

CBMaths.fr
<https://cbmaths.fr>

CAPES de Mathématiques session 2020— Épreuve de mise en situation professionnelle

LEÇON n° 28
Applications des mathématiques à d'autres disciplines

Clément BOULONNE

Propositions de plan et de contenu

Dernière mise à jour : 22 août 2020

Préambule

Niveau de la leçon

Lycée

Prérequis

Fonctions, équations différentielles, fonctions exponentielles, logarithmes, congruences, graphes

Références

- S. HANNETON, *Vitesse (d'un objet dans l'espace)*. URL : www.hanneton.org/temp/vitesse.pdf.
- J. GEADOT, *Chapitre 5 : Le travail d'une force*. Classe de 1ère S. URL : <http://www.physagreg.fr/accueil.php>.
- Contributeurs de WIKIPÉDIA, *Principe de Hardy-Weinberg*. Wikipédia.
- G. COSTANTINI, *Exercices sur les équations différentielles*. Terminale S. URL : <http://bacamaths.net>.
- A. SAMIER & C. RASSON, *Leçon sur les suites*. Leçon de Math S2, Master 1 Ens. Math, 2010-2011.
- J.-D. ASTIER & al., *Mathématiques, BEP Tertiaire*. Nathan Technique.
- J.-P. QUELEN, *Petit théorème de Fermat et codage RSA*. 15 janvier 2011.

Plan de la leçon

1 Démographie : fonction logistique	2
2 Médecine - SVT	3
3 Cryptographie : système RSA	6
4 Physique et équations différentielles	8
5 Économie d'entreprise	8

1 Démographie : fonction logistique

La fonction logistique est une famille de fonctions découverte par Verhulst. C'est une fonction de la forme :

$$t \mapsto f(t) = \frac{k}{1 + ae^{-bt}}$$

avec

- t le temps ;
- $f(t)$ le nombre de personnes (bactéries, cellules) présentes au temps t ;
- $b > 0$, b dépend du taux de natalité et du taux de mortalité ($b = \alpha - \omega$, α naissance, ω mort)
- $k > 0$ dépend du type de population et de la contrainte liée au territoire (ou l'environnement) ;
- a provient de l'équation différentielle ($a > 0$) car en effet, ces fonctions sont des solutions à l'équation différentielle suivante :

$$\begin{cases} y' = by \left(1 - \frac{y}{k}\right) \\ y(0) = y_0 \end{cases} .$$

Cette modélisation du développement d'une population est une amélioration de la modélisation faite par Malthus qui prenait comme équation différentielle : $y' = by$.

Cependant, cette modélisation n'est valable que si on considère que le territoire permet un développement infini (suivant la fonction exponentielle) de la population.

C'est pour cela que l'on ajoute la constante k que l'on peut aussi voir comme étant le nombre maximal de personnes qui peuvent vivre sur le territoire.

Résolution de l'équation différentielle. \diamond On veut résoudre l'équation différentielle suivante :

$$\begin{cases} y' = by \left(1 - \frac{y}{k}\right) & (E) \\ y(0) = y_0 \end{cases} .$$

On pose $z = \frac{1}{y}$ (l'on peut car y représente un nombre de personnes qui ne peut jamais s'annuler).

$$(E) \Leftrightarrow -\frac{z'}{z^2} = \frac{b}{z} \left(1 - \frac{1}{kz}\right) \Leftrightarrow z' = b \left(\frac{1}{k} - z\right) \quad (E')$$

Les solutions de (E') sont : $z : t \mapsto \lambda e^{-bt} + \frac{1}{k}$, $\lambda \in \mathbb{R}$ donc les solutions de (E) sont

$$y : t \mapsto \frac{1}{\lambda e^{-bt} + \frac{1}{k}} = \frac{k}{\lambda e^{-bt} + 1} .$$

On pose $a = \frac{\lambda}{k}$ donc $y(t) = \frac{k}{ae^{-bt} + 1}$. De plus, $y(0) = y_0$ donc $y_0 = \frac{k}{a+1} \Rightarrow a = \frac{k}{y_0} - 1$.

