Exercices d'arithmétique

Exercice 1.26. Compléter avec l'entier naturel le plus petit possible :

$$15 \equiv \dots \quad (2) \qquad ; \qquad 109 \equiv \dots \quad (11) \qquad ; \qquad 71 \equiv \dots \quad (4)$$

$$67 \equiv \dots \quad (7) \qquad ; \qquad 31 \equiv \dots \quad (3) \qquad ; \qquad 80 \equiv \dots \quad (6)$$

Exercice 1.27.

1. Compléter par l'entier le plus petit possible : $90 \equiv \dots \quad [7]$ et $66 \equiv \dots \quad [7]$.
2. En utilisant les propriétés des congruences et sans calculatrice, compléter les résultats suivants en mettant l'entier le plus petit possible :

$$90 + 66 \equiv \dots \quad [7] \qquad 4 \times 90 \equiv \dots \quad [7] \qquad 90 \times 66 \equiv \dots \quad [7]$$

$$90^2 \equiv \dots \quad [7] \qquad 66^3 \equiv \dots \quad [7]$$

Exercice 1.28.

1. Faire les divisions euclidiennes de 200 et 900 par 13 et traduire les résultats en congruences.
2. En utilisant les propriétés des congruences, compléter les résultats suivants en mettant l'entier le plus petit possible :

$$200 + 900 \equiv \dots \quad [13] \qquad 200 \times 900 \equiv \dots \quad [13]$$

$$200^2 \equiv \dots \quad [13] \qquad 900^3 \equiv \dots \quad [13]$$

3. Quel est le reste de la division euclidienne de $200^4 + 900^6$ par 13 ?

Exercice 1.29.

1. Montrer que $1789 \equiv 4 \quad [7]$. Compléter la congruence suivante : $1789^3 \equiv \dots \quad [7]$
2. Montrer que $1789^{1789} = (1789^3)^{596} \times 1789$.
3. Compléter $1789^{1789} \equiv \dots \quad [7]$. Exprimer de résultat avec une phrase évoquant la division euclidienne.

Exercice 1.30. Démontrer que $47^{900} - 25^{900}$ est un multiple de 11, que $393^{500} \equiv 1 \quad (7)$. Déterminer le reste de la division de 142^{142} par 3.

Exercice 1.31. Épreuve de 2013. Un jeu classique consiste à coder des messages. Pour cela, on utilise la correspondance entre les lettres de l'alphabet et un nombre entier x compris entre 0 et 25.

Le tableau ci-dessous donne cette correspondance :

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

Le codage consiste à choisir une clé formée de deux nombres entiers a et b compris entre 0 et 25 et à remplacer une lettre par une autre selon le principe suivant :

— on lit sur le tableau le nombre x correspondant à la lettre ; on calcule le reste r de la division de $ax + b$ par 26 ;

— on lit sur le tableau la lettre correspondant au nombre r qui est donc la lettre codée.

Exemple : avec la clé $(a\ ;\ b) = (7\ ;\ 12)$, pour coder la lettre T , on calcule $7 \times 19 + 12 = 145$, puis le reste de la division euclidienne de 145 par 26, soit 15. La lettre codée est ainsi la lettre P.

1. Coder les lettres A, K et W avec la clé $(a\ ;\ b) = (5\ ;\ 17)$.
2. Que se passe-t-il si on prend $a = 0$ et $b = 17$?
3. On considère un entier x compris entre 0 et 25.
   (a) Donner, sans justification, les restes obtenus dans la division euclidienne de $13x + 6$ par 26 pour x compris entre 0 et 25.
   (b) Coder le mot PREMIER avec la clé (13 ; 6). Commenter le résultat obtenu.
4. Un codage est dit acceptable lorsque deux lettres distinctes quelconques sont toujours codées différemment. On admet que les clés $(a\ ;\ b)$ donnant un codage acceptable sont celles pour lesquelles a est un entier premier avec 26, quel que soit l'entier b compris entre 0 et 25.
   (a) Donner la liste des nombres entiers compris entre 0 et 25 et premiers avec 26.
   (b) Déterminer le nombre de clés donnant un codage acceptable.
5. Le mot ABSURDE a été codé à l'aide d'une clé $(a\ ;\ b)$ selon le principe décrit ci-dessus et l'on a obtenu VOZLGAT. Déterminer cette clé.

