Index

Antilles-Guyane TES-L spé 14 septembre 2012

La qualité de la rédaction, la clarté et la précision des raisonnements, la cohérence globale des réponses sont valorisées.
Le recours à des tableaux et graphiques pour soutenir une argumentation ou présenter des résultats est valorisé, sous réserve qu'un commentaire en précise clairement la signification.
Extrait du B.O. concernant la notation de l'épreuve au baccalauréat.

EXERCICE 2 5 points
Pour les candidats ayant suivi l'enseignement de spécialité

Analyse de l'énoncé …
Les employés d'une grande zone commerciale ont le choix entre deux types de restaurants : un « self » ou un restaurant « traditionnel » avec service à la place. On admet que tous les employés mangent chaque jour dans l'un des deux restaurants.
On a constaté que :
• si un employé mange au « self » un jour donné, alors le lendemain il y mange également avec une probabilité de 0,8 ;

C'est-à-dire : $P_{\text{self-jour-n}}(\text{self-jour-n+\{1\}}) = 0{,}8$

• si un employé mange dans le restaurant « traditionnel » un jour donné, alors le lendemain il change pour le « self » avec une probabilité de 0,4.

C'est-à-dire : $P_{\text{traditionnel-jour-n}}(\text{self-jour-n+\{1\}}) = 0{,}4$.

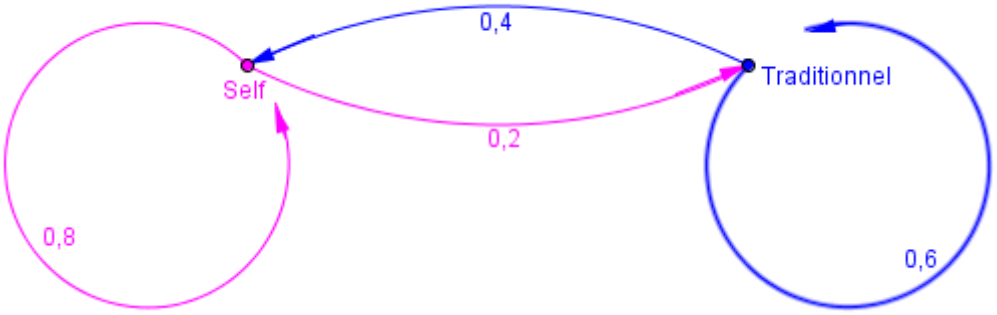
On choisit au hasard un employé de la zone commerciale.
Si n est un entier naturel non nul, on appelle s_n la probabilité que l'employé choisi mange au « self » le n-ième jour, et par $t_n = 1 - s_n$ la probabilité qu'il mange au restaurant « traditionnel » le n-ième jour.

Remarque : Dans la mesure où il n'y a que deux issues (self, traditionnel), l'auteur de l'exercice aurait pu ne pas indiquer $t_n = 1 - s_n$.

Pour l'état initial, on admet que $s_1 = t_1 = 0{,}5$, c'est-à-dire que le premier jour, les probabilités de choix du « self » ou du restaurant « traditionnel » sont égales.
Dans la suite, pour tout entier naturel n non nul, on note P_n la matrice $P_n = (s_n \quad t_n)$.

P_n est la matrice traduisant l'état probabiliste à la date n.

1. *Traduire les données de l'énoncé par un graphe probabiliste.*



Remarque :
Distinguer le lieu " Self " de l'événement " être au self à la date n " et de la probabilité s_n .

2. *Justifier l'égalité matricielle $P_{n+1} = P_n \times M$ où M désigne la matrice $\begin{pmatrix} 0,8 & 0,2 \\ 0,4 & 0,6 \end{pmatrix}$ et n un entier naturel non nul.*

Soit $P_n = (s_n \quad t_n)$ l'état probabiliste à la date n.
Notons S_n l'événement " choisir le self à la date n, et, T_n l'événement " choisir le traditionnel à la date n "
$P(S_n) = s_n$ et $P(T_n) = t_n$
Comme $P_{S_n}(S_{n+1}) = 0,8$, d'où, $P_{S_n}(T_{n+1}) = 1 - 0,8 = 0,2$
et que $P_{T_n}(S_{n+1}) = 0,4$, d'où, $P_{T_n}(T_{n+1}) = 1 - 0,4 = 0,6$
en appliquant la formule des probabilités totales, on a : $P(S_{n+1}) = P_{S_n}(S_{n+1}) \times P(S_n) + P_{T_n}(S_{n+1}) \times P(T_n)$
d'où, $s_{n+1} = 0,8\ s_n + 0,4\ t_n$.
de même, $t_{n+1} = 0,2\ s_n + 0,6\ t_n$
Ce système se traduit par l'égalité matricielle : $P_{n+1} = P_n \begin{pmatrix} 0,8 & 0,2 \\ 0,4 & 0,6 \end{pmatrix}$