♪ Remarque 28.1.

$a > 0$ car $\frac{k}{y_0} > 1$ du fait que :

$$\begin{cases} k := \text{population maximale} \\ y_0 := \text{population initiale} \end{cases}$$

□

2 Médecine - SVT

2.1 Fonction de Gompertz

Cette fonction modélise la croissance des cellules d'une tumeur. Elle de type :

$$t \mapsto x(t) = A \exp(k \exp(-at))$$

avec :

- x : biomasse
- t : temps
- A : taille maximale de la tumeur (10^{11})
- a : taux de croissance ($0,003 \text{ j}^{-1}$)
- $k = \ln\left(\frac{x_0}{A}\right)$.

Cette fonction est la solution à l'équation différentielle suivante :

$$\begin{cases} x' = ax \ln\left(\frac{A}{x}\right) \\ x(0) = x_0 \end{cases}$$

Résolution de l'équation différentielle. \diamond On veut résoudre l'équation différentielle suivante :

$$\begin{cases} x' = ax \ln\left(\frac{A}{x}\right) & (E) \\ x(0) = x_0 \end{cases} .$$

Pour cela, on pose $y = \ln x$.

$$x' = ax \ln\left(\frac{A}{x}\right) \Leftrightarrow \frac{x'}{x} = A (\ln A - \ln x) \Leftrightarrow y' = a (\ln A - y) \quad (E')$$

Les solutions de (E') sont :

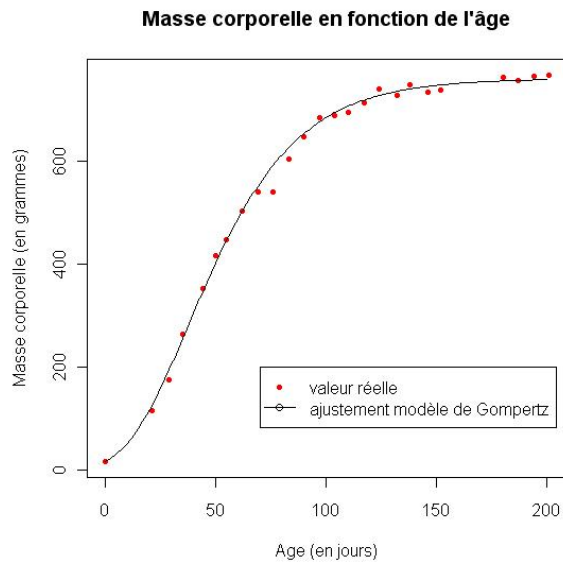
$$y: t \mapsto \lambda e^{-at} + \ln A, \quad \lambda \in \mathbb{R}$$

Les solution de (E) sont :

$$x: t \mapsto \exp(\lambda e^{-at} + \ln A) = A \exp(\lambda \exp(-at)).$$

De plus, $x(0) = x_0$ donc $x_0 = Ae^\lambda \Rightarrow \lambda = \ln\left(\frac{x_0}{A}\right)$.

□



2.2 Phénotype-génotype et probabilités

On a un gène avec 2 allèles : A et a . A est prédominant sur a . La transmission d'un allèle du parent à l'enfant est aléatoire.

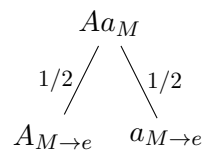
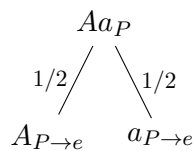
1. Déterminer la loi du génotype d'un enfant lorsque les deux parents ont pour génotype Aa .
2. On se place dans une population où les proportions des génotypes AA , Aa et aa sont respectivement p , q et r .
 - a) Sachant qu'un individu a le phénotype A , déterminer la loi de son génotype.
 - b) Même question avec un individu du phénotype aa .
 - c) Un enfant a 2 parents ayant le phénotype A , déterminer la loi de son phénotype.
 - d) Un enfant ayant 2 parents avec les phénotypes A et a , déterminer la loi de son phénotype.
 - e) Déterminer la loi du phénotype d'un enfant choisi au hasard.

