Index

Activité 5 page 17 Chiffrement affine

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

La fonction permettant de chiffrer (coder) la lettre est une fonction affine f telle que $f(x) = ax + b$

x est le rang de la lettre à coder, $r(x)$ est le rang de la lettre codée où $r(x)$ est le reste de $f(x)$ par 26.
le couple (a, b) est la clé du codage.
Les tableurs ont une fonction permettant de donner les code ASCII pour une lettre donnée, et, la lettre ayant un code ASCII
Pour OpenCalc : " =CODE(lettre) " renvoie le code ASCII, et " = CAR(nombre) " renvoie la lettre.
=CODE(E) renvoie 69 (Faire =CODE(lettre)–65 pour retrouver x)
= CAR(69) renvoie E (Faire =CAR(r(x) + 65) pour obtenir le caractère chiffré)
1) clé de codage (7, 17)

	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	AB	AC	AD	AE	AF
1	Clé	a=	7		b=	17																										
2	Texte en clair	E	T	S	I	L	N	E	N	R	E	S	T	E	Q	U	U	N	J	E	S	E	R	A	I	C	E	L	U	I	L	A
3	ax+b	45	150	143	73	94	108	45	108	136	45	143	150	45	129	157	157	108	80	45	143	45	136	17	73	31	45	94	157	73	94	17
4	r(x)	19	20	13	21	16	4	19	4	6	19	13	20	19	25	1	1	4	2	19	13	19	6	17	21	5	19	16	1	21	16	17
5	texte chiffré	T	U	N	V	Q	E	T	E	G	T	N	U	T	Z	B	B	E	C	T	N	T	G	R	V	F	T	Q	B	V	Q	R

2) clé de codage (5, 11)

	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	AB	AC	AD	AE	AF
1	Clé	a=	5		b=	11																										
2	Texte en clair	E	T	S	I	L	N	E	N	R	E	S	T	E	Q	U	U	N	J	E	S	E	R	A	I	C	E	L	U	I	L	A
3	ax+b	31	106	101	51	66	76	31	76	96	31	101	106	31	91	111	111	76	56	31	101	31	96	11	51	21	31	66	111	51	66	11
4	r(x)	5	2	23	25	14	24	5	24	18	5	23	2	5	13	7	7	24	4	5	23	5	18	11	25	21	5	14	7	25	14	11
5	texte chiffré	F	C	X	Z	O	Y	F	Y	S	F	X	C	F	N	H	H	Y	E	F	X	F	S	L	Z	V	F	O	H	Z	O	L

Clé de codage (31,11)

	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	AB	AC	AD	AE	AF
1	Clé	a=	31		b=	11																										
2	Texte en clair	E	T	S	I	L	N	E	N	R	E	S	T	E	Q	U	U	N	J	E	S	E	R	A	I	C	E	L	U	I	L	A
3	ax+b	135	600	569	259	352	414	135	414	538	135	569	600	135	507	631	631	414	290	135	569	135	538	11	259	73	135	352	631	259	352	11
4	r(x)	5	2	23	25	14	24	5	24	18	5	23	2	5	13	7	7	24	4	5	23	5	18	11	25	21	5	14	7	25	14	11
5	texte chiffré	F	C	X	Z	O	Y	F	Y	S	F	X	C	F	N	H	H	Y	E	F	X	F	S	L	Z	V	F	O	H	Z	O	L

Clé de codage (265,37)

	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	AB	AC	AD	AE	AF
1	Clé	a=	265		b=	37																										
2	Texte en clair	E	T	S	I	L	N	E	N	R	E	S	T	E	Q	U	U	N	J	E	S	E	R	A	I	C	E	L	U	I	L	A
3	ax+b	1097	5072	4807	2157	2952	3482	1097	3482	4542	1097	4807	5072	1097	4277	5337	5337	3482	2422	1097	4807	1097	4542	37	2157	567	1097	2952	5337	2157	2952	37
4	r(x)	5	2	23	25	14	24	5	24	18	5	23	2	5	13	7	7	24	4	5	23	5	18	11	25	21	5	14	7	25	14	11
5	texte chiffré	F	C	X	Z	O	Y	F	Y	S	F	X	C	F	N	H	H	Y	E	F	X	F	S	L	Z	V	F	O	H	Z	O	L

b) Les trois textes codés sont identiques au 2/a) mais différents du texte chiffré au 1/
au 2a) les différences $a - a'$ et $b - b'$ sont des multiples de 26.
Soit x un nombre entier : $f(x) = ax + b$ et $f(x) = 26\times q + r(x)$ avec $0 \leqslant r(x) < 26$
$g(x) = a'x + b'$ et $g(x) = 26\times q' + r'(x)$ avec $0 \leqslant r'(x) < 26$
$a' = a + 26k$ et $b' = b + 26k'$.
$g(x) = (a + 26k)x + b + 26k' = f(x) + 26kx + 26k' = 26\times q + r(x) + 26kx + 26k'$
$= 26(q + kx + k') + r(x)$ avec $0 \leqslant r(x) < 26$
Les restes sont donc égaux.
(Cette activité a pour but de préparer à la notion de congruence).
Données : $f(x) = 26\times q + r(x)$ avec $0 \leqslant r(x) < 26$
$g(x) = 26\times q' + r'(x)$ avec $0 \leqslant r'(x) < 26$
$a - a'$ et $b - b'$ sont des multiples de 26.