3. *Déterminer la probabilité que l'employé tiré au sort mange au « self » le deuxième jour.*

Comme $P_1 = (0,5 \quad 0,5)$, on a : $P_2 = (0,5 \quad 0,5) \begin{pmatrix} 0,8 & 0,2 \\ 0,4 & 0,6 \end{pmatrix}$
$= (0,5\times0,8 + 0,5\times0,4 \quad 0,5\times0,2 + 0,5\times0,6) = (0,6 \quad 0,4)$
La probabilité que l'employé tiré au sort mange au *« self »* le deuxième jour est : $s_2 = 0,6$

4. *Déterminer l'état probabiliste stable et l'interpréter.*
On cherche $P = (s \quad t)$ tel que $P = P\times M$
On résout donc le système : $\begin{cases} s = 0,8\,s + 0,4\,t \\ t = 0,2\,s + 0,6\,t \\ s + t = 1 \end{cases}$
Les deux premières équations sont équivalentes et se ramènent à l'équation : $0,2s - 0,4t = 0$
d'où, le système : $\begin{cases} 0,2\,s - 0,4\,t = 0 \\ t = 1 - s \end{cases} \Leftrightarrow \begin{cases} 0,2\,s - 0,4(1-s) = 0 \\ t = 1 - s \end{cases} \Leftrightarrow \begin{cases} 0,6\,s = 0,4 \\ t = 1 - s \end{cases} \Leftrightarrow \begin{cases} s = \dfrac{2}{3} \\ t = \dfrac{1}{3} \end{cases}$
L'état stable $P = \left(\dfrac{2}{3} \quad \dfrac{1}{3}\right)$
Sur la durée, la proportion des employés choisissant un restaurant se stabilise :

$\frac{2}{3}$ des employés vont au self, $\frac{1}{3}$ des employés vont au traditionnel.

5. *Démontrer que pour tout entier nature n non nul, on a :* $s_{n+1} = \frac{2}{5}\ s_n + \frac{2}{5}$.

À la question 2/ on a vu : $s_{n+1} = 0{,}8\ s_n + 0{,}4\ t_n$.
Comme $t_n = 1 - s_n$, il vient : $s_{n+1} = 0{,}8\ s_n + 0{,}4(1 - s_n)$.

soit : $s_{n+1} = 0{,}4\ s_n + 0{,}4 = \frac{2}{5}\ s_n + \frac{2}{5}$.

6. *Dans la suite, pour tout entier naturel n non nul, on pose :* $u_n = s_n - \frac{2}{3}$.

a. *Démontrer que la suite* (u_n) *est une suite géométrique de raison* $\frac{2}{5}$ *et de premier terme* $u_1 = -\frac{1}{6}$.

On cherche à exprimer u_{n+1} en fonction de u_n.

Par définition de la suite (u_n) : $u_{n+1} = s_{n+1} - \frac{2}{3}$ (1)

Or, $s_{n+1} = \frac{2}{5}\ s_n + \frac{2}{5}$

en remplaçant dans l'égalité précédente (1) : $u_{n+1} = \frac{2}{5}\ s_n + \frac{2}{5} - \frac{2}{3} = \frac{2}{5}\ s_n - \frac{4}{15}$ (2)

Or, $s_n = u_n + \frac{2}{3}$ par définition de la suite (u_n).

en remplaçant dans l'égalité précédente (2) : $u_{n+1} = \frac{2}{5}(u_n + \frac{2}{3}) - \frac{4}{15}$ (3)

En réduisant : $u_{n+1} = \frac{2}{5}u_n + \frac{4}{15} - \frac{4}{15} = \frac{2}{5}u_n$

Cette dernière égalité prouve que la suite (u_n) est une suite géométrique de raison $\frac{2}{5}$.

Son premier terme est $u_1 = s_1 - \frac{2}{3} = \frac{1}{2} - \frac{2}{3} = -\frac{1}{6}$.

b. *Déterminer l'expression de* u_n *en fonction de n, où n est un entier naturel non nul.*

puisque la suite (u_n) est une suite géométrique de raison $\frac{2}{5}$ et de premier terme est $u_1 = -\frac{1}{6}$, on sait :

pour tout n non nul, $u_n = -\frac{1}{6} \times \left(\frac{2}{5}\right)^{n-1}$

c. *En déduire que, pour tout entier naturel n non nul,* $s_n = -\frac{1}{6} \times \left(\frac{2}{5}\right)^{n-1} + \frac{2}{3}$.

