Coder un mot avec une fonction

Année 2025 - 2026

Owen Ferrand, Elsa Dusseaux, Alexandra Duboc, Axel Polin : élèves de classes de seconde et terminale.

Établissement : Lycée Olympe de Gouges de Montech.
Enseignant.es : Adeline Cavailles, Chloé Samson et Fabien Bourg.
Chercheur et chercheuse : Lucas Monteiro et Caroline Guinet de l'Université Paul-Sabatier à Toulouse.

1. Clés de codage de la forme f(x)=3x+1

1.1. Présentation du sujet

Dans le cadre du projet MATh en JEANS, nous avons traité un sujet qui nous a été proposé par les deux chercheurs. Nous avons choisi de travailler le sujet "Coder un mot avec une fonction". Celui-ci nous a attiré car il nous paraissait intéressant, en particulier le fait de pouvoir coder un mot avec des chiffres et de pouvoir le décoder par la suite grâce à une clé inconnue. Ce principe est aussi plutôt concret et facile à visualiser. En effet, l'utilisation d'un code mathématique afin de dissimuler des messages est un principe qui a été utilisé fréquemment au cours de l'histoire, du code César à la machine Enigma de la Seconde Guerre mondiale.

Notre sujet se base sur le principe suivant : on identifie une lettre par sa position dans l'alphabet. On prend alors A représenté par 1, B par 2 et ainsi de suite jusqu'à Z qui est représenté par 26. Puis on repart à 27 avec A et on continue indéfiniment.

Ce qui nous permet de coder par exemple le mot "BONJOUR" par la séquence de nombres suivants: "2,15,14,10,15,21,18".

Ce qui nous conduit à coder une lettre "x" en lui appliquant la fonction : f(x)=3x+1. Par conséquent, le mot BONJOUR se transforme pour chaque lettre et devient alors, pour B=2, 2*3+1=7 ce qui correspond à la lettre G. Le mot BONJOUR devient alors "GTQETLC".

De manière générale, si on note une telle fonction "f", le mot $x_1,x_2\ldots,x_n$ est codé par $f(x_1),f(x_2),\ldots,f(x_n)$.

Nos questions sont orientées vers une principale : Comment retrouver le mot d'origine sachant qu'on a obtenu le mot et la clé qui l'a codé, ici f(x)=3x+1 ?

1.2. Premier raisonnement

Afin de retrouver le mot d'origine, nous avons eu l'idée de soustraire 1 à la lettre codée, puis de diviser ce résultat par 3. Pour vérifier le fonctionnement de cette méthode, nous avons représenté un tableau afin de visualiser chaque étape du codage et du décodage.

On obtient le tableau ci-contre :

Lettre non-codé	Position dans l'alphabet	Après utilisation de la clé : f(x)=3x+1	Lettre codé	Lettre non-codé	Position dans l'alphabet	Après utilisation de la clé : f(x)=3x+1	Lettre codé
A	1	3*1+1=4	4=D	N	14	3*14+1=43	43-26=17=Q
B	2	3*2+1=7	7=G	O	15	3*15+1=46	46-26=20=T
C	3	3*3+1=10	10=J	P	16	3*16+1=49	49-26=23=W
D	4	3*4+1=13	13=M	Q	17	3*17+1=52	52-26=26=Z
E	5	3*5+1=16	16=P	R	18	3*18+1=55	55-2*26=3=C
F	6	3*6+1=19	19=S	S	19	3*19+1=58	58-2*26=6=F
G	7	3*7+1=22	22=V	T	20	3*20+1=61	61-2*26=9=I
H	8	3*8+1=25	25=Y	U	21	3*21+1=64	64-2*26=12=L
I	9	3*9+1=28	28-26=2=B	V	22	3*22+1=67	67-2*26=15=O
J	10	3*10+1=31	31-26=5=E	W	23	3*23+1=70	70-2*26=18=R
K	11	3*11+1=34	34-26=8=H	X	24	3*24+1=73	73-2*26=21=U
L	12	3*12+1=37	37-26=11=K	Y	25	3*25+1=76	76-2*26=24=X
M	13	3*13+1=40	40-26=14=N	Z	26	3*26+1=79	79-3*26=1=A

En complétant ce tableau, nous avons remarqué qu'après l'utilisation de la clé f(x)=3x+1 certaines valeurs étaient supérieures à 26, à partir du codage de la lettre I. Donc pour obtenir la

lettre codée, nous avons retiré 26 au résultat, puis 2*26 à partir de R, et enfin 3*26 pour le Z.

