Institut de Recherche sur l'Enseignement des Mathématiques

Université de Franche-Comté

Arithmétique en Terminale S.

B. Duffaud.
F. Pétiard.
avec la participation
du groupe Lycée
de l'IREM
de Besançon.

MCMXCVIII

Institut de Recherche sur l'Enseignement des Mathématiques

Arithmétique en Terminale S.

B. Duffaud.
F. Pétiard.
avec la participation
du groupe Lycée
de l'IREM
de Besançon.

MCMXCVIII

Cette brochure a été écrite à l'origine à l'intention des professeurs de lycée de l'académie de Besançon qui ont assisté à un stage MAFPEN intitulé "Arithmétique en vue de l'enseignement de spécialité en Terminale S".

Le but de ce travail n'était pas de proposer des cours-types mais de rappeler les notions fondamentales d'arithmétique dans $\mathbb{Z}$ tout en les rattachant aux notions sous-jacentes d'arithmétique dans un anneau euclidien, principal ou factoriel.

Les leçons s'appuient chacune sur un point particulier de ces notions :

* la leçon 1 donne le vocabulaire de la divisibilité commun à tout anneau commutatif intègre.

* la leçon 2 s'attache à l'aspect "anneau euclidien" de $\mathbb{Z}$ (algorithme d'Euclide).

* la leçon 3 s'attache à l'aspect "anneau principal" de $\mathbb{Z}$ (théorème de Bézout).

* la leçon 4 s'attache à l'aspect "anneau factoriel" de $\mathbb{Z}$ (existence et unicité de la décomposition).

Le point de vue pédagogique adopté face à des élèves de Terminale S sera certainement différent de celui-ci.

Nous donnons en annexe quelques algorithmes permettant de programmer certains calculs sur calculatrice (sauf, peut-être, le crible d'Ératosthène).

Les T.P. ne sont pas, *a priori*, à réinvestir tels quels en Terminale ; il s'agissait principalement par leur biais d'appliquer et de développer, lors du stage, les résultats énoncés dans les leçons. Ils ont donné lieu à des calculs pratiques et à l'utilisation d'ordinateurs.

Table des matières.

LEÇON 1.

Divisibilité dans $\mathbb{N}$ et $\mathbb{Z}$.

1. Quelques propriétés utiles de $\mathbb{N}$ et $\mathbb{Z}$.

Il existe dans $\mathbb{N}$ et dans $\mathbb{Z}$ une addition, une multiplication et une relation d'ordre total vérifiant :
$+$ et $\times$ sont internes, commutatives, associatives, possèdent un élément neutre noté 0 pour l'addition, 1 pour la multiplication.
Les éléments de $\mathbb{N}$, à part 0, n'ont pas d'opposé dans $\mathbb{N}$; ce qui se traduit par :

$$\forall n \in \mathbb{N},\ \forall m \in \mathbb{N},\ (n+m=0) \Rightarrow (n=m=0)$$

Tout entier relatif a a un opposé dans $\mathbb{Z}$, noté $-a$: $a+(-a)=0$.
$(\mathbb{Z},+)$ est un groupe abélien.
Tout élément de $\mathbb{Z}$ est régulier pour l'addition.

La multiplication est distributive par rapport à l'addition dans $\mathbb{Z}$.
$(\mathbb{Z},+,\times)$ est un anneau commutatif et intègre :

$$\forall a \in \mathbb{N},\ \forall b \in \mathbb{N},\ (ab=0) \iff (a=0 \text{ ou } b=0)$$

Tout élément de $\mathbb{Z}-\{0\}$ est régulier pour la multiplication.

Définition 1.1.
n est inversible dans $\mathbb{N}$ s'il existe $n' \in \mathbb{N}$, $nn'=1$;
a est inversible dans $\mathbb{Z}$ s'il existe $a' \in \mathbb{Z}$, $aa'=1$.

Les éléments de $\mathbb{N}$ et $\mathbb{Z}$ n'ont pas d'inverses pour la multiplication sauf 1 inversible dans $\mathbb{N}$, et $1,-1$ qui sont les seuls inversibles de $\mathbb{Z}$:

$$\forall n \in \mathbb{N},\ \forall m \in \mathbb{N},\ (nm=1) \Rightarrow (n=m=1)$$
$$\forall n \in \mathbb{Z},\ \forall m \in \mathbb{Z},\ (nm=1) \Rightarrow (n=m=1 \text{ ou } n=m=-1)$$

La relation d'ordre définie dans $\mathbb{N}$ par

$$n \in \mathbb{N},\ m \in \mathbb{N},\ (n \leqslant m) \iff (\exists d \in \mathbb{N},\ n+d=m)$$

est compatible avec l'addition et la multiplication de $\mathbb{N}$; de même que l'ordre strict (qui n'est pas une relation d'ordre) défini par :

$$n \in \mathbb{N},\ m \in \mathbb{N},\ (n<m) \iff (\exists d \in \mathbb{N},\ d \neq 0,\ n+d=m)$$

$\mathbb{N}$ est un ensemble **bien ordonné** par $\leqslant$ c-à-d. :

Proposition 1.1. Principe du bon ordre
Toute partie ***non vide*** S *de* $\mathbb{N}$ *admet un plus petit élément.*

On en déduit que l'ordre sur $\mathbb{N}$ est total ($S = \{a, b\}$ a un plus petit élément donc deux entiers sont toujours comparables), que $]0,1[_{\mathbb{N}} = \emptyset$ (sinon, il existerait x dans $\mathbb{N}$ plus petit élément de $]0,1[$; alors $0 < x < 1$ entraîne $0 < x^2 < x < 1$ en multipliant par x, ce qui est contradictoire avec x plus petit élément de $]0,1[$).

Conséquence :

$$b \in \mathbb{N},\ (b > 0) \iff (b \geqslant 1)$$

puis

$$n \in \mathbb{N},\ (n > a) \iff (n \geqslant a+1) \qquad (*)$$

Tout entier naturel n a un successeur $n+1$.
Tout entier naturel non nul n a un prédécesseur $n-1$.
0 n'a pas de prédécesseur.

On prolonge la relation d'ordre à $\mathbb{Z}$ par :

$$n \in \mathbb{Z},\ m \in \mathbb{Z},\ (n \leqslant m) \iff (\exists\, d \in \mathbb{N},\ n+d = m)$$

$\mathbb{Z}_+ = \{n \in \mathbb{Z},\ 0 \leqslant n\} = \mathbb{N}$ et $\mathbb{Z}_- = \{n \in \mathbb{Z};\ n \leqslant 0\}$.
$(\mathbb{Z}, +, \times, \leqslant)$ est un anneau totalement ordonné (compatibilités de $\leqslant$ avec $+$ dans $\mathbb{Z}$ et avec $\times$ dans $\mathbb{Z}_+$), mais $\mathbb{Z}$ perd le principe du bon ordre.
On a encore la propriété $(*)$ sur $\mathbb{Z}$.

2. Définitions.

Définition 1.2.
Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, *on dit que* b ***divise*** a *et on écrit*

$$b \mid a$$

si et seulement si il existe $q \in \mathbb{Z}$, $a = bq$.

Vocabulaire :
b est un diviseur de a, a est divisible par b ou a est un multiple de b.
"b ne divise pas a" se note $b \nmid a$.

Remarques :

1. Avec cette définition, $0 \mid 0$ est correct.
2. $\forall a \in \mathbb{Z},\ a \mid 0$.
3. $\forall a \in \mathbb{Z},\ 1 \mid a$ et $-1 \mid a$.

Définition 1.3.
Un entier ***naturel*** $p > 1$, *est appelé* ***nombre premier*** *s'il n'a pas dans* $\mathbb{N}$ *d'autre diviseur que 1 et lui-même.*
Un entier naturel plus grand que 1 qui n'est pas premier est dit ***composé***.

Remarque :
Il est à remarquer avant toute chose que **1 n'est pas un nombre premier**.

Notation :
a étant donné dans $\mathbb{Z}$, on note $a\mathbb{Z}$ l'ensemble de tous ses multiples dans $\mathbb{Z}$:

$$a\mathbb{Z} = \{ak,\ k \in \mathbb{Z}\}$$

$0,\ a,\ -a \in a\mathbb{Z}$.

Proposition 1.2.

$$\boxed{a \in \mathbb{Z}, b \in \mathbb{Z}, (b \mid a) \iff (a \in b\mathbb{Z}) \iff (a\mathbb{Z} \subseteq b\mathbb{Z})}$$

Exercice 1 : Montrer que :

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (a \mid b \text{ et } b \mid a) \Rightarrow (a = \pm b).$$

Définition 1.4.
Si $a \mid b$ *et* $b \mid a$ *dans* $\mathbb{Z}$, a *et* b *sont dits* ***associés***. *Dans* $\mathbb{Z}$, *les nombres associés sont donc égaux ou opposés.*
Un ***diviseur propre*** *de* a *est un diviseur de* a *qui n'est ni inversible, ni associé à* a.
Un élément ***irréductible*** *est un élément qui n'est pas inversible et qui n'a pas de diviseur propre.*

Remarque :
Les irréductibles de $\mathbb{Z}$ sont les nombres premiers et leurs opposés.

3. Propriétés de la divisibilité dans $\mathbb{N}$ et $\mathbb{Z}$.

Proposition 1.3.
1. $\forall a \in \mathbb{Z}, a \mid a$ ***réflexivité***
2. $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall c \in \mathbb{Z}, (a \mid b \text{ et } b \mid c) \Rightarrow (a \mid c)$ ***transitivité***
3. $\forall a \in \mathbb{N}, \forall b \in \mathbb{N}, (a \mid b \text{ et } b \mid a) \Rightarrow (a = b)$ ***antisymétrie***.

Donc $\mid$ est une relation d'ordre dans $\mathbb{N}$.
Cet ordre est partiel : $2 \nmid 3$ et $3 \nmid 2$.
Ce n'est pas un ordre dans $\mathbb{Z}$ mais un préordre, car il n'y a pas l'antisymétrie.

Exercice 2 : Montrer :

$$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z},\ (d \mid a \text{ et } d \mid b) \Rightarrow \big(\forall x, y \in \mathbb{Z}, d \mid (ax + by)\big).$$

Exercice 3 : Déterminer toutes les valeurs de n de $\mathbb{N}$ vérifiant :
1) $n \mid (n+8)$.
2) $(n-1) \mid (n+1)$.
3) $(n-4) \mid (3n+24)$.

Attention : Il y a souvent de "fausses intuitions" en arithmétique :
$a \mid c$ et $b \mid c$ n'entraîne pas $ab \mid c$. Exemple : $6 \mid 12$ et $4 \mid 12$ mais $24 \nmid 12$.
$d \mid ab$ n'entraîne pas $d \mid a$ ou $d \mid b$. Exemple : $6 \mid 3 \times 4$.
(cf. théorème de Gauss et corollaires).

Proposition 1.4. Lien entre $\leqslant$ et $\mid$
Si $a \mid b$, alors $|a| \leqslant |b|$ ou $b = 0$.

◇ Preuve :
Si $b \neq 0$, alors $b = aq$ avec $a \neq 0$ et $q \neq 0$, donc $|b| = |a|.|q|$ et $|q|$ est un élément de $\mathbb{N}$ non nul, donc $|q| \geqslant 1$ (cf. page 2), donc $|b| \geqslant |a|$. ◇

Corollaire 1.4.1.
Si $b \in \mathbb{N} - \{0\}$ et $a \in \mathbb{N}$ est un diviseur propre de b, alors $1 < a < b$.

4. Propriétés élémentaires des nombres premiers ou composés.

Théorème 1.1.
Tout nombre entier naturel $n > 1$ a un diviseur premier.

D'après le principe du bon ordre, $S = \{q \in \mathbb{N},\ q \mid n,\ 1 < q \leqslant n\}$ est une partie non vide de $\mathbb{N}$. Il est facile de montrer alors que le plus petit élément de S est premier.

Théorème 1.2.
Tout nombre entier naturel $n > 1$ se décompose en un produit fini de nombres premiers.

◇ Preuve :
• Si n est premier, c'est fini.
• Si n n'est pas premier, n admet un diviseur premier p_1 qui vérifie $1 < p_1$ car 1 n'est pas un nombre premier et $p_1 < n$ car n n'est pas premier (donc $p_1 \neq n$) et p_1 divise n (donc $p_1 \leqslant n$). On obtient alors $n = p_1.n_1$ avec $1 < n_1 < n$.
  * Si n_1 est premier, c'est fini.
  * Si n_1 n'est pas premier, on recommence : il existe p_2 premier, $1 < p_2 < n_1$, tel que $n_1 = p_2.n_2$ avec $1 < n_2 < n_1$.
Et ainsi de suite... On construit ainsi une suite strictement décroissante d'entiers naturels tous strictement supérieurs à 1 ; cette suite est nécessairement finie ; soit n_k son dernier terme (qui est aussi le plus petit) : n_k est nécessairement un nombre premier, sinon, toujours selon la même construction, on obtiendrait un entier n_{k+1} et un nombre premier p_{k+1} tels que $n_k = p_{k+1}.n_{k+1}$ avec $1 < n_{k+1} < n_k$ et $1 < p_{k+1} < n_k$ ce qui est

impossible d'après la définition de n_k. Donc, n_k est premier et $n = p_1.p_2.\ldots.p_k.n_k$ qui est bien une décomposition de n en un produit fini de nombres premiers. ◇

Théorème 1.3. (d'Euclide [1])
L'ensemble des nombres premiers est infini.

◇ Preuve :
Par l'absurde : soit $\mathcal{P}$ l'ensemble des nombres premiers. Supposons qu'il est fini et écrivons $\mathcal{P} = \{p_1, p_2, \ldots, p_n\}$ où les p_i sont rangés dans l'ordre croissant. Le nombre $n = p_1 \times p_2 \times \cdots \times p_n + 1 > p_n \notin \mathcal{P}$.
Il est donc composé et admet, d'après le théorème 1.1., un diviseur premier noté d qui est l'un des p_i. Mais alors $d \mid n$ et $d \mid \prod_{i=1}^{n} p_i$ donc d divise 1 ; donc $d = 1$; absurde car 1 n'est pas premier. ◇

• **Crible d'Ératosthène [2]**

Lemme 1.1.
Tout entier $\boldsymbol{n > 1}$ *,* ***non premier****, admet au moins un diviseur premier* p *vérifiant* $p^2 \leqslant n$.

◇ Preuve :
Montrons d'abord que n admet un diviseur propre m vérifiant $m^2 \leqslant n$: en effet, n étant composé, s'écrit $n = \alpha.\beta$ avec $1 < \alpha < n$ et $1 < \beta < n$; donc $m = \min\{\alpha, \beta\}$.
Si m est premier, on a terminé ; sinon, m admet un diviseur premier p qui, d'une part divise n, d'autre part vérifie $p^2 \leqslant m^2 \leqslant n$. ◇

C'est en s'appuyant sur le lemme 1.1. qu'Ératosthène a construit sa méthode pour donner tous les nombres premiers inférieurs ou égaux à un nombre donné $n \in \mathbb{N}$.
Supposons par exemple ici que $n = 100$.
– On écrit la liste des nombres plus petits que 100 ; on barre 1 qui n'est pas premier et 2 est un nombre premier car il n'a pas de diviseurs dans $\mathbb{N}$ autres que 1 et lui-même.
– On barre alors dans la liste tous les multiples de 2 ; le premier nombre non barré différent de 2 qui apparaît est nécessairement premier. En effet puisqu'il n'est pas barré c'est qu'il n'est multiple d'aucun nombre plus petit que lui-même, sauf de 1.
3 n'est pas barré ; il est donc premier.
– On barre ensuite dans la liste tous les multiples de 3 ; le plus petit nombre non barré qui apparaît alors, différent de 2 et 3, est premier, car s'il n'est pas barré c'est qu'il n'est multiple d'aucun des nombres qui lui sont inférieurs ; il est donc divisible uniquement par 1 et lui-même etc...
– D'après le lemme 1.1., on s'arrête quand le plus petit nombre qui n'a pas été rayé est strictement plus grand que $\sqrt{n}$.

[1] Mathématicien grec ($\approx$ 330 av. JC–$\approx$ 275 av. JC).
[2] Mathématicien né à Cyrène ($\approx$ 276 av. JC–$\approx$ 194 av. JC).

Nombres premiers de 1 à 100

~~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~~	~~27~~	~~28~~	(29)	~~30~~
(31)	~~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~~	~~64~~	~~65~~	~~66~~	(67)	~~68~~	~~69~~	~~70~~
(71)	~~72~~	(73)	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	(79)	~~80~~
~~81~~	~~82~~	(83)	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	(89)	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	(97)	~~98~~	~~99~~	~~100~~

On s'arrête à 11 non barré car $11 > \sqrt{100}$.
Tous les autres nombres qui restent non barrés sont premiers.

Voir en annexe page 65 un algorithme basé sur le crible d'Ératosthène.

COMMENTAIRES :
On voit ici, adaptés à $\mathbb{Z}$, le vocabulaire et les propriétés de la divisibilité dans tout anneau commutatif et intègre. En revanche, l'existence d'un diviseur premier pour tout nombre naturel est basée sur le principe du bon ordre $\leqslant$ de $\mathbb{N}$. On ne trouvera donc pas nécessairement de propriété analogue dans un anneau non ordonné.

LEÇON 2.

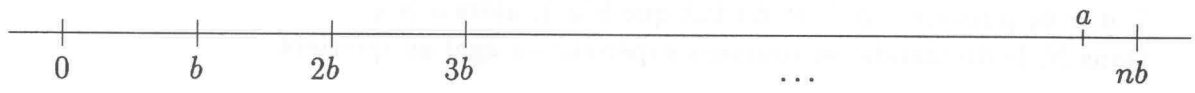
Division euclidienne dans $\mathbb{N}$ et $\mathbb{Z}$ et applications.

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

1.1. Existence de la division euclidienne dans $\mathbb{N}$.

Théorème 2.1. (Lemme d'Archimède [1])
Soit $a, b \in \mathbb{N}$, $b \neq 0$. Alors il existe un entier naturel n tel que $nb > a$.

Le lemme d'Archimède signifie qu'on peut toujours "dépasser" n'importe quel entier a, en ajoutant un certain nombre de fois un autre entier $b \neq 0$ à lui-même, b étant éventuellement plus petit que a.



En effet, puisque $b > 0$ est équivalent à $b \geqslant 1$, alors $(a+1)b \geqslant (a+1) > a$.

Théorème 2.2.
Quels que soient $a \in \mathbb{N}$ et $b \in \mathbb{N} - \{0\}$, il existe un unique couple d'entiers naturels (p, q) vérifiant :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

◇ Preuve :
La preuve de ce théorème s'appuie sur le lemme d'Archimède et le principe du bon ordre.
– Existence : $S = \{s \in \mathbb{N},\ bs > a\}$. $S \neq \emptyset$ (lemme d'Archimède). D'après le principe du bon ordre, S admet un plus petit élément t.
$t \neq 0$ (sinon $b \times 0 > a \geqslant 0$), il a donc un prédécesseur $q \in \mathbb{N} : t = q + 1$.
$(q < t) \Rightarrow (q \notin S)$ puisque t en est le plus petit élément. Donc $bq \leqslant a$. D'autre part $(t \in S) \Rightarrow (bt > a)$, soit

$$bq \leqslant a < b(q+1) \tag{2.1}$$

D'où l'existence d'un couple (q, r) répondant à la question, en posant $r = a - bq$.
– Unicité :

$$\begin{cases} a = bq + r = bq' + r' \\ 0 \leqslant r < b \\ 0 \leqslant r' < b \end{cases}$$

[1] Mathématicien grec né à Syracuse (262 av. JC–190 av. JC).

Supposons $r' \geqslant r$; on a $b(q-q') = r'-r$ avec $r'-r \geqslant 0$. D'autre part, $r \geqslant 0$ donc $r'-r \leqslant r' < b$. Il vient alors $0 \leqslant b(q-q') < b$, soit, puisque b n'est pas nul, $0 \leqslant q-q' < 1$.
Comme il n'y a pas d'entier strictement compris entre 0 et 1, on conclut que nécessairement $q = q'$ et, de ce fait, $r = r'$. ◇

Définition 2.1.
L'opération permettant de passer du couple (a,b), $a \in \mathbb{N}$, $b \in \mathbb{N}$, $\boldsymbol{b \neq 0}$ *au couple* (q,r) *s'appelle "la division euclidienne de* a *par* b*".*
q *et* r *sont respectivement le quotient et le reste de cette division.*

En général a est appelé **le dividende** et b, **le diviseur** de la division euclidienne.

Remarques :

1. Dans la division euclidienne, il est hors de question que $b = 0$ (cf. lemme d'Archimède).
2. Si $a < b$, $q = 0$ et $r = a$;
3. $a \geqslant bq$ puisque $r \geqslant 0$, et du fait que $b \geqslant 1$, alors $a \geqslant q$.
Dans $\mathbb{N}$, le dividende est toujours supérieur ou égal au quotient.

Exemples :

$26 = 4 \times 6 + 2$ représente la division euclidienne de 26 par 4, ou par 6.
$25 = 7 \times 3 + 4$ représente la division euclidienne de 25 par 7.
$10 = 3 \times 2 + 4$ n'est pas une division euclidienne.

1.2. Un critère de primalité.

Voici une méthode simple pour tester si un nombre est premier, issue du lemme 1.1. (crible d'Ératosthène) et de la division euclidienne dans $\mathbb{N}$:

• **Propriété** : $\boxed{\text{Si } n = pq + r,\ 0 \leqslant r < p, \text{ alors } (q < p) \iff (p^2 > n).}$

◇ Preuve :
⋆ Soit $n = pq + r$ $(0 \leqslant r < p)$. Dans $\mathbb{N}$, $q < p \iff q + 1 \leqslant p$;
$pq + r < pq + p \leqslant p(q+1) \leqslant p^2$.
⋆ $n < p^2 \iff pq + r < p^2$; donc $pq < p^2$ car $r \geqslant 0$; d'où $q < p$ $(p > 0)$. ◇

Pour tester si un nombre est premier, on peut donc aussi regarder les quotients q des divisions euclidiennes de n par les différents p premiers. On s'arrête soit si un reste est nul (dans ce cas le nombre est composé), soit lorsque le quotient devient inférieur au diviseur sans qu'aucun reste n'ait été nul (dans ce cas le nombre est premier).
Il faut d'abord disposer d'une table des premiers entiers premiers, obtenue par exemple par le crible d'Ératosthène.
On pourra affiner la recherche en utilisant des critères de divisibilités apparentes (voir les exercices à la fin de cette leçon).

Exemple : $n = 911$.

p	q	r
2	455	1
3	303	2
5	182	1
7	130	1
11	82	9
13	70	1
17	53	10
19	47	18
23	39	14
29	31	12
31	29	12

Dans la dernière division euclidienne, le quotient est strictement plus petit que le diviseur premier, sans que le reste ne soit nul . Donc 911 est premier.
Voir en annexe page 66 un algorithme de critère de primalité.
Exercice 4 : On effectue une division euclidienne en base dix : le dividende est égal à 53 et le reste à 5. Quels peuvent être le diviseur et le quotient ?
Exercice 5 : On divise un nombre a par un nombre b. On trouve pour quotient 109 et pour reste 3057. Quels nombres entiers naturels peut–on ajouter à la fois au dividende et au diviseur pour ne pas modifier le quotient ?
Exercice 6 : On divise deux entiers distincts a et b par leur différence $a - b$. Comparer les quotients et les restes obtenus.

1.3. Systèmes de numération dans $\mathbb{N}$.

C'est la représentation de nombres entiers par un nombre fini de symboles appelés chiffres, comme on écrit des mots avec des lettres.

Soit $b \in \mathbb{N}$, $\boldsymbol{b \geqslant 2}$, soit l'entier naturel :

$$a_n.b^n + a_{n-1}.b^{n-1} + \cdots + a_1.b + a_0$$

avec $0 < a_n < b$ et $0 \leqslant a_i < b$ pour tout $i \in \{1, 2, \ldots, n-1\}$.

On convient de noter ce nombre de la manière suivante :

$$\overline{a_n a_{n-1} a_{n-2} \ldots a_1 a_0}^{(b)}$$

b est appelé "*base de numération*".

