2013-2014

Les cours du Lycée J. Durand

Mathématiques

Terminale S

Enseignement de spécialité

Rédaction :

David Zancanaro

Réalisé à l'aide de :

LaTeX

Table des matières

Leçon 1

Arithmétiques et problèmes de codage

LSB \ MSB	8 1000	9 1001	A 1010	B 1011	C 1100	D 1101	E 1110	F 1111
0 0000	Ç	É	á	▒	└	ð	Ó	-
1 0001	ü	æ	í	▓	┴	Ð		±
2 0010	é	Æ	ó	▓	┬	Ê	ô	‗
3 0011	â	ô	ú	│	├	Ë	ò	¾
4 0100	ä	ö	ñ	┤	─	È	õ	¶
5 0101	à	ò	Ñ	Á	┼	ı	Õ	§
6 0110	å	û	ª	Â	ã	Í	µ	÷
7 0111	ç	ù	º	À	Ã	Î	þ	¸
8 1000	ê	ÿ	¿	©	╚	Ï	Þ	°
9 1001	ë	Ö	®	╣	╔	┘	Ú	¨
A 1010	è	Ü	¬	║	╩	┌	Û	·
B 1011	ï	ø	½	╗	╦	█	Ù	¹
C 1100	î	£	¼	╝	╠	▄	ý	³
D 1101	ì	Ø	¡	¢	=	¦	Ý	²
E 1110	Ä	×	«	¥	╬	Ì	¯	■
F 1111	Å	ƒ	»	┐	¤	▀	´	

I. Divisibilité dans $\mathbb{Z}$

I.1. Définition

Exercice 1. Les codes-barres sont omniprésents dans la vie courante. Ils trouvent leurs applications dans des domaines aussi variés que la gestion des prêts d'une bibliothèque, les caisses enregistreuses à lecture optique ou le contrôle de la production dans l'industrie.
Les codes-barres.
Les codes EAN 13 (European Article Numbering à 13 chiffres) sont des codes-barres utilisés dans le monde entier sur l'ensemble des produits de grande consommation. Ils comportent 13 chiffres :

- les deux premiers chiffres correspondent au pays de provenance du produit ou à une classe normalisée de produits ;
- les quatre chiffres suivants correspondent au codage du fabriquant ;
- les six suivants forment le numéro d'article ;
- le treizième chiffre est une clé de contrôle calculée en fonction des douze précédents.

La clé de contrôle sert à la vérification de la bonne saisie du code. Nous allons nous intéresser à son calcul.
Calcul de la clé de contrôle
Un code-barres est symbolisé par le tableau suivant :

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	R

où $C_1, C_2, \ldots, C_{12}$ et R sont les 13 chiffres constituant le code-barres ; R est donc la clé.
Les chiffres $C_1, C_3, \ldots, C_{11}$ sont ceux de rangs impairs et $C_2, C_4, \ldots, C_{12}$ sont les chiffres de rangs pairs.
La clé R est calculée de telle sorte que :

[(**somme des chiffres de rang impair**) + 3(**somme des chiffres de rang pair**) + R] est un multiple de 10

1. Vérifier que l'on ne détecte pas d'erreur dans le code-barres ci-dessous.

2. Déterminer la clé associée au code-barres suivant :

3. Le système de lecture optique d'une caisse enregistreuse étant défectueux, un employé doit saisir les codes à la main. Parmi les codes saisis, lesquels comportent à coup sûr une erreur ?

9782940199617

9782940199167

3782940199617

4. Calculer la clé des deux codes suivants :

1672345678900

7612345678900

Toutes les erreurs de saisie peuvent-elles être détectée grâce à la clé de contrôle ?

5. Déterminer x sachant que le code est le suivant :

$374284x179317$

Remarques :

– La clé de contrôle permet de détecter des erreurs de saisie d'un code-barres (l'inversion de deux chiffres consécutifs ou un chiffre erroné par exemple) mais elle ne permet pas de détecter toutes les erreurs.

– Le calcule de la clé de contrôle fait appel à la notion de divisibilité, objet d'étude de ce premier chapitre.

Définition 1.

Soient a et b deux entiers relatifs quelconques. (On note $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$).
On dit que a est un multiple de b, ou que b divise a ou encore que b est un diviseur de a si et seulement si il existe un entier relatif k tel que :

$$a = b \times k$$

On note $b|a$

Remarques :

- 1 et -1 divisent tous les entiers relatifs.
- Un nombre a admet au minimum 4 diviseurs : $\{-a;-1;1;a\}$. Dans le cas où a a exactement 4 diviseurs, a est un nombre premier.
- La relation de divisibilité est *réflexive* i.e a divise a.
- L'ensemble des multiples de a se notent $\{ak,\text{ où } k\in\mathbb{Z}\}$; par exemple l'ensemble des multiples de 7 se note donc $\{7k,\text{ où } k\in\mathbb{Z}\}=\{\ldots,-21;-14;-7;0;7;14;21;\ldots\}$
- 0 est un multiple de tous les nombres ce qui revient à dire que tous les entiers relatifs divisent 0.

Exercice 2.

Partie A

Un triangle rectangle a des côtés de longueurs entières. L'un des côtés de l'angle droit a pour longueur 6. On aimerait déterminer les longueurs des deux autres côtés.

1. En notant x et y les longueurs cherchées (avec $x>y$), vérifier que le problème se traduit par :
$$(x-y)(x+y)=36$$
2. Quels sont les diviseurs positifs de 36 ?
3. Quels sont les couples d'entiers naturels $(a;b)$ tels que $ab=36$?
4. En déduire les différentes solutions du problème.