Comme $s_n = u_n + \frac{2}{3}$ par définition de la suite (u_n), on trouve : $s_n = -\frac{1}{6} \times \left(\frac{2}{5}\right)^{n-1} + \frac{2}{3}$.

d. *Déterminer la limite de la suite* (s_n) *quand n tend vers* $+\infty$ *et interpréter ce résultat.*

puisque $0 < \frac{2}{5} < 1$, la suite $\left(\left(\frac{2}{5}\right)^{n-1}\right)$ converge vers 0, d'où,

en multipliant par la constante $-\frac{1}{6}$, $\lim\limits_{n \to +\infty} -\frac{1}{6} \times \left(\frac{2}{5}\right)^{n-1}$

puis en ajoutant la constante $\frac{2}{3}$: $\lim\limits_{n\to+\infty} -\frac{1}{6}\times\left(\frac{2}{5}\right)^{n-1}+\frac{2}{3}=\frac{2}{3}$.

On retrouve la probabilité calculée lors de la recherche de l'état stable.

---

108 page 113 Comment payer avec deux billets

a et b sont deux entiers naturels non nuls.

On ne dispose pour payer les achats que de deux sortes de billets d'un montant respectif a et b.

A- on suppose qu'on peut rendre la monnaie

1) Si a et b sont premiers entre eux, on peut payer toute somme entière S.

En effet, a et b étant premiers entre eux, il existe deux entiers u et v tels que $au + bv = 1$, d'où,

$(Su)a + (Sv)b = S$.

Il est suffisant d'avoir $|Su|$ billets d'un montant a et $|Sv|$ billets d'un montant b pour tout achat de montant S.

2) Si a et b ne sont pas premiers entre eux.

Soit g le PGCD(a ; b).

il existe deux entiers u et v tels que $au + bv = g$,

Rappel : $\frac{a}{g} = a'$ et $\frac{b}{g} = b'$ avec a' et b' premiers entre eux. $a'u + b'v = 1$.

On ne peut payer que les sommes multiples de g.

Si $S = kg$ alors $(ku)a + kv)b = kg = S$.

Si, pour tout entier k, $S \neq kg$ et $xa + yb = S$ avec x et y entiers, on a en divisant par g, $xa' + yb' = \frac{S}{g}$ (non entier) ce qui est contradictoire ...

B- On suppose qu'on ne rend plus la monnaie.

a et b sont premiers entre eux.

1) On ne peut payer une somme S (entier naturel) si et seulement si il existe deux entiers naturels m et n tels que : $am + bn = S$.

Évident : puisqu'on ne rend pas la monnaie, le nombre m (resp. n) de billets a (resp. b) est un entier naturel, et, réciproquement,

puisque a, b, m, n sont des entiers naturels, la somme de produits d'entiers naturels est un entier naturel.

2)a) b)c) Expérimentation : $a = 3$

a) $b = 8$.

Comme $2\times3 + 1\times8 = 14$

et $5\times3 = 15$

et $2\times8 = 16$

on peut payer les sommes de 14, 15 et 16 euros.

En ajoutant à chaque fois un billet de 3 euros, on peut payer toutes les sommes à partir de 14 €.

Tout entier supérieur ou égal à 14 peut s'écrire de la façon suivante : $14 + 3k$, $15 + 3k$, $16 + 3k$ où $k \in \mathbb{N}$.

La plus grande somme M ne pouvant pas être payée avec des billets de 3 et 8 est 13.

Supposons $M = 13 = 3x + 8y$ avec x et y entiers naturels.

On a : $x \leqslant 4$ et $y \leqslant 1$.

Si $y = 0$, impossible,

si $y = 1$, on obtient : $3x = 5$ impossible.

On peut tester toutes les sommes possibles avec 0 ; 1 ; 2 … billets de chaque sorte jusqu'à obtenir 14.

On peut avoir au plus 2 billets de 8 et au plus 5 de 3 ….