Théorème 2.3.
Tout entier naturel admet une représentation unique dans le système de numération de base b, $b \in \mathbb{N}$, $b \geqslant 2$.

◇ Preuve :

Existence : Soit a un entier naturel :

- Si $a < b$, a est représentable par un des chiffres.
- Si $a \geqslant b$, on effectue la division euclidienne de a par b et on obtient $a = bq_1 + r_0$ avec $q_1 \neq 0$ et $0 \leqslant r_0 < b$.
  - ⋆ Si $q_1 < b$, $a = q_1 \times b + r_0$ se représente par $\overline{q_1 r_0}$.
  - ⋆ Si $q_1 \geqslant b$, on divise à nouveau q_1 par b et ainsi de suite jusqu'à ce qu'on obtienne un quotient non nul q_n et inférieur strictement à b.

On a alors la succession de divisions euclidiennes :

$$\begin{cases} a = bq_1 + r_0, & 0 \leqslant r_0 < b, & q_1 \neq 0 \\ q_1 = bq_2 + r_1, & 0 \leqslant r_1 < b, & q_2 \neq 0 \\ q_2 = bq_3 + r_2, & 0 \leqslant r_2 < b, & q_3 \neq 0 \\ \quad\vdots & & \\ q_{n-1} = bq_n + r_{n-1}, & 0 \leqslant r_{n-1} < b, & 0 < q_n < b \end{cases}$$

Ce qui donne en remplaçant successivement :

$$a = q_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0$$

D'où $a = \overline{q_n r_{n-1} \ldots r_1 r_0}^{(b)}$. L'existence d'une telle décomposition est donc assurée.

Unicité : il s'agit de prouver que l'indice n est unique et les entiers $a_n, a_{n-1}, \ldots, a_1, a_0$, tous strictement inférieurs à b, a_n non nul, sont uniques.
Supposons que a admette deux décompositions selon la base b :

$$a = a_n.b^n + \cdots + a_1.b + a_0 = a'_m.b^m + \cdots + a'_1.b + a'_0$$

avec $n \in \mathbb{N}, m \in \mathbb{N}, a_i \in \mathbb{N}, a_i < b, a_n \neq 0$, $a'_j \in \mathbb{N}, a'_j < b$, $a'_m \neq 0$.
Supposons par exemple $n < m$.
On obtient par différence :
$a'_m.b^m + \cdots + (a'_n - a_n).b^n + \cdots + (a'_1 - a_1).b + (a'_0 - a_0) = 0$. Donc :
$a'_m.b^m = -a'_{m-1}b^{m-1} - \cdots - (a'_n - a_n).b^n - \cdots - (a'_1 - a_1).b - (a'_0 - a_0)$. D'où :

$$\begin{aligned} |a'_m.b^m| &= |-a'_{m-1}b^{m-1} - \cdots - (a'_n - a_n).b^n - \cdots - (a'_1 - a_1).b - (a'_0 - a_0)| \\ &\leqslant |a'_{m-1}|.b^{m-1} + \cdots + |a'_n - a_n|.b^n + \cdots + |a'_1 - a_1|.b + |a'_0 - a_0| \end{aligned}$$

Or, $1 \leqslant a'_m \leqslant b-1$, $0 \leqslant a'_{m-1} \leqslant b-1$, …, $0 \leqslant a'_j \leqslant b-1$ et $0 \leqslant a_j \leqslant b-1$ donc $-(b-1) \leqslant a'_j - a_j \leqslant b-1$, donc $|a'_j - a_j| \leqslant b-1$; on en déduit :

$$\begin{aligned} b^m \leqslant |a'_m.b^m| &\leqslant (b-1).b^{m-1} + \cdots + (b-1).b^n + \cdots + (b-1).b + (b-1) \\ &\leqslant (b-1).(b^{m-1} + \cdots + b^n + \cdots + b + 1) \\ &\leqslant (b-1).\frac{1-b^m}{1-b} \\ \text{soit : } b^m &\leqslant b^m - 1 \quad \text{ce qui est impossible} \end{aligned}$$

Donc $n \geqslant m$; si l'on suppose $m < n$, par le même raisonnement en échangeant les rôles de m et n, on arrivera à $m \geqslant n$, donc $m = n$. Ensuite, en reprenant le même calcul, on arrive à :

$$(a'_n - a_n).b^n = -(a'_{n-1} - a_{n-1}).b^{n-1} - \cdots - (a'_1 - a_1).b - (a'_0 - a_0).$$

Si l'on suppose que $a'_n - a_n \neq 0$, en effectuant toujours les mêmes calculs, on arrive à :

$$\begin{aligned} b^n \leqslant |a'_n - a_n|.b^n &\leqslant (b-1).b^{n-1} + \cdots + (b-1).b + (b-1) \\ &\leqslant (b-1).(b^{n-1} + \cdots + b + 1) \\ &\leqslant (b-1).\frac{1-b^n}{1-b} \\ \text{soit : } b^n &\leqslant b^n - 1 \quad \text{ce qui est impossible} \end{aligned}$$

Donc $a_n = a'_n$; en raisonnant de la même façon, de proche en proche, on montre ainsi que $a'_i = a_i$ pour tout i. $\diamond$

Les nombres a_i, tous strictement plus petits que la base b, constituent les symboles utilisés pour "écrire" un nombre entier. On les appelle "chiffres de numération" en base b.

• La base en général utilisée est la base "dix" (qui se représente par "10" en base dix !) ; c'est la numération décimale. Les chiffres utilisés sont les "*chiffres arabes*".

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9$$

Dans ce cas on ne met pas de trait au–dessus des chiffres.
Ainsi le nombre $1 \times 10^3 + 9 \times 10^2 + 9 \times 10 + 8$ s'écrit 1998.

• Si la base de numération b est inférieure ou égale à dix, on utilise les chiffres arabes $0, 1, 2 \ldots$ pour représenter les b premiers entiers naturels dans l'ordre croissant. On s'arrête au chiffre représenté par $b - 1$.
Exemple : $3 \times 5^3 + 2 \times 5^2 + 5 + 1$ s'écrit $\overline{3211}^{(5)}$.

• Si b est strictement plus grande que dix, on rajoute des symboles qui sont des chiffres (mais plus les chiffres arabes), en général $\alpha, \beta, \gamma, \ldots$

Exemple : Si b vaut douze, (qui s'écrit 12 en base dix), on prend comme chiffres supplémentaires α pour représenter dix, β pour représenter onze.
Le nombre $5 \times 12^4 + \alpha \times 12^3 + \beta \times 12^2 + 4 \times 12 + 9$ s'écrit $\overline{5\alpha\beta49}^{(12)}$.
Ce nombre se représente dans la base dix par :

$$\begin{aligned} 5 \times 12^4 + 10 \times 12^3 + 11 \times 12^2 + 4 \times 12 + 9 &= \\ 5 \times 20736 + 10 \times 1728 + 11 \times 144 + 4 \times 12 + 9 &= 122601 \end{aligned}$$

• **Présentation pratique** : Par exemple, écrire en base huit l'entier naturel a qui se représente par 343 en base dix.

343	8	
23	42	8
7	**2**	**5**

On obtient donc

$$\begin{aligned} a &= 42 \times 8 + 7 = [(5 \times 8 + 2) \times 8] + 7 \\ &= 5 \times 8^2 + 2 \times 8 + 7 \end{aligned}$$

et a est représenté en base huit par : $a = \overline{527}^{(8)}$.
On remarque donc qu'on peut connaître directement l'écriture en base huit à partir du tableau des divisions euclidiennes successives, en lisant de droite à gauche le dernier quotient qui est le chiffre a_2, le dernier reste pour a_1 et l'avant–dernier reste pour a_0.

Exercice 7 : Quelle est l'écriture de b en base b, $b \in \mathbb{N}$, $b \geqslant 2$?
Exercice 8 : Écrire en base sept, le nombre dont l'écriture décimale est 1998.
Exercice 9 : Écrire en base douze, le nombre qui s'écrit $\overline{53660}^{(8)}$ en base huit.

• **Comparaison de deux entiers écrits en base b :**

Proposition 2.1.
Quel que soit l'entier naturel x écrit dans le système de base b :

$$x = \overline{a_n a_{n-1} \dots a_1 a_0}^{(b)}$$

avec $a_n \neq 0$, on a

$$b^n \leqslant x < b^{n+1}$$

◇ Preuve :
⋆ Puisque chacun des nombres $a_0, a_1, \dots, a_n$ est strictement inférieur à b, d'après la propriété $(*)$ page 8, chacun d'eux est inférieur ou égal à $b-1$, d'où :
$x \leqslant (b-1).b^n + \dots + (b-1).b + (b-1)$,
$x \leqslant (b-1)(b^n + b^{n-1} + \dots + b + 1)$,
ce qui donne en utilisant l'identité remarquable $b^{n+1} - 1 = (b-1)(b^n + b^{n-1} + \dots + b + 1)$
$x \leqslant b^{n+1} - 1$, soit $x < b^{n+1}$.
⋆ D'autre part $x = a_n b^n + y$ avec $y = a_{n-1}.b^{n-1} + \dots + a_1.b + a_0$ et $0 < a_n < b \Rightarrow a_n \geqslant 1$.
On déduit que $x \geqslant b^n$. ◇

Proposition 2.2.
• *Si deux nombres x et x' écrits en base b n'ont pas le même nombre de chiffres, le plus grand est celui qui s'écrit avec le plus de chiffres.*
• *Si deux nombres x et x' écrits en base b ont le même nombre de chiffres, on regarde le premier rang en partant de la gauche où les chiffres sont distincts. Le plus grand nombre est celui qui a le plus grand chiffre à ce rang-là.*

◇ Preuve :
• Si $x = \overline{a_n \dots a_1 a_0}^{(b)}$ a $n+1$ chiffres avec $a_n \neq 0$ et $x' = \overline{a'_{n'} \dots a'_1 a'_0}^{(b)}$ a $n'+1$ chiffres avec $a'_{n'} \neq 0$, on a $b^n \leqslant x < b^{n+1}$ et $b^{n'} \leqslant x' < b^{n'+1}$.
Si $n < n'$, alors $n+1 \leqslant n'$ et par suite $b^n \leqslant x < b^{n+1} \leqslant b^{n'} \leqslant x' < b^{n'+1}$. D'où $x < x'$.
• Si $x = \overline{a_n \dots a_1 a_0}^{(b)}$ et $x' = \overline{a'_n \dots a'_1 a'_0}^{(b)}$ ont $n+1$ chiffres avec $a_n \neq 0$ et $a'_n \neq 0$,
– si $a_n < a'_n$ c'est-à-dire $a_n + 1 \leqslant a'_n$, puisque $x = a_n.b^n + r$, $0 \leqslant r < b^n$ et $x' = a'_n.b^n + r'$,

$0 \leqslant r' < b^n$, on a

$$a_n.b^n \leqslant x < (a_n+1).b^n \quad \text{et} \quad a'_n.b^n \leqslant x' < (a'_n+1).b^n,$$

soit : $a_n.b^n \leqslant x < (a_n+1).b^n \leqslant a'_n.b^n \leqslant x' < (a'_n+1).b^n$ donc $x < x'$.
– si $a_n = a'_n$ et s'il existe un rang p tel que $a_p < a'_p$ et pour tout indice k tel que $p < k \leqslant n$, $a_k = a'_k$, on a :
$x - (\overline{a_n a_{n-1} \dots a_{p+1}}^{(b)}).b^{p+1} = \overline{a_p a_{p-1} \dots a_1 a_0}^{(b)} = r$, et
$x' - (\overline{a_n a_{n-1} \dots a_{p+1}}^{(b)}).b^{p+1} = \overline{a'_p a'_{p-1} \dots a'_1 a'_0}^{(b)} = r'$.
On raisonne comme précédemment avec r et r' et, comme $a_p < a'_p$, on en déduit immédiatement que $r < r'$ donc que $x < x'$. ◇
Exemples :
$\overline{321642}^{(7)} \geqslant \overline{321542}^{(7)}$ car au quatrième rang en partant de la gauche $6 \geqslant 5$, et $\overline{12345}^{(12)} \geqslant \overline{\beta\beta\beta\beta}^{(12)}$ car $\overline{12345}^{(12)}$ a plus de chiffres que $\overline{\beta\beta\beta\beta}^{(12)}$.

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

Théorème 2.4.
Étant donnés $a \in \mathbb{Z}$ et $b \in \mathbb{Z} - \{0\}$, il existe un couple unique d'entiers (q,r) tels que :

$$\begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}$$

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

La preuve de l'existence de la division euclidienne tient lieu de méthode pratique de recherche du quotient et du reste dans le cas où un des entiers est négatif :
◇ Preuve :
• **Existence** :
1) Cas où $a \in \mathbb{N}$, $b \in \mathbb{N} - \{0\}$: on est ramené au cas de la division euclidienne dans $\mathbb{N}$.
2) Cas où $a \in \mathbb{Z}_-$, $b \in \mathbb{N} - \{0\}$: on effectue la division euclidienne de $-a \in \mathbb{N}$ par $b \in \mathbb{N} - \{0\}$:

$$\begin{cases} -a = bq' + r' \\ 0 \leqslant r' < b \end{cases} \quad \text{avec } q' \in \mathbb{N},\ r' \in \mathbb{N}, \text{ uniques.}$$

a) si $r' = 0$, alors $a = b(-q')$; $q = -q'$ et $r = 0$.
b) si $r' \neq 0$, $a = b(-q') - r'$ avec $0 < r' < b$.
Mais ce résultat n'est pas la division euclidienne de a par b car $(-r')$ n'est pas positif.
On écrit : $a = b(-q'-1) + b - r'$.
L'inégalité : $0 < r' < b$ entraîne $-b < -r' < 0$ et donc $b - b < b - r' < b$.
Si on pose $q = -q' - 1$ et $r = b - r'$, on aura $a = bq + r$ avec $0 < r < b$.
3) Si $a \in \mathbb{N}$, $b \in \mathbb{Z}_- - \{0\}$, on effectue la division euclidienne de a par $(-b)$:

$$a = (-b)q' + r',\ q' \in \mathbb{N},\ r' \in \mathbb{N},\ 0 \leqslant r' < |b|$$

Ceci peut encore s'écrire : $a = b(-q') + r'$; $q = -q'$ et $r = r'$.

4) Si $a \in \mathbb{Z}_-$, $b \in \mathbb{Z}_- - \{0\}$, on effectue la division euclidienne de $(-a)$ par $(-b)$:

$$-a = (-b)q' + r',\ q' \in \mathbb{N},\ r' \in \mathbb{N},\ 0 \leqslant r' < |b|$$

a) si $r' = 0$, alors $a = bq'$; $q = q'$ et $r = 0$.
b) si $r' \neq 0$, $a = bq' - r'$ avec $0 < r' < |b|$.

Mais $(-r')$ n'est pas un reste car il est négatif.
Donc $a = b(q' + 1) - b - r'$, soit $a = bq + r$, avec $q = q' + 1$ et $r = |b| - r'$, (alors $0 \leqslant (-b - r') < |b|$).

• **Unicité de q et r.** Supposons qu'il existe $q \in \mathbb{Z}$, $r \in \mathbb{N}$, $\begin{cases} a = bq + r \\ 0 \leqslant r < |b| \end{cases}$

et qu'il existe $q' \in \mathbb{Z}$, $r' \in \mathbb{N}$, $\begin{cases} a = bq' + r' \\ 0 \leqslant r' < |b| \end{cases}$

Alors $\begin{cases} bq + r = bq' + r' \\ 0 \leqslant r < |b| \\ 0 \leqslant r' < |b| \end{cases}$. D'où $\begin{cases} b(q - q') = r' - r \\ -|b| < r' - r < |b| \end{cases}$, soit $\begin{cases} |b|.|q - q'| = |r' - r| \\ 0 \leqslant |r' - r| < |b| \end{cases}$

Si $r' \neq r$, c-à-d $|r' - r| \neq 0$, on aurait $|q - q'| \neq 0$, donc $|q - q'| \geqslant 1$ et $|b|.|q - q'| \geqslant |b|$, ce qui est contradictoire avec $|r' - r| < |b|$. Donc $r' = r$ et de là $q = q'$. ◇

Quand on effectue une division euclidienne dans $\mathbb{Z}$, bien vérifier que **le reste** est un nombre **positif ou nul**, inférieur à la valeur absolue du diviseur.

Exemples :

1. $a = -47$ et $b = 6$:

$$\begin{aligned} 47 &= 6 \times 7 + 5 \\ -47 &= 6 \times (-7) + (-5) \\ -47 &= 6 \times (-8) + 6 + (-5) \\ -47 &= 6 \times (-8) + 1 \qquad \text{avec } 0 \leqslant 1 < 6 \end{aligned}$$

Donc, dans la division euclidienne de -47 par 6, le quotient est -8 et le reste 1.

2. $a = 47$ et $b = -6$:

$$\begin{aligned} 47 &= 6 \times 7 + 5 \\ -47 &= (-6) \times (-7) + 5 \qquad \text{avec } 0 \leqslant 5 < 6 \end{aligned}$$

Donc, dans la division euclidienne de 47 par -6, le quotient est -7 et le reste 5.

3. $a = -47$ et $b = -6$:

$$\begin{aligned} 47 &= 6 \times 7 + 5 \\ -47 &= (-6) \times 7 + (-5) \\ -47 &= (-6) \times 8 + 6 + (-5) \\ -47 &= (-6) \times 8 + 1 \qquad \text{avec } 0 \leqslant 1 < 6 \end{aligned}$$

Donc, dans la division euclidienne de -47 par -6, le quotient est 8 et le reste 1.

3. Algorithme d'Euclide.

On effectue la division euclidienne de $a \in \mathbb{Z}$ par $b \in \mathbb{Z}-\{0\}$: $a = bq+r$ avec $0 \leqslant r < |b|$; puis on divise b par r : $b = rq' + r'$ avec $0 \leqslant r' < r \ldots$
Jusqu'où aller ?
La succession des restes obtenus vérifiant $|b| > r > r' \cdots \geqslant 0$, est une succession **strictement** décroissante d'entiers naturels ; elle est alors nécessairement finie (au plus $|b|$ restes possibles de $(|b|-1)$ à 0). Il arrive une étape où le reste est nul.

L'algorithme d'Euclide est cet algorithme des divisions euclidiennes successives :
pour des commodités d'écriture, on pose : $r_{-1} = a$ et $r_0 = b$;

$$\left\{\begin{array}{rcrcrcl}
r_{-1} & = & & q_0 r_0 & + \; r_1 & , \; q_0 \in \mathbb{Z}, & 0 < r_1 < |r_0|; \\
r_0 & = & & q_1 r_1 & + \; r_2 & , \; q_1 \in \mathbb{Z}, & 0 < r_2 < r_1; \\
r_1 & = & & q_2 r_2 & + \; r_3 & , \; q_2 \in \mathbb{Z}, & 0 < r_3 < r_2; \\
\vdots & & & & & & \\
r_{i-1} & = & & q_i . r_i & + \; r_{i+1} & , \; q_i \in \mathbb{Z}, & 0 < r_{i+1} < r_i; \\
\vdots & & & & & & \\
r_{n-2} & = & q_{n-1} r_{n-1} & + & r_n & , \; q_{n-1} \in \mathbb{Z}, & 0 < r_n < r_{n-1}; \\
r_{n-1} & = & & q_n r_n & & , \; q_n \in \mathbb{Z}. &
\end{array}\right.$$

• Propriétés de l'algorithme d'Euclide

À chaque étape de l'algorithme, chaque reste r_i peut s'exprimer comme combinaison linéaire à coefficients dans $\mathbb{Z}$ des nombres de départ a et b.

Proposition 2.3.
Pour tout i compris entre -1 et n, il existe $u_i, v_i \in \mathbb{Z}$ tels que $r_i = u_i.a + v_i.b$.

◇ Preuve :
Par récurrence sur i, l'hypothèse de récurrence étant :

$$(H_i) \left\{\begin{array}{rcrcr} r_{i-1} & = & u_{i-1}.a & + & v_{i-1}.b \\ r_i & = & u_i.a & + & v_i.b \end{array}\right.$$

⋆ Au rang $i = 0$, on a : $\left\{\begin{array}{rcrcr} r_{-1} = 1 \times a & + & 0 \times b \\ r_0 = 0 \times a & + & 1 \times b \end{array}\right.$; avec $u_{-1} = 1$, $v_{-1} = 0$; et $u_0 = 0$, $v_0 = 1$.
⋆ Supposons qu'on ait (H_i) et prouvons (H_{i+1}).
Par l'algorithme d'Euclide, on a : $r_{i-1} = q_i r_i + r_{i+1}$. Mais en remplaçant r_{i-1} et r_i par leurs valeurs supposées dans (H_i), on a :
$u_{i-1}.a + v_{i-1}.b = q_i(u_i.a + v_i.b) + r_{i+1}$.
Soit $r_{i+1} = (u_{i-1} - q_i u_i)a + (v_{i-1} - q_i v_i)b = u_{i+1}.a + v_{i+1}.b$.

Et finalement $(H_{i+1}) \left\{\begin{array}{rcrcr} r_i & = & u_i.a & + & v_i.b \\ r_{i+1} & = & u_{i+1}.a & + & v_{i+1}.b \end{array}\right.$ ◇

On remarquera que les coefficients r_i, u_i, et v_i se calculent par le même procédé. En

effet on a : $\boxed{\begin{array}{lcl} r_{i+1} & = & r_{i-1} - q_i r_i \\ u_{i+1} & = & u_{i-1} - q_i u_i \\ v_{i+1} & = & v_{i-1} - q_i v_i \end{array}}$ $(*)$.

• **Une présentation pratique de l'algorithme d'Euclide** : en utilisant les récurrences indiquées ci-dessus $(*)$, on peut présenter l'algorithme d'Euclide sous forme de tableau comme suit :
Division de $a = 1997$ par $b = 17$.

$-q_i$	r_i	u_i	v_i	i
	1997	1	0	**−1**
	17	0	1	**0**

Le quotient de la division euclidienne de 1997 par 17 est 117 ; on calcule alors r_1, u_1 et v_1 par les formules $(*)$ et on obtient :

$-q_i$	r_i	u_i	v_i	i
	1997	1	0	**−1**
−117	17	0	1	**0**
	8	1	−117	**1**

Le quotient de la division euclidienne de 17 par 8 est 2 ; on calcule alors r_2, u_2 et v_2 par les formules $(*)$ et on obtient :

$-q_i$	r_i	u_i	v_i	i
	1997	1	0	**−1**
−117	17	0	1	**0**
−2	8	1	−117	**1**
	1	−2	235	**2**

Le quotient de la division euclidienne de 8 par 1 est 8 ; on calcule alors r_3, u_3 et v_3 par les formules $(*)$ et on obtient :

$-q_i$	r_i	u_i	v_i	i
	1997	1	0	**−1**
−117	17	0	1	**0**
−2	8	1	−117	**1**
−8	1	−2	235	**2**
	0	17	−1997	**3**

$r_3 = 0$ donc on s'arrête là.

Remarque : On peut exprimer chaque reste partiel comme combinaison linéaire de 1997 et de 17 en lisant le tableau. Par exemple :

$8 = 1997 \times 1 - 17 \times 117$.

$1 = 1997 \times (-2) + 17 \times 235$.

À titre de vérification on a toujours : $0 = r_{n+1} = au_{n+1} + bv_{n+1}$.

Soit ici $0 = 1997 \times 17 + 17 \times (-1997)$.

Vérifier que, pour $a = 1998$ et $b = 185$, le tableau est le suivant :

$-q_i$	r_i	u_i	v_i	i
	1998	1	0	**−1**
−10	185	0	1	**0**
−1	148	1	−10	**1**
−4	37	−1	11	**2**
	0	5	−54	**3**

Exercice 10 : Écrire l'algorithme d'Euclide pour les nombres a et b suivants :

$a = 57 \quad , \quad b = 17 \quad ;$

$a = -39 \quad , \quad b = 16 \quad ;$

$a = 452 \quad , \quad b = -35 \quad ;$

$a = -67 \quad , \quad b = -19 \quad ;$

$a = 264 \quad , \quad b = -126 \quad .$

4. Congruences dans $\mathbb{Z}$.

4.1. Définition.

Définition 2.2.
$a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, on dit que a est ***congru*** *à b modulo n et on écrit $a \equiv b \pmod{n}$ s'il existe $k \in \mathbb{Z}$ tel que $a - b = kn$, c'est-à-dire si $a - b \in n\mathbb{Z}$.*

On écrit parfois plus simplement $a \equiv b\ (n)$ au lieu de $a \equiv b \pmod{n}$.