Partie B

Ayant à traiter un grand nombre de tels triangles, on cherche à systématiser la recherche des couples $(a;b)$ tels que $ab=n$ où n est un entier naturel.
On propose l'algorithme suivant :

Algorithme 1 :

Données: n est un entier naturel, $n>2$.
Entrer n
Pour j allant de 1 à $\text{E}(\sqrt{n})$ **Faire**
  Remarque : La fonction E utilisée ici est la fonction « partie entière ».
  Si (j est un diviseur de n) **Alors**
    Afficher j
    Afficher $\dfrac{n}{j}$
  Fin Si
Fin Pour

1. Quels sont les affichages obtenus en faisant tourner cet algorithme pour $n=36$? $n=38$?
2. On veut programmer cet algorithme sur un ordinateur.
   (a) Comment traduire la condition « j est un diviseur de n » ?

(b) Programmer cet algorithme.

(c) Vérifier vos réponses à la question 2.

3. Soient a et b deux entiers naturels tels que $ab = n$ avec $a \leq b$.
Montrer que l'on a $a \leq \sqrt{n} \leq b$. En déduire que le programme proposé affiche bien tous les couples d'entiers naturels $(a;b)$ tels que $ab = n$.

```
def triangle(n):
    p=[]
    e=int(sqrt(n))
    for i in range(1,e+1):
        if int(n/i)==n/i:
            l=[]
            l.append(i)
            l.append(int(n/i))
            p.append(l)
    return p
n=36
print(triangle(n))
```

```
Python 3.3.2 Shell
File  Edit  Shell  Debug  Options  Windows  Help
>>>
[[1, 36], [2, 18], [3, 12], [4, 9], [6, 6]]
>>>
```

Exercice 3. Un cube est constitué de n^3 petits cubes identiques, où n est un entier supérieur ou égal à 2.
On lui en enlève un petit cube et on souhaite regrouper les petits cubes restants en plusieurs paquets identiques.

1. Vérifier qu'un tel regroupement n'est pas possible pour $n = 2$.
2. On suppose $n > 2$
   (a) Vérifier que $8^3 - 1$ est divisible par 7.
   (b) Vérifier que $23^3 - 1$ est divisible par 22.
   (c) Conjecturer un diviseur de $n^3 - 1$ pour un entier n quelconque.
   (d) Prouver votre conjecture.
   (e) proposer une solution au problème.

Exercice 4. Déterminer les entiers naturels n tels que 6 divise $n + 17$

Exercice 5. Déterminer les entiers naturels n tels que $2n - 5$ divise 6

I.2. Propriétés

Bien que ces propriétés soient relativement simples on portera une attention toute particulière à leurs démonstrations, qui donneront de bons réflexes pour les exercices.

Propriété 1.

Si b divise a alors $-b$ divise a, et réciproquement.

Preuve

En effet si $b|a$ alors $\exists k \in \mathbb{Z}$ tel que $a = bk \iff a = (-b) \times (-k)$. $-k$ est un entier relatif par conséquent $-b|a$.

Remarques :

- a et $-a$ ont donc les mêmes diviseurs dans $\mathbb{Z}$ et les diviseurs négatifs de a sont les opposés des diviseurs positifs de a.
  Ainsi on se restreindra pour la recherche des diviseurs dans $\mathbb{Z}$ à la recherche des diviseurs dans $\mathbb{N}$ et on complètera par les opposés.
- Tout nombre $a \in \mathbb{Z}$ admet un nombre fini de diviseur, compris $-a$ et a.

Exemple :

On a vu que les diviseurs positifs de 36 sont $\{1;2;3;4;6;9;12;18;36\}$ donc les diviseurs de 36 dans $\mathbb{Z}$ sont $\{-36;-18;-12;-9;-6;-4;-3;-2;-1;1;2;3;4:6;9;12;18;36\}$

Exercice 6. Déterminer l'ensemble des diviseurs de 42

Propriété 2.

Si b divise $a \neq 0$ alors $|b| \leq |a|$.

Preuve

$b|a \iff \exists k \in \mathbb{Z} / a = bk \implies |a| = |b| \times |k|$. Puisque a est non nul, il est en de même pour k donc $|k| \geq 1$ d'où :

$$|a| \geq |b|$$

Propriété 3.

Si $a|b$ et $b|a$ alors $a = b$ ou $a = -b$

Preuve

D'après la propriété précèdente, si $a|b$ alors $|a| \leq |b|$. De même puisque $b|a$ alors $|a| = |b|$ ce qui permet de conclure que $a = \pm b$.

Propriété 4.

Si $a|b$ et $b|c$ alors $a|c$.
La relation de divisibilité est *transitive*.

Preuve

$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = ak$, de même $b|c \iff \exists k' \in \mathbb{Z}$ tel que $c = bk'$
Ces deux égalités impliquent que :

$$c = akk'$$

$kk' \in$ Z en tant que produit de deux entiers relatifs donc $a|c$.

Propriété 5.

Si $a|b$ alors a divise tout multiple de b i.e $a|bc$ pour tout entier c.

Preuve

$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = ak \implies bc = akc$, puisque $kc \in \mathbb{Z}$ $a|bc$.

Propriété 6.

Si $a|b$ alors $ac|bc$ pour tout entier c.

Preuve

$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = ak \implies bc = ack$, puisque $k \in \mathbb{Z}$ alors $ac|bc$

Propriété 7.

