03/10/14 *DM n° 1*

Trinômes
Cryptographie

1eS3

Toutes les coordonnées sont données dans un repère orthonormé.

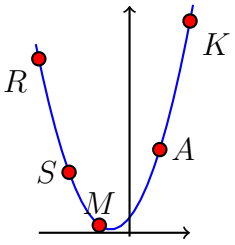
Question 1 (Interpolation polynômiale)**.**

(a) *(Optionnel)* Soient trois points $(-3;23)$, $(2;28)$, $(-1;1)$. Montrer que le polynôme $f : x \mapsto 4x^2 + 5x + 2$ est l'unique polynôme du second degré passant par ces trois points.

(b) Soient deux points $(2;28)$ et $(-1;1)$. Trouver au moins deux polynômes du second degré dont la représentation graphique passe par ces points.

Bilan On admet la propriété suivante : Par deux points d'abscisses différentes passe une infinité de polynômes du seconde degré ; par trois points d'abscisses différentes passe un et un seul polynôme du second degré.

Question 2 (Application pratique)**.** Cinq bandits Robin, Samah, Margot, Alex et Killian ont caché leur butin dans un coffre fermé par un code à trois chiffres. Ils se font confiance, mais il se disent que si l'un d'entre eux est capturé par la police, il finira, sous la pression, par donner le code aux autorités. Pour se protéger de cette situation, ils se partagent le secret de la manière suivante.



Ils décident d'un code à trois chiffres abc pour le coffre. Ils considèrent ensuite le polynôme ax^2+bx+c, et chacun se voit attribuer un point sur la courbe de ce polynôme, connu de lui seul.

(a) Pour préparer un nouveau larcin, Robin, Killian et Margot veulent ouvrir le coffre y prendre du matériel. Retrouver le code du coffre à partir de leurs points respectifs $R(-3;23)$, $K(2;28)$, $M(-1;1)$.

(b) Leur larcin ne s'est pas passé comme prévu, et Killian et Margot ont été pris. Ils finissent par donner leurs points $K(2;28)$ et $M(-1;1)$ à la police. Montrer qu'à partir de ces seules informations, la police ne peut pas retrouver le trinôme original, et donc le code du casier.

Question 3 (Cassage de code)**.** Nos cinq 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.

Rayane et Véronique, policiers peu scrupuleux, ont pu obtenir les points de Killian et Margot $K(2;28)$ et $M(-1;1)$ et vont, chacun de leur côté, essayer de déterminer le code du coffre, pour voler son contenu.

(a) *(Optionnel)* Rayane est passionné d'informatique. Il se dit que pour trouver le code, il lui suffit d'énumérer tous les polynômes possibles, et de ne conserver que ceux qui passent par les points de Killian et Margot.

(i) Compléter l'algorithme suivant, mis en place par Rayane.

```
for a from 0 to 9
  for b from 0 to 9
    for c from 0 to 9
      Si ···
      Alors
        Afficher "Une solution possible est" ...
      FinSi
    FinPour
  FinPour
FinPour
```

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

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

(b) Véronique, quant à elle, va essayer de trouver le code du casier par un raisonnement mathématique. Elle recherche un polynôme $P(x) = ax^2 + bx + c$ passant par les points de Killian et Margot.

(i) Vérifier qu'à partir des points de Killian et Margot, Véronique peut déduire que $a = 9-b$, et $c = 2b - 8$.

(ii) Quelles sont les valeurs possibles de b ?

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

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

(c) Comparer et commenter les méthodes de Véronique et Rayane.

Question 4 (Pour aller plus loin (optionnel))**.** Voici quelques pistes pour réfléchir un peu plus à cette méthode.

(a) Une des modifications apportée à la méthode originale est que dans notre cas, le secret est l'ensemble des paramètres du polynôme (a, b et c), alors que dans la méthode originale, le secret n'est que l'ordonnée à l'origine c (les paramètres a et b étant choisis au hasard). Véronique et Rayane peuvent-ils casser ce nouveau code en utilisant des méthodes similaires ?

(b) La méthode présentée ici ne permet de chiffrer que trois nombres. La modifier pour pouvoir chiffrer une information arbitraire (par exemple, le nombre 1729, le texte `Hello world!`, un fichier, etc.).

(c) Avec la méthode étudiée dans la question 2, il faut au moins trois personnes pour retrouver le secret. Comment modifier cette méthode pour que deux personnes suffisent ? Et quatre personnes ? Et n personnes ?

(d) Mettre en pratique cette méthode de chiffrement dans deux algorithmes permettant respectivement de chiffrer un secret en le partageant entre plusieurs personnes, et de déchiffrer ce secret à partir des informations des différentes personnes.

(e) Se renseigner sur le partage de clef secrète de Shamir (commencer par Wikipédia, par exemple).

(f) Essayer un programme mettant en œuvre cet algorithme de Shamir :

`http://point-at-infinity.org/ssss/demo.html`