Nombre de billets a / b	0	1
0	0	8
1	3	11
2	6	14
3	9	17
4	12	20

b) $a = 3$ et $b = 11$

Nombre de billets a / b	0	1	2
0	0	11	22
1	3	14	25
2	6	17	28
3	9	20	31
4	12	23	34
5	15	26	37
6	18	29	40
7	21	32	43

La première série de trois sommes consécutives est 20 ; 21 ; 22
M = 19

$a = 3$ et $b = 13$

Nombre de billets a / b	0	1	2
0	0	13	26
1	3	16	29
2	6	19	32
3	9	22	35
4	12	25	38
5	15	28	41
6	18	31	44
7	21	34	47

8	24	37	50

La première série de trois sommes consécutives est 24 ; 25 ; 26
M = 23

c) Les points A(8 ; 13), B(11 ; 19) et C(13 ; 23) sont alignés sur la droite d'équation $y = 2x - 3$
On peut supposer : M = $2b - 3$
Si $b = 14$, alors : M = 25
On peut atteindre $26 = 4\times3 + 14$
$27 = 9\times3$
$28 = 2\times14$
Supposons $25 = 3m + 14n$ avec m et n entiers tels que $m \leqslant 8$ et $n \leqslant 1$
si $m = 0$ ou $n = 0$, impossible.
si $n = 1$ alors $11 = 3m$ impossible.
On ne peut pas atteindre 25.

2)d)e) Expérimentation : $a = 5$ et conjecture.
a = 5 et b = 8 ***M = 27***
On cherche la première série de 5 entiers consécutifs :
$28 = 4\times5 + 1\times8$, $29 = 1\times5 + 3\times8$, $30 = 6\times5$, $31 = 3\times5 + 2\times8$, $32 = 4\times8$ sont cinq entiers consécutifs, et, on ne peut pas avoir : $27 = 5m + 8n$ avec m et n entiers tels que $m \leqslant 5$ et $n \leqslant 3$

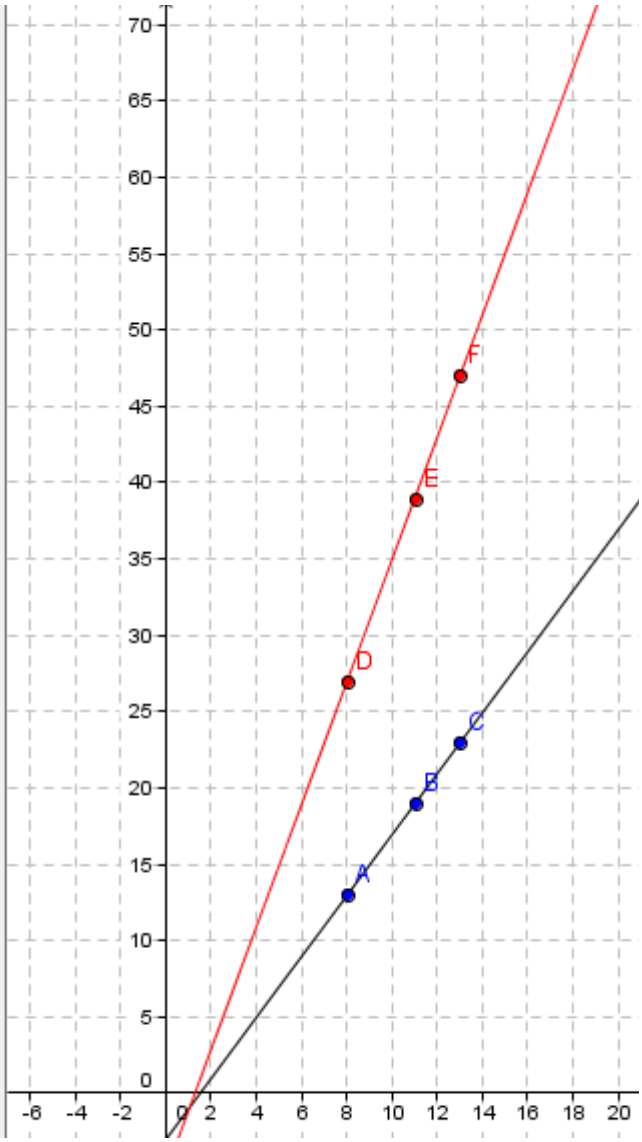
a = 5 et b = 11 ***M = 39***
$40 = 8\times5$, $41 = 6\times5 + 1\times11$, $42 = 4\times5 + 2\times11$, $43 = 2\times5 + 3\times11$, $44 = 4\times11$ sont cinq entiers consécutifs, et, on ne peut pas avoir : $39 = 5m + 11n$ avec m et n entiers tels que $m \leqslant 8$ et $n \leqslant 3$

a = 5 et b = 13 ***M = 47***
$48 = 7\times5 + 1\times13$, $49 = 2\times5 + 3\times13$; $50 = 10\times5$; $51 = 5\times5 + 2\times13$; $52 = 4\times13$ sont cinq entiers consécutifs, et, on ne peut pas avoir : $47 = 5m + 13n$ avec m et n entiers tels que $m \leqslant 9$ et $n \leqslant 3$.