Si $a|b$ et $a|c$ alors quelque soit les entiers u et v on a :

$$a|ub + vc$$

Preuve

$a|b \iff \exists k \in \mathbb{Z}$ tel que $b = ak$, de même :
$a|c \iff \exists k' \in \mathbb{Z}$ tel que $c = ak'$, d'où :
$ub = auk$ et $vc = ak'v$ ce qui implique que :

$$ub + vc = auk + ak'v = a(uk + k'v)$$

Puisque $uk + k'v \in \mathbb{Z}$ on a $a|ub + vc$.

Exercice 7. Déterminer les entiers n tels que $2n+3$ divise $n-2$

Exercice 8. Soit n un entier naturel, montrer que les diviseurs communs de $10n+3$ et $6n+1$ sont des diviseurs de 4

Exercice 9. Démontrer par récurrence que pour $n \in \mathbb{N}*$, $3^{2n} - 2^n$ est divisible par 7.

Exercice 10. En choisissant le raisonnement qui vous semble le plus judicieux(raisonnement par l'absurde, par disjonction de cas, par contraposée, par la recherche d'un contre-exemple), répondre aux questions suivantes :

1. Montrer que $3n+7$ n'est pas divisible par 3 pour tout entier naturel n
2. Pour tout entier n, si n^2 est impair alors n est impair.
3. Pour tout entier n, l'entier $n(n+1)$ est pair
4. L'entier n^2-n+3 est-il divisible par 3 pour tout entier naturel n ?

Exercice 11. Un entier naturel est parfait s'il est égal à la somme de ses diviseurs positifs autres que lui-même.
Parmi les entiers suivants déterminer ceux qui sont parfaits : 20, 28 et 104.

Exercice 12. On veut déterminer les entiers relatifs $n \neq -2$ tels que $\dfrac{2n-29}{n+2}$ soit un entier.

1. Montrer que si n esy solution alors $n+2$ divise 33. [1]
2. Etablir la liste des diviseurs de 33 dans $\mathbb{Z}$.
   En déduire les valeurs possibles de n.
3. Conclure.

1. Utiliser la propriété 7

II. Division euclidienne

Exercice 13. Le relevé d'identité bancaire (RIB) est formé :

- d'un nombre de 21 chiffres :
  - cinq chiffres identifiant la banque,
  - cinq chiffres identifiant le guichet et,
  - onze chiffres représentant le numéro du compte.
- suivi d'un nombre de 2 chiffres qui est une clé de détection d'erreur dans l'un des 21 précédents.

La clé est définie ainsi :
On note A le nombre constitué des 21 chiffres on calcule le reste r de la division euclidienne de 100A par 97 ; la clé K est alors définie par $K = 97 - r$.
Soit A = 200410101278340238431.

1. Ecrire 100A sous la forme $a \times 10^{12} + b \times 10^6 + c$ avec $0 \leq c < 10^6$ et dire combien de chiffres comporte 100A.
2. Identifier a, b et c.
3. Calculer le reste de la division euclidienne de 10^6 par 97 puis de 10^{12} par 97.
4. Calculer la clé du nombre A.

II.1. Division euclidienne dans $\mathbb{N}$

Théorème 1.

Pour tout entier naturel a et pour tout entier naturel b non nul, il existe un unique couple $(q;r)$ d'entiers naturels tels que :

$$a = bq + r \qquad \text{avec } 0 \leq r < b$$

Preuve

- Existence du couple $(q;r)$ Posons $q = \text{E}\left(\frac{a}{b}\right)$.
  q est donc un entier naturel tel que $q \leq \frac{a}{b} < q+1$
  Puisque $b > 0$ on a $bq \leq b\frac{a}{b} < b(q+1)$ c'est à dire $bq \leq a < bq + b \iff 0 \leq a - bq < b$
  Posons $r = a - bq$, on a : $a = bq + r$ et $0 \leq r < b$
  Ainsi pour tout entier relatif a et tout entier naturel b non nul, on a trouvé deux entiers naturels q et r tels que $a = bq + r$ et $0 \leq r < b$
- unicité du couple $(q;r)$ Raisonnons par l'absurde et supposons qu'il existe deux couples d'entiers naturels (q,r) et (q',r') tels que : $a = bq + r = bq' + r'$ et $0 \leq r < b$ et $0 \leq r' < b$
  Par différence : $r - r' = b(q' - q)$ ainsi $r - r'$ est un multiple de b. Ce multiple est compris entre $-b$ et b donc cela ne peut être que 0. donc $r = r'$.
  Donc $b(q' - q) = 0$ et $b \neq 0$ donc $q' = q$. Les deux couples sont identiques.

Définition 2.

Pour tout entier relatif a et tout entier naturel b non nul, les entiers relatifs q et r vérifiant $a = bq + r$ et $0 \leq r < b$ sont respectivement appelés **quotient** et **reste** de la division euclidienne de a par b. a est le dividende et b le diviseur.

Exercice 14. En athlétisme, le 3000 mètres steeple se court sur une piste de 390 mètres de long passant par le saut d'une rivière.
A quelle distance avant la ligne d'arrivée doit-on positionner la ligne de départ ?

Exercice 15.

1. Le reste de la division euclidienne de l'entier naturel a par 18 est 13.
   Quel est le reste de la division euclidienne de a par 9 ? par 6 ? par 3 ?
2. (a) Montrer que tout entier naturel n s'écrit nécessairement sous l'une des trois formes $3k$, $3k+1$, $3k+2$ avec $k \in \mathbb{N}$.
   (b) Montrer que dans la division euclidienne de (n^2+n) (où n est un entier quelconque) par 3, le reste n'est jamais égal à 1.