Solution. \diamond

1. On note :

- AA_P : « le père a pour phénotype AA »
- AA_M : « la mère a pour phénotype AA »
- $A_{P \rightarrow e}$: « le père donne A à son enfant »
- AA_e : « l'enfant a pour génotype AA ».

Les dons des allèles sont indépendants.



$$P(AA_e) = P(A_{P \rightarrow e} \cap A_{M \rightarrow e}) = P(A_{P \rightarrow e}) \times P(A_{M \rightarrow e}) = \frac{1}{4}$$

$$P(aa_e) = P(a_{P \rightarrow e} \cap a_{M \rightarrow e}) = \frac{1}{4}$$

$$P(Aa_e) = P((A_{P \rightarrow e} \cap a_{M \rightarrow e}) \cup (A_{M \rightarrow e} \cap a_{P \rightarrow e})) = P(A_{P \rightarrow e} \cap a_{M \rightarrow e}) + P(A_{M \rightarrow e} \cap a_{P \rightarrow e}) = \frac{1}{2}$$

2. Pour un individu quelconque :

géno	AA	Aa	aa
P	1/4	1/2	1/4

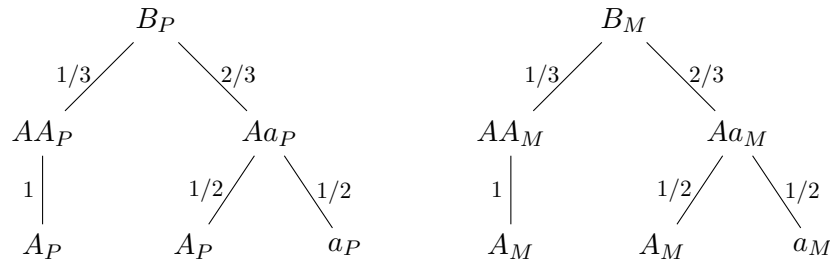
a) On note B : « individu du phénotype A » et b : « individu du phénotype a ».

$$P(B) = P(AA \cup Aa) = \frac{3}{4} \quad \text{et} \quad P(b) = P(aa) = \frac{1}{4}$$

$$P_B(AA) = \frac{P(AA \cap B)}{P(B)} = \frac{1/4}{3/4} = \frac{1}{3}; \quad P_B(aa) = 0; \quad P_B(Aa) = \frac{2}{3}$$

b) $P_B(AA) = 0; P_B(Aa) = 0; P_b(aa) = 1$.

c) On note B_P : « le père est du phénotype A ».



Ici :

$$P(A_P) = \frac{2}{3} = P(A_M)$$

$$P(a_P) = \frac{1}{3} = P(a_M)$$

$$P(b_e) = P(a_P \cap a_M) = \frac{1}{9}; \quad p(B_e) = \frac{1}{9}$$

d)



Si on a B_P et b_M :

$$P(b_e) = P(a_P \cap a_M) = \frac{1}{3} \times 1 = \frac{1}{3}$$

Si on a b_P et B_M , on a :

$$P(b_e) = P(a_P \cap a_m) = 1 \times \frac{1}{3} = \frac{1}{3}$$

e) Pour cette question, on balaye les 6 cas possibles de génotypes :

$$(AA_P, AA_M), (Aa_P, AA_M), (aa_P, AA_M), (aa_P, Aa_M), (Aa_P, Aa_M), (aa_M, aa_P).$$

On peut construire l'arbre de probabilités (long à faire!).