On place les points D(8 ; 27), E(11 ; 39) et F(13 ; 47).
Ces trois points sont alignés sur la droite $y = 4x - 5$
Conjectures :
Il semble :
dans le cas où $a = 5$, M = $4b - 5$
dans le cas où $a = 3$, M = $2b - 3$
A-t-on dans le cas général : M = $(a - 1)b - a = ab - b - a$?
Remarquer la symétrie de la relation :
a et b ont le même rôle.
c-à-d : M = $(b - 1)a - b = (a - 1)b - a = ab - b - a$

Droite
- a: y = 2x - 3
- b: y = 4x - 5

Point
- A = (8, 13)
- B = (11, 19)
- C = (13, 23)
- D = (8, 27)
- E = (11, 39)
- F = (13, 47)



3) a et b sont strictement positifs et premiers entre eux.
On suppose qu'il existe deux entiers positifs x et y tels que $ax + by = ab - a - b$.
a) $ax + by = ab - a - b \Leftrightarrow ax + a = ab - b - by$
$\Leftrightarrow a(x + 1) = b(a - 1 - y)$
b divise le produit $a(x + 1)$.
a et b étant premiers entre eux, on peut appliquer le théorème de Gauss.
b divise $x + 1$, et, il existe donc un entier k tel que $x + 1 = kb$.
Or, $x \geqslant 0$, d'où, $x + 1 \geqslant 1$ et $b \geqslant 1$, donc, $k > 0$ (comme k entier, $k \geqslant 1$).

b) $a(x + 1) = b(a - 1 - y)$ et $x + 1 = kb$ implique $a(kb) = b(a - 1 - y)$ et comme $b \geqslant 1$,
en divisant par b, $ak = a - 1 - y$, soit : $y = a - ak - 1 = a(1 - k) - 1$
Conclusion :
$x + 1 = kb$ avec $k \geqslant 1$
$y + 1 = a(1 - k)$.
c) Comme $y \geqslant 0$, $y + 1 \geqslant 1$ ($y + 1$ strictement positif)
$a \geqslant 1$ et $1 - k \leqslant 0$, soit : $a(1 - k) \leqslant 0$ ($a(1 - k)$ négatif ou nul)
On n'a donc une contradiction : un nombre strictement positif ne peut pas être égal à un nombre négatif ou nul.
La supposition du 3/ es impossible :
il n'existe pas d'entiers positifs x et y tels que $ax + by = ab - a - b$.

Remarque : il n'est pas démontré dans cet exercice que M est la plus grande somme ne pouvant être atteinte ..

Quelques pistes de réflexion :

Supposons $a < b$,

il faut prouver que M + 1, M + 2, …., M + a peuvent s'écrire $xa + yb$ avec x et y entiers naturels .

* Pour $M + a = ab - a - b + a = (a - 1)b$, $x = 0$ et $y = a - 1$

** Dans une liste de a entiers consécutifs, il y a nécessairement un et un seul multiple de a.

Il existe donc un i tel que $1 \leqslant i < a - 1$ et $M + i = ka$ $x = k, y = 0$ (on doit avoir $b - i$ multiple de a, ce qui est possible puisque $b - i$ est une liste de a entiers consécutifs).

*** Soit $K = M + j$ avec $1 \leqslant j \leqslant a - 1$

Comme a et b sont **premiers entre eux**, l'équation $xa + yb = K$ a pour solutions (Bezout et Gauss), l'ensemble $E = \{(x_0 + qb ; y_0 - qa) / q \in \mathbb{Z}\}$ et $(x_0 ; y_0)$ une solution particulière de l'équation.

Deux nombres consécutifs $y_0 - qa$ et $y_0 - (q - 1)a$ diffèrent de a, il existe donc un des nombres $y_1 = y_0 - q_1 a$ appartenant à $[0 ; a - 1]$.

**** Il reste à montrer que $x_1 = x_0 + q_1 b$ positif ….

Les cas $y_1 = 0$ et $y_1 = a - 1$ sont déjà traités.

Soit $0 < y_1 < a - 1$

On a : $ax_1 + by_1 = M + j = ab - a - b + j$

soit : $a(x_1 + 1) = b(a - 1 - y_1) + j$.

