Index

objectif bac : étudier un codage affine (bac Antilles-Guyane juin 2008)

A- **Dans toute l'activité *x* et *y* sont des entiers relatifs.**

1) Puisque $11\times(-7) - 26\times(-3) = -77 + 78 = 1$,

le couple (–7 ; –3) est bien une solution de (E) : $11x - 26y = 1$

2) On en déduit l'équation suivante :

* si $(x ; y)$ est solution de (E) alors : $11x - 26y = 11\times(-7) - 26\times(-3)$

qui mène à : $11(x + 7) = 26(y + 3)$. (E′)

Comme $x + 7$ est un entier, 11 est un diviseur du produit : $26(y + 3)$

Comme 11 et 26 sont premiers entre eux, on a, d'après le théorème de Gauss, 11 divise $y + 3$,

soit : il existe un entier relatif k tel que $y + 3 = 11k$.

En substituant dans (E′), et en divisant par 11, il vient : $x + 7 = 26k$.

Si le couple $(x ; y)$ est solution de (E) alors il s'écrit $(-7 + 26k ; -3 + 11k)$ où $k \in \mathbb{Z}$.

** Réciproquement : si $x = -7 + 26k$ et $y = -3 + 11k$ alors : $11\times(-7 + 26k) - 26\times(-3 + 11k) = 1$.

*** Conclusion :

l'ensemble des solutions de (E) est l'ensemble des couples $(x ; y) = (-7 + 26k ; -3 + 11k)$ où $k \in \mathbb{Z}$.

3) On cherche k entier tel que $0 \leqslant -7 + 26k \leqslant 25$, soit : $7 \leqslant 26k \leqslant 32$.

Le seul entier possible est donc 1.

$k = 1$, $u = -7 + 26 = 19$ et $v = -3 + 11 = 8$.

Le couple (u, v) cherché est le couple (19 ; 8). (Important pour B/2a))

B- Chaque lettre de l'alphabet est assimilée à un nombre x selon le tableau suivant :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

On code une lettre par la lettre assimilée à l'entier y compris entre 0 et 25 selon le procédé suivant :

$y \equiv 11x + 8$ (modulo 26)

1) W est assimilée à 22

$11\times22 + 8 = 240$ et $240 = 26\times9 + 16$ comme $0 \leqslant 16 \leqslant 25$, W est codé par Q.

2) a) **rappel** : on a vu au A/3) : $11\times19 - 26\times8 = 1$, soit : $11\times19 \equiv 1$ (modulo 26)

$11x - 26y = 1$ équivaut à $11x \equiv 1$ (modulo 26).

Méthode : pour résoudre une équation du type $11x \equiv j$ (modulo 26), il faut connaître au moins un entier q tel que $11q \equiv 1$ (modulo 26) de façon à ce qu'en multipliant chaque membre de l'équation par cet entier q on puisse " isoler " l'inconnue x.

Rédaction :

* Si $11x \equiv j$ (modulo 26) alors $19\times11x \equiv 19j$ (modulo 26) (compatibilité des congruences et de la multiplication)

Comme $19\times11 \equiv 1$ (modulo 26), on obtient : Si $11x \equiv j$ (modulo 26) alors $x \equiv 19j$ (modulo 26)

** Réciproquement :

Si $x \equiv 19j$ (modulo 26) alors $11x \equiv 11\times19j \equiv 1$ (modulo 26)

*** L'équivalence est donc démontrée.

b) pour décoder, on connaît y et on doit retrouver x. (entier entre 0 et 25)

Or, $y \equiv 11x + 8$ (modulo 26) qui équivaut à $11x \equiv y - 8$ (modulo 26)

en appliquant le B/2a), il vient : $x \equiv 19(y - 8)$ (modulo 26) et $0 \leqslant x \leqslant 25$.

On décode donc en prenant le numéro de la lettre codée, en retranchant 8, en multipliant par 19 et en prenant le reste dans la division euclidienne par 26.

La lettre W est assimilée à 22

$22 - 8 = 14$ et $19\times14 = 266 = 26\times10 + 6$

W est décodée par G (assimilée à 6).

---

objectif bac : déterminer les couples *(u, v) tels que au + bv = d*

1) a) Il suffit de vérifier que $239 \equiv 5$ (13) et $239 \equiv 1$ (17)

$239 = 13\times18 + 5$ et $239 = 17\times14 + 1$ ce qui prouve que 239 est une solution du système $\begin{cases} N \equiv 5 \ (13) \\ N \equiv 1 \ (17) \end{cases}$.

b) Attention : équivalence ….

* Soit N une solution du système, on a alors : $N \equiv 5$ (13) et $239 \equiv 5$ (13), d'où, par différence :

$N - 239 \equiv 0$ (13)

et, de même, $N \equiv 1\ (17)$ et $239 \equiv 1\ (17)$, d'où, $N - 239 \equiv 0\ (17)$

Si N est une solution du système, alors $N - 239 \equiv 0\ (13)$ et $N - 239 \equiv 0\ (17)$

$N - 239$ est donc un multiple de 13 et de 17

** Réciproquement :

Soit $N - 239$ un multiple de 13 et de 17, on a alors : $N - 239 \equiv 0\ (13)$, soit : $N \equiv 239 \equiv 5\ (13)$

et, de même, $N - 239 \equiv 0\ (17)$, soit : $N \equiv 239 \equiv 1\ (17)$

*** L'équivalence est démontrée.

c) Attention : équivalence ….

D'après b), N est solution du système $\begin{cases} N \equiv 5\ (13) \\ N \equiv 1\ (17) \end{cases}$ équivaut à $N - 239$ est un multiple de 13 et de 17.

*** Soit N une solution du système, on a alors : $N - 239 = 13k$ avec $k \in \mathbb{Z}$ et $N - 239 = 17k'$ avec $k' \in \mathbb{Z}$.

On en déduit : $13k = 17k'$.

Comme 13 et 17 sont premiers entre eux, on a d'après le théorème de Gauss : k' est un multiple de 13, d'où, il existe un entier q tel que $13k = 17 \times 13 \times q$

On obtient : $N - 239 = 13k = 17 \times 13 \times q$

Comme $17 \times 13 = 221$ et $239 = 221 + 18$, il vient : $N - 18 \equiv 0\ (221)$, soit : $N \equiv 18\ (221)$

*** Réciproquement :

soit $N \equiv 18\ (221)$, c'est-à-dire : $N = 18 + 221q$ où $q \in \mathbb{Z}$.

$N - 239 = -221 + 211q = 13(-17 + 17q)$ et donc, $N - 239$ est un multiple de 13.

$N - 239 = -221 + 211q = 17(-13 + 13q)$ et donc, $N - 239$ est un multiple de 17.

D'après l'équivalence du 2b/, N est solution du système.

*** L'équivalence : $N \equiv 18\ (221) \Leftrightarrow \begin{cases} N \equiv 5\ (13) \\ N \equiv 1\ (17) \end{cases}$ est démontrée.

2) a) Un algorithme :

Initialisation : k prend la valeur 1

n prend la valeur 10

Traitement : Tant que reste $(n\ ;\ 17) \neq 1$

Affecter $k + 1$ à k

Affecter $10n$ à n

Fin TantQue

Sortie : Afficher k

Analyse de l'algorithme :

k est un compteur … lorsqu'on va afficher k, le reste de n par 17 est 1 (sortie de boucle).

À chaque boucle, on multiplie n par 10, et, à la première boucle, on a : $n = 10$

La variable n contient donc les puissances de 10 (ici : 10^k)

Départ : $k = 1$, $n = 10$

Premier passage : 10 divisé par 17 reste 10, la boucle est effectuée

$k = 2$, $n = 10^2$

Deuxième passage : 10^2 divisé par 17 reste 15, la boucle est effectuée

$k = 3$, $n = 10^3$

…....

Dernier passage : 10^{15} divisé par 17 reste différent de 1, la boucle est effectuée

$k = 16$, $n = 10^{16}$

Comme le " Tant que " n'est pas réalisé, cela signifie que $10^{16} \equiv 1\ (17)$

16 est le plus petit entier tel que $10^k \equiv 1\ (17)$

b) $10^l \equiv 18\ (221) \Leftrightarrow \begin{cases} 10^l \equiv 5\ (13) \\ 10^l \equiv 1\ (17) \end{cases}$

D'après 2a), on sait que l est un entier multiple de 16 puisqu'on a :

$10^{16} \equiv 1\ (17)$,

écrivons $l = 16 + m$, $10^{16+m} = 10^{16} \times 10^m$, d'où, $10^{16+m} \equiv 10^m\ (17)$

Il reste donc à étudier $10^l \equiv 5\ (13)$

Remarquer : on établit un cycle de restes … dès qu'un reste est 1 …

Exposant *l*	**1**	**2**	**3**	**4**	**5**	**6**
Puissances de 10	10	100	1000	10000	100000	1000000
		$100 = 13\times7 + 9$	$1000 = 10\times100$, on étudie : $10\times9 = 90 = 13\times6 + 12$	$10000 = 100\times100$ on étudie : $9\times9 = 81$ $13\times6 + 3$	$100000 = 10\times10000$ on étudie : $10\times3 = 30$	10000×100 on étudie : $3\times9 = 27$
Restes dans la division par 13	10	9	12	3	4	1

On n'aura jamais un reste égal à 5.

