Chapitre IV
Applications

4.1 *Liban, juin 2005*

1. On considère l'équation (E) :

$$109x - 226y = 1$$

où x et y sont des entiers relatifs.

a. Déterminer le pgcd de 109 et 226. Que peut-on en conclure pour l'équation (E) ?

b. Montrer que l'ensemble de solutions de (E) est l'ensemble des couples de la forme $(141 + 226k,\ 68 + 109k)$, où k appartient à $\mathbf{Z}$.
En déduire qu'il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel non nul e tels que $109d = 1 + 226e$. (On précisera les valeurs des entiers d et e.)

2. Démontrer que 227 est un nombre premier.

3. On note A l'ensemble des 227 entiers naturels a tels que $a \leqslant 226$.
On considère les deux fonctions f et g de A dans A définies de la manière suivante :
- à tout entier de A, f associe le reste de la division euclidienne de a^{109} par 227.
- à tout entier de A, g associe le reste de la division euclidienne de a^{141} par 227.

a. Vérifier que $g[f(0)] = 0$.
On rappelle le résultat suivant appelé petit théorème de Fermat :
Si p est un nombre premier et a un entier non divisible par p alors $a^{p-1} \equiv 1$ modulo p.

b. Montrer que, quel que soit l'entier non nul a de A, $a^{226} \equiv 1$ [modulo 227].

c. En utilisant **1. b.**, en déduire que, quel que soit l'entier non nul a de A, $g[f(a)] = a$. Que peut-on dire de $f[g(a)]$?

4.2 *Centres étrangers, juin 2006*

Le but de l'exercice est d'étudier certaines propriétés de divisibilité de l'entier $4^n - 1$, lorsque n est un entier naturel.
On rappelle la propriété connue sous le nom de petit théorème de Fermat : « si p est un nombre premier et a un entier naturel premier avec p, alors $a^{p-1} - 1 \equiv 0 \bmod p$ ».

Partie A – Quelques exemples

1. Démontrer que, pour tout entier naturel n, 4^n est congru à 1 modulo 3.

2. Prouver à l'aide du petit théorème de Fermat, que $4^{28} - 1$ est divisible par 29.

3. Pour $1 \leqslant n \leqslant 4$, déterminer le reste de la division de 4^n par 17. En déduire que, pour tout entier k, le nombre $4^{4k} - 1$ est divisible par 17.

4. Pour quels entiers naturels n le nombre $4^n - 1$ est-il divisible par 5 ?

5. A l'aide des questions précédentes déterminer quatre diviseurs premiers de $4^{28} - 1$.

Partie B – Divisibilité par un nombre premier

Soit p un nombre premier différent de 2.

1. Démontrer qu'il existe un entier $n \geqslant 1$ tel que $4^n \equiv 1 \bmod p$.

2. Soit $n \geqslant 1$ un entier naturel tel que $4^n \equiv 1 \bmod p$. On note b le plus petit entier strictement positif tel que $4^b \equiv 1 \bmod p$ et r le reste de la division euclidienne de n par b.

a. Démontrer que $4^r \equiv 1 \bmod p$. En déduire que $r = 0$.

b. Prouver l'équivalence : $4^n - 1$ est divisible par p si et seulement si n est multiple de b.

c. En déduire que b divise $p - 1$.

4.3 *La Réunion, juin 2004*

On rappelle la propriété, connue sous le nom de petit théorème de Fermat : « soit p un nombre premier et a un entier naturel premier avec p ; alors $a^{p-1} - 1$ est divisible par p ».

1. Soit p un nombre premier impair.

a. Montrer qu'il existe un entier naturel k, non nul, tel que $2^k \equiv 1\ [p]$.

b. Soit k un entier naturel non nul tel que $2^k \equiv 1\ [p]$ et soit n un entier naturel. Montrer que, si k divise n, alors $2^n \equiv 1\ [p]$.

c. Soit b tel que $2^b \equiv 1\ [p]$, b étant le plus petit entier non nul vérifiant cette propriété.
Montrer, en utilisant la division euclidienne de n par b, que si $2^n \equiv 1\ [p]$, alors b divise n.

2. Soit q un nombre premier impair et le nombre $A = 2^q - 1$.
On prend pour p un facteur premier de A.

a. Justifier que : $2^q \equiv 1\ [p]$.

b. Montrer que p est impair.

c. Soit b tel que $2^b \equiv 1\ [p]$, b étant le plus petit entier non nul vérifiant cette propriété.
Montrer, en utilisant **1.** que b divise q. En déduire que $b = q$.

d. Montrer que q divise $p - 1$, puis montrer que $p \equiv 1\ [2q]$.