II.2. Division euclidienne dans $\mathbb{Z}$

Cela n'a qu'une importance toute relative (et théorique) mais on peut définir la division euclidienne dans $\mathbb{Z}$:

Théorème 2.

Pour deux entiers relatifs a et b (avec $b \neq 0$), il existe un unique couple $(q;r)$ avec $q \in \mathbb{Z}$, $r \in \mathbb{N}$; tel que :

$$a = bq + r \qquad \text{avec } 0 \leq r < |b|$$

Définition 3.

q est alors le quotient et r le reste de la division euclidienne de a par b.

Remarque : $b|a$ si et seulement si, le reste de la division euclidienne de a par b est nul.

Exercice 16. Effectuer les divisions euclidiennes de a par b pour chacun des quatre cas suivants :

1. $a = 2013$ et $b = 7$;
2. $a = 2013$ et $b = -7$;
3. $a = -2013$ et $b = 7$;
4. $a = -2013$ et $b = -7$.

Preuve

La démonstration du théorème précédent est quasiment identique à celle effectué dans le cas où a et b sont des entiers naturels ; en particulier l'unicité du couple $(q;r)$ se démontre comme précédemment. En ce qui concerne l'existence il convient de distinguer les cas suivants, et de vérifier que les couples proposées fonctionnent :

- $a>0$ et $b>0$ alors $q=\mathrm{E}\left(\frac{a}{b}\right)$ et $r=a-bq$.
- $a<0$ et $b>0$ alors $q=\mathrm{E}\left(\frac{a}{b}\right)$ et $r=|bq|-|a|$
- $a>0$ et $b<0$ alors $q=\mathrm{E}\left(\frac{a}{b}\right)+1$ et $r=a-bq$
- $a<0$ et $b<0$ alors $q=\mathrm{E}\left(\frac{a}{b}\right)$ et $r=|bq|-|a|$
- si $a=0$ alors $q=0=r$

Exercice 17.

1. Montrer, en effectuant une division euclidienne posée, que le développement décimal d'un rationnel est périodique.
2. Réciproquement, montrer qu'un réel dont le développement décimal est périodique est un rationnel.
3. (a) Quelle est la période du développement décimal de $\frac{3}{7}$?
   (b) Quelle fraction possède pour développement décimal $0,\overline{63}$? $34,\overline{63}$? $0,\overline{0,99}$? $31,123\overline{45}$?

Exercice 18. Que peut-on dire d'une suite d'entier naturel strictement décroissante ? [2]

Exercice 19.

1. Effectuer la div euclidienne de 3217 par 19, de -1273 par 17, de 228 par -15 et de -329 par -30.
2. Déterminer des entiers naturels a et b tels que leur somme soit égale à 283 et que dans la division de a par b, le quotient soit 5 et le reste 13.
3. n désigne un entier naturel.
   (a) Réaliser la division de n^2+2n+2 par $n+3$ pour montrer que $n^2+2n+2=(n+3)(n-1)+5$.
   (b) Déterminer les entiers naturels n tels que $\frac{n^2+2n+2}{n+3}\in\mathbb{N}$
4. Soit $n$un entier naturel non nul. Effectuer la division euclidienne de :
   (a) $2n^2+n$ par $n+1$; (b) n^2+2n+3 par $n+2$; (c) 3^n-2 par 3^{n-1}.

Page suivante l'exemple d'un programme en python basé sur cette démonstration :

2. L'ensemble $\mathbb{N}$ est archimédien i.e que toute ensemble non vide de $\mathbb{N}$ possède un plus petit élément. Ce n'est pas le cas pour l'ensemble des réels positifs.

```
def eucl(a,b):
    qr=[]
    if a==0:
        q,r=0,0
        qr.append(q)
        qr.append(r)
        if a==b*q+r and r<abs(b):
            print('ce programme marche très bien')
        else:
            print('Il est impossible de voir ce message')
        return(qr)
    if a>0 and b>0:
        q,r=floor(a/b),a-b*q
        qr.append(q)
        qr.append(r)
        if a==b*q+r and 0<=r<abs(b):
            print('ce programme marche très bien')
        return(qr)
    if a<0 and b>0:
        q,r=floor(a/b),abs(b*q)-abs(a)
        qr.append(q)
        qr.append(r)
        if a==b*q+r and 0<=r<abs(b):
            print('ce programme marche très bien')
        return(qr)
    if a>0 and b<0:
        q,r=floor(a/b)+1,a-b*q
        qr.append(q)
        qr.append(r)
        if a==b*q+r and 0<=r<abs(b):
            print('ce programme marche très bien')
        return(qr)
    if a<0 and b<0:
        q,r=floor(a/b)+1,abs(b*q)-abs(a)
        qr.append(q)
        qr.append(r)
        if a==b*q+r and 0<=r<abs(b):
            print('ce programme marche très bien')
        return(qr)
```

```
>>>
Respectivement le quotient et le reste de la division de  2013 par 7 sont :
ce programme marche très bien
[287, 4]
>>> ================================ RESTART ================================
>>>
Respectivement le quotient et le reste de la division de  2013 par -7 sont :
ce programme marche très bien
[-287, 4]
>>> ================================ RESTART ================================
>>>
Respectivement le quotient et le reste de la division de  -2013 par 7 sont :
ce programme marche très bien
[-288, 3]
>>> ================================ RESTART ================================
>>>
Respectivement le quotient et le reste de la division de  -2013 par -7 sont :
ce programme marche très bien
[288, 3]
>>>
```

III. Congruence

Exercice 20. L'année 2012 a débuté par un Dimanche.

