ⋆⋆ Entraînement

Exercice 6 : carrés et cubes ⋆⋆

a. Décomposer 1 350 en produit de facteurs premiers.

b. Justifier qu'un entier $N \geqslant 2$ est le carré d'un entier si, et seulement si, tous les exposants de sa décomposition sont pairs.

c. Déterminer le plus petit entier naturel k non nul tel que $1\,350\,k$ soit le carré d'un entier. Préciser cet entier.

d. Déterminer le plus petit entier naturel k non nul tel que $1\,350\,k$ soit le cube d'un entier.

Exercice 7 : un nombre de diviseurs imposé ⋆⋆

a. Montrer que les entiers naturels qui ont exactement 3 diviseurs positifs sont les carrés des nombres premiers.

b. Quelles sont les formes possibles d'un entier naturel qui a exactement 4 diviseurs positifs ? Donner deux exemples de chaque forme.

c. Déterminer le plus petit entier naturel qui a exactement 10 diviseurs positifs.

Exercice 8 : des expressions rarement premières ⋆⋆

a. Vérifier que, pour tout entier n : $n^4 + 4 = \left(n^2 + 2n + 2\right)\left(n^2 - 2n + 2\right)$.

b. En déduire les entiers naturels n pour lesquels $n^4 + 4$ est un nombre premier.

c. On considère $E(n) = n^2 + n + 41$. Calculer $E(0)$, $E(1)$, …, $E(5)$: que constate-t-on ?
Montrer que $E(40)$ n'est pas premier. Que peut-on en conclure ?

Exercice 9 : nombres parfaits ⋆⋆

Un entier $N \geqslant 2$ est dit **parfait** si la somme de ses diviseurs positifs est égale à $2N$ (autrement dit, N est égal à la somme de ses diviseurs positifs autres que lui-même).

a. Vérifier que 6 et 28 sont parfaits.

b. Décomposer 496, écrire la liste de ses diviseurs positifs et montrer que 496 est parfait.

c. Soit $k \geqslant 2$ un entier tel que $p = 2^k - 1$ soit premier, et $N = 2^{k-1}\,p$.
Écrire la liste des diviseurs positifs de N, puis montrer que N est parfait.
On rappelle que $1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$.

Exercice 10 : une divisibilité par 42 ⋆⋆

a. Justifier que, pour tout entier n, 7 divise $n^7 - n$.

b. Montrer que n^7 et n ont la même parité. En déduire que 2 divise $n^7 - n$.

c. En utilisant $n^3 \equiv n\ [3]$, montrer que $n^7 \equiv n\ [3]$.

d. En déduire que $n^7 - n$ est divisible par 42 pour tout entier n.

Série C ⋆⋆⋆ Approfondissement

Exercice 11 : $\sqrt{2}$ est irrationnel ⋆⋆⋆

On suppose qu'il existe deux entiers naturels non nuls a et b tels que $\sqrt{2} = \dfrac{a}{b}$.

a. Montrer que $a^2 = 2b^2$.

b. On note α l'exposant de 2 dans la décomposition de a (avec $\alpha = 0$ si 2 ne divise pas a) et β celui de b. Quel est l'exposant de 2 dans la décomposition de a^2 ? Dans celle de $2b^2$?

c. Conclure à l'aide de l'unicité de la décomposition.

d. En adaptant ce raisonnement, montrer que $\sqrt{p}$ est irrationnel pour tout nombre premier p.

Exercice 12 : une infinité de nombres premiers de la forme $4k+3$ ⋆⋆⋆

a. Montrer qu'un nombre premier impair s'écrit soit sous la forme $4k+1$, soit sous la forme $4k+3$, avec k entier naturel.

b. Montrer que le produit de deux entiers de la forme $4k+1$ est encore de cette forme. Qu'en est-il d'un produit de plusieurs tels entiers ?

c. On suppose qu'il n'existe qu'un nombre fini de nombres premiers de la forme $4k+3$; on les note $p_1 = 3, p_2, \ldots, p_r$. On pose $N = 4\,p_1 p_2 \cdots p_r - 1$.

1) Montrer que N est impair et que N est de la forme $4k+3$.

2) Montrer qu'aucun des nombres premiers $p_1, \ldots, p_r$ ne divise N.

3) En utilisant la décomposition de N, aboutir à une contradiction et conclure.

Exercice 13 : les puissances de 2 modulo 7 ⋆⋆⋆

a. Déterminer, suivant les valeurs de l'entier naturel n, le reste de la division euclidienne de 2^n par 7.

b. En déduire les entiers naturels n tels que 7 divise $2^n - 1$.

c. Le petit théorème de Fermat donne $2^6 \equiv 1\ [7]$. Est-ce que 6 est le plus petit exposant $k \geqslant 1$ tel que $2^k \equiv 1\ [7]$? Commenter.

d. Déterminer le reste de la division euclidienne de $2^{2\,026} + 3^{2\,026}$ par 7.

Exercice 14 : un « faux premier » ⋆⋆⋆

a. Montrer que 341 n'est pas premier.

b. Montrer que $2^{340} \equiv 1\ [11]$, puis, en remarquant que $2^5 \equiv 1\ [31]$, que $2^{340} \equiv 1\ [31]$.

c. En déduire que $2^{340} \equiv 1\ [341]$. La réciproque du petit théorème de Fermat est-elle vraie ?

d. Montrer que $3^5 \equiv -5\ [31]$, puis que $3^{340} \equiv 25\ [31]$. En déduire que $3^{340} \not\equiv 1\ [341]$: le test « avec la base 3 » démasque 341.

