DM — Systèmes et Droites

Partage de clé secrète de Shamir

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 ?*

On appelle A et B ces deux points. Le coefficient directeur de la droite est $\frac{y_B - y_A}{x_B - x_A} = \frac{7-15}{1-3} = \frac{-8}{-2} = 4$. Notre équation est donc de la forme $y = 4x + b$. Puisque A appartient à la droite, on a : $y_A = 4x_A + b$, c'est-à-dire $15 = 4 \times 3 + b$, d'où on déduit que $b = 3$. L'équation de la droite est donc $y = 4x + 3$.

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

Nous avons déjà trouvé la droite d'équation $y = 4x + 3$. On peut également cite $y = 5x$, $y = 15$, $x = 3$, etc.

Question 2 (Application pratique)**.** (a) *Retrouver le code du cadenas à partir de leurs points respectifs* $A(3;15)$, $S(1;7)$.

Cela revient à trouver l'équation de la droite passant par ces deux points. Cela a déjà été résolu dans la première question, et nous avons trouvé $y = 4x + 3$. Le code est donc 43.

(b) *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.*

Nous avons montré dans la première question que plusieurs droites (une infinité en fait) passaient par ce point. Le petit frère a donc une infinité de possibilités, et il ne peut donc pas retrouver le code.

Question 3 (Cassage de code)**.** (a) (i) *Vérifier que* $b = 15 - 3a$.

Puisque la droite passe par le point A, on sait que $y_A = ax_A + b$, c'est-à-dire $15 = 3a + b$. Donc, en isolant b, on trouve : $b = 15 - 3a$.

(ii) *Quelles sont les valeurs possibles de a ?*

a étant un chiffre, c'est un nombre entier compris entre 0 et 9.

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

a	0	1	2	3	4	5	6	7	8	9
b	15	12	9	6	3	0	-3	-6	-9	-12

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

Puisque b est également un chiffre, ses valeurs possibles sont aussi entre 0 et 9. Donc les couples ab qui peuvent correspondre sont 29, 36, 43 et 50.

Puisqu'Émilie n'a que quatre possibilités, elle peut toutes les essayer et trouver le code.

(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) L'algorithme complet est le suivant.

```
Pour a allant de 0 jusqu'a 9
Faire
  Pour b allant de 0 jusqu'a 9
  Faire
    Si 3×a+b=15
    Alors
      Afficher a, b
    FinSi
  FinPour
FinPour
```

Les boucles permettent d'énumérer tous les codes du cadenas. Ensuite, il suffit de vérifier si le code est possible, et de l'afficher le cas échéant.

(ii) Par exemple en Python :

```
for a in range(10):
  for b in range(10):
    if 3*a+b==15:
      print a, b
```

(iii) Le programme affiche comme codes possibles 29, 36, 43 et 50. Alan va pouvoir essayer les quatre possibilités et ouvrir le cadenas.

(c) Les deux méthodes utilisent des approchent différentes pour résoudre le même problème. La méthode d'Émilie est plus fine, dans le sens où elle trouve, par le calcul, toutes les solutions possibles. La technique d'Alan est une technique *par force brute* qui consiste à essayer toutes les possibilités ; c'est moins fin, mais cela fonctionne aussi.