Par exemple, si nous souhaitons coder la lettre O, on effectue 3*15+1 = 46. On enlève alors 26 pour obtenir un nombre compris entre 1 et 26 : 46-26 = 20. Donc on obtient la lettre T. Donc le codage de la lettre T n'est pas 3x+1 mais 3x+1-26.

Pour revenir en arrière, on fait face à un problème: si on soustrait 1 à 20 pour diviser par 3, on obtient: (20-1)/3 ≈ 6,33. Pour revenir à la forme initiale, nous devons donc additionner un multiple de 26 au 20, avant de lui soustraire 1 et de le diviser par 3.

Il nous reste donc à savoir quel multiple de 26 il faut additionner à 20 pour bien obtenir la lettre de départ, soit O.

Une fois avoir codé toutes les lettres, nous avons observé que toutes les lettres codées n'apparaissent qu'une seule fois, ce qui veut dire que nous pouvons bien écrire tous les mots avec cette clé.

1.3. Résolution du décodage de la clé f(x)=3x+1

Pour savoir combien de fois il faut ajouter 26, il faut comprendre quels numéros en ont besoin et lesquels n'en ont pas besoin.

On observe que les lettres codées [D,G,J,M,P,S,V,Y] n'ont pas besoin de l'ajout de 26 car leur résultat est inférieur à 26. Par exemple : C=3 devient 3*3+1=7=G et on retrouve cette forme 3x+1. On observe donc que les lettres qui restent à la forme 3x+1 n'ont pas besoin de l'ajout de 26 car la fonction inverse marche sur ces nombres. C'est à dire que lorsqu'on utilise cette fonction on a : ((3x+1)-1)/3 et ils nous reste x soit le nombre de départ et lorsqu'on a enlevé 1 on a obtenu un multiple de 3 et donc un reste de 0 si on le divise par 3 ce qui caractérise les nombres de la forme 3x+1.

Alors que la lettre d'après est f(I)=28=B et 28 supérieure à 26 donc on a enlevé 26 qui symbolise le tour de l'alphabet et on revient donc à 2=B. On en déduit donc que c'est à ce moment-là que la fonction inverse ne fonctionne plus. Cela marche pour les lettres [B,E,H,K,N,Q,T,W,Z] qui sont impactés par ce moins 26 et passe de la forme 3x+1 à la forme de 3x+2 donc la fonction inverse moins 1 et divisée par 3 ne fonctionne plus. Par conséquent, en ce qui concerne les nombres qui passent de la forme 3x+1 à la forme 3x+2 nécessite l'ajout de 26 pour obtenir la forme qui fonctionne avec la fonction inverse. Par exemple, N=14 est de la forme 3x+2 donc si on enlève 1 et qu'on divise par 3 la fonction inverse ne fonctionne pas car on obtient pas un nombre entier. Il nous faut ajouter 26 et on obtient : 14+26=40 qui est de la forme 3x+1 et où la fonction inverse nous permet d'obtenir 13 (=(40-1)/3) ce qui correspond bien à M.

Et si on se concentre sur le moment où on a enlevé 1, on est passé de la forme 3x+2 à la forme 3x+1. De plus, après avoir divisé par 3, on a eu un reste de 1 et on sait qu'on avait besoin d'ajouter une seule fois 26 pour obtenir la bonne forme. En conclusion on peut supposer que le reste de la division euclidienne de notre nombre codé (en soustrayant 1 puis en divisant par trois) pourrait

nous donner le nombre de fois que l'on doit ajouter 26.

Poursuivons ce raisonnement avec le groupe de lettres suivant : [C,F,I,L,O,R,U,X] qui est impacté également, mais nécessite la soustraction de 26 deux fois car le nombre est supérieur à 52(=2*26). De ce fait, ils passent de la forme 3x+1 à la forme 3x et la fonction inverse de marche plus non plus. Par conséquent, en ce qui concerne les nombres qui passent de la forme 3x+1 à la forme 3x, ils nécessitent l'ajout de deux fois 26 pour obtenir la forme qui fonctionne avec la fonction inverse. Par exemple, L=12 est de la forme 3x donc si on utilise la fonction inverse on obtient pas de nombre entier. Il nous faut ajouter deux fois 26 et on obtient : 12+2*26= 64 qui est de la forme 3x+1 et où la fonction inverse nous permet d'obtenir 21 (=(64-1)/3) ce qui correspond bien à U.
Et si on se concentre sur le moment où on a enlevé 1, on est passé de la forme 3x à la forme 3x+2. De plus, après avoir divisé par 3, on a eu un reste de 2 et on sait qu'on avait besoin d'ajouter deux fois 26 pour obtenir la bonne forme. Donc notre supposition se confirme ici.