Exercice 15 : le crible d'Ératosthène en Python ⋆⋆⋆

Python

```
def crible(n):
    est_p = [True] * (n + 1)
    est_p[0] = False
    est_p[1] = False
    d = 2
    while d * d <= n:
        if est_p[d]:
            for m in range(d * d, n + 1, d):
                est_p[m] = False
        d = d + 1
    premiers = []
    for k in range(n + 1):
        if est_p[k]:
            premiers.append(k)
    return premiers
```

La fonction `crible` « barre » les multiples des nombres premiers et renvoie la liste des entiers restants.

a. Que renvoie `crible(30)` ?

b. Expliquer pourquoi on peut arrêter la boucle `while` dès que $d^2 > n$.

c. Expliquer pourquoi on peut commencer à barrer à partir de d^2.

d. Écrire une instruction qui affiche le nombre de nombres premiers inférieurs à 1 000. Le programme affiche 168 ; combien y en a-t-il inférieurs à 100 ?

e. Deux nombres premiers sont **jumeaux** s'ils diffèrent de 2 (comme 11 et 13). Écrire un programme qui affiche les couples de nombres premiers jumeaux inférieurs à 100. Combien y en a-t-il ?

Série D Problèmes en situation concrète

Exercice 16 : installer une salle de spectacle ⋆⋆

Pour un concert, on doit installer 360 chaises en rangées qui comptent toutes le même nombre de chaises.

a. Décomposer 360 en produit de facteurs premiers.

b. Combien y a-t-il de dispositions possibles ? *(Une disposition est donnée par le nombre de rangées ;* 10 *rangées de* 36 *chaises et* 36 *rangées de* 10 *chaises sont deux dispositions différentes.)*

c. Pour des raisons de sécurité et de visibilité, il faut au moins 10 rangées et au moins 10 chaises par rangée. Donner toutes les dispositions possibles.

Exercice 17 : deux roues dentées ⋆⋆

Deux roues dentées s'engrènent : la roue A a 24 dents et la roue B en a 36. On marque d'un point de peinture une dent de chaque roue, au moment où ces deux dents sont en contact.

a. Au bout de combien de tours de chaque roue les deux dents marquées seront-elles à nouveau en contact pour la première fois ?

b. On remplace la roue B par une roue de 35 dents. Même question.

c. Pour que l'usure soit répartie sur toutes les dents, les mécaniciens choisissent souvent des nombres de dents premiers entre eux. Expliquer pourquoi, à l'aide des questions précédentes.

Exercice 18 : un cube de briques ⋆⋆

Un artiste dispose de briques en forme de pavés droits de dimensions 12 cm, 18 cm et 30 cm. Il veut construire un cube plein en empilant ces briques, toutes posées dans le même sens.

a. Expliquer pourquoi la longueur, en centimètres, de l'arête du cube doit être un multiple commun de 12, 18 et 30.

b. Quelle est la plus petite arête possible ? Combien de briques faut-il alors ?

c. Quelles arêtes sont possibles si le cube doit mesurer moins de 5 mètres ?

Exercice 19 : les cigales périodiques ⋆⋆⋆

En Amérique du Nord, certaines espèces de cigales passent toute leur vie sous terre et n'en sortent, toutes ensemble, que tous les 13 ans ou tous les 17 ans. Une hypothèse explique ces durées par la présence de prédateurs, qui apparaissent eux aussi périodiquement, avec un cycle de c années, c étant compris entre 2 et 6.
On suppose qu'une année, cigales et prédateurs apparaissent en même temps.

a. Expliquer pourquoi ils se rencontrent de nouveau pour la première fois au bout de $\text{PPCM}(13\,;c)$ années pour des cigales de cycle 13 ans.

b. Calculer $\text{PPCM}(13\,;c)$ pour $c = 2, 3, 4, 5, 6$, puis $\text{PPCM}(12\,;c)$ pour les mêmes valeurs. Comparer.

c. Soit p un nombre premier supérieur à 6 et c un entier compris entre 2 et 6. Montrer que $\text{PPCM}(p\,;c) = pc$. Pourquoi un cycle de durée première est-il avantageux pour les cigales ?

d. Deux espèces de cycles 13 et 17 ans vivent dans la même forêt. Tous les combien d'années sortent-elles la même année ?

Exercice 20 : un chiffrement à clé publique ⋆⋆⋆⋆

Alice veut recevoir des messages secrets. Elle publie le nombre $n = 55 = 5 \times 11$ et la **clé publique** $e = 3$, et garde secrète sa **clé privée** $d = 27$.
Un message est un entier a tel que $0 \leqslant a \leqslant 54$.
• Pour chiffrer a, on calcule le reste b de la division euclidienne de a^3 par 55.
• Pour déchiffrer b, Alice calcule le reste de la division euclidienne de b^{27} par 55.

a. Bob chiffre le message $a = 7$. Quel nombre b envoie-t-il ?

b. Vérifier que $3 \times 27 \equiv 1\ [40]$, où $40 = (5-1)(11-1)$.

c. Montrer que, pour tout entier a : $a^{81} \equiv a\ [5]$ et $a^{81} \equiv a\ [11]$. *On pourra distinguer selon que a est divisible ou non par* 5 *(respectivement par* 11*).*

d. En déduire que, pour tout entier a, $a^{81} \equiv a\ [55]$.

e. Expliquer pourquoi Alice retrouve toujours le message de départ. Vérifier, en remarquant que $13^2 \equiv 4\ [55]$, qu'Alice obtient bien 7 en déchiffrant le nombre envoyé par Bob.

f. Alice a choisi d tel que $3d \equiv 1\ [40]$, avec $40 = (5-1)(11-1)$: pour calculer d, un espion doit donc connaître les facteurs premiers 5 et 11 de n. Pourquoi ce système n'est-il sûr que si n est le produit de deux très grands nombres premiers ?