

Devoir à faire à la Maison – Terminale

Option mathématiques expertes

jeudi 25 janvier 2024

On donne ci-dessous 20 sujets de DM. Vous choisirez au choix un de ces sujets, en fonction des compétences que vous souhaitez travailler.

Ce travail est à faire par équipe de trois élèves au maximum. Attention, aucun sujet ne peut être simultanément pris par deux groupes.

Pour valider le sujet choisi, chaque groupe d'élève enverra (par École Directe) un mail indiquant au professeur le sujet souhaité et les noms des élèves concernés. Chaque groupe aura un temps de passage de 12 min, dont 8 min de présentation et 4 minutes d'échange avec la classe et le professeur.

Pour tous les sujets, une trace écrite devra être rendue à votre professeur. Pour les sujets 1 à 9, celle-ci ne contiendra que la résolution des questions mathématiques posées. Pour les sujets 12 à 20, vous rendrez une synthèse de lecture tenant sur une feuille au format A4 (recto-verso).

La présentation orale sera à faire à l'aide du vidéo-projecteur et d'un document (type powerpoint, ou format libre du même type) qui sera à fournir sur une clef usb.

Sujet 1 Résoudre l'exercice 120 p. 161 du livre : «Changer de couleur ou non».

Sujet 2 Résoudre le problème 167 p. 195 du livre : «Payer en euros».

Sujet 3 Résoudre le problème 133 p. 223 du livre : «Déterminer une fonction».

Sujet 4 Méthode générale de résolution d'une équation diophantienne.

On se donne trois entiers a , b et c avec $ab \neq 0$. La relation suivante, aux inconnues entières x et y ,

$$ax + by = c, \quad (1)$$

se nomme *équation diophantienne*.

1. Montrer que, si une solution (x, y) existe dans \mathbb{Z}^2 , alors $d = \text{PGCD}(a; b)$ divise c .
2. Cette condition étant remplie, on pose $a = d\alpha$, $b = d\beta$, $c = d\gamma$. Montrer que l'équation (1) est équivalente à

$$\alpha x + \beta y = \gamma \quad (\text{PGCD}(\alpha; \beta) = 1).$$

Donner les solutions de cette équation.

3. Application : donner effectivement les solutions de l'équation

$$476x + 364y = 140$$

4. Qui était Diophante? Faire une note historique sur ce personnage (ses œuvres, son influence dans l'histoire des mathématiques).

Sujet 5 *Système de congruences.*

On se propose de déterminer les entiers relatifs x vérifiant le système

$$\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 4 \pmod{15} \end{cases} \quad (2)$$

1. Montrer que la résolution de (2) se ramène à celle de l'équation

$$11u + 15v = 1, \quad u, v \text{ dans } \mathbb{Z}. \quad (3)$$

2. Résoudre (3). En déduire les solutions de (2).
3. Faire une recherche historique sur le *théorème des restes chinois*. En particulier expliquer comment ce type de problème permet de résoudre des problèmes d'astronomie.

Sujet 6 *Le magicien.*

Le magicien dit : «Choisissez, sans me le dire, un nombre entier entre 1 et 500. Je vais seulement vous demander trois nombres construits à l'aide de celui-ci et je retrouverais sans trop de difficulté le nombre que vous aviez choisi. Pour cela, divisez votre nombre par 5 et donnez moi le reste obtenu. Faites de même avec la division par 7 et celle par 19. Ces trois restes me suffisent pour retrouver votre nombre.»

1. Expliquer pourquoi le magicien trouve toujours le bon nombre.
2. Amusez-vous bien.

Sujet 7 *Le chiffrement de Hill*

Dans les années 1920, Lester Hill montra comment appliquer l'algèbre à la cryptographie : son procédé permettait de coder non pas lettre par lettre, mais par bloc de deux, trois ou quatre lettres. Dans ce qui suit, les blocs seront composés de deux lettres (bigrammes).

Principe du chiffrement de Hill (cas des bigrammes)

On commence par écrire le message à crypter en clair en supprimant espace et ponctuation.