Exemples :

$1998 \equiv 3 \pmod 5$

$-224 \equiv 1 \pmod 5$

n pair $\iff n \equiv 0 \pmod 2$

n impair $\iff n \equiv 1 \pmod 2$.

4.2. Propriétés.

1) Pour tout $x \in \mathbb{Z}$, $x \equiv x$ (**réflexivité**) ;

2) Pour tous $x, y \in \mathbb{Z}$, $x \equiv y \Rightarrow y \equiv x$ (**symétrie**) ;

3) si $a \equiv b \pmod n$ et $b \equiv c \pmod n$ alors $a \equiv c \pmod n$ (**transitivité**).

En fait la congruence modulo n ($n \in \mathbb{Z}$) est un outil qui va permettre de trouver le reste de tout nombre entier dans sa division euclidienne par n sans pour autant avoir

à faire cette division.
En particulier, cela permettra de savoir si un nombre est divisible par n ou pas.

Théorème 2.5.
Soient $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$; $a \equiv b \pmod{n}$ si et seulement si a et b ont le même reste dans leur division euclidienne par n.

◇ Preuve :
- Si $\begin{cases} a = nq + r \\ 0 \leqslant r < n \end{cases}$ et $\begin{cases} b = nq' + r \\ 0 \leqslant r < n \end{cases}$, alors $a - b = (q - q').n$ donc $a \equiv b \pmod{n}$.
- Soit $\begin{cases} a = nq + r \\ 0 \leqslant r < n \end{cases}$ la division euclidienne de a par n dans $\mathbb{Z}$, et $\begin{cases} b = nq' + r' \\ 0 \leqslant r' < n \end{cases}$ celle de b par n.

Si $a \equiv b \pmod{n}$, alors $a - b = n.(q - q') + (r - r') = kn$, $k \in \mathbb{Z}$. D'où $r - r' \in n\mathbb{Z}$.
Or $0 \leqslant r < n$ et $0 \leqslant r' < n$ impliquent que $-n < r - r' < n$.
Le seul multiple de n strictement compris entre $-n$ et n est 0. Donc $r - r' = 0$ et a, b ont le même reste dans leur division par n. ◇

Remarque :
Ainsi, il n'y a que n valeurs possibles de congruence modulo n pour tout entier relatif.
Dans la congruence modulo 8 par exemple, il n'y a que 8 valeurs possibles car 8 restes possibles : 0, 1, 2, 3, 4, 5, 6, 7.
En particulier on retiendra :

Corollaire 2.5.1.
Soit $a \in \mathbb{N}$, $a \equiv r \pmod{n}$, avec $0 \leqslant r < n$, alors $-a \equiv (n - r) \pmod{n}$

Exemple :
$\left.\begin{array}{l} -19 \equiv -3 \pmod{8} \\ -3 \equiv 8 - 3 \pmod{8} \end{array}\right\}$ donc $-19 \equiv 5 \pmod{8}$.

Voici maintenant des propriétés très utilisées dans le calcul sur les congruences :

Proposition 2.4.
C1. $\left(\begin{cases} a \equiv b \pmod{n} \\ a' \equiv b' \pmod{n} \end{cases}\right) \Rightarrow \left(a + a' \equiv b + b' \pmod{n}\right)$;
C2. $\left(\begin{cases} a \equiv b \pmod{n} \\ a' \equiv b' \pmod{n} \end{cases}\right) \Rightarrow \left(a \times a' \equiv b \times b' \pmod{n}\right)$;
C3. Si $a \equiv b \pmod{n}$ alors, pour tout $k \in \mathbb{Z}$, $ka \equiv kb \pmod{n}$;
C4. Si $a \equiv b \pmod{n}$ alors, pour tout $m \in \mathbb{N}$, $a^m \equiv b^m \pmod{n}$.

Exemples :
$n \equiv 0 \pmod{2} \Rightarrow n^2 \equiv 0 \pmod{2}$;
$n \equiv 1 \pmod{2} \Rightarrow n^2 \equiv 1 \pmod{2}$.
Ce qui peut s'énoncer :
le carré de tout nombre pair est pair, et celui de tout nombre impair est impair.

Remarque La réciproque de la propriété C3 est fausse en général :
$[ac \equiv bc \pmod{n}]$ n'implique pas que $a \equiv b \pmod{n}$.
Par exemple : $4 \times 5 \equiv 4 \times 8 \pmod{6}$ et pourtant 5 n'est pas congru à 8 modulo 6.
On ne peut donc pas simplifier sans danger les deux membres d'une congruence.

4.3. Critères de divisibilité.

Par exemple par 3 : on a vu dans le paragraphe consacré à la numération qu'un nombre entier peut être décomposé sous la forme : $x = x_n.10^n + \cdots + x_0$, où les x_i sont des entiers compris entre 0 et 9 sauf x_n qui est compris par convention entre 1 et 9 .
On a $1 \equiv 1 \pmod{3}$;
$10 \equiv 1 \pmod{3}$ et par la propriété C.4 : $10^n \equiv 1 \pmod{3}$ pour tout n positif.
En utilisant la propriété d'addition des congruences et celle de multiplication par un entier quelconque (C.1 et C.3), on obtient $x \equiv x_n + x_{n-1} + ... + x_0 \pmod{3}$.
Donc x est divisible par 3 si et seulement s'il est congru à 0 modulo 3, c'est-à-dire si et seulement si :

$$0 \equiv x_n + x_{n-1} + \cdots + x_0 \pmod{3}$$

On retrouve la règle bien connue :
"Un nombre entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3."

Quelques exercices

Exercice 11 :

Quel est le reste dans la division euclidienne par 3 de 153899 ?

Exercice 12 :

a) Un nombre s'écrit 1 101 010 011 en base deux. Écrire ce nombre dans le système de numération de base huit.

b) Soit $b = 12$. On note α le chiffre représentant dix et β celui représentant onze ; écrire en base douze le nombre qui s'écrit 3203 en base dix.

c) Quels sont les nombres de 3 chiffres qui s'écrivent $\overline{xyz}^{(7)}$ dans le système de numération de base sept et $\overline{zyx}^{(11)}$ dans le système de base onze ? (x, y et z représentent des chiffres).

d) Dans le système de numération de base x ($x > 2$), démontrer que les nombres $N = (x-1)^2$ et $P = 2(x-1)$ s'écrivent respectivement $\overline{ab}^{(x)}$ et $\overline{ba}^{(x)}$, où a et b sont des chiffres en base x.

Exercice 13 :

1. Existe-t-il un système de numération de base x dans lequel on a

$$\overline{41}^{(x)} \times \overline{14}^{(x)} = \overline{1224}^{(x)} \ ?$$

2. Déterminer $b \geqslant 2$ telle que $\overline{46}^{(b)} + \overline{53}^{(b)} = \overline{132}^{(b)}$.
Effectuer ensuite $\overline{46}^{(b)} \times \overline{53}^{(b)}$ dans cette base.
3. Dans quel système de numération 13^4 (écriture décimale) s'écrit-il $\overline{14641}^{(b)}$?

Exercice 14 :

On donne la table d'addition en base deux :

a \ b	0	1
0	0	1
1	1	10

Effectuer directement en base deux l'addition suivante :

$$\begin{array}{rcccccccc} & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ + & & 1 & 0 & 1 & 1 & 0 & 1 \\ \hline = & & & & & & & & \end{array}$$

Exercice 15 :

Quel est le reste de la division euclidienne par 19 de 57383^{40} ?

Exercice 16 :

Montrer en utilisant les congruences que :

1. Un nombre est divisible par 2 (respectivement par 5) si et seulement s'il se termine par un chiffre divisible par 2 (respectivement par 5).

2. Un nombre est divisible par 3 (respectivement par 9) si et seulement si la somme de ses chiffres est divisible par 3 (respectivement par 9).

3. Un nombre est divisible par 4 (respectivement par 25) si et seulement si le nombre formé par les deux chiffres de droite (dizaines et unités) est divisible par 4 (respectivement par 25).
Remarque : on peut aussi prouver que si n s'écrit $a_n a_{n-1} \ldots a_1 a_0$ en numération décimale, il est divisible par 4 si et seulement si $2a_1 + a_0$ est divisible par 4.
4. Un nombre est divisible par 11 si et seulement si la différence entre la somme de ses chiffres de rang pair et de ses chiffres de rang impair est divisible par 11.

Exercice 17 :

1) Déterminer selon les valeurs de n de $\mathbb{N}$ le reste de la division euclidienne de 4^n par 7.

2) Déterminer selon les valeurs de n de $\mathbb{N}$, le reste de la division euclidienne de

$$A = 851^{3n} + 851^{2n} + 851^n + 2 \text{ par } 7.$$

3) On considère le nombre B qui dans le système à base quatre s'écrit $B = \overline{2\,103\,211}^{(4)}$. Déterminer dans le système décimal le reste de la division euclidienne du nombre B par 7.

Exercice 18 :

Soit N un nombre entier naturel qui s'écrit en base douze :

$$N = \overline{aabc}^{(12)}$$

où a, b, c sont des chiffres en base douze, **tous non nuls**.
On représentera le chiffre dix en base douze par α et le chiffre onze par β.

1. En utilisant les congruences adéquates, déterminer les conditions portant sur les chiffres a, b, c exprimant le fait que N est divisible par 6. Montrer alors que $c = 6$. Dans la suite de l'exercice, on supposera que $c = 6$.

2. Si N est divisible par 9, quelles sont les valeurs possibles de b ?

3. Exprimer les conditions portant sur les chiffres a, b, c pour que le reste dans la division euclidienne de N par 11 soit 7 et que le reste dans la division euclidienne de N par 13 soit 9. En déduire la valeur de b puis celle de a.

4. Écrire alors le nombre N en base dix.

COMMENTAIRES :
On prouve ici que $\mathbb{Z}$ est un **anneau euclidien**, *c-à-d. un anneau A commutatif, intègre et possédant une application :*

$$\varphi : A \longrightarrow \mathbb{N}$$

vérifiant : 1. $(\varphi(a) = 0) \iff (a = 0)$
2. $(a \mid b,\ b \neq 0) \Rightarrow (\varphi(a) \leqslant \varphi(b))$
3. $(b \neq 0) \Rightarrow \left(\exists\, q, r \in A^2 \text{ tels que } \begin{cases} a = bq + r \\ \varphi(r) < \varphi(b) \end{cases}\right)$

Ainsi, dans $\mathbb{Z}$, $\varphi(a) = |a|$.
L'intérêt d'un anneau euclidien est qu'on peut obtenir effectivement un p.g.c.d. par un algorithme, alors que dans un anneau non euclidien, on doit se débrouiller avec les relations de Bézout s'il est principal ou avec les décompositions en irréductibles s'il est factoriel, ce qui est loin d'être simple effectivement (voir leçons 3 et 4).

LEÇON 2.

LEÇON 3.

P.g.c.d. – Nombres étrangers – P.p.c.m.

Souvent, dans la littérature, on présente le p.g.c.d. de deux entiers comme le plus grand, au sens de la relation $\leqslant$, des diviseurs communs aux deux entiers. Or, dans l'arithmétique des anneaux commutatifs (qui ne sont pas nécessairement ordonnés), un p.g.c.d. est le plus grand, au sens de la relation "divise", des diviseurs communs aux deux entiers. C'est ce dernier point de vue qui est adopté dans cette leçon.

1. P.g.c.d.(a, b).

1.1. Existence et définitions.

L'ensemble des diviseurs communs à a et à b est non vide, car il contient toujours au moins 1 et -1.

Théorème 3.1.
Le dernier reste non nul de l'algorithme d'Euclide est le plus grand des diviseurs communs à a et b (au sens de la relation "divise" dans $\mathbb{N}$).

La preuve se fait par récurrence "descendante" sur i, pour $0 \leqslant i \leqslant n$.
◇ Preuve :
Soit r_n le dernier reste non nul de l'algorithme d'Euclide (voir page 21). Posons $r_n = d$.
1) Soit l'hypothèse de récurrence au rang i :

$$(H_i) : \quad d \mid r_i \text{ et } d \mid r_{i-1}$$

⋆ Au rang $i = n$ (récurrence descendante, on commence par l'indice le plus élevé), on a $d \mid r_n$ (car $d = r_n$) et $d \mid r_{n-1}$ (car $r_{n-1} = q_n r_n = q_n d$).

⋆ Au rang i $(1 \leqslant i \leqslant n)$, on suppose que (Hi) est vraie ; a-t-on alors (H_{i-1}) vraie ? (récurrence descendante).
D'après l'algorithme, on a $r_{i-2} = q_{i-1}.r_{i-1} + r_i$. Donc, comme $d \mid r_i$ et $d \mid r_{i-1}$ (hypothèse de récurrence), alors $d \mid r_{i-2}$. On obtient bien $d \mid r_{i-1}$ et $d \mid r_{i-2}$.
L'hypothèse de récurrence est vraie au rang n ; si elle est vraie au rang i $(1 \leqslant i \leqslant n)$, alors elle est vraie au rang $i - 1$; elle est donc vraie pour tout i, $0 \leqslant i \leqslant n$.
Conclusion : pour tout i $(0 \leqslant i \leqslant n)$, $d \mid r_i$ et $d \mid r_{i-1}$.
En particulier, $d \mid r_0 = b$ et $d \mid r_{-1} = a$.
2) On a $r_n = a.u_n + b.v_n$ avec u_n, $v_n \in \mathbb{Z}$ (voir proposition 2.3. page 21). Tout diviseur commun à a et à b divise $r_n = d$.
Conclusion : d est un diviseur commun à a et à b, et tout autre diviseur commun est plus petit que lui au sens de la relation divise. ◇

Définition 3.1.
On appelle p.g.c.d.(a,b), et on note souvent simplement (a,b) ou $a \wedge b$ (et on choisit la notation la plus adaptée), tout diviseur commun à a et b, qui est plus grand que tout autre au sens de la relation divise.

$$\Big(d = \text{p.g.c.d.}(a,b)\Big) \iff \left(\begin{cases} 1) & d \mid a \text{ et } d \mid b\ ; \\ 2) & \text{si } \delta \mid a \text{ et } \delta \mid b, \text{ alors } \delta \mid d \end{cases}\right)$$

Corollaire 3.1.1.
Le dernier reste non nul de l'algorithme d'Euclide est un p.g.c.d. de a et b.

Voir en annexe page 66 un algorithme utilisant l'algorithme d'Euclide pour la recherche d'un p.g.c.d. de deux entiers.

Remarques :

1. p.g.c.d.$(0,0) = 0$.
2. $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, non tous les deux nuls, admettent exactement deux p.g.c.d opposés (qui sont des associés). En effet, si d et d' sont deux p.g.c.d. de a et b, alors $d \mid d'$ et $d' \mid d$, donc $d = \pm d'$ (voir l'exercice 1 page 9).
3. Le p.g.c.d. positif (le dernier reste non nul de l'algorithme d'Euclide) est parfois appelé *p.g.c.d. canonique* de a et b.
4. Si $\delta \mid d$ et $\delta \geqslant 0$, alors $\delta \leqslant |d|$. Dans $\mathbb{N}$, la notion de p.g.c.d.(a,b) au sens de la relation "divise" coïncide donc avec la notion de "plus grand" au sens de $\leqslant$.

1.2. Propriétés des p.g.c.d.

Je parle ici de p.g.c.d. positif.

a) Pour tout $a \in \mathbb{Z}$, p.g.c.d.$(a,0) = |a|$;
b) Pour tout $a \in \mathbb{Z}$, p.g.c.d.$(a,1) = 1$;
c) Pour tout $k \in \mathbb{Z}$, pour tous $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, p.g.c.d.$(ka,kb) = |k|$. p.g.c.d.(a,b).

Exercice 19 : Pour tout $k \in \mathbb{Z}$, pour tous $a,b \in \mathbb{Z}$, $(a, b+ka) = (a,b) = (a,-b)$.

1.3. Théorème de Bézout [1].

Théorème 3.2. de Bézout
Soient $a,b \in \mathbb{Z}$, alors il existe $u \in \mathbb{Z}$, il existe $v \in \mathbb{Z}$ tels que :

$$\text{p.g.c.d.}(a,b) = au + bv$$

Posons $d = \text{p.g.c.d.}(a,b)$:
– si $d > 0$, $d = r_n = au_n + bv_n$ (cf. algorithme d'Euclide et proposition 2.3. page 21). On peut prendre $u = u_n$ et $v = v_n$.
– si $d < 0$, alors $d = -r_n$ et d peut s'écrire $d = a.(-u_n) + b.(-v_n)$.

[1] Étienne Bézout (1730–1783). Ce théorème devrait en réalité s'appeler théorème de Bachet (1581–1638) qui est le premier à l'avoir établi pour des entiers naturels. Bézout l'a appliqué aux polynômes.

⚠ **Attention :** u et v ne sont pas uniques (voir en T.P. la résolution des équations diophantiennes).

Remarque :
L'existence d'une relation du type $au + bv = c$ entre a et b, n'entraîne pas que c est le p.g.c.d.(a, b), comme l'indique le corollaire suivant :

Corollaire 3.2.1.
$M = \{ax + by\,;\, x, y \in \mathbb{Z}\} = d\mathbb{Z}$ avec $d =$ p.g.c.d.(a, b).

⚠ Autrement dit, si $au + bv = c$, avec $a,\ b,\ u,\ v \in \mathbb{Z}$, alors **$c$ est un multiple du p.g.c.d.(a, b).**

◇ Preuve :
- Si $m \in M$, $m = ax + by$; alors $d \mid ax + by = m$ puisque $d \mid a$ et $d \mid b$; soit $m \in d\mathbb{Z}$;
- $d \in M$, $d = au + bv$ (théorème de Bézout) ;

$$m \in d\mathbb{Z} \Rightarrow m = dq = (au + bv)q = a(qu) + b(qv) \in M. \qquad \diamond$$

1.4. Une caractérisation des p.g.c.d.

Théorème 3.3.

$$\Big(d = p.g.c.d.(a, b)\Big) \iff \left(\begin{cases} (1) & d \mid a \text{ et } d \mid b \\ (2) & \text{il existe } u \in \mathbb{Z}, \text{ il existe } v \in \mathbb{Z},\ d = ua + vb \end{cases}\right)$$

◇ Preuve :
$\Longrightarrow$: C'est le théorème de Bézout.
$\Longleftarrow$: Si $d' \mid a$ et $d' \mid b$ alors $d' \mid (au + bv)$, donc $d' \mid d$ donc d est p.g.c.d. de a et b par définition. ◇

2. Nombres étrangers.

Définition 3.2.
On dit que les nombres a et b sont étrangers, si leur p.g.c.d. (positif) est 1.

Remarque :
La terminologie souvent employée est "nombres premiers entre eux". Mais cela entraîne un risque de confusion avec le terme de "nombres premiers".
On a vu (cf. corollaire 3.2.1. page 31) que la réciproque du théorème de Bézout est fausse en général.
Cependant elle est vraie dans le cas particulier où ils sont étrangers :

Corollaire 3.2.2. Identité de Bézout
Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $u \in \mathbb{Z}$, $v \in \mathbb{Z}$, $(au + bv = 1) \iff \Big((a, b) = 1\Big)$.

Autrement dit, deux entiers sont étrangers **si et seulement si** 1 peut s'écrire comme combinaison linéaire à coefficients dans $\mathbb{Z}$ de ces deux entiers.

La relation $au + bv = d$, où d est un p.g.c.d. de a et b porte le nom de *"relation de Bézout entre a et b"*. Dans le cas particulier où $d = 1$, on l'appelle aussi *"identité de Bézout"* entre a et b.

Remarque :
Dès qu'on trouve une identité de Bézout entre deux nombres, cela suffit à conclure qu'ils sont étrangers.
Mais inversement il existe une infinité d'identités de Bézout liant deux nombres étrangers. Par exemple, on a vu lors de la recherche de l'algorithme d'Euclide pour 1997 et 17 (page 22) que $1997 \times (-2) + 17 \times 235 = 1$; mais on a aussi :

$$1997 \times 15 + 17 \times (-1762) = 1.$$

Voir en annexe page 67 un algorithme de recherche de coefficients de Bézout.

Les conséquences du théorème de Bézout qui vont suivre sont très importantes. Il s'agit des caractérisations des p.g.c.d., et des propriétés liées aux nombres étrangers, avec surtout l'essentiel théorème de Gauss.

2.1. Une autre caractérisation des p.g.c.d.

Théorème 3.4.
Soient a, b, a', b', $d \in \mathbb{Z}$, tels que : $a = da'$ et $b = db'$.

$$\Big(d = p.g.c.d.(a,b)\Big) \iff (a' \text{ et } b' \text{ sont étrangers}).$$

◇ Preuve :
$d = \text{p.g.c.d.}(a,b) = \text{p.g.c.d.}(da', db') = |d|.\text{p.g.c.d.}(a',b')$ [propriété c) page 30]. Donc, $\Big(d = \text{p.g.c.d.}(a,b)\Big) \iff (\text{p.g.c.d.}(a',b') = \pm 1) \iff a'$ et b' sont étrangers. ◇

2.2. Nombres étrangers et nombres premiers.

Proposition 3.1.
1) Un nombre $a \in \mathbb{Z}$ est étranger à p premier si et seulement si p ne le divise pas.
2) p premier et q premier, $(p \mid q \iff p = q)$ ou aussi $(p \neq q) \iff (p.g.c.d.(p,q) = 1)$.
3) p est un nombre premier si et seulement si p est étranger à tous les nombres ***strictement positifs*** *qui le précèdent : 1, 2, 3, ..., $p-2$, $p-1$.*

◇ Preuve :
1) Les deux seuls diviseurs positifs de p sont 1 et p donc :
   * si $p \mid a$, alors $\text{p.g.c.d.}(a,p) = p \neq 1$
   * si $p \nmid a$, alors $\text{p.g.c.d.}(a,p) = 1$.
2) on applique 1) avec $a = q$ premier. 3)

$\Longrightarrow$: en effet, les nombres qui précèdent p ne peuvent avoir de diviseur commun avec p autre que 1 puisque, si un tel diviseur existait, ce serait un diviseur propre de p strictement inférieur à p, mais p est premier.

$\Longleftarrow$: si p n'est pas premier, il admet un diviseur q dans $\mathbb{N}$ qui vérifie $1 < q < p$; donc p n'est pas étranger à tous les entiers strictement positifs qui le précèdent (il n'est pas étranger à q). $\diamond$

2.3. Propriétés des nombres étrangers.

Proposition 3.2.
$\big((a,c) = 1 \text{ et } (b,c) = 1\big) \Longrightarrow \big((ab,c) = 1\big)$;
$\big((a,b) = 1\big) \Longrightarrow \big(\text{pour tous } n,\ p \in \mathbb{N},\ (a^n, b^p) = 1\big)$

Exemple : $(9,35) = 1$ et $(12,35) = 1$ donc $(108,35) = 1$.

$\diamond$ Preuve :
– $\begin{cases} au + cv = 1 \\ bu' + cv' = 1 \end{cases}$ donc, en effectuant le produit membre à membre :

$$ab.uu' + c.(bvu' + auv' + cvv') = 1$$

ce qui signifie bien $(a,c) = 1$.
– Si $(a,b) = 1$ alors $(a^n, b) = 1$ (récurrence et application de ci-dessus) ; puis on inverse les rôles de a et b. $\diamond$

Proposition 3.3.
Si a et b sont étrangers, alors :

$$\left(\begin{cases} a \mid c \\ \textbf{et} \\ b \mid c \end{cases}\right) \Longrightarrow (ab \mid c).$$

$\diamond$ Preuve :

$$\left(\begin{cases} au + bv = 1 \\ c = na = mb \end{cases}\right) \Longrightarrow (c = acu + bcv = abmu + banv = ab.k) \qquad \diamond$$

En fait, sous l'hypothèse que a et b sont étrangers, on a une équivalence car le sens :

$$(ab \mid c) \Longrightarrow (a \mid c \text{ et } b \mid c)$$

est trivial.