1. Calculer N le nombre de jours qui séparent sa propre naissance, du 1er janvier 2012.
   Attention : tous les 4 ans, il y a une année bissextile qui compte 366 jours : 2000 était une année bissextile.
2. Calculer le reste de la division euclidienne de N par 7. Expliquer le choix du nombre 7.
3. En déduire le jour de sa propre naissance.

Exemple :
Mr.Z est né le

25 avril 1982

Curieux il aimerait savoir à quel jour de la semaine cela correspond.
On sait que le premier jour de 2012 était un dimanche.
Entre le 25 avril 1982 et le 1 janvier 2012 il s'est écoulé

$$2012 - 1982 - 1 = 29 \text{ années complètes}$$

Or, $29 = 4 \times 7 + 1$, parmi ces 29 années 7 furent bissextiles et donc 22 ne le furent pas, au total il y eut :

$$366 \times 7 + 365 \times 22 = 10592 \text{ journées}$$

Du 25 avril jusqu'au terme de cette merveilleuse année 1982 on dénombre pas moins de :

$$30 - 25 + 1 + 31 + 30 + 31 + 31 + 30 + 31 + 30 + 31 = 6 + 31 \times 5 + 30 \times 3 = 251 \text{ jours}$$

Notons que durant le mois d'avril pour le jeune bébé 6 jours sont passés.
Ainsi nous concluons qu'entre le 25 avril 1982 et le 1 janvier 2012 :

$$\text{Monsieur Z. a vécu } 251 + 10592 = 10843 \text{ journées paisibles.}$$

Enfin $10843 \equiv 0[7]$, on en conclut que Mr. Z est né un dimanche, ce qui explique beaucoup de choses...

Définition 4.

Soit a et b deux entiers relatifs.
Soit $n \in \mathbb{N}^*$, on dit que a et b sont congrus module n si, et seulement si, a et b ont le même reste dans la division euclidienne par n. On écrit :

$$a \equiv b(n) \qquad \text{ou} \qquad a \equiv b[n]$$

Exemples :
Puisque $145 = 13 \times 11 + 2$ et $119 = 13 \times 9 + 2$ on conclut que :

$$145 \equiv 119[13]$$

Exercice 21. Vérifier que $29 \equiv -121[5]$ et $-623 \equiv 17[10]$.

Remarque : Si le reste de la division euclidienne de a par n est r alors $a \equiv r[n]$. Dès lors que $0 \leq r < n$ et $a \equiv r[n]$ alors r est le reste de la division euclidienne de a par n.

Voici une propriété très pratique :

Propriété 8.

Pour tout entier naturel $n \geq 2$ on a :

$$a \equiv b[n] \quad \text{si, et seulement si} \quad n \text{ divise } a-b$$

Preuve
$\Rightarrow$: Si $a \equiv b[n]$ alors il existe un unique couple (q,r) d'entiers tel que $a = qn + r$ avec $0 \leq r < n$ et un unique couple (q',r) d'entiers tels que $b = q'n + r$.
Donc $a - b = qn - q'n = (q-q')n$ et $n|(a-b)$
$\Leftarrow$: Si $n|(a-b)$ alors il existe $k \in \mathbb{N}$ tel que $a - b = kn$.
D'après la division euclidienne, il existe un unique couple (q,r) avec $0 \leq r < n$ tel que $a = qn + r$ et un unique couple (q',r') avec $0 \leq r' < n$ tel que $b = q'n + r'$.
Donc $a - b = (q-q')n + r - r'$ avec $-n < r - r' < n$. Comme $a - b$ est un multiple de n on a $r - r'$ est un multiple de n.
Or $r - r' \in \mathbb{N}$ et le seul multiple de n dans $]-n;n[$ est 0. Donc $r = r'$ et $a \equiv b[n]$

Exercice 22. Vérifier à l'aide de cette propriété que $29 \equiv -121[5]$ et $-623 \equiv 17[10]$.

Propriété 9.

Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$

Preuve
Puisque $a \equiv b[n]$ et $b \equiv c[n]$ on en déduit que $n|a-b$ et que $n|b-c$, par conséquent $n|1 \times (a-b) + 1 \times (b-c)$ i.e :

$$n|a-c$$

Et donc

$$a \equiv c[n]$$

Propriété 10.

$a \equiv 0\,[n] \iff n|a$

Preuve

$a \equiv 0\,[n] \iff n|a-0 \iff n|a$

Propriété 11.

Si $n'|n$ alors $a \equiv b\,[n] \Rightarrow a \equiv b\,[n']$

Preuve

Puisque $a \equiv b[n]$ on a $n|a-b$ et comme de plus $n'|n$ on a encore $n'|a-b$ par conséquent :

$$a \equiv b[n']$$

Notons que la réciproque, pour s'en convaincre observons l'exemple suivant :

$$10|20 \quad 12 \equiv 2[10]$$

or, 12 n'est pas congrue à 2 modulo 20 puisque 20 ne divise pas $12-2=10$.

Théorème 3.