3. Soit $A_1 = 2^{17} - 1$. Voici la liste des nombres premiers inférieurs à 400 et qui sont de la forme $34m + 1$, avec m entier non nul : 103, 137, 239, 307. En déduire que A_1 est premier.

4.4 *France métropolitaine, septembre 2003*

On rappelle que 2003 est un nombre premier.

1. **a.** Déterminer deux entiers relatifs u et v tels que $123u + 2003v = 1$.

b. En déduire un entier relatif k_0 tel que $123k_0 \equiv 1[2003]$.

c. Montrer que, pour tout entier relatif x, $123x \equiv 456[2003]$ si et seulement si $x \equiv 456k_0[2003]$.

d. Déterminer l'ensemble des entiers relatifs x tels que $123x \equiv 456[2003]$.

e. Montrer qu'il existe un unique entier n tel que $1 \leqslant n \leqslant 2002$ et $123n \equiv 456[2003]$.

2. Soit a un entier tel que $1 \leqslant a \leqslant 2002$.

a. Déterminer PGCD$(a, 2003)$. En déduire qu'il existe un entier m tel que $am \equiv 2[2003]$.

b. Montrer que, pour tout entier b, il existe un unique entier x tel que $0 \leqslant x \leqslant 2002$ et $ax \equiv b[2003]$.

4.5 *Antilles-Guyane, juin 2008*

Partie A

On considère l'équation (E) : $11x - 26y = 1$, où x et y désignent deux nombres entiers relatifs.

1. Vérifier que le couple $(-7; -3)$ est solution de (E).

2. Résoudre alors l'équation (E).

3. En déduire le couple d'entiers relatifs $(u; v)$ solution de (E) tel que $0 \leqslant u \leqslant 25$.

Partie B

On assimile chaque lettre de l'alphabet à un nombre entier comme l'indique le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

On "code" tout nombre entier x compris entre 0 et 25 de la façon suivante :
– on calcule $11x + 8$;
– on calcule le reste de la division euclidienne de $11x + 8$ par 26, que l'on appelle y.
x est alors "codé" par y.
Ainsi, par exemple, la lettre L est assimilée au nombre 11 ; $11 \times 11 + 8 = 129$ or $129 \equiv 25[26]$; 25 est le reste de la division euclidienne de 129 par 26. Au nombre 25 correspond la lettre Z.
La lettre L est donc codée par la lettre Z.

1. Coder la lettre W.

2. Le but de cette question est de déterminer la fonction de décodage.

a. Montrer que pour tous nombres entiers relatifs x et j, on a :

$$11x \equiv j[26] \text{ équivaut à } x \equiv 19j[26].$$

b. En déduire un procédé de décodage.

c. Décoder la lettre Q.

4.6 *France métropolitaine, juin 2006*

Partie A

1. Énoncer le théorème de Bézout et le théorème de Gauss.

2. Démontrer le théorème de Gauss en utilisant le théorème de Bézout.

Partie B

Il s'agit de résoudre dans $\mathbf{Z}$ le système

$$(S) \quad \begin{cases} n \equiv 13 \quad [19] \\ n \equiv 6 \quad [12] \end{cases}$$

1. Démontrer qu'il existe un couple $(u; v)$ d'entiers relatifs tel que : $19u + 12v = 1$.
(On ne demande pas dans cette question de donner un exemple d'un tel couple).
Vérifier que, pour un tel couple, le nombre $N = 13 \times 12v + 6 \times 19u$ est une solution de (S).

2. **a.** Soit n_0 une solution de (S), vérifier que le système (S) équivaut à

$$\begin{cases} n \equiv n_0 \quad [19] \\ n \equiv n_0 \quad [12] \end{cases}$$

b. Démontrer que le système $\begin{cases} n \equiv n_0 \quad [19] \\ n \equiv n_0 \quad [12] \end{cases}$ équivaut à $n \equiv n_0 \quad [12 \times 19]$.

3. **a.** Trouver un couple $(u; v)$ solution de l'équation $19u + 12v = 1$ et calculer la valeur de N correspondante.

b. Déterminer l'ensemble des solutions de (S) (on pourra utiliser la question 2. b.).