D'où :
$f(x) \equiv r(x)$ (26) avec $0 \leqslant r(x) < 26$, et, $g(x) \equiv r'(x)$ (26) avec $0 \leqslant r'(x) < 26$
$a - a'$ et $b - b'$ sont des multiples de 26, d'où, $a - a' \equiv 0$ (26) et $b - b' \equiv 0$ (26), soit : $a \equiv a'$ (26) et $b \equiv b'$ (26)
Comme $f(x) = ax + b$, on a : $f(x) \equiv a'x + b'$ (26)
Conclusion : $f(x) \equiv g(x)$ (26)

c) A priori, il existe : $25^2 = 625$ chiffrements possibles.

3) $a = 13$
a)

	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	AB	AC	AD	AE	AF
1	Clé	a=	13		b=	37																										
2	Texte en clair	E	T	S	I	L	N	E	N	R	E	S	T	E	Q	U	U	N	J	E	S	E	R	A	I	C	E	L	U	I	L	A
3	ax+b	89	284	271	141	180	206	89	206	258	89	271	284	89	245	297	297	206	154	89	271	89	258	37	141	63	89	180	297	141	180	37
4	r(x)	11	24	11	11	24	24	11	24	24	11	11	24	11	11	11	11	24	24	11	11	11	24	11	11	11	11	24	11	11	24	11
5	texte chiffré	L	Y	L	L	Y	Y	L	Y	Y	L	L	Y	L	L	L	L	Y	Y	L	L	L	Y	L	L	L	L	Y	L	L	Y	L

Le message chiffré ne contient que deux lettres différentes.
b) $13x + b = 26q + r(x)$et $13x' + b = 26q' + r(x')$ avec q, q' entiers et $0 \leqslant r(x) < 26$ et $0 \leqslant r(x') < 26$
$r(x) - r(x') = 13(x - x') - 26(q - q') = 13(x - x' - 2q + 2q')$ et $x - x' - 2q + 2q'$ est un entier.
D'autre part : $-26 < r(x) - r(x') < 26$
Les seuls multiples de 13 strictement compris entre –26 et 26 sont : –13, 0 et 13.
Comme –13 et 13 ont le même reste 13 dans la division 26, on n'a que deux valeurs possibles pour le codage.
On a un reste r et l'autre $r + 13$ (ou $r - 13$). (Dans l'exemple du 3a/ : 11 et 24)

c) 13 est un diviseur de 26.
Lorsque $a = 2$ (autre diviseur de 26), la même démarche va amener :
$r(x) - r(x')$ est un multiple de 2.
On n'a alors 13 lettres dans le codage (deux lettres différentes sont codées par la même lettre :
Le A (0) et le N (13), le B(1) et le O(14), ..., le E(4) et le R(17) .... ,

	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	AB	AC	AD	AE	AF
1	Clé	a=	2		b=	37																										
2	Texte en clair	E	T	S	I	L	N	E	N	R	E	S	T	E	Q	U	U	N	J	E	S	E	R	A	I	C	E	L	U	I	L	A
3	ax+b	45	75	73	53	59	63	45	63	71	45	73	75	45	69	77	77	63	55	45	73	45	71	37	53	41	45	59	77	53	59	37
4	r(x)	19	23	21	1	7	11	19	11	19	19	21	23	19	17	25	25	11	3	19	21	19	19	11	1	15	19	7	25	1	7	11
5	texte chiffré	T	X	V	B	H	L	T	L	T	T	V	X	T	R	Z	Z	L	D	T	V	T	T	L	B	P	T	H	Z	B	H	L

118 page 44 ***Asie juin 2004***

E est l'ensemble des entiers naturels qui peuvent s'écrire sous la forme $9 + a^2$ où a est un entier naturel non nul.

Autrement dit : $E = \{9 + a^2 / a \in \mathbb{N}^*\}$

1) Étude de l'équation d'inconnue a : $a^2 + 9 = 2^n$ où $a \in \mathbb{N}$, $n \in \mathbb{N}$ et $n \geqslant 4$.

Remarque : on commence à l'entier 4, car, $a^2 + 9 > 9$, et, si $n < 4$, $2^n \leqslant 8$

a) **Par l'absurde** :

Supposons a existe et a pair.

En ce cas : $a = 2p$ et $a^2 = 4p^2$ avec $p \in \mathbb{N}$. a^2 est par conséquent pair, ainsi que $2^n - a^2$

Comme $2^n - a^2 = 9$ et que 9 est impair, on a une contradiction.

Si a existe et si $a^2 + 9 = 2^n$ alors a est impair.

Autre démonstration :

$a^2 = 2^n + 9$.

La somme d'un entier pair et d'un entier est impair, d'où, a^2 est impair.