On découpe ensuite le message par blocs de deux lettres (quitte à rajouter «x» si le message comporte un nombre impair de lettres).

Puis à chaque lettre, on associe un nombre selon le tableau suivant :

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

On choisit quatre entiers a , a' , b et b' tels que le système

$$\begin{cases} ax + by \equiv c & [26] \\ a'x + b'y \equiv c' & [26] \end{cases}$$

admette toujours une solution unique dans $\{0; 1; \dots; 25\} \times \{0; 1; \dots; 25\}$ quels que soient c et c' .

Les coefficients a , b , a' et b' sont des éléments de la clef secrète.

Pour un bigramme, on remplace x et y par les deux nombres correspondants aux lettres du bigramme. On en déduit les deux nombres c et c' , que l'on remplace par les lettres correspondantes dans le tableau.

On recommence pour le bigramme suivant.

Si le nombre de lettre est impair, on convient d'ajouter la lettre X au message.

Par exemple : on choisit $a = 8$, $b = 3$, $a' = 5$ et $b' = 2$. Pour coder «AH», on remplace x par 0 et y par 7, on en déduit $c = 21$, qui correspond à V, et $c' = 14$, qui correspond à O. Ainsi, «AH» est chiffré en «VO».

Questions

1. Démontrer que le système

$$\begin{cases} 8x + 3y \equiv c & [26] \\ 5x + 2y \equiv c' & [26] \end{cases}$$

admet toujours des solutions, quels que soient c et c' .

Calculer x et y en fonction de c et c' .

2. On choisit $a = 8$, $b = 3$, $a' = 5$ et $b' = 2$. Coder le message «message top secret». Donner les formules qui permettent de le déchiffrer (on connaît c et c' et on cherche x et y).
3. Démontrer que le système

$$\begin{cases} ax + by \equiv c & [26] \\ a'x + b'y \equiv c' & [26] \end{cases}$$

admet des solutions quels que soient c et c' si $ab' - a'b$ et 26 sont premiers entre eux.

4. Expliquez pourquoi, si vous aviez en votre possession la fréquence d'apparition des bigrammes de la langue française, vous pourriez décrypter un texte codé par la méthode du chiffrement de Hill.
5. Qu'est-ce que la cryptographie? Faire une description succincte des techniques de cryptographie actuellement utilisées et de leurs domaines d'utilisation.

Sujet 8 Autour de la suite de Fibonacci

Les parties B et C sont indépendantes, l'une propose une exploration par l'analyse et l'autre par l'arithmétique.

Soit la suite (dite suite de Fibonacci) définie par :

$$\begin{cases} u_1 = 1, u_2 = 1 \\ u_n = u_{n-1} + u_{n-2} \quad \text{pour tout entier } n \geq 3. \end{cases}$$

- A.
1. Calculer les quinze premiers termes de cette suite.
 2. Démontrer que deux termes consécutifs de la suite (u_n) sont premiers entre eux.
 3. Démontrer que, pour tout entier $n \geq 2$,

$$u_n^2 - u_{n-1}u_{n+1} = (-1)^{n+1}. \quad (4)$$

Expliquer en quoi cette relation permet de retrouver le résultat de la question 2..

Pour $n \geq 2$, déterminer en fonction de n , des entiers α et β tels que : $\alpha u_n + \beta u_{n+1} = 1$.

- B.
1. Démontrer que, pour tout entier $n \geq 5$, $u_n \geq n$. En déduire la limite de la suite (u_n) . Utiliser ce résultat ainsi que le relation (4) pour donner un sens à l'affirmation suivante : «Pour de grandes valeurs de n , (u_n) se comporte presque comme une suite géométrique.»
 2. Pour tout entier $n \geq 2$, on pose $q_n = \frac{u_n}{u_{n-1}}$.