On note a, a', b et b' quatre entiers relatifs quelconques et $n \geq 2$ un entier naturel. Si $a \equiv a'\,[n]$ et $b \equiv b'\,[n]$ alors :

$$a+b \equiv a'+b'\,[n]$$
$$a-b \equiv a'-b'\,[n]$$
$$ab \equiv a'b'\,[n]$$
$$\forall k \in \mathbb{Z}, \quad ka \equiv ka'\,[n]$$
$$\forall p \in \mathbb{N}, \quad a^p \equiv a'^p\,[n]$$

Remarque : $ka \equiv ka'\,[n] \not\Rightarrow a \equiv a'\,[n]$

Contre-Exemple :

$16 \equiv 20\,[4]$ mais 8 et 10 ne sont pas congrus modulo 4

Preuve

Si $a \equiv a'\,[n]$ il existe $k_1 \in \mathbb{N}$ tel que $a = a' + k_1 n$ Si $b \equiv b'\,[n]$ il existe $k_2 \in \mathbb{N}$ tel que $b = b' + k_2 n$
Donc :

$$a+b = (a'+b') + n(k_1+k_2) \quad \text{Donc } a+b \equiv a'+b'\,[n]$$

$$a-b = (a'-b') + n(k_1-k_2) \quad \text{Donc } a-b \equiv a'-b'\,[n]$$

$$ab = (a'+k_1 n)(b'+k_2 n) = a'b' + n(a'k_2 + b'k_1 + k_1 k_2 n) \quad \text{Donc } ab \equiv a'b'\,[n]$$

$$\forall k \in \mathbb{Z}, \quad ka = ka' + nk_1 \quad \text{Donc } ka \equiv ka'\,[n]$$

On démontre cette partie par récurrence :
Initialisation : On a $a^1 \equiv a'^1\,[n]$
Hérédité : On suppose que la propriété est vraie au rang k, donc que $a^k \equiv a'^k\,[n]$
Alors $a^{k+1} = a^k \times a \equiv a'^k\,[n]$. Donc $a^{k+1} \equiv a'^{k+1}\,[n]$.
La propriété est héréditaire et vraie au rang 1. Elle est vraie pour tout $p \in \mathbb{N}^*$

Exercice 23. Une annale des temps très ancien - Asie 2002

On considère les suites (x_n) et (y_n) définies par $x_0 = 1$, $y_0 = 8$ et

$$\begin{cases} x_{n+1} = \dfrac{7}{3}x_n + \dfrac{1}{3}y_n + 1 \\ y_{n+1} = \dfrac{20}{3}x_n + \dfrac{8}{3}y_n + 5 \end{cases}, \; n \in \mathbb{N}$$

1. Montrer, par récurrence, que les points M_n de coordonnées $(x_n\,;\,y_n)$ sont sur la droite (Δ) dont une équation est $5x - y + 3 = 0$. En déduire que $x_{n+1} = 4x_n + 2$.
2. Montrer, par récurrence, que tous les x_n sont des entiers naturels. En déduire que tous les y_n sont aussi des entiers naturels.
3. Montrer que :
   (a) x_n est divisible par 3 si et seulement si y_n est divisible par 3.
   (b) Si x_n et y_n ne sont pas divisibles par 3, alors ils sont premiers entre eux.
4. (a) Montrer, par récurrence, que $x_n = \dfrac{1}{3}\left(4^n \times 5 - 2\right)$.
   (b) En déduire que $4^n \times 5 - 2$ est un multiple de 3, pour tout entier naturel n.

Exercice 24. Le numéro **INSEE** (Institut National des Statistiques et des Etudes Economiques) d'un individu est constitué de 15 chiffres.
Le premier chiffre est 1 si le sujet est un homme, 2 si le sujet est une femme ;
les deux suivants correspondent aux deux derniers chiffres de son année de naissance ;
les deux suivants correspondent au mois de sa naissance ;
les deux suivants correspondent au département de sa naissance ;
les trois suivants correspondent au numéro de la commune de sa naissance ;
les trois derniers correspondent au numéro d'inscription sur le registre d'état civil ;
les trois derniers correspondent au numéro d'inscription sur le registre d'état civil.
On accorde à ce numéro, une clé de 2 chiffres calculée à partir des 13 précédents.
Par exemple le numéro :2960622645001 est celui d'une femme, née en 1996, au mois de Juin dans le département des côtes d'Armor, dans la commune 645 ; elle est la première enregistrée au mois de Juin.
Le calcul de la clé suit l'algorithme suivant :

Algorithme 2 :

Données: A est un entier constitué de 13 chiffres.
r et K sont des nombres entiers.
Entrer A
r est le reste de la division euclidienne de A par 97.
K vaut $97 - r$.
Afficher K

On appelle A **le numéro INSEE de l'exemple précédent.**

1. Calculer la clé K de A
2. On écrit A sous la forme $A = x \times 10^6 + y$ avec $0 \leq y < 10^6$, montrer que $10^6 \equiv 27[97]$. En déduire que $r \equiv 27x + y[97]$.
3. Déterminer la clé de son propre numéro INSEE.

Exercice 25. Démontrer que $2^{3n} - 1$ est divisible par 7 pour tout $n \in \mathbb{N}$.

Exercice 26. Démontrer que $671^{800} - 1$ est divisible par 6.

Exercice 27. Le but de cet exercice est de calcuer le reste de la division par 7 du nombre 247^{349}

1. Vérifier que $247 \equiv 2\,[7]$
2. Vérifier que $2^{3k} \equiv 1$, $2^{3k+1} \equiv 2$,$2^{3k+2} \equiv 4\,[7]$
3. En déduire le reste de la division de 247^{349} par 7.

Exercice 28.