Enfin on retrouve la lettre A, toute seule, qui a dépassé 78(=3*26) donc on a eu besoin de lui soustraire trois fois 26 mais qui garde sa forme 3x+1. Par conséquent, A devrait rejoindre le groupe des lettres qui ont gardé la forme de 3x+1. Cependant lorsqu'on utilise la fonction inverse on a : (1-1)/3=0 et on ne retombe pas sur Z. Donc comme on tombe sur 0, il nous faut ajouter 26 et on obtient Z. Ce qui fait de A un cas particulier qui demande l'intervention d'un ajout de 26 bien qu'il soit de la forme 3x+1.

On en déduit donc qu'il faut regarder le reste de la division euclidienne de la lettre codée par 3x+1. On modélisera cette recherche du reste par les congruences et les modulos.
Ces termes ne sont pas très connus mais ils sont simples à comprendre. Lorsqu'on écrit : $3 \equiv 1\ [2]$ il se lit : 3 congrue à 1 modulo 2. C'est-à-dire, que 3 et 1 ont le même reste lorsqu'on les divise par 2. En effet, tous deux étant des nombres impairs ils auront comme reste 1 lorsqu'on procède à leur division euclidienne. Même exemple avec : $9 \equiv 24\ [3]$ (qui se lit : 9 congrue à 24 modulo 3) car comme 9 et 24 sont des multiples de 3, alors 9 et 24 auront tout deux zéro comme reste de la division euclidienne par 3.

Il nous faut donc nous intéresser à la division euclidienne de notre nombre codé. On aura donc le calcul suivant : (lettre codée) - $1 \equiv r\ [3]$. Ce calcul, par le moins 1 et par le modulo 3, reconstitue la fonction inverse où "lettre codée" signifie le numéro de la lettre codée. Et ici "r" représente le reste de la division euclidienne de notre lettre codée par 3 après avoir soustrait 1. Ainsi la valeur du "r" obtenus nous donne le nombre de fois qu'il faut ajouter 26 à notre lettre codée pour que la fonction inverse fonctionne à nouveau et ainsi décoder la lettre codée.

D'où la fonction inverse suivante : ((Code +26*r) -1) /3.

Vérifions notre formule et reprenons le mot codé : 'GTQETLC'.
Donc : G=7, T=20, Q=17, E=5, L=12 et C=3

Pour G on a : Code-1 ≡ r [3] ⇔ 7-1 ≡ 0 [3] donc : ((7+26*0)-1)/3 = 2 = B

Pour T on a : Code-1 ≡ r [3] ⇔ 20-1 ≡ 1 [3] donc : ((20+26*1)-1)/3 = 15 = O

Pour Q on a : Code-1 ≡ r [3] ⇔ 17-1 ≡ 1 [3] donc : ((17+26*1)-1)/3 = 14 = N

Pour E on a : Code-1 ≡ r [3] ⇔ 5-1 ≡ 1 [3] donc : ((5+26*1)-1)/3 = 10 = J

Pour L on a : Code-1 ≡ r [3] ⇔ 12-1 ≡ 2 [3] donc : ((12+26*2)-1)/3 = 21 = U

Pour C on a : Code-1 ≡ r [3] ⇔ 3-1 ≡ 2 [3] donc : ((3+26*2)-1)/3 = 18 = R

Donc le mot codé 'GTQUETLC' est en réalité 'BONJOUR'. On retombe bien sur notre énoncé du début. De plus, grâce à ce mot on a pu tester tous les restes de la division euclidienne par trois (zéro, un, deux) donc notre fonction inverse fonctionne pour toutes les lettres.
On est donc capable de retrouver n'importe quel mot et on sait qu'il n'y aura qu'une seule possibilité. En effet, la fonction étudiée n'admet qu'un seul antécédent par image.

1.4. Résolution du décodage de la clé f(x)=ax

Maintenant on cherche à faire de même mais avec une clé de la forme : f(x)=ax avec a appartenant à l'ensemble des entiers naturels.

Tout d'abord, on a remarqué que le coefficient "a" appartient à un ensemble de nombre réel finis. Il appartient à l'intervalle fermé [1 ; 25]. En effet, lorsque l'on prend des fonctions où le coefficient "a" est supérieur à 26 on pouvait remarquer qu'elle codait de la même manière une fonction déjà vue où "a"était plus petit.