Exercice 1.32. Épreuve de 2013 (Polynésie)

Le but de cet exercice est l'étude d'un procédé de cryptage des lettres majuscules de l'alphabet français. Chacune des 26 lettres est associée à l'un des entiers de 0 à 25, selon le tableau de correspondance suivant.

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

Le cryptage se fait à l'aide d'une clé, qui est un nombre entier k fixé, compris entre 0 et 25.

Pour crypter une lettre donnée :
— on repère le nombre x associé à la lettre, dans le tableau de correspondance précédent ;
— on multiplie ce nombre x par la clé k ;
— on détermine le reste r de la division euclidienne de $k \times x$ par 26 ;
— on repère la lettre associée au nombre r dans le tableau de correspondance ; c'est la lettre cryptée.

Par exemple, pour crypter la lettre « P » avec la clé $k = 11$:
— le nombre x associé à la lettre « P » est le nombre 15 ;
— on multiplie 15 par la clé k, ce qui donne $11 \times 15 = 165$;
— on détermine le reste de 165 dans la division par 26 : on trouve 9 ;
— on repère enfin la lettre associée à 9 dans le tableau : c'est « J ».

Ainsi, avec la clé $k = 11$, la lettre « P » est cryptée en la lettre « J ».
On crypte un mot en cryptant chacune des lettres de ce mot.

Partie A - Cryptage d'un mot avec la clé $k = 11$

Dans cette partie, la clé de cryptage est $k = 11$. Le but de cette partie est de crypter le mot « BTS ».

1. Déterminer en quelle lettre est cryptée la lettre « S ». On détaillera les différentes étapes du processus de cryptage.
2. Crypter le mot « BTS ». On ne demande pas le détail du cryptage.

Partie B - Décryptage avec la clé $k = 11$

Dans cette partie, la clé de cryptage est toujours $k = 11$.
Le but de cette partie est de retrouver une lettre initiale connaissant la lettre cryptée.

1. Prouver que $19 \times 11 \equiv 1 \mod 26$.
2. Une lettre associée à un nombre x a été cryptée. Le nombre associé à la lettre cryptée est noté y.
   (a) Justifier que $11 \times x \equiv y \mod 26$.
   (b) Montrer que $19 \times y \equiv x \mod 26$.

   Ces propriétés montrent que pour décrypter une lettre codée y avec la clé $k = 11$, il suffit de crypter cette lettre avec la clé de cryptage $k' = 19$.

   Exemple : si une lettre est codée par $y = 22$, on multiplie 22 par 19 et on prend le reste du résultat dans la division euclidienne par 26 ; on obtient $x = 2$. Donc la lettre de départ est C.
3. Utiliser les résultats précédents pour décrypter le mot « WGA ».

Partie C - Recherche des bonnes clés de cryptage

Une clé k ne possède pas forcément une clé de décryptage associée.
On dit qu'une clé est une bonne clé de cryptage si elle possède une clé de décryptage associée.
On admet qu'une clé k est une bonne clé de cryptage si et seulement si les nombres k et 26 sont premiers entre eux.
Le but de cette partie est de trouver les bonnes clés de cryptage, parmi les nombres entiers compris entre 0 et 25.

1. Décomposer 26 en un produit de facteurs premiers.
2. En déduire la liste des nombres k compris entre 0 et 25 qui sont de bonnes clés de cryptage.

Exercice 1.33. Épreuve de 2014

Partie A

1. (a) Décomposer le nombre 2 014 en produit de facteurs premiers.
   (b) En déduire la liste des diviseurs positifs de 2 014.
2. Calculer le PGCD des nombres 2 014 et 212. On note d ce PGCD.
   Déterminer l'entier p tel que : $2\,014 = p \times d$.

Partie B

Un jury de concours doit établir l'ordre de passage des 2014 candidats qui doivent passer une épreuve orale. Le président du jury envisage la procédure automatique décrite ci-après.