Il n'existe pas d'entier l tel que $10^l \equiv 18\ (221)$

Problème 1 page 94 Clé du relevé d'identité bancaire (RIB)

1) R = 17515 90000 04243246509 87

$R = 1715\times10^{18} + 90000\times10^{13} + 04243246509\times10^2 + 87$

$R = B\times10^{18} + G\times10^{13} + C\times10^{2} + K$

b) $10^2 = 97 + 3$, d'où, $10^2 \equiv 3\ (97)$

on peut rapidement étudier quelques puissances de 10, $10^3 \equiv 30\ 97)$,

comme $10^4 = (10^2)^2$, $10^4 \equiv 9\ (97)$, $10^5 \equiv 27\ (97)$

comme $10^6 = 10^4 \times 10^2$, $10^6 \equiv 27\ (97)$, etc ...

puis, $10^{13} = (10^2)^6 \times 10$, d'où, $10^{13} \equiv 3^6 \times 10\ (97)$

comme $3^6 = 243\times3$ et $243 = 2\times97 + 49$, $49\times3 = 147 = 97 + 50$

on a : $10^{13} \equiv 50\times10\ (97)$ et $500 = 5\times97 + 15$, soit : $10^{13} \equiv 15\ (97)$

et, $10^{18} = (10^2)^9$ d'où, $10^{18} \equiv 3^9\ (97)$ comme $3^9 = 3^6 \times 3^3$, $3^9 \equiv 50\times27\ (97)$,

soit : $3^9 = 1350 = 97\times13 + 89$

$10^{18} \equiv 89\ (97)$

On a donc : $R \equiv B\times89 + G\times15 + C\times3 + K\ (97)$

Or, R est divisible par 97, donc : $R \equiv 97\ (97)$

Conclusion : $K \equiv 97 - 89\times G - 15\times C - 3\times C\ (97)$

Supposons deux clés différentes K et K′,

on a : $K \equiv 97 - 89\times G - 15\times C - 3\times C\ (97)$ et $K' \equiv 97 - 89\times G - 15\times C - 3\times C\ (97)$

c'est-à-dire : $K \equiv K'(97)$

La clé est unique puisque la différence de deux entiers congrus modulo 97 est un multiple de 97.

Comme $1 \leqslant K \leqslant 97$ et $1 \leqslant K' \leqslant 97$ alors $-96 \leqslant K - K' \leqslant 96$.

Le seul multiple de 97 dans [–96 ; 96] est 0.

Conclusion : K = K′, K est unique.

c) $89\times1715 \equiv 45\ (97)$, $15\times90000 \equiv 51\ (97)$, $4243246509\times3 \equiv 11\ (97)$

$K \equiv 97 - 45 - 51 - 11\ (97)$ $97 - 45 - 51 - 11 = -10$ et $-10 = 87 - 97$

$K \equiv 87\ (97)$

2) On suppose une erreur sur un seul chiffre. On a donc deux nombres R et R′.

$R' > R$

a) Les nombres R et R′ sont de la forme :

$R = r_{22}\times10^{22} + r_{21}\times10^{21} + \ldots + r_1\times10 + r_0 = \sum_{i=0}^{i=22} r_i\times10^i$ avec r_i entier et $0 \leqslant r_i \leqslant 9$.

$R' = r'_{22}\times10^{22} + r'_{21}\times10^{21} + \ldots + r'_1\times10 + r'_0 = \sum_{i=0}^{i=22} r'_i\times10^i$ avec r'_i entier $0 \leqslant r'_i \leqslant 9$.

Il existe un et un seul rang *n* tel que $r_n \neq r'_n$, pour $i \neq n$, $r_i = r'_i$, d'où, $R' - R = r_n \times10^n$ et *n* entier compris entre 0 et 22.

b) Par définition de la clé, R et R′ sont des multiples de 97, donc, si la clé ne détecte pas l'erreur, cela signifie que R′ – R est un multiple de 97.

97 étant un nombre premier, $r_n \times 10^n$ n'est pas divisible par 97 puisque ni r_n, ni 10 ne sont divisibles par 97.

La clé permet donc de détecter toute erreur sur un seul chiffre.

c) La clé ne permet pas de détecter une erreur où la différence R′ – R est un multiple de 97.

par exemple : R = 17515 90000 042432**465**09 87 et R′ = 17515 90000 042432**562**09 87 ont la même clé, puisque $R' - R = 97 \times 10^4$.

Problème 2 page 94 chiffrement et déchiffrement

Voir le problème 5 de la page 17 dans le chapitre 1

1) Clé (5 ; 22)

La lettre M est associée à l'entier 12

$y = 5 \times 12 + 22 = 82$ et $82 = 26 \times 3 + 4$
le reste $c(x) = 4$. La lettre associée à 4 est E
M est codé par E.

2) Clé (7 ; 23)
Le mot codé est XYYMZKSMZ
a) Par définition du chiffrement affine de clé (7 ; 23), on a : $y \equiv 7x + 23$ (26)
Comme $23 \equiv -3$ (26), on a : $y + 3 \equiv 7x$ (26)

b) 7 et 26 étant premiers entre eux, il existe deux entiers u et v' tels que $7u + 26v' = 1$
En posant $v' = -v$, $7u - 26v = 1$

c) Recherche d'un couple (u_0, v_0) solution de l'équation du 2/b).
On peut utiliser l'algorithme d'Euclide :
$26 = 7 \times 3 + 5$ (Soit : $5 = 26 - 7 \times 3$)
$7 = 5 \times 1 + 2$ (soit : $2 = 7 - 5 \times 1 = 7 - 26 + 7 \times 3 = 7 \times 4 - 26$)
$5 = 2 \times 2 + 1$, donc : $1 = 5 - 2 \times 2 = 26 - 7 \times 3 - (7 \times 4 - 26) \times 2 = 26 \times 3 - 11 \times 7$
On peut prendre $u_0 = -11$ et $v_0 = -3$
(On peut trouver une infinité de couples :
autres couples possibles $(-11 + 26k ; -3 + 7k)$ (Application du théorème de Gauss))

d) Puisque $7u_0 - 26v_0 = 1$, on a : $7u_0 \equiv 1$ (26)
L'équation du 2a) est : $7x \equiv y + 3$ (26)
on multiplie les deux membres de la congruence par u_0,
d'où : $7u_0x \equiv u_0(y + 3)$ (26) et comme $7u_0 \equiv 1$ (26), il vient : $x \equiv u_0 y + 3u_0$ (26)
$u_0 = -11$ et $-33 \equiv 19$ (26)
par conséquent : $x \equiv -11y + 19$ (26)
D'autre part, par définition du chiffrement affine, $y \equiv c(x)$ (26)

e) Le déchiffrement du texte s'obtient avec la clé (–11, 19) (Remarque : (15 ; 19) convient aussi ...)
Le mot décodé : APPRENDRE

3) Dès que a est premier avec 26, **il existe un couple (u_0, v_0) solution de l'équation $au - 26v = 1$**

En multipliant les deux membres de la congruence : $y \equiv ax + b$ (26) par u_0, on obtient :
$u_0\, y \equiv x + bu_0$ (26), soit : $x \equiv u_0\, y - bu_0$ (26)
Le déchiffrement est donc obtenu avec la clé $(u_0, -bu_0)$
Retenir :
Résoudre une équation de la forme $ax \equiv c$ (d)
Lorsque a et d sont premiers entre eux, il existe un couple (u, v) d'entiers tels que $u\, a + v\, d = 1$,
d'où, $u\, a \equiv 1$ (d)
En multipliant chaque membre de l'équation $ax \equiv c$ (d) par u, il vient : $x \equiv cu$ (d) (la multiplication est associative et commutative).

Problème 4 page 96 Chiffrement de Hill (1891- 1961)

Les lettres de l'alphabet sont codées de 0 à 25, mais, le codage est fait par blocs.

Ici, on code par blocs de deux lettres .

Un couple d'entiers $(x ; y)$ est codé par un couple $(x' ; y')$ où $\begin{cases} x' \equiv ax+b \,(mod\ 26) \\ y' \equiv cx+d \,(mod\ 26) \end{cases}$

a, b, c, d sont des entiers (clé du chiffrement).

A- Exemples de chiffrement :
Chiffrement de ETUDIER
On partage le mot en bloc de deux lettres :

si le nombre de lettres est impair, on complète au hasard le dernier bloc.

ET-UD-IE-R*A*

1) $a = -5$, $b = 8$, $c = -2$, $d = 3$.

a) b) c)

Le chiffrement du mot ET-UD-IE-R est CX-CV-SW-T

Le premier E est chiffré par C et le deuxième par W.

L'analyse fréquentielle est donc rendue beaucoup plus difficile …

	A	B	C	D	E	F	G	H	I
1	Clé	a =	6	b =	7	c =	-8	d =	5
2									
3	Texte en clair	E	T	U	D	I	E	R	A
4	u, v	4	19	20	3	8	4	17	0
5	x, y	157	63	141	-145	76	-44	102	-136
6	Nombres entre 0 et 25	1	11	11	11	24	8	24	20
7	Texte chiffré	B	L	L	L	Y	I	Y	U

Le couple de lettres (U ; D)est codé par (L ; L).

B- À la recherche de deux peintres

1) Clé de codage : $a = 3$, $b = 5$, $c = 4$ et $d = 7$.

Nom codé : KTCEMAHS

a) $\begin{cases} x' = 3x + 5y \\ y' = 4x + 7y \end{cases}$ équivaut à $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$

b) Soit A = $\begin{pmatrix} 3 & 5 \\ 4 & 7 \end{pmatrix}$. Le déterminant de A vaut : $3\times7 - 4\times5 = 1$.

comme dét(A) ≠ 0, la matrice A est inversible et $A^{-1} = \frac{1}{dét(A)} \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix}$

On a donc : $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$

c) Décodage de KTCEMAHS

Clé de décodage		$a = 7$	$b = -5$		$c = -4$		$d = 3$	
Texte codé	K	T	C	E	M	A	H	S
x' ; y'	10	19	2	4	12	0	7	18
x ; y	1	17	20	4	6	4	11	0
Texte décodé	B	R	U	E	G	E	L	A
Nom du peintre	BRUEGEL (tableau : *La Tour de Babel* (1563))							

Pieter Brueghel ou Bruegel dit l'Ancien est un peintre brabançon né à Bruegel (près de Bréda) vers 1525 et mort le 9 septembre 1569 à Bruxelles.

$\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 10 \\ 19 \end{pmatrix} = \begin{pmatrix} -25 \\ 17 \end{pmatrix}$ et $-25 \equiv 1\ (26)$ $\quad$ $\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} -6 \\ 4 \end{pmatrix}$ et $-6 \equiv 20\ (26)$

$\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 84 \\ -48 \end{pmatrix}$ et $84 = 3\times26 + 6$, $-48 = 2\times52 + 4$;

$\begin{pmatrix} 7 & -5 \\ -4 & 3 \end{pmatrix} \begin{pmatrix} 7 \\ 18 \end{pmatrix} = \begin{pmatrix} -41 \\ 26 \end{pmatrix}$ et $-41 \equiv 11\ (26)$; $26 \equiv 0\ (26)$

La dernière lettre S du chiffrement correspond à la lettre A, rajoutée au nom pour avoir un nombre pair de lettres. Le chiffrement de Hill porte sur des couples de lettres. Si on supprime le S, ou si on remplace cette lettre par une autre, on ne retrouve pas la terminaison L du nom.