□

3 Cryptographie : système RSA

Le cryptage RSA (du nom des inventeurs, Ronald Rivest, Adi Shamir et Leonard Adleman) est intéressant car la clé de cryptage est publique et il n'a donc pas de risques liés à l'envoi de la clé et au procédé de codage des données. Bob, comme tout le monde, peut crypter et envoyer un message. Par contre, seul la destinataire, Alice, qui connaît la clé privée correspondante pourra reconstituer le message initial.

Alice, la destinataire rend publique deux nombres n et c où n est le produit de deux grands nombres premiers p et q qu'elle est seule à connaître, où c est un entier premier avec le produit $(p-1)(q-1)$ compris entre 2 et $(p-1)(q-1)$.

Pour coder le message « Bonjour », par exemple, on commence par remplacer les lettres par leurs positions dans l'ordre alphabétique, ce qui donne

02 15 14 10 15 21 18.

Si on utilise $n = 10573 = 97 \times 109$, on peut regrouper les chiffres par 4 sans risquer de dépasser n . Ce qui donne 0215 1410 1521 0018. Pour chaque nombre a de la série, on détermine alors b , reste de la division de a^c par n . On obtient alors dans ce cas avec $c = 5$ la série :

9131 7391 0690 7574.

C'est cette série de nombres qu'envoie Bob à Alice.

Alice qui connaît les deux facteurs premiers de n (ici $p = 97$ et $q = 109$) détermine alors facilement le nombre entier d vérifiant $1 < d < (p-1)(q-1)$ et tel que

$$cd \equiv 1 \pmod{(p-1)(q-1)}.$$

Ici $d = 6221$.

Alice peut alors retrouver la série initiale de nombres car, pour chaque entier b de cette série, on démontre que b^d est congru à a modulo n .

L'intérêt pour Alice est bien sûr d'avoir un nombre n produit de deux nombres premiers très grands de façon à ce que les calculateurs même les plus rapides ne puissent pas trouver en un temps suffisamment court les deux facteurs premiers nécessaires pour calculer d .

On note d'autre part que c et d jouent le même rôle et sont interchangeables. Ainsi Alice peut décider de coder elle-même un message en utilisant sa clé privée $d = 6621$. Bob décryptera alors aisément ce message avec la clé publique c . Le message envoyé à Bob constitue en fait une signature du message d'Alice. En effet, si Bob réussit à décrypter sans problème le message à l'aide de la clé c , c'est que ce message a été codé avec la clé privée d connue d'Alice seule et cela suffit pour en garantir l'authenticité.

On donne quelques propriétés permettant de justifier la robustesse de la méthode RSA.

Propriété 28.2.

Soient p et q deux nombres premiers. Si c , tel que $1 < c < (p-1)(q-1)$, est premier avec le produit $(p-1)(q-1)$ alors il existe un unique d tel que $1 < d < (p-1)(q-1)$ et vérifiant

$$cd \equiv 1 \pmod{(p-1)(q-1)}$$

Démonstration de la propriété 28.2. \diamond Si c et $(p-1)(q-1)$ sont premiers entre eux, il existe, d'après le théorème de Bézout, deux entiers relatifs u_0 et v_0 tels que $u_0c + v_0(p-1)(q-1) = 1$. Par suite (u, v) est solution de

$$uc + v(p-1)(q-1) = 1$$

si et seulement si il existe un entier relatif k tel que

$$u = u_0 - k(p-1)(q-1) \quad \text{et} \quad v = v_0 + kc.$$

Soit donc k tel que u soit le plus petit des entiers positifs. Dans ces conditions

$$uc = 1 - v(p-1)(q-1) \equiv 1 \pmod{(p-1)(q-1)}$$

et le nombre d recherché est par conséquent égal à u .