Tout d'abord, il classe les 2 014 candidats par ordre alphabétique et attribue à chacun, en suivant cet ordre, un numéro allant de 1 à 2 014. Ainsi, pour définir un ordre de passage à l'oral des candidats il suffit de dresser la liste des numéros des candidats qui seront appelés l'un après l'autre à passer l'épreuve orale.

Pour établir cette liste, le président du jury choisit un entier n compris entre 1 et 400, puis procède de la manière suivante :

- le premier numéro inscrit sur la liste est le nombre n ;

- le deuxième numéro inscrit sur la liste est le nombre $2n$;
- le troisième numéro inscrit est le nombre $3n$;
- de faàçon générale, pour obtenir chaque numéro inscrit à partir du deuxième, on ajoute n au numéro précédent et :
  - — si la somme s obtenue est inférieure ou égale à 2 014, le numéro inscrit est égal à cette somme s ;
  - — sinon, le numéro inscrit est égal à $s - 2\,014$.

Par exemple, en choisissant la valeur $n = 257$, les premiers numéros inscrits sur la liste sont, dans l'ordre :

257–514–771–1 028–1 285–1 542–1799–42–299–556–...– etc.

En effet :

- le premier numéro inscrit est $n = 257$;
- du 2e numéro (égal à 514) au 7e numéro (égal à 1 799), on a ajouté 257 au numéro précédent puisque la somme ne dépassait pas 2 014 ;
- le 8e numéro inscrit est le numéro 42 car $1\,799 + 257 = 2\,056$ et, comme 2 056 dépasse 2 014, le numéro à inscrire est $2\,056 - 2\,014 = 42$.

Ainsi le candidat 257 passera en premier l'oral ; il sera suivi du candidat 514 et ainsi de suite.
Le président du jury se demande si cette procédure permet de convoquer tous les candidats, c'est-à -dire si la liste obtenue, en 2 014 étapes, contient tous les nombres de 1 à 2 014.

1. Dans cette question, le président du jury choisit $n = 212$.
   (a) Les 9 premiers numéros inscrits sont donc :

   212–424–636–848–1 060–1 272–1 484–1 696–1 908.

   Donner la liste des 15 numéros suivants.
   La valeur $n = 212$ permet-elle de convoquer tous les candidats ?
   (b) Avec cette valeur de n, combien de numéros différents la liste comporte-t-elle ?
2. Dans cette question, le président du jury choisit $n = 38$.
   Déterminer combien de numéros différents comporte la liste. Justifier la réponse. On pourra remarquer que 38 est un diviseur de 2 014.

Partie C

D'après la partie B, il apparait que, pour certaines valeurs de n, la procédure utilisée ne permet pas de convoquer tous les candidats, c'est-à -dire de constituer une liste comportant tous les nombres de 1 à 2 014.
On admet le résultat suivant :
≪ Le nombre n choisi permet de former une liste complète comportant tous les numéros de 1 à 2 014 dans le cas où le PGCD de 2 014 et de n est égal à 1, et dans ce cas seulement ≫.
Ainsi, les nombres n permettant de convoquer tous les candidats sont les entiers n compris entre 1 et 400 qui sont premiers avec 2 014.

1. Si $n = 15$, la procédure utilisée permet-elle de convoquer tous les candidats ?
2. Dans cette question, on cherche à déterminer le nombre d'entiers n, parmi ceux compris entre 1 et 400, qui permettent par la procédure utilisée de convoquer tous les candidats.
   (a) Donner le nombre de multiples de 2 non nuls, inférieurs ou égaux à 400.
   (b) Donner la liste des multiples **impairs** de 19, inférieurs ou égaux à 400.
   (c) Donner la liste des multiples **impairs** de 53, inférieurs ou égaux à 400.
   (d) En déduire le nombre d'entiers n qui ne permettent pas de convoquer tous les candidats, puis le nombre d'entiers n qui le permettent.

Exercice 1.34. Déterminer[2] le chiffre des unités de 227^{541} et de 743^{2018}.

(on pourra utiliser le fait que tout entier naturel est congru au chiffre de ses unités modulo 10).

2. 100% exos Hatier 2004, 30 page 17.