Par exemple, si on compare les fonctions f(x)=29x et f(x)=3x on remarque qu'elles codent les mêmes lettres. En effet, avec R on a : f(18)=29*18=522=B (522-26*20=2=B) et pareil pour la seconde : f(18)=3*18=54=B (54-26*2=2=B). On peut également poursuivre l'exemple avec G, d'une part on a : f(7)=29*7=203=U (203-26*7=21=U), d'autre part on a : f(7)=3*7=21=U. Ces fonctions sont autant liées que si on en prenait d'autres telles que les fonctions f(x)=34 et f(x)=8. Ce lien est dû à la soustraction du coefficient par 26 (29-26=3), ce qui nous permet de simplifier et de limiter le nombre de codage possible avec la forme ax.
Enfin, l'intervalle sur lequel appartient notre coefficient "a" est limité entre 1 et 25 mais ne comporte pas 0 et 26 car lorsqu'on utilise leur fonction associée (f(x)=0x et f(x)=26x) on obtient toujours la même lettre. C'est-à-dire, qu'avec la fonction f(x)=0x, on aura que des 0 et 0 ne correspond pas à une lettre et pour f(x)=26x, on aura que des multiples de 26 donc lorsque l'on réduira le nombre en enlevant 26, comme on faisant pour la clés précédente, on obtiendra que

des Z car on obtiendra que des 26. Donc ces fonctions sont inexploitables.
On a également remarqué que “a” ne peut pas prendre comme valeur un nombre pair car comme la multiplication d’un nombre n, appartenant à l’ensemble des entiers naturels, par un nombre pair donnera forcément un autre nombre pair. Autrement dit, si tous nos nombres sont pairs et compris entre 1 et 26, alors on aura des doublons et donc on ne pourra pas savoir quel était le mot d’origine.

Maintenant on cherche à trouver la fonction inverse qui décodera les lettres codées tout en connaissant la valeur du coefficient “a”.

Nous avons débuté en reprenant nos réflexions quant à notre première résolution de clé. En effet, nous avons fait plusieurs essais en regardant les résultats d’une fonction où “a” avait comme valeur 5 (pris aléatoirement).
On a constaté le même problème pour revenir à la lettre de base que dans notre clé précédente. En effet, lorsque l’on prend C on a : f(3)=5*3=15=O la fonction inverse est facile à trouver car il nous suffit simplement de rediviser par 5 (le coefficient lui-même) et on obtient bien : 15/5=3=C soit la valeur de départ.

Cependant, le problème apparaît au moment où on prend une valeur plus grande. Par exemple avec P on a : f(16)=5*16=80=B (80-26*3=2=B) donc cette fois on ne pourra pas simplement rediviser par 5 pour revenir à notre lettre non codée, il nous faudrait rajouter 3 fois 26. En effet, si on décide de diviser notre nombre par 5 on aura pas un nombre entier et on aura un reste de 2.
Même phénomène avec la lettre V on a : f(22)=5*22=110=F (110-26*4=6=F), impossible de diviser par 5 et il nous faudrait rajouter 4 fois 26 pour que cela marche correctement. En effet, ici sans ajout de plusieurs fois 26 le reste serait de 1.

Ainsi on commence à remarquer une relation entre le reste lors de la division par 5 et le nombre de fois qu’il faudrait rajouter 26. En effet, dans le premier cas on avait un manque de 3 fois 26 et un reste de 2. Dans l’autre cas, on avait un manque de 4 fois 26 et un reste de 1. En conclusion, notre hypothèse serait de penser que le reste de la division par 5 et le nombre de fois qu' il faudrait rajouter 26 serait complémentaire au coefficient (3+2= 5 et 4+1=5).

Vérifions notre hypothèse en reprenant comme exemple la fonction f(x)=5x, on sait que : f(1)=5*1=5=E, f(15)=75=W (75-26*2=23=W) et f(20)=100=V (100-26*3=22).

Pour le premier cas on a : E=5 qui à 0 comme reste de la division euclidienne par 5 donc le complément à 5 est 5. Or on observe que pour faire la fonction inverse et passer de E à A nous n’avons pas besoin d’ajouter 5 fois 26. Donc pour ce premier cas où le reste est égal à 0, nous n’avons pas besoin d’ajouter 26 et notre hypothèse ne marche pas dans ce cas là.

Pour le second cas on a : W=23 qui a un reste de 3 lorsqu’on le divise par 5 et son complément à 5 est 2. Or on observe que pour effectuer la fonction inverse et passer de W à O on a besoin de 2 fois 26. Donc ici notre hypothèse se confirme.