2. Nom codé : JPXH clé de codage : 3 ; 2 ; 5 ; 7.

a.La matrice de codage est A = $\begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix}$. Elle est inversible puisque det(A) = 11 ≠ 0.

La matrice inverse est $A^{-1} = \frac{1}{11} \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$

En posant $\begin{pmatrix} x \\ y \end{pmatrix} = A^{-1} \begin{pmatrix} x' \\ y' \end{pmatrix}$, alors, si x' et y' sont des entiers alors x et y ne sont pas entiers.

On ne peut pas décoder avec cette matrice.

b) Recherche d'un couple (u, v) solution de : $11u - 26v = 1$

$26 = 11\times2 + 4$

$11 = 4\times2 + 3$

$4 = 3 + 1$,

d'où, $1 = 4 - 3 = 4 - (11 - 4\times2) = 3\times4 - 11 = 3\times(26 - 2\times11) - 11 = -7\times11 - (-3)\times26$

$u = -7$ et $v = -3$

c) $11u - 26v = 1$ mène à $11u \equiv 1\ (26)$

-7 est l'inverse de 11 modulo 26.

d) Soit $B = 11\times A^{-1} = \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$, d'où, uB.A $= u \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 5 & 7 \end{pmatrix} = u \begin{pmatrix} 11 & 0 \\ 0 & 11 \end{pmatrix} = \begin{pmatrix} 11u & 0 \\ 0 & 11u \end{pmatrix}$

Comme $11u \equiv 1\ (26)$, on a : uB.A $\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (modulo 26)

uBA $\equiv 1\times I_2\ (26)$

e) On a : $\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$

On multiplie les deux membres de l'égalité à gauche par uB, d'où, uB $\begin{pmatrix} x' \\ y' \end{pmatrix} = u$BA $\begin{pmatrix} x \\ y \end{pmatrix}$

soit, par congruence modulo 26, uB $\begin{pmatrix} x' \\ y' \end{pmatrix} \equiv \begin{pmatrix} x \\ y \end{pmatrix}$ (modulo 26).

Comme $u = -7$ et $B = \begin{pmatrix} 7 & -2 \\ -5 & 3 \end{pmatrix}$, on a : uB $= \begin{pmatrix} -49 & 14 \\ 35 & -21 \end{pmatrix}$ et,

par congruence modulo 26, uB $\equiv \begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix}\ (26)$

On en déduit : $\begin{cases} x = 3x' + 14y' \\ y = 9x' + 5y' \end{cases}$

f) Décodage :

JP est codé par : 9 ; 15, $\begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} \begin{pmatrix} 9 \\ 15 \end{pmatrix} = \begin{pmatrix} 237 \\ 156 \end{pmatrix} \equiv \begin{pmatrix} 3 \\ 0 \end{pmatrix}\ (26)$. JP est décodé par DA

XH est codé par : 23 ; 7 , $\begin{pmatrix} 3 & 14 \\ 9 & 5 \end{pmatrix} \begin{pmatrix} 23 \\ 7 \end{pmatrix} = \begin{pmatrix} 167 \\ 242 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 8 \end{pmatrix}\ (26)$. XH est décodé par LI

Le nom du peintre est : DALI.

Salvador Dalí Domènech (Figueras 1904 – 1989),(Tableau : Plage d'El llane à Cadaquès (1921))

3) Soit le déterminant d de la matrice A.

$du - 26v = 1$ si et seulement si d et u sont premiers entre eux.

À la question A.2, la matrice $A = \begin{pmatrix} 6 & 7 \\ -8 & 5 \end{pmatrix}$ a pour déterminant $d = 86$

86 et 26 ne sont pas premiers entre eux.

Le codage du couple (U, D) a donné (L, L) : soit (11, 11).

Si on veut décoder, on cherche x et y solutions de : $\begin{cases} 6x+7y=11 \\ -8x+5y=11 \end{cases}$, soit : $\begin{cases} 30x+35y=55 \\ -56x+35y=77 \end{cases}$,

$86x = -22$. $8x \equiv 4\ (26)$ qui n'a pas de solutions.

Table de multiplication des congruences modulo 26 :

	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	AA
1		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
2	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0
3	2	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24	0
4	3	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23	0
5	4	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22	0
6	5	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21	0
7	6	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20	0
8	7	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	0
9	8	8	16	24	6	14	22	4	12	20	2	10	18	0	8	16	24	6	14	22	4	12	20	2	10	18	0
10	9	9	18	1	10	19	2	11	20	3	12	21	4	13	22	5	14	23	6	15	24	7	16	25	8	17	0
11	10	10	20	4	14	24	8	18	2	12	22	6	16	0	10	20	4	14	24	8	18	2	12	22	6	16	0
12	11	11	22	7	18	3	14	25	10	21	6	17	2	13	24	9	20	5	16	1	12	23	8	19	4	15	0
13	12	12	24	10	22	8	20	6	18	4	16	2	14	0	12	24	10	22	8	20	6	18	4	16	2	14	0
14	13	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0	13	0
15	14	14	2	16	4	18	6	20	8	22	10	24	12	0	14	2	16	4	18	6	20	8	22	10	24	12	0
16	15	15	4	19	8	23	12	1	16	5	20	9	24	13	2	17	6	21	10	25	14	3	18	7	22	11	0
17	16	16	6	22	12	2	18	8	24	14	4	20	10	0	16	6	22	12	2	18	8	24	14	4	20	10	0
18	17	17	8	25	16	7	24	15	6	23	14	5	22	13	4	21	12	3	20	11	2	19	10	1	18	9	0
19	18	18	10	2	20	12	4	22	14	6	24	16	8	0	18	10	2	20	12	4	22	14	6	24	16	8	0
20	19	19	12	5	24	17	10	3	22	15	8	1	20	13	6	25	18	11	4	23	16	9	2	21	14	7	0
21	20	20	14	8	2	22	16	10	4	24	18	12	6	0	20	14	8	2	22	16	10	4	24	18	12	6	0
22	21	21	16	11	6	1	22	17	12	7	2	23	18	13	8	3	24	19	14	9	4	25	20	15	10	5	0
23	22	22	18	14	10	6	2	24	20	16	12	8	4	0	22	18	14	10	6	2	24	20	16	12	8	4	0
24	23	23	20	17	14	11	8	5	2	25	22	19	16	13	10	7	4	1	24	21	18	15	12	9	6	3	0
25	24	24	22	20	18	16	14	12	10	8	6	4	2	0	24	22	20	18	16	14	12	10	8	6	4	2	0
26	25	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
27	26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Les éléments ayant un inverse modulo 26, apparaissent lorsque le produit est égal à 1

Problème 5 page 98 Le système RSA

RSA : du nom des inventeurs Rivest, Shamir, Adleman en 1977

Principe : La clé publique consiste en la donnée d'un entier pq obtenu par le produit de deux nombres premiers p et q, et, d'un exposant c qui est un entier naturel premier avec l'entier $n = (p-1)(q-1)$.

Le chiffrement est obtenu en calculant $b \equiv a^c \pmod{pq}$ et $0 \leqslant a < pq$.

Pour déchiffrer b, on cherche l'entier d tel que $cd \equiv 1 \pmod{n}$, et, on sait que $a = b^d \pmod{pq}$.

Le déchiffrement est rendu difficile, car on ne connaît pas p et q, et on ne connaît donc pas l'entier n permettant de calculer d.

A- Un exemple

$p = 5$, $q = 19$ et $c = 61$ (La clé publique est : (95, 61)

1) le nombre $n = 4 \times 18 = 72$ est premier avec 61.

2) Codage de $a = 3$

$b \equiv 3^{61} \pmod{95}$ et $0 \leqslant b < 95$

***b* = 78** (Pour déterminer ce nombre à la main, on cherche les congruences modulo 95 des premières puissances ….)

$3^5 = 243$ et $243 = 2 \times 95 + 53$

$3^6 \equiv 53 \times 3\ (95)$ $159 = 95 + 64$

$3^7 \equiv 64 \times 3\ (95)$ $192 = 2 \times 95 + 2$

Comme $61 = 7 \times 8 + 5$, on a : $3^{61} = (3^7)^8 \times 3^5$, d'où, $3^{61} \equiv 2^8 \times 53\ (95)$

$2^8 \times 53 = 256 \times 53$ (95) $\quad 256 = 2 \times 95 + 66$
$66 \times 53 = 3\,498 \quad 3\,498 = 36 \times 95 + 78$
D'où, $3^{61} \equiv 78$ (95)

3a) Résolution de l'équation diophantienne $61x - ny = 1$.
($n = 72$) L'existence de solutions est assurée par le ***théorème de Bézout***.
Algorithme d'Euclide
$72 = 1 \times 61 + 11$
$61 = 5 \times 11 + 6$
$11 = 1 \times 6 + 5$
$6 = 1 \times 5 + 1$
d 'où : $1 = 6 - 5 = (61 - 5 \times 11) - (11 - 1 \times (61 - 5 \times 11)) = 2 \times 61 - 11 \times 11 = 2 \times 61 - 11 \times (72 - 1 \times 61)$
$1 = 13 \times 61 - 11 \times 72$
$x = 13$ et $y = 11$ conviennent.
Théorème de Gauss
$61x - 72y = 61 \times 13 - 11 \times 72$ équivaut à $61(x - 13) = 72(y - 11)$
Comme 61 divise le produit $72(y - 11)$ et que 61 est premier avec 72 , 61 divise $y - 11$.
On a alors : $y = 11 + 61k$, $k \in \mathbb{Z}$, puis : $61(x - 13) = 72 \times 61k$: soit : $x = 13 + 72k$
Comme : $61(13 + 72k) - 72(11 + 61k) = 61 \times 13 - 72 \times 11 = 1$,
les solutions de l'équation $61x - 72y = 1$ sont les couples $(13 + 72k ; 11 + 61k)$ avec $k \in \mathbb{Z}$.

b) $61x - ny = 1$ mène à $61x \equiv 1 \pmod{n}$,
d'où, $61 \times 13 \equiv 1$ (72).
Comme $0 \leqslant 13 < 72$, le nombre d permettant le décodage est 13.

c) $b = 78$ et $d = 13$,
on cherche 78^{13} modulo 95.
$78^2 = 6084$ et $6084 = 64 \times 95 + 4$
Comme $13 = 2 \times 6 + 1$, on a : $78^{13} = (78^2)^6 \times 78$
$78^{13} \equiv 4^6 \times 78$ (95) $\quad 4^6 = 4096$ et $4096 = 43 \times 95 + 11$
$78^{13} \equiv 11 \times 78$ (95) $\quad 11 \times 78 = 858$ et $858 = 9 \times 95 + 3$
$78^{13} \equiv 3$ (95)
On retrouve le nombre a.
B- Une justification
p et q sont ***deux nombres premiers*** et c est un entier naturel ***premier avec*** $n = (p - 1)(q - 1)$.
$a \in \mathbb{N}$ et $b \equiv a^c \pmod{pq}$.
1 a) Soit l'équation diophantienne $cx - ny = 1$.
L'existence de solutions est assurée par le ***théorème de Bézout***.
Notons $(x_0 ; y_0)$ l'une des solutions.

