04/04/2016
DM 6

Fonctions affines

2^{de}10

Exercice 1 (Tableau de signe)**.**

Tracer la courbe d'une fonction (pas nécessairement affine) qui puisse correspondre au tableau de signes suivant.

x	-2		3		5		10		12
$f(x)$		$-$	0	$+$	0	$-$	0	$+$	

Exercice 2 (Partage de clef secrète)**.**

1. *Interpolation polynomiale*
   (a) Déterminer l'équation d'une fonction affine f telle que $f(5) = 147$ et $f(18) = 56$. Existe-t-il d'autres fonctions affines passant aussi par ces points ?
   (b) Déterminer les équations de deux fonctions affines différentes telles que $f(5) = 147$.
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 trois 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 utilisent la méthode appelée *partage de clef secrète de Shamir*, présentée par Shamir en 1979. C'est une méthode sûre et robuste, réellement utilisée en pratique.

Ils décident d'un code à trois chiffres b pour le cadenas, et choisissent un nombre a au hasard. Ils considèrent ensuite la fonction $f(x) = ax + b$, et chacun se voit attribuer les coordonnées d'un point sur cette droite, connu de lui seul. Le code est donc l'ordonnée à l'origine de l'équation de la fonction affine correspondante.

(a) Un jour, Alex (qui sait que $f(5) = 147$) et Sara (qui sait que $f(18) = 56$) veulent manger des bonbons présents dans la boîte. Déterminer l'équation de la fonction affine qui vérifie leurs deux informations, et en déduire le code du cadenas.

(b) Le petit frère trouve le papier sur lequel Alex avait écrit son information, par peur de l'oublier. Donner deux fonctions f possibles vérifiant l'information $f(5) = 147$, et les codes correspondants. À partir de cette information, le petit frère pourra-t-il ouvrir la boîte ?

(c) *(Optionnel)* Comment adapter cette méthode pour que trois personnes soient nécessaires pour trouver le code et ouvrir le coffre ?