Pour le troisième cas on a : V=22 qui a un reste de 2 lorsqu'on le divise par 5 et son complément à 5 est 3. Or on observe que pour effectuer la fonction inverse et passer de V à T on a besoin de 3 fois 26. Donc ici notre hypothèse se confirme à nouveau.

En conclusion, on distingue deux cas :
-Si le reste de la division euclidienne est nul alors il nous suffit simplement de diviser par notre coefficient "a". Ce qui correspond à effectuer ces deux étapes : d'abord, on remarque : lettre codée ≡ 0 [a] puis on effectue la fonction inverse sans ajout de multiples de 26 : lettre codée / a.

-Si le reste de la division euclidienne est différent de 0 alors on ajoute son complément à notre coefficient "a". Ce qui correspond à effectuer ces deux étapes : d'abord, on remarque : lettre codée ≡ r [a] puis on effectue la fonction inverse en ajoutant cette fois-ci le bon nombre de multiples de 26 qui correspond à : (lettre codée + (a - r)*26) / 5.

Enfin vérifions si notre conclusion est bonne en codant le mot "BONJOUR" grâce à la clé f(x)=5x. "BONJOUR" devient alors "JWRXAL" et essayons de revenir en arrière.
Donc : J=10, W=23, R=18, X=24, A=1, L=12 et notre coefficient a=5.

Pour J on a : lettre codée ≡ r [5] ⇔ 10 ≡ 0 [5] donc : 10 /5 = 2 = B

Pour W on a : lettre codée ≡ r [5] ⇔ 23 ≡ 3 [5] donc : (23+26*(5-3)) /5 = 15 = O

Pour R on a : lettre codée ≡ r [5] ⇔ 18 ≡ 3 [5] donc : (18+26*(5-3)) /5 = 14 = N

Pour X on a : lettre codée ≡ r [5] ⇔ 24 ≡ 4 [5] donc : (24+26*(5-4)) /5 = 10 = J

Pour A on a : lettre codée ≡ r [5] ⇔ 1 ≡ 1 [5] donc : (1+26*(5-1)) /5 = 21 = U

Pour L on a : lettre codée ≡ r [5] ⇔ 12 ≡ 2 [5] donc : (12+26(5-2)) /5 = 18 = R

Ici la fonction inverse fonctionne bien est le mot original est retrouvé. Cependant, lorsqu'on prend une autre clé, notre méthode de résolution ne fonctionne pas. En effet, on se retrouve souvent avec soit trop de fois 26 ajouter soit au contraire pas assez de fois 26.

Comme avec la clé de la forme f(x)=7x qui code "BONJOUR" en "NATRAQU".
Donc de la même manière on procède pareil : N=14, A=1, T=20, R=18, Q=17, U=21 et notre coefficient a=7.

Pour N on a : lettre codée ≡ r [7] ⇔ 14 ≡ 0 [7] donc : 14 /7 = 2 = B

Pour A on a : lettre codée ≡ r [7] ⇔ 1 ≡ 1 [7] donc : (1+26*(7-1)) /7 = 22,428 ≠ O

Pour T on a : lettre codée ≡ r [7] ⇔ 20 ≡ 6 [7] donc : (20+26*(7-6)) /7 =6,571 ≠ N

Pour R on a : lettre codée ≡ r [7] ⇔ 18 ≡ 4 [7] donc : (18+26*(7-4)) /7 =13,714 ≠ J

Pour Q on a : lettre codée ≡ r [7] ⇔ 17 ≡ 3 [7] donc : (17+26*(7-1)) /7 =24.714 ≠ U

Pour U on a : lettre codée ≡ r [7] ⇔ 21 ≡ 0 [7] donc : 21 /7 = 3 ≠ R

Donc ici on remarque qu'il y a des moment où notre méthode de résolution ne fonctionne pas. Ainsi par faute de temps nous n'avons pas pu trouver de méthode capable de décoder n'importe qu'elle clés de la forme f(x)=ax ni de savoir retrouver ce coefficient.

Merci d'avoir porté attention à nos recherches en espérant que ces recherches vous ont intéressé et fait réfléchir.

Note d'édition

La méthode de résolution proposée pour a=5 repose sur le fait que 26 est congru à 1 modulo 5. En effet, lettre codée + (5-r)*26 ≡ lettre codée + 5 – r ≡ lettre codée – r ≡ 0 [5], donc on peut diviser par 5. Comme 26 est congru à 5 modulo 7, il n'est pas surprenant que la même formule ne s'applique pas. Ce qu'on cherche, c'est le plus petit multiple de 26 qu'il faut ajouter à lettre codée pour obtenir un multiple de a. En général, ce n'est pas a – r.