Exemple :

$$\left(\begin{cases} 12 \mid 840 \\ 35 \mid 840 \\ (12,35) = 1 \end{cases}\right) \Longrightarrow (12 \times 35 = 420 \quad \text{et} \quad 420 \mid 840)$$

Remarque :
Si a et b ne sont pas étrangers, la propriété est fausse :
$4 \mid 12$, $6 \mid 12$, mais $24 \nmid 12$ comme nous l'avions déjà indiqué dans la leçon 1 page 10.

2.4. Théorème de Gauss[2].

Le théorème de Gauss peut être vu comme une conséquence immédiate du théorème de Bézout.

Théorème 3.5. de Gauss
Si $a \mid bc$ et si a est étranger à b, alors $a \mid c$.

◇ Preuve :

$$\begin{aligned} \left(\begin{cases} a \mid bc \\ (a,b)=1 \end{cases}\right) &\iff \left(\begin{cases} bc = ka \\ au+bv=1 \end{cases}\right) \\ &\iff \left(\begin{cases} bc = ka \\ acu+bcv=c \end{cases}\right) \\ &\implies \big(a(cu+kv)=c\big) \end{aligned}$$

◇

3. Applications aux congruences.

3.1. Résolution de $ax \equiv b \pmod{n}$.

• Si $(a,n)=1$ alors il existe $u \in \mathbb{Z}, v \in \mathbb{Z}$, tels que $au+bn=1$, soit $au \equiv 1 \pmod{n}$. Donc, $aux \equiv x \pmod{n}$. Or, $ax \equiv b \pmod{n} \Rightarrow aux \equiv bu \pmod{n}$. Par transitivité des congruences, il vient $x \equiv bu \pmod{n}$. On vérifie immédiatement que $x \equiv bu \pmod{n}$ est bien une solution convenable.
Donc l'équation congruentielle a une solution unique $\pmod{n}$.

Exemple :

$$(3x \equiv 2 \pmod{14}) \iff (x \equiv 10 \pmod{7})$$

En effet :

$$\begin{aligned} 3 \times 5 &\equiv 1 \pmod{14} \\ 5 \times (3 \times x) &\equiv 5 \times 2 \pmod{14} \\ \text{donc } 1 \times x &\equiv 10 \pmod{14} \end{aligned}$$

• Si $(a,n) \neq 1$, soit on n'a aucune solution, soit on a plusieurs solutions distinctes modulo n.

Exemples :
* $(3x \equiv 3 \pmod{6}) \Longrightarrow (x \equiv 1 \pmod{6}$ ou $x \equiv 3 \pmod{6})$.
* $3x \equiv 4 \pmod{6}$ n'a pas de solution.

[2]Karl Friedrich Gauss (1777–1855).

3.2. Simplification de $ax \equiv ay \pmod{n}$.

Théorème 3.6.
Si a et n sont étrangers alors, pour tout b et tout c de $\mathbb{Z}$:

$$\big(ab \equiv ac \pmod{n}\big) \Longrightarrow \big(b \equiv c \pmod{n}\big).$$

◇ Preuve :
$(a, n) = 1$; montrons que :

dès que $ab \equiv ac \pmod{n}$, alors nécessairement $b \equiv c \pmod{n}$.

Or, $\big(ab \equiv ac \pmod{n}\big) \iff \big(a(b-c) = kn,\ n \in \mathbb{Z}\big)$.
D'après le théorème de Gauss, $\big((a, n) = 1\big) \Longrightarrow \big(n \mid (b-c)\big)$, d'où $b \equiv c \pmod{n}$. ◇

Remarque : Si a et n ne sont pas étrangers, on peut toujours trouver deux nombres b et c de $\mathbb{Z}$ tels que $\begin{cases} ab \equiv ac \pmod{n} \\ b \not\equiv c \pmod{n} \end{cases}$
En effet, soit p.g.c.d.$(a, n) = d > 1$ et $a = a'd$ et $n = n'd$ avec $(a', n') = 1$. Prenons par exemple b quelconque et $c = n' + b$; on a $ac = a(n' + b)$ soit $ac = an' + ab$; mais alors $ac = a'dn' + ab = a'n + ab$.
Ainsi ce choix de b et c fait que $ab \equiv ac \pmod{n}$ et $b \not\equiv c \pmod{n}$; en effet, on a bien $b \not\equiv c \pmod{n}$ sinon $c-b$ pourrait s'écrire kn, c'est-à-dire $n' = kn$ d'où $n' = kn'd$ et $kd = 1$; puisque ces éléments sont dans $\mathbb{Z}$ et que d est positif, on aboutirait à $d = 1$, ce qui est contraire à l'hypothèse faite.
Autrement dit, on ne peut simplifier par a les deux membres d'une congruence modulo n que si a et n sont étrangers.
Ainsi : $\big(15u \equiv 15v \pmod{4}\big) \Longrightarrow \big(u \equiv v \pmod{4}\big)$; mais $\big(15u \equiv 15v \pmod{6}\big)$ ne peut se "simplifier" par 15 ; (en revanche, on peut la simplifier par 5).

4. Généralisation : p.g.c.d. de n nombres ($n \geqslant 2$).

Les notions de p.g.c.d. et nombres étrangers se généralisent à un nombre fini d'entiers $a_1, a_2, \ldots, a_n$, $n \geqslant 2$.

Définition 3.3.
$a_1 a_2 \ldots a_n \neq 0$, $a_i \in \mathbb{Z}$,

$$\text{p.g.c.d.}(a_1, a_2, \ldots, a_n) = d \iff \begin{cases} 1. & d \mid a_1,\ d \mid a_2,\ \ldots,\ d \mid a_n \\ 2. & \text{si } \delta \mid a_1,\ \delta \mid a_2,\ \ldots,\ \delta \mid a_n,\ \text{alors } \delta \mid d \end{cases}$$

Proposition 3.4. Associativité des p.g.c.d.
p.g.c.d.(a_1, a_2, a_3) = p.g.c.d.[p.g.c.d.$(a_1, a_2), a_3$] = p.g.c.d.[a_1, p.g.c.d.(a_2, a_3)]

◇ Preuve :
Posons $d_{1,2} = (a_1, a_2)$, $d = (d_{1,2}, a_3)$, $d_{2,3} = (a_2, a_3)$ et $d' = (a_1, d_{2,3})$.

$$\left(\begin{cases} d \mid d_{1,2} \\ d \mid a_3 \end{cases}\right) \Longrightarrow \left(\begin{cases} \begin{cases} d \mid a_1 \\ d \mid a_2 \end{cases} \\ d \mid a_3 \end{cases}\right)$$

$$\Longrightarrow \left(\begin{cases} d \mid a_1 \\ \begin{cases} d \mid a_2 \\ d \mid a_3 \end{cases} \end{cases}\right)$$

$$\Longrightarrow \left(\begin{cases} d \mid a_1 \\ d \mid d_{2,3} \end{cases}\right)$$

$$\Longrightarrow (d \mid d')$$

et réciproquement, donc $d = d'$ (si on se restreint aux p.g.c.d. positifs).
Ceci se généralise immédiatement à n entiers ($n \geqslant 2$). ◇

Définition 3.4.
$a_1, a_2, \ldots, a_n \in \mathbb{Z}$ sont dits étrangers dans leur ensemble (ou premiers entre eux dans leur ensemble, ou relativement étrangers) si p.g.c.d.$(a_1, a_2, \ldots, a_n) = \pm 1$

Proposition 3.5.
Si $a_1, a_2, \ldots, a_n$ sont étrangers deux à deux, alors ils sont étrangers dans leur ensemble.

◇ Preuve :
On utilise l'associativité des p.g.c.d. ◇

Remarque : Le fait d'être étrangers dans leur ensemble n'est pas équivalent à être étrangers deux à deux.
Exemple :
6, 10 et 15 sont étrangers dans leur ensemble car leur p.g.c.d. est 1.
En revanche, 6 et 10 ne sont pas étrangers : ils ont pour p.g.c.d. 2 ;
6 et 15 ne sont pas étrangers : ils ont pour p.g.c.d. 3 ;
15 et 10 ne sont pas étrangers : ils ont pour p.g.c.d. 5.

Théorème 3.7.
1) d = p.g.c.d.$(a_1, a_2, \ldots, a_n)$. Alors il existe des entiers relatifs $u_1, u_2, \ldots, u_n$ tels que

$$d = \sum_{i=1}^{n} a_i u_i$$

2) $S = \left\{ \sum_{i=1}^{n} a_i y_i \, , \, y_i \in \mathbb{Z} \right\}$ est l'ensemble de tous les multiples de d et $d \in S$ ($S = d\mathbb{Z}$).

◇ Preuve :
1) Avec les mêmes notations que précédemment :

$$d = \text{p.g.c.d.}(a_1, a_2, a_3) = \text{p.g.c.d.}(d_{1,2}, a_3)\,;$$

le théorème de Bézout nous donne :
$\exists \alpha \in \mathbb{Z}$, $\exists u_3 \in \mathbb{Z}$ tels que $d = \alpha d_{1,2} + u_3 a_3$. Appliquons encore le théorème de Bézout à $d_{1,2}$:
$\exists \nu_1 \in \mathbb{Z}$, $\exists \nu_2 \in \mathbb{Z}$ tels que $d_{1,2} = \nu_1 a_1 + \nu_2 a_2$. Alors :
$d = \alpha\nu_1 a_1 + \alpha\nu_2 a_2 + u_3 a_3 = u_1 a_1 + u_2 a_2 + u_3 a_3$.
La généralisation au cas de n entiers se fait par récurrence.
2) Soit $d = \text{p.g.c.d.}(a_1, a_2, \ldots, a_n)$. Soit $m = a_1 y_1 + a_2 y_2 + \cdots + a_n y_n$ (tous les y_i étant éléments de $\mathbb{Z}$). Alors, il est clair que $d \mid m$ puisque d divise chaque a_i. Donc, $m \in d\mathbb{Z}$. Réciproquement, si $m \in d\mathbb{Z}$, alors $m = dq$. Or, $d = a_1 u_1 + \cdots + a_n u_n$ (nous venons de le démontrer) ; donc, $m = a_1(qu_1) + a_2(qu_2) + \cdots + a_n(qu_n)$ et m est bien un élément de S. ◇
Le corollaire suivant donne les relations de Bézout pour des nombres étrangers dans leur ensemble :

Corollaire 3.7.1.
$\text{p.g.c.d.}(a_1, a_2, \ldots, a_n) = 1 \iff$ *il existe des entiers relatifs* $u_1, u_2, \ldots, u_n$ *tels que*

$$1 = \sum_{i=1}^{n} a_i u_i$$

5. P.p.c.m.(a, b).

5.1. Existence et définition.

L'ensemble des multiples communs à a et b est non vide ; il y a le produit ab par exemple.
D'autre part, si on considère que $a = da'$ et $b = db'$ où d est un p.g.c.d de a et b, alors le nombre $m = da'b'$ est aussi un multiple commun à a et b.
En effet $m = (da').b = a.b' = a'.(db') = a'b$.

Si on considère un autre multiple commun μ à a et à b, alors il existe $k \in \mathbb{Z}$, $k' \in \mathbb{Z}$ tels que

(3.1) $$\mu = ka = k'b = k.(da') = k'.(db')$$

Puisque d est un p.g.c.d de a et b, on sait alors que a' et b' sont étrangers.
(3.1) entraîne $ka' = k'b'$ avec $(a', b') = 1$. D'après le théorème de Gauss, on peut déduire que $a' \mid k'$, donc il existe $\lambda \in \mathbb{Z}$ tel que $k' = \lambda a'$.
En remplaçant dans (3.1), on obtient :

(3.2) $$\mu = ka = k'b = k'.(db') = \lambda a'.(db') = \lambda.(da'b') = \lambda m$$

Donc si μ est un multiple commun à a et à b, il est multiple de m.

$m = da'b'$ est donc un "plus petit commun multiple" au sens de la relation divise.

Définition 3.5.
On appelle p.p.c.m.(a, b) tout multiple commun de a et b, qui est plus petit que tout autre au sens de la relation divise :

$$m = \text{p.p.c.m.}(a,b) \iff \begin{cases} 1. & a \mid m \text{ et } b \mid m \\ 2. & \text{si } a \mid \mu \text{ et } b \mid \mu, \text{ alors } m \mid \mu \end{cases}$$

Remarques :
1) De même que pour les p.g.c.d, on trouve dans $\mathbb{Z}$ exactement deux p.p.c.m. de a et b qui sont $m = da'b'$ défini plus haut et $-m$.
On choisit en général le p.p.c.m. positif et on l'appelle *canonique*.
D'après ce qui précède, si $a = da'$ et $b = db'$ avec $(a', b') = 1$, alors le p.p.c.m. canonique de a et b s'exprime par : $\boxed{m = |da'b'|}$.

2) Si $m \mid \mu$ et $m \geqslant 0$, alors $m \leqslant |\mu|$. Dans $\mathbb{N}$, la notion de p.p.c.m.(a, b) au sens de la relation "divise" coïncide donc avec la notion de "plus petit" au sens de $\leqslant$.

5.2. Propriétés du p.p.c.m.

On considère ici le p.p.c.m. canonique :
- Pour tout $a \in \mathbb{Z}$, p.p.c.m.$(a, 1) = |a|$.
- Pour tout $a \in \mathbb{Z}$, p.p.c.m. $(a, 0) = 0$.
- Pour tout $k \in \mathbb{Z}$, pour tous $a, b \in \mathbb{Z}$, p.p.c.m.$(ka, kb) = |k|$. p.p.c.m.(a, b) .
- De la définition de m on déduit la relation très importante suivante (en considérant également le p.g.c.d. canonique de a et b) :

(3.3) $$\boxed{\text{p.g.c.d.}\,(a,b) \times \text{ p.p.c.m.}\,(a,b) = |ab|}$$

- enfin une caractérisation des nombres étrangers utilisant le p.p.c.m. :

Théorème 3.8.
p.p.c.m. $(a, b) = \pm ab \iff$ *a et b sont étrangers*

5.3. Généralisation : p.p.c.m. de n nombres ($n \geqslant 2$).

Définition 3.6.
$a_1 a_2 \ldots a_n \neq 0$, $a_i \in \mathbb{Z}$,

$$\text{p.p.c.m.}(a_1, a_2, \ldots, a_n) = m \iff \begin{cases} 1. & a_1 \mid m, a_2 \mid m, \ldots, a_n \mid m \\ 2. & \text{si } a_1 \mid \mu, a_2 \mid \mu, \ldots, a_n \mid \mu, \text{ alors } m \mid \mu \end{cases}$$

On a l'analogue de la proposition 3.4. page 35 : associativité des p.p.c.m.

Quelques exercices

Exercice 20 : Quel est le reste dans la division par 3 de $\dfrac{n(n+1)}{2}$?

Exercice 21 : Déterminer les entiers naturels s'écrivant $\overline{abca}$ dans le système de numération décimale, divisibles par 7 et congrus à 1 modulo 99.

Exercice 22 :

a) Résoudre dans $\mathbb{N}^2$: $a^2 - b^2 = 24$;

b) Résoudre dans $\mathbb{N}^2$: $n^3 - m^3 = 999$.

c) Déterminer le p.p.c.m. des nombres n, $n+1$, $n+2$, où n est un entier naturel quelconque .

Exercice 23 : Trouver les nombres qui, divisés par 12, donnent pour reste 5 et qui, divisés par 15, donnent pour reste 14.

Exercice 24 :

a) Déterminer deux entiers naturels connaissant leur p.g.c.d. et leur somme, ou leur p.g.c.d. et leur produit. On note $d = \text{p.g.c.d.}(a, b)$:

$a+b$	72	96
d	9	32

ab	360	6480
d	5	18

b) Trouver deux entiers naturels a et b tels que la différence entre leur p.p.c.m. et leur p.g.c.d. soit égale à 187.

Exercice 25 :

a et b sont deux entiers relatifs non nuls. On note m un de leurs p.p.c.m. et d un de leurs p.g.c.d.

Déterminer a et b pour qu'ils vérifient les 3 conditions suivantes :

$$a \leqslant b, \quad a + b = 105, \quad m = 12d$$

Exercice 26 :

k étant un entier relatif, on pose $x = 2k - 1$, $y = 9k + 4$.

Montrer que tout diviseur commun à x et à y divise 17. En déduire, suivant les valeurs de k, le p.g.c.d. de x et y.

Exercice 27 :

Résoudre dans $\mathbb{N}^2$: $x^2 - 9y^2 = -35$.

Exercice 28 :

On rappelle que, pour $0 \leqslant k \leqslant n$, $\mathsf{C}_n^k = \dfrac{n!}{k!(n-k)!}$. Montrer que p est premier si et seulement si p divise tous les C_p^k $(1 \leqslant k \leqslant p-1)$.

LEÇON 3.

COMMENTAIRES :
Un anneau principal est un anneau A intègre commutatif dont tout idéal est principal, c'est-à-dire engendré par un seul élément (on note $I = aA$ si a est un générateur de I).
L'essentiel de cette leçon est basé sur la principalité de $\mathbb{Z}$:
$*$ les idéaux $a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ u \in \mathbb{Z},\ v \in \mathbb{Z}\}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ sont principaux, c'est-à-dire engendrés par un seul élément.
$*$ un générateur de $a\mathbb{Z} + b\mathbb{Z}$ est un p.g.c.d. de a et b ; un générateur de $a\mathbb{Z} \cap b\mathbb{Z}$ est un p.p.c.m. de a et b.
Ainsi, dans tout anneau principal, on peut exprimer le p.g.c.d. de deux éléments a et b par une relation de Bézout : $aA + bA = dA$.
La principalité nous offre des relations de Bézout entre deux nombres et entraîne le théorème de Gauss.

LEÇON 4.

Factorialité de $\mathbb{Z}$.

Un anneau factoriel est un anneau commutatif intègre dans lequel tout élément non inversible a une décomposition unique en produit d'irréductibles aux inversibles près et à l'ordre des facteurs près.

1. Existence et unicité d'une décomposition d'un entier.

Proposition 4.1. Lemme d'Euclide
Si p est un nombre premier et si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

◇ Preuve :
On applique le théorème de Gauss. ◇

Théorème 4.1. Théorème fondamental de l'arithmétique
Tout nombre naturel $n > 1$ peut s'écrire comme produit de nombres premiers, et cette représentation est unique, à part l'ordre dans lequel les facteurs premiers sont écrits.

◇ Preuve :
Nous allons procéder en deux temps :
– Démontrons d'abord par récurrence l'existence de la décomposition : on vérifie aisément que 2 s'écrit comme produit de nombres premiers ($2 = 2$).
Hypothèse de récurrence : au rang n ($n \geqslant 2$), on suppose que, pour tout k vérifiant $2 \leqslant k \leqslant n$, on a : k se décompose comme produit de nombres premiers.
* si $n+1$ est premier, alors $n+1$ s'écrit trivialement sous la forme $n+1 = n+1$.
* si $n+1$ n'est pas premier, alors il peut s'écrire $n+1 = p.q$ avec $1 < p < n+1$ et $1 < q < n+1$, soit $2 \leqslant p \leqslant n$ et $2 \leqslant q \leqslant n$; on applique alors l'hypothèse de récurrence à p et q et on obtient ainsi une décomposition de $n+1$ en produit de nombres premiers.
On a donc bien montré que l'hypothèse de récurrence est vraie au rang $n+1$, donc qu'elle est vraie pour tout n de $\mathbb{N} - \{0, 1\}$.
– Unicité : cette décomposition est unique car, si l'on suppose qu'un entier n admet deux décompositions distinctes, cela signifie qu'il existe au moins un nombre premier p_i qui n'apparaît pas avec le même exposant dans les deux décompositions : $n = p_i^{\alpha_i}.q_1 = p_i^{\beta_i} q_2$ avec $p_i \nmid q_1$, $p_i \nmid q_2$ et $\alpha_i \neq \beta_i$; si l'on suppose, par exemple, $\alpha_i < \beta_i$ alors, en simplifiant par $p_i^{\alpha_i}$, on obtient : $q_1 = p_i^{\beta_i - \alpha_i}.q_2$ et, comme $\beta_i - \alpha_i > 0$, on en déduit que p_i divise q_1, ce qui est faux par hypothèse. Ceci prouve que tous les nombres premiers qui apparaissent dans les deux décompositions apparaissent avec le même exposant, donc que les deux décompositions sont identiques. ◇

Corollaire 4.1.1.
Tout nombre naturel $n > 1$ peut s'écrire de façon unique sous la forme :

$$(*) \quad n = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_r^{\alpha_r},$$

où les q_i sont des nombres premiers distincts et où les α_i sont des entiers strictement positifs.

On appelle souvent l'égalité $(*)$ la *décomposition canonique* ou la *forme canonique* d'un entier n.

Exemples :

1) La forme canonique de 756 est : $756 = 2^2 \times 3^3 \times 7$.

2) Décomposition de 1998 en produit de facteurs premiers et présentation pratique :

q	p
1998	2
999	3
333	3
111	3
37	37
1	

D'où 1998 s'écrit : $1998 = 2 \times 3^3 \times 37$.

Voir en annexe page 67 un algorithme de décomposition en produit de facteurs premiers.

Corollaire 4.1.2. Factorialité de $\mathbb{Z}$
Tout nombre de $\mathbb{Z} - \{-1, 0, 1\}$ se décompose de façon unique en produit de facteurs premiers de la façon suivante :

$$n = \varepsilon.p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

avec $\varepsilon = \pm 1$ et $\alpha_i \in \mathbb{N} - \{0\}$, pour tout i de 1 à k.

Grâce à cette décomposition, on va pouvoir caractériser les différentes opérations arithmétiques que nous avons vues dans la leçon précédente.

2. Applications.

Par convention, si $a = \varepsilon.q_1^{\gamma_1} \dots q_r^{\gamma_r}$ (avec $\varepsilon = \pm 1$ et $\gamma_i \in \mathbb{N} - \{0\}$) et $b = \varepsilon'.s_1^{\delta_1} \dots s_t^{\delta_t}$ (avec $\varepsilon' = \pm 1$ et $\delta_i \in \mathbb{N} - \{0\}$), on écrira $P = \{q_1, \dots, q_r\} \bigcup \{s_1, \dots, s_t\}$, avec $k = \text{card}(P)$; donc, $P = \{p_1, \dots, p_k\}$ et $a = \varepsilon.p_1^{\alpha_1} \dots p_k^{\alpha_k}$ avec $\alpha_i = 0$ si p_i n'appartient pas à $\{q_1, \dots, q_r\}$ et $\alpha_i = \gamma_j$ si $p_i = q_j$. Il en sera de même pour b : $b = \varepsilon'.p_1^{\beta_1} \dots p_k^{\beta_k}$.

Exemple :
$a = 1960 = 2^3 \times 5^1 \times 7^2 : \varepsilon = 1,\ q_1 = 2,\ \gamma_1 = 3,\ q_2 = 5,\ \gamma_2 = 1,\ q_3 = 7,\ \gamma_3 = 2.$
$b = 77175 = 3^2 \times 5^2 \times 7^3 : \varepsilon' = 1,\ s_1 = 3,\ \delta_1 = 2,\ s_2 = 5,\ \delta_2 = 2,\ s_3 = 7,\ \delta_3 = 3.$
$P = \{2,3,5\} \bigcup \{3,5,7\} = \{2,3,5,7\} : p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7.$
$\alpha_1 = 3,\ \alpha_2 = 0,\ \alpha_3 = 1,\ \alpha_4 = 2 : a = 2^3 \times 3^0 \times 5^1 \times 7^2$
$\beta_1 = 0,\ \beta_2 = 2,\ \beta_3 = 2,\ \beta_4 = 3 : b = 2^0 \times 3^2 \times 5^2 \times 7^3$

2.1. Divisibilité.

Théorème 4.2.
Soit $a = \varepsilon.p_1^{\alpha_1}.p_2^{\alpha_2}.\ldots.p_k^{\alpha_k}$, *et* $b = \varepsilon'.p_1^{\beta_1}.p_2^{\beta_2}.\ldots.p_k^{\beta_k}$,

$$(a \mid b) \iff (\textit{pour tout } i \textit{ de } 1 \textit{ à } k, \quad \alpha_i \leqslant \beta_i.)$$

Exemple :
$a = 2^3 \times 3^0 \times 5^1 \times 7^2$ et $b = 2^0 \times 3^2 \times 5^2 \times 7^3$;
a ne divise pas b car l'exposant de 2 dans a est supérieur à celui de 2 dans b ; en revanche, $c = -2^0 \times 3^1 \times 5^1 \times 7^2$ divise b.