Théorème de Gauss
On a : $cx - ny = 1$ et $cx_0 - ny_0 = 1$
$cx - ny = cx_0 - ny_0$ équivaut à $c(x - x_0) = n(y - y_0)$
Comme c divise le produit $n(y - y_0)$ et que c est premier avec n , c divise $y - y_0$.
On a alors : $y = y_0 + ck$, $k \in \mathbb{Z}$, puis : $c(x - x_0) = n \times ck$: soit : $x = x_0 + nk$
Comme : $c(x_0 + nk) - n(y_0 + ck) = cx_0 - ny_0 = 1$,
les solutions de l'équation $cx - ny = 1$ sont les couples $(x_0 + nk ; y_0 + ck)$ avec $k \in \mathbb{Z}$.
b) On cherche parmi les solutions de la forme $x_0 + nk$ celle qui vérifie $0 \leqslant x_0 + nk < n$.

on a successivement : $-x_0 \leqslant nk < -x_0 + n$, puis : $\frac{-x_0}{n} \leqslant k < \frac{-x_0}{n} + 1$

Soit $\alpha = -\frac{x_0}{n}$, le seul entier k_d vérifiant $\alpha \leqslant k_d < \alpha + 1$ (intervalle de longueur 1)

permet de déterminer l'unique entier d tel que $0 \leqslant d < n$. En ce cas, $y_d = y_0 + ck_d$

Puis, comme $cd - ny_d = 1$, on a : $cd \equiv 1 \pmod n$.

2) **petit théorème de Fermat** :

Énoncé :

Si p est premier et a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \pmod p$.

En prenant a non divisible par p et par q, le petit théorème de Fermat s'applique, d'où,
$a^{p-1} \equiv 1 \pmod p$.
En élevant à la puissance $q-1$ les deux membres de la congruence : $\left(a^{p-1}\right)^{q-1} \equiv 1^{q-1} \ (p)$
soit : $a^{(p-1)(q-1)} \equiv 1 \ (p)$

et,
$a^{q-1} \equiv 1 \pmod q$.
En élevant à la puissance $p-1$ les deux membres de la congruence : $\left(a^{q-1}\right)^{p-1} \equiv 1^{p-1} \ (q)$
soit : $a^{(p-1)(q-1)} \equiv 1 \ (q)$.

$a^{(p-1)(q-1)} \equiv 1 \ (p)$ implique qu'il existe un entier k tel que $a^{(p-1)(q-1)} = 1 + kp$.
$a^{(p-1)(q-1)} \equiv 1 \ (q)$ implique qu'il existe un entier k' tel que $a^{(p-1)(q-1)} = 1 + k'q$.
Par différence (ou par comparaison des deux égalités), il vient : $kp = k'q$.
Comme q divise $k'p$ et que q est premier avec p, d'après le ***théorème de Gauss***, q divise k.
Il existe donc un entier k'' tel que $qk'' = k$.
On obtient : $a^{(p-1)(q-1)} = 1 + kp = 1 + k''pq$.
Conclusion : $\left(a^{p-1}\right)^{q-1} \equiv 1^{q-1} \ (pq)$ Comme $n = (p-1)(q-1)$, on a : $a^n \equiv 1 \ (pq)$

b) Soit un entier $k = 1 + mn$.
$a^k = a^{1+mn} = a \times \left(a^n\right)^m$ Or, $a^n \equiv 1 \ (pq)$, d'où, par produit des congruences, $a^k \equiv a \ (pq)$.

3) On cherche $b^d \pmod{pq}$.
Par définition : $b \equiv a^c \pmod{pq}$ En élevant à la puissance d,
$b^d \equiv \left(a^c\right)^d \pmod{pq}$
$b^d \equiv a^{cd} \pmod{pq}$
D'après 1b), $cd = 1 + mn$ avec m entier.
$b^d \equiv a^{1+mn} \pmod{pq}$
D'après 2b), $a^{1+mn} \equiv a \pmod{pq}$
Par transitivité de la congruence : $b^d \equiv a \pmod{pq}$

---

6 page 101

Soit d un diviseur commun de a et de b.

Les deux premières questions sont l'application de la propriété :

Si d divise a et b alors d divise toute combinaison linéaire à coefficients entiers de a et b.

On peut redémontrer cette propriété :

1) $d \mid a$, il existe un entier q tel que $a = dq$.

$d \mid b$, il existe un entier q' tel que $b = dq'$.

$4a + 3b = 4dq + 3dq' = d(4q + 3q')$

Comme q et q' sont entiers, $4q + 3q'$ est un entier q''.

Conclusion : $4a + 3b = dq''$ avec $q'' \in \mathbb{Z}$, ce qui prouve que d divise $4a + 3b$

De même : $5a + 4b = dq'''$ avec $q''' \in \mathbb{Z}$, ce qui prouve que d divise $5a + 4b$

2) Réciproquement, soit d un diviseur commun à $4a + 3b$ et $5a + 4b$

il existe deux entiers q et q' tels que : $4a + 3b = dq$ et $5a + 4b = dq'$

On en déduit : $-5(4a + 3b) + 4(5a + 4b) = -5dq + 4dq' = d(-5q + 4q')$, soit : $b = d(-5q + 4q')$

et $4(4a + 3b) - 3(5a + 4b) = 4dq - 3dq' = d(4q - 3q')$, soit : $a = d(4q - 3q')$

d divise a et b.

3) D'après l'équivalence démontrée en 1) et 2) :

d divise a et b si et seulement si d divise $4a + 3b$ et $5a + 4b$,

l'ensemble des diviseurs communs $\mathcal{D}(a,b)$ est égal à l'ensemble des diviseurs communs $\mathcal{D}(4a+3b,5a+4b)$.

Ces deux ensembles ont le même plus grand élément : PGCD(a, b) = PGCD($4a + 3b$; $5a + 4b$).

---

9 page 101

a) le PGCD de n et $n + 1$ est 1.

En effet, d étant un diviseur de n et $n + 1$, divis $(n + 1) - n = 1$

Par conséquent : $d = 1$.

b) le PGCD de $2n$ et $2(n + 1)$ est 2.

En effet, d étant un diviseur de $2n$ et $2(n + 1)$, divis $2(n + 1) - 2n = 2$

Par conséquent : $d = 1$ ou $d = 2$.

Comme $2 \mid 2n$ et $2 \mid 2(n + 1)$ alors le PGCD de $2n$ et $2(n + 1)$ est 2.

c) le PGCD de $2n + 1$ et $2n + 3$ est 1.

En effet, d étant un diviseur de $2n + 1$ et $2n + 3$, divis $2n + 3 - (2n + 1) = 2$

Par conséquent : $d = 1$ ou $d = 2$.

2 est impossible, d'où, $d = 1$

---

10 page 101

PGCD de A et B lorsque :

a) $A = 3n^2 + n$ et $B = 3n^2$

Si $n = 0$, $A = 0$ et $B = 0$, il n'y a pas de PGCD.

Si $n \neq 0$, alors, d divise $3n^2 + n$ et $3n^2$, donc, d divise $3n^2 + n - 3n^2 = n$.

Les diviseurs de A et B sont des diviseurs de n.

Comme n divise $3n^2 + n$ et $3n^2$, PGCD(A, B) = n.

Remarque : PGCD($3n^2 + n$, $3n^2$) = PGCD(n, $3n^2$) = n puisque $3n^2$ est un multiple de n.

b) $A = 3n^2 + 2n$ et $B = 2n^2 + n$

Si $n = 0$, $A = 0$ et $B = 0$, il n'y a pas de PGCD.

Si $n \neq 0$,

méthode des soustractions successives :

PGCD($3n^2 + 2n$, $2n^2 + n$) = PGCD($2n^2 + n$, $n^2 + n$) = PGCD($n^2 + n$, n^2) = PGCD(n^2 , n) = n puisque n^2 est un multiple de n.

---

26 page 102

$x^2 - y^2 = 5\,440$ et PGCD(x ; y) = 8

On peut remarquer que si (x ; y) est solution alors ($-x$; y), (x ; $-y$), ($-x$; $-y$) sont solutions.

On peut limiter la recherche aux nombres positifs. (Sinon ne pas oublier les opposés lors de la recherche des diviseurs).

On a donc : $x = 8q$, $y = 8q'$ avec q et q' premiers entre eux.

$64q^2 - 64q'^2 = 5\,440$, soit : $q^2 - q'^2 = 85$

$(q - q')(q + q') = 85$ Les paires d'entiers positifs diviseurs de 85 sont {1 ; 85} et {5 ; 17}.

$q + q' = 1$ est impossible. En choisissant q et q' positifs, $q - q' < q + q'$

$\begin{cases} q-q'=1 \\ q+q'=85 \end{cases} \Leftrightarrow \begin{cases} 2q=86 \\ q'=q-1 \end{cases} \Leftrightarrow \begin{cases} q=43 \\ q'=42 \end{cases}$ (q et q' sont premiers entre eux).

$\begin{cases} q-q'=5 \\ q+q'=17 \end{cases} \Leftrightarrow \begin{cases} 2q=22 \\ q'=q-5 \end{cases} \Leftrightarrow \begin{cases} q=11 \\ q'=6 \end{cases}$ (q et q' sont premiers entre eux).

Les couples solutions sont :
(344 ; 336), (–344 ; 336), (344 ; –336), (–344 ; -336),
(88 ; 48), (–88 ; 48), (88 ; –48), (–88 ; –48).

---

27 page 102 irréductible

a et b sont deux entiers naturels non nuls.