a) Démontrer les égalités :

$$q_{n+1} = q_n + \frac{(-1)^n}{u_n u_{n-1}} \quad \text{et} \quad q_n^2 = q_n + 1 + \frac{(-1)^{n+1}}{(u_{n-1})^2}.$$

b) Soit (a_n) et (b_n) les suites définies pour tout entier $n \geq 1$ par :

$$a_n = q_{2n} \quad \text{et} \quad b_n = q_{2n+1}.$$

Démontrer que les suites (a_n) et (b_n) sont adjacentes (on dit que deux suites a_n et b_n sont adjacentes si et seulement si (a_n) est croissante, (b_n) est décroissante et $\lim_{n \rightarrow +\infty} (b_n - a_n) = 0$).

c) En déduire que la suite (q_n) admet une limite qui est égale au nombre d'or : $\frac{1 + \sqrt{5}}{2}$.

- C.
1. Démontrer que, pour tout entiers n non nul et tout entier p , $p \geq 2$,

$$u_{n+p} = u_{p-1}u_n + u_{n+1}u_p. \quad (5)$$

2. Soit n et k des entiers naturels non nuls. Démontrer que u_n divise u_{kn} .
3. Soit n et p des entiers naturels non nuls. On pose $d = \text{PGCD}(n; p)$. Le but de cette question est de prouver que

$$\text{PGCD}(u_n; u_p) = u_d.$$

- a) Vérifier que l'égalité est vraie pour $n = 15$ et $p = 10$, puis pour $n = 15$ et $p = 12$.
- b) Démontrer que u_d divise $\text{PGCD}(u_n; u_p)$.
- c) Justifier qu'il existe deux entiers naturels a et b tels que

$$d = an - bp \quad \text{ou} \quad d = ap - bn.$$

- d) Démontrer que $\text{PGCD}(u_n; u_p)$ divise u_d .
- e) Conclure.

Sujet 9 Triplets Pythagoriciens

Partie A : géométrie. Une paramétrisation rationnelle du cercle unité.

On se place dans un repère orthonormé $(O; I, J)$ du plan. On note $I'(-1; 0)$. Soit \mathcal{C}_1 le cercle unité, d'équation $x^2 + y^2 = 1$. Pour un paramètre $t \in \mathbb{R}$, le point A_t est le point de coordonnées $A_t(0; t)$ et \mathcal{D}_t est la droite passant par I' et A_t .

1. a) Tracer, dans $(O; I, J)$, le cercle \mathcal{C}_1 et la droite \mathcal{D}_t pour $t = -1, 0, 1$ et 2 . Conjecturer l'ensemble des points d'intersection de \mathcal{D}_t avec \mathcal{C}_1 distincts de I' quand t varie dans \mathbb{R} . Remarque : on pourra réaliser cette figure avec GeoGebra et la rendre dynamique.
b) Déterminer l'équation réduite de \mathcal{D}_t .
c) Démontrer que, pour tout $t \in \mathbb{R}$, \mathcal{D}_t coupe \mathcal{C}_1 en un unique point M distinct de I' dont on donnera les coordonnées en fonction de t .

Le système d'équations

$$\begin{cases} x(t) = \frac{1-t^2}{1+t^2} \\ y(t) = \frac{2t}{1+t^2} \end{cases}, \quad t \in \mathbb{R} \quad (\text{S})$$

est appelé *système d'équations paramétriques* de \mathcal{C}_1 .

2. À l'aide de Geogebra (ou à l'aide d'une calculatrice permettant le tracé de courbes paramétriques), vérifier que l'ensemble des points $M(x(t); y(t))$ (où $x(t)$ et $y(t)$ sont donnés par le système (S) ci-dessus) est bien \mathcal{C}_1 privé de I' .
3. On dit qu'un point du plan est *rationnel* si ses coordonnées sont rationnelles. Démontrer que l'ensemble des points rationnels de \mathcal{C}_1 privé de I' est l'ensemble des points décrits par le système S où $t \in \mathbb{Q}$.

Partie B : arithmétique. Les triplets pythagoriciens, définition et classification.