2.2. Nombres étrangers.

Théorème 4.3.
Deux nombres sont étrangers s'ils n'ont aucun diviseur premier commun.

Exemple : $e = 2^2 \times 5^3$ et $f = 3^1 \times 7^2$ sont étrangers.

2.3. P.g.c.d et p.p.c.m de deux nombres.

Théorème 4.4.
Si $a = \varepsilon.p_1^{\alpha_1}.p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, *et* $b = \varepsilon'.p_1^{\beta_1}.p_2^{\beta_2}\ldots p_k^{\beta_k}$, *alors :*

$$p.g.c.d.(a,b) = p_1^{\inf(\alpha_1,\beta_1)}.p_2^{\inf(\alpha_2,\beta_2)}\ldots p_k^{\inf(\alpha_k,\beta_k)};$$

$$p.p.c.m.(a,b) = p_1^{\sup(\alpha_1,\beta_1)}.p_2^{\sup(\alpha_2,\beta_2)}\ldots p_k^{\sup(\alpha_k,\beta_k)}$$

(on considère ici le p.g.c.d. et le p.p.c.m. canoniques).

Autrement dit :
• Le **p.g.c.d.** de deux nombres s'obtient à partir de leurs décompositions en produit de facteurs premiers en prenant **tous** les facteurs premiers **communs** affectés de **l'exposant le plus petit** figurant dans les deux décompositions, et le **p.p.c.m.** en prenant **tous** les nombres premiers figurant dans les deux décompositions **communs ou non**, avec **l'exposant le plus grand**.

Exemple :
Si $a = 2^3 \times 5^1 \times 7^2$ et $b = 3^2 \times 5^2 \times 7^3$, alors
p.g.c.d.$(a, b) = 2^0 \times 3^0 \times 5^1 \times 7^2 = 5 \times 49 = 245$
et p.p.c.m.$(a, b) = 2^3 \times 3^2 \times 5^2 \times 7^3 = 8 \times 9 \times 25 \times 343 = 617400$.

Exercice 29 : Nombre de diviseurs d'un entier naturel
Soit a un élément de $\mathbb{N} - \{0, 1\}$ dont la décomposition en produit de facteurs premiers s'écrit :

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k} \quad \text{avec } \alpha_i > 0 \text{ pour tout } i = 1, \dots, k$$

On note d le nombre de diviseurs strictement positifs de a.
Montrer que $d = (1 + \alpha_1) \dots (1 + \alpha_k)$.
Application : Donner le nombre de diviseurs de 108 et la liste des diviseurs de 108.

COMMENTAIRES :
Dans un anneau factoriel, pour tout nombre il existe une décomposition unique en produit d'irréductibles. On définit alors un p.g.c.d. de deux nombres comme étant le produit des irréductibles affectés du plus petit exposant figurant dans chacune des décompositions (aux inversibles près), et un p.p.c.m. comme le produit des irréductibles affectés du plus grand exposant figurant dans chacune des décompositions (aux inversibles près).
On dispose encore du théorème de Gauss, issu du lemme d'Euclide qui est lié à l'existence et à l'unicité de la décomposition.

ANNEXE A.

Solutions des exercices

1. Solutions des exercices de la leçon 1.

Exercice 1 : (page 9).
On suppose que a et b sont deux entiers relatifs vérifiant $a \mid b$ et $b \mid a$; ceci signifie qu'il existe m dans $\mathbb{Z}$ tel que $b = ma$ et qu'il existe n dans $\mathbb{Z}$ tel que $a = nb$. Remarquons d'abord que, si $a = 0$, alors $b = 0$ et que, si $b = 0$, alors $a = 0$. Dans la suite, nous supposerons donc a et b non nuls (et alors, m et n sont non nuls). On a alors $a = mna$ et $b = mnb$, soit $mn = 1$. Donc, $|m|.|n| = 1$. Puisque $m \neq 0$, $|m| \geqslant 1$ et il en est de même pour $|n|$. Si l'on suppose $|m| \neq 1$, alors $|m| \geqslant 2$, donc $|m|.|n| \geqslant 2$ ce qui est impossible ; on en déduit donc que $|m| = 1$, donc que $|n| = 1$. Comme $mn = 1$, si $m = 1$, alors $n = 1$ et, si $m = -1$, alors $n = -1$; donc $m = n = \pm 1$ et on en déduit que $a = \pm b$ (résultat qui reste d'ailleurs valable pour $a = b = 0$).

Exercice 2 : (page 9).
$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, (d \mid a \text{ et } d \mid b) \Rightarrow \big(\forall x \in \mathbb{Z},\ \forall y \in \mathbb{Z},\ d \mid (ax + by)\big)$.

$$(d \mid a) \iff (\exists\, k \in \mathbb{Z},\ a = kd) \quad (1)$$
$$(d \mid b) \iff (\exists\, k' \in \mathbb{Z},\ b = k'd) \quad (2)$$

D'où, pour tout x et y de $\mathbb{Z}$, $ax + by = kdx + k'dy = (kx + k'y)d$. Il existe donc $k" \in \mathbb{Z}$, $k" = kx + k'y$, tel que : $ax + by = k"d$, donc $d \mid (ax + by)$.

Exercice 3 : (page 10).
1) $n \mid (n+8)$:
• On utilise l'exercice précédent 2. Comme n divise n et que n divise $(n+8)$, n divise toute combinaison linéaire à coefficients dans $\mathbb{Z}$ de n et $(n+8)$, en particulier n divise la différence $(n+8) - n$, soit n divise 8.
• Réciproquement : $(n \mid 8 \text{ et } n \in \mathbb{N}) \Rightarrow \big(n \mid (n+8)\big)$.

Conclusion : $\{n \in \mathbb{N}\ ;\ n \mid (n+8)\} = \{1, 2, 4, 8\}$ l'ensemble des diviseurs positifs de 8.
2) $(n-1) \mid (n+1)$:
Toujours en utilisant les combinaisons linéaires à coefficients entiers, on a :
• $\big((n-1) \mid (n-1) \text{ et } (n-1) \mid (n+1)\big) \Rightarrow \big((n-1) \mid \big[(n+1)-(n-1)\big]\big)$, soit $(n-1) \mid 2$.
On a donc que $n - 1 = -1$, $n - 1 = 1$ ou $n - 1 = 2$, c'est-à-dire que $n = 0$, $n = 2$ ou $n = 3$.
• Réciproquement :
si $n = 0$, alors $n - 1 = -1$ et -1 divise tout nombre, en particulier $(n + 1)$;
si $n = 2$, alors $n - 1 = 1$ et 1 divise tout nombre, en particulier $(n + 1)$;
si $n = 3$ alors $n - 1 = 2$ et $n + 1 = 4$; $2 \mid 4$.

Conclusion : $\{n \in \mathbb{N} \ ; \ (n-1) \mid (n+1)\} = \{0, 2, 3\}$.

3) $(n-4) \mid (3n+24)$:

• $(n-4) \mid (n-4)$ et $(n-4) \mid (3n+24)$ donc $(n-4) \mid \big[(3n+24) - 3 \times (n-4)\big]$ soit $(n-4) \mid 36$.

Or on cherche $n \geqslant 0$, donc $n - 4 \geqslant -4$. Une condition nécessaire est donc que $(n-4)$ soit un diviseur de 36 supérieur ou égal à -4.

• Réciproquement si $(n-4) \mid 36$, alors $(n-4) \mid \big(3\times(n-4)+36\big)$, donc $(n-4) \mid (3n+24)$.

Conclusion : $(n-4) \in \{-4; -3; -2; -1; 1; 2; 3; 4; 6; 9; 12; 18; 36\}$

$$n \in \{0; 1; 2; 3; 5; 6; 7; 8; 10; 13; 16; 22; 40\}$$

2. Solutions des exercices de la leçon 2.

Exercice 4 : (page 15).

Notons b le diviseur et q le quotient ; on doit avoir $53 = bq + 5$ avec $0 \leqslant 5 < b$. Donc, $bq = 48$ avec $b > 5$: b doit être un diviseur de 48 strictement supérieur à 5, c'est-à-dire que b vaut 6 (et alors $q = 8$) ou 8 (et alors $q = 6$).

Exercice 5 : (page 15).

On a : $a = 109b + 3057$ avec $0 \leqslant 3057 < b$ et on veut trouver n de $\mathbb{N}$ tel que $a + n = 109(b + n) + r$ avec $0 \leqslant r < b + n$.

Comme $a = 109b + 3057$, il vient alors $109b + 3057 + n = 109(b + n) + r$, donc $3057 = 108n + r$. Comme n est positif, on en déduit que $r \leqslant 3057$ et, puisque $3057 < b$, on a alors $r < b$ donc $r < b + n$. D'autre part, r doit être positif, donc $108n$ doit être inférieur à 3057. On en déduit alors facilement les valeurs possibles pour n : ce sont toutes les valeurs positives qui vérifient $0 \leqslant 108n \leqslant 3057$, donc n appartient à $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28\}$.

Exercice 6 : (page 15).

On divise deux entiers distincts a et b par leur différence $a - b$. Comparer les quotients et les restes obtenus.

$a \neq b$, supposons par exemple que $a > b$.

$\begin{cases} a = (a-b)q_1 + r_1 \\ 0 \leqslant r_1 < a - b \end{cases}$, et $\begin{cases} b = (a-b)q_2 + r_2 \\ 0 \leqslant r_2 < a - b \end{cases}$.

Faisons la différence : $a - b = (a-b)(q_1 - q_2) + (r_1 - r_2)$ soit $(a-b)\big[1 - (q_1 - q_2)\big] = r_1 - r_2$.

Or $b - a < r_1 - r_2 < a - b$ puisque $0 \leqslant r_1 < a - b$ et $0 \leqslant r_2 < a - b$.

On voit donc que $a - b$ doit être un diviseur de $|r_1 - r_2|$. Or $|r_1 - r_2|$ lui est strictement inférieur. La seule possibilité est $|r_1 - r_2| = 0$, soit $r_1 = r_2$ et alors $q_1 = q_2 + 1$.

Finalement, si $a > b$, $a = (a-b)q + r$ avec $0 \leqslant r < a - b$ et $b = (a-b)(q-1) + r$.

Exemple : Si $a = 57$, $b = 49$, alors $a - b = 8$ et $57 = 8 \times 7 + 1$; $49 = 8 \times 6 + 1$.

Exercice 7 : (page 18).
C'est bien évidemment $\overline{10}^{(b)}$ $(b = 1 \times b^1 + 0 \times b^0)$

Exercice 8 : (page 18).

1998	7		
59	285	7	
38	05	40	7
3	**5**	**5**	**5**

Donc, $1998 = \overline{5553}^{(7)}$.

Exercice 9 : (page 18).

$$\begin{aligned}\overline{53660}^{(8)} &= 5 \times 8^4 + 3 \times 8^3 + 6 \times 8^2 + 6 \times 8 + 0 \\ &= 5 \times 4096 + 3 \times 512 + 6 \times 64 + 6 \times 8 + 0 \\ &= 20480 + 1536 + 384 + 48 \\ &= 22448\end{aligned}$$

22448	12			
104	1870	12		
84	67	155	12	
08	70	35	12	12
8	**10**	**11**	**0**	**1**

Donc, $\overline{53660}^{(8)} = \overline{10\beta\alpha 8}^{(12)}$.

Exercice 10 : (page 23).

$-q_i$	r_i	u_i	v_i	i
	57	1	0	**−1**
−3	17	0	1	**0**
−2	6	1	−3	**1**
−1	5	−2	7	**2**
−5	1	3	−10	**3**
	0	−17	57	**4**

$-q_i$	r_i	u_i	v_i	i
	−39	1	0	**−1**
3	16	0	1	**0**
−1	9	1	3	**1**
−1	7	−1	−2	**2**
−3	2	2	5	**3**
−2	1	−7	−17	**4**
	0	16	39	**5**

$-q_i$	r_i	u_i	v_i	i
	452	1	0	**−1**
12	−35	0	1	**0**
2	32	1	12	**1**
−1	29	2	25	**2**
−9	3	−1	−13	**3**
−1	2	11	142	**4**
−2	1	−12	−155	**5**
	0	35	452	**6**

$-q_i$	r_i	u_i	v_i	i
	−67	1	0	**−1**
−4	−19	0	1	**0**
3	9	1	−4	**1**
−1	8	3	−11	**2**
−8	1	−2	7	**3**
	0	19	−67	**4**

$-q_i$	r_i	u_i	v_i	i
	264	1	0	**−1**
2	−126	0	1	**0**
11	12	1	2	**1**
−2	6	11	23	**2**
	0	−21	−44	**3**

Exercice 11 : (page 25).
On a :

$$\begin{aligned} 153899 &\equiv 1+5+3+8+9+9 \pmod 3 \\ 1+5+3+8+9+9=35 &\equiv 3+5 \pmod 3 \\ 3+5=8 &\equiv 2 \pmod 3 \end{aligned}$$

Donc, le reste de la division euclidienne de 153899 par 3 est égal à 2.

Exercice 12 : (page 25).

a) Il n'est pas utile de passer par la base dix. On peut répondre à la question en faisant apparaître directement les puissances de 2^3 dans l'écriture du nombre. Ainsi :

$$\begin{aligned} \overline{1\,101\,010\,011}^{(2)} &= 2^9+2^8+2^6+2^4+2+1 \\ &= \left(2^3\right)^3+\left(2^3\right)^2\times 2^2+\left(2^3\right)^2+\left(2^3\right)\times 2+3 \\ &= 8^3+8^2(4+1)+8\times 2+3 \\ &= \overline{1523}^{(8)} \end{aligned}$$

b)

3203	12		
80	266	12	
83	26	22	12
11	**2**	**10**	**1**

En base douze, 11 s'écrit β et 10 s'écrit α, donc on a $3203 = \overline{1\alpha 2\beta}^{(12)}$.

c) Soit $n = \overline{xyz}^{(7)} = \overline{zyx}^{(11)}$; par convention x, y, z sont des chiffres en base sept (et onze). Donc ils sont inférieurs ou égaux à 6 nécessairement.
D'autre part, par convention, le chiffre de gauche n'est jamais 0 ($0 < a_n < b$). Donc $x \neq 0$ et $z \neq 0$.
Il vient : $0 \leqslant y \leqslant 6$, $1 \leqslant x \leqslant 6$, $1 \leqslant z \leqslant 6$.
n s'écrit donc :

$$\begin{array}{rcccccc} n & = & \overline{xyz}^{(7)} & = & x \times 7^2 + y \times 7 + z & = & 49x + 7y + z \\ n & = & \overline{zyx}^{(11)} & = & z \times 11^2 + y \times 11 + x & = & 121z + 11y + x \end{array}$$

On est donc ramené à résoudre dans $\mathbb{N}$ l'équation :

$$48x - 4y - 120z = 0$$

soit

$$12x = y + 30z \text{ avec } \begin{cases} 1 \leqslant x \leqslant 6 \\ 0 \leqslant y \leqslant 6 \\ 1 \leqslant z \leqslant 6 \end{cases}$$

Or $12 \leqslant 12x \leqslant 72$ et $30 \leqslant y + 30z \leqslant 6 + 180$, ce qui donne comme conditions nécessaires :

$$\begin{cases} (1) & 30 \leqslant 12x \leqslant 72 \quad \text{soit encore} \quad 5 \leqslant 2x \leqslant 12 \\ (2) & 30z \leqslant 30z + y \leqslant 72 \end{cases}$$

Comme $1 \leqslant x \leqslant 6$ et $1 \leqslant z \leqslant 6$ on déduit :

$$\begin{cases} (1) & 3 \leqslant x \leqslant 6 \\ (2) & 1 \leqslant z \leqslant 2 \end{cases}$$

• si $z = 1$: $12x = y + 30$. Or $30 \leqslant y + 30 \leqslant 36$ dans $\mathbb{N}$, donc $5 \leqslant 2x \leqslant 6$ et $x = 3$, par conséquent $y = 6$.
Vérification :
$\overline{361}^{(7)} = 3 \times 49 + 6 \times 7 + 1 = 190$
$\overline{163}^{(11)} = 1 \times 121 + 6 \times 11 + 3 = 190$.
• si $z = 2$, $12x = y + 60$. Or $60 \leqslant y + 60 \leqslant 66$, soit $10 \leqslant 2x \leqslant 11$, donc $x = 5$ et $y = 0$.
Vérification :
$\overline{502}^{(7)} = 5 \times 49 + 2 = 247$
$\overline{205}^{(11)} = 2 \times 121 + 5 = 247$.

d) $N = (x-1)^2 = x^2 - 2x + 1$. Ce n'est pas l'écriture du nombre en base en base x car -2 ne peut représenter un chiffre.
On écrit $(x-1)^2 = x(x-2) + 1$. Alors, puisque par hypothèse $x > 2$, on a bien $0 < x - 2 < x$ et $x - 2$ représente bien un chiffre non nul en base x. Si on pose $x - 2 = a$, N s'écrit :

$$N = \overline{a1}^{(x)}$$

$P = 2x - 2$, ne donne pas l'écriture de P en base x car -2 ne peut être un chiffre. Mais $P = x + (x - 2)$ et s'écrit donc avec la même convention de chiffrage que ci-dessus :

$$P = \overline{1a}^{(x)}$$

Exercice 13 : (page 25).

1.

Nécessairement $x \geqslant 5$, puisque le chiffre 4 est utilisé dans l'écriture de ces nombres. On a :

$$\begin{aligned} (4x+1)(x+4) &= x^3 + 2x^2 + 2x + 4 \\ 4x^2 + 17x &= x^3 + 2x^2 + 2x \\ x(4x+17) &= x(x^2 + 2x + 2) \end{aligned}$$

et, puisque $x \geqslant 5$, $x \neq 0$ donc $4x + 17 = x^2 + 2x + 2$ soit à résoudre :

$$x^2 - 2x - 15 = 0 \text{ avec } x \in \mathbb{N},\ x \geqslant 5$$

Or $x^2 - 2x - 15 = (x - 5)(x + 3)$.
Seul $x = 5$ convient.
Vérification :
$(4 \times 5 + 1)(5 + 4) = 21 \times 9 = 189$;
$\overline{1224}^{(5)} = 125 + 50 + 10 + 4 = 189$

2.

D'après les chiffres utilisés, il est nécessaire que la base de numération soit supérieure ou égale à 7, puisque 6 figure dans l'écriture.
Si nous additionnons les unités, nous avons 6+3=9 en base dix, qui doit s'écrire avec 2 pour chiffres d'unités en base b, soit à effectuer $6 + 3 = nb + 2$.
$7 = nb$, avec $b \geqslant 7$, ce qui entraîne $b = 7$ et $n = 1$.
La base cherchée ne peut être que 7.
Vérification :
$(4 \times 7 + 6) + (5 \times 7 + 3) = 9 \times 7 + 9 = 9(7 + 1) = (7 + 2)(7 + 1) = 7^2 + 7 + 2 \times 7 + 2 = 7^2 + 3 \times 7 + 2 = \overline{132}^{(7)}$

Essayons de faire la multiplication demandée directement en base 7. Pour cela, écrivons d'abord la table de multiplication en base 7 :

×	2	3	4	5	6
2	4	6	11	13	15
3		12	15	21	24
4			22	26	33
5				34	42
6					51

Alors

$$\begin{array}{rr} & \overline{46}^{(7)} \\ \times & \overline{53}^{(7)} \\ \hline & \overline{204}^{(7)} \\ & \overline{332}^{(7)} \\ \hline = & \overline{3524}^{(7)} \end{array}$$

La multiplication s'effectue ainsi : $3 \times 6 = \overline{24}^{(7)}$; on pose 4 et on retient 2.
$3 \times 4 = 12$, $12 + 2 = \overline{20}^{(7)}$ etc. On convertit à chaque fois en base sept le résultat calculé en base dix, en tenant compte des retenues qu'il faut.

3.
$13^4 = \overline{14641}^{(x)}$ entraîne que $x \geqslant 7$, puisque le chiffre 6 figure dans l'écriture. On a $13^4 = x^4 + 4x^3 + 6x^2 + 4x + 1 = (x+1)^4$ d'après la formule du binôme de Newton.
D'où $13 = x + 1$, puisqu'on est dans $\mathbb{N}$ et finalement $x = 12$.

Exercice 14 : (page 26).

$$\begin{array}{cccccccccc} & & \textcircled{1} & \textcircled{1} & \textcircled{1} & & & \textcircled{1} & & \\ & & 1 & 0 & 1 & 1 & 0 & 0 & 1 & \\ + & & & 1 & 0 & 1 & 1 & 0 & 1 & \\ \hline = & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & \end{array}$$

La ligne du haut est constituée des retenues.

Exercice 15 : (page 26).
$57383 \equiv 3 \pmod{19}$ car $57383 = 19 \times 3020 + 3$.
D'après les propriétés des congruences, on a :

$$57383^n \equiv 3^n \pmod{19}.$$

Calculons les puissances successives de 3 modulo 19.

$$\begin{aligned} 3 &\equiv 3 \pmod{19} \\ 3^2 &\equiv 9 \pmod{19} \\ 3^3 \equiv 3^2 \times 3 \equiv 9 \times 3 &\equiv 8 \pmod{19} \\ 3^4 \equiv 3^3 \times 3 \equiv 8 \times 3 &\equiv 5 \pmod{19} \\ 3^5 \equiv 3^4 \times 3 \equiv 5 \times 3 &\equiv 15 \pmod{19} \\ 3^6 \equiv 3^5 \times 3 \equiv 15 \times 3 &\equiv 7 \pmod{19} \\ 3^7 \equiv 3^6 \times 3 \equiv 7 \times 3 &\equiv 2 \pmod{19} \\ 3^8 \equiv 3^7 \times 3 \equiv 2 \times 3 &\equiv 6 \pmod{19} \\ 3^9 \equiv 3^8 \times 3 \equiv 6 \times 3 \equiv 18 &\equiv -1 \pmod{19} \end{aligned}$$

Le but est d'obtenir une puissance de 3 congrue à 1 modulo 19.
Or, si $3^9 \equiv -1 \pmod{19}$, alors $(3^9)^2 \equiv (-1)^2 \equiv 1 \pmod{19}$, soit :

$$3^{18} \equiv 1 \pmod{19}.$$

Écrivons alors la division euclidienne de 40 par 18 :

$$40 = 2 \times 18 + 4.$$

D'où : $3^{40} = 3^{2\times 18+4} = 3^{2\times 18} \times 3^4 = \left(3^{18}\right)^2 \times 3^4 \equiv 1 \times 5 \equiv 5 \pmod{19}$.
$57383^{40} \equiv 3^{40} \pmod{19}$, donc le reste de la division euclidienne de 57383^{40} par 19 est 5.

Exercice 16 : (page 26).
Si un nombre entier naturel A s'écrit : $a_m a_{m-1} \cdots a_1 a_0$ en base 10, cela signifie que

$$A = a_m \times 10^m + a_{m-1} \times 10^{m-1} + \cdots + a_1 \times 10 + a_0$$

D'après les propriétés des congruences, si $10 \equiv \alpha \pmod{n}$ alors :

$$A \equiv a_m \times \alpha^m + a_{m-1} \times \alpha^{m-1} + \cdots + a_1 \times \alpha + a_0 \pmod{n}$$

Appliquons cela successivement avec $n = 2, 5, 3, 9, 4, 25, 11$.

1. $10 \equiv 0 \pmod 2$ ou $\pmod 5$; donc $10^m \equiv 0 \pmod 2$ ou $\pmod 5$ et $A \equiv a_0 \pmod 2$ ou $\pmod 5$

Donc modulo 2 ou 5, un entier naturel est congru à son chiffre d'unités ; il est donc divisible par 2 quand a_0 est divisible par 2, c'est-à-dire lorsque son chiffre d'unités est pair, il est divisible par 5 quand son chiffre d'unités est divisible par 5, c'est-à-dire si a_0 est égal à 0 ou 5.
Exemple :
Le reste de la division de 1738 par 5 est congru à 8 modulo 5, donc c'est 3 car $8 \equiv 3 \pmod 5$.