1) On pose : $\dfrac{3a+4b}{5a+7b}$ est une fraction irréductible.

Avec le théorème de Bézout :

On a donc : $3a + 4b$ et $5a + 7b$ premiers entre eux.

il existe deux entiers u et v tels que $(3a + 4b)u + (5a + 7b)v = 1$

En développant, puis, en factorisant a et b, il vient : $a(3u + 5v) + b(4u + 7v) = 1$.

Comme $3u + 5v$ et $4u + 7v$ sont entiers, a et b sont premiers entre eux.

Autre méthode (en cherchant les diviseurs communs).

Soit d un diviseur positif commun à a et à b.

d divise toute combinaison linéaire à coefficients entiers de a et b , donc, d divise $3a + 4b$ et $5a + 7b$

Comme $3a + 4b$ et $5a + 7b$ sont premiers entre eux, le seul diviseur positif est 1.

Conclusion : a et b sont premiers entre eux.

Avec la contraposée :

Énoncé de la contraposée : Si $\frac{a}{b}$ n'est pas irréductible alors $\frac{3a+4b}{5a+7b}$ n'est pas irréductible.

Soit d un diviseur supérieur à 1 commun à a et à b.
d divise toute combinaison linéaire à coefficients entiers de a et b , donc, d divise $3a + 4b$ et $5a + 7b$
d est donc un diviseur supérieur à 1 commun à $3a + 4b$ et $5a + 7b$
$\frac{3a+4b}{5a+7b}$ n'est pas irréductible.

2) On pose : $\frac{3a+4b}{5a+7b}$ n'est pas une fraction irréductible.
Il existe donc un entier d supérieur à 1 tel que d divise $3a + 4b$ et $5a + 7b$
d divise alors : $7(3a + 4b) – 4(5a + 7b) = a$ et divise $3(5a + 7b) – 5(3a + 4b) = b$.
d est un diviseur commun à a et à b supérieur à 1, la fraction $\frac{a}{b}$ n'est pas irréductible.

---

28 page 102 Vrai-faux

" Si a, b, c sont des entiers supérieurs à 1, si PGCD(a ; b) = c alors PGCD(a^2 ; b^2) = c^2 "

La proposition est vraie

Preuve :

Soit PGCD(a ; b) = c

on peut écrire $a = ca'$ et $b = cb'$ avec a' et b' premiers entre eux.

D'où, $a^2 = c^2a'^2$ et $b^2 = c^2b'^2$ avec a'^2 et b'^2 premiers entre eux. (Application de la propriété vue en cours, si a et b sont premiers entre alors a^n et b^p sont premiers entre eux).

" $a^2 = c^2a'^2$ et $b^2 = c^2b'^2$ avec a'^2 et b'^2 premiers entre eux " montre que PGCD(a^2 ; b^2) = c^2

2) **La réciproque est vraie.**

Énoncé de la réciproque :

" Si a, b, c sont des entiers supérieurs à 1, si PGCD(a^2 ; b^2) = c^2 alors PGCD(a ; b) = c "

Preuve :

Soit PGCD(a^2 ; b^2) = c^2

soit une décomposition en facteurs premiers de a : $a = p_1 \times p_2 \times \dots p_n = \prod_{i=1}^{n} p_i$ où les p_i pour $1 \leqslant i \leqslant n$ sont des nombres premiers. (Certains facteurs peuvent être égaux).

soit une décomposition en facteurs premiers de b : $b = q_1 \times q_2 \times \dots q_k = \prod_{i=1}^{r} q_i$ où les q_i pour $1 \leqslant i \leqslant r$ sont des nombres premiers. (Certains facteurs peuvent être égaux).

On a donc les décompositions en facteurs premiers de a^2 et b^2 :

$a^2 = \prod_{i=1}^{n} p_i^2$ et $b^2 = \prod_{i=1}^{r} q_i^2$.

Comme c^2 est le PGCD(a^2, b^2), on sait : $a^2 = c^2 \times p$ et $b^2 = c^2 \times q$ avec p et q premiers entre eux.

Il existe donc un certain nombre de facteurs p_i égaux aux facteurs q_i tels que $c^2 = \prod_{i=1}^{k} p_i^2$ et $p_i \neq q_i$ lorsque

i ⩾ $k + 1$.

$c = \prod_{i=1}^{k} p_i$. On a donc : $a = \prod_{i=1}^{k} p_i \times \prod_{i=k+1}^{n} p_i$ et $b = \prod_{i=1}^{k} p_i \times \prod_{i=k+1}^{r} q_i$.

Posons $a' = \prod_{i=k+1}^{n} p_i$ et $b' = \prod_{i=k+1}^{r} q_i$.

On obtient : $a = c \times a'$ et $b = c \times b'$

a' et b' sont premiers entre eux puisque les facteurs premiers p_i et q_i sont différents lorsque i ⩾ $k + 1$.

---

29 page 103

1. a. D'après les données, a (arête du cube) est un entier positif qui divise l et L.
$l = 882$ et $L = 945$
Les diviseurs communs de 882 et 945 sont les diviseurs de leur PGCD.
Algorithme d'Euclide :
$945 = 1 \times 882 + 63$
$882 = 63 \times 14 + 0$
Les diviseurs communs de 882 et 945 sont : 1 ; 3 ; 7 ; 9 ; 21 ; 63

b. le volume $v = 77\,760$
$l = 12l'$ et $L = 12L'$, $v = l^2 \times L = (12l')^2 \times (12L') = 12^3 l'^2 \times L'$ (l' et L' sont premiers entre eux)
et $77\,760 = 2^6 \times 3^5 \times 5 = 12^3 \times 45$.
On peut donc mettre 45 cubes d'arêtes 12.
Comme $45 = 1^2 \times 45 = 3^2 \times 5$ (la base de la boîte B est carrée),
on peut faire : 1 cube à la base et 45 cubes en hauteur, d'où,
la boîte B a pour dimensions : $l = 12$ et $L = 45 \times 12 = 540$ B a pour dimensions : 12×12×540
ou
3 cubes à la base et 5 cubes en hauteur,
d'où, la boîte B a pour dimensions : $l = 3 \times 12 = 36$ et $L = 5 \times 12 = 60$ B a pour dimensions : 36×36×60

2. La boîte cubique C d'arête c contient des boîtes B sans laisser de vide lorsque c est un multiple commun à l et L.
a) $l = 882$ et $L = 945$
Les arêtes c possibles sont les multiples du PPCM(882 ; 945)
PPCM(882 ; 945)×PGCD(882 ; 945) = 882×945
PPCM(882 ; 945) = $\frac{882 \times 945}{63}$ = 13 230
$c = \{13230 \times k / k \in \mathbb{N}^*\}$

b. Comme $c = 105$, alors, le volume de la caisse C est 105^3 = = 1 157 625.

Il y a donc : $\frac{1157625}{15435}$ = 75 boîtes B.

Comme $75 = 3 \times 5^2$, on a 5 fois la dimension l de B qui vaut 105, d'où, $l = \frac{105}{5} = 21$

et 3 fois la dimension L qui vaut 105, d'où, $L = \frac{105}{3} = 35$,

B a pour dimensions : 21×21×35

41 page 103

On sait : $n = 60q + 15$ et $n = 156q' + 15$, où q et q' sont des entiers.

On en déduit : $60q + 15 = 156q' + 15$, soit : $60q = 156q'$, puis : $5q = 13q'$ *(1)*

Comme 5 et 17 sont premiers entre eux, d'après le théorème de Gauss, 5 divise q'.

Il existe un entier k tel que $q' = 5k$ et en remplaçant q' par $5k$ dans (1) : $q = 13k$.

Conclusion : $n = 60\times13k + 15$ (ou $n = 156\times5k + 15$).

$n = 780k + 15$, $k \in \mathbb{Z}$.

---

51 page 105

1) $18 = 2\times3^2$ et $35 = 5\times7$, étant premiers entre eux, il existe deux entiers x et y tels que $18x - 35y = 1$

2) Il est évident que $x_0 = 2$ et $y_0 = 1$ conviennent.

3) a. Il s'agit de démontrer une équivalence :

Sachant que $18x_0 - 35\,y_0 = 1$,

le couple $(x\,;\,y)$ est solution de $18x - 35y = 1$ si et seulement si $18(x - x_0) = 35(y - y_0)$.

Sens direct :

On a : $18x - 35y = 1$ et $18x_0 - 35\,y_0 = 1$.

Par différence membre à membre, on en déduit :

$18(x - x_0) = 35(y - y_0)$.

Sens réciproque :

si $18(x - x_0) = 35(y - y_0)$, alors $18x - 35y = 18x_0 - 35y_0$

Or, $18x_0 - 35y_0 = 1$, d'où $18x - 35y = 1$ et donc : le couple $(x\,;\,y)$ est solution de $18x - 35y = 1$

L'équation $18x - 35y = 1$ est équivalente à l'équation $18(x - x_0) = 35(y - y_0)$ où $18x_0 - 35\,y_0 = 1$

b. Puisque $18(x - x_0) = 35(y - y_0)$, 35 divise $18(x - x_0)$.

Comme 18 et 35 sont premiers entre eux, d'après le théorème de Gauss, 35 divise $x - x_0$

soit : il existe un entier k tel que : $x - x_0 = 35k$.

On a de même, 18 divise $y - y_0$, et, donc il existe un entier k' tel que $y - y_0 = 18k'$.

c. D'après b/, un couple solutions est de la forme $(x_0 + 35k\,;\,y_0 + 18k')$.

On remplace dans l'équation $18(x - x_0) = 35(y - y_0)$, et on obtient : $18\times35k = 35\times18k'$

On en déduit $k = k'$.

L'ensemble des couples $(x\,;\,y)$ solutions de l'équation $18x - 35y = 1$ est $\{(x_0 + 35k\,;\,y_0 + 18k)/k \in \mathbb{Z}\}$.

56 page 105

Au jour J_0 le corps céleste A est observé : période d'apparition 105 jours.

Au jour $(J_0 + 6)$le corps céleste B est observé : période d'apparition 81 jours.

Objectif : Déterminer le jour J_1 où les deux objets apparaîtront simultanément.

1) ***Recherche*** : $J_1 - J_0$ est un multiple de 105 et $J_1 - J_0 - 6$ est un multiple de 81.

On a donc, il existe un entier u (nombre de périodes de l'objet A) tel que $J_1 - J_0 = 105u$

et un entier v (nombre de périodes de l'objet B) tel que $J_1 - J_0 - 6 = 81v$.