1. Le nombre $A = 1305^{1305} + 900^{900}$ est-il divisible par 29 ?
2. On considère un entier naturel n supérieur ou égal à 2.
   Calculer le reste de la division euclidienne de 27^{2012} par 7.
   On pourra utiliser le fait que :
   $$n - 1 \equiv -1[n]$$

3. (a) Quel est le reste de la division euclidienne de 1000 par 37 ?
   (b) En déduire que pour tout entier naturel n, le reste de la division euclidienne de 10^{3n} par 37 est égal à 1.
   (c) Quel est le reste de la division euclidienne du nombre $N = 10^{10} + 10^{20} + 10^{30}$ par 37 ?

Exercice 29. On considère un entier n quelconque.

1. Quels sont les restes possibles de la division euclidienne de n^2 par 5 ?
2. Quels sont les restes possibles de la division euclidienne de n^3 par 5 ?

Exercice 30.

1. Déterminer le reste dans la division euclidienne de 25×2^{17} par 7
2. Montrer que, pour tout entier n, $7^n + 3^n + 2$ est divisible par 4.

Exercice 31. Une annale des temps anciens - Amérique du nord 2006

1. *Cette question constitue une restitution organisée de connaissances*
   (a) Soient a, b, c et d des entiers relatifs.
   Démontrer que : si $a \equiv b \mod 7$ et $c \equiv d \mod 7$ alors $ac \equiv bd \mod 7$.
   (b) En déduire que : pour a et b entiers relatifs non nuls
   si $a \equiv b \mod 7$ alors pour tout entier naturel n, $a^n \equiv b^n \mod 7$.
2. Pour $a = 2$ puis pour $a = 3$, déterminer un entier naturel n non nul tel que $a^n \equiv 1 \mod 7$.
3. Soit a un entier naturel non divisible par 7.
   (a) Montrer que : $a^6 \equiv 1 \mod 7$.
   (b) On appelle *ordre* de $a \mod 7$, et on désigne par k, le plus petit entier naturel non nul tel que $a^k \equiv 1 \mod 7$. Montrer que le reste r de la division euclidienne de 6 par k vérifie $a^r \equiv 1 \mod 7$.
   En déduire que k divise 6.
   Quelles sont les valeurs possibles de k ?
   (c) Donner l'ordre modulo 7 de tous les entiers a compris entre 2 et 6.
4. A tout entier naturel n, on associe le nombre

$$A_n = 2^n + 3^n + 4^n + 5^n + 6^n.$$

Montrer que $A_{2006} \equiv 6 \mod 7$.

IV. Application aux codages

IV.1. Les nombres premiers - définitions

Définition 5.

On dit qu'un entier naturel p est premier s'il possède exactement 2 diviseurs positifs : 1 et lui-même.

Exemples :

- 0 n'est pas premier car il admet une infinité de diviseurs
- 1 n'est pas premier car il n'admet qu'*un seul* diviseur : lui-même.
- 2 est le seul nombre premier pair (les autres sont divisibles au moins par 1, eux-mêmes et 2).
- 3, 5, 7, 11, 13 sont des nombres premiers.
- 6 n'est pas un nombre premier, car il est divisible par 1, 6, 2 et 3.

Lemme 1.

Lemme d'euclide

Si un nombre premier p divise le produit ab alors il divise a ou il divise b.

Preuve

Raisonnons par l'absurde i.e supposons qu'il existe deux entiers naturels a et b tels que p divise ab mais ne divise ni a ni b.Notons cette propriété $*$
Pour p et a fixés, considérons le plus petit entier b tel que p divise ab et p ne divise ni a ni b.
Notons r le reste (qui ne vaut pas 0 puisque p ne divise pas b) de la division euclidienne de b par p alors

$$b \equiv r\,[p] \qquad \text{et} \qquad 1 \leq r < p$$

Par conséquent, en multipliant par a on a $ab \equiv ar\,[p]$. Puisque p divise ab alors il divise ar mais ne divise ni a ni r. Puisque b est le plus entier satisfaisant $*$ que r satisfait aussi $*$ alors $b \leq r$.
Notons qu'il existe un entier naturel q tel que $b = pq + r$, par conséquent $b \geq r$ donc $b = r$. Par conséquent :

$$1 \leq b < p$$

Notons alors b' le reste de la division euclidienne de p par b, alors il existe un entier naturel m tel que

$$p = mb + b' \qquad \text{avec } 0 \leq b' < b$$

Si $b' = 0$ alors b divise p qui est un nombre premier. Comme $b \in \mathbb{N}$ et $b < p$ alors $b = 1$, ce qui contredit notre hypothèse de départ (en effet puisque $p|ab = a$ alors p divise a). Par conséquent :

$$1 \leq b' < b < p$$

Enfin $ab' = a(p - mb) = ap - abm$, puisque ab est un multiple de p, alors ab' est un multiple de p aussi.
La situation est donc la suivante :

$$p \text{ divise } ab \text{ mais ne divise ni } a, \text{ ni } b \qquad *.$$

1. b est le plus petit des entiers naturels satisfaisant $*$.
2. p divise ab' mais ne divise ni a ni b' (en effet $1 \leq b' < b < p$). Par conséquent b' satisfait $*$.
3. Enfin $1 \leq b' < b$. Ceci est en contradication avec le point 1.

Il n'existe donc pas de plus petit entier naturel b satisfaisant $*$, on en déduit qu'il n'existe pas d'entier b tel que $p|ab$ et p ne divise ni a ni b, quelque soit a et p.

IV.2. Chiffrement Affine

A chaque lettre de l'alphabet, on associe, grâce au tableau ci-dessous, un nombre entier m compris entre 0 et 25.