2. $10 \equiv 1 \pmod 3$ ou $\pmod 9$; donc $10^m \equiv 1 \pmod 3$ ou $\pmod 9$ et

$$A \equiv a_m + a_{m-1} + \cdots + a_0 \pmod 3 \text{ ou } \pmod 9.$$

Un nombre est congru à la somme de ses chiffres modulo 3 ou modulo 9. Donc en particulier, il est divisible par 3 (resp. 9), si sa somme des chiffres est divisible par 3 (resp. 9).
Exemple :
$41738 \equiv 4+1+7+3+8 \equiv 1+1+1+0+2 \equiv 2 \pmod 3$. Le reste de la division euclidienne de 41738 par 3 est 2.
$41738 \equiv 4+1+7+3+8 \equiv 4+7+3 \equiv 5 \pmod 9$ Le reste de la division euclidienne de 41738 par 9 est 1.

3. Par 4 et par 25, on s'intéresse à 100 car $100 = 4 \times 25$. Or $100 \equiv 0 \pmod 4$ ou $\pmod{25}$.
$A = 10^2(a_m \times 10^{m-2} + a_{m-1} \times 10^{m-3} + \cdots + a_2) + 10a_1 + a0$.
Donc $A \equiv 10a_1 + a_0 \pmod 4$ ou $\pmod{25}$. Donc A est divisible par 4 ou 25 si et seulement si le nombre $10a_1 + a_0$, qui s'écrit $a_1 a_0$ en base 10, l'est.
Exemple : 1738 n'est ni divisible par 4 ni par 25 car 38 ne l'est pas.
Les nombres de deux chiffres divisibles par 25 sont 00, 25, 50, 75 ; donc un nombre est divisible par 25 si et seulement s'il se termine par 00, 25, 50, 75.

Les nombres de deux chiffres divisibles par 4 sont moins visibles "à l'œil nu". On peut donc améliorer la règle en constatant que si $A \equiv 10a_1 + a_0 \pmod 4$ alors $A \equiv 2a_1 + a_0 \pmod 4$ car $10 \equiv 2 \pmod 4$.
Ainsi $1738 \equiv (2 \times 3 + 8) \equiv 2 \pmod 4$. Donc 1738 n'est pas divisible par 4, mais son reste dans la division par 4 est 2.

4. $10 \equiv -1 \pmod{11}$; donc $10^m \equiv (-1)^m \pmod{11}$ et :

$$A \equiv a_m(-1)^m + a_{m-1}.(-1)^{m-1} + \cdots + a_2 - a_1 + a_0 \pmod{11}$$

$A \equiv (a_m + a_{m-2} + \cdots + a_2 + a_0) - (a_{m-1} + a_{m-3} + \cdots + a_1) \pmod{11}$ si m est pair
$A \equiv (a_{m-1} + a_{m-3} + \cdots + a_2 + a_0) - (a_m + a_{m-2} + \cdots + a_1) \pmod{11}$ si m est impair
D'où la règle : un nombre est divisible par 11 si la somme de ses chiffres de rang pair moins la somme de ses chiffres de rang impair est divisible par 11.
Exemples : $1738 \equiv (7 + 8) - (1 + 3) \equiv 15 - 4 \equiv 0 \pmod{11}$.
$2318582 \equiv (2 + 1 + 5 + 2) - (3 + 8 + 8) \equiv 10 - 8 \equiv 2 \pmod{11}$.
2 318 582 n'est pas divisible par 11 et le reste de la division euclidienne de 2 318 582 par 11 est 2.

Exercice 17 : (page 26).

1) On a : $4^1 \equiv 4 \pmod 7$, $4^2 \equiv 2 \pmod 7$, $4^3 \equiv 2 \times 4 \equiv 8 \equiv 1 \pmod 7$.
Par suite, pour tout entier naturel k :

$$4^{3k} \equiv 1 \pmod 7,\ 4^{3k+1} \equiv 4 \pmod 7,\ 4^{3k+2} \equiv 2 \pmod 7$$

2) On a $851 = 121 \times 7 + 4$ donc $851 \equiv 4 \pmod 7$.
Il en découle que $A \equiv 4^{3n} + 4^{2n} + 4^n + 2 \pmod 7$.
- Si n est multiple de 3, $A \equiv 1 + 1 + 1 + 2 \equiv 5 \pmod 7$;
- si $n = 3k + 1$, $A \equiv 1 + 4^2 + 4^1 + 2 \equiv 1 + 2 + 4 + 2 \equiv 2 \pmod 7$;
- si $n = 3k + 2$, $A \equiv 1 + 4^4 + 4^2 + 2 \equiv 1 + 4 + 2 + 2 \equiv 2 \pmod 7$.

A a pour reste 5 dans sa division par 7, si n est multiple de 3, et pour reste 2 sinon.

3) $B = \overline{2103211}^{(4)}$.
Puisque $B = 2 \times 4^6 + 4^5 + 3 \times 4^3 + 2 \times 4^2 + 4 + 1$, le résultat de la première question montre que $B \equiv 2 \times 1 + 2 + 3 \times 1 + 2 \times 2 + 4 + 1 \pmod 7$, c–à–d. $B \equiv 2 \pmod 7$.
Donc, le reste (dans la numération décimale) de la division euclidienne de B par 7 est 2.

Exercice 18 : (page 27).

1) En numération décimale, on a : $N = a.12^3 + a.12^2 + b.12 + c$, donc N est divisible par 6 si et seulement si $(12^3 + 12^2)a + 12b + c \equiv 0 \pmod 6$.
Or, $12 \equiv 0 \pmod 6$, donc cette condition devient : $c \equiv 0 \pmod 6$, c'est-à-dire, puisque c est un chiffre de la numération en base douze et qu'il est supposé non nul, $c = 6$.

$$\boxed{c = 6.}$$

2) N est divisible par 9 si et seulement si $(12^3 + 12^2)a + 12b + 6 \equiv 0 \pmod 9$ et, comme $12 \equiv 3 \pmod 9$, on a $12^2 \equiv 9 \equiv 0 \pmod 9$ et $12^3 = 12 \times 12^2 \equiv 0 \pmod 9$;

donc $(12^3+12^2)a+12b+6 \equiv 3b+6 \pmod 9$. On obtient alors : N est divisible par 9 si et seulement si $3b+6 \equiv 0 \pmod 9$ ou $3b \equiv 3 \pmod 9$, soit $3b = 3+9k$ ($k \in \mathbb{Z}$ et $0 < b \leqslant 11$). On voit immédiatement que les seules valeurs possibles pour b sont 1, 4, 7 et 10.

Les seules valeurs possibles pour b sont 1, 4, 7 et 10.

3)

$$\begin{aligned} 1 &\equiv 1 \pmod{11} \\ 12 &\equiv 1 \pmod{11} \\ 12^2 &\equiv 1 \pmod{11} \\ 12^3 &\equiv 1 \pmod{11} \\ \text{donc } N &\equiv a.1 + a.1 + b.1 + c \pmod{11} \end{aligned}$$

Le reste de la division euclidienne de N par 11 est 7 si et seulement si $N \equiv 7 \pmod{11}$, soit $2a+b+c \equiv 7 \pmod{11}$.

$$\begin{aligned} 1 &\equiv 1 \pmod{13} \\ 12 &\equiv -1 \pmod{13} \\ 12^2 &\equiv 1 \pmod{13} \\ 12^3 &\equiv -1 \pmod{13} \\ \text{donc } N &\equiv a.(-1) + a.1 + b.(-1) + c \pmod{13} \end{aligned}$$

Le reste de la division euclidienne de N par 13 est 9 si et seulement si $N \equiv 9 \pmod{13}$, soit $-b+c \equiv 9 \pmod{13}$.
Or, $c = 6$, donc on a $-b+6 \equiv 9 \pmod{13}$, soit $b \equiv 10 \pmod{13}$ et, comme b est un chiffre de la numération en base douze, il vient : $b = 10$ (α en base douze).
D'autre part, on a $2a+b+c \equiv 7 \pmod{11}$ et, comme $b = 10$ et $c = 6$, on obtient $2a \equiv 2 \pmod{11}$ ou $2a = 2+11k$ ($k \in \mathbb{Z}$ et $0 < a \leqslant 11$). On voit immédiatement que la seule solution est $k = 0$ et $a = 1$.

$a = 1$ et $b = \alpha$.

4) On a alors : $N = \overline{11\alpha 6}^{(12)}$ donc, en base dix :

$$\begin{aligned} N &= 1 \times 12^3 + 1 \times 12^2 + 10 \times 12 + 6 \\ &= 1728 + 144 + 120 + 6 \\ &= 1998. \end{aligned}$$

$N = 1998.$

3. Solutions des exercices de la leçon 3.

Exercice 19 : (page 30).

• Soit $d = (a, b)$; d est un diviseur de a et de b, donc il divise $(b + ka)$ $(k \in \mathbb{Z})$; comme il divise également a, il divise le p.g.c.d. de a et de $(b + ka)$.

Réciproquement, soit $d' = (a, b + ka)$; d' est un diviseur de a et de $(b + ka)$, donc il divise $\Big((b + ka) - ka\Big)$, c'est-à-dire b ; on a : d' divise a et b, donc d' divise le p.g.c.d. de a et de b.

On en déduit donc que $d = d'$, c'est-à-dire $(a, b) = (a, b + ka)$ pour tout a de $\mathbb{Z}$, pour tout b de $\mathbb{Z}$ et pour tout k de $\mathbb{Z}$.

• Soit $d = (a, b)$; d est un diviseur de a et de b, donc il divise aussi $(-b)$; comme il divise également a, il divise le p.g.c.d. de a et de $(-b)$.

Réciproquement, soit $d'' = (a, -b)$; d'' est un diviseur de a et de $(-b)$, donc il divise $\Big(-(-b)\Big)$, c'est-à-dire b ; on a : d'' divise a et b, donc d'' divise le p.g.c.d. de a et de b.

On en déduit donc que $d = d''$, c'est-à-dire $(a, b) = (a, -b)$ pour tout a de $\mathbb{Z}$ et pour tout b de $\mathbb{Z}$.

Exercice 20 : (page 39).

Il est à remarquer que le produit $n(n + 1)$ est toujours pair car n et $n + 1$ sont deux entiers consécutifs et un des deux est pair. Donc $A = \dfrac{n(n+1)}{2} \in \mathbb{N}$.

On va raisonner modulo 3 sur la nombre $2A$.

– Si $n \equiv 0 \pmod 3$, alors $n(n + 1) \equiv 0 \pmod 3$, d'où $2A \equiv 0 \pmod 3$.

Comme 2 et 3 sont étrangers, d'après le théorème 3.6. page 35, on peut "simplifier" par 2 la congruence modulo 3.

Donc si $n \equiv 0 \pmod 3$, alors $A \equiv 0 \pmod 3$.

– Si $n \equiv 1 \pmod 3$, alors $n(n + 1) \equiv 2 \pmod 3$, d'où $2A \equiv 2 \pmod 3$, et par suite, toujours d'après le théorème 3.6., $A \equiv 1 \pmod 3$.

Donc si $n \equiv 1 \pmod 3$, alors $A \equiv 1 \pmod 3$.

– Si $n \equiv 2 \pmod 3$, alors $n(n+1) \equiv 3 \equiv 0 \pmod 3$, d'où $2A \equiv 0 \pmod 3$, on est ramené au premier cas $A \equiv 0 \pmod 3$.

Conclusion : A est divisible par 3 si et seulement si n est de la forme $n = 3k$ ou $n = 3k + 2$.

Le reste de la division euclidienne de A par 3 est 1 si n est lui-même congru à 1 modulo 3.

Exercice 21 : (page 39).

$n = 1000.a+100.b+10.c+a = 1001.a+100.b+10.c$ avec $a \neq 0$ puisque a est le premier chiffre.

Les relations $10 \equiv 3 \pmod 7$, $100 \equiv 2 \pmod 7$ et $1000 \equiv -1 \pmod 7$ montrent que n est divisible par 7 si et seulement si $2b + 3c \equiv 0 \pmod 7$ $(*)$.

n doit être congru à 1 modulo 99, c'est-à-dire $n - 1 \equiv 0 \pmod{99}$.

Puisque 9 et 11 sont premiers entre eux, pour que $n - 1$ soit divisible par 99 il faut et il suffit que $n - 1$ soit divisible par 9 et par 11 (en effet $a \mid c$, $b \mid c$ et a et b étrangers

implique que ab divise c (voir corollaire 3.3. page 33), le sens $ab \mid c \Rightarrow a \mid c$ et $b \mid c$ étant trivial).
D'où le système :

$$\begin{cases} 2a + b + c - 1 \equiv 0 \pmod 9 \\ \quad\ b - c - 1 \equiv 0 \pmod{11} \end{cases}$$

Puisque b et c sont deux entiers naturels inférieurs à 9, la dernière condition impose $b = c + 1$.
La première condition se réduit alors à $2a + 2c \equiv 0 \pmod 9$, ou encore, puisque 2 et 9 sont étrangers, en appliquant le théorème 3.6. page 35, $a + c \equiv 0 \pmod 9$.
Ainsi $a = 9 - c$ où $1 \leqslant c \leqslant 8$.
D'autre part $b = c + 1$ entraîne $c \equiv 1 \pmod 7$ d'après $(*)$. D'où les solutions :

$$\begin{array}{cccccccccc} c & = & 1, & b & = & 2, & a & = & 8, & n & = & 8218 \\ c & = & 8, & b & = & 9, & a & = & 1, & n & = & 1981 \end{array}$$

Exercice 22 : (page 39).
a)
Conditions nécessaires :
On doit résoudre $(a - b)(a + b) = 24$ avec a et b entiers naturels.
On remarque que $(a - b)$ et $(a + b)$ sont de même parité, que $a - b \leqslant a + b$ car $b \geqslant 0$, que $(a - b)$ est positif ou nul car $(a + b)$ l'est et leur produit aussi $(= 24)$. Donc $(a - b)$ et $(a + b)$ sont à chercher parmi les couples de diviseurs associés de 24 vérifiant ces conditions, à savoir :

$a-b$	$a+b$	
1	24	non
2	12	oui
3	8	non
4	6	oui

(les cas exclus l'étant car pas de même parité).
Il vient soit $\begin{cases} a - b = 2 \\ a + b = 12 \end{cases}$ soit $\begin{cases} a - b = 4 \\ a + b = 6 \end{cases}$ c'est-à-dire : soit $a = 7$ et $b = 5$; soit $a = 5$ et $b = 1$.
On vérifie réciproquement que ces deux couples conviennent.

$$S = \{(7,5);(5,1)\}$$

b) • Conditions nécessaires : $n^3 - m^3 = 999 = (n - m)(n^2 + nm + m^2)$ (identité remarquable)
$n^3 - m^3 = 999 > 0 \Longrightarrow n > m \Longrightarrow n > m$. Donc $(n - m)$ est un diviseur positif de 999 ainsi que $(n^2 + nm + m^2)$.
D'autre part $(n^2+nm+m^2) = (n-m)^2+3nm \geqslant (n-m)^2$, ou encore $n^3-m^3 \geqslant (n-m)^3$ (on peut avoir l'égalité pour $n = m$).

Soit $999 \geqslant (n-m)^3$ c'est-à-dire $10^3 > (n-m)^3$ ce qui entraîne que $10 > (n-m)$. Donc $(n-m)$ est un diviseur positif de 999 inférieur strictement à 10 et $(n-m) \in \{1,3,9\}$.
* si $n-m=1$: $(n-m)(n^2+nm+m^2) = (n-m)\left[(n-m)^2+3nm\right] = 1 \times [1+3nm]$.
Ceci est impossible car alors on aurait : $3nm = 999-1$ et 998 n'est pas divisible par 3.
* si $n-m=3$: $999 = 3 \times (9+3nm)$ d'où $nm = 108$. n et m sont alors solutions entières du système :

$$\begin{cases} n-m=3 \\ nm=108 \end{cases}$$

c'est-à-dire m est solution de l'équation $m^2+3m-108=0$.
On trouve $m=9$ (l'autre solution est à exclure, c'est -12) et $n=12$.
* si $n-m=9$: on a $999 = 9 \times (81+3nm)$ soit $nm=10$, ce qui donne

$$\begin{cases} n-m=9 \\ nm=10 \end{cases}$$

et m est solution de $m^2+9m-10=0$. On trouve $m=1$ et $n=10$.

• Conditions suffisantes :
$(n,m) \in \{(12,9);(10,1)\}$ sont bien solutions : $12^3-9^3 = 1728-729 = 999$ et $10^3-1=999$.

c) D'abord :

$$\begin{aligned} \text{p.p.c.m.}(a,b,c) &= \text{p.p.c.m.}\left[p.p.c.m.(a,b),c\right] \\ &= \text{p.p.c.m.}\left[a,\text{p.p.c.m.}(b,c)\right] \\ &= \text{p.p.c.m.}\left[b,\text{p.p.c.m.}(c,a)\right] \end{aligned}$$

(c'est l'associativité des p.p.c.m.).
n et $n+1$ sont étrangers car $1=(n+1)-n$ (relation de Bézout). De même, $n+1$ et $n+2$ le sont. Alors p.p.c.m.$(n,n+1) = n \times (n+1)$ et il faut chercher p.p.c.m.$\left[n(n+1),n+2\right]$.

Or $(n+2)-n=2$ (relation de Bézout), donc 2 est un multiple du p.g.c.d.$(n,n+2)$.
* Si n est impair, $n+2$ aussi et 2 n'est pas diviseur de n ni de $n+2$; alors 2 ne peut être le p.g.c.d.$(n,n+2)$ et celui-ci vaut 1. On a :

$$\left.\begin{array}{l} n,(n+2) \text{ sont étrangers} \\ (n+1),(n+2) \text{ sont étrangers} \end{array}\right\} \Rightarrow n \times (n+1) \text{ et } (n+2) \text{ sont étrangers}$$

(voir la proposition 3.2. page 33)
et p.p.c.m.$(n,n+1,n+2) = \text{p.p.c.m}\left[n(n+1),n+2\right] = n(n+1)(n+2)$.

* Si n est pair : $n+2$ aussi et 2 est à la fois diviseur commun de n et $n+2$ donc diviseur de leur p.g.c.d. et multiple de leur p.g.c.d. toujours d'après la relation de Bézout : $2=(n+2)-n$.

Donc, p.g.c.d.$(n, n+2) = 2$; d'où :

$$\begin{aligned} \text{p.p.c.m.}\big[n(n+1), n+2\big] &= \frac{n(n+1)(n+2)}{\text{p.g.c.d.}\big[n(n+1), n+2\big]} \\ &= \frac{n(n+1)(n+2)}{2} \end{aligned}$$

Exercice 23 : (page 39).

$$\left(\begin{matrix} n \equiv 5 \pmod{12} \\ n \equiv 14 \pmod{15}) \end{matrix} \right\} \Big) \iff (n = 12k + 5 = 15k' + 14,\ k \in \mathbb{Z},\ k' \in \mathbb{Z})$$

D'où $12k - 15k' = 9$, soit encore $4k - 5k' = 3 \quad (*)$
Or 4 et 5 sont étrangers. D'après l'identité de Bézout il existe u et v, tels que $4u+5v = 1$.
Ici on peut facilement trouver $u = -1$ et $v = 1$ (dans des cas plus compliqués, on peut trouver les coefficients u et v grâce à l'algorithme d'Euclide).
Une solution particulière de l'équation $(*)$ est donc $k = 3u$ et $k' = -3v$, soit $k = -3$ et $k' = -3$.
Cherchons <u>toutes</u> les solutions de l'équation $(*)$.

$$\begin{array}{rcrcl} 4k & - & 5k' & = & 3 \\ 4 \times (-3) & - & 5 \times (-3) & = & 3 \end{array}$$

En soustrayant membre à membre ces deux égalités, on obtient :

$$4 \times (k+3) - 5 \times (k'+3) = 0,$$

soit :

$$4 \times (k+3) = 5 \times (k'+3) \quad (**)$$

Mais, d'après le théorème de Gauss, 4 divisant le produit $5 \times (k'+3)$ et étant étranger à 5 , alors 4 divise $(k'+3)$. Il existe $\lambda \in \mathbb{Z}$ tel que $k'+3 = 4.\lambda$ et en remplaçant dans $(**)$, il vient :
$4 \times (k+3) = 5 \times (4\lambda)$; d'où $k+3 = 5\lambda,\ \lambda \in \mathbb{Z}$.
Finalement on obtient toutes les valeurs de k et k' par : $k = 5\lambda - 3$ et $k' = 4\lambda - 3,\ \lambda \in \mathbb{Z}$.
En reportant ceci dans l'expression de n, on a : $n = 12(5\lambda - 3) + 5 = 15(4\lambda - 3) + 14$, soit :
$n = 60\lambda - 31$ ou encore : $n = 60\lambda' + 29$ (avec $\lambda' = \lambda - 1$).
Donc, les nombres qui divisés par 12 donnent pour reste 5 et divisés par 15 donnent pour reste 14, sont les nombres congrus à 29 modulo 60.

Exercice 24 : (page 39).

a) Soit $d = \text{p.g.c.d.}(a, b)$ alors $a = da'$ et $b = db'$ avec a' et b' étrangers.

- On connaît le p.g.c.d. et la somme :

  $a + b = d(a' + b')$. Cela revient à chercher a' et b' étrangers tels que leur somme vaut $\dfrac{a+b}{d}$ qui est connue. On a nécessairement que a' et b' ne sont pas tous les deux pairs (car étrangers). On peut remarquer que le problème est symétrique en a et b, donc en a' et b'. Dès qu'on aura trouvé un couple solution, le couple "symétrique" le sera aussi.

  - $a' + b' = \dfrac{72}{9} = 8$ avec $(a', b') = 1$, a' et b' non tous les deux pairs :

    $a' = 1$ et $b' = 7$ ce qui donne : $a = 9$ et $b = 63$; et $a = 63$, $b = 9$ aussi.
    $a' = 3$ et $b' = 5$ ce qui donne : $a = 27$ et $b = 45$; et $a = 45$ et $b = 27$ aussi.
  - $a' + b' = \dfrac{96}{32} = 3$ $(a', b') \in \big\{(1,2);(2,1)\big\}$ ce qui donne $a = 32$ et $b = 64$ ou le symétrique.

- On connaît le p.g.c.d. et le produit :

  $ab = da'db' = da'b'$. On cherche donc deux nombres naturels étrangers tels que leur produit soit un nombre donné $\dfrac{ab}{d^2}$.

  - $a'b' = \dfrac{360}{25}$; impossible car 25 ne divise pas 360.
  - $a'b' = \dfrac{6480}{324} = 20$. On cherche les diviseurs naturels de 20 deux à deux étrangers. $(1, 20)$ et $(4, 5)$ sont les seules possibilités (avec les couples symétriques), ce qui donne
    $$(a, b) \in \big\{(18, 360); (360, 18); (72, 90); (90, 72)\big\}$$

b) Posons $d = \text{p.g.c.d.}(a, b)$ et $m = \text{p.p.c.m.}(a, b)$. On a à résoudre dans $\mathbb{N} \times \mathbb{N}$:

$$\begin{cases} m - d = 187 \\ md = ab \end{cases}.$$

Conditions nécessaires : $d \mid m$ (puisque $d \mid a$ et $a \mid m$ par exemple) donc $d \mid (m - d)$;
$0 < d \leqslant m$
Or $187 = 11 \times 17$. L'ensemble des diviseurs de 187 est donc : $d \in \{1, 11, 17, 187\}$

$d = 1$: Alors, $m = 187 + 1 = 188 = ab$, avec a et b étrangers.
$ab = 2^2 \times 47$, a et b étrangers, donne : $a = 1$, $b = 188$ ou $a = 4$ et $b = 47$, et les cas symétriques.