4. Un entier naturel n est tel que lorsqu'on le divise par 12, le reste est 6 et lorsqu'on le divise par 19 le reste est 13.
On divise n par $228 = 12 \times 19$. Quel est le reste r de cette division ?

4.7 Inde, mai 2001

1. On considère l'équation (1) d'inconnue $(n\ ,\ m)$ élément de $\mathbf{Z}^2$:

$$11n - 24m = 1.$$

a. Justifier, à l'aide de l'énoncé d'un théorème, que cette équation admet au moins une solution.

b. En utilisant l'algorithme d'Euclide, déterminer une solution particulière de l'équation (1).

c. Déterminer l'ensemble des solutions de l'équation (1).

2. Recherche du P.G.C.D. de $10^{11} - 1$ et $10^{24} - 1$.

a. Justifier que 9 divise $10^{11} - 1$ et $10^{24} - 1$.

b. $(n,\ m)$ désignant un couple quelconque d'entiers naturels solutions de (1), montrer que l'on peut écrire

$$\left(10^{11n} - 1\right) - 10\left(10^{24m} - 1\right) = 9.$$

c. Montrer que $10^{11} - 1$ divise $10^{11n} - 1$ (on rappelle l'égalité $a^n - 1 = (a - 1)\left(a^{n-1} + a^{n-2} + \cdots + a^0\right)$, valable pour tout entier naturel n non nul).
Déduire de la question précédente l'existence de deux entiers N et M tels que :

$$\left(10^{11} - 1\right) N - \left(10^{24} - 1\right) M = 9.$$

d. Montrer que tout diviseur commun à $10^{24} - 1$ et $10^{11} - 1$ divise 9.

e. Déduire des questions précédentes le P.G.C.D. de $10^{24} - 1$ et $10^{11} - 1$.

4.8 Le chiffrement de LESTER HILL

Dans ce chiffrement, la fonction de codage agit sur des couples de nombres choisis dans $\{0, 1, \cdots, 25\}$:

$$f : (x_1, x_2) \mapsto (y_1, y_2)$$

Posons par exemple :

$$\left\{ \begin{array}{rcll} y_1 & = & 5x_1 + 11x_2 & [26] \\ y_2 & = & 8x_1 + 3x_2 & [26] \end{array} \right. \qquad (1)$$

Ainsi le mot KL correspondant au couple $(10, 11) = (x_1, x_2)$ est codé par $(y_1, y_2) = (15, 9)$ soit PJ.

1. Coder le mot REQUIN en détachant les trois blocs de deux lettres.

2. *Décodage*

a. Montrer que si x_1, x_2, y_1 et y_2 vérifient (1) alors :

$$\left\{ \begin{array}{rcll} -3y_1 + 11y_2 & = & 73x_1 & [26] \\ 8y_1 - 5y_2 & = & 73x_2 & [26] \end{array} \right.$$

b. Résoudre dans $\mathbf{Z} \times \mathbf{Z}$ l'équation $73x + 26y = 1$, avec $0 \leqslant x \leqslant 25$.

c. Décoder alors le mot KQJLRHTN.

4.9 La Poste distribue à titre promotionnel un jeu composé de six cartes dont les reproductions sont données ci-dessous, suivies de la règle du jeu :

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

Carte A

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

Carte B

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

Carte C

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

Carte D

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

Carte E

32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

Carte F

Épater votre entourage.
Ce jeu se joue à 2 ou à plusieurs et vous avez le pouvoir de deviner le numéro magique choisi en secret par l'un des joueurs...

1. Demandez à quelqu'un de choisir mentalement un numéro entre 1 et 63, et de le révéler aux autres personnes présentes, sans vous le dire.
2. Disposez une par une les six cartes devant la personne choisie, dans n'importe quel ordre. Le joueur doit éliminer les cartes sur lesquelles le numéro qu'il a choisi ne figure pas.
3. Additionnez alors le numéro inscrit dans la première case – en haut à gauche – de chaque carte restante et vous trouverez le numéro magique. Étonnez les joueurs en leur annonçant ce numéro connu d'eux seuls.

1. Vérifier que le jeu fonctionne pour les nombres 61 et 17.
2. Quelle est la forme générale des nombres de la carte A ?
3. Sur quelles cartes trouve-t-on les nombres 2, 21, 48 et 63 ?
4. Etablir la liste des nombres que l'on trouve seulement sur une carte.
5. Donner la décomposition et l'écriture en base 2 des nombres trouvés à la question précédente, puis des nombres 21, 63, 48, 17 et 61.
6. Quel est le lien entre la décomposition d'un nombre en base 2 et les cartes sur lesquelles il apparait ?