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 définit un système de codage en associant à l'entier m l'entier p qui est le reste de la division euclidienne de $f(m)$ par 26 où f est une fonction affine.

Un tel codage est dit affine. On cherche la fonction g de décodage.

Exercice 32. La fonction f est définie par $f(m) = 21m + 11$.

1. Coder NOTE.
2. Trouver un entier x tel que $21x \equiv 1[26]$.
3. Démontrer que
$$105m + 55 \equiv m + 3[26]$$
4. Démontrer que si $21m + 11 \equiv p[26]$ alors $m \equiv 5p - 3[26]$.
5. Démontrer que si $m \equiv 5p - 3[26]$ alors $21m + 11 \equiv p[26]$.
6. Donner alors la fonction g de décodage et décoder GLB.

Exercice 33. La fonction f est définie par $f(m) = 15m + 14$

1. Coder le mot BAC.
2. Ecrire un algorithme permettant de trouver le plus petit entier x tel que $15x \equiv 1[26]$. Donner x.
3. Démontrer que
$$105m + 98 \equiv m + 20[26]$$
4. Démontrer que si $15m + 14 \equiv p[26]$ alors $m \equiv 7p - 20[26]$.
5. Démontrer que si $m \equiv 7p - 20[26]$ alors $15m + 14 \equiv p[26]$.
6. Donner alors la fonction g de décodage et décoder GLB.

IV.3. Autre codage

Exercice 34. On considère la fonction f de codage définie par $f(x)$ est égal au reste de la division euclidienne de x^5 par 26.

1. A l'aide d'un programme ou de votre calculatrice dresser le tableau de congruence des valeurs de x^5 modulo 26.
2. Coder le mot TEST.
3. (a) Compléter le tableau de congruence pour obtenir les valeurs de x^{25} modulo 26 et vérifier que pour tout entier x :
$$x^{25} \equiv x[26]$$
   (b) Décoder le mot STK.
   (c) En déduire que la fonction de décodage est f elle-même.

IV.4. Chiffrement de Vigenère

On se fixe une clé sous la forme d'un mot (exemple : SINUS).
On veut coder le message « VIVE LA SPE MATH ».
On écrit la phrase à coder et en dessous, la clé autant de fois que nécessaire.
Chaque lettre est codée par son rang entre 0 et 24. On additionne les nombres de chaque lettre avec celui de la lettre de la clé et on calcule les restes modulo 26 de chaque résultat. On obtient le message codé.

clé	S	I	N	U	S								
Message en clair	V	I	V	E	L	A	S	P	E	M	A	T	H
Rang correspondant	21	8	21	4	11	0	18	15	4	12	0	19	7
Clé	S	I	N	U	S	S	I	N	U	S	S	I	N
Rang correspondant	18	8	13	20	18	18	8	13	20	18	18	8	13
Restes modulo 26 de la somme	13	16	8	24	3	18	0	2	24	4	18	1	20
Message codé	N	Q	I	Y	D	S	A	C	Y	E	S	B	U

Pour décrypter il suffit de soustraire la clé au texte chiffré.

Exercice 35.

1. Crypter le mot SPECIALITE avec la clé BAC.
2. On suppose que la longueur de la clé est de 3 lettres. On donne un texte crypté avec cette clé dont le début est donné ci-dessous. Les lettres ont été regroupées par paquets de 3.
   NEK UVG DST CIC VWW SYP BVD SIR FVE IIV FRC JXG OWQ OFG DYP GVQ NEI F…
   En étudiant les fréquences d'apparation des lettres sur l'ensemble du texte, on a les résultats suivants :
   - La première lettre de chaque mot la plus fréquente est le F ;
   - la lettre centrale de chaque mot la plus fréquente est le I ;
   - la lettre finale de chaque mot la plus fréquente est le G.

   (a) En admettant que la lettre la plus fréquente d'un groupe de lettre assez grand est le E, déterminer la clé de ce chiffrement.

   (b) Décrypter le début du texte proposé.

IV.5. Codage Affine par bigramme

Tous les codes qui substituent une lettre à une autre lettre peuvent être assez facilement déchiffrés par une analyse fréquentielle. Pour éviter cela et rendre le code plus sûr on peut coder les mots par bloc de 2 lettres. A chaque bloc de 2 lettres, appelé bigramme, on associe un entier compris entre 0 et 625 à l'aide du tableau suivant. La première lettre correspond à la colonne et la deuxième lettre à la ligne.

	A	B	C	D	E	F	G	H	I	...
A	0	1	2	3	4	5	6	7	8	...
B	26	27	28	29	30	31	32	33	34	...
C	52	53	54	55	56	57	58	59	60	...
...										

Par exemple le bigramme BC correspond à l'entier 53 et le bigramme CB correspond à l'entier 28.

1. A quel entier correspond le bigramme FD ? et CG ?
2. Quel bigramme correspond à l'entier 440 ? à 108 ?
   Effectuer la division euclidienne par 26. A quoi correspondent q et r ?
   On peut alors effectuer un chiffrement affine par la fonction f de codage définie par $f(x)$ est égal au reste de la division euclidienne de $ax+b$ par 626. Pour la suite de l'exercice on prendre les clés de codage $a=31$ et $b=10$.
   (a) Coder alors le message PATIENTE

	PA	TI	EN	CE
X	15	227		
Y	475			
	HS			KG

   (b) Vérifier que $31\times 101\equiv 1[626]$.
   (c) En déduire que si $31x+10\equiv y[626]$ alors $x\equiv 101y+242[626]$.
   (d) Décoder le message RUEOUK.