On appelle triplet pythagorien tout triplet d'entiers $(a, b, c) \in \mathbb{Z}^3$ tel que $a^2 + b^2 = c^2$. La solution triviale $(0, 0, 0)$ est la seule solution telle que $c = 0$. On suppose désormais que $c \neq 0$.

1. Donner quelques exemples de triplets pythagoriciens.
2. Soit (a, b, c) un triplet pythagorien. Montrer qu'il existe une infinité de triplets pythagorien constructibles à partir de (a, b, c) .
3. Soit (a, b, c) un triplet pythagorien tel que a et b ne sont pas premiers entre eux. Montrer qu'on peut construire à partir de (a, b, c) un unique triplet pythagorien (a', b', c') où a', b' et c' sont premiers entre eux deux à deux. Exprimer (a, b, c) en fonction de (a', b', c') .

Un triplet pythagorien (a, b, c) tel que a, b et c sont premiers entre eux deux à deux sera appelé *primitif*. On vient de démontrer que tout triplet pythagorien peut être construit à partir d'un unique triplet pythagorien primitif. On peut donc se limiter à partir de maintenant à la recherche des triplets pythagorien primitifs.

Partie C : retour à la géométrie. Les triplets pythagoriciens dans le cercle unité.

Soit (a, b, c) un triplet pythagorien primitif. On remarque que

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

Donc le point $M\left(\frac{a}{c}; \frac{b}{c}\right)$ est sur \mathcal{C}_1 .

1. Démontrer qu'il existe un couple (m, n) d'entiers premiers entre eux tels que

$$\begin{cases} \frac{a}{c} = \frac{n^2 - m^2}{n^2 + m^2} \\ \frac{b}{c} = \frac{2mn}{n^2 + m^2} \end{cases}$$

2. Démontrer que a et b sont nécessairement de parité différente.

3. On suppose dans cette question que a est impair et que b est pair.

a) Démontrer qu'il existe un entier d positif tel que

$$\begin{cases} da = n^2 - m^2 \\ db = 2mn \\ dc = n^2 + m^2 \end{cases}$$

En déduire que $d \in \{1; 2\}$, puis que $d = 1$.

b) Conclure quand à une formule donnant (a, b, c) en fonction de m et n lorsque a est impair et b pair.

4. On suppose dans cette question que a est pair et que b est impair. Démontrer qu'il existe un couple (m, n) d'entiers premiers entre eux tel que

$$(a, b, c) = (2mn, n^2 - m^2, n^2 + m^2).$$

5. Réciproquement, les triplets construits à partir des formules obtenues aux questions 3 et 4 sont-ils pythagoriciens ?

6. Conclure en donnant l'ensemble des triplets pythagoricien sous forme explicite.

Sujet 10 Implémenter l'algorithme d'Euclide-Bézout

Soit a et b deux entiers naturels, $a > b > 0$ et g leur pgcd. On sait qu'il existe u et v entiers relatifs tels que $au + bv = g$.

Détermination de u et v sur un exemple numérique

Prenons $a = 47$ et $b = 35$.

Méthode : on met en œuvre l'algorithme d'Euclide et on calcule les restes successifs en fonction de a et de b . On sait que le dernier reste non nul est le pgcd. On développe les calculs de façon à faire apparaître à chaque étape une écriture de la forme $au + bv$.

$$47 = 35 \times 1 + 12 \quad \text{d'où } 12 = 47 - 35$$

$$35 = 12 \times 2 + 11 \quad \text{d'où } 11 = 35 - 2 \times 12 = 35 - 2 \times (47 - 35) = -2 \times 47 + 3 \times 35$$

$$12 = 11 \times 1 + 1 \quad \text{d'où } 1 = 12 - 11 \times 1 = 47 - 35 - (-2 \times 47 + 3 \times 35) = 3 \times 47 - 4 \times 35$$

$$11 = 11 \times 1 + 0$$

Généralisation

Dans l'algorithme d'Euclide, on sait qu'on peut noter r_i le reste obtenu à la i ème division euclidienne et écrire celle-ci sous la forme