Il est unique car s'il en existait un autre, d' , alors on aurait

$$c(d - d') \equiv 0 \pmod{(p-1)(q-1)}.$$

Comme c est premier avec $(p-1)(q-1)$, alors, d'après le théorème de Gauss,

$$d - d' \equiv 0 \pmod{(p-1)(q-1)}.$$

Mais comme on a $1 < d < (p-1)(q-1)$ et $1 < d' < (p-1)(q-1)$ et bien, on peut avoir que $d = d'$. \square

Propriété 28.3.

Dans les conditions précédentes, si p et q sont différents et si $b \equiv a^c \pmod{pq}$ alors $b^d \equiv a \pmod{pq}$.

Démonstration de la propriété 28.3. \diamond Si $b \equiv a^c \pmod{pq}$ alors $b^d \equiv a^{cd} \pmod{pq}$ et $cd \equiv 1 \pmod{(p-1)(q-1)}$. Il existe donc un entier $k \geq 0$ tel que $cd = 1 + k(p-1)(q-1)$. On obtient donc

$$a^{cd} = a \left((a^{p-1})^{q-1} \right)^k.$$

Si a est divisible par p alors de façon évidente, $a^{cd} \equiv a \equiv 0 \pmod{p}$, sinon, d'après le petit théorème de Fermat, $a^{p-1} \equiv 1 \pmod{p}$ d'où $a^{cd} \equiv a \pmod{p}$. De même $a^{cd} \equiv a \pmod{q}$. Il existe donc deux entiers k et k' tels que $a^{cd} = a + kp$ et $a^{cd} = a + k'q$. Ainsi $kp = k'q$, entier qui se trouve donc être multiple de pq puisque p et q sont des nombres premiers différents. On obtient donc dans ces conditions $a^{cd} \equiv a \pmod{pq}$. \square

4 Physique et équations différentielles

4.1 Désintégration des noyaux radioactifs

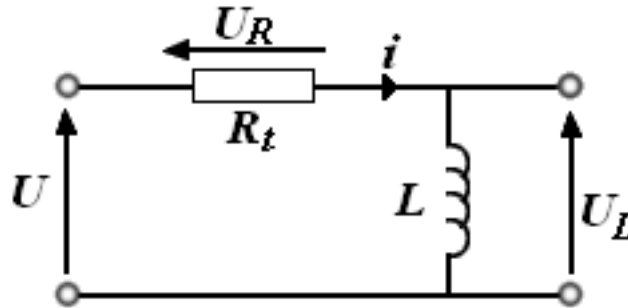
Soit $N(t)$ le nombre de noyaux radioactifs dans le corps au temps t . On note λ la constante radioactive (t^{-1}), $t_{1/2}$ le temps tel que $N(t_{1/2}) = \frac{N_0}{2}$. Il existe un tableau donnant les temps de demi-vie ($t_{1/2}$) de tous les noyaux radioactifs. De plus $t_{1/2}$ et λ sont liés par $\lambda = \frac{\ln 2}{t_{1/2}}$. N vérifie l'équation différentielle :

$$\begin{cases} N' = -\lambda N \\ N(0) = N_0 \end{cases}$$

donc $N(t) = N_0 e^{-\lambda t}$.

Application : datation au carbone 14 : $t_{1/2} = 5730$ ans.

4.2 Circuit RL



L'équation différentielle qui régit le circuit est la suivante :

$$U = L \frac{di}{dt} + R_t \cdot i$$

avec :

- U la tension aux bornes du montage, en V ;
- i l'intensité du courant électrique en A ;
- L l'inductance de la bobine en H ;
- R_t la résistance totale du circuit en Ω .

5 Économie d'entreprise

5.1 Théorie des graphes

Une entreprise doit respecter pour les mois de mai, juin et juillet, une commande de 2 chalets par mois.