$d = 11$: Alors, $m = 187 + 11 = 198 = 11 \times 18$; $m = da'b' = 11a'b'$. Cela revient à chercher deux entiers naturels a' et b' étrangers tels que leur produit soit égal à :

$$a'b' = \frac{m}{d} = \frac{11 \times 18}{11} = 18 = 2 \times 3^2$$

On trouve $a' = 1$ et $b' = 18$ ou $a' = 2$ et $b' = 9$ et les cas symétriques ; finalement

$$(a, b) \in \big\{(11, 198); (198, 11); (22, 99); (99, 22)\big\}$$

$d = 17$: Alors, $m = 187 + 17 = 204$, $a'b' = 12$ avec a' et b' naturels étrangers ; il vient $a' = 1$ et $b' = 12$ ou $a' = 4$ et $b' = 3$ et les cas symétriques.

$$(a, b) \in \big\{(17, 204); (204, 17); (68, 51); (51, 68)\big\}$$

$d = 187$: Alors, $m = 187 + 187 = 374$, $a'b' = 2$ avec a' et b' naturels étrangers ; il vient $a' = 1$ et $b' = 2$ et les cas symétriques.

$$(a, b) \in \big\{(187, 374); (374, 187)\big\}.$$

Exercice 25 : (page 39).
Posons $a = da'$ et $b = db'$ avec a' et b' entiers relatifs étrangers. Alors, $m = da'b'$ (ou $m = -da'b'$) ; or, par hypothèse, $m = 12d$, donc $a'b' = 12$ ou $a'b' = -12$. Comme $12 = 2^2 \times 3$, on a les solutions suivantes pour (a', b') :

$$(1, 12) \quad (-1, 12) \quad (1, -12) \quad (-1, -12) \quad (3, 4) \quad (-3, 4) \quad (3, -4) \quad (-3, -4)$$

D'autre part, $a + b = 105$, donc $d(a' + b') = 105$, donc $(a' + b')$ doit diviser 105 :

a'	b'	$a' + b'$	$(a' + b')$ divise 105	d	a	b	$a \leqslant b$
1	12	13	non				
−1	12	11	non				
1	−12	−11	non				
−1	−12	−13	non				
3	4	7	oui	15	45	60	oui
−3	4	1	oui	105	−315	420	oui
3	−4	−1	oui	−105	315	−420	non
−3	−4	−7	oui	−15	−315	−420	non

On s'aperçoit finalement qu'il n'y a que deux solutions :

$$(a, b) = (45, 60) \text{ et } (a, b) = (-315, 420).$$

Exercice 26 : (page 39).
Tout diviseur commun à x et à y divise $2y - 9x$, c'est-à-dire 17.
Donc le p.g.c.d. de x et y ne peut être que 1 ou 17.
Pour que x soit divisible par 17, il faut et il suffit que $2k \equiv 1 \pmod{17}$, c'est-à-dire $2k \equiv 18 \pmod{17}$, soit encore k est congru à 9 modulo 17 (car 2 et 17 sont étrangers).
Dans ces conditions, le nombre y est congru à $9 \times 9 + 4 \equiv 85 \equiv 0$ modulo 17 (car $85 = 17 \times 5$).
En résumé :
- si $k \equiv 9 \pmod{17}$, le p.g.c.d. de x et y est 17 ;
- si $k \not\equiv 9 \pmod{17}$, x et y sont étrangers.

Exercice 27 : (page 39).
L'équation $x^2 - 9y^2 = -35$ s'écrit encore : $(3y - x)(3y + x) = 35$.
Comme x et y sont des entiers naturels, il en est de même pour $(3y + x)$ et donc aussi pour $(3y - x)$. En outre : $3y - x \leqslant 3y + x$.
Il y a donc deux possibilités :

$$\begin{cases} 3y - x &= 1 \\ 3y + x &= 35 \end{cases} \qquad \begin{cases} 3y - x &= 5 \\ 3y + x &= 7 \end{cases}$$

On obtient respectivement les couples $(17, 6)$ et $(1, 2)$. Les deux couples étant constitués d'entiers naturels conviennent.

Exercice 28 : (page 39).
On sait que C_p^k est un entier ($0 \leqslant k \leqslant p$). Notons-le λ. On a :

$$p\,! = \lambda . k\,!(p-k)\,!$$

Si p est premier :

p divise $p\,!$, donc p divise $\lambda . k\,!(p-k)\,!$; si $1 \leqslant k \leqslant p-1$, alors $1 \leqslant p-k \leqslant p-1$ et tous les termes de $k\,!$ et de $(p-k)\,!$ sont des entiers strictement positifs et strictement inférieurs à p, donc étrangers à p (voir proposition 3.1. page 32). On en déduit que p est étranger à $k\,!$ et à $(p-k)\,!$, donc (théorème de Gauss), p divise λ, c'est-à-dire : p divise C_p^k pour tout k $(1 \leqslant k \leqslant p-1)$

Si p n'est pas premier :

Soit $p = k.p_1$ avec k premier et $1 < p_1 < p$. Considérons $\lambda = C_p^k$ (qui est un entier) :

$$\lambda = \frac{p\,!}{k\,!(p-k)\,!} = \frac{p(p-1)\ldots(p-k+1)}{k(k-1)\ldots 1}.$$

Supposons que p divise λ : $\lambda = p.\lambda_1$ avec λ_1 entier ; il vient :

$$\begin{aligned} p.\lambda_1 &= \frac{p(p-1)\ldots(p-k+1)}{k(k-1)\ldots 1} \\ \lambda_1.k(k-1)\ldots 1 &= (p-1)\ldots(p-k+1) \\ \text{(A.1)} \qquad \lambda_1.k(k-1)\ldots 1 &= (k.p_1-1)(k.p_1-2)\ldots(k.p_1-k+1) \end{aligned}$$

Or :

$$\begin{aligned} k.p_1 - k + 1 &\equiv 1 \pmod{k} \\ k.p_1 - k + 2 &\equiv 2 \pmod{k} \\ &\vdots \quad \vdots \quad \vdots \\ k.p_1 - 2 &\equiv k - 2 \pmod{k} \\ k.p_1 - 1 &\equiv k - 1 \pmod{k} \end{aligned}$$

k est premier, ces $(k-1)$ congruences successives prouvent que les $(k-1)$ entiers $(k.p_1 - k + 1)$, $(k.p_1 - k + 2)$, ..., $(k.p_1 - 2)$, $(k.p_1 - 1)$ sont tous étrangers à k, donc qu'il en est de même pour leur produit ; or, dans l'équation (A.1), on a k qui divise le membre de gauche, il doit donc aussi diviser le membre de droite, ce qui est impossible. Il y a donc contradiction, donc p ne divise pas λ ; on a donc trouvé un k $(1 \leqslant k \leqslant p-1)$ tel que p ne divise pas C_p^k ; par contraposition, on a donc le résultat cherché.

4. Solutions des exercices de la leçon 4.

Exercice 29 : (page 44).
$a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ avec $\alpha_i > 0$ pour tout $i = 1, \dots, k$. Soit b un diviseur strictement positif de a. Montrons que :

$$(b \mid a) \iff (b \text{ s'écrit } b = p_1^{\beta_1} \dots p_k^{\beta_k} \text{ avec } 0 \leqslant \beta_i \leqslant \alpha_i \text{ pour tout } i = 1, \dots, k)$$

$\Longleftarrow$: c'est immédiat : si $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ avec $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $i = 1, \dots, k$ alors, en posant $c = p_1^{\alpha_1 - \beta_1} \dots p_k^{\alpha_k - \beta_k}$, on a c entier naturel (car $0 \leqslant \beta_i \leqslant \alpha_i$ pour tout $i = 1, \dots, k$) et $a = bc$, donc $b \mid a$.

$\Longrightarrow$:

- si $b = 1$, alors b est bien de la forme $b = p_1^0 \dots p_k^0$.
- si $b \neq 1$, alors, soit p un diviseur premier quelconque de b, alors p divise b qui divise a, donc p divise a ; d'après le lemme d'Euclide (proposition 4.1. page 41), on en déduit que p divise l'un des p_i et, comme il s'agit de deux nombres premiers, on a alors $p = p_i$. Donc, tout diviseur premier de b est un des p_i ; b s'écrit donc sous la forme $b = p_1^{\gamma_1} \dots p_k^{\gamma_k}$ avec $\gamma_i \geqslant 0$ pour tout $i = 1, \dots, k$. Il est immédiat d'autre part que γ_i doit être inférieur à α_i pour tout $i = 1, \dots, k$ sinon b ne serait pas un diviseur de a.

On vient donc de caractériser les diviseurs de a ; considérons maintenant deux diviseurs de a : $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ et $c = p_1^{\gamma_1} \dots p_k^{\gamma_k}$. Comme la décomposition d'un entier en produit de facteurs premiers est unique, on a :

$$(b \neq c) \iff \{\beta_1, \dots, \beta_k\} \neq \{\gamma_1, \dots, \gamma_k\}$$

Si l'on appelle D l'ensemble des diviseurs de a, on a donc :

$$D = \{p_1^{\beta_1} \dots p_k^{\beta_k}, 0 \leqslant \beta_1 \leqslant \alpha_1, \dots, 0 \leqslant \beta_k \leqslant \alpha_k\}$$

On a donc $(1 + \alpha_1)$ choix possibles pour β_1, ..., $(1 + \alpha_k)$ choix possibles pour β_k, ce qui nous donne $(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$ diviseurs possibles.

$$\boxed{d = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k).}$$

Remarque : On a un procédé pratique pour obtenir tous les diviseurs de a : on effectue les produits

$$(1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \dots + p_2^{\alpha_2}) \dots (1 + p_k + p_k^2 + \dots + p_k^{\alpha_k})$$

et chacun des termes obtenus dans le développement est un diviseur de a.

Exemple : $108 = 2 \times 54 = 2^2 \times 27 = 2^2 \times 3 \times 9 = 2^2 \times 3^2 \times 3 = 2^2 \times 3^3$.
Donc, $k = 2$, $\alpha_1 = 2$ et $\alpha_2 = 3$, ce qui nous donne $d = (1 + 2)(1 + 3) = 12$: il y a 12 diviseurs de 108. Pour les obtenir :

$$(1 + 2 + 4)(1 + 3 + 9 + 27) = 1 + 2 + 4 + 3 + 6 + 12 + 9 + 18 + 36 + 27 + 54 + 108$$

Les douze diviseurs de 108 sont donc 1, 2, 4, 3, 6, 12, 9, 18, 36, 27, 54 et 108.

ANNEXE A.

ANNEXE B.

Quelques algorithmes

1. Crible d'Ératosthène

```
Lire n
Déclarer T comme tableau booléen de dimension n
T(1) = faux
Pour i = 2 jusqu'à n
|   T(i) = vrai
Fin Pour
a = 2
M = √n
Tant que a ⩽ M
|   Si T(a) = vrai
|   |   b = a × a
|   |   Tant que b ⩽ n
|   |   |   T(b) = faux
|   |   |   b = b + a
|   |   Fin Tant que
|   Fin Si
|   a = a + 1
Fin Tant que
Pour i = 1 jusqu'à n
|   Si T(i) = vrai
|   |   Afficher i
|   Fin Si
Fin Pour
```

2. Savoir si un nombre est premier ou non

Lire n
$p = 2$
$M = \sqrt{n}$
$r = 1$
Tant que ($p \leqslant M$ et $r \neq 0$)
    $q = \mathrm{E}\left(\frac{n}{p}\right)$
    $r = n - p \times q$
    Si $p = 2$
        $p = 3$
    Sinon
        $p = p + 2$
    Fin Si
Fin Tant que
Si $r = 0$
    $p = \frac{n}{q}$
    Afficher p et q
Sinon
    Afficher "n premier"
Fin Si

3. Algorithme d'Euclide d'obtention du p.g.c.d. de deux nombres.

Lire a et b
Tant que $b \neq 0$
    $q = \mathrm{E}\left(\frac{a}{b}\right)$
    $r = a - b \times q$
    $a = b$
    $b = r$
Fin Tant que
Afficher a

4. Coefficients de Bézout

Lire a et b
$u = 1$; $v = 0$; $uu = 0$; $vv = 1$
Tant que $b \neq 0$
    $q = \mathrm{E}\left(\frac{a}{b}\right)$
    $r = a - b \times q$
    $a = b$
    $b = r$
    $uuu = u - uu \times q$
    $u = uu$
    $uu = uuu$
    $vvv = v - vv \times q$
    $v = vv$
    $vv = vvv$
Fin Tant que
Afficher u et v

5. Décomposition d'un nombre en facteurs premiers

Lire n
$p = 2$
$r = 0$
Tant que $r = 0$
    $M = \sqrt{n}$
    $r = 1$
    Tant que ($p \leqslant M$ et $r \neq 0$)
        $q = \mathrm{E}\left(\frac{n}{p}\right)$
        $r = n - p \times q$
        Si $p = 2$
            $p = 3$
        Sinon
            $p = p + 2$
        Fin Si
    Fin Tant que
    Si $r = 0$
        $p = \frac{n}{q}$
        Afficher p
        $n = q$
    Sinon
        Afficher n
    Fin Si
Fin Tant que

ANNEXE B.

ANNEXE C.

Travaux pratiques

Les TP qui suivent ne sont pas, *a priori*, à réinvestir tels quels en Terminale ; il s'agissait principalement par leur biais d'appliquer et de développer, lors du stage, les résultats énoncés dans les leçons. Ils ont donné lieu à des calculs pratiques et à l'utilisation d'ordinateurs.

TP 1

Équations diophantiennes

• Équations diophantiennes [1]

Soit à résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation

(C.1) $$ax + by = c.$$

a) Il est nécessaire que c soit un multiple de p.g.c.d. de a et b (justifiez pourquoi).

b) Dans ce cas on divise (1) par p.g.c.d.(a, b) et on obtient

(C.2) $$a'x + b'y = c'$$

avec a' et b' étrangers.

On peut déterminer une solution particulière x_0 et y_0 de (C.2) en utilisant une relation de Bézout et l'algorithme d'Euclide, ou en utilisant les congruences.

c) On trouve enfin toutes les solutions de (C.2) en soustrayant membre à membre :

$$\begin{array}{rcl} a'x + by' & = & c' \\ a'x_0 + b'y_0 & = & c' \\ \hline a'(x - x_0) + b'(y - y_0) & = & 0 \end{array} \qquad \text{(C.3)}$$

puis en utilisant le théorème de Gauss pour résoudre (C.3).

• Recherche d'une solution particulière dans $\mathbb{Z}^2$ de $au + bv = c$:

On peut chercher une solution particulière avec les coefficients d'une relation de Bézout, grâce à l'algorithme d'Euclide, ou bien utiliser les congruences ainsi :

Soit par exemple : $121u + 37v = 3$.

$\star$ L'équation implique $121u \equiv 3 \pmod{37}$;

mais $121 \equiv 10 \pmod{37}$ (car $121 = 37 \times 3 + 10$) ; le travail se ramène donc à la recherche de la solution de $10u \equiv 3 \pmod{37}$;

$\star$ $10u \equiv 3 \pmod{37}$ équivaut à : il existe $w \in \mathbb{Z}$ tel que $10u + 37w = 3$; ce qui signifie $37w \equiv 3 \pmod{10}$ qui équivaut à $7w \equiv 3 \pmod{10}$.

$\star$ $7w + 10k = 3$ ou $10k \equiv 3 \pmod{7}$ soit encore : $3k \equiv 3 \pmod{7}$;

Or, d'après le cours, comme 3 et 7 sont étrangers,

$$\big(3k \equiv 3 \pmod{7}\big) \iff \big(k \equiv 1 \pmod{7}\big).$$

On peut prendre par exemple $k = 1$ et on trouve alors : $7w + 10 = 3$ soit $w = -1$ et $10u - 37 = 3$ soit $u = 4$; puis $121 \times 4 + 37v = 3$ donc $v = -13$.

Applications : Résoudre les équations diophantiennes suivantes :

$$\begin{array}{llllll} (1) & 3x - 4y = 1 & ; & (2) & 7x - 9y = 5 \\ (3) & 8x + 14y = 3 & ; & (4) & 24x - 90y = -12 \end{array}$$

[1] du nom de Diophante, mathématicien grec (325–409) qui le premier les étudia.

TP 2

Théorème des restes chinois

• Problème du cuisinier chinois[1]

Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent et 6 d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés et le partage laisserait alors 5 pièces d'or à ce dernier.
Quelle est la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

• Méthodes de résolution

Soit X le nombre cherché ; on doit avoir :

$$\begin{cases} X \equiv 3 \pmod{17} \\ X \equiv 4 \pmod{11} \\ X \equiv 5 \pmod{6} \end{cases}$$

Première méthode :

- On écrit $x = 3 + 17k$.
- puis : $3 + 17k \equiv 4 \pmod{11}$, ce qui équivaut à $3 + 6k \equiv 4 \pmod{11}$, donc :

$$6k \equiv 1 \pmod{11}.$$

  Comme 6 et 11 sont étrangers, il y a une solution ; on cherche l'inverse de 6 modulo 11 (identité de Bézout en général), ici on a immédiatement $6 \times 2 \equiv 1 \pmod{11}$. Donc $k \equiv 2 \pmod{11}$, c'est-à-dire : $k = 2 + 11\lambda$.

- $\begin{cases} x = 3 + 17(2 + 11\lambda) \\ x \equiv 5 \pmod{6} \end{cases}$ D'où : $37 + 17 \times 11 \times \lambda \equiv 5 \pmod{6}$ ou encore :

$$1 + \lambda \equiv 5 \pmod{6};$$

  donc $\lambda \equiv 4 \pmod{6}$, c'est-à-dire : $\lambda = 4 + 6\mu$.

- on remonte et on obtient :

$$x = 3 + 17\big[2 + 11(4 + 6\mu)\big] = 3 + 34 + 748 + 17 \times 11 \times 6 \times \mu = 785 + 17 \times 11 \times 6 \times \mu.$$

  La plus petite solution est donc 785 et toutes les autres solutions lui sont congrues modulo $17 \times 11 \times 6 = 1122$.

Deuxième méthode : 17 et 11×6 sont étrangers donc il existe u_1 tel que $11 \times 6 \times u_1 \equiv 1 \pmod{17}$; on trouve, par exemple, $u_1 = 8$.
11 et 17×6 sont étrangers donc il existe u_2 tel que $17 \times 6 \times u_2 \equiv 1 \pmod{11}$; on trouve, par exemple, $u_2 = 4$.
6 et 17×11 sont étrangers donc il existe u_3 tel que $17 \times 11 \times u_3 \equiv 1 \pmod{6}$; on trouve, par exemple, $u_3 = 1$.
Soit $X_0 = 3 \times 66 \times 8 + 4 \times 102 \times 4 + 5 \times 187 \times 1$; alors X_0 est une solution du système.
Soit x une autre solution de ce système ; on doit avoir :

$$\begin{cases} X - X_0 \equiv 0 \pmod{17} \\ X - X_0 \equiv 0 \pmod{11} \\ X - X_0 \equiv 0 \pmod{6} \end{cases}$$

$$X - X_0 = 17k_1 = 11k_2 = 6k_3$$

11 et 17 sont étrangers donc $11 \mid k_1$; $k_1 = 11\ell_1$ et $k_2 = 17\ell_1$.

$$X - X_0 = 11 \times 17\ell_1 = 6k_3$$

11×17 et 6 sont étrangers donc $6 \mid \ell_1$; $\ell_1 = 6\ell_2$ et $k_3 = 17 \times 11\ell_2$.
D'où :

$$X - X_0 = 17 \times 11 \times 6\ell_2$$

Les solutions du système sont les X congrus à X_0 modulo $6 \times 11 \times 17$.
La solution recherchée (minimale) est 785.

• **Cas général**

Théorème des restes chinois

Soient $m_1, m_2, \ldots, m_r$ des entiers ***étrangers deux à deux*** *; soient $a_1, a_2, \ldots, a_r$ des entiers quelconques ; on pose $p_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} m_j$ et on définit b_i par : $p_i.b_i \equiv 1 \pmod{m_i}$.*

Alors, le système

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

a une solution $x_0 = \sum_{i=1}^{r} p_i.b_i.a_i$.

De plus, toutes les solutions sont congrues à x_0 modulo le produit des m_i.

TP 3

Période du développement décimal illimité d'un rationnel

Tout nombre rationnel admet un développement décimal illimité périodique et, réciproquement tout développement décimal illimité périodique représente un rationnel. Pour une démonstration, voir [7].

• **Exemple :** $\frac{17}{37} = 0,459459459\ldots = 0,\overline{459}$. 459 est le **cycle** de $\frac{17}{37}$ et sa **période** est 3.

• **Résultat**

Théorème

Soit $x = \frac{m}{n}$ *un rationnel positif non décimal écrit sous forme irréductible (c'est-à-dire* $m \in \mathbb{N} - \{0\}$, $n \in \mathbb{N} - \{0\}$, $(m,n) = 1$*).*

1. *n s'écrit sous la forme $n = 2^\alpha \times 5^\beta \times q$ avec $(10,q) = 1$ et $q > 1$*
2. *Il existe un plus petit entier strictement positif h tel que $10^h \equiv 1 \pmod{q}$*
3. *La période du développement décimal illimité de x est égale à cet entier h.*

Preuve :

1. Un rationnel est un décimal si et seulement si le dénominateur de sa forme irréductible se décompose sous la forme $2^\alpha \times 5^\beta$; comme x est supposé non décimal, dans la décomposition de n en facteurs premiers : $n = 2^\alpha \times 5^\beta \times \prod p_i^{\alpha_i}$ (avec p_i premier différent de 2 et de 5), les α_i ne sont pas tous nuls ; on pose alors $q = \prod p_i^{\alpha_i}$ et l'on a bien $q > 1$ et $(10,q) = 1$ puisque ni 2, ni 5 ne divisent q.

2. Démontrons maintenant l'existence de h : lorsque l'on écrit $10^j \equiv \delta_j \pmod{q}$ (avec $0 \leqslant \delta_j \leqslant q-1$) pour $j \geqslant 1$, on a en réalité $0 < \delta_j$ puisque $(10,q) = 1$ et donc l'ensemble des δ_j ne contient que $(q-1)$ éléments au plus. Dans l'ensemble $\left\{10^1, 10^2, \ldots, 10^q\right\}$, deux (au moins) éléments sont donc congrus au même $\delta_j \pmod{q}$, donc congrus entre eux (mod q) :

$$\exists\, a \in \left\{1,2,\ldots,q\right\} \quad \exists\, b \in \left\{1,2,\ldots,q\right\} \quad \text{tels que} \quad \begin{cases} a \neq b \\ 10^a \equiv 10^b \pmod{q} \end{cases}$$

On peut prendre par exemple $a > b$; alors $10^{a-b} \times 10^b \equiv 10^b \pmod{q}$; par hypothèse, q et 10 sont étrangers, donc q et 10^b sont étrangers ; d'après le théorème 3.6. p. 35, on en déduit $10^{a-b} \equiv 1 \pmod{q}$. L'ensemble des entiers μ strictement

positifs vérifiant $10^\mu \equiv 1 \pmod{q}$ est donc non vide, il possède donc un plus petit élément que l'on note h.

3. Posons $\gamma = \max\{\alpha, \beta\}$. x s'écrit alors :

$$x = \frac{2^{\gamma-\alpha} \times 5^{\gamma-\beta} \times m}{10^\gamma \times q} = \frac{m'}{10^\gamma \times q} \quad \text{avec } (m', q) = 1 \text{ car } q \text{ étranger à 2, à 5 et à } m.$$

On pose alors $y = \dfrac{m'}{q} = 10^\gamma \times x$ donc y a la même période que x (on obtient y en décalant la virgule dans l'écriture de x de γ rangs vers la gauche).

On effectue ensuite la division euclidienne de m' par q :

$$m' = q \times e + \ell \qquad \text{avec } 0 \leqslant \ell < q.$$

On a même, plus précisément, $0 < \ell < q$ car $(m', q) = 1$.

Alors, $y = \dfrac{q \times e + \ell}{q} = e + \dfrac{\ell}{q}$, et on pose $z = \dfrac{\ell}{q}$.

z est la partie décimale de y (e en est sa partie entière), donc z a la même période que y, donc que x. Remarquons de plus que $\begin{cases} \ell = m' - q \times e \\ (m', q) = 1 \end{cases}$ donc que $(\ell, q) = 1$.