Or, a et a^2 ont la même parité, d'où, a est impair.

b) On a : $9 \equiv 1\ (4)$

a étant impair, $a = 2p + 1$ et $a^2 = 4p^2 + 4p + 1$, d'où $a^2 \equiv 1\ (4)$
On a donc : $a^2 + 9 \equiv 2\ (4)$
Or, $n \geqslant 4$, d'où, $n = 4 + x$ avec $x \in \mathbb{N}$, $2^n = 2^{4+x} = 16 \times 2^x$, d'où $2^n \equiv 0\ (4)$
L'égalité est impossible, l'équation $a^2 + 9 = 2^n$ n'a pas de solution.

2) Étude de l'équation d'inconnue a : $a^2 + 9 = 3^n$ où $a \in \mathbb{N}$, $n \in \mathbb{N}$ et $n \geqslant 3$.
Remarque : on commence à l'entier 3, car, $a^2 + 9 > 9$, et, si $n < 3$, $3^n \leqslant 9$

a) $n \geqslant 3$.

Disjonction des cas :

*** n est pair, d'où, $n = 2p$ et $3^n = 9^p$.

Comme $9 \equiv 1\ (4)$, on a : $3^n \equiv 1\ (4)$

*** n est impair, d'où, $n = 2p + 1$ et $3^n = 9^p \times 3$.

Comme $9 \equiv 1\ (4)$, on a : $3^n \equiv 3\ (4)$

b) **Par l'absurde** :

Supposons a existe et a impair.

En ce cas : $a = 2p + 1$ et $a^2 = 4p^2 + 4p + 1$ avec $p \in \mathbb{N}$. a^2 est par conséquent impair.

La somme de deux nombres impairs est paire, d'où, $a^2 + 9$ est paire.

Or, 3^n est impair, on a une contradiction.

Si a existe et si $a^2 + 9 = 3^n$ alors a est pair.

Puisque a est pair, on peut poser $a = 2p$ et $a^2 + 9 = 4p^2 + 9$ avec $p \in \mathbb{N}^*$.

Comme $4p^2 + 9 \equiv 1\ (4)$, il vient : $3^n \equiv 1\ (4)$

Dans le 2a), on a montré que ceci n'est vrai que lorsque n est pair.

Conclusion : Si a existe et si $a^2 + 9 = 3^n$ alors a est pair et n est pair.

c) Puisque n est pair et $n \geqslant 3$, on peut écrire $n = 2p$ avec $p \geqslant 2$.

$3^n - a^2 = 3^{2p} - a^2 = (3^p)^2 - a^2 = (3^p - a)(3^p + a)$

D 'autre part : $(3^p - a)(3^p + a) = 9$

Les diviseurs de 9 sont : 1, 3 et 9.

Comme $a > 0$, $3^p - a < 3^p + a$

La seule possibilité est donc : $\begin{cases} 3^p - a = 1 \\ 3^p + a = 9 \end{cases}$

On en déduit par somme membre-à-membre : $2 \times 3^p = 10$, soit : $3^p = 5$ ce qui est impossible.

Conclusion : l'équation $a^2 + 9 = 3^n$ n'a pas de solution.

3) Étude de l'équation d'inconnue a : $a^2 + 9 = 5^n$ où $a \in \mathbb{N}$, $n \in \mathbb{N}$ et $n \geqslant 2$.

a) $9 \equiv 0\ (3)$et $5 \equiv -1\ (3)$

Si n est pair, $5^n \equiv 1\ (3)$

Si n impair, $5^n \equiv -1\ (3)$

Si n est impair alors $a^2 \equiv -1\ (3)$

ou encore $a^2 \equiv 2\ (3)$

Or $a \equiv 0\ (3)$ ou $a \equiv 1\ (3)$ ou $a \equiv 2\ (3)$

d'où, $a^2 \equiv 0\ (3)$ ou $a^2 \equiv 1\ (3)$ ou $a^2 \equiv 4 \equiv 1\ (3)$

L'égalité $a^2 \equiv 2\ (3)$ est impossible.

Conclusion : l'équation $a^2 + 9 = 5^n$ n'a pas de solution lorsque n est impair.

b) Puisque n est pair et $n \geqslant 2$, on peut écrire $n = 2p$ avec $p \geqslant 1$.

$5^n - a^2 = 5^{2p} - a^2 = (5^p)^2 - a^2 = (5^p - a)(5^p + a)$

D 'autre part : $(5^p - a)(5^p + a) = 9$

Les diviseurs de 9 sont : 1, 3 et 9.

Comme $a > 0$, $5^p - a < 5^p + a$

La seule possibilité est donc : $\begin{cases} 5^p - a = 1 \\ 5^p + a = 9 \end{cases}$

On en déduit par somme membre-à-membre : $2 \times 5^p = 10$, soit : $5^p = 5$, donc, $p = 1$.

On en déduit : $5 - a = 1$, soit $a = 4$.

On a bien : $4^2 + 9 = 5^2$

Conclusion : l'équation $a^2 + 9 = 5^n$ a une et une seule solution : $a = 4$
