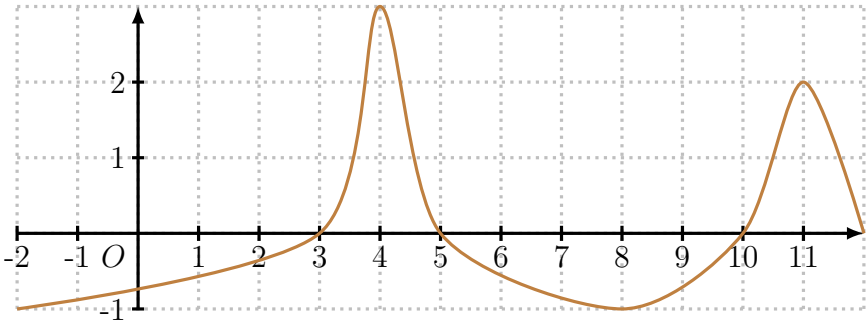
Exercice 1 (Tableau de signe)**.**

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 ?* On cherche une fonction de la forme $f(x) = ax + b$. Le coefficient directeur a est donné par la formule $a = \frac{f(5)-f(18)}{5-18} = \frac{147-56}{5-18} = \frac{91}{-13} = -7$. Donc f est de la forme $f(x) = -7x + b$.

   Puisque $f(5) = 147$, alors $-7 \times 5 + b = 147$, donc $b = 147 - (-7 \times 5) = 182$.

   Donc la fonction f a pour expression $f(x) = -7x + 182$.

   Il n'existe qu'une seule telle fonction. On peut justifier cela de différentes manières. Par exemple, la résolution que nous

venons de mener n'a donné qu'une solution pour a et b, donc cela ne correspond qu'à une fonction. Nous pouvons aussi dire que chaque information $f(5) = 147$ et $f(18) = 56$ correspond à un point du plan, et une fonction affine à une droite. Puisqu'il n'existe qu'une seule droite passant par deux points distincts, il n'existe qu'une fonction affine vérifiant ces conditions.

(b) *Déterminer les équations de deux fonctions affines différentes telles que* $f(5) = 147$. Une première expression est celle déterminée à la question précédente : $f(x) = -7x + 182$. Il y a plusieurs manières de calculer une seconde fonction.

Première méthode : Choix d'un autre point On choisit un autre point au hasard, par exemple $f(0) = 7$, et on détermine l'équation d'une fonction affine $f : x \mapsto ax + b$ passant par ces deux points. Le coefficient directeur est $\frac{f(5)-f(0)}{5-0} = \frac{147-7}{5-0} = \frac{140}{5} = 28$. Donc la fonction est de la forme $f(x) = 28x + b$. Puisque $f(0) = 7$, alors $7 = 28 \times 0 + b = b$. Donc la fonction f a pour expression $f(x) = 7x$. Il faut encore vérifier que cette fonction est bien différente de la précédente (au cas où, par malchance, nous ayons choisi un point appartenant à la droite de la fonction précédente), ce qui est bien le cas.

Deuxième méthode : Choix du coefficient directeur Nous savons que $f(5) = 147$. Nous choisissant arbitrairement le coefficient directeur de notre fonction f, par exemple 2. Donc la fonction est de la forme $f(x) = 2x+b$. Or $f(5) = 147$, donc $f(5) = 2 \times 5 + b = 147$, et $b = 147 - 2 \times 5 = 137$. Donc l'expression de la fonction est $f(x) = 2x + 137$.

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.* Nous cherchons l'expression d'une fonction telle que $f(5) = 147$ et $f(18) = 56$. Cette expression a été calculée à la question précédente, et c'est $f(x) = -7x + 182$. L'ordonnée à l'origine de cette fonction est 182, donc le code du cadenas est 182.

(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 ?* Nous avons calculé à la question précédente plusieurs fonctions vérifiant $f(5) = 147$. Par exemple $f_1(x) = -7x + 182$, $f_2(x) = 7x$, $f_3(x) = 2x + 137$. L'ordonnée à l'origine de ces fonctions est respectivement 182, 0 et 137. Donc les codes correspondants sont 182, 000 et 137. Il existe une infinité de telles fonctions, et les ordonnées à l'origine peuvent être n'importe lequel des nombres entre 0 et 999. Donc l'information $f(5) = 147$ n'apporte aucune information pour le code du cadenas : le petit frère ne pourra pas ouvrir la boîte.

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

ouvrir le coffre, il faut prendre comme fonction non pas une fonction affine mais une fonction trinôme du second degré de la forme $ax^2 + bx + c$. Le principe est le même (chaque personne se voit donné un antécédent et une image), et le code du cadenas est c.

Avec un trinôme, trois couples antécédent/image sont nécessaires pour trouver l'équation d'origine, donc deux personnes ne pourront pas ouvrir le coffre, mais trois personnes pourront.