On en déduit : $J_1 - J_0 = 105u = 81v + 6$

$105u = 81v + 6$ équivaut à $35u - 27v = 2$.

Le couple $(u ; v)$ est donc solution de l'équation diophantienne : $35x - 27y = 2$. (E_1)

2) $35 = 5\times7$ et $27 = 3^3$, donc, 35 et 27 sont premiers entre eux

Il existe au moins un couple $(x_0 ; y_0)$ d'entiers solutions de $35x - 27y = 1$. (E_2)

Algorithme d'Euclide :

$35 = 27\times1 + 8$ $\quad$ $8 = 35 - 27\times1 = 35 - 27$

$27 = 8\times3 + 3$ $\quad$ $3 = 27 - 8\times3 = 27 - (35 - 27)\times3 = -3\times35 + 4\times27$

$8 = 2\times3 + 2$ $\quad$ $2 = 8 - 2\times3 = 35 - 27 - 2(-3\times35 + 4\times27) = 7\times35 - 9\times27$

$3 = 2\times1 + 1$ $\quad$ $1 = 3 - 2 = -3\times35 + 4\times27 - (7\times35 - 9\times27) = -10\times35 + 13\times27$

Un couple solution de (E_2) est : $(-10 ; -13)$

b) En multipliant l'égalité du 2a), par 2, on a : $2 = -20\times35 + 26\times27$

Un couple solution de (E_1) est : $(-20 ; -26)$

Remarque : dans la recherche précédente avec l'algorithme d'Euclide, on a un autre couple solution : $(7 ; 9)$.

c) Soit $(x ; y)$ une autre solution de (E_1) : $35x - 27y = 2$ et $2 = -20\times35 + 26\times27$,

on en déduit : $35x - 27y = -20\times35 + 26\times27$, soit : $35(x + 20) = 27(y + 26)$

D'après le théorème de Gauss, 35 divise $y + 26$, d'où, $y = -26 + 35k$ avec $k \in \mathbb{Z}$.

Puis, $x + 20 = 27k$. $\quad$ Soit : $x = -20 + 27k$.

Réciproquement :

Soit le couple $(-20 + 27k ; -26 + 35k)$ avec $k \in \mathbb{Z}$.

$35\times(-20 + 27k) - 27(-26 + 35k) = 2$.

Les solutions de (E_1) sont les couples qui s'écrivent : $(-20 + 27k ; -26 + 35k)$ avec $k \in \mathbb{Z}$.

d) Pour avoir J_1 (jour de la première apparition simultanée), on cherche les plus petites solutions positives de (E_1) : soit pour $k = 1$, $u = 7$ et $v = 9$.

3. a.Il s'écoulera 7×105 jours (ou $9\times81 + 6$), soit 735 jours, entre J_0 et J_1 ..

b. J_0 est le mardi 7 décembre 1999.

$735 = 7\times105$ Il y a donc 105 semaines entre J_0 et J_1 . J_1 sera un mardi …

2000 était une année bissextile :

$735 = 366 + 365 + 4$, donc, 2 ans et 4 jours entre J_0 et J_1 .

J_1 est le mardi 11 décembre 2001.

Rappel : année bissextile

Une année *n* est bissextile si *n* vérifie l'une des propositions suivantes :

- *n* est divisible par 4 et n'est pas divisible par 100

- *n* est divisible par 400

Ainsi : 1 952 étant divisible par 4 et n'étant pas divisible par 100 était bissextile.

1 700 est divisible par 4, mais, est pas divisible par 100 et n'est pas divisible par 400 n'est pas bissextile.

1 600 est divisible par 400, donc, 1 600 était une année bissextile.

2 014 n'est pas divisible par 4, donc, 2 014 n'est pas bissextile.

La négation de la définition mène à :

Une année *n* n'est pas bissextile si " *n* n'est pas divisible par 4 ou est divisible par 100 " et " *n* n'est pas divisible par 400 "

c. Les prochains passages simultanés seront obtenus lors des multiples communs à 105 et 81.

Les multiples communs de 105 et 81 sont les multiples de leur PPCM.

Le premier passage après le mardi 11 décembre 2001 aura lieu dans PPCM (105 ; 81)= 2 835.

---

57 page 105

1) x et y sont des entiers relatifs et (E) : $91x + 10y = 1$

a) 91 et 10 sont premiers entre eux ($91 = 7\times13$ et $10 = 2\times5$ n'ont aucun facteur premier commun, donc, PGCD(91 ; 10) = 1), d'où, d'après le théorème de Bézout, l'équation (E) a des solutions.

b) Il est évident que $x_0 = 1$ et $y_0 = -9$ fournissent un couple $(x_0 ; y_0)$ solution de (E).

En multipliant par 412 les deux membres de l'équation (E), on a : $412\times x_0 \times 91 + 412\times y_0 \times 10 = 412$

Une solution de (E ′) : $91x + 10y = 412$ est donc $(412 ; -9\times412)$, soit : $(412 ; -3708)$

c) On a : $\begin{cases} 91\times412-10\times3708=412 \\ 91x+10y=412 \end{cases} \Leftrightarrow \begin{cases} 91\times412-10\times3708=412 \\ 91(x-412)=-10(y+3708) \end{cases}$

Comme 91 et 10 sont premiers entre eux, le théorème de Gauss s'applique :

91 divise le produit $-10(y + 3708)$ et ne divise pas 10, d'où, 91 divise $y + 3708$.

Il existe un entier k tel que $y + 3708 = 91k$,

puis, en substituant dans (E ′) et en réduisant par 91 : $x - 412 = -10k$.

Les couples $(x ; y)$ solutions de (E ′) sont de la forme $(412 - 10k ; -3708 + 91k)$ avec $k \in \mathbb{Z}$.

Réciproquement, quelque soit l'entier k, $91\times(412 - 10k) + 10(-3708 + 91k) = 91\times412 - 10\times3708 = 412$

on peut conclure : l'ensemble des couples $(x ; y)$ solutions de (E ′) est $\{(412 - 10k ; -3708 + 91k)/\ k \in \mathbb{Z}\}$.

2) $A_n = 3^{2n} - 1$ où $n\in\mathbb{N}^*$.

Raisonnement direct : $3^2 = 9$ et $9 \equiv 1\ (8)$, d'où, $(3^2)^n \equiv 1^n\ (8)$, soit : $3^{2n} - 1 \equiv 0\ (8)$

Raisonnement par récurrence :

Initialisation : $n = 1$

$A_1 = 3^2 - 1 = 8$ et 8 est divisible par 8

Hérédité : Soit un entier $n \geqslant 1$ tel que A_n est divisible par 8. (Autrement dit : $A_n = 8q$ où q entier)

$A_{n+1} = 3^{2(n+1)} - 1 = 3^{2n}\times3^2 - 1$

Comme $3^{2n} = A_n + 1$, il vient : $A_{n+1} = (A_n + 1)\times9 - 1 = 9\times A_n + 8$.

Or, d'après l'hypothèse de récurrence, il existe un entier q tel que $A_n = 8q$

Finalement : $A_{n+1} = 8q + 8 = 8(q + 1)$

Conclusion : d'après l'axiome de récurrence, A_n divisible par 8 quelque soit l'entier $n\in\mathbb{N}^*$.

3) (E ″) : $A_3 x + A_2 y = 3296$

a) Comme d'après 2), A_3 et A_2 sont divisibles par 8, on réduit en divisant tous les termes par 8.

$A_3 x + A_2 y = 3296 \Leftrightarrow 728x + 80y = 3\,296 \Leftrightarrow 91x + 10y = 412$ (E′)

L'ensemble des couples $(x ; y)$ solutions de (E ″) est celui de (E ′) : $\{(412 - 10k ; -3708 + 91k)/\ k \in \mathbb{Z}\}$.

b) On cherche les solutions vérifiant : $\begin{cases} 412-10k\geqslant0 \\ -3708+91k\geqslant0 \end{cases}$

On a donc : k entier ET $k \leqslant 41{,}2$ ET $k \geqslant \frac{3708}{91}$ $(\approx 40{,}7)$

L'unique entier vérifiant ces conditions est 41.

Le seul couple d'entiers naturels solutions de (E ″) est : $(412 - 10\times41 ; -3\,708 + 91\times41)$, soit : $(2 ; 23)$

---

91 page 109 Descente infinie Racine de 2 (voir aussi 16 page 36, 122 page 45)

On suppose qu'il existe deux entiers naturels p et q non nuls tels que $\frac{p}{q} = \sqrt{2}$.

1) Étant donné que les nombres sont strictement positifs, on a les équivalences suivantes :

$\frac{p}{q} = \sqrt{2} \Leftrightarrow p = \sqrt{2}\,q \Leftrightarrow p^2 = 2q^2$

p^2 est par conséquent pair.

Rappel : p et p^2 ont même parité (voir les exercices du début d'année)

Conclusion : p est pair

2) Puisque p est pair, on peut écrire : $p = 2p'$

On a la nouvelle égalité : $4p'^2 = 2q^2$, soit : $q^2 = 2p'^2$

q^2 est par conséquent pair et il en est de même de q.

3) Puisque q est pair, on peut écrire : $q = 2q'$

Les entiers p' et q' sont strictement inférieurs à p et à q, et, $\sqrt{2} = \frac{p}{q} = \frac{2p'}{2q'} = \frac{p'}{q'}$

4) La démarche appliquée aux questions 1) et 2) s'appliquent à p' et à q'.

On peut donc créer deux **suites d'entiers strictement positifs et strictement décroissantes**

$0 < \ldots < p'' < p' < p$ et $0 < \ldots < q'' < q' < q$

Les ensembles $\{\ldots, p'', p', p\}$ et $\{\ldots, q'', q', q\}$ sont des sous-ensembles bornés de $\mathbb{N}$.

Tout sous-ensemble d'entiers naturels possèdent un plus petit élément et comme ici, ils ont aussi un plus grand élément, leur nombre d'élément est infini.

On ne peut pas " descendre " indéfiniment dans les entiers naturels.

c'est le principe de descente infinie. (Voir Fermat)

D'après ce principe, $\sqrt{2}$ est irrationnel.

Compléments :

Soit la droite Δ d'équation $y = \sqrt{2}\,x$.