Nous sommes donc ramenés à étudier la période de $z = \dfrac{\ell}{q}$ avec $0 < \ell < q$, $(\ell, q) = 1$ et $(10, q) = 1$.

Supposons alors que la périodicité commence au rang $i+1$ après la virgule et que la période soit égale à d $(d > 0)$; on écrit :

$$z = 0, z_1 \dots z_i \overline{z_{i+1} \dots z_{i+d}}$$

Alors :

$$\begin{aligned} 10^i \times z - z_1 \dots z_i &= 0, \overline{z_{i+1} \dots z_{i+d}} \\ 10^d \times \left(10^i \times z - z_1 \dots z_i\right) &= z_{i+1} \dots z_{i+d}, \overline{z_{i+1} \dots z_{i+d}} \\ &= z_{i+1} \dots z_{i+d} + 0, \overline{z_{i+1} \dots z_{i+d}} \\ &= z_{i+1} \dots z_{i+d} + \left(10^i \times z - z_1 \dots z_i\right) \end{aligned}$$

Donc :

$$\left(10^d - 1\right) \times \left(10^i \times z - z_1 \dots z_i\right) = z_{i+1} \dots z_{i+d}$$

$$z = \frac{\ell}{q} \quad \text{donc} \quad \left(10^d - 1\right) \times \left(10^i \times \ell - q \times z_1 \dots z_i\right) = q \times z_{i+1} \dots z_{i+d}$$

q divise $q \times z_{i+1} \dots z_{i+d}$ donc q divise $\left(10^d - 1\right) \times \left(10^i \times \ell - q \times z_1 \dots z_i\right)$; comme q est étranger à 10 et à ℓ, il est étranger à $10^i \times \ell$ donc étranger également à

$\left(10^i \times \ell - q \times z_1 \dots z_i\right)$; le théorème de Gauss nous permet alors d'affirmer que q divise $\left(10^d - 1\right)$ donc que $10^d \equiv 1 \pmod{q}$. Donc, d'après la définition de h, on en déduit que $d \geqslant h$ (on peut même démontrer que d est un multiple de h).

Enfin, traduisons le fait que $10^h \equiv 1 \pmod{q}$:

$$\begin{aligned} 10^h &= 1 + \lambda \times q \qquad \lambda \in \mathbb{N} - \{0\} \\ 10^h \times z &= z + \lambda \times q \times z \\ z_1 \dots z_h, z_{h+1} \dots &= 0, z_1 \dots + \lambda \times q \times \frac{\ell}{q} \\ &= 0, z_1 \dots + \lambda \times \ell \qquad \text{et } \lambda \times \ell \in \mathbb{N} - \{0\} \end{aligned}$$

Donc :

$$\begin{cases} z_1 \dots z_h = \lambda \times \ell \\ z_{h+1} = z_1 \\ z_{h+2} = z_2 \\ \qquad \vdots \end{cases}$$

Ceci prouve, d'une part, que h est un multiple de la période du développement décimal de z (c'est-à-dire : h multiple de d) et, d'autre part, que ce développement décimal de z est périodique à partir du premier rang après la virgule.

On en déduit donc que $h = d$ (ce que l'on voulait démontrer) et que le développement décimal de z est périodique à partir du premier rang après la virgule.

Exemple : $x = \dfrac{11}{42}$. On a $m = 11$ et $n = 42$.

Alors, $x = \dfrac{11}{2 \times 3 \times 7} = \dfrac{5 \times 11}{10 \times 21} = \dfrac{55}{10 \times 21}$. On a $m' = 55$, $\gamma = 1$, $q = 21$, $y = \dfrac{55}{21}$.

$55 = 2 \times 21 + 13$ donc on a $e = 2$, $\ell = 13$, $q = 21$, $z = \dfrac{13}{21}$.

Cherchons h :

$$\begin{aligned} 10^1 &\equiv 10 \pmod{21} \\ 10^2 &\equiv 16 \pmod{21} \\ 10^3 &\equiv 13 \pmod{21} \\ 10^4 &\equiv 4 \pmod{21} \\ 10^5 &\equiv 19 \pmod{21} \\ 10^6 &\equiv 1 \pmod{21} \end{aligned}$$

Donc, $h = 6$. La période du développement décimal de z (donc de x) est égale à 6. En effet, on vérifie immédiatement que $x = 0,2\overline{619047}$ ($z = 0,\overline{619047}$).

TP 4

Tests de primalité : Fermat [1] et Wilson [2]

Théorème de Wilson
p entier naturel est premier si et seulement si $(p-1)!+1 \equiv 0 \pmod{p}$.

Preuve :

$\Longleftarrow$:

$$\begin{aligned} (p-1)!+1 &= kp \\ kp-(p-1)! &= 1 \end{aligned}$$

Donc p est étranger à $(p-1)!$, donc étranger à tous les entiers compris entre 1 et $(p-1)$. On en déduit que p est un nombre premier.

$\Longrightarrow$:

$p = 2$ et $p = 3$: C'est immédiat.

$p > 3$: on va multiplier entre eux tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ en les regroupant par couple d'inverses ; il faut donc d'abord chercher ceux qui sont leur propre inverse.

- Cherchons les x compris entre 0 et $(p-1)$ tels que $x^2 \equiv 1 \pmod{p}$:
  $x = 0$ ne convient pas ; $x = 1$ convient ; résolvons dans le cas $2 \leqslant x \leqslant p-1$:

$$\begin{aligned} x^2-1 &= kp \\ (x-1)(x+1) &= kp \end{aligned}$$

$1 \leqslant x-1 \leqslant p-2$ et p premier donc p et $x-1$ sont étrangers ; d'après le théorème de Gauss, on en déduit que p divise $x+1$; or $3 \leqslant x+1 \leqslant p$, donc $x+1 = p$, soit $x = p-1$.
Les deux seuls nombres compris entre 0 et $p-1$ qui sont leur propre inverse modulo p sont 1 et $p-1$.

[1] Pierre Simon de Fermat (1601–1665).
[2] John Wilson (1741–1793).

- Pour $2 \leqslant x \leqslant p-2$, cherchons son inverse modulo p :
  On cherche à résoudre l'équation en y :

  (C.1) $\qquad xy \equiv 1 \pmod{p} \qquad$ avec $0 \leqslant y \leqslant p-1$;

  $y = 0$, $y = 1$, $y = p-1$ ne conviennent pas d'après ce qui précède, donc $2 \leqslant y \leqslant p-2$.
  On rappelle que l'équation $ay \equiv b \pmod{n}$ a une solution unique modulo n lorsque a et n sont étrangers. Or, x et p sont étrangers ; on en déduit que l'équation (C.1) a une solution unique en y modulo p.
  Notons $E = \{2, 3, \ldots, p-2\}$ (ensemble à $p-3$ éléments) et f l'application de E dans E qui à x associe y ; vu la symétrie du problème, f est une involution, donc une bijection de E dans E, c'est-à-dire une permutation de E. De plus, d'après ce qui précède, pour tout x de E, $f(x) \neq x$.
  On obtient donc $\dfrac{p-3}{2}$ paires $\{x, f(x)\}$ qui forment une partition de E.

- $$\begin{aligned} \prod_{x=2}^{p-2} &= (p-2)! \\ &\equiv 1 \pmod{p} \\ \text{Donc} \qquad (p-1)! &\equiv p-1 \pmod{p} \end{aligned}$$

  Donc $(p-1)! + 1 \equiv 0 \pmod{p}$.[3]

Théorème de Fermat (petit)
Il y a deux formes équivalentes du petit théorème de Fermat qui sont :

1. *Soit p premier, $a \in \mathbb{N}$, $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.*
2. *Soit p premier, $a \in \mathbb{N}$, alors $a^p \equiv a \pmod{p}$.*

Prouvons 1 $\iff$ 2 :

1 $\Longrightarrow$ 2 : Si $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}$ (compatibilité)
Si $p \mid a$, alors $a \equiv 0 \pmod{p}$ donc $a^p \equiv a \pmod{p}$.

2 $\Longrightarrow$ 1 :

$$\begin{aligned} a^p &\equiv a \pmod{p} \\ a^p - a &\equiv 0 \pmod{p} \\ a(a^{p-1} - 1) &\equiv 0 \pmod{p} \end{aligned}$$

Si $p \nmid a$, alors a et p sont étrangers ; d'après le théorème de Gauss, p divise $a^{p-1} - 1$.

[3] Cette preuve utilise uniquement des notions élémentaires ; cependant on peut obtenir une preuve plus élégante en utilisant la théorie des groupes.

Prouvons 1 : $p \nmid a$ donc les produits $a \times 1$, $a \times 2$, ..., $a \times (p-1)$ donnent, modulo p, tous les entiers compris entre 1 et $p-1$ (cf. théorème 3.6. page 35).

Donc $(a \times 1) \times (a \times 2) \times \cdots \times (a \times (p-1)) \equiv (p-1)! \pmod{p}$

Donc $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$.

Or, p et $(p-1)!$ sont étrangers puisque p est premier, donc, d'après le théorème de Gauss, $a^{p-1} \equiv 1 \pmod{p}$.

Prouvons 2 : Nous allons démontrer, pour un p premier fixé, $a^p \equiv a \pmod{p}$ en faisant une récurrence sur a.

Pour $a = 0$, c'est vrai.

Pour $a \geqslant 0$, supposons $a^p \equiv a \pmod{p}$:

$$(a+1)^p = a^p + 1 + \sum_{k=1}^{p-1} C_p^k a^k$$

Or, si p est premier, p divise C_p^k pour $1 \leqslant k \leqslant p-1$ (cf. exercice 28 page 39). Donc, $(a+1)^p \equiv a^p + 1 \pmod{p} \equiv a + 1 \pmod{p}$.

Application : soit p un nombre premier et a un entier non multiple de p. On cherche les n de $\mathbb{N}$ solutions de l'équation $a^n \equiv 1 \pmod{p}$.
Le petit théorème de Fermat donne une solution : $p-1$. Soit m la plus petite solution strictement positive de l'équation ; on a $0 < m \leqslant p-1$. Effectuons la division euclidienne de $p-1$ par m :

$$\begin{cases} p-1 = mq + r \\ 0 \leqslant r < m \end{cases}$$

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ a^{mq+r} &\equiv 1 \pmod{p} \\ (a^m)^q . a^r &\equiv 1 \pmod{p} \\ \text{donc } a^r &\equiv 1 \pmod{p} \end{aligned}$$

Par définition de m et de r, il vient $r = 0$. Donc la solution strictement positive minimale est un diviseur de $p-1$ et toute solution est un multiple de cette solution minimale (même démonstration).

Exemple : $1998^n \equiv 1 \pmod{17}$.
$1998 \equiv 9 \pmod{17}$, donc 17 ne divise pas 1998. D'après ce qui précède, la solution minimale est un diviseur de $17 - 1 = 16$. Le calcul montre que c'est 8.

TP 5

Messages secrets

Un cryptosystème[8] est un procédé mathématique pour coder ou transformer une information afin qu'elle soit inintelligible pour ceux à qui elle n'est pas destinée.
Le procédé de codage débute généralement par la transcription du texte en clair, ou message non codé par une suite de nombres à l'aide d'un alphabet numérique tel que celui indiqué ci-dessous.

Alphabet décimal

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Nous allons étudier deux types de cryptosystèmes : les cryptosystèmes conventionnels ou "à clef secrète" et les cryptosystèmes "à clef publique" ou "à clef révélée".

Cryptosystèmes à clef secrète

Quiconque veut envoyer un message codé utilise un algorithme, ou procédé général de codage G, et reçoit une clef K.
La clef (qui doit être tenue secrète) est un ensemble de paramètres permettant d'utiliser l'algorithme, lequel peut être rendu public. En d'autres termes, l'algorithme C et la clef K déterminent ensemble le codage C_K envisagé.
Ainsi, si M est le message numérisé, on code :

$$P = C_K(M)$$

Le décryptage s'effectue par un autre algorithme public D et la clef K tels que

$$D_K(P) = D_K\big(C_K(M)\big) = M$$

Par suite, la sûreté de tels systèmes repose entièrement sur le secret de la clef.

ANNEXE C.

Sans décoder

"ET J'EN AI ASSURÉMENT TROUVÉ L'ADMIRABLE DÉMONSTRATION. LA MARGE TROP EXIGUË NE LA CONTIENDRAIT PAS."

Voici l'annotation qu'écrivit en 1660 Pierre de Fermat dans son "Précis de l'arithmétique" de Diophante à propos de sa fameuse conjecture : "Une puissance $n^{\text{ème}}$ d'entier ne peut se décomposer en somme de deux puissances $n^{\text{èmes}}$ d'entiers dès que $n \geqslant 3$". Nous avons crypté la phrase de Fermat de diverses manières. Votre mission, si vous l'acceptez, sera de découvrir les différents processus de codage et de les expliquer.

Nous vous indiquons à chaque fois la clef secrète K utilisée (sauf pour le premier exemple). À vous de découvrir C_K connaissant M, K et $C_K(M)$ et de donner une interprétation mathématique du processus de codage.

1. À la manière de Jules César[1] : (pas de clef)

T I Y T C P X P H H J G T B T C I I G D J

K T A P S B X G P Q A T S T B D C H I G P

I X D C A P B P G V T I G D E T M X V J T

C T A P R D C I X T C S G P X I E P H

2. À la manière de Vigénère[2] : (clef K = HAUSDORFF)

M U E X R P A G Y A V M X Q T F Z Z Z P P

O I A S J S Q S V U P T V K S W O N M V P

L O U V M V F E G Y K Z Z P K X B X Y A K

V F G T G D F Z O M O Y K E X L V G A

[1] Jules César (101 av. JC–44 av. JC).

[2] Vigénère (1523–1596).

3. Processus MIAS : (clef K = PHILON)

B D L H B N N H O T C R B Z S L N T B P G

D W L P F M D J N F R S V W Z F H O F J N

H T E L X N Z H F F W T B P N H V V H L S

L W L P X E L N V B H J H O V H X I T

4. À la manière de Jefferson[3] **:** (clef K = NEPER, 11)

C W D H D Y L U V I S U Y P U L W N U E S

Y Y O Q B P C U Q Z O Y G U K R H V J P D

N L E L O U P Q P J Y W H M S Y A Y E X Y

Q U J D W R D R L Y Q T P D C W F Y V

5. À la manière de Jefferson (bis) : (clef K = NEPER, 11)

Q Q V H P Y Z A F S K U S R U L Q B U A K

M S G C F R K U C J G S W U A N N F D D P

B Z A L G A R C D D S Q H W Y S I M M B S

C U P P W N P Z Z S C J D P K Q L Y F

[3] Thomas Jefferson (1743–1826).

Décodons un peu

Voici trois messages que nous avons cryptés en utilisant les mêmes processus que ceux donnés ci-dessus. Pour chacun, nous vous donnons la clef et la méthode. Pouvez-vous les décrypter ?

1. À la manière de Vigénère : (clef K = VANDERMONDE)

M V S N F A Z T O J F E S S G T F A P W X W A V B

R T E O G S Y Y E M S E Z P F P U I X E N A S W L

R A O V H D J A I I W

2. Processus MIAS : (clef K = GAUSS)

F E D V Q A R A M Q B E X G P D A Q Y D I E D S O

J A X R Q F E B S X K S R Q R A N D S I L A H Q W

B E R S C I O M Q P V I A

3. Processus MIAS : (clef K = ZERMELO)

Z S F M A T J Z A D M S T Y Z Z R Z Y J J Z B V M L

J W Z Y D M E F W Z W N M Y F W Z V L M Q T Q Z V

Cryptosystème à clef publique : l'exemple du système RSA.[4]

On se donne deux grands nombres premiers p et q et on pose $n = pq$.
Soit $\lambda = (p-1)(q-1)$. On choisit un entier m assez grand tel que m soit étranger à λ.
D'après l'identité de Bezout, il existe des entiers u et v tels que :

$$um - \lambda v = 1.$$

On s'impose de plus $0 < u < \lambda$.
La clef publique sera le couple $(u; n)$. La clef secrète sera m.

Algorithmes de codage et de décodage :

- On numérise le message (alphabet décimal).
- On partage la succession de chiffres en blocs de longueur ℓ fixe (ℓ est strictement inférieure au nombre de chiffres de n).
- Chaque bloc constitue un entier x que l'on va coder, grâce à la clef publique du récepteur, par $x^u \pmod n$; on obtient ainsi un nombre $y \pmod n$.
- Le récepteur décode, grâce à sa clef secrète, par $y^m \equiv x \pmod n$.

Pourquoi ça marche ?

$$\begin{aligned} x^{um} &\equiv x^{1+\lambda v} \pmod n \\ &\equiv x.\left(x^{\lambda}\right)^{v} \pmod n \end{aligned}$$

Or :

1. Si p ne divise pas x, d'après le petit théorème de Fermat, $x^{p-1} \equiv 1 \pmod p$, donc $x^{\lambda} \equiv 1 \pmod p$ et donc :
   (C.1) $$x^{um} \equiv x \pmod p.$$
2. Si p divise x, on a alors $x \equiv 0 \pmod p$, donc la relation (C.1) reste vraie. En résumé, pour tout x, $x^{um} \equiv x \pmod p$. De même :
   (C.2) $$x^{um} \equiv x \pmod q.$$

[4] Rivest, Shamir et Adleman, 1978.

Des relations (C.1) et (C.2), on déduit :

$$\begin{cases} x^{um} \equiv x \pmod{p} \\ x^{um} \equiv x \pmod{q} \end{cases} \iff \begin{cases} x^{um} = x + kp & (k \in \mathbb{Z}) \\ x^{um} = x + k'q & (k' \in \mathbb{Z}) \end{cases}$$
$$\implies kp = k'q$$

D'après le théorème de Gauss, il vient : p divise k'. Par conséquent, $x^{um} = x + k''pq$, donc :

$$x^{um} \equiv x \pmod{n}.$$

À vous de jouer

La clef publique étant (715; 513581), codez le message suivant par le processus RSA :

EUREKA

(l'usage des calculatrices programmables ou des ordinateurs est **indispensable**).

ANNEXE D.

Une autre présentation du crible d'Ératosthène

422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443			
421	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	444			
420	343	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	364	445			
419	342	273	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	292	365	446			
418	341	272	211	158	159	160	161	162	163	164	165	166	167	168	169	170	171	228	293	366	447			
417	340	271	210	157	112	113	114	115	116	117	118	119	120	121	122	123	172	229	294	367	448			
416	339	270	209	156	111	74	75	76	77	78	79	80	81	82	83	124	173	230	295	368	449			
415	338	269	208	155	110	73	44	45	46	47	48	49	50	51	84	125	174	231	296	369	450			
414	337	268	207	154	109	72	43	22	23	24	25	26	27	52	85	126	175	232	297	370	451			
413	336	267	206	153	108	71	42	21	8	9	10	11	28	53	86	127	176	233	298	371	452			
412	335	266	205	152	107	70	41	20	7	2	3	12	29	54	87	128	177	234	299	372	453			
411	334	265	204	151	106	69	40	19	6	5	4	13	30	55	88	129	178	235	300	373	454			
410	333	264	203	150	105	68	39	18	17	16	15	14	31	56	89	130	179	236	301	374	455			
409	332	263	202	149	104	67	38	37	36	35	34	33	32	57	90	131	180	237	302	375	456			
408	331	262	201	148	103	66	65	64	63	62	61	60	59	58	91	132	181	238	303	376	457			
407	330	261	200	147	102	101	100	99	98	97	96	95	94	93	92	133	182	239	304	377	458			
406	329	260	199	146	145	144	143	142	141	140	139	138	137	136	135	134	183	240	305	378	459			
405	328	259	198	197	196	195	194	193	192	191	190	189	188	187	186	185	184	241	306	379	460			
404	327	258	257	256	255	254	253	252	251	250	249	248	247	246	245	244	243	242	307	380	461			
403	326	325	324	323	322	321	320	319	318	317	316	315	314	313	312	311	310	309	308	381	462			
402	401	400	399	398	397	396	395	394	393	392	391	390	389	388	387	386	385	384	383	382	463			
485	484	483	482	481	480	479	478	477	476	475	474	473	472	471	470	469	468	467	466	465	464			

ANNEXE D.

ANNEXE E.

Table des nombres premiers inférieurs à 2000

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999							

ANNEXE E.

ANNEXE F.

Bibliographie.

[1] ACHACHE et RICHARD. *Mathématiques du CAPES.* Hermann, Paris, 1976.

[2] BOUVIER, GEORGE, LE LIONNAIS. *Dictionnaire des mathématiques.* PUF, 1993.

[3] CHABERT. *Histoire d'algorithmes : du caillou à la puce.* Regards sur la science. Belin, 1994.

[4] FARAUT et KHALILI. *Arithmétique : cours, exercices et TP sur micro-ordinateur.* Ellipses, 1990.

[5] GRAS. *Anneaux (licence de mathématiques par correspondance).* CTU Besançon, 1991.

[6] GUINOT. *Les "resveries" de Fermat.* Arithmétique pour amateurs. ALÉAS Éditeur, 1992.

[7] GUINOT. *Pythagore, Euclide et toute la clique.* Arithmétique pour amateurs. ALÉAS Éditeur, 1992.

[8] MERCIER. Cryptographie classique et cryptographie publique à clé révélée. *Bulletin Vert de l'APMEP*, n° 406 : 568–581, Septembre–Octobre 1996.

[9] PICHON. *Théorie des ensembles, logique, les entiers.* Ellipses, 1989.

[10] PICHON. *Arithmétique, systèmes linéaires, structures.* Ellipses, 1992.

[11] QUEYSANNE et REVUZ. *Mathématique : Terminale CDE. Tome 1 : nombres–probabilités.* Collection Queysanne Revuz. Fernand Nathan, Paris, 1971.

I. Auteurs.

Duffaud, Brigitte ; Pétiard, François
Avec la participation du groupe Lycée de l'IREM de Franche-Comté.

II. Titre.

Arithmétique en Terminale S.

III. Caractéristiques de l'édition.

Édité par l'IREM de Franche-Comté à Besançon en 1998.
Format : A4 ; 90 pages.
ISBN : 2-909963-22-5

IV. Types de documents et supports.

Type : document pour l'enseignant.
Support : papier.

VI. Public visé.

Enseignant.
Niveau : Terminale Scientifique.
Âge : 17.

VII. Contenus.

Résumé : Cette brochure a été écrite à l'origine à l'intention des professeurs de lycée de l'académie de Besançon ayant assisté à un stage MAFPEN intitulé "Arithmétique en vue de l'enseignement de spécialité en Terminale S".
Le but de ce travail n'est pas de proposer des cours-types mais de rappeler les notions fondamentales d'arithmétique dans $\mathbb{Z}$ tout en les rattachant aux notions sous-jacentes d'arithmétique dans un anneau euclidien, principal ou factoriel.
Les leçons s'appuient chacune sur un point particulier de ces notions :

la leçon 1 donne le vocabulaire de la divisibilité commun à tout anneau commutatif intègre.

la leçon 2 s'attache à l'aspect "anneau euclidien" de $\mathbb{Z}$ (algorithme d'Euclide).

la leçon 3 s'attache à l'aspect "anneau principal" de $\mathbb{Z}$ (théorème de Bézout).

la leçon 4 s'attache à l'aspect "anneau factoriel" de $\mathbb{Z}$ (existence et unicité de la décomposition).

Le point de vue pédagogique adopté face à des élèves de Terminale S sera certainement différent de celui-ci.
Sont donnés en annexe quelques algorithmes permettant de programmer certains calculs sur calculatrice.
Des énoncés de travaux pratiques sont également fournis ; ils ne sont pas, *a priori*, à réinvestir tels quels en Terminale ; lors du stage, ils ont servi à appliquer et à développer les résultats énoncés dans les leçons et ont donné lieu à des calculs pratiques et à l'utilisation d'ordinateurs.
Bibliographie : page 89.
Mots-clés : algorithme, anneau, Archimède, arithmétique, base, Bézout, chinois, codage, congruences, cryptographie, décomposition, Diophante, divisibilité, Ératosthène, Euclide, euclidien, factoriel, Fermat, Gauss, nombres étrangers, nombre premier, numération, p.g.c.d., p.p.c.m., principal, travaux pratiques, Wilson.