Comme $0 < y_1 < a - 1$, on a : $0 < a - 1 - y_1 < a - 1$, d'où le nombre $b(a - 1 - y_1) + j > 0$

On en déduit : $x_1 + 1 > 0$ et comme x_1 est un entier $x_1 \geqslant 0$

		x	y	
a entiers consécutifs de M + 1 à M + a.	M+1			y prend les a valeurs de 0 à $a - 1$ (pas nécessairement dans l'ordre)
	M+i	k	0	
	M+a	0	$a - 1$	

Voici avec les exemples traités:

a=3 ; b=8 ; M=13				a=3 ; b=11 ; M=19				a=3 ; b=13 ; M=23		
	x	y			x	y			x	y
M+1=14	2	1		20	3	1		24	8	0
M+2=15	5	0		21	7	0		25	4	1
M+3=16	0	2		22	0	2		26	0	2

a=5 ; b=8 ; M=27				a=5 ; b=11 ; M=39				a=5 ; b=13 ; M=47		
	x	y			x	y			x	y
M+1=28	4	1		40	8	0		48	7	1
M+2=29	1	3		41	6	1		49	2	3
M+3=30	6	0		42	4	2		50	10	0
M+4=31	3	2		43	5	3		51	5	2
M+5=32	0	4		44	0	4		52	0	4

109 page 113 codage exponentiel

p est un entier premier et C est un entier naturel inférieur à p tel que C et $p - 1$ sont premiers entre eux .

C est la clé du codage.

Un entier n inférieur à p est codé par l'entier naturel m défini par : $m \equiv n^C$ (modulo p) et $0 \leqslant m < p$.

(m est donc le reste dans la division euclidienne de n^C par p).

A- Chiffrement de :

" les sanglots longs des violons de l'automne "

Chaque lettre est codé par deux chiffres de 00 à 25 (le tableau ci-dessous) :

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

À un bloc de deux lettres, on associe un nombre à 4 chiffres.
On a : $25^2 = 625$ blocs de deux lettres ou nombres à quatre chiffres et le plus grand nombre est 2525.
2) $p = 2\,851$ et $C = 221$
On vérifie que p est premier en testant tous les diviseurs premiers jusqu'à $\sqrt{2851}$: soit 53
2 851 n'est pas divisible par 2, ni par 3 ($2 + 8 + 5 + 1 \equiv 7$ (9)), ni par 5, ni par 11 ($2 + 5 = 7$ et $8 + 1 = 9$).

Nombres premiers	Divisible par :		Nombres premiers	Divisible par :		Nombres premiers	Divisible par :
2	Non		17			41	
3	Non		19			43	
5	Non		23			47	
7	$7\times407 + 2$		29			53	
11	Non		31				
13	…		37				

221 et 2851 – 1 = 2850 sont premiers entre eux.
Algorithme d'Euclide :

$2850 = 221\times12 + 198$ $\quad$ $23 = 14\times1 + 9$ $\quad$ $5 = 4\times1 + 1$
$221 = 198\times1 + 23$ $\quad$ $14 = 9\times1 + 5$
$198 = 23\times8 + 14$ $\quad$ $9 = 5\times1 + 4$

3)

LE	SS	AN	GL	OT	SL	ON	GS	DE
1104	1818	0013	0611	1419	1811	1413	0618	0304
SV	IO	LO	NS	DE	LA	UT	OM	NE
1821	0814	1114	1318	0304	1100	2019	1412	1304

a) m est l'unique reste dans la division euclidienne de 1104^{221} par 2 851
Deux nombres distincts m et m' tels que $m \equiv 1104^{221}$ (2 851) et $m' \equiv 1104^{221}$ (2 851) diffèrent d'un multiple de 2 851.
b) En appliquant les propriétés des congruences, $a \equiv b$ (p) implique $a^n \equiv b^n$ (p) et,
$a \equiv b$ (p) et $c \equiv d$ (p) implique $ac \equiv bd$ (p), on décompose l'exposant afin de ne pas dépasser les capacités de la calculatrice.