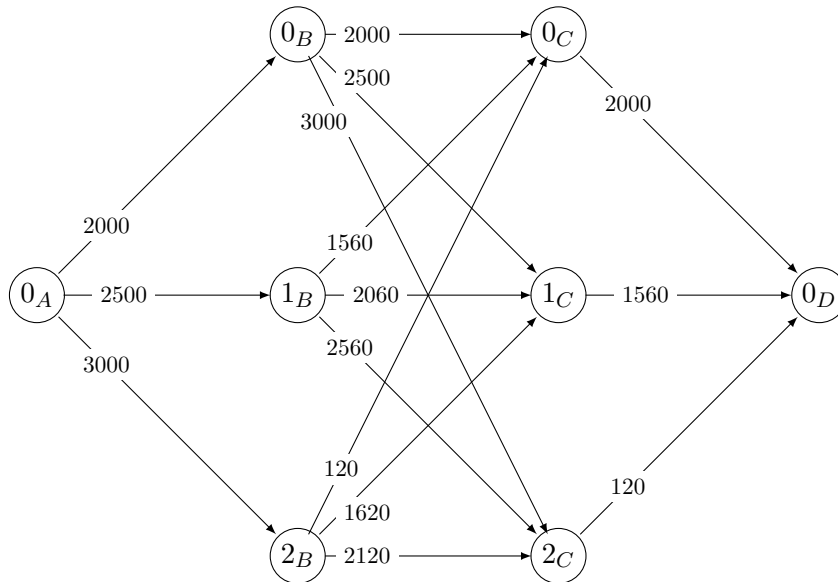
L'entreprise peut stocker au maximum 2 chalets. Le stock coûte 60 € par chalet par mois.

L'entreprise peut construire un maximum de 4 chalets par mois. Le premier chalet coûte 1500 € pour sa construction mais les chalets suivants que l'on construit dans le même mois ne coûtent que 500 € par chalet.

À la fin du mois de juillet, l'entreprise ne doit plus avoir de chalet en stock.

Comment faire pour minimiser les coûts ?

On utilise un graphe pondéré orienté pour visualiser la situation.
 Les sommets représentent le nombre de chalets mis en stock.
 Les indices A, B, C et D représentent « début de mai », « fin de mai », « fin de juin » et « fin de juillet ».
 On pondère avec les coûts entre 2 mois (en comptant le stock sur le mois suivant).



On cherche la chaîne la plus courte, on utilise donc l'algorithme de Dijkstra pour la trouver :

0_A	0_B	1_B	2_B	0_C	1_C	2_C	0_D
0							
	2000 (0_A)	2500 (0_A)	3000 (0_A)	$+\infty$	$+\infty$	$+\infty$	$+\infty$
				3120 (2_B)	4500 (0_B)	5000 (0_B)	
							5120 (2_C)
							5120 (0_C)

Il existe donc 2 chaînes de poids minimal :

$$0_A - 2_B - 0_C - 0_D \quad \text{et} \quad 0_A - 0_B - 2_C - 0_D.$$

Il y a donc deux possibilités :

- construire 4 chalets en mai, en stocker 2, ne rien construire en juin, en construire 2 en juillet.
- construire 2 chalets en mai, en construire 4 en juin, en stocker 2, ne rien construire en juillet.

5.2 Suite arithmético-géométrique

Une entreprise compte 220000 employés. Cette entreprise veut diminuer le nombre d'employés et pour cela, elle ne remplace pas tous les départs à la retraite. L'objectif de l'entreprise est de diminuer de 45000 le nombre de postes. Les départs à la retraite représentent 3% par an et l'entreprise fait 300 nouvelles embauches.

Quand l'entreprise atteindra-t-elle son objectif?

Soit $n \in \mathbb{N}$. On pose u_n le nombre de personnes dans l'entreprise après n années. On a donc :

$$\begin{cases} u_{n+1} = 0,97u_n + 300 \\ u_0 = 220000 \end{cases}$$

Ensuite, on résout classiquement : on pose $v_n = u_n - 10000$.
(la résolution est à faire en exercice!)