$$r_i = r_{i+1}q_{i+1} + r_{i+2} \tag{6}$$

en convenant que $r_0 = a$ et $r_1 = b$. La situation peut se résumer ainsi :

$$\begin{array}{lll}
& r_0 = a; & r_1 = b \\
\text{division 1 :} & r_0 = r_1q_1 + r_2 & \text{soit } a = bq_1 + r_2 \\
\text{division 2 :} & r_1 = r_2q_2 + r_3 & \\
& \dots & \\
\text{division } i + 1 : & r_i = r_{i+1}q_{i+1} + r_{i+2} & \\
& \dots & \\
\text{division } n - 1 : & r_{n-2} = r_{n-1}q_{n-1} + r_n & \\
\text{division } n : & r_{n-1} = r_nq_n + r_{n+1} & \text{avec } r_{n+1} = 0
\end{array}$$

On voit que la relation (6) permet de calculer r_{i+2} en fonction des deux restes précédents r_{i+1} et r_i . Il en résulte que, si l'on a réussi à exprimer r_{i+1} et r_i à l'aide de a et b , on va pouvoir en déduire r_{i+2} en fonction de a et b . Supposons donc que l'on ait pu trouver u_i, v_i, u_{i+1} et v_{i+1} tels que :

$$\begin{cases} r_i = u_i a + v_i b \\ r_{i+1} = u_{i+1} a + v_{i+1} b \end{cases}$$

1. Démontrer, en utilisant (6), que r_{i+2} s'exprime alors en fonction de a et b sous la forme $r_{i+2} = u_{i+2}a + v_{i+2}b$ où

$$\begin{cases} u_{i+2} = u_i - u_{i+1}q_{i+1} \\ v_{i+2} = v_i - v_{i+1}q_{i+1} \end{cases}$$

2. Démontrer qu'on peut initialiser les relations précédentes avec $u_0 = 1, v_0 = 0, u_1 = 0$ et $v_1 = 1$ pour initialiser r_0 à a et r_1 à b .
3. D'après ce qui précède, le calcul des coefficients u_k, v_k et r_k est possible à l'aide des coefficients $u_{k-1}, v_{k-1}, r_{k-1}, u_{k-2}, v_{k-2}$ et r_{k-2} . D'un point de vue algorithmique, on peut remarquer qu'il n'est pas nécessaire de stocker tous les termes précédents pour passer du rang k au rang $k + 1$ du moment qu'on conserve, dans une variable de stockage, le terme de rang $k - 2$, avant qu'il ne soit écrasé. On note u, u_1, v, v_1, r, r_1 les variables $u_{k-2}, u_{k-1}, v_{k-2}, v_{k-1}, r_{k-2}$ et r_{k-1} . La variable tampon est notée t et q est le quotient de la division euclidienne de r_{k-2} par r_{k-1} . Une implémentation en pseudo-code de l'algorithme d'Euclide-Bézout qui tient compte de ce qui précède est :

Fonction EUCLIDE_BEZOUT(a, b)

▷ Renvoie le pgcd g de a et b et les coefficients u et v tels que $g = au + bv$. Méthode itérative. ◁

initialiser r, r_1, u, u_1, v et v_1 ,

tant que $r_1 \neq 0$ **faire**

$q \leftarrow$ quotient de la division entière de r par r_1

$t \leftarrow u$

$u \leftarrow u_1$

$u_1 \leftarrow t - q \times u_1$

$t \leftarrow v$

$v \leftarrow v_1$

$v_1 \leftarrow t - q \times v_1$

$t \leftarrow r$

$r \leftarrow r_1$

$r_1 \leftarrow t - q \times r_1$

renvoyer r, u, v

Implémenter l'algorithme précédent en Python. Le tester sur les couples suivants : $(a, b) = (33810, 4146)$ et $(a, b) = (15561, 3470)$.