$221 = 128 + 93$ $93 = 64 + 29$ $29 = 16 + 13$ $13 = 8 + 5$ $5 = 4 + 1$

Avec les puissances de 2 :

Puissances	congrues à	congrues à		Puissances	congrues à	congrues à
1104^2	1439 (2851)	1439 (2851)		1104^5	895×1104 (2851)	1634 (2851)
1104^4	1439^2 (2851)	895 (2851)		1104^{13}	2745×1634 (2851)	707 (2851)
1104^8	895^2 (2851)	2745 (2851)		1104^{29}	2683×707 (2851)	966 (2851)
1104^{16}	2745^2 (2851)	2683 (2851)		1104^{93}	1968×966 (2851)	2322 (2851)
1104^{32}	2683^2 (2851)	2565 (2851)				
1104^{64}	2565^2 (2851)	1968 (2851)		1104^{221}	1366×2322 (2851)	1540 (2851)
1104^{128}	1968^2 (2851)	1366 (2851)				

c) $221 = 2^7 + 2^6 + 2^4 + 2^3 + 2^2 + 1$ En effet : $128 + 64 + 16 + 8 + 4 + 1 = 221$

Remarque :

On obtient ainsi l'écriture de 221 en base deux.

pour obtenir l'écriture en base deux d'un nombre écrit en base 10, on divise par 2 autant de fois qu'il le faut :

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7
$221 = 2\times110 + 1$	$110 = 2\times55 + 0$	$55 = 2\times27 + 1$	$27 = 2\times13 + 1$	$13 = 2\times6 + 1$	$6 = 2\times3 + 0$	$3 = 2\times1 + 1$	
1	0	1	1	1	0	1	1

$\overline{221}^{10} = \overline{11011101}^2$

$1104^{221} = 1104^{2^7} \times 1104^{2^6} \times 1104^{2^4} \times 1104^{2^3} \times 1104^{2^2} \times 1104.$

En regroupant par 3 pour ne pas dépasser les capacités de la calculatrice :

$1104^{221} \equiv (1366\times 1968 \times 2683) \times (2745 \times 895 \times 1104) \equiv 228\times 707 \equiv 1540$ (2851)

On a au minimum 5 multiplications …

4a) Algorithme

$1104^{221} = 1104^{2^7} \times 1104^{2^6} \times 1104^{2^4} \times 1104^{2^3} \times 1104^{2^2} \times 1104.$

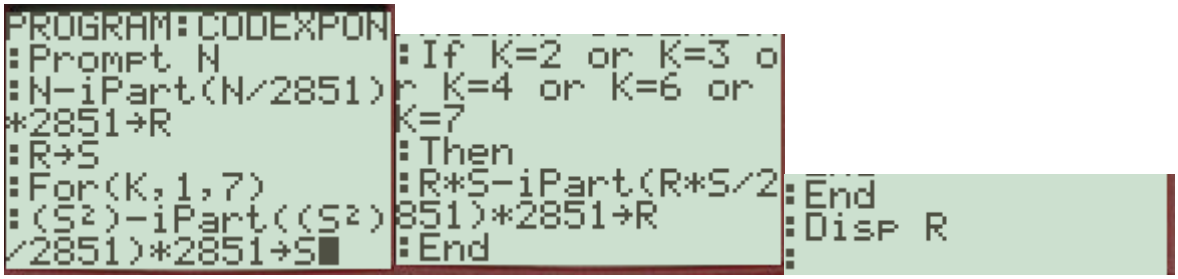
En langage naturel :

Entrer une valeur de *n*.	Entrer l'entier *n* (on veut le reste de n^{221} par 2851)
Soit la liste L = {2 ; 3 ; 4 ; 6 ; 7}	Liste des exposants de 2
Calculer le reste R de *n* par 2 851	R contient le reste de *n* par 2851
Mettre R dans S	
Pour *k* de 1 à 7	
calculer le reste S de S^2 par 2851	S contient successivement les restes de n^{2^k}
Si *k* est dans la liste L	
faire R×S et calculer le reste P par 2851	P contient les restes des produits successifs.
Remplacer R par P	
Fin si	
Fin Pour	
Afficher R	

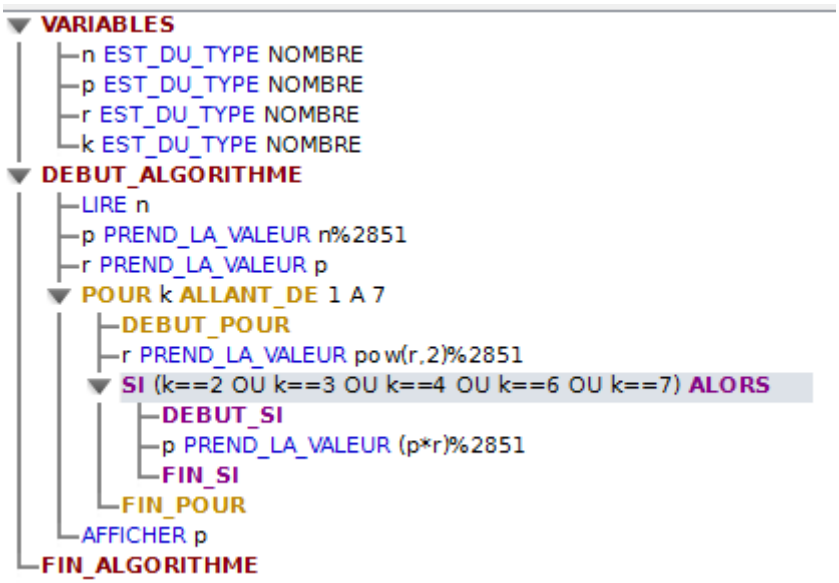
Avec Xcas

```
saisir(n);
p:=irem(n,2851);
r:=p;
L:=[2,3,4,6,7];
pour k de 1 jusque 7 faire
r:=irem(r^2,2851);
si member (k,L) <> 0 alors p:=irem (p*r,2851);
fsi;
fpour;
afficher(p):;
```