On suppose qu'il existe un point de Δ à coordonnées entières $(p\,;\,q)$

Alors, le point à coordonnées entières $(p'\,;\,q')$ est aussi sur Δ et ainsi de suite indéfiniment ….

ce qui est impossible.

---

92 page 109 Nature de racine de *n*.

Soit n un entier naturel.

Si $n = 0$, $\sqrt{0} = 0$

Soit $n \geqslant 1$ et $\sqrt{n} = \frac{p}{q}$ fraction irréductible (p et q deux entiers naturels non nuls premiers entre eux).

On en déduit : $p^2 = nq^2$ $(q^2 \times n = p^2 \times 1)$

Comme p et q sont premiers entre eux, d'après le théorème de Gauss, q^2 divise 1.

$q^2 = 1$.

Lorsque $\sqrt{n} = \frac{p}{q}$ alors $\sqrt{n} = p$.

Ou bien $\sqrt{n}$ est un entier ou bien $\sqrt{n}$ est irrationnel.

---

93 page 109

$n \geqslant 2$ et $r^n = 2$

Supposons $r = \frac{p}{q}$ fraction irréductible (p et q deux entiers naturels non nuls premiers entre eux).

On a alors $r^n \times q^n = p^n$, soit : $2\ q^n = p^n$

p^n est pair et peut s'écrire : $p^n = 2^n\ p'^n$.

On a alors $q^n = 2^{n-1}\ p'^n$

q^n étant pair, on a : $q = 2q'$ ce qui contredit l'hypothèse : p et q premiers entre eux.

---

94 page 109

$x = \sqrt{3} + \sqrt{13}$.

1) $x^2 = \left(\sqrt{3}+\sqrt{13}\right)^2 = 3 + 2\sqrt{3}\ \sqrt{13} + 13 = 16 + 2\sqrt{39}$

$(16 - x^2)^2 = \left(2\sqrt{39}\right)^2 = 4\times 39$, d'où, $16^2 - 2\times 16\times x^2 + x^4 = 4\times 39$.

Comme $16^2 - 4\times 39 = 256 - 156 = 100$, on en déduit : $x^4 - 32x^2 + 100 = 0$. (1)

2) On pose $x = p/q$ avec p et q entiers premiers entre eux. (p/q est une fraction irréductible).

a) D'après (1) : $\left(\frac{p}{q}\right)^4 - 32\ \left(\frac{p}{q}\right)^2 + 100 = 0$.

En multipliant par q^4 non nul, on a l'équivalence suivante :

$\left(\frac{p}{q}\right)^4 - 32\ \left(\frac{p}{q}\right)^2 + 100 = 0 \Leftrightarrow p^4 - 32p^2q^2 + 100q^4 = 0.$

b) $p^4 - 32p^2q^2 + 100q^4 = 0 \Leftrightarrow q(32p^2q + 100q^3) = p^4$

Comme $32p^2q + 100q^3$ est un entier, q divise p^4,

et, comme p et q sont premiers entre eux, p^4 et q *sont premiers entre eux.*

Par conséquent : $q = 1$

c) On obtient $x = p$ et donc x est un entier (ce qui est faux).

3) x ne peut pas être un rationnel.

---

95 page 109

1) Rappel : $\cos(a + b) = \cos a \cos b - \sin a \sin b$

$\cos 2a = \cos^2 a - \sin^2 a$ $\qquad\qquad$ $\cos^2 a + \sin^2 a = 1$

$= 2\cos^2 a - 1$

$= 1 - 2\sin^2 a$

$\sin(a + b) = \sin a \cos b + \cos a \sin b$

$\sin 2a = 2\sin a \cos a$

$\cos(3x) = \cos(x + 2x) = \cos x \cos(2x) - \sin x \sin(2x)$

$= \cos x(2\cos^2 x - 1) - \sin x(2\sin x \cos x)$

$= 2\cos^3 x - \cos x - 2(1 - \cos^2 x)\cos x$

Conclusion : $\cos(3x) = 4\cos^3 x - 3\cos x$ (1)

2) $X = \cos\left(\frac{2\pi}{9}\right)$.

Posons $x = \frac{2\pi}{9}$, d'où, $3x = \frac{2\pi}{3}$ et $\cos(3x) = -\frac{1}{2}$.

D'après (1) : $-\frac{1}{2} = 4X^3 - 3X$ ce qui équivaut à : $8X^3 - 6X + 1 = 0$

3) On suppose $X = p/q$ (fraction irréductible) (p et q sont des entiers premiers entre eux).

a) $8X^3 - 6X + 1 = 0$ devient : $8\left(\frac{p}{q}\right)^3 - 6\left(\frac{p}{q}\right) + 1 = 0$

En multipliant par q^3 non nul, il vient : $8p^3 - 6pq^2 + q^3 = 0$

b) On a donc : $q(6pq + q^2) = 8p^3$

Comme q est premier avec p (donc avec p^3), q divise 8.

Les valeurs possibles de q sont : 1, 2, 4 ou 8.

c) on a aussi : $p(6q^2 - 8p^2) = q^3$

La seule valeur possible de p est 1.

4) On a donc : $X = 1$ ou $X = \frac{1}{2}$ ou $X = \frac{1}{4}$ ou $X = \frac{1}{8}$ et $8X^3 - 6X + 1 = 0$

Comme $8 - 6 + 1 \neq 0$, la valeur 1 est exclue.

Comme $8\left(\frac{1}{2}\right)^3 - 6\left(\frac{1}{2}\right)^2 + 1 \neq 0$, la valeur $\frac{1}{2}$ est exclue …

de même en remplaçant, X par $\frac{1}{4}$, et, par $\frac{1}{8}$, on montre qu'aucune de ces valeurs n'est solution de l'équation $8X^3 - 6X + 1 = 0$.

Conclusion : $\cos\left(\frac{2\pi}{9}\right)$ est un irrationnel.

---

101 page 110 (Wilson John (1741–1793))

Partie A

p est un nombre premier et x un entier compris entre 1 et $p - 1$.

Notons la liste $\mathcal{L} = \{1 ; 2 ; \ldots ; p - 1\}$ (liste des $p - 1$ entiers consécutifs de 1 à $p - 1$).

x est donc un élément de $\mathcal{L}$.

Notons r_y le reste de la division euclidienne du produit xy par p avec y est un élément de la liste $\mathcal{L}$.

1) a) **Une remarque :**

Par définition de la divisibilité, p ne divise aucun nombre entier naturel non nul qui le précède.

Soit $1 \leqslant x < p - 1$, on a : $x = 0 \times p + x$ avec $0 \leqslant x < p$ qui est la définition de la division euclidienne.

Comme $x \neq 0$, p ne divise pas x.

Retour à l'énoncé :

Soit $1 \leqslant x < p - 1$ et $1 \leqslant y < p - 1$, p ne divise ni x, ni y et,

comme ***p* est premier**, p ne divise aucun produit de la forme xy.

Aucun reste r_y n'est nul.

b) Soit a et b deux entiers différents de la liste 1, 2, …, $p - 1$ et r_a , r_b les restes de ax et bx dans la division par p.

Une démonstration :

Supposons $a < b$, on a donc : $1 \leqslant a < b \leqslant p - 1$, d'où, $1 \leqslant b - a \leqslant p - 2$

(En effet : $1 \leqslant b \leqslant p - 1$ et $-(p - 1) \leqslant -a \leqslant -1$, d'où, par somme : $2 - p \leqslant b - a \leqslant p - 2$.

Comme $b - a > 0$, on a : $1 \leqslant b - a \leqslant p - 2$)

$b - a$ est par conséquent un entier de la liste $\mathscr{L}$.

Raisonnement par l'absurde :

Si $r_a = r_b$ alors $ax \equiv bx\ (p)$ *définition des congruences,*

d'où : $(b - a)x \equiv 0\ (p)$, mais, d'après 1/a), aucun reste n'est nul.

Il est impossible d'avoir $r_a = r_b$

Tous les restes sont donc distincts.

Une autre démonstration :

$ax \equiv r_a\ (p)$ et $bx \equiv r_b\ (p)$
Par différence : $(b - a)x \equiv r_b - r_a\ (p)$
Or, $b - a \in \mathscr{L}$ (voir précédemment), d'où, $r_b - r_a$ non congru à 0 modulo p *d'*après 1a).

Remarque : on a $p - 1$ nombres entiers de la forme xy et tous les restes r_y sont distincts et $1 \leqslant r_y \leqslant p - 1$ par définition du reste dans la division par p et d'après 1/a/

c) D'après la remarque précédente, tous les restes de 1 à $p - 1$ sont atteints une et une seule fois, en particulier 1.

Soit x un entier de $\mathscr{L}$.

Il existe donc un seul y dans $\mathscr{L}$ tel que $xy \equiv 1\ (p)$.

(En d'autres termes : dans la table de multiplication modulo 13, chaque entier x de $\mathscr{L}$ a un et un seul inverse y dans $\mathscr{L}$.)

Plus généralement :

Soit x un entier de $\mathscr{L}$, il existe un et un seul entier y_i dans $\mathscr{L}$ tel que $xy \equiv i$ où i est un entier entre 1 et p – 1.

2) a) Premier cas : soit $x = 1$

$1 \times 1 = 1$ donc l'unicité de y impose $y = 1$. Dans le cas où $x = 1$, on a : $x = y$.

Deuxième cas : soit $x = p - 1$.

$(p - 1) \times (p - 1) = p^2 - 2p + 1$, d'où, $(p - 1) \times (p - 1) \equiv 1\ (p)$

ou encore : $p - 1 \equiv -1\ (p)$, d'où, $(p - 1) \times (p - 1) \equiv (-1)^2\ (p)$ ...

$(p - 1) \times (p - 1) \equiv 1\ (p)$ donc l'unicité de y impose $y = p - 1$. Dans le cas où $x = p - 1$, on a : $x = y$.

b) **Tous les autres cas :** $x \neq 1$ et $x \neq p-1$.

Raisonnement par l'absurde :

Supposons $x = y$, c'est-à-dire : $x^2 \equiv 1\ (p)$

On a donc : $x^2 - 1 \equiv 0\ (p)$

$(x-1)(x+1) \equiv 0\ (p)$

Comme p est premier, p divise $x-1$ ou p divise $x+1$.

