DM — Systèmes et Droites

Partage de clé secrète de Shamir

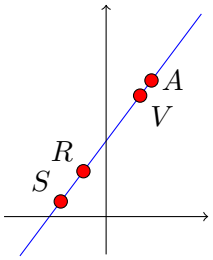
À rendre le 31 janvier

Question 1 (Interpolation polynômiale)**.**

(a) Soient deux points (3;15), (1;7). Trouver l'équation d'une droite passant par ces deux points. Existe-t-il d'autres droites passant aussi par ces points ?

(b) Soit le point (3;15). Trouver les équations d'au moins deux droites passant par ce points.

Question 2 (Application pratique)**.** Quatre amis Alex, Sara, Volodia et Robin veulent stocker leur confiseries chez l'un d'entre eux. Mais leur petit frère est au courant et voudrait se servir. Pour s'en protéger, ils stockent leur marchandise dans une boîte verrouillée avec un cadenas à code à deux chiffres. Ils se font confiance, mais le petit frère est malin, et ils se disent qu'il pourrait bien obtenir le code de l'un d'entre eux par fourberie. Pour se protéger de cette situation, ils se partagent le secret de la manière suivante.



Ils décident d'un code à deux chiffres ab pour le cadenas. Ils considèrent ensuite la droite d'équation $y = ax + b$, et chacun se voit attribuer un point sur cette droite, connu de lui seul.

(a) Un jour, Alex et Sara veulent manger des bonbons présents dans la boîte. Retrouver le code du cadenas à partir de leurs points respectifs $A(3;15)$, $S(1;7)$.

(b) Le petit frère trouve le papier sur lequel Alex avait écrit son point, par peur de l'oublier. Montrer qu'à partir de ce seul point $A(3;15)$ le petit frère ne peut pas retrouver l'équation de la droite originale, et donc le code de la boîte.

Question 3 (Cassage de code)**.** Nos quatre compères n'ont pas inventé cette méthode : ils se sont inspirés du *partage de clef secrète de Shamir*, présentée par Shamir en 1979. C'est une méthode sûre et robuste, réellement utilisée en pratique. Malheureusement, la simplification qu'ils en ont faite pour pouvoir l'utiliser facilement a introduit (au moins) une grosse faille.

Le petit frère raconte un jour son histoire à ses cousins Alan et Émilie. Intéressés par les bonbons, ils vont utiliser chacun une méthode différente pour trouver le code de la boîte et voler le butin, à partir de l'information à priori insuffisante $A(3;15)$.

Les questions (a) et (b) sont indépendantes

(a) Émilie va essayer de trouver le code par un raisonnement mathématique. Elle recherche une droite d'équation $y = ax + b$ passant par le point d'Alex.

(i) Vérifier que $b = 15 - 3a$.

(ii) Quelles sont les valeurs possibles de a ?

(iii) Faire une table de toutes les valeurs possibles de a, et des valeurs de b correspondantes.

(iv) En déduire les codes possibles. Émilie va-t-elle réussir à ouvrir le cadenas ?

(b) Alan, lui, est passionné d'informatique. Il se dit que pour trouver le code, il lui suffit d'énumérer toutes les équations de droites possibles, et de ne conserver que ceux qui passent par le point d'Alex.

(i) Alan a commencé l'algorithme suivant.

```
Pour a allant de 0 jusqu'a 10
Faire
  Pour b allant de 0 jusqu'a 10
  Faire
    COMPLETER ICI :
    VERIFIEZ SI y=ax-b EST LA
    DROITE RECHERCHEE
  FinPour
FinPour
```

Pour le moment, deux boucles permettent d'énumérer tous les codes possibles. Il ne reste plus qu'à compléter l'algorithme pour vérifier si un code donné est possible. Complétez cet algorithme.

(ii) Écrire le programme correspondant dans le langage de votre choix (sur calculatrice par exemple), et l'exécuter.

(iii) Quels sont les résultats ? Alan va-t-il arriver à ses fins ?

(c) Comparer et commenter les méthodes de Émilie et Alan.