Avec la TI82



Avec Algobox



Texte	LE	SS	AN	GL	OT	SL	ON	GS	DE
	1104	1818	0013	0611	1419	1811	1413	0618	0304
codage	1540	1576	1904	2022	1204	0695	0817	1705	0200
Texte	SV	IO	LO	NS	DE	LA	UT	OM	NE
	1821	0814	1114	1318	0304	1100	2019	1412	1304
codage	0583	459	2739	2574	0200	1929	0861	0432	0511

B- Déchiffrement

1) a) 221 et 2850 sont premiers entre eux donc il existe un couple (u, v) tel que $221u + 2850v = 1$
Une solution particulière : $u = -619$ et $v = 48$
On a donc l'équation : $221u + 2850v = 221\times(-619) + 2850\times48$
ce qui se ramène à : $221(u + 619) = 2850(48 - v)$
le théorème de Gauss permet de dire qu'il existe un entier k tel que : $u + 619 = 2850k$ et en remplaçant dans l'équation : $48 - v = 221k$.
réciproquement : tout couple (u, v) tel que $u = 2850k - 619$ et $v = 48 - 221k$ avec $k \in \mathbb{Z}$ vérifie :
$221(2850k - 619) + 2850(48 - 221k) = 221\times(-619) + 2850\times48 = 1$
L'ensemble des solutions est : $\{(2850k - 619 ; v = 48 - 221k) / k \in \mathbb{Z}\}$
b) Deux entiers u diffèrent de 2 850, il existe donc un seul entier u tel que $0 \leqslant u < 2\,851$.
Lorsque $k = 1$, on a : $u = 2850 - 619 = 2231$ et $v = 48 - 221 = -173$.
D = 2231

2) On a donc : $221\times D + (-173)\times2850 = 1$, soit, puisque C = 221 : $CD = 1 + 173\times2850$
Comme $m \equiv n^C$ (2851), on a en élevant à la puissance D,
$m^D \equiv (n^C)^D$ (2851), soit : $m^D \equiv n^{CD}$ (2851)
Comme $CD = 1 + 173\times2850$, $n^{CD} = n^{1+173\times2850} = n\times n^{173\times2850} = n\times (n^{2850})^{173}$
$m^D \equiv n\times (n^{2850})^{173}$ (2851)

Le petit théorème de Fermat s'applique ici puisque 2851 est un nombre premier et que n est un entier positif inférieur à 2851.
On a donc : $n^{2851-1} = n^{2850} \equiv 1$ (2851)
En élevant à la puissance 173, il vient : $(n^{2850})^{173} \equiv 1$ (2851)
et finalement : $m^D \equiv n$ (2851)

Décomposition de D en base 2 :

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
2231= 2×1115 +1	1115 = 2×557 + 1	557 = 2×278 + 1	277 = 2×139 + 0	139 = 2×69 + 1	69 = 2×34 + 1	34 = 2×17 + 0	17 = 2×8 + 1	8 = 2×4 + 0	4 = 2×2 + 0	2 = 2×1 + 0	
1	1	1	0	1	1	0	1	0	0	0	1

$\overline{2231}^{10} = \overline{100010110111}^{2}$

Il suffit d 'aménager un des programmes en modifiant la borne supérieure de k et la liste L
par exemple dans Xcas : **L := [1, 2, 4, 5, 7, 11]** et " pour k de 1 jusque **11** faire "

```
saisir (n);
p:=irem(n,2851);
r:=p;
L:=[1,2,4,5,7,11];
pour k de 1 jusque 11 faire
  r:=irem(r^2,2851)
    si member (k,L)<>0 alors p:=irem(p*r,2851);
    fsi;
    fpour;
    afficher (p):;
```