4. Implémenter l'algorithme précédent sur une calculatrice (de marque casio ou ti) de façon à disposer d'un algorithme capable, deux nombres a et b étant saisis au clavier, de donner les nombres u , v et $\text{PGCD}(a; b)$ tels que $u \times a + v \times b = \text{PGCD}(a; b)$. Tester l'algorithme avec les couples donnés à la question précédente.

Sujet 11 *Implémenter un algorithme de test de primalité*

En utilisant le principe du crible d'Ératosthène, écrire un algorithme en Python, puis en langage de calculatrice (casio ou ti) permettant de déterminer si un nombre donné est premier.

Prolongement possible : écrire un algorithme réalisant la décomposition en facteurs premiers d'un entier donné.

Sujet 12 *Méthode de Descartes pour résoudre les équations algébriques du troisième et du quatrième degré*

En utilisant le paragraphe III.5 (p. 318-322) du livre «Mathématiques, vol. 1», de Alexandrov, Kolmogorov et Laurentiev (traduit par A. Cabannes), aux éditions du Bec de l'Aigle, publié en 2020, ISBN-13 : 978-2-9572391-2-2, faire une présentation de la méthode trouvée par Descartes pour résoudre les équations du troisième et du quatrième degré dans \mathbb{R} .

Sujet 13 *Le dernier théorème de Fermat*

Lire et faire un résumé du livre : «Le dernier théorème de Fermat», de Simon Singh, édité par Fayard, collection Pluriel, publié en 2011, ISBN-13 : 978-2818502037.

Sujet 14 *Histoire des codes secrets*

Lire et faire un résumé des chapitres 1 et 2 du livre : «Histoire des codes secrets», de Simon Singh, édité par Le livre de Poche, publié en 2001, ISBN-13 : 978-2070301874. Cette partie du livre présente les premiers codes qui ont été inventés et va jusqu'au chiffrement polyalphabétique de Vigenere.

Sujet 15 *Histoire des codes secrets*

Lire et faire un résumé des chapitres 3 et 4 du livre : «Histoire des codes secrets», de Simon Singh, édité par Le livre de Poche, publié en 2001, ISBN-13 : 978-2070301874. Ces chapitres traitent des machines de chiffrement, en particulier d'Enigma qui a été «cassée» par l'équipe de Bletchley Park, dont Alan Turing a fait partie.

N.B. : même si l'exposé ne doit porter que sur les chapitres 3 et 4 du livre de S. Singh, il sera utile d'avoir lu les deux premiers chapitres et de replacer dans leur contexte le contenu des chapitres 3 et 4.

Sujet 16 *Histoire des codes secrets*

Lire et faire un résumé du chapitre 5 du livre : «Histoire des codes secrets», de Simon Singh, édité par Le livre de Poche, publié en 2001, ISBN-13 : 978-2070301874. Cette partie traite des codes basés sur des langues, et aborde l'histoire du déchiffrement de certaines langues anciennes (dont le Linéaire B).

Sujet 17 *Histoire des codes secrets*

Lire et faire un résumé des chapitres 6 et 7 du livre : «Histoire des codes secrets», de Simon Singh, édité par Le livre de Poche, publié en 2001, ISBN-13 : 978-2070301874. Cette partie traite du cryptage RSA actuellement utilisé et du logiciel libre PGP qui offre plusieurs services de chiffrement utilisables dans les communications numériques.

Sujet 18 *La symphonie des nombres premiers*

Lire et faire un résumé du livre : «La symphonie des nombres premiers», de Marcus du Sautoy, édité par Points, publié en 2007, ISBN-13 : 978-2757804292.

Sujet 19 *Merveilleux nombres premiers*

Lire et faire un résumé d'un chapitre du livre : «Merveilleux nombres premiers», de Jean-Paul Delahaye, édité par Belin- Pour la science, publié en 2010, ISBN-10 : 2-84245-017-5.

Sujet 20 *Gödel, Escher, Bach.*

Lire et faire un résumé d'un chapitre du livre : «Gödel, Escher, Bach. Les brins d'une guirlande éternelle.», de Douglas Hofstadter, réédité par Dunod en 2021, ISBN : 978-2-10-082933-0.