Comme $x \in \mathscr{L}$, on a : $0 \leqslant x-1 \leqslant p-2$, et, le seul cas possible est 0, ce qui est exclu puisque $x \neq 1$

et $2 \leqslant x+1 \leqslant p$, et, le seul cas possible est p, ce qui est exclu puisque $x \neq p-1$

On ne peut donc pas avoir $x = y$

Remarque *: les questions 2a) et 2b) peuvent être traitées en même temps.*

En cherchant les valeurs de x tels que $x^2 \equiv 1\ (p)$ *on obtient que les seules solutions sont 1 et p – 1.*

3) Étude de $(p-1)$!.

$(p-1)\,! = 1\times2\times3\times \ldots \times(p-1)$ et p premier. (Pour utiliser les questions précédentes, comprendre comment on regroupe les facteurs deux à deux).

Quelques cas particuliers :

$p = 2$, $p-1 = 1$ et $1\,! = 1$, et, $1 \equiv -1\ (2)$ est vrai

$p = 3$, $p-1 = 2$ et $2\,! = 2$, et, $2 \equiv -1\ (3)$ est vrai

$p = 5$, $p-1 = 4$ et $4\,! = 1\times2\times3\times4$ Or, $2\times3 \equiv 1\ (5)$ et $4 \equiv -1\ (5)$ d'où, le produit $4\,! \equiv -1\ (5)$

dans le produit $1\times2\times3\times \ldots \times(p-1)$, on sait : $1 \equiv 1\ (p)$ et $p-1 \equiv -1\ (p)$

Si $p \geqslant 3$ (le cas $p = 2$ est traité), il reste $p-3$ facteurs de 2 à $p-2$.

p étant impair, $p-3$ est pair. Posons $p-3 = 2n$

On regroupe d'après le 2b/ les facteurs 2 à 2 tels que $xy \equiv 1\ (p)$

On obtient n produits congrus à 1 modulo p.

$$1\times2\times3\times \ldots \times(p-1) \equiv 1\times \overbrace{1\times\ldots\times1}^{n\text{ produits}} \times(-1) \quad (p)$$

On a montré :

si p est un nombre premier alors

$(p-1)\,! \equiv -1\ (p)$ ou encore $(p-1)\,! + 1 \equiv 0\ (p)$ ou encore $(p-1)\,! + 1$ est divisible par p.

(La réciproque est vraie, c'est cette propriété qui est appelée théorème de Wilson)

Partie B : étude d'un exemple

$p = 13$

1) Dans ce cas, le nombre $(p-1)\,! + 1$ est $12\,! + 1 = 479\,001\,601 = 13\times36\,846\,277$

2)

x	1	2	3	4	5	6	7	8	9	10	11	12
y	1	7	9	10	8	11	2	5	3	4	6	12
xy	1	14	27	40	40	66	14	40	27	40	66	144
$1 = 0\times13 + 1,\ 14 = 1\times13 + 1,\ 27 = 2\times13 + 1,\ 40 = 3\times13 + 1\ ;\ 66 = 5\times13 + 1,\ 144 = 11\times13 + 1$												

On a donc : $1 \equiv 2\times7 \equiv 3\times9 \equiv 4\times10 \equiv 5\times8 \equiv 6\times11 \equiv 12\times12 \quad (13)$

Table de multiplication modulo 13 :

x* y	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	4	6	8	10	12	1	3	5	7	9	11
3	3	6	9	12	2	5	8	11	1	4	7	10
4	4	8	12	3	7	11	2	6	10	1	5	9
5	5	10	2	7	12	4	9	1	6	11	3	8
6	6	12	5	11	4	10	3	9	2	8	1	7
7	7	1	8	2	9	3	10	4	11	5	12	6
8	8	3	11	6	1	9	4	12	7	2	10	5
9	9	5	1	10	6	2	11	7	3	12	8	4
10	10	7	4	1	11	8	5	2	12	9	6	3
11	11	9	7	5	3	1	12	10	8	6	4	2
12	12	11	10	9	8	7	6	5	4	3	2	1

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.

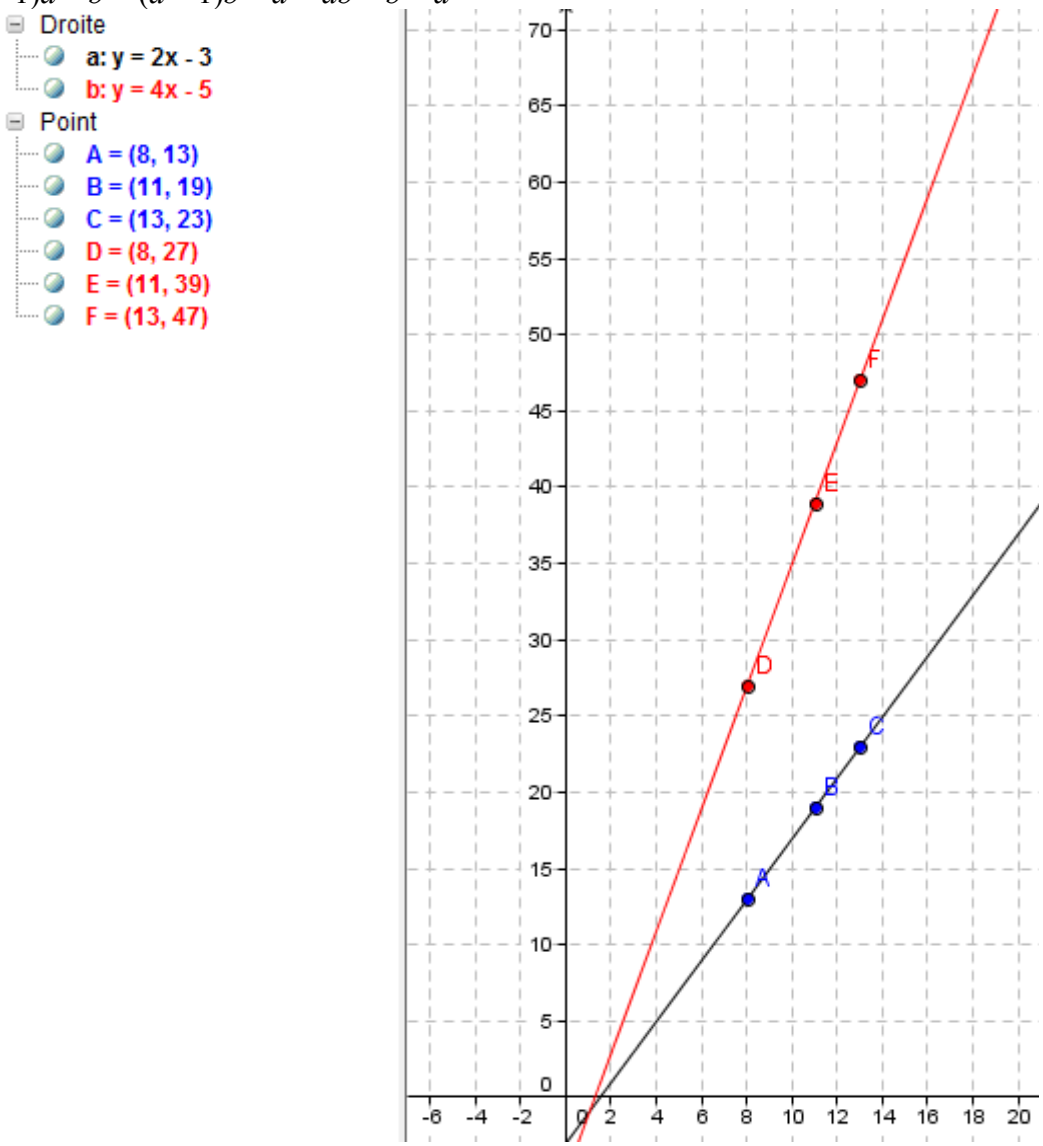
2)d)e) Expérimentation : $a = 5$ et conjecture.
a = 5 et b = 8 ***M = 27***
On cherche la première série de 5 entiers consécutifs :
$28 = 4\times5 + 1\times8$, $29 = 1\times5 + 3\times8$, $30 = 6\times5$, $31 = 3\times5 + 2\times8$, $32 = 4\times8$ sont cinq entiers consécutifs, et, on ne peut pas avoir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



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 : $26^2 = 676$ 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 :
$2850 = 221\times12 + 198$ $23 = 14\times1 + 9$ $5 = 4\times1 + 1$
$221 = 198\times1 + 23$ $14 = 9\times1 + 5$
$198 = 23\times8 + 14$ $9 = 5\times1 + 4$

ou bien : $2\,850 = 2\times3\times5^2\times19$ $221 = 13\times17$ PGCD(2850 ; 221) = 1

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

m est défini par $0 \leqslant m < 2\,851$ et $m \equiv 1104^{221}$ modulo 2 851
a) m est l'unique reste dans la division euclidienne de 1104^{221} par 2 851
2 851 est un nombre premier et 1104^{221} n'est pas divisible par 2 851. D'où $m \neq 0$.
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 S² 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

```
PROGRAM:CODEXPON
:Prompt N
:N-iPart(N/2851)
*2851→R
:R→S
:For(K,1,7)
:(S²)-iPart((S²)
/2851)*2851→S
:If K=2 or K=3 o
r K=4 or K=6 or
K=7
:Then
:R*S-iPart(R*S/2
851)*2851→R
:End
:End
:Disp R
:
```

Avec Algobox

```
VARIABLES
    n EST_DU_TYPE NOMBRE
    p EST_DU_TYPE NOMBRE
    r EST_DU_TYPE NOMBRE
    k EST_DU_TYPE NOMBRE
DEBUT_ALGORITHME
    LIRE n
    p PREND_LA_VALEUR n%2851
    r PREND_LA_VALEUR p
    POUR k ALLANT_DE 1 A 7
        DEBUT_POUR
        r PREND_LA_VALEUR pow(r,2)%2851
        SI (k==2 OU k==3 OU k==4 OU k==6 OU k==7) ALORS
            DEBUT_SI
            p PREND_LA_VALEUR (p*r)%2851
            FIN_SI
        FIN_POUR
    AFFICHER p
FIN_ALGORITHME
```

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 $CD = 1 + 173\times2850$, $n^{CD} = n^{1+173\times2850} = n\times n^{173\times2850} = n\times\left(n^{2850}\right)^{173}$
$m^D \equiv n\times\left(n^{2850}\right)^{173}\ (2851)$

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 : $\left(n^{2850}\right)^{173} \equiv 1\ (2851)$
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):;
```