7. Quel est le point commun des nombres présents sur la carte F ? Même question pour la carte E, puis la carte D, la carte C, la carte B et enfin la carte A.

8. **a.** Pourquoi les nombres de la carte F sont-ils tous supérieurs à 32 ?

b. Pourquoi les nombres de la carte A sont-ils tous impairs ?

c. Pourquoi chaque ligne de la carte C est-elle composée de 4 nombres consécutifs ?

d. Pourquoi les nombres de la carte E sont-ils répartis en 2 suites de 16 nombres consécutifs ?

9. Expliquer complètement le "secret" du fonctionnement de ce jeu.

4.10 *Nouvelle-Calédonie, mars 2007*

Pour coder un message, on procède de la manière suivante : à chacune des 26 lettres de l'alphabet, on commence par associer un entier n de l'ensemble $\Omega = \{0\ ;\ 1\ ;\ 2\ ;\ \ldots\ ;\ 24\ ;\ 25\}$ selon le tableau ci-dessous :

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

a et b étant deux entiers naturels donnés, on associe à tout entier n de Ω le reste de la division euclidienne de $(an+b)$ par 26 ; ce reste est alors associé à la lettre correspondante.
Exemple : pour coder la lettre P avec $a = 2$ et $b = 3$, on procède de la manière suivante :
– Étape 1 : on lui associe l'entier $n = 15$.
– Étape 2 : le reste de la division de $2 \times 15 + 3 = 33$ par 26 est 7.
– Étape 3 : on associe 7 à H. Donc P est codé par la lettre H.

1. Que dire alors du codage obtenu lorsque l'on prend $a = 0$?

2. Montrer que les lettres A et C sont codées par la même lettre lorsque l'on choisit $a = 13$.

3. *Dans toute la suite de l'exercice*, on prend $a = 5$ et $b = 2$.

a. On considère deux lettres de l'alphabet associées respectivement aux entiers n et p. Montrer, que si $5n + 2$ et $5p + 2$ ont le même reste dans la division par 26 alors $n - p$ est un multiple de 26. En déduire que $n = p$.

b. Coder le mot AMI.

4. On se propose de décoder la lettre E.

a. Montrer que décoder la lettre E revient à déterminer l'élément n de Ω tel que $5n - 26y = 2$, où y est un entier.

b. On considère l'équation $5x - 26y = 2$, avec x et y entiers relatifs.

i. Donner une solution particulière de l'équation $5x - 26y = 2$.

ii. Résoudre alors l'équation $5x - 26y = 2$.

iii. En déduire qu'il existe un unique couple $(x\ ;\ y)$ solution de l'équation précédente, avec $0 \leqslant x \leqslant 25$.

c. Décoder alors la lettre E.

4.11 **Devoir maison 4** Pour tout entier naturel n supérieur ou égal à 2, on pose $A(n) = n^4 + 1$.
L'objet de l'exercice est l'étude des diviseurs premiers de $A(n)$.

1. Quelques résultats

a. Étudier la parité de l'entier $A(11)$.

b. Montrer que, quel que soit l'entier n, $A(n)$ n'est pas un multiple de 3.

c. Montrer que tout entier d diviseur de $A(n)$ est premier avec n.

d. Montrer que, pour tout entier d diviseur de $A(n)$:

$$n^8 \equiv 1 \mod d.$$

2. Recherche de critères
Soit d un diviseur de $A(n)$. On note s le plus petit des entiers naturels non nuls k tels que $n^k \equiv 1 \mod d$.

a. Soit k un tel entier. En utilisant la division euclidienne de k par s, montrer que s divise k.

b. En déduire que s est un diviseur de 8.

c. Montrer que si, de plus, d est premier, alors s est un diviseur de $d-1$. On pourra utiliser le petit théorème de Fermat.

3. Recherche des diviseurs premiers de $A(n)$ dans le cas où n est un entier pair.
Soit p un diviseur premier de $A(n)$. En examinant successivement les cas $s = 1$, $s = 2$ puis $s = 4$, conclure que p est congru à 1 modulo 8.

4. *Dans cette question toute trace de recherche, même incomplète, sera prise en compte dans l'évaluation.*
Appliquer ce qui précède à la recherche des diviseurs premiers de $A(12)$.
Indication : la liste des nombres premiers congrus à 1 modulo 8 débute par 17, 41, 73, 